MSE:Context Awareモビリティソリューション導入ガイド

内容

はじめに
前提条件
　要件
　使用するコンポーネント
　表記法
背景説明
セクション1：ソリューションの概要
　用語
　技術的な背景
　RSSI（受信信号強度表示）
　TDoA（到達時間差）
　アクティブ RFID タグ
セクション2:Context Awareネットワークの計画とセットアップ
　アクセス ポイントの配置
　Tracking Optimized Monitor Mode（TOMM）
　AP とアンテナの配置
　信号の減衰
　複数階のビル、病院、および倉庫のサーベイランス
　ロケーション レールとリージョン
　システム マネージャでのマスクの作成
　タグ用 Context Aware Engine 内のセル
　セル設定のための初期運用
　調整：クライアント用 Context Aware Engine
　励振器（チョークポイント トリガー）テクノロジー
　既存のデータおよび音声サービスがあるときの Context Aware 展開の考慮事項
　一般的なガイドライン：TDoA
　有線ロケーション
セクション3:Context Awareネットワークの検証と改善
　WCS 確度ツール
　Location Readiness ツール
　Context-Aware：システムのパフォーマンス
　RFID タグおよび WLC の設定および調整
　WCS および MSE の設定および調整（「トラブルシューティング」）
セクション4：最終チェックリスト
　ハードウェア要件
セクション5：よくある技術的な質問
付録A:MSEの設定
　MSE の WCS への追加
付録B:WLCおよびMSEコマンド
付録C:5.Xから6.0へのMSEアップグレード
付録D:MSEデータベースの復元
関連情報

はじめに

このドキュメントの目的は、設定と展開のガイドラインを示し、トラブルシューティングのヒントを提供すること、およびシスコ モビリティ サービス エンジン（MSE）を Cisco Unified WLAN に追加して Context Aware Services を実行する場合によくある技術的な質問に答えることです。このドキュメントでは、次のことを目的としています。

- Cisco モビリティ ソリューションのさまざまな要素およびフレームワークの説明
- Cisco モビリティ ソリューションを展開するための全般的な展開ガイドラインの提供

このドキュメントでは、MSE および関連コンポーネントの詳細設定は扱いません。これらの情報は、他のドキュメントに含まれており、関連資料に示してあります。Context Aware モビリティ サービスの設定および設計に関するドキュメントのリストについては、「関連情報」セクションを参照してください。適応型 wIPS の設定もこのドキュメントでは扱いません。

前提条件

要件

このドキュメントに関する固有の要件はありません。

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

表記法の詳細については、『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。

背景説明

Cisco MSE では、ワイヤレス LAN コントローラ（WLC）および Cisco Aironet Lightweight アクセス ポイント（LAP）を使用して、有線とワイヤレスの両方について、ネットワーク デバイスの物理ロケーションを追跡できます。お客様は、このソリューションによって、クライアント、アクティブ RFID タグ、不正なクライアント、アクセス ポイント（AP）などの任意の Wi-Fi デバイスを追跡できます。MSE は、以下の要件を踏まえて設計されました。

- 管理性：Cisco Wireless Control System（WCS）は、MSE の管理および監視に使用されます。さらに、MSE は、ワイヤレス LAN アーキテクチャと直接統合されます。この結果、複数の個別のワイヤレス ネットワークではなく、1 つの統合されたネットワークを管理することができます。
- スケーラビリティ：Cisco MSE シリーズでは、18,000 個までのネットワーク要素を同時に追跡できます。WCS では、拡張性を高めるために複数のモビリティ サービス エンジンを管理できます。コントローラである WCS と MSE は、拡張性と性能を向上させるために、別々のデバイスを介して実装されます。

- セキュリティ：MSE、WCS、およびワイヤレス LAN コントローラには、堅牢でセキュアなインターフェイスとデータにアクセスするためのセキュアなプロトコルが用意されています。MSE では、ロケーション情報の履歴を記録しており、この記録は監査証跡および法規制の遵守に使用されます。
- オープンで標準に準拠：MSE には、外部のシステムおよびアプリケーションからアクセスできる SOAP/XML API があり、MSE からのロケーション情報を利用できます。
- ビジネス アプリケーションを容易に展開可能：MSE は、資産の追跡、インベントリ管理、ロケーションに基づくセキュリティ、自動化されたワークフロー管理などの新しいビジネス アプリケーションと統合できます。

この文書は次の 5 つのセクションに分けられています。

1. ソリューションの概要
2. Context Aware 用 Wi-Fi ネットワークの計画とセットアップ
3. Context Aware ネットワークの検証と改良
4. （「トラブルシューティング」）
5. 最終チェック項目

セクション1：ソリューションの概要

Context Aware Service（CAS）では Wi-Fi 802.11a/b/g/n ネットワークの機能が提供され、ワイヤレス クライアント、アクティブ RFID タグなどのアクティブ Wi-Fi デバイスを備えた人または物のロケーションを判別したり、ワイヤレス インフラストラクチャを介してエンド ポイントからアップストリーム クライアントに渡される関連データを特定したりします。適切なライセンスを持つバージョンの WCS を使用して、シスコ モビリティ サービス エンジン（MSE）を Cisco Unified Wireless Network（CUWN）に追加した場合、MSE では、複数の重要な作業を受け持つことを想定しています。

- 位置決めアルゴリズムの実行
- 調整情報のメンテナンス
- ロケーション通知のトリガーとディスパッチ
- ロケーションの統計情報および履歴の処理
- 地理的な情報、マップ、およびすべてのワイヤレス デバイスの保管

WCS は MSE とのインターフェイスとなる管理システムで、MSE で提供されるサービスのユーザ インターフェイス（UI）として機能します。メンテナンスおよび診断を目的として、SSH またはコンソール セッションを介して MSE に直接アクセスすることはできますが、オペレータおよびユーザによる MSE とのすべての対話は、通常は、WCS（管理用）またはサードパーティのロケーション クライアント アプリケーションから実行します。

用語

シスコの中央集中型ワイヤレス LAN アーキテクチャおよび Context Aware ロケーション サービスを使用すると、管理者は、802.11 に基づく任意のデバイスのロケーションや、各デバイスの具体的なタイプまたはステータスを判別できます。クライアント（関連付け、調査などが目的）、不正なアクセス ポイント、不正なクライアント、およびアクティブ タグは、いずれもシステムによって識別され、ロケーションを判別できます。この情報は、イベントの発生から数秒のうちに API で利用できるようになり、履歴の検索やセキュリティ監査のために MSE データベースで保持できます。

モビリティサービスエンジン(MSE):MSEは、一連のモビリティサービスプログラムをサポートしています。MSE は、オープンなプラットフォームとして設計されており、ネットワーク トポロジと必要なサービスのタイプに基づくさまざまな設定オプションを持つモジュラ形式によって、モビリティ サービス ソフトウェアをサポートします。MSE の値は、さまざまなモビリティ サービス アプリケーションを介して配信されます。シスコでは、次のような既存および将来的なソフトウェアをサポートします。

- Context-Aware Services：これらのプログラムは、ロケーション、温度、可用性、使用アプリケーションなどに関する詳細なコンテキスト情報を取得し、ビジネスプロセスに統合します。Context Aware アプリケーションは、リアルタイム ロケーション、プレゼンス検出、チョークポイントの可視性、テレメトリなどの幅広いロケーション オプションを備えています。拡張受信信号強度表示（RSSI）と到達時間差（TDoA）テクノロジーのサポートにより、さまざまな環境で高い尺度の確度と性能を提供します。Context Aware ソフトウェアは、2 つの主要コンポーネントで構成されています。
    - クライアント用Context Aware Engine:Cisco Location Engine(RSSI)は、Wi-Fiクライアント、不正なクライアント、不正なAP、および有線クライアントを追跡するために使用されます。
    - タグ用Context Aware Engine：パートナー(AeroScout)ロケーションエンジン（RSSIとTDOAの両方）は、Wi-FiアクティブRFIDタグを追跡するために使用されます。

      サードパーティ アプリケーションは、MSE API を介してサポートされます。
- Adaptive Wireless Intrusion Prevention System(wIPS):wIPSソフトウェアは、無線および有線ネットワークの脆弱性の監視、アラート、分類、および修復を通じて、モビリティネットワークの可視性と包括的な脅威防御を提供します。

Network Mobility Services Protocol:WLCとMSE間のセキュアな通信に使用されるシスコ定義のプロトコル。

Wireless Control System(WCS)：シスコが開発およびサポートするワイヤレスネットワーク管理システム。以下の機能を備えています。

- WLAN の設定
- WLAN パフォーマンス モニタリング

- レポート作成（リアルタイムおよび履歴）
- ネットワークのグラフィカル表示（ワイヤレス LAN コントローラ、アクセス ポイント、クライアントおよびタグ）

ワイヤレスLANコントローラ(WLC):CUWNアーキテクチャは、WLANの設定と制御をWLANコントローラ(WLC)と呼ばれるデバイスに一元化します。これにより、自律した個別のアクセス ポイントで構成されている従来の 802.11 WLAN インフラストラクチャとは異なり、拡張サービスをサポートするためのアクセス メディアとしてワイヤレスを使用するインテリジェント ネットワークとして、WLAN 全体を運用できます。CUWN では、大量の管理対象エンドポイント（自律アクセス ポイント）を、1 つ以上の WLAN コントローラとこれに対応する結合されたアクセス ポイントで構成された単一の管理対象システムとしてまとめることで、運営管理が簡素化されます。

CUWN アーキテクチャでは、AP は「Lightweight（軽量）」です。つまり、WLC から独立して動作できません。AP は通常は「ゼロ タッチ」で展開され、AP の個別の設定は必要ありません。AP では、コントローラ ディスカバリ アルゴリズムによって、1 つ以上の WLC の IP アドレスを学習し、次に「加入」プロセスを通じてコントローラとの信頼関係を確立します。信頼関係が確立されると WLC は AP にファームウェア（必要な場合）および実行時コンフィギュレーションをプッシュします。AP では、設定をローカルに保存しません。

クライアント：ワイヤレスネットワーク上のコントローラベースのLightweightアクセスポイントに関連付けられたすべてのデバイス。

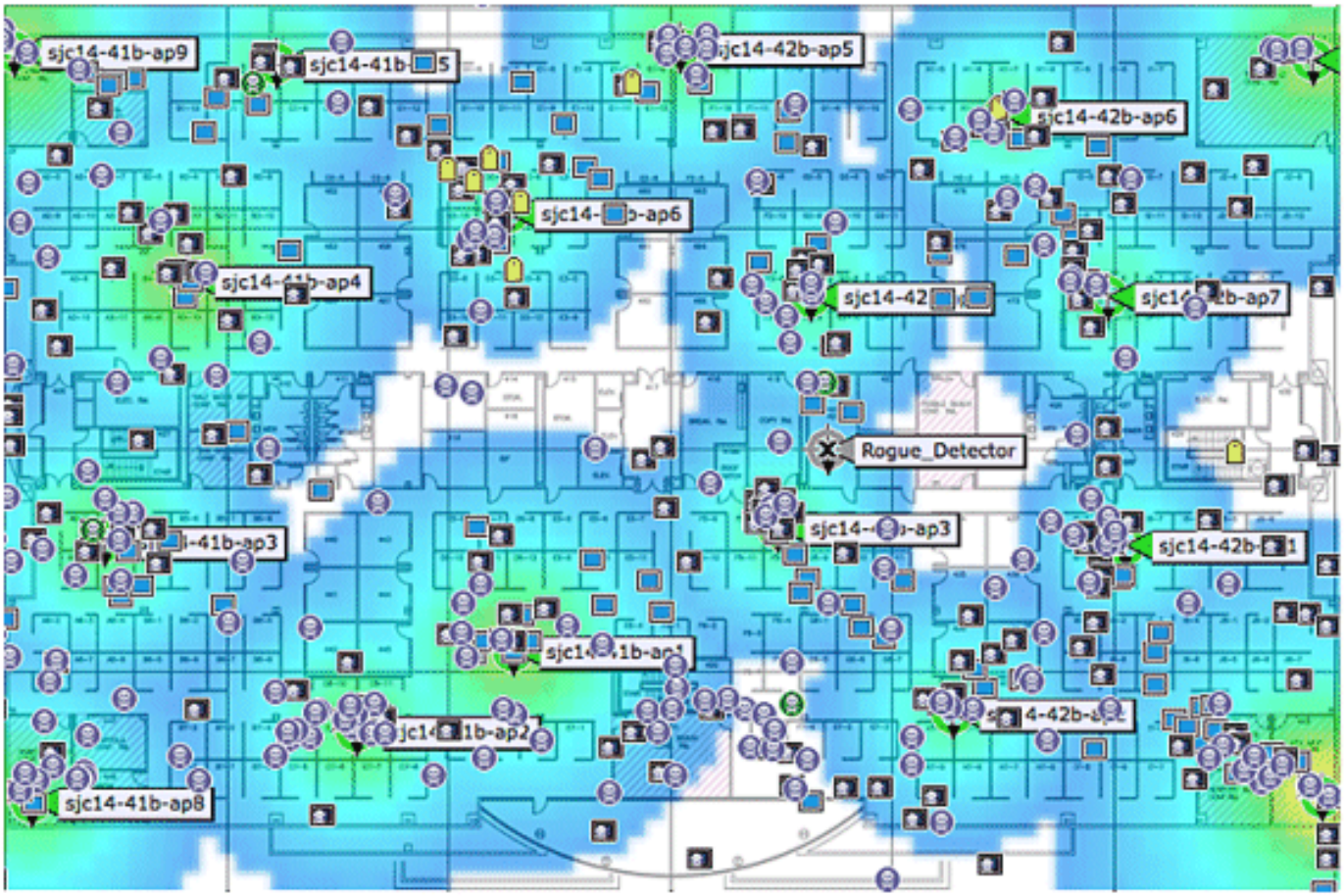
不正アクセスポイント：検出したワイヤレスLANモビリティグループに属さないと判断されたアクセスポイント。これは、Lightweight アクセス ポイントの RF 範囲内にある、このシステム以外のすべてのアクセス ポイントで構成されます。これには、有線ネットワーク上のアクセス ポイントや、別の有線ネットワーク上のアクセス ポイント（ネイバーのアクセス ポイントなど）を含みます。すべての Lightweight アクセス ポイントは、特殊なキーによってビーコン フレームの一部をハッシュするため、スプーフィングされたインフラストラクチャ アクセス ポイントの場合であっても、不正アクセス ポイントとして識別されます。スプーフィングされたアクセス ポイントとして WCS でフラグが付けられた、正規のアクセスポイントと誤解されることはありません。

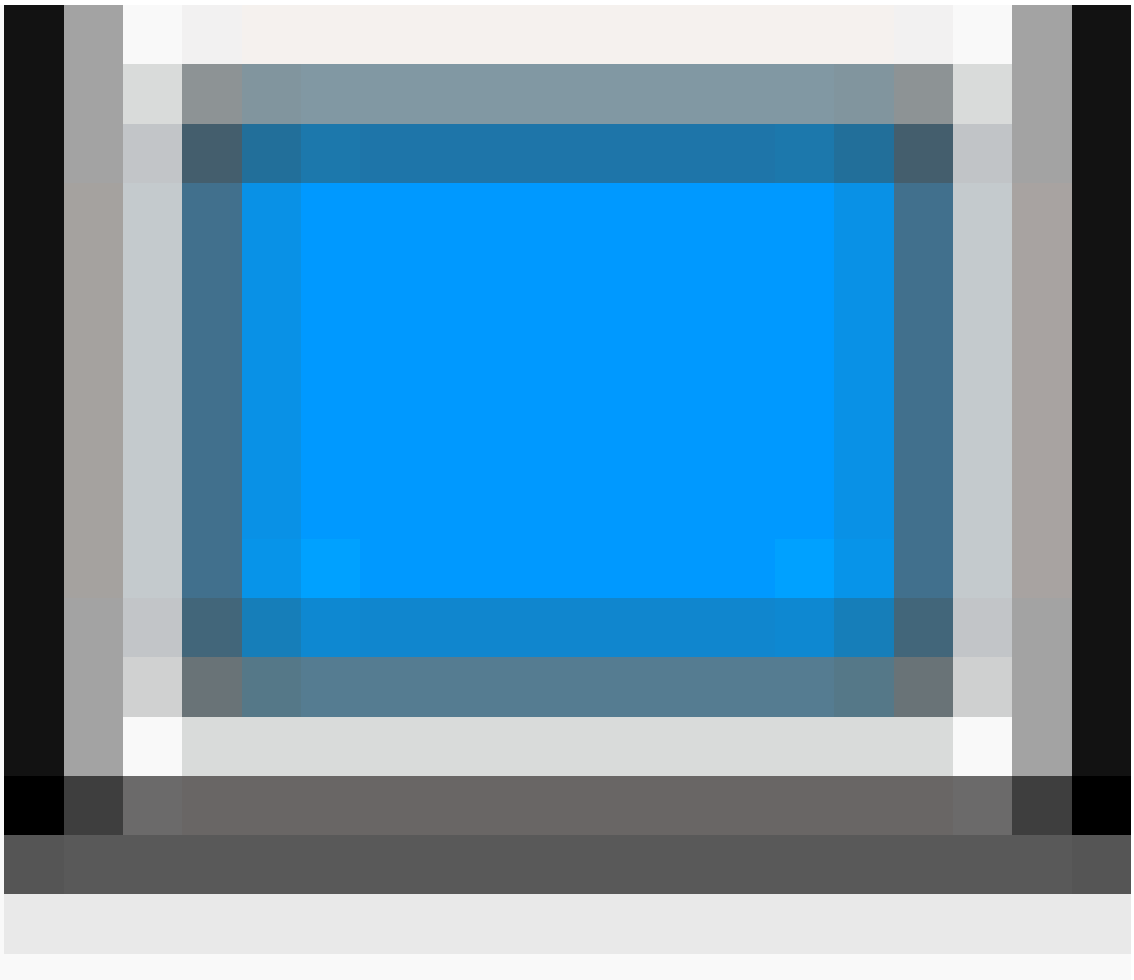
Rogue Clients：不正なアクセスポイントに関連付けられたすべてのデバイス。

アクティブRFIDタグ:Wi-Fiネットワーク上で検出および検出できるWi-Fiデバイス。Wi-Fi 互換のさまざまなタグが市販されています。タグは、温度と湿度などの動作と環境に関するデータのテレメトリ、コール ボタン、屋内運用と屋外運用、本質的に安全なバージョン、柔軟性のある取り付けオプションなど、さまざまな機能を提供します。

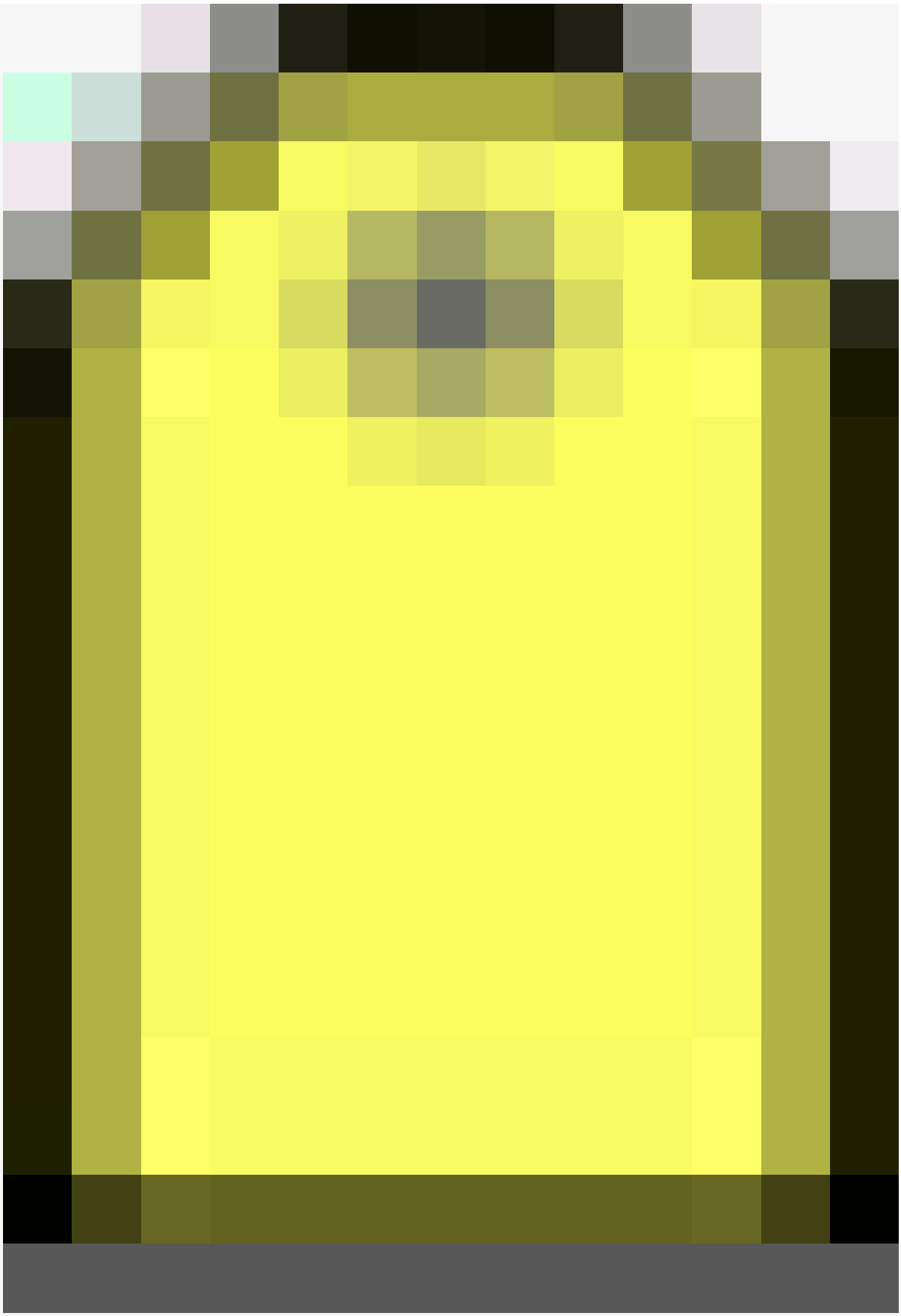
MSE では、最大 18,000 台のデバイス（タグ、クライアント、不正なクライアントおよび AP）を追跡できます。図 1 は、WCS に表示されるフロア マップの例で、タグ、クライアント、不正なクライアント、および不正な AP が表示されています。このフロア マップは、MSE で追跡できるデバイス クラスの規模と多様さを示しています。WCS では、検索パラメータを定義して、デバイスのサブセットのみを表示できます。たとえば、医療業務に携わるユーザに対しては、不正なデバイスや、暗号のような MAC アドレスまたは IP アドレスを持つデバイスではなく、わかりやすい識別子の付いた輸液ポンプや心電図装置のみを表示することができます。

図1：追跡対象デバイスを含むWCSフロアマップ


sjc14-41b-ap9
sjc14-42b-ap5
sjc14-42b-ap6
sjc14-42b-ap7
Rogue_Detector
sjc14-41b-ap8

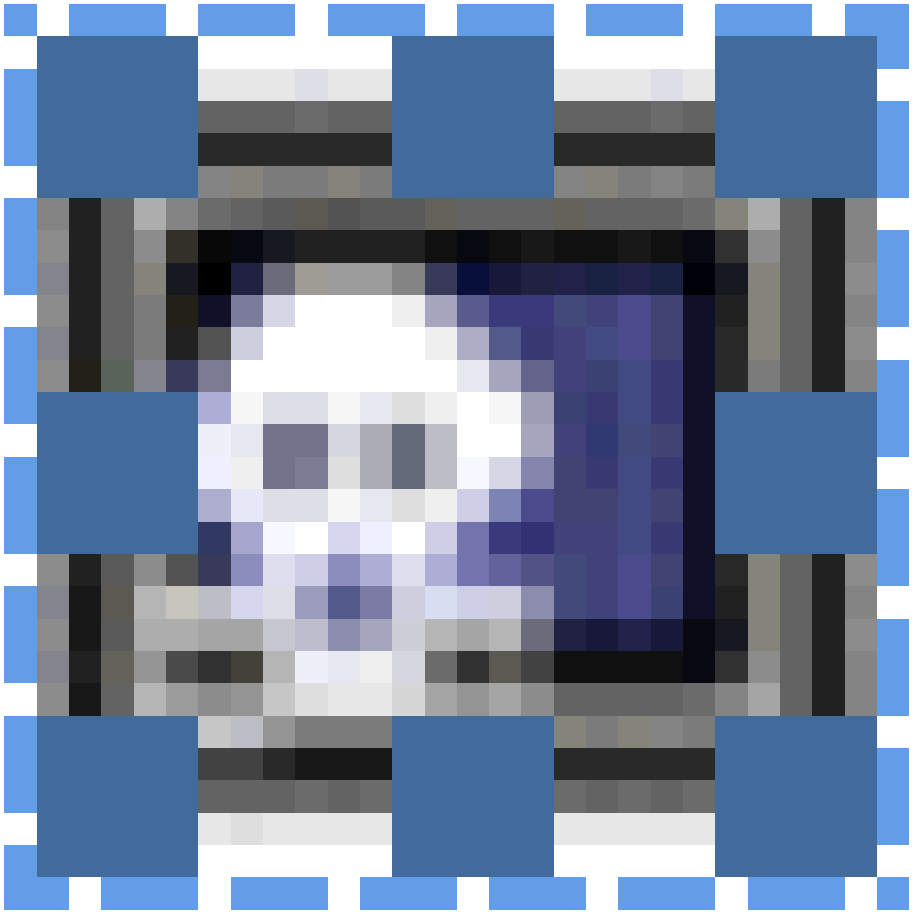


クライアント:



タグ：

不正な AP（赤 = 悪意あり、緑 = 友好、灰色 = 未分類）



不正クライアント：

技術的な背景

Cisco モビリティ ソリューションで Wi-Fi デバイスを追跡するために使用されるテクノロジーは 2 種類あります。

- RSSI（受信信号強度表示）
- TDoA（到達時間差）

これらのテクノロジーの詳細は、『Wi-Fi ロケーションベース サービス 4.1 デザイン ガイド』に記載されています。

RSSI（受信信号強度表示）

RSSI は、受信する無線信号の電力によって測定されます。任意のワイヤレス デバイスによって送信されるパケットは、複数の AP（フレームを送信したチャネルをリッスンしている AP であることが前提）で受信されます。AP では、AP で測定した対応する RSSI 情報と一緒に、このパケットをワイヤレス LAN コントローラに転送します。ワイヤレス LAN コントローラでは、さまざまな AP から得たこの情報をデバイスごとに集約します。このデータは、NMSP を介して MSE に転送されます。MSE 上の Context Aware Services では、1 つ以上の WLC から受信した RSSI データを使用して、ワイヤレス デバイスのロケーションを判別します。

通常 RSSI は、信号が反射する、屋内や、天井の低い環境で推奨されます。TDoA と異なり、RSSI では AP 間で時間が厳密に同期する必要はありません。さまざまな AP から取得する測定された RSSI 値を使用して、フロア上のさまざまなポイントでデバイスのロケーションの確率が計算されます。この確率に基づいて、ロケーションが推定ロケーションとして返されます。

TDoA（到達時間差）

屋外や、天井の高い屋内環境などの屋外に似た環境でタグを追跡する場合は、デバイス ロケーションを判別する方式として到達時間差（TDoA）メカニズムをお勧めします。TDoA では、時刻の同期された 3 台以上の Wi-Fi TDoA 受信機から送信された信号を伝送するときの到達時間（TOA）の差異に基づいて、WLAN デバイスのロケーションが判別されます。到達時間データが収集されて MSE 上のタグ用 Context Aware Engine に報告され、そこで、複数組の Wi-Fi TDoA 受信機間の到達時間差が計算されます。異なる Wi-Fi TDoA 受信機が特定のメッセージを受信するために必要な時間は、伝送モバイル デバイスと各 TDoA 受信機の間の伝送パスの長さに比例します。このデバイス ロケーション計算メカニズムでは、Wi-Fi TDoA 受信機間の時刻の同期が必要です。

この方式で位置を正確に計算するためには、3 台以上の Wi-Fi TDoA 受信機のセットが必要です。Wi-Fi TDoA 受信機間の距離は、屋内の RSSI による位置決めで必要なアクセス ポイント間の距離に比べて大きくなります。RSSI 位置決め同様、この方式は単方向通信（タグが通知フレームを伝送し、関連付けは不要）に基づいています。

『Context-Aware Service Software コンフィギュレーション ガイド』を参照してください。

アクティブ RFID タグ

CCX 準拠のアクティブ RFID タグは、タグから送信されて 802.11 AP で受信されるタグ通知フレームに基づいて、Wi-Fi ネットワーク上で検出されます。タグ通知フレーム レートは、具体的な使用例シナリオに基づいてプログラムできます。通常、タグは、ロケーション アップデートの頻度とバッテリ寿命を最適化するために、3 ~ 5 分おきにタグ通知フレームを送信するように設定されます。

コール ボタン機能では、タグ上のプッシュ ボタンに基づいてイベントをトリガーできます。これにより、緊急レポート、部品の補充など拡張機能が実現されます。一部のタグには、複数のコー

ル ボタンが装備されています。2 つ目のコール ボタンは、付加機能用にプログラムできます。

タグには、事前にプログラムされており、ワイヤレス ネットワーク インフラストラクチャで受信できるメッセージを保存できます。アクティブ タグの電源として、最長 4 年のバッテリ寿命を持つバッテリが使用されます。バッテリ寿命は、タグ通知フレームの伝送頻度と反復レートなどのタグ設定パラメータの数によって異なります。タグでは、タグのバッテリ レベルを報告でき、電力が低下したときはアラートできます。タグには、移動されたときにタグ通知フレームを送信するための内蔵動作センサーも組み込み可能です。これにより、タグが固定されている場合のバッテリ寿命を節約できます。移動しない場合の送信頻度を減らすようにタグを設定します。

他の口ケーションおよびステータスの情報に加えて、周囲温度など、資産の状態を正確に監視する拡張センサー テクノロジーを付加する、別のタグ カテゴリがあります。これらのセンサー タグでは、標準 Wi-Fi ネットワークを使用して、資産の口ケーションおよびセンサー データを転送します。専用のセンサー ネットワークを設ける必要はありません。

Wi-Fi タグ用の Cisco Compatible Extensions（CCX）仕様に準拠する Wi-Fi RFID タグでは、タグ メッセージ ペイロードの一部として、オプションで、タグ テレメトリ情報を口ケーション認識型の Cisco UWN に渡すことができます。テレメトリ情報は、アクセス ポイントが受け取り、WLC が収集します。MSE では、起動時に、タグの測定など、MSE で対象とするすべてのサービスに申し込みます。WLC では、各集約サイクルの終わりに、MSE 通知の送信を続行します。

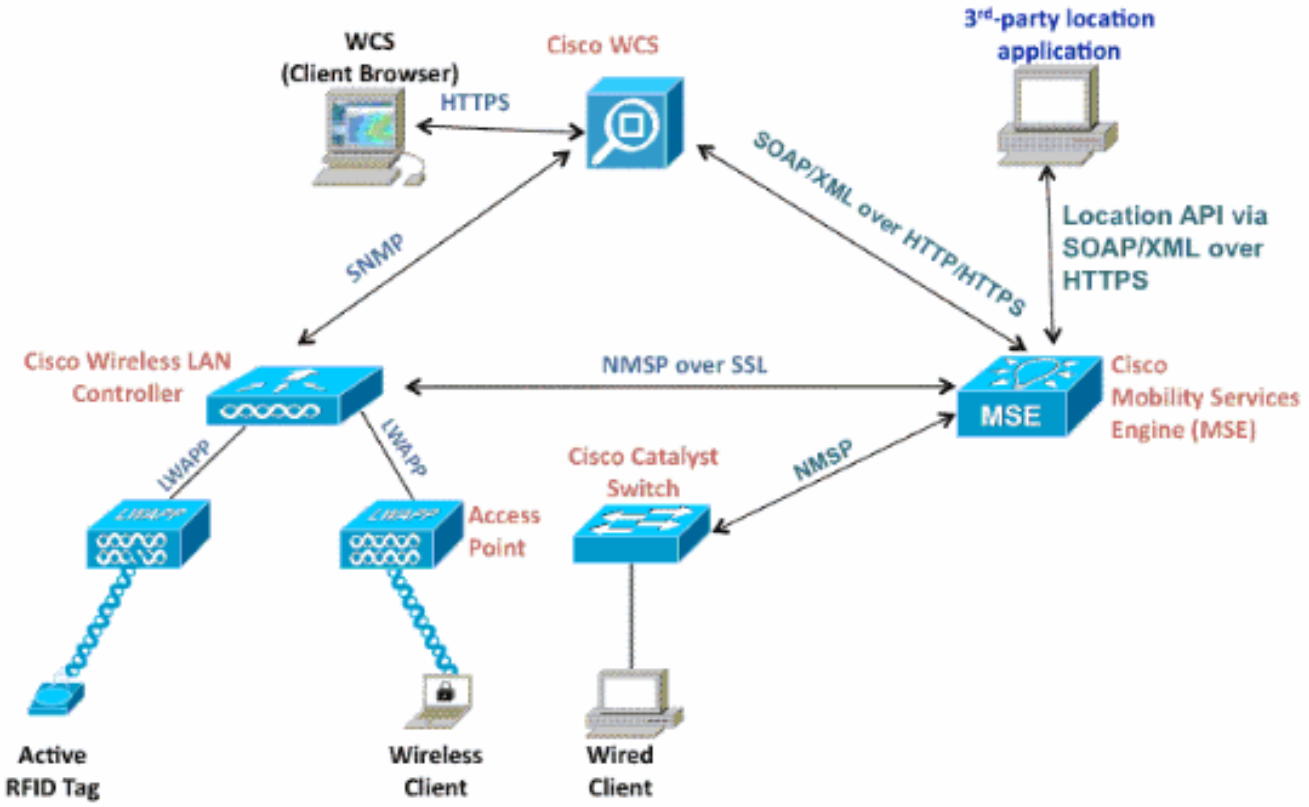
テレメトリ情報は、CCX 互換のタグから送信されて 1 台以上の AP または口ケーション受信機（Wi-Fi TDoA 受信機）、あるいはその両方で受信されます。さらに、このテレメトリ情報は、それぞれが登録されている WLAN コントローラに渡されます。タグが、チャネルごとに複数のフレーム コピー（またはバースト）を送信するよう設定されている場合、コントローラは重複するすべてのタグ テレメトリを削除し、重複を除外したテレメトリ値を MSE に渡します。MSE 内のデータベースに新しいテレメトリ情報が更新され、SOAP/XML API を介して口ケーション クライアントに提供されます。

テレメトリ値を渡すタグの場合、NMSP は、複数のタグからのテレメトリ値を同様な方式で効率的に転送するように設計されています。複数のタグからのテレメトリ トラフィックは、NMSP フレーム フラグメンテーションを実行できる各 NMSP エンドポイントを使用して WLC によって集約され、必要に応じて再構成されます。すべてのタグ データをノースバウンド通知に含めることができます。これには、テレメトリ、コール ボタン、チョークポイントの検出などが含まれます。

システム アーキテクチャ

MSE は、図 2 に示すように、シスコの中央集中型ワイヤレス LAN アーキテクチャと統合されます。MSE は、ワイヤレス LAN のデータ パスを外れた場所にあり（図を参照）、NMSP を介して WLC からデータを受信します。WCS は、MSE の設定に使用されます。いったん設定すれば MSE は、自己完結しています。

図2：システムアーキテクチャ



Context Aware ソリューションを展開するときは、追跡対象のデバイスのタイプおよび最大デバイス数を考慮する必要があります。個別または同時に追跡するように設定された、5 種類の任意のデバイス タイプ（Wi-Fi クライアント、アクティブ RFID タグ、不正なクライアント、不正な AP、または有線クライアント）を追跡できます。

1 つの MSE は、1 つの WCS のみで管理できます。つまり、単一の MSE は、複数の WCS インスタンスによって管理できません。一方、単一の WCS では、複数の MSE を管理できます。管理するデバイスの数が 1 台の MSE のキャパシティを超える場合は、独立した複数の MSE を展開する必要があります。拡張用に複数の MSE を展開する機能は、MSE 上で現在サポートされているすべてのサービスに適用されます。Context Aware Service の一環として 1 台の Cisco MSE 3350 で追跡できるデバイスの最大数は、クライアント、アクティブ RFID タグ、不正なクライアント、不正な AP、および有線クライアントを合わせて 18,000 台です。Cisco MSE 3310 では、最大 2,000 台のデバイスを追跡できます。管理するデバイスの数が 1 台の MSE ボックスのキャパシティを超える場合は、複数の独立した MSE アプライアンスを配置する必要があります。このためには、場合によっては、特定のコントローラ上に MSE を配置する必要があります。クライアントまたは資産のローミングが物理的に異なるビルやドメインを交差する広大なキャンパスであればなおさらです。この例では、コントローラは、最大 10 台の MSE アプライアンスと通信できます。

Cisco LAP は、クライアントにサービスを提供するチャネル上のデバイスと、ワイヤレス クライアントにデータ アクセスを提供したままで定期的にバックグラウンド スキャンを実行する場合に、他のすべてのチャネル上のデバイスの両方を検出する、固有のデュアル モードで動作します。収集された未加工ロケーション データは、次に、LWAPP または標準ベースの CAPWAP プロトコルを介して、各アクセス ポイントからこれに関連付けられた WLC に転送されます。データは、セキュアな NMSP 接続を通じて、ワイヤレス LAN コントローラと MSE の間を転送されます。

Cisco WCS は、MSE の管理および設定に使用され、追跡対象の Wi-Fi デバイスを表示する、MSE のビジュアルなフロントエンドにもなります。すべてのデバイス（有線およびワイヤレス）の詳細情報および個別のロケーション情報の履歴に、MSE ノースバウンド API によってアクセスできます。WCS では、このインターフェイスを使用して、ロケーション情報の可視化および Context-Aware パラメータの表示と設定を行います。

Cisco モビリティ ソリューションは、2 種類のロケーション エンジンおよび統合された単一のアプリケーション プログラミング インターフェイス（API）で構成されています。

- クライアント用 Context Aware Engine（Cisco エンジン）
- タグ用 Context Aware Engine（パートナー製エンジン）

クライアント用 Context Aware Engine は、RSSI ベースのソリューションであり、オフィス、病院、その他の天井の低い環境などの屋内空間で、Wi-Fi クライアント デバイスを追跡する場合に適しています。このエンジンは、デフォルトで、すべての Cisco MSE サーバに付属しています。クライアントの追跡にあたって、お客様は Cisco MSE に加えて 2 種類の追加コンポーネントを購入する必要があります。

- 適切なクライアント数を含む MSE 用クライアント追跡ライセンス
- ロケーションを含む Cisco WCS PLUS

タグ用 Context Aware Engine では、RSSI ベースと TDoA ベースの両方のエンジンを使用でき、屋内の天井の低い環境（RSSI）、屋内の天井の高い環境（TDoA）、および屋外（TDoA）で Wi-Fi デバイスを追跡する場合に使用することを想定しています。また、このエンジンは、デフォルトで、すべての MSE プラットフォームにインストールされており、ライセンスがイネーブルにされています。お客様は、クライアントの追跡用に、これらの追加のコンポーネントを購入する必要があります。

- 適切なタグ数を含む MSE 用のタグの追跡ライセンス（TDoA または RSSI）
- Wi-Fi TDoA ロケーション受信機（必要な場合）
- 各 Wi-Fi TDoA 受信機用の LR ライセンス
- ロケーションを含む Cisco WCS PLUS

Cisco MSE を Cisco Unified Wireless Network に追加した場合、MSE では、複数の重要な作業を受け持つことを想定しています。

- 位置決めアルゴリズムの実行
- 調整情報のメンテナンス
- ロケーション通知のトリガーとディスパッチ
- ロケーションの統計情報および履歴の処理

WCS は、MSE サーバ用の管理プラットフォームであり、MSE で提供されるサービス用のユーザ

インターフェイス (UI) です。メンテナンスおよび診断を目的とする場合は、SSH またはコンソール セッションを介して MSE に直接アクセスします。オペレータおよびユーザによる MSE とのすべての対話は、通常は、WCS を介して行われます。

Cisco MSE を Cisco Unified Wireless Network アーキテクチャに統合すると、ベースレベルの ロケーション機能を即座に向上できます。以下の改善点が含まれています。

拡張性：Cisco MSE を追加すると、Cisco UWN の拡張性が向上して、一度に 1 つのデバイスを追跡するオンデマンド追跡から、MSE ごとに最大 18,000 台のデバイス (WLAN クライアント、RFID タグ、不正なアクセス ポイント、および不正なクライアント) を同時追跡できるまでに、追跡キャパシティが強化されます。大量のデバイスをサポートする必要のある展開では、1 台以上の WCS サーバの下に追加の MSE アプライアンスを配置して管理できます。

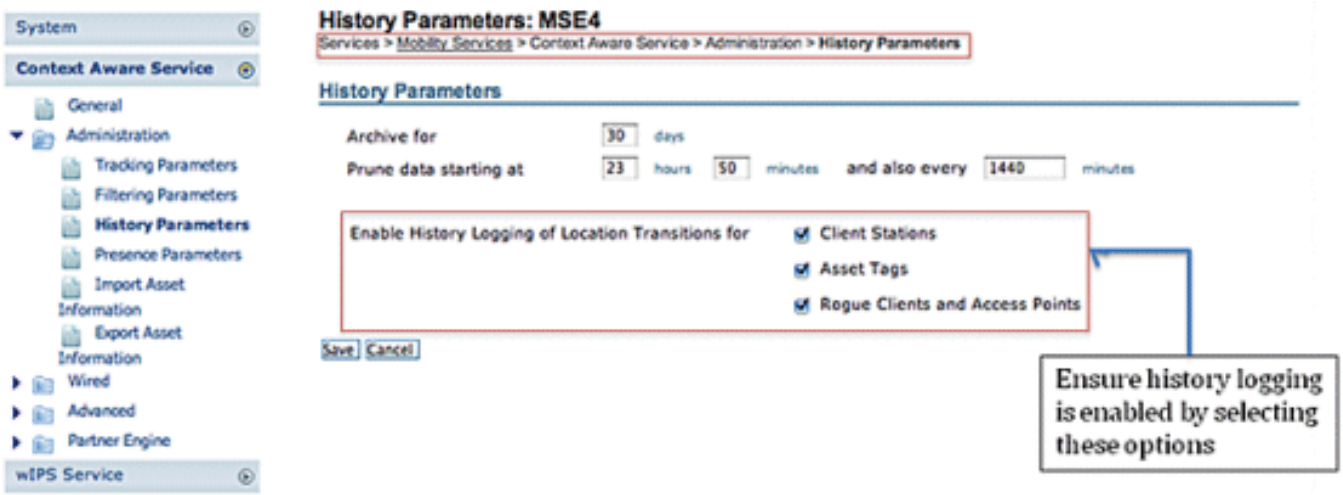
履歴および統計のトレンディング：MSE では、クライアントおよびタグの ロケーションの統計情報および履歴を記録し、保守します。この情報は、WCS またはサードパーティ ロケーション クライアントを使用して表示できます。この履歴情報は、ロケーション トレンディング、資産損失の調査、RF キャパシティ管理、およびネットワークに関する問題の解決の促進に使用できます。

履歴パラメータは、図 3 に示すように、WCS で設定できます。

MSEに保存できる履歴データの量に影響を与える変数がいくつかあります。移動する要素の平均数、移動があるたびにカバーされる平均距離、情報の移行、タグからのテレメトリ情報などです。

デフォルトでは、30 日間の履歴データが MSE に保存されます。

図3：履歴パラメータの設定



ロケーションの履歴に関しては、次の点が重要です。

1. 要素に関するすべての履歴情報を取得するには、図のように、履歴の追跡をイネーブルにする必要があります。
2. 適切な履歴の日数および削除時刻を選択する必要があります (スクリーン ショットを参照)。

