Déploiement de téléphone IP Vocera dans une infrastructure de réseau sans fil unifié Cisco

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 soutien des Produits de Vocera devrait être obtenu directement des canaux de support de Vocera. Le support technique de Cisco n'est pas formé pour prendre en charge les questions liées Vocera.

Ce guide est un supplément au guide Sans fil de déploiement de contrôleur LAN de Cisco et adresse seulement les paramètres de configuration qui sont particuliers aux périphériques de Vocera VoWLAN en architecture légère. Référez-vous à déployer le pour en savoir plus Sans fil de contrôleurs LAN de gamme de Cisco 440X.

Conditions préalables

Conditions requises

On le suppose que les lecteurs sont au courant des termes et des concepts présentés dans la Téléphonie sur IP SRND de Cisco et le RÉSEAU LOCAL Sans fil SRND de Cisco.

Guide de conception UC de radio — 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

Composants utilisés

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.

Synthèse

Cette table récapitule les quatre fonctions principales et comment elles se comportent dans un réseau de Cisco Unified Wireless.

	Contrôleur simple	Itinérance de la couche 2 de Contrôleur-à-contrôleur	Itinérance de la couche 3 de Contrôleur-à-contrôleur
Badge-à-badge	Aucune configuration spéciale	Aucune configuration spéciale	Aucune configuration spéciale
Badge-à-téléphone	Aucune configuration spéciale	Aucune configuration spéciale	Aucune configuration spéciale
Badge-à-émission	Multidiffusion de contrôleur d'enable	Surveillance IGMP ou passage 4.0.206.0 de Vocera VLAN de débronchement de Multidiffusion de contrôleur d'enable ou plus tard	4.0.206.0 ou plus tard
Emplacement de badge	Aucune configuration spéciale	Aucune configuration spéciale	Aucune configuration spéciale

Aperçu de badge de Vocera

Les badges de transmission permettent à un porteur la transmission instantanée avec n'importe quel autre porteur de badge aussi bien un cheminement d'intégration de l'autocommutateur privé (PBX) et d'emplacement de badge. L'utilisation d'un réseau 802.11b/g Sans fil exige l'utilisation de la livraison de Multidiffusion et de paquet monodiffusion d'UDP avec des conditions requises limitées pour le Qualité de service (QoS) en date de la version 3.1 de logiciel de serveur de

Vocera (construction 1081). Les capacités de cryptage sont 64/128 Confidentialité équivalente aux transmissions par fil (WEP) de bit, Protocole TKIP (Temporal Key Integrity Protocol), Message Integrity Check (MIC), et Temporal Key Integrity Protocol de Cisco (CKIP) combiné avec les capacités d'authentification Open, de la clé Access-Pré-partagée par Wi-Fi Protected (WPA-PSK), de l'Extensible Authentication Protocol WPA-protégé (PEAP) et du Lightweight Extensible Authentication Protocol (LEAP).

Avec le pousser d'un bouton, le serveur de Vocera répond avec `Vocera`, qui est une demande pour émettre des commandes telles que l'**enregistrement**, **où (AM I) /is..** , **appel**, **jeu**, **émission**, **messages**, et ainsi de suite. Le serveur de Vocera fournit les services et/ou l'établissement d'appel nécessaires pour se terminer la demande.

Le système de communication capable 802.11b de Vocera se sert du compactage de propriété industrielle de Voix et de l'utilisation d'une chaîne de port UDP. Le logiciel système de Vocera fonctionne sur des Windows Server qui gèrent l'établissement d'appel, la connexion d'appel et les profils utilisateurs. Ils partnered avec le logiciel de reconnaissance vocale et d'empreinte vocale de la nuance 8.5 afin d'activer des communications vocales de badge. Vocera recommande un serveur de fenêtres séparées pour exécuter le logiciel de solutions de téléphonie de Vocera pour activer la Connectivité de réseau téléphonique public commuté (POTS) avec les badges.

Considérations de capacité d'appel de Vocera

Voyez la section de dimensionnement de réseau de ce document pour d'autres détails.

Capacité de Communications Server de Vocera

Référez-vous aux spécifications système de transmissions de Vocera pour plus d'informations sur la matrice de dimensionnement de serveur de Vocera.

La solution de Vocera

Le badge de Vocera utilise l'unicast et la livraison de paquet de multidiffusion pour fournir plusieurs fonctionnalités principales qui composent cette solution complète. Voici quatre des caractéristiques essentielles qui se fondent sur la livraison appropriée de paquet. Également fournie est une compréhension de base de la façon dont chaque caractéristique utilise le réseau sous-jacent pour la livraison et la fonctionnalité.

- Badge aux transmissions de badge — Quand un utilisateur de Vocera appelle un autre utilisateur, le badge contacte d'abord le serveur de Vocera, au lequel les consultations l'adresse IP du badge de l'appelé et contacte l'utilisateur de badge pour demander l'utilisateur si elles peuvent prendre un appel. Si l'appelé reçoit l'appel, le serveur de Vocera informe le badge appelant de l'adresse IP du badge d'appelé d'installer la transmission directe entre les badges sans davantage d'intervention de serveur. Toute la transmission avec le serveur de Vocera utilise G.711 les codecs et toute la transmission de badge-à-badge utilise un codec de classe des propriétaires de Vocera.
- Transmission de téléphonie de badge — Quand un serveur de téléphonie de Vocera est installé et installation avec une connexion à un PBX, un utilisateur peut appeler des extensions internes hors fonction des lignes téléphoniques PBX ou d'extérieur. Vocera permet à des utilisateurs pour faire des appels ou en disant les nombres (cinq, six, trois, deux) ou en

créant une entrée du carnet d'adresses dans la base de données de Vocera pour la personne ou fonction à ce nombre (par exemple, pharmacie, maison, pizza) le serveur de Vocera détermine le nombre qui s'appelle, en interceptant les nombres dans l'extension ou en regardant le nom dans la base de données et en sélectionnant le nombre. Le serveur de Vocera passe alors ces informations au serveur de téléphonie de Vocera qui se connecte au PBX et génère la Signalisation téléphonique appropriée (par exemple, DTMF). Toute la transmission entre le badge et le serveur de Vocera et le serveur de Vocera et le serveur de téléphonie de Vocera utilisent G.711 les codecs au-dessus de l'UDP d'unicast.

- Émission de Vocera — Un utilisateur de badge de Vocera peut appeler et communiquer à un groupe de porteurs de badge de Vocera en même temps à l'aide de la commande d'émission. Quand un utilisateur annonce à un groupe, le badge de l'utilisateur envoie la commande au serveur de Vocera que puis les consultations les membres du groupe, détermine quels membres du groupe sont en activité, assigne une adresse de multidiffusion pour les utiliser pour cette session d'émission, et envoie un message au badge de chaque utilisateur actif lui demandant de joindre le groupe de multidiffusion avec l'adresse de multidiffusion assignée.
- Fonction d'emplacement de badge — Le serveur de Vocera maintient le Point d'accès auquel chaque badge actif est associé pendant que chaque badge envoie une seconde keepalive 30 au serveur avec le BSSID associé. Ceci permet au système de Vocera pour estimer rudement l'emplacement d'un utilisateur de badge. Cette fonction a un degré de précision relativement bas parce qu'un badge ne pourrait pas être associé au Point d'accès duquel il est le plus proche.

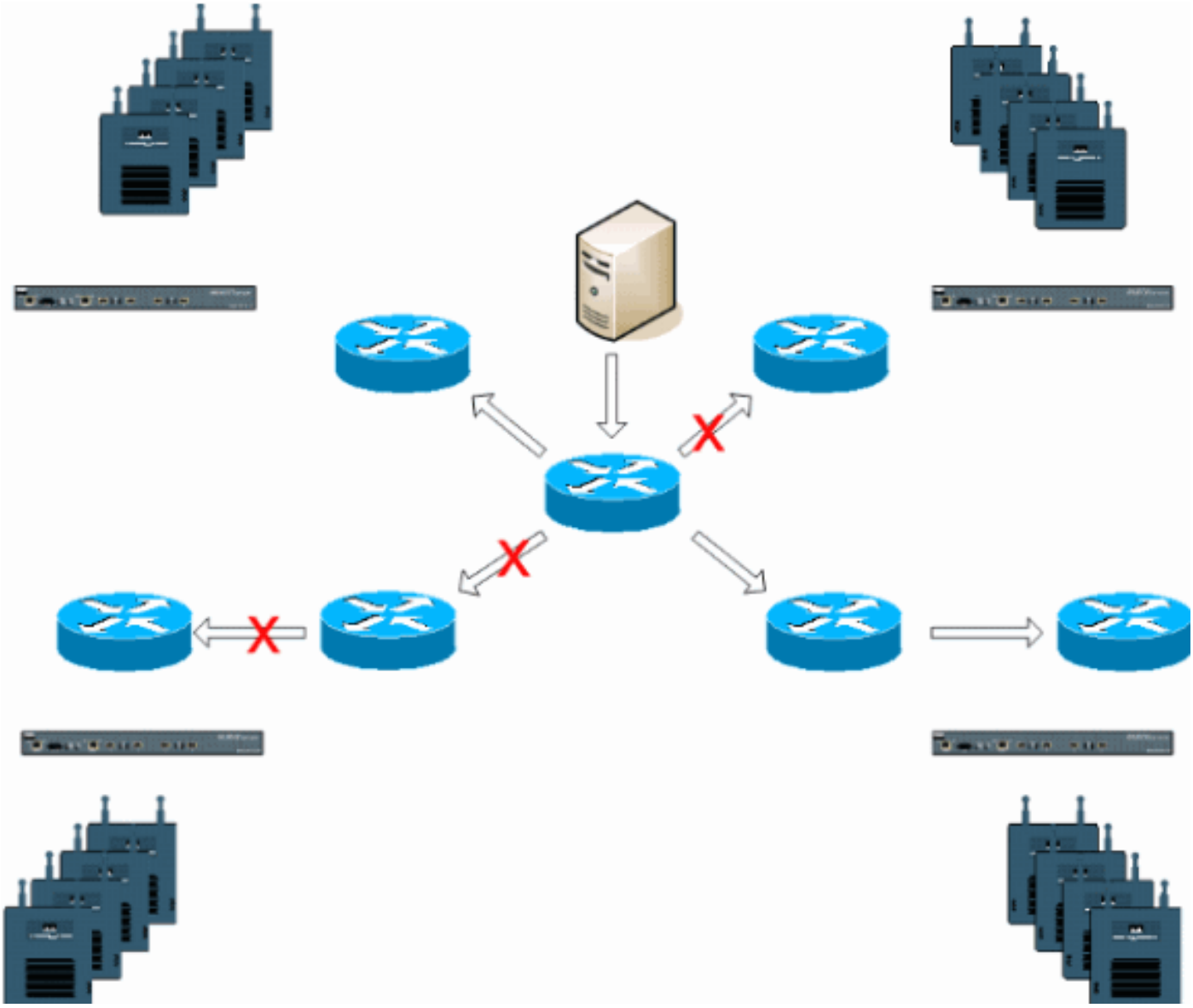
Planification de l'infrastructure de Vocera

Le guide de planification d'infrastructure de Vocera de whitepaper de Vocera , décrit les conditions requises minimum d'analyse de site qui prouvent que le badge devrait avoir un minimum de force du signal de réception de dBm -65, DB que 25 de rapport signal/bruit un plus grand et une superposition et séparation du canal appropriées de Point d'accès. Bien que les badges utilisent une antenne directionnelle semblable d'omni comme carnet qui est utilisé pour une analyse de site, elle n'imite pas le comportement du badge très bien, donné les affects des porteurs sur la force du signal. Donné cette propre exigence et ce comportement du périphérique transmetteur, l'utilisation de l'architecture Cisco et la gestion des ressources de radio est idéale afin de s'assurer qu'il y a un manque de caractéristiques peu communes de site de Radiofréquence (RF).

Le badge de Vocera est un bas périphérique connecté, utilisé à côté du corps avec des capacités limitées de correction d'erreurs de signal. Les conditions requises de Vocera dans ce document peuvent être facilement réalisées. Cependant, il peut devenir accablé s'il y a trop de SSID pour qu'il traite et pour permet au badge pour fonctionner efficacement.

Vue d'ensemble de l'architecture

Figure 1 — Multidiffusion générale en avant et pruneau avec la radio de Protocol de point d'accès léger (LWAPP)



Multidiffusion dans un déploiement LWAPP

La compréhension de la Multidiffusion dans un déploiement LWAPP est nécessaire de déployer la fonction d'émission de Vocera. Ce document couvre plus tard les étapes essentielles pour activer la Multidiffusion dans la solution basée sur contrôleur. Il y a actuellement deux méthodes de la livraison que le contrôleur LWAPP l'utilise pour fournir la Multidiffusion aux clients :

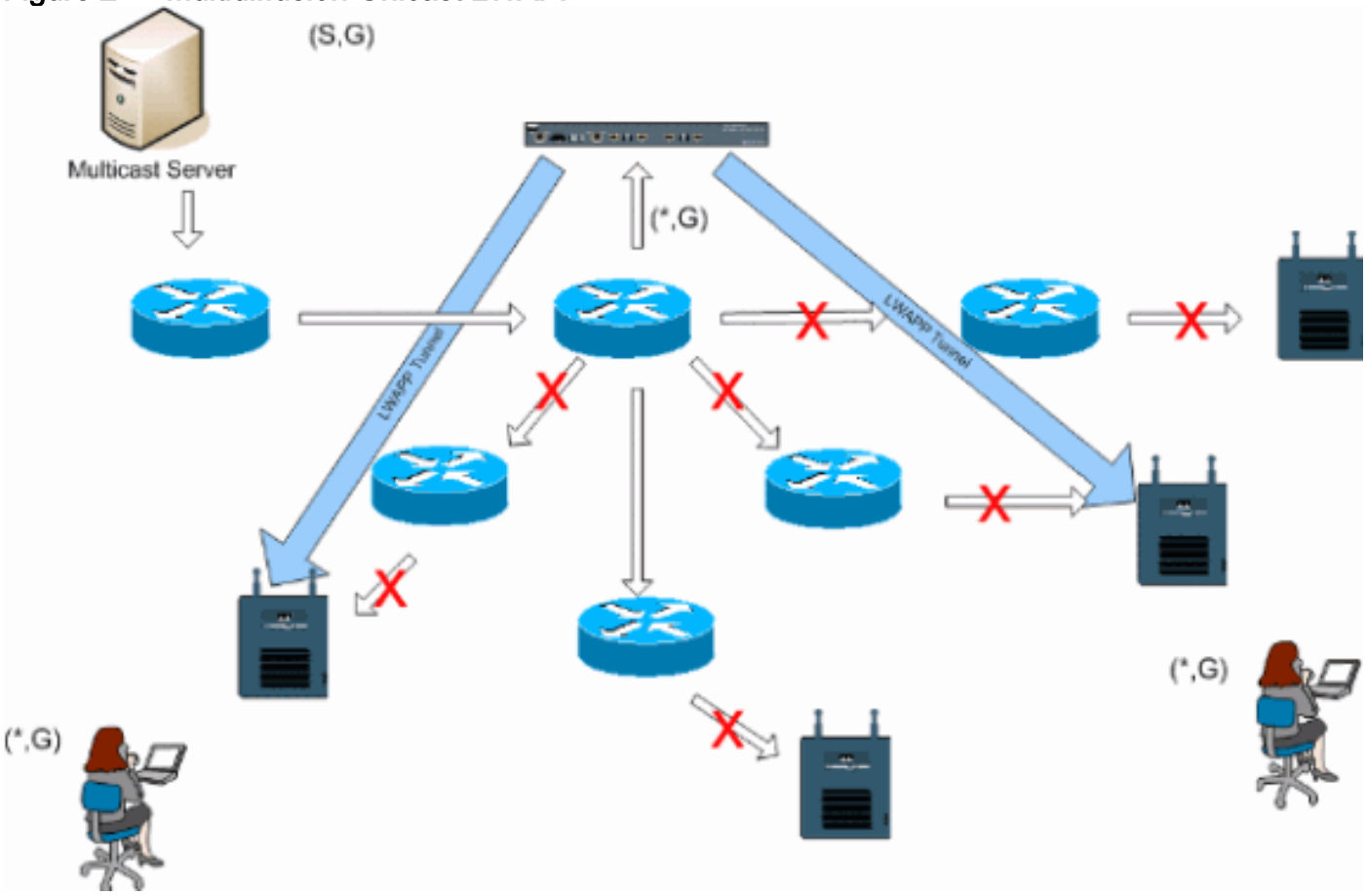
- Unicast-Multidiffusion
- Multidiffusion-Multidiffusion

Méthode de la livraison d'Unicast-Multidiffusion

La méthode de la livraison d'unicast-Multidiffusion crée une copie de chaque paquet de multidiffusion et en avant elle à chaque access-point. Quand un client envoie une Multidiffusion joignez au RÉSEAU LOCAL Sans fil, le Point d'accès en avant que ceci se joignent par le tunnel LWAPP au contrôleur. Le contrôleur pont cette Multidiffusion se joignent sur lui est directement une connexion connectée de réseau local qui est le par défaut VLAN pour le WLAN associé du client. Quand un paquet de multidiffusion IP arrive du réseau au contrôleur, le contrôleur réplique ce paquet avec une en-tête LWAPP pour chaque Point d'accès qui a un client dans le domaine Sans fil qui a joint ce groupe spécifique. Quand la source de Multidiffusion est également un

récepteur dans le domaine Sans fil, ce paquet est également reproduit et expédié de nouveau au même client qui a envoyé ce paquet. Pour des badges de Vocera, ce n'est pas la méthode préférée de la livraison de Multidiffusion dans la solution de contrôleur LWAPP. La méthode de la livraison d'unicast fonctionne avec de petits déploiements. Cependant, en raison du temps système considérable sur le contrôleur LAN Sans fil (WLC), ce n'est jamais la méthode recommandée de la livraison de Multidiffusion.

