Déploiement de téléphones IP Vocera dans l'infrastructure UWN

Contenu

Introduction

Ce document fournit des considérations de conception et des instructions de déploiement pour l'implémentation de la technologie VoceraMD Badge Voice over WLAN (VoWLAN) sur l'infrastructure de réseau sans fil unifié Cisco.

Note : Le support des produits Vocera doit être obtenu directement auprès des canaux de support Vocera. L'assistance technique Cisco n'est pas formée pour prendre en charge les problèmes liés à Vocera.

Ce guide est un complément au Guide de déploiement du contrôleur de réseau local sans fil Cisco et traite uniquement des paramètres de configuration spécifiques aux périphériques VoWLAN Vocera dans une architecture légère. Référez-vous à Déploiement de contrôleurs de réseau local sans fil Cisco 440X pour plus d'informations.

Conditions préalables

Conditions requises

Il est supposé que les lecteurs connaissent les termes et les concepts présentés dans Cisco IP Telephony SRND et Cisco Wireless LAN SRND. .

Guide de conception des communications unifiées sans fil : http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_wireless_uc.html

Cisco Unified Communications SRND basé sur Cisco Unified Communications Manager

7.x—http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_uc_mgr.html

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Résumé

Ce tableau récapitule les quatre fonctions clés et leur comportement au sein d'un réseau sans fil unifié Cisco.

	Contrôleur unique	Itinérance de couche 2 contrôleur à contrôleur	Itinérance de couche 3 contrôleur à contrôleur
Badge-to-Badge	Aucune configuration spéciale	Aucune configuration spéciale	Aucune configuration spéciale
Badge vers téléphone	Aucune configuration spéciale	Aucune configuration spéciale	Aucune configuration spéciale
Badge-to-Broadcast	Activer la multidiffusion du contrôleur	Activer la multidiffusion du contrôleur Désactiver Vocera VLAN IGMP-Snooping ou exécuter 4.0.206.0 ou version ultérieure	4.0.206.0 ou ultérieure
Emplacement du badge	Aucune configuration spéciale	Aucune configuration spéciale	Aucune configuration spéciale

Présentation du badge Vocera

Les badges de communication permettent de communiquer instantanément avec tout autre porteur de badge, ainsi qu'avec l'intégration d'un autocommutateur privé (PBX) et le suivi de l'emplacement des badges. L'utilisation d'un réseau sans fil 802.11b/g nécessite l'utilisation de la distribution de paquets monodiffusion multidiffusion et UDP avec des exigences limitées en matière de qualité de service (QoS) depuis la version 3.1 du logiciel Vocera Server (Build 1081).

Les fonctionnalités de cryptage sont WEP (Wired Equivalent Privacy) 64/128 bits, TKIP (Temporal Key Integrity Protocol), MIC (Message Integrity Check) et CKIP (Cisco Temporal Key Integrity Protocol), associées aux fonctionnalités d'authentification Open, WPA-PSK (Wi-Fi Protected Access-Pre-shared Key), PEAP (WPA-Protected Extensible Authentication Protocol) et LightAP LEAP (Extensible Authentication Protocol).

En appuyant sur un bouton, le serveur Vocera répond avec Vocera, qui est une invite à émettre des commandes telles que record, où (am I) /is..., call, play, **broadcast**, **messages**, etc. Le serveur Vocera fournit les services et/ou la configuration des appels nécessaires pour compléter la demande.

Le système de communication compatible 802.11b de Vocera utilise la compression vocale propriétaire et l'utilisation d'une plage de ports UDP. Le logiciel Vocera System s'exécute sur un serveur Windows qui gère la configuration des appels, la connexion des appels et les profils utilisateur. Ils se sont associés au logiciel de reconnaissance vocale et d'impression vocale Nuance 8.5 afin d'activer les communications vocales par badge. Vocera recommande un serveur Windows distinct pour exécuter le logiciel Vocera Telephony Solutions afin d'activer la connectivité de Plain Old Telephone Service (POTS) avec les badges.

Considérations sur la capacité des appels Vocera

Consultez la section Taille du réseau de ce document pour plus de détails.

Capacité du serveur de communications Vocera

Reportez-vous aux Spécifications du système de communication Vocera pour plus d'informations sur la matrice de dimensionnement du serveur Vocera.

La solution Vocera

Le badge Vocera utilise à la fois la transmission de paquets monodiffusion et multidiffusion pour fournir plusieurs fonctionnalités clés qui composent cette solution complète. Voici quatre des fonctionnalités essentielles qui reposent sur une livraison correcte des paquets. Vous y trouverez également une compréhension de base de la manière dont chaque fonction utilise le réseau sous-jacent pour la fourniture et la fonctionnalité.

- Badge to Badge Communications : lorsqu'un utilisateur Vocera appelle un autre utilisateur, le badge contacte d'abord le serveur Vocera, qui recherche l'adresse IP du badge de l'appelant et contacte l'utilisateur du badge pour lui demander s'il peut passer un appel. Si l'appelant accepte l'appel, le serveur Vocera avertit le badge appelant de l'adresse IP du badge appelé pour établir une communication directe entre les badges sans autre intervention du serveur. Toutes les communications avec le serveur Vocera utilisent le codec G.711 et toutes les communications de badge à badge utilisent un codec propriétaire Vocera.
- Badge Telephony Communication : lorsqu'un serveur de téléphonie Vocera est installé et configuré avec une connexion à un PBX, un utilisateur peut appeler des postes internes hors du PBX ou des lignes téléphoniques externes. Vocera permet aux utilisateurs de passer des appels en indiquant les numéros (cinq, six, trois, deux) ou en créant une entrée de carnet d'adresses dans la base de données Vocera pour la personne ou la fonction à ce numéro (par

exemple, pharmacie, maison, pizza), le serveur Vocera détermine le numéro appelé, soit en interceptant les numéros dans le poste, soit en recherchant le nom dans la base de données et en sélectionnant le numéro. Le serveur Vocera transmet ensuite ces informations au serveur de téléphonie Vocera qui se connecte au PBX et génère la signalisation téléphonique appropriée (par exemple, DTMF). Toutes les communications entre le badge et le serveur Vocera et le serveur Vocera et le serveur Vocera Telephony utilisent le codec G.711 sur UDP monodiffusion.

- Vocera Broadcast : un utilisateur de badge Vocera peut appeler et communiquer simultanément avec un groupe de porteurs de badges Vocera à l'aide de la commande Broadcast. Lorsqu'un utilisateur diffuse vers un groupe, le badge de l'utilisateur envoie la commande au serveur Vocera qui recherche ensuite les membres d'un groupe, détermine quels membres du groupe sont actifs, attribue une adresse de multidiffusion à utiliser pour cette session de diffusion et envoie un message au badge de chaque utilisateur actif lui demandant de rejoindre le groupe de multidiffusion avec l'adresse de multidiffusion attribuée.
- Fonction d'emplacement du badge : le serveur Vocera garde une trace du point d'accès auquel chaque badge actif est associé, car chaque badge envoie un message de maintien en vie de 30 secondes au serveur avec le BSSID associé. Cela permet au système Vocera d'estimer approximativement l'emplacement d'un utilisateur de badge. Cette fonction a un degré de précision relativement faible car un badge peut ne pas être associé au point d'accès auquel il est le plus proche.

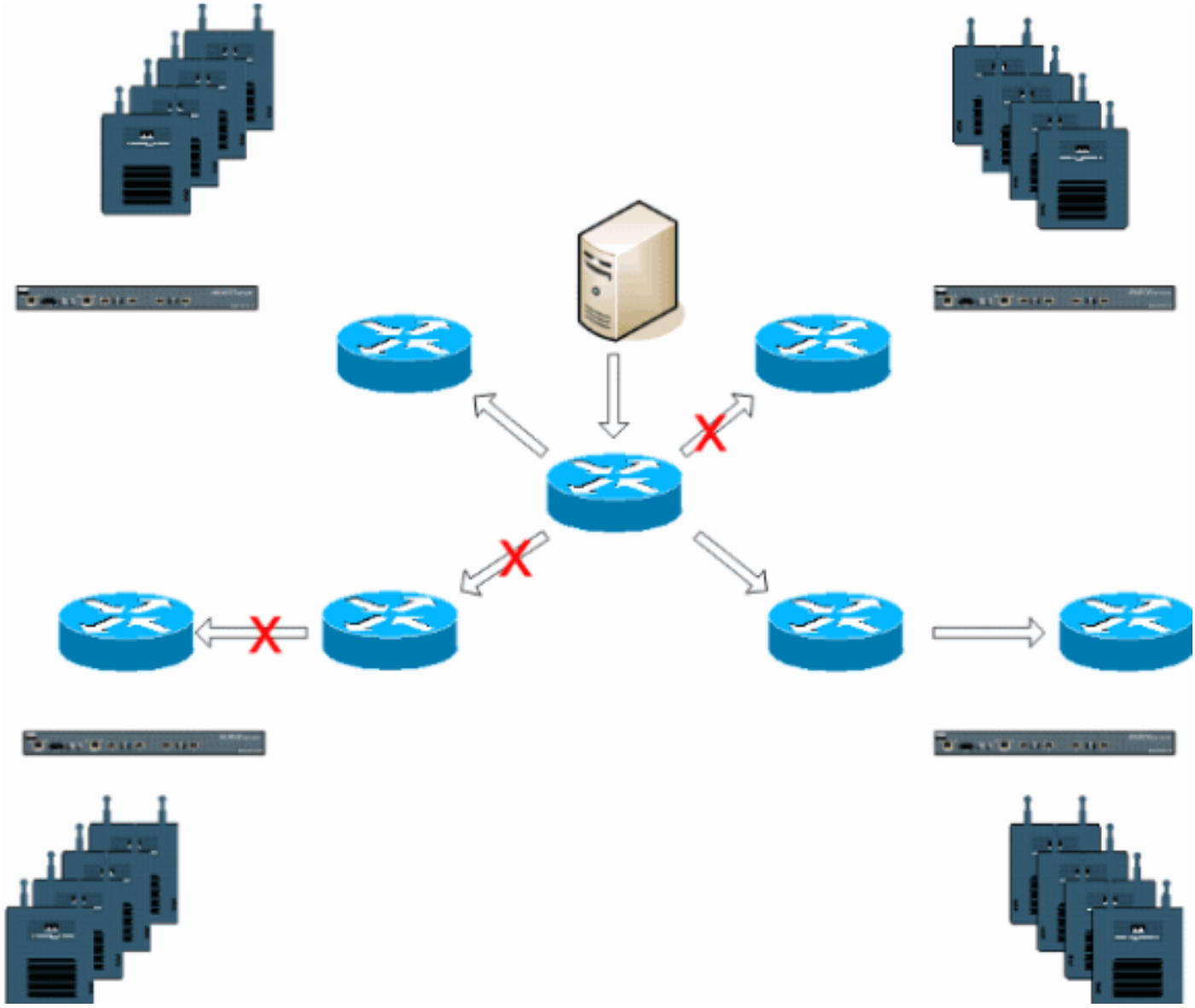
Planification de l'infrastructure de Vocera

Le livre blanc Vocera Vocera Infrastructure Planning Guide , décrit les exigences minimales de l'étude de site qui montrent que le badge doit avoir une intensité de signal minimale de -65 dBm, un rapport signal/bruit supérieur à 25 db et un chevauchement approprié des points d'accès et une séparation des canaux. Bien que les badges utilisent une antenne directionnelle omnidirectionnelle similaire comme bloc-notes utilisé pour une étude de site, ils ne simulent pas très bien le comportement du badge, étant donné les effets des porteurs sur la puissance du signal. Compte tenu de cette exigence unique et de ce comportement du périphérique émetteur, l'utilisation de l'architecture Cisco et de la gestion des ressources radio est idéale pour s'assurer qu'il n'y a pas de caractéristiques de site de radiofréquence inhabituelles.

Le badge Vocera est un appareil à faible puissance, porté à côté du corps avec des capacités limitées de correction des erreurs de signal. Les exigences de Vocera dans ce document peuvent être facilement atteintes. Cependant, il peut devenir submergé s'il y a trop de SSID pour qu'il traite et permette au badge de fonctionner efficacement.

Présentation de l'architecture

Figure 1 : transmission et élongation multidiffusion générale avec protocole LWAPP (Lightweight Access Point Protocol) sans fil



Multidiffusion dans un déploiement LWAPP

Il est nécessaire de comprendre la multidiffusion dans un déploiement LWAPP pour déployer la fonction de diffusion Vocera. Ce document décrit plus loin les étapes essentielles pour activer la multidiffusion dans la solution basée sur un contrôleur. Il existe actuellement deux méthodes de distribution que le contrôleur LWAPP utilise pour transmettre la multidiffusion aux clients :

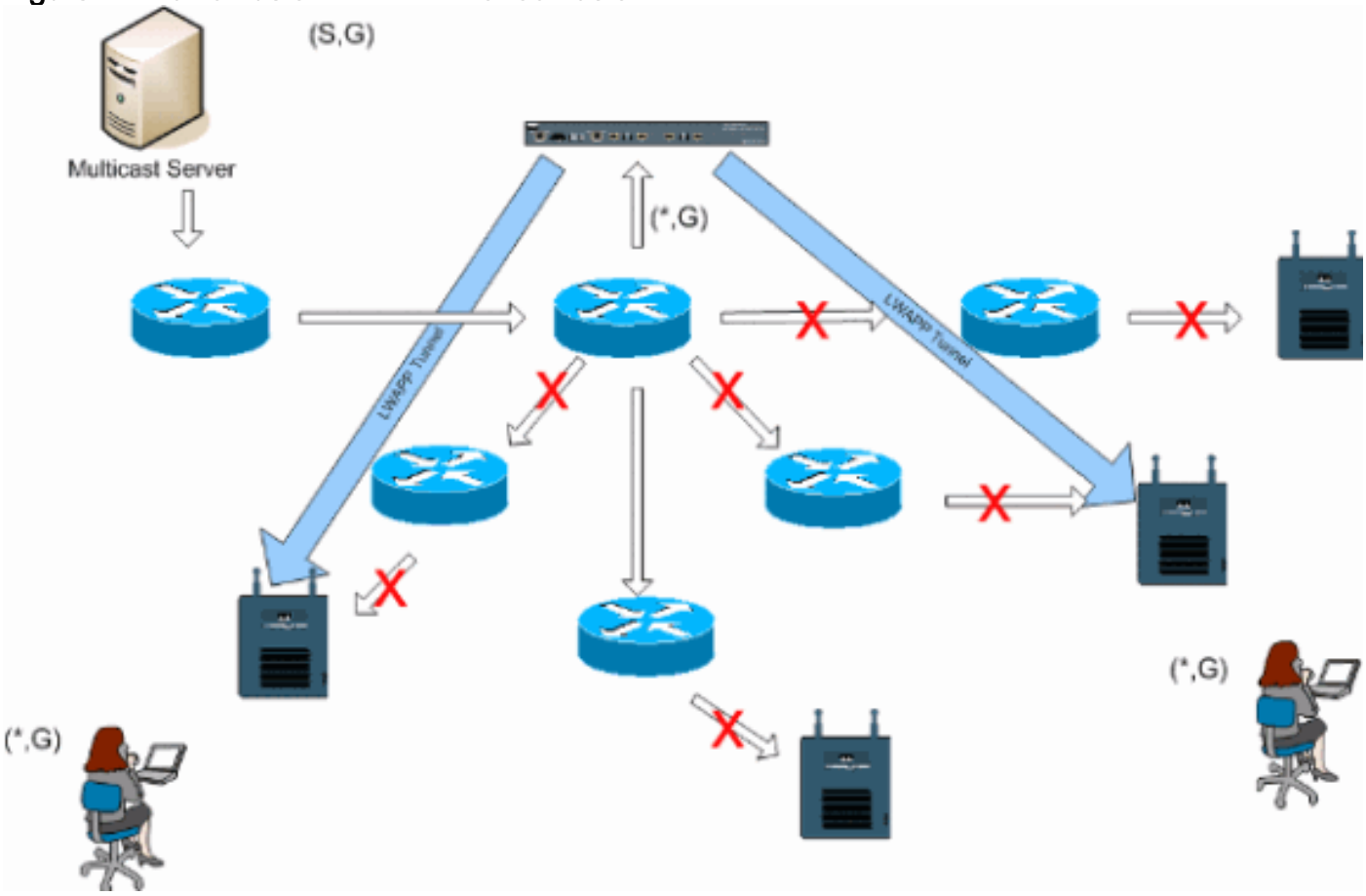
- Monodiffusion-multidiffusion
- Multicast-Multicast

Méthode de livraison monodiffusion-multidiffusion

La méthode de distribution monodiffusion-multidiffusion crée une copie de chaque paquet multidiffusion et la transmet à chaque point d'accès. Lorsqu'un client envoie une jointure multicast au réseau local sans fil, le point d'accès transfère cette jointure via le tunnel LWAPP au contrôleur. Le contrôleur relie cette jonction de multidiffusion à sa connexion réseau local directement connectée qui est le VLAN par défaut pour le WLAN associé du client. Lorsqu'un paquet de multidiffusion IP arrive du réseau au contrôleur, le contrôleur répliquera ce paquet avec un en-tête LWAPP pour chaque point d'accès qui a un client dans le domaine sans fil qui a rejoint ce groupe spécifique. Lorsque la source de multidiffusion est également un récepteur dans le domaine sans

fil, ce paquet est également dupliqué et renvoyé au même client qui a envoyé ce paquet. Pour les badges Vocera, il ne s'agit pas de la méthode de diffusion multicast préférée dans la solution de contrôleur LWAPP. La méthode de livraison monodiffusion fonctionne avec les petits déploiements. Cependant, en raison de la surcharge considérable sur le contrôleur de réseau local sans fil (WLC), il ne s'agit jamais de la méthode de diffusion multicast recommandée.