3. UI 上では履歴の保存日数に制限はありませんが、サーバ上に保存される履歴は、ディスク領域とシステム全体に対する性能上の影響によって制限されます。

4. 要素の履歴は、次の状況が発生する場合のみ記録されます。

    a. 10 m（30 フィート）を超えて移動する。

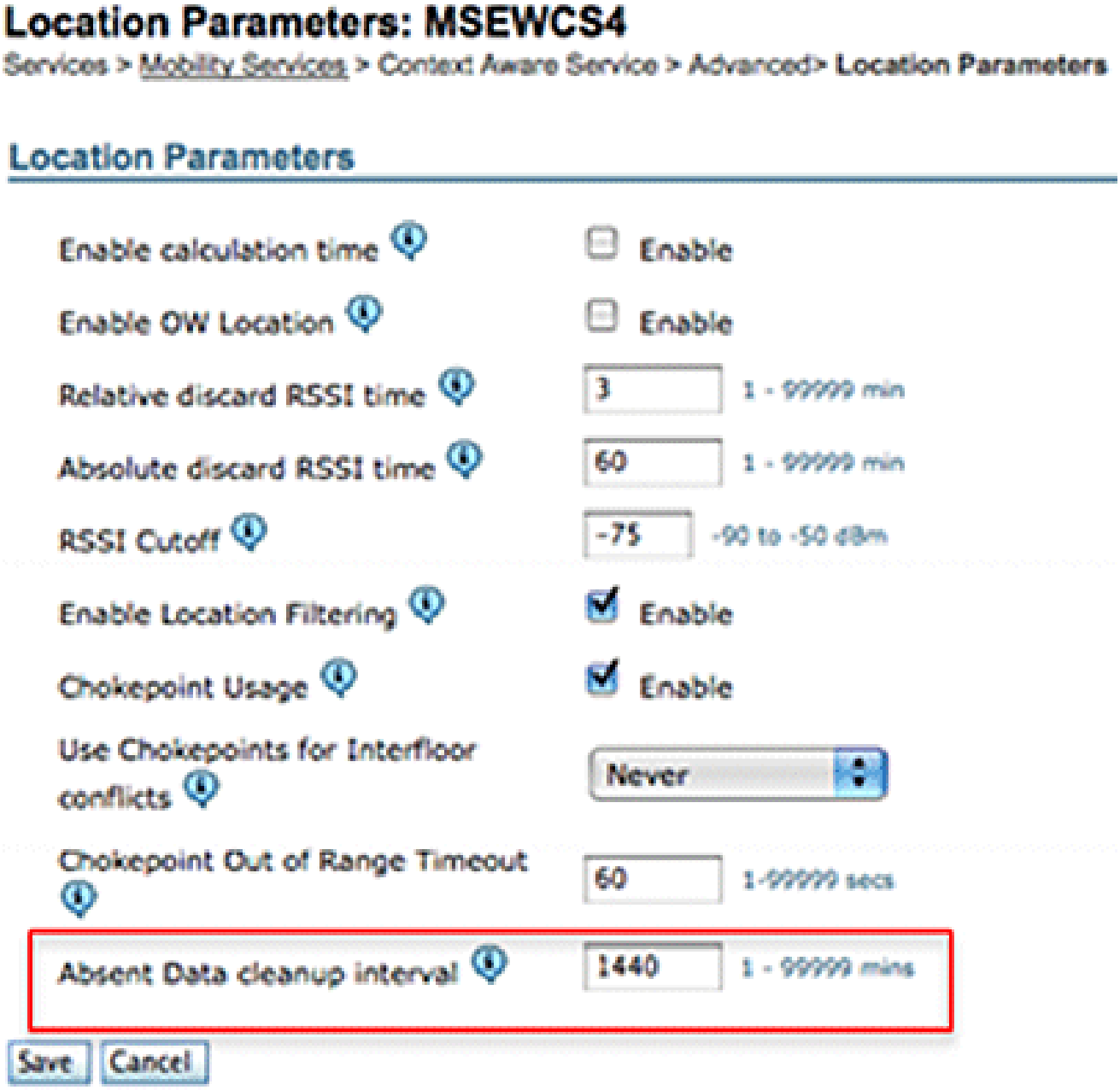
    b. タグ上の緊急ボタンまたはパニック ボタンが押された。

    c. タグが励振器のそばを通った。

    d. フロアが代わった、つまり、要素がフロア間で移動された。

5. 要素は、1 時間以上非アクティブな場合、「非アクティブ」であると宣言されます。24 時間非アクティブなままであった場合は、追跡テーブルから削除されます。要素が追跡テーブルから削除された場合、要素の履歴は 30 日間はまだ MSE に保存されていますが、WCS の監視ページで要素の口ケーション履歴は参照できません。[Absent Data Cleanup Interval] エントリ（図 4 を参照）は、追跡テーブルの制御に役立ちます。

図4：口ケーションパラメータ



すべての推移を 1 つのイベントとして保管用に履歴データベースに記録し、性能上の理由でロケーション履歴テーブルを 1000 万行に制限した場合に、この制限に達するまでの日数を表 1 に、まとめてあります。1 分あたりの要素数の推移が多いほど、消費されるディスク領域の量が多くなります。この表によると、1 分あたり 1000 回の推移がある場合は、わずか 7.14 日間で 1000 万行に達します。デフォルトの 30 日間履歴データを保持する場合、MSE では、30 日の時間枠に達するまでは履歴データを削除しないため、毎分 1000 回の推移があると膨大なディスク領域を消費します。

頻繁に移動するデバイスの履歴パラメータについては、30 日未満の値に変更することを推奨します。

表1：ロケーション履歴データベースの制限

1 分あたりの推移	1000 万行に到達するまでの日数
100	69.44

200	34.72
300	23.15
400	17.36
500	13.89
600	11.57
700	9.92
800	8.68
900	7.75
1,000	7.14

チョークポイント ロケーション：MSE には、チョークポイントと呼ばれる制約された物理エリアを通過する資産に基づく、高精度で決定論的なローカリゼーションが装備されています。そのような エリアおよびタグ付き資産に近接して配置されたチョークポイント トリガー（「励振器」とも呼ぶ）では、低周波信号（125 kHz）によってタグに働きかけます。RFID タグは、次に、チョークポイント トリガーの ID を Cisco UWN インフラストラクチャに送信します。タグ パケットに格納されたチョークポイント情報は、MSE では、RF フィンガープリントのロケーション座標を上書きする情報となり、所定の期間はこの位置がチョークポイントの位置になります。この近傍ロケーションの確度は、チョークポイント トリガーの機能に応じて、半径 25 ～ 650 cm（1 ～ 20 フィート）を超える範囲になります。チョークポイント ロケーション用のアプリケーションには、高価な資産の盗難防止などに使用する汎用的なアプリケーションもあれば、製造工場でプロセス制御イベントに使用する業界固有のアプリケーションもあります。

Wi-Fi タグ テレメトリ情報と緊急通知のためのシスコ拡張：シスコでは、802.11 Wi-Fi ベースのアクティブ資産タグ用の拡張可能な規格を作成するために、さまざまな資産タグ ベンダーと提携しています。Cisco Compatible Extensions（CCX）Wi-Fi タグ仕様では、タグ ベンダーが Context Aware Cisco UWN との相互運用に使用できる、共通伝送フォーマットを定義しています。これには、テレメトリ、タグ送信電力レベル、バッテリ情報、および緊急グループとチョークポイントのための拡張フィールドを網羅するベースライン フィーチャ セットが含まれます。MSE を加えることにより、お客様はこれらの機能を活用でき、さまざまなベンダーから提供されている「ミックスアンドマッチ」に対応した資産タグを同じネットワークで使用できるという利点があります。現在、タグ ベンダーは、CCXv1 を実装しています。タグ参照 URL:http://www.cisco.com/web/partners/pr46/pr147/ccx_wifi_tags.html。

セクション2:Context Awareネットワークの計画とセットアップ

ワイヤレス ネットワークを展開するときに従う必要のある、ロケーションの確度のレベルに直接影響する、複数のガイドラインがあります。

ロケーションおよび音声用のワイヤレス LAN の設計

一般的なガイドライン：RSSI

ワイヤレス LAN カバレッジ エリア内のすべてのデバイスについて最適なロケーションを判別するために、アクセス ポイントの密度および配置を検討します。

アクセス ポイントの配置

妥当なレベルのロケーションの確度を実現するために満たす必要のあるベスト プラクティスとしては、アクセス ポイントを適切に配置すること、配置を改善すること、そしてアンテナのタイプがあります。多くの既存のオフィス ワイヤレス LAN では、アクセス ポイントが内部空間全体に分散されるため、周辺の作業エリアにまでサービスを提供することになります。これらのアクセスポイントの場所は、従来、カバレッジ（WLAN帯域幅、チャネルの再利用、セル間のオーバーラップ、セキュリティ、美観、導入の実現可能性）に基づいて選択されてきました。ロケーション認識型の WLAN 設計では、基礎データと音声アプリケーションの要件を、優れたロケーション忠実度を実現するための要件と組み合わせる必要があります。サイトによりますが、ロケーション認識機能を提供する Cisco UWN の要件には、シスコのベスト プラクティスに従って設計されている音声システムにロケーション追跡機能を追加するなど、十分な柔軟性があります。この場合、広範囲にわたる再作業は必要ありません。対象エリアの特性によっては、受け入れられた音声のベスト プラクティスに従って展開されているインフラストラクチャは、多くの場合、ロケーション追跡のベスト プラクティス要件も同様に満たすように増強できます（たとえば、周辺部アクセス ポイントの配置を行うなど）。

ロケーションの準備が完了した設計では、アクセス ポイントを内部で単にクラスタ化するだけではなく、フロアの中心部に向かうようにすることが重要です。より正確に言うと、周辺部アクセス ポイントは、フロアの内部エリアに配置されているアクセス ポイントを補完します。さらに、アクセス ポイントはフロアの四隅にそれぞれ配置する必要があります。四隅以外にも、フロア周囲に隅（角）になるところがあれば、その場所にもアクセス ポイントを配置することが必要です。これらの周辺部アクセス ポイントは、包囲しているエリア内での優れたロケーションの忠実度を確実にするために重要な役割を果たし、一般的な音声またはデータのカバレッジも実現できます。

チョークポイント ロケーションを使用する場合は、チョークポイント トリガーの設置を予定しているすべてのエリアが、明確にアクセス ポイントの RF 範囲内にあることを確認してください。パッシブ RFID スキャナとは異なり、タグでは、WLAN を使用して励振器の内容をインフラストラクチャに送信します。適切に計画することで、チョークポイント エリア内に配置されている資産タグから送信されるメッセージがシステムによって適切に受信されるだけでなく、資産タグがチョークポイントに向かうときやチョークポイントから離れるときに、RF フィンガープリントを使用して資産タグを追跡できるようになります。RF フィンガープリントを使用して資産タグを追跡する機能は、高い精度を備えたチョークポイント ロケーション技術を駆使してチョークポイント エリア内にあるタグ付き資産の場所を特定するシステム機能を補完します。

フロアの周辺部および隅を形成するアクセス ポイントは、高い確度や精度を実現する可能性が最も高い凸包または候補となるデバイス ロケーションのセットであると考えることができます。内部エリア（凸包内のエリア）は、優れたロケーションの確度を示す潜在性の高いエリアであると見なすことができます。追跡対象デバイスが凸包の外のエリアに移動すると、確度が低下します。

優れたロケーション確度を実現する可能性が高いロケーション データ ポイント セットを囲むように適切な凸包を構築するには、フロアの各隅と、隅と隅を結ぶフロア周囲に沿ってアクセス ポイントを配置する必要があります。周辺部に配置するアクセス ポイントの間隔は、一般的なアクセス ポイントの間隔についてのガイドライン（後述）に従ってください。設計者は、これらのアクセス ポイントによって音声サービスまたはデータ サービスをフロアに提供するために、必要に

応じてこの間隔を狭めることができます。

デバイスの口ケーションを必要とするすべてのエリアに対するカバレッジが、必ず 3 台以上のアクセス ポイントによって提供されるようにしてください。最適な確度を得るには、4 台以上の AP が必要です。これにより、他の WLAN アクティビティが原因で、口ケーションに寄与しないことのある AP が生じるというリスクを低減することもできます。通常のオフィス環境では、追跡するすべての Wi-Fi デバイスの口ケーションを囲むようにアクセス ポイントを配置する必要があります。アクセスポイントは40 ~ 70リ二アフィート (約12 ~ 20 m) ごとに設置する必要があります。つまり、2,500 ~ 5,000平方フィート (約230 ~ 450平方メートル) ごとに1つのアクセスポイントが存在することになります。たとえば、200,000 平方フィートの施設の場合、適切な Wi-Fi カバレッジのためには、40 台の AP (200,000/5,000) が必要です。AP のアンテナは、最低 10 フィートから最高 20 フィートの高さに配置する必要があります。これらのガイドラインは、構築構造および使用されている建築資材の影響を強く受けるため、その他のファクタおよび推奨事項を考慮する必要があります。一般的なルールとして、最小の 3 台の AP が同じフロアにある場合のデバイス追跡では、最小信号レベルとして -75 dBm を使用する必要があります。

次のガイドラインに従えば、アクセス ポイントで追跡対象デバイスを正常に検出する確率が高くなります。

2 つの物理環境が同じ RF 特性を持つことはほとんどありません。ユーザは特定の環境や要件に合わせてこれらのパラメータを変更する必要があります。

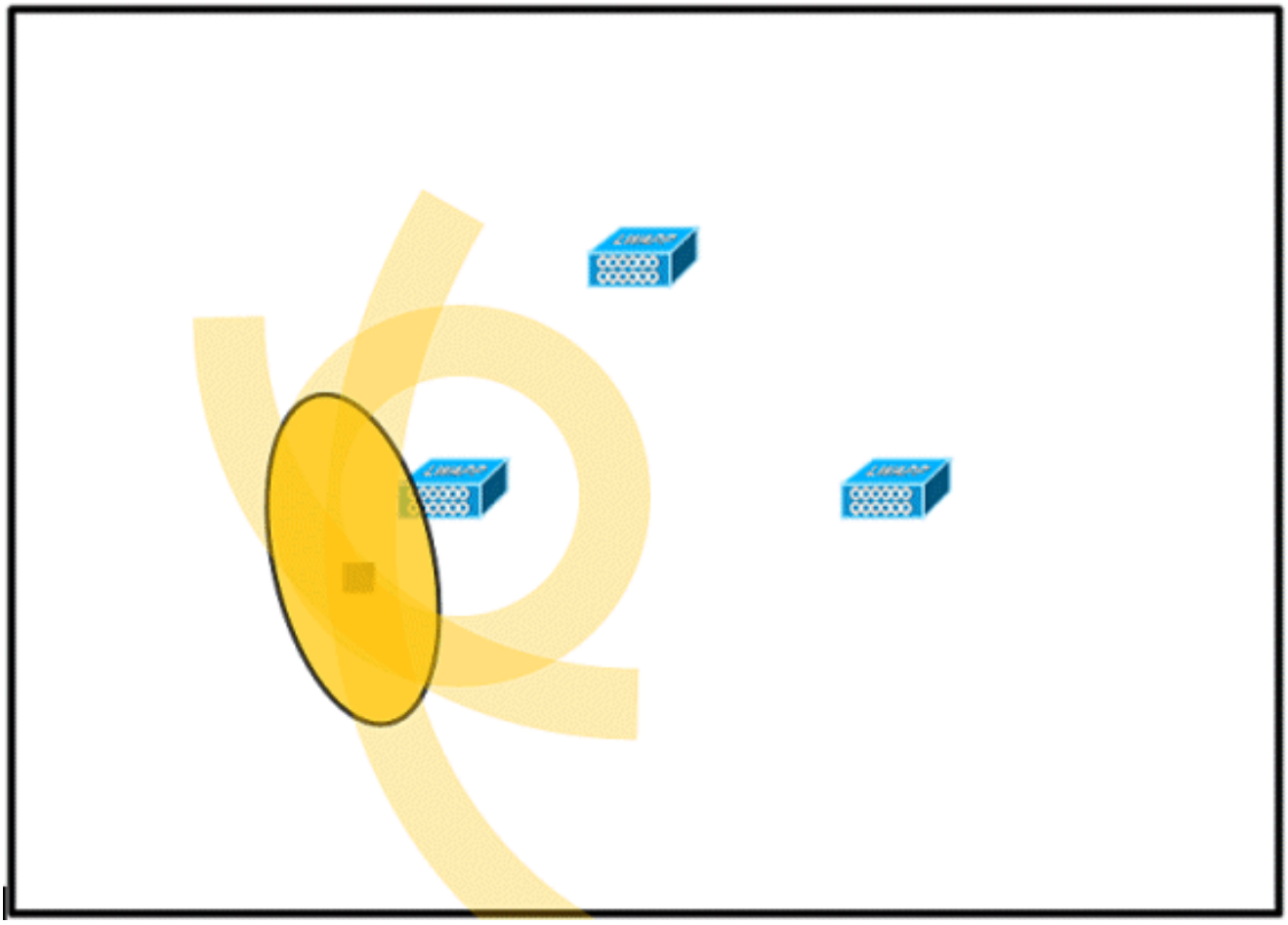
口ケーションの確度に寄与する AP 配置の基本ルールを次に示します。

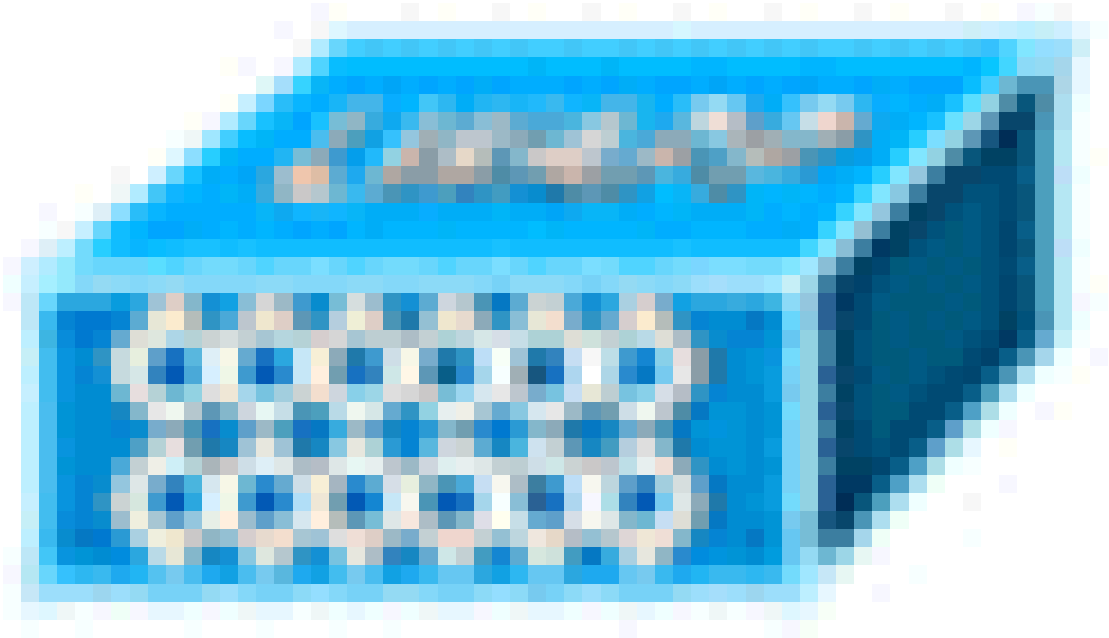
1. AP 周辺部のカバレッジを行う。
2. 十分な AP 密度を確保する。
3. 特に、カバレッジ エリアが細長い場合は、AP を交互にずらす。
4. すべてのアプリケーション (データ、音声、および口ケーション) に対応するように、ワイヤレス ネットワークを設計する。
5. サイト調査によってワイヤレス展開を検証する。
6. 各フロアの形状が似ているビルの場合は、各フロアに、同様なパターンで AP を展開します。これにより、システムのフロア分離の性能が向上します。

適切な AP の配置および密度の判別と検証に WCS Planning ツールを使用できます。

1. カバレッジ エリアの外周沿いおよびコーナーにアクセス ポイントを配置して、部屋および建物の出口近くにあるデバイスを見つけやすくします。このようなカバレッジ エリアの中心に設置されたアクセス ポイントからは、場合によっては他の全アクセス ポイントから等距離に見えてしまうデバイスに関しても有益なデータが得られます (図 5 ~ 8 を参照)。

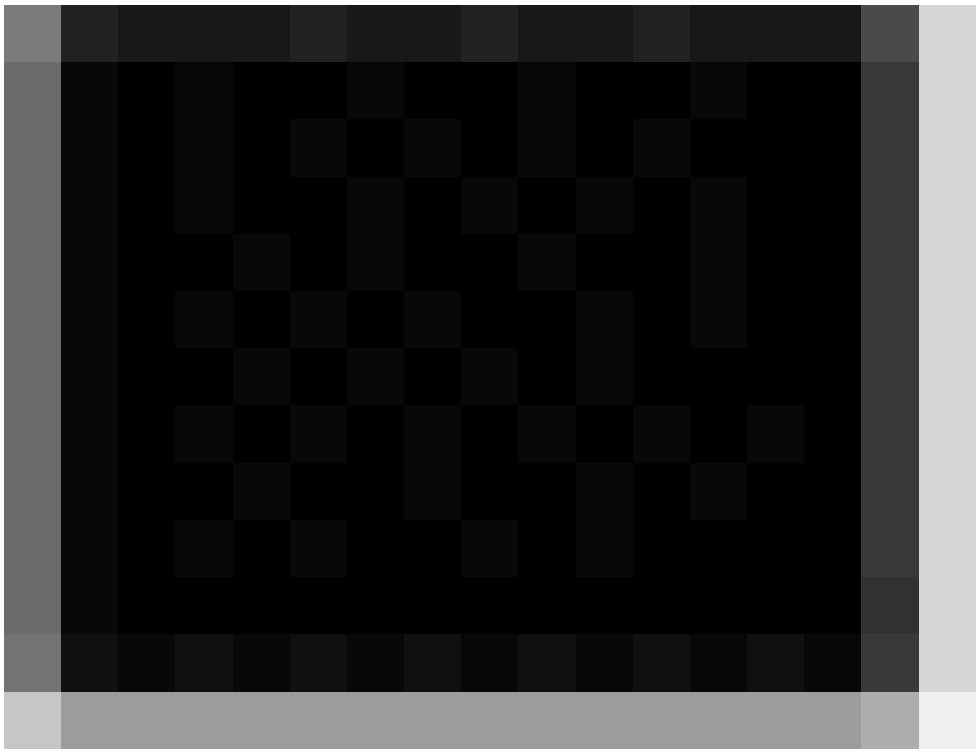
   図5：アクセスポイントのクラスタ化による口ケーション結果の低下





AP：

Wi-Fi デバイス：

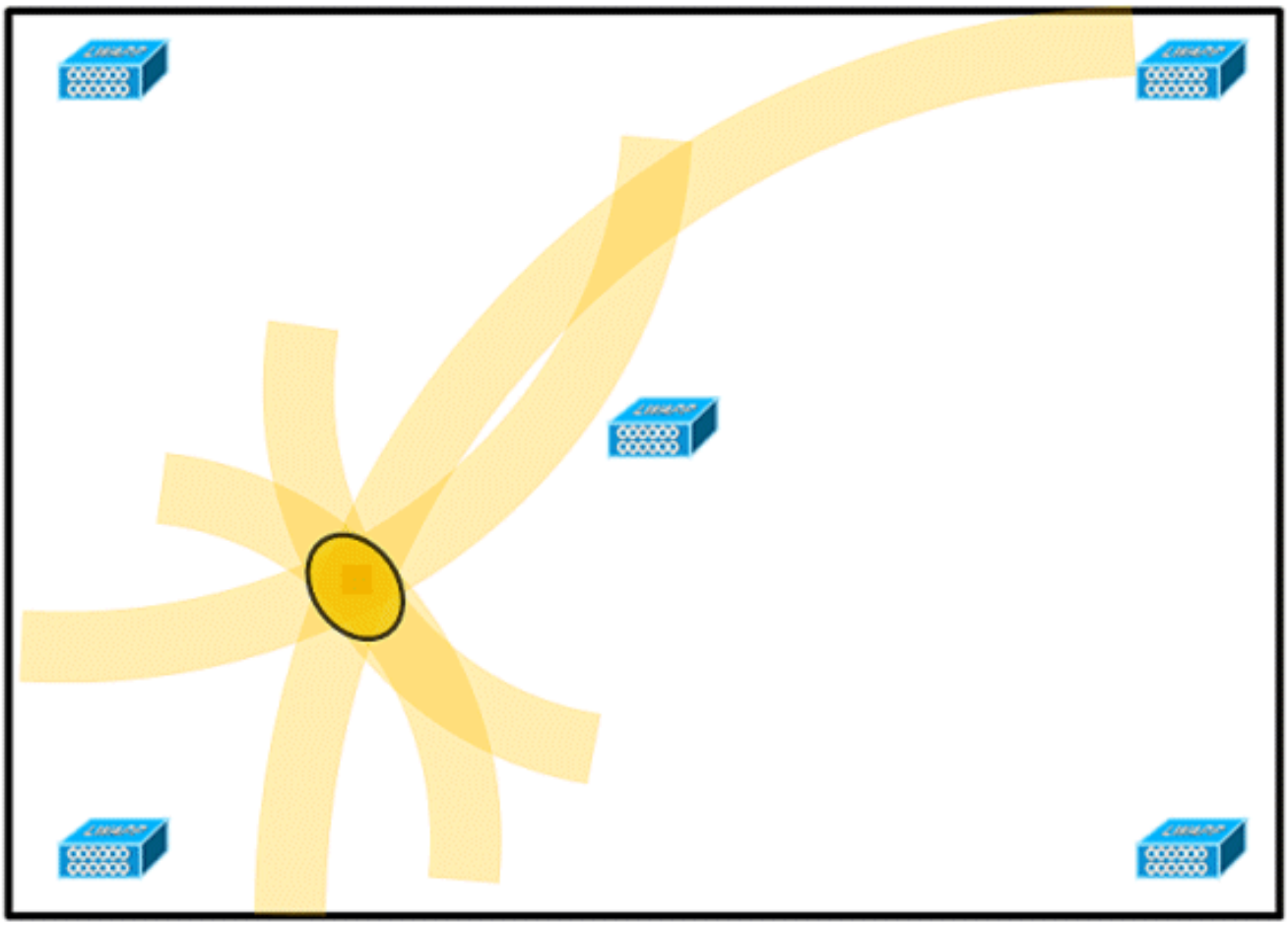


RF ジッタ (ロケーションの候補) :

2. アクセス ポイントの全体的な密度を上げてカバレッジ エリアの周辺部方向へアクセス ポイ

ントを移動すると、ロケーションの確度が大幅に向上します（図を参照）。

図6：適切なAP配置によるロケーション精度の向上



3. 細長いカバレッジ エリアでは、アクセス ポイントを直線的に配置しないでください（図 7 および 8 を参照）。

   AP を交互にずらすと、Wi-Fi カバレッジ マップ上のすべてのポイントに対して RF シグニチャが一意になるため、この方式の展開をお勧めします。直線的な展開では、RF マップが鏡像のようになります。このタイプの展開では、マップの上側にあるポイントの RF シグニチャは、マップの下側にある、鏡像となるポイントでの RF シグニチャときわめて似ています。

   図7：直線上のAPの配置の回避

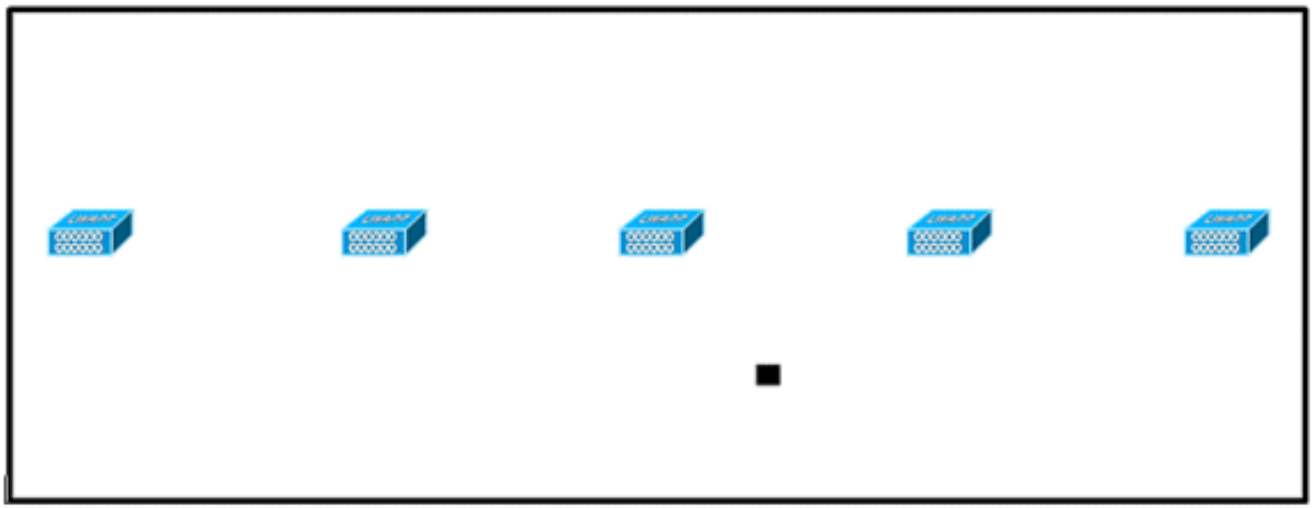
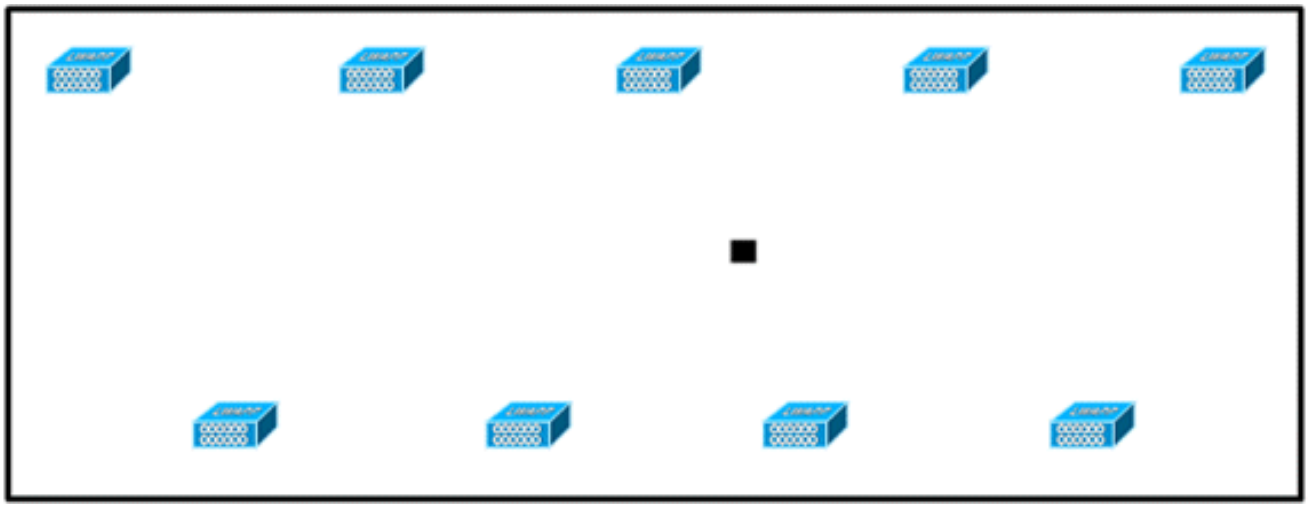


図 7 の設計は、高帯域幅アプリケーションにとっては十分なアクセス ポイント密度になっています。一方、各アクセス ポイントから単一のデバイスを見た場合の違いが十分でないため、ロケーションの場合には問題になり、デバイスのロケーションを容易に判別できません。

アクセス ポイントをカバレッジ エリアの周辺部に移動し、交互にずらして配置します。それぞれのポイントからのデバイスの見え方は、異なっている場合が多くなるため、ロケーションの忠実度を高める結果になります（図 8 を参照）。

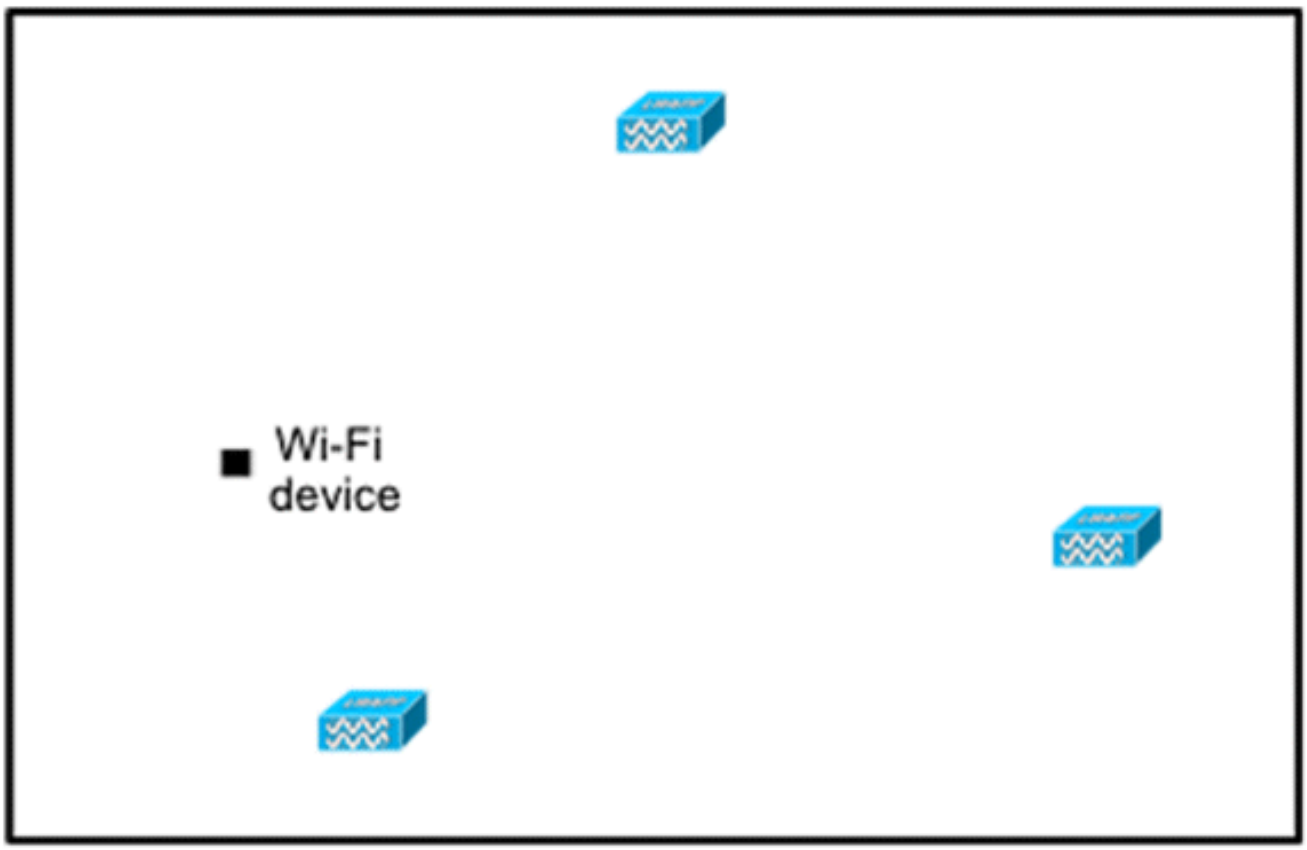
図8：周囲にAPを移動させることでロケーションの精度を向上



4. 音声も対象にしながら Context Aware モビリティ ソリューション用にワイヤレス LAN を設計する場合は、設計ファクタの数も考慮する必要があります。最新の無線ハンドセットは、オーバーラップしない 3 個のチャネルのみを提供する、802.11b のみをサポートしているため、テレフォニー用に設計されたワイヤレス LAN は、データ伝送用に比べて密度が低くなりがちです。また、トラフィックが Platinum QoS バケット（通常は音声トラフィック、および遅延の影響を受けやすい他のトラフィック用に予約されている）にキューイングされると、Lightweight アクセス ポイントはスキャン機能を延期します。これにより、スキャン機能は他のチャネルで最大となり、アクセス ポイントは他の情報とともにデバイスのロケーション情報を収集します。したがって、ユーザは、monitor-only モードに設定したアクセス ポイントでワイヤレス LAN 展開を必要に応じて補完できます。監視機能だけを実行するア

クセス ポイントは、クライアントにサービスを提供せず、干渉を引き起こしません。電波をスキャンしてデバイス情報を収集するだけです（図 9 および 10 を参照）。

図9：低密度のワイヤレスLANの設置



音声ネットワークなど、低密度で設置されているワイヤレス LAN の場合は、ロケーション最適化監視モードのアクセス ポイントを追加して適切に配置することにより、ロケーション忠実度が大幅に向上します。

5. ワイヤレス ラップトップ、ハンドヘルド端末、および場合によっては電話機でカバレッジ検証を実行し、デバイスで 3 台以上のアクセス ポイントを検出することを確認します。クライアントと資産タグの位置を確認するには、指定した確度の範囲内（10 m、90 %）で、WCS がクライアントのデバイスとタグを報告することを確認します。このレベルの確度を達成するには、調整を必要とする場合があります。

Tracking Optimized Monitor Mode（TOMM）

ソフトウェア バージョン 5.0 からの Cisco Aironet 1100 および 1200 AP は、Tracking Optimized Monitor Mode AP として動作できます。この機能は、次のような場合に使用できます。

- ロケーションと音声の共存：モニタモードAPが混在する環境では、ロケーションのAP密度を高める必要があるため、音声に対する悪影響はありません。
- 現場での手作業が少ないため、既存のインフラストラクチャに影響しません。

ロケーション用の Tracking Optimized Monitor Mode は、クライアントおよびタグを追跡する場合に使用できます。

周辺部または凸包内のいずれかで Wi-Fi のカバレッジに隙間があるかどうかにかかわらず、TOMM AP は、ロケーション追跡のカバレッジを向上するために適しています。TOMM AP は、ローカル モード AP の動作に干渉しません。タグの監視と位置計算を最適化するには、アクセス ポイントの 2.4 GHz 帯域（802.11b/g 無線通信）内で、最大 4 つのチャネルに対して TOMM を有効にします。これによって、通常はタグが機能するようにプログラミングされているチャネルだけを対象にチャネル スキャンを実行できます（チャネル 1、チャネル 6、チャネル 11 など）。

図10：トラッキング最適化モニタモードAPの導入

AP とアンテナの配置

AP および外部アンテナの位置は、ワイヤレス ネットワークのパフォーマンスに大きく影響することがあります。このことは、データおよび音声の伝送にも、ロケーションの追跡にも当てはまります。AP およびアンテナは、信号パターンを歪めるおそれのある場所（I 型梁の近くなど）に配置しないでください。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 RF 信号が反射した際に生じます。このような場所に配置すると、AP の背後のカバレッジはほとんどなく、AP の前側の信号品質も低下します。I 型梁により、送信と受信の両方のパケットで多数の反射が生じます。反射信号は、ヌル ポイントおよびマルチパスによる干渉を招いて信号品質を極端に低下させることがある一方で、信号を増幅させることのある I 型梁のごく近くに AP アンテナがあることで、信号強度は強まることがあります。反射信号を低減し、ヌル ポイントを減らし、マルチパスによる干渉を減らすために、AP およびアンテナは、I 型梁から離れた場所に

配置してください。この原則は、標準的な企業の環境で天井内部または天井近くに AP 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おそれのある、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、その障害から離れた場所にアンテナを設置することを強くお勧めします。エレベータ、空調ダクトなど金属製の大型物体がある場合は、数フィート離れた場所までアンテナを移動してください。これは、信号の反射および歪みを解消するために有用です。図 11 ~ 13 は、性能の低い AP 配置を示します。

図11：不適切なAP配置 – 物理的な障害物の近くに配置されたAP

図12：不適切なAP配置：物理的な障害物の近くに配置されたAP

図13：不適切なAP配置 – 互いに近接して配置されたAP

内部アンテナまたは外部アンテナを持つアクセス ポイントを設置する場合は、WCS 内でアクセス ポイントの配置と選択したアクセス ポイントのアンテナの方向の両方が、実際の物理アクセス ポイントの配置およびアンテナの方向と一致している必要があります。これにより、ロケーション追跡と、ヒート マップの予測的表示の双方において、確度と精度を確保できます。優れた確度を得るには、アンテナの種類、位置、方向、およびフロアからの高さが重要です。WCS 内で AP を設置するときは、アンテナの方向および種類が、配置するアンテナと一致していることを確認してください。

注：ワイヤレスクライアントを追跡する場合、正式にサポートされているのはCiscoアンテナだけです。シスコ以外のアンテナの場合は、WCS にヒートマップに生成されません。これは、これらのアンテナから受信する RSSI 値を無視して、ロケーションが計算されることも意味します。タグの追跡については、シスコとシスコ以外の両方のアンテナを使用できます。

一般的な Cisco Aironet アクセス ポイントは、アンテナ ダイバーシティを有効にして設置します。アンテナ ダイバーシティによって、高マルチパス環境における適切な範囲とスループットを確保できるようになります。アンテナ ダイバーシティは、常にイネーブルにすることをお勧めします。Context-Aware Cisco UWN は、追跡対象デバイスのローカリゼーション（ロケーション）を行うときに双方のアクセス ポイント アンテナからの RSSI 情報を考慮するように設計されています。優れた確度を保つため、有効になっているすべてのアクセス ポイント アンテナ ポートにアンテナが物理的に存在するようにしてください。そうしないと、アンテナが取り付けられていないのに有効に設定されているアンテナ ポートで、不規則な RSSI 測定値が報告されることがあり

ます。アンテナを取り付けていないアンテナ ポートから異常に低い RSSI 値が報告されると、ロケーションの確度が低下します。

いずれのワイヤレス ネットワーク展開においても、AP で使用するアンテナの選択が、展開の特性に大きく影響します。基本的に、指向性アンテナと全方向性アンテナの2種類のアンテナがあります。各アンテナのタイプには、特定の用途があり、特定のタイプの展開に適しています。アンテナは、アンテナの設計によって決まる、ローブの大きいカバレッジ エリアに RF 信号を配信するため、カバレッジが成功するかどうかはアンテナの選択に大きく依存します。

アンテナには、ゲイン、指向性、偏波という3つの基本的な特性があります。

- ゲイン：電力の増加を示す単位。ゲインとは、アンテナにより RF 信号に付加される工ネルギーの増分の総量です。すべてのアンテナは受動要素です。アンテナによって電力は増幅されませんが、全方向性（等方性）アンテナによって送信される以上の放射電力を特定の方向に放射するように再分配されます。工ネルギーはアンテナによって維持されるため、特定の方向でアンテナのゲインが 1 よりも大きい場合、その他の方向のゲインは必ず 1 未満になります。

- 指向性：伝送パターンの形状。アンテナのゲインが増加すると、カバレッジ エリアは減少します。カバレッジ エリアや放射パターンは角度で表されます。これらの角度は度数で表現され、ビーム幅と呼ばれます。

  注：ビーム幅は、アンテナが空間の特定の方向に向けて無線信号工ネルギーを集中させる能力の尺度として定義されます。通常、ビーム幅は度数で表現され、水平ビーム幅（HB）は垂直ビーム幅（VB）（上下の）放射パターンとともに最も重要です。アンテナのプロットまたはパターンを見るとき、角度は通常、メイン ローブの最大効果放射電力を基準とした場合の、メイン ローブの半電波強度（3 dB）ポイントで測定されます。

- 偏波：空間を通過する電磁波の電界の方向。アンテナは、水平方向または垂直方向のいずれかに偏向される可能性がある一方で、他の種類の偏波特性も可能です。1 つのリンク内にあるアンテナは、無用な信号損失を増やさないために、両方が同じ偏波特定を持つ必要があります。パフォーマンスを向上させるため、アンテナを時々回転させると、偏波特性を変更し干渉を減少できます。概して、コンクリートで囲まれた谷間のようなエリアに RF 波を送信するときは垂直方向の偏波が適しており、広範囲に配信するときには水平方向の偏波の方が適しています。偏波特性は、隣接する構造物まで届く RF 工ネルギーの削減が重要であるときに、RF Bleed-over を最適化するためにも利用できます。ほとんどの全方向性アンテナは、デフォルトとして垂直偏波を設定して出荷されています。

  アンテナから放射される無線工ネルギーを有効等方性放射電力（EIRP）と呼びます。EIRP 値は、通常は、ワット数または dBm で表されます。ライセンス不要の帯域を公正、公平に共有できるように、規制区域では最大の EIRP レベルが要求されます。EIRP は、アンテナからの電力によって測定されるため、EIRP には、アンテナ ゲインとケーブル損失およびトランスミッタからの電力を含める必要があります。アンテナ ケーブルによって損失が多くなる場合があり、その結果、伝送信号が減衰することがあります。ケーブルが長いほど、減衰が大きくなり、ケーブル内での信号損失が多くなります。これは、電力の受信と伝送の両方に影響します。ケーブルによる減衰は、グレードおよびメーカーによって異なります。低損失ケーブルの場合、通常は、2.4 GHz において 30 m（100 フィート）あたり約 6.7 dB です。

信号の減衰

信号の減衰や信号損失は、RF 信号が任意の媒体を通過するときに起こります。信号の減衰は、信号が通過する物質の種類によって異なります。表 2 は、さまざまな物体の信号損失値を示します。

表2：さまざまな物体による信号の減衰値

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

注：これは大まかな目安にすぎません。国によって建築規制は異なります。このさまざまな規制は、許可される最大 EIRP およびその他のパラメータに適用されます。

20 mW の伝送パワーは 13 dBm に相当します。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 ならば、壁を抜けるときの信号強度は 10 dBm に減少します。

さまざまなタイプの施設でサイト調査を実施すると、さまざまなレベルのマルチパスによる歪み、信号損失、および信号ノイズが観測されます。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、通常は調査に時間がかかり、AP の密度を高くする必要があります。製造工場と作業現場もサイト調査が難しい環境です。このような場所では、一般的に、信号を反射してマルチパスによる歪みを再作成することになる、金属含有量の多い物体が建造物の内部に存在しています。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。特定の環境で RF 信号が到達する距離を判別する方法は適切なサイト調査の実施以外にありません。

