設計ガイドCX – 大規模パブリックネットワークのワイヤレス

内容

はじめに

このドキュメントでは、大規模なパブリックWi-Fiネットワークの設計と設定のガイドラインについて説明します。

CX設計ガイド

CX設計ガイドは、Cisco Technical Assistance Center(TAC)とCisco Professional Services(PS)の専門家が作成し、シスコ内の専門家が相互にレビューします。このガイドは、シスコのベストプラクティスに加え、長年にわたってお客様が数多くの導入経験を積み重ねてきた知識と経験に基づいています。このドキュメントの推奨事項に従って設計および設定されたネットワークは、一般的な落とし穴を回避し、ネットワーク運用を改善するのに役立ちます。

範囲と定義

このドキュメントでは、大規模なパブリックワイヤレスネットワークの設計と設定のガイドラインを示します。

定義：大規模なパブリックネットワーク：何千もの未知のクライアントデバイスやアンマネージドクライアントデバイスにネットワーク接続を提供する、高密度のワイヤレス展開。

このドキュメントでは、ターゲットネットワークが大規模なイベントや一時的なイベントにサービスを提供していることを想定していることがよくあります。また、多くのゲストを受け入れる

施設用のスタティックな固定ネットワークにも適しています。たとえば、ショッピングモールや空港は、スタジアムやコンサート会場のWi-Fiネットワークと似ています。これは、エンドユーザを制御できず、ネットワーク内にエンドユーザが通常は数時間、つまり1日しか存在しないという意味です。

大規模なイベントや会場のワイヤレスカバレッジには独自の要件があり、大企業、製造業、または大規模な教育ネットワークとは異なる傾向があります。大規模なパブリックネットワークでは、数千ものユーザが1つか数棟の建物に集中して勤務しています。常時またはピーク時に頻繁にクライアントのローミングが発生することがあり、さらにネットワークは無線クライアントデバイスに関して可能な限りすべてに対応する必要があり、クライアントデバイスの設定やセキュリティは制御できません。

このガイドでは、高密度および実装の詳細に関する一般的なRFの概念について説明します。このガイドに記載されている無線の概念の多くは、Cisco Merakiを含むすべての高密度ネットワークに適用されます。ただし、実装の詳細と設定は、Catalyst 9800ワイヤレスコントローラを使用するCatalystワイヤレスに焦点を当てています。これは、現在、大規模なパブリックネットワークに導入されている最も一般的なソリューションであるためです。

このドキュメントでは、ワイヤレスコントローラ(WLC)とワイヤレスLANコントローラ(WLC)という用語を同じ意味で使用しています。

大規模なパブリックネットワーク

大規模なパブリックネットワークとイベントネットワークは多くの面でユニークです。このドキュメントでは、これらの主要領域について説明し、ガイダンスを提供します。

- 大規模なパブリックネットワークは負荷が高く、無線周波数(RF)スペースが縮小された数千台のデバイスが存在し、ユーザが歩き回るにつれてローミングが著しく増加します。特定の時間に帯域幅のピークが生じると、一部のイベントや会場は静的になる可能性があります。インフラストラクチャは、エリア内を出入りするクライアントに対して、これらの状態の変更を可能な限り適切に処理する必要があります。
- 重要な優先事項は、オンボーディングの容易さです。関連付けられたクライアントは正常なクライアントです。つまり、ネットワークへのクライアントの関連付けを可能な限り迅速に行う必要があります。Wi-Fiに接続されていないクライアントが利用可能なアクセスポイントをスキャンすると、不要なRFエネルギーが生成され、それが空気中での輻輳の増加や容量の損失につながります。
- RF展開は、可能な限り慎重に設計する必要があります。非常に高い密度が必要な場合、または施設に大きなオープンスペースや高い天井がある場合は、指向性アンテナを使用した適切なRF設計が必須です。
- もう1つの主要な設計要素は互換性です。802.11仕様では標準となっている機能もあれば、独自仕様であるため、クライアントに問題を引き起こさない機能もあります。しかし、現実は異なり、理解できない複雑なビーコンや機能/設定を見ると誤動作する、プログラムが不十分なクライアントドライバが多数あります。
- 規模や時間の制約があるため、トラブルシューティングは困難です。特定のクライアントで何かが動作しない場合、そのエンドユーザと協力して問題を理解することができません。ユーザは見つけるのが難しい場合もありますが、施設での一時的な訪問により非協力的になる場合もあります。

- セキュリティは重要な要素です。大量のゲスト訪問者と攻撃対象領域の拡大により、制御が低下します。

外部参照

ドキュメント名	出典	場所
Cisco Catalyst 9800シリーズ設定のベストプラクティス	『シスコ	リンク
ワイヤレスLANコントローラCPUのトラブルシューティング	『シスコ	リンク
Wi-Fiスループットの検証：テストおよびモニタリングガイド	『シスコ	リンク
Cisco Catalyst CW9166D1アクセスポイント導入ガイド	『シスコ	リンク
Catalyst 9104スタジアムアンテナ(C-ANT9104)導入ガイド	『シスコ	リンク
Catalyst 9800のKPI（重要業績評価指標）の監視	『シスコ	リンク
Catalyst 9800クライアントの接続の問題のトラブルシューティングフロー	『シスコ	リンク
Cisco Catalyst 9800シリーズワイヤレスコントローラソフトウェアコンフィギュレーションガイド(17.12)	『シスコ	リンク
Wi-Fi 6E:Wi-Fiに関するホワイトペーパーの次の章	『シスコ	リンク

免責事項

このドキュメントでは、多数の導入から得られた特定のシナリオ、前提条件、および知識に基づいた推奨事項を提供します。ただし、読者は、このガイドに記載されているガイダンスまたは推奨事項に従うかどうかを含め、ネットワーク設計、ビジネス、法規制の遵守、セキュリティ、プ

ライバシー、およびその他の要件を決定する責任があります。

ネットワークの設計

RFの考慮事項

会場のタイプ

このガイドでは、一般に公開されている大規模なゲストネットワークについて説明し、エンドユーザとクライアントデバイスタイプに対する制御が限定的であることを中心に説明します。これらのタイプのネットワークは、さまざまな場所に展開でき、一時的または永続的です。主な使用例は通常、訪問者にインターネットアクセスを提供することですが、これが唯一の使用例であることはほとんどありません。

標準的な場所：

- スタジアムとアリーナ
- 会議場
- 大講堂

RFの観点からは、これらの口ケーションタイプにはそれぞれ固有の二ュアンスがあります。これらの例の多くは、会議会場とは別に通常、常設設置です。常設設置の場合もあれば、特定の展示会に一時的に設置する場合もあります。

その他の場所：

- クルーズ船
- 空港
- ショッピングセンター/モール

空港やクルーズ船は、大規模なパブリックネットワークのカテゴリに適合する展開の例でもあります。ただし、これらの展開では、それぞれのケースに固有の追加の考慮事項があり、多くの場合、内部の全方向性APを使用します。

カバレッジ戦略

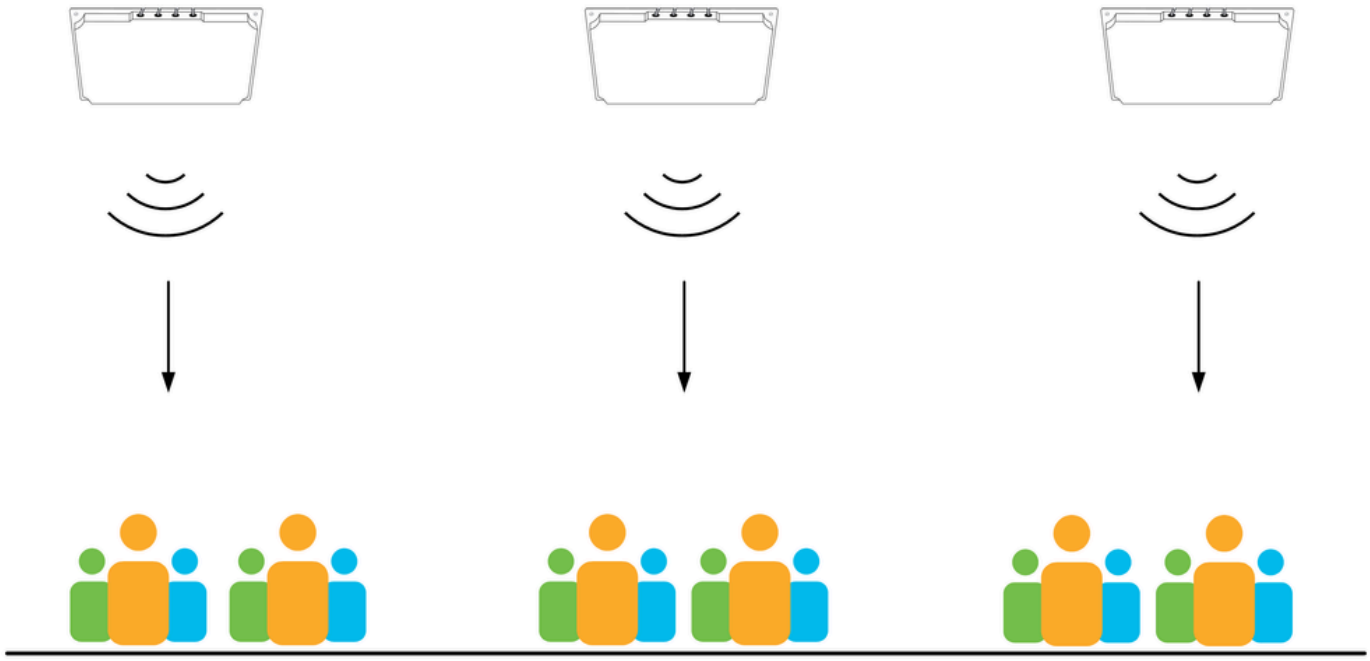
カバレッジ戦略は、施設のタイプ、使用するアンテナ、および使用可能なアンテナ取り付け場所によって大きく異なります。

オーバーヘッド

可能な限り、常にオーバーヘッドカバレッジが優先されます。

オーバーヘッドソリューションには、混雑した状況でも、通常はすべてのクライアントデバイスがアンテナのオーバーヘッドに対して直接見通し線を持つという明確な利点があります。指向性アンテナを使用したオーバーヘッドソリューションでは、カバレッジ工リアが適切に制御されるため、無線チューニングの観点から見たカバレッジ工リアの複雑性が軽減され、優れたロードバランシングとクライアントのローミング特性が得られます。詳細については、パワーバランスに

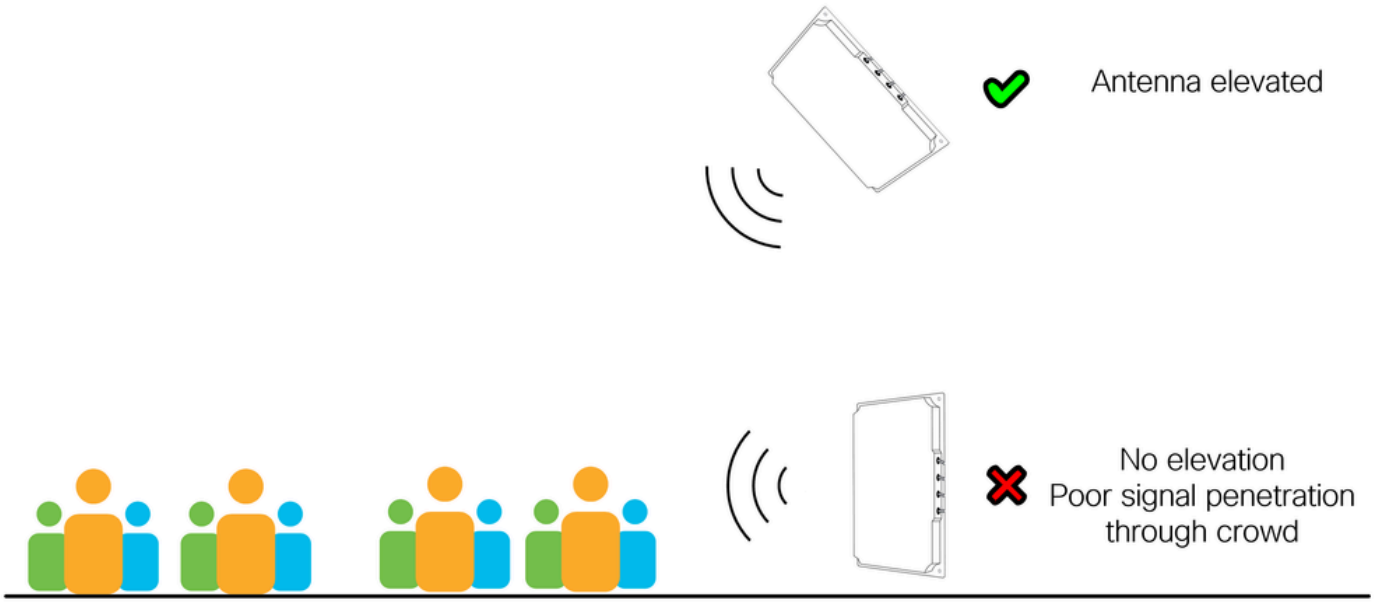
関するセクションを参照してください。



クライアントより上のAP

Side

サイドマウント型指向性アンテナは一般的な選択肢であり、高さや取り付け制限のためにオーバーヘッドの取り付けが不可能な場合は特に、さまざまなシナリオで効果的に動作します。サイドマウントを使用するときは、アンテナでカバーされるエリアのタイプを理解することが重要です。たとえば、屋外のオープンエリアや密集した屋内エリアですか。カバレッジエリアが多数の人がいる高密度のエリアである場合、アンテナは、人間の群集を通る信号の伝播が常に不良であるために、できるだけ高い位置に置く必要があります。ほとんどのモバイルデバイスは、ユーザの頭の上ではなく、腰の下のレベルで使用されていることに注意してください。アンテナの高さはそれほど重要ではありません。カバレッジエリアが低密度のエリアの場合。



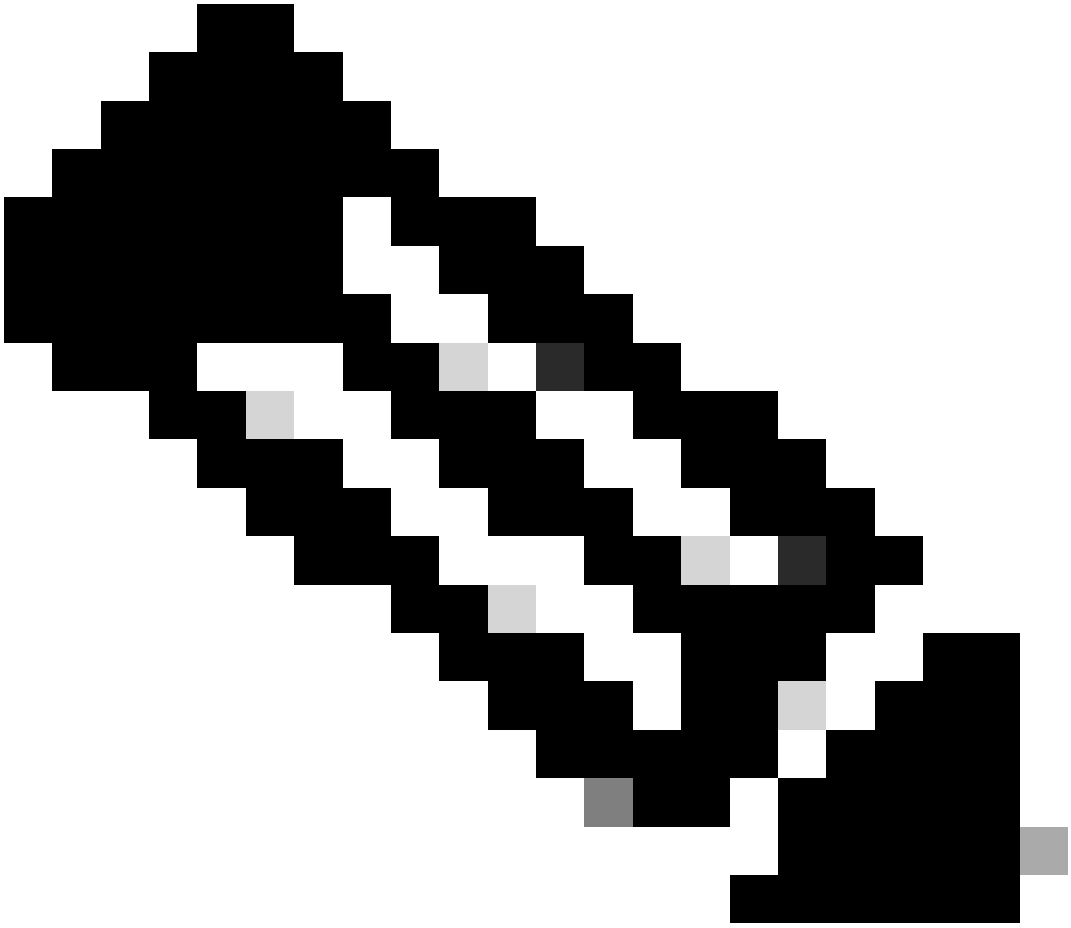
全方向性

全方向性アンテナ（内部または外部）の使用は、一般に、非常に高密度のシナリオでは避ける必要があります。これは、共通チャネル干渉の影響を受ける領域が大きくなる可能性があるためです。全方向性アンテナは、6 mを超える高さでは使用しないでください（高ゲインの屋外ユニットには適用されません）。

座席の下

一部のアリーナやスタジアムでは、適切なアンテナの取り付け場所がない場合があります。残りの選択肢は、ユーザが座っている席の下にAPを配置して、下からカバレッジを提供することです。このタイプのソリューションは正しく導入するのが難しく、通常は非常に多くのAPと特定のインストール手順を必要とするため、コストがかかります。

座席下での展開における主な課題は、満席の会場と空席の会場のカバレッジの大きな違いです。人体は無線信号を減衰する点で非常に効率的です。つまり、APの周囲に大勢の人がいると、そのカバレッジは、大勢の人がいないときに比べて非常に小さくなります。この人間の群集減衰係数により、より多くのAPを展開して全体的なキャパシティを増やすことができます。しかし、会場が空いているときは、人体による減衰や大きな干渉はなく、会場が部分的に満室の場合は複雑になります。



注：アンダー・シート導入は有効ですが、一般的ではないソリューションです。ケースバイケースで評価する必要があります。このドキュメントでは、下位の展開については詳しく説明しません。

美観

一部の導入では、美観の問題が関係しています。これらは、特定のアーキテクチャ設計、歴史的価値を持つ領域、または広告やブランディングによって機器を設置できる（または設置できない）場所を示す領域です。配置の制限を回避するために、特定のソリューションが必要になる場合があります。これらの回避策には、APやアンテナの非表示、APやアンテナの塗装、機器の格納場所への取り付け、または単に別の場所を使用することなどがあります。アンテナを塗装すると、保証が無効になります。アンテナを塗装する場合は、必ず非金属塗料を使用してください。シスコは一般にアンテナ用のエンクロージャを販売していませんが、多くのエンクロージャは様々なプロバイダーから簡単に入手できます。

このような回避策はすべて、ネットワークのパフォーマンスに影響を与えます。無線アーキテクトは常に、最適な無線力バレッジを得るための最適な取り付け位置を提案することから始めます