Figure 2 : multidiffusion LWAPP-monodiffusion



Remarque : si des VLAN de groupe AP sont configurés et qu'une jointure IGMP est envoyée par un client via le contrôleur, elle est placée sur le VLAN par défaut du WLAN sur lequel le client est connecté. Par conséquent, il se peut que le client ne reçoive pas ce trafic de multidiffusion à moins qu'il ne soit membre de ce domaine de diffusion par défaut.

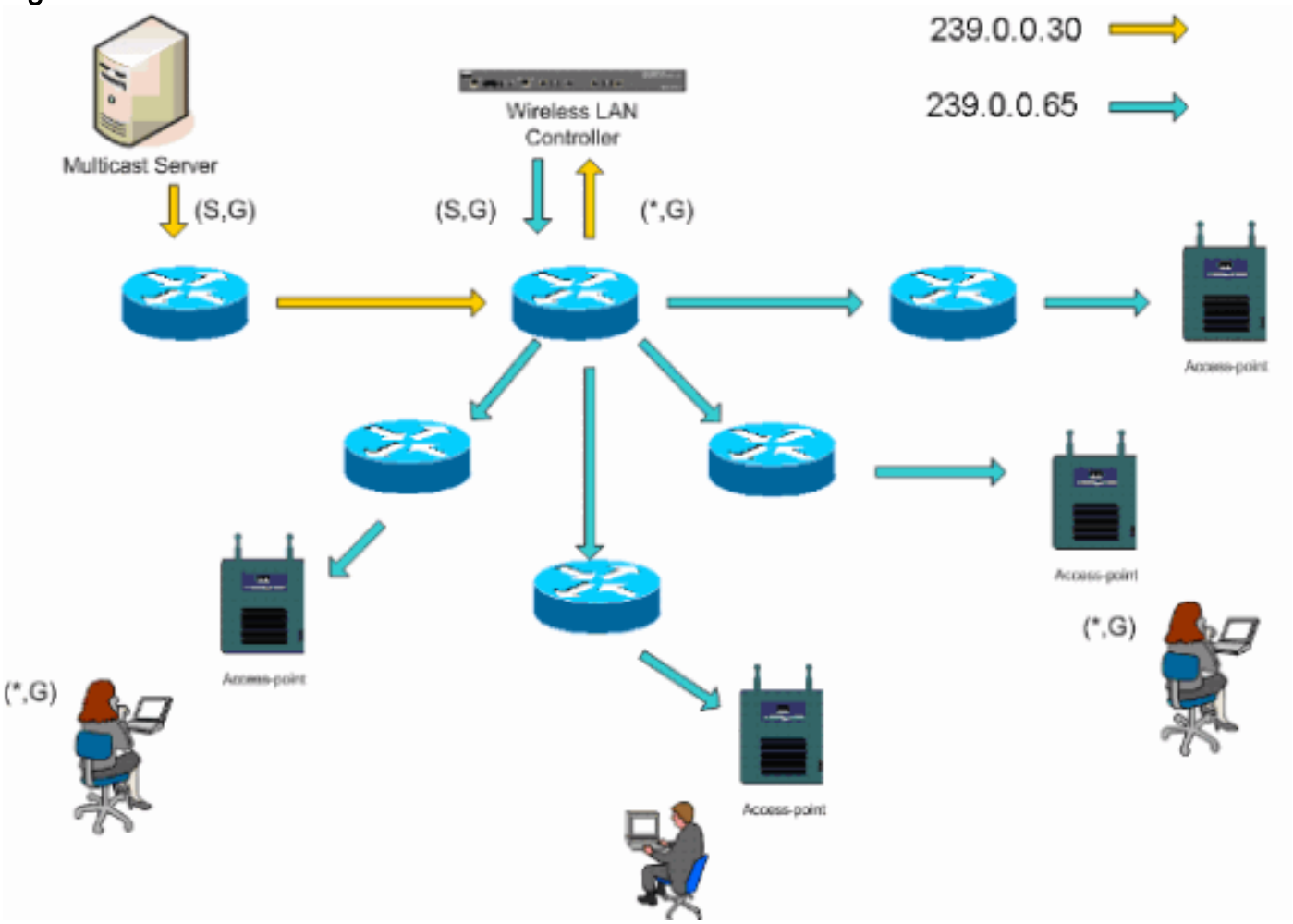
Méthode de transmission multidiffusion

La méthode de distribution multicast-multicast ne nécessite pas que le contrôleur réplique chaque paquet multicast reçu. Le contrôleur est configuré pour une adresse de groupe de multidiffusion non utilisée dont chaque point d'accès devient membre. Avec la Figure 3, le groupe de multidiffusion défini du WLC au point d'accès est 239.0.0.65. Lorsqu'un client envoie une jointure multicast au WLAN, le point d'accès transfère cette jointure via le tunnel LWAPP au contrôleur. Le contrôleur transfère ce protocole de couche liaison sur sa connexion réseau local directement connectée qui est le VLAN par défaut pour le WLAN associé du client. Le routeur qui est local au contrôleur ajoute ensuite cette adresse de groupe de multidiffusion à cette interface pour l'entrée de transfert (*, G). Avec la Figure 3, l'exemple de jointure multicast a été envoyé au groupe multicast 239.0.0.30. Lorsque le réseau transfère maintenant le trafic de multidiffusion, l'adresse de multidiffusion 239.0.0.30 est transférée au contrôleur. Le contrôleur encapsule ensuite le paquet de multidiffusion dans un paquet de multidiffusion LWAPP adressé à l'adresse du groupe de multidiffusion (par exemple, 239.0.0.65) qui est configuré sur le contrôleur et transféré au réseau. Chaque point d'accès du contrôleur reçoit ce paquet en tant que membre du groupe de

multidiffusion des contrôleurs. Le point d'accès transfère ensuite le paquet de multidiffusion client/serveur (par exemple, 239.0.0.30) en tant que diffusion au WLAN/SSID identifié dans le paquet de multidiffusion LWAPP.

Remarque : si vous ne configurez pas correctement votre réseau de multidiffusion, vous pourriez finir par recevoir les paquets de multidiffusion d'un autre point d'accès du contrôleur. Si le premier contrôleur doit fragmenter ce paquet de multidiffusion, le fragment est transféré au réseau et chaque point d'accès doit passer du temps à supprimer ce fragment. Si vous autorisez tout le trafic, tel qu'un trafic provenant de la plage de multidiffusion 224.0.0.x, il est également encapsulé et ensuite transféré par chaque point d'accès.

Figure 3 : multidiffusion LWAPP



Configuration de la multidiffusion des routeurs et des commutateurs

Ce document n'est pas un guide de configuration de multidiffusion réseau. Référez-vous à Configuration du routage de multidiffusion IP pour un article complet sur l'implémentation. Ce document couvre les bases permettant d'activer la multidiffusion dans votre environnement réseau.

Activer le routage multidiffusion IP

Le routage multicast IP permet au logiciel Cisco IOS® de transférer des paquets multicast. La commande de configuration globale **ip multicast-routing** est requise pour permettre au multicast de fonctionner dans n'importe quel réseau compatible multicast. La commande **ip multicast-routing** doit être activée sur tous les routeurs de votre réseau entre les WLC et leurs points d'accès

respectifs.

```
Router(config)#ip multicast-routing
```

Activer PIM sur une interface

Ceci active l'interface de routage pour le fonctionnement du protocole IGMP (Internet Group Management Protocol). Le mode PIM (Protocol Independent Multicast) détermine comment le routeur remplit sa table de routage de multidiffusion. L'exemple fourni ici n'exige pas que le point de rendez-vous (RP) soit connu pour le groupe de multidiffusion. Par conséquent, le mode dense-clairsemé est le plus souhaitable étant donné la nature inconnue de votre environnement de multidiffusion. Il ne s'agit pas d'une recommandation de multidiffusion à configurer pour fonctionner bien que l'interface de couche 3 directement connectée à votre contrôleur doive être activée par PIM pour que la multidiffusion fonctionne. Toutes les interfaces entre vos WLC et leurs points d'accès respectifs doivent être activées.

```
Router(config-if)#ip pim sparse-dense-mode
```

Désactiver la surveillance IGMP VLAN du commutateur

La surveillance IGMP permet à un réseau commuté dont la multidiffusion est activée de limiter le trafic aux ports de commutation dont les utilisateurs veulent que la multidiffusion soit visible tout en élaguant les paquets de multidiffusion des ports de commutation qui ne souhaitent pas voir le flux de multidiffusion. Dans un déploiement Vocera, il peut être indésirable d'activer CGMP ou IGMP Snooping sur le port de commutation en amont vers le contrôleur avec des versions logicielles antérieures à 4.0.206.0.

L'itinérance et la multidiffusion ne sont pas définies avec un ensemble de conditions permettant de vérifier que le trafic de multidiffusion peut suivre un utilisateur abonné. Bien que le badge client soit conscient qu'il a circulé, il ne transfère pas une autre jointure IGMP pour s'assurer que l'infrastructure réseau continue à acheminer le trafic de multidiffusion (diffusion Vocera) vers le badge. En même temps, le point d'accès LWAPP n'envoie pas de requête multicast générale au client itinérant pour demander cette jointure IGMP. Avec une conception de réseau Vocera de couche 2, la désactivation de la surveillance IGMP permet de transférer le trafic à tous les membres du réseau Vocera, quel que soit l'endroit où ils se déplacent. Cela garantit que la fonctionnalité de diffusion Vocera fonctionne indépendamment de l'endroit où le client se déplace. Désactiver la surveillance IGMP globalement est une tâche très indésirable. Il est recommandé que la surveillance IGMP ne soit désactivée que sur le VLAN Vocera directement connecté à chaque WLC.

Référez-vous à Configuration de IGMP Snooping pour plus d'informations.

```
Router(config)#interface vlan 150
Router(config-if)#no ip igmp snooping
```

Améliorations de la multidiffusion dans les versions 4.0.206.0 et ultérieures

Avec la version 4.0.206.0, Cisco introduit une requête IGMP pour permettre aux utilisateurs de se déplacer au niveau de la couche 2 en envoyant une requête IGMP générale lorsque cela se

produit. Le client répond ensuite avec le groupe IGMP dont il est membre et qui est relié au réseau câblé comme décrit précédemment dans ce document. Lorsqu'un client se déplace vers un contrôleur qui n'a pas de connectivité de couche 2, ou une itinérance de couche 3, le routage synchrone est ajouté pour les paquets source de multidiffusion. Lorsqu'un client qui a terminé une route de couche 3 génère un paquet de multidiffusion à partir du réseau sans fil, le contrôleur étranger encapsule ce paquet dans le tunnel IP Ethernet over IP (EoIP) du contrôleur d'ancrage. Le contrôleur d'ancrage le transmet ensuite aux clients sans fil associés localement et le raccorde au réseau câblé où il est routé à l'aide des méthodes de routage multicast normales.

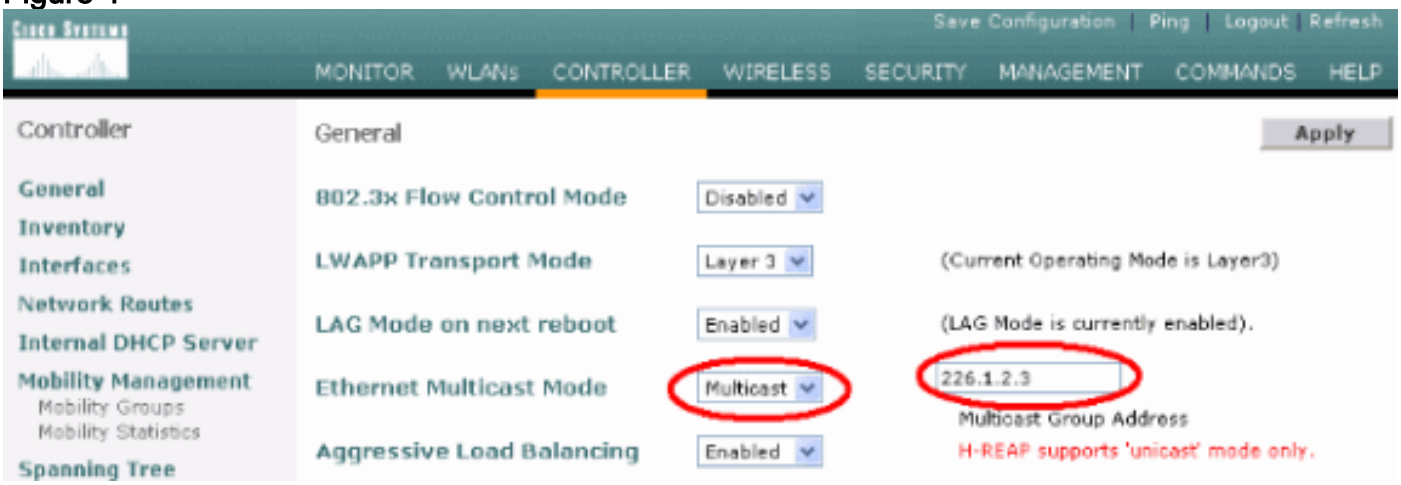
Scénarios de déploiement

Ces trois scénarios de déploiement couvrent les meilleures pratiques et les paramètres de conception pour aider à un déploiement réussi du badge Vocera :

- Déploiement d'un contrôleur unique
- Déploiement de plusieurs contrôleurs de couche 2
- Déploiement de plusieurs contrôleurs de couche 3

Il est essentiel de comprendre comment les fonctionnalités du badge Vocera interagissent dans un environnement MAC partagé LWAPP. Dans tous les scénarios de déploiement, la multidiffusion doit être activée et l'équilibrage de charge agressif doit être désactivé. Tous les réseaux locaux sans fil de badge doivent être contenus dans le même domaine de diffusion sur l'ensemble de votre réseau.