注：サイト調査データを収集するクライアントではなく、追跡するAPとデバイスのRx信号レベルを考慮することが重要です。経験からいうと、サイト調査を実行するときは、50 mW 程度の比較的高い電力設定に AP を設定することが有用です。大部分のアンテナは対称性のある Tx および Rx の特性を持つため、結果のカバレッジ パターンには AP の概算 RSSI が反映されます。

複数階のビル、病院、および倉庫のサーベイランス

複数階のビル、病院、および倉庫を調査する場合に考慮する必要のある要因は多数存在します。

構築構造をできるだけ詳細に調べることが重要です。AP 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、配管と取り付け具などがあります。さまざまなタイプおよびレベルの在庫品、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もあります。注意を必要とするものには、プリンタ用紙、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。サイト調査は、必ず、在庫のレベルや活動がピークのときに実施します。同じ倉庫でも、在庫レベルが 50 % の場合と空きがない場合では、RF のフットプリントが大きく異なります。

同様に、同じオフィス エリアでも、人のいる時間帯と人のいない時間帯では 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、在室者がいて、通常の活動が行わ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欠かせません。

利用率の要件が高く、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。AP 上のアンテナのダイバーシティは、このような条件を最小限にするために役立ちます。

一般的な複数階のオフィス 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 RF 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）では、電子レンジによって 2.4 GHz の干渉が生じる可能性がある。
- 実験室は、2.4 GHz または 5 GHz の干渉を発生させる可能性がある。干渉があると、ノイズ フロアが増え、受信信号の SNR（信号対雑音比）が下がるという問題があります。ノイズ フロアが大きいと、AP の有効範囲が狭まります。
- オフィスのパーティションは信号を吸収し、遮断する傾向にある。
- 教室の窓やパーティションは、RF 信号を反射および遮断する。
- 浴室のタイルは、RF 信号を吸収したり遮断したりすることがある。
- 会議室は、Wi-Fi 使用率が高いエリアであるため、高い AP カバレッジを必要とする。

複数階の施設を調査する場合は、異なるフロアの AP どうしが、同じフロアにある AP と同様、簡単に干渉し合うことがあります。このことは、音声やデータの展開によっては有益なことがある一方で、Context Aware を展開するときには問題を生じます。このソリューションを適切に機能させるには、フロアの分離が重要です。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、近隣の部屋やオフィスに信号が伝わらないように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、増改築が繰り返されていることが多い。増築のたびに、信号の減衰レベルの異なる、さまざまな建築資材が使用されていることが考えられます。

- 患者の立ち入る工リアの壁と床は、通常、最小限の信号しか貫通せず、マイクロセルが生じやすい。したがって、十分な RF カバレッジを達成するためには AP の密度をずっと高める必要があります。

- 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。

- AP 密度を高くする必要があることから、セルのオーバーラップが多くなることがあり、その結果、チャネルが再利用される。

- 病院には、2.4 GHz の非 802.11 機器を含んだ複数のタイプの無線ネットワークが設置されている場合がある。この機器により他の 2.4 GHz または 5 GHz の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。

倉庫には広いオープンな工リアがあり、多くの場合、ここには高い収納棚があります。その高さは AP が通常設置される天井まで達することもよくあります。このような収納棚により、AP でカバーできる工リアが制限される可能性があります。その場合は、AP 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 AP の数が異なる。想定した配置場所に 2 台か 3 台の AP を使用してカバレッジをテストします。

- カバレッジ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 AP よりも遠くにある AP との方が関連付けと操作性がよい場合があります。

- 調査時には、通常は、AP およびアンテナにアンテナ ケーブルを接続しませんが、実稼動環境では、AP およびアンテナにアンテナ ケーブルを必要とすることがあります。すべてのアンテナ ケーブルには信号損失があります。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、倉庫のサーベイランスと同様です。重要な違いの 1 つは、製造施設では RF 干渉の原因となる要素がずっと多いため、周囲の RF 環境でノイズがずっと多い点にあります。また、製造施設で使用するアプリケーションは、通常は、倉庫環境で使用するアプリケーションよりも多くの帯域幅を必要とします。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。

サイト調査では、信号レベルを測定するだけでなく、RF 環境の特性を適切に評価するために、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。

人の流れが多いエリア（オフィス、学校、小売店および病院など）では、人目に触れない場所にAP を配置し、目立たないアンテナを天井に設置することを推奨します。

ロケーション レールとリージョン

指定された導入ガイドラインでは、10 m/90 %、5 m/50 %という高い精度が得られます。10 m/90 % という値は、特定のデバイスに対する実際の物理ロケーションから半径 10 m に対応します。したがって、この確度目標が満たされていても、追跡対象のデバイスが存在するはずのないフロアやビルの階のエリア内に、そのデバイスが表示されることがあります。

レールとリージョン機能は、ロケーション サービスに包含または除外するエリアをネットワーク管理者が定義できるメカニズムを備えています。この機能では、マップ上の特定のリージョンを、有効なロケーション エリアのスコープの内側または外側であると定義できます。

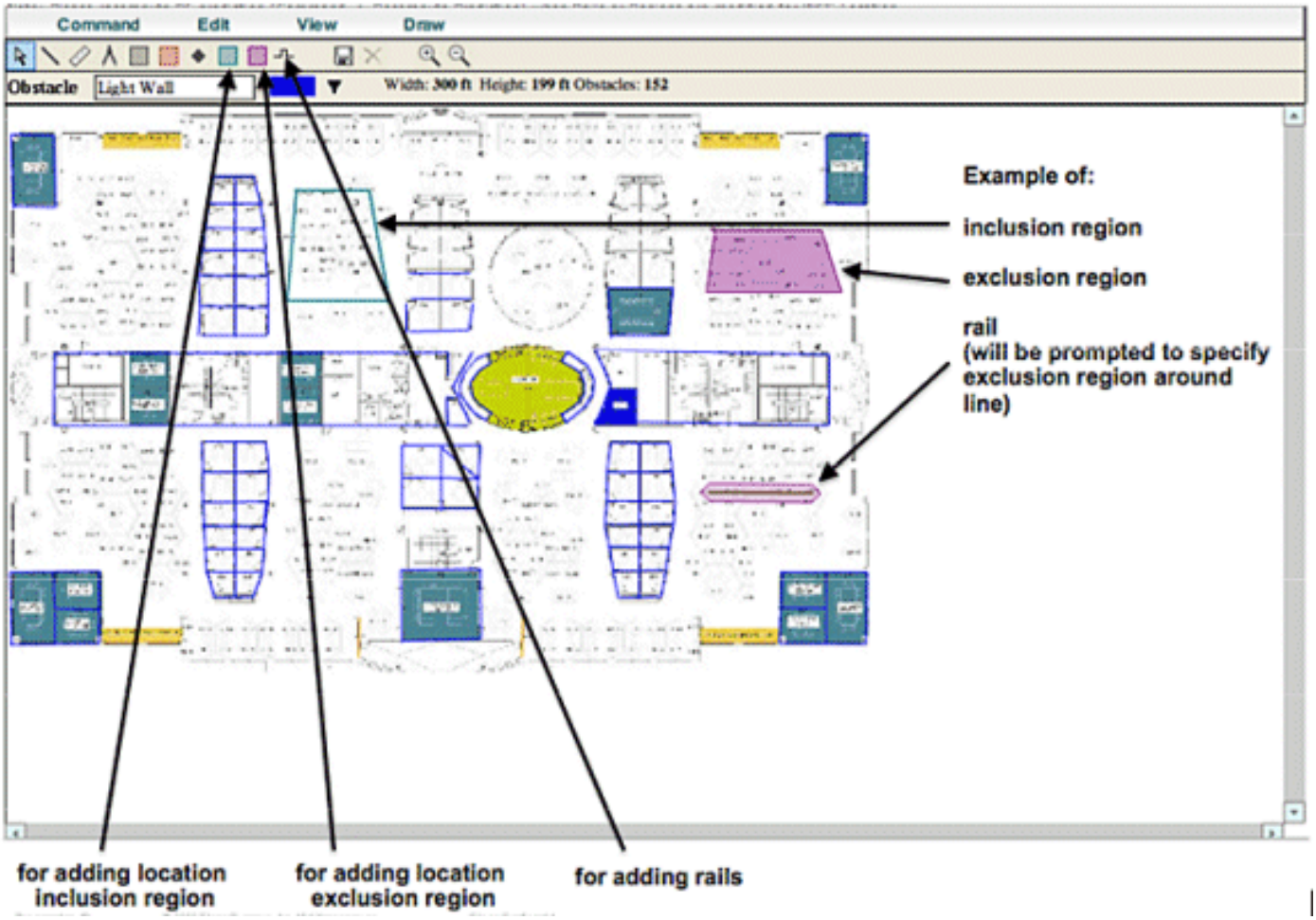
図 14 に示す 3 種類のリージョンを指定できます。

- ロケーションの包含リージョン：追跡対象デバイスをこのポリゴンの外側（例：建物の外壁の外側）に配置することはできません。
- 場所の除外領域：追跡対象のデバイスをこのポリゴンの内側に配置することはできません（例：吹き抜けアトリウムまたは建物の障害物）。競合するリージョンを描画した場合は、除外の方が包含よりも優先されます。
- レール：トラッキング対象デバイスは、狭帯域で定義されたエリア内に設置する必要があります。通常は除外領域（コンベアベルトなど）内で使用します。

WCS 内でレールとリージョンのエリアを定義した後で、同期プロセスによってフロア アップデートを WCS から MSE に送る必要があります。

注：MSEでは、Location Rails and RegionsはContext Aware Engine for Clientsでのみ機能します。AeroScout には、タグを追跡する場合に同様な機能を提供する、セルおよびマスクという機能が実装されています。Cisco 2710 ロケーション アプライアンスの場合、レールとリージョン機能は、クライアントの追跡とタグの追跡の両方で機能します。

図14：レールとリージョン



システム マネージャでのマスクの作成

マスクは、除外するエリアを区切るポリゴンをマップ上に描画することによって定義されます。

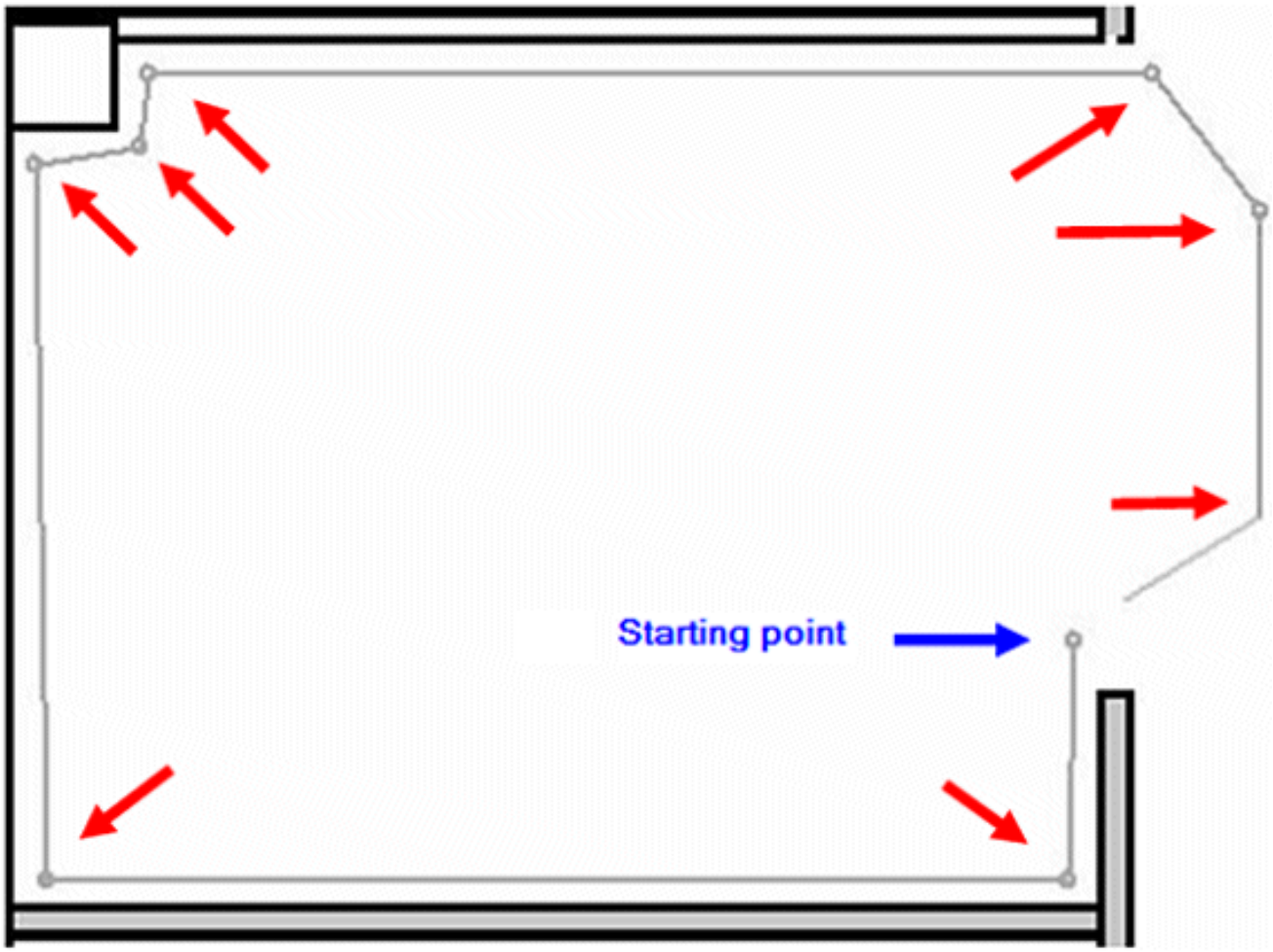
マスクを作成するには、次の手順を実行します。

1. [Configuration]、[Maps]、[Mask]、[Edit Mask] を選択します。

   システムがマスク編集モードに切り替わります。マウス ポインタが十字に変わります。

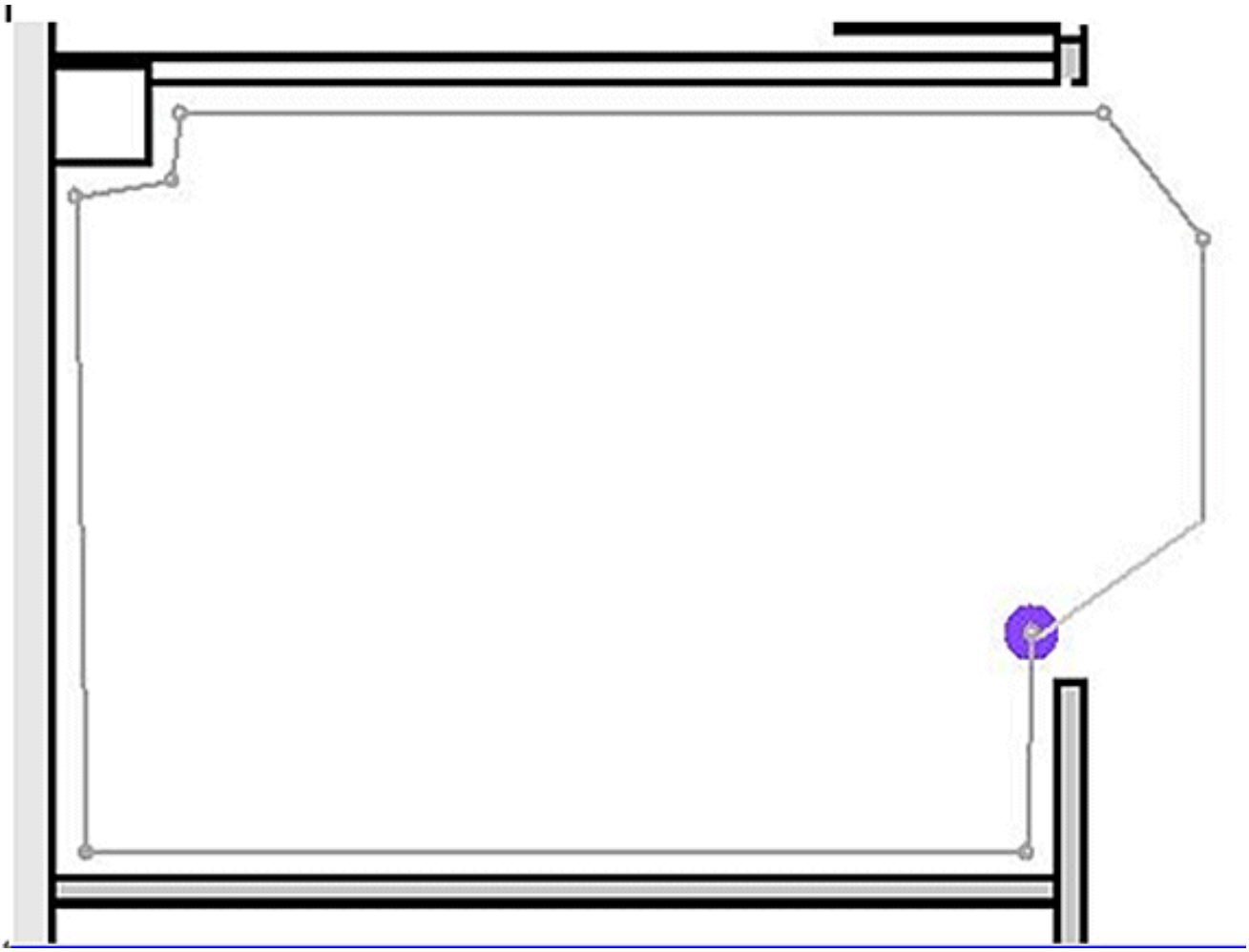
2. マップ上の点をクリックします。次の点までマウスをスライドして再度クリックし、このプロセスを繰り返してポリゴンの頂点をマークします(図15を参照)。

   図15：マスクの作成 – ポリゴンの頂点のマーキング



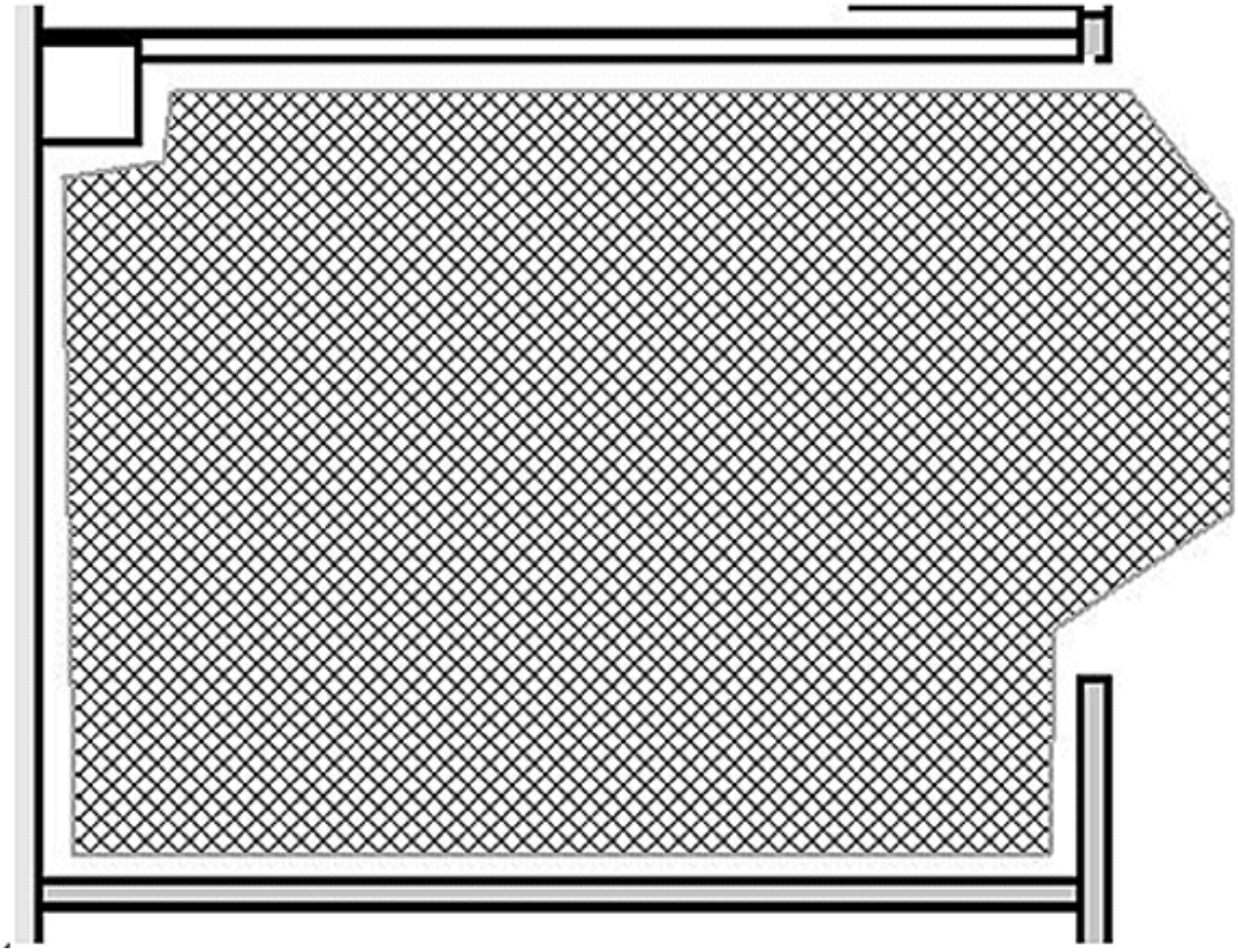
ポリゴンを閉じる場合は開始ポイントまでマウスをスライドします。紫色の円が表示されます。これは、終結ポイントを示します（図 16 を参照）。

図16：マスクの作成 – 閉じる点を示す紫色の円



クリックして、マスクの定義を完了します。マップ上にマスクが表示されます (図 17 を参照) 。

図17：マスクの作成：マップにマスクが表示される



3. マップ上の任意の場所を右クリックし、[Exit Mask Drawing Mode] を選択するか Esc キーを押して、マスク編集モードを終了します。

   デフォルトでは、マスク描画モードを終了すると、マスクは表示から削除されます。マスクのイネーブル化とディセーブル化、または編集以外の詳細については、Aeroscout Documentation を参照してください。

タグ用 Context Aware Engine 内のセル

セルは、ロケーション計算プロセスを最適化して位置決めの確度を向上するために、マップを小さい部分に分割するように設計されています。セルは、タグの位置決めにおける地理的な境界を定義します。また、どの個別デバイス (TDoA 受信機およびアクセス ポイント) がこの境界内でのロケーション計算プロセスに加わるのかも定義します。

セルのメカニズムは、RSSI と TDoA の両方のロケーション計算で使用されます。

エンジンは、着信ロケーション データを処理します。

- タグのロケーションを示すレポートは、複数のアクセス ポイントまたは Wi-Fi TDoA 受信機から同時に着信することがあります。エンジンのマップ弁別アルゴリズムによってデバイスの存在している可能性の最も高いマップが選択され、その他のマップを指しているロケーション レポートは廃棄されます。

- マップが決定されると、エンジンはセルを検索します。マップがセルに分割されている場合は、同じ最適化メカニズムによって、最も精度の高いロケーション レポートを届けた可能性の高い TDoA 受信機またはアクセス ポイントのセルが選択されます。次に、このセルおよびこのセルの境界内と関連付けられている TDoA 受信機またはアクセス ポイントから受信したデータに従って、デバイスのロケーションが計算されます。

セルと関連付けられている TDoA 受信機またはアクセス ポイントは、セルの境界によって区切られたエリアの内部に存在するとは限らないことに注意してください。

セル設定のための初期運用

最初に、マップ エリア全体をカバーするために、マップごとにデフォルト セルが自動作成されます。マップを個々のセルに分割するには、次の操作を実行します。

1. マップ エリアの一部のみをカバーするようにデフォルト セルを編集します（セルの変更方法についての説明を参照）。
2. 必要に応じてマップにセルをさらに追加します。セル全体を別のセルに含めることはできません。
3. 各ロケーション デバイス（アクセス ポイントおよび TDoA 受信機）のプロパティを確認し、このデバイスを適切なセルに関連付けます。
4. セルに関連付けられているデバイスを、別のセルに関連付けられているデバイスに含めることはできません。他のセルに関連付けられていないデバイスが、各セルに関連付けられていることを確認してください。

調整：クライアント用 Context Aware Engine

ロケーションの確度は、主に次の 2 つのファクタによって決まります。

- AP の配置およびロケーションに寄与する AP の数
- 特定の環境に対する AP の正しい RF 信号特性（正確な AP ヒート マップ）

調整フェーズでは、モバイル デバイスを持って対象の環境内を歩き回り、このデバイスの信号強度を複数の AP でサンプリングできるようすることで、WCS サーバ上でデータが収集されます。WCS にログインした 1 台以上のラップトップ（無線帯域ごとに最大 5 台のデバイス）を使用して、調整するエリアのマップを選択する方法をお勧めします。このエリアは、通常は、サンプル データを取得する必要のある正確な場所をオペレータが判断できるように、グリッド ポイントのセットまたはメモによってオーバーレイ表示されます。マップ上の各サンプリング ポイントで、調整デバイスと関連付けられた RSSI 値のセットが WLC から MSE に転送されます。個々のデータ セットのサイズは、モバイル デバイスを検出する、受信側アクセス ポイントの数に基づいて変わります。フェーディングなどの RF 環境特性が原因となって、特定のロケーションで観察されるモバイル デバイスの信号強度は時間変異性を持ちます。つまり、時間の経過に伴って変わることがあります。この結果、調整プロセスで 1 台の調整デバイスに関して、多数のデータ サンプルが記録されます。

各環境は固有であり、特定の環境における AP の信号特性は大きく変動します。WCS は、ユーザが環境に合わせて信号特性を調整するためのメカニズムを備えています。ここで要約したロケーション展開ガイドラインに従って AP を展開することが、確度を最適化するための第一歩となります。AP のカバレッジおよび配置が不十分な状態で、調整によってロケーションの確度を向上させようとすると、通常は十分な結果が得られないばかりでなく、確度を損ねるおそれもあります。

WCS に付属している 3 つのデフォルト調整モデル：

- 個室および壁で囲まれたオフィス
- 乾式壁のオフィスのみ
- 屋外のオープン スペース

各モデルは、一般的なお客様の環境における最も一般的なファクタに基づいています。このうち、最初の 2 つの RF モデルは通常のオフィス環境で有用です。

提供されている RF モデルではフロア レイアウトの特性が十分に表されていない場合は、WCS を使用して調整モデルを作成し、フロアに適用することによって、特定の環境での減衰特性をよりよく表現できるようになります。多くのフロアで同じ減衰特性を持つ環境の場合は、調整モデルを 1 つ作成して、類似するすべてのフロアに適用できます。

屋内環境でも、一般的なオフィス環境よりも高い減衰が見られる場合があります。適切に設計された屋内への設置で、減衰が大きくなっているためにロケーションの確度を最適な状態よりも低下させている場合は、サイト調整が最適なパフォーマンスの復元に役立つことがあります。オンサイト調整を実行すると、システムは環境全体の既知のポイントからパス損失のサンプルをとることができます。この結果、その環境固有の伝播特性を理解するためのカスタム RF モデルを考案することができます。

多くの場合、デフォルト モデルではなく調整で収集された情報を使用するほうが、計算されたクライアント ロケーションと実験によって得られるデータの間に見られる誤差が大幅に減ります。多くのフロアで減衰特性がほとんど一致している環境では、ロケーション間の類似性が高いために、任意の 1 つのロケーションで実行した調整によって作成された RF モデルを他の同様な エリアに適用すると優れた結果を得られます。

混合的な RF 減衰特性を持つエリアについても考慮すべきことがあります。このような エリアとは、建物の一部の エリアに商品が積み上げられていたり、障害物がぎっしり詰まっていたりする一方で、組み立てまたは出荷に使用するオープン スペースもある製造工場または倉庫です。これらの エリアは独立したゾーンとして扱い、最高の確度を必要とする エリアに対する調整を制限する必要があります。混合 エリアにあるすべてのゾーンで最高の確度を必要とする場合は、フロア エリアを個別のセルまたはマップに分割し、別々の RF モデルを適用することをお勧めします。

注：このタイプのRFモデリングのパフォーマンスは複雑で、展開に関してさらに考慮する必要があります。これはこのドキュメントの範囲外です。

調整は、実際には複数の段階プロセスで構成されます。このプロセスは、新しい調整モデルを定義することから始めます（ [Monitor] > [Maps] > [RF Calibration Models] > [Create New Model] ）。調整プロセスのステップごとの説明については、『Cisco Context-Aware Software コンフィギュ

レーション ガイド』の「調整モデルの作成と適用」を参照してください。

調整プロセスでは、調整クライアントが、すべてのチャネル上にプローブ要求を繰り返し送信します。特定の調整クライアントを使用する場合は、ネットワーク要求を介してクライアントをトリガーして、オンデマンドでプローブ要求を送信できます。これらの要求を認識できないクライアントの場合は、認証および関連付けを解除することにより、ワイヤレス ネットワークに対してプローブ要求を発行させることができます。その結果、関連付けと認証がやり直されます。クライアントの圏内にあるアクセス ポイントは、これらのプローブ要求の RSSI を検出し、登録されているコントローラにその情報を渡します。コントローラは、調整プロセスで検出された RSSI 情報を WCS に提供します。WCS では、この情報を使用して、新規調整モデルを定義するために使用されるパス損失を計算します。

調整モデルを作成する場合は、データ ポイントの収集が重要なステップになります。WCS における調整プロセスのデータ ポイント収集フェーズは、2 つの方法のうちいずれかの方法を使って実行できます。WLAN に関連付けられている Web に対応した単一のモバイル デバイスから実行できます。このデバイスで、ネットワーク調査と実際のデータ収集の両方を管理します。また、WLAN インフラストラクチャに関連付けられている 2 台の異なるデバイスからデータ ポイント収集フェーズを実行することもできます。この場合、WCS GUI との対話はキーボードとマウスの機能を備えている 1 台目のデバイスから制御し、実際のプローブ要求の生成は、既知の MAC アドレスを選択して、関連付けられている 2 台目のデバイス上で行います。

調整データの収集は、帯域ごとに別々に実行することをお勧めします。デュアルバンド クライアントを使用する場合は、次のいずれかの代替方法を使用してください。

1. 帯域ごとに個別に Cisco Aironet 802.11a/b/g Wireless CardBus Adapter（AIR-CB21AG）を備えるラップトップ 1 台を使用して調整データ収集を実行します。2.4 GHz 帯域用の調整を実行する場合は、5 GHz 帯域をディセーブルにし、2.4 GHz 帯域のみでデータ収集を完了します。この調整プロセスの完了後に 2.4 GHz 帯域をディセーブルにし、5 GHz 帯域をイネーブルにして、5 GHz 帯域で調整データ収集プロセスを繰り返します。

   注：PCの無線帯域を選択することが困難な実稼働環境では、11b/gまたは11aのみをアクティブにして特定の調整SSIDを定義することをお勧めします。

2. 無線帯域ごとに、それぞれラップトップを装備した最大 5 台のクライアントを使用して調整を実行します。各ラップトップには Cisco AIR-CB21AG を装備し、それぞれ専用の帯域を使用するインフラストラクチャに関連付ける必要があります。各調整クライアントは、独立して稼動できます。

調整を実行する前に、複数の事前設定手順が必要です。

1. 実稼動環境で、スタッフや作業者にプロセスについて通知します。これにより、割り込みは減り確度は向上します。フォークリフトを操作している製造工場では、とりわけ、事故のリスクを低減してください。

2. コントローラ上または調整を実行する AP 上のダイナミック RRM AP 電力モードをディセーブルにします。

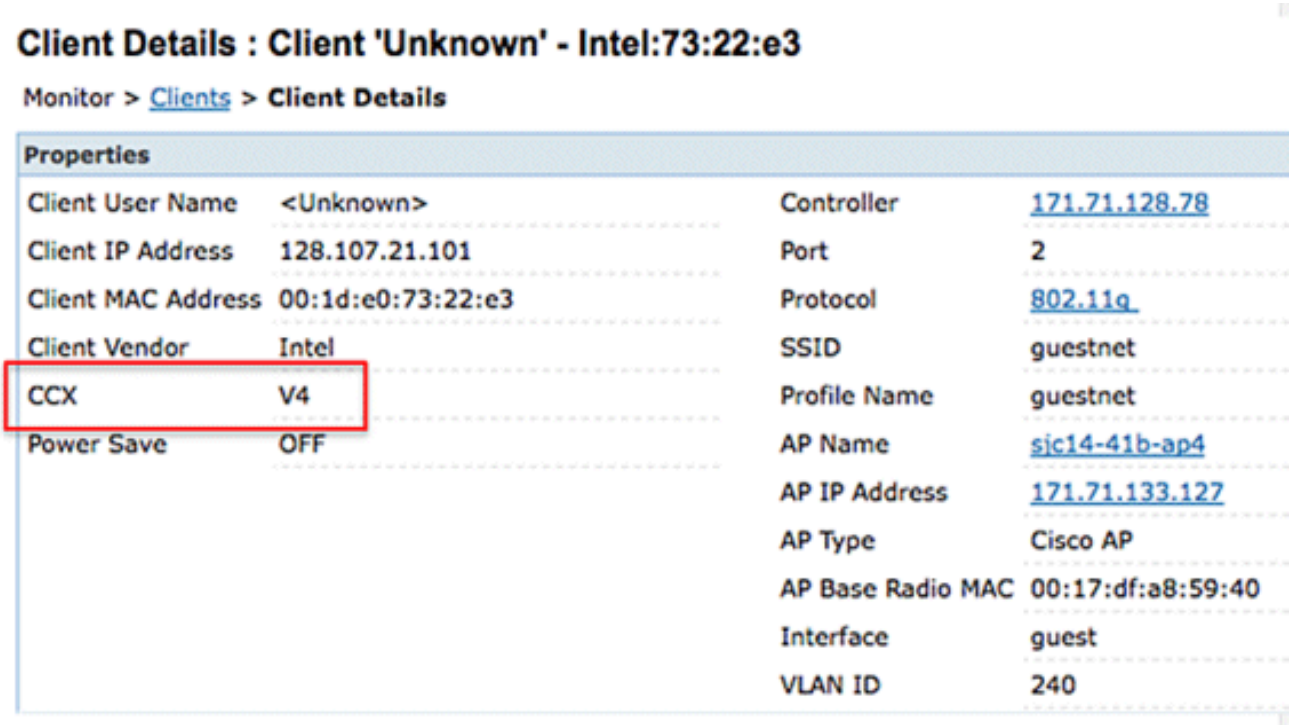
3. WCS 上のマップが拡大または縮小されており、正しいアンテナの種類、方向、および高さ

を指定して AP が適切に配置されていることを確認します。

4. 調整に使用する PC またはデバイスは、処理するマップ上に配置されている 1 つの AP と関連付けられています。

5. 調整に使用するワイヤレス クライアントは CCXv2 以上である必要があります。最適な結果を得るには CCXv4 をお勧めします。クライアント用の CCX バージョン情報は、WCS で参照できます（図 18 を参照）

   図18：クライアントのCCXバージョンの確認



6. Cisco Secure Services Client（CSSC）を使用して調整を実行しないでください。

7. 1 つのフロア マップで 50 個以上のデータ ポイントを収集する必要があります。

8. 調整モデルを作成し、このモデルをフロア マップに適用した後で、WCS を MSE に同期する必要があります。

複数階のビルの場合は、調整データ収集は、一度に 1 つのフロアで実行する必要があります。フロア間における RF 波の漏出により、隣接するフロア上の AP を調整クライアントが検出したり、検出されたりする可能性があるため、一度に 1 つのフロアで調整データを収集することで、MSE でフロアごとの調整データが混合するリスクを最小化します。

CCXv2 以上と互換性のあるクライアントを WLAN インフラストラクチャと関連付け、WCS で調整クライアントとして指定する場合は、調整したフロアに含まれているアクセス ポイントを処理するすべてのコントローラのロケーション調整テーブルに、クライアントの MAC アドレスが挿入されます。最初の挿入は、調整クライアントの MAC アドレス、調整キャンパス、ビル、およびフロアの指定直後に行われます。収集したデータ ポイントを保存するごとに、クライアントの MAC アドレスは、コントローラのロケーション調整テーブルから削除されます。以降、データ ポイントが保存されるごとに、クライアントの MAC アドレスはコントローラのロケーション調

整テーブルに一時的に再度挿入され、その後、すぐに削除されます。このプロセスは、収集されるデータ ポイントごとに繰り返されます。

CCXv2 以上のクライアントの MAC アドレスが WLC のロケーション調整テーブルにある場合は、ユニキャスト無線測定要求がこのクライアントに送信されます。通常動作中に、互換性のあるクライアントのロケーション確度の向上にブロードキャスト無線測定要求が役立つのと同様、一定の短い間隔（4 秒）で発行されるユニキャスト無線測定要求により、互換性のある調整クライアントが高い頻度でプローブ要求を送信することになります。CCX 無線測定要求および CCXv2 以上のクライアントを使用すると、関連付けの解除と再関連付けをクライアントに継続的に行わせることなく、これを実現できます。これにより、ネットワークの調査の一貫性と信頼性が高くなり、調整クライアントの動作がよりスムーズになります。これは、調整データ収集 GUI を使用して WCS と対話するワークステーションとしてクライアントを使用する場合には特に顕著になります。

調整モデルがフロアに適用されて、フロアの減衰特性がより正確に表現されます。一般的な減衰特性を多くのフロアで共有している環境（図書館など）では、調整モデルを 1 つ作成して、同一の物理レイアウトおよび同一の展開を持つフロアに適用できます。

調整データは、2 つの方法のいずれかで収集できます。

- ポイント モード収集：調整ポイントが選択されて、一度に 1 つのロケーションについてカバレッジ エリアが計算されます（図 19 および 20 を参照）
- 線形モード収集：一連の直線状のパスが選択されて、パスをたどりながら計算が行われます。通常、このアプローチはデータ ポイント収集よりも高速です。また、データ ポイント収集を使用すると、リニア パスで見つからないロケーションに対するデータ収集を強化できます（図 21 を参照）。

この両方の方式を正式にサポートしていますが、ポイント モードの方が優れた結果を得られるため、ポイント モードを使用して調整することをお勧めします。

図19：調整：ポイントモード

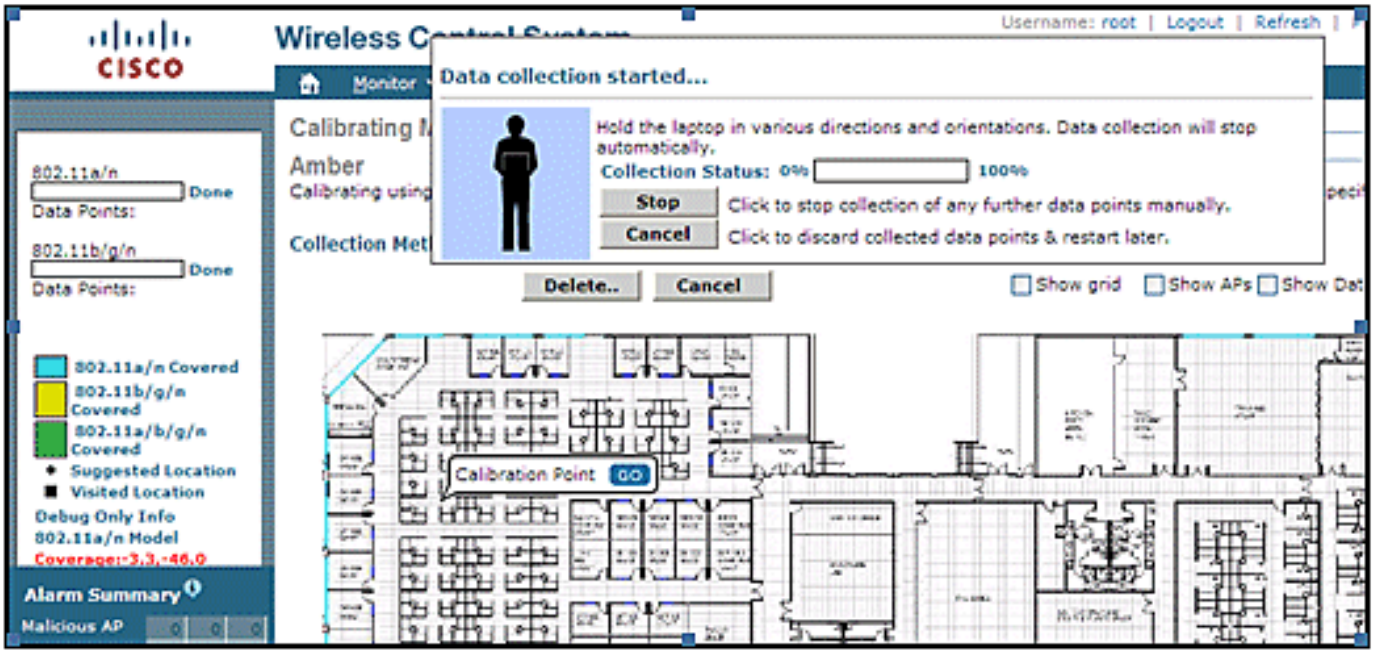


図20：ポイントモード：調整結果

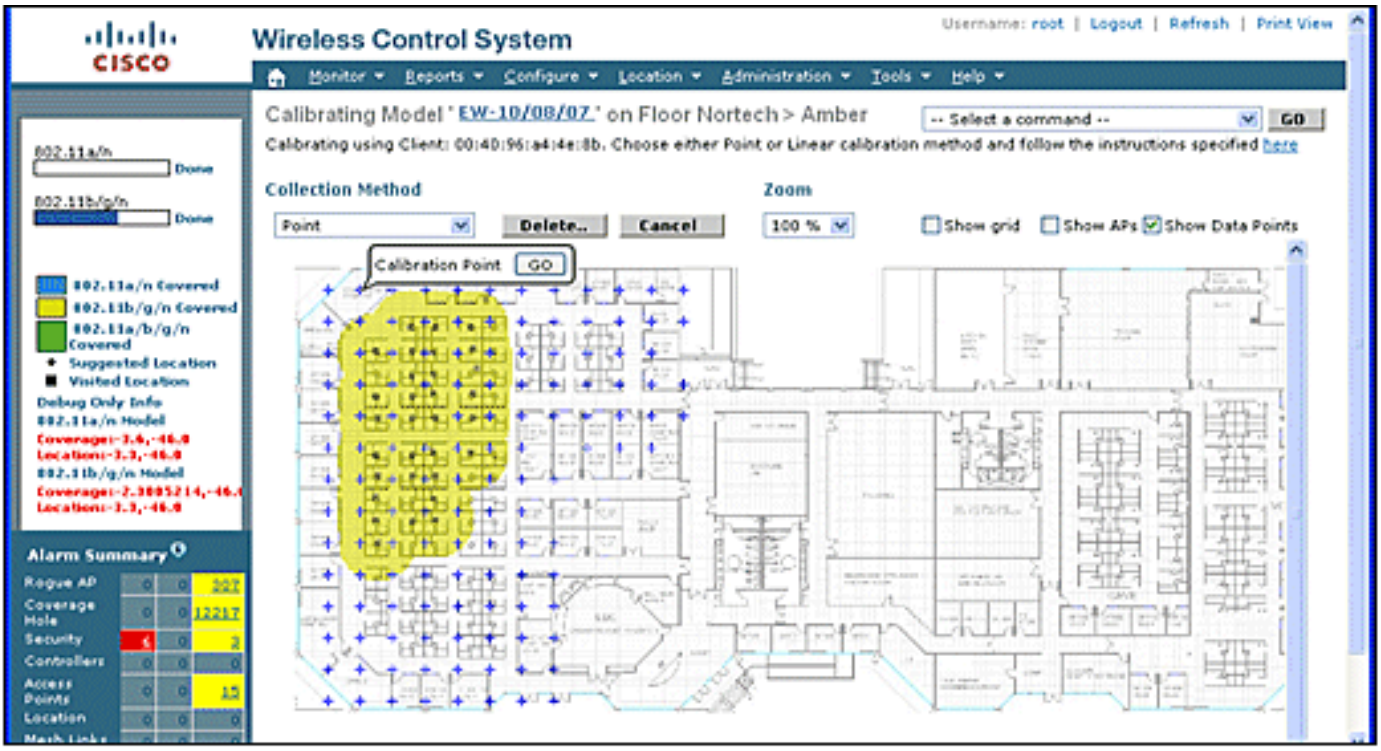


図21：調整：リニアモード

調整モデルは、クライアント、不正なクライアント、および不正なアクセス ポイントのみに適用できます。タグ用の調整には、AeroScout システム マネージャを使用します。

調整：タグ用 Context Aware Engine

MSEには、クライアントを追跡するロケーションエンジン（前の項で説明したシスコエンジン）と、タグを追跡するロケーションエンジン(AeroScout)の2つのエンジンがあります。エンジンごとに個別の調整モデルがあるため、タグの調整はまた別のプロセスになります。

