# UWNインフラストラクチャでのVocera IP Phoneの導入

## 内容

# 概要

このドキュメントでは、Cisco Unified Wireless Network インフラストラクチャに Vocera® Badge Voice over WLAN（VoWLAN）テクノロジーを実装する上での設計に関する考慮事項と導入のガイドラインを示します。

**注：Vocera製品**のサポートは、Veraサポートチャネルから直接取得する必要があります。Cisco テクニカルサポートは、Vocera に関する問題をサポートするためのトレーニングを受けていません。

このガイドは『Cisco ワイヤレス LAN コントローラ導入ガイド』の補足であり、Lightweight アーキテクチャにおける Vocera VoWLAN デバイスに固有の設定パラメータだけに焦点を当てています。詳細については、『Cisco 440X シリーズ ワイヤレス LAN コントローラの導入』を参照してください。

# 前提条件

## 要件

このドキュメントは、読者に Cisco IP 電話の SRND と Cisco ワイヤレス LAN の SRND で使用されている用語や説明されている概念についての知識があるものと想定して書かれています。.

ワイヤレスUC設計ガイド：
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_wireless_uc.html

Cisco Unified Communications Manager 7.xに基づくCisco Unified Communications SRND:http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_uc_mgr.html

## 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

## 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# 要旨

次の表には、主要な 4 つの機能と、それらの Cisco Unified Wireless Network での動作のしくみが要約されています。

| | シングル コントローラ | コントローラ間レイヤ2ローミング | コントローラ間レイヤ3ローミング |
|---|---|---|---|
| バッジ対バッジ | 特別な設定なし | 特別な設定なし | 特別な設定なし |
| バッジ対電話機 | 特別な設定なし | 特別な設定なし | 特別な設定なし |
| バッジ対ブロードキャスト | コントローラのマルチキャストをイネーブルにする | Enable Controller Multicast Disable Vocera VLAN IGMP-Snoopingまたは4.0.206.0以降を実行 | 4.0.206.0以降 |
| バッジ位置特定 | 特別な設定なし | 特別な設定なし | 特別な設定なし |

# Vocera バッジの概要

通信バッジを装着すると、バッジの装着者は他の装着者と即座に通信できるようになります。その他にも、Private Branch Exchange（PBX; 構内交換機）との統合や、バッジの位置の追跡なども行えます。802.11b/g ワイヤレス ネットワークを使用するには、マルチキャストおよび UDP ユニキャストのパケット配信を利用することが必要です。この場合、Vocera Server Software リリース 3.1（ビルド 1081）の時点では Quality of Service（QoS）に関して限定的な要件があります。 暗号化機能には、64/128 ビットの Wired Equivalent Privacy（WEP）、Temporal Key Integrity Protocol（TKIP）、Message Integrity Check（MIC）、および Cisco Temporal Key

Integrity Protocol（CKIP）に、Open、Wi-Fi Protected Access-Pre-shared Key（WPA-PSK）、WPA-Protected Extensible Authentication Protocol（PEAP）、および Lightweight Extensible Authentication Protocol（LEAP）の認証機能が組み合されて使用されます。

ボタンを押すと、VoceraサーバはVoceraで応答します。VoceraはVoceraで応答します。Voceraは、record、where (am I) /is...、call、play、**broadcast messages**など。Vocera サーバは必要なサービスを提供したり、要求を処理するためのコール設定を行います。

Vocera の 802.11b 対応の通信システムでは、独自の音声圧縮技術と、UDP ポート範囲が使用されます。Vocera のシステム ソフトウェアが Windows サーバ上で稼働して、コール設定、コール接続、ユーザ プロファイルの管理を行います。これらが Nuance 8.5 音声認識および声紋ソフトウェアと組み合されて、バッジ音声通信が実現されます。Vocera では、バッジと Plain Old Telephone Service（POTS; 一般電話サービス）とを接続するための Vocera Telephony Solutions Software は、別の Windows サーバで稼働させることを推奨しています。

## Vocera のコール キャパシティにおける考慮事項

詳細については、このドキュメントの「ネットワーク規模の決定」のセクションを参照してください。

## Vocera Communications Server の規模

Voceraサーバのサイジングマトリックスの詳細は、『Vocera通信システムの仕様』を参照してください。

## Vocera のソリューション

Vocera バッジでは、このソリューション全体を構成する重要な機能を提供に、ユニキャストとマルチキャストのパケット配信が使用されています。次に示す 4 つの必須機能は、適切なパケット配信に依存するものです。さらに、ここでは配信やその他の機能のために基盤となるネットワークをどのように使用しているかについて、基本的な事項を説明しています。

- バッジからバッジへの通信：あるVoceraユーザが別のユーザにコールすると、バッジは最初にVoceraサーバに接続します。Voceraサーバは着信者のバッジのIPアドレスを検索し、バッジユーザにコールできるかどうかを尋ねます。受信者側がコールを受けた場合は、Vocera サーバは発信側のバッジに受信側のバッジの IP アドレスを通知し、バッジ間での直接通信を設定します。その後、サーバは通信に関与しません。Vocera サーバとの通信にはすべて G.711 コーデックが使用され、バッジ対バッジの通信ではすべて Vocera 独自のコーデックが使用されます。
- バッジテレフォニー通信：Voceraテレフォニーサーバがインストールされ、PBXへの接続が設定されると、ユーザはPBXまたは外部の電話回線から内線番号をコールできます。Vocera で電話をかけるためには、番号（5、6、3、2 など）を発音するか、あるいは Vocera データベースにその番号で人名や組織（薬局、自宅、ピザ屋）についてのアドレス帳のエントリを作成します。Vocera サーバでは、内線番号の数字を傍受するか、あるいはデータベース内でその名前を探して番号を選択することにより、宛先番号が判断されます。次に、Vocera サーバではその情報を Vocera Telephony サーバに渡します。Vocera Telephony サーバでは PBX に接続して、適切な電話信号（DTMF など）を生成します。 バッジと Vocera サーバ間、および Vocera サーバと Vocera Telephony サーバ間の通信には、すべてユニキャスト UDP で

G.711 コーデックが使用されます。

- Voceraブロードキャスト：Voceraバッジユーザは、Broadcastコマンドを使用して、Voceraバッジのウェアラグループに同時にコールして通信できます。ユーザがグループにブロードキャストする場合、ユーザのバッジはVoceraサーバにコマンドを送信し、グループのメンバーを検索し、アクティブなメンバーを判別し、このブロードキャストセッションに使用するマルチキャストアドレスを割り当て、マルチキャストグループに参加するように指示します。
- Badge Location Function(BSSID)：各バッジが関連付けられたBSSIDを持つサーバに30秒のキープアライブを送信するため、Voceraサーバは、各アクティブバッジが関連付けられたアクセスポイントを追跡します。この仕組みにより、Vocera システムではバッジ ユーザのおおよその場所が推定できます。ただし、バッジは最も近いアクセス ポイントに対応付けられているとは限らないため、この機能の精度はあまり高くありません。

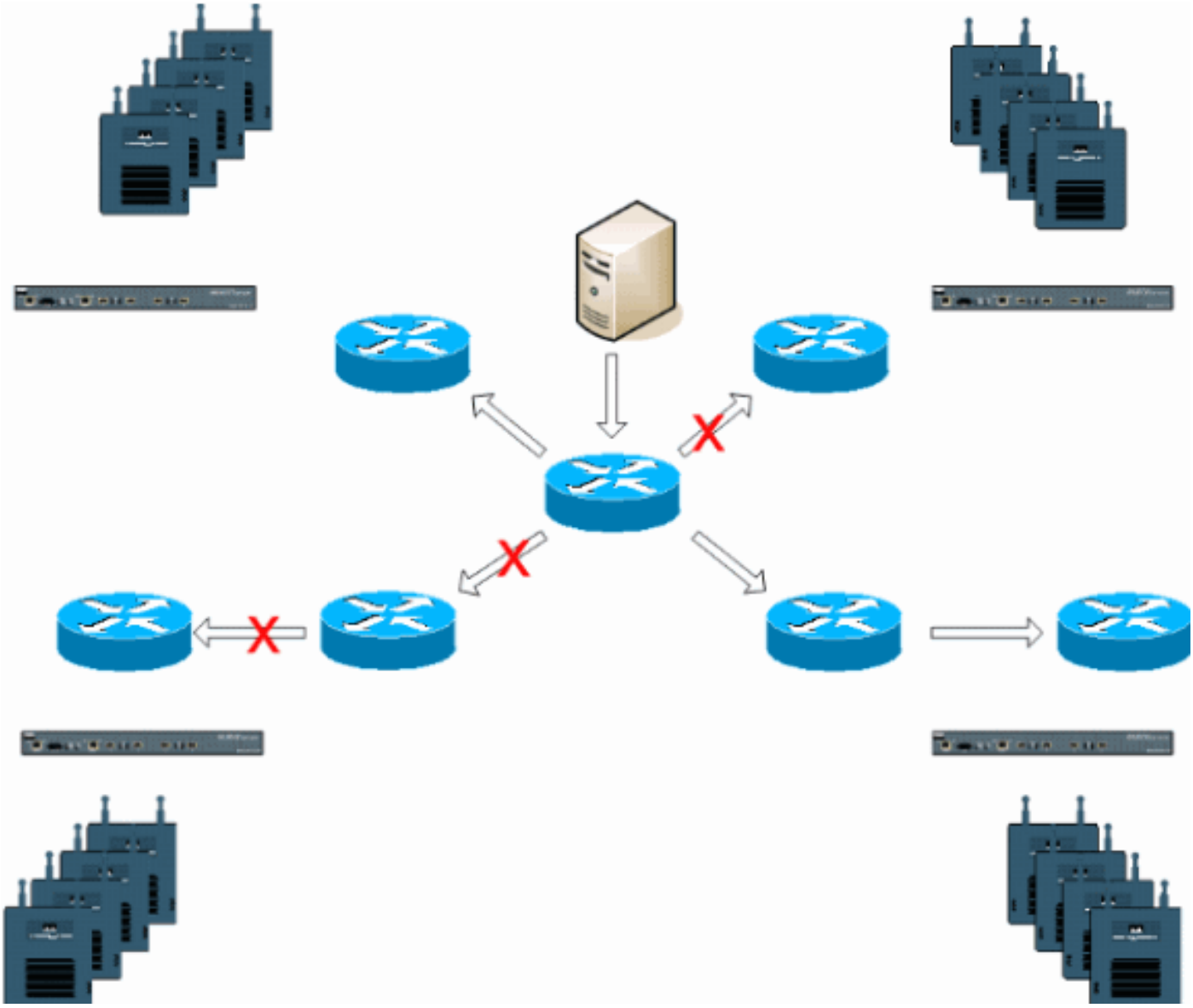
## Vocera のインフラストラクチャ計画

Vocera のホワイトペーパー『Vocera Infrastructure Planning Guide』に、サイト調査の最低限の要件が記載されています。それには、バッジが最低でも -65 dBm の信号強度を受信でき、信号対雑音比が 25 db より大きく、適切なアクセス ポイントのオーバーラップやチャネルの分離が必要なことが示されています。 バッジではサイト調査に使用するノートブックと同様の全方位型アンテナが使用されていますが、装着者が信号強度に及ぼす影響を考慮すると、バッジの動作が忠実に模倣されるわけではありません。この独自の要件と送信デバイスの動作を考慮とすると、サイトの特性として異常な radio frequency ( RF; 無線周波数 ) がないことを確実にするには、Cisco のアーキテクチャと Radio Resource Management が理想的です。

Vocera バッジは低電力のデバイスであり、身体に装着が可能で、限定的ながら信号エラー訂正機能も備えています。このドキュメントに記載されている Vocera の要件を満たすのは、難しくはありません。ただし、SSID の数が多すぎると、処理とバッジの効率的な動作のための負荷が過大になる可能性があります。

## アーキテクチャ概要

**図1:Lightweight Access Point Protocol(LWAPP)ワイヤレスでの一般的なマルチキャスト転送およびプルーニング**



## LWAPP 環境におけるマルチキャスト

Vocera のブロードキャスト機能を展開するには、LWAPP が導入されている環境でのマルチキャストを理解することが必要です。以降では、コントローラ ベースのソリューションでマルチキャストをイネーブルにするために不可欠な手順について説明します。LWAPP コントローラがクライアントへのマルチキャストの配信に使用する方式には、現在 2 種類の方式があります。

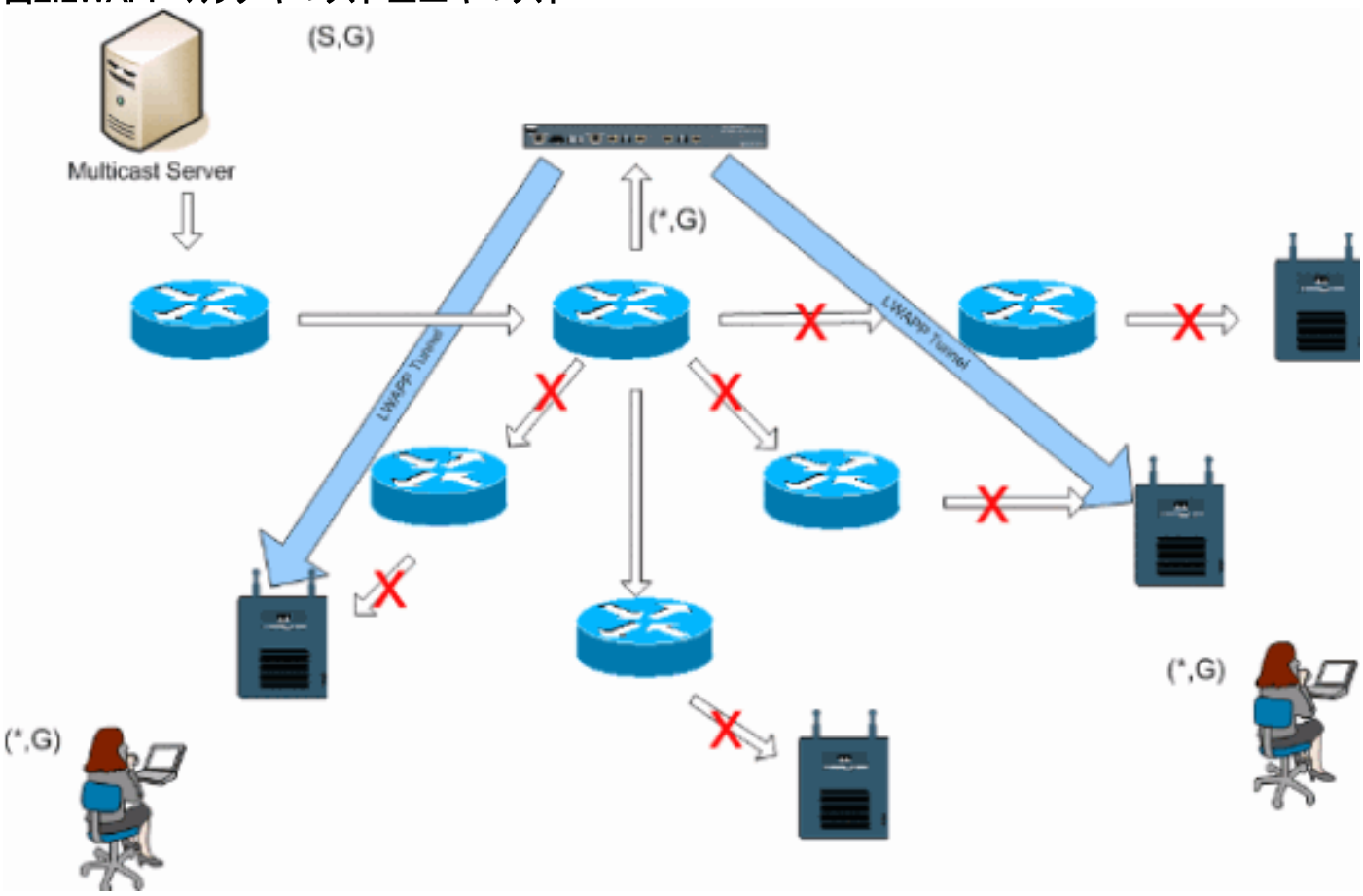
- ユニキャスト - マルチキャスト
- マルチキャスト - マルチキャスト

### ユニキャスト - マルチキャストの配信方式

ユニキャスト - マルチキャストの配信方式では、それぞれのマルチキャスト パケットのコピーが作成され、それが各アクセス ポイントに転送されます。クライアントがワイヤレス LAN へのマルチキャスト加入を送信すると、この加入はアクセス ポイントから LWAPP トンネル経由でコントローラに転送されます。コントローラでは、このマルチキャスト加入が直接接続されているローカル エリア ネットワーク接続にブリッジされます。このネットワークはクライアントの WLAN に対応付けられているデフォルトの VLAN です。IP マルチキャスト パケットがネットワークからコントローラに着信すると、コントローラでは、ワイヤレス ドメイン内で特定のグループに属しているクライアントがいる各アクセス ポイントに対して、このパケットに LWAPP ヘッ