Figure 4



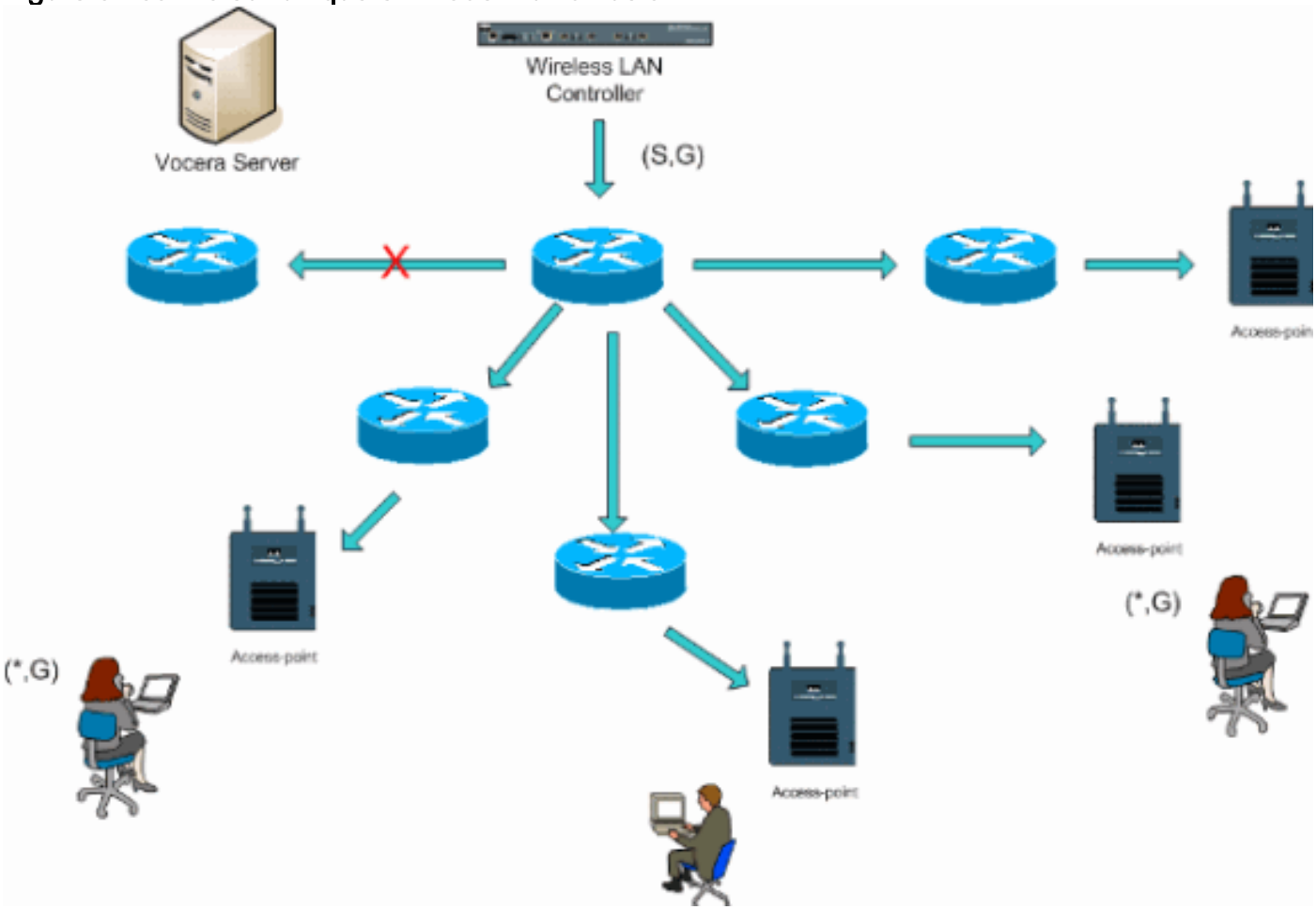
Déploiement d'un contrôleur unique

Il s'agit du scénario de déploiement le plus simple. Il vous permet de déployer la solution Vocera Badge avec peu de problèmes de déploiement. Votre réseau doit être activé pour le routage de multidiffusion IP uniquement pour permettre aux points d'accès de recevoir les paquets de multidiffusion LWAPP. Si nécessaire, vous pouvez limiter la complexité de la multidiffusion réseau en configurant tous les routeurs et commutateurs avec le groupe de multidiffusion des contrôleurs.

Avec la multidiffusion configurée globalement sur le contrôleur, le SSID approprié, les paramètres de sécurité et tous les points d'accès ont enregistré la solution Vocera Badge et toutes ses fonctions fonctionnent comme prévu. Avec la fonction de diffusion Vocera, un utilisateur se déplace et le trafic de multidiffusion suit comme prévu. Aucun paramètre supplémentaire n'est nécessaire pour permettre à cette solution de fonctionner correctement.

Lorsqu'un badge Vocera envoie un message de multidiffusion, comme il le fait avec la diffusion Vocera, il est transféré au contrôleur. Le contrôleur encapsule ensuite ce paquet de multidiffusion dans un paquet de multidiffusion LWAPP. L'infrastructure réseau transfère ce paquet à chaque point d'accès connecté à ce contrôleur. Lorsque le point d'accès reçoit ce paquet, il examine l'en-tête de multidiffusion LWAPP pour déterminer à quel WLAN/SSID il diffuse ensuite ce paquet.

Figure 5 : contrôleur unique en mode multidiffusion

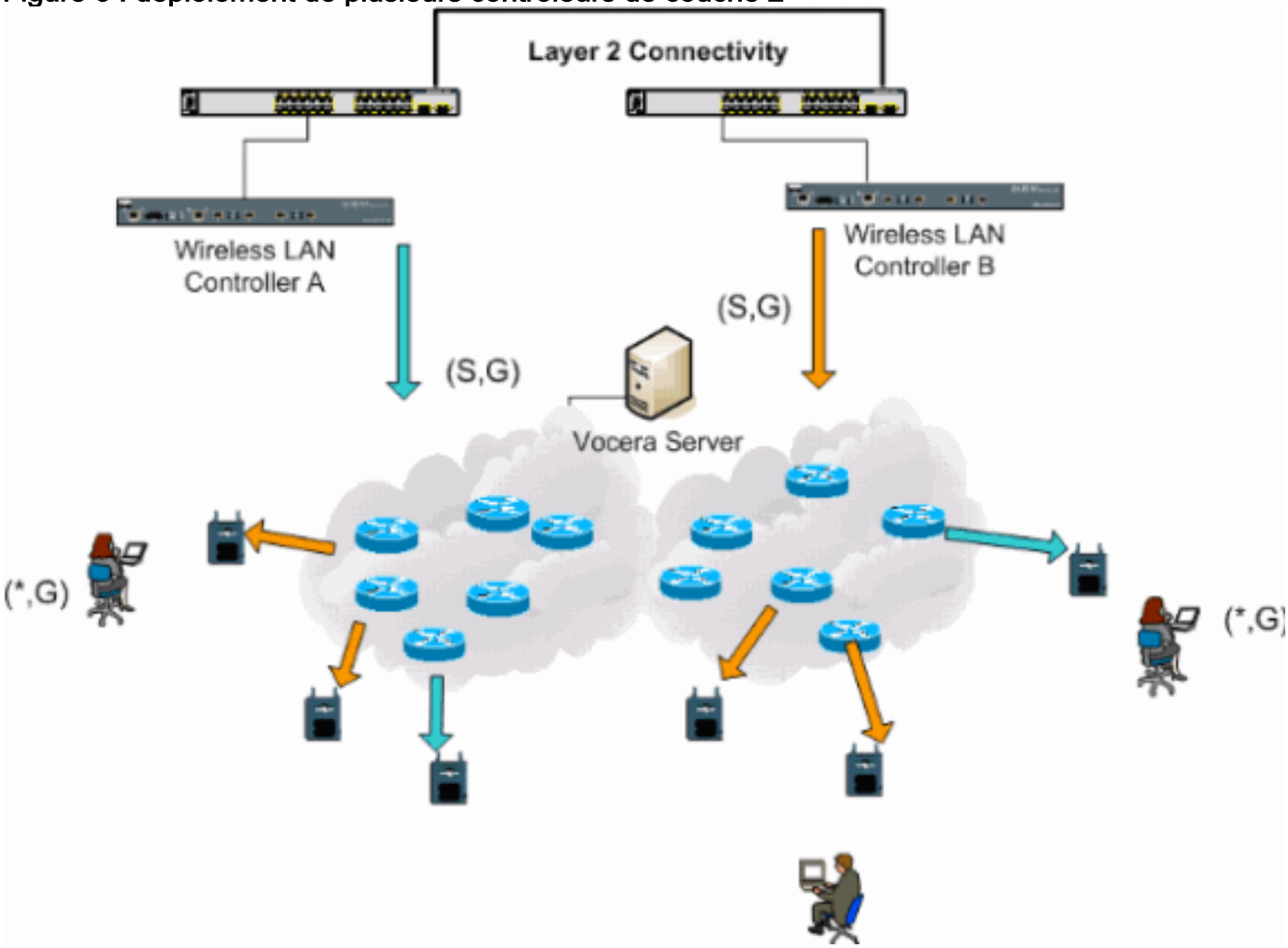


Déploiement de plusieurs contrôleurs de couche 2

Plusieurs contrôleurs doivent tous avoir une connectivité entre eux via le même domaine de diffusion de couche 2. Les deux contrôleurs sont configurés pour la multidiffusion comme indiqué, en utilisant les mêmes groupes de multidiffusion de point d'accès sur chaque contrôleur pour limiter la fragmentation. En supposant que ce domaine de diffusion de couche 2 est connecté via un commutateur commun ou un ensemble commun de commutateurs, la surveillance CGMP/IGMP sur ces commutateurs doit être désactivée pour ce VLAN unique ou exécuter le logiciel WLC 4.0.206.0 ou ultérieur. Avec la fonction de diffusion Vocera et une itinérance utilisateur d'un point d'accès sur un contrôleur à un point d'accès sur un contrôleur différent, il n'y a aucun mécanisme pour que les jointures IGMP soient transférées au nouveau port de couche 2 pour que la surveillance IGMP fonctionne. Sans qu'un paquet IGMP atteigne le commutateur CGMP ou IGMP en amont, le groupe de multidiffusion spécifié n'est pas transféré au contrôleur et n'est donc pas reçu par le client. Dans certains cas, cela peut fonctionner, si un client qui fait partie du même groupe de diffusion Vocera a déjà envoyé ce paquet IGMP avant que le client itinérant ne se déplace sur le nouveau contrôleur Avec les avantages de la version 4.0.206.0, un client qui se déplace vers un autre contrôleur en tant que route de couche 2 reçoit une requête IGMP générale immédiatement après l'authentification. Le client doit alors répondre aux groupes intéressés et le nouveau contrôleur est ensuite relié au commutateur connecté localement. Cela permet d'exploiter les avantages d'IGMP et CGMP sur vos commutateurs en amont.

Vous pouvez créer des SSID de badge supplémentaires et des domaines de couche 2 pour des réseaux de badge distincts, à condition que votre réseau soit configuré pour transmettre le trafic de multidiffusion de manière appropriée. En outre, chaque domaine de diffusion de couche 2 Vocera créé doit exister partout où un contrôleur est connecté au réseau afin de ne pas interrompre la multidiffusion.

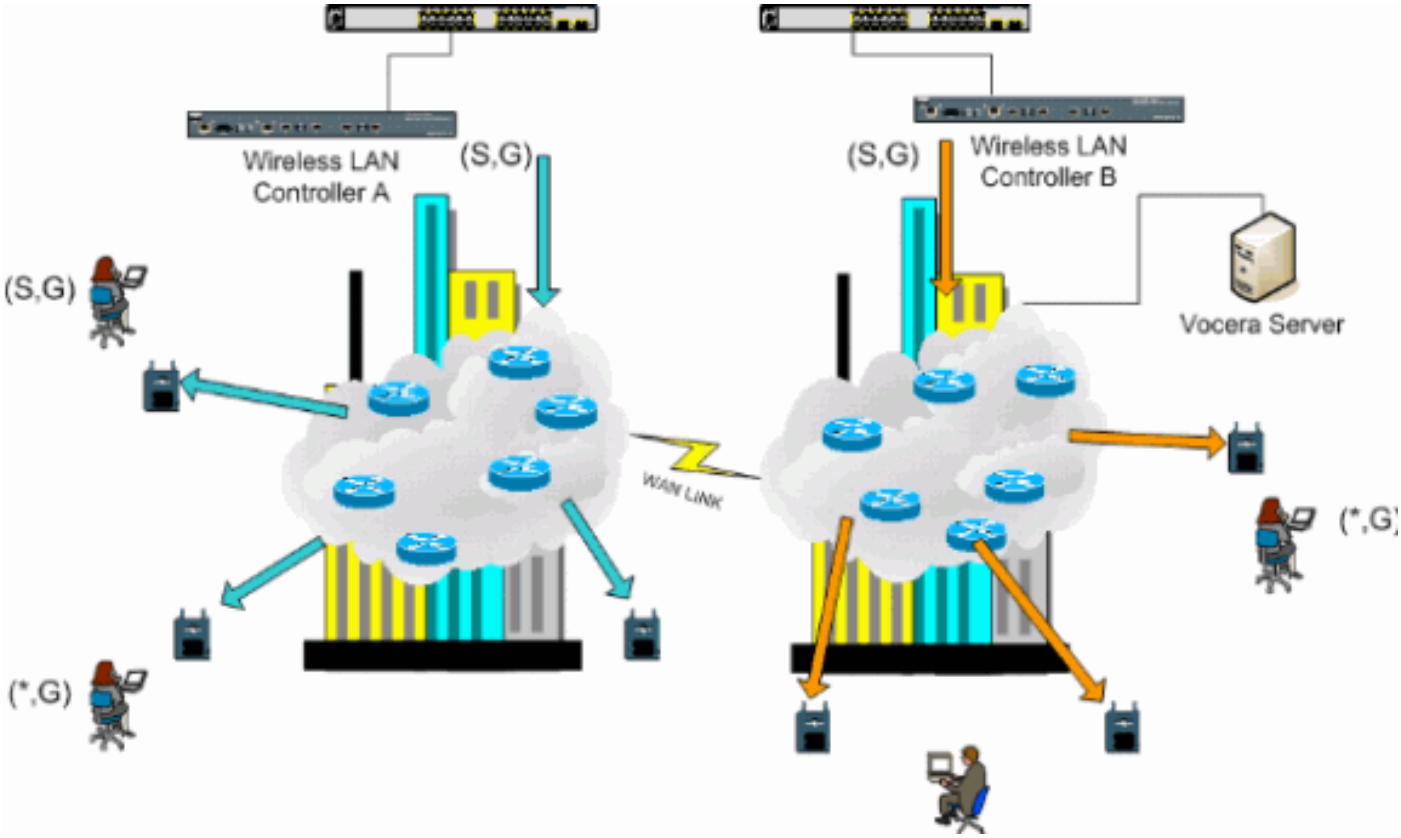
Figure 6 : déploiement de plusieurs contrôleurs de couche 2



Déploiement de plusieurs contrôleurs de couche 3

La stratégie de déploiement de l'itinérance de couche 3 ne doit être utilisée qu'avec l'itinérance contrôleur-contrôleur avec le logiciel WLC version 4.0.206.0 ou ultérieure. Si un client qui a été connecté au groupe de diffusion Vocera et reçoit le flux de multidiffusion approprié et se déplace vers un autre contrôleur en tant que itinérance de couche 3 avec l'itinérance de couche 3 LWAPP configurée, il est interrogé pour les groupes de multidiffusion intéressés. Le client, lorsqu'il effectue une source vers le même groupe de diffusion Vocera, reçoit ces paquets au contrôleur d'ancrage via le tunnel EoIP et les achemine via des méthodes de routage multicast normales.

Figure 7 : Déploiement de plusieurs contrôleurs de couche 3



Déploiements VoWLAN : Recommandations de Cisco

Les réseaux de téléphonie IP sans fil nécessitent une planification RF minutieuse. Il est souvent nécessaire d'effectuer une analyse approfondie du site vocal pour déterminer les niveaux de couverture sans fil appropriés et identifier les sources d'interférence. Le positionnement des points d'accès et la sélection des antennes peuvent être grandement simplifiés grâce aux résultats d'une étude de site vocal valide. La plus importante considération est la puissance de transmission du téléphone sans fil. Idéalement, le téléphone apprend la puissance de transmission du point d'accès et adapte sa puissance de transmission à celle du point d'accès.