。通常、これらの初期位置は最高のパフォーマンスを提供します。これらの位置を変更すると、アンテナが最適な位置から離れることがよくあります。

アンテナが取り付けられている場所は高くなっている場合が多く、天井、キャットウォーク、屋根構造、梁、歩道など、目的のカバレッジエリアの高さを提供するあらゆる場所に設置できます。これらの場所は通常、オーディオ機器、空調、照明、各種の検出器/センサーなど、他の設置場所と共有されます。たとえば、オーディオ機器や照明機器は特定の場所に設置する必要がありますが、なぜですか。これは単純に、ボックス内や壁の後ろに隠されていると音声や照明器具が正しく動作せず、誰もがこれを認めているためです。

同じことが無線アンテナにも当てはまり、無線クライアントデバイスに見通し線がある場合に最も効果的に機能します。審美性を優先すると、ワイヤレスパフォーマンスに悪影響を及ぼす可能性があり（実際に悪影響を及ぼす場合も多い）、インフラストラクチャへの投資価値が低下します。

不正なネットワーク

不正なWi-Fiネットワークは、共通のRF空間を共有するワイヤレスネットワークですが、同じオペレータによって管理されることはありません。一時的または永続的なデバイスであり、インフラストラクチャデバイス(AP)や個人デバイス（Wi-Fiホットスポットを共有する携帯電話など）が含まれます。不正なWi-Fiネットワークは干渉源であり、場合によってはセキュリティリスクにもなります。不正がワイヤレスパフォーマンスに与える影響を過小評価しないでください。Wi-Fi伝送は、すべてのWi-Fiデバイス間で共有される比較的狭い範囲の無線スペクトルに制限され、近接して誤動作しているデバイスは、多くのユーザのネットワークパフォーマンスを中断させる可能性があります。

大規模なパブリックネットワークのコンテキスト内では、これらは通常、特別なアンテナを使用して慎重に設計および調整されています。優れたRF設計とは、必要な工リアだけを対象とし、多くの場合、指向性アンテナを使用し、最大の効率を得るために送受信特性を調整することです。

コンシューマ向けのデバイスや、インターネットサービスプロバイダーが提供するデバイスもあります。これらは、細かいRF調整のオプションが限られているか、または最大範囲と感知されるパフォーマンス（多くの場合、高出力、低データレート、およびワイドチャネル）用に設定されています。このようなデバイスを大規模なイベントネットワークに導入すると、混乱が生じる可能性があります。

何ができますか。

個人的なホットスポットの場合、会場に入ってくる数万人の人々を監視することはほとんど不可能であるため、実行できる方法はほとんどありません。インフラストラクチャまたは半永久的なデバイスの場合は、いくつかのオプションがあります。可能な改善は、認識のためのシンプルなサイネージを含むシンプルな教育から、署名された無線ポリシー文書を通じて始まり、積極的な適用とスペクトル分析で終わります。いずれの場合も、特定の施設内の無線スペクトルの保護に関するビジネス上の決定を行う必要があります。また、その決定を実施するための具体的な手順も必要です。

不正ネットワークのセキュリティ面は、3rdパーティによって制御されるデバイスが管理対象ネットワークと同じSSIDをアドバタイズすると影響を及ぼします。これはハニーポット攻撃に相当し

、ユーザクレデンシャルを盗む手段として使用できます。管理対象外のデバイスからアドバタイズされたインフラストラクチャSSIDの検出に対してアラートを発する不正ルールを作成することが常に推奨されます。「セキュリティ」セクションでは、不正について詳細に説明しています。

シングル5 GHzとデュアル5 GHz

デュアル5 GHzとは、サポートされているAPでの両方の5 GHz無線の使用を意味します。外部アンテナを使用するデュアル5 GHzと、内部アンテナ（全方向性AP上のマイクロ/マクロセル）を使用するデュアル5 GHzの間には、大きな違いがあります。外部アンテナの場合は、デュアル5 GHzが有用なメカニズムであることが多く、カバレッジと容量を増加させると同時に、APの総数を削減できます。

マイクロ/マクロ/メソ

内部APでは、両方のアンテナが（AP内部で）近接しており、デュアル5 GHzを使用する場合の最大Tx電力に関する制限があります。2つ目の無線は、低いTx電力（ワイヤレスコントローラによって適用）に制限されるため、無線間のTx電力の不均衡が大きくなります。これにより、プライマリ（電力が大きい）無線が多くのクライアントを引き付ける一方で、セカンダリ（電力が小さい）無線は十分に活用されない可能性があります。この場合、2番目の無線は、クライアントにメリットをもたらすことなく、環境に工ネルギーを追加します。このシナリオが見られる場合、追加のキャパシティが必要な場合は、2つ目の無線をディセーブルにして、別の（シングル5GHz）APを追加するほうが良い場合があります。

APモデルによって設定オプションが異なり、9130や9136などの新しいマクロ/メゾ APでは2番目の5GHz無線がより高い電力レベルで動作する場合があります。9160シリーズなどの一部の内部Wi-Fi 6E APは、場合によってはマクロ/マクロで動作する場合もあります。使用しているAPモデルの機能を必ず確認してください。2つ目の5GHzスロットのチャネル使用率も制限されます。1つのスロットが1つのUNII帯域で動作している場合、もう1つのスロットは別のUNII帯域に制限されます。これはチャネル計画に影響を与え、使用可能な送信電力にも影響します。デュアル5 GHz無線間のTx電力の違いは常に考慮する必要があります。これは、内部APを含むすべての場合に当てはまります。

FRA

Flexible Radio Assignment(FRA)は、追加の2.4GHz無線を5GHzモードに、または未使用の可能性がある5GHz無線をモニタモード（これをサポートするAP用）に切り替えることで、5GHzカバレッジを向上させるテクノロジーとして導入されました。このドキュメントでは大規模なパブリックネットワークを取り上げているため、カバレッジエリアと無線設計は指向性アンテナを使用して明確に定義されていることを前提としています。そのため、動的な設定よりも決定論的な設定が優先されます。FRAの使用は、大規模なパブリックネットワークには推奨されません。

オプションで、FRAは、ネットワークが5GHzに変換する無線を決定する際に役立つように設定されている場合に使用できますが、結果に満足のいくものであれば、FRAをフリーズすることをお勧めします。

規制

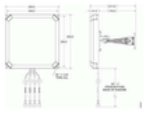
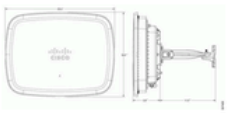
各規制ドメインでは、使用可能なチャネルとその最大電力レベルが定義されています。また、屋

内と屋外で使用できるチャネルに関する制限もあります。規制区域によっては、5GHzデュアルソリューションを効果的に利用できないことがあります。この例はETSIドメインで、UNII-2eチャネルでは30dBmが許可され、UNII1/2では23dBmのみが許可されます。この例では、（通常はアンテナまでの距離が長いために）30dBmを使用する必要がある設計の場合、単一の5GHz無線を使用することが唯一の現実的なソリューションです。

アンテナ

大規模なパブリックネットワークでは、あらゆるタイプのアンテナを使用でき、通常は業務に最適なアンテナを選択します。同じカバレッジエリア内にアンテナを混在させると、無線設計プロセスが難しくなり、可能であれば回避する必要があります。ただし、大規模なパブリックネットワークでは、カバレッジエリアが広く、同じエリア内でも取り付けオプションが異なることが多いため、場合によってはアンテナを混在させる必要があります。全方向性アンテナについては、他のアンテナと同様に理解および機能しますが、このガイドでは外部指向性アンテナについて説明します。

次の表に、最もよく使用される外部アンテナを示します。

	C-ANT9103 Patch antenna (8x8) 6 dBi	5GHz Beamwidth 70°x70° ~33ft (10m)
	ANT2566P4W-R/S Patch antenna (4x4) 6 dBi	5GHz Beamwidth 110°x55° (120°x60°) ~33ft (10m)
	ANT2566D4M-R/S Patch antenna (4x4) 6 dBi	5GHz Beamwidth 55°x60° (60°x60°) ~33ft (10m)
	ANT2513P4M-N/S HD “Stadium” antenna 13 dBi	5GHz Beamwidth 31°x27° (30°x30°) ~66ft (20m)
	C-ANT9104 HD “Stadium” antenna Narrow 10dBi / Wide 7dBi	5GHz Beamwidth Narrow 25°x25° Wide 80°x25°

アンテナリスト

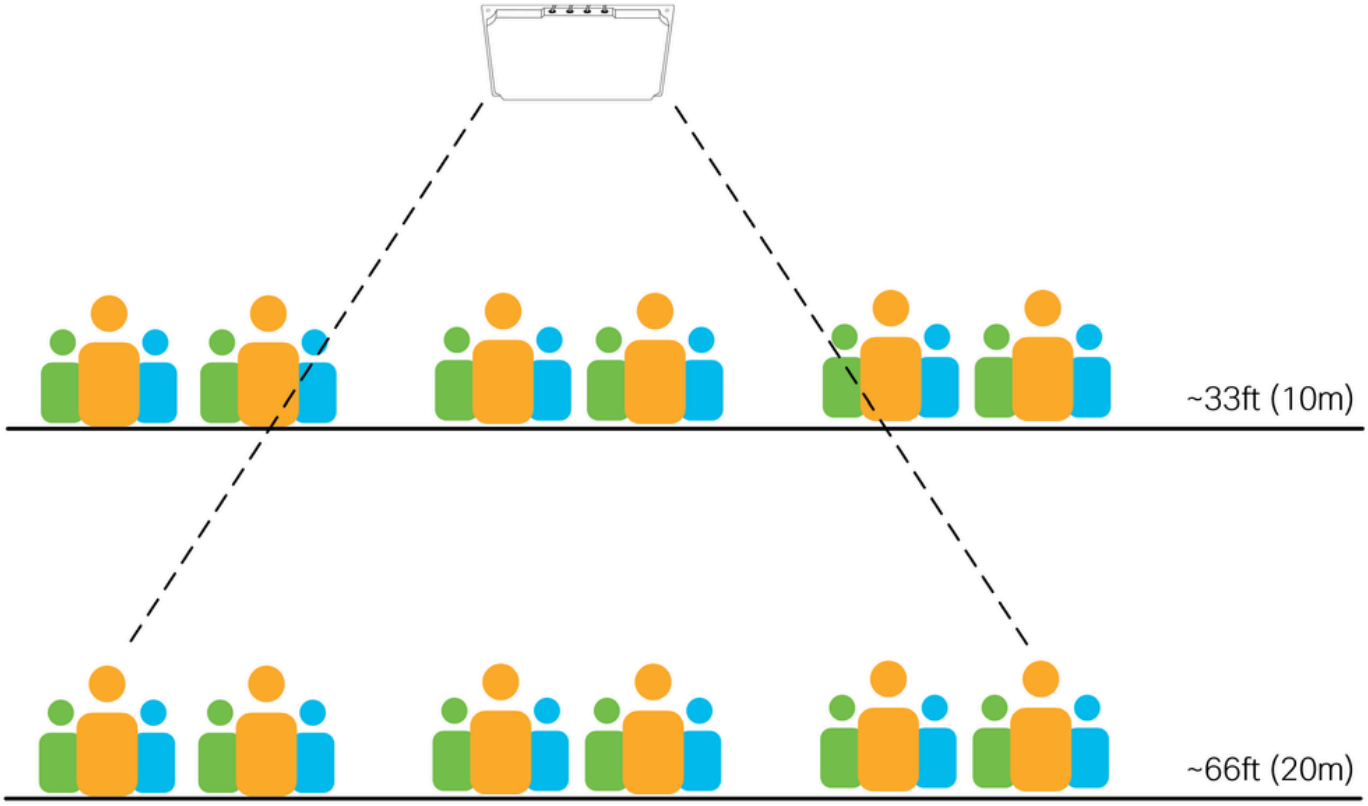
アンテナを選択する際に考慮すべき主な要素は、アンテナのビーム幅とアンテナが取り付けられる距離/高さです。次の表に、各アンテナの5 GHzビーム幅を示します。角括弧内の数字は丸められた値（覚えやすい値）を示しています。

表の推奨される距離は厳格なルールではなく、経験に基づくガイドラインのみです。電波は光の速度で移動し、任意の距離に到達した後に停止することはありません。アンテナはすべて推奨距離を超えて動作しますが、距離が長くなるほどパフォーマンスは低下します。設置の高さは、計画時の重要な要素です。

次の図は、高密度エリアにおける約33フィート(10m)および約66フィート(20m)の同じアンテナの2つの取り付け可能な高さを示しています。アンテナで認識（および接続を受け入れる）できるク

ライアントの数が距離とともに増加していることに注意してください。セルサイズを小さくすることは、距離が長くなるほど難しくなります。

ユーザ密度が高くなるほど、一定の距離に対して正しいアンテナを使用することが重要になります。



スタジアムアンテナ

C9104スタジアムアンテナは、長距離の高密度エリアのカバーに適しています。詳細については、『Catalyst 9104スタジアムアンテナ(C-ANT9104)導入ガイド』を参照してください。

時間の経過に伴う変化

時間の経過に伴う物理環境の変化は、ほとんどすべての無線設備で共通です（内壁の移動など）。定期的な現地訪問と目視検査が常に推奨される方法である。イベントネットワークでは、音声および照明システムの扱いが複雑になり、多くの場合、他の通信システム（5Gなど）も複雑になります。これらすべてのシステムは、ユーザよりも上の高い場所に設置されることが多く、同じスペースに対する競合が発生する場合があります。無線スタジアムアンテナに適した場所は、5Gアンテナにも適した場所です。さらに、これらのシステムは時間の経過に伴ってアップグレードされるため、ワイヤレスシステムを妨害する場所やワイヤレスシステムに対してアクティブに干渉する場所に再配置できます。すべてのシステムが互いに干渉することなく（物理的または電磁的に）適切な場所に設置されるように、他の設置を追跡し、それらを設置したチームと通信することが重要です。

高密度および6 GHz

このドキュメントの作成時点では、6 GHz対応の外部アンテナの選択肢は限られています。

CW9166D1統合AP/アンテナは6GHzで動作しますが、詳細なアンテナ仕様については『Cisco Catalyst CW9166D1アクセスポイント導入ガイド』を参照してください。CW9166D1は、60 °x 60 °のビーム幅で6 GHzのカバレッジを提供し、このタイプのアンテナの条件を満たす環境で効果的に使用できます。たとえば、統合ユニットは屋内用の指向性アンテナ機能を備えているため、講堂や倉庫はCW9166D1の導入に適しています。

	CW9166D1 6GHz (4x4) or XOR 5GHz	 60° x60° 8 dBi
	5GHz (4x4)	70° x70° 6 dBi
	2.4GHz (4x4)	70° x70° 6 dBi

9166D1

大規模なパブリックネットワークの場合、これらにはさまざまな大きな工リアがあり、さまざまな高さのアンテナの組み合わせを使用する必要があります。距離の制限により、60 °x 60 °のアンテナのみを使用して大規模なパブリックネットワークをエンドツーエンドで導入するのは困難な場合があります。そのため、大規模なパブリックネットワークでCW9166D1のみを使用して6 GHzのエンドツーエンドのカバレッジを提供することも困難な場合があります。

1つの可能なアプローチは、プライマリカバレッジ帯域として5 GHzを使用し、特定のエリアでのみ6 GHzを使用して、対応するクライアントデバイスをクリーンな6 GHz帯域にオフロードすることです。このタイプのアプローチでは、より広いエリアで5 GHz専用アンテナを使用し、可能な場所および追加の容量が必要な場所では6 GHzアンテナを使用します。

たとえば、取引会議の大規模なイベントホールを考えてみます。メインホールはスタジアムアンテナを使用して5GHzでのプライマリカバレッジを提供します。設置の高さによってスタジアムアンテナの使用が義務付けられます。この例では、CW9166D1は距離の制限によりメインホールでは使用できませんが、より高い密度が必要な隣接のVIPホールやプレスエリアでは効果的に使用できます。5 GHz帯域と6 GHz帯域の間のクライアントローミングについては、このドキュメントで後ほど説明します。

規制

5 GHzと同様に、6 GHzの使用可能な電力とチャネルは、規制ドメインによって大幅に異なります。特に、使用可能なスペクトルはFCCドメインとETSIドメインの間で大きく異なり、屋内および屋外用の使用可能な送信電力、Low Power Indoor(LPI)、およびStandard Power(SP)に関する厳格なガイドラインも存在します。6 GHzでは、クライアントの電力制限、外部アンテナの使用、アンテナのダウンティルト、および（現時点では米国でのみ）SP導入の自動周波数調整(AFC)要件など、追加の制限があります。

Wi-Fi 6Eの詳細については、『Wi-Fi 6E:Wi-Fiホワイトペーパーの次の章』を参照してください。

Radio Resource Management（RRM）

Radio Resource Management(RRM)は、無線動作の制御を担当するアルゴリズムのセットです。このガイドでは、Dynamic Channel Assignment（DCA；動的チャネル割り当て）とTransmit Power Control（TPC；送信電力制御）という2つの主要なRRMアルゴリズムを参照しています。RRMは、スタティックチャネルおよび電力設定の代替手段です。

- DCAは設定可能なスケジュール（デフォルトは10分）で実行されます。
- TPCは自動スケジュールで実行されます（デフォルトは10分）。

Cisco Event Driven RRM(ED-RRM)は、チャネル変更の決定を標準のDCAスケジュール外で（通常は重大なRF状態に応じて）行えるようにするDCAオプションです。過剰なレベルの干渉が検出されると、ED-RRMによってチャネルが即座に変更される可能性があります。ノイズが多い環境や不安定な環境では、ED-RRMを有効にすると過剰なチャネル変更が発生するリスクがあり、クライアントデバイスに悪影響を及ぼす可能性があります。

RRMの使用は推奨されますが、一般的にはスタティック設定よりも推奨されますが、注意が必要な点と例外があります。

- TPCは、必要に応じてTPCのmin/max設定を使用して狭い範囲の値に制限する必要があります。また、常にRF設計に合わせる必要があります。
    - 高密度環境でTPC Channel Awareを有効にします。

- DCAサイクルをデフォルト設定の10分から変更する必要があります。
    - HD環境ではED-RRMを使用しないでください。
    - Avoid Cisco AP Loadを無効にします。
    - 不正が多い場合、「外部AP干渉の回避」などの不正AP回避オプションを使用すると、不安定な環境になる可能性があります。不正に対して応答を試みるよりも、不正を削除する方が常に優れています。
- RRMの決定は、指向性アンテナが互いに向かい合っている場合のように、互いに正しく聞き取り合わないAPやアンテナの影響を受ける可能性があります。
- 一部のアンテナ（C9104など）はRRMをサポートしておらず、常にスタティック設定が必要です。
- RRMでは、不適切なRF設計は修正されません。

いずれの場合も、期待される結果を理解したうえでRRMを導入し、特定のRF環境に適した境界内で動作するように調整する必要があります。このドキュメントの以降のセクションでは、これらのポイントについて詳しく説明します。

RF設定

チャネル

一般に、チャネルの数が多いほど優れています。高密度の導入では、使用可能なチャネルと比較して桁違いに多くのAPと無線が導入されることがあり、これはチャネルの再利用率が高いことを

意味し、それに加えて共通チャネル干渉のレベルも高いことを意味します。使用可能なチャネルはすべて使用する必要があります。通常は、使用可能なチャネルのリストを制限することを推奨しません。