ダーを付けて複製されます。マルチキャストの発信元がワイヤレス ドメイン内にいる受信者の 1 人である場合は、このパケットを送信したクライアントに対してもパケットが複製され、転送されます。Vocera バッジにとっては、これは LWAPP コントローラ ソリューションでのマルチキャスト配信の好ましい方式ではありません。ユニキャスト配信方式は、小規模な導入環境では有効です。ただし、Wireless LAN Controller ( WLC; ワイヤレス LAN コントローラ ) に与える負荷が相当に大きいため、これは推奨できるマルチキャスト配信方式ではありません。

**図2:LWAPPマルチキャストユニキャスト**




**注**：APグループVLANが設定されていて、コントローラを介してクライアントからIGMP参加が送信される場合、クライアントが接続されているWLANのデフォルトVLANに配置されます。したがって、クライアントがこのデフォルトのブロードキャスト ドメインのメンバでないと、このマルチキャスト トラフィックを受信できない可能性があります。

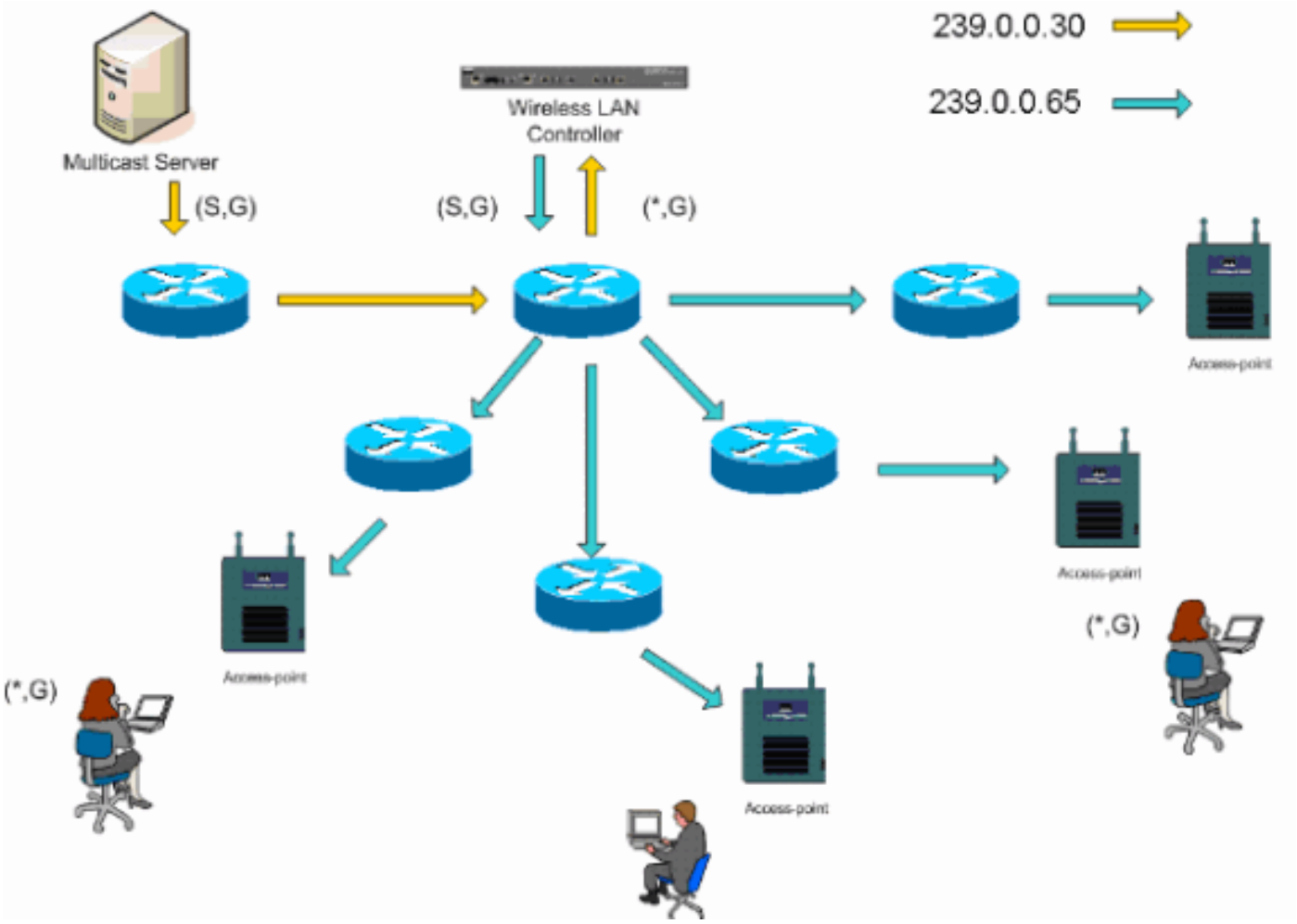
## マルチキャスト - マルチキャストの配信方式

マルチキャスト - マルチキャストの配信方式では、コントローラが受信したマルチキャスト パケットを複製する必要はありません。コントローラは、使用されていないマルチキャスト グループ アドレスに設定され、各アクセス ポイントがそのメンバになります。図3では、WLCからアクセスポイントに定義されたマルチキャストグループは239.0.0.65です。クライアントがWLANにマルチキャスト加入を送信すると、アクセスポイントはLWAPPトンネルを介してこの加入をコントローラに転送します。コントローラでは、このリンク層のプロトコルが直接接続されているローカル エリア ネットワーク接続に転送されます。このネットワークはクライアントの WLAN に対応付けられているデフォルトの VLAN です。コントローラにローカルなルータは、このマルチキャストグループアドレスを転送(*,G))エントリ用のインターフェイスに追加します。図3では、マルチキャスト参加の例がマルチキャストグループ239.0.0.30に送信されています。ネットワークがマルチキャストトラフィックを転送すると、239.0.0.30のマルチキャストアドレスがコントローラに転送されます。次に、コントローラではマルチキャスト パケットが LWAPP マルチキャスト パケットにカプセル化されます。この LWAPP のパケットにはコントローラで設定されている

マルチキャスト グループのアドレスが指定されており（この例では 239.0.0.65）、ネットワークに転送されます。コントローラに属する各アクセス ポイントでは、コントローラのマルチキャスト グループのメンバとして、このパケットが受信されます。次に、アクセス ポイントではクライアント/サーバのマルチキャスト パケット（この例では 239.0.0.30）が、LWAPP マルチキャスト パケット内で識別される WLAN/SSID 宛てにブロードキャストとして転送されます。

**注：マルチキャスト**ネットワークを不適切に設定すると、別のコントローラのアクセスポイントのマルチキャストパケットを受信してしまう可能性があります。最初のコントローラがこのマルチキャスト パケットをフラグメント化する必要がある場合には、そのフラグメントがネットワークに転送され、各アクセス ポイントではこのフラグメントを廃棄するのに時間を費やしてしまいます。たとえば 224.0.0.x のマルチキャストの範囲から送られるあらゆるトラフィックを許可すると、これも各アクセス ポイントからカプセル化した後に転送されます。

**図3:LWAPPマルチキャスト**




## ルータとスイッチのマルチキャスト設定

このドキュメントはネットワークのマルチキャスト設定ガイドではありません。実装の詳細については、『IP マルチキャスト ルーティングの設定』を参照してください。このドキュメントでは、使用しているネットワーク環境でマルチキャストをイネーブルにするための基本的な事項について説明しています。

## IP マルチキャスト ルーティングのイネーブル化

IPマルチキャストルーティングにより、Cisco IOS®ソフトウェアはマルチキャストパケットを転送できます。マルチキャストがイネーブルになっているネットワークでマルチキャストが機能す

るようにするには、グローバル設定コマンドの ip multicast-routing が必要です。**ip multicast-routing**コマンドは、WLCとそれぞれのアクセスポイント間のネットワーク内のすべてのルータで有効にする必要があります。

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

## インターフェイスでの PIM のイネーブル化

これにより、Internet Group Management Protocol ( IGMP; インターネット グループ管理プロトコル ) が動作するためのルーティング インターフェイスがイネーブルになります。Protocol Independent Multicast ( PIM ) モードでは、ルータがマルチキャスト ルーティング テーブルにデータを入れる方法が決定されます。この例では、rendezvous point ( RP; ランデブー ポイント ) をマルチキャスト グループに周知させる必要はなく、したがってマルチキャスト環境の未知の特性を仮定すると、sparse-dense-mode が最も望ましいと考えられます。これは稼働するための設定としては推奨するマルチキャストではありませんが、コントローラに直接接続されたレイヤ 3 インターフェイスでは、マルチキャストが機能するように PIM をイネーブルにする必要があります。WLCとそれぞれのアクセスポイント間のすべてのインターフェイスを有効にする必要があります。

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

## スイッチでの VLAN IGMP スヌーピングのディセーブル化

IGMP スヌーピングにより、マルチキャストが有効になっている交換回線ネットワークでは、トラフィックを、マルチキャストを受信したいユーザが使用するスイッチポートに限定する一方で、マルチキャスト ストリームを受信したくないスイッチポートからマルチキャスト パケットをプルーニングすることができます。Vocera の展開では、4.0.206.0 よりも前のソフトウェア リリースを使用してコントローラと接続しているアップストリーム スイッチポートで、CGMP または IGMP のスヌーピングをイネーブルにすることは望ましくない場合があります。

ローミングとマルチキャストは、マルチキャスト トラフィックが加入しているユーザを処理の対象にしていることを確認するための一連の要件には定義されていません。クライアントのバッジではローミングしていることが認識されていますが、ネットワーク インフラストラクチャがマルチキャスト ( Vocera ブロードキャスト ) トラフィックを継続的にバッジに配送していることを確認するために、さらに IGMP の加入を転送することは行われません。この際に、LWAPP アクセス ポイントでは、一般的なマルチキャスト クエリをローミングされたクライアントに送信して、この IGMP の加入を求めることは行われません。レイヤ 2 の Vocera ネットワーク設計では、IGMP スヌーピングをディセーブルにすると、Vocera ネットワーク メンバのローミング先にかかわらず、すべてのメンバにトラフィックが転送されるようになります。これにより、クライアントのローミング先に関係なく Vocera のブロードキャスト機能が機能します。IGMP スヌーピングをグローバルにディセーブルにすることは、非常に好ましくない処理です。IGMP スヌーピングは、各 WLC に直接接続された Vocera VLAN でのみディセーブルにするのを推奨します。

詳細は、『IGMP スヌーピングの設定』を参照してください。

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

## バージョン 4.0.206.0 以降でのマルチキャストの機能拡張

4.0.206.0 リリースでは、IGMP クエリが導入されています。これにより、ユーザはローミング発生時に通常の IGMP クエリを送信することで、レイヤ 2 でのローミングが行えるようになっています。その後、クライアントは自身がメンバになっている IGMP グループで応答します。そして、これはこのドキュメントで先に説明したように有線ネットワークにブリッジされます。クライアントがレイヤ 2 の接続がないコントローラにローミングする場合、つまりレイヤ 3 のローミングでは、マルチキャストのソース パケットに同期ルーティングが付加されます。レイヤ 3 のローミングを完了したクライアントが、ワイヤレス ネットワークからマルチキャスト パケットを発信すると、外部コントローラでは、このパケットがアンカー コントローラへの IP トンネルで Ethernet over IP ( EoIP ) でカプセル化されます。次に、アンカー コントローラでは、ローカルに対応付けられているワイヤレス クライアントにこのパケットが転送され、さらにこれが有線ネットワークに再度ブリッジされます。ここでは通常のマルチキャスト ルーティング方式を使用してルーティングされます。

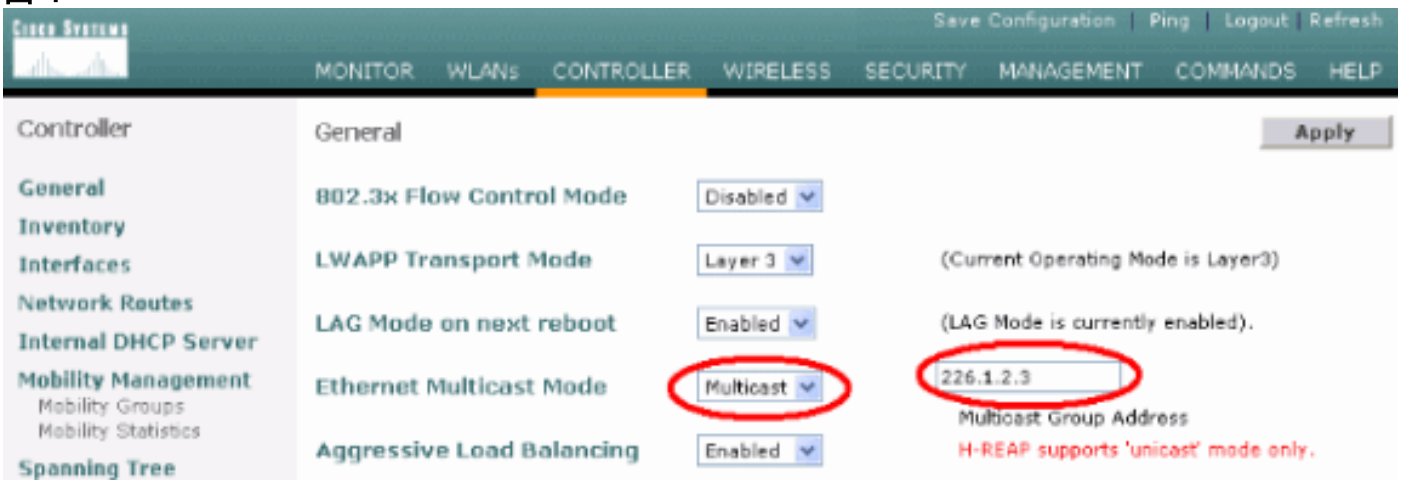
## 導入シナリオ

次の 3 つの導入シナリオでは、Vocera バッジの展開を成功させるためのベスト プラクティスや設計パラメータが説明されています。

- シングル コントローラの導入
- マルチ コントローラのレイヤ 2 導入
- マルチ コントローラのレイヤ 3 導入

Vocera バッジの各機能が LWAPP のスプリット MAC 環境で相互に作用するしくみを理解することは不可欠です。すべての導入シナリオで、マルチキャストをイネーブルにする必要があり、アグレッシブ ロード バランシングはディセーブルにすることが望まれます。バッジの WLAN は、全体のネットワークにおいてすべて同じブロードキャスト ドメインに属している必要があります。