Bien que la majorité des réseaux sans fil actuels soient déployés après une étude approfondie du site RF, ils sont réalisés en gardant également à l'esprit le service de données. Les téléphones VoWLAN ont probablement des caractéristiques d'itinérance et des exigences de couverture différentes de celles d'une carte WLAN classique pour un client mobile tel qu'un ordinateur portable. Par conséquent, il est souvent recommandé d'effectuer une étude de site supplémentaire pour la voix afin de se préparer aux exigences de performances de plusieurs clients VoWLAN. Cette enquête supplémentaire permet de régler les points d'accès pour s'assurer que les téléphones VoWLAN disposent d'une couverture RF et d'une bande passante suffisantes pour fournir une qualité vocale adéquate.

Pour plus d'informations sur les considérations de conception RF, reportez-vous au chapitre sur les considérations de conception de radiofréquence WLAN du Guide de conception de LAN sans fil Cisco, disponible à l'adresse http://cisco.com/go/srnd.

Recommandations pour les bâtiments, hôpitaux et entrepôts à plusieurs étages

Tenez compte des facteurs répertoriés dans cette section lorsque vous effectuez une enquête sur les bâtiments, les hôpitaux et les entrepôts à plusieurs étages.

Méthodes de construction et matériaux

De nombreux aspects de la construction du bâtiment sont inconnus ou cachés dans l'étude de site, vous devrez peut-être donc obtenir ces informations auprès d'autres sources (telles que les dessins architecturaux). Parmi les méthodes et matériaux de construction typiques qui influent sur la portée et la zone de couverture des points d'accès, on peut citer le film métallique sur le verre de fenêtre, le verre plombé, les parois en acier, les sols et les murs en ciment avec renfort en acier, l'isolation à dos de feuille, les puits d'escalier et les puits d'ascenseur, les tuyauteries et accessoires de plomberie, et bien d'autres.

Inventaire

Divers types d'inventaire peuvent affecter la plage RF, en particulier ceux qui ont une forte teneur en acier ou en eau. Parmi les produits à surveiller figurent les boîtes en carton, les aliments pour animaux de compagnie, la peinture, les produits pétroliers, les pièces de moteur, etc.

Niveaux de stock

Assurez-vous d'effectuer une analyse de site aux niveaux de stock les plus élevés ou en période d'activité la plus élevée. Un entrepôt au niveau de stockage de 50 % a une empreinte RF très différente de celle du même entrepôt au niveau de stock de 100 %.

Niveaux d'activité

De même, une zone de bureau en dehors des heures de bureau (sans personne) a une empreinte RF différente de la même zone pleine de personnes pendant la journée. Bien que de nombreuses parties de l'étude de site puissent être effectuées sans occupation complète, il est essentiel de procéder à la vérification de l'étude de site et de modifier les valeurs clés au moment où l'emplacement est occupé. Plus les besoins d'utilisation sont élevés et la densité des utilisateurs élevée, plus il est important d'avoir une solution de diversité bien conçue. Lorsque plus d'utilisateurs sont présents, plus de signaux sont reçus sur le périphérique de chaque utilisateur. Les signaux supplémentaires provoquent plus de conflits, plus de points nuls et plus de distorsion multichemin. La diversité des points d'accès (antennes) contribue à réduire ces conditions.

Bâtiments à plusieurs étages

Gardez à l'esprit ces directives lorsque vous effectuez une étude de site pour un bâtiment de bureau type :

- L'ascenseur bloque et reflète les signaux RF.
- Les salles d'approvisionnement avec les signaux d'absorption des stocks.
- Les bureaux intérieurs à parois dures absorbent les signaux RF.
- Les salles de pause (cuisines) peuvent produire des interférences de 2,4 GHz grâce à l'utilisation de fours à micro-ondes.
- Les laboratoires de test peuvent produire des interférences 2,4 GHz ou 5 GHz, créant ainsi une distorsion multichemin et des ombres RF.
- Les bicules ont tendance à absorber et à bloquer les signaux.
- Les salles de conférence nécessitent une couverture élevée des points d'accès car il s'agit de zones à forte utilisation.

Des précautions supplémentaires doivent être prises lorsque vous inspectez des installations à plusieurs étages. Les points d'accès situés à différents étages peuvent interférer les uns avec les autres aussi facilement que les points d'accès situés au même étage. Il est possible d'utiliser ce comportement à votre avantage lors d'une enquête. En utilisant des antennes à gain élevé, il peut être possible de pénétrer dans les sols et les plafonds et d'assurer la couverture aux étages supérieurs et inférieurs où le point d'accès est monté. Veillez à ne pas chevaucher les canaux entre les points d'accès situés à des étages différents ou les points d'accès situés au même étage. Dans les bâtiments multilocataires, il peut y avoir des problèmes de sécurité qui nécessitent l'utilisation de puissances de transmission plus faibles et d'antennes à gain plus faible pour empêcher les signaux de sortir des bureaux voisins.

Hôpitaux

Le processus d'enquête d'un hôpital est sensiblement le même que celui d'une entreprise, mais la disposition d'un établissement hospitalier tend à différer de ces façons :

- Les bâtiments hospitaliers ont tendance à passer par de nombreux projets de reconstruction et d'agrandissement. Chaque construction supplémentaire est susceptible d'avoir différents matériaux de construction avec différents niveaux d'atténuation.
- La pénétration des signaux dans les murs et les sols des zones de patients est généralement minime, ce qui contribue à créer des micro-cellules et des variations de trajets multiples.
- Le besoin de bande passante augmente avec l’utilisation croissante d’appareils d’échographie WLAN et d’autres applications d’imagerie portatives. Le besoin de bande passante augmente avec l'ajout de la voix sans fil.
- Les cellules de soins de santé sont petites et l'itinérance transparente est essentielle, en particulier pour les applications vocales.
- Le chevauchement des cellules peut être élevé, tout comme la réutilisation des canaux.
- Plusieurs types de réseaux sans fil peuvent être installés dans les hôpitaux. Cela inclut les équipements non 802.11 2,4 GHz. Cet équipement peut provoquer des conflits avec d'autres réseaux 2,4 GHz.
- Les antennes murales de raccordement de diversité et les antennes omnidirectionnelles montées au plafond sont populaires, mais gardez à l'esprit que la diversité est nécessaire.

Entrepôts

Les entrepôts sont dotés de grands espaces ouverts qui contiennent souvent des racks de stockage élevés. Souvent, ces bâtis atteignent presque le plafond, où les points d'accès sont généralement placés. De tels racks de stockage peuvent limiter la zone couverte par le point d'accès. Dans ces cas, envisagez de placer des points d'accès à d'autres endroits que le plafond, comme les murs latéraux et les piliers de ciment. Tenez également compte de ces facteurs lorsque vous inspectez un entrepôt :

- Les niveaux d'inventaire affectent le nombre de points d'accès nécessaires. Testez la couverture avec deux ou trois points d'accès dans des emplacements estimés.
- Les chevauchements inattendus de cellules sont probablement dus à des variations de chemins multiples. La qualité du signal varie plus que la puissance de ce signal. Les clients peuvent s'associer et fonctionner mieux avec des points d'accès plus éloignés qu'avec des points d'accès voisins.
- Lors d'une étude, les points d'accès et les antennes ne sont généralement pas reliés par un

câble d'antenne. Mais dans un environnement de production, le point d'accès et l'antenne peuvent nécessiter des câbles d'antenne. Tous les câbles d'antenne entraînent une perte de signal. L'étude la plus précise comprend le type d'antenne à installer et la longueur du câble à installer. Un atténuateur est un bon outil à utiliser pour simuler le câble et sa perte.

L'inspection d'une installation de fabrication est similaire à l'inspection d'un entrepôt, sauf qu'il peut y avoir beaucoup plus de sources d'interférence RF dans une installation de fabrication. En outre, les applications d'une usine nécessitent généralement plus de bande passante que celles d'un entrepôt. Ces applications peuvent inclure l'imagerie vidéo et la voix sans fil. La distorsion multivoie est probablement le problème de performance le plus important dans une usine de fabrication.

Mécanismes de sécurité pris en charge

Outre le protocole WEP statique et le protocole LEAP Cisco pour l'authentification et le chiffrement des données, les badges Vocera prennent également en charge le protocole WPA-PEAP (MS-CHAP v2)/WPA2-PSK.

Considérations LEAP

Le protocole LEAP permet aux périphériques d'être mutuellement authentifiés (badge-to-access point-to-badge) en fonction d'un nom d'utilisateur et d'un mot de passe. Lors de l'authentification, une clé dynamique est utilisée entre le téléphone et le point d'accès pour chiffrer le trafic. Cependant, l'attaque du dictionnaire ASLEAP doit être prise en compte lorsque vous décidez d'utiliser LEAP comme solution de sécurité :

Référez-vous à Attaque par dictionnaire sur la vulnérabilité Cisco LEAP pour plus d'informations.

Si LEAP est utilisé, un serveur RADIUS compatible LEAP, tel que Cisco Access Control Server (ACS), est requis pour fournir l'accès à la base de données utilisateur. Cisco ACS peut stocker localement le nom d'utilisateur et le mot de passe ou accéder à ces informations à partir d'un répertoire Microsoft Windows NT externe. Lorsque vous utilisez LEAP, assurez-vous que des mots de passe forts sont utilisés sur tous les périphériques sans fil. Les mots de passe forts sont définis comme comportant entre 10 et 12 caractères et peuvent inclure des caractères majuscules et minuscules ainsi que des caractères spéciaux.

Puisque tous les badges utilisent le même mot de passe et qu'ils sont stockés dans le badge, Cisco vous recommande d'utiliser différents noms d'utilisateur et mots de passe sur les clients de données et les clients vocaux sans fil. Cette pratique permet de suivre et de dépanner les problèmes, ainsi que la sécurité. Bien qu'il soit possible d'utiliser une base de données externe (hors ACS) pour stocker les noms d'utilisateur et les mots de passe des badges, Cisco ne recommande pas cette pratique. Étant donné que l'ACS doit être interrogé chaque fois que le badge se déplace entre les points d'accès, le délai imprévisible pour accéder à une base de données hors ACS peut provoquer un retard excessif et une mauvaise qualité vocale.

Infrastructure réseau sans fil

Le réseau de téléphonie IP sans fil, tout comme un réseau de téléphonie IP câblé, nécessite une planification minutieuse de la configuration VLAN, du dimensionnement du réseau, du transport multidiffusion et des choix d'équipement. Pour les réseaux de téléphonie IP câblés et sans fil, les VLAN voix et données séparés constituent souvent le moyen le plus efficace de déploiement

suggéré pour garantir une bande passante réseau suffisante et une facilité de dépannage.

VLAN voix, données et voix

Les VLAN fournissent un mécanisme de segmentation des réseaux en un ou plusieurs domaines de diffusion. Les VLAN sont particulièrement importants pour les réseaux de téléphonie IP, où la recommandation type est de séparer le trafic voix et données en différents domaines de couche 2. Cisco vous recommande de configurer des VLAN distincts pour les badges Vocera à partir d'autres trafics voix et données : un VLAN natif pour le trafic de gestion de point d'accès, un VLAN de données pour le trafic de données, un VLAN voix ou auxiliaire pour le trafic vocal et un VLAN pour les badges Vocera. Un VLAN voix distinct permet au réseau de tirer parti du marquage de couche 2 et assure la mise en file d'attente prioritaire au niveau du port du commutateur d'accès de couche 2. Cela garantit que la QoS appropriée est fournie pour différentes classes de trafic et aide à résoudre des problèmes tels que l'adressage IP, la sécurité et le dimensionnement du réseau. Les badges Vocera utilisent une fonction de diffusion qui utilise la multidiffusion pour transmettre. Ce VLAN commun garantit que lorsqu'un badge circule entre les contrôleurs, il reste une partie du groupe de multidiffusion. Ce dernier processus est traité en détail lorsque la multidiffusion est traitée plus loin dans ce document.

Dimensionnement du réseau

Le dimensionnement du réseau de téléphonie IP est essentiel pour garantir que la bande passante et les ressources nécessaires sont disponibles pour répondre aux demandes présentées par la présence du trafic vocal. En plus des directives habituelles de conception de téléphonie IP pour le dimensionnement de composants tels que les ports de passerelle RTPC, les transcodeurs, la bande passante WAN, etc., tenez également compte de ces problèmes 802.11b lorsque vous dimensionnez votre réseau de téléphonie IP sans fil. Les badges Vocera sont une application spécialisée qui étend le nombre de clients filaires au-delà de nos recommandations de déploiement habituelles.

Nombre de périphériques 802.11b par point d'accès

Cisco recommande de ne pas avoir plus de 15 à 25 périphériques 802.11b par point d'accès.

Nombre d'appels actifs par point d'accès

Vocera utilise deux codecs différents selon qu'il s'agit d'un appel de badge à badge (codec propriétaire à faible débit) ou d'un appel de badge à téléphone (codec G.711). Ce tableau montre un pourcentage de la bande passante disponible par débits de données et vous donne une image plus claire du débit attendu :

Processus d'appel	1 Mbit/s	2 Mbit/s	5,5 Mbit/s	11 Mbit/s
Badge-to-Phone (G.711)	20.7%	11.8%	6,3 %	4.7%
Badge-to-Badge (codec propriétaire à faible débit)	9.4%	6.1%	4.2%	3.6%

Recommandations de commutateur

Remarque : Si vous utilisez un commutateur de la gamme Cisco Catalyst 4000 comme routeur principal du réseau, assurez-vous qu'il contient au minimum un module Supervisor Engine 2+ (SUP2+) ou Supervisor Engine 3 (SUP3). Le module SUP1 ou SUP2 peut provoquer des retards d'itinérance, tout comme les commutateurs Cisco Catalyst 2948G, 2980G, 2980G-A, 4912 et 2948G-GE-TX.

Vous pouvez créer un modèle de port de commutateur à utiliser lorsque vous configurez un port de commutateur pour la connexion à un point d'accès. Ce modèle doit ajouter toutes les fonctions de sécurité et de résilience de base du modèle de bureau standard. En outre, lorsque vous reliez le point d'accès à un commutateur Cisco Catalyst 3750, vous pouvez optimiser les performances du point d'accès en utilisant les commandes QoS MLS (Multilayer Switching) pour limiter le débit des ports et mapper la classe de service aux paramètres DSCP (Differentiated Services Code Point).

Tout trafic qui n’est pas requis par les clients WLAN ne doit pas être envoyé à un point d’accès. Un modèle doit être conçu de manière à créer une connexion réseau sécurisée et résiliente avec les fonctionnalités suivantes :

- Return Port Configurations to default : évite les conflits de configuration en supprimant les configurations de ports préexistantes.
- Disable Dynamic Trunking Protocol (DTP) : désactive l'agrégation dynamique, qui n'est pas nécessaire pour la connexion à un point d'accès.
- Disable Port Aggregation Protocol (PagP) : le protocole PagP est activé par défaut mais n'est pas nécessaire pour les ports orientés utilisateur.
- Enable Port Fast : permet à un commutateur de reprendre rapidement le transfert du trafic en cas de défaillance d'une liaison Spanning Tree.
- Configure Wireless VLAN : crée un VLAN sans fil unique qui isole le trafic sans fil des autres VLAN de données, voix et gestion. Cela isole le trafic et assure un meilleur contrôle du trafic.
- Activer la qualité de service (QoS); do not trust port (mark down to 0) : assure un traitement approprié du trafic prioritaire, y compris les téléphones logiciels, et empêche les utilisateurs de consommer une bande passante excessive en reconfigurant leurs PC.

Les commutateurs d'alimentation en ligne WS-C3750-48PS-S peuvent être utilisés pour alimenter les points d'accès capables de recevoir une alimentation en ligne.

Le Catalyst 6500 vous permet de transférer des paquets au débit de ligne avec toutes les fonctionnalités décrites ici et d'intégrer de nombreux modules de service. Le module de service sans fil (WiSM) vous permet d'avoir deux contrôleurs chacun avec la capacité de contrôler 150 points d'accès chacun. Avec un maximum de cinq WiSM par châssis, vous pouvez contrôler plus de 1 500 points d'accès qui prennent en charge 50 000 clients au sein d'une seule architecture de commutation hautes performances.