特定の（および個別の）無線システムを同じ物理空間に共存させ、専用チャネルをそのシステムに割り当てる必要がある場合があります。また同時に、割り当てられたチャネルをプライマリシステムのDCAリストから削除する必要があります。これらのタイプのチャネル除外は、慎重に評価し、必要な場合にのみ使用する必要があります。たとえば、プライマリネットワークに隣接するオープンエリアで動作するポイントツーポイントリンクや、スタジアム内の記者席などです。複数のチャネルがDCAリストから除外されている場合は、提案するソリューションを再評価する必要があります。場合によっては、単一のチャネルを除いた非常に高密度のスタジアムなど、実現可能なオプションではないことがあります。

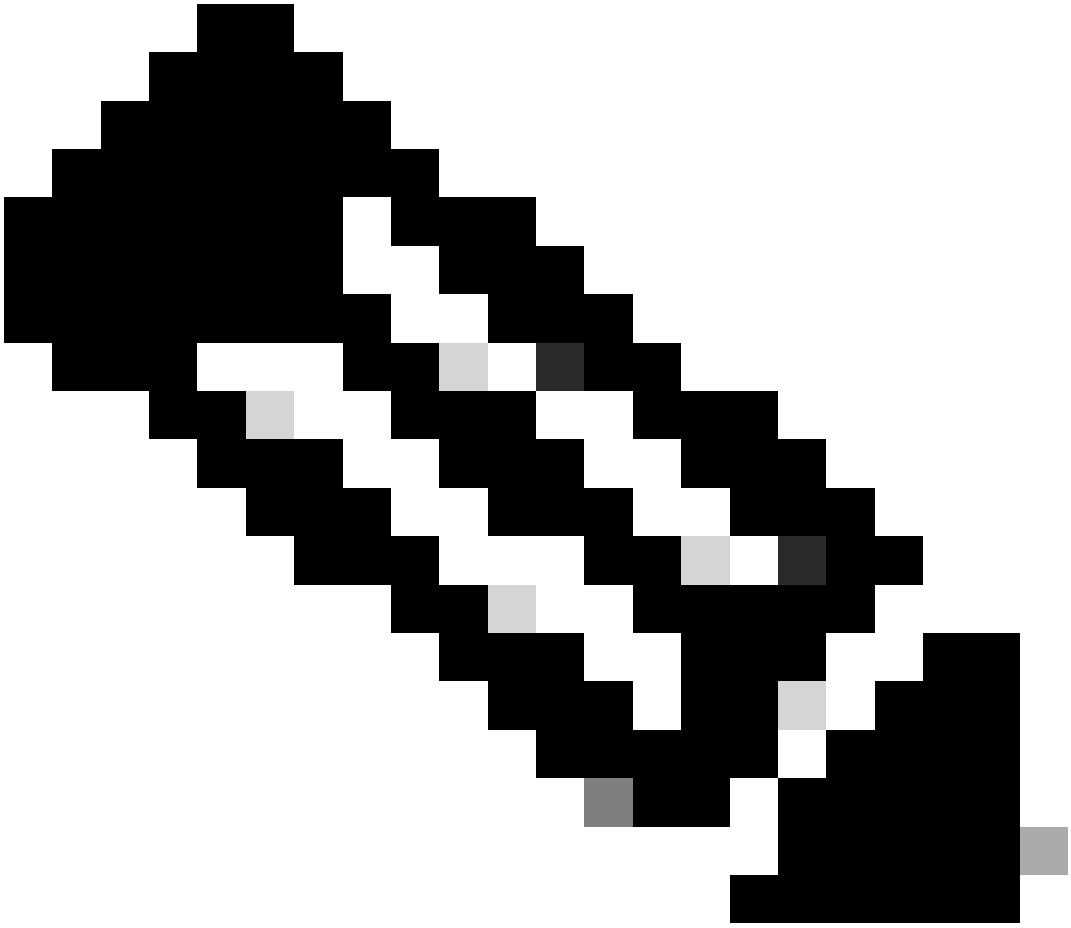
ダイナミックチャネル割り当て(DCA)は、WLCベースのRRMまたはAI拡張RRMとともに使用できます。

デフォルトのDCA間隔は10分で、不安定なRF環境では頻繁にチャネルが変更される可能性があります。デフォルトのDCAタイマーは、すべてのケースでデフォルトの10分から増やす必要があります。特定のDCA間隔は、対象のネットワークの動作要件に合わせる必要があります。設定の例としては、DCA間隔4時間、アンカー時間8などがあります。これにより、午前8時から4時間ごとにチャネルを変更できます。

干渉の多くは一時的なものであるため、干渉は必ずしも発生するはずなので、すべてのDCAサイクルに対応することが価値をもたらすとは限りません。最初の数時間は自動DCAを使用し、満足できる安定した状態が得られたら、アルゴリズムとチャネル計画を凍結することをお勧めします。

WLCがリブートされると、DCAは100分間アグレッシブモードで実行され、適切なチャネルプランを検索します。RF設計に大きな変更（多数のAPの追加や削除、チャネル幅の変更など）が行われた場合は、手動でプロセスを再起動することをお勧めします。このプロセスを手動で開始するには、次のコマンドを使用します。

```
ap dot11 [24ghz | 5ghz | 6ghz] rrm dca restart
```



注：チャネルを変更すると、クライアントデバイスに悪影響が及ぶ可能性があります。

2.4 GHz

2.4GHz帯域は批判されることが多い。オーバーラップしないチャネルが3つしかなく、Wi-Fi以外の多くのテクノロジーが使用するため、望ましくない干渉が発生します。一部の組織はサービスの提供を主張していますが、合理的な結論は何ですか？2.4GHz帯域では、エンドユーザに満足のいくエクスペリエンスが提供されないのは事実です。さらに、2.4GHzでサービスを提供しようとすると、Bluetoothなどの他の2.4GHzテクノロジーに影響が及びます。大規模な会場やイベントでも、多くの人がワイヤレスヘッドセットを使用してコールを発信したり、スマートウェアラブルを使用して通常どおりに動作することを期待しています。高密度Wi-Fiが2.4GHzで動作している場合、2.4GHz Wi-Fiを使用していないデバイスにも影響が及びます。

確かなことが1つあります。2.4GHz Wi-Fiサービスを提供する必要がある場合は、別のSSIDで提供することをお勧めします（IoTデバイスに専用にするか、「レガシー」と呼びます）。つまり、デュアルバンドデバイスは2.4GHzに強制的に接続されず、シングルバンド2.4GHzデバイスのみが接続されます。

シスコでは、2.4GHzでの40MHzチャネルの使用を推奨したり、サポートしたりしていません。

5 GHz

高密度ワイヤレスの一般的な導入。可能な限り、すべての使用可能なチャネルを使用します。

チャネルの数は規制ドメインによって異なります。特定の場所でのレーダーの影響を考慮し、可能な場合はDFSチャネル（TDWRチャネルを含む）を使用します。

すべての高密度導入では、20 MHzチャネル幅を強く推奨します。

40MHzは2.4GHzと同じ基準で使用できます。これは、絶対に必要な場合（および必要な場所）にのみ使用できます。

特定の環境における40MHzチャネルの必要性と実際の利点を評価します。40MHzチャネルでは、スループットの改善を実現するために、より高い信号対雑音比(SNR)が必要です。より高いSNRを実現できない場合は、40MHzチャネルは有用な目的を果たしません。高密度ネットワークでは、1人のユーザのスループットよりも、すべてのユーザの平均が優先されます。セカンダリチャネルとして40MHzを使用するAPがデータフレームのみに使用されるため、それぞれが20MHzで動作する2つの異なる無線セルを使用する場合よりも、20MHzチャネルに配置するAPの方がはるかに効率的に使用されます（単一クライアントのスループットではなく、合計容量の点で）。

6 GHz

6GHz帯域は、まだ各国で利用できるわけではありません。さらに、一部のデバイスには6GHz対応のWi-Fiアダプタがありますが、デバイスを操作している特定の国で有効にするにはBIOSアップデートが必要です。現在、クライアントが6GHz無線を検出する最も一般的な方法は、5GHz無線でのRNRアドバタイズメントを介する方法です。つまり、同じAP上で5 GHz無線を使用しない場合、6 GHzは単独で動作してはなりません。6 GHzは、クライアントとトラフィックを5 GHz無線からオフロードし、一般的に対応クライアントにより優れたエクスペリエンスを提供するために使用されます。6GHzチャネルでは、より大きなチャネル帯域幅を使用できますが、規制ドメインで使用可能なチャネルの数に大きく依存します。ヨーロッパでは24個の6GHzチャネルが利用可能であるため、おそらく5GHzで使用している20MHzよりも優れた最大スループットを提供するために40MHzチャネルを使用するのは無理はありません。チャネル数が約2倍の米国では、40MHzの使用は簡単です。また、80MHzを使用することは、大規模な密度イベントにとって不合理ではありません。高密度のイベントや会場では、より大きな帯域幅を使用しないでください。

データレート

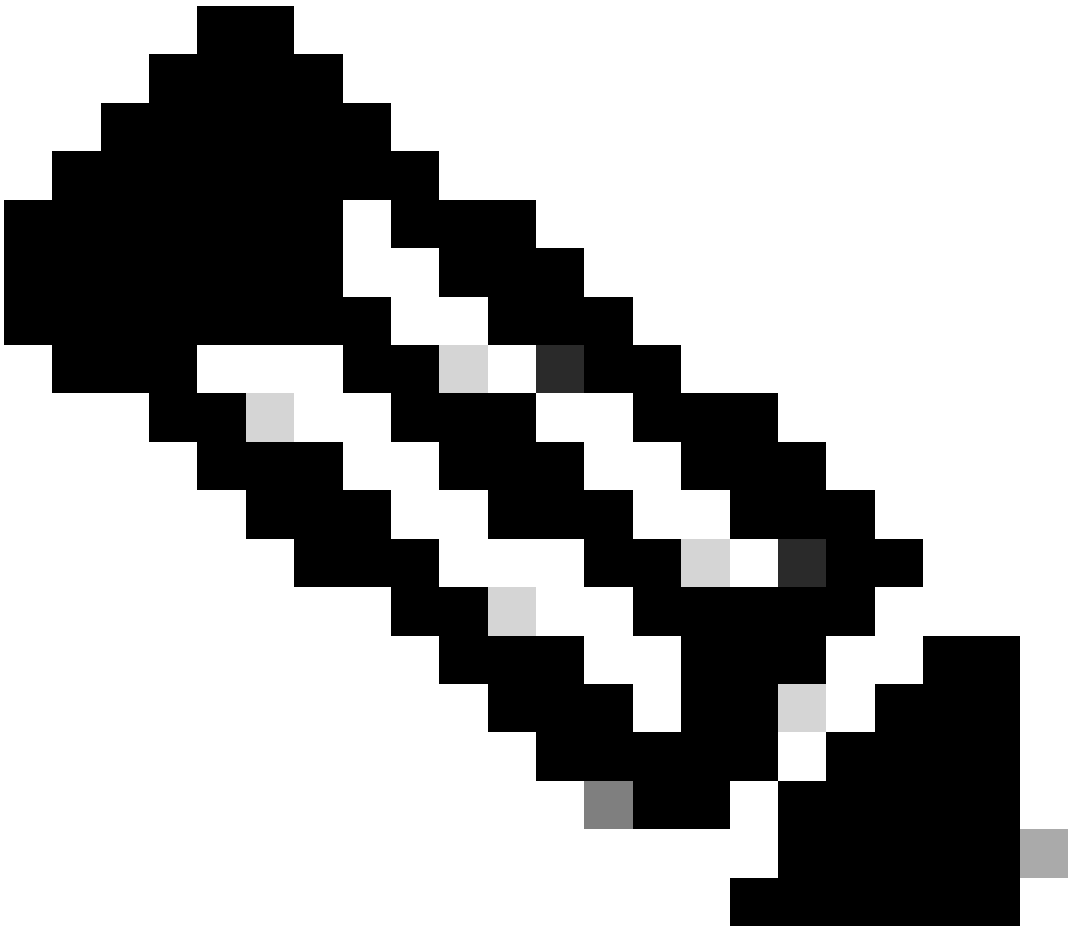
クライアントがAPとネゴシエートするデータレートの大部分は、その接続の信号対雑音比(SNR)の関数であり、逆も真です。つまり、データレートが高いほど、高いSNRが必要です。実際には、可能な最大リンク速度を決定するのは主にSNRですが、データレートを設定する際にこれが重要なのはなぜですか。これは、一部のデータレートが特別な意味を持っているためです。

従来のOFDM(802.11a)データレートは、無効、サポート、必須の3つの設定のいずれかで設定できます。OFDMレートは（Mbps単位）:6、9、12、18、24、36、48、54であり、クライアントとAPは使用する前に両方ともレートをサポートする必要があります。

Supported:APはレート

必須：APはこのレートを使用し、このレートを使用して管理トラフィックを送信します。

Disabled:APはレートを使用しないため、クライアントは強制的に別のレートを使用します



注：必須レートは、基本レートとも呼ばれます

必須レートの重要な点は、すべての管理フレームがブロードキャストフレームとマルチキャストフレームと同様に、このレートを使用して送信されることです。複数の必須レートが設定されている場合、管理フレームでは最も低く設定された必須レートが使用され、ブロードキャストとマルチキャストでは最も高く設定された必須レートが使用されます。

管理フレームには、クライアントがAPに関連付けるために受信する必要があるビーコンが含まれています。必須レートを上げると、その伝送のSNR要件も増加します。データレートを上げるとSNRを上げる必要があり、これは通常、ビーコンをデコードして関連付けられるようにするには、クライアントをAPに近づける必要があることを意味します。したがって、必須データレートを操作することで、APの有効な関連付け範囲も操作し、クライアントをAPの近くに強制的に近づ

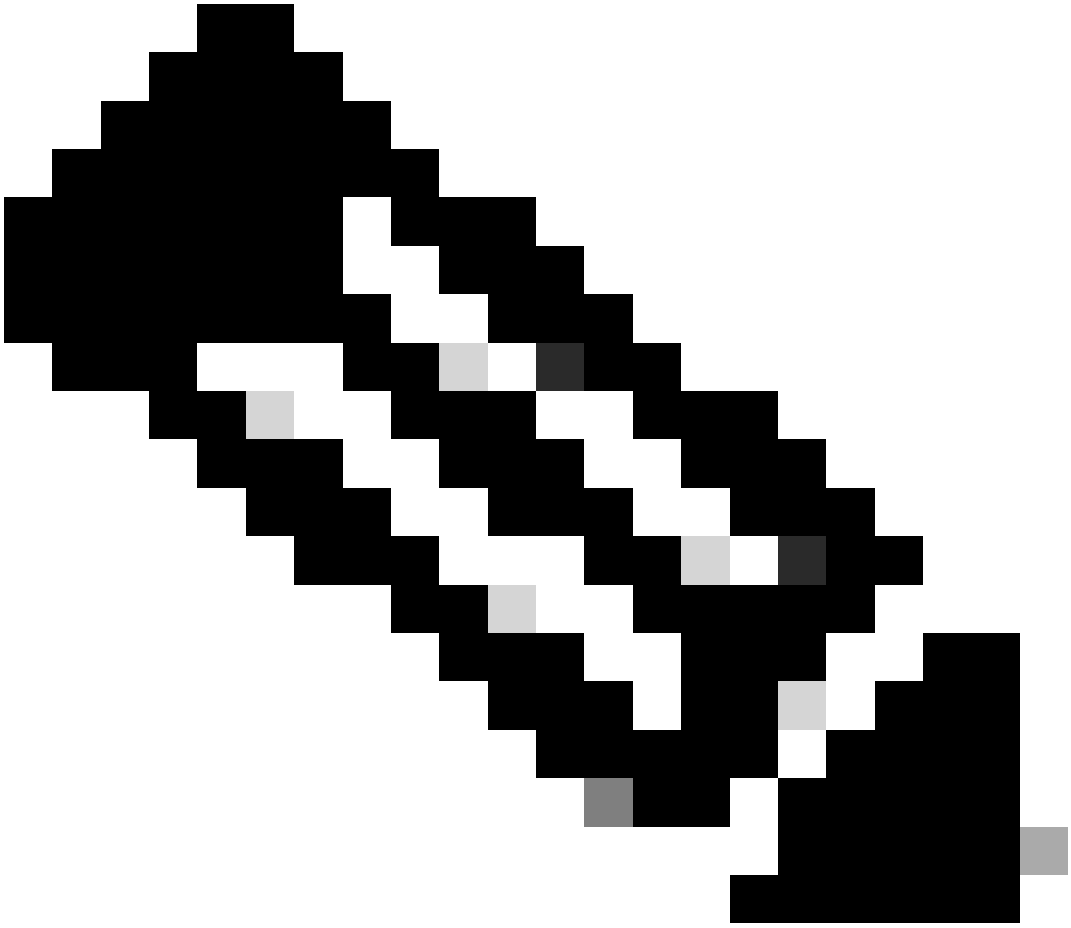
けるか、潜在的なローミングの決定に近づけます。APに近いクライアントは高いデータレートを使用し、高いデータレートは通信時間が短くなります。意図した効果はセルの効率性です。データレートの増加は、特定のフレームの伝送レートにのみ影響を与え、アンテナのRF伝播や干渉範囲には影響を与えないことに注意してください。共用チャネル干渉とノイズを最小限に抑えるには、優れたRF設計手法が依然として必要です。

逆に、低いレートを必須のままにしておくと、通常はクライアントが遠くからアソシエートできるようになり、AP密度が低いシナリオでは有用ですが、密度が高いシナリオではローミングに大打撃を与える可能性があります。6 Mbpsでブロードキャストしている不正APを見つけようとしたユーザは、そのAPが物理的な場所から非常に遠く離れた場所にあることが分かります。

ブロードキャストとマルチキャストのトピックでは、マルチキャストトラフィックの配信率を高めるために、場合によっては2番目の（より高い）必須レートが設定されます。これは、フレームが失われた場合にマルチキャストが確認応答されず、再送信されないため、ほとんど成功しません。すべての無線システムに損失が内在するため、設定されたレートに関係なく、一部のマルチキャストフレームが失われることは避けられません。信頼性の高いマルチキャスト配信へのより優れたアプローチは、マルチキャストをユニキャストストリームとして送信するマルチキャストからユニキャストへの変換技術です。この方法には、高いデータレートと信頼性の高い（確認応答された）配信の両方の利点があります。

1つの必須レートのみを使用することを推奨します。必須レートより下のすべてのレートを無効にし、必須レートより上のすべてのレートをサポート対象のままにします。使用する特定のレートは使用例によって異なります。すでに説明したように、レートを下げると、AP間の距離が長くなる低密度の屋外シナリオで役立ちます。高密度およびイベントネットワークでは、低レートを無効にする必要があります。

どれから始めればよいかわからない場合は、低密度の導入には12 Mbpsの必須レートを使用し、高密度の導入には24 Mbpsを使用します。大規模なイベント、スタジアム、さらには高密度のエンタープライズオフィス環境の多くは、24 Mbpsの必須レート設定で確実に動作することが実証されています。12 Mbpsを下回るレートまたは24 Mbpsを上回るレートが必要な特定の使用例に対しては、適切なテストが推奨されます。