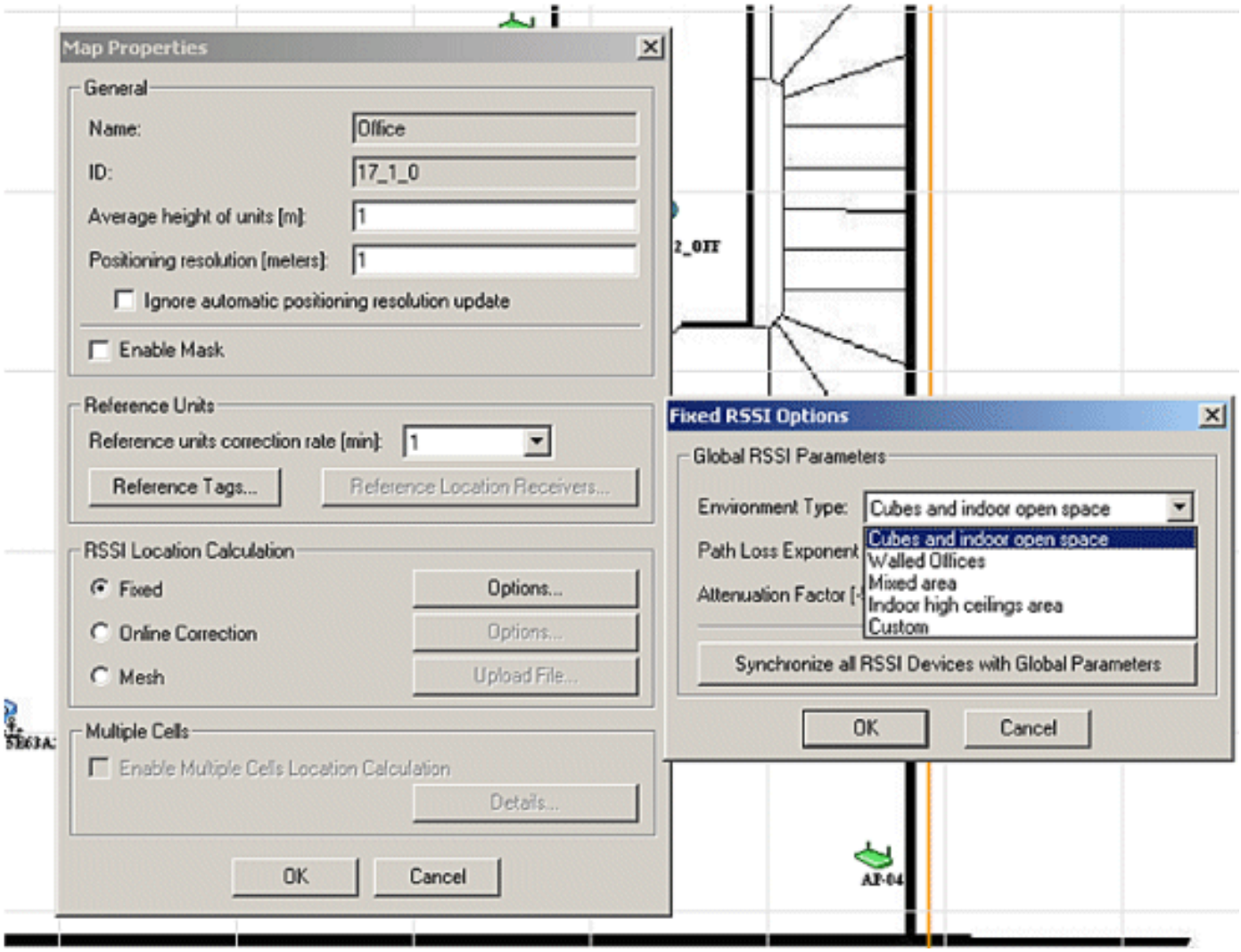
AeroScout エンジンでは、インポートしたすべての WCS マップについて、通常のオフィスのデフォルト RF パス損失モデルを使用します。このモデルがご使用の環境に当てはまらない場合は、ロケーションの確度を高めるために、マップまたはセルごとにデフォルト モデルを変更する必要があります。

AeroScout システム マネージャ：デフォルトのパス損失モデル（PLM）設定を変更するには、AeroScout システム マネージャ アプリケーションをインストールして実行する必要があります。ダウンロードおよびインストールについては、AeroScout Documentation を参照してください。

システム マネージャ アプリケーションを起動してから、MSE エンジンにログインし、変更する必要のある実際のマップ フロアに切り替えます。プルダウン タブを使用し、[Configuration] > [Map] > [Properties] に移動します。図 22 に示すように、[RSSI Location Calculation] オプションを使用すると、4 つの定義済みモデルで表される物理仕様に適した固定環境タイプを選択できます。モデルを選択してから、選択したフロアに適用します。[OK] タブまたは [Synchronize all RSSI Devices with Global Parameters] オプションを使用します。このオプションでは、同じモデルが既存のすべてのマップに新しいデフォルト モデルとしてプッシュされます。

注：5番目のオプション「Custom」は、AeroScoutまたはシスコテクニカルサポートから要求された場合にのみ使用する必要があります。

図22:AeroScout Systems Managerで使用可能なモデル



調整方法：個々のタグを静的基準デバイスとする複数のオプションがあり、定期的または 1 回限りの記録を実行する場合は、マップまたはセルごとの精度の高いモデルの分析および計算にこのオプションを使用できます。

基準タグ：これは、資産の追跡に使用される標準タグです。唯一違いがあるとすれば、設定にあります。通常、基準タグでは、定義された測定間隔に対して速いビーコン周期を使用します。

基準タグは、図 23 に示すように MAC アドレスで定義でき、セルまたはマップ上に直接置かれて、青色の錨付きタグによって示されます。マップ上を右クリックすることにより、座標を手動で入力できます。[Map Properties] > [Reference Units] の下の基準タグの選択ボックスで、ロケーションの動的適応に使用する基準タグをイネーブルにする必要があります（図 22 を参照）。この調整方法は、TDoA を対象に記述されています。

図23：参照タグプロパティ

ワン クリック記録：お勧めの調整方法として、ワン クリック記録操作があります。この方法では、タグのグループを定義し、事前に設定した短い時間の間、このグループをマップ上に配置します。記録が開始され、キャプチャされたデータは、タイムスタンプとマップ ID に基づいて MSE 上に直接保存されます。

タグの基準グループは、密な状態で小さいキューブまたはポール上に取り付けた場合に、最良の結果が得られます。グループの場所を変更してマウスを 1 回クリックして記録を再開すれば、同じマップ上で同じグループの場所を変更して手順を複数回反復できます。または、同じマップ上に複数のグループを定義し、1 回のシーケンスで記録することもできます。

図24:AeroScout Systems Manager Tools

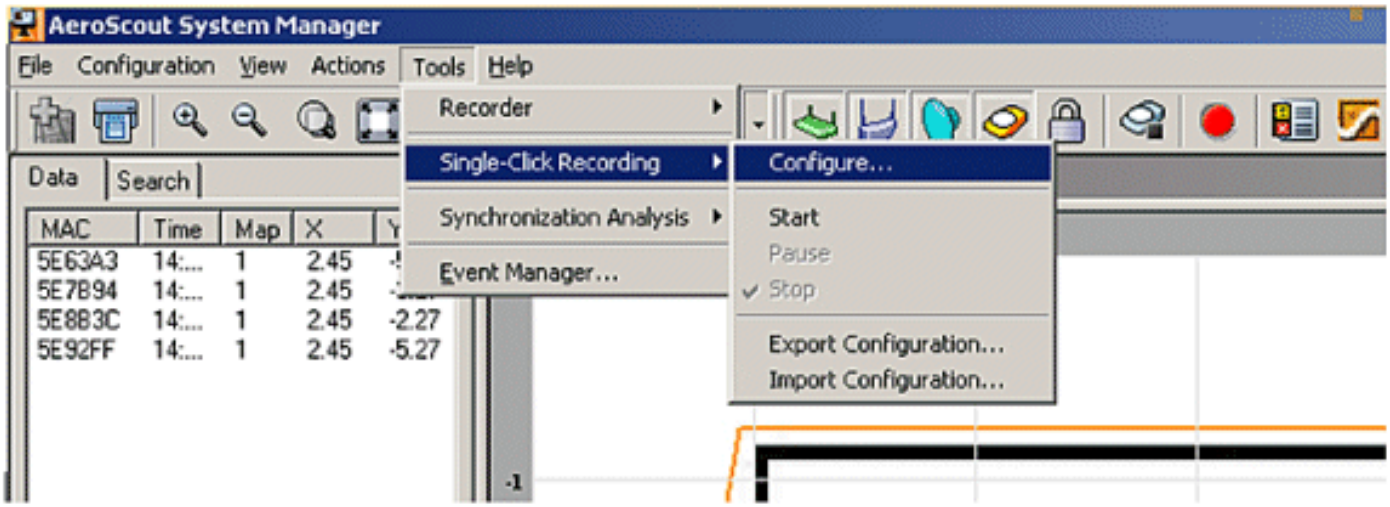
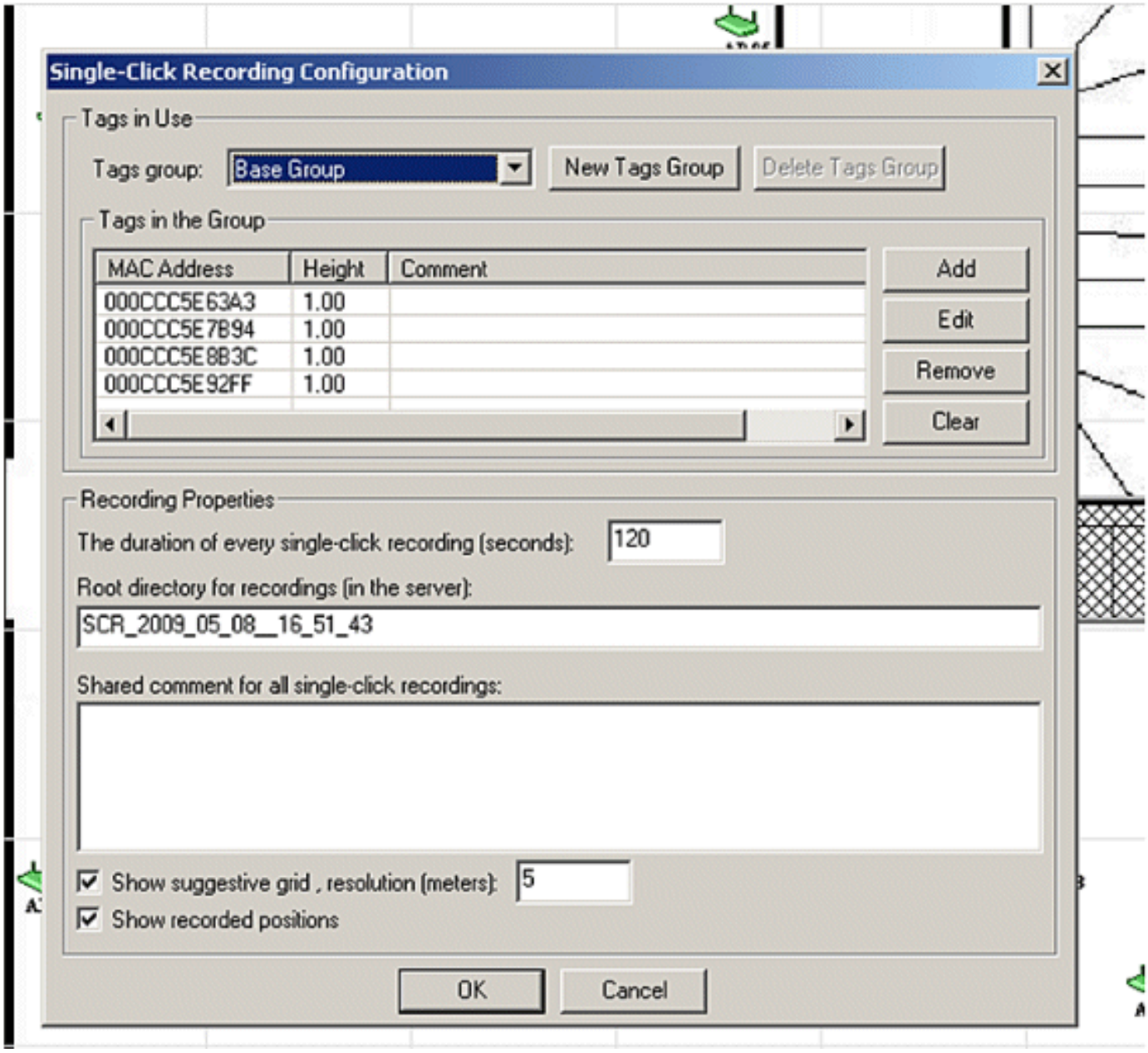


図25：ワンクリック記録の設定



この方法を実行するには、図 24 および 25 に示すように、[Tools] > [Single-Click Recording] の下にある設定情報を入力します。デフォルト値が適切でない場合は、[Recording Properties] を変更できます。記録したデータは、日時に基づいて、自動的にサブディレクトリに保存されます。

アナライザ ツール：ワン クリック記録データを調整に使用する前に、このデータを表示してメッシュ ファイルに変換する必要があります。MSE 上に保存されている、記録されたデータ ファイルは、システム マネージャを使用して、システムにエクスポートする必要があります。エクスポート先のシステムでは、メッシュ ファイルを作成する前に、必要に応じて、アナライザ ツールを使用して、記録されたデータを表示および変更できます。結果として作成されたメッシュ ファイルを MSE にインポートし直します。MSE では、アップロード ファイルの選択と一緒に RSSI ロケーション計算メッシュを選択して、マップ プロパティにこのファイルを適用できます。

設定情報および調整プロセスの詳細については、AeroScout Documentation を参照してください。

AeroScout Documentation の「AeroScout Mesh File Generation」を参照してください。

励振器（チョークポイント トリガー）テクノロジー

励振器は、資産タグが励振器の近傍に入ったときに、資産タグをトリガーして動作を変更させる、近傍通信デバイスです。この動作の変更によって、RFID タグに固有識別子を送信させたり、タグに内部設定またはステータスを変更させたりすることができます。チョークポイント トリガーの主要機能の 1 つとして、資産タグが特定のエリアに入ったあるいは出たことを MSE に示すように、資産タグに働きかけることがあります。チョークポイントとは、接続されたリージョン間の通路の入口または出口のポイントです。一般的なチョークポイントとしては、出入口、廊下、および階段室があります。屋内チョークポイント ロケーションには、連絡口となっている入口または出口が含まれます。

励振器では三角測量を使用しないため、3 台以上の AP による信号の検出を必要としません。

励振器では、タグ内での動作の変更を行うことで、タグ付き資産がチョークポイント エリアに入ったあるいは出たことをロケーション システムに即座にアラートできます。RFID タグは、次に、チョークポイント トリガーの ID を Cisco UWN インフラストラクチャに送信します。タグ パケットに格納されたチョークポイント情報は、MSE では、RF フィンガープリントのロケーション座標を上書きする情報となり、所定の期間はこの位置がチョークポイントの位置になります。

励振器およびタグの設定および調整のベスト プラクティスは、AeroScout Documentation の『Exciter and Tag Configuration Guide』で説明されています。

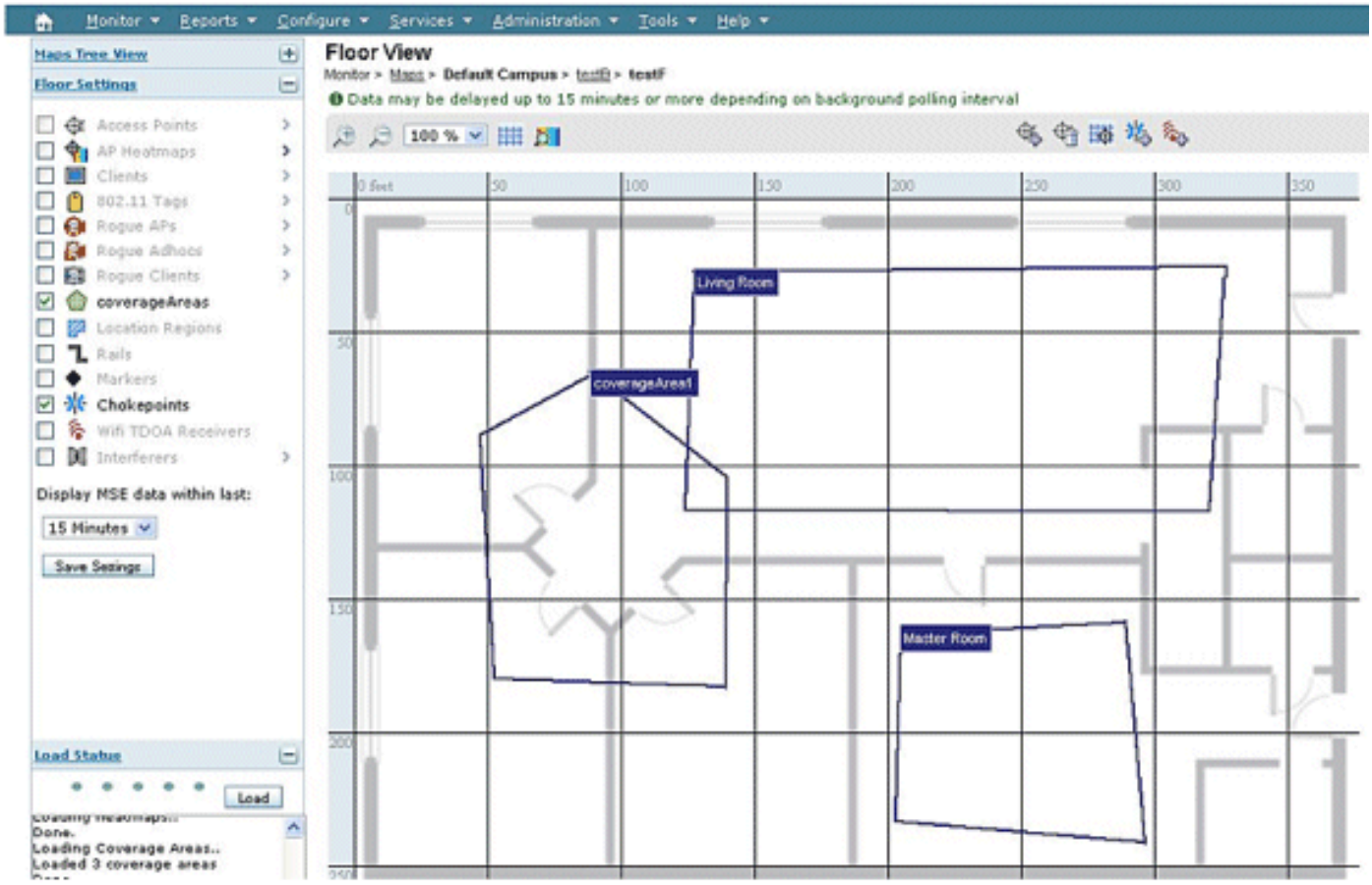
既存のデータおよび音声サービスがあるときの Context Aware 展開の考慮事項

既存のワイヤレス ネットワークが配備されているお客様のオフィス環境の場合に、Context Aware モビリティ ソリューションを追加で配備するには、展開全体を調べて、確度および発生するおそれのあるカバレッジ ホールを評価し直す必要があります。次の一般的なガイドラインに従う必要があります。

- ほとんどのオフィス環境で有効な最大アクセスポイント間隔：12 ~ 21 m（40 ~ 70フィート）
- すべてのクライアントの送信範囲に少なくとも 3 台の AP（冗長性のために 4 台の AP を推奨）が必要です。
- アクセス ポイントは、ロケーション カバレッジの対象のエリアを取り囲む必要があるため、周囲の AP を最初に配置します。
- 次に内部の AP を配置して、最小の -75 dBm に対するカバレッジの隙間を最小化します。
- 四角形のエリアでは、エリアの 4 隅を占める、最低 4 台の AP を設置する必要があります。
- 精度に影響する要因：APの配置、壁材、大きな移動体、RF干渉
- おそらくは、フロア空間をサブエリアに分割し、RF 信号を妨害する大型の障壁に対処するように、サブエリアを個別に設計する必要があります（図 26 を参照）。フロアに対して最大 50 個のカバレッジ エリアがサポートされています。カバレッジエリアのサイズは、通常

のロケーション範囲（10 m以下）より小さくすることはできません。

図26：複数のカバレッジエリアを示すWCSのマップエディタ



- AP は、できれば、囲まれたエリアの周辺部沿いと、その内部に配置します。
- AP は均等に分配させる必要があります。つまり、AP は、互いに比較的等距離である必要があります。
- AP を等距離で配置する場合であっても、AP の物理配置は直線状にならないようにする必要があります。
- WCS の Location Readiness ツールを使用して、フロア全体のカバレッジの効果を測定します。
- AP の分散状況による幾何学形状は、確度に影響します。
    - 正三角形で配置した場合の方が鈍角三角形で配置した AP よりも確度が優れます。
    - 正方形に展開した配置の方が長方形で配置した AP よりも良い結果を得られます。

図 27 は、802.11bg を使用する Cisco 7921G VoWLAN ハンドセットのセルのオーバーラップを示します。Cisco 7921G の場合、『Voice Over Wireless LAN デザイン ガイド』に記載されている推奨ベスト プラクティスでは、802.11bg を使用する場合 20 % 程度、802.11a を使用する場合 15 % 程度のセル間のオーバーラップが推奨されています。

データ アプリケーションの場合、パケット損失の影響は音声アプリケーションの場合ほど目立ちません。したがって、データ アプリケーションでは、VoWLAN 展開と同じレベルのセル間のオーバーラップを必要としません。ほとんどの場合、図 28 に示すように、最小の 10 % のセル間のオーバーラップがあれば、データ アプリケーションによる確実なローミングに十分です。高速データ アプリケーションや、音声とデータの機能を単一のデバイスで兼ね備えるアプリケーション（スマートフォンなど）では、データ設計ではなく VoWLAN 設計に似たセル間のオーバーラップを必要とすることがあります。

図27：セル間オーバーラップ：音声とデータの導入（セルのオーバーラップ20 %）

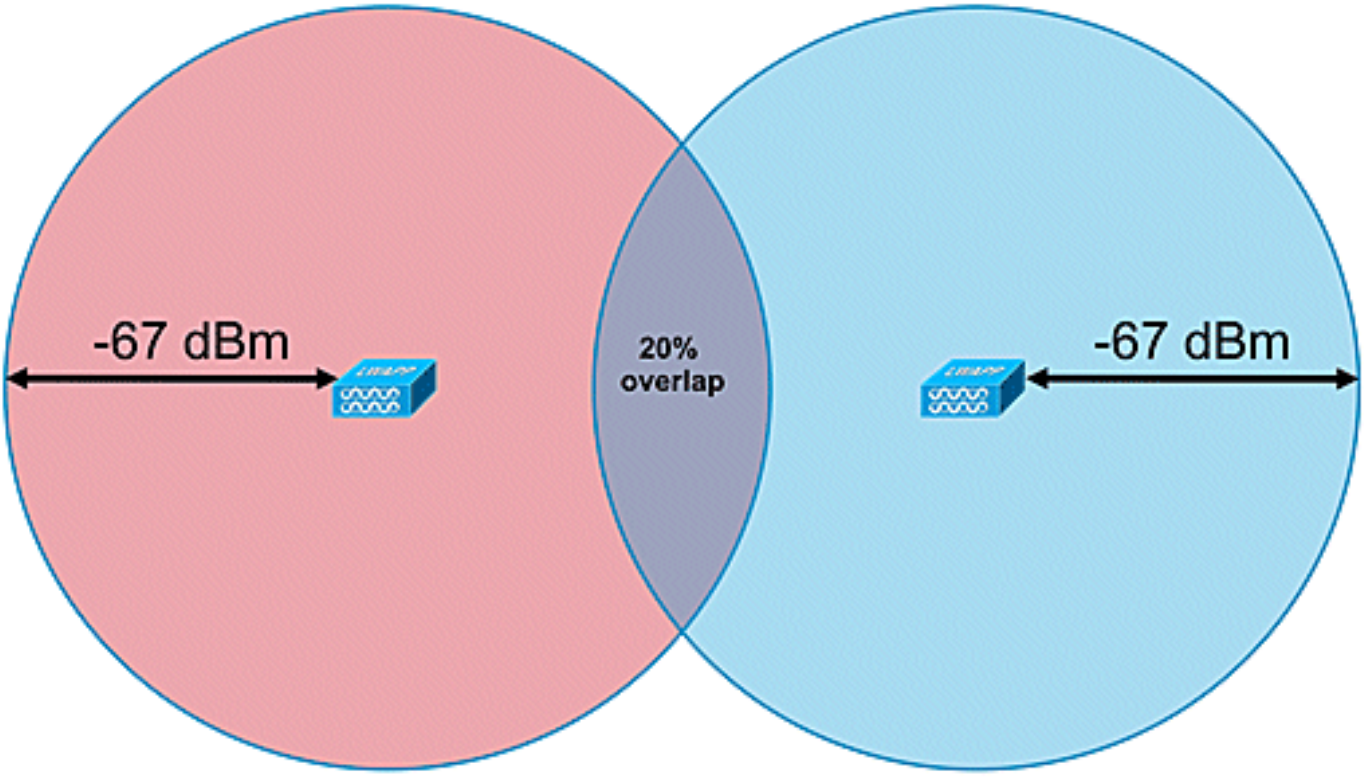
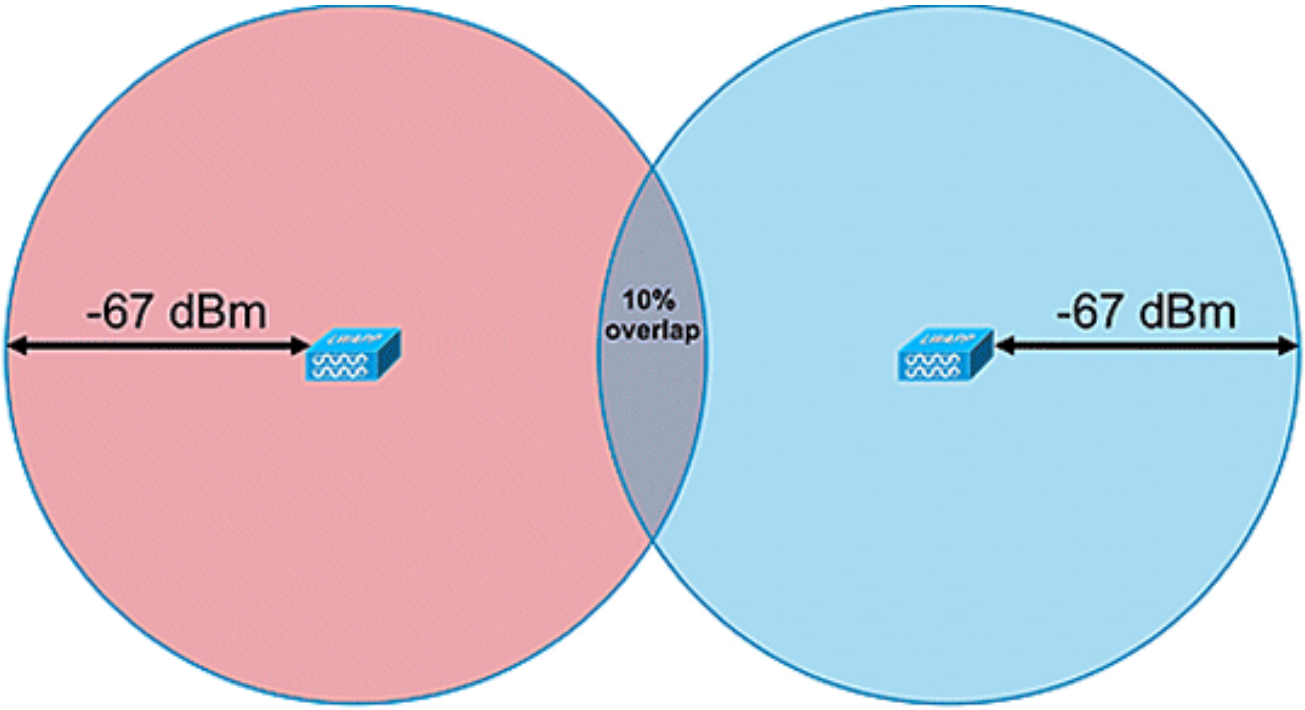


図28：セル間オーバーラップ：データ展開（セルのオーバーラップ10 %）



一般的なガイドライン：TDoA

TDoA ベースの展開では、最低 3 台の受信機を必要としますが、受信機を 4 台にすれば正確な結果を得られます。TDoA 受信機の密度については、次の一般的な規則があります。

- 屋外：平均密度は 1,900 ~ 4,700 平方メートル（20,000 ~ 50,000 平方フィート）ごとに 1 台の TDoA 受信機です。
- 広い屋内エリア：平均密度は 450 ~ 1,300 平方メートル（5,000 ~ 14,000 平方フィート）ごとに 1 台の TDoA 受信機です。
- 同期された発信源と TDoA 受信機の間の距離は、屋外展開の場合 150 m 以下です。
- 同期された発信源と TDoA 受信機の間の距離は、広い屋内の展開の場合 70 m 以下です。

TDoAに関する2つの重要な考慮事項：レシーバ密度の展開は、レシーバの同期とトラッキング対象デバイスのRFカバレッジのRx感度によって異なります。2 つ目の重要な考慮事項は、ロケーション受信機のカバレッジを十分にして、ロケーション エリア内のすべてのポイントで、ロケーション受信機が 3 台以上という、受容性のある密度にすることです。

特定のシナリオでは、広いエリアをサブエリアに分割する必要がある場合があります。たとえば、広い倉庫を分ける壁が 1 つある場合は、2 つのサブエリアとして設計する必要があります。同期ソースと Wi-Fi TDoA 受信機の間でライン オブ サイトを維持した場合に、最良の結果が得られます。

Wi-Fi TDoA 受信機の配置の場合は、さらに次のガイドラインが適用されます。

- Wi-Fi TDoA 受信機は、外周に沿って等間隔に設置する必要があります。
- エリアのサイズによっては、周辺部の受信機の境界内に Wi-Fi TDoA 受信機をさらに必要とすることがあります。

- TDoA 受信機は等間隔で配置し、正三角形（3 台の Wi-Fi TDoA 受信機を使用する場合）またはポリゴン（4 台以上の Wi-Fi TDoA 受信機を使用）の形に並べる必要があります。

Wi-Fi TDoA 受信機アンテナの場合は、ダイバーシティ アンテナを使用して、マルチパスの問題に対処します。カバーするエリアの周辺部に沿って設置する Wi-Fi TDoA 受信機は、カバーするエリア内の受信のみに集中するために、指向性アンテナを含む必要があります。周辺部の隅には 90 度の指向性アンテナを使用し、周辺部に沿った部分には 180 度の指向性アンテナを使用します。周辺部で囲まれた内部に配置されている Wi-Fi TDoA 受信機には、全方向性アンテナを使用する必要があります。受信機のアンテナは、同期ソース（できればライン オブ サイト）と該当エリアの両方を指す必要があります。

アンテナは、コンクリート壁、大型の金属製の物体、密集する樹木で覆われたエリアなどの障害物によって妨害されないエリアに設置する必要があります。アンテナは、カバーするエリアに向けてのライン オブ サイトが可能な限り良好な状態で設置する必要があります。追跡対象資産の表面から 3 ~ 5 m（10 ~ 16 フィート）高い場所に取り付けることをお勧めします。環境が原因でこれを実現できない場合は、カバレッジ パターン、つまり仰角パターンを適宜調整する必要があります。通常のアンテナの仰角はほぼ 35 度です。周辺部に沿いの高い位置に配置したアンテナでは、カバレッジ エリアに向けて仰角を傾けてください（上昇分を補うために最大 30 度下に向ける）。

詳細については、『AeroScout TDOA Deployment Guide』を参照してください。

有線ロケーション

6.0 ソフトウェア リリースでは、Context Aware ソリューションによって、ワイヤレス デバイスと有線（イーサネット）デバイスの両方を追跡できます。有線ロケーションの場合、MSE には、スイッチおよびスイッチ ポートの CIVIC ロケーション情報を収集および保守する機能が用意されています。Catalystスタッカブルスイッチ（3750、3750-E、3560、2960、およびIE-3000スイッチ）、スイッチブレード（3110、3120、3130、3040、3030、および3020）およびCatalyst 4Kシリーズ(WS-C49)に接続されているイーサネット有線デバイスの場所を特定できますWS-C4948-10GE、ME-4924-10GE、WS-4928-10GE、WS-C4900M、WS-X4515、WS-X4516、WS-X4013+、WS-X4013+TS、WS -X4516-10GE、WS-X4013+10GE、WS-X45-SUP6-E、およびWS-X45-SUP6-LE)。有線ロケーションの場合は、Catalyst 3KスイッチのIOS 12.2(50)SE、Catalyst 4KスイッチのIOS 12.2(52)SGという、各スイッチモデルに対応するIOSバージョンを使用します。有線ロケーション情報は、NMSP を介して、これらのスイッチから MSE に送信されます。

ロケーション情報は、IOS CLI を介してシスコ スイッチに設定されます。有線スイッチは WCS に定義され、MSE と同期されます。有線クライアントの詳細は、NMSP 接続を介して、ロケーション対応スイッチから MSE に送信されます。その後、Cisco WCS を使用して、有線スイッチおよび有線クライアントを表示できます。

civic 情報および緊急ロケーション情報（ELIN）のインポートおよび表示は、http://tools.ietf.org/html/rfc4776#section-3.4 で説明されている RFC4776 の仕様を満たしています。

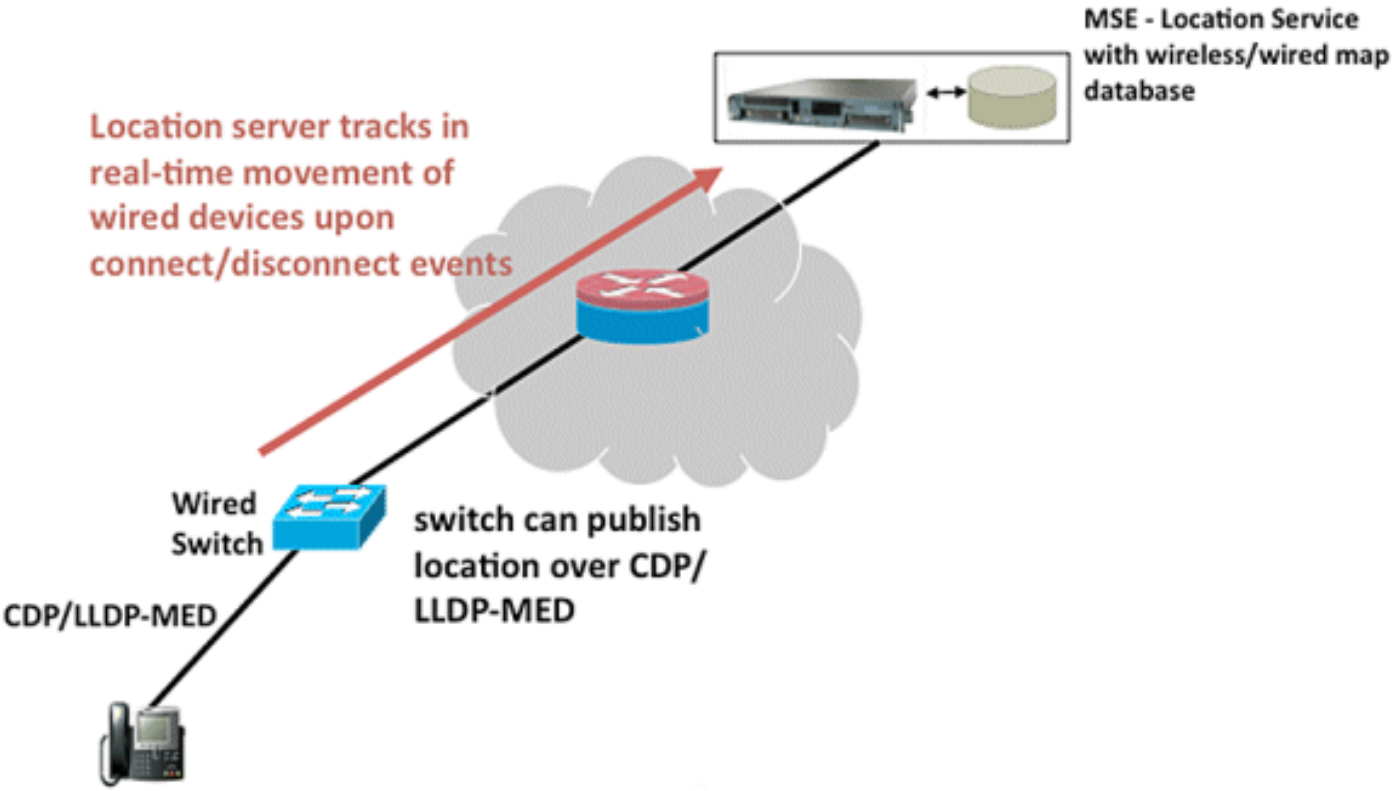
MSE では、有線クライアントのロケーション履歴を追跡するだけでなく、シャーシまたはエンドポイント デバイスのロケーションを処理する外部システムや、有線とワイヤレスのカテゴリをま

たいでクライアントを検索または追跡する外部システムで使用する SOAP/XML API も用意されています。図 29 を参照してください。

- スイッチは、シャーシおよびラインカードの口ケーションおよび UDI 情報を含む、接続されているデバイスのスイッチ ポート マッピングを MSE に報告します。
- MSE では、デバイスとシャーシの両方の通信情報と口ケーションをアクティブに追跡します。

注：現在、有線口ケーション機能には、フロアマップ上で有線クライアントを検索したり表示したりする機能はありません。

図29：有線口ケーションアーキテクチャ



必ず、手順に従って有線口ケーションを表示してください。

次に、スイッチ側の設定手順を示します。

1. スロット、モジュール、ポートの設定（1、0、20）を理解します。
2. 各スイッチモデルに該当する正しいIOSバージョン(Catalyst 3KスイッチではIOS 12.2(50)SE、Catalyst 4KスイッチではIOS 12.2(52)SG)を使用してください。
3. NMSP をイネーブルにします。
4. IP デバイスの追跡をイネーブルにします。
5. SNMP コミュニティに読み取りおよび書き込みアクセスを設定します。
6. Civic/ELIN 口ケーション識別番号を設定します。

7. スイッチ インターフェイスに識別子を割り当てます。

次に、WCS 上の設定手順を示します。

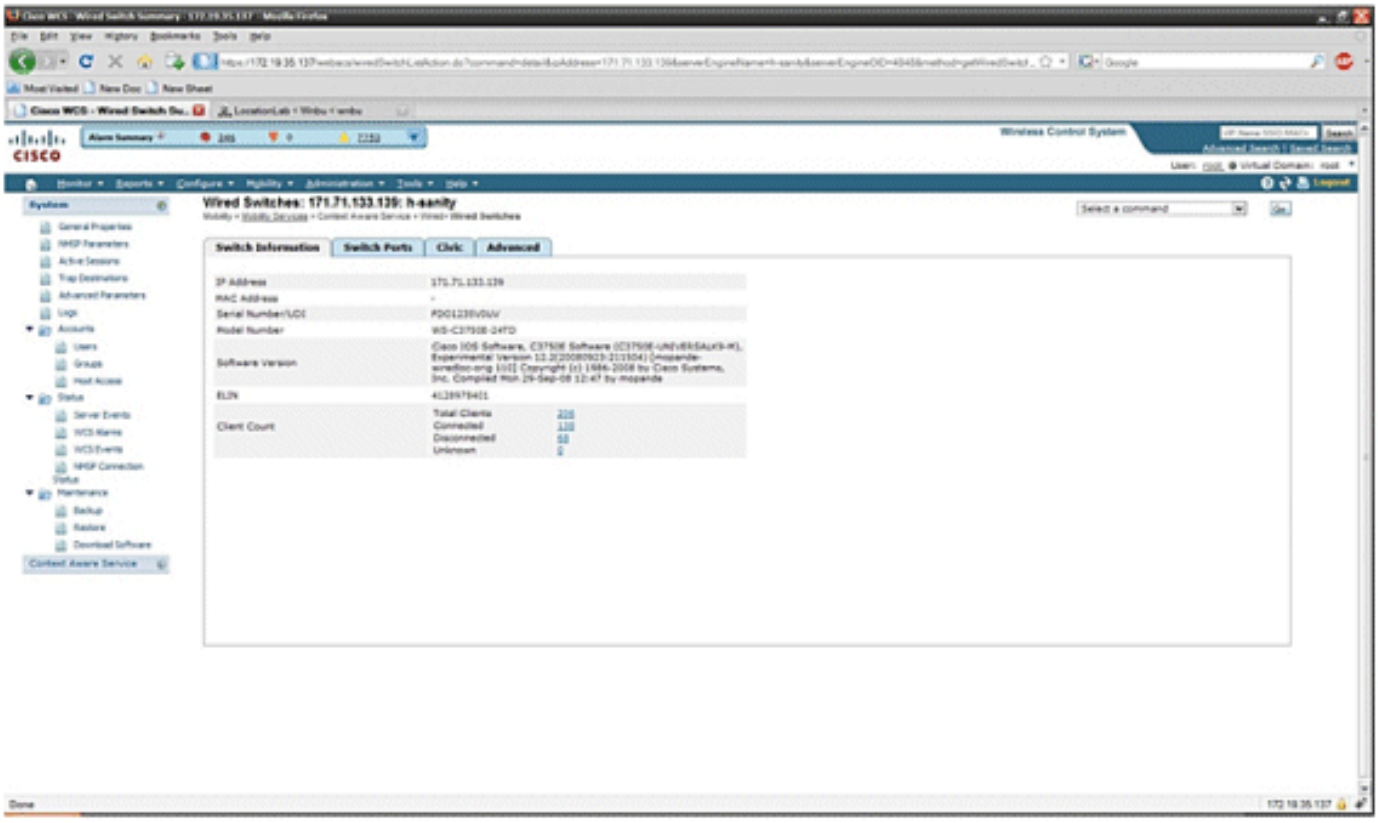
1. [Configure] > [Ethernet Switches] に移動します。
2. イーサネット スイッチを追加します。
    a. IP アドレスを追加します。
    b. [Location Capable] をイネーブルにします。
    c. SNMP コミュニティ（読み取りおよび書き込み）を入力します。入力した SNMP コミュニティ ストリングは、Catalyst スイッチに割り当てた値に一致する必要があります。
3. [Services] > [Synchronize Services] > [Switches] に移動します。
    a. [Assign] をクリックして、優先する MSE に割り当てます。
    b. スイッチを選択し、同期します。
4. [Services] > [Mobility Services] に移動し、[MSE] をクリックします。
    a. [System] > [Status] > [NMSP Connection status] に移動します。
    b. スイッチごとにアクティブな NMSP ステータスを確認します。

スイッチおよび WCS 上で手順を完了すると、WCS 上に有線要素を表示できます。

- [Context Aware Services] の [Wired] の下にある [Wired Switches] をクリックします。
- スイッチのリストが表示されます。
- [Switch IP Address] をクリックして、詳細を表示します（図 30 を参照）。

注：WCSにWLCを追加するには、読み取り/書き込みSNMPアクセスが必要です。WLC では、SNMP 読み取り専用アクセス モードの MSE キー ハッシュを受け取りません。

図30：有線スイッチ – スイッチ情報



- スイッチ ポートおよび Civic 情報（図 31 ～ 33 を参照）を表示することや、ポート IP アドレス、スロット番号、モジュール番号、およびポート番号のリスト順（昇順、降順）を変更することもできます。対応する列見出しをクリックします。