Déploiements et configuration

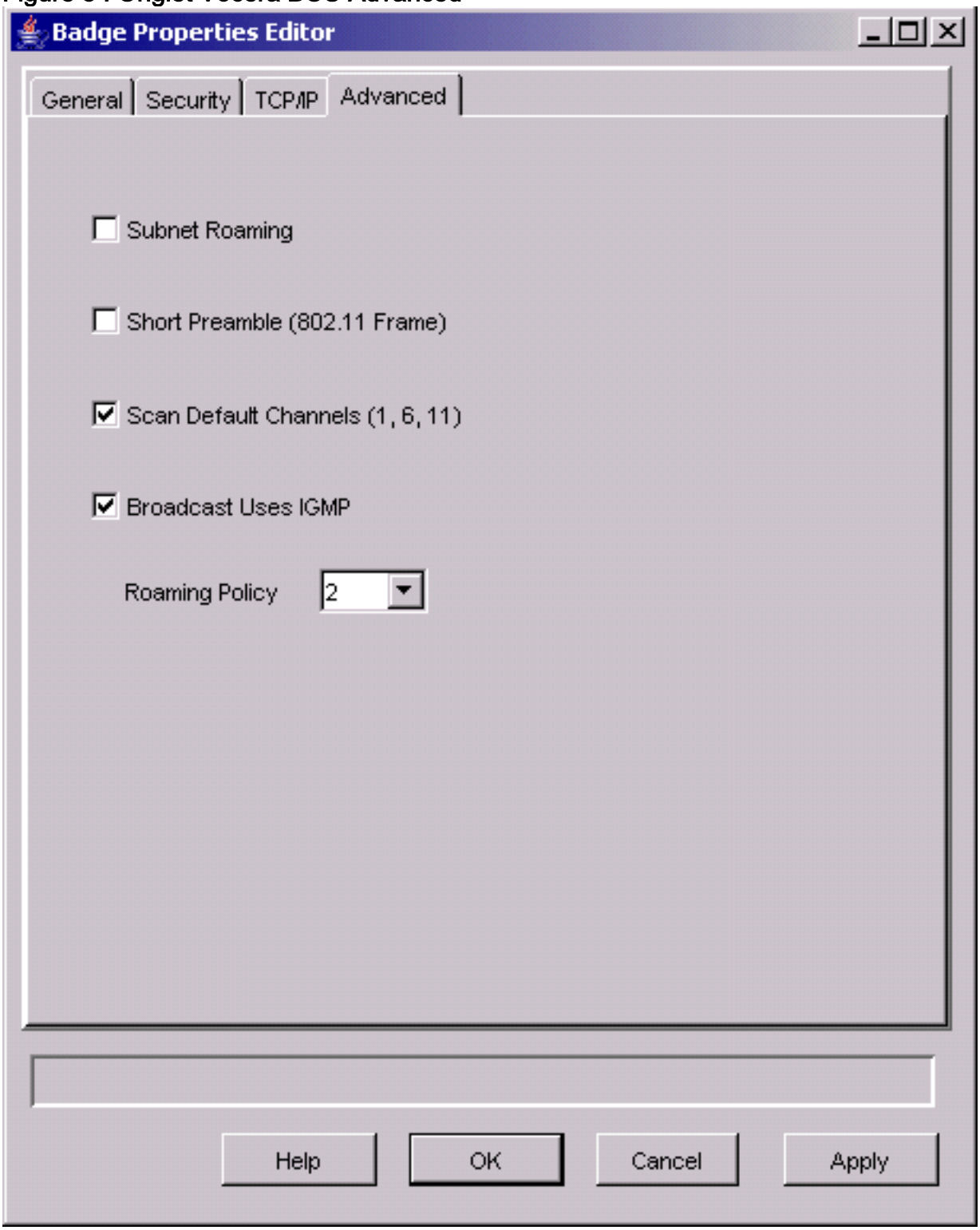
Configuration du badge

L'utilitaire de configuration de badge Vocera (BCU) et la configuration du badge peuvent introduire l'itinérance et la latence dans votre environnement si cela n'est pas fait correctement. À l'aide de la

BCU et de l'Éditeur de propriétés de badge (BPE), vérifiez ces paramètres (voir Figure 8) :

- **L'itinérance de sous-réseau** est désactivée.
- **Analyser les canaux par défaut (1,6,11)** est coché.
- **Utilisations de diffusion IGMP** est activé.
- La stratégie d'itinérance est définie sur **2** ou supérieur.

Figure 8 : Onglet Vocera BCU Advanced



Lorsque **l'itinérance de sous-réseau** est cochée, il demande au badge de demander une nouvelle adresse IP après chaque itinérance. Dans l'environnement LWAPP, l'infrastructure contribue à maintenir la connectivité client au niveau de la couche 3. Lorsqu'un client vocal doit attendre que le serveur DHCP réponde avant de pouvoir envoyer ou recevoir des paquets, le délai et la gigue

sont introduits. Si **Scan Default Channels (1,6,11)** n'est pas coché, le badge analyse tous les canaux 802.11b lorsque le badge recherche l'itinérance. Cela empêche le transfert des paquets et l'itinérance transparente.

Régler AutoRF pour votre environnement

Comme il est décrit dans la section Recommandations de ce document, il est important de comprendre que chaque site a ses propres caractéristiques RF. Il peut être nécessaire d'ajuster AutoRF ou Radio Resource Management (RRM), étant entendu que chaque site est différent et que AutoRF/RRM doit être adapté à votre environnement.

Avant de régler AutoRF, reportez-vous à Gestion des ressources radio sous Réseaux sans fil unifiés pour plus d'informations.

RRM vous permet d'ajuster la puissance de transmission de chaque point d'accès, en ajustant la force de chaque point d'accès à entendre son troisième voisin le plus fort. Cette valeur ne peut être ajustée qu'à partir de l'interface de ligne de commande à l'aide de la commande **config advanced 802.11b tx-power-batth** comme décrit dans Paramètres d'affectation de niveau de puissance Tx.

Avant de régler AutoRF, parcourez le site de déploiement à l'aide du badge Vocera tel qu'il est porté par l'utilisateur final et utilisez un outil d'analyse de site afin de mieux comprendre comment le badge se déplace et quelle puissance chaque point d'accès est visible. Une fois cette opération terminée et qu'il est déterminé que l'ajustement de cette valeur est nécessaire, commencez par une valeur de -71 dBm pour l'algorithme de contrôle de puissance de transmission. Utilisez ce paramètre CLI :

```
config advanced 802.11b tx-power-thresh -71
```

Autorisez le réseau à effectuer ce réglage avec un minimum de 30 minutes à une heure avant d'observer toute modification. Une fois que le réseau dispose de suffisamment de temps, parcourez le site à l'aide du même outil d'enquête et des mêmes badges. Observez les mêmes caractéristiques d'itinérance et la même puissance de point d'accès. L'objectif ici est de tenter d'avoir les badges en itinérance au point d'accès suivant ou avant pour obtenir le meilleur rapport signal/bruit possible.

- **Comment savoir si la puissance de transmission est trop chaude ou trop froide ?**Pour déterminer si votre seuil de puissance de transmission est trop élevé ou trop faible, vous devez bien comprendre votre environnement. Si vous avez parcouru l'ensemble de votre zone de déploiement (où vous vous attendez à ce que vos badges Vocera fonctionnent), vous devez savoir où se trouvent vos points d'accès et connaître le comportement d'itinérance de votre badge.
- **Que dois-je faire si ma puissance de transmission est trop élevée ?**Le badge Vocera fonctionne uniquement en fonction de la puissance du signal plutôt que de la qualité du signal. Si le badge Vocera ne se déplace pas après avoir passé plusieurs points d'accès lors de l'utilisation du tutoriel d'accueil ou de la tonalité de test, le badge est considéré comme collant. Si ce comportement indique l'ensemble de la zone de déploiement du campus, votre seuil de puissance de transmission est trop chaud et doit être désactivé. Si seulement une ou deux zones isolées affichent ce comportement et que le reste de la zone de déploiement présente des caractéristiques d'itinérance plus idéalistes, cela n'indique pas que votre réseau

fonctionne trop chaud.

- **Que dois-je faire si ma puissance de transmission est trop froide ?**Le seuil de transmission par défaut ne doit presque jamais vous fournir une zone de déploiement où votre réseau est trop froid. Si le seuil de puissance de transmission est ajusté et que vous parcourez les couloirs avec le badge Vocera, vous bénéficiez d'un environnement dans lequel le badge se déplace bien, mais perd la connectivité et/ou la couverture morte/intempestive, votre réseau a peut-être été réglé trop bas. Si cela n'est pas caractéristique de l'ensemble de votre réseau mais isolé à une ou deux zones, cela indique davantage un trou de couverture qu'un problème à l'échelle du réseau.
- **Comportement isolé**Si vous trouvez que dans une ou deux zones, l'insigne s'accroche à un point d'accès plutôt que de se déplacer de manière idéaliste, examinez cette zone.En quoi cette zone est-elle différente du reste du campus ?Si ces zones sont proches des sorties de bâtiments ou des zones en construction, la détection des trous de couverture pourrait-elle forcer ces points d'accès à augmenter la puissance ?Examinez le fichier journal du WLC et les listes de voisinage des points d'accès pour déterminer pourquoi une telle anomalie pourrait se produire.Si vous constatez que dans une ou plusieurs zones isolées, l'insigne est couvert de mort ou de vaches, alors vous devez examiner ces zones séparément.Cette zone est-elle proche d'un puits d'ascenseur, d'une radiologie ou d'une salle de pause ?Ces zones pourraient être mieux adaptées par l'installation ou un meilleur emplacement d'un point d'accès pour permettre une meilleure couverture vocale.Dans les deux cas, il est toujours conseillé de comprendre que vous travaillez dans un spectre radio sans licence et que le comportement idéaliste ne sera peut-être jamais réalisable. Cela peut se produire lorsque vous vous trouvez à côté d'une tour ou d'un périphérique de transmission radio, d'un émetteur de télévision ou éventuellement d'une installation de réparation non-802.11 2,4 GHz (téléphones sans fil, etc.).

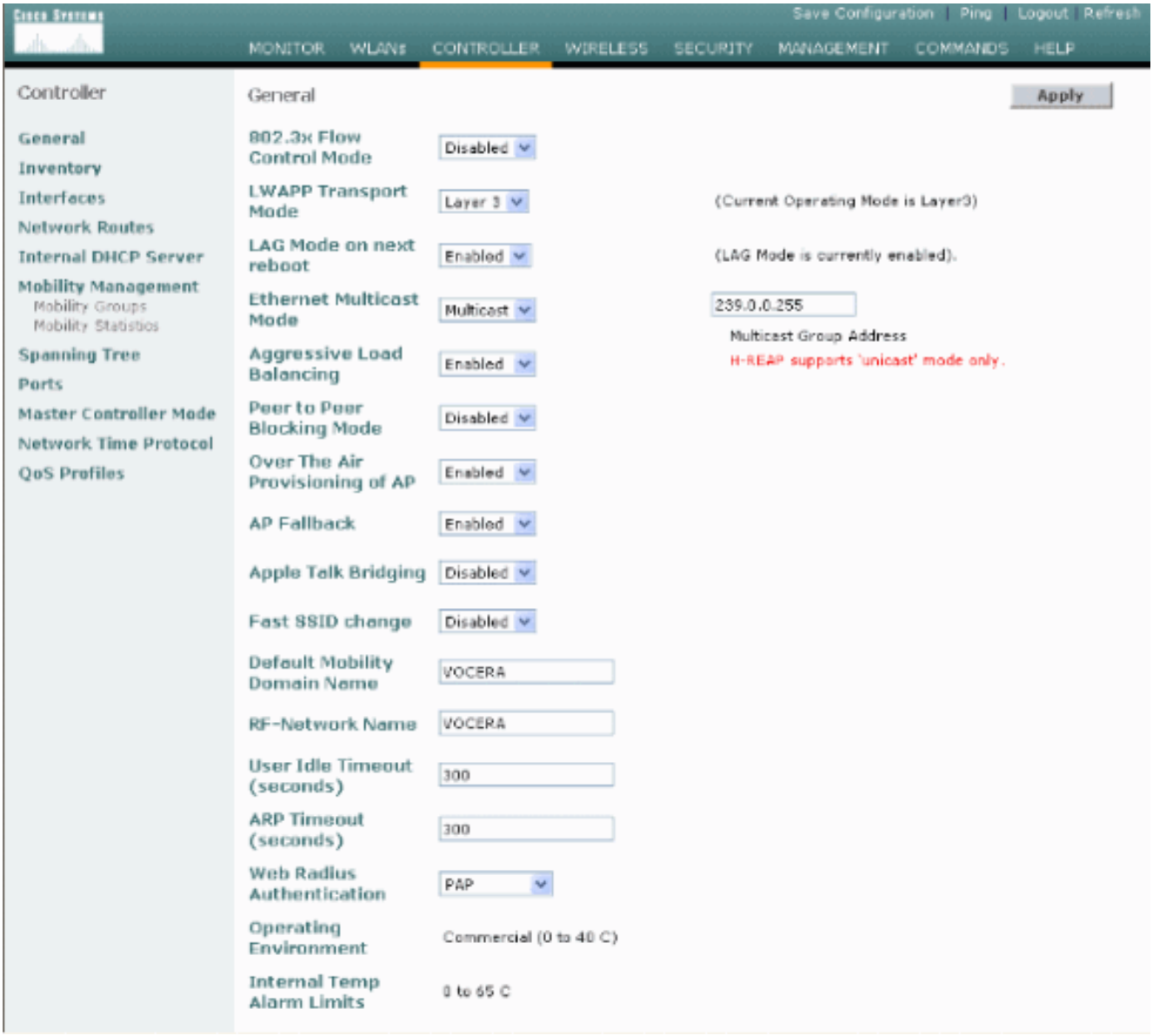
Configuration de l'infrastructure réseau sans fil

Le guide de conception et de déploiement du réseau sans fil unifié Cisco doit être suivi pour la configuration globale de votre ou vos WLC. Cette section fournit des recommandations supplémentaires spécifiques aux badges de communication Vocera®.

Remarque : Les modifications ne sont pas enregistrées si vous n'appuyez pas sur le bouton **Appliquer** avant de passer à l'étape suivante.

Effectuez ces étapes sous le menu de niveau supérieur **Contrôleur** :

1. Remplacez le mode de multidiffusion Ethernet par **Multicast**.
2. Définissez l'adresse du groupe de multidiffusion sur **239.0.0.255** (ou une autre adresse de groupe de multidiffusion inutilisée).
3. Définissez le nom de domaine de mobilité par défaut et le nom de réseau RF sur la conception de votre réseau.
4. Désactivez **l'équilibrage de charge agressif**.**Figure 9 : Configuration générale du WLC**

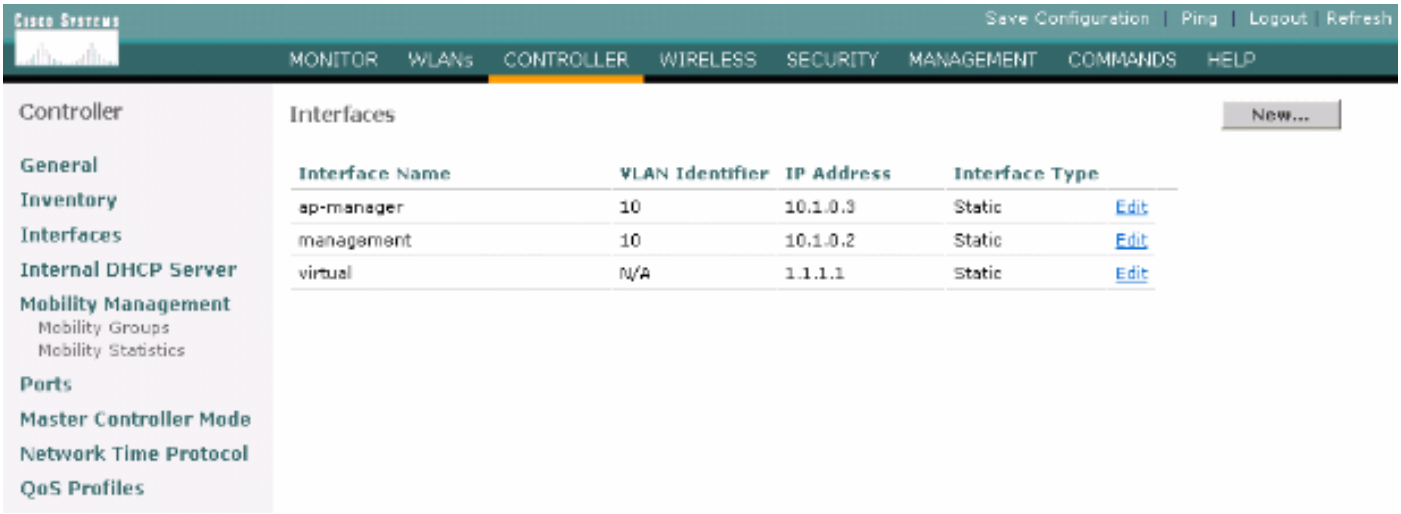


Créer des interfaces

Cliquez sur **Controller > Interfaces**.