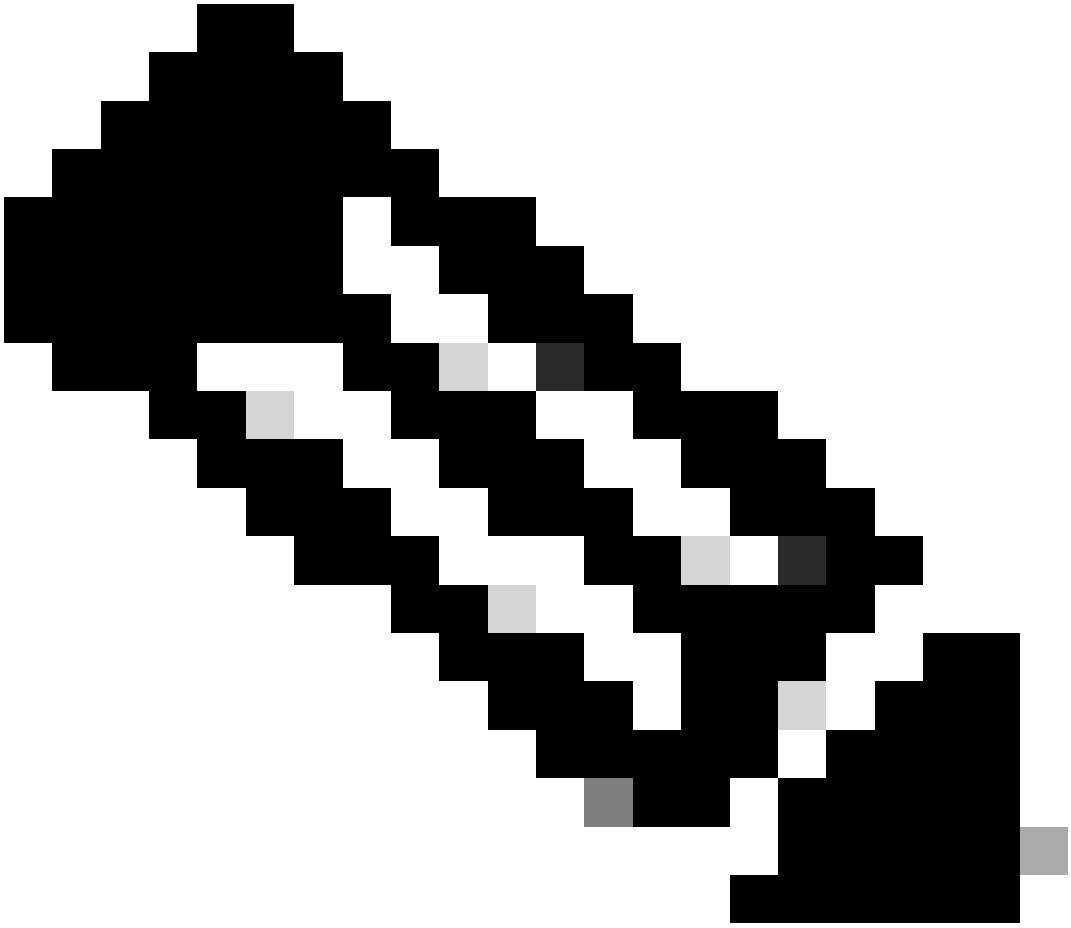


注：すべての802.11n/ac/axレートをイネーブル（WLC GUIのHigh Throughputセクションのすべてのレート）のままにすることをお勧めします。これらのいずれもディセーブルにする必要はほとんどありません。

送信電力

送信電力の推奨値は、導入タイプによって異なります。ここでは、全方向性アンテナを使用した屋内の導入と、指向性アンテナを使用した屋内の導入を区別します。どちらのタイプのアンテナも大規模なパブリックネットワークに存在できますが、通常は異なるタイプのエリアをカバーします。

全方向性の導入では、自動伝送パワーコントロール(TPC)を静的に設定された最小しきい値で使用するのが一般的で、場合によっては静的に設定された最大しきい値も使用します。



注:TPCしきい値は、無線送信電力を示し、アンテナゲインを除外します。使用するアンテナモデルに対してアンテナゲインが正しく設定されていることを常に確認してください。これは、内部アンテナと自己識別アンテナの場合は自動的に行われます。

例 1

TPC最小：5 dBm、TPC最大：最大(30 dBm)

これにより、TPCアルゴリズムは送信電力を自動的に決定しますが、設定された最小しきい値である5 dBmを下回ることはありません。

例 2

TPC最小値：2dBm、TPC最大値：11 dBm

この結果、TPCアルゴリズムは送信電力を自動的に決定しますが、常に2dBmと11dBmの間に留まります。

適切なアプローチは、異なるしきい値を持つ複数のRFプロファイル(低電力(2 ~ 5dBm)、中電力(5 ~ 11dbM)、高出力(11 ~ 17dBM)を作成し、必要に応じて全方向性APを各RFプロファイルに割り当てることです。各RFプロファイルの値は、目的の使用例とカバレッジエリアに合わせて調整できます。これにより、RRMアルゴリズムは事前定義された境界内に留まりながら動的に動作できます。

指向性アンテナのアプローチも非常によく似ていますが、唯一異なる点は、必要な精度のレベルです。指向性アンテナの配置は、導入前のRF調査で設計および検証する必要があります。通常、特定の無線設定値がこのプロセスの結果です。

たとえば、天井に取り付けられたパッチアンテナで約26フィート(8m)の高さから特定のエリアをカバーする必要がある場合、RF調査では、この目的のカバレッジを実現するために必要な最小のTx電力を決定する必要があります（これにより、RFプロファイルの最小TPC値が決定されます）。同様に、同じRF調査から、このアンテナと次のアンテナの間に必要なオーバーラップの可能性、またはカバレッジを終了するポイントを理解します。これにより、RFプロファイルの最大TPC値が得られます。

指向性アンテナのRFプロファイルは、通常、同じ最小および最大TPC値か、または可能な値の範囲が狭く（通常は3dBm未満）設定されます。

設定の一貫性を確保するためにRFプロファイルが推奨されますが、個々のAPのスタティック設定は推奨されません。カバレッジエリア、アンテナタイプ、および使用例（RF-Auditorium-Patch-Ceilingなど）に従ってRFプロファイルに名前を付けることをお勧めします。

正しいTx電力量は、必要なSNR値が、対象カバレッジエリア内で最も弱いクライアントによって、それ以下の場合に得られます。30dBmは、実際の環境（つまり、人でいっぱいの施設）におけるクライアントSNRの目標値として最適です。

CHD（必須）

カバレッジホール検出(CHD)は、カバレッジホールを特定して修復するための別のアルゴリズムです。CHDはWLAN単位だけでなく、グローバルにも設定できます。CHDの影響としては、カバレッジホール（クライアントが低信号で常に検出されるエリア）を補正するために送信電力を増加させることがあります。この影響は無線レベルで発生し、CHDに設定された単一のWLANによってトリガーされた場合でも、すべてのWLANに影響します。

大規模なパブリックネットワークは通常、RFプロファイルを使用して特定の電力レベルに設定されます。一部のネットワークはオープンエリアにあり、クライアントがエリアの内外にローミングする場合があります。これらのクライアントイベントに応答してAPの送信電力を動的に調整するアルゴリズムは必要ありません。

大規模なパブリックネットワークでは、CHDをグローバルに無効にする必要があります。

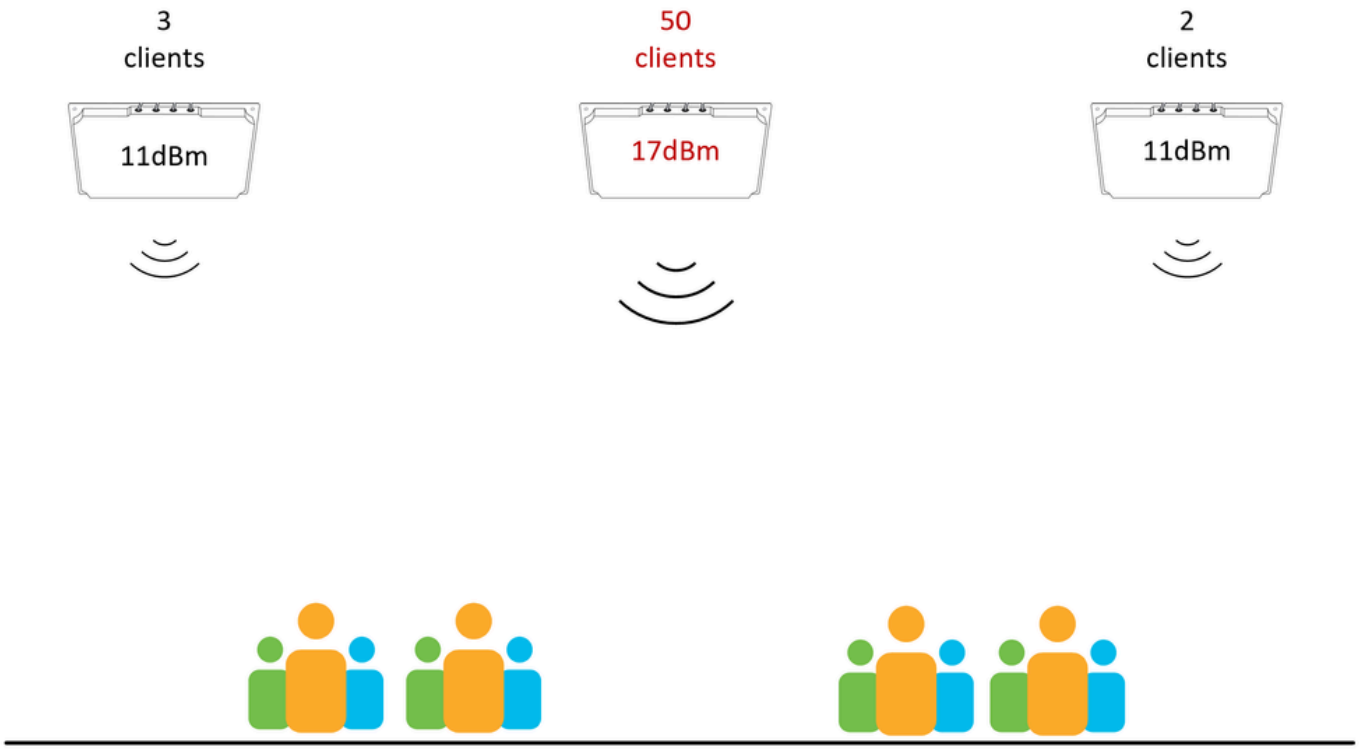
パワーバランス

ほとんどのクライアントデバイスは、関連付けるAPを選択する際に、より高い受信信号を優先します。APが周囲の他のAPに比べて著しく高いTx電力で設定されている状況は回避する必要があります。より高い送信電力で動作するAPはより多くのクライアントを引き付け、AP間のクライ

アント分配の不均等につながります（たとえば、1つのAP/無線がクライアントで過負荷になり、周囲のAPが十分に活用されないなど）。この状況は、複数のアンテナからのカバレッジが大きくオーバーラップする展開や、1つのAPに複数のアンテナが接続されている場合によく見られます。

C9104などのスタジアムアンテナは、設計上アンテナビームがオーバーラップするため、特に送信電力を選択する必要があります。詳細については、『Catalyst 9104 Stadium Antenna(C-ANT9104)Deployment Guide』を参照してください。

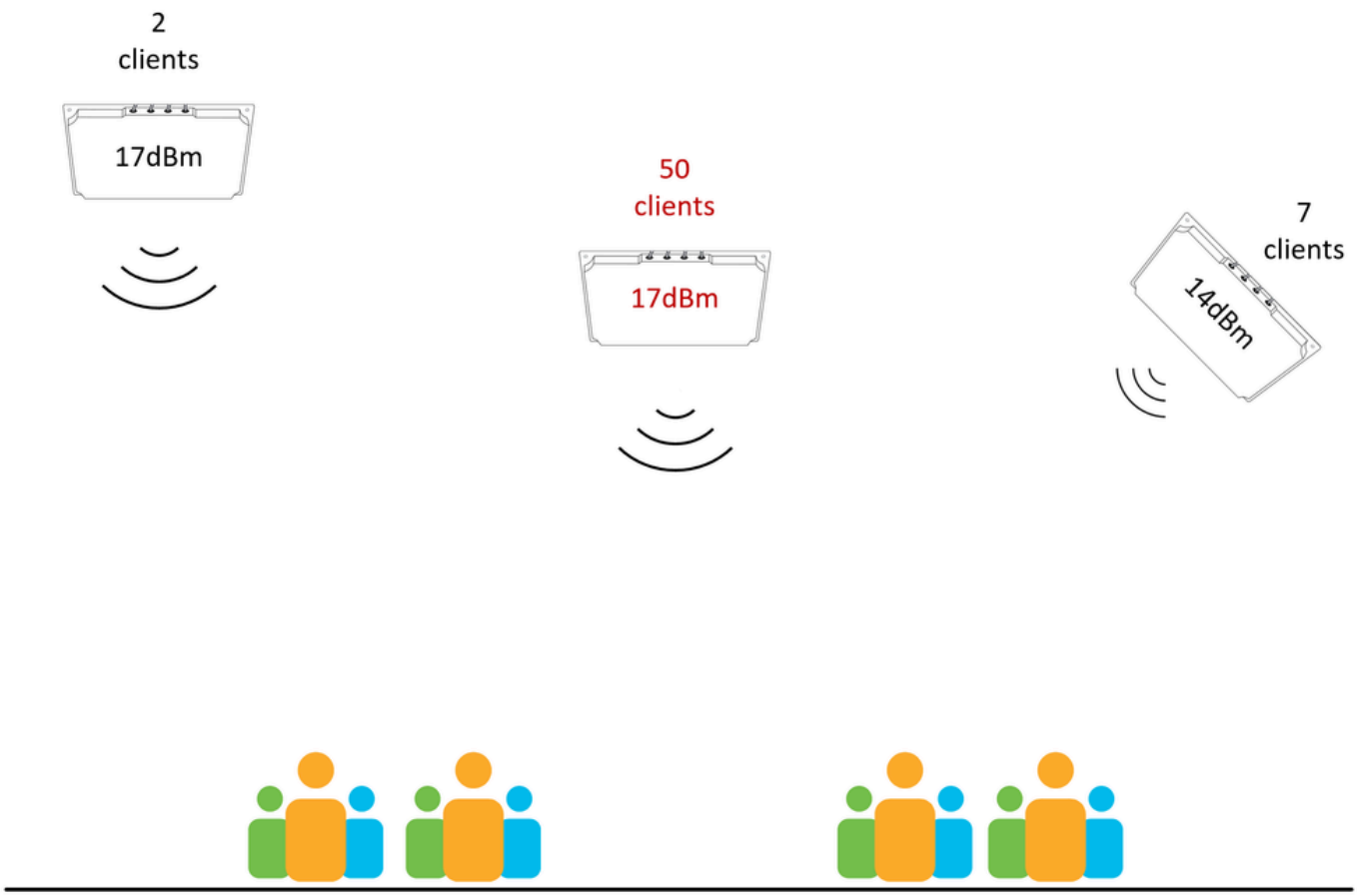
次の図では、中央のアンテナは、周囲のアンテナよりも高いTx電力で設定されています。この設定では、クライアントが中央のアンテナに「スタック」する可能性があります。



ネイバーAPよりも高い出力を持つAPは、周囲のすべてのクライアントを引き付けます

次の図は、より複雑な状況を示しています。すべてのアンテナが同じ高さにあるわけではなく、すべてのアンテナが同じ傾き/方向を使用しているわけではありません。すべての無線に同じTx電力を設定するだけでは、バランスのとれた電力を実現することはより複雑です。このようなシナリオでは、導入後のサイト調査が必要になる場合があります。この調査により、クライアントデバイスの観点（地上）からカバレッジを確認できます。この調査データを使用して、最適なカバレッジとクライアントの分散を実現するための設定のバランスを取ることができます。

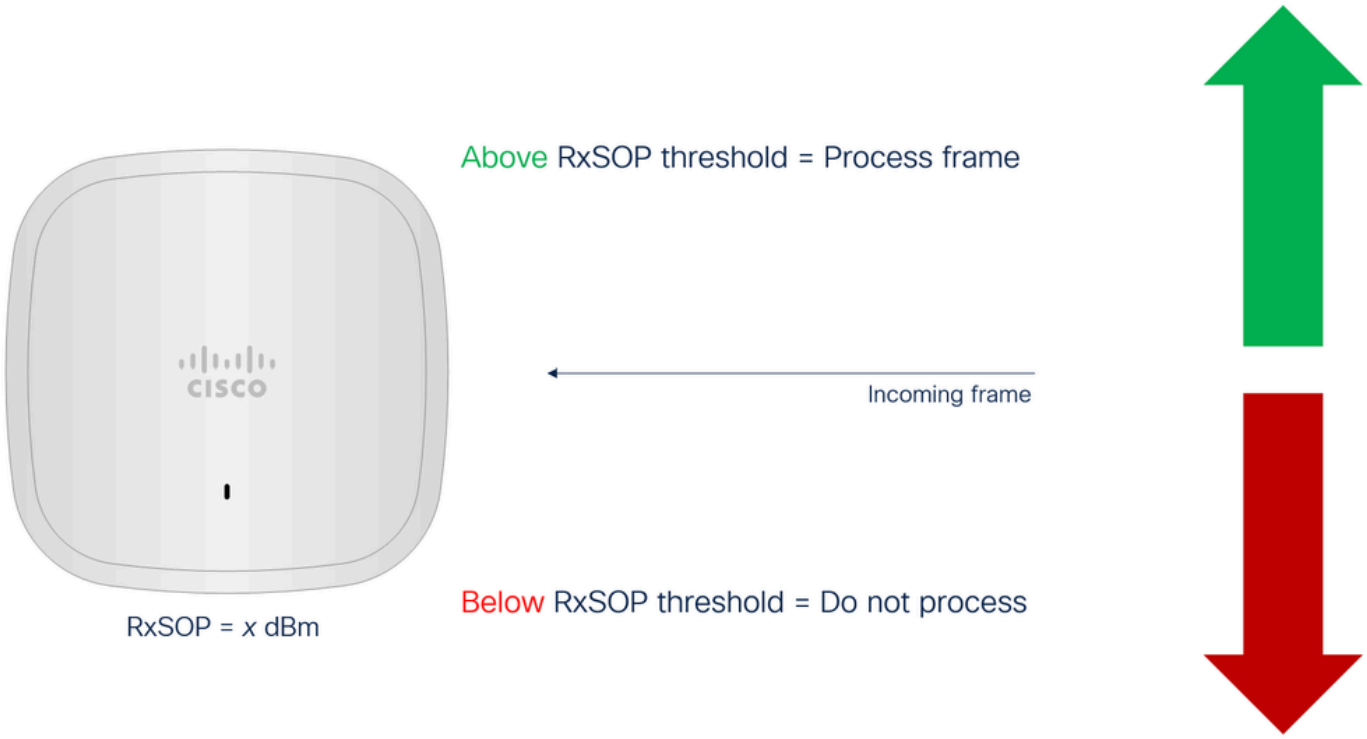
このような複雑な状況を回避する均一なAP配置ロケーションを設計することが、困難なRF調整シナリオを回避する最善の方法です（ただし、他に選択肢がない場合もあります）。



送信電力は同程度であるにもかかわらず、1つのAPがすべてのクライアントを引き付けているが、高さと角度が役割を果たしている

RxSOP

送信セルの特性に影響を与えるTx電力やデータレートなどのメカニズムとは対照的に、RxSOP(Receiver Start of Packet)は受信セルのサイズに影響を与えることを目的としています。基本的に、RxSOPはノイズのしきい値と考えることができます。この値を下回ると、APが送信のデコードを試行しない受信信号レベルを定義します。設定されたRxSOPしきい値よりも弱い信号レベルで着信する送信はAPで処理されず、実際にはノイズとして扱われます。