Figure 2 — Multidiffusion-Unicast LWAPP



Note: Si le groupe VLAN AP sont configurés, et un IGMP se joint est envoyé d'un client par le contrôleur, il est placé sur le par défaut VLAN du WLAN que le client est en ligne. Par conséquent, le client ne pourrait pas recevoir ce trafic de multidiffusion à moins que le client soit un membre de ce domaine par défaut d'émission.

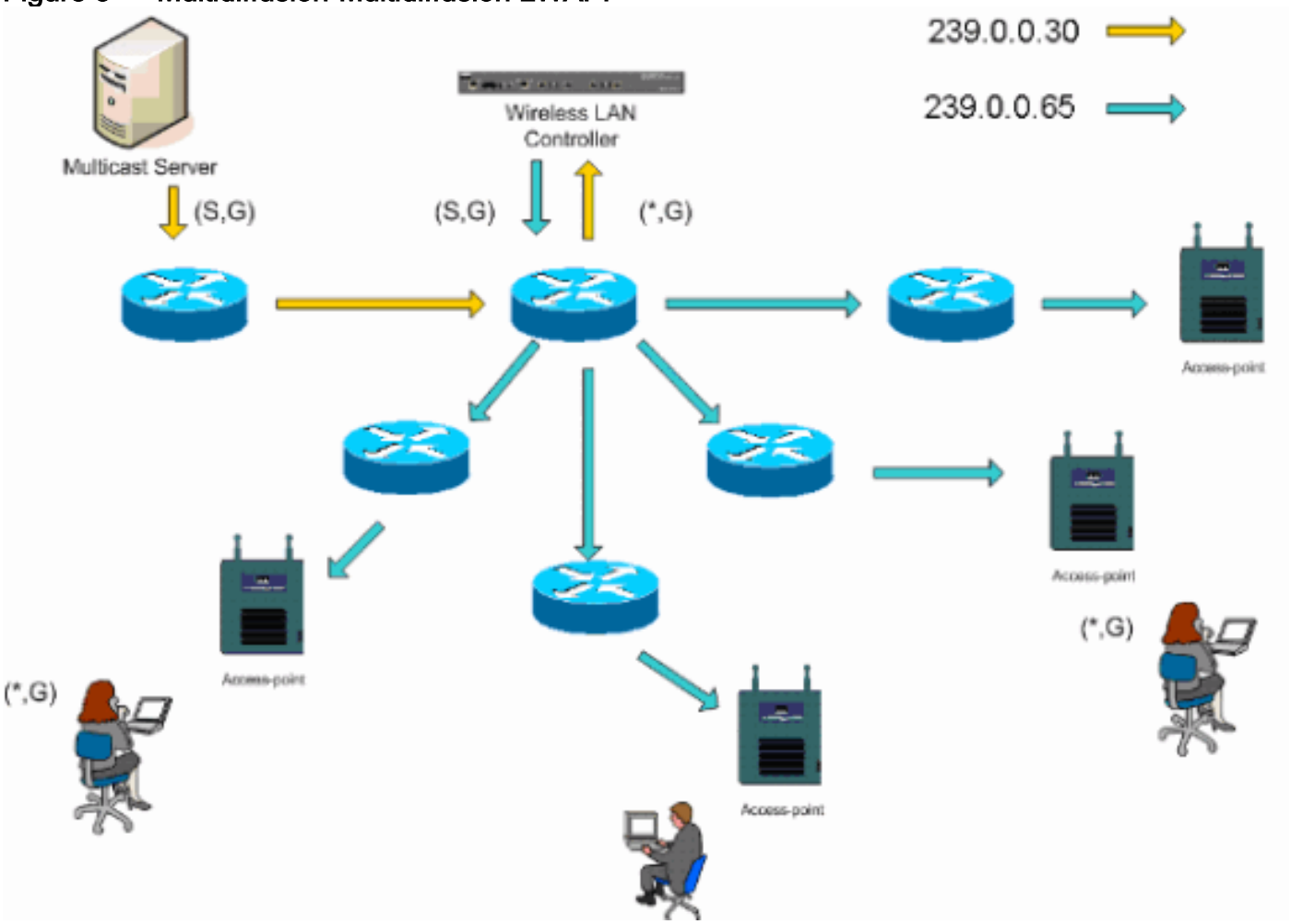
Méthode de la livraison de Multidiffusion-Multidiffusion

La méthode de la livraison de Multidiffusion-Multidiffusion n'exige pas du contrôleur de répliquer chaque paquet de multidiffusion reçu. Le contrôleur est configuré pour une adresse inutilisée de groupe de multidiffusion que chaque Point d'accès va bien à un membre de. Avec la figure 3, le groupe de multidiffusion défini du WLC au Point d'accès est 239.0.0.65. Quand un client envoie une Multidiffusion joignez au WLAN, le Point d'accès en avant que ceci se joignent par le tunnel LWAPP au contrôleur. Le contrôleur en avant ce protocole de couche de liaison sur lui est directement une connexion connectée de réseau local qui est le par défaut VLAN pour le WLAN associé du client. Le routeur qui est local au contrôleur puis ajoute cette adresse de groupe de multidiffusion à cette interface pour expédier ((*, G)) entrée. Avec la figure 3, la Multidiffusion d'exemple se joignent a été envoyée au groupe de multidiffusion 239.0.0.30. Quand de réseau le trafic de multidiffusion maintenant en avant, l'adresse de multidiffusion de 239.0.0.30 est expédié au contrôleur. Le contrôleur encapsule alors le paquet de multidiffusion dans un paquet de multidiffusion LWAPP adressé à l'adresse de groupe de multidiffusion (l'exemple ici est

239.0.0.65) qui est configurée sur le contrôleur et expédiée au réseau. Chaque Point d'accès sur le contrôleur reçoit ce paquet en tant que membre du groupe de multidiffusion de contrôleurs. Le Point d'accès puis en avant les clients/paquet de multidiffusion de serveurs (l'exemple ici est 239.0.0.30) comme émission au WLAN/SSID l'a identifié dans le paquet de multidiffusion LWAPP.

Note: Si vous configurez incorrectement votre réseau multicast, vous pourriez finir par recevant les paquets de multidiffusion du Point d'accès d'un autre contrôleur. Si le premier contrôleur doit fragmenter ce paquet de multidiffusion, le fragment est expédié au réseau et chaque Point d'accès doit passer le temps de relâcher ce fragment. Si vous permettez tout le trafic tel que n'importe quoi de la plage de la Multidiffusion 224.0.0.x, ceci est également encapsulé et ultérieurement expédié par chaque Point d'accès.

Figure 3 — Multidiffusion-Multidiffusion LWAPP



Configuration de Multidiffusion de routeur et de commutateur

Ce document n'est pas un guide de configuration de Multidiffusion de réseau. Référez-vous à configurer le Protocole IP Multicast conduisant pour une histoire complète d'implémentation. Ce document couvre les fondements pour activer la Multidiffusion dans votre environnement de réseau.

Acheminement de Protocole IP Multicast d'enable

L'acheminement de Protocole IP Multicast permet au logiciel de Cisco IOS® pour expédier des paquets de multidiffusion. La commande de configuration globale d'**ip multicast-routing** est exigée pour permettre à la Multidiffusion pour fonctionner dans n'importe quel réseau activé par

Multidiffusion. La commande d'**ip multicast-routing** devrait être activée sur tous les Routeurs dans votre réseau entre le WLC et leurs Points d'accès respectifs.

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

Enable PIM sur une interface

Ceci active l'interface de routage pour l'exécution de Protocole IGMP (Internet Group Management Protocol). Le mode du Protocol Independent Multicast (PIM) détermine comment le routeur remplit sa table de routage de Multidiffusion. L'exemple fourni ici n'exige pas du point de rendez-vous (RP) d'être connu pour le groupe de multidiffusion et donc le clairsemé-dense-mode est le plus desirable donné la nature inconnue de votre environnement de Multidiffusion. Ce n'est pas une recommandation de Multidiffusion d'être configurée pour fonctionner bien que l'interface de la couche 3 directement connectée à votre contrôleur devrait être PIM activé pour que la Multidiffusion fonctionne. Toutes les interfaces entre votre WLC et leurs Points d'accès respectifs devraient être activées.

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

Surveillance IGMP du commutateur VLAN de débronchement

La surveillance IGMP permet un réseau commuté avec la Multidiffusion activée limiter le trafic à ces switchports qui ont des utilisateurs qui veulent que la Multidiffusion soit vue tandis qu'élagage les paquets de multidiffusion des switchports qui ne souhaitent pas voir le flot de Multidiffusion. Dans un déploiement de Vocera, il peut être indésirable pour activer le CGMP ou la surveillance IGMP sur le switchport en amont au contrôleur avec des versions logicielles plus tôt que 4.0.206.0.

L'itinérance et la Multidiffusion ne sont pas définies avec un ensemble de conditions requises de vérifier que le trafic de multidiffusion peut suivre un utilisateur abonné. Bien que le badge de client se rende compte qu'il ait erré, il n'expédie pas un autre IGMP se joignent pour s'assurer que l'infrastructure réseau continue à fournir le trafic de Multidiffusion (émission de Vocera) au badge. En même temps, le Point d'accès LWAPP n'envoie pas une requête générale de Multidiffusion au client d'itinérance pour inciter pour cet IGMP se joignent. Avec une conception de réseaux de Vocera de la couche 2, désactiver la surveillance IGMP permet le trafic à expédier à tous les membres du réseau de Vocera n'importe où ils errent. Ceci s'assure que la caractéristique d'émission de Vocera fonctionne indépendamment d'où le client erre. Désactiver la surveillance IGMP est globalement une tâche très indésirable. La surveillance IGMP d'il est recommandé que seulement soit désactivée sur le Vocera VLAN qui est directement connecté à chaque WLC.

Référez-vous à configurer le pour en savoir plus de surveillance IGMP.

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

Améliorations de Multidiffusion dans la version 4.0.206.0 et plus tard

Avec la release de 4.0.206.0, Cisco introduit une requête IGMP pour permettre à des utilisateurs pour errer à la couche 2 en envoyant une requête du général IGMP quand ceci se produit. Le

client répond alors avec le groupe IGMP qu'ils sont un membre de et ceci pont au réseau câblé comme décrit plus tôt dans ce document. Quand un client erre à un contrôleur qui n'a pas Connectivité de la couche 2, ou une couche 3 errent, le routage synchrone est ajouté pour des paquets de source multicast. Quand un client, qui s'est terminé une couche 3 errent des sources un paquet de multidiffusion du réseau Sans fil, le contrôleur étranger encapsule ce paquet dans les Ethernets au-dessus d'IP (EoIP) dans le tunnel IP au contrôleur d'ancre. Le contrôleur d'ancre puis en avant qui aux clients sans fil localement a associé aussi bien que jette un pont sur ceci de nouveau au réseau câblé où il est conduit suivre des méthodes normales de routage de Multidiffusion.

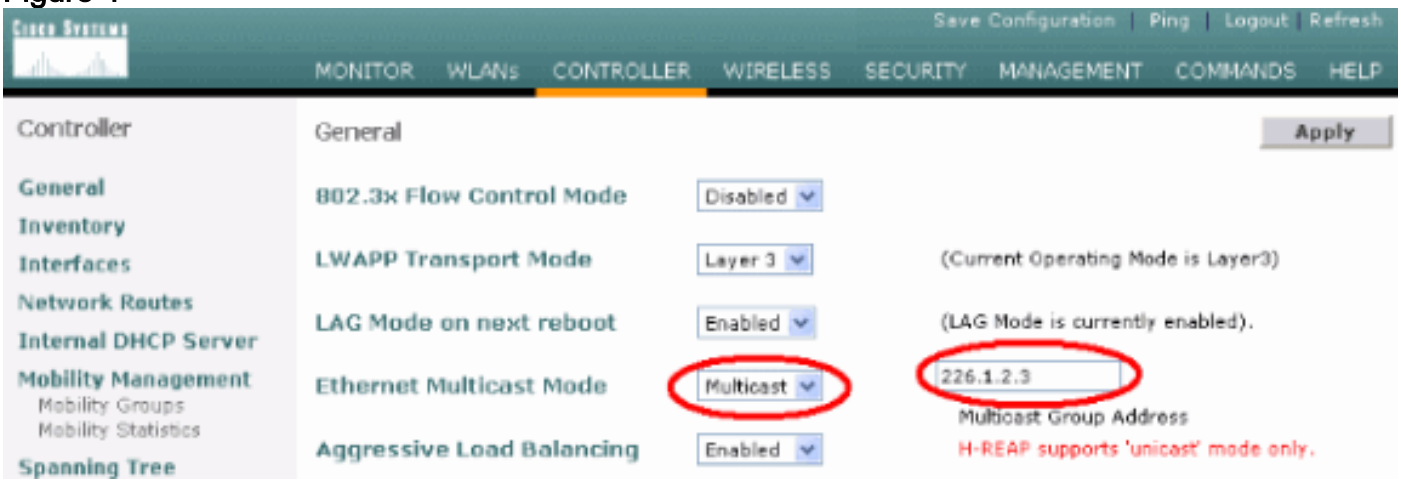
Scénarios de déploiement

Ces trois scénarios de déploiement couvrent des pratiques recommandées et des paramètres de conception d'aider avec un déploiement réussi de badge de Vocera :

- Déploiement simple de contrôleur
- Plusieurs déploiement de la couche 2 de contrôleur
- Plusieurs déploiement de la couche 3 de contrôleur

Comprenant comment les caractéristiques de badge de Vocera interactives dans un environnement de split MAC LWAPP est essentielle. Avec tous les scénarios de déploiement, la Multidiffusion devrait être activée et l'Équilibrage de charge agressif devrait être désactivé. Tout le badge WLAN devrait être contenu dans le même domaine d'émission à travers votre tout le réseau.