**図 4**




## シングル コントローラの導入

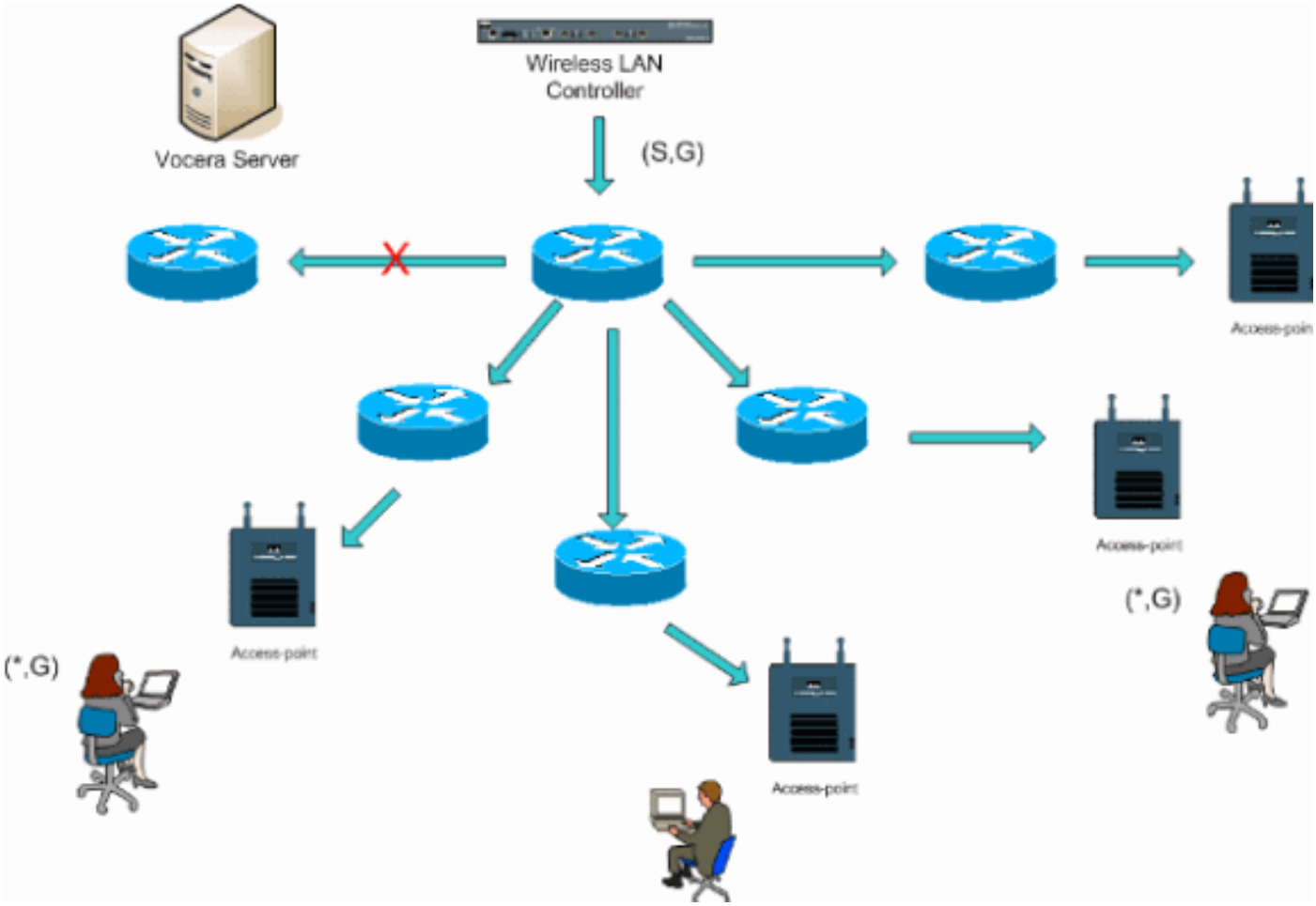
これは最も単純な導入シナリオです。この方法では、導入上の懸念はほとんどなく、Vocera バッジ ソリューションを導入できます。使用するネットワークで IP マルチキャスト ルーティングをイネーブルにする必要があります。この目的はアクセス ポイントが LWAPP マルチキャスト パケットを受信できるようにするためだけです。必要であれば、すべてのルータとスイッチをコントローラのマルチキャスト グループで設定すると、ネットワークのマルチキャストの複雑さを緩和できます。

コントローラでマルチキャストをグローバルに設定すると、正しい SSID、セキュリティ設定、

Vocera バッジ ソリューションに登録されたすべてのアクセス ポイントや、すべての機能が意図したとおりに動作するようになります。また、Vocera ブロードキャスト機能を使用すれば、ユーザのローミングやマルチキャスト トラフィックが意図したとおりに動作するようになります。これ以上の設定は必要なく、ソリューションが正しく動作するようになります。

バッジ ソリューションがマルチキャスト メッセージを送信する際には、Vocera ブロードキャストが使用されるため、メッセージはコントローラに転送されます。次に、コントローラで、このマルチキャスト パケットが LWAPP マルチキャスト パケットにカプセル化されます。次に、ネットワーク インフラストラクチャにより、コントローラに接続されているすべてのアクセス ポイントにこのパケットが転送されます。アクセス ポイントでこのパケットが受信されると、LWAPP マルチキャスト ヘッダーを調べて、このパケットをブロードキャストする WLAN/SSID が判別されます。

**図5：マルチキャストマルチキャストモードのシングルコントローラ**



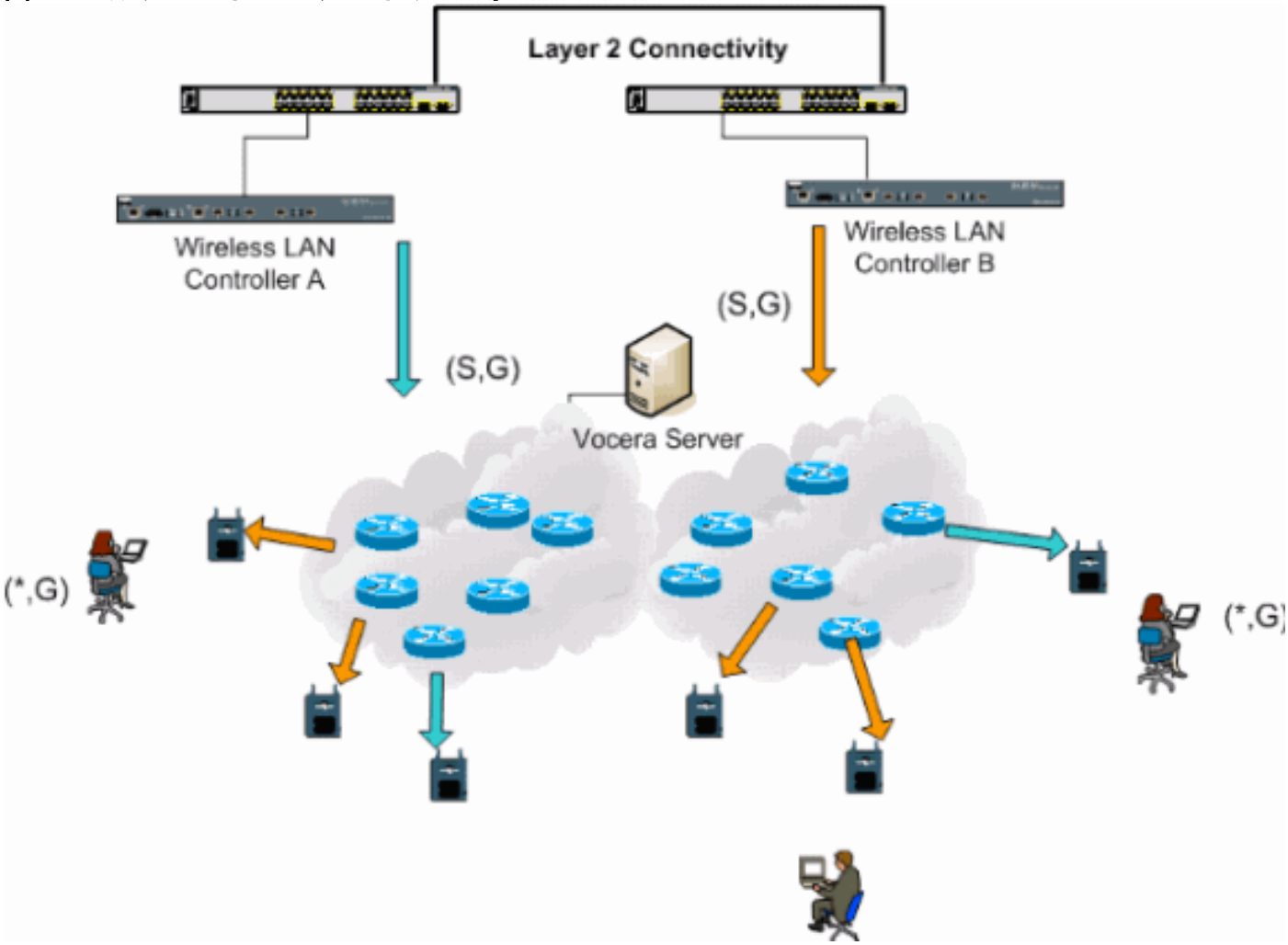

## マルチ コントローラのレイヤ 2 導入

コントローラを複数設置する場合は、すべてのコントローラが同一のレイヤ 2 ブロードキャスト ドメインを介して相互に接続されている必要があります。双方のコントローラにマルチキャストを設定し、フラグメンテーションを制限するために、各コントローラで同一のアクセス ポイントのマルチキャスト グループを使用します。レイヤ 2 のブロードキャスト ドメインが共通のスイッチやスイッチ群を経由して接続されていると想定すると、この単一の VLAN にはこれらのスイッチでの CGMP/IGMP スヌーピングをディセーブルにするか、4.0.206.0 以降の WLC ソフトウェアを稼働させる必要があります。Vocera ブロードキャスト機能を使用していて、1 つのコントローラ上にあるアクセス ポイントから別のコントローラ上にあるアクセス ポイントにあるユーザがローミングする場合、IGMP スヌーピングが動作するように IGMP の加入を新しいレイヤ 2 ポートに転送するメカニズムはありません。IGMP パケットがアップストリーム CGMP または IGMP 対応のスイッチに着信しない場合、指定されたマルチキャスト グループがコントローラに

転送されないため、クライアントでは受信されません。同じ Vocera ブロードキャスト グループに属するクライアントが、ローミングするクライアントが新しいコントローラにローミングされるより前に IGMP パケットを送信していた場合には、これがうまく動作することもあります。バージョン 4.0.206.0 の利点を使用すれば、他のコントローラにレイヤ 2 のローミングとしてローミングされたクライアントでは、認証の直後に一般的な IGMP クエリを受信できるようになります。次に、クライアントは対象グループで応答し、新しいコントローラはこれをローカルに接続されたスイッチにブリッジします。これにより、アップストリーム スイッチでの IGMP と CGMP での利点を活用できます。

使用しているネットワークがマルチキャスト トラフィックを適切に通過させるように設定されていると、別々のバッジ ネットワークにバッジ SSID とレイヤ 2 ドメインを追加作成できます。また、作成されたそれぞれの Vocera レイヤ 2 ブロードキャスト ドメインは、マルチキャストを途切れさせないように、コントローラがネットワークに接続されているすべての場所に存在する必要があります。

**図6：マルチコントローラレイヤ2の導入**

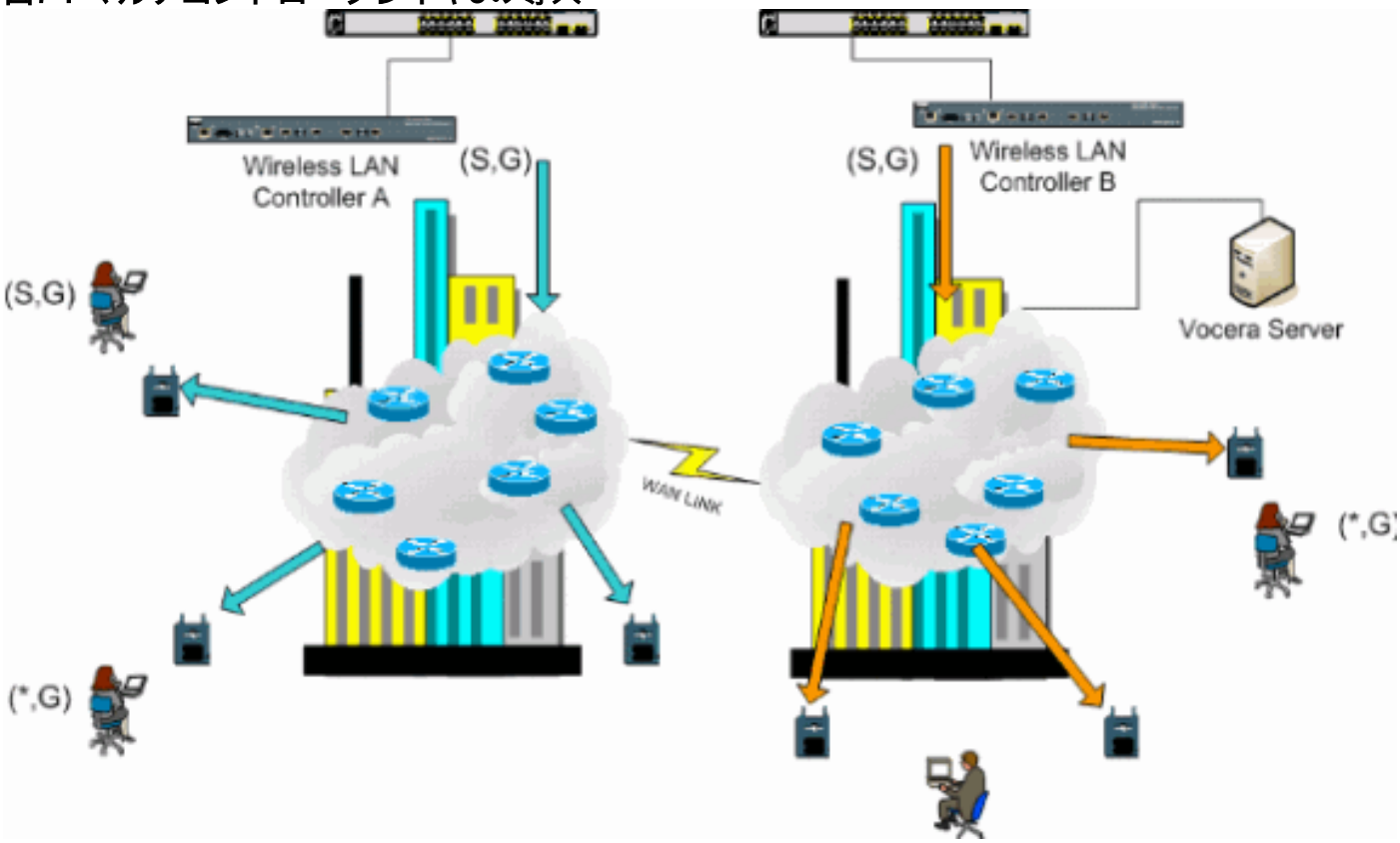



## マルチ コントローラのレイヤ 3 導入

このレイヤ 3 ローミングの導入戦略が使用されるのは、WLC ソフトウェア リリース 4.0.206.0 以降を使用するコントローラ間でのローミングでだけです。クライアントが Vocera ブロードキャスト グループに接続済みで、適切なマルチキャスト ストリームを受信していて、設定されている LWAPP レイヤ 3 ローミングを使用したレイヤ 3 ローミングで他のコントローラにローミングしている場合、対象となるマルチキャスト グループに関するクエリーを受けます。このクライアントが同じ Vocera ブロードキャスト グループに発信する場合、これらのパケットは EoIP トンネルを経由してアンカー コントローラに配信され、通常のマルチキャスト ルーティング方式を使