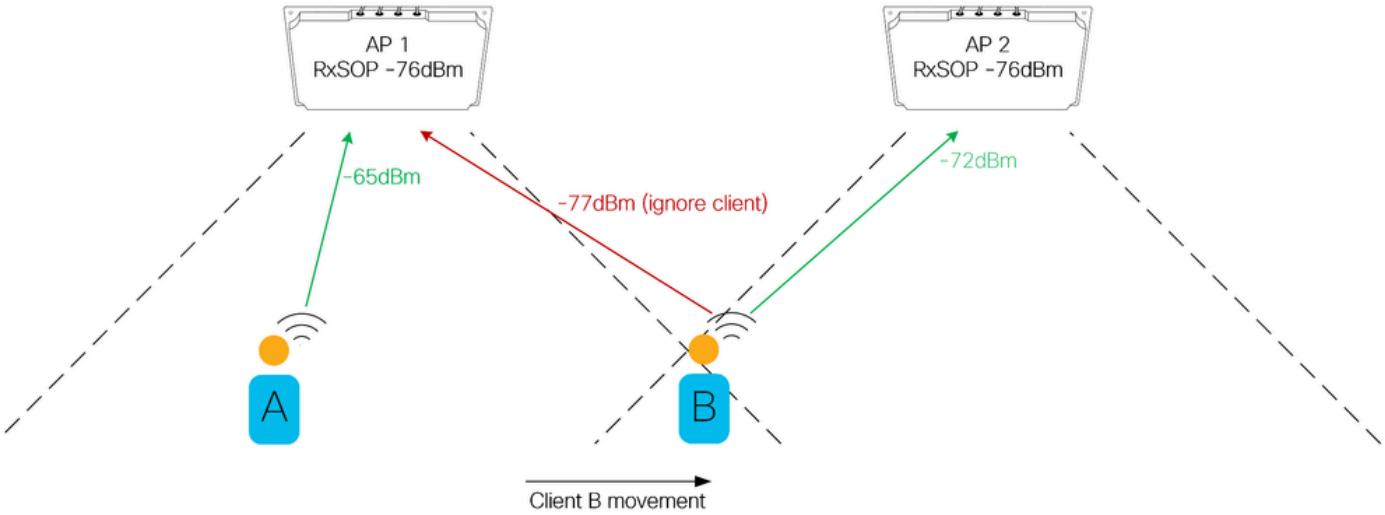
RxSOPの概念の説明

RxSOPの重要性

RxSOPには複数の用途があります。この機能を使用すると、ノイズの多い環境で送信を行うAPの機能を向上させたり、アンテナ間でのクライアントの分散を制御したり、弱いクライアントやスティッキなクライアントを最適化したりできます。

ノイズの多い環境では、802.11フレームを送信する前に、送信ステーション（この場合はAP）がメディアの可用性を評価する必要があることを思い出してください。このプロセスの一部は、すでに発生している送信を最初にリッスンすることです。高密度のWi-Fi環境では、多くのAPが比較的限られたスペースに共存し、同じチャネルを使用することが一般的です。このような混雑した環境では、APは周囲のAPからのチャネル使用率（リフレクションを含む）を報告し、自身の送信を遅らせることができます。適切なRxSOPしきい値を設定することにより、APは、より頻繁な送信の機会とパフォーマンスの向上につながる送信の低下（感知されるチャネル使用率の低下）を無視できます。クライアントの負荷がない（空の場所がある）状態でAPから著しいチャネル使用率（たとえば、10 %を超える）が報告される環境は、RxSOPの調整に適しています。

RxSOPを使用したクライアント最適化の場合は、次の図を検討してください。



rxsopの影響を受けるクライアントのローミング

この例では、カバレッジエリアが明確に定義された2つのAP/アンテナがあります。クライアントBはAP1のカバレッジエリアからAP2のカバレッジエリアに移動しています。AP1よりもAP2の方がクライアントからのヒアリングが良好であるにもかかわらず、クライアントがAP2にまだローミングしていないクロスオーバーポイントがあります。これは、RxSOPしきい値を設定してカバレッジエリアの境界を強制する方法の良い例です。クライアントが常に最も近いAPに接続されるようにすることで、低いデータレートで処理される離れたクライアント接続や弱いクライアント接続を排除し、パフォーマンスを向上させます。この方法でRxSOPしきい値を設定するには、各APの予想されるカバレッジエリアの開始場所と終了場所を十分に理解する必要があります。

RxSOPの危険性。

RxSOPしきい値を設定すると、APが有効なクライアントデバイスからの有効な伝送をデコードしないため、カバレッジホールが発生しやすくなります。APが応答しないため、クライアントにとっては悪影響が及ぶ可能性があります。結局のところ、クライアントの送信が受信されなければ、応答する理由はありません。RxSOPしきい値の調整は慎重に行う必要があります。必ず、カバレッジエリア内の有効なクライアントが設定値によって除外されないようにする必要があります。この方法で無視されても、一部のクライアントは適切に応答できないことに注意してください。RxSOPの設定が厳しすぎると、クライアントが自然にローミングする機会がなくなり、クライアントは別のAPを探さざるを得なくなります。APからビーコンをデコードできるクライアントは、そのAPに送信できることを前提としています。そのため、RxSOPチューニングの目的は、受信セルのサイズをAPのビーコン範囲に一致させることです。（有効な）クライアントデバイスからAPへの直接的な見通し線が常に存在するわけではないことに注意してください。アンテナから離れた方向を向いているユーザや、バッグまたはポケットにデバイスを入れているユーザによって、信号が減衰することがよくあります。

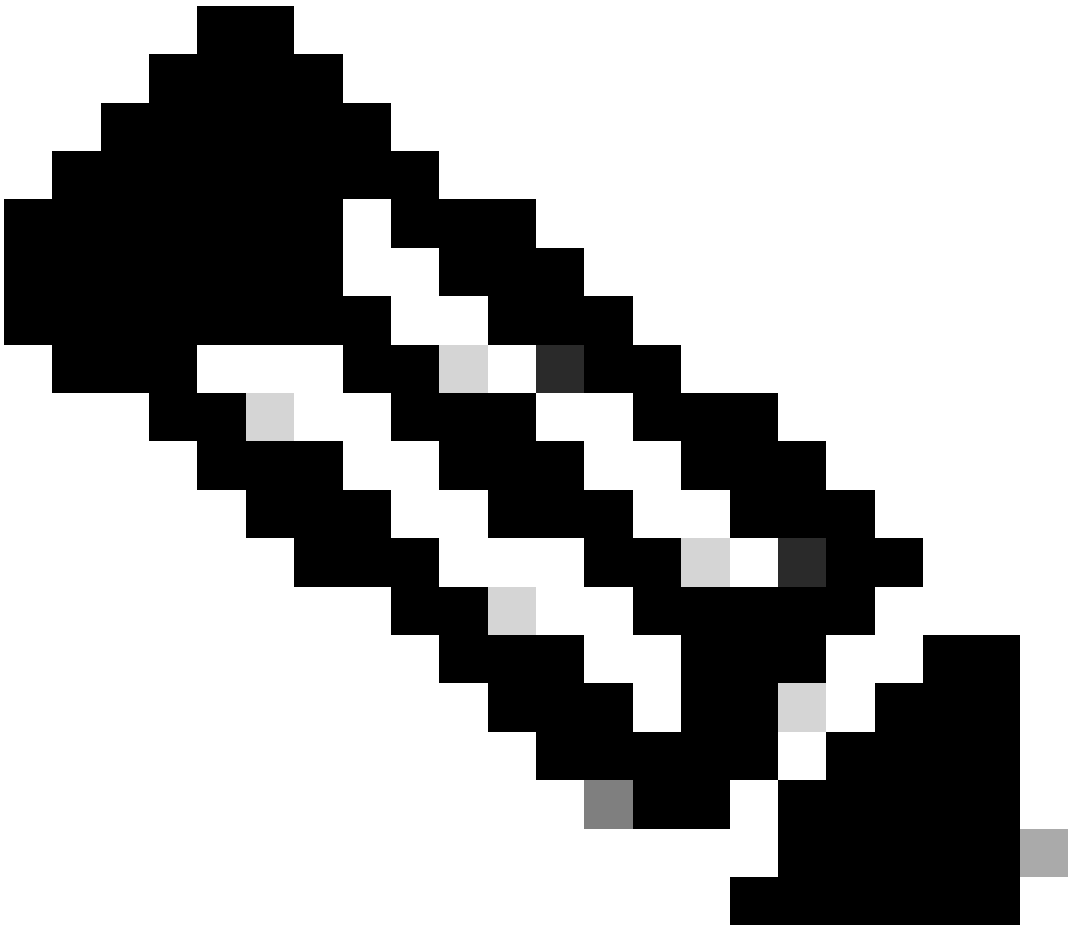
RxSOPの設定

RxSOPはRFプロファイルごとに設定します。

帯域ごとに、事前定義されたdBm値がプリセットされたしきい値（低/中/高）があります。ここで推奨する方法は、使用可能なプリセットの値が目的の値であっても、常にカスタム値を使用することです。これにより、設定が読みやすくなります。

Setting	Value
Auto	Not configured
Low	-80dBm
Medium	-78dBm
High	-76dBm
Custom	-60dBm to -85dBm

RxSop設定テーブル



注:RxSOPの変更は無線をリセットする必要がないため、オンザフライで実行できます。

ネットワークの拡張

一般に、文書化されている機能の上限までデバイスを使用するのは良くない考えです。データシートには真実が記載されていますが、記載されている数値は特定の活動条件に該当する可能性があります。ワイヤレスコントローラは、特定の数のクライアントとAP、および特定のスループットをサポートするようにテストおよび認定されていますが、これは、クライアントが毎秒ローミングし、非常に長い一意のACLをクライアントごとに設定したり、使用可能なすべてのスヌーピング機能をイネーブルにしたりできるとは限りません。したがって、すべての側面を慎重に検討して、ピーク時間帯にネットワークが拡張されるようにし、将来の成長に向けて安全マージンを維持することが重要です。

APの数

ネットワークの導入における最初のタスクの1つは、適切な機器の予算編成と発注です。最大の変動要因は、アクセスポイントとアンテナの数とタイプです。ワイヤレスソリューションは常に無線周波数(RF)設計に基づいている必要がありますが（残念ながら）、これがプロジェクトのライフサイクルの2番目のステップになることがよくあります。単純な屋内企業の導入の場合、多数の予測手法により、妥当なレベルの確実性をもって、ワイヤレス設計者がフロアプランを確認する前でも必要なAPの数を予測できます。この場合、予測モデルも非常に便利です。

産業、屋外、大規模な公衆ネットワーク、外部アンテナが必要な場所など、より困難な設置では、単純な推定手法では不十分なことが多くあります。以前の同様のインストールでは、必要な機器のタイプと量を適切に見積もるために、ある程度の経験が必要です。複雑な施設や施設のレイアウトを理解するには、少なくともワイヤレスアーキテクトによるサイト訪問が必要です。

このセクションでは、特定の展開におけるAPおよびアンテナの最小数を決定する方法のガイドラインを示します。最終的な数量と具体的な取り付け場所は、要件の分析と無線設計プロセスを通じて常に決定されます。

最初の部品表は、アンテナのタイプとアンテナの数という2つの要素に基づいて作成する必要があります。

アンテナタイプ

ここにはショートカットはありません。アンテナのタイプは、カバーする必要がある工リアと、その工リアで使用可能な取り付けオプションによって決まります。これは、物理的なスペースを理解しなければ判断できません。つまり、アンテナとそのカバレッジパターンを理解しているユーザがサイトを訪問する必要があります。

アンテナの数

必要な機器の数は、予想されるクライアント接続数を理解することで判断できます。

1人あたりのデバイス数

人間ユーザ数は、過去の統計に基づいて、会場の座席数、販売チケット数、または予想される来場者数によって決定できます。複数のデバイスを同時にアクティブに使用できるヒューマン・ユーザの能力には疑問が残りますが、各ヒューマン・ユーザは複数のデバイスを持つことができ、

ユーザごとに複数のデバイスを想定するのが一般的です。ネットワークにアクティブに接続するビジターの数は、イベントのタイプや展開によっても異なります。

例1：座席数80,000人のスタジアムには80,000台のデバイスが接続されていないのは正常な状態です。この割合は通常、著しく低くなります。20 %の接続ユーザ率はスポーツイベント中に珍しくなく、これは、座席数80,000のスタジアムの例では、予想される接続デバイス数が16,000台(80,000 x 20 % = 16,000)であることを意味します。この数は、使用するオンボーディングメカニズムによっても異なります。ユーザが何らかのアクション（Webポータルのクリックなど）を実行する必要がある場合、デバイスのオンボーディングが自動で行われる場合よりも数が少なくなります。自動オンボーディングは、以前のイベントから記憶されたPSKのような単純なものから、ユーザの操作なしでデバイスをオンボーディングするOpenRoamingの使用のような高度なものまで可能です。OpenRoamingネットワークは、ユーザの取得率を50 %を大きく上回る可能性があり、キャパシティプランニングに大きな影響を与える可能性があります。

例2：テクノロジー会議のユーザ接続率は高いと考えられます。会議出席者は、ネットワークへの接続時間が長くなり、Eメールにアクセスして1日を通して毎日のタスクを実行できることを期待します。また、このタイプのユーザが複数のデバイスをネットワークに接続する可能性も高くなります。ただし、ユーザが複数のデバイスを同時に使用できるかどうかについては疑問が残ります。テクノロジー会議の場合、100 %の訪問者がネットワークに接続することを前提としています。会議のタイプによっては、この数値が低くなる場合があります。

どちらの例でも、重要なことは、予想される接続デバイスの数を理解することであり、大規模なパブリックネットワークごとに単一のソリューションが存在することはありません。どちらの場合も、アンテナは無線に接続され、その無線に接続するのは（ヒューマンユーザではなく）クライアントデバイスです。したがって、無線ごとのクライアントデバイスは使用可能なメトリックです。

無線あたりのデバイス数

Cisco APでは、Wi-Fi 6アクセスポイントの場合、無線ごとに最大200台の接続デバイスが存在し、Wi-Fi 6Eアクセスポイントの場合、無線ごとに400台のデバイスが存在します。ただし、最大クライアント数を考慮して設計することは推奨されません。計画を立てる際は、無線ごとのクライアント数を最大APキャパシティの50 %よりもかなり低く抑えることをお勧めします。また、無線の数は使用するAPとアンテナのタイプによって異なります。これについては、「シングルとデュアルの5GHz」のセクションで詳しく説明しています。

この段階では、ネットワークを複数のエリアに分割し、エリアごとのデバイス数を予測することをお勧めします。このセクションの目的は、APとアンテナの最小数を見積もることです。

3つのカバレッジエリアの例を考えてみます。予想されるクライアント数はエリアごとに提供され、必要な無線数の見積もりに無線あたり75クライアントという（正常な）値が使用されます。

Area	Expected Devices	Devices / Radio	Radios
Area 1	1000	75	14
Area 2	2000	75	27
Area 3	2500	75	34
Total			75

予想される無線/クライアント数（エリアごと）

これらの初期値は、各エリアに導入されているAPとアンテナのタイプ、およびシングルまたはデュアルの5GHzが使用されているかどうかについての理解と組み合わせる必要があります。6 GHzの計算は5 GHzと同じロジックに従います。この例では、2.4GHzは考慮されていません。

3つのエリアがそれぞれ、2566Pパッチアンテナと9104スタジアムアンテナの組み合わせ、およびシングルとデュアル5 GHzの組み合わせを使用していると仮定します。このシナリオは説明のために使用します。

Area	Total Radios	2566P (Dual 5GHz)	2566P (Single 5GHz)	9104 (Dual 5GHz)
Area 1	14	0	6	4
Area 2	27	6	3	6
Area 3	34	7	0	10
Total Antennas		26	9	20
Total APs		13	9	0 (integrated)

エリアあたりのアンテナ数

各エリアには、必要なアンテナとAPのタイプがリストされています。デュアル5 GHzの場合は、1つのAPに対して2つのアンテナの比率であることに注意してください。

このセクションでは、導入に必要なアンテナとAPの初期数を見積もるためのアプローチを示します。この概算では、物理エリア、各エリアで可能な取り付けオプション、各エリアで使用するアンテナのタイプ、および予想されるクライアントデバイスの数を理解する必要があります。

導入はそれぞれ異なり、特定の領域や困難な領域をカバーするために機器の追加が必要になることも少なくありません。このタイプの見積りは、クライアント容量（カバレッジではない）のみを考慮し、必要な投資規模の概要を示すものです。APとアンテナの最終的な設置場所と機器の合計は、常に、経験豊富な無線技術者によるユースケースとオンサイト検証を十分に理解していることが条件となります。

予想スループット

各ワイヤレスチャネルは、通常スループットに変換される利用可能な容量を提供できます。この容量は、無線に接続されているすべてのデバイス間で共有されます。つまり、無線にユーザ接続が追加されると、各ユーザのパフォーマンスが低下します。このパフォーマンスの低下は線形的ではなく、接続されているクライアントの正確な組み合わせに依存します。

クライアントの機能は、クライアントのチップセットとクライアントがサポートする空間ストリーム数によってデバイスごとに異なります。サポートされる空間ストリーム数ごとの最大クライアントデータレートを次の表に示します。

Client Capability	20MHz channel Wi-Fi 5 (802.11ac)	20MHz channel Wi-Fi 6 (802.11ax)
1 Spatial Stream(s)	86.7Mbps	121.9Mbps
2 Spatial Stream(s)	173.3Mbps	243.8Mbps
3 Spatial Stream(s)	288.9Mbps	365.6Mbps
4 Spatial Stream(s)	346.7Mbps	487.5Mbps

各クライアントタイプに予想される実際の最大スループット

リストされているレートは、802.11標準から導き出された理論上の最大MCS（変調および符号化方式）レートであり、信号対雑音比(SNR)が30dBmを超えると仮定されています。優れたパフォーマンスのワイヤレスネットワークの主な設計目標は、すべてのロケーションのすべてのクライアントに対してこのレベルのSNRを実現することですが、実際にそうなることはほとんどありません。ワイヤレスネットワークは本質的に動的で、ライセンス不要の周波数を使用します。制御されない干渉は、クライアント機能だけでなく、クライアントのSNRにも影響を与えます。

必要なレベルのSNRが達成された場合でも、前述のレートではプロトコルオーバーヘッドは考慮されないため、（さまざまな速度テストツールで測定される）実際のスループットには直接マッピングされません。実世界は常にMCSレートよりも低くなります。

すべてのワイヤレスネットワーク（大規模なパブリックネットワークを含む）で、クライアントのスループットは常に次の要素に依存します。

- クライアントの機能。
- その特定の時点でのクライアントの信号対雑音比。

- その特定の時点で接続している他のクライアントの数。
- その特定の時点における他のクライアントの機能。
- その特定の時点における他のクライアントのアクティビティ。
- 特定の時点での干渉。

これらの要因の変動性に基づいて、機器ベンダーに関係なく、ワイヤレスネットワーク全体でクライアントごとの最小を保証することはできません。

詳細については、『Wi-Fiスループットの検証：テストおよび監視ガイド』を参照してください。

WLC プラットフォーム

WLCプラットフォームの選択は簡単に行えます。まず、管理対象とするAPの推定数とクライアント数を確認します。各WLCプラットフォームのデータシートには、プラットフォームでサポートされている最大のすべてのオブジェクト（ACL、クライアント数、サイトタグなど）が含まれています。これらはリテラルの最大数であり、多くの場合、厳格な適用があります。たとえば、6001 APを、6000 APだけをサポートする9800-80に加入させることはできません。しかし、あらゆる場所で最大限を目指すことは賢明ですか？