図31：有線スイッチ – スイッチポート情報

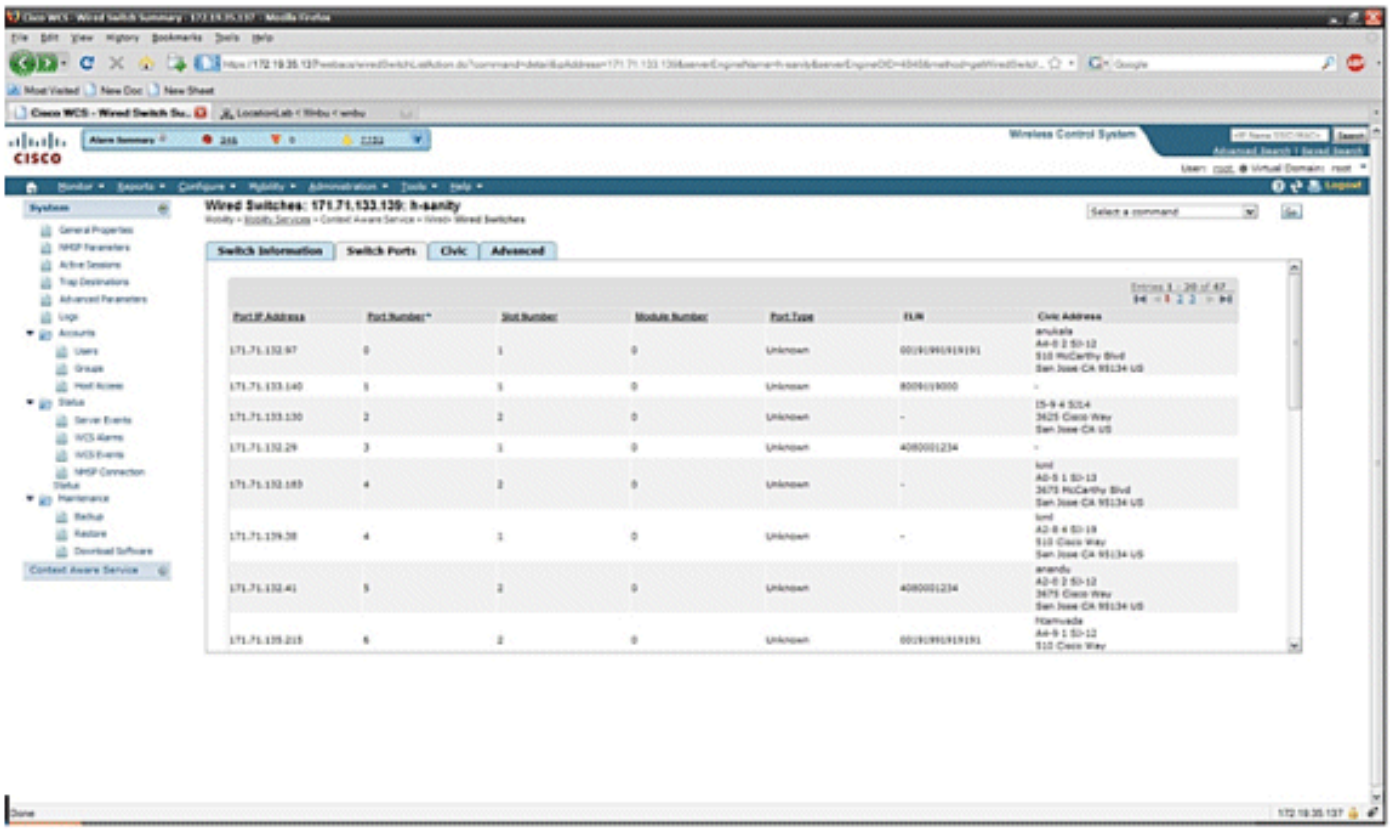
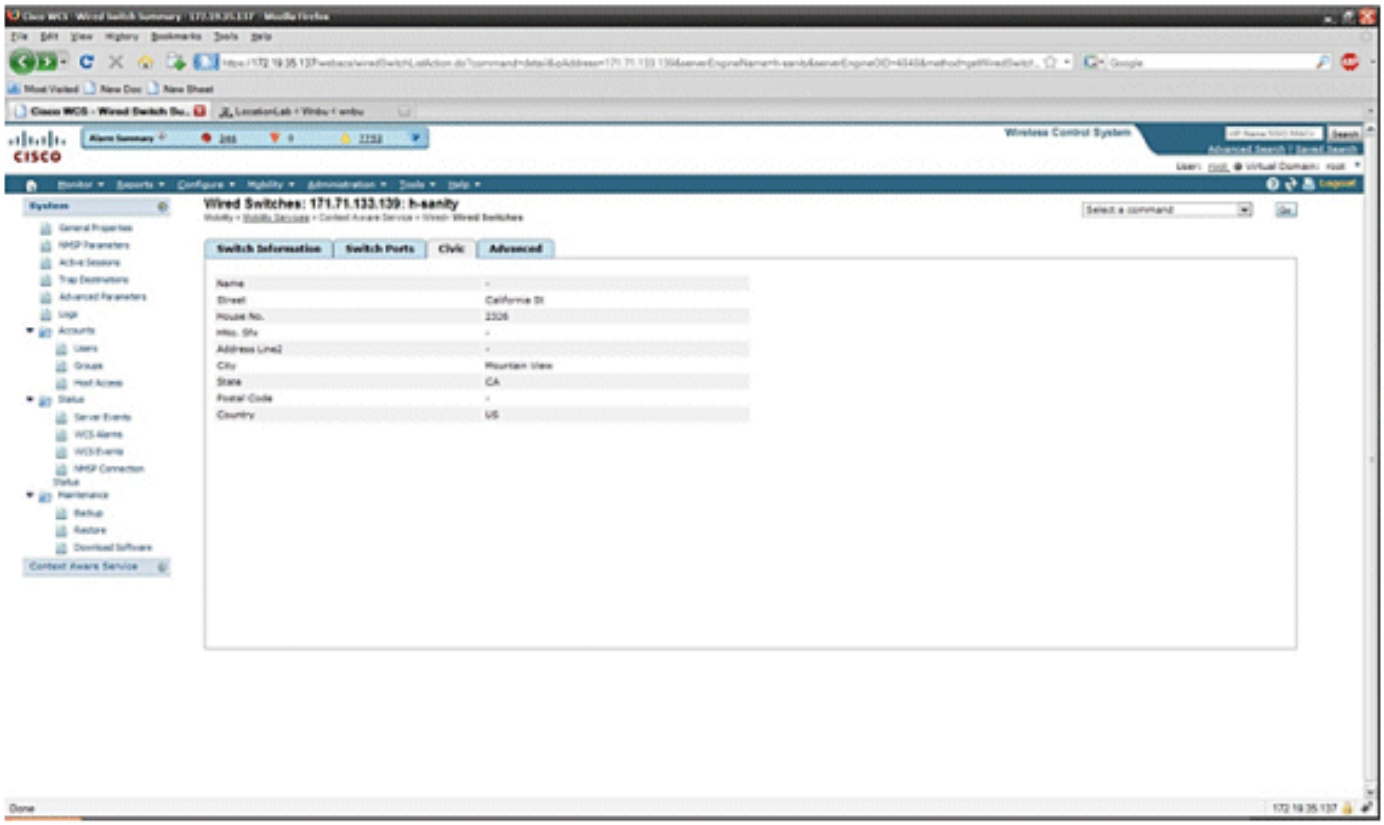
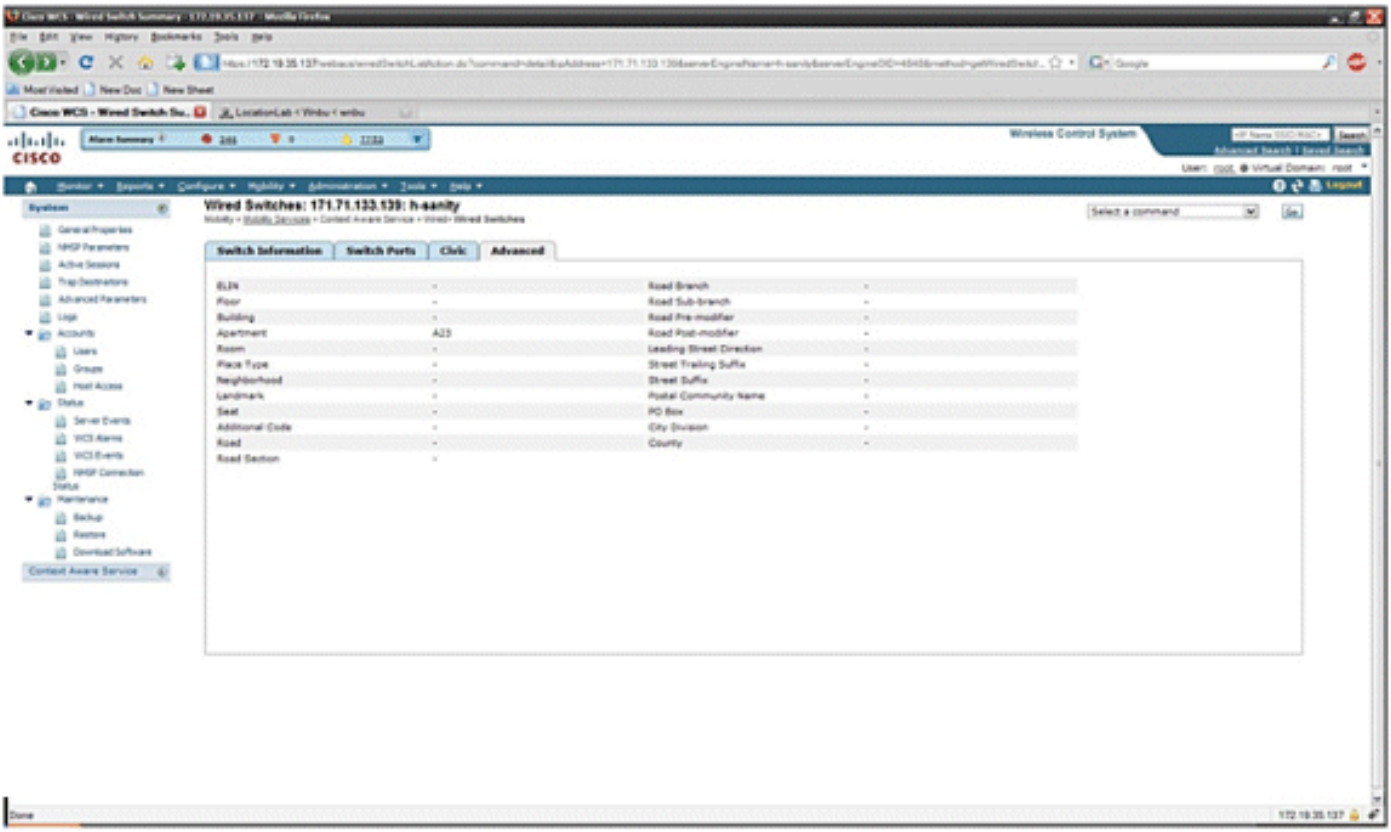


図32：有線スイッチ – Civic情報



[Advance] タブには、付加的な Civic 情報が表示されます。

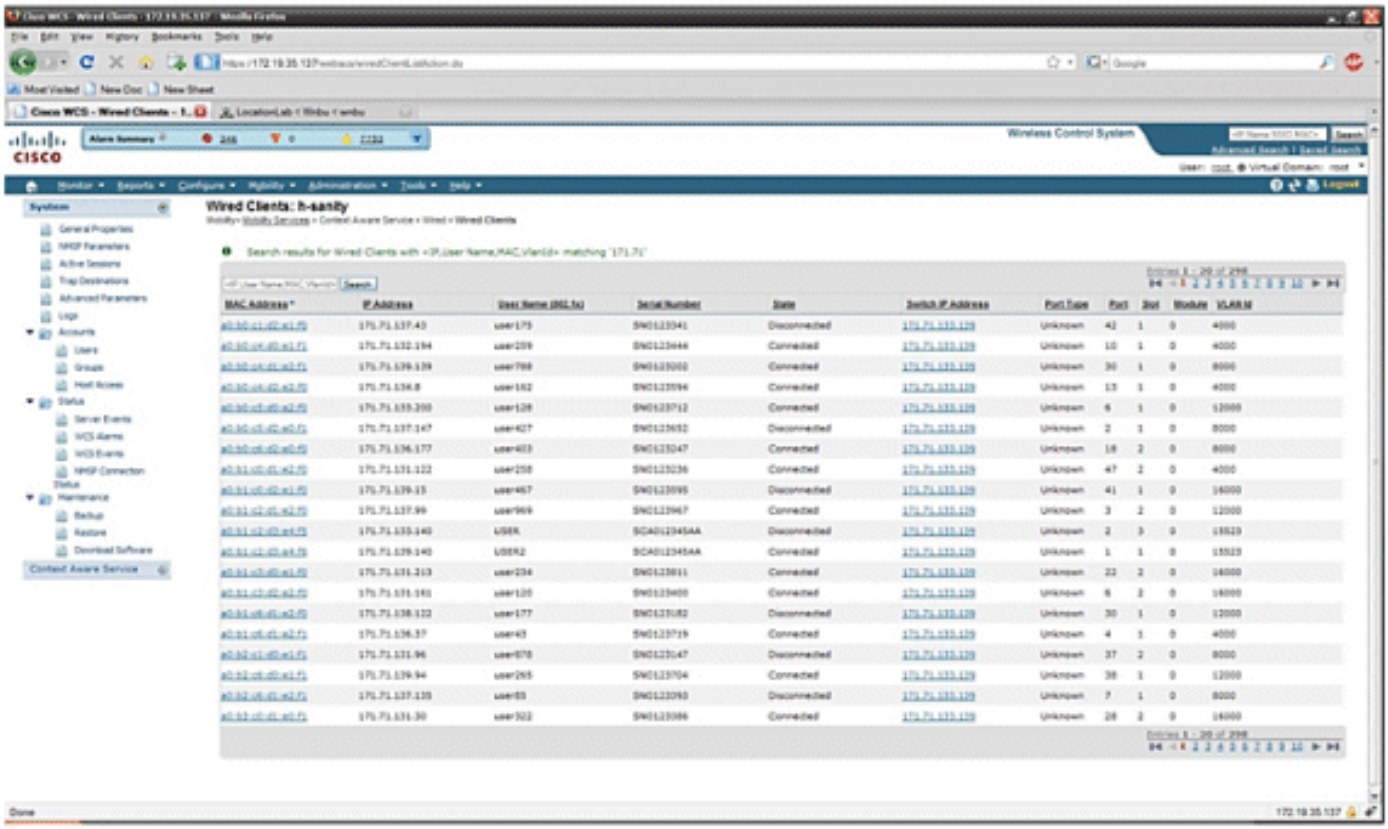
図33：有線スイッチ – 詳細情報



[Wired Context Aware Service] > [Wired] > [Wired Clients] の下の [Wired Clients] をクリックすると、すべてのスイッチから参照可能な有線クライアントを表示できます。

有線クライアントは、IP アドレス、IP アドレスの一部、MAC アドレス、MAC アドレスの一部、802.1x ユーザ名、ユーザ名、VLAN ID で検索できます（図 34 を参照）。

図34：有線クライアント – 検索結果

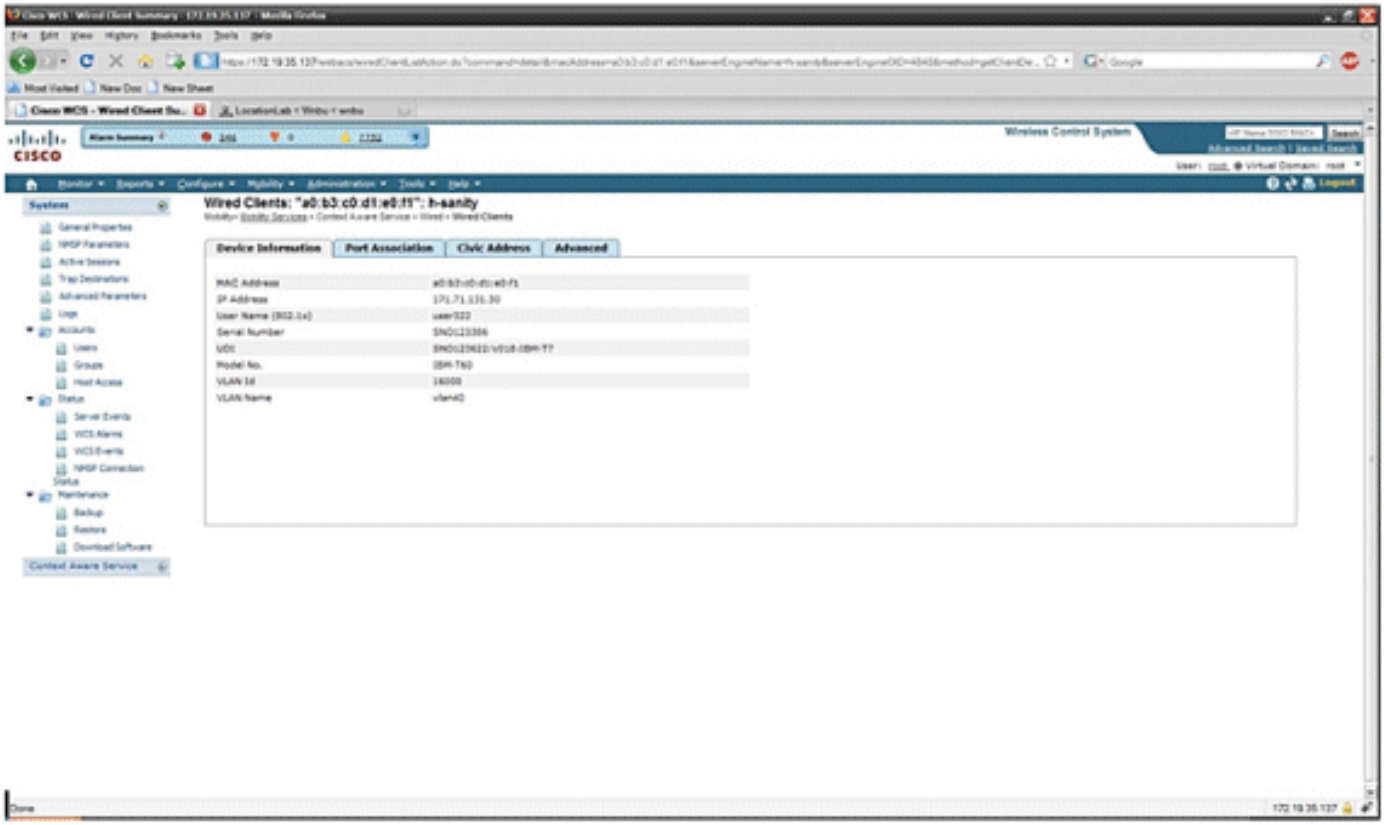


スイッチには指定された数のスイッチポートとクライアントがあり、ホストはこれらのポートで接続されます。個別のスイッチ ポートの口ケーションを設定した場合、そのポートに接続されているクライアントの口ケーションは、そのポート 口ケーションであると見なされます。

スイッチ（switch2）が別のスイッチ（switch1）のポート（port1 など）に接続されている場合は、port1 に設定されている口ケーションが、switch2 に接続されているすべてクライアントに割り当てられます。

対応するクライアントをクリックすると有線クライアントの詳細を表示して、デバイス情報、ポートの関連付け、civic アドレスなども取得できます（図 35 ～ 38 を参照）。

図35：有線クライアント – デバイス情報



有線クライアントが終端するスイッチ ポート、スロット、またはモジュールの物理ロケーション、クライアントのステータス（接続、切断、または不明）およびスイッチの IP アドレスを参照するには、[Port Association] タブをクリックします。

図36：有線クライアント – ポートアソシエーション情報

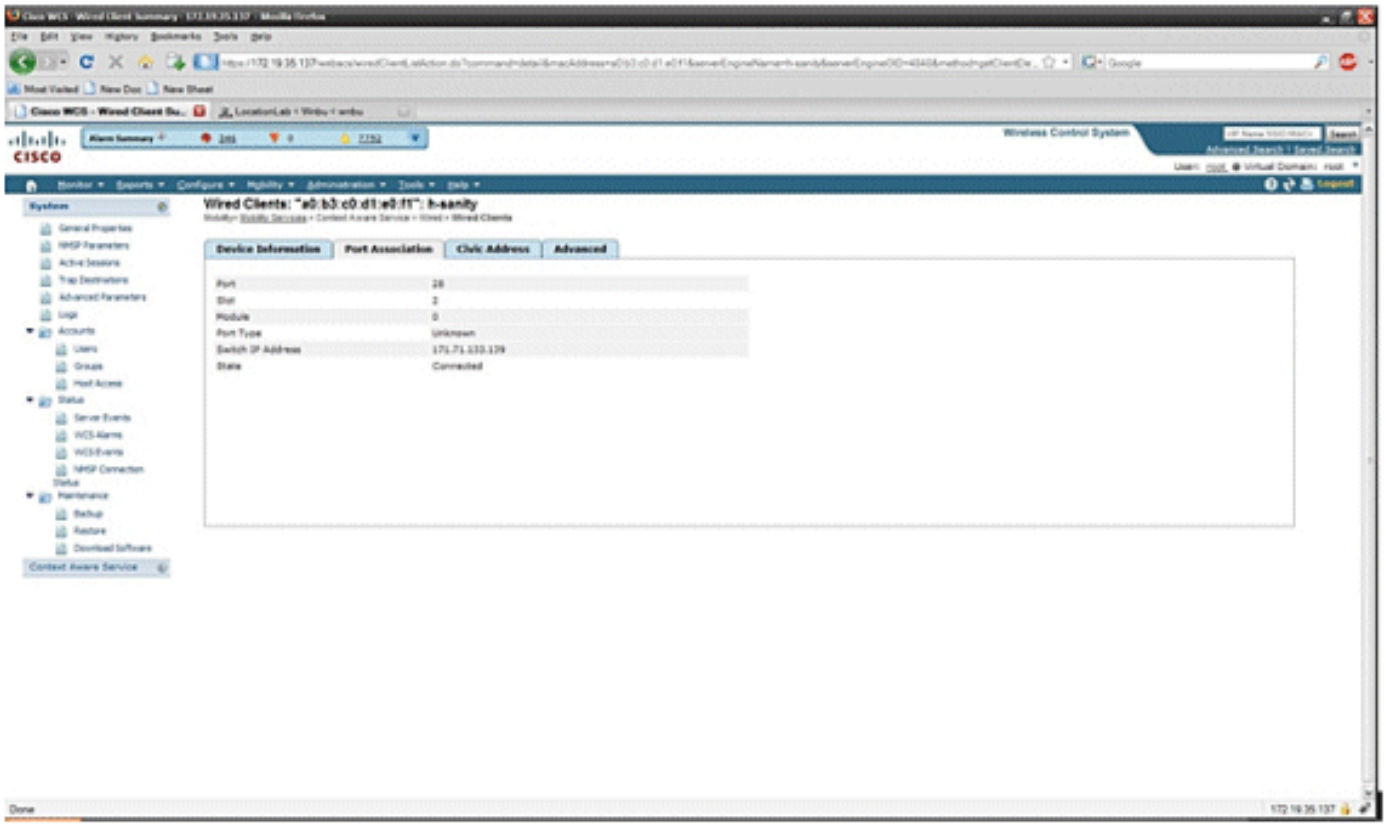


図37：有線クライアント – Civicアドレス情報

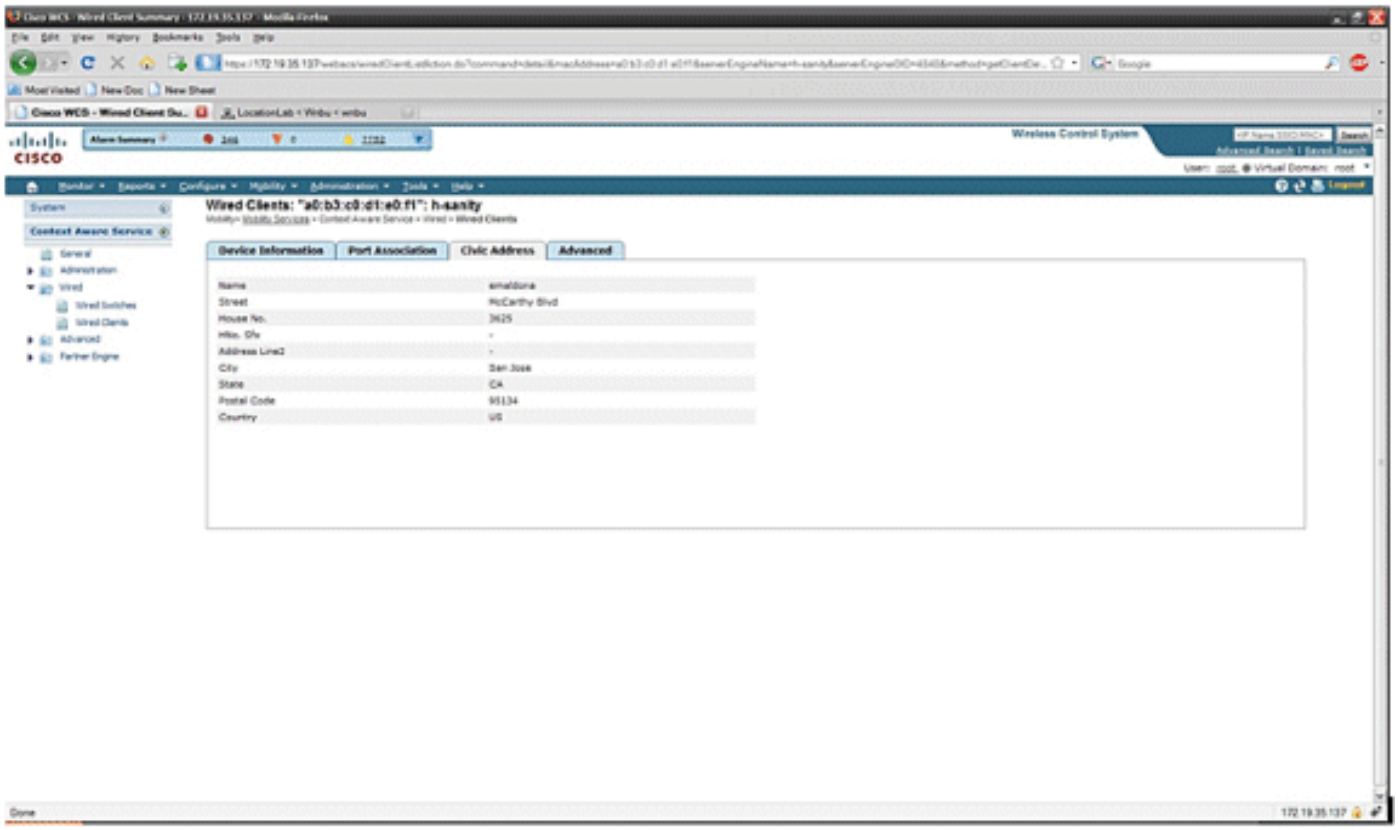
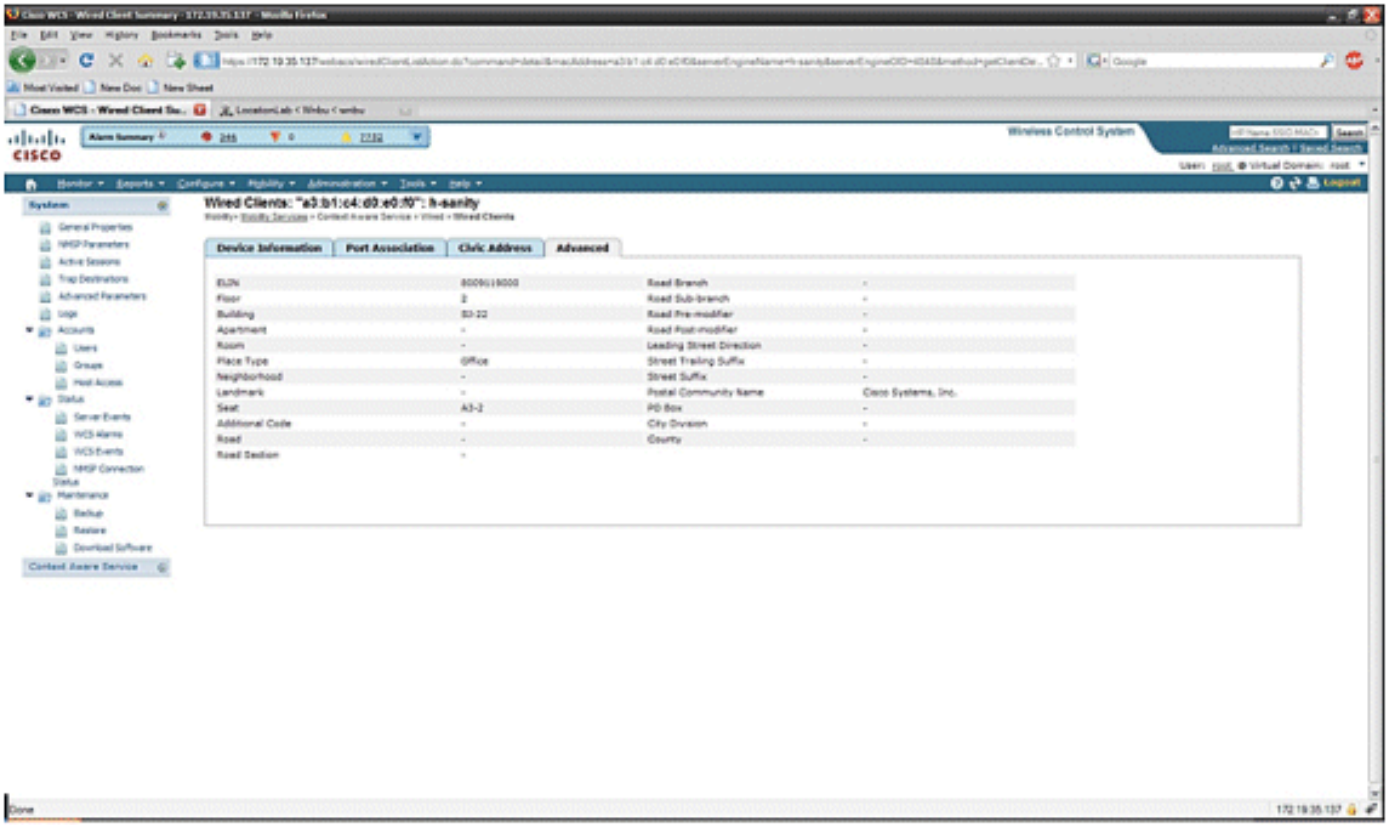


図38：有線クライアント – 詳細情報



セクション3:Context Awareネットワークの検証と改善

WCS 確度ツール

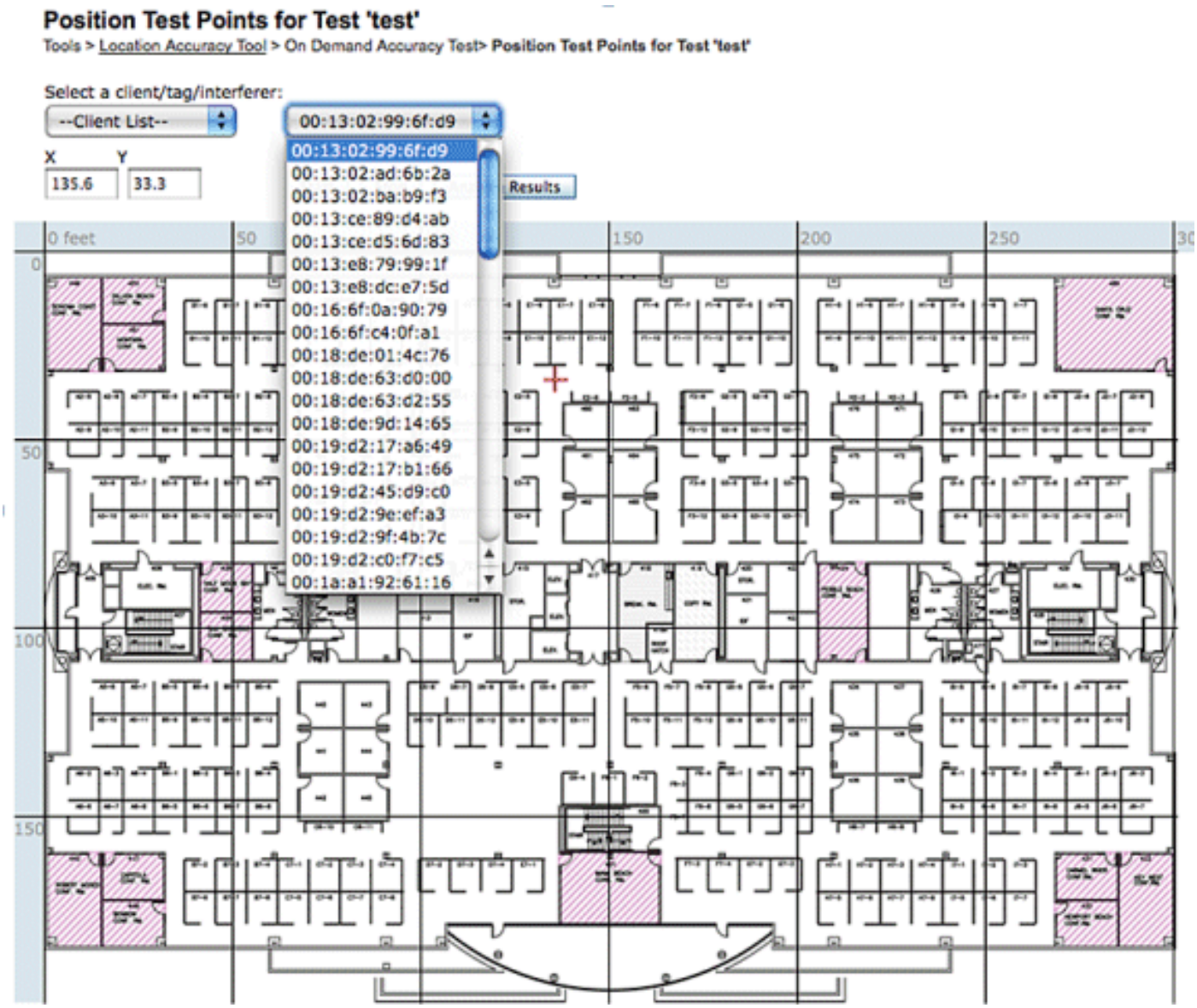
5.0 よりも前のリリースの WCS では、ワイヤレス ネットワークの確度をユーザが判別することは困難でした。Context Aware を展開した状態で、確度のレベルを定量化する標準的な方法はありませんでした。WCS 5.0 リリースでは、統合された確度ツールが導入されました。タグや Wi-Fi クライアントは、WCS 内でフロア マップ上のリファレンス ポイントに置かれます。時間と空間をまたがるさまざまなレベルの確度および誤差の分布を含む詳細レポートが WCS によって生成されます。

確度テストには、2 つの形式があります。

- スケジュール済み確度
- オンデマンドの確度

ユーザは、確度テストを実行するフロアを選択してから、このいずれかの方法を選択できます（図 39 を参照）。これらのテストは、同じフロアで実行されます。

図39：オンデマンドの確度テスト



スケジュール済み確度テスト：このテストは、アクティブな環境（ライブネットワーク）で実行

されます。クライアントやタグはフロア上に事前に置かれ、テストは WCS からスケジュールされます。このテストでは、要素の「実際」の口ケーションと「測定」された口ケーションを比較します。ユーザはテストを変更できます。

- 要素の追加および削除
- 位置の変更
- スケジュールの変更

テストは、スケジュール済みタスクとして実行でき、一定の確度の範囲を下回った場合にアラームを生成できます。特定の展開における RF 環境は変わる場合があり、これは口ケーションの確度に影響するため、このタイプのテストは定期的に実行する必要があります。

図40：精度テストの結果

Accuracy Test Result (%)
98.14

Error Range (Meters)	% of Total
3.00 or less	49.31
3.01 to 5.00	25.86
5.01 to 7.00	17.53
7.01 to 10.00	5.11
10.01 or more	1.86

図 40 の例で、98.14 % は 10 m 以内で検出されたテストに含まれるデバイスの数を表します。これは、49.31、25.86、17.53、5.11 の合計です。

オンデマンド確度テスト：このテストは、ユーザのネットワークにアクティブなクライアントやタグが導入されておらず、確度の測定に関心がある場合に実行されます。このテストは、事前に置かれたタグおよびクライアントのないフロアの場合に実行できます。これは、単一クライアントでリリース 5.0 よりも前の WCS で実施していた確度テストと同様です。特定のロケーションにクライアントを設置し、「ドラッグ アンド ドロップ」によってテストをドラッグすることにより、WCS 内のフロア マップ上でこのロケーションを指示します。 [Start] をクリックし、RSSI 収集プロセスが完了するまで数分間待ってから [Stop] ボタンをクリックします。テストを続行して、フロア マップ上の次のポイントまで移動できます。すべてのポイントが収集されたら、[Analyze results] ボタンをクリックしてテストを実行できます。これにより、確度の結果がレポート形式で生成されます。

いずれの確度テストを実行する場合でも留意する必要のある重要なポイントを次に示します。

- クライアントは、3 台以上の AP から受信する必要がある
- 確度は、三角測量技法および RF フィンガープリントに依存する
- MSE 上で [Advanced debugging] をイネーブルにする必要がある
- 確度テストを実行する前に、静止状態のクライアントを 1 台配置して、フロア マップ上の特定のポイントで 1 分程度待ちます。これは、ワイヤレス クライアントのロケーションを MSE に更新する十分な時間を確保するためです。テストを 2 分間実行します。

Location Readiness ツール

WCS には、Inspect Location Readiness 機能というツールが用意されており、ネットワーク設計者は、ケーブルの引き込み、設備の配置、調整の実行を行う前に、フロアのロケーションのパフォーマンスを予測的にすばやくチェックできます。

このツールは、距離に基づく予測ツールで、標準的なオフィス タイプのビルを想定しています。したがって、予測と実際の結果には一定の違いが生じます。Location Readiness ツールは、他のベスト プラクティス テクニックと組み合わせて使用することをお勧めします。

Inspect Location Readiness では、各アクセス ポイントの配置およびフロア マップ上に示されたアクセス ポイント間の間隔を踏まえて、推定されるロケーション追跡の確度が、全ケースの 90 % で 10 m 以内になるかどうかを予測します。ロケーション レディネス検査の出力では、このレベルの確度を得られると予測されるエリアは緑色で、問題のあるエリアは赤で表示されます。

Location Readiness ツールでは、アクセス ポイントおよびコントローラが WCS に既知であり、WCS フロア マップに定義されていると想定しています。アクセス ポイントおよびアンテナを壁および天井に実際に設置する必要はありません。ただし、ロケーション レディネス評価を実施するには、該当するすべてのコントローラおよびこれに登録されているアクセス ポイントを、WCS に追加する必要があります。このとき、適切なフロア マップ上に配置されたアクセス ポイントを表すアイコンを使用します。フロア マップ上に設置されるアクセス ポイントを WCS データベースに追加すれば、その時点で WCS から到達できない場合であっても、この同じアクセス ポイントを使用して、以降のロケーション レディネス評価を実施できます。ロケーション レディネス検査は、アクセス ポイントの配置とフロア マップ上に示されたアクセス ポイント間の距離に基づくため、このツールを使用する場合は、アクセス ポイントをマップ上に正確に配置するこ

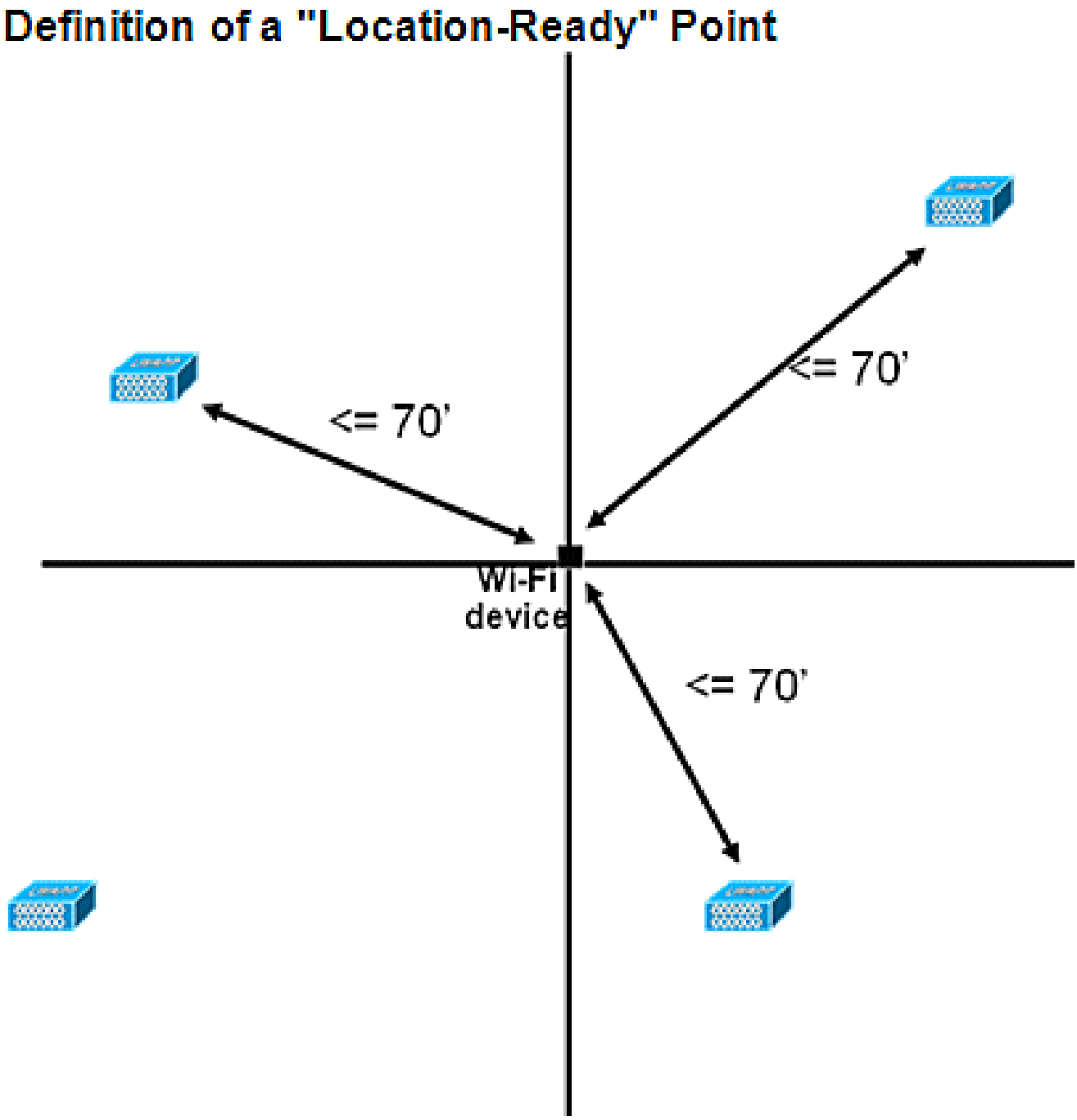
とが重要です。Location Readiness ツールは、RF フィンガープリント ベースの口ケーション追跡を実行できる状態の設計になっているかどうかを評価するためにのみ使用されます。チョークポイント 口ケーションを実行するための設計（特にチョークポイント トリガーの位置の定義に関して）を検証することはありません。アクセス ポイントの配置を実行した後で、口ケーション レディネスを確認するフロア マップを選択し、次に、右上のドロップダウン コマンド メニューから [Inspect Location Readiness] を選択します。

次のすべての条件を満たす場合、そのポイントは「口ケーションの準備が完了した」と判断されます。

- 少なくとも 4 つのアクセス ポイントがフロア上に展開されている。
- 対象のポイントを囲む各 4 分割エリア内に、1 つ以上のアクセス ポイントが存在している。
- ポイントを囲む 4 分割エリアの 3 つ以上で、対象のポイントから 70 フィート以内に 1 つ以上のアクセス ポイントが存在している。

  図 41 に、上記 3 つの口ケーション レディネスのルールを示します。

  図41：口ケーションレディポイント

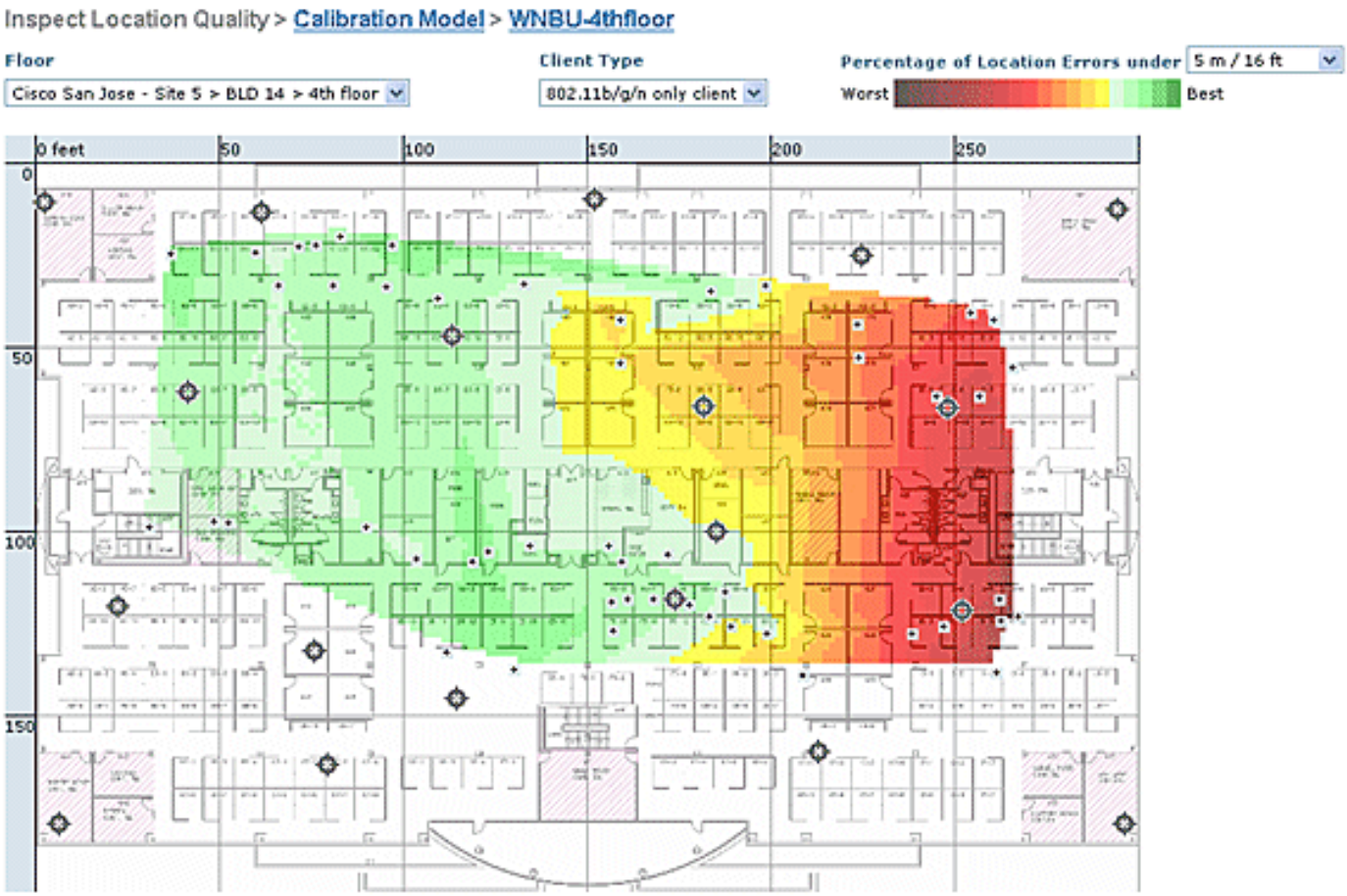


次の WCS スクリーン キャプチャは、10 m/90 % の確度を得るために必要な前述の 3 ポイントの ロケーション レディネス評価を満たさないエリアがある、フロア展開の例を示します。図の中心に向けて緑のエリアがある一方で、凸包を表す周辺部アクセス ポイントよりも外側は赤いエリアで囲まれています。ロケーション レディネスを規定する要件をしっかり理解すれば、この図に含まれている情報から、パフォーマンスを向上するために、いくつの AP を移動または追加する必要があるのかを判断できます。たとえば、赤いエリアで 10 m/90 % 以上のロケーションの確度を必要とする場合は、追加のアクセス ポイントを導入して、フロアの周辺部をより明確に描くことができます。これには、フロアの各隅にアクセス ポイントを配置することと、アクセス ポイント間の距離を再確認することが含まれます。このような修正を加えると、Cisco UWN で、ここで強調したエリアにある追跡対象デバイスのロケーションをより正確に判別できるようになります。