Remarque : Votre VLAN et votre adresse IP varient. Les captures d'écran ici fournissent un exemple d'adressage qui ne doit pas être suivi directement.

Figure 10 : liste des interfaces WLC



Créer l'interface vocale Vocera

Procédez comme suit :

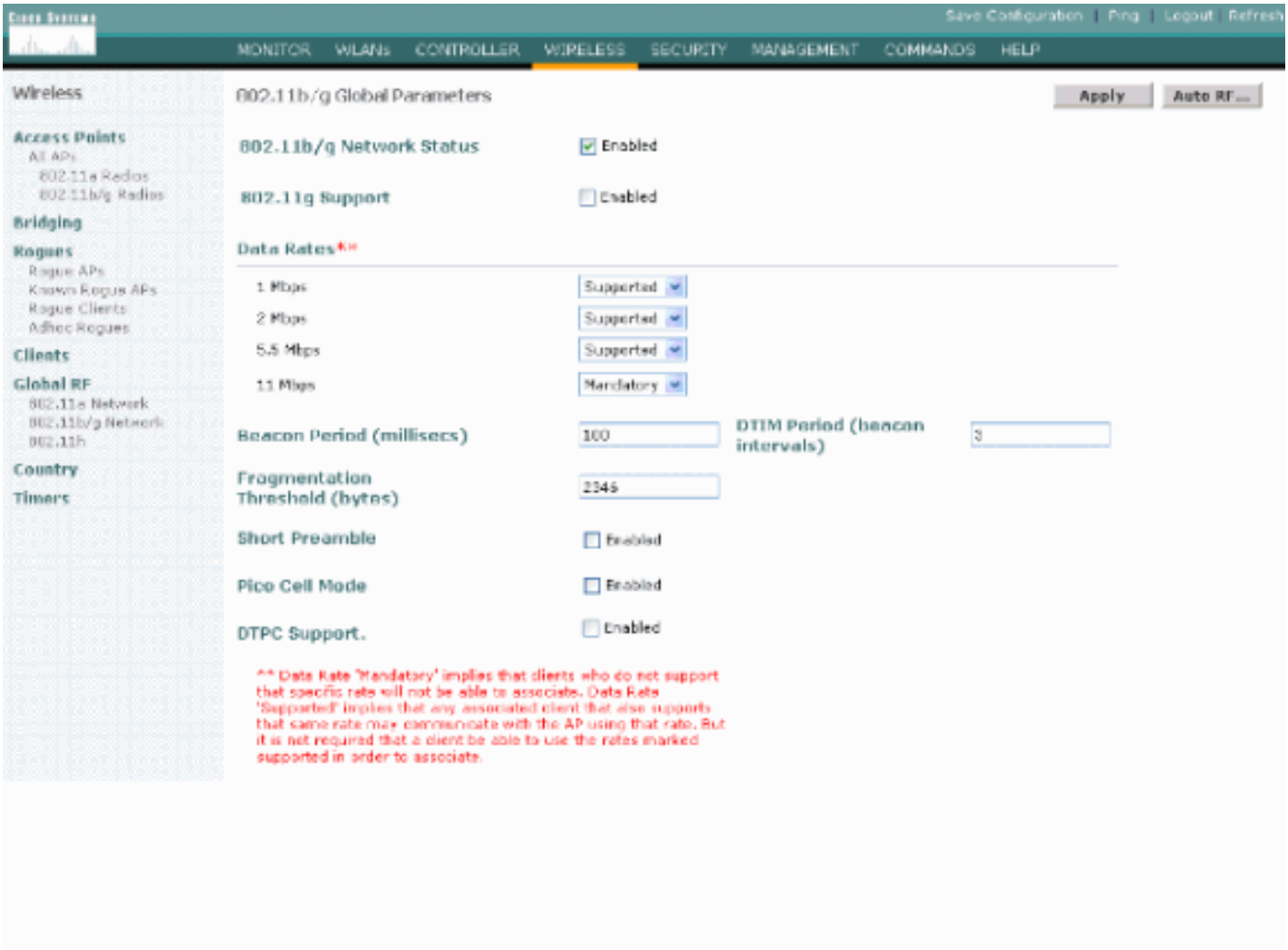
1. Cliquez sur **New**.
2. Saisissez un nom de balise représentatif de votre réseau VoWLAN Vocera dans le champ Interface Name.
3. Saisissez le numéro de VLAN de ce réseau VoWLAN dans le champ VLAN ID.
4. Cliquez sur **Apply**, puis sur **Edit** afin de modifier l'interface que vous venez de créer.
5. Saisissez l'adressage IP de cette interface qui se trouve dans la plage du VLAN et d'autres informations associées.
6. Cliquez sur Apply.

Configuration spécifique au sans fil

Dans le cas d'un réseau local sans fil ne comportant que des badges Vocera, cette configuration fournit des exemples de paramètres qui prennent le mieux en charge l'application de diffusion Vocera.

- La période DTIM est **1**.
- La prise en charge de la norme 802.11g est désactivée. Seul le débit de données 802.11b de **11 Mpbs** est **obligatoire**.
- Le préambule court est désactivé.
- DTPC est désactivé.

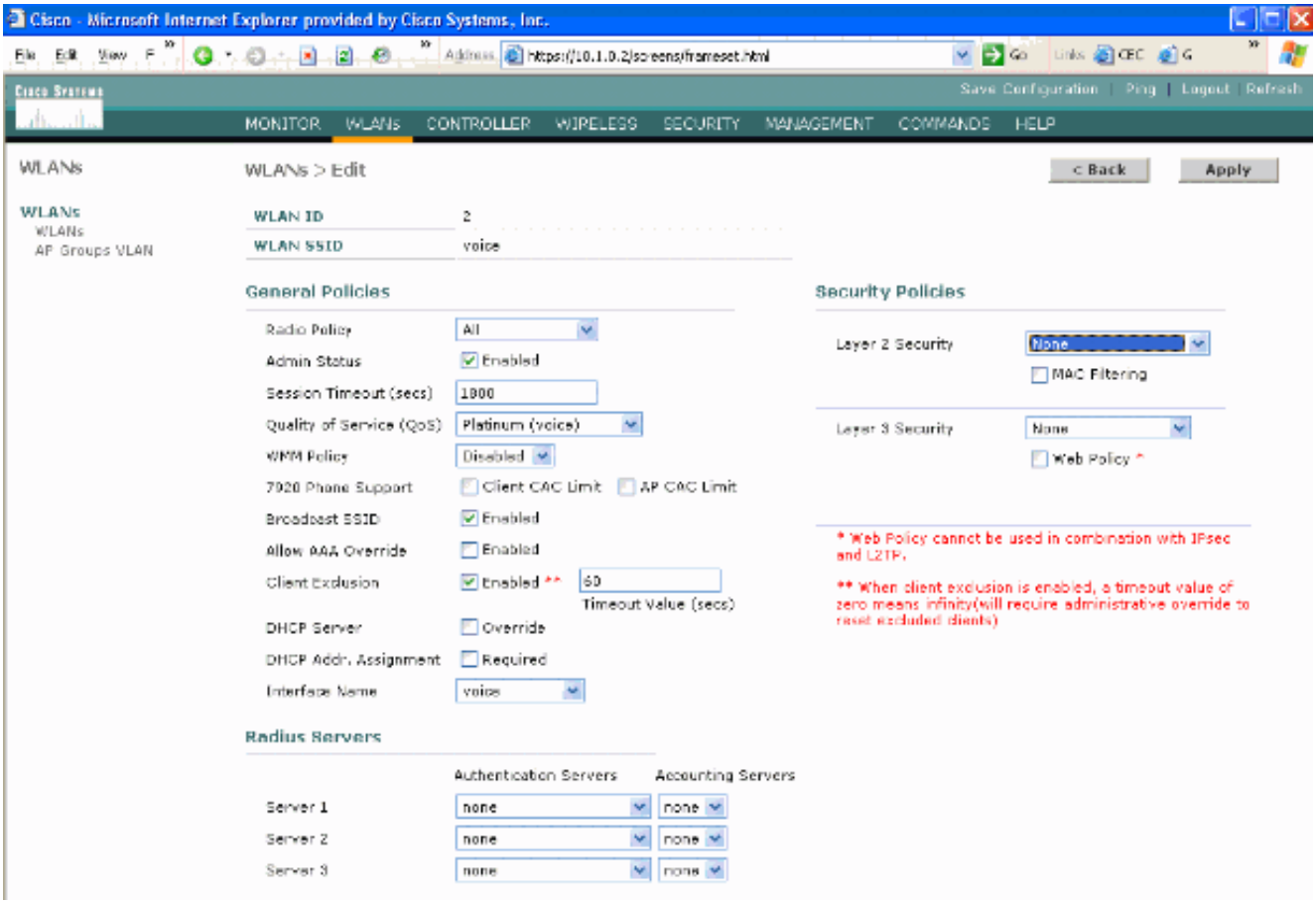
Figure 11 : configuration 802.11b/g



Configuration WLAN

Procédez comme suit :

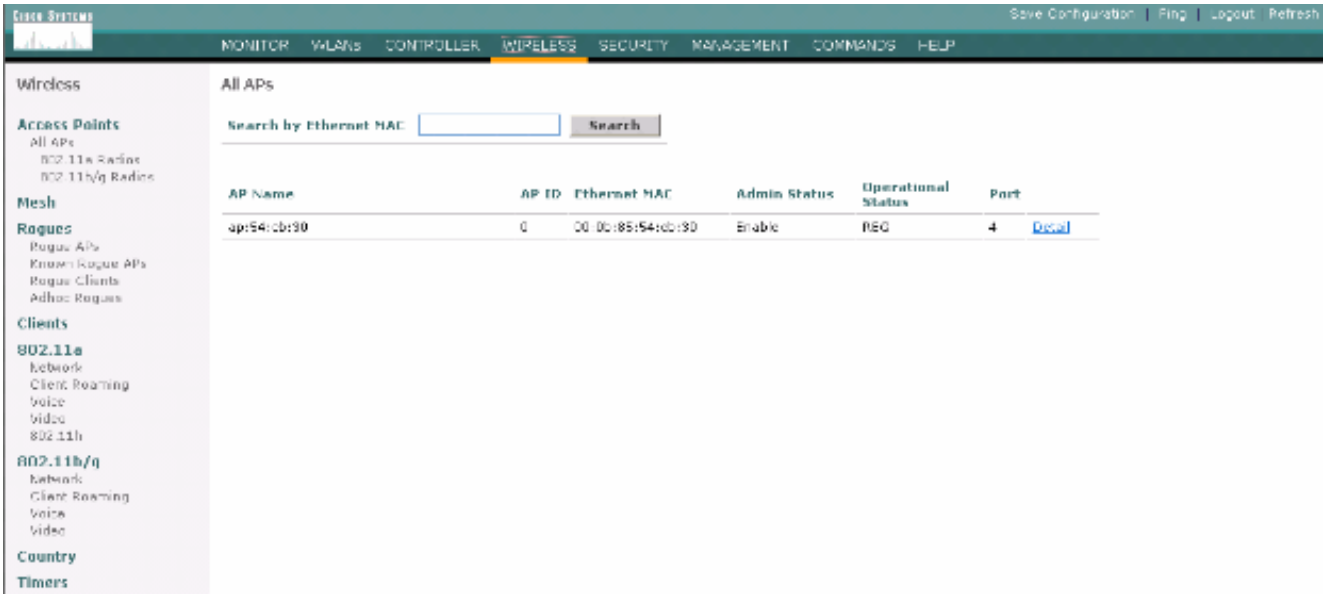
1. Mettez à jour le champ Stratégie radio en fonction de vos besoins.
2. Remplacez l'état Admin par **Activé**.
3. Définissez le délai d'attente de session sur **1800**.
4. Définir la qualité de service sur **Platinum**.
5. Définissez le SSID de diffusion sur **Activé**.
6. Définissez le nom de l'interface sur l'interface créée pour les badges de communication Vocera.
7. Définissez les options de sécurité pour qu'elles correspondent aux stratégies de votre entreprise.**Figure 12 : Configuration WLAN**



Configurer les détails du point d'accès

Procédez comme suit :

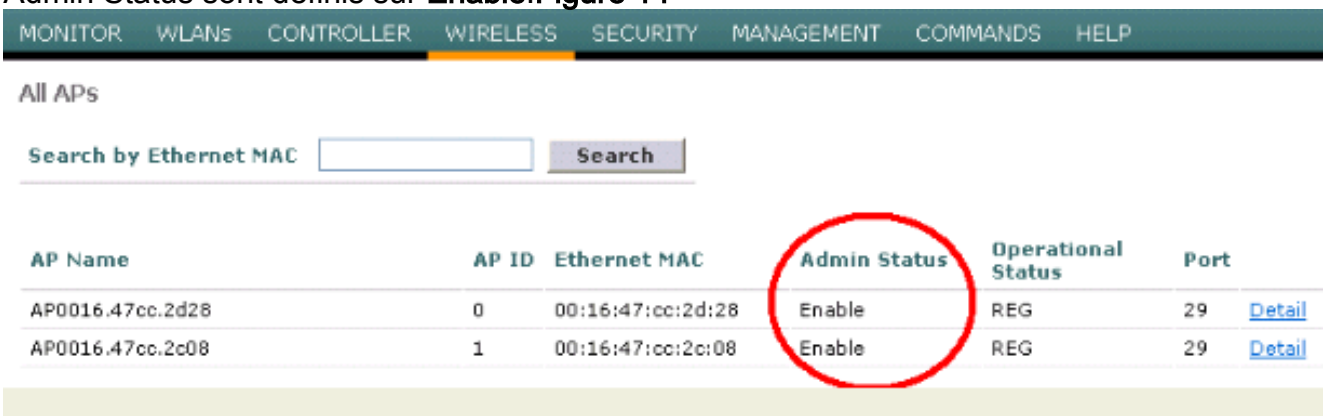
1. Cliquez sur **Detail**.
2. Configurez le nom du point d'accès.
3. Assurez-vous que le point d'accès est configuré pour DHCP.
4. Vérifiez que l'état Admin est **activé**.
5. Le ” du module AP doit être défini sur **local**.
6. Saisissez l'emplacement du point d'accès.
7. Entrez le nom du contrôleur auquel appartient le point d'accès. Le nom du contrôleur se trouve sur la page Moniteur.
8. Cliquez sur Apply.**Figure 13 : Détails des points d'accès**