Ciscoワイヤレスコントローラは、これらの最大値に到達できるかどうかをテストされていますが、すべての条件下で同時にすべてのドキュメント化された最大値に到達できるとは限りません。スループットの例を見てみましょう。9800-80は最大80 Gbpsのクライアントデータ転送に到達できますが、これは各クライアントパケットが最大で最適なサイズである1500バイトの場合です。パケットサイズが混在する場合、実効最大スループットは低くなります。DTLS暗号化を有効にすると、スループットがさらに低下し、アプリケーションの可視性も同じになります。多くの機能が有効になっている大規模なネットワークでは、現実的な状況で9800-80から40 Gbps以上の帯域幅が期待できます。これは、使用している機能やネットワークアクティビティのタイプによって大きく異なるため、実際の容量を把握するには、このコマンドを使用してデータパスの使用率を測定する以外に方法はありません。負荷メトリックに注目します。これは、コントローラが転送できる最大スループットのパーセンテージです。

```
WLC#show platform hardware chassis active qfp datapath utilization summary

  CPP 0:                      5 secs        1 min        5 min       60 min

Input:     Total (pps)            9            5            5            8

                  (bps)        17776         7632         9024        10568

Output:    Total (pps)            5            3            3            6

                  (bps)        11136        11640        11440        41448

Processing: Load (pct)            0            0            0            0


WLC#
```

同様の方法で、9800-80は通常のアクティビティで6000台のAPを完全に処理できます。ただし、スタジアムや空港などの公共の場所にある6,000台のAPは通常のアクティビティとしてカウントされません。クライアントのローミング量と周囲プローブの量を考慮すると、大規模なパブリックネットワークが最大スケールで存在する場合、1つのWLCでCPU使用率が増加する可能性があります。クライアントが移動するたびに送信されるモニタリングとSNMPトラップを追加すると、負荷が急激に過大になる可能性があります。大規模な公共施設や大規模なイベントの特徴の1つは、人々が移動し、常に関連付け/関連付けの解除が行われるにつれて、クライアントのオンボーディングイベントが大幅に増加するため、CPUとコントロールプレーンに余計な負荷がかかることです。

多数の導入により、9800-80ワイヤレスコントローラの単一(HA)ペアは、1000を超えるAPを持つ大規模なスタジアムの導入に対応できることが示されています。アップタイムとアベイラビリティが最も重要なイベントでは、2つ以上のコントローラペアにAPを分散させることも一般的です。大規模なネットワークを複数のWLCに分散するとコントローラ間ローミングがさらに複雑になる場合は、スタジアムボウルなどの狭い空間でのクライアントのローミングを慎重に考慮する必要があります。

このドキュメントの「サイトタグ」セクションも参照してください。

WLCハイアベイラビリティ

ハイアベイラビリティステートフルスイッチオーバー(HA SSO)ペアを使用することをお勧めします。これにより、ハードウェアの冗長性が提供されますが、ソフトウェアの障害からも保護されます。HA SSOを使用すると、セカンダリWLCがシームレスに引き継ぐため、1つのデバイスでのソフトウェアクラッシュはエンドユーザに対して透過的です。HA SSOペアのもう1つの利点は、インサービスソフトウェアアップグレード(ISSU)機能によって提供される無中断アップグレードです。

ネットワークが十分に大きい場合は、追加のコントローラ(N+1)を使用することも推奨されます。これは、HA SSOが実行できない複数の目的に使用できます。実稼働ペアをアップグレードする前に、このWLCで新しいソフトウェアバージョンをテストできます（ネットワークの特定のセクションをテストするために、少数のテストAPのみを移行できます）。まれな条件として、HAペアの両方のWLCに影響を与える可能性があり（問題がスタンバイに複製される場合）、ここでは、N+1によりアクティブ – アクティブシナリオの安全なWLCを使用して、AP間で段階的な移行を実行できます。また、新しいAPを設定するためのプロビジョニングコントローラとしても使用できます。

9800-CLは非常に拡張性が高く、強力です。これらのスイッチのデータ転送容量ははるかに小さく（SR-IOVイメージでは2 Gbpsから4 Gbps）、FlexConnectのローカルスイッチングシナリオに制限される傾向があることに注意してください（中央スイッチングでは少数のAPになる場合もあります）。ただし、メンテナンスウィンドウ中に追加のコントローラが必要な場合や、問題のトラブルシューティングを行う場合には、N+1デバイスとして役立ちます。

外部システム

このドキュメントでは主に大規模イベントネットワークのワイヤレスコンポーネントを中心に扱いますが、拡張および設計段階で検討が必要なサポートシステムも数多く存在します。これらの

システムの一部をここで説明します。

コアネットワーク

大規模なワイヤレスネットワークは通常、中央スイッチングモードで大規模なサブネットとともに展開されます。これは、非常に多数のクライアントMACアドレスとARPエントリが隣接する有線インフラストラクチャにプッシュされることを意味します。さまざまなL2およびL3機能専用の隣接システムが、この負荷を処理するために十分なリソースを備えていることが重要です。L2スイッチの場合、一般的な設定はスイッチデバイスマネージャ(SDM)テンプレートの調整です。SDMテンプレートは、システムリソースの割り当てを行い、ネットワーク内のデバイスの機能に応じてL2機能とL3機能の間でバランシングを行います。コアL2デバイスが予期されるMACアドレスエントリの数をサポートできることを確認することが重要です。

ゲートウェイNAT

パブリックネットワークの最も一般的な使用例は、訪問者にインターネットアクセスを提供することです。データパスのどこかに、NAT/PAT変換を行うデバイスが存在する必要があります。インターネットゲートウェイには、負荷を処理するために必要なハードウェアリソースとIPプール設定が必要です。単一のワイヤレスクライアントデバイスが多数のNAT/PAT変換を処理できることに注意してください。

DNS/DHCP

この2つのシステムは、優れたクライアントエクスペリエンスを実現するための鍵となります。DNSサービスとDHCPサービスの両方で、負荷を処理するための適切なスケーリングだけでなく、ネットワーク内の配置についても考慮する必要があります。高速で応答性の高いシステムをWLCと同じ場所に配置することで、最適なエクスペリエンスを実現し、クライアントのオンボーディング時間を短縮できます。

AAA/Webポータル

遅いWebページが好きな人はいません。外部Web認証に適した適切で拡張性の高いシステムを選択することは、優れたクライアントオンボーディングエクスペリエンスにとって重要です。同様に、AAAの場合、RADIUS認証サーバは無線システムの要求に対応できる必要があります。場合によっては、重要な瞬間の間に負荷が急上昇する可能性があることに注意してください。たとえば、サッカーの試合中に半時間が発生し、短時間で高い認証負荷が発生する可能性があります。適切な同時負荷に合わせてシステムを拡張することが重要です。AAAアカウンティングなどの機能を使用する場合は、特に注意が必要です。すべてのコストで時間ベースのアカウンティングを回避し、アカウンティングを使用する場合は、中間アカウンティングを無効にしてみてください。考慮すべきもう1つの重要な項目は、ロードバランサの使用です。ここでは、完全な認証フローを保証するためにセッションピニングメカニズムを使用する必要があります。RADIUSタイムアウトを5秒以上に設定してください。

クライアント数が多い802.1X SSIDを使用する場合（OpenRoamingなど）、必ず802.11r Fast Transition(FT)を有効にしてください。有効にしないと、クライアントがローミングするたびに認証ストームが発生する可能性があります。

DNS/DHCP

DHCPに関するいくつかの推奨事項：

- DHCPプールが、予想されるクライアント数の3倍以上であることを確認します。IPは、クライアントが切断された後も、しばらくの間割り当てられたままになります。そのため、ゲストの滞留時間によっては、IPアドレスを多く消費する可能性があります。リース時間をユーザが施設を訪問する予想期間に合わせるようにしてください。一般的な訪問期間が2時間の場合、1週間のIPアドレスを割り当てても意味がありません。これは古いリースをサイクルするのに役立ちます。
- クライアントに単一の大きなサブネットを使用することが推奨されます。WLCにはプロキシARP機能があり、デフォルト（DHCP以外）ではブロードキャストを転送しません。クライアントに大きなクライアントサブネット（/16など）を使用しても、問題は発生しません。多数のVLANがあるVLANグループと比べると、単一の大きなVLANの方が簡単です。多数の小さなサブネット（/24など）とVLANグループを設定しても、ブロードキャストドメインに影響を与えず、設定がより複雑になるだけであるため、VLANのダーティ化などの問題が発生し、均等に使用できない各種のDHCPプールを追跡する必要があります。
- サブネットのレイヤ3ゲートウェイで処理されるDHCPリレー機能を使用して、ワイヤレスコントローラでDHCPをブリッジモードに保ちます。これにより、最大限の効率性と簡素化が実現します。これは、ワイヤレスコントローラがDHCPプロセスに一切関与しないようにするためです。
- 認証方式に関係なく、すべてのパブリックWLANでDHCP Requiredを使用します。これにより、ごく一部のクライアントアソシエーションが失敗する場合もありますが、クライアントが自身にスタティックIPアドレスを割り当てようとしたり、クライアントの誤動作や権限のない古いIPアドレスの再利用などによって、重大なセキュリティ上の問題が発生する可能性があります。

ネットワークの運用

適切な設定

最新のWi-Fiのすべての最新機能を活用するために、多くのオプションを有効にしたいと考えています。ただし、特定の機能は小規模な環境では効果的ですが、大規模で高密度な環境では大きな影響を与えます。同様に、特定の機能が互換性の問題を引き起こす可能性があります。シスコの機器はすべての標準を尊重し、幅広い種類のテスト済みクライアントとの互換性を提供しますが、世界にはバグのあるドライバソフトウェアバージョンや特定の機能との非互換性を持つ場合がある唯一のクライアントデバイスが溢れています。

クライアントに対する制御レベルに応じて、保守的である必要があります。たとえば、会社の大規模な年次集会用にWi-Fiを導入する場合、ほとんどのクライアントが会社のデバイスであることがわかっているので、それに応じて有効になるように機能セットを計画できます。一方、空港のWi-Fiを運用している場合、ゲストの満足度はネットワークへの接続能力に直接関係し、ユーザが使用できるクライアントデバイスを制御することはできません。

SSID

SSIDはいくつですか。

SSIDはできる限り少なくすることを常に推奨しています。同じチャネル上に複数のAPが存在する可能性がほぼ保証されるため、高密度ネットワークではこの状況がさらに悪化します。一般的に、多くの導入では使用するSSIDの数が多すぎると認識し、SSIDの数が多すぎると認識しますが、使用するSSIDの数を減らすことはできません。複数のSSIDを1つに統合する場合のSSIDとオプションの類似点を理解するには、各SSIDについてビジネス上および技術上の調査を実施する必要があります。

いくつかのセキュリティ/SSIDタイプとその用途について説明します。

WPA2/3パーソナル

事前共有キーのSSIDは、そのシンプルさのために非常に人気があります。バッジや紙、サインのどこかにキーを印刷するか、何らかの方法で訪問者に伝えることができます。事前共有キーのSSIDが、ゲストSSIDに対しても好まれる場合があります（このキーがすべての出席者によく知られている場合）。これは、接続の意図的な性質によるDHCPプールの枯渇を防ぐのに役立ちます。通過するデバイスは自動的にネットワークに接続しないため、DHCPプールのIPアドレスを使用できません。

WPA2 PSKは、すべてのユーザが同じキーを使用するため、トラフィックが簡単に復号化できるため、プライバシーを提供しません。逆に、WPA3 SAEはプライバシーを提供し、すべてのユーザがマスターキーを持っていても、他のクライアントが使用する暗号キーを取得することはできません。

WPA3 SAEはセキュリティに適しており、多くのスマートフォン、ラップトップ、オペレーティングシステムでサポートされています。一部のIoTデバイスまたはスマートウェアラブルは、サポートが限られている可能性があり、最近のドライバまたはファームウェアのアップデートを受信していない古いクライアントでは、一般的に問題が発生する可能性があります。

物事を簡素化するために、移行モードWPA2 PSK-WPA3 SAE SSIDを検討したくなるかもしれませんが、これは互換性の問題を引き起こすフィールドで示されています。適切にプログラムされていないクライアントでは、同じSSIDで2種類の共有キー方式を使用することは想定されていません。WPA2とWPA3の両方のオプションを提供する場合は、個別のSSIDを設定することを推奨します。

WPA2/3エンタープライズ

WPA3 Enterprise（AES 128ビット暗号化を使用）は、技術的にはWPA2 Enterpriseと同じセキュリティ方式であり（少なくともSSIDビーコンでアドバタイズされる）、互換性を最大限に高めます。

802.1Xでは、最近のデバイス（Android 8または古いApple IOSバージョンで問題が報告された）では互換性の問題が見られないため、移行モードSSIDをお勧めします。IOS XE 17.12以降のリリースでは、単一のTransition Enterprise(TXE)SSIDを使用できます。このSSIDでは、6GHzでWPA3のみが使用およびアドバタイズされ、5GHz帯域でWPA2がオプションとして提供されます。できるだけ早く、エンタープライズSSIDでWPA3を有効にすることを推奨します。

WPAエンタープライズSSIDは、ユーザのアイデンティティに応じてAAAパラメータ（VLANやACLなど）を返すことができるアイデンティティプロバイダーデータベースが存在するキーユー

ザに使用できます。このようなタイプのSSIDには、ゲストSSIDの利点（クレデンシャルを入力せずに簡単に接続できる機能をゲストに提供することによって）と企業のSSIDのセキュリティを組み合わせたeduroamまたはOpenRoamingがあります。電話にプロファイル（イベントアプリで簡単に提供できます）があれば、クライアントはeudroamまたはOpenRoaming SSIDに参加するために何もする必要がないため、802.1Xに通常関連するオンボーディングの複雑さが大幅に軽減されます

ゲストSSID

ゲストSSIDは、しばしばオープン認証と同義です。外部、ローカル、または中央のWeb認証など、さまざまな形式でWebポータルを背後に追加することができます（目的の利便性やローカル要件に応じて）。ただし、概念は変わりません。ゲストポータルを使用する場合、大規模な環境ではスケーラビリティが問題になる可能性があります。詳細は、「スケーラビリティの設定」セクションを参照してください。

6 GHzの動作では、ゲストSSIDでOpenだけでなくEnhanced Openを使用する必要があります。この方法でも接続は可能ですが、プライバシー（WPA2-PSKよりもさらに優れたプライバシー）と暗号化が提供されます。ただし、SSIDで接続する際にキーやクレデンシャルを入力する必要はありません。主要なスマートフォンのベンダーとオペレーティングシステムは現在、Enhanced Openをサポートしていますが、このサポートはワイヤレスクライアントベースにはまだ広まっていません。拡張オープン移行モードでは、適切な互換性オプションが提供されます。このオプションでは、対応デバイスは（拡張オープンを使用して）暗号化されたゲストSSIDに接続しますが、非対応デバイスは以前のように単純にオープンなSSIDを使用します。エンドユーザが認識するSSIDは1つだけですが、この移行モードではビーコンで2つのSSIDをブロードキャストすることに注意してください（1つだけが表示されます）。

大規模なイベントや会場では、純粋にオープンのままにするのではなく、ゲストSSIDでPSKを設定することが推奨されます（拡張オープン移行モードの方が適していますが、これにより2つのSSIDが作成され、クライアントの互換性を広く証明する必要があります）。これによりオンボーディングは少し複雑になりますが（PSKを人々のバッジやチケットに印刷するか、何らかの方法でアドバタイズする必要があります）、エンドユーザがネットワークを使用する意図なしに、不意にクライアントがネットワークに自動的に接続することを回避します。また、オープンなネットワークの優先順位を下げ、セキュリティ警告を表示するモバイルオペレーティングシステムベンダーが増えています。その他の状況では、接続する通行人の最大数が必要になるため、オープンの方が適しています。

SSID数の結論

保持する必要があるSSIDの数に関する質問に対して満足な回答はありません。この影響は、設定されている最小データレート、SSIDの数、および同じチャネルでブロードキャストしているAPの数によって異なります。ある大規模なシスコのイベントでは、ワイヤレスインフラストラクチャで5つのSSIDを使用しました。メインのWPA2 PSK、セキュリティと6GHzカバレッジのためのWPA 3 SAE SSID、教育関係者のアクセスを容易にするためのエンタープライズEduroam SSID、イベントアプリからWi-Fiを設定したすべてのユーザを安全に迎え入れるOpenRoaming SSID、スタッフと管理者ネットワークアクセスのための別の88882X SSIDです。 これはすでに多すぎましたが、使用可能なチャネルの数が多く、チャネルのオーバーラップを可能な限り減ら

すために使用される指向性アンテナのおかげで、効果は妥当でした。

レガシーSSIDとメインSSIDの概念

一定期間、2.4GHzサービスを2.4GHzでのみアドバタイズされる「レガシー」の個別のSSIDに制限することが推奨されました。2.4GHzサービスの提供を完全に停止するユーザが増えるにつれて、この方法はあまり一般的ではなくなってきています。ただし、この概念は他の概念と共存できますが、継続する必要があります。WPA3 SAEを展開したいのですが、移行モードではクライアントとの互換性の問題が発生します。WPA2「レガシー」SSIDとメインWPA3 SAE SSIDを使用する最もパフォーマンスの低いSSIDに「legacy」という名前を付けてもクライアントは引き付けられず、メインSSIDとの互換性の問題に直面してこのレガシーSSIDを必要とするクライアントの数を簡単に確認できます。

でもなぜそこで止まる？802.11vが一部の古いクライアントで問題を引き起こしたり、一部のクライアントドライバがSSIDでDevice Analyticsを有効にするのを嫌がるという噂を耳にしましたか。高度なメインSSIDでこれらのすべての便利な機能を有効にし、レガシー/互換性SSIDではこれらの機能をオフのままにします。これにより、メインSSIDで新しい機能の展開をテストしながら、クライアントがフォールバックできる最大の互換性SSIDを提供できます。このシステムはこの方法でのみ動作します。互換性に基づくSSIDをメインとして逆の名前を付け、拡張SSIDに「<name>-WPA3」などの名前を付けると、使用していた古いSSIDが人々によって使用され、「新しい」SSIDでの採用が何年も続かないことがわかります。新しい設定または機能を展開すると、接続するクライアント数が少なくなるため、結果が不確定になります。

SSID機能

- Aironet拡張機能は無効にしておくことをお勧めします。これらはサイト調査やWGB操作に特に便利ですが、一部のレガシークライアントで問題が発生する場合があります。Aironet IEでは、セキュリティを意識した導入では不要なAPホスト名もアドバタイズされます。
- CCKMは非推奨のプロトコル（FTを推奨）であり、無効にする必要があります。
- 現時点では、クライアントでの高度な暗号化のサポートが低いため、WPA3でもAES-128暗号化を使用するのが最善です（より安全で制限の厳しい特定のSSIDを購入する余裕がない場合）
- カバレッジホール検出は（すべてのSSIDに対して）無効にするのが最適です。大規模な導入では通常、指向性アンテナを使用し、綿密なサイト調査が必要になります。各アンテナの電力レベルはRF設計プロセスの結果であり、通常は特定のレベルに設定されます。
- 一部のクライアントでは、FTが完全にはアドバタイズされないが、一部の属性には存在する場合に問題が発生する可能性があるため、Adaptive FTを無効にする必要があります。FTを完全に無効にする（互換性を最大にする）か、ほとんどのクライアントがサポートしているFT+802.1Xを使用してください（古いFTまたはIoT指向のFTを除く）。FT+802.1Xを設定すると、FT以外のクライアントでもSSIDへの参加が許可されます。考えられる唯一の問題は、同じSSIDで2つのセキュリティオプションが表示されることを許容しない一部のクライアントです。
- 802.11ac MU-MIMOを無効にします。802.11acでは複雑さが増し、利点は非常に少なくなります。
- BSSターゲットウェイクアップ時間を無効にします。現在、クライアント側での導入が少なくなっています。