用してルーティングされます。

**図7：マルチコントローラレイヤ3の導入**




## VoWLAN の導入：シスコの勧告

無線 IP テレフォニー ネットワークでは、RF の慎重な計画が必要です。無線カバレッジの適切なレベルを決定し干渉源を特定するためには、多くの場合、徹底的な音声サイト調査が必要です。有効な音声サイト調査の結果により、アクセス ポイントの設置とアンテナの選択が非常に容易になる場合があります。最も重要な考慮事項は、ワイヤレス電話の伝送パワーです。電話がアクセス ポイントの伝送パワーを学習して、アクセス ポイントに合せて伝送パワーを調節すれば理想的です。

今日のワイヤレス ネットワークの大多数は大掛かりな RF サイト調査後に導入されていますが、これらの調査はデータ サービスも念頭において行われています。VoWLAN 電話の場合、ラップトップなどのモバイル クライアント向けの一般的な WLAN アダプタとはローミング特性やカバレッジ要件が異なると考えられます。したがって、複数の VoWLAN クライアントのパフォーマンス要件に備えるため、多くの場合、音声のためのサイト調査を追加的に行うことが推奨されます。この追加調査により、VoWLAN 電話に十分な RF カバレッジと帯域幅を確保し、適切な音声品質を提供できるようアクセス ポイントを調整できます。

RF 設計時の考慮事項に関するその他の情報は、『Cisco ワイヤレス LAN 設計ガイド』の「WLAN 無線周波数（RF）の設計に関する考慮事項」のセクションを参照してください。このドキュメントは http://cisco.com/go/srnd で入手できます。

## 多層ビルディング、病院、倉庫に関する推奨事項

複数階の建物、病院、および倉庫を対象として調査を行う場合は、このセクションに記載する要素について考慮してください。

### 建築方式と建築資材

サイト調査では、建築に関する多くの側面が不明か、または表示されていません。そのため、建築図面など別の情報源からその情報を得る必要がある場合もあります。 アクセス ポイントの範囲とカバレッジ エリアに影響する建築方式および建築資材の一般的な例としては、窓ガラスに貼られた金属性の被膜、鉛入りガラス、釘止めした壁、鉄筋コンクリートの床と壁、金属箔を使用した断熱材、階段室とエレベータ シャフト、配管と取付具などがあります。

### インベントリ

さまざまなタイプの在庫品、特に鋼材や水分を多く含む在庫品が RF 範囲に影響する可能性があります。注意を必要とするものには、厚紙製の箱、ペット フード、塗料、石油製品、エンジン パーツなどがあります。

### 在庫のレベル

サイト調査は、在庫のレベルや活動がピークのときに実施するようにします。同じ倉庫でも、在庫レベルが 50 % の場合と 100 % の場合では、RF のフットプリントが大きく異なります。

### 活動のレベル

同様に、同じオフィス エリアでも、一日のうち最も人の多い時間帯と（人のいない）就業時間外では RF のフットプリントが異なります。満員の状態でなくてもサイト調査の多くの部分は実施できますが、その場所が使用されているときにサイト調査を実施し、キーとなる値を微調整することも非常に重要です。利用率の要件とユーザの密度が高いほど、入念に設計されたダイバーシティ ソリューションが重要になります。より多くのユーザがいれば、各ユーザのデバイスが受信する信号は多くなります。信号の増加は、コンテンション、ヌル ポイント、およびマルチパスによる歪みの増加につながります。アクセス ポイントのアンテナのダイバーシティ構成は、このような条件を最小限にするのに役立ちます。

### 多層ビルディング

一般的なオフィス ビルのサイト調査を行う場合は、次のガイドラインを念頭においてください。

- エレベータ シャフトは RF 信号を遮断し、反射させる。
- 在庫品のある貯蔵室は信号を吸収する。
- 堅い壁で囲まれた内側のオフィスは RF 信号を吸収する。
- 休憩室（給湯室）は、電子レンジの使用によって 2.4 GHz の干渉を発生させる可能性がある。
- 実験室は、2.4 GHz または 5 GHz の干渉を発生させ、マルチパスによる歪みと RF の不達域を生む可能性がある。
- パーティションは信号を吸収し、遮断する傾向にある。
- 会議室は利用率が高いため、高いアクセス ポイント カバレッジを必要とする。

複数の階がある施設を調査する場合は、特別な対策を施します。同じフロアにあるアクセス ポイントと同様に、異なる階のアクセス ポイントどうしが簡単に干渉し合う場合があります。この動作を調査に利用できる場合があります。ゲインの大きいアンテナを使用すれば、アクセス ポイントが取り付けられている下のフロアだけでなく、床と天井を貫通させて上のフロアにもカバレッジを提供できる可能性があります。異なるフロアのアクセス ポイント間または同じフロアのアクセス ポイント間のチャネルをオーバーラップさせないように注意します。複数のテナントが入っ

ているビルでは、セキュリティの懸念から、近隣のオフィスに信号が伝わらないよう伝送パワーとアンテナのゲインを低くする必要がある場合があります。

**病院**

病院の調査プロセスは、企業の調査プロセスとほとんど同じです。しかし、病院施設のレイアウトは次の点で異なる傾向にあります。

- 病院の建物は増改築を繰り返す傾向にある。増築のたびに、減衰レベルの異なる建築資材が使用されることが考えられます。
- 患者の立ち入るエリアの壁と床は、通常、最小限の信号しか貫通せず、マイクロセルやマルチパスの変化が生じやすい。
- WLAN 超音波機器や他のポータブルな画像アプリケーションの使用が増加すると、帯域幅の必要性が増す。ワイヤレス音声の追加によっても帯域幅の必要性は増します。
- 病棟のセルは小さく、特に音声アプリケーションの場合、シームレスなローミングが不可欠。
- セルのオーバーラップが多く、チャネルの再利用率も高い可能性がある。
- 病院には複数のタイプのワイヤレス ネットワークがインストールされている場合がある。これには、2.4 GHz の非 802.11 機器などがあります。この機器により他の 2.4 GHz ネットワークとのコンテンションがもたらされる可能性があります。
- 壁面マウント ダイバーシティ パッチ アンテナと天井マウント ダイバーシティ全方向性アンテナが一般的ですが、ダイバーシティ構成を必要とすることに留意してください。

**倉庫**

倉庫には広いオープンな領域があり、多くの場合は高い収納棚があります。多くの場合、これらの棚は、通常アクセス ポイントが設置される天井まで届くものです。このような収納棚により、アクセス ポイントがカバーできるエリアが制限される可能性があります。その場合は、アクセス ポイントを側壁やコンクリートの支柱など天井以外の場所に設置することを考慮します。また、倉庫の調査を行う場合は次の要素を考慮します。

- 在庫のレベルによって必要なアクセス ポイントの数が異なる。予定設置場所に 2 つか 3 つのアクセス ポイントを使用してカバレッジをテストします。
- マルチパスの具合によって予想外のセルのオーバーラップが考えられる。信号品質は、信号強度よりも大きく変動します。クライアントは、近くのアクセス ポイントよりも遠くにあるアクセス ポイントとの方が関連付けと操作性がよい場合があります。
- 調査では、通常アクセス ポイントとアンテナはケーブル接続になっていません。しかし、実稼働環境では、アクセス ポイントとアンテナの間にアンテナ ケーブルが必要な場合があります。アンテナ ケーブルは必ず信号損失をもたらします。厳密な調査には、設置するアンテナのタイプとケーブルの長さを含めます。ケーブルと、ケーブルによる損失をシミュレーションするのに適したツールとして、調査キットの中の減衰器を使用できます。

製造施設の調査は倉庫の調査と類似していますが、製造施設には RF 干渉源がさらに多い点が異なります。さらに、通常、製造施設での適用では、倉庫での適用よりも多くの帯域幅が必要となります。このような適用例には、ビデオ画像とワイヤレス音声が含まれる場合があります。製造施設では、最大のパフォーマンス問題はマルチパスによる歪みと考えられます。

## サポートされるセキュリティ メカニズム

認証とデータ暗号化に使用する静的な WEP と Cisco LEAP の他に、Vocera バッジでは WPA-PEAP (MS-CHAP v2)/WPA2-PSK もサポートされています。

### LEAP の考慮事項

LEAP では、ユーザ名とパスワードに基づいたデバイスの相互認証 ( バッジからアクセス ポイント、アクセス ポイントからバッジ ) が可能になります。認証時、トラフィックを暗号化するため電話とアクセス ポイントの間にダイナミックなキーが使用されます。ただし、LEAP をセキュリティ ソリューションとして使用する場合は、ASLEAP 辞書攻撃を考慮する必要があります。

詳細については、『Cisco LEAP 脆弱性に対する辞書攻撃』を参照してください。

LEAP を使用する場合は、ユーザ データベースへのアクセスを提供するために Cisco Access Control Server ( ACS ) など LEAP に準拠した RADIUS サーバが必要です。Cisco ACS は、ユーザ名とパスワードのデータベースをローカルに格納するか、または外部の Microsoft Windows NT ディレクトリからその情報へアクセスできます。LEAP を使用する場合は、すべてのワイヤレス デバイスに強力なパスワードを使用するようにします。強力なパスワードとは、10 から 12 文字の長さで、大文字と小文字のほか特殊文字も含んだパスワードのことです。

ほとんどのバッジで同じパスワードを使用し、それをバッジに保存するため、Cisco ではデータ クライアントとワイヤレス音声クライアントには異なるユーザ名とパスワードを使用することを推奨しています。この方法は、セキュリティだけでなくトラッキングやトラブルシューティングにも役立ちます。バッジのユーザ名とパスワードの保存に外部 ( ACS 以外 ) のデータベースを使用することは有効な設定オプションですが、Cisco ではこの方法を推奨しません。バッジがアクセス ポイント間をローミングするたびに ACS へのクエリが必要なため、ACS 以外のデータベースへアクセスすることによる予測不可能な遅延によって、過度の遅延と音声品質の低下が生じる可能性があります。

## ワイヤレス ネットワーク インフラストラクチャ

有線 IP テレフォニー ネットワークと同様、無線 IP テレフォニー ネットワークでは VLAN 設定、ネットワーク規模の決定、マルチキャストの転送、および機器の選択に慎重な計画が必要です。有線またはワイヤレスのどちらの IP テレフォニー ネットワークでも、十分なネットワーク帯域幅を確保して、トラブルシューティングを簡単に行えるようにするには、多くの場合、音声とデータに別の VLAN を使用するのが推奨する最も効率的な導入方法です。

### 音声、データ、および Vocera の各 VLAN

VLAN は、ネットワークを 1 つ以上のブロードキャスト ドメインにセグメント化するメカニズムです。音声とデータのトラフィックを異なったレイヤ 2 ドメインに分離することが一般的に推奨される IP テレフォニー ネットワークでは、VLAN は特に重要です。Voceraバッジ用に、他の音声およびデータトラフィックとは別のVLANを設定することを推奨します。アクセスポイント管理トラフィック用のネイティブVLAN、データトラフィック用のデータVLAN、音声トラフィック用の音声または補助VLAN、およびVoceraバッジ用のVLAN。音声 VLAN を切り離すことにより、ネットワークはレイヤ 2 のマーキングを利用してレイヤ 2 アクセス スイッチ ポートでプライオリティ キューイングを提供できます。それにより、さまざまなクラスのトラフィックに適切な QoS が確実に提供され、IP アドレッシング、セキュリティ、およびネットワークの規模決定などのアドレッシング問題の解決が助けられます。Vocera バッジでは、配信にマルチキャストを使用するブロードキャスト機能が使用されます。一般的な VLAN では、バッジがコントローラ間をローミングする際、引き続きマルチキャスト グループに残ります。この最後の処理については、このドキュメントの後半でマルチキャストについて説明する際に詳しく説明します。

## ネットワーク規模の決定

音声トラフィックの存在によって生じる需要を満たすように適切な帯域幅とリソースを確保するには、IP テレフォニー ネットワークの規模を決定することが不可欠です。通常の IP テレフォニーで PSTN ゲートウェイ ポート、トランスコーダ、WAN 帯域幅などのコンポーネントの規模を決定するための設計ガイドラインに加え、ワイヤレス IP テレフォニー ネットワークの規模を決定する際には、下記の 802.11b に関する問題を考慮します。Vocera バッジは、一般的に推奨する導入の規模を上回る数の有線クライアントを拡張する専門的なアプリケーションです。

### アクセス ポイントあたりの 802.11b デバイス数

Cisco では、アクセス ポイントあたりの 802.11b デバイス数が 15 ～ 25 を超えないようにすることを推奨いたします。

### アクセス ポイントあたりのアクティブ コール数

Vocera では、バッジ対バッジ（独自の低ビット レートのコーデック）コールかバッジ対電話（G.711 コーデック）コールかによって、2 つの異なるコーデックが使用されています。次の表では、データ レートごとに使用可能な帯域幅の割合を示しています。ここから、予想できるスループットが明確にわかります。

| コール プロセス | 1 Mbps | 2 Mbps | 5.5 Mbps | 11 Mbps |
|---|---|---|---|---|
| バッジ対電話（G.711） | 20.7 % | 11.8 % | 6.3 % | 4.7 % |
| バッジ対バッジ（独自の低ビット レート コーデック） | 9.4% | 6.1% | 4.2 % | 3.6 % |

# スイッチに関する推奨事項

**注：ネットワークのメインルータとして**Cisco Catalyst 4000シリーズスイッチを使用する場合は、Supervisor Engine 2+(SUP2+)またはSupervisor Engine 3(SUP3)モジュールが少なくとも含まれていることを確認してください。Cisco Catalyst 2948G、2980G、2980G-A、4912、2948G-GE-TX スイッチと同様に、SUP1 や SUP2 モジュールにより、ローミングの遅延が発生する可能性があります。

スイッチ ポート テンプレートを作成し、アクセス ポイントへ接続するスイッチ ポートの設定に使用できます。このテンプレートには、標準デスクトップ テンプレートの基本的なセキュリティおよび復元機能がすべて含まれている必要があります。さらに、アクセス ポイントを Cisco Catalyst 3750 スイッチにアタッチする場合は、Multilayer Switching（MLS; マルチレイヤ スイッチング）QoS コマンドを使用してポート速度を制限したり、Class of Service（CoS; サービス クラス）を Differentiated Services Code Point（DSCP）設定にマッピングしたりすることで、アクセス ポイントのパフォーマンスを最適化できます。

WLAN クライアントに必要のないトラフィックは、アクセス ポイントに送信する必要がありません。テンプレートは、次の機能を使用して、セキュアで復元力のあるネットワーク接続が作成されるように設計する必要があります。

- [ポート設定をデフォルトに戻す(Return Port Configurations to default)]：既存のポート設定をすべてクリアすることで、設定の競合を防止します。

- ダイナミックトランキングプロトコル(DTP)の無効化：ダイナミックトランキングを無効にします。ダイナミックトランキングはアクセスポイントへの接続には必要ありません。
- Disable Port Aggregation Protocol(PagP):PagPはデフォルトで有効になっていますが、ユーザ側のポートには必要ありません。
- PortFast をイネーブルにする：スパニング ツリー リンクがダウンしても、トラフィックの転送をスイッチですばやく再開できます。
- ワイヤレスVLANの設定：ワイヤレストラフィックを他のデータ、音声、および管理VLANから分離する一意のワイヤレスVLANを作成します。このようにトラフィックを分離することで、トラフィックの管理性が高まります。
- Quality of Service(QoS)の有効化[ポートを信頼しない（0にマークダウン）(do not trust port (mark down to 0))]：ソフトフォンを含む優先度の高いトラフィックを適切に処理し、ユーザがPCを再設定して過剰な帯域幅を消費しないようにします。

WS-C3750-48PS-S インライン電源スイッチを使用すると、インライン パワー対応のアクセス ポイントへ電力を供給できます。

Catalyst 6500 を使用すると、ここで説明したすべての機能を使用し、さらに多数のサービス モジュールを統合することにより、パケットを回線レートで転送できます。Wireless Service Module（WiSM）を使用すると、それぞれが 150 台のアクセス ポイントを制御する機能を備えたコントローラを 2 台使用できます。シャーシあたり最大で 5 つの WiSM を使用すると、単一の高性能スイッチング アーキテクチャで 50,000 台のクライアントをサポートできる 1,500 台のアクセス ポイントを制御できます。