図42：ロケーションレディネスツールの使用例

ワイヤレス展開の口ケーションの品質は、口ケーション仕様（10 m、90 %）を満たすことができるかどうかと、物理検査および調整で収集されたデータ ポイントに基づいて確認できます（図 42 を参照）。Location Readiness ツールを使用すると、10 m、90 % の口ケーション仕様を満たすエリア（緑 = Yes）と満たさないエリア（赤 = No）を表示した、色分けしたマップが表示されます。

図43:Inspect Location Qualityツール



特定のエリアまたはマップ上で調整を実行してから、このデータをレビューして、調整中に収集された未加工データを確認できます（図 43 を参照）。各データ収集ポイントの未加工データの物理測定値および関連する AP RSSI 値を確認することが重要です。AP の位置決め、アンテナ、さらには測定リファレンス ポイントの異常であっても、簡単に特定して、マップに適用する前に修正できます。感知した確度のレベルおよび寄与している AP に関する補足情報も、全体的な口ケーションの確度を評価するために役立つことがあります。

Context-Aware：システムのパフォーマンス

配置された Context Aware ソリューション内で、複数のタグおよびクライアントを同時に移動できます。移動するデバイスの数が多いほど、MSE 上での処理の負荷は大きくなります。このことは、ネットワーク全体の遅延に影響します。この場合の遅延は、MSE がデバイスに関する RSSI 情報を受信してから、MSE が口ケーションを計算するまでの遅れを指します。任意の期間に移動する最大要素数は次のとおりです。

- MSE-3310 の場合、100 要素/秒の移動
- MSE-3350 の場合、650 要素/秒の移動

システムのエンドツーエンドの遅延：

- クライアントとタグ：650要素の移動/秒（WLCソフトウェアリリース5.1以降）によるフルロード時の10秒

遅延は、NMSP 集約時間枠にも関連します。この値は調整できます。「RFID タグおよび WLC の

設定および調整」セクションの「反復間隔」サブセクションを参照してください。

- アプリケーションセッションの最大数：1024
- ノースバウンドAPIの最大デスティネーション数：1024
- カバレッジエリアの最大数：フロアあたり50
    - カバレッジ エリアのサイズは、通常の口ケーションの確度（10 m）未満にはできません。通常の力バレッジ サイズは、最小 50 X 50 フィート（2,500 平方フィート）です。

•フロアあたりの AP 数：

MSE/2710 では無制限です。主な制限は、WCS の推奨事項のとおりに、AP を 100 台未満にすることです。これを満たさない場合、WCS マップを管理し難くなり、解像度が低下して、マップ詳細の作成に長時間かかるようになります。WCS マップ上に表示できる追跡対象デバイスの数にも制限があります。

•MSE あたりのコントローラ数：

一部の例外を除き、同じコントローラを複数の MSE と同期できます。

1. コントローラが 4.2 または 5.0 のコード上で稼動している場合、複数 NMSP 接続はサポートされていないため、複数の MSE と同期する必要はありません。
2. wIPS AP を持つ WLC は、複数の MSE と NMSP 接続を確立できません。これは、wIPS AP は、wIPS 適応型サービスを実行している MSE 1 つのみと通信できるためです。

1 つの WLC で最大 10 個の NMSP 接続を処理できます。

1 つの MSE は、最大 500 個の NMSP 接続をサポートします。ただし、これを CAS 展開の観点から理解することが重要です。各 WLC は、複数のクライアント（WLC4400 1 台あたり 5,000 クライアント）を追跡できます。したがって、コントローラのほとんどない実際的な展開では、MSE CAS で追跡するデバイスの最大数は 18,000 台となります。留意する必要のある、目に見えない制限が 2 つあります。コントローラ 1 台あたり 5,000 台のクライアントと、MSE 3350 1 台あたり 18,000 台のデバイスです。このいずれかの制限に達した場合は、システムのキャパシティを最大化します。

拡張性テストの実行には常に制限が伴うため、口ケーション トラフィックを処理している MSE 1 台あたり 100 台のコントローラを使用してストレス テストを実行しました。

•WCS あたりの MSE の数：

MSE は単一の WCS で管理できますが、WCS では複数の MSE を管理できます。WCS には、さまざまな観点の制限があります。これによって、MSE 全体にわたるこれらのユニットの分布に基づいて、WCS で管理できる MSE の数が決まることがあります。したがって、サポートされる要素の最大数、サポートされるフロアの最大数、またはサポートされる AP の最大数などのファクタが作用します。公式には、WCS ごとに 5 個の MSE をサポートしています。

•ネットワーク設計の数：

MSE に追加するネットワーク設計の数に制限はありません。ただし、AeroScout エンジンには、フロア数、寸法、および MSE 用の要素の量に応じた制限があります。フロアの最大数は、255 に制限されています。60 m ごとにデバイスを配置し、グリッド解像度が 1 m の場合、小規模な設置では 15 個のマップをサポートでき、大規模な設置（メモリ要件が大きい）では 90 個のマップをサポートできます。

ノースバウンド通知

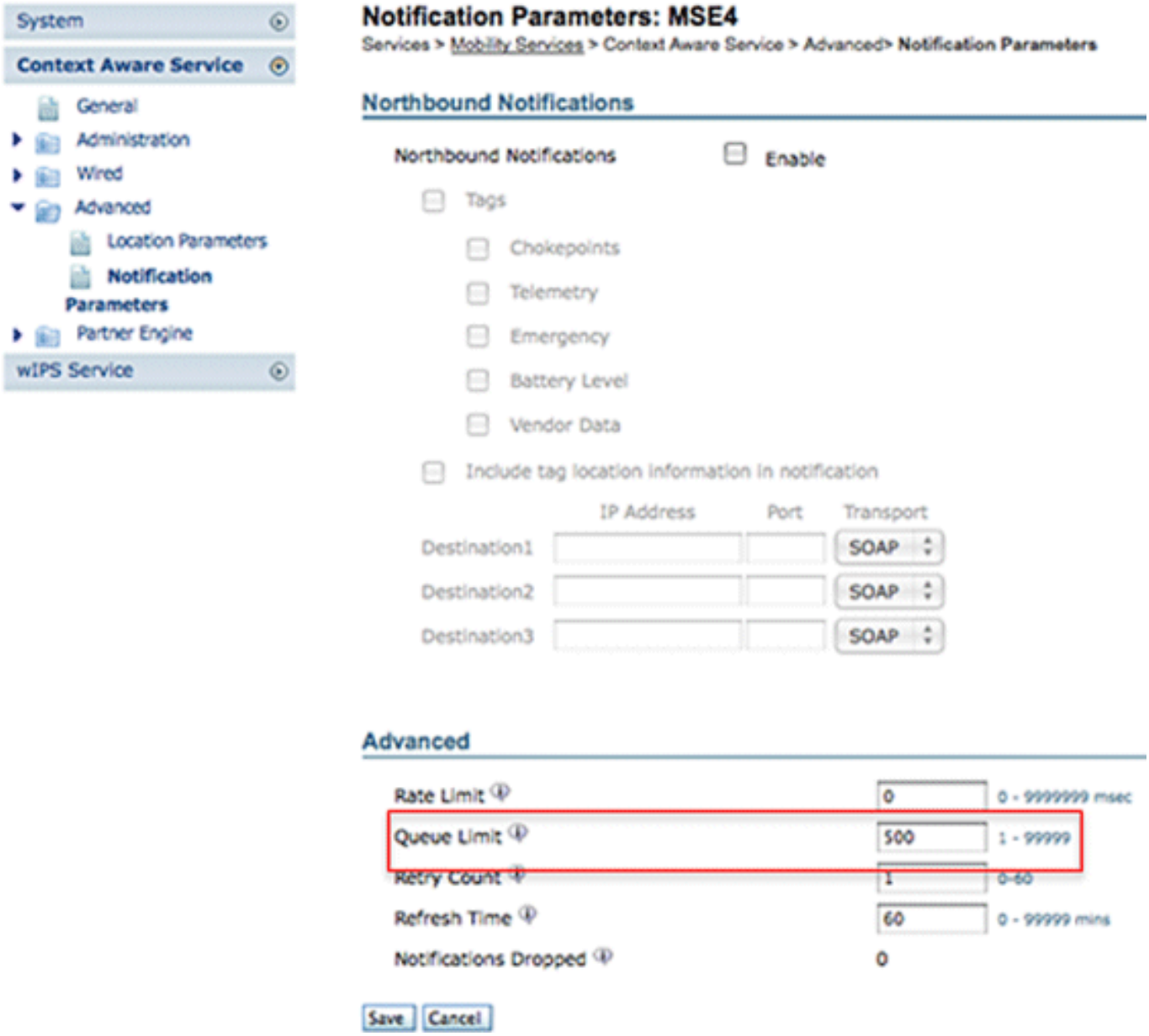
MSE では、既知のすべてのタグ データをノースバウンド SOAP リスナーに転送できます。設定された場合は、タグ通知フレームが MSE に報告されるたび、または、タグの口ケーションを MSE で計算するたびに、MSE からリスナーに通知できます。この機能は、定期的に照会するのではなく、タグが読み取られるたびに即時アップデートを受信する必要のあるサードパーティ アプリケーションの場合に有用です。これは、通知パラメータUIで設定できます。Services > Mobility Services > Context Aware Service > Advanced > Notification Parameters。

ノースバウンド通知をサポートするには、次の推奨事項に従ってください。

- 定期タグ ビーコンは、3 ~ 5 分間隔未満にはできません。
- タグ移動のタグ通知フレーム間隔は、1 ~ 10 秒である必要があります。
- 通知パラメータ上のキュー制限には、サポートされるタグの数よりも大きい値を設定する必要があります。
- SOAP リスナーが停止していないことを確認します。
- SOAP リスナーが、通知への応答として、空の有効な SOAP エンベロープを返すことを確認します。
- SOAP リスナーが、着信通知を迅速に処理することを確認します。

以上の条件が満たされていないと、MSE の通知キューがオーバーフローすることがあります。この状態は、[Notification Parameters] ページに [Notifications Dropped] カウンタとして表示されます（図 44 を参照）。

図44：ノースバウンド通知



このセクションは、ノースバウンド リスナーでノースバウンド通知のトラフィックを処理できず、レポートに含める重要な情報（または処理対象の情報）がタグに含まれていなければこのトラフィックを抑制する場合にのみ有効です。

対象のタグのペイロードに基づいてノースバウンド通知をフィルタして、システムをスケーラブルにします。たとえば、タグが数秒ごとにビーコンを発信する一方で、バッテリ情報または処理対象でない移動テレメトリのみがタグのペイロードに含まれている場合は、これらのタグ ペイロードを受け取ったことによるノースバウンド イベントの生成を抑制できます。

ノースバウンド イベントのフィルタリングは、aes-config.xml ファイルにある新規パラメータ 6 個で制御されます。

```
<entry key="send-event-on-location-calc">true</entry>
<entry key="send-event-on-every-beacon">true</entry>
<entry key="send-event-on-vendor">true</entry>
<entry key="send-event-on-emergency">true</entry>
<entry key="send-event-on-chokepoint">true</entry>
```

```
<entry key="send-event-on-telemetry">true</entry>
```

すべての通知を受け取るには、send-event-on-location-calc および send-event-on-every-beacon をオンにします。重要でないタグ ペイロードがある場合は、選択して設定します。たとえば、ロケーションを計算したとき、コール ボタンを押したとき、またはチョークポイントに遭遇したときのみに MSE で通知を送信するには、対応するパラメータをオンにします。（ファイル内に「true」を設定します。次の値は削除しないでください）。

```
send-event-on-location-calc
send-event-on-emergency
send-event-on-chokepoint
```

他の 3 つのフラグはオフにします。

```
After install/upgrade, ssh into MSE and issue the following commands :
rm /opt/mse/locserver/conf/aes-config.xml         (won't exist for new install)
/etc/init.d/msed start                 (creates the aes-config.xml)
/etc/init.d/msed stop
vi /opt/mse/locserver/conf/aes-config.xml
```

要件に合わせてフィルタを変更します。ファイルを保存して終了します。msed プロセスを再起動します。

```
/etc/init.d/msed start
```

通知の詳細については、API のドキュメントを参照してください。

RFID タグおよび WLC の設定および調整

RFID タグは、トランスミッタとアンテナを備えた Wi-Fi デバイスです。アクセス ポイントと関連付けられないため、他のワイヤレス クライアントとは動作が異なります。RFID タグは、定期的に情報を送信します。これは、タグ通知フレームと呼ばれる、低データ レートで送信されるマルチキャスト パケットです。RFID タグは、設定されているチャネルに、x 秒ごとにタグ通知フレームを送信します。タグ通知フレームは、17 dBm の信号強度で送信することをお勧めします。設定されているすべてのチャネルに対する送信を完了すると、RFID タグはスタンバイ状態になり、次の送信期間まで待機してからタグ通知フレームを送信します。

Wi-Fi を使用して資産を追跡するために RFID を展開する場合は、次の内容を設定する必要があります。

1. RFID タグでチャネルごとに送信するタグ通知フレームの数

802.11 ネットワークでのマルチキャスト トラフィックの性質上、通常は、チャネルごとのタグ通知フレームの数を多くすることが推奨されます。

新規インストールした RF 環境では、チャネルごとに 1 つのタグ通知フレームを送信するようにタグが設定されている場合でも、AP はタグ アップデートを受け取って WLC に報告します。実際の展開では、RF ノイズまたはその他のアクティビティが原因で、特定の AP 上でタグ アップデートが行われないことがよくあります。付近の AP 上でタグ アップデートが行われていないと、ロケーション計算が正しくなくなります。付近の AP でタグ アップデートが行われない確率を下げるため、チャネルごとのタグ通知フレームの反復回数をデフォルトの 1 ではなく 2 または 3 にします。

タグのバッテリ寿命に関する考慮事項も、確度とタグ通知フレームの間隔において重要な側面の 1 つであり、折衷策を必要とする場合がよくあります。移動する物体を追跡する場合のベスト プラクティスとしては、動作感知タグを使用することをお勧めします。固定された物体の場合で 3 ~ 5 分のタグ通知フレーム間隔を設定し、移動のある場合はフレーム間隔を 1 または 2 秒延ばすと、確度が向上し、バッテリ寿命が長くなります。設定およびベスト プラクティスの推奨事項は、タグのメーカーから入手してください。

AeroScout Documentation を参照してください。

特定のアクセス ポイントでタグ アップデートが行われない場合の補正手段としては、WLC 上で RFID RSSI 有効期限値を大きくすることもできます。間隔の 3 倍に 5 秒を加えた値が推奨されます。この値を設定すると、AP で特定のタグからの最新の反復を検出しなかった場合に、WLC 上の最新の RSSI が保持されます。新規のアップデートと前の反復による保持されたデータがまとめて MSE に送信されます。

この手法には、確度に影響することがあるという難点があります。RFID タグ上で動作の伝送がイネーブルにされておらず、タグ通知フレームを送信した最後のロケーションからタグが高速で移動した場合、ロケーションは古いデータに基づいて計算されます。動作のプローブをイネーブルにして、常に新しい AP データに基づいてロケーション計算が行われるようにすることと、WLC タイマーをできるだけ小さく保って遅延を減らすことをお勧めします。

注：WLCコード5.xには、WLCで保持されるデータにも影響を与える新しいコマンドが用意されています。この有効期限タイマーは、RFID タグ、クライアント、および不正要素に対して個別に設定可能です。デフォルトの有効期限設定は 5 秒です。この場合、5 秒前よりも古いデータは、コントローラからプルーニングされます。RFID タイムアウト設定では、RFID タグが範囲外に移動するか、伝送を停止した後に、このタグをコントローラ上で保持する合計時間を制御します。これらのタイマーおよび MSE 上の必須設定を組み合わせることにより、コントローラと MSE の間の NMSP アップデートを最小にしながら、最適な確度を実現できます。

RFID RSSI の有効期限は、WLC CLI を使用して設定できます。

```
(Cisco Controller) >config location expiry tags ?

<seconds>      Time in seconds
```

次のコマンドでは、AP で特定の RFID タグを検出したかどうかを確認します。

```
(Cisco Controller) >show location ap-detect rfid ?

<AP name>      Display information for AP name
```

2. 対象のチャネル

2.4 GHz 展開では、チャネル 1、6、および 11 はスペクトル内でオーバーラップしないチャネルです。RFID タグ上で設定を推奨されるチャネルは 1、6、および 11 です。場合によっては、AP は動作しているチャネルとは異なるチャネル上の RFID タグのアップデートを読み取ることができることに注意してください。AP は、これらのアップデートをドロップして、WLC には転送しない設計になっています。

3. 反復間隔

タグ通知フレーム間隔の設定は、ロケーション計算またはアップデートの間の時間の分離を定義するため、ロケーション追跡において重要な役割を持ちます。前述のように、バッテリ寿命およびロケーションの確度を最適化するには、タグ通知フレーム間隔を設定する必要があります。これは、固定されたタグの場合、3 ~ 5 分です。

タグが移動する場合にロケーションを計算するには、リアルタイム性の高い情報が必要であることに留意してください。移動するタグを追跡する場合は、タグ通知フレーム間隔を <10 秒にして、RFID タグ上で動作の伝送をイネーブルにする必要があります。

4. フレーム伝送間で RFID が待機する間隔

Aeroscount RFID タグでは、フレームの伝送またはビーコンの送信時に、事前設定されている時間を待機してから伝送します。この待機時間は、128、256、または 512 ミリ秒に設定でき、「メッセージ反復間隔」と呼ばれます。512 ミリ秒に設定しており、タグでチャネルごとに 1 つのビーコンを送信する場合、RFID タグによる反復は約 1.5 秒で完了します。同じ「メッセージ反復間隔」でチャネルごとに 2 個のフレームを送信する場合、タグによる反復は 3 秒で完了されます。

RFID タグでは、設定された数のフレームを特定のチャネルに送信してから、次のチャネルに移動して同じ手順を実行します。各フレーム伝送を分離する時間を「メッセージ反復間隔」と呼びます。

WLC では、チャネル 1、6、および 11 上の寄与しているすべての AP からタグ アップデートを受信したうえで、NMSP を介して MSE にこのデータを送信することが不可欠です。WLC は、集約時間枠と呼ばれる設定可能な期間を待機してから、単一の RFID タグに対する付近の AP のリストを MSE に送信します。

WLC 5.1 ソフトウェアからは、NMSP 集約時間枠を設定でき、デフォルトで 2 秒に設定されます。5.1 よりも前のリリースでは、WLC 上の集約時間枠は 8 秒であり、設定できません。同じ集約時間枠に複数の AP から同じパケットを受信した場合、コントローラでは重複するパケットをドロップします。一部のパケットを 1 つの時間枠で受信し、残りのパケットを次の時間枠で受信し

た場合、コントローラでは重複パケットを 1 つ (第 2 時間枠の最初のパケット) 送信しますが、残りの重複パケットはドロップします。

WLC で、すべての AP からアップデートを必ず受信するように、適切な集約時間枠のサイズを設定することが重要です。この時間枠は、RFID タグでサイクルを完了するために費やす時間よりも長く設定する必要があります。一般的には、WLC の待機時間を十分確保するために、1 秒以上余分に追加します。集約時間枠を短く設定すると、ロケーション計算が正しくなくなります。

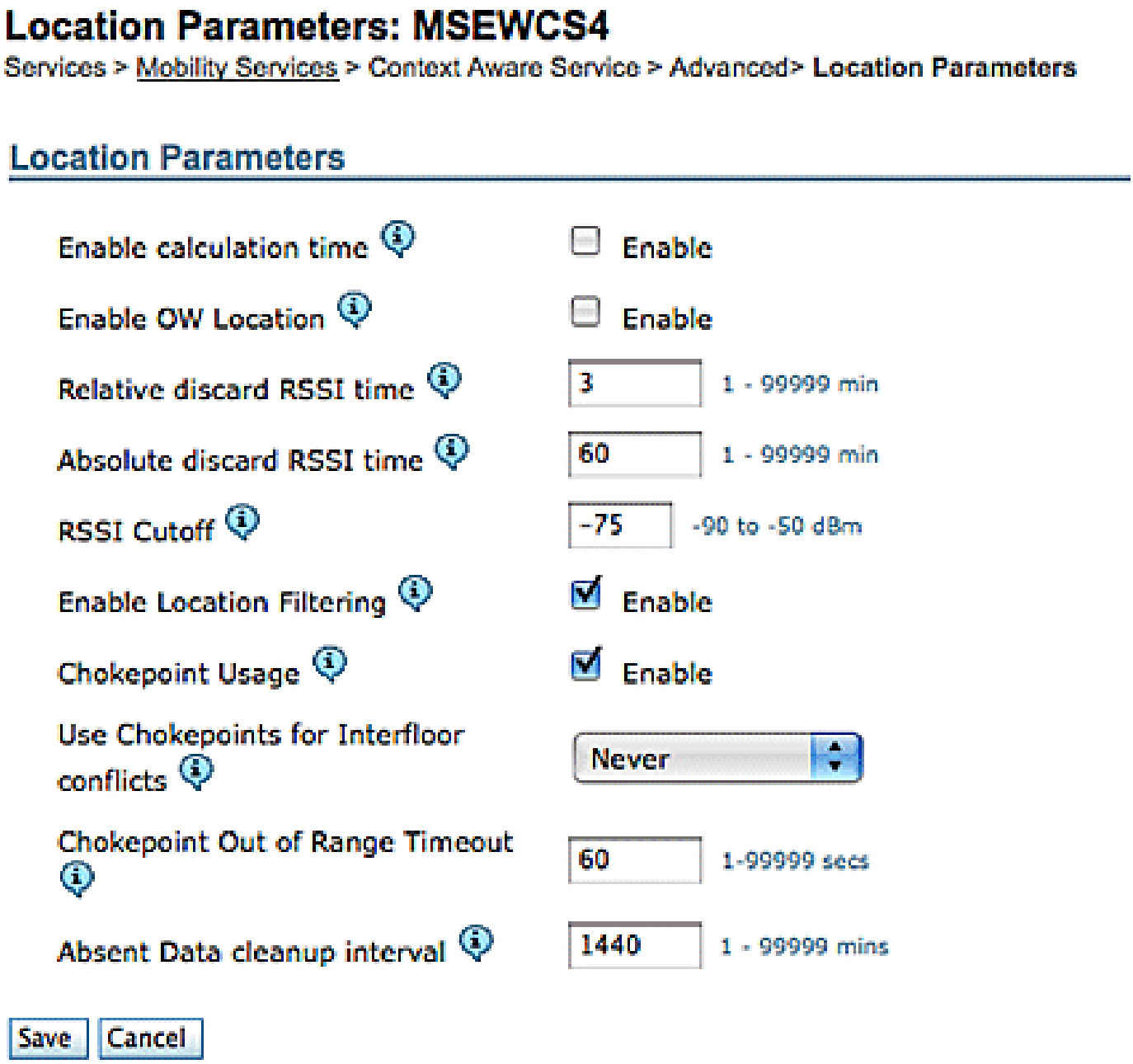
CCA (クリア チャネル アセスメント) を行う場合は、RFID タグで 3 つのチャネルすべてのアップデートを完了するまでの時間が長くなることがあります。大部分の RFID タグは、キャリア検知を行ってから送信します。ワイヤレス メディアがビジーの場合、タグでは、バックオフ時間を加えて、伝送を控えます。事前定義された時間が経過してメディアがビジーでなくなった場合、タグは、送信を実行して次のチャネルに移動します。メディアがまだビジーの場合、タグでは、このチャネルに対する伝送の反復を中断して、次のチャネルに移動します。バックオフの最大時間は固定されておらず、ベンダーごとに異なることがあります。

注：WLC 4.xまたはWLC 5.xソフトウェアリリースをMSEとともに使用する場合、MSEのNMSP集約時間枠は8秒に設定されます。

WCS および MSE の設定および調整

WCS および MSE で設定でき、ロケーション追跡に影響を与える、多数の重要な設定パラメータがあります (図 45 を参照) 。

図45：ロケーションパラメータ



[RSSI Cutoff] は、特定の環境に合わせて調整できる重要なフィールドです。このフィールドは、MSE で特定の要素の口ケーションを計算するときに、この値を下回れば無視する、最小 RSSI 値を指定します。この値は、追跡対象のクライアントのみに適用可能です。つまり、タグの追跡には適用できません。

AP 密度が低いときに、-60、-50 などの非常に高い RSSI Cutoff を指定すると、MSE では、確実に読み取っている AP の RSSI 値を計算から除外するため、口ケーション計算の精度が低くなります。

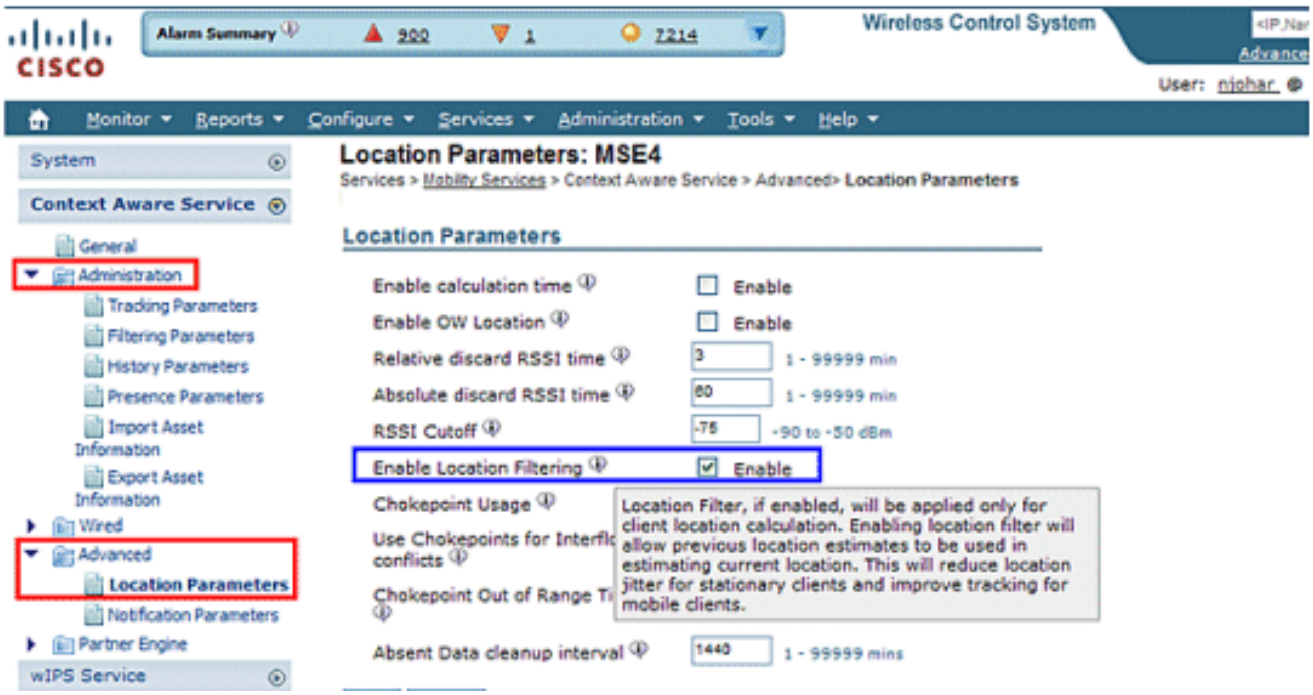
-85、-90 などの低い RSSI Cutoff を使用し、オープン スペース エリアまたは壁の低いフロア間の減衰エリアで操作すると、MSE では、範囲外の AP の RSSI 値を計算に含めるため、口ケーション計算の精度が下がります。

RSSI Cutoff は固定値ですが、最後の反復による低い RSSI 値を補完したり、関連する廃棄リポジトリから値を取得したりして、アルゴリズムによる欠落値の補償が行われます。理想を言えば、

同じフロアにある -75 dBm よりも大きい RSSI 値を持つ AP 6 台以上が寄与している場合に、最適な RSSI Cutoff 値を得られます。RF 損失特性の見られないビルの場合は、このパラメータの調整が必要な場合がありますが、通常、これは最適な展開にならないことを示しています。

ジッタ:5.2リリース以前は、MSEにはクライアントを追跡するロケーションスムージングメカニズムがありました。クライアントの移動平均が計算され、クライアントの移動量が平均化されていました。5.2 ソフトウェア リリースからは、このメカニズム全体が「ロケーション フィルタ」に置き換えられました。 ロケーション フィルタは、内部でクライアントごとに適用されます。MSE では、クライアントの移動および固定の状態を常に認識し、これに応じてフィルタリングを適用します。これにより、システム全体のジッタが減少します。ロケーション フィルタリングは、デフォルトでイネーブルになっています。図 46 を参照してください。

図46：ロケーションフィルタリング



WCS/MSE通信:WCSとMSE間の通信を設定するための導入の推奨事項を次に示します。

- MSE:HTTPSは常に有効です（デフォルト）。HTTP はデフォルトでディセーブルになっています。HTTP をイネーブルにするには、コンソール アクセス（直接または SSH）から MSE に対して手動設定が必要です。

- WCS：デフォルトでは、WCSはHTTPSを使用してMSEと通信します。HTTP は、WCS GUI を使用してイネーブルにできます。

場合によっては、WCS は、HTTPS を介して MSE と通信できません。この場合、MSE を WCS に追加するか、[MSE General Properties] ページで保存すると、「HTTPS connection to server failed」というエラーが何度も報告されます。 WCS から MSE に ping できる（到達できる）必要があり、MSE 上で「getserverinfo」コマンドを発行してステータス情報が表示される必要があります。MSE 上で HTTP をイネーブルにし、HTTP を介して MSE と通信するように WCS を設定することをお勧めします。

MSE での HTTP サポートは、リリース 5.1、5.2、および 6.0 で使用できます。

バージョン6.0ソフトウェアリリースが稼働するMSEでHTTPを有効にする:ssh/consoleを使用してMSEにログオンします。次のコマンドを実行します。

```
root@mse ~]# enablehttp
```

バージョン5.xソフトウェアリリースが稼働するMSEでHTTPを有効にします。ssh/コンソールからMSEにログオンします。次のコマンドを実行します。

```
[root@mse ~]# getdatabaseparams
<DB PASSWORD>
```

このコマンドは、db のパスワードを返します。このパスワードを次のコマンドで使用します。

```
[root@ mse ~]# /opt/mse/locserver/bin/tools/solid/solsql "tcp 2315" dba <DB PASSWORD>
Solid SQL Editor (teletype) v.06.00.1049
Copyright ©) Solid Information Technology Ltd 1993-2008
Connected to 'tcp 2315'.
Execute SQL statements terminated by a semicolon.
Exit by giving command: exit;

update AESSERVERINFO set USEHTTP=1;
Command completed successfully, 1 rows affected.

commit work;
Command completed successfully, 0 rows affected.
```

Ctrl + C キーを押してデータベース シェルを終了します。`/etc/init.d/msed stop; /etc/init.d/msed start`を使用して、MSEプラットフォームの再起動を実行します。

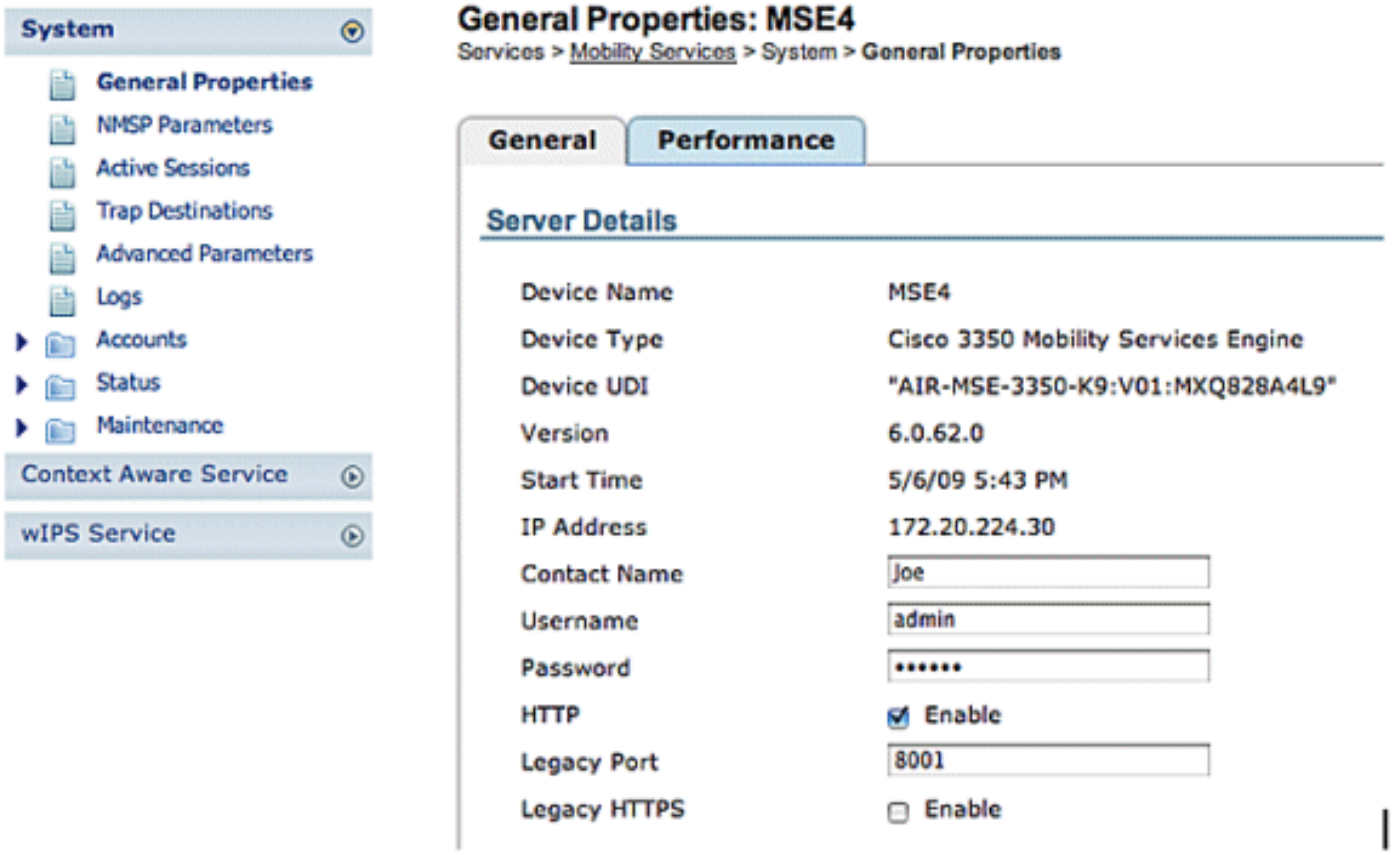
WCS (ソフトウェア リリース 6.x を稼動) から MSE への HTTP 通信をイネーブルにします。

- 前のステップで、MSE 上で HTTP をイネーブルにしてあることを確認してください。
- WCS の [MSE General Properties] ページで [HTTP] を選択します。これにより、WCS と MSE の間の HTTP 通信がイネーブルになります。図 47 を参照してください。

これで、WCS は、HTTP を介して MSE との通信を開始します。

注：WCS 5.2でHTTPを有効にするには、『WCS 5.2コンフィギュレーションガイド』を参照してください。

図47:MSEとWCS間のHTTP通信の有効化



MSE ライセンス

MSE ライセンスは、6.0 コード以降で、アクセス ポイントからタグおよびクライアント上のコンテキスト情報を取得するために必要です。クライアントのライセンスには、ワイヤレス クライアントと有線クライアント、不正なクライアント、および不正なアクセス ポイントの追跡が含まれます。タグ用とクライアント用のライセンスは、別々に申し込みます。タグおよびクライアント用のライセンスは、数量範囲で提供されています。提供されている数量範囲は、デバイス 1,000、3,000、6,000、および 12,000 台です。シスコでは、クライアント用のライセンスとタグ用のライセンスを提供しています。実際のライセンスの作成と SKU 関連情報の管理には、SWIFT チームが開発および保守している、FlexLM ライセンス システムを使用します。

WCS は、MSE にクライアントと wIPS のライセンスをインストールするために使用される管理システムです。タグ用のライセンスは、AeroScout を介してアクティベートし、AeroScout システム マネージャを使用して MSE にインストールする必要があります。

MSE ライセンスの詳細については、『Cisco 3300 シリーズ Mobility Services Engine のライセンスおよび発注ガイド』を参照してください。

新規購入

クライアント

- お客様は、ソフトウェア ライセンスを購入し、Product Authorization Key（PAK）を郵送（ライセンス文書）で受け取ります。
- お客様は、https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet（登録ユーザ

のみ）で、クライアントの PAK を登録します。

- [Host ID] フィールドに MSE UDI 情報を入力します。契約書に同意して続行します。ライセンスは、電子メールによってお客様に送信されます。
- MSE UDI は、WCS 上で次のタブから取得できます。
  - [Services] > [Mobility Services] > [MSE] > [System] > [General Properties]
- ライセンスがない場合、MSE には、60 日間の「購入前試用」機能（評価ライセンス）が用意されています。
- 評価ライセンスは使用ベースで、60日間有効です。延長できるのは1回だけです。
- 評価ライセンスの制限：
  - クライアント：100
  - タグ：100
  - wIPS AP数：20
- 評価ライセンスは常に適用されますが、インストールされているライセンスに基づいてプラットフォーム制限に達した場合、個々のサービスの評価ライセンスは、引き続き使用できます。たとえば、MSE-3350 1 台を所有し、18,000 台のデバイス（クライアントおよび/またはタグ）を追跡するライセンスがインストールされていて、18,000 台のデバイスがアクティブに追跡されている場合は、プラットフォーム制限を超えますが、wIPS 用の評価ライセンスをまだ使用できます。
- 評価ライセンスのタイマーは生成された日に始動されるため、評価ライセンスの拡張をすぐにインストールする必要があります。
- インストールされたライセンスは、サービスがイネーブルなのかディセーブルなのかに基づいて使用されます。
- 評価ライセンスの期限が切れてから MSE を再起動していない場合、コア MSE サービスは引き続き実行され、Context Aware などのライセンスを要するサービスも引き続き実行されますが、デバイスは追跡されません。
- 評価ライセンスの期限が切れてから MSE を再起動した場合、ライセンスは再起動され、ライセンスを要するサービスは開始されません。デバイスは追跡されません。

PAK がない場合

- Sales Order Status ツール（http://tools.cisco.com/qtc/status/tool/action/LoadOrderQueryScreen）に移動します。
- [Type of Query] ドロップダウン リストから [Sales Order from] を選択します。
- [Value] フィールドに発注番号を入力します。

- [Check Show Serial Number] によって表示し、[Search] をクリックします。
- MSE 注文詳細情報を含むウィンドウが表示されます。
- [Order detailed] ウィンドウの表で、[expand Line 1.1] をクリックします。
- [Product] カラムの下で、ライセンスを取得するために登録する必要のある、2 行目の PAK 番号（3201J で始まる番号）をコピーします。
- PAK を登録するために https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet（登録ユーザのみ）に移動します。
- 左側の [Product License registration] リンクをクリックし、空白のフィールドに PAK 番号を入力して送信します。
- [Host ID] フィールドに MSE UDI 情報を入力します。契約書に同意して続行します。
- ライセンスが生成され、お客様の電子メール ID に電子メールが送信されます。

タグ

1. お客様は、ソフトウェア ライセンスを購入して、PAK（製品認証キー）を郵送（ライセンス文書）で受け取ります。
2. お客様は、タグ用の PAK を http://support.AeroScout.com で登録します。
3. アカウントがない場合は、[Create New Account] リンクを使用して新しいアカウントを作成します。
4. アカウントが作成されると、ユーザ名とパスワードを含む電子メールの通知が送信されます。
5. AeroScout Support Portal にログインします。
6. [Home] タブの下の [Register Products Purchased from Cisco] リンクをクリックします。
7. 製品を登録し、連絡先の詳細、PAK#、MSE ID（MSE S/N）、およびインストール タイプを指定します。登録を確認する電子メール メッセージが送られます。
8. SE シリアル番号は、WCS のタブから取得できます。

   [Services] > [Mobility Services] > [MSE] > [Advance Parameters]
9. AeroScout は、2 営業日以内に PAK 番号を確認します。確認が終わると、ライセンス キー、Context Aware Engine ソフトウェアのダウンロード方法の手順、および関連するユーザ ガイドを含む通知が、お客様の電子メール アドレスに送信されます。無効な PAK 番号の場合は、有効な PAK 番号を登録し直すよう要求されます。

アップグレード：クライアント ライセンス

1. お客様は、新しいライセンスを購入し、PAK を郵送で受け取ります。

2. PAK を受け取り、ライセンス キーを電子メールで入手します。

3. ライセンス キーを MSE にインストールします。

4. 評価ライセンス数の追加（既存またはインストール済みのクライアントライセンス数がMSEの最大数と等しい場合）:WCSでは、MSEの最大デバイス（クライアント）数に達している場合でも、評価ライセンスを追加できます。たとえば、お客様が MSE-3350 を所有しており、18,000 のクライアント ライセンスをインストールしている場合に、タグ追跡や wIPS を追加しようとするとき、WCS では、このいずれかまたは両方のサービス用の評価ライセンスを追加できます。

アップグレード：タグ ライセンス

- タグライセンス数の追加（既存/インストールされているタグライセンス数がMSEの最大数未満の場合）：既存のタグライセンスは新しいライセンスで上書きされます。たとえば、1Kタグを追跡する既存のライセンスがあり、4Kタグを追跡するためにアップグレードする場合、お客様は3Kライセンスを購入して既存の1Kライセンスに追加します。AeroScout では、新規のタグ数全体をカバーする、4,000 タグ ライセンスを発行します。

- タグライセンス数の追加（既存またはインストール済みのタグライセンス数がMSEの最大数と等しい場合）:AeroScoutシステムマネージャからエラーメッセージが返されます。既存のタグ ライセンスは依然として有効です。たとえば、お客様が MSE-3350 を所有しており、MSE に 18,000 タグ ライセンスがインストールされているとします。3,000 タグ ライセンスをインストールしようとすると、AeroScout システム マネージャはエラー メッセージを出します。AeroScout システム マネージャにはタグ ライセンスを削除する機能がないため、このタグ ライセンスは、手動で MSE から削除する必要があります。新規タグ ライセンスを削除するには、MSE イメージをアンインストールし、データベース オプションを削除し、MSE ソフトウェアを再インストールする必要があります。

- 評価ライセンス数の追加（既存またはインストール済みのタグライセンス数がMSEの最大数と等しい場合）:WCSでは、MSEの最大デバイス（タグ）数に達しても評価ライセンスを追加できます。たとえば、お客様が MSE-3350 を所有しており、18,000 タグ ライセンスをインストールしている場合に、クライアント追跡や wIPS を追加しようとするとき、WCS では、このいずれかまたは両方のサービス用の評価ライセンスを追加できます。

既存のお客様（6.0 ソフトウェア リリースにアップグレードする場合のみ）

1. https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet（登録ユーザのみ）を表示して、クライアント用の PAK を登録し、上の「新規購入」セクションの説明に従ってライセンス キーを取得します。PAK を紛失した場合、お客様は、TAC/GLO に問い合わせる必要があります。