- アグレッシブロードバランシングと帯域選択を無効にします。2.4GHzでSSIDをアドバタイズしない場合（または専用SSID上にある場合）、およびアグレッシブロードバランシングがロードされたAPへの接続を要求する場合、クライアントが受け入れる前に数回クライアントを拒否してクライアント関連付けを遅延させる場合は、Band Selectは必要ありません。ビジーな環境でAPをロードしましたが、これはクライアントエクスペリエンスにとってマイナスです。
- Fastlane+を無効にします。
- Universal Adminを無効にします。この機能は3700 AP用で、-UXドメイン内でのみ使用できます。葉の上に残すと、不要な攻撃ベクトルが開きます。
- Opportunistic Key Caching(OKC)を有効のままにします。FTをサポートしていないクライアントの高速ローミングメカニズムとして機能します。
- WMMを許可したままにします。この機能を無効にすると、ネットワークが802.11gの時代に戻るため、この機能を必要としても9800プラットフォームでは利点が得られません。
- IPソースガードを有効にします。
- RADIUSプロファイリングを無効にします。非常にビジーな環境では、クライアントがDHCPを実行したりHTTPパケットを送信するたびに大量のRADIUSアカウンティングメッセージが送信される可能性があり、RADIUSサーバが過負荷になる可能性が非常に高くなります。
- 隠しSSIDの使用は避けます。これはセキュリティ上の目的には適していません。SSID名は、単純なアプリケーションを使用するか、スニファキャプチャを実行することで簡単に検出できます。SSIDを非表示にすると、パッシブビーコンスキャンの利点がなくなるため、すべてのクライアントローミングが遅くなり、隣接するAP情報を取得するためにアクティブスキャンに依存する必要があります。
- RF使用率に大きな影響があるため、無線ごとに4つ以上のWLANを使用しないようにしてください。これは困難な制限ではありません。5つのWLANを使用することで機能しますが、より多くのWLANを使用することで無駄な通信時間が生じることを非常に意識しています。
- 802.11vと802.11kは、一般的なクライアントタイプでますますサポートされる標準です。通常、クライアント接続に関して問題を引き起こすことはありません。そのメリットは、クライアントがそれらのプロトコルをどのように利用するかによって大きく異なり、場合によっては（802.11kの場合）、CPU使用率が若干高くなることがあります。IoTまたはレガシーSSIDには含めませんが、実稼働SSIDで可能であれば有効にする必要があります。

サイト タグ

サイトタグは、同じFlexConnect設定やAP参加プロファイル設定（クレデンシャル、SSHの詳細、国コードなど）を共有するアクセスポイントをグループ化できる設定項目です。サイトタグが重要な理由サイトタグは、Catalyst 9800内部のWNCDプロセスによるAPの処理方法も定義します。例をいくつか挙げて説明します。

- 8つのWNCDプロセスを持つ9800-80で4つのサイトタグを設定すると、各サイトタグは（それぞれ別のCPUコアで実行される）異なるWNCDプロセスに割り当てられ、4つのWNCDプロセスは何も行いません。これは、9800-80のすべてのCPUを使用しているわけではないことを意味し、サポートされている最大6000のAPでロードすることは推奨されません。

Site tag 1	Site tag 2	Site tag 3	Site tag 4	-	-	-	-
WNCD 1	WNCD 2	WNCD 3	WNCD 4	WNCD 5	WNCD 6	WNCD 7	WNCD 8
CPU	CPU	CPU	CPU	CPU	CPU	CPU	CPU

サイトタグバランシングの最初の例

- 8つのWNCDプロセスを持つ9800-80で10個のサイドタグを設定した場合、2つのWNCDプロセスがそれぞれ2つのサイトタグを処理し、残りの6個が1つのサイトタグをそれぞれ処理します。

Site tag 1 Site tag 9	Site tag 2 Site tag 10	Site tag 3	Site tag 4	Site tag 5	Site tag 6	Site tag 7	Site tag 8
WNCD 1	WNCD 2	WNCD 3	WNCD 4	WNCD 5	WNCD 6	WNCD 7	WNCD 8
CPU	CPU	CPU	CPU	CPU	CPU	CPU	CPU

サイトタグバランシングの2番目の例

多数のサイトと多数のサイトタグを含む地理的に大規模な展開では、サイトタグの数は、使用しているプラットフォーム上のWNCDプロセスの数の倍数にすることを推奨します。

ただし、通常は1つの屋根の下にあるイベントネットワーク、または同じ施設内の複数の建物の場合は、サイトタグの数を特定のプラットフォーム上の正確な数のWNCDと一致させることを推奨します。最終的な目標は、各WNCDプロセス（およびワイヤレスタスクに割り当てられた各CPUコア）がほぼ同じ数のクライアントローミングイベントを処理し、すべてのCPUコアに負荷が分散されるようにすることです。

Platform type	Number of WNCD processes
9800-CL small OVA	1
9800-CL medium OVA	3
9800-CL large OVA	7
9800-L	1
9800-40/CW9800-M	5
9800-80/CW9800-H	8

各プラットフォームタイプのWNCDプロセス数

コアで本当に重要なことは、これらのAP間の頻繁なクライアントローミングイベントが同じCPUプロセス内に留まるように、同じ物理的な近隣にあるAPを同じサイトタグにグループ化することです。つまり、1つの大きな施設がある場合でも、施設を複数のサイトタグに分割し（施設を処理するWNCDプロセスと同じ数）、APをできる限り論理的にこれらにグループ化して、複数のサイトタグ間に均等に分散された論理的なRFネイバーフッドグループを形成することをお勧めします。

IOS XE 17.12以降では、WLCがRFプロキシミティに基づいてAPをグループ化するように、ロードバランシングアルゴリズムを有効にできます。これにより、ユーザの負担が軽減され、WNCDプロセス全体でAPがバランスよく分散されます。これは、正しい数のサイトタグに配置するネイバーAPのグループを簡単に作成できない場合に役立ちます。このアルゴリズムの特異性の1つは、サイトタグの割り当てに関係なくAPをWNCDプロセスに割り当てることです。つまり、APのサイトタグ割り当ては変更されません。その後、純粋に基本的な設定ロジックに基づいてサイトタグを割り当て、アルゴリズムが最適な方法でAPとCPUの間のバランスを取るようにします。

RFベースの自動APロードバランシング機能については、『Cisco Catalyst 9800シリーズワイヤレスコントローラソフトウェアコンフィギュレーションガイド、Cisco IOS XE Dublin 17.12.x』を参照してください。

WNCDプロセスのCPU使用率は、大規模なイベントの発生時に監視する必要があります。1つ以上のWNCDプロセスの使用率が高い場合は、WNCDが処理しているAPまたはクライアントが多すぎるか、あるいは、処理しているAPまたはクライアントが平均よりもビジーである（空港などで常にすべてのAPまたはクライアントがローミングする場合など）可能性があります。

ポリシー プロファイル

- ARPおよび重複アドレス検出(DAD)プロキシを有効にします。これにより、デバイスがワイヤレスデバイスのMACアドレスを学習しようとする際に、WLCがワイヤレスクライアントに代わって応答できます。これにより、ワイヤレスクライアントのバッテリも節約されます。
- 必要でない限り、WGB機能を有効にしないでください。
- スタティックIPアドレスを持つクライアントを回避するために必要なDHCPを有効にします。
- idle-timeoutを短く（300秒）します。一部の管理者は、クライアントの再認証を回避するために長い時間を費やしますが、アイドルタイムアウトが長いと、クライアント数がリアルタイムから遅延するため、ゴーストクライアントエントリが発生し（レポートに影響します）、結果として発生します。クライアントが削除される際のアカウンティングフラッドを回避するには、idle -timeoutをgroup key rotationタイマーよりも小さくするのが最善の方法です。Web UIのConfiguration > Security > Advanced EAPでGroup Key Rotation間隔を「EAP-Broadcast Key Interval」として設定できます
- 不要な切断と再認証を回避するために、セッションタイムアウトを86400秒にします。

AP Join プロファイル

- TCP adjust MSSがイネーブルになっていることを確認します。
- Trust DSCP upstreamをイネーブルにします。残念ながら、多くのワイヤレスクライアント

は802.11e WMM UPタギングを行っていません。DSCPフィールドを信頼することは、音声アプリケーションに適切な優先順位を提供する確実な方法です。
- アクセスポイントのSyslogを有効にします。SyslogサーバIPを設定すると、APはコンソールログをユニキャストでIPに送信します。これはAPのトラブルシューティングに役立つだけでなく、APがローカルVLANでSyslogをブロードキャストするデフォルト設定よりもネットワークに適しています。APのSyslogがモニタされていない場合でも、APのロギングによって大量のメッセージ負荷が発生する可能性があります。メッセージのブロードキャストを防止するには、適切なメッセージ重大度を設定するか、ダミーのSyslog IPアドレス（0.0.0.0など）を設定するか、あるいはその両方を行って、イベントの数を制限することをお勧めします。
- CAPWAPの再試行とタイムアウトを最大化します。問題の検出速度は遅くなりますが、ネットワークは軽度の一時的なパケットのドロップに対してより耐性があります。
- SSHを有効にし、クレデンシャルを設定します。APコンソールを無効にします。
- 必要に応じてAPモニタを有効にしますが、無線モニタは有効にしません。
- 不正検出を有効にし、RSSIしきい値を–70 dBmに設定します。

ネットワークのモニタリング

ネットワークが起動して稼働したら、問題がないかネットワークを詳細に監視する必要があります。標準的なオフィス環境では、ユーザはネットワークを把握しており、問題が発生した場合はお互いに助け合うか、内部のヘルプデスクチケットを開くことができます。多くの訪問者が訪れる大規模な場所では、設定ミスが発生する可能性のある特定の個人ではなく、最大の問題に焦点を当てるため、適切な監視戦略が必要です。

Catalyst 9800のCLIまたはGUIからネットワークを監視することは可能ですが、日常的に監視する最適なツールではありません。問題に関する疑いやデータがあり、特定のコマンドをリアルタイムで実行したい場合に最も直接的です。主なモニタリングオプションは、Cisco Catalyst Center、またはカスタムのテレメトリダッシュボードです。サードパーティ製の監視ツールを使用することは可能ですが、プロトコルとしてSNMPを使用する場合、データはリアルタイムにはほど遠く、通常のサードパーティ製監視ツールでは、すべてのワイヤレスベンダー仕様に対して十分にきめ細かくなりません。SNMPプロトコルを選択する場合は、SNMPv2のセキュリティが古いため、必ずSNMPv3を使用してください。

Cisco Catalyst Centerは、ネットワークの監視に加えてネットワークの管理も可能にする最適なオプションです。モニタリングだけでなく、ライブでのトラブルシューティングや多くの状況の修復も可能です。

カスタム遠隔測定ダッシュボードは、NOCまたはSOCに対して常にオンの状態で非常に具体的な測定指標やウィジェットを画面に表示する場合に便利です。ネットワークの特定の領域を監視したい場合は、専用のウィジェットを構築して、その領域のネットワークメトリックを任意の方法で表示できます。

イベントネットワークでは、システム全体のRF統計情報、特にチャネル使用率とAPごとのクライアント数を監視することをお勧めします。これはCLIから実行できますが、特定の時点でのスナップショットのみが提供され、チャネル使用率は動的である傾向があり、時間の経過に伴う監視に適しています。このタイプのモニタリングでは、通常、カスタムダッシュボードが適切なアプローチです。時間の経過とともに監視する場合に役立つその他のメトリックには、WNCDの使用

率、クライアントの数とその状態、および施設固有のメトリックなどがあります。施設固有のメトリックの例としては、特定のエリアまたは場所(会議センターの場合はホールX、イベント会場の場合は座席エリアYなど)の使用状況や負荷のモニタリングがあります。

カスタムモニタリングでは、NETCONF RPC（プル）とNETCONFストリーミングテレメトリ（プッシュ）の両方が有効なアプローチですが、カスタムストリーミングテレメトリをCatalyst Centerと組み合わせて使用する場合は、WLCで設定できるテレメトリサブスクリプションの数に制限があり、Catalyst Centerではこれらの多くを事前に入力（および使用）するため、ある程度の注意が必要です。

NETCONF RPCを使用する場合、WLCがNETCONF要求によって過負荷になっていないことを確認するためにテストが必要になります。特に、一部のデータポイントの更新率と、データが返されるまでにかかる時間に注意してください。たとえば、APチャネルの使用率は60秒ごとに更新され（APからWLCへ）、1000台のAP（WLCから）のRFメトリックの収集には数秒かかります。この例では、WLCを5秒ごとにポーリングするのは有効ではなく、システム全体のRFメトリックを3分ごとに収集するほうが適切な方法です。

NETCONFは常にSNMPよりも優先されます。

DHCPプールの使用率やコアルータ上のNATエントリの数など、コアネットワークコンポーネントの監視は遅延なく行われます。これらの障害が原因でワイヤレスが停止することは容易です。

大規模ネットワークに固有の問題

Web認証を使用するSSIDがある場合、1つの問題として、そのSSIDに接続し、IPアドレスを取得するが認証を行わないクライアントが考えられます。これは、エンドユーザが（デバイスが自動的に接続する）接続をアクティブに試行していないためです。コントローラは、「Web authentication pending」という状態のクライアントから送信されるHTTPパケットをすべて代行受信する必要があり、代行受信にはWLCリソースが使用されます。ネットワークが稼働し始めたら、特定の時点でWeb認証保留状態になっているクライアントの数を定期的に監視して、ベースライン数との比較を確認します。IP Learn状態のクライアントでも同じです。DHCPプロセスを実行しているクライアントは常にその状態にありますが、ネットワークの正しい動作番号を知っておくと、ベースラインを設定したり、この番号が高すぎる可能性のある瞬間を特定したり、より大きな問題を示したりする際に役立ちます。

大規模な会場では、クライアントの10 %以下がWeb Auth Pending状態になっていることはめずらしくありません。

2日目のモニタリング：ユーザの満足度を監視

ネットワークが稼動し始めると、エンドユーザから次の2種類の苦情が寄せられます。接続できない、接続が困難（切断）、またはWi-Fiの動作が予想より遅い。後者は、速度の期待値と特定の領域のリアルタイム密度に最初に依存するため、識別が非常に難しくなります。大規模な公共施設のネットワークを日常的に監視する際に役立つ、いくつかのリソースについて説明します。

Wi-Fiスループットの検証：テストおよびモニタリングガイド。このcisco.comドキュメントでは、ネットワークを監視してスループットの問題を特定する方法について説明します。このテストでは、静かな状態でクライアントがネットワーク内で適切に予測できるスループットを算出し、

クライアントの数と負荷が増加するにつれて予測されるスループットの値を推定します。これは、エンドユーザがスループットに関して述べている苦情が技術的な観点から正当なものであるかどうかを評価し、潜在的に直面している負荷に対応して、そのエリアを再設計する必要があるかどうかを評価するための鍵です。

クライアントが接続の問題を報告する際には、その問題をCatalyst Centerで切り分けて明確にした後、「Catalyst 9800クライアントの接続の問題のトラブルシューティングのフロー」を参照してください。

最後に、一般的なベストプラクティスとして、Catalyst 9800のKPI（重要業績評価指標）のモニタを使用して、WLCの全体的な主要指標を常に監視します。

スケーラビリティのための設定

9800のSVIおよびインターフェイス

WLCでクライアントVLAN用のSVIを作成することは避けてください。古いAireOS WLCに慣れた管理者は、各クライアントVLANにレイヤ3インターフェイスを作成する傾向がありますが、これが必要になることはほとんどありません。インターフェイスはコントロールプレーンの攻撃ベクトルを増大させるため、より複雑なエントリを含む多くのACLが必要になる可能性があります。デフォルトでは、WLCはどのインターフェイスでもアクセスできますが、WLCを保護するために必要な作業は、インターフェイスの数を増やすだけです。また、ルーティングが複雑になるため、これを回避するのが最善です。

IOS XE 17.9以降、mDNSスヌーピングまたはDHCPリレーのシナリオでSVIインターフェイスは不要になりました。したがって、クライアントVLANでSVIインターフェイスを設定する理由はごくわずかです。

集約プローブ応答

大規模なパブリックネットワークでは、アクセスポイントから送信されるデフォルトの集約プローブ間隔を変更することをお勧めします。デフォルトでは、APはクライアントから送信されたプローブに関して500ミリ秒ごとにWLCを更新します。この情報は、ロードバランシング、帯域選択、ロケーション、および802.11k機能で使用されます。クライアントとアクセスポイントの数が多い場合は、更新間隔を変更して、WLCでのコントロールプレーンのパフォーマンスの問題を防ぐことをお勧めします。推奨される設定は、64秒ごとに50の集約プローブ応答です。また、APがローカルで管理されるMACアドレスからのプローブを報告していないことを確認します。これは、ポイントトラッキングがないためです。これは、1つのクライアントが意図的にトラッキングを回避するためにスキャン中に多数のローカルで管理されるMACを使用している可能性を考慮している場合です。

```
wireless probe limit 50 64000

no wireless probe localy-administered-mac
```

IPv6

多くのネットワーク管理者は、依然としてIPv6を拒否しています。IPv6で受け入れられるオプションは2つだけです。1つはサポートし、すべての場所で適切な設定を導入する必要があります。もう1つはサポートせず、ブロックする必要があります。IPV6を気にせず、適切な設定なしに有効のままにしておくことは受け入れられません。これにより、ネットワークセキュリティが認識できないIPの世界が生まれます。

IPv6を有効にする場合、仮想IPv6アドレスを2001:DB8::/32の範囲で設定する必要があります（これは忘れられがちな手順です）。

IPv6の基本動作はマルチキャストに大きく依存していますが、WLCでマルチキャスト転送を無効にすると動作する可能性があることに注意してください。マルチキャストフォワーディングとは、クライアントマルチキャストデータのフォワーディングを指すもので、ネイバー探索、ルータ要請、およびIPv6を動作するために必要なその他のプロトコルを指すものではありません。

インターネット接続またはインターネットサービスプロバイダーがIPv6アドレスを提供している場合は、クライアントにIPv6を許可できます。これは、インフラストラクチャでIPv6を有効にする方法とは異なる方法です。APはIPv4でのみ動作し続けることができますが、CAPWAPパケット内では引き続きIPv6クライアントデータトラフィックを伝送します。インフラストラクチャでIPv6を有効にするには、AP、WLC、および管理サブネットへのクライアントアクセスの保護についても検討する必要があります。