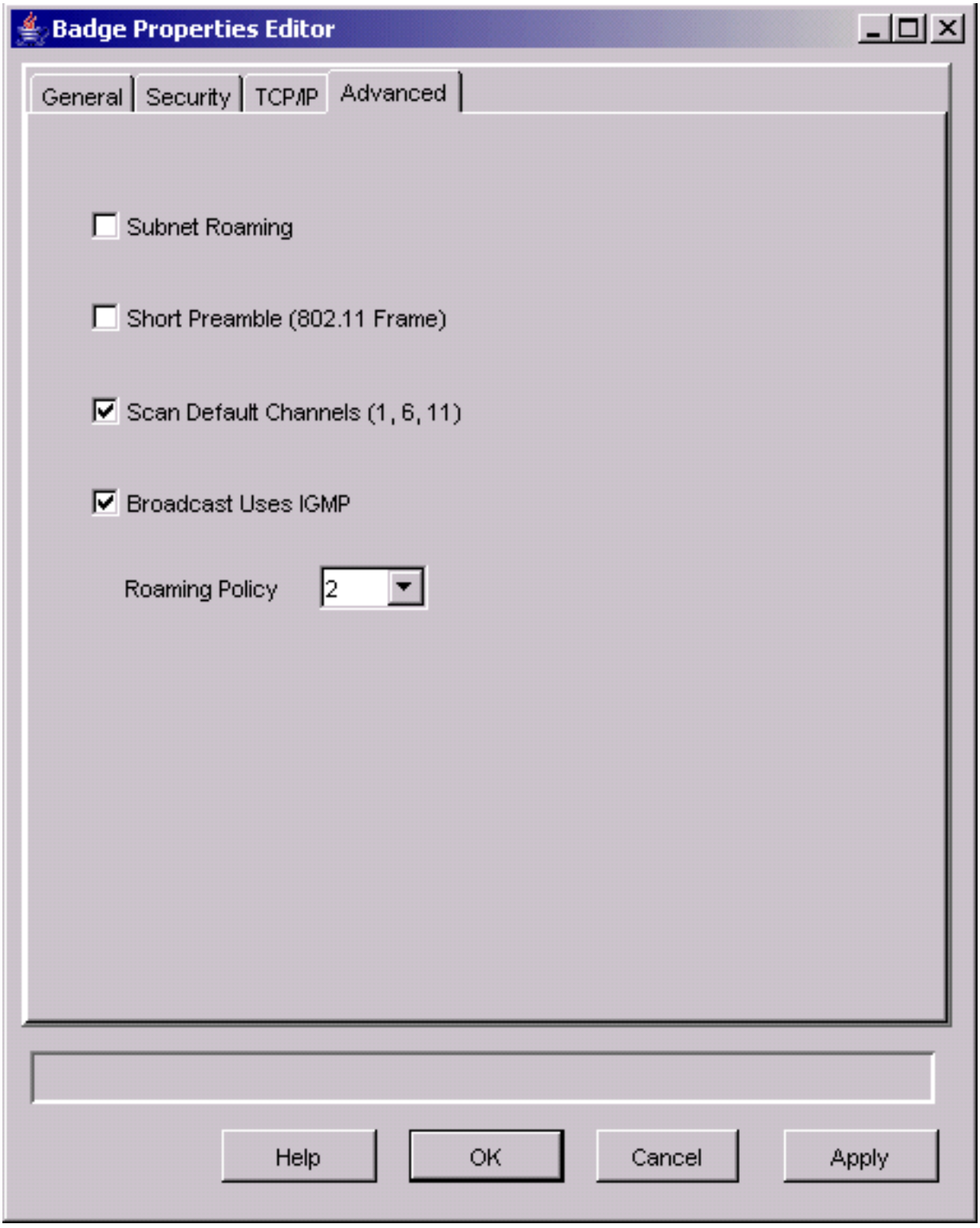
# 導入と設定

## バッジの設定

Vocera Badge Configuration Utility（BCU）とバッジの設定を行う場合、誤って設定すると、ユーザ環境でローミングと遅延が発生する可能性があります。BCU と Badge Properties Editor（BPE）を使用して、次の設定を確認してください（図 8 を参照）。

- **Subnet Roaming がディセーブルになっている。**
- **Scan Default Channels (1,6,11) にチェックマークが付いている。**
- **Broadcast Uses IGMP がイネーブルになっている。**
- Roaming Policy が 2 以上に設定されている。

**図8:[Vocera BCU Advanced]タブ**




Subnet Roaming にチェックマークが付いていると、それぞれのローミング処理の後にバッジに新しい IP アドレスを要求するように指示が出ます。LWAPP環境では、インフラストラクチャはレイヤ3でのクライアント接続の維持に役立ちます。音声クライアントがDHCPサーバの応答を待ってからパケットの送受信を行う必要がある場合、遅延とジッタが発生します。Scan Default Channels (1,6,11) がチェックされていないと、バッジではローミングを試みる際にすべての 802.11b チャネルがスキャンされます。このため、パケットの転送やシームレスなローミングが阻害されます。

## 導入する環境に合せた AutoRF の調整

このドキュメントの「Cisco の推奨する方式」のセクションで説明されているように、各サイト

ごとにそれぞれの RF 特性があることを理解することが大切です。各サイトごとに異なり、AutoRF または Radio Resource Management（RRM）を使用している環境に合せて調整することが必要であることを理解した上で、調整用に AutoRF/RRM が必要です。

AutoRF を調整する前に、詳細について『Unified Wireless Network における Radio Resource Management（RRM）』を参照してください。

RRM では、各アクセス ポイントが 3 番目に強い隣接装置を受信する強度を調整して、各アクセス ポイントの伝送パワーを調整します。この値を調整する唯一の方法は、『Tx Power Level Assignment の設定』で説明されているように、CLI から config advanced 802.11b tx-power-thresh コマンドを使用することです。

AutoRF を調整する前に、エンドユーザが着用するように Vocera バッジを使用して導入先のサイトを歩き、サイト調査ツールを使用して、バッジがローミングを行うようすや、各アクセス ポイントにアクセスできるパワーについてよく理解してください。これが完了し、この値の調整が必要と判断されたら、送信電力制御(TPC)アルゴリズムの値–71 dBmから開始します。次の CLI パラメータを使用してください。

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

この調整によって何か変化が見られるまで、少なくとも 30 分間から 1 時間はネットワークを稼働させます。十分な時間が経過したら、同じ調査ツールとバッジを使用して、サイトを再度歩いてみます。先ほどと同じローミング特性やアクセス ポイントのパワーを観察します。ここでの目的は、次のアクセス ポイントが実質的に最適な信号対雑音比を得た時点で、あるいはそれよりも前にバッジがローミングされるようにすることです。

- **伝送パワーが高すぎるまたは低すぎるのを見極める方法**伝送パワーのしきい値が高すぎるか低すぎるかを判断するには、使用している環境についてよく理解することが必要です。導入エリア全体（Vocera バッジが機能することを想定しているエリア）を歩き回る場合には、アクセス ポイントの設置場所を認識した上で、バッジのローミングの動作を体験する必要があります。
- **伝送パワーが高すぎる場合に取る手段**Vocera バッジのローミングは、信号の品質ではなく信号の強度に基づいて行われます。いくつかのアクセス ポイントを通過して、その間にウェルカム チュートリアルやテスト トーンを処理しながら、Vocera バッジでローミングが行われなかった場合、そのバッジは変化が鈍いと判断できます。この傾向がキャンパスの導入エリア全体で見られる場合には、現在の伝送パワーのしきい値が高すぎるため、低くする必要があります。この現象が見られるのが 1 個所か 2 個所程度の特定の場所だけで、他のエリアでは理想的なローミング特性が見られる場合は、ネットワークでの伝送パワーが高すぎることによる兆候ではありません。
- **伝送パワーが低すぎる場合に取る手段**デフォルトの伝送しきい値では、導入エリアで伝送パワーが低くなりすぎるようなことはほとんどありません。伝送パワーのしきい値を低く調整した状態で Vocera バッジを装着してエリア内を歩くと、バッジのローミングは正しく行われるものの、接続が失われたり、カバーされていないエリアが生じたり、カバー領域にむらが生じたりします。この場合は、ネットワークの伝送パワーが低すぎる可能性があります。この特性がネットワーク全体でみられるのではなく、1 個所か 2 個所の特定のエリアで見られる場合は、ネットワーク規模の問題というよりも、カバレッジ ホールの存在が示唆されています。
- **特定の場所での動作**バッジがあるアクセス ポイントから離れず理想的な方法でローミングが行われないのが、1 個所か 2 個所程度のエリアである場合は、その エリアを調べてください。このエリアは他のキャンパスとどのように異なるのか。このようなエリアが建物の出口の

近くや工事中のエリアである場合は、これらのアクセス ポイントに対してカバレッジ ホールの検出を行ってパワーを上げることができるか。WLC のログ ファイルとアクセス ポイントのネイバー リストを調べて、このような異常が生じる原因を調査する。1 個所や 2 個所程度の特定のエリアにおいて、カバーされていなかったり、カバーにむらがあるところがバッジで検出された場合は、これらのエリアを個別に調査する必要があります。そのエリアはエレベータ シャフト、放射線施設、または休憩室の近くか。音声のカバー領域が改善するようにアクセス ポイントを新たに設置したり位置を調整することによって、これらのエリアの状態が改善する。ただし、いずれの場合でも、ライセンス不要の無線スペクトラムを使用しているわけであり、理想的な動作を得るのは難しいことを理解してください。このような現象は、設置場所が、無線送信用の塔や装置、テレビ用送信施設、あるいは 802.11 2.4 GHz 以外の電波を発生する装置（ワイヤレス電話など）の近くにある場合に発生することがあります。

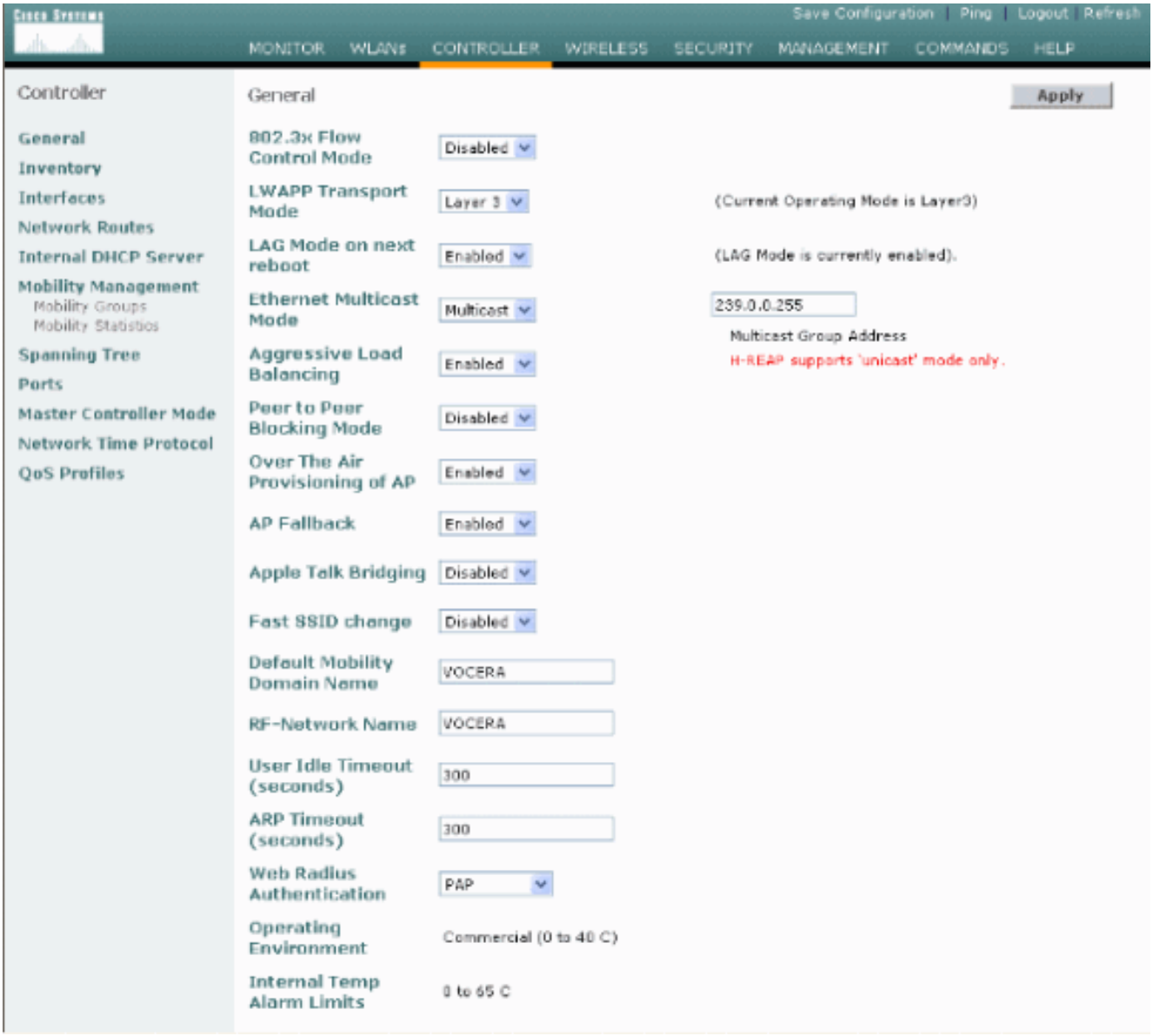
## 無線ネットワーク インフラストラクチャの設定

WLCの全体的な設定については、Cisco Unified Wireless Networkの設計および導入ガイドに従う必要があります。 このセクションでは、Vocera®の通信バッジに固有の追加の推奨事項について説明します。

**注：次のステ**ップに移動する前に[適用]ボタンを押さないと、**変更**は保存されません。

次の手順を、トップレベルのメニューの Controller の下で実行します。

1. Ethernet Multicast Mode を Multicast に変更します。
2. Multicast Group Address を 239.0.0.255（または他の使用されていないマルチキャスト グループ アドレス）に設定します。
3. Default Mobility Domain Name と RF-Network Name をネットワークの設計に合わせて設定します。
4. Aggressive Load Balancing をディセーブルにします。**図9：一般的なWLCの設定**