Figure 4



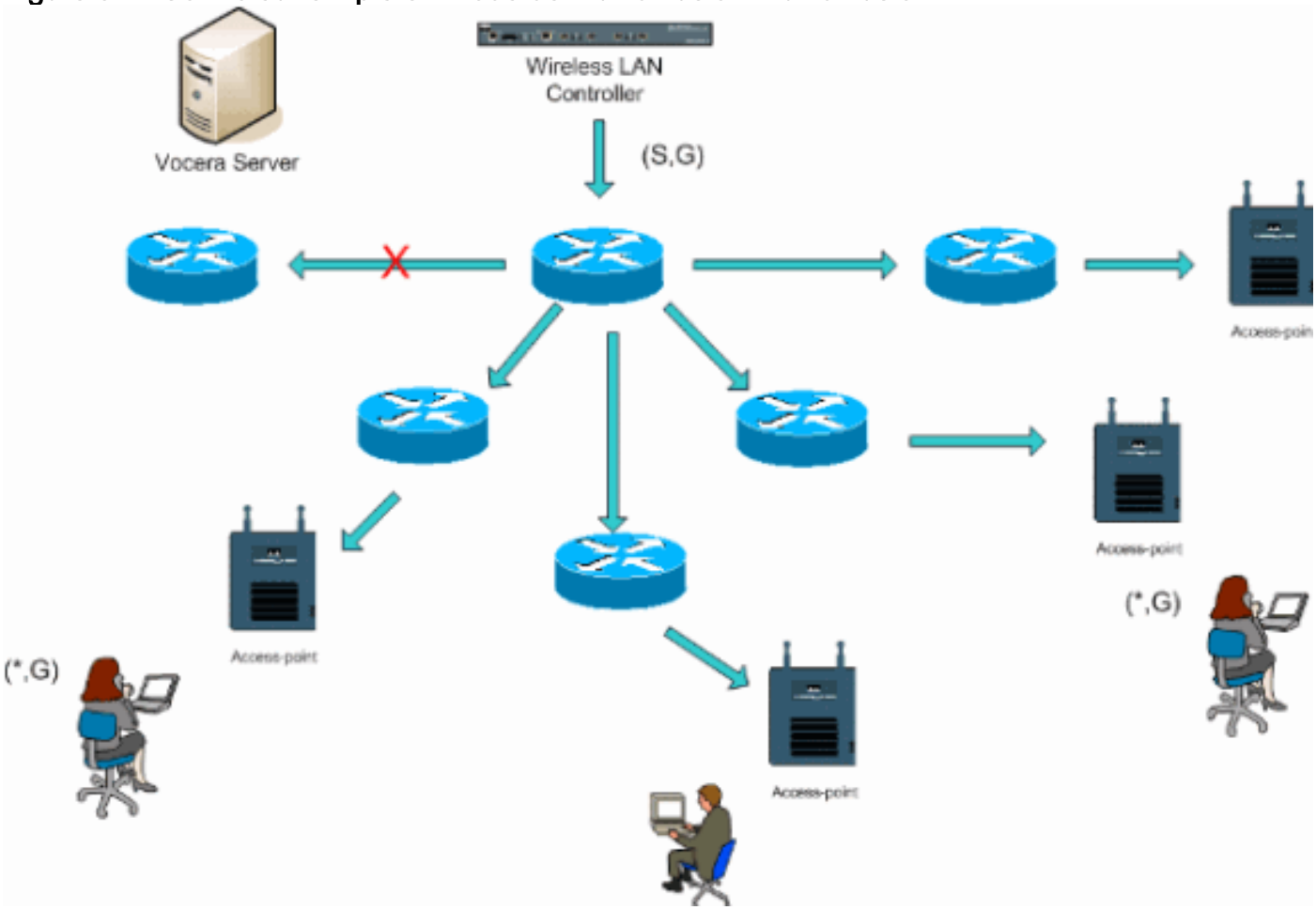
Déploiement simple de contrôleur

C'est le scénario de déploiement le plus simple. Il te permet pour déployer la solution de badge de Vocera avec peu de soucis de déploiement. Votre réseau doit être activé pour le Protocole IP Multicast conduisant pour laisser seulement les Points d'accès pour recevoir les paquets de multidiffusion LWAPP. S'il y a lieu, vous pouvez limiter la complexité de Multidiffusion de réseau en configurant tous les Routeurs et Commutateurs avec le groupe de multidiffusion de contrôleurs.

La Multidiffusion étant configuré globalement sur le contrôleur, le SSID approprié, les paramètres de sécurité, et tous les Points d'accès ont enregistré la solution de badge de Vocera et toutes ses fonctions fonctionne comme prévu. Avec la fonction d'émission de Vocera, un utilisateur erre et le trafic de multidiffusion suit comme prévu. Il n'y a aucun paramétrage supplémentaire exigé pour être configuré pour permettre à cette solution pour fonctionner correctement.

Quand un badge de Vocera envoie un message multicast, comme il fait avec l'émission de Vocera, il est expédié au contrôleur. Le contrôleur encapsule alors ce paquet de multidiffusion dans un paquet de multidiffusion LWAPP. L'infrastructure réseau en avant ce paquet à chaque Point d'accès qui est connecté à ce contrôleur. Quand le Point d'accès reçoit ce paquet, il regarde alors l'en-tête de Multidiffusion LWAPP déterminer à quel WLAN/SSID il annonce alors ce paquet.

Figure 5 — Contrôleur simple en mode de Multidiffusion-Multidiffusion



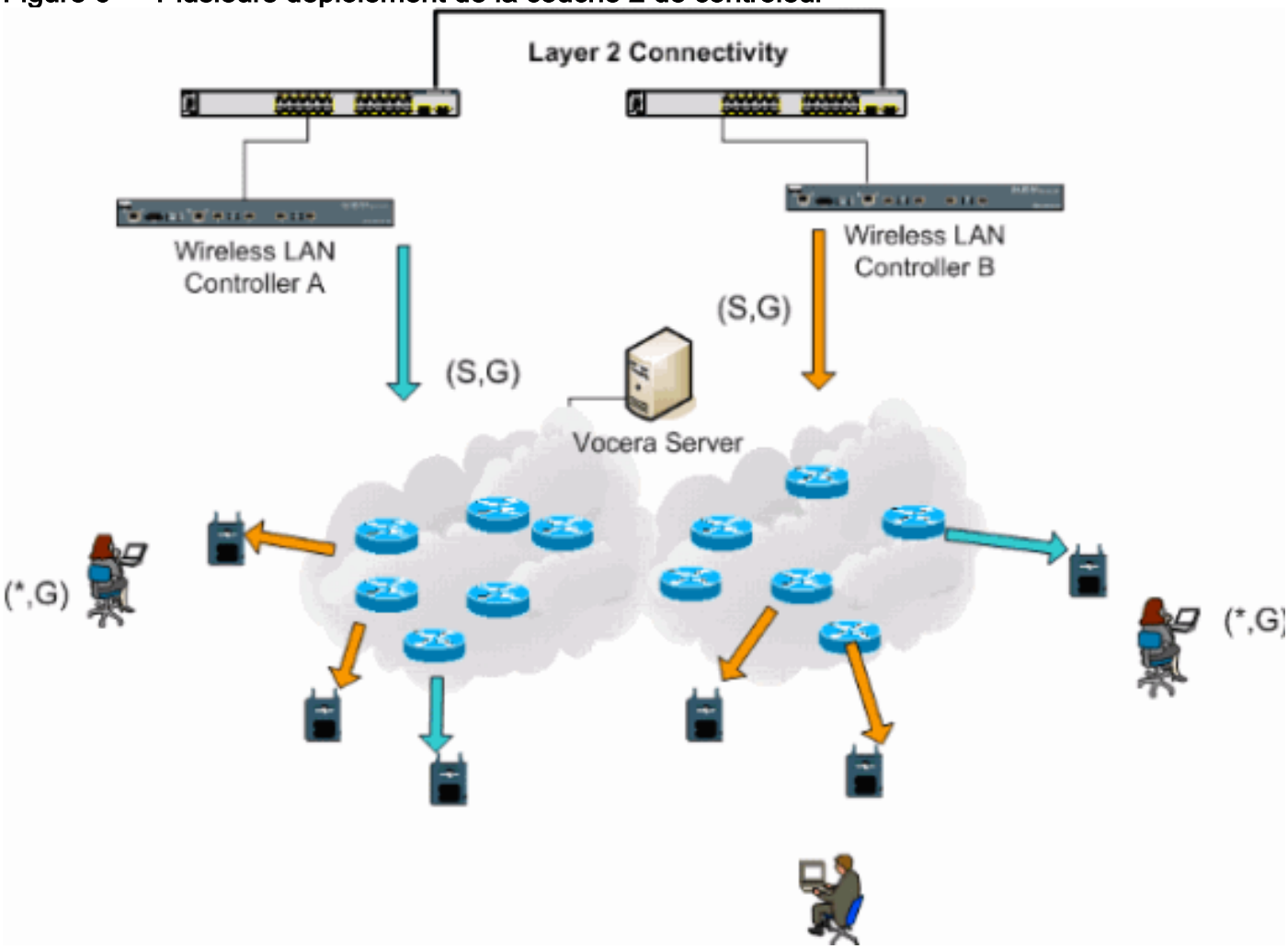
Plusieurs déploiement de la couche 2 de contrôleur

Les plusieurs contrôleurs doivent tout avoir la Connectivité entre eux par l'intermédiaire du même domaine d'émission de la couche 2. Les deux contrôleurs sont configurés pour la Multidiffusion comme affiché, utilisant les groupes de multidiffusion identiques de Point d'accès sur chaque contrôleur pour limiter la fragmentation. Avec la supposition que ce domaine d'émission de la couche 2 est connecté par l'intermédiaire d'un commutateur commun ou un ensemble commun de Commutateurs, CGMP/IGMP pillant sur ces Commutateurs doit être désactivé pour ce VLAN simple ou passage 4.0.206.0 ou logiciel postérieur WLC. Avec la fonction d'émission de Vocera et un utilisateur errez d'un Point d'accès sur un contrôleur à un Point d'accès sur un contrôleur différent, là n'est aucun mécanisme pour IGMP se joint pour être expédié au nouveau port de la couche 2 pour que la surveillance IGMP fonctionne. Sans paquet IGMP atteignant le commutateur capable en amont de CGMP ou IGMP, le groupe de multidiffusion spécifié n'est pas expédié au contrôleur et donc n'est pas reçu par le client. Dans certains cas ceci pourrait fonctionner, si un client qui fait partie du même groupe d'émission de Vocera a déjà envoyé ce paquet IGMP avant que le client d'itinérance erre sur le nouveau contrôleur avec les avantages de la version 4.0.206.0, un client qui erre à un autre contrôleur pendant qu'une couche 2 errent reçoit une requête du général IGMP juste après l'authentification. Le client devrait alors répondre avec les groupes d'intérêt et le nouveau contrôleur est alors jeté un pont sur ceci localement au commutateur connecté. Ceci permet les avantages d'IGMP et de CGMP sur vos Commutateurs

en amont.

Vous pouvez créer le badge supplémentaire SSID et poser 2 domaines pour les réseaux distincts de badge tant que votre réseau est configuré pour passer le trafic de multidiffusion convenablement. En outre, chaque domaine d'émission de la couche 2 de Vocera créé doit exister partout un contrôleur est connecté au réseau pour pour ne pas casser la Multidiffusion.

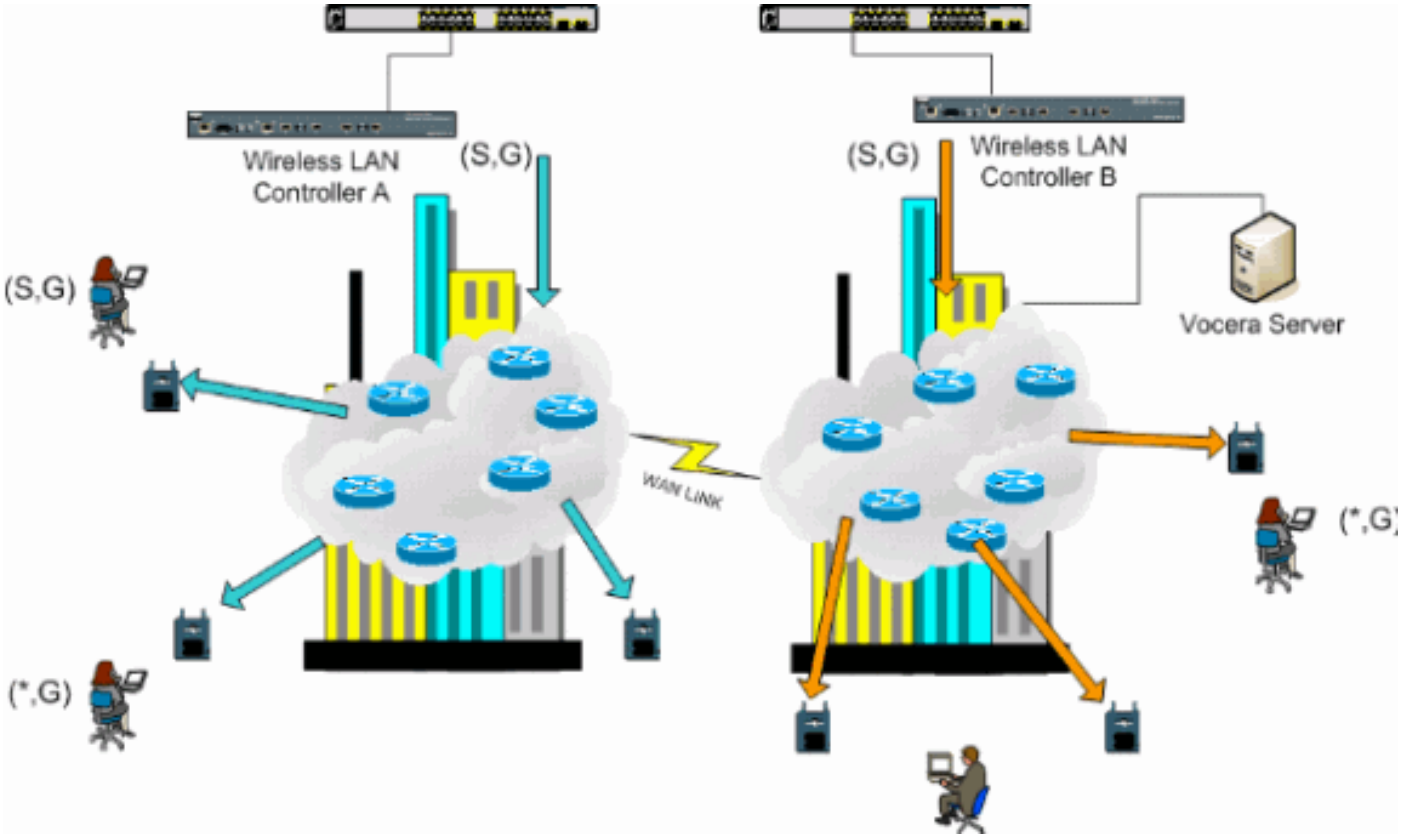
Figure 6 — Plusieurs déploiement de la couche 2 de contrôleur



Plusieurs déploiement de la couche 3 de contrôleur

La stratégie errante de déploiement de la couche 3 devrait seulement être utilisée avec l'itinérance de contrôleur-à-contrôleur avec version logicielle 4.0.206.0 WLC ou plus tard. Si un client qui a été connecté au groupe d'émission de Vocera et reçoit le flot approprié de Multidiffusion et erre à un autre contrôleur pendant qu'une couche 3 errent avec l'itinérance de la couche 3 LWAPP configurée, il est questionné pour les groupes de multidiffusion. Le client, quand approvisionnement au même groupe d'émission de Vocera, a ces paquets livrés au contrôleur d'ancre par le tunnel d'EoIP et a ces paquets conduits par des méthodes de routage normales de Multidiffusion.

Figure 7 — Plusieurs déploiement de la couche 3 de contrôleur



Déploiements VoWLAN : Reccommendations de Cisco

Les réseaux de Téléphonie IP sans fil exigent la planification soigneuse rf. Une analyse de site complète de Voix est souvent exigée pour déterminer les niveaux appropriés de la couverture Sans fil et pour identifier des sources d'interférence. Des choix de placement de Point d'accès et de sélection d'antenne peuvent être considérablement soulagés avec l'aide des résultats d'une analyse de site valide de Voix. La considération la plus importante est la puissance de transmission du téléphone Sans fil. Dans le meilleur des cas le téléphone apprend la puissance de transmission du Point d'accès et ajuste sa puissance de transmission à celle du Point d'accès.