2. WCS から MSE にライセンス ファイルをインストールします。

3. ライセンスは MSE UID と結び付けられます。

4. プラットフォーム（MSE 3310 または 3350）および一意なシリアル番号を構成します

UDI例：AIR-MSE-3310-K9:V01:QCN1224001Yこの例では、シリアル番号はQCN1224001Y です。

5. MSE ライセンスは、Unique Device Identifier (UDI) と結び付けられます。同じ装置を修正できる場合、UDI は同じで、同じライセンスを再ホストできます。一方、装置を交換する必要がある場合は、UDI が変わるため、新しいライセンスを生成する必要があります。UDI が一致しない場合、MSE ではライセンスを受け入れません。お客様は、TAC に問い合わせて、新旧の UDI を提供できます。TAC では、旧ライセンスを非アクティブ化し、新しいライセンスを発行します。

6. 適切なライセンスを購入すれば、MSE-3350 では、最大 18,000 台のデバイス (クライアントとタグの任意の組み合わせ) を追跡できます。追跡対象要素の口ケーションのアップデートは、Cisco ワイヤレス LAN コントローラからモビリティ サービス エンジンに提供されます。

7. このうち、コントローラから追跡対象として指定したデバイスだけを、Cisco WCS マップ、クエリー、およびレポートで表示できます。追跡対象でない要素については、イベントおよびアラームは収集されず、クライアントまたはタグに対する 18,000 台の要素制限の対象として計算されません。

ライセンスを正常にインストールすると、図 48 に示すように、ライセンス タイプに「Permanent」と表示されるようになります。

図48:License Center

License Center

Administration > License Center > Summary > **MSE Summary**

Entries 1 - 3 of 3

MSE Name (UDI)	Type	Limit	Count	Unlicensed Count	% Used	License Type	Status
(H) mse-3350 (AIR-MSE-3350-K9:V01:MXQ821A31P)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (60 days left)	Inactive
	Tag Elements	100	0	0	0%	Evaluation (60 days left)	Active
	Client Elements	100	0	0	0%	Evaluation (60 days left)	Active
(H) heitz-3350 (AIR-MSE-3350-K9:V01:USE810N5HR)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (59 days left)	Active
	Tag Elements	100	5	0	5%	Evaluation (59 days left)	Active
	Client Elements	100	100	372	100%	Evaluation (59 days left)	Active
(L) heitz-3310 (AIR-MSE-3310-K9:V01:QSH78150059)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (Less than a day left)	Inactive
	Tag Elements	1000	4	0	0%	Permanent	Active
	Client Elements	1000	667	0	66%	Permanent	Active

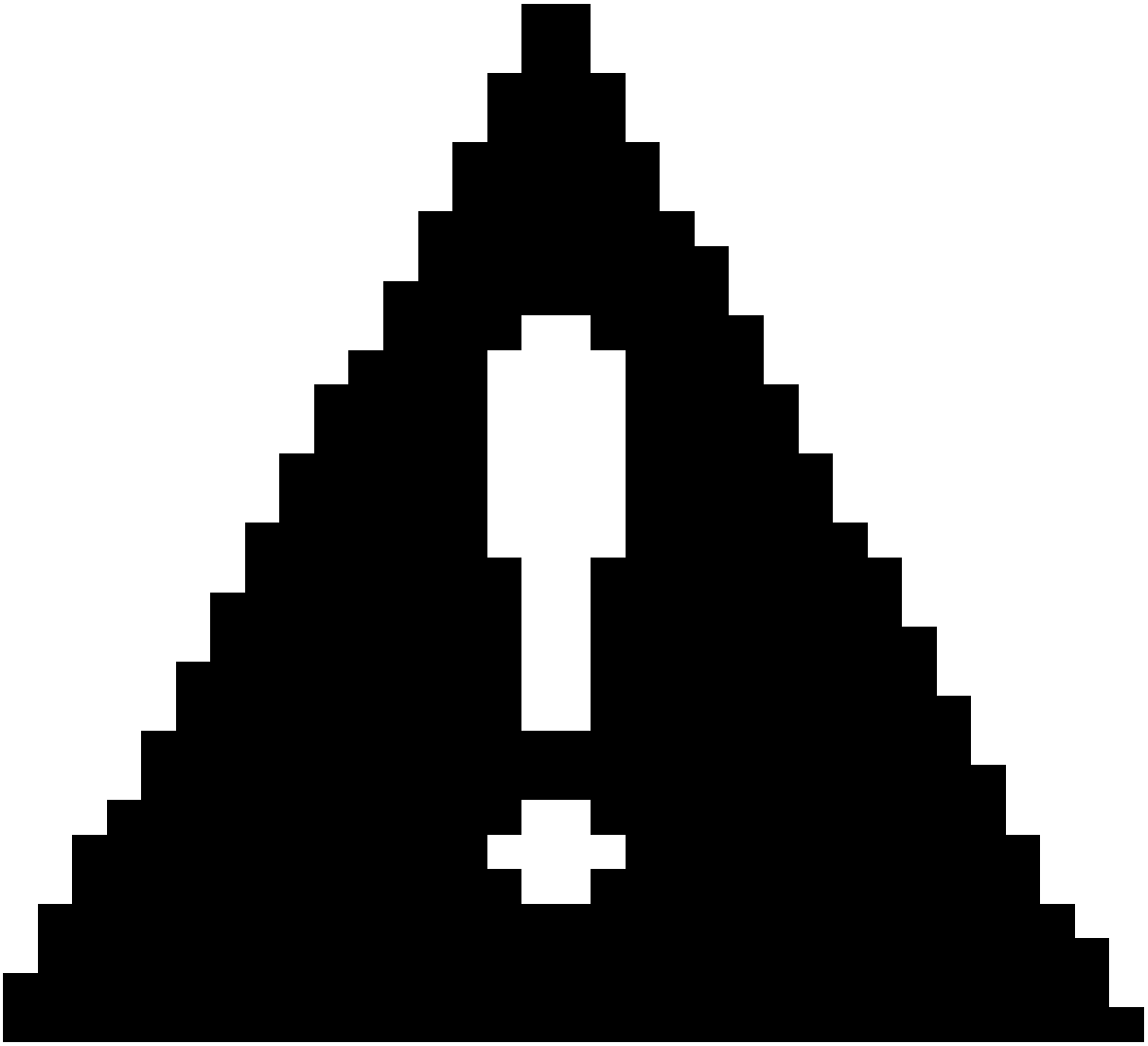
注：クライアントまたはタグが24時間非アクティブになると、それぞれのライセンス数に対してカウントされなくなります。

ライセンス ファイルは「opt/mse/licensing」に保存されます。

MSE 5.x から 6.x にアップグレードするときは、次の手順を順に実行してください。

1. WCS を使用して、現在実行中の MSE システムである MSE 5.x の MSE データベースのバックアップを実行します。
2. タグのデータおよび設定をバックアップするには、『Context-Aware Service Software コンフィギュレーション ガイド』を参照してください。
3. MSE を 6.x ソフトウェアにアップグレードします。MSE 上のアップグレード プロセスで、インストール時の「ライセンス」に関するアラート メッセージが表示されます。
4. WCS から MSE ライセンスをインストールします。MSE システムのキャパシティを超えるライセンスをインストールすると、警告メッセージが表示されて、ライセンス インストール プロセスがブロックされます。たとえば、お客様が MSE-3310 を所有しており、6,000 のクライアント ライセンスをインストールしようとした場合、MSE-3310 で追跡できるデバイスは最大 2,000 台であるため、警告メッセージが表示されます。
5. WCS を使用して MSE データベースを復元します。
6. タグ エンジンのデータおよび設定を復元するには、AeroScout Documentation に従ってください。
7. この手順の詳細については、このドキュメントの「付録 B」および『Context Aware コンフィギュレーション ガイド リリース 6.x』を参照してください。

   注：ソフトウェアリリース6.0では、タグのトラッキングに関して、AeroScoutエンジンの設定とライセンスデータはWCS/MSEのバックアップおよび復元プロセス内に保持されます。6.0 よりも前のソフトウェア バージョンが稼動する MSE 上で実行された設定は、いずれも自動で保持されません。6.0 から 6.x にアップグレードする場合、シスコのドキュメントで説明されている MSE のバックアップおよび復元手順を使用すれば、この設定データは維持されます。5.2 から 6.0 にアップグレードする場合は、AeroScout Documentation で説明されている手動手順に従う必要があります。



注意：適切なライセンスなしでリリース 6.x にアップグレードした場合、サポートされるクライアント、タグ、およびアクセス ポイント（wIPS）の数は、100 クライアント、100 タグ、20 AP にリセットされます。100 個を超えた分の要素は、非アクティブであるとマークされます。追跡されていたすべての要素の履歴データはデータベースに残っており、MSE 上の口ケーション API 内で照会できます。これらの制限は、ライセンスなしの MSE にデフォルトで付属している 60 日間の評価ライセンスに対応するものです。

Cisco WCS を使用して、次の追跡パラメータを変更します（図 49 を参照）。

1. アクティブに追跡する要素の口ケーション（有線クライアントおよびワイヤレス クライアント、アクティブ資産タグ、および不正なクライアントとアクセス ポイント）をイネーブルおよびディセーブルにします。

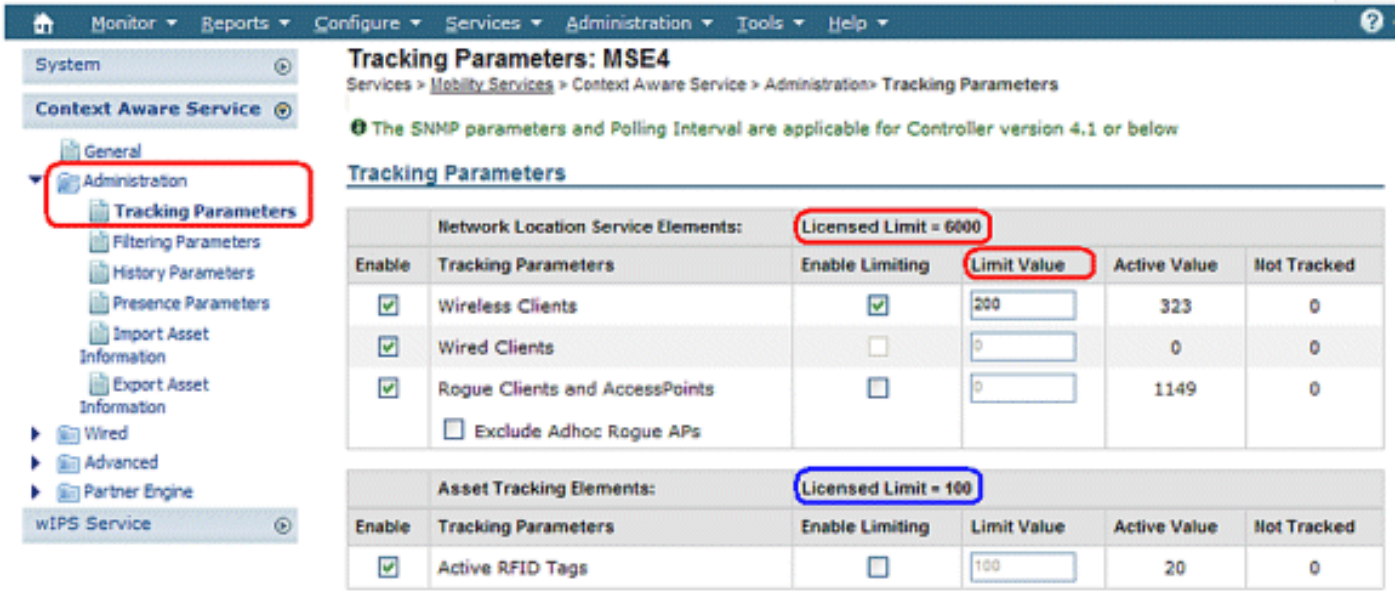
2. 追跡対象とする特定要素の個数上限を設定します。

3. たとえば、12,000 台のデバイス（有線およびワイヤレス）を追跡できるクライアント ライセンスの場合に、8,000 台のクライアント ステーションのみを追跡するように制限を設定できます（残りの 4,000 台のデバイスは、不正なクライアントと不正なアクセス ポイントの追跡に使用可能）。特定の要素の追跡制限に達した場合は、追跡されなかった要素の数が

[Tracking Parameters] ページに集計されます。

4. アドホックの不正クライアントと不正アクセス ポイントの追跡およびレポートをディセーブルにします。

図49:Context Aware Servicesのトラッキングパラメータ



追跡されるクライアントの実際の数は、購入したライセンスによって決まります。

Active Value(図49を参照)：現在追跡中のクライアントステーションの数を示します。

Not Tracked(図49を参照)：制限を超えているクライアントステーションの数を示します。

図 50 に示すように、超過要素（タグ、クライアント、不正要素）は追跡されません。

図50：ライセンスの使用状況

MSE Name (UDI)	Type	Limit	Count	Unlicensed Count	% Used	License Type	Status
mse-3350 (AIR-MSE-3350-K9:V01:MXQ821A31P)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (60 days left)	Inactive
	Tag Elements	100	0	0	0%	Evaluation (60 days left)	Active
	Client Elements	100	0	0	0%	Evaluation (60 days left)	Active
heitz-3350 (AIR-MSE-3350-K9:V01:USE810N5HR)							
	wIPS Monitor Mode APs	20	0	0	0%	Evaluation (59 days left)	Active
	Tag Elements	100	5	0	5%	Evaluation (59 days left)	Active
	Client Elements	100	100	372	100%	Evaluation (59 days left)	Active

複数サービスの拡張の方法

6.0 ソフトウェア リリースを稼動する MSE では、Context Aware と wIPS の同時運用をサポートしています。機能の共存制限が実施されます。制限を超える組み合わせを TAC ではサポートしておらず、MSE のキャパシティを超えてライセンスを追加することはできないため、そもそも不可能です。

サポートされる組み合わせを図 51 および 52 に示します。

図51:MSE-3350システム容量：wIPSモニタモードAPおよびContext-Awareデバイス

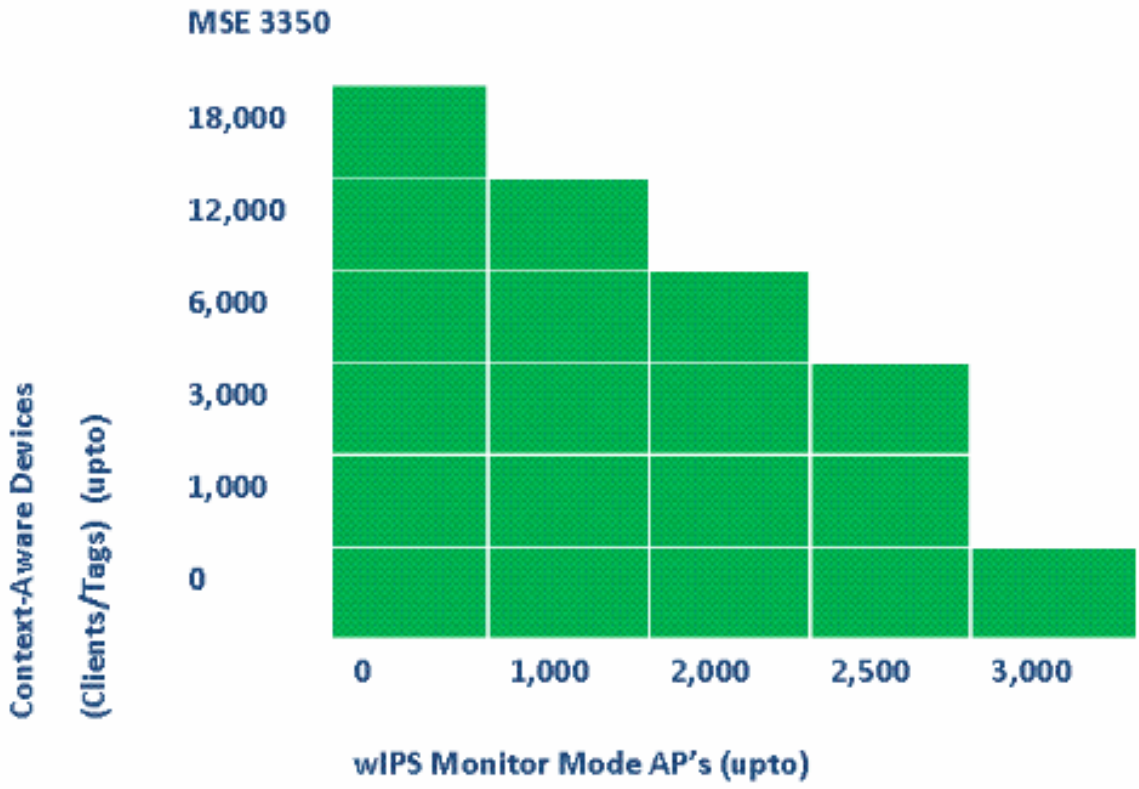
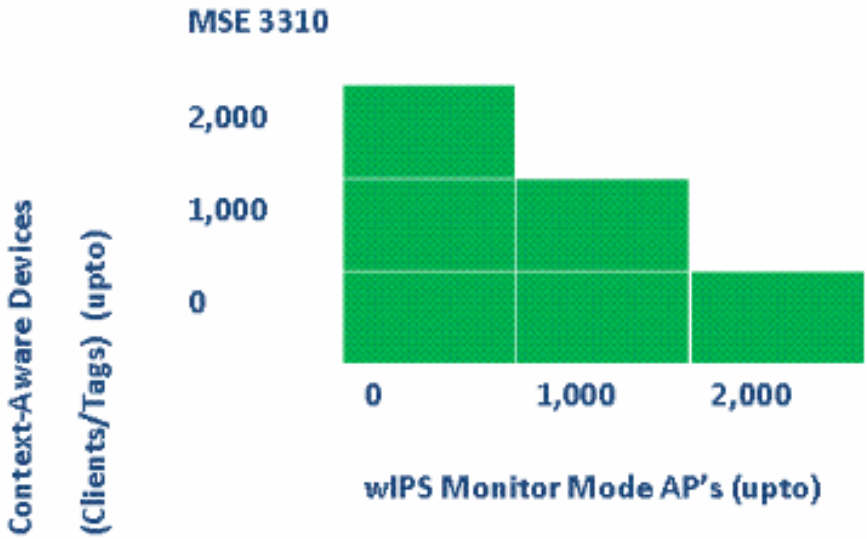


図52:MSE-3310システム容量：wIPSモニタモードAPおよびContext-Awareデバイス



例：

- Context Aware Service を使用して 6,000 台のデバイスを追跡しようとしており、MSE 3350 上に最大 2,000 台の wIPS モニタ モード AP を処理するキャパシティがあります。
- Context Aware Service を使用して 3,000 台のデバイスを追跡しようとしており、MSE 3350 上に最大 2,500 台の wIPS モニタ モード AP を処理するキャパシティがあります。
- Context Aware Service を使用して 1,000 台のデバイスを追跡しようとしており、MSE 3310 上に最大 1,000 台の wIPS モニタ モード AP を処理するキャパシティと、MSE 3350 上に 2,500 台の wIPS モニタ モード AP を処理するキャパシティがあります。

（「トラブルシューティング」）

MSE に到達できない

WCS から見て MSE に到達不能であると検出される場合は、次のような原因が考えられます。

- WCS に設定されている API ログイン クレデンシャルが正しくない。アプライアンスには2つのクレデンシャルのセットがあります。1つはアプライアンスシェルインターフェイス用で、もう1つはAPIクレデンシャル用です。WCS では、MSE を追加する場合に API クレデンシャルが必要です。このドキュメントの「付録 A」を参照してください。
- ルートおよびファイアウォールの接続規則によって、WCS と MSE の間の接続がブロックされている。このドキュメントの「ネットワーク接続の確認」セクションを参照してください。
- WCS のバックグラウンド タスクである「モビリティ サービス ステータス」がディセーブルになっている。WCS で [Administration] > [Background Tasks] > [Other Background Tasks] > [Mobility Service Status] からこのタスクをイネーブルにします。
- MSE サービスの Context Aware がイネーブルにされており、MSE CLI から起動されている

。

- まれに、HTTPS 接続に問題があることがある。WCS の [MSE General Properties] ページで [HTTP] オプションをイネーブルにできます。詳細については、このドキュメントの「WCS/MSE コミュニケーション」セクションを参照してください。
- MSE がクラッシュした。MSE で、CLI の「getserverinfo」が出力を返せません。/opt/mse/logs ディレクトリにあるすべてのログを収集して、Cisco TAC に連絡します。

要素が見つからない

MSE で要素が見つからない場合は、次のような原因が考えられます。

- MSE に到達できない。
- 評価ライセンスの期限が切れた。
- MSE は到達可能で、ライセンスは適用されているが、MSE Context Aware モジュール サービスがイネーブルにされていない。
- [MSE Tracking Parameters] ページで、クライアントやタグの追跡がイネーブルにされていない。詳細については、このドキュメントの「MSE ライセンス」セクションを参照してください。
- ネットワーク設計やコントローラが MSE と同期されていない。
- アクセス ポイントが WCS マップ上に配置されていない。
- NMSP 接続が MSE とコントローラの間に確立されていない。詳細については、このドキュメントの「WLC と MSE の間の NMSP 接続の確認」セクションを参照してください。
- WCS 内のアクセス ポイントがシスコ以外のアンテナ（選択したタイプが [Other]）になっている。この場合は、サポートされている別の似たようなアンテナの種類を WCS 内のアクセス ポイントに設定し、MSE とネットワーク設計を同期し直す必要があります。
- ワイヤレス LAN コントローラ（WLC）がクライアントを検出しない。CLI の「show client summary」を使用して、WLC をトラブルシューティングします。
- ワイヤレス LAN コントローラ（WLC）がアクティブ RFID タグを検出しない。CLI の「show rfid summary」を使用して、WLC をトラブルシューティングします。

タグが見つからない

タグが見つからない場合（他のクライアントが見つかった場合）、AeroScout工ンジン内で問題が発生する可能性があります。考えられる原因は次のとおりです。

- アクティブ RFID タグが WLC によって追跡されていない。WLC設定にconfig rfid status enableコマンドが存在している必要があります。
- ワイヤレス LAN コントローラ（WLC）がアクティブ RFID タグを検出しない。CLI の「show rfid summary」を使用して、WLC をトラブルシューティングします。

- WLC からはタグを参照できるが、WCS からは参照できない。debug rfid nmsp enableコマンドを使用して、NMSP通知がMSEに送信されることを確認します。
- AeroScout エンジンが MSE にインストールされていない。リリース 5.1 および 5.2 では、このエンジンを個別にインストールする必要があります。リリース 6.0 以降では、このエンジンは MSE にバンドルされています。
- AeroScout エンジン用のライセンスがインストールされていない。
- AeroScout エンジンが MSE に登録されていない。WCS の [Partner Engine status] ページを確認してください。
- MSE に含まれているマップの数が多すぎるか、マップが大きすぎる。AeroScout エンジンのガイドラインを参照してください。
- アップグレード後に設定を AeroScout エンジンに復元する必要がある場合がある。
- フロア マップにイメージが含まれていない（最近のリリースでは解決済み）。
- MSE では、CCX 互換のタグのみを追跡しますが、展開にはサポートされていない CCX 以外のタグのみが含まれているか、CCX 形式で送信するように設定されていません。

特定の要素（クライアントまたはタグ）が見つからない

MSE で特定の要素を追跡する一方で、他の要素は表示されない場合は、次のような原因が考えられます。

- MSE が、100 要素に制限された評価ライセンスで実行されている。
- MSE は有効なライセンスで実行されているが、そのキャパシティが超過している。そのため、すべての追加要素（クライアント、タグ、不正な要素）が廃棄されます。
- 特定のコントローラが、MSE に NMSP 接続されていない。
- 要素がネットワークから外れており、送信をしなくなった。MSE では、この要素を履歴レコードに保存しますが、WCS 画面には表示されません。
- フィルタリング オプションが WCS マップ レイヤに適用されているために、一部の要素が非表示になっている。
- MAC フィルタリング オプションが、MSE フィルタリング パラメータでイネーブルにされているために、一部の要素が廃棄されている。
- MSEはCCX互換のタグのみを追跡します。展開にはCCXタグと非CCXタグの組み合わせが含まれます。
- ロケーションに関するクライアントおよびタグの拡張トラブルシューティング：
    - WCS でこのクライアントを認識しているかどうかを確認します。この機能は、SNMP を介して、クライアント用にすでに存在しています（クライアントのトラブルシューティング）。これをタグ用に拡張する必要があります。

- ロケーションが割り当てられたコントローラ内でクライアントを探します。WLC コマンド show client summary を使用します。
- WLC コマンド show client <MAC address> detail を使用して、WLC でクライアントを検出した時点からの時間を判別します。
- WLC コマンド show client <MAC address> detail を使用して、AP でクライアントを最後に検出した時点からの時間を判別します。

WLC に MSE が接続されていない

コントローラが MSE との接続を確立しない場合は、次のような原因が考えられます。

- MSE または WCS からコントローラに到達できない。
- WCS とコントローラの接続に一時的な問題があり、NSMP 接続用のハッシュ セキュリティ キーをプッシュできない。WCS とコントローラの間の SNMP 接続を確認します。
- コントローラおよび MSE に適切な NTP 設定が行われていないか、これらの時刻の差が大きい。時刻を正しく設定してください。
- 4.2 リリースよりも前のコントローラは、NMSP をサポートしていない。
- リリース 5.1 よりも前のコントローラは、複数 MSE 接続をサポートしていない。
- wIPS をイネーブルにしてコントローラを MSE に割り当てた場合に、同じコントローラを別の MSE に同時に割り当てることはできない。
- 同期が完了したとき、WCS には、WLC に対する読み取りおよび書き込みアクセスがない。この結果、WCS では、MSE MAC およびキー ハッシュを WLC にプッシュできません。

通知が外部パートナー アプリケーションに届かない

MSE からの通知をパートナー アプリケーションが受信しない場合は、次のような原因が考えられます。

- MSE と外部アプリケーションの間の接続が確立されていない。XML および API のトラフィックを確認します。
- 外部リスナー アプリケーションが停止している。
- 外部リスナーで着信通知を解析する処理が遅い。この場合、MSE では、外部リスナーの処理を待機します。その結果、MSE 送信キューで輻輳が発生することがあります。
- ネットワーク内で想定されるタグ通知フレームの量に比べて送信キューのサイズが相対的に小さい。この場合、MSE では通知をドロップします。特に動作の加速と減速に関して、タグの設定が妥当であることを確認します。MSE 通知パラメータにあるキュー サイズを大きくします。このドキュメントの「ノースバウンド通知」セクションを参照してください。

有線ロケーションが機能しない

有線ロケーションを使用する場合に要素がまったく追跡されないときは、次のような原因が考えられます。

- MSE と有線スイッチの間の NMSP 接続に問題がある。
- 有線スイッチで、有線ロケーションをサポートしていない、より古いバージョンを実行している。
- 有線スイッチは適切なバージョンだが、NMSP がイネーブルにされていない。CLI オプションでイネーブルにしてください。
- 接続されているクライアントの追跡を開始するには、有線スイッチの IP 追跡オプションをイネーブルにしてある必要がある。
- 有線スイッチが、WCS に追加されていなかった。
- WCS に有線スイッチを追加するときは、次のような問題の発生が考えられます。
    - SNMP コミュニティ ストリングが正しくない
    - スイッチ OID が WCS でサポートされていない。
- 有線スイッチは WCS に追加されたが、MSE と同期されていない。
- 有線スイッチは同期で使用可能。[Location Capable] フラグをイネーブルにしてスイッチが WCS に追加されていることを確認します。
- 有線スイッチは、単一の MSE との 1 つの NMSP 接続のみをサポートしている。
- MSE 追跡パラメータで、有線追跡がイネーブルにされていない。

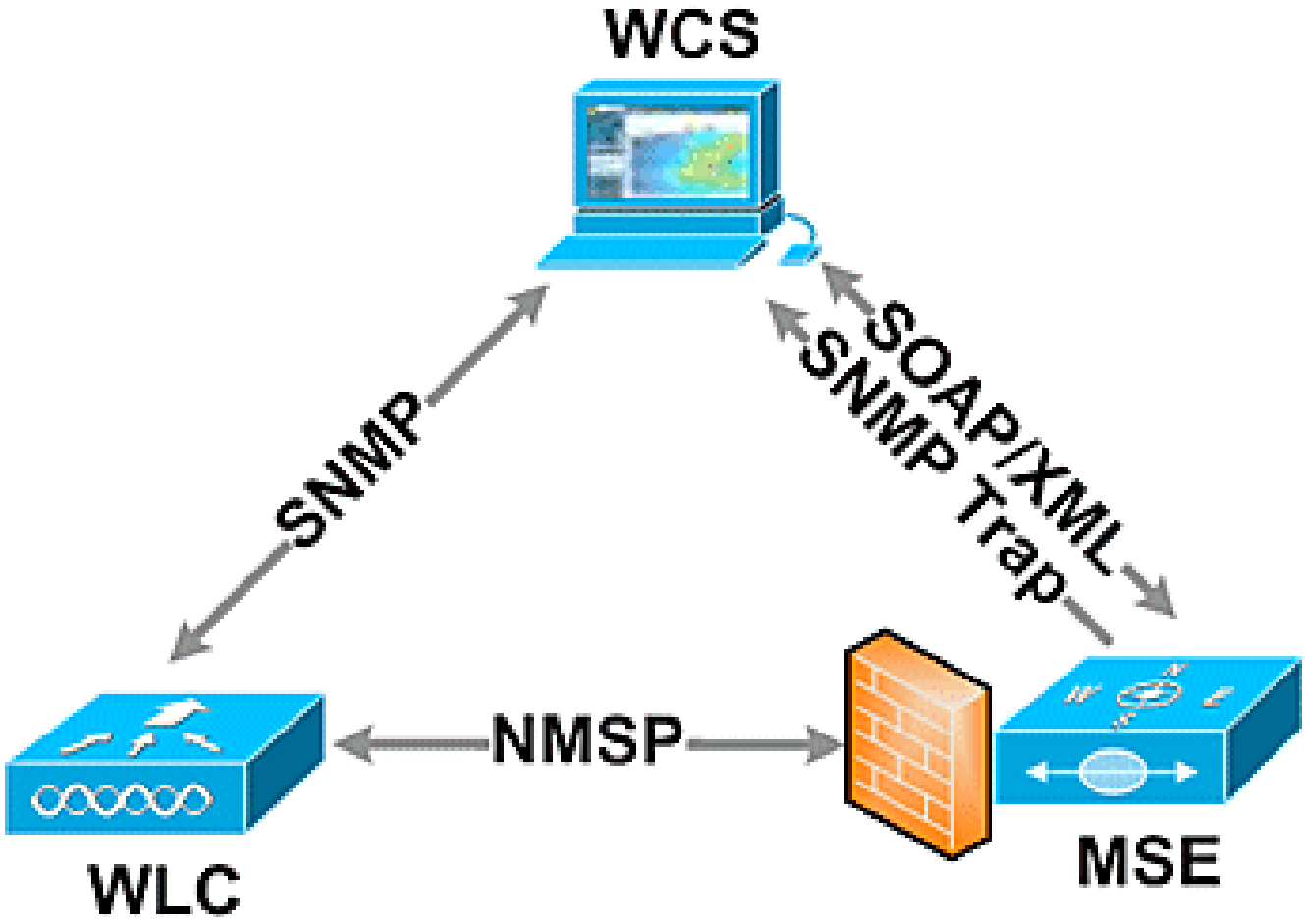
MSE ライセンス

- ライセンスをインストールすると UDI 不一致メッセージが出る：MSE ライセンスは、MSE UDI と関連付けられるため、正しい MSE を対象として作成されたライセンスをインストールしていることを確認してください。異なる MSE 間でのライセンスの交換はできません。
- この MSE で許可されている制限を超える要素があるため、ライセンスのインストールがブロックされている：「はじめに」セクションの説明を参照して、さまざまな MSE プラットフォーム上の各サービスのライセンス キャパシティを確認します。
- 2 つのライセンスを連続してインストールまたは削除しようとすると エラーが表示されることがある：これは、CAS ライセンスをインストールするたびにすべてのサービスが再開され、wIPS ライセンスをインストールするたびに wIPS サービスが再開されることが原因です。別のライセンスのインストールに進む前に、すべてのサービスが起動されていることを確認してください。
- MSE ライセンスは、/opt/MSE/licenses にインストールされます。

ネットワーク接続の確認

MSE、WLC、および WCS 間の接続がファイアウォールによってブロックされていないことを確認します。これらのマシンのファイアウォールをオフにする必要がある場合は、ワイルドカードルールを作成して、これらのマシンが互いに正常に通信できるようにしてください（図 53 を参照）。

図53：ネットワーク接続の確認



WLC と MSE の間の NMSP 接続の確認

```
(Cisco Controller) >show nmsp status

LocServer IP    TxEchoResp        RxEchoReq    TxData    RxData
--------------  -----------       ---------    --------   -------
172.20.224.17       18006           18006        163023      10

(Cisco Controller) >show auth-list

<snip>

Mac Addr                  Cert Type    Key Hash
------------------------  ----------   ----------------------------------------
00:1e:0b:61:35:60         LBS-SSC      5384ed3cedc68eb9c05d36d98b62b06700c707d9
```

MSE を WCS に追加した後で NMSP 接続が確立されない原因の 1 つとして、WLC と MSE の時

刻の不一致が考えられます。NTP サーバを使用して時刻を同期することをお勧めします。この方法を取れない場合は、WLC および MSE の時刻を手動で設定できます。システム クロックに関する主な問題は、WLC の時刻が MSE に設定されている時刻より後でないことです。

注：コントローラ間の時刻同期は、大規模な複数のWLCの導入では不可欠です。

NMSP セッションがまだ確立されない場合は、ネットワーク管理者が MSE キー ハッシュを WLC に入力して、NMSP セッションを手動でセットアップできます。

```
MSE
root@mse ~]# cmdshell
cmd> show server-auth-info
invoke command: com.aes.server.cli.CmdGetServerAuthInfo
----------------
Server Auth Info
----------------
MAC Address: 00:1e:0b:61:35:60
Key Hash: 5384ed3cedc68eb9c05d36d98b62b06700c707d9
Certificate Type: SSC


WLC
(Cisco controller) >config auth-list add lbs-ssc <MSE Ethernet MAC> <MSE key hash>
```

MSE の動作可能性と WLC からのタグ情報およびクライアント情報の受信の確認

MSE 上で getserverinfo コマンドを発行すると、次のような出力が生成されます。

```
[root@MSEWCS4 ~]# getserverinfo
MSE Platform is up, getting the status

-------------
Server Config
-------------

Product name: Cisco Mobility Service Engine
Version: 6.0.49.0
Hw Version: V01
Hw Product Identifier: AIR-MSE-3350-K9
Hw Serial Number: MXQ828A4L9
Use HTTP: false
Legacy HTTPS: false
Legacy Port: 8001
Log Modules: 262143
Log Level: INFO
Days to keep events: 2
Session timeout in mins: 30
DB backup in days: 2

-------------
Services
-------------
```

```
Service Name: Context Aware Service
Service Version: 6.0.35.0
Admin Status: Enabled
Operation Status: Up

Service Name: Wireless Intrusion Protection Service
Service Version: 1.0.1096.0
Admin Status: Enabled
Operation Status: Up

--------------
Server Monitor
--------------

Mon Mar 16 14:43:52 PDT 2009
Server current time: Thu Apr 02 14:55:00 PDT 2009
Server timezone: America/Los_Angeles
Server timezone offset: -28800000
Restarts: 3
Used Memory (bytes): 166925392
Allocated Memory (bytes): 238354432
Max Memory (bytes): 1908932608
DB virtual memory (kbytes): 6694
DB virtual memory limit (bytes): 0
DB disk memory (bytes): 241696768
DB free size (kbytes): 6304

---------------
Active Sessions
---------------

Session ID: 17155
Session User ID: 1
Session IP Address: 172.20.224.30
Session start time: Tue Mar 17 16:50:48 PDT 2009
Session last access time: Thu Apr 02 14:50:30 PDT 2009

-------------
Context Aware Service
-------------

Total Active Elements(Clients, Rogues, Interferers): 2263
Active Clients: 591
Active Tags: 24
Active Rogues: 1648
Active Interferers: 0
Active Wired Clients: 0
Active Elements(Clients, Rogues, Interferers) Limit: 6000
Active Tag Limit: 100
Active Wired Clients Limit: 0
Active Sessions: 1
Clients Not Tracked due to the limiting: 0
Tags Not Tracked due to the limiting: 0
Rogues Not Tracked due to the limiting: 0
Interferers Not Tracked due to the limiting: 0
Wired Clients Not Tracked due to the limiting: 0
Total Elements(Clients, Rogues, Interferers)
   Not Tracked due to the limiting: 0

-------------
Context Aware Sub Services
-------------
```

```
Sub Service Name: AeroScout
Version: 3.2.0 - 4.0.14.9
Description: AeroScout® Location Engine
   for RSSI and TDOA asset tracking
Registered: true
Active: true
Watchdog Process ID: 8492
Engine Process ID: 8665
[root@MSEWCS4 ~]#
```

WLC による RFID タグの検出の確認

タグは、3 個のチャネル (1、6、11) で送信し、3 回以上反復するように設定されている必要があります。

例： 1,6,11, 1,6,11, 1,6,11

コントローラ上のグローバル RFID 設定を確認します。

```
show rfid config
```

RFID タグの検出がイネーブルにされていない場合は、次のコマンドを使用してイネーブルにします。

```
config rfid status enable
```

タイムアウト パラメータを確認、設定します。

```
config rfid timeout 1200
config rfid auto-timeout disable
```

RSSI の有効期限のタイムアウトを確認します。

```
show location summary
```

WLC がまだタグを検出しない場合は、次のデバッグ コマンドを使用します。

```
debug mac addr <tag mac addr>
debug rfid receive enable
```

WLC でタグを検出するかどうかを確認します。

```
show rfid summary
show rfid detail <MAC address>
```

WLC ではタグを検出する一方で、WCS では検出しない場合は、NMSP 通知が MSE に送信されているかどうかを確認します。

```
debug rfid nmsp enable
```

WLC における NMSP 通知のイネーブル化の確認

```
show nmsp subscription summary
Server IP        Services
<MSE IP>    RSSI, Info, Statistics, IDS
```

WLC 上の NMSP レイヤによる通知の送信が行われているかどうかを確認します。

```
debug nmsp message tx enable
```

RSSIカットオフ：MSEは、4つの最高信号強度値と、RSSIカットオフ値と一致するか、それを超える信号強度レポートを保持します。デフォルトは、-75 dBm です。

show rfid summary コマンド（WLC）

このコマンドは、AP によって報告されたすべての RFID タグをリストします。次の情報を含みます。

- RFID MAC アドレス
- 一番近い AP
- RSSI 値
- タグを最後に読み取ってからの経過時間

```
(Cisco Controller) >show rfid summary
Total Number of RFID   : 4
```

```
----------------- -------- ------------------ ------ ---------------------
     RFID ID      VENDOR       Closest AP      RSSI  Time Since Last Heard
----------------- -------- ------------------ ------ ---------------------
00:04:f1:00:04:ea Wherenet sjc14-42b-ap4       -69       52 seconds ago
00:04:f1:00:04:eb Wherenet sjc14-42b-ap4       -75       27 seconds ago
00:0c:cc:5b:fc:54 Aerosct  sjc14-31b-ap9       -87       63 seconds ago
00:0c:cc:5b:fe:29 Aerosct  sjc14-31b-ap2       -92       22 seconds ago
```

show rfid detail コマンド

このコマンドに MAC アドレスを指定すると、RFID タグのパラメータの詳細が表示されます。

```
(Cisco Controller) >show rfid detail 00:0c:cc:5b:fe:29

RFID address..................................... 00:0c:cc:5b:fe:29
Vendor........................................... Aerosct
Last Heard....................................... 4 seconds ago
Packets Received................................. 561211
Bytes Received................................... 16836330
Detected Polling Interval........................ 14 seconds
Bluesoft Type.................................... TYPE_NORMAL
Battery Status................................... MEDIUM
Nearby AP Statistics:
      sjc14-41b-ap8(slot 0, chan 6) 3 seconds.... -88 dBm

(Cisco Controller) >
```

WLC による Wi-Fi クライアントの検出の確認

クライアントが関連付けられている AP を判別し、AP で検出する RSSI 値を判別します。

```
show client summary
show client detail <MAC address>
```

クライアントの RSSI タイムアウトが、デフォルト値に設定されていることを確認します。

```
show location summary
```

RSSI 値がデフォルト値と異なる場合は、次のコンフィギュレーション コマンドを使用してデフォルトに設定します。

```
config location expiry client <seconds>
config location rssi-half-life client <seconds>
```

ロードバランシングデバッグを有効にし、クライアントを受信したAPとRSSIを表示します。

```
debug mac addr <client mac>
debug dot11 load-balancing enable
```

次のコマンドを使用して通知関連の問題をデバッグします。

```
debug mac addr <client mac>
debug dot11 locp enable
debug nmsp message tx enable
```

“「show client summary」コマンド

```
(Cisco Controller) >show client summary

Number of Clients................................ 276

<snip>

MAC Address       AP Name           Status        WLAN/Guest-Lan Auth Protocol Port Wired
----------------- ----------------- ------------- -------------- ---- -------- ---- -----

00:02:8a:ea:55:15 sjc14-12b-ap5     Associated    7               Yes  802.11b   2    No
```

“「show client detail」コマンド

```
Cisco Controller) >show client detail 00:02:8a:ea:55:15

<snip>

Nearby AP Statistics:
    TxExcessiveRetries: 0
    TxRetries: 0
    RtsSuccessCnt: 0
    RtsFailCnt: 0
    TxFiltered: 0
    TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
      sjc14-11b-ap2(slot 0) .....................
antenna0: 308 seconds ago -86 dBm.................
   antenna1: 308 seconds ago -80 dBm
      sjc14-11b-ap1(slot 0) .....................
antenna0: 307 seconds ago -82 dBm.................
   antenna1: 307 seconds ago -91 dBm
      sjc14-12b-ap6(slot 0) .....................
antenna0: 307 seconds ago -66 dBm.................
```

```
   antenna1: 307 seconds ago -66 dBm
      sjc14-12b-ap3(slot 0) .....................
antenna0: 307 seconds ago -76 dBm.................
   antenna1: 307 seconds ago -64 dBm
      sjc14-12b-ap5(slot 0) .....................
antenna0: 7217 seconds ago -53 dBm................
   antenna1: 7217 seconds ago -48 dBm
      sjc14-11b-ap5(slot 0) .....................
antenna0: 7217 seconds ago -79 dBm................
   antenna1: 7217 seconds ago -75 dBm
```

セクション4：最終チェックリスト

ハードウェア要件

表3: Cisco MSE 3310 – ハードウェア仕様

項目	説明
フォームファクタ	1U ラック フォーム ファクタ、高さ 4.45 cm（1.75 インチ）、奥行 70.5 cm（27.75 インチ）
プロセッサ	Intel Core2 Duo（1.8 GHz）
メモリ	4 GB（PC2-5300）
ハード ディスク ドライブ	2 x 250 GB（SATA）
ロケーション追跡キャパシティ	最大 2,000 台のデバイス（最大 1,000 台のクライアントおよび最大 1,000 台のタグ）
接続	ネットワーク：組み込み型マルチファンクション ギガビットネットワークアダプタX 2（TCP/IPオフロードエンジン搭載）
電源	120/240V AC 電源 X 1

モジュール	
ネットワーク管理	Internet Explorer 6.0 Service Pack 1 以降が実行される Cisco WCS Location v5.2 以上
サポートされるネットワーク デバイス	Cisco 2100、4400シリーズワイヤレスLANコントローラ、Cisco Catalyst 6500シリーズワイヤレスサービスモジュール、Cisco Catalyst 3750G Integrated Wireless LAN Controller、サービス統合型ルータ用Cisco Wireless LAN Controller Module（WLCMおよびWLCM-E）、Cisco Aironet Lightweightアクセスポイント

表4: Cisco MSE 3550 – ハードウェア仕様

項目	説明
フォームファクタ	1U ラック フォーム ファクタ、高さ 4.45 cm（1.75 インチ）、奥行 70.5 cm（27.75 インチ）
プロセッサ	2 クアッドコア インテル Xeon プロセッサ（2.33 GHz）
メモリ	8 GB PC2-5300（4 x 2 GB）
ハード ディスク ドライブ	ホットプラグ対応SAS（シリアル接続SCSI）ドライブ：146 GB(10,000 RPM)X 2
ロケーション追跡キャパシティ	最大 18,000 台のデバイス（クライアントおよびタグの組み合わせは任意）
接続	ネットワーク：組み込み型マルチファンクション

	ギガビットネットワークアダプタX 2（TCP/IPオフロードエンジン搭載）
電源モジュール	2 基の冗長 120/240V AC（ホットスワップ可能）
ネットワーク管理	Internet Explorer 6.0 Service Pack 1 以降が実行される Cisco WCS Location v5.1 以上
サポートされるネットワーク デバイス	Cisco 2100、4400シリーズワイヤレスLANコントローラ、Cisco Catalyst 6500シリーズワイヤレスサービスモジュール、Cisco Catalyst 3750G Integrated Wireless LAN Controller、サービス統合型ルータ用Cisco Wireless LAN Controller Module（WLCMおよびWLCM-E）、Cisco Aironet Lightweightアクセスポイント