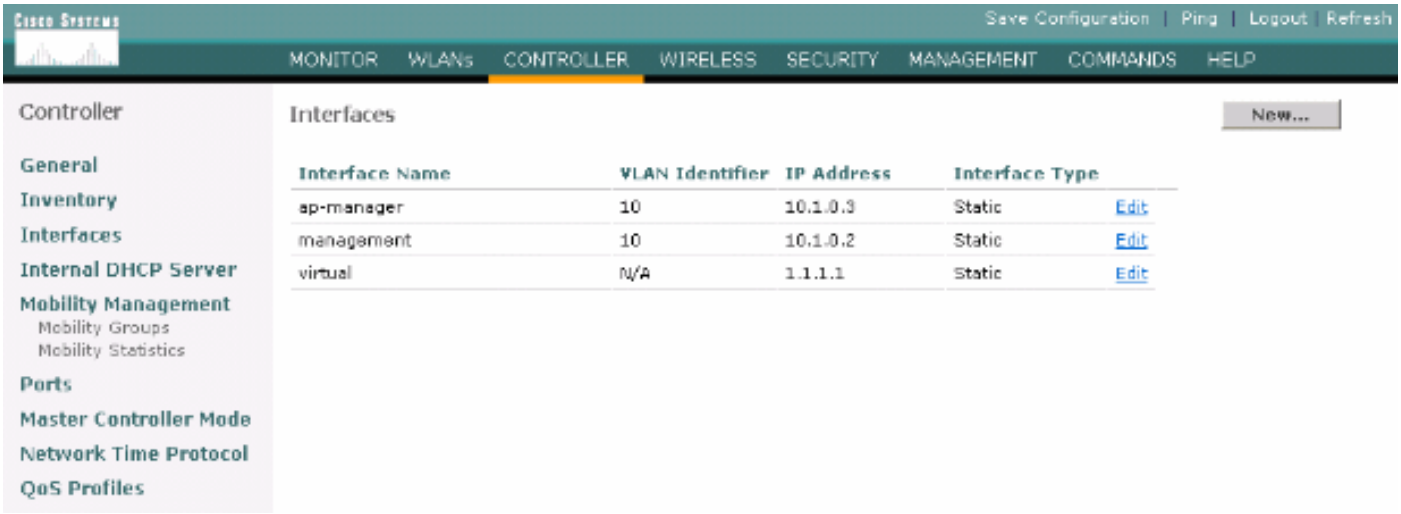



## インターフェイスの作成

[コントローラ] > [インターフェイス]をクリックします。

注：VLANとIPアドレスは異なります。この画面で使用しているアドレスは例なので、この値をこのまま使用しないでください。

図10:WLCインターフェイスのリスト




## Vocera音声インターフェイスの作成

次のステップを実行します。

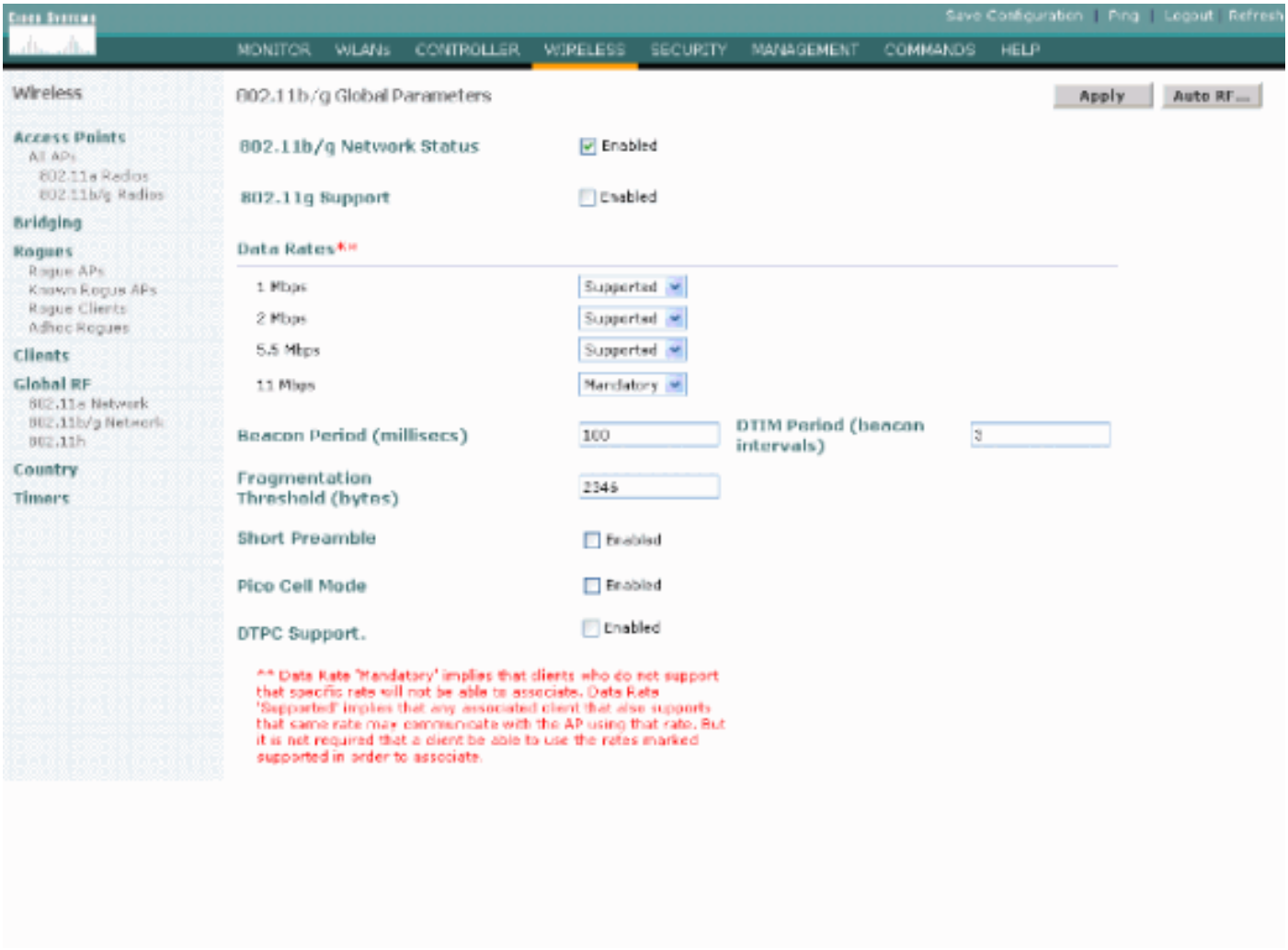
1. [New] をクリックします。
2. Interface Name フィールドに、Vocera VoWLAN ネットワークを表すタグ名を入力します。
3. VLAN ID フィールドに、その VoWLAN ネットワークの VLAN 番号を入力します。
4. 作成したインターフェイスを編集するため、Apply、続いて Edit をクリックします。
5. このインターフェイスに関し、VLAN 範囲内の IP アドレッシングと他の関連情報を入力します。
6. [Apply] をクリックします。

## 無線固有の設定

Vocera バッジのみを使用する WLAN では、次の設定例が Vocera ブロードキャスト アプリケーションを最適にサポートする例となります。

- DTIM Period は 1 にします。
- 802.11g のサポートはディセーブルにします。11 Mpbs の 802.11b データ レートだけを Mandatory にします。
- Short Peamble をディセーブルにします。
- DTPC をディセーブルにします。

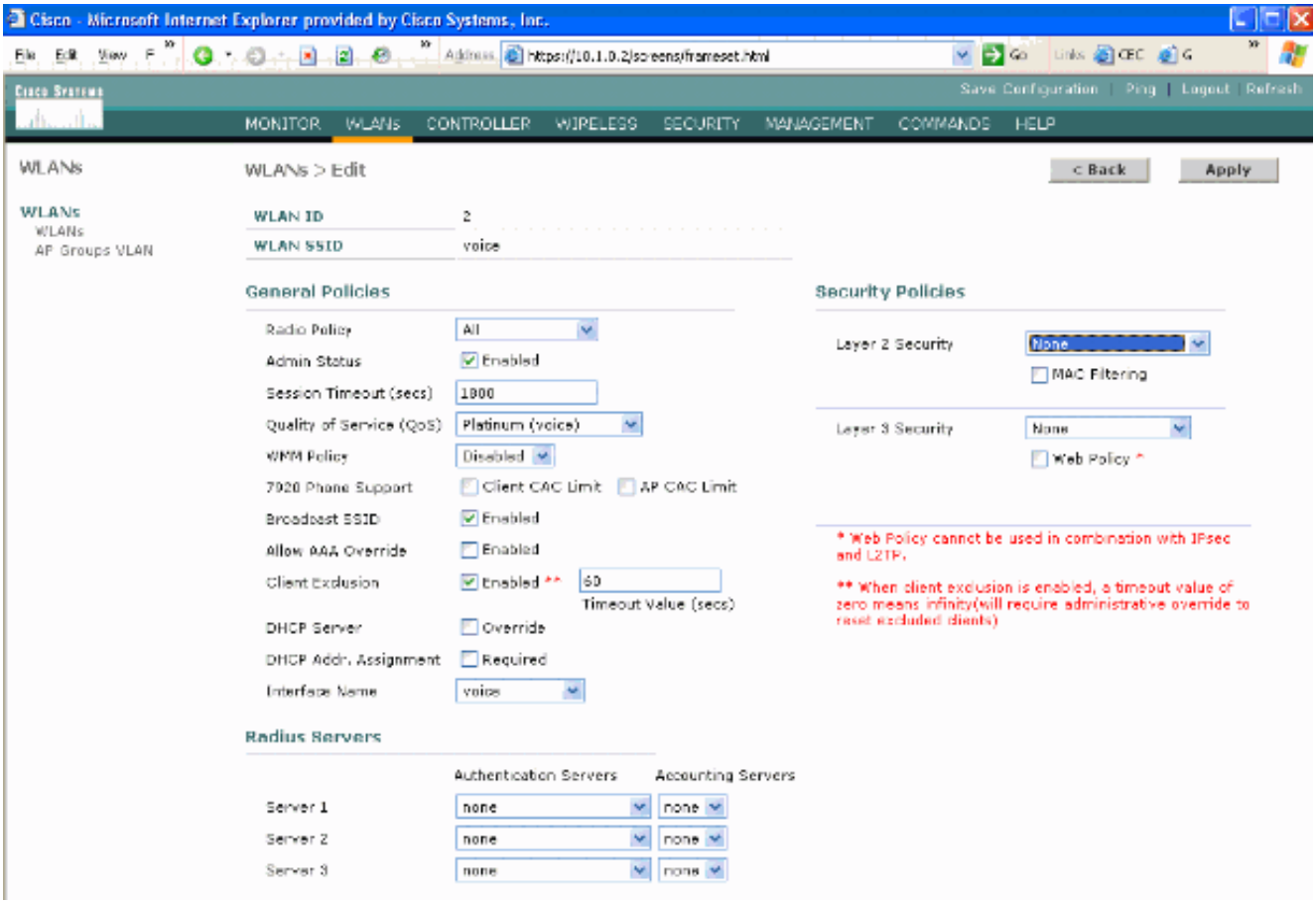
**図11:802.11b/gの設定**




## WLAN 設定

次のステップを実行します。

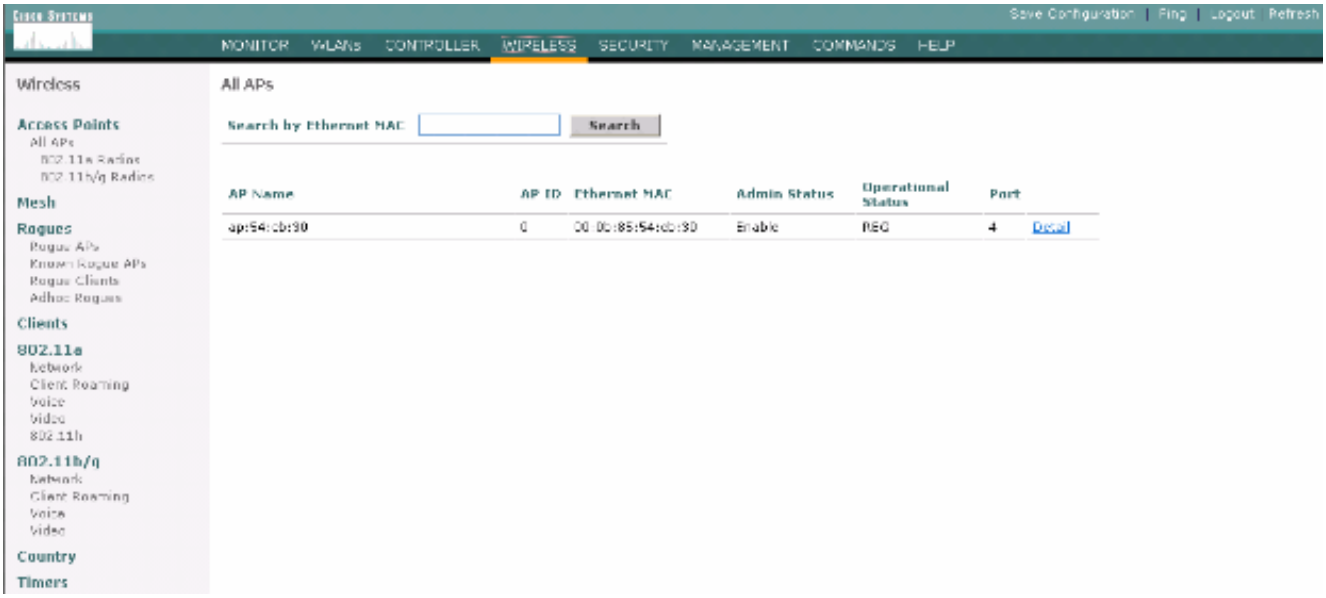
1. Radio Policy フィールドを、ニーズに最適な値に更新します。
2. Admin Status を Enabled に変更します。
3. Session Timeout を 1800 に設定します。
4. Quality of Service を Platinum に設定します。
5. Broadcast SSID を Enabled に設定します。
6. Interface Name を、Vocera 通信バッジ用に作成したインターフェイスに設定します。
7. 自社のポリシーに合うように、セキュリティのオプションを設定します。**図12:WLANの設定**




## アクセス ポイントの詳細設定

次のステップを実行します。

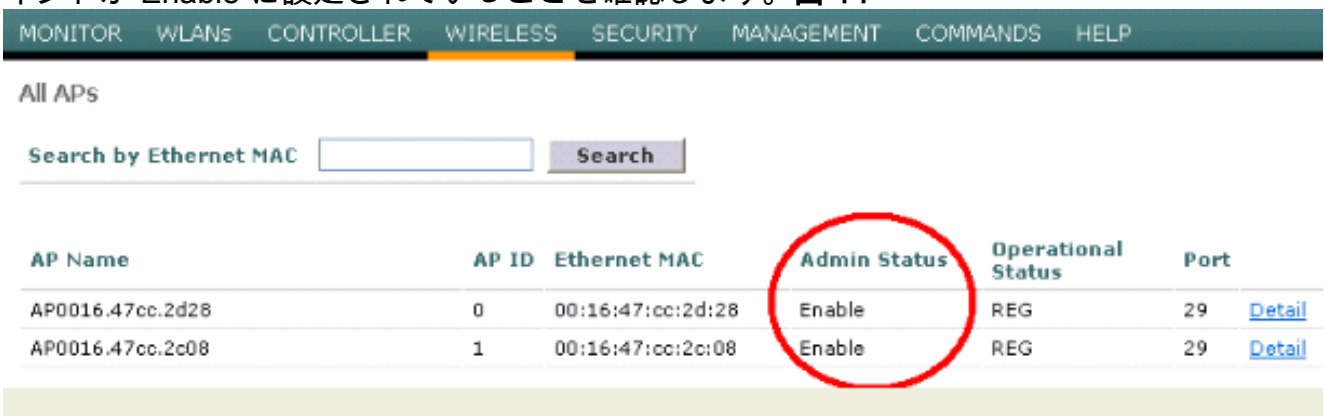
1. Detail をクリックします。
2. AP Name を設定します。
3. アクセス ポイントが DHCP に設定されていることを確認します。
4. Admin Status が Enabled であることを確認します。
5. AP Mod」をlocalに設定する必要が**あります**。
6. アクセス ポイントの位置を入力します。
7. アクセス ポイントが所属するコントローラ名を入力します。コントローラ名は Monitor ページに表示されています。
8. [Apply] をクリックします。**図13:APの詳細**