Bien que la majorité des réseaux Sans fil aujourd'hui soient déployées après une analyse de site étendue rf, ils sont faits avec maintenir le service de données dans l'esprit aussi bien. Les téléphones VoWLAN sont susceptibles d'avoir différentes caractéristiques d'itinérance et différentes conditions requises de couverture que ceux d'un adaptateur typique WLAN pour un client mobile tel qu'un ordinateur portable. Par conséquent, une analyse de site supplémentaire pour la Voix est souvent recommandée pour se préparer aux exigences de marche de plusieurs clients VoWLAN. Cette analyse supplémentaire donne l'occasion d'accorder les Points d'accès pour s'assurer que les téléphones VoWLAN ont assez de couverture et bande passante rf pour fournir la Qualité vocale appropriée.

Pour des informations supplémentaires sur des considérations de conception rf, référez-vous au chapitre sur des considérations de conception de Radiofréquence (RF) WLAN du guide Sans fil de conception de RÉSEAU LOCAL de Cisco, disponible chez http://cisco.com/go/srnd.

Recommandations pour des bâtiments, des hôpitaux, et des entrepôts de Multi-plancher

Considérez les facteurs répertoriés dans cette section quand vous examinez des bâtiments, des hôpitaux, et des entrepôts de multi-plancher.

Méthodes et matériaux de construction

Beaucoup d'aspects de la construction de bâtiments sont inconnus ou masqués de l'analyse de site, ainsi vous pourriez devoir saisir ces informations d'autres sources (telles que les dessins architecturaux). Quelques exemples des méthodes et les matériaux typiques de construction qui affectent la plage et la zone de couverture de Points d'accès incluent le film métallique sur le verre de fenêtre, verre plombé, murs acier-cloutés, planchers de ciment et murs avec le renfort en acier, isolation soutenue par la feuille métallique, cages d'escalier et axes d'argumentaire, mettant d'aplomb des canaux et des éléments, et beaucoup d'autres.

Stocks

Les divers types d'inventaire peuvent affecter la plage rf, en particulier ceux avec la teneur élevée d'acier ou en eau. Quelques éléments à surveiller incluent des boîtes en carton, aliment pour animaux familiers, paint, des produits pétroliers, des pièces de moteur, et ainsi de suite.

Niveaux d'inventaire

Veillez-vous pour exécuter une analyse de site aux niveaux d'inventaire maximaux ou à une époque de plus de forte activité. Un entrepôt à un niveau des stocks de 50% a une empreinte de pas très différente rf que le même entrepôt à un niveau d'inventaire de 100%.

Niveaux d'activité

De même, une zone de bureau après des heures (sans personnes) a une empreinte de pas différente rf que la même zone complètement des personnes au cours de la journée. Bien que beaucoup de parties de l'analyse de site puissent être conduites sans pleine profession, il est essentiel de conduire la vérification d'analyse de site et de tordre les valeurs principales pendant un moment où l'emplacement est occupé. Plus les conditions requises d'utilisation et la densité des utilisateurs sont élevées, plus il est d'avoir une solution bien conçue de diversité important. Quand plus d'utilisateurs sont présents, plus de signaux sont reçus sur le périphérique de chaque utilisateur. Les signaux supplémentaires entraînent plus de conflit, de zéros, et de déformation plus multivoie. La diversité sur les aides de Point d'accès (Antennes) réduisent ces conditions.

Bâtiments de Multi-plancher

Maintenez dans l'esprit ces instructions quand vous menez une analyse de site pour un immeuble de bureau typique :

- Le bloc d'axes d'argumentaire et reflètent des signaux rf.
- Les réserves à matériel avec l'inventaire absorbent des signaux.
- Les bureaux intérieurs avec les murs durs absorbent des signaux rf.
- Les salles de pause (cuisines) peuvent produire 2.4 gigahertz d'interférence par l'utilisation des fours à micro-ondes.
- Les laboratoires de test peuvent produire 2.4 gigahertz ou 5 gigahertz d'interférence, créant la distorsion multivoie et les shadow rf.
- Les compartiments tendent à absorber et signaux de bloc.
- Les salles de conférence exigent la couverture élevée de Point d'accès parce qu'elles sont des domaines de l'utilisation élevée.

La précaution supplémentaire doit être gérée quand vous examinez des équipements de multi-plancher. Les Points d'accès sur différents planchers peuvent gêner les uns avec les autres aussi facilement que des Points d'accès placés sur le même plancher. Il est possible d'utiliser ce comportement à votre avantage pendant une analyse. Utilisant des Antennes plus à gain élevé, il pourrait être possible de pénétrer des planchers et des plafonds et de fournir la couverture aux planchers au-dessus aussi bien qu'au-dessous du plancher où le Point d'accès est monté. Faites attention à ne pas superposer des canaux entre les Points d'accès sur différents planchers ou les Points d'accès sur le même plancher. Dans des bâtiments de multi-locataire, il pourrait y avoir des problèmes de sécurité qui exigent l'utilisation des alimentations inférieures de transmission et diminuent des Antennes de gain pour garder des signaux hors des bureaux voisins.

Hôpitaux

Le procédé d'analyse pour un hôpital est plus ou moins identique que celui pour une entreprise, mais l'affichage d'une installation d'hôpital tend à différer de ces manières :

- Les bâtiments d'hôpital tendent à passer par beaucoup de projets et d'ajouts de reconstruction. Chaque construction supplémentaire est susceptible d'avoir différents matériaux de construction avec des différents niveaux d'atténuation.
- La traversée de signal par des murs et des planchers dans les zones patientes est en général minimale, que les aides créent des micro-cellules et des variations multivoies.
- Le besoin de bande passante augmente avec l'utilisation croissante du matériel d'ultrason WLAN et d'autres applications portatives de représentation. Le besoin d'augmentations de bande passante en plus de Voix Sans fil aussi bien.
- Les cellules de santé sont petites, et l'itinérance sans couture est essentielle, particulièrement avec des Applications voix.
- La superposition de cellules peut être élevée, et ainsi peut creuser des rigoles la réutilisation.
- Les hôpitaux peuvent avoir plusieurs types de réseaux Sans fil installés. Ceci inclut 2.4 gigahertz de matériel non-802.11. Ce matériel peut entraîner le conflit avec d'autres réseaux 2.4 gigahertz.
- Les Antennes fixées au mur de correctif de diversité et les Antennes omnidirectionnelles plafond-montées de diversité sont populaires, mais maintiennent dans l'esprit que la diversité est exigée.

Entrepôts

Les entrepôts ont de grands terrains découverts qui contiennent souvent les étagères élevées de mémoire. Beaucoup de fois, ces étagères atteignent presque au plafond, où des Points d'accès sont typiquement placés. De telles étagères de mémoire peuvent limiter le domaine que le Point d'accès peut couvrir. Dans des ces cas, envisagez de placer des Points d'accès sur d'autres emplacements sans compter que le plafond, tel que les murs latéraux et les piliers de ciment. Considérez également ces facteurs quand vous examinez un entrepôt :

- Les niveaux d'inventaire concernent le nombre de Points d'accès requis. Testez la couverture avec deux ou trois Points d'accès dans des emplacements prévus de placement.
- Les superpositions inattendues de cellules sont probables en raison des variations multivoies. La qualité du signal varie plus que le point fort de ce signal. Les clients pourraient s'associer et opérer mieux avec des Points d'accès plus loin loin qu'avec les Points d'accès voisins.
- Pendant une analyse, les Points d'accès et les Antennes habituellement n'ont pas un câble

d'antenne les connectant. Mais dans un environnement de production, le Point d'accès et l'antenne pourraient exiger des câbles d'antenne. Tous les câbles d'antenne introduisent la perte de signal. L'analyse la plus précise inclut le type d'antenne à installer et la longueur de câble à installer. Un bon outil à l'utiliser pour simuler le câble et sa perte est un atténuateur dans un kit d'analyse.

L'examen d'une installation industrielle est semblable à examiner un entrepôt, sauf qu'il pourrait y avoir beaucoup plus de sources d'interférence rf à une installation industrielle. En outre, les applications à une installation industrielle exigent habituellement plus de bande passante que ceux d'un entrepôt. Ces applications peuvent inclure la représentation visuelle et la Voix Sans fil. La déformation multivoie est susceptible d'être le plus grand problème de performances à une installation industrielle.

Mécanismes de sécurité pris en charge

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

Considérations de LEAP

Le LEAP permet des périphériques à authentifier mutuellement (point de badge-à-Access et point-à-badge d'accès) a basé sur un nom d'utilisateur et 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 par dictionnaire ASLEAP devrait être considérée quand vous décidez d'utiliser le LEAP en tant que votre solution de sécurité :

Référez-vous à l'attaque par dictionnaire sur le pour en savoir plus de vulnérabilité de LEAP de Cisco.

Si le LEAP est utilisé, un serveur LEAP-conforme de RAYON, tel que le serveur de contrôle d'accès de Cisco (ACS), est requis de permettre d'accéder à la base de données utilisateur. Cisco ACS peut ou enregistrer le nom d'utilisateur et la base de données de mots de passe localement, ou elle peut accéder à ces informations à partir d'un répertoire externe de NT de Microsoft Windows. En utilisant le LEAP, assurez-vous que des mots de passe fort sont utilisés sur tous les périphériques sans fil. Des mots de passe fort sont définis en tant qu'être entre 10 et 12 caractères longs et peuvent inclure le haut de casse et les minuscules aussi bien que les caractères particuliers.

Puisque tous les badges utilisent le même mot de passe et il est enregistré dans le badge, Cisco recommande que vous utilisiez différents noms d'utilisateur et mots de passe sur des clients de données et des clients Sans fil de Voix. Cette pratique aide avec le cheminement et le dépannage aussi bien que la Sécurité. Bien que ce soit une option de configuration valide d'employer une base de données externe (d'off-ACS) pour enregistrer les noms d'utilisateur et les mots de passe pour les badges, Cisco ne recommande pas cette pratique. Puisque l'ACS doit être questionné toutes les fois que le badge erre entre les Points d'accès, le retard imprévisible pour accéder à une base de données d'off-ACS pourrait entraîner le retard excessif et la médiocre qualité de voix.

Infrastructure de réseau sans fil

Le réseau de Téléphonie IP sans fil, juste comme un réseau de câble de Téléphonie sur IP, exige la planification rigoureuse pour la configuration VLAN, le dimensionnement de réseau, le transport

de Multidiffusion, et les choix de matériel. Pour les réseaux câblé et de Téléphonie IP sans fil, séparez la Voix et les données VLAN sont souvent la plupart de façon efficace de déploiement suggéré d'assurer la bande passante de réseau et la facilité suffisantes du dépannage.

Voix, données et Vocera VLAN

Les VLAN fournissent un mécanisme pour segmenter des réseaux dans un ou plusieurs domaines d'émission. Les VLAN sont particulièrement importants pour des réseaux de Téléphonie sur IP, où la recommandation typique est de séparer le trafic voix et de données dans différents domaines de la couche 2. Cisco recommande que vous configuriez des VLAN distincts pour les badges de Vocera de l'autre trafic voix et de données : un VLAN indigène pour le trafic d'administration de Point d'accès, données VLAN pour le trafic de données, une Voix ou un VLAN auxiliaire pour le trafic vocal, et un VLAN pour les badges de Vocera. Une Voix distincte VLAN permet au réseau de tirer profit du marquage de la couche 2 et fournit la file d'attente à priorité déterminée au port de commutateur d'accès de la couche 2. Ceci s'assure que QoS approprié est donné pour de diverses classes du trafic et aide à résoudre des problèmes d'adressage tels que l'adressage IP, la Sécurité, et le calcul des dimensions de réseau. Les badges de Vocera utilisent une caractéristique d'émission qui utilise la Multidiffusion pour livrer. Ce VLAN commun s'assure que quand un badge erre entre les contrôleurs, ce reste une partie du groupe de multidiffusion. Ce dernier processus est discuté en détail quand la Multidiffusion est adressée plus tard dans ce document.

Dimensionnement de réseau

Le dimensionnement de réseau de Téléphonie sur IP est essentiel pour s'assurer que la bande passante et les ressources adéquates sont disponibles pour satisfaire les exigences présentées par la présence du trafic vocal. En plus des directives de conception habituelles de Téléphonie sur IP pour les composants de classement par taille tels que des ports de passerelle PSTN, les transcodeurs, bande passante BLÊME, et ainsi de suite, considèrent également ces questions 802.11b quand vous classez votre réseau de Téléphonie IP sans fil. Les badges de Vocera sont une application spécialisée qui épuisent le nombre de clients câblés au delà de nos recommandations typiques de déploiement.

Nombre de périphériques 802.11b par Point d'accès

Cisco recommande que vous ayez pas 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 basés en fonction si c'est un appel de badge-à-badge (codec de propriété industrielle de faible débit) ou un appel de badge-à-téléphone (G.711 codec). Cette table affiche un pourcentage de bande passante disponible par des débits de données et te donne une image plus claire du débit prévu :

Processus d'appel	Mbits/s 1	2 Mbits/s	5.5 Mbits/s	11 Mbits/s
Badge-à-téléphone (G.711)	20.7%	11.8%	6.3%	4.7%
Badge-à-badge (codecs de propriété	9.4%	6.1%	4.2%	3.6%

industrielle de faible débit)				

Commutez les recommandations

Note: Si vous utilisez une gamme Cisco Catalyst 4000 commute en tant que routeur principal dans le réseau, s'assure qu'il contient, au minimum, une engine 2+ (SUP2+) de superviseur ou le module de l'engine 3 de superviseur (SUP3). Le module SUP1 ou SUP2 peut entraîner des retards d'itinérance, de même que peut Cisco Catalyst 2948G, 2980G, 2980G-A, 4912, et les Commutateurs 2948G-GE-TX.

Vous pouvez créer un modèle de port de commutateur pour l'usage quand vous configurez n'importe quel port de commutateur pour la connexion à un Point d'accès. Ce modèle devrait ajouter toutes les caractéristiques de Sécurité et de résilience de spécification de base du modèle de bureau standard. En outre, quand vous reliez le Point d'accès à un commutateur de Cisco Catalyst 3750, vous pouvez optimiser la représentation du Point d'accès à l'aide des commandes multicouche de QoS de la commutation (MLS) de limiter le débit de port et de tracer le Classe de service (Cos) aux configurations de Differentiated Services Code Point (DSCP).

Aucun trafic qui n'est pas exigé par des clients WLAN ne devrait être envoyé à un Point d'accès. Un modèle devrait être conçu de telle manière que les aides créent une connexion réseau sécurisée et résiliente avec ces configurations :

- Renvoyez les configurations des ports pour se transférer — Empêche des conflits de configuration en effaçant toutes les configurations des ports préexistantes.
- Protocole DTP (Dynamic Trunking Protocol) de débronchement — Désactive la jonction dynamique, qui n'est pas nécessaire pour la connexion à un Point d'accès.
- Protocole PAgP (Port Aggregation Protocol) de débronchement — PagP est activé par défaut mais n'est pas nécessaire pour des ports d'utilisateur-revêtement.
- Port Fast d'enable — Permet à un commutateur pour reprendre rapidement la transmission du trafic si un lien de spanning-tree descend.
- Configurez le VLAN sans fil — Crée un seul VLAN sans fil qui isole le trafic Sans fil d'autres données, Voix, et VLAN de gestion. Ceci isole le trafic et assure un plus grand contrôle du trafic.
- Qualité de service (QoS) d'enable ; ne faites pas confiance au port (marque vers le bas à 0) — assure le traitement approprié du trafic prioritaire, y compris des téléphones IP, et empêche des utilisateurs de la bande passante excessive consumante en modifiant leurs PC.

Des interrupteurs d'alimentation en ligne WS-C3750-48PS-S peuvent être utilisés pour fournir l'alimentation aux Points d'accès qui sont capables de recevoir l'alimentation en ligne.