Cisco 2710 から Cisco MSE へのロケーション サービスの移行

シスコでは、MSE プラットフォームの導入までは、Cisco 2710 ベースのソリューションによってロケーション ベースのサービスを提供していました。表 5 では、この 2 つのソリューションを比較し、MSE ソリューションの長所を示しています。

表5: Cisco 2710とCisco MSE

機能	Cisco 2710	MSE
サポートされるお客様の環境	天井の低い屋内（RSSI）	天井の低い屋内（RSSI）、天井の高い屋内（TDoA）、屋外（TDoA）
サポートされるロケーション テクノロジー	RSSI のみ	RSSI TDoA
サポートされるロケーション エンジン	シスコのみ	シスコ パートナー エンジン
追跡されるWi-Fiデバイスの最大数	2,500	18,000

サポートされるサービスの数	単一（ロケーションのみ）	複数（Context Aware モビリティ ソリューション、wIPS、将来のサービス）
サポートされるタグ	CCX または非 CCX（ポーリングのみ）	CCX
レールとリージョン	はい（クライアントおよびタグ）	はい（クライアントのみ）タグ：AeroScout セルおよびマスク機能
ロケーション センサー	サポート対象外	サポート対象外

既存 Cisco 2710 インストールのあるお客様は、設定を保持しながら新規 Cisco MSE に移行できます。

ソフトウェア要件

Context Aware ソフトウェア用 Cisco Aironet 1000 シリーズ アクセス ポイントは、バージョン 4.2.xxx（xxx>112）でのみサポートされています。

注：Cisco Aironet 1000シリーズアクセスポイントは、サポート終了および販売終了の製品です。Cisco Context Aware ソリューション用 Cisco Aironet 1000 シリーズ アクセス ポイントは、バージョン 4.2.xxx（xxx>112）でのみサポートされています。Cisco 3300シリーズMobility Services Engine上のCisco Context-Awareソリューションのみがサポートされています。Cisco 3300シリーズMobility Services Engine上のその他のサービスはサポートされていません。5.x.xxx バージョンおよび以降のバージョンのソフトウェアでは、Cisco Aironet 1000 シリーズ アクセス ポイントをサポートしません。Cisco Aironet 1130、1140、1240、または 1250 シリーズ アクセス ポイントに移行して、導入された最新機能を活用することをお勧めします。後継製品の詳細については、シスコにお問い合わせください。

表 6 に、MSE、WLC、および WCS 上で使用する必要のあるソフトウェア リリースをリストします。縦の各列は、MSE、WLC、および WCS の互換バージョンを表します。

表6：ソフトウェア互換性マトリクス

サービス	システム コンポーネント	最低限のソフトウェア リリース			
CAS および wIPS[1]	MSE	リリース 5.1.30.0	リリース 5.1.35.0	リリース 5.2.91.0	リリース 6.0.75.0
	Cisco Wireless LAN Controller（WLC）	リリース 4.2:4.2.130（またはそれ以降）リリース 5.1:5.1.151.0（またはそれ以降）	リリース 4.2:4.2.130（またはそれ以降）リリース 5.1:5.1.163.0（またはそれ以降）	リリース 4.2:4.2.130（以上）リリース 5.2:5.2.157.0（以上）リリース 5.1:5.1.151.0（以	リリース 4.2:4.2.130（以上）リリース 5.2:5.2.157.0（以上）リリース 5.1:5.1.151.0（以

				上）	上）リリース6.0:6.0.182.0以上注：リリース5.0.xはMSEをサポートしていません。
	Cisco WCS	リリース5.1:5.1.64.0（またはそれ以降）	リリース5.1.65.4（以上）	リリース5.2:5.2.110.0（またはそれ以降）	リリース6.0:6.0.132.0以上
	Cisco WCS Navigator	リリース1.3.64.0（以上）	リリース1.3.65.4（以上）	リリース1.4.110.0 以上	リリース1.4.110.0 以上

注：[1]リリース5.2は、コントローラ、WCS、およびMSEでwIPSをサポートするための最小ソフトウェア要件です。

注：WCSソフトウェアのバージョンはMSEソフトウェアのバージョンと同じである必要があります。つまり、MSE 6.0.xを実行する場合、WCSも6.0.xである必要があります。ソフトウェア リリース 6.0 からはライセンスが適用されています。

展開チェックリスト

ワイヤレスの設計

- 適切な AP 配置のガイドライン（ロケーションおよび密度）に従います。適切な AP 周辺部のカバレッジを確認します。AP の密度と配置の判別に、WCS Planning ツールを使用できます。
- サイト調査ツールおよび WCS（Location Readiness ツール）を利用して、Wi-Fi カバレッジを確認します。
- AP 配置を確認して、カバレッジ ホールをなくします。ロケーション最適化監視モード AP を利用して、カバレッジ ホールを埋めます。
- WCS の [MSE Synchronization] ページで、いずれのコントローラがいずれの MSE と通信する必要があるのかを指定します。
- 証明書が正しく交換されていることを確認します。

WLC

- すべての AP および無線が起動しており、Radio Resource Manager（RRM）がイネーブルにされていることを確認します。
- WLC と MSE の両方に NTP サーバを設定するか、適切な時刻および時間帯によって両方のデバイス（およびできれば WCS）を手動で同期します。

  注：WLCはGMT(UTC)時間と正しいタイムゾーンを使用してローカル時間を導出するため、時間はUTCで入力し、正しいタイムゾーンを指定する必要があります。

- 次のコマンドを使用して、クライアントおよびタグが WLC によって検出されていることを確認します。show [rfid | client] summary
- WLC で show nmsp status コマンドを使用するか、WCS で [Services] > [Mobility services] > ["MSE"] > [System] >[Active Sessions] に移動して、MSE とコントローラの間に NMSP が確立されていることを確認します。
- show nmsp subscription summary コマンドを使用して、WLC が適切なサービスにサブスクライブされているかどうかを確認します。
- CCXクライアントの精度をテストする場合は、CCXが有効になっていることを確認します。config location plm client enable <interval>設定を確認するには、次のコマンドを使用します。show location plm
- WLC には、次のデフォルト NMSP パラメータが設定されている必要があります。

  使用するアルゴリズム：

  クライアント

  - RSSI期限切れタイムアウト：5秒
  - 半減期：0秒
  - 通知しきい値：0 db

  調整クライアント

  - RSSI期限切れタイムアウト：5秒
  - 半減期：0秒

  不正な AP

  - RSSI期限切れタイムアウト：5秒
  - 半減期：0秒
  - 通知しきい値：0 db

  RFID タグ

  - RSSI期限切れタイムアウト：5秒
  - 半減期：0秒
  - 通知しきい値：0 db

  コンフィギュレーション コマンド

  config location <cmd>

これらの値を確認するコマンド

show location summary

WCS/MSE

- WLC と MSE の両方に NTP サーバを設定するか、適切な時刻および時間帯によって両方のデバイス（およびできれば WCS）を手動で同期します。
- ロケーション計算が実行されていることを追跡ページまたは MSE コンソール（getserverinfo コマンドを使用）で確認します。
- WCS の「監査」機能を使用して、WCS の値と WLC の値が一致していることを確認します。
- すべての AP にマップが割り当てられていることを確認します。
- MSE は、ネットワーク設計、WLC、有線スイッチ、およびイベントと同期されている必要があります。
- マップおよび AP の位置が、WCS と MSE の間で同期されていることを確認します。
- MSE 上で、クライアントおよびタグの追跡が [Services] > [Mobility Services] > [<MSE>] > [Context Aware Service] > [Administration] > [Tracking Parameters] の下でイネーブルにされている必要があります。
- WCS の [Monitor] > [Client/Tag] の下で、クライアントおよびタグが表示されていることを確認します。
- クライアントおよびタグが WCS に表示されない場合は、クライアントおよびタグのライセンスが MSE にインストールされていることを確認します。Context Aware（WCS PLUS）をサポートする適切なバージョンの WCS がインストールされていることも確認します。
- WCS で調整ツールを使用して、個別の環境に合わせて信号特性を調整します。
- ロケーション レールとリージョン（クライアントの追跡）およびセルとマスク（タグの追跡）を使用して、Wi-Fi クライアントが存在する可能性のあるまたはない、フロア マップ上の個別エリアを包含または除外します。
- WCS にある確度ツールを使用して、ロケーションの確度のレベルを確認します。

クライアントの場合

- MSE 上で追跡がイネーブルにされていることを確認します。
- クライアントが WLC によって検出されていることを確認します。

タグの場合

- MSE 上で追跡がイネーブルにされていることを確認します。

- タグが WLC によって検出されていることを確認します。
- チャネル 1、6、11 がイネーブルにされている必要があります。
- チャネルごとの反復が 3 である必要があります。
- バッテリのステータスをチェックします。

セクション5：よくある技術的な質問

Q. RFフィンガープリントとは何ですか。RF 三角測量と同じものですか。

A. RFフィンガープリントは、2つの点に焦点を当てて口ケーションを決定する方法です。1つは、無線LANの特定の環境で電波がどのように相互作用するかを理解すること、もう1つは、これらの減衰特性をデバイスの信号情報に適用して、口ケーションを決定することです。三角測量では、環境変数を考慮しない代わりに、読み取った信号強度だけからデバイスの口ケーションを概算します。具体的な構築特性は、RF 信号の伝播および口ケーション判別の確度に影響することがあるため、RF フィンガープリントで考慮されます。

Q.口ケーションの忠実度はどのようになりますか。

A.口ケーションは統計的な性質を持ちます。シスコの口ケーションの確度仕様では、10 m 以内にある確率を 90 %、5 m 以内にある確率を 50 % としています。

Q.情報はリアルタイムですか。

A.口ケーション情報および関連するクライアント情報の応答時間は、主にシステム処理の機能です。応答時間は、一般的に、数秒から数分の範囲になることがあります。

Q. MSEはどの程度スケーラブルですか。

A. Cisco MSE 3350では、最大18,000台のデバイスを追跡できます。サポートするデバイスの台数を増やすには、同じシステムに追加の MSE を追加できます。同時デバイス数の上限は、MSE の処理能力に基づきます。

Q.口ケーション履歴はどのくらいの期間保存できますか。

A. MSEが保存およびリプレイできる口ケーション履歴の量は設定可能です。デフォルト値は 30 日です。

Q.口ケーショントラフィックはネットワークにどのような影響を与えますか。

A.口ケーショントラフィックの量は、コントローラの数、APの数、そして最終的には特定のネットワークインフラストラクチャによって追跡されるデバイスの数に依存します。ネットワークの成長に伴って AP からワイヤレス コントローラに転送されるトラフィックが増え、このトラフィックが MSE に転送されます。個々の測定によるトラフィックの量はわずかですが、測定の数はデバイスの数と測定頻度によって変わります。

Q. MSEはどのように管理されるのですか。

A.クライアント用Context Aware Engineを使用したクライアントトラッキングの場合、CLIコマンドによる初期セットアップの他に、MSEのすべての設定と管理はWCSを介して実行されます。タグ用 Context Aware Engine を使用する場合（屋内および屋外または屋外に似た環境でタグを追跡）は、シスコ（WCS）と AeroScout（システム マネージャ）の両方のネットワーク管理ソリューションが必要です。

Q. MSEをサポートするためにワイヤレスLANアーキテクチャに必要なものは何ですか。

A. MSEは、LWAPP対応インフラストラクチャなど、Cisco Centralized Wireless LAN(CWLAN)アーキテクチャでのみ動作します。ロケーションには、適切な AP 配置が不可欠です。このドキュメントの説明に従って、カバレッジ エリアの周辺部付近および内部に AP を配置する必要があります。「既存のデータおよび音声サービスがあるときの Context Aware 展開の考慮事項」セクションを参照してください。Context Aware Engine のライセンスのある WCS が必要です。

Q. WCSとMSEで提供されるロケーションの違いは何ですか。

A. WCSベースは、特定のデバイスを検出できるAPと、そのデバイスが検出された信号強度を示します。ロケーション対応の WCS では、高度な RF フィンガープリントを使用しており、オンデマンド方式で単一デバイスのロケーションを正確に特定できます。MSE では、ロケーション対応の WCS と同じロケーション方式を使用しますが、Cisco MSE 3350 を使用すれば、同時に最大 18,000 台のデバイスを追跡できます。これにより、サードパーティ アプリケーションでは、資産の追跡など、アプリケーション用のデバイス情報の履歴を利用できます。

Q.クライアントを見つけるためにクライアントソフトウェアは必要ですか。

A.クライアントソフトウェアは必要ありません。ロケーションは、ワイヤレス LAN インフラストラクチャに直接統合されるため、AP では、データ、音声、およびその他のアプリケーションに対して通常行うように、Wi-Fi デバイスをリッスンします。CCX クライアントは、CCX 以外のクライアントよりも確実に追跡されます。したがって、CCX（v4 または v5）互換のクライアントを購入されることを推奨します。

Q. Wi-Fiタグは、バッテリを交換する前にどのくらいの期間使用できますか。

A.タグのバッテリ寿命は、特定のデバイスのバッテリ寿命と、ビーコンまたは点滅の頻度に依存します。タグの寿命は、場所を問わず 100 日間から 1 年程度であり、もっと長いものもあります。メーカーによっては、3 ~ 5 年の寿命を宣伝していますが、これもビーコン レートによって異なります。

Q. Wi-Fiタグのコストはいくらですか。

A.タグの製造元に問い合わせてください。シスコではタグの製造および再販を行っていません。タグの価格はさまざまで、量によっても異なります。Wi-Fi タグでは、ロケーションを連続的に表示でき、再利用可能なバッテリ電源を使用するため、パッシブな RFID タグよりも高価です。Wi-Fi タグはアクティブに信号を送信し、一般に到達範囲も広く（数百フィート）、さまざまな取り付けオプションを持つ多様なフォーム ファクタのものが用意されています。アクティブ RFID は、主に、通常パッシブ RFID によって追跡される資産よりも、移動が多い高価な資産または法的責任の重い資産を、より連続的に追跡する場合に使用します。

付録A:MSEの設定

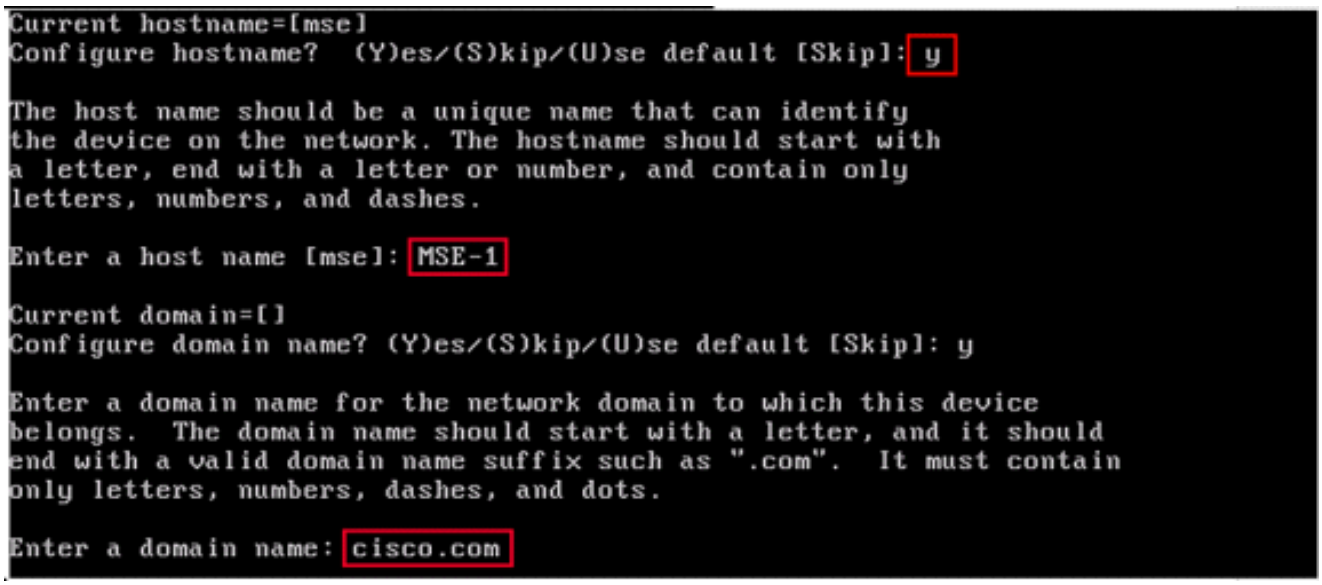
次のステップを実行します。

1. ログイン:root/passwordのクレデンシャルでログインします。
2. セットアッププロセスの開始：初期ブート時に、MSEは管理者にセットアップスクリプトの起動を求めるプロンプトを表示します。このプロンプトで「yes」を入力します。

   注：MSEからセットアップのプロンプトが表示されない場合は、次のコマンドを入力します。

   ```
   /opt/mse/setup/setup.sh
   ```

3. ホスト名と DNS ドメイン名の設定：



4. イーサネット インターフェイス パラメータの設定：

```
Current IP address=[1.1.1.10]
Current eth0 netmask=[255.255.255.0]
Current gateway address=[1.1.1.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter an IP address for first ethernet interface of this machine.

Enter eth0 IP address [1.1.1.10]: 172.20.229.200

Enter the network mask for IP address 172.20.229.200.

Enter network mask [255.255.255.0]: 255.255.255.0

Enter an default gateway address for this machine.

Note that the default gateway must be reachable from
the first ethernet interface.

Enter default gateway address [1.1.1.1]: 172.20.229.1
```

2 つ目の NIC は動作に必要ないため、「eth1」インターフェイス パラメータを要求するプロンプトが表示されたら、「Skip」を入力して次のステップに進みます。

注：設定するアドレスは、対象のワイヤレスLANコントローラとこのアプライアンスで使用するWCS管理システムにIP接続を提供する必要があります。

5. DNSサーバ情報の入力：ドメインの解決に必要なDNSサーバは1つだけです。復元力を確保するには、バックアップサーバを入力します。

```
Domain Name Service (DNS) Setup
DNS is currently enabled.
No DNS servers currently defined
Configure DNS related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enable DNS (yes/no) [yes]: y
Enter primary DNS server IP address: 172.20.229.10
Enter backup DNS server IP address (or none) [none]: 172.20.229.20
Enter another backup DNS server IP address (or none) [none]:
```

6. タイムゾーンの設定:New Yorkのデフォルトタイムゾーンが環境に適用されない場合は、ロケーションメニューを参照して正しく設定します。

```
Current timezone=[America/New_York]
Configure timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
```

7. NTPまたはシステム時間の設定:NTPはオプションですが、システムが正確なシステム時間を維持することを保証します。「No」を選択した場合は、システムの現在時間を設定します。

```
Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be
configured from NTP servers that you select.  Otherwise,
you will be prompted to enter the current date and time.

NTP is currently disabled.
Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter whether or not you would like to set up the
Network Time Protocol (NTP) for this machine.

If you choose to enable NTP, the system time will be
configured from NTP servers that you select.  Otherwise,
you will be prompted to enter the current date and time.

Enable NTP (yes/no) [no]: yes
Enter NTP server name or address: time.nist.gov
Enter another NTP server IP address (or none) [none]:
```

注：モビリティサービスエンジン、ワイヤレスLANコントローラ、およびWCS管理システムで正しい時刻を設定する必要があります。これは、この 3 つのシステムすべてで同じ NTP サーバを指し、正しい時間帯をこれらに設定することによって実現できます。

8. Enable Local Console Root Login：このパラメータは、システムへのローカルコンソールアクセスを有効または無効にするために使用します。ローカル トラブルシューティングを実施するには、これをイネーブルにする必要があります。

```
Remote root login is currently disabled.
Configure remote root access? (Y)es/(S)kip/(U)se default [Skip]: yes

Enter whether or not you would like to allow
remote root login via secure shell for this machine.

Enable remote root login (yes/no) [no]: yes
```

9. Enable SSH (Secure Shell) Root Login:オプション：このパラメータは、システムへのリモートコンソールアクセスを有効/無効にするために使用されます。リモート トラブルシューティングを行うには、これをイネーブルにする必要があります。ただし、企業のセキュリティ ポリシーによっては、このオプションをディセーブルにする必要があります。

```
SSH root access is currently disabled.
Configure ssh access for root (Y)es/(S)kip/(U)se default [Skip]: yes

Enter whether or not you would like to enable ssh
root login. If you disable this option, only console
root login will be possible.

Enable ssh root access (yes/no): yes
```

10. シングルユーザモードとパスワード強度の設定：これらの設定パラメータは必須ではなく、デフォルト設定はこれをスキップする「s」の入力です。

```
Single user mode password check is currently disabled.
Configure single user mode password check (Y)es/(S)kip/(U)se default [Skip]: s

Login and password strength related parameter setup
Maximum number of days a password may be used : 99999
Minimum number of days allowed between password changes : 0
Minimum acceptable password length : 5
Login delay after failed login :
Checking for strong passwords is currently disabled.
Configure login/password related parameters? (Y)es/(S)kip/(U)se default [Skip]:
s
```

11. ログインバナーの設定：ログインバナーは、ユーザにシステムの使用を通知し、権限のないユーザがシステムにアクセスするのを防ぐための警告を表示するために使用されます。ログイン バナーは複数行のメッセージにすることができるため、単一のピリオド (.) によってメッセージを終了し、次のステップに進みます。

```
Current Login Banner = [Cisco Mobility Service Engine]
Configure login banner (Y)es/(S)kip/(U)se default [Skip]: yes

Enter text to be displayed as login banner. Enter a single period
on a line to terminate.

Login banner [Cisco Mobility Service Engine]:
MSE-1
Unauthorized Access is not allowed
.
```

12. ルートパスワードの変更：この手順は、システムのセキュリティを確保するために重要です。必ず、辞書に記載されていない文字と数字で構成される強力なパスワードを選択してください。パスワードの最小長は 8 文字です。

```
Configure root password? (Y)es/(S)kip/(U)se default [Skip]: y

Enter a password for the superuser.

Enter root password:
Confirm root password:
```

13. GRUBパスワードの設定：オプション：この設定パラメータは必須ではなく、デフォルト設定でこれをスキップする場合は「s」を入力します。

```
GRUB password is not currently configured.
Configure GRUB password (Y)es/(D)isable/(S)kip/(U)se default [Skip]: s
```

14. WCS 通信パスワードの設定：

```
Configure WCS communication password? (Y)es/(S)kip/(U)se default [Skip]: yes

Enter a password for the admin user.
The admin user is used by the WCS and other northbound systems
to authenticate their SOAP/XML session with the server.
Once this password is updated, it must correspondingly be updated
on the WCS page for MSE General Parameters so that the WCS can
communicate with the MSE.

Enter WCS communication password:
Confirm WCS communication password:
```

15. Save Changes and Reboot：セットアップスクリプトが完了したら、プロンプトが表示されたら変更を保存します。保存後に、プロンプトに従って MSE をリブートし、すべての設定が正常に適用されたことも確認します。

16. MSEサービスを開始します。ステップ12で事前に設定したユーザ名rootとパスワードでMSEにログインします。コマンド service msed start を実行して、MSE サービスを開始します。

```
login as: root
Cisco Mobility Service Engine

root@172.20.226.203's password:
Last login: Wed Jul 23 10:11:58 2008 from dhcp-171-71-123-7.cisco.com
[root@MSE-1 ~]# service msed start
Starting MSE Platform
Cannot find UDI information. Exiting
null
Invalid Platform type. Now Exiting.
Starting MSE Platform, waiting to check the status.
Starting MSE Platform, waiting to check the status.
MSE Platform is up, getting the status
```

17. ブートアップ時にMSEサービスが開始されるようにする:chkconfig msed onコマンドを実行します。

MSE の WCS への追加

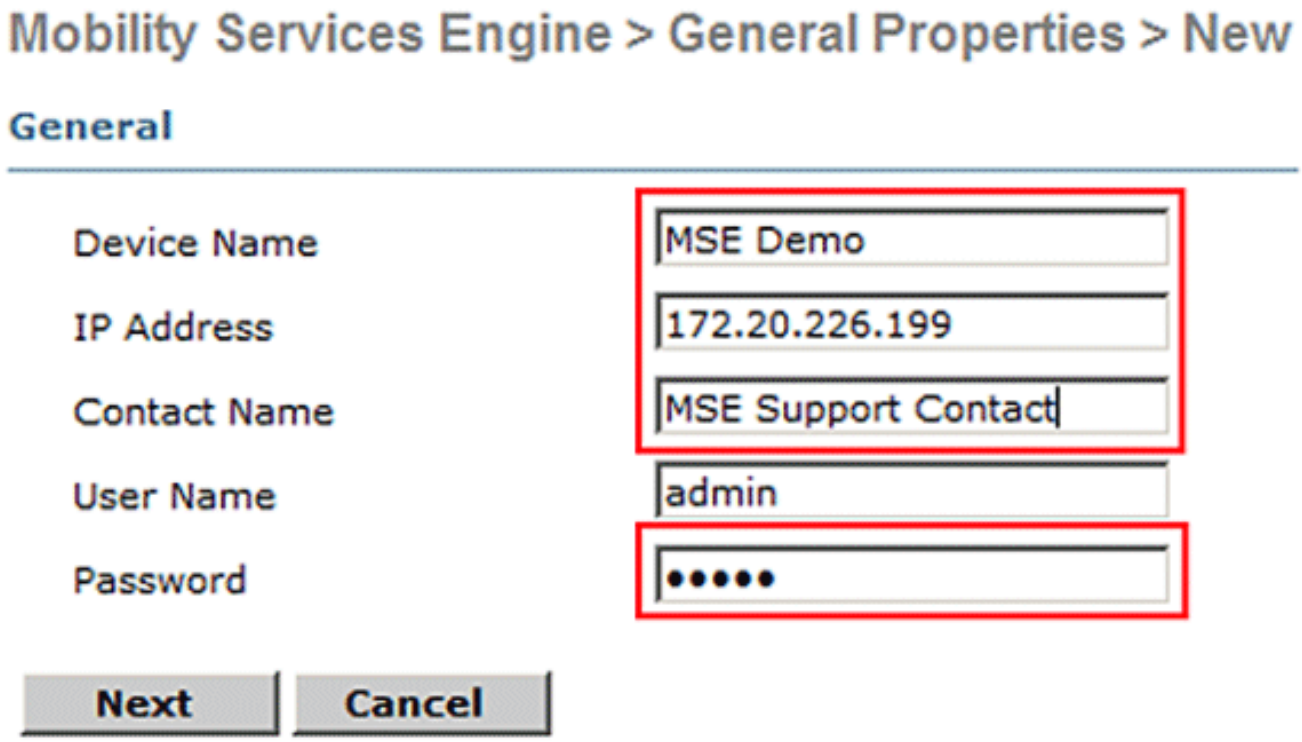
次のステップを実行します。

1. Mobility Services Configuration Page:WCSにログインして、Mobilityドロップダウンメニューから Mobility Servicesをクリックします。

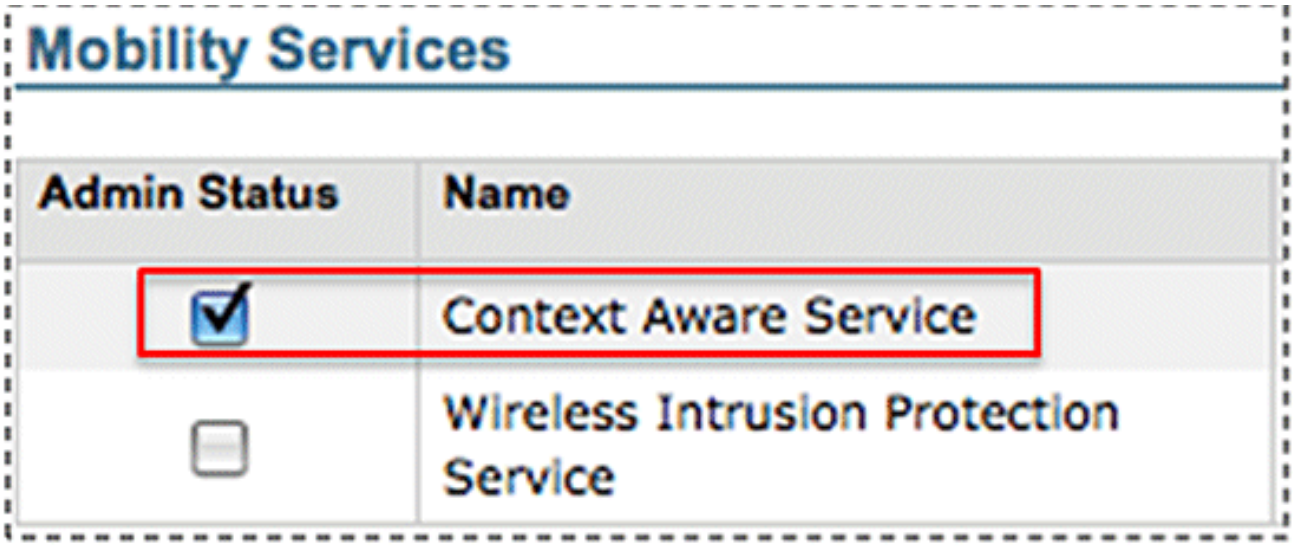
2. モビリティサービスエンジンをWCSに追加する：右側のドロップダウンメニューからAdd

Mobility Services Engineを選択し、Goをクリックします。

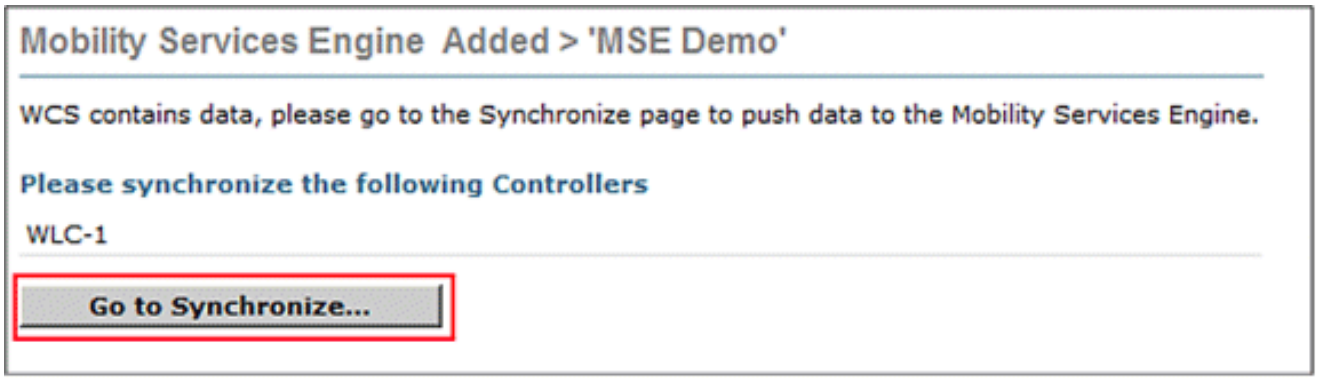
MSE の一意のデバイス名、MSE セットアップで事前に設定した IP アドレス、サポート用の連絡先名、および MSE セットアップ時に設定した「WCS 通信パスワード」を入力します。ユーザ名は、デフォルトの admin から変更しないでください。

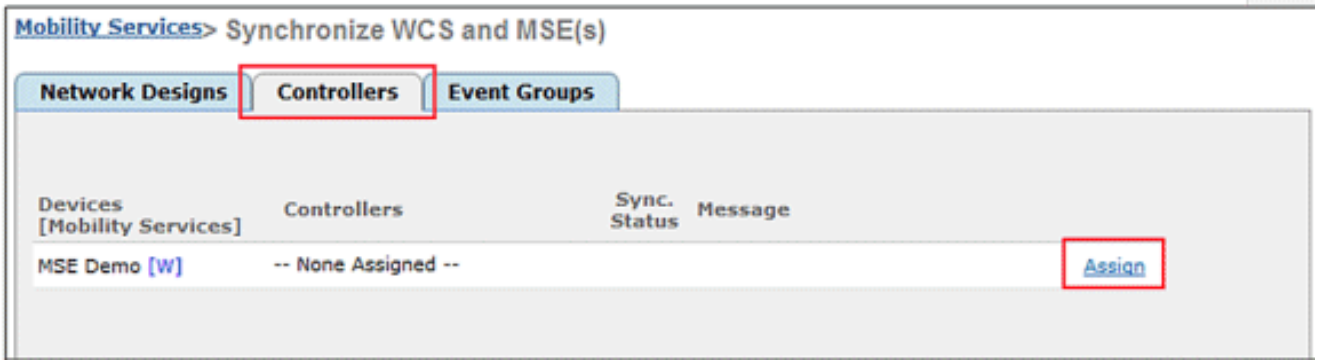


3. MSE 上で実行する Context Aware Service を選択します。



4. 同期:ネットワーク設計、コントローラ、およびイベントグループを必ず同期してください。





5. 同期するコントローラ:MSEを同期するコントローラのリストを示すポップアップが表示されます。同期するコントローラを選択し、[OK] をクリックします。

ポップアップ ウィンドウが閉じられてから、[Synchronize WCS and MSE(s)] ダイアログの下部にある [Synchronize] をクリックします。

注：Cisco Context Aware Serviceは、ワイヤレスLANコントローラ、WCS、およびMSE間の同期クロックに大きく依存しています。この 3 つのシステムすべてが同じ NTP サーバを指しており、同じ時間帯設定が設定されていなければ、Context Aware は正しく機能しません。トラブルシューティングを試行する前に、Context Aware システムのすべてのコンポーネントでシステム クロックが同一であることを確認してください。

付録B:WLCおよびMSEコマンド

WLC コマンド

<#root>

```
config location expiry ?
```

```
client         Timeout for clients
calibrating-client Timeout for calibrating clients
tags           Timeout for RFID tags
rogue-aps      Timeout for Rogue APs
```

show location ap-detect ?

```
all            Display all (client/rfid/rogue-ap/rogue-client) information
client         Display client information
rfid           Display rfid information
rogue-ap       Display rogue-ap information
rogue-client   Display rogue-client information
(Cisco Controller) >show location ap-detect client
```

show client summary

```
Number of Clients................................ 7
MAC Address       AP Name           Status        WLAN/Guest-Lan Auth Protocol Port Wired
----------------- ----------------- ------------- -------------- ---- -------- ---- -----
00:0e:9b:a4:7b:7d AP6               Probing       N/A            No   802.11b  1    No
00:40:96:ad:51:0c AP6               Probing       N/A            No   802.11b  1    No
(Cisco Controller) >show location summary
 Location Summary
 Algorithm used:                 Average
 Client
        RSSI expiry timeout:     5 sec
        Half life:               0 sec
        Notify Threshold:        0 db
 Calibrating Client
        RSSI expiry timeout:     5 sec
        Half life:               0 sec
 Rogue AP
        RSSI expiry timeout:     5 sec
        Half life:               0 sec
        Notify Threshold:        0 db
 RFID Tag
        RSSI expiry timeout:     5 sec
        Half life:               0 sec
        Notify Threshold:        0 db
```

show rfid config

```
RFID Tag data Collection........................ Enabled
RFID  timeout................................... 1200 seconds
RFID mobility................................... Oui:00:14:7e : Vendor:pango  State:Disabled

(Cisco Controller) >config location ?
plm            Configure Path Loss Measurement (CCX S60) messages
algorithm      Configures the algorithm used to average RSSI  and SNR values
notify-threshold Configure the LOCP notification threshold for RSSI measurements
rssi-half-life Configures half life when averaging two RSSI readings
expiry         Configure the timeout for RSSI values
```

config location expiry client ?

```
<seconds>      A value between 5 and 3600 seconds
```

config location rssi-half-life client ?

```
<seconds>      Time in seconds (0,1,2,5,10,20,30,60,90,120,180,300 sec)
```

```
show nmsp subscription summary

Mobility Services Subscribed:
Server IP                Services
---------                --------
172.19.32.122            RSSI, Info, Statistics, IDS
```

MSE コマンド

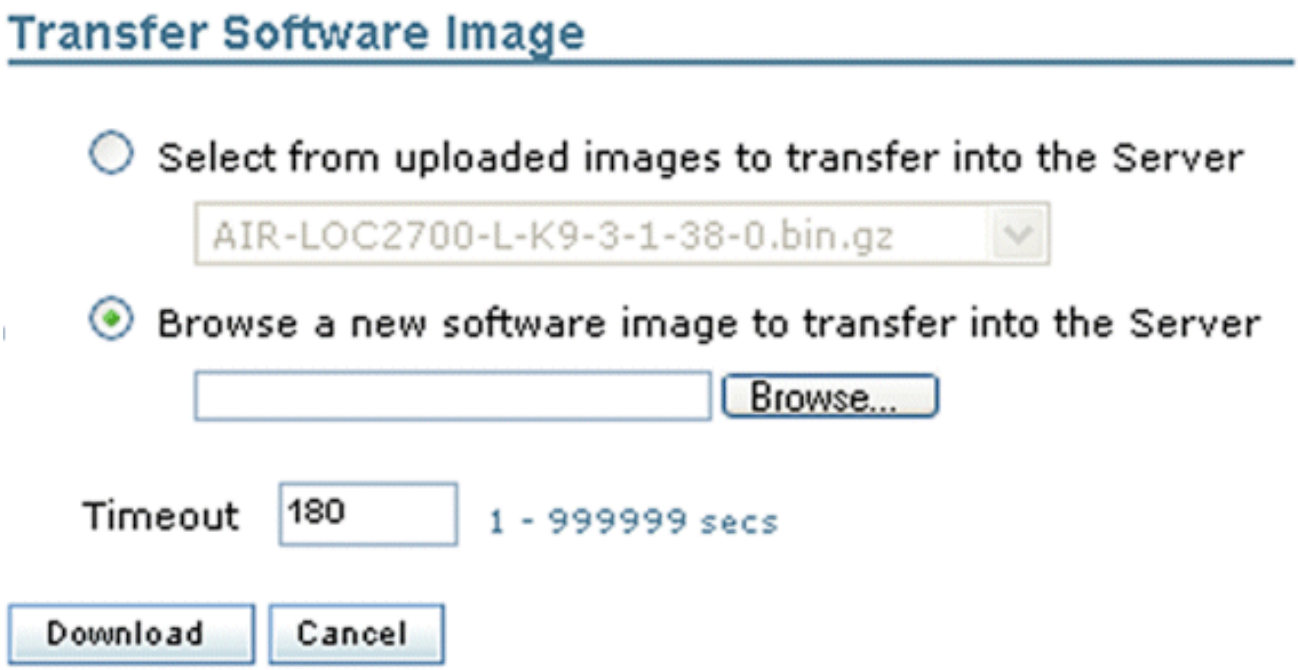
```
to determine status of MSE services
[root@MSE ~]# getserverinfo

to start Context Aware engine for client tracking
[root@MSE ~]# /etc/init.d/msed start

to determine status of Context Aware engine for client tracking
[root@MSE ~]# /etc/init.d/msed status

to stop Context Aware engine for client tracking
[root@MSE ~]# /etc/init.d/msed stop

diagnostics command
[root@MSE ~]# rundiag
```

注：rundiagコマンドを使用して、クライアント用Context Aware Engineのライセンスファイルを取得するために必要なMSE UDI情報を表示することもできます。

付録C:5.Xから6.0へのMSEアップグレード

次のステップを実行します。

1. WCSから6.x以前のイメージMSEデータベースをバックアップし、Service >Mobility Services >select MSE >Maintenance >Backupのリンクに移動します。
2. タグのデータおよび設定をバックアップするには、AeroScout Documentation に従ってください。
3. WCSからMSEに6.xイメージをダウンロードし、次のリンクに移動します。Services > Mobility Service > MSEを選択し、左側のペインでMaintenance > Download Softwareの順に選択し、PCからMSEイメージを参照して選択し、Downloadをクリックします。ダウンロードされた MSE イメージは、自動的に解凍されて、MSE の /opt/installers フォルダに配置されます。MSE の CLI からイメージを手動でインストールする必要があります。



4. MSEフレームワークを停止するには、/etc/init.d/msed stopコマンドを発行します。

5. MSE コンソールから、cd /opt/installers を発行します。ステップ 3 でダウンロードしたファイルがこのディレクトリにあります。ディレクトリは、次のようになります。

```
[root@heitz-3350 installers]# cd /opt/installers
[root@heitz-3350 installers]# ls
CISCO-MSE-L-K9-6-0-73-0-64bit.bin  diagnostics.log
CISCO-MSE-L-K9-6-0-75-0-64bit.bin  MSE_6_0_70_0.bin
[root@heitz-3350 installers]#
```

6. MSE イメージをインストールするには、ファイルを実行し、プロンプトに従います。

```
[root@heitz-3350 installers]# ./CISCO-MSE-L-K9-6-0-73-0-64bit.bin
```

注：6.0 MR1リリース以降では、要素を追跡するためのMSEのライセンス要件に関する警告メッセージが事前に表示されます。この警告メッセージは、インストールが完了して終了するときにも表示されます。6.0 リリースでは、インストール完了後の最後の時点にだけ、このメッセージが表示されます。ライセンスの適用に関して、ユーザへのアラートを強化するために、6.0 MR1 では事前警告が追加されました。

メッセージは次のようになります。「Mobility Services Engineのライセンスは、このリリースのソフトウェアで適用されます。Please ensure you have the Product Authorization Key (PAK) available and refer to the instructions outlined in the paper PAK certificate and the MSE User Guide to enable licensing on the system.」

ユーザは、このファイルの実行中に、データベースを維持するのか削除するのかを選択でき

ます。

7. イメージがインストールされたら、次のコマンドを実行してMSEフレームワークを起動します。/etc/init.d/msed start。

8. MSE が開始されて、6.0 ソフトウェア リリースに含まれている評価ライセンスが使用されます。

9. WCSからPAK番号を登録して、受け取ったパーマネントライセンスを追加します。次のリンクに移動します。Administration > License Center > Files > MSE Files > Add 。ドロップダウン メニューから [MSE] を選択し、PC 上のライセンス ファイルを参照して選択し、アップロードします。

10. ライセンスが MSE にアップロードされると MSE サービスは再起動されます。数分間待ってから他の操作を実行してください。MSE のステータスは、/etc/init.d/msed status コマンドを発行すると表示されます。

11. MSEイメージのインストール中に、ステップ6で示したようにデータベースオプションを保持することを選択した場合は、以前にバックアップしたデータベース（クライアントおよびタグ用）を復元する必要はありません。それ以外の場合は、MSEデータベースを復元する必要があります。[Service] > [Mobility Services] に移動し、左側のペインで [MSE] および [Maintenance] を選択して [Restore] をクリックします。

    注：タグ情報を復元するには、AeroScout Documentationに従ってください。

付録D:MSEデータベースの復元

MSE DB は、3 通りの方法で復元できます。

- オプション 1：

  MSE イメージを 6.0 にアップグレードするときに、すでに実行されている MSE がインストーラによって検出された時点で、続行を選択します。メッセージは次のように表示されます。「The system looks have a Cisco Mobility Services Engine already installed.If you choose Continue, all the currently installed components will be removed permanently (Only database and license files will be preserved).」

- オプション 2：

  MSE イメージをアンインストールする際に、2 つのオプションがあります。データベースを維持するオプションと、データベースを削除するオプションです。データベースを維持する場合、手動復元は不要です。データベースを削除した場合は、オプション 3 を実行してください。

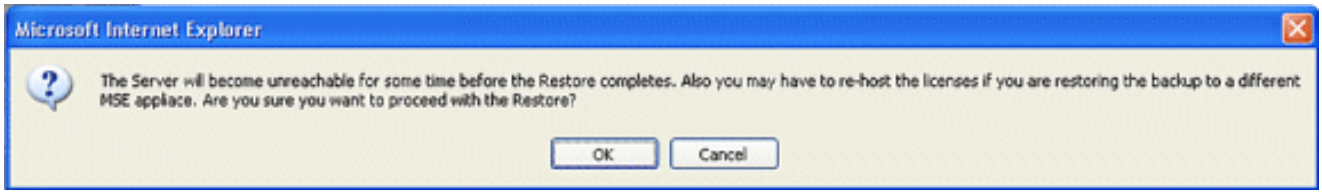
- オプション 3：

  新規インストールを実行します。6.0 よりも前のイメージがインストールされた新しい MSE マシンを用意するか、データベースを削除した MSE を用意します。バックアップしたデータベースを復元する必要があります（オプション 1「6.0 を実行する MSE」を参照

）。

バックアップした MSE イメージを別の MSE に復元した場合は、現在の MSE で使用できるように、ライセンスを再ホストする必要があります。MSE ライセンスは、MSE UDI と関連付けられています。

復元中に、ユーザはWCSに「バックアップを別のMSEアプライアンスに復元する場合は、ライセンスを再ホストする必要がある場合があります」というメッセージを受信します。



関連情報

- Cisco 3350 モビリティ サービス スタートアップ ガイド
- Cisco 3310 モビリティ サービス エンジン スタートアップ ガイド
- シスコ モビリティ サービス エンジン：Context Aware モビリティ ソリューション導入ガイド
- モビリティ グループの FAQ
- Wi-Fi ロケーションベース サービス 4.1 デザイン ガイド
- Cisco Context-Aware Service コンフィギュレーション ガイド、リリース 6.0
- Cisco 3300 シリーズ Mobility Services Engine のライセンスおよび発注ガイド
- Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド
- RFID Tags, a closer look to them and to their configuration
- Cisco Aironet アンテナおよびアクセサリのリファレンス ガイド
- AeroScout Support
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。