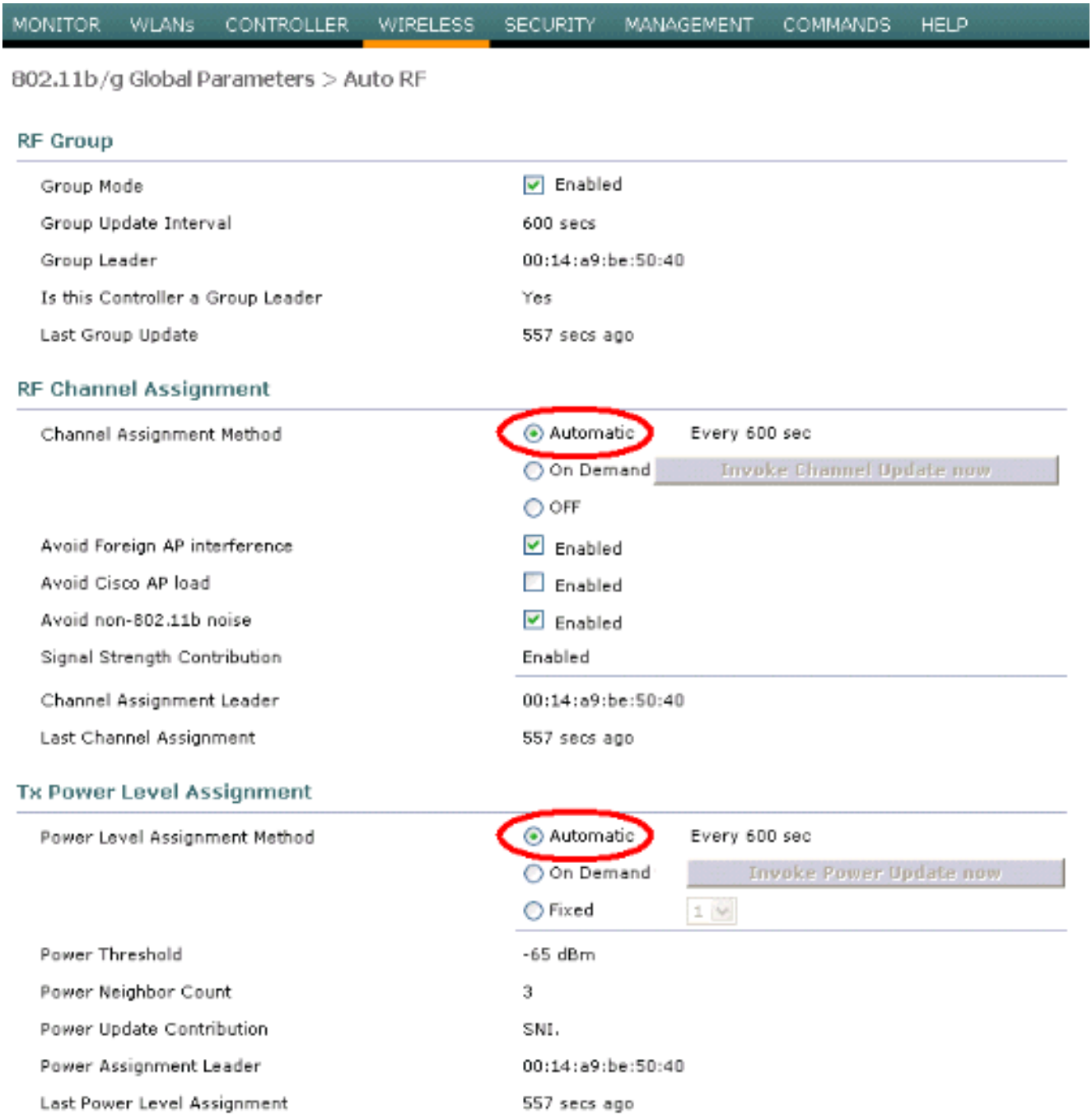

## 802.11b/g 無線の設定

次のステップを実行します。

1. WLC の最上部にある Wireless をクリックして、Admin Status の下ですべてのアクセス ポイントが Enable に設定されていることを確認します。**図 14**




2. Network ( 802.11b/g の近く ) をクリックします。
3. AutoRF をクリックします。
4. AutoRF を使用し、オーバーラップしない RF チャネルと伝送パワーを設定して完全なカバレッジを作成します。そのためには、RF Channel Assignment と Tx Power Level Assignment の両方で Automatic を選択します。**図 15**




5. [Apply] をクリックします。
6. Save Configuration をクリックし、このドキュメントの「導入する環境に合せた AutoRF の調整」のセクションを参照してください。
7. **[Wireless] > [Access Points] > [802.11b/g Radios]を選択します。図 16**

# ワイヤレス IP テレフォニーの確認

RF サイト調査を実施し、アクセス ポイントと電話の設定を行ったら、すべての動作が期待通りに行われることを確認するために、確認テストを行うことが非常に重要です。このテストは、次のすべての場所で実行します。

- 各アクセス ポイント セルの主要エリア ( バッジがそのアクセス ポイントに接続する可能性の最も高い場所 ) 。
- 通話量が多いと考えられる場所。
- 使用頻度は低いが、カバレッジの保証が必要な場所 ( たとえば、階段室や化粧室など )
- アクセス ポイントのカバレッジ エリアの外縁
- •これらのテストは並行して、または順次実行できます。テストを並行して行う場合、各ロケーションでの完全な関連付け、認証、および登録をテストするために、テストするポイント間で電話機の電源がオフになっていることを確認します。ローミング テストと負荷テストは、最終的なテストとなります。

# 関連付け、認証、および登録

このセクションでは、バッジが正しく関連付けられ、認証され、登録されることを確認する方法について説明しています。

- 環境全体における複数のポイントでバッジの電源を投入し、アクセス ポイントとの関連付けを確認します。バッジがアクセス ポイントに関連付けられない場合、次のチェックを行います。バッジの設定をチェックし、SSID や認証タイプなどが適切であることを確認します。WLC の設定をチェックし、SSID、認証タイプ、無線チャネルなどが適切であることを確認します。サイトの調査書をチェックし、その場所の RF カバレッジが適切であることを確認します。
- 環境全体における複数のポイントで、電話がアクセス ポイントを通じて正しく認証されることを確認します。クライアントの認証が行われない場合は、バッジで WEP キーか LEAP のユーザ名とパスワードを確認します。また、同じクレデンシャルでワイヤレス ラップトップを使用して、AAA サーバのユーザ名とパスワードを確認します。
- 環境全体における複数のポイントで、バッジが Vocera 通信サーバに登録されることを確認します。クライアント登録が行われない場合、次のチェックを行います。バッジの IP アドレス、サブネット マスク、プライマリ ゲートウェイ、プライマリ TFTP、プライマリおよびセカンダリ DNS が正しいことを確認します。
- 固定音声コール：環境全体における複数のポイントで、静止した状態で他のバッジに通話を行い、音声品質を確認するため 60 ～ 120 秒間の音声テストを行います。音声品質が許容範囲ではない場合は、一方のバッジをより適した位置に移動させて、再度、テストします。音声品質は受容できるものかどうかを確認し、受容できないレベルの場合は、無線のカバレッジを確認してください。テレフォニー サーバが設定されている場合は、環境全体における複数のポイントで、静止した状態で有線電話に通話を行い、音声品質を確認するため 60 ～ 120 秒間の音声テストを行います。音声品質が許容範囲ではない場合は、有線電話を使用して電話をかけていることを確認します。音声品質は受容できるものかどうかを確認し、許容範囲でない場合は、設計ガイドラインで有線ネットワークを確認します。
- サイト調査ツールを使用して、信号強度(受信信号強度インジケータ(RSSI))が35より大きいRFチャネルごとに1つのアクセスポイントが存在しないことを確認します。同じチャネルに2つのアクセスポイントがある場合は、干渉を最小限に抑えます。たとえば、強いアクセスポ

イントのRSSIが35の場合、弱いアクセスポイントのRSSIは20未満であることが理想的です。この目標を達成するには、アクセスポイントの送信電力を1つ減らすか、アクセスポイントを移動する必要があります。
- アクセス ポイントの QoS 設定をチェックし、推奨される正しい設定であることを確認します。
- バッジ コールのローミング：テレフォニー サーバが使用できない場合は、Begin Tutorial コマンドを使用して Vocera チュートリアルを開始します。またはテレフォニー サーバが使用できる場合は、固定デバイスからバッジに電話をかけます。無線のカバレッジ エリア全体を移動しながら、音声品質を継続的に確認します。音声品質が十分でない場合は、次の手順を実行してください。許容できない音質品質の変化をすべて聞き取り、その場所、ラップトップ上での無線の値、バッジからの CQ 値を記録します。バッジが次のアクセス ポイントへローミングするのを注意して聞き取ります。カバレッジと干渉を確認するため、サイトの調査書に他方の利用可能なアクセス ポイントを記録します。
- アクセス ポイントの設置方法と設定を調節して WLAN を微調整し、音声品質を確保するため次のチェックを行います。サイト調査ツールを使用し、任意の場所で RSSI の値が 35 を超えるアクセス ポイントが 1 チャネルに 1 つしか存在しないことを確認します。同じチャネルの他のすべてのアクセス ポイントは、RSSI の値をできるだけ低く（できれば 20 未満に）するのが理想的です。 カバレッジ エリアの境界で RSSI が 35 の場所では、同じチャネルの他のすべてのアクセス ポイントの RSSI を 20 未満にするのが理想的です。サイト調査ツールを使用して、すべての場所で目視でき、十分な信号強度を持つアクセス ポイントが 2 つ以上（合計、別のチャネルで）あることを確認します。ローミング エリア内のアクセス ポイントがすべてレイヤ 2 ネットワーク上にあることを確認します。

## 一般的なローミングの問題

ローミングでは次の問題が発生する可能性があります。

- バッジがアクセス ポイントの直下にある場合に、ローミングが行われない。
- バッジの received signal strength indicator（RSSI）と Channel Utilization（CU; チャネル使用率）が、ローミングの差分しきい値に達していないと思われる。 WLCから[Transmit Power Threshold]を調整します。
- バッジでアクセス ポイントからのビーコンやプローブ応答が受信されない。
- バッジのローミングが非常に遅い。

### ローミングの際にバッジとネットワークとの接続が失われる、あるいは音声サービスができなくなる

- 認証をチェックし、WEP の不一致がないかを確認します。
- ローミングの際に、バッジから IGMP 加入が送信されないか、ネットワークから IGMP クエリーが送信されます。したがって、レイヤ 2/レイヤ 3 のローミング中に Vocera ブロードキャスト機能が処理に失敗します。
- バッジには、（レイヤ 3 のモビリティ メカニズムが設定されていない限り）レイヤ 2 のシームレスなローミング機能しかありません。 新しい WLC が別の IP サブネットにサービスを提供していないことを確認してください。
- 関連付けられているアクセス ポイントとコントローラに、Vocera 通信サーバへの IP 接続があることを確認します。
- RF の信号強度とバッジの CQ 値を確認します。

## バッジがローミング時に音声クオリティを失う

- 宛先アクセス ポイントの RSSI が低くないか確認します。
- チャネルのオーバーラップが不十分な可能性があります。バッジには、元のアクセス ポイントの信号を失うまでに、通話をスムースに受け渡す時間が必要です。
- 元のアクセス ポイントからの信号が失われている可能性があります。

# 音声の問題

音声では、いくつか共通した設定エラーが原因で問題が起こる場合があり、それらは簡単に解決できます。可能であれば、音声の問題を固定（基準用）バッジに比較して確認すれば、ワイヤレスの問題を絞り込むのに役立ちます。一般的な音声の問題には次のものが含まれます。

- 単一方向の音声
- 音声が途切れたり不自然な音声になる
- 登録と認証の問題

## 単一方向の音声

- この問題は、バッジ側かアクセス ポイント側のどちらかの信号が極端に弱くなるアクセス ポイントの外縁エリアで発生する可能性があります。可能であれば、アクセス ポイントの出力設定をバッジと同じ（20 mW）にすると、問題が修正できることがあります。この問題は、アクセス ポイントの設定とバッジの設定の差が大きい場合（たとえば、アクセス ポイントが 100 mW でバッジが 28 mW など）に最も一般的に発生します。
- ゲートウェイと IP ルーティングの音声品質を確認します。
- 独自 UDP のパケットのパスにファイアウォールまたは NAT がないかどうかを確認します。デフォルトでは、ファイアウォールと NAT は、音声がまったくまたは片方向しか聞こえない原因となります。Cisco IOS®およびPIXのNATとファイアウォールには、双方向の音声が流れるように、これらの接続を変更する機能があります。レイヤ 3 のモビリティを使用する場合、Unicast Reverse Path Forwarding（uRPF）チェックによりネットワークでアップストリーム トラフィックがブロックされている可能性があります。
- WLC で ARP キャッシングが設定されていないと、音声は片方向しか聞こえません。

## 音声が途切れたり不自然な音声になる

- 近くで電子レンジが作動していると、一般的に音声が途切れたり不自然になる原因となります。電子レンジの影響はチャネル 9 で始まり、チャネル 6 から 14 まで拡張される可能性があります。
- Cognio などのツールを使用して、2.4 Ghz のワイヤレス電話や他のナース コールの無線デバイスをチェックします。

## 登録と認証の問題

認証の問題が発生したら、次のチェックを実行します。

- バッジとアクセス ポイント（またはネットワーク）の SSID が一致することを確認します。また、ネットワークに Vocera サーバへのルートがあることを確認します。

- WEP キーをチェックし、それらが一致することを確認します。WEP キーやパスワードの入力時にはタイプ エラーが起こりやすいため、Badge Configuration Utility（BCU）で再入力した上で、バッジを再プログラムすることを推奨いたします。

次のメッセージや現象が起こる可能性があります。

- 要求されたすべての機能をサポートできない：おそらく、アクセスポイントとクライアントの間で暗号化の不一致が発生しています。
- Authentication Failed / No AP Found：アクセスポイントとクライアントで認証タイプが一致していることを確認します。
- No Service - IP Config Failed:Static WEPを使用する場合は、キーが正しく設定されていることを確認します。同じ SSID を使用して、他のクライアントが DHCP を受信できることを確認します。
- APからすべてのTKIPクライアントの認証解除：この問題は、アクセスポイントが60秒以内に2つのMIC工ラーを検出したときに発生します。この対応策により、すべての TKIP クライアントで 60 秒間再認証が行われません。
- 再認証/セッションタイムアウト：設定すると、セッションタイムアウトによって再認証がトリガーされ、音声ストリームにギャップが生じます（802.1x認証では300ミリ秒+ WAN遅延）。

# 付録 A

## AP とアンテナの配置

このセクションでは、アクセス ポイントとアンテナの適切な設置例と不適切な設置例を紹介します。

図 17 は、信号パターンの歪みが派生する H 型梁（I-beam）に近い、不適切なアクセス ポイントおよびアンテナの設置方法を示しています。RF のヌル ポイントは信号波の交差によって生じ、マルチパスによる歪みは信号波が反射した際に生じます。この設置方法では、アクセス ポイントの背後のカバレッジはほとんどなく、アクセス ポイントの前側の信号品質も低下します。

**図17:I型梁の近くにアンテナを不適切に設置**

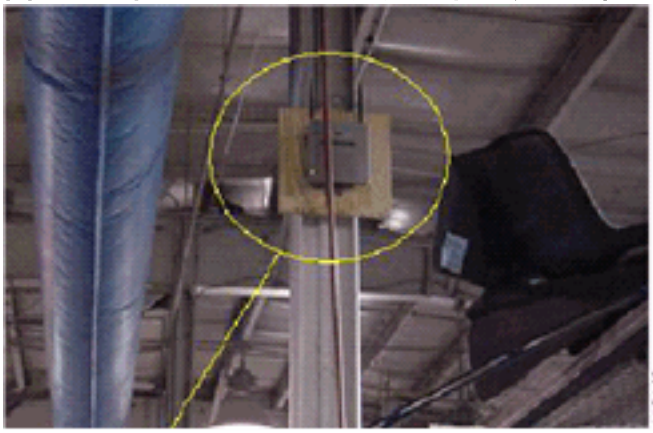


図 18 は H 型梁（I-beam）による信号伝播の変化や歪みを示しています。I 型梁により、送信と受信両方のパケットで多数の反射が生じます。反射した信号は、ヌル ポイントとマルチパスの干渉によって信号品質を著しく低下させます。しかし、アクセス ポイントのアンテナが H 型梁（I-beam）にきわめて近接しているため、信号強度は高くなります。