Le Catalyst 6500 te permet pour expédier des paquets à la ligne débit avec toutes les configurations décrites ici aussi bien qu'intégrer de nombreux modules de service. Le module de service sans fil (WiSM) te permet pour avoir deux contrôleurs chacun avec la capacité pour contrôler 150 Points d'accès pièce. Avec jusqu'à cinq WiSMs par châssis, ceci te permet pour contrôler plus de 1500 Points d'accès qui prennent en charge 50,000 clients dans une architecture de commutation simple de hautes performances.

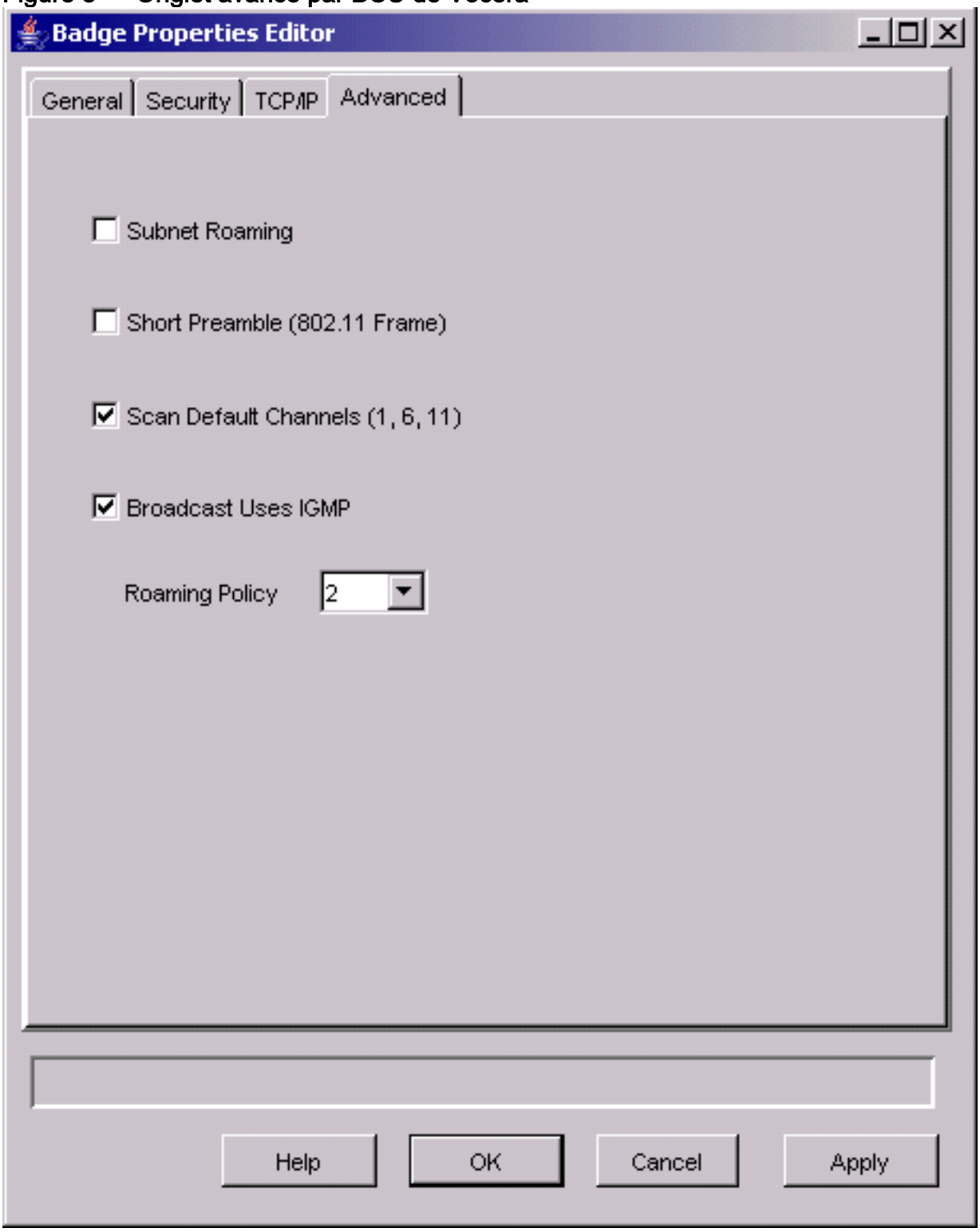
Déploiements et configuration

Configuration de badge

L'utilitaire de configuration de badge de Vocera (BCU) et la configuration du badge peuvent introduire l'itinérance et la latence dans votre environnement si faits inexactement. Utilisant le BCU et l'éditeur de Properties de badge (BPE), vérifiez ces configurations (voir le schéma 8) :

- **L'itinérance de sous-réseau** est désactivée.
- **Les canaux par défaut de balayage (1,6,11)** est vérifiés.
- **Les utilisations IGMP d'émission** est activées.
- La stratégie errante est placée à **2** ou plus élevé.

Figure 8 — Onglet avancé par BCU de Vocera



Quand l'**itinérance de sous-réseau** est vérifiée, elle demande au badge de demander une nouvelle adresse IP après chacune errent. Dans l'environnement LWAPP, les aides d'infrastructure mettent à jour la Connectivité de client à la couche 3. Quand un client de Voix doit attendre le serveur DHCP pour répondre avant qu'il puisse envoyer ou recevoir des paquets, le retard et instabilité sont introduits. Si les **canaux par défaut de balayage (1,6,11)** n'est pas vérifiés, le badge balaye tous les canaux 802.11b quand le badge regarde pour errer. Ceci empêche l'expédition des paquets et de l'itinérance sans couture.

Optimisation AutoRF pour votre environnement

Comme décrit dans la section de recommandations de ce document, il est important de comprendre que chaque site l'a est de posséder des caractéristiques rf. AutoRF ou Gestion des ressources radio (RRM) pourrait devoir être accordé, à condition que chaque site soit différent et AutoRF/RRM est accordé pour votre environnement.

Avant que vous ajustiez AutoRF, référez-vous à la gestion des ressources par radio sous le pour en savoir plus de réseaux sans fil unifié.

RRM te permet pour ajuster la puissance de transmission de chaque Point d'accès, en ajustant combien fort chaque Point d'accès entend son troisième voisin plus fort. Cette valeur peut seulement être ajustée du CLI utilisant le **802.11b avancé par config tx-alimentation-battent la** commande comme décrit dans des configurations d'affectation de niveau de puissance de Tx.

Avant que vous ajustiez AutoRF, marchent le site de déploiement utilisant le badge de Vocera comme porté par l'utilisateur final et utilisent un outil d'analyse de site afin de gagner une compréhension forte de la façon dont le badge erre et à quelle alimentation chaque Point d'accès est vu. Une fois que c'est complet et on le détermine qu'ajuster cette valeur est exigé, commencez par une valeur – du dBm 71 pour l'algorithme de Transmit Power Control. Utilisez ce paramètre CLI :

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

Permettez au réseau pour fonctionner par ce réglage avec un minimum de 30 minutes à une heure avant que vous observiez toutes les modifications. Une fois que le réseau est donné une durée suffisante, marchent le site utilisant le mêmes outil et badges d'analyse de nouveau. Observez les mêmes caractéristiques d'itinérance et alimentation de Point d'accès. Le but ici est de tenter de faire errer les badges ou avant au prochain Point d'accès pour obtenir le meilleur rapport de signal-bruit.

- **Comment est-ce que je sais si la puissance de transmission est trop chaude ou trop froide ?**La détermination si vous avez de votre seuil de puissance de transmission trop élevé ou si bas exige une bonne compréhension de votre environnement. Si vous avez marché votre zone entière de déploiement (où vous vous attendez à ce que vos badges de Vocera fonctionnent), vous devriez savoir où vos Points d'accès se trouvent aussi bien qu'éprouvez le comportement d'itinérance du badge.
- **Queest-ce que je fais si ma puissance de transmission est trop chaude ?**Le badge de Vocera erre basé seulement sur la force du signal plutôt que la qualité du signal. Si le badge de Vocera n'erre pas après qu'il passe plusieurs Points d'accès tandis qu'occupé dans le tutoriel bienvenu ou la tonalité de test, le badge est considérée Rémanente. Si ce comportement est

indicatif de la zone entière de déploiement de campus, alors votre seuil de puissance de transmission est trop chaud et devrait être soutenu vers le bas. Si seulement un ou deux zones d'isolement affichent ce comportement et le reste des caractéristiques plus idéalistes d'itinérance d'expositions de zone de déploiement ce n'est pas une indication que votre réseau exécute trop chaud.

- **Queest-ce que je fais si ma puissance de transmission est trop froide ?**Le par défaut transmettent le seuil devrait ne presque jamais te fournir une zone de déploiement où votre réseau exécute trop froid. Si le seuil de puissance de transmission est ajusté vers le bas, et la marche les corridors avec le badge de Vocera te fournit un environnement où le badge erre bien, mais perd la Connectivité et/ou les morts/couverture tachetée, alors votre réseau pourrait avoir été si bas accordé. Si ce n'est pas caractéristique de votre tout le réseau mais n'est pas isolé à un ou deux zones, alors il est plus indicatif d'un trou de couverture plutôt qu'un problème sur l'ensemble du réseau.
- **Comportement d'isolement**Si vous trouvez cela dans un ou deux zones, le badge colle à un Point d'accès plutôt que l'itinérance d'une manière idéaliste, examinent ce domaine.Comment cette zone est-elle différente du reste du campus ?Si ce/ces zones sont les sorties ou les zones proches de bâtiment en construction, la détection de trou de couverture pourrait-elle forcer ces Points d'accès pour soulever l'alimentation ?Regardez les listes de voisin de fichier journal et de Point d'accès WLC pour aider à déterminer pourquoi une telle anomalie pourrait se produire.Si vous trouvez cela dans un ou plusieurs zones d'isolement, le badge éprouve la couverture morte ou tachetée, alors vous devez examiner ces domaines séparément.Cette zone est-elle près d'un axe d'argumentaire, de la radiologie, ou d'une salle de pause ?Ces zones pourraient mieux être adaptées par l'installation ou le placement meilleur d'un Point d'accès pour tenir compte d'une meilleure couverture de Voix.Dans des les deux cas, il est toujours recommandé de comprendre que vous fonctionnez en spectre radio non enregistré et le comportement idéaliste ne pourrait pas jamais être réalisable. Ceci pourrait se produire quand vous êtes situé à côté d'un tower ou un périphérique de transmission radio, un émetteur de télévision ou probablement un non-802.11 installation de réparation 2.4 gigahertz (téléphones Sans fil, et ainsi de suite).

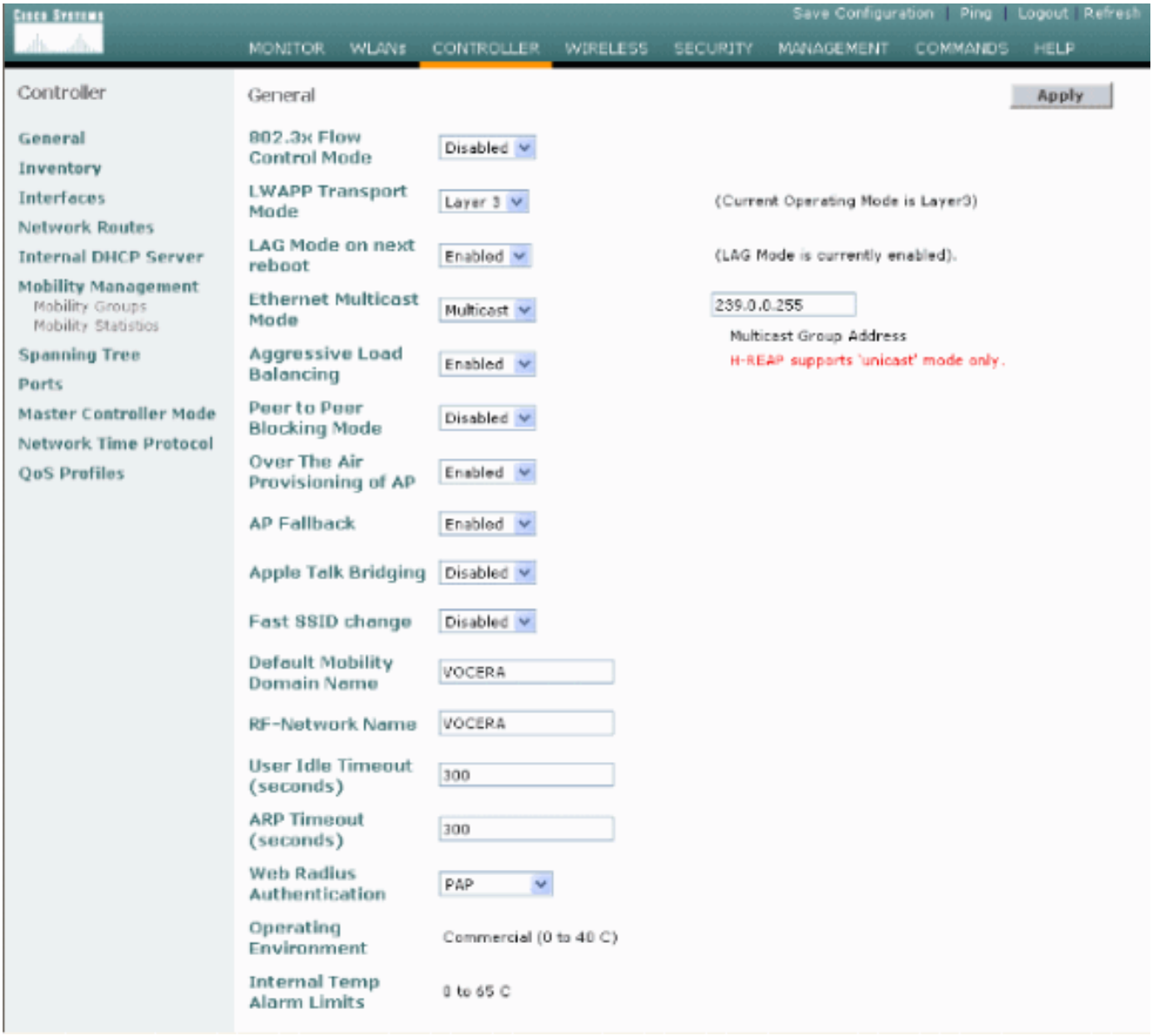
Configuration d'infrastructure de réseau sans fil

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

Note: Des modifications sont laissées unsaved si vous n'appuyez sur pas le **bouton Apply** avant que vous vous déplaciez à l'étape suivante.

Terminez-vous ces étapes sous le menu supérieur de **contrôleur** :

1. Modification Ethernet Multicast Mode à la **Multidiffusion**.
2. Placez l'adresse de groupe de multidiffusion à **239.0.0.255** (ou une autre adresse inutilisée de groupe de multidiffusion).
3. Placez le nom de domaine de mobilité et le nom par défaut de Rf-réseau à votre conception de réseaux.
4. **Équilibrage de charge agressif de** débronchement.**Figure 9 — Configuration de général WLC**

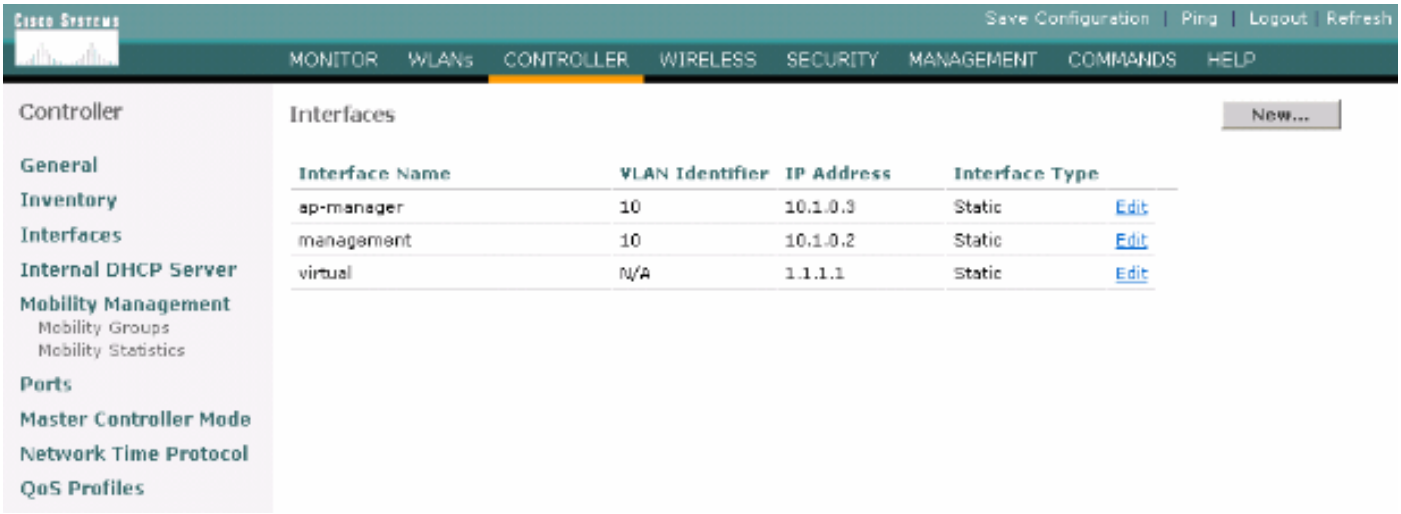


Créez les interfaces

Controller > Interfaces de clic.