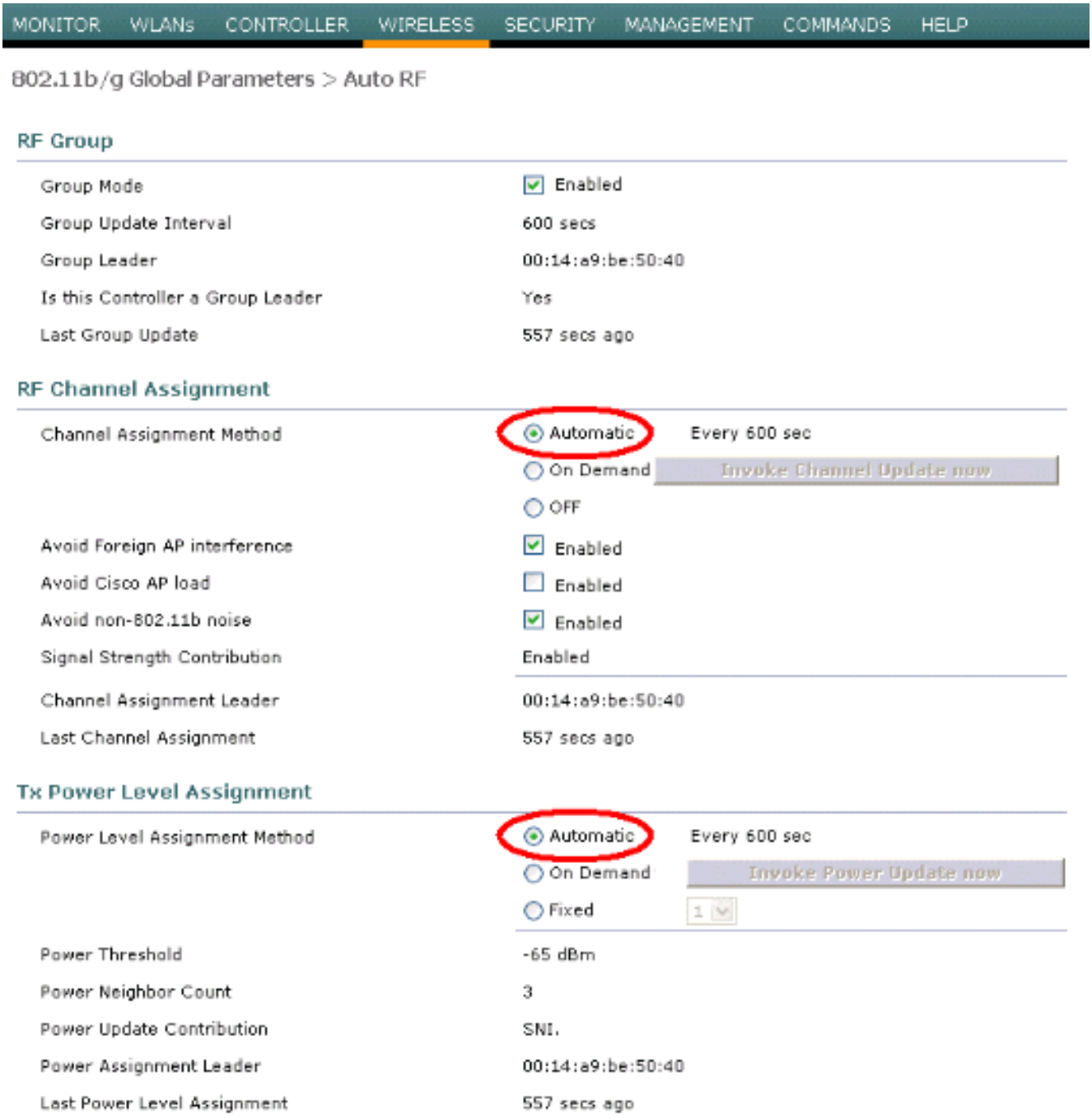
Configurer la radio 802.11b/g

Procédez comme suit :

1. Cliquez sur **Wireless** situé en haut du WLC et vérifiez que tous les points d'accès sous Admin Status sont définis sur **Enable**.**Figure 14**



2. Cliquez sur **Réseau** (situé près de 802.11b/g).
3. Cliquez sur **AutoRF**.
4. Utilisez AutoRF pour créer une couverture complète avec un canal RF sans chevauchement et une puissance de transmission. Pour ce faire, sélectionnez **Automatique** pour l'affectation de canal RF et l'affectation de niveau d'alimentation Tx.**Figure 15**



5. Cliquez sur Apply.
6. Cliquez sur **Enregistrer la configuration** et consultez la section [Régler l'AutoRF pour votre environnement](#) de ce document.
7. Choisissez **Wireless > Access Points > 802.11b/g Radios**.**Figure 16**

Vérification de la téléphonie IP sans fil

Après avoir effectué une analyse de site RF et configuré les points d'accès et les téléphones, il est essentiel de procéder à des tests de vérification pour s'assurer que tout fonctionne comme vous le souhaitez. Ces essais doivent être effectués à tous les endroits suivants :

- La zone principale de chaque cellule de point d'accès (où les badges sont le plus susceptibles de se connecter à ce point d'accès particulier).
- Tout emplacement où le volume d'appels peut être élevé.
- Emplacements où l'utilisation est peu fréquente mais où la couverture doit encore être certifiée (par exemple, escaliers, toilettes, etc.).
- En périphérie de la zone de couverture du point d'accès.
- ·Ces essais peuvent être effectués en parallèle ou en série. S'il est exécuté en parallèle, assurez-vous que les téléphones sont mis hors tension entre les points de test pour tester l'association complète, l'authentification et l'enregistrement à chaque emplacement. Les tests d'itinérance et de charge doivent être les tests finaux.

Association, authentification et enregistrement

Cette section explique comment vérifier que le badge s'associe, s'authentifie et s'enregistre correctement.

- Àplusieurs points de l'environnement, mettez les badges sous tension et vérifiez leur association avec le point d'accès. Si le badge n'est pas associé au point d'accès, effectuez les vérifications suivantes :Vérifiez la configuration du badge pour vous assurer que le SSID, le type d'authentification, etc. sont corrects.Vérifiez la configuration du WLC pour vous assurer que le SSID, le type d'authentification, les canaux radio, etc. sont appropriés.Vérifiez l'étude de votre site pour vous assurer que l'emplacement dispose d'une couverture RF adéquate.
- Àplusieurs points de l'environnement, assurez-vous que le téléphone s'authentifie correctement via le point d'accès. Si le client ne s'authentifie pas, vérifiez la clé WEP ou le nom d'utilisateur et le mot de passe LEAP sur les badges. Vérifiez également le nom d'utilisateur et le mot de passe sur le serveur AAA en utilisant un ordinateur portable sans fil avec des informations d'identification identiques.
- Àplusieurs endroits dans l'environnement, assurez-vous que les badges s'enregistrent auprès du serveur de communication Vocera. Si le client ne s'enregistre pas, effectuez les vérifications suivantes :Vérifiez que le badge possède l'adresse IP, le masque de sous-réseau, la passerelle principale, le TFTP principal, le principal/secondaire et le DNS corrects.
- Appels vocaux fixes :Àplusieurs endroits de l'environnement, pendant que vous restez immobile, appelez un autre badge et effectuez des tests vocaux de 60 à 120 secondes pour vérifier la qualité de la voix. Si la qualité vocale est inacceptable, déplacez un badge vers un meilleur emplacement et testez à nouveau. La qualité vocale est-elle acceptable ? Si ce n'est pas le cas, vérifiez votre couverture sans fil.Si le serveur de téléphonie est configuré, à plusieurs points de l'environnement, restez immobile et passez un appel à un téléphone câblé et effectuez des tests vocaux de 60 à 120 secondes pour vérifier la qualité de la voix. Si la qualité vocale est inacceptable, demandez si vous passez un appel à l'aide du téléphone câblé. La qualité vocale est-elle acceptable ? Si ce n’est pas le cas, vérifiez la conception du réseau câblé conformément aux directives.

- Utilisez les outils d'analyse de site pour vérifier qu'il n'y a pas plus d'un point d'accès par canal RF à partir de cet emplacement avec une puissance de signal (indicateur de puissance de signal reçu [RSSI]) supérieure à 35. Si deux points d'accès sont présents sur le même canal, assurez-vous que le rapport signal/bruit (SNR) est le plus élevé possible pour minimiser les interférences. Par exemple, si le point d'accès le plus puissant a un RSSI de 35, idéalement le point d'accès le plus faible devrait avoir un RSSI de moins de 20. Pour atteindre cet objectif, vous devrez peut-être réduire la puissance de transmission d'un point d'accès ou déplacer le point d'accès.
- Vérifiez les paramètres QoS du point d'accès pour confirmer les paramètres recommandés appropriés.
- Appels de badge d'itinérance :Si le serveur de téléphonie n'est pas disponible, lancez le didacticiel Vocera à l'aide de la commande **Begin Tutorial**.OUSi le serveur de téléphonie est disponible, lancez un appel avec un périphérique fixe sur le badge.Vérifiez en permanence la qualité vocale pendant que vous traversez la zone de couverture sans fil totale. Si la qualité vocale est insuffisante, effectuez les tâches suivantes :Écoutez toutes les modifications inacceptables de la qualité de la voix et prenez note des valeurs d'emplacement et de radio de votre ordinateur portable et de votre CQ à partir du badge.Regardez et écoutez le badge pour vous déplacer jusqu'au point d'accès suivant.Notez les autres points d'accès disponibles dans l'étude de site pour vérifier la couverture et les interférences.
- Apportez des ajustements à l'emplacement et aux paramètres des points d'accès pour affiner le WLAN et effectuez ces vérifications pour garantir la qualité de la voix :Utilisez les outils d'analyse de site et vérifiez qu'il n'y a pas plus d'un point d'accès par canal avec une valeur RSSI supérieure à 35 à un emplacement donné. Idéalement, tous les autres points d'accès sur le même canal devraient avoir des valeurs RSSI aussi basses que possible (de préférence inférieures à 20). À la frontière de la zone de couverture où le RSSI est 35, le RSSI pour tous les autres points d'accès sur le même canal devrait idéalement être inférieur à 20.Utilisez les outils d'analyse de site pour vérifier qu'au moins deux points d'accès (au total, sur des canaux distincts) sont visibles à tous les emplacements avec une puissance de signal suffisante.Vérifiez que les points d'accès d'une zone d'itinérance donnée se trouvent tous sur un réseau de couche 2.

Problèmes courants d'itinérance

Ces problèmes d'itinérance peuvent se produire :

- Le badge ne se déplace pas lorsqu'il est placé directement sous le point d'accès.
- Le badge n'atteint probablement pas les seuils différentiels d'itinérance pour l'indicateur de puissance du signal reçu (RSSI) et l'utilisation du canal (CU). Ajustez le seuil de puissance de transmission à partir du WLC.
- Le badge ne reçoit pas de balises ni de réponses de sonde du point d'accès.
- Le badge avance trop lentement.

Le badge perd la connexion au réseau ou au service vocal lors de l'itinérance

- Vérifiez l'authentification pour détecter une éventuelle incompatibilité WEP.
- Le badge n'envoie pas de jointures IGMP ou le réseau envoie des requêtes IGMP pendant une itinérance. Par conséquent, la fonction de diffusion Vocera échoue pendant une

itinérance de couche 2/couche 3.
- Le badge peut uniquement être en itinérance transparente de couche 2 (sauf si un mécanisme de mobilité de couche 3 est configuré). Assurez-vous que le nouveau WLC ne dessert pas un sous-réseau IP différent.
- Vérifiez que le point d'accès/contrôleur associé dispose d'une connectivité IP au serveur de communication Vocera.
- Vérifiez la puissance du signal RF et les valeurs CQ du badge.

Le badge perd la qualité vocale lors de l'itinérance

- Vérifiez que le RSSI est faible sur le point d'accès de destination.
- Le chevauchement des canaux peut être insuffisant. Le badge doit avoir le temps de transmettre l'appel en douceur avant de perdre son signal avec le point d'accès d'origine.
- Le signal du point d'accès d'origine peut être perdu.

Problèmes audio

Quelques erreurs de configuration courantes peuvent entraîner des problèmes audio facilement résolus. Si possible, comparez les problèmes audio à un badge fixe (de référence) pour résoudre le problème à un problème sans fil. Les problèmes audio courants sont les suivants :

- Audio monoface
- Audio changeant ou robotique
- Problèmes d'enregistrement et d'authentification

Audio monoface

- Ce problème peut se produire dans les zones périphériques d’un point d’accès, où un signal peut être trop faible du côté badge ou du côté point d’accès. Si possible, la mise en correspondance des paramètres d'alimentation du point d'accès avec le badge (20 mW) peut résoudre ce problème. Ce problème est plus fréquent lorsque la variation entre le paramètre du point d'accès et le paramètre du badge est importante (par exemple, 100 mW sur le point d'accès et 28 mW sur le badge).
- Vérifiez la qualité vocale de la passerelle et du routage IP.
- Vérifiez si un pare-feu ou une NAT se trouve sur le chemin des paquets UDP propriétaires. Par défaut, les pare-feu et les NAT provoquent un signal audio unidirectionnel ou aucun signal audio. Les NAT et les pare-feu Cisco IOS® et PIX ont la possibilité de modifier ces connexions de sorte que le flux audio bidirectionnel puisse circuler.Si vous utilisez la mobilité de couche 3, votre réseau peut bloquer le trafic en amont grâce aux contrôles uRPF (Unicast Reverse Path Forwarding).
- L'audio unidirectionnel peut se produire si la mise en cache ARP n'est pas configurée sur le WLC.

Audio changeant ou robotique

- Une raison courante de l'audio mobile ou robotique est quand un micro-ondes fonctionne à proximité. Les micro-ondes commencent au canal 9 et peuvent s'étendre des canaux 6 à 14.

- Vérifiez que les téléphones sans fil 2,4 GHz et les autres infirmières appellent des périphériques sans fil à l'aide d'outils tels que Cognio.

Problèmes d'enregistrement et d'authentification

Lorsque vous rencontrez des problèmes d'authentification, effectuez les vérifications suivantes :

- Vérifiez les SSID pour vous assurer qu'ils correspondent sur le badge et le point d'accès (ou réseau). Assurez-vous également que le réseau a une route vers le serveur Vocera.
- Vérifiez les clés WEP pour vous assurer qu'elles correspondent. Il est recommandé de les saisir à nouveau dans l'utilitaire de configuration de badge (BCU) et de reprogrammer le badge, car il est facile de faire une erreur de saisie lorsque vous saisissez une clé ou un mot de passe WEP.

Ces messages ou symptômes peuvent se produire :

- Impossible de prendre en charge toutes les fonctionnalités demandées : il s'agit probablement d'une non-correspondance de chiffrement entre le point d'accès et le client.
- Échec de l'authentification / Aucun point d'accès trouvé : assurez-vous que les types d'authentification correspondent sur le point d'accès et le client.
- Aucun service - Échec de la configuration IP : si vous utilisez un WEP statique, assurez-vous que les clés sont correctement configurées. Assurez-vous que les autres clients peuvent recevoir DHCP à l’aide du même SSID.
- Désauthentifier tous les clients TKIP à partir d'AP : ce problème se produit lorsque le point d'accès détecte deux erreurs MIC en 60 secondes. Cette contre-mesure empêche tous les clients TKIP de se réauthentifier pendant 60 secondes.
- Re-authentication / Session Timeout : si elle est configurée, une session timeout déclenche une nouvelle authentification qui entraîne des lacunes dans le flux vocal (300 ms + délai WAN pour l'authentification 802.1x).

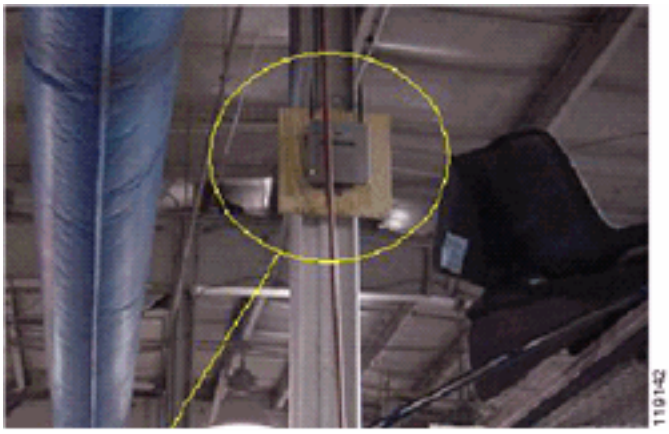
Annexe A

Emplacement des points d'accès et des antennes

Cette section donne des exemples de positionnement correct et incorrect des points d'accès (AP) et des antennes.