**図18：アンテナをI型梁に近くに配置することによる信号の歪み**

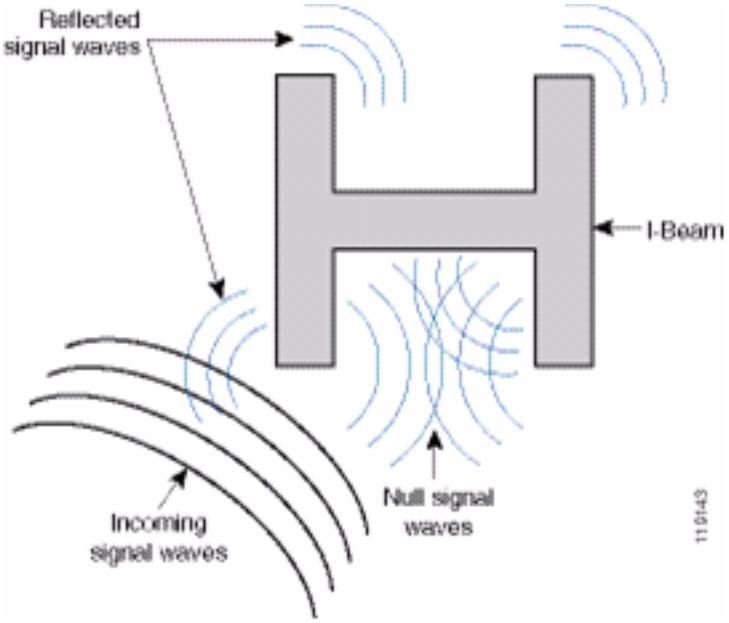



図 19 のアクセス ポイントとアンテナの設置方法は、H 型梁（I-beam）から離れており、信号の反射、ヌル ポイント、およびマルチパスによる干渉が少ないため、より適切と言えます。この設置方法も、イーサネットケーブルがアンテナに非常に近い場所で巻きついているため完全とはいえません。また、2.4GHz のアンテナを床の方向に向けることによって、アクセス ポイントの向きを変えることもできます。このようにすると、アクセス ポイントの直下のカバレッジがよくなります。アクセス ポイントより上にはユーザはいません。

**図19:I型梁から離れた壁面に設置されたアクセスポイントとアンテナ**

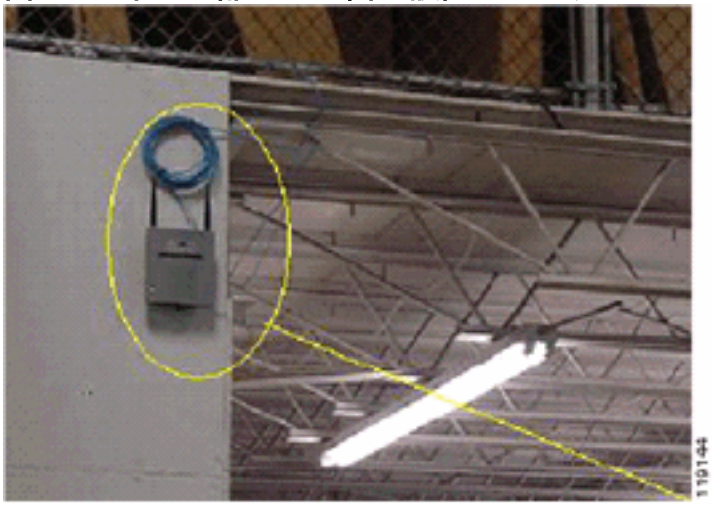
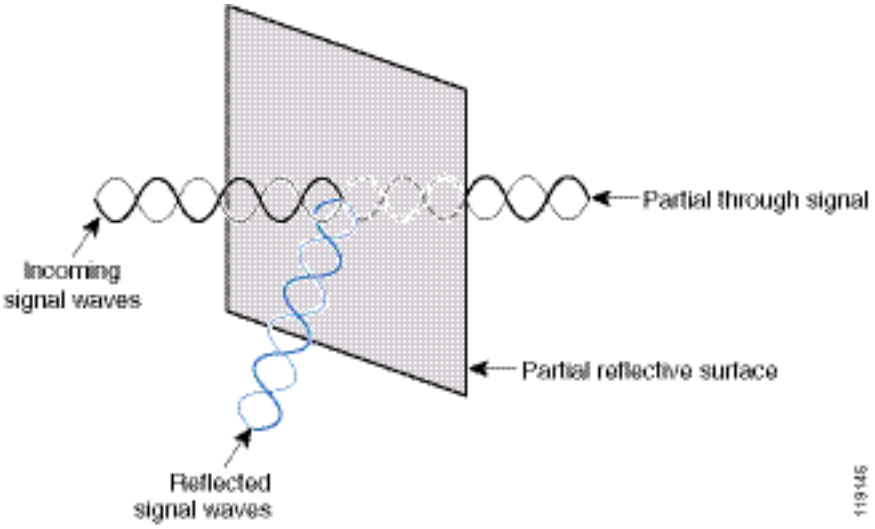



図 20 は、アクセス ポイントが設置されている壁による信号の伝播を示しています。

**図20：壁による信号反射**




先の例は、標準的な企業の環境で天井内部または天井近くにアクセス ポイントとアンテナを設置する場合にも適用できます。信号の反射やマルチパスによる干渉を引き起こす恐れのある、金属製の空調ダクトや エレベータ シャフトその他の物理的障害がある場合は、アンテナを移動させてそれらの障害から遠ざけることを強くお勧めします。エレベータの場合、信号の反射と歪みを取り除くには、アンテナを数フィート離します。天井内の空調ダクトについても、これが該当します。

パケットの送受信なしで調査を行うのは不十分です。I 型梁の例は、CRC エラーのあるパケットによってヌル ポイントが発生することを示しています。CRC エラーを含んだ音声パケットは消失したパケットであり、音声品質に悪影響を及ぼします。この例では、これらのパケットは調査ツールで測定したノイズ フロアを超えている可能性があります。したがって、サイト調査では信号レベルを測定するだけでなく、パケットを生成してパケット エラーをレポートすることが重要です。

図 21 は、Cisco AP1200 が天井の T バーに適切に取り付けられ、アンテナが全方向の位置に設置されているようすを示しています。

**図21：天井に取り付けられたCisco AP1200**

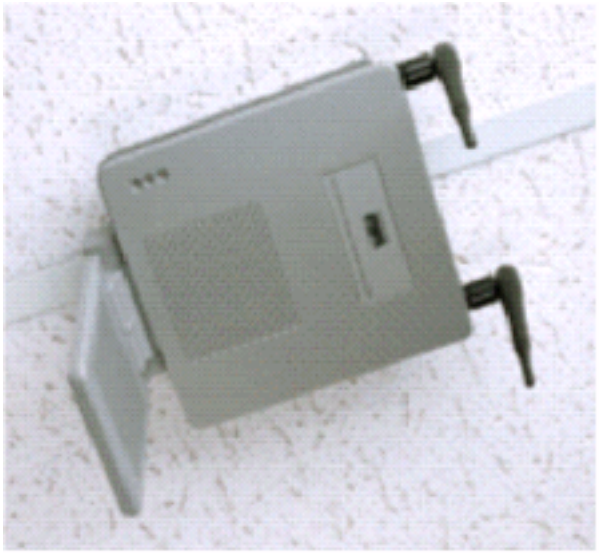



図 22 は、Cisco Aironet 5959 全方向性ダイバーシティ アンテナが、天井の T バーに適切に取り付けられているようすを示しています。この場合、Cisco AP1200 は天井のタイル表面に取り付けられています。

**図22：天井に取り付けられたCisco Aironet 5959アンテナ**

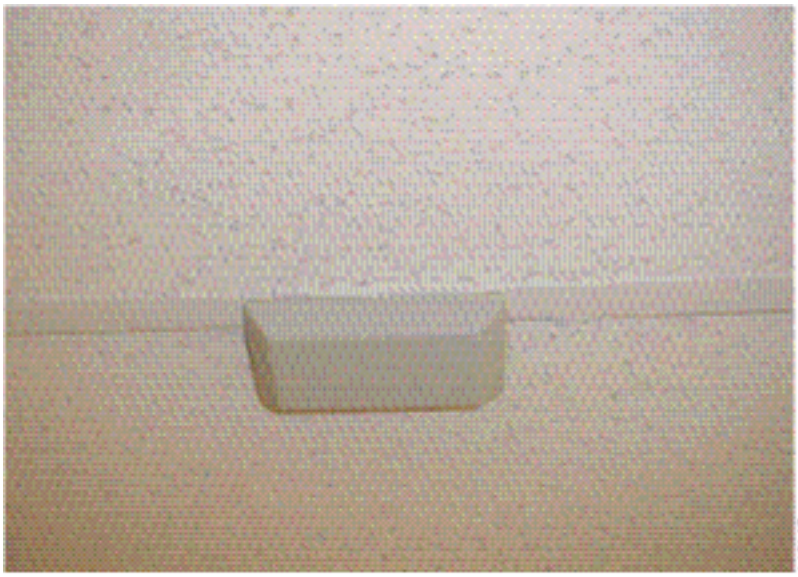


図 23 は、Cisco AP1200 が壁面に適切に取り付けられているようすを示しています。

**図23：壁に取り付けられたCisco AP1200**

図 24 は、Cisco Aironet 2012 ダイバーシティ パッチ アンテナが壁面に取り付けられているようすを示しています。この場合、Cisco AP1200 は天井のタイル表面に取り付けられています。

**図24：壁に取り付けられたCisco Aironet 2012アンテナ**

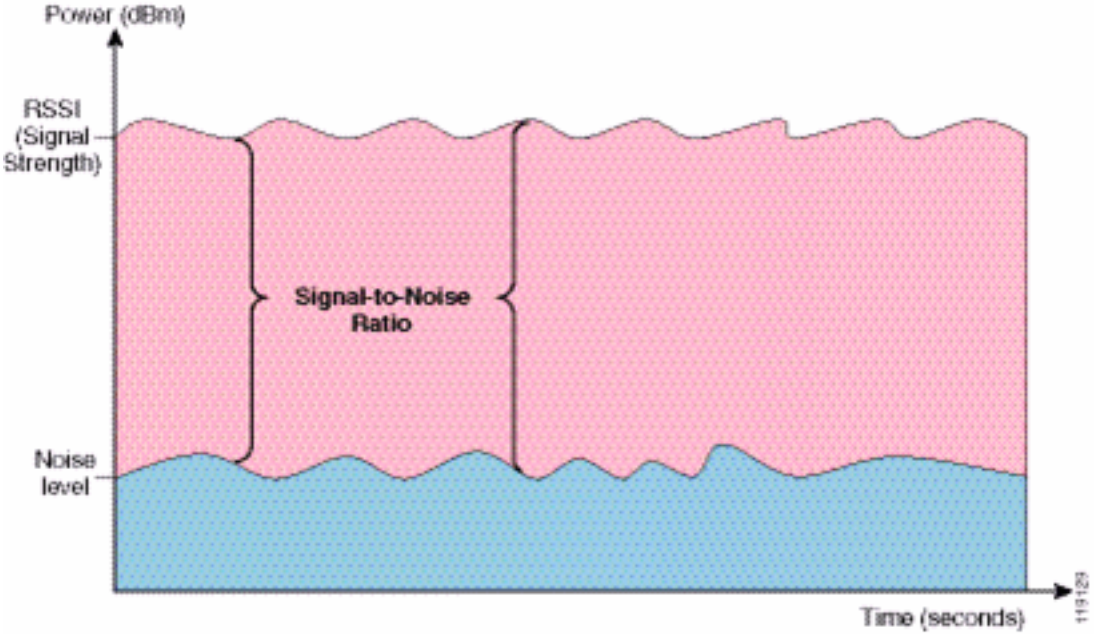
ユーザ トラフィックの高いエリア（オフィス、学校、小売店および病院など）では、アクセス ポイントを目に付かないところに配置し、パッチアンテナなどの外部アンテナをダイバーシティ構成で天井の下などに取り付けることを推奨いたします。この際、左右の外部アンテナは 45 cm 以内に配置する必要があります。

## 干渉とマルチパスによる歪み

WLAN ネットワークにおけるスループットのパフォーマンスは、使用不可能な信号の影響を受けます。WLAN 干渉は、電子レンジ、2.4 GHz のコードレス電話、Bluetooth デバイス、または 2.4 GHz 帯域で動作する他の電子機器によって生じる可能性があります。干渉はまた、WLAN に属しているが離れているために信号が弱くなったり途絶えたりしている他のアクセス ポイントやクライアント デバイスからも、発生することが一般的にあります。ネットワーク インフラストラクチャの一部ではないアクセス ポイントが WLAN 干渉を引き起こし、不正なアクセス ポイントとして識別される場合もあります。

干渉とマルチパスによる歪みは、伝送される信号を変動させます。干渉により、特定のデータ レートの signal-to-noise ratio（SNR; 信号対雑音比）が低下します。干渉やマルチパスによる歪みが多い場所では、パケットの再試行数が増加します。干渉は、ノイズ レベルあるいはノイズ フロアとも呼ばれます。関連付けられているアクセス ポイントからの受信信号の強度は、信号が正しくデコードされるためにレシーバのノイズ レベルよりも高くする必要があります。この強度のレベルを信号対雑音比、または SNR と呼びます。Vocera バッジの理想的な SNR は 25 dB です。たとえば、ノイズ フロアが 95 decibels per milliwatt（dBm; デシベル / ミリワット）でバッジの受信信号が 70 dBm ならば、SNR は 25 dB です（図 25 参照）。

**図25：信号対雑音比(SNR)**




アンテナのタイプと場所を変更することで、マルチパスによる歪みと干渉を低減できます。干渉しているトランスミッタが指向性アンテナの正面に直接入っていなければ、アンテナ ゲインがシステム ゲインに加わり、干渉が緩和されます。

指向性アンテナは、特定の室内用アプリケーションでは非常に有用ですが、室内への設置の大多数では全方向性アンテナが使用されます。方向性は、正しく適切なサイト調査で厳密に決定される必要があります。全方向性アンテナを使用してもパッチ アンテナを使用しても、室内環境ではマルチパスによる歪みを緩和させるためにダイバーシティ アンテナ構成が必要です。Cisco Aironet シリーズのアクセス ポイント無線は、ダイバーシティのサポートを想定しています。

## 信号の減衰

信号の減衰や信号損失は、信号が空中を通過する際にも起こります。信号強度の損失は、信号が空気以外の物体を通過する際により顕著になります。20 mW の伝送パワーは 13 dBm に相当します。したがって、プラスターボード壁へのエントリ ポイントの伝送パワーが 13 dBm とすると、壁を抜ける時点の信号強度は 10 dBm に減少します。次の表は、さまざまなタイプの物体による信号強度の損失を示しています。

**さまざまなタイプの物体による信号の減衰**

| 信号パスにある物体 | 物体による信号の減衰 |
|---|---|
| プラスターボード壁 | 3 dB |
| 金属サッシの付いたガラス壁 | 6 dB |
| シンダー ブロック壁 | 4 dB |
| オフィスの窓 | 3 dB |
| 金属製のドア | 6 dB |
| レンガ壁にある金属製のドア | 12 dB |
| 人体 | 3 dB |

調査する場所によって、マルチパスによる歪み、信号損失、および信号ノイズのレベルは異なります。病院は、マルチパスによる歪み、信号損失、および信号ノイズが高いため、一般に最も調査の難しい環境です。病院の場合、調査に時間がかかり、アクセス ポイントをより密集して配置する必要があり、高いパフォーマンス基準が要求されます。次に調査が難しいのは、工場と店舗です。このようなサイトには、一般的に金属製外壁材が使用されており、フロアに金属製のものが多く、それらが信号を反射して、マルチパスによる歪みが再生成されます。オフィスビルとホスピタリティ施設では、一般に信号の減衰は高いものの、マルチパスによる歪みはあまりありません。

# 関連情報

- Cisco 440X シリーズ ワイヤレス LAN コントローラの配備
- Solution Reference Network Design
- Vocera Communications System Specifications
- テクニカル サポートとドキュメント – Cisco Systems