Note: Votre VLAN et adresse IP varie. Les copies d'écran ici fournissent l'adressage d'échantillon qui ne devrait pas être directement suivi.

Figure 10 — Liste d'interfaces WLC



Créez l'interface vocale de Vocera

Procédez comme suit :

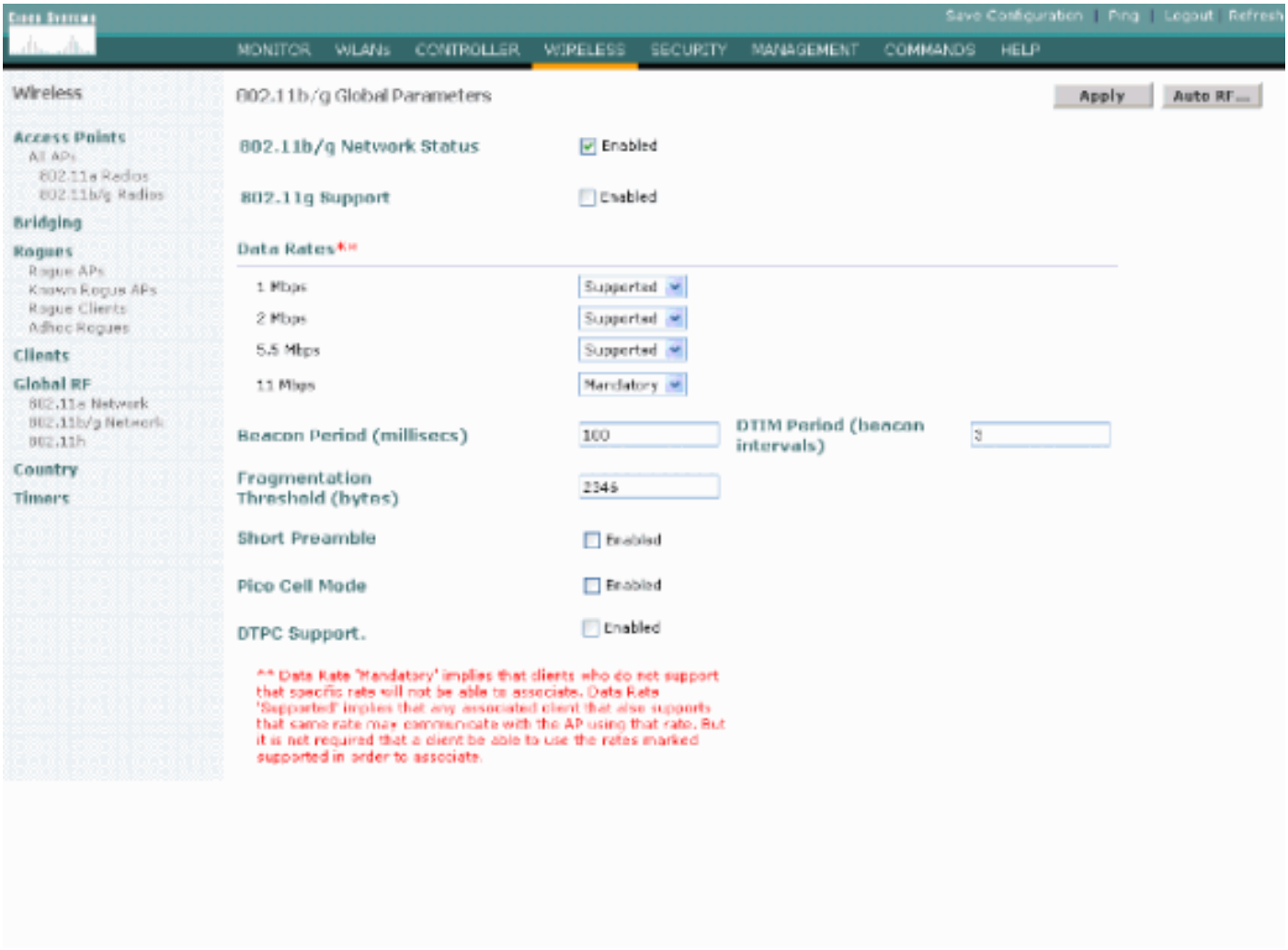
1. Cliquez sur **New**.
2. Entrez dans un représentant de nom de balise de votre réseau de Vocera VoWLAN dans le champ Interface Name.
3. Introduisez le nombre VLAN de ce réseau VoWLAN dans le domaine d'ID DE VLAN.
4. Cliquez sur Apply et puis cliquez sur Edit afin d'éditer l'interface que vous avez juste créée.
5. Écrivez l'adressage IP pour cette interface qui est de l'ordre du VLAN et d'autres informations relatives.
6. Cliquez sur **Apply**.

Configuration de Radio-particularité

Pour un WLAN qui a seulement des badges de Vocera, cette configuration fournit des configurations témoin que le meilleur prenez en charge l'application d'émission de Vocera.

- La période DTIM est **1.**
- Le soutien de 802.11g est désactivé. Seulement le débit de données 802.11b de **11 Mpbs** est **obligatoire**.
- Le préambule court est désactivé.
- DTPC est désactivé.

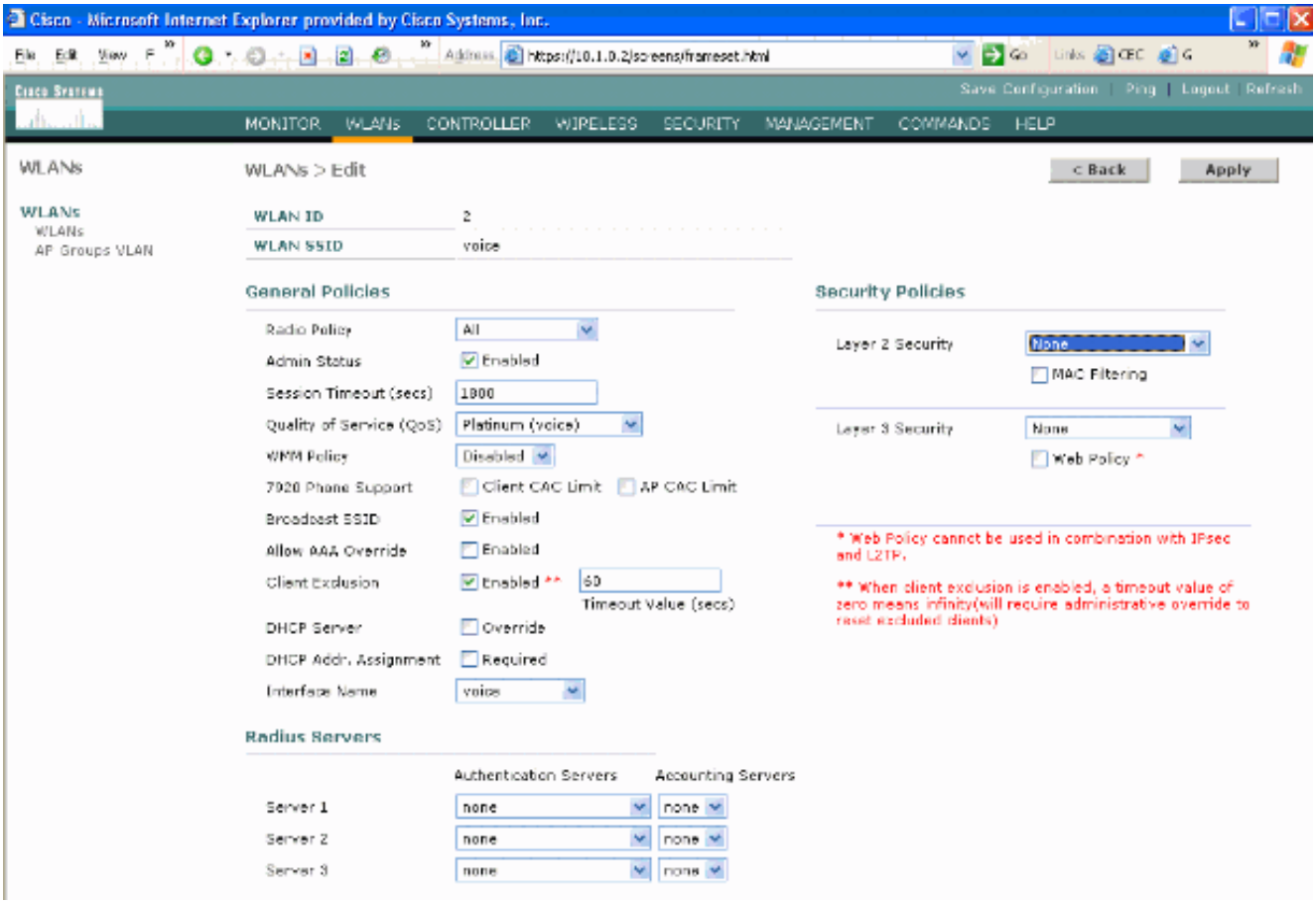
Figure 11 — configuration 802.11b/g



Configuration WLAN

Procédez comme suit :

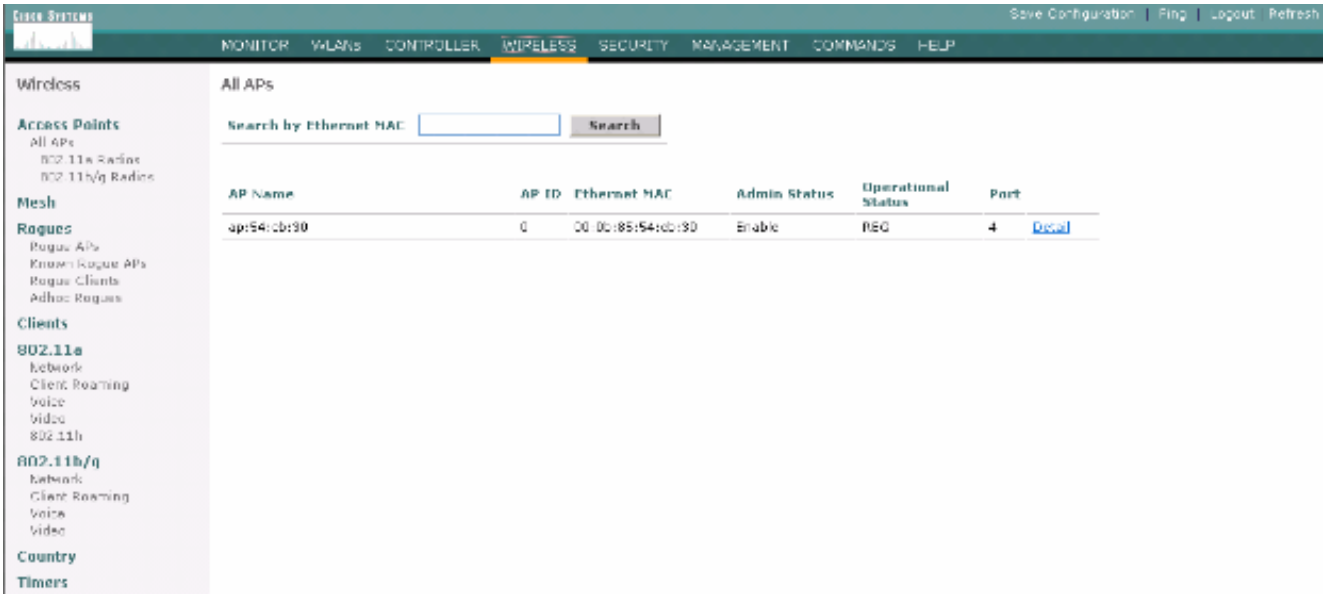
1. Mettez à jour le champ par radio de stratégie à une valeur de la laquelle les ajustements vous a besoin.
2. Modification Admin Status à **activer**.
3. Placez la Session Timeout à **1800**.
4. Fixez la qualité de service au **platine**.
5. Placez le Broadcast SSID à **activer**.
6. Placez le nom d'interface à l'interface créée pour les badges de transmission de Vocera.
7. Placez les options de Sécurité d'apparier vos stratégies entreprises.**Figure 12 — Configuration WLAN**



Configurez le détail de Point d'accès

Procédez comme suit :

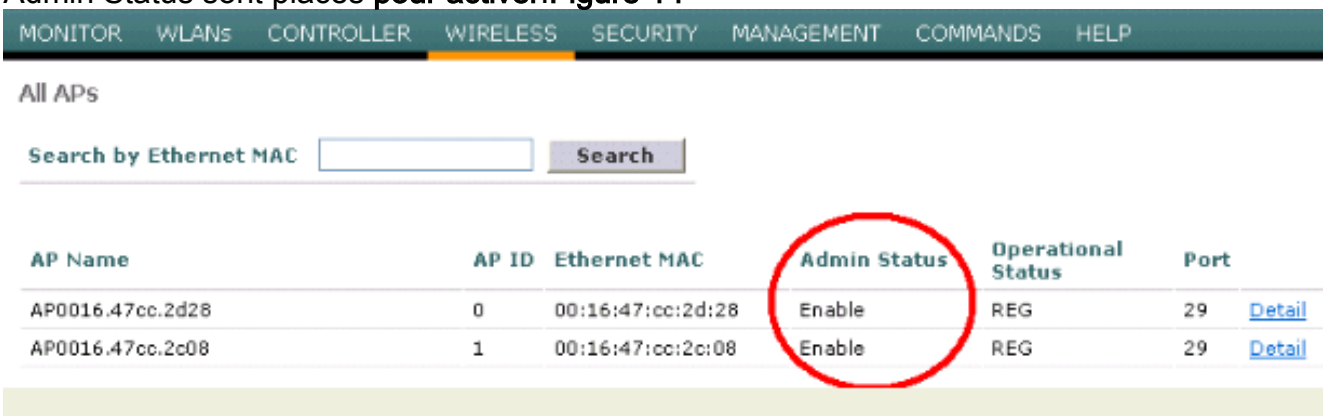
1. **Détail de** clic.
2. Configurez le nom AP.
3. Assurez-vous que le Point d'accès est configuré pour le DHCP.
4. Assurez-vous qu'Admin Status **est activé**.
5. Le modèle AP » devrait être placé aux **gens du pays**.
6. Entrez l'emplacement du Point d'accès.
7. Écrivez le nom de contrôleur que le Point d'accès appartient à. Le nom de contrôleur peut être trouvé à la page de moniteur.
8. Cliquez sur **Apply.Figure 13 — Détail AP**