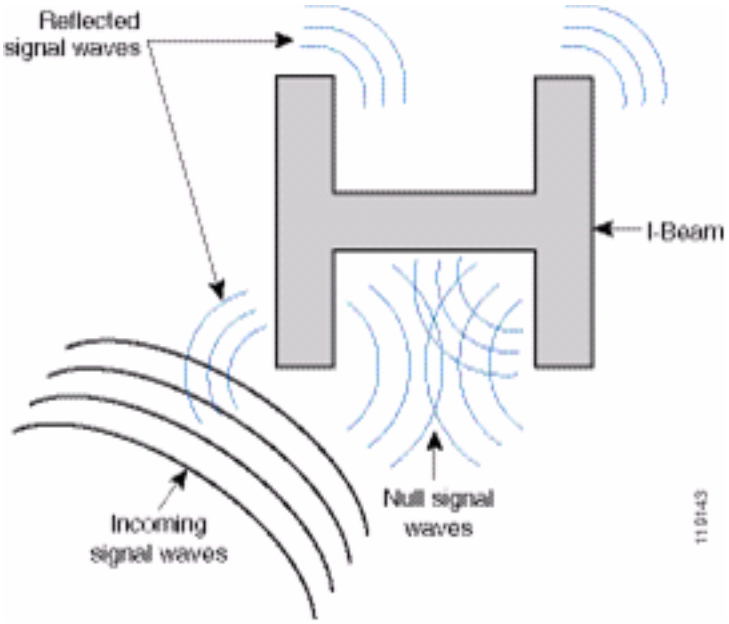
La Figure 17 montre le placement incorrect d'un point d'accès et d'antennes à proximité d'un faisceau d'I, ce qui crée des modèles de signaux déformés. Un point nul RF est créé par le croisement des ondes de signal et la distorsion par trajets multiples est créée lorsque les ondes de signal sont réfléchies. Ce positionnement entraîne une très faible couverture derrière le point d'accès et une réduction de la qualité du signal devant le point d'accès.

Figure 17 : emplacement incorrect des antennes à proximité d'un faisceau d'E



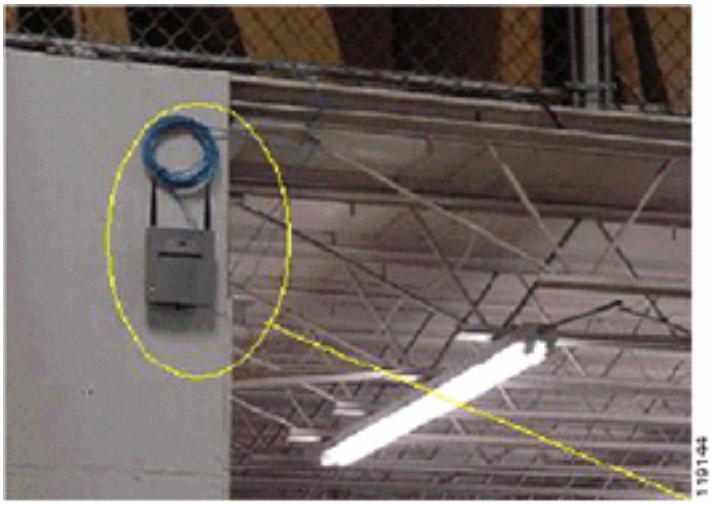
La figure 18 montre les changements ou les distorsions de propagation du signal causés par un faisceau I. Le faisceau I crée de nombreuses réflexions à partir des paquets reçus et des paquets transmis. Les signaux réfléchis produisent une qualité de signal très médiocre en raison de points nuls et d'interférences de trajets multiples. Cependant, la puissance du signal est élevée car les antennes du point d'accès sont si proches du faisceau I.

Figure 18 - Distorsions de signal causées par le placement des antennes trop près d'un faisceau d'E



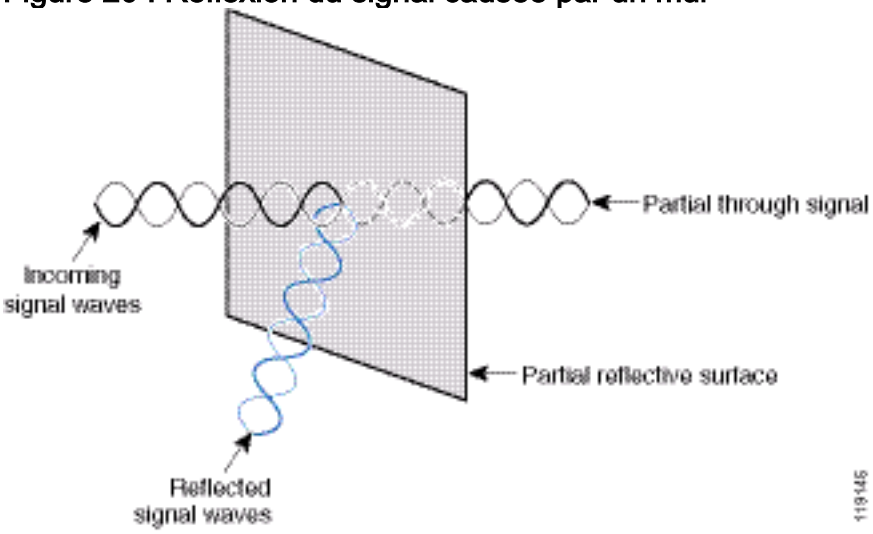
Le positionnement du point d'accès et de l'antenne dans la Figure 19 est préférable car il est éloigné des E-Beams et il y a moins de signaux réfléchis, moins de points nuls et moins d'interférences de trajets multiples. Cette position n'est toujours pas parfaite, car le câble Ethernet ne doit pas être enroulé si près de l'antenne. En outre, le point d'accès peut être tourné avec les antennes 2,4 GHz pointées sur le sol. Cela offre une meilleure couverture directement en dessous du point d'accès. Il n'y a aucun utilisateur au-dessus du point d'accès.

Figure 19 : point d'accès et antennes montés sur un mur, à l'écart des poutres en I



La Figure 20 illustre la propagation du signal causée par le mur sur lequel le point d'accès est monté.

Figure 20 : Réflexion du signal causée par un mur

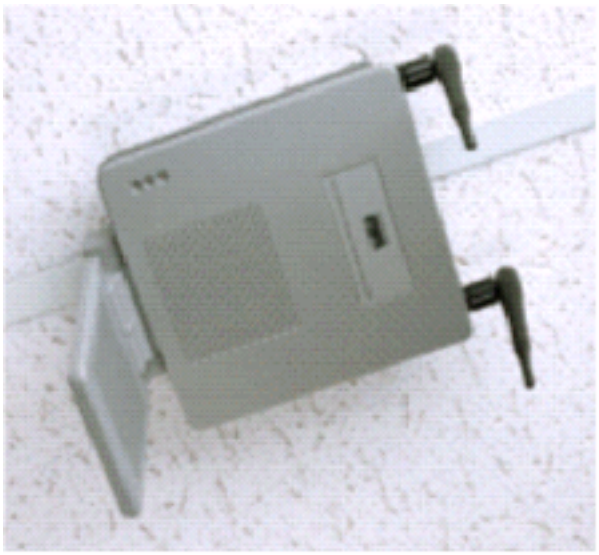


Les exemples précédents s'appliquent également lorsque vous placez des points d'accès et des antennes dans ou près du plafond dans un environnement d'entreprise standard. S'il existe des conduits d'air métalliques, des puits d'ascenseur ou d'autres barrières physiques susceptibles de provoquer une réflexion du signal ou des interférences multivoies, Cisco recommande vivement de déplacer les antennes de ces barrières. Dans le cas de l'ascenseur, déplacez l'antenne à quelques pieds afin d'éliminer la réflexion et la distorsion du signal. Il en va de même pour les conduits d'air au plafond.

Une enquête menée sans envoyer et recevoir de paquets n'est pas suffisante. L'exemple de faisceau d'E montre la création de points nuls qui peuvent résulter de paquets ayant des erreurs CRC. Les paquets vocaux avec des erreurs CRC sont des paquets manqués qui affectent négativement la qualité de la voix. Dans cet exemple, ces paquets peuvent être situés au-dessus de la surface sonore mesurée par un outil d'analyse. Par conséquent, il est très important que l'étude de site non seulement mesure les niveaux de signal, mais génère également des paquets, puis signale des erreurs de paquets.

La Figure 21 montre un point d'accès Cisco AP1200 correctement monté sur une barre T de plafond, les antennes étant en position omnidirectionnelle.

Figure 21 : Cisco AP1200 monté au plafond



La Figure 22 présente une antenne multidirectionnelle omnidirectionnelle Cisco Aironet 5959 correctement montée sur une barre en T au plafond. Dans ce cas, le point d'accès Cisco AP1200 est monté au-dessus de la plaque de plafond.

Figure 22 : Antenne Cisco Aironet 5959 montée au plafond

La Figure 23 montre un point d'accès Cisco AP1200 correctement monté sur un mur.

Figure 23 : Cisco AP1200 monté sur un mur

La figure 24 montre l'antenne de raccordement de diversité Cisco Aironet 2012 montée sur un mur. Dans ce cas, le point d'accès Cisco AP1200 est monté au-dessus de la plaque de plafond.

Figure 24 : Antenne Cisco Aironet 2012 montée sur un mur

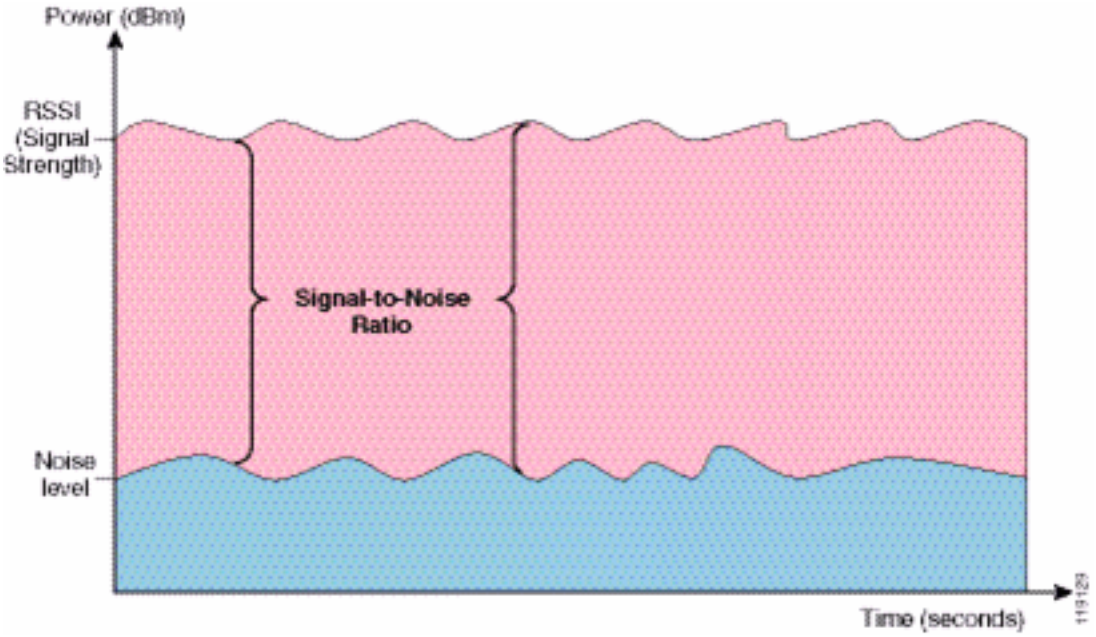
Pour les zones où le trafic utilisateur est important (bureaux, écoles, magasins de détail et hôpitaux), Cisco recommande de mettre le point d'accès hors de vue et de placer des antennes discrètes sous le plafond. La séparation des antennes non diversaires ne doit pas dépasser 18 pouces.

Distorsion des interférences et des trajets multiples

Les performances de débit du réseau WLAN sont affectées par des signaux inutilisables. Les interférences WLAN peuvent être générées par des fours à micro-ondes, des téléphones sans fil 2,4 GHz, des périphériques Bluetooth ou tout autre équipement électronique fonctionnant dans la bande 2,4 GHz. Les interférences proviennent également généralement d'autres points d'accès et périphériques clients qui appartiennent au WLAN mais qui sont suffisamment éloignés pour que leur signal soit affaibli ou endommagé. Les points d'accès qui ne font pas partie de l'infrastructure réseau peuvent également provoquer des interférences WLAN et être identifiés comme des points d'accès non autorisés.

Les interférences et les distorsions de trajets multiples provoquent des fluctuations du signal transmis. L'interférence diminue le rapport signal/bruit (SNR) pour un débit de données particulier. Le nombre de tentatives de paquets augmente dans une zone où les interférences et/ou les distorsions de trajets multiples sont élevées. L'interférence est également appelée niveau sonore ou plancher de bruit. La puissance du signal reçu de son point d'accès associé doit être suffisamment élevée au-dessus du niveau de bruit du récepteur pour être décodée correctement. Ce niveau de puissance est appelé rapport signal/bruit, ou SNR. Le SNR idéal pour le badge Vocera est de 25 dB. Par exemple, si le niveau sonore est de 95 décibels par milliwatt (dBm) et que le signal reçu au téléphone est de 70 dBm, le rapport signal/bruit est de 25 dB. (Voir la figure 25.)

Figure 25 : rapport signal/bruit (SNR)



Lorsque vous modifiez le type et l'emplacement de l'antenne, elle peut réduire la distorsion et les interférences de trajets multiples. Le gain de l'antenne ajoute au gain du système et peut réduire les interférences si l'émetteur interférant n'est pas directement devant l'antenne directionnelle.

Bien que les antennes directionnelles puissent être d'une grande valeur pour certaines applications internes, la grande majorité des installations internes utilisent des antennes omnidirectionnelles. La direction doit être strictement déterminée par une étude de site correcte et appropriée. Que vous utilisiez une antenne omnidirectionnelle ou de raccordement, les environnements intérieurs ont besoin d'antennes de diversité pour atténuer la distorsion multichemin. Les radios des points d'accès Cisco Aironet permettent la prise en charge de la diversité.

Atténuation du signal

L'atténuation ou la perte du signal se produit même lorsque le signal passe par l'air. La perte de puissance du signal est plus prononcée lorsque le signal passe par différents objets. Une puissance de transmission de 20 mW équivaut à 13 dBm. Par conséquent, si la puissance transmise au point d'entrée d'une paroi de plâtre est de 13 dBm, la puissance du signal est réduite à 10 dBm lors de la sortie de cette paroi. Ce tableau indique la perte probable de puissance du signal causée par divers types d'objets.

Atténuation du signal causée par différents types d'objets

Objet dans le chemin du signal	Atténuation du signal via l'objet
Mur en plâtre	3 dB
Mur en verre avec cadre métallique	6 dB
Mur de cendres	4 dB
Fenêtre Office	3 dB
Porte métallique	6 dB
Porte métallique en brique	12 dB
Corps humain	3 dB

Chaque site interrogé présente des niveaux différents de distorsion multichemin, de perte de signal et de bruit de signal. Les hôpitaux sont généralement l'environnement le plus difficile à surveiller en raison d'une forte distorsion de trajets multiples, de pertes de signal et de bruit de signal. Les hôpitaux ont besoin de plus de temps pour effectuer des enquêtes, d'une population plus dense de points d'accès et de normes de performance plus élevées. Les ateliers de fabrication et les ateliers sont les prochains plus difficiles à surveiller. Ces sites ont généralement des bardages métalliques et de nombreux objets métalliques sur le sol, ce qui entraîne des signaux réfléchis qui recréent la distorsion multivoie. Les immeubles de bureaux et les sites d'accueil ont généralement une atténuation élevée du signal, mais un degré moindre de distorsion par trajets multiples.

Informations connexes

- Déployer les Contrôleurs de LAN sans fil de la gamme Cisco 440X
- Conception du réseau de référence de la solution
- Caractéristiques techniques du système de communication Vocera
- Support et documentation techniques - Cisco Systems

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.