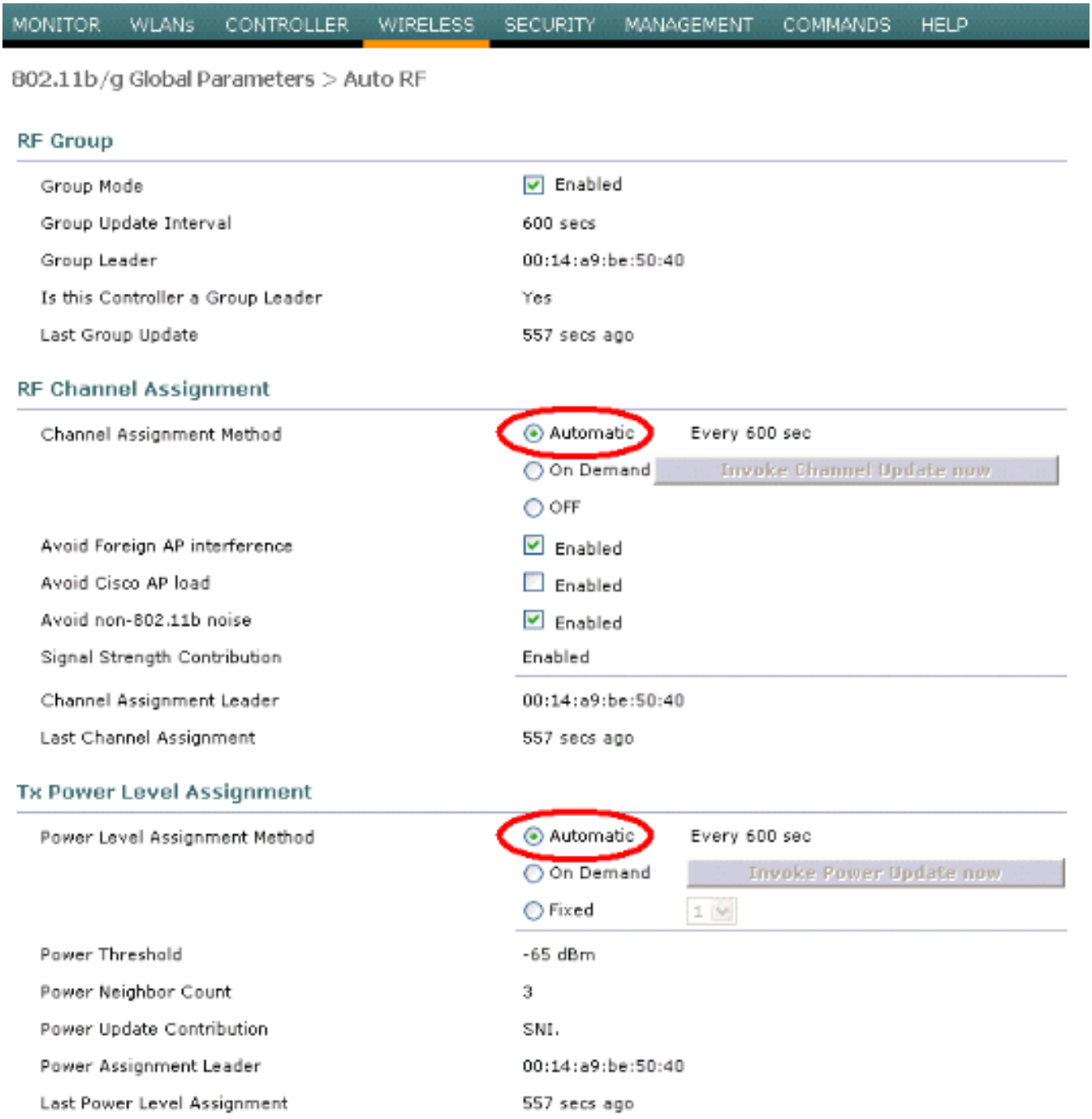
Configurez la radio 802.11b/g

Procédez comme suit :

1. Cliquez sur la **radio** située en haut du WLC et la vérifiez que tous les Points d'accès sous Admin Status sont placés **pour activer**.**Figure 14**



2. **Réseau de** clic (situé près de 802.11b/g).
3. Clic **AutoRF**.
4. Employez AutoRF pour créer une couverture complète avec le canal non-recouvert rf et une puissance de transmission. Afin de faire ceci, **automatique** choisi pour le transfert de la Manche rf et l'affectation de niveau de puissance de Tx.**Figure 15**



5. Cliquez sur **Apply**.
6. Cliquez sur la **save configuration** et voyez l'optimisation AutoRF pour votre section d'environnement de ce document.
7. Choisissez la **radio > les Points d'accès > les radios 802.11b/g.Figure 16**

Vérification de Téléphonie IP sans fil

Après que vous meniez une analyse de site rf et configuriez les Points d'accès et les téléphones, il est crucial d'effectuer des tests de vérification pour s'assurer que tout fonctionne comme désiré. Ces essais devraient être réalisés du tout de ces emplacements :

- La zone primaire de chaque cellule de Point d'accès (où il est le plus susceptible se connecter les badges à ce Point d'accès particulier).
- Tout emplacement où il pourrait y avoir volume d'appels élevé.
- Des emplacements où l'utilisation pourrait être peu fréquente mais la couverture doit encore être certifiés (par exemple, des cages d'escalier, des toilettes, et ainsi de suite).
- Aux franges de la zone de couverture du Point d'accès.
- • Ces essais peuvent être réalisés en parallèle ou des séries. Si exécuté en parallèle, assurez-vous que des téléphones sont mis hors tension entre les points test de mesure pour tester la pleins association, authentification, et enregistrement à chaque emplacement. L'itinérance et les tests de chargement doivent être les essais finaux.

Association, authentification, et enregistrement

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

- Àde plusieurs points dans tout l'environnement, la mise sous tension les badges et vérifient l'association avec le Point d'accès. Si le badge ne s'associe pas avec le Point d'accès, exécutez ces contrôles :Vérifiez la configuration de badge pour assurer le SSID approprié, type d'authentification, et ainsi de suite.Vérifiez la configuration WLC pour assurer le SSID approprié, type d'authentification, des canaux radios, et ainsi de suite.Vérifiez votre analyse de site pour s'assurer que l'emplacement a la couverture adéquate rf.
- Àde plusieurs points dans tout l'environnement, assurez-vous que le téléphone authentifie par le Point d'accès avec succès. Si le client n'authentifie pas, vérifiez la clé WEP ou le nom d'utilisateur et mot de passe de LEAP sur les badges. En outre, vérifiez le nom d'utilisateur et mot de passe sur le serveur d'AAA à l'aide d'un ordinateur portable sans fil avec les qualifications identiques.
- Àde plusieurs points dans tout l'environnement, assurez-vous que les badges s'inscrivent au serveur de communication de Vocera. Si le client ne s'enregistre pas, exécutez ces contrôles :Vérifiez que le badge a l'adresse IP correcte, le masque de sous-réseau, la passerelle principale, le TFTP, primaires primaire/secondaires et des DN.
- Communications voix stationnaires :Àde plusieurs points dans tout l'environnement, alors que vous vous tenez tranquille, faites un appel à un autre badge et conduisez 60 aux tests de la Voix 120-second pour vérifier la Qualité vocale. Si la Qualité vocale est inacceptable, déplacez un badge à un meilleurs emplacement et test de nouveau. La Qualité vocale est-elle acceptable ? Sinon, vérifiez votre couverture Sans fil.Si le serveur de téléphonie est configuré, à de plusieurs points dans tout l'environnement, tenez-vous toujours et faites un appel à un téléphone de câble et conduisez 60 aux tests de la Voix 120-second pour vérifier la Qualité vocale. Si la Qualité vocale est inacceptable, demandez si vous faites un appel utilisant le téléphone de câble. La Qualité vocale est-elle acceptable ? Sinon, vérifiez la conception de réseau câblé contre les instructions.

- Utilisez les outils d'analyse de site pour vérifier qu'il n'y a pas plus d'un Point d'accès par canal rf de cet emplacement avec une force du signal (indicateur reçu de force du signal [RSSI]) plus considérablement que 35. S'il y a deux Points d'accès actuels sur le même canal, assurez-vous que le rapport signal/bruit (SNR) est aussi élevé comme possible de réduire l'interférence. Par exemple, si le Point d'accès plus fort a un RSSI de 35, idéalement le Point d'accès plus faible devrait avoir un RSSI de moins de 20. Afin d'atteindre ce but, vous pourriez devoir réduire une puissance de transmission du Point d'accès ou déplacer le Point d'accès.
- Vérifiez les configurations de QoS sur le Point d'accès pour confirmer les configurations recommandées appropriées.
- Appels errants de badge :Si le serveur de téléphonie n'est pas disponible, initiez le tutoriel de Vocera avec la commande **commencent le tutoriel**.OUSi le serveur de téléphonie est disponible, initiez un appel avec un périphérique stationnaire au badge.Vérifiez continuellement la Qualité vocale tandis que vous traversez toute la zone de couverture sans fil. Si la Qualité vocale est insuffisante, effectuez ces tâches :Écoutez tous les changements inacceptables de Qualité vocale et notez l'emplacement et les valeurs par radio sur votre ordinateur portable et les valeurs CQ du badge.Observez et écoutez le badge pour errer au prochain Point d'accès.Notez les autres Points d'accès disponibles dans l'analyse de site pour vérifier la couverture et l'interférence.
- Faites les réglages au placement et aux configurations de Point d'accès pour régler avec précision le WLAN, et exécutez ces contrôles pour assurer la Qualité vocale :Utilisez les outils d'analyse de site et les vérifiez qu'il n'y a pas plus d'un Point d'accès par canal avec une valeur RSSI plus grande que 35 dans n'importe quel emplacement donné. Dans le meilleur des cas, tous autres Points d'accès sur le même canal devraient avoir des valeurs RSSI que le bas comme possible (de préférence moins de 20). Au cadre de la zone de couverture où le RSSI est 35, le RSSI pour tous autres Points d'accès sur le même canal devrait idéalement être moins de 20.Utilisez les outils d'analyse de site pour vérifier qu'il y a au moins deux Points d'accès (total, sur les canaux distincts) visibles dans tout l'emplacement avec la force du signal suffisante.Vérifiez que tous les Points d'accès dans une zone errante indiquée sont sur un réseau de la couche 2.

Questions communes d'itinérance

Ces questions d'itinérance peuvent se produire :

- Le badge n'erre pas une fois placé directement au Point d'accès.
- Le badge est le plus susceptible n'atteignant pas les seuils différentiels d'itinérance pour l'indicateur reçu de force du signal (RSSI) et l'utilisation de canal (CU). Ajustez la forme de seuil de puissance de transmission le WLC.
- Le badge ne reçoit pas des balises ou des réponses de sonde du Point d'accès.
- Le badge erre trop lentement.

Le badge perd la connexion au réseau ou le service vocal est perdu en errant

- Authentification de contrôle pour une non-concordance possible WEP.
- Le badge n'envoie pas IGMP se joint ou le réseau envoie des requêtes IGMP pendant un errer. Par conséquent, la fonction d'émission de Vocera échoue pendant une couche 2/Layer

3 errent.
- Le badge est capable d'une couche sans couture 2 errant seulement (à moins qu'un mécanisme de mobilité de la couche 3 est configuré). Assurez-vous que le nouveau WLC ne sert pas un différent IP de sous-réseau.
- Vérifiez que le Point d'accès associé/contrôleur a la connectivité IP au serveur de communication de Vocera.
- Vérifiez les valeurs CQ de force du signal et de badge rf.

Le badge perd la Qualité vocale tout en errant

- Vérifiez le bas RSSI sur le Point d'accès de destination.
- La superposition de la Manche pourrait être insuffisante. Le badge doit avoir le temps pour remettre outre de l'appel sans à-coup avant qu'il perde son signal avec le Point d'accès d'origine.
- Le signal du Point d'accès d'origine pourrait être perdu.

Problèmes sonores

Il y a quelques erreurs communes de configuration qui peuvent entraîner quelques questions sonores facilement résolues. Si possible, vérifiez les problèmes sonores contre un badge stationnaire (de référence) pour aider l'étroit le problème à une question Sans fil. Les problèmes sonores communs incluent :

- Audio unilatéral
- Audio variable ou robotique
- Problèmes d'enregistrement et d'authentification

Audio unilatéral

- Ce problème peut se poser dans les superficies de frange d'un Point d'accès, où un signal pourrait être trop faible du côté de badge ou du côté de Point d'accès. Apparier les paramètres d'alimentation sur le Point d'accès au badge (20 mW), si possible, peut réparer ce problème. Ce problème est le plus commun quand la variation entre la configuration de Point d'accès et la configuration de badge est grande (par exemple, 100 mW sur le Point d'accès et 28 mW sur le badge).
- Vérifiez la passerelle et le Routage IP pour la Qualité vocale.
- Vérifiez pour voir si un Pare-feu ou un NAT est dans le chemin des paquets UDP de propriété industrielle. Par défaut, les Pare-feu et le NATs n'entraînent l'audio à sens unique ou aucun audio. Le Cisco IOS® et les PIX NATs et Pare-feu ont la capacité de modifier connexions de sorte que l'audio bi-directionnel puisse circuler.Si vous utilisez la mobilité de la couche 3, votre réseau pourrait bloquer le trafic en amont avec des contrôles de Fonction Unicast Reverse Path Forwarding (uRPF).
- L'audio à sens unique peut se produire si la mise en cache d'ARP n'est pas configurée sur le WLC.

Audio variable ou robotique

- Une raison commune pour l'audio variable ou robotique est quand une micro-onde fonctionne tout près. Les micro-ondes commencent au canal 9 et peuvent s'étendre des canaux 6 14.
- Vérifiez les téléphones Sans fil 2.4 gigahertz et d'autres périphériques sans fil d'appel d'infirmière utilisant des outils comme Cognio.

Problèmes d'enregistrement et d'authentification

Quand vous rencontrez des problèmes avec l'authentification, exécutez ces contrôles :

- Vérifiez le SSID pour s'assurer qu'ils s'assortissent sur le badge et le Point d'accès (ou réseau). Soyez également sûr que le réseau a une artère au serveur de Vocera.
- Vérifiez les clés WEP pour s'assurer qu'elles s'assortissent. C'est une bonne idée de les ressaisir sur l'utilitaire de configuration de badge (BCU) et de reprogrammer le badge, parce qu'il est facile de faire une erreur tapante quand vous entrez une clé WEP ou un mot de passe.

Ces messages ou symptômes peuvent se produire :

- Ne peut pas prendre en charge toutes les capacités demandées — C'est le plus susceptible une non-concordance de cryptage entre le Point d'accès et le client.
- Échec de l'authentification/aucun AP trouvé — Assurez la correspondance de types d'authentification sur le Point d'accès et le client.
- Aucun service – Le config IP a manqué — Si vous utilisez le WEP statique, assurez que les clés sont configurées correctement. Assurez que d'autres clients peuvent recevoir le DHCP utilisant le même SSID.
- De-authentifiez tous les clients TKIP d'AP — Ce problème se produit quand le Point d'accès détecte deux erreurs MIC dans 60 secondes. Ce les contre-mesures garde tous les clients TKIP d'authentifier à nouveau pendant 60 secondes.
- Ré-authentification/Session Timeout — Si configuré, un délai d'attente de session déclenche une ré-authentification qui entraîne des lacunes dans le flux voix (300 ms + retard BLÊME pour l'authentification de 802.1x).

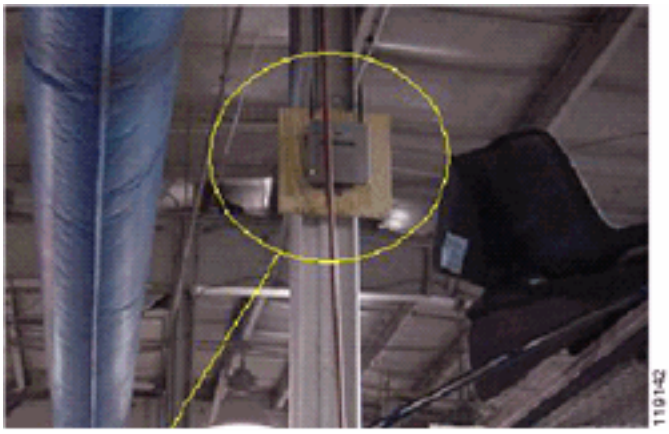
Annexe A

AP et placement d'antenne

Cette section donne des exemples du placement approprié et inexact des Points d'accès (aps) et des Antennes.

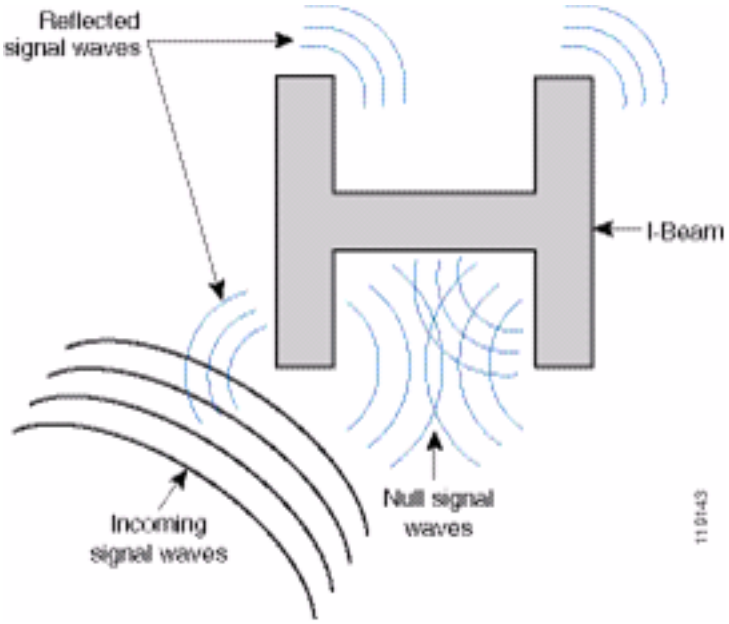
La figure 17 affiche le placement inexact d'un Point d'accès et des Antennes près d'un Je-faisceau, qui crée les signaux patterns tordus. Un zéro rf est créé par le croisement des ondes de signal, et la déformation multivoie est créée quand des ondes de signal sont reflétées. Ce placement a comme conséquence la couverture très petite derrière le Point d'accès et la qualité du signal réduite devant le Point d'accès.

Figure 17 — Placement inexact des Antennes près d'un Je-faisceau



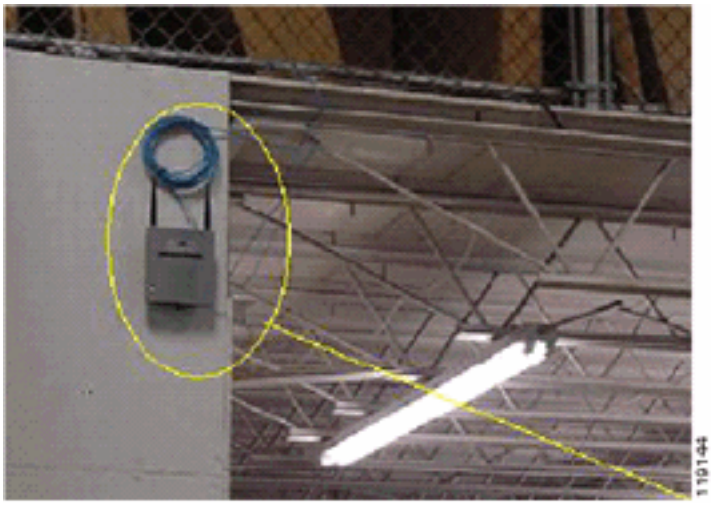
La figure 18 affiche les modifications ou les déformations de propagation de signal provoquées par un Je-faisceau. Le Je-faisceau crée beaucoup de réflexions des paquets reçus et des paquets transmis. Les signaux reflétés ont comme conséquence la qualité du signal très pauvre en raison des zéros et de l'interférence multivoie. Cependant, la force du signal est élevée parce que les Antennes de Point d'accès sont tellement étroitement au Je-faisceau.

Figure 18 — Déformations de signal provoquées en plaçant les Antennes trop étroitement à un Je-faisceau



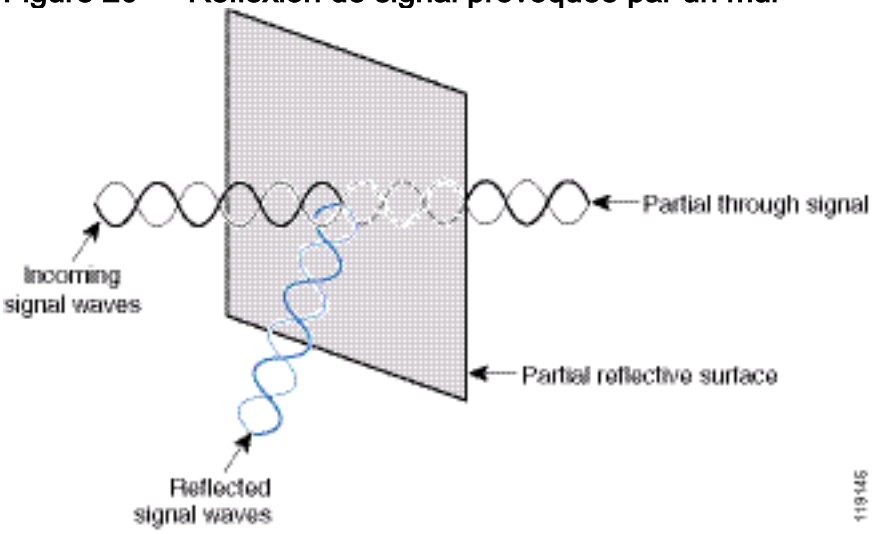
Le placement de Point d'accès et d'antenne dans la figure 19 est meilleur parce qu'il est à partir des Je-faisceaux et il y a moins signaux reflétés, moins zéros, et moins d'interférence par trajets multiples. Ce placement n'est toujours pas parfait parce que le câble Ethernet ne devrait pas être lové vers le haut si proche de l'antenne. En outre, le Point d'accès a pu être tourné avec les Antennes 2.4GHz indiquées le plancher. Ceci fournit une meilleure couverture directement au-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 partir des Je-faisceaux



La figure 20 affiche la propagation de signal provoquée par le mur sur lequel le Point d'accès est monté.

Figure 20 — Réflexion de signal provoquée par un mur

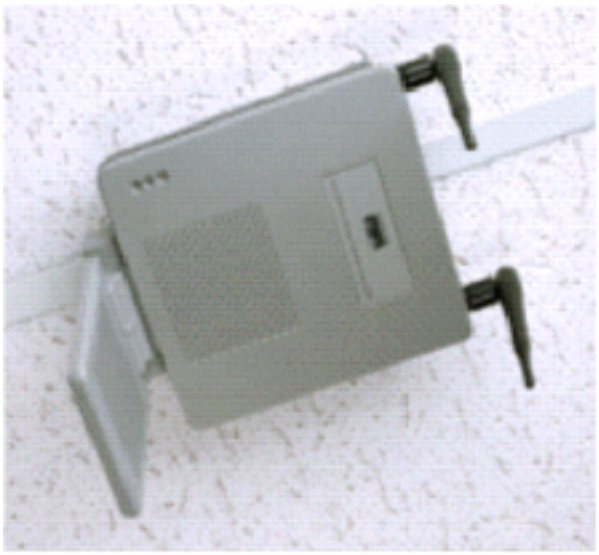


Les exemples précédents s'appliquent également quand vous placez des Points d'accès et des Antennes dans ou à côté du plafond dans un environnement d'entreprise standard. S'il y a les conduits métal-air, les axes d'argumentaire, ou d'autres entraves physiques qui peuvent entraîner la réflexion de signal ou l'interférence multivoie, Cisco recommande fortement que vous déplaciez les Antennes à partir de ces barrières. Dans le cas de l'argumentaire, déplacez l'antenne quelques pieds loin afin d'aider à éliminer la réflexion et la déformation de signal. Le même est vrai avec des conduits d'air dans le plafond.

Une analyse menée sans envoyer et recevoir des paquets n'est pas suffisante. L'exemple de Je-faisceau affiche la création des zéros qui peuvent résulter des paquets qui ont des erreurs de CRC. Des paquets vocaux avec des erreurs de CRC sont manqués les paquets qui compromettent la Qualité vocale. Dans cet exemple, ces paquets ont pu être au-dessus du plancher de bruit mesuré par un outil d'analyse. Par conséquent, il est très important que les niveaux de signal de mesures d'analyse de site non seulement mais génère également des paquets et signale alors des erreurs de paquets.

La figure 21 affiche un Cisco AP1200 correctement monté à une T-barre de plafond, avec les Antennes dans une position omnidirectionnelle.

Figure 21 — Cisco AP1200 monté à un plafond



La figure 22 affiche une antenne omnidirectionnelle de diversité de Cisco Aironet 5959 correctement montée à une T-barre de plafond. Dans ce cas, Cisco AP1200 est monté au-dessus de la tuile de plafond.

Figure 22 — Antenne de Cisco Aironet 5959 montée à un plafond

La figure 23 affiche un Cisco AP1200 correctement monté à un mur.

Figure 23 — Cisco AP1200 monté à un mur

La figure 24 affiche l'antenne de correctif de diversité de Cisco Aironet 2012 montée à un mur. Dans ce cas, Cisco AP1200 est monté au-dessus de la tuile de plafond.

Figure 24 — Antenne de Cisco Aironet 2012 montée à un mur

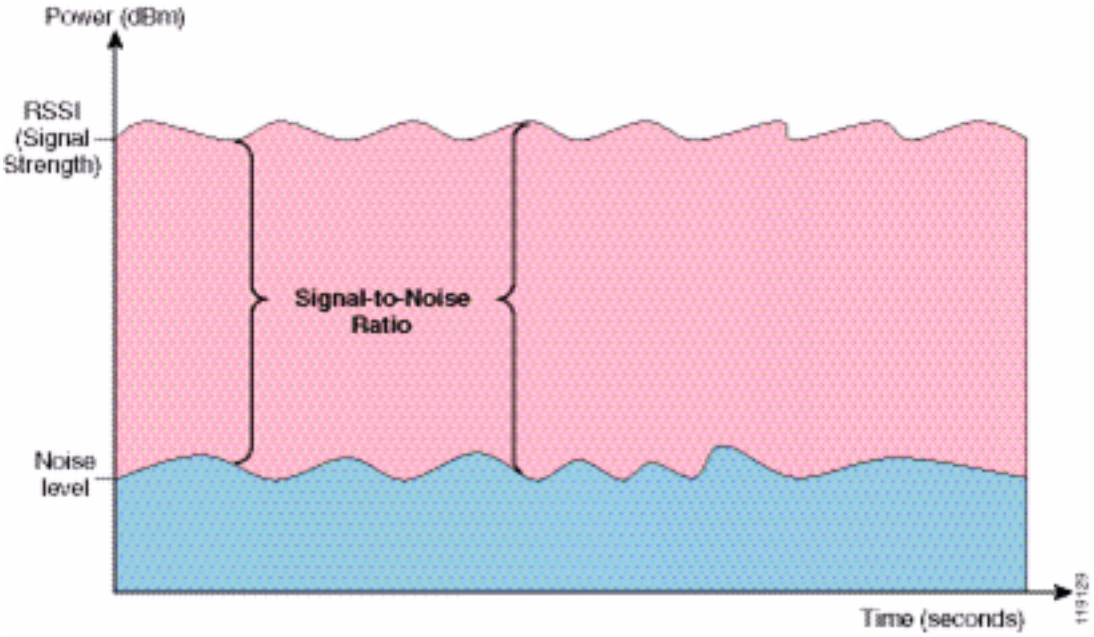
Pour des zones où le trafic d'utilisateur est élevé (comme les espaces de bureau, des écoles, des commerces de détail, et des hôpitaux), Cisco recommande que vous placiez l'accès précisiez de la vue et placiez les Antennes discrètes au-dessous du plafond. La séparation pour des Antennes de non-diversité ne devrait pas dépasser 18 pouces.

Interférence et déformation multivoie

La représentation de débit du réseau WLAN est affectée par les signaux inutilisables. L'interférence WLAN peut être générée par des fours à micro-ondes, des téléphones sans fil 2.4 gigahertz, des périphériques Bluetooth, ou tout autre équipement électronique fonctionnant dans la bande 2.4 gigahertz. L'interférence provient également typiquement d'autres Points d'accès et périphériques de client qui appartiennent dans le WLAN mais qui soyez assez loin parti de sorte que leur signal soit affaibli ou soit devenu corrompu. Les Points d'accès qui ne sont pas une partie de l'infrastructure réseau peuvent également entraîner l'interférence WLAN et sont identifiés comme points d'accès non autorisé.

L'interférence et la déformation multivoie entraînent le signal transmis pour flotter. L'interférence diminue le rapport signal/bruit (SNR) pour un débit de données particulier. Les nombres de tentatives de paquet entrent dans une zone où l'interférence et/ou la déformation multivoie sont élevées. L'interférence désigné également sous le nom du plancher de niveau sonore ou de bruit. Le point fort du signal reçu de son Point d'accès associé doit être assez élevé au-dessus du niveau sonore du récepteur à décoder correctement. Ce niveau de point fort désigné sous le nom du rapport signal/bruit, ou du SNR. Le SNR idéal pour le badge de Vocera est 25 dB. Par exemple, si le plancher de bruit est de 95 décibels par milliwatt (dBm) et le signal reçu au téléphone est le dBm 70, puis le rapport signal/bruit est 25 dB. (Voir la figure 25.)

Figure 25 — Rapport signal/bruit (SNR)



Quand vous changez le type et l'emplacement de l'antenne, elle peut réduire la déformation multivoie et l'interférence. Le gain d'antenne ajoute au gain du système et peut réduire l'interférence si l'émetteur de intervention n'est pas directement devant l'antenne directionnelle.

Tandis que les antennes directionnelles peuvent être de grande valeur pour certaines applications d'intérieur, l'immense majorité d'installations d'intérieur utilisent les Antennes omnidirectionnelles. La directionnalité devrait être strictement déterminée par une analyse de site correcte et appropriée. Si vous utilisez un omnidirectionnel ou corrigez l'antenne, les environnements intérieurs exigent des Antennes de diversité d'atténuer la déformation multivoie. Les radios de Point d'accès de gamme Cisco Aironet tiennent compte du support de diversité.

Atténuation de signal

La perte d'atténuation de signal ou de signal se produit même pendant que le signal traverse l'air. Le point fort de perte de signal est plus prononcé car le signal traverse différents objets. Une puissance de transmission de 20 mW est équivalente au dBm 13. Par conséquent, si l'alimentation transmise au point d'entrée d'un mur de plaque de plâtre est au dBm 13, la force du signal est réduite au dBm 10 en quittant ce mur. Cette table affiche la perte probable dans la force du signal provoquée par de divers types d'objets.

Atténuation de signal provoquée par de divers types d'objets

Objet dans le chemin de signaux	Atténuation de signal par l'objet
Mur de plaque de plâtre	3 dB
Mur de verre avec la trame en métal	6 dB
Mur de bloc de cendre	4 dB
Fenêtre de bureau	3 dB
Porte en métal	6 dB
Porte en métal dans le mur de briques	12 dB
Corps humain	3 dB

Chaque site examiné a des différents niveaux de déformation multivoie, le signal perd, et bruit de signal. Les hôpitaux sont typiquement l'environnement le plus provocant pour examiner en raison de la déformation multivoie élevée, des pertes de signal et bruit de signal. Les hôpitaux prennent plus long pour examiner, pour exiger une population plus dense des Points d'accès, et pour exiger des normes de performance supérieure. La fabrication et les ateliers sont les prochains le plus dur à examiner. Ces sites ont généralement la voie de garage en métal et beaucoup metal les objets sur le plancher, qui ont comme conséquence les signaux reflétés qui recréent la déformation multivoie. Les immeubles de bureau et les sites de tourisme ont généralement l'atténuation élevée de signal mais un peu de degré de déformation multivoie.

Informations connexes

- Déployer les Contrôleurs de LAN sans fil de la gamme Cisco 440X
- Conception de réseaux de référence de solution
- Spécifications système de transmissions de Vocera
- Support et documentation techniques - Cisco Systems