クライアントゲートウェイのRA周波数を確認します。WLCは、クライアントに転送されるRAの数を制限するRAスロットリングポリシーを提供します。これは、クライアントが通信できなくなる場合があるためです。

mDNS

一般的に、大規模な施設展開ではmDNSを完全に無効にしておくのが最善です。

mDNSブリッジングとは、mDNSパケットをレイヤ2マルチキャストとして（したがってクライアントサブネット全体に）送信できるようにする概念を指します。mDNSは、サブネット内のサービスを検出するのが非常に現実的なホームオフィスやスモールオフィスのシナリオで広く使用されるようになりました。ただし、大規模なネットワークでは、これはサブネット内のすべてのクライアントにパケットを送信することを意味し、大規模なパブリックネットワークのトラフィックの観点からは問題になります。一方、ブリッジは通常のデータトラフィックと見なされるため、APまたはWLCのCPUにオーバーヘッドを発生させません。mDNSプロキシまたはmDNSゲートウェイは、ネットワーク内のすべてのサービスのディレクトリとしてWLCを使用する概念を指します。これにより、様は効率的な方法でレイヤ2の境界を越えてmDNSサービスを提供でき、トラフィック全体を削減できます。たとえばmDNSゲートウェイを使用する場合、プリンタは同じサブネットのレイヤ2マルチキャストを使用してmDNS経由で定期的なサービスアナウンスを送信しますが、WLCはその他すべてのワイヤレスクライアントにそれを転送しません。代わりに、提供されるサービスをメモし、サービスディレクトリに登録します。クライアントが利用可能な特定のタイプのサービスを要求すると、WLCがアナウンスをプリンタに代わって応答します。これにより、他のすべてのワイヤレスクライアントが不要な要求やサービス提供について聞くことを回避し、周囲にあるサービスについて尋ねるたびに応答を得るだけです。トラフィック効率を大幅

に改善する一方で、mDNSトラフィックのスヌーピングによりWLC（または、FlexConnectシナリオでAP mDNSを使用する場合はAP）でオーバーヘッドが発生します。mDNSゲートウェイを使用している場合は、CPU使用率を常に監視することが重要です。

ブリッジすると、大規模なサブネットでマルチキャストストームが発生し、スヌーピング（mDNSゲートウェイ機能を使用）するとCPU使用率が高くなります。グローバルおよび各WLANでディセーブルにします。

一部のサービスでは特定の場所でmDNSが必要になるため、一部の管理者はmDNSを有効にしますが、この機能によって不要なトラフィックがどの程度増加するかを理解することが重要です。Appleデバイスは、しばしば自分自身を広告するだけでなく、サービスを絶えず探し求め、誰も特定のサービスを使用していない場合でも、mDNSクエリのバックグラウンドノイズを引き起こします。特定のビジネス要件のためにmDNSを許可する必要がある場合は、グローバルに有効にしてから、必要なWLANでのみ有効にし、mDNSが許可される範囲を制限します。

ネットワークの強化

セキュリティ

大規模なパブリックネットワークでは、管理者が把握していなくても多くのことが起こる可能性があります。ランダムな場所でケーブルの引き込みを要求したり、シェナニガンのためにホームグレードのスイッチを引き込んでスイッチポートを増やしたりする人が多い。このような人は通常、最初に許可を求めずに試みている。つまり、たとえ悪い攻撃者が関与していなくても、善意の顧客や従業員によってセキュリティがすでに侵害されている可能性があります。悪い俳優がケーブルを探してケーブルを探し、そこから得られるネットワークアクセスを確認することは非常に簡単です。すべてのスイッチポートで802.1X認証を設定することは、大規模ネットワークで適切なセキュリティを維持するための要件に近い要件です。Catalyst Centerはこの展開の自動化を支援します。802.1X認証をサポートしていないが、実際のセキュリティとは異なり、MACベースの認証にできるだけ依存しないようにしている特定のデバイスは例外として扱うことができます。

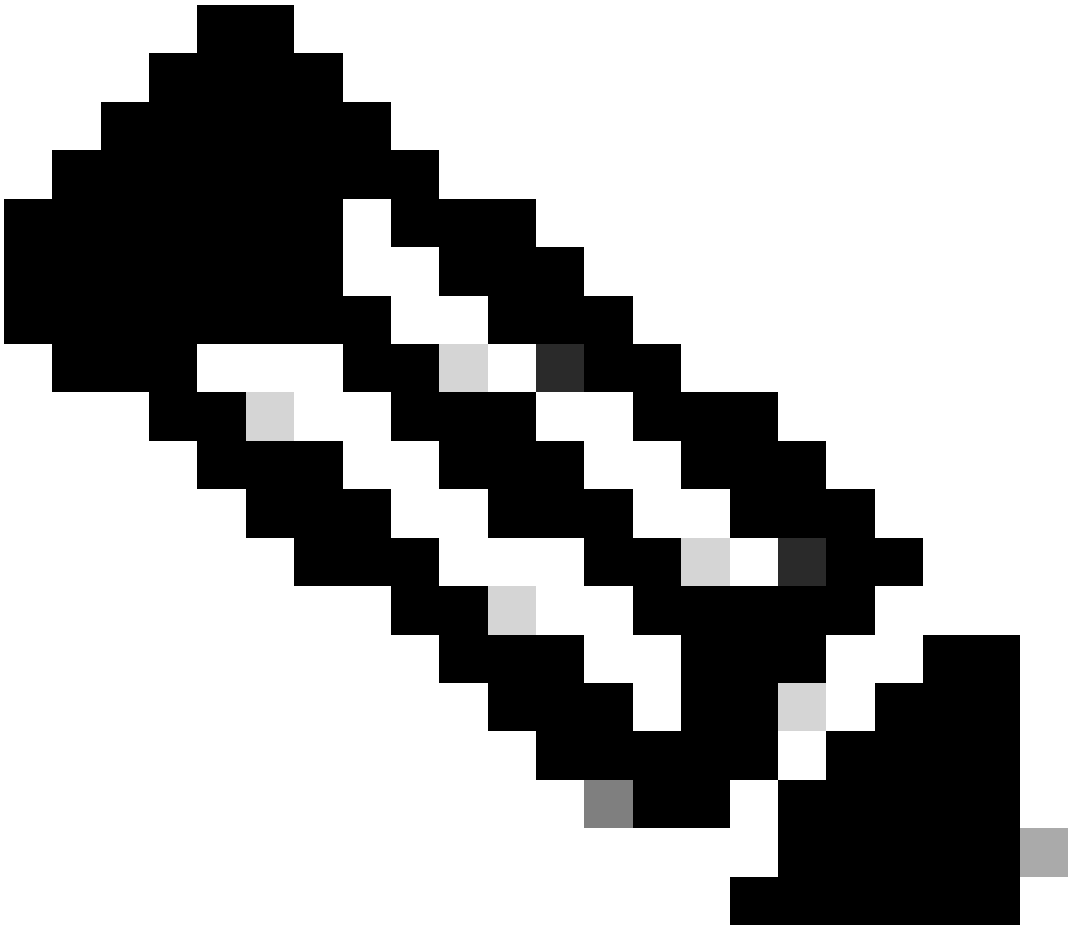
偽のアクセスポイント

不正と戦うあなたの戦略はいくつかの要因に依存します。多くの管理者は直感的に非常に厳しい規則を求めていますが、主な質問は次のとおりです。

- 数百（数千ではない）もの不正アラートを受け取った場合、すべての不正アラートを確認し、それらすべてに対してアクションを実行する人材が確保されていますか。
- 目標は、不正を物理的に除去してクリーンなRFスペクトルを維持することですか。その場合、この操作を実行するには多くの人が必要です。あるいは、あなたの目標は、セキュリティ要因に目を離さないようにし、不正が危険を表していないことを確認することだけでしょうか。これは、人間の作業コストを大幅に抑えることができます。
- 不正検出を有効にすると通信時間に影響を与え、不正抑止の影響は通常、さらに大きくなっています。この影響を分析して考慮しましたか。

不正検出の影響に関しては、9120および9130には専用のCleanAirチップが搭載されており、オフチャネルスキャン（したがって不正検出）を実行して、クライアントサービス無線への影響をほ

ぼヌル状態にします。CleanAir Proチップを搭載した9160シリーズAPにも同様の影響なしスキャン機能がありますが、CleanAirチップを搭載していない他のAPでは、不正のスキャンや抑止のためにクライアントサービス無線をオフチャネルにする必要があります。したがって、使用しているAPモデルは、不正の検出と抑止に専用モニタモードAPを使用するかどうかを決定する際の役割を果たします。

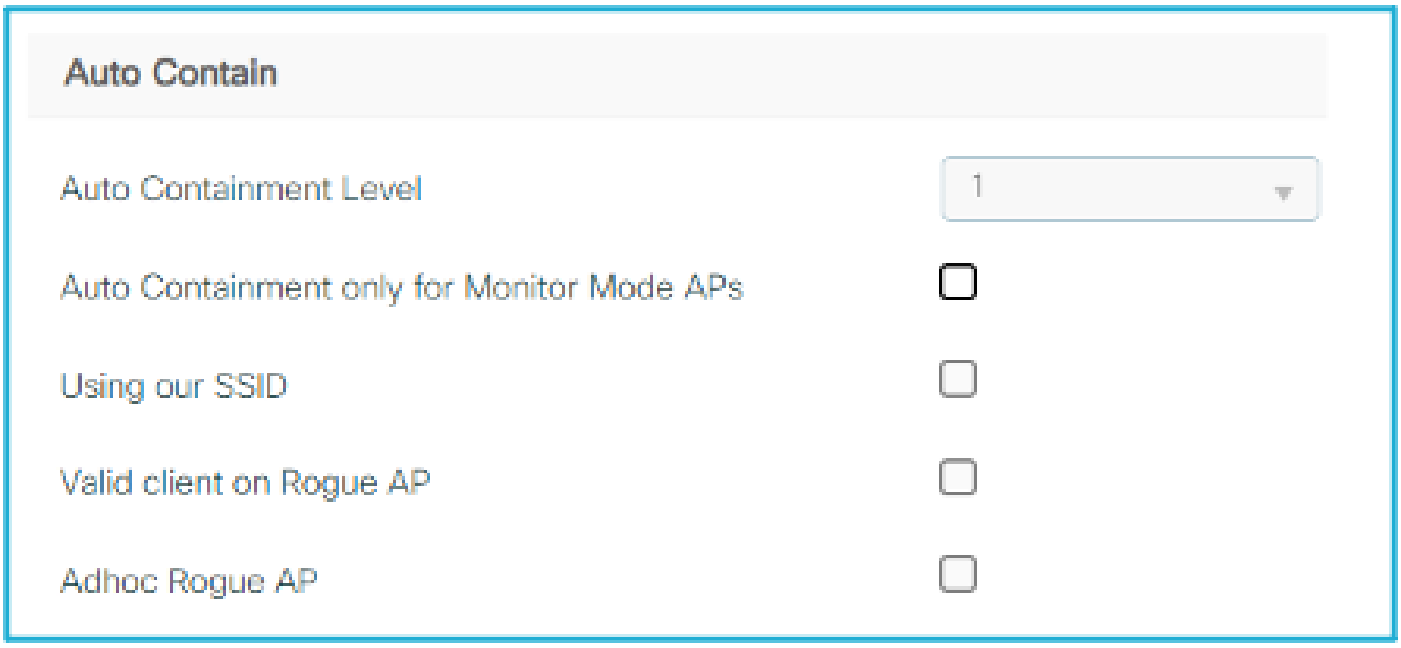


注:Wi-Fiホットスポットを共有する携帯電話は、従来のAPと同様に「インフラストラクチャ」モードで動作します。「アドホック」モードは、モバイルデバイス間の直接接続を指し、あまり一般的ではありません。

不正の抑止は規制ルールによって禁止されていることが多いため、有効にする前に地域の機関に確認することが重要です。不正を抑止することは、リモートから不正をシャットダウンすることではなく、不正なアクセスポイントに接続しようとするクライアントに対して認証解除フレームを使用して接続を試行しないようにスパミングを行うことを意味します。この方法は、アクセスポイントが認証解除フレームに正しく署名できないため、従来のセキュリティSSID（WPA3またはWPA2でPMFが有効になっている場合には機能しない）でのみ機能します。APが認証解除フレームで通信時間を満たしているため、抑止はターゲットチャネルのRFパフォーマンスに悪影響を

及ぼします。したがって、これをセキュリティ対策と見なして、正当なクライアントが誤って不正なアクセスポイントにアソシエートするのを防ぐ必要があります。前述のすべての理由から、抑止は不正の問題を完全に解決せず、さらにRFの問題を引き起こすため、抑止は行わないことをお勧めします。抑止を使用する必要がある場合は、管理SSIDの1つをスプーフィングする不正に対して抑止を有効にするだけで十分です。これは、明白なハニーポット攻撃であるためです。

次のように、「SSIDを使用」オプションで自動抑止を設定できます。



自動封じ込め設定

また、独自の基準に従って悪意のある不正アクセスポイントとして分類するように不正ルールを設定することもできます。アラームリストから削除する場合は、隣接するSSIDと承認されたSSIDの名前を友好的な不正として入力することを忘れないでください。

AP認証またはPMFを有効にして、なりすましからAPを保護します。

有線の不正は、有線ネットワークに接続されている不正なアクセスポイントであり、明らかにセキュリティ上の脅威です。有線の不正の検出は、不正のイーサネットMACアドレスが無線MACアドレスと異なることが一般的なため、より複雑です。Cisco Catalyst Centerには、不正が有線かどうかを検出しようとするアルゴリズムと、有線インフラストラクチャ上で検出され、無線通信網上に存在する不正なクライアントMACを探すアルゴリズムがあります。有線の不正を完全に防止する最善のソリューションは、すべてのスイッチポートを802.1X認証で保護することです。

不正なアクセスポイントを物理的に使用する場合は、Cisco Spacesを活用して不正の正確な場所を特定することが重要です。不正なAPを隠す傾向があるため、サイト内で1回検索する必要があることがほとんどですが、検索領域を数メートルに減らすことは、非常に実行可能な取り組みです。スペースを使用しない場合、不正はAPの横のマップ上に表示され、APを検出する際に最も大きくなるので、かなり大きな検索エリアになります。不正なアクセスポイントの信号をリアルタイムで表示し、不正の物理的な位置を特定できる多くのワイヤレスツールやワイヤレスデバイスが存在します。

不正とは正確には関連しませんが、CleanAirについては説明したばかりであるため、CleanAirを

有効にしても、2.4GHzのパフォーマンスに影響を与えるBLEビーコン検出以外は、パフォーマンスに著しい悪影響を及ぼさないことに注意してください。Bluetooth干渉源は今日の世界ではいたるところに存在するため、ワイヤレスを設定してBluetooth干渉源を完全に無視することができます。また、クライアントがBluetoothを有効にすることを妨げることはできません。

WiPS

WiPSは、許可されていない不正デバイスの存在を検出するだけでなく、より高度な攻撃ベクトルをカバーします。これらの攻撃に加えて、フォレンジック分析のためのイベントのPCAPが提供されることもあります。

これは企業にとって非常に便利なセキュリティ機能ですが、パブリック側のネットワークは、そのネットワークに対して何をすべきかという永遠の問いに直面する必要があります。

制御できない多数のクライアントを管理することは困難であるため、アラームを2つのカテゴリに分けることができます。次のアラームが多すぎる場合は、Cisco Catalyst Centerから無視できます。

- 10001: DoS：認証フラッドアラーム
- 10002:DoS：関連付け要求アラーム
- 10003:DoS：ブロードキャストプローブフラッドアラーム
- 10004:DoS：関連付け解除フラッドアラーム
- 10005:DoS：ブロードキャスト関連付け解除アラーム
- 10006:DoS：認証解除フラッドアラーム
- 10007:DOS：ブロードキャスト認証解除アラーム
- 10008:DOS:EAPOL-Logoff攻撃アラーム
- 10009:CTSフラッドアラーム
- 10010:RTS関連付け要求アラーム
- 10011:ペアによる認証解除フラッディング
- 10021:Airdropセッション（これは通常、あらゆるネットワークで頻繁に発生し、Appleデバイス間の定期的なピアツーピアアクティビティを示すものです）
- 10022：関連付け要求の形式が正しくありません
- 10023：シグニチャによる認証障害のフラッディング
- 10024：シグニチャによる無効なMAC OUI
- 10025：認証の形式が正しくありません

これらのアラームは、クライアントの誤動作によって発生する可能性があります。基本的に、障害のあるクライアントによってエアタイムがビジー状態にされることを防ぐことはできないため、サービス拒否攻撃を自動的に防ぐことはできません。インフラストラクチャがクライアントを無視しても、メディアと通信時間を使用して送信できるため、その結果、そのインフラストラクチャ周辺のクライアントのパフォーマンスに影響が及びます。

その他のアラームは非常に詳細であるため、実際の悪意のある攻撃を示している可能性が高く、クライアントドライバの不良によりほとんど発生しません。次のアラームを継続的に監視することをお勧めします。

- 10012:Fuzzzed Beacon（ぼかしビーコン）

- 10013：ファズドされたプローブ要求
- 10014：ファズド・プローブ応答
- 10015：シグニチャによるPSポーリングフラッド
- 10016：シグニチャによるEAPOL Start V1フラッディング
- 10017：宛先による再関連付け要求フラッディング
- 10018：シグニチャによるビーコンフラッド
- 10019：宛先によるプローブ応答フラッディング
- 10020：シグニチャによるブロックAckフラッディング
- 10026/10027:RTSおよびCTS仮想キャリア検知攻撃

ワイヤレスインフラストラクチャは、問題のデバイスのブロックリストなどの緩和措置を実行できる場合がありますが、そのような攻撃を排除するための唯一の実際の措置は、物理的にそこに移動して、問題のデバイスを削除することです。

障害のあるクライアントとやり取りすることで無駄になる通信時間を節約するために、あらゆる形式のクライアント除外を有効にすることを推奨します。

クライアントアクセスの制限

すべてのWLANでピアツーピアブロッキングを有効にすることを推奨します（クライアント間通信に関する厳格な要件がある場合を除きます。ただし、この方法は慎重に検討する必要があり、場合によっては制限が必要です）。この機能は、同じWLAN上のクライアントが相互に通信することを防止します。異なるWLAN上のクライアントは引き続き相互に接続でき、モビリティグループ内の異なるWLCに属するクライアントもこの制限を回避できるため、これは完全なソリューションではありません。しかし、セキュリティと最適化の簡単で効率的な第1レイヤとして機能します。ピアツーピアブロッキングのこの機能のもう1つの利点は、アプリケーションがローカルネットワーク上の他のデバイスを検出するのを防ぐクライアントツークライアントARPを防ぐことです。ピアツーピアブロッキングを行わないと、クライアントに単純なアプリケーションをインストールしたときに、サブネットに接続している他のすべてのクライアントがIPアドレスとホスト名を使用して表示される可能性があります。

さらに、クライアント間通信を防ぐために、IPv4とIPv6（ネットワークでIPv6を使用している場合）の両方のACLをWLANに適用することを推奨します。クライアントからクライアントへの通信をWLANレベルでブロックするACLを適用すると、クライアントSVIがあるかどうかにかかわらず動作します。

もう1つの必須ステップは、ワイヤレスコントローラの任意の形式の管理へのワイヤレスクライアントアクセスを防止することです。

以下に例を挙げます。

```
ip access-list extended ACL_DENY_CLIENT_VLANS

 10 deny ip any 10.131.0.0 0.0.255.255

 20 deny ip 10.131.0.0 0.0.255.255 any

 30 deny ip any 10.132.0.0 0.0.255.255
```

```
 40 deny ip 10.132.0.0 0.0.255.255 any
 50 deny ip any 10.133.0.0 0.0.255.255
 60 deny ip 10.133.0.0 0.0.255.255 any
 70 deny ip any 10.134.0.0 0.0.255.255
 80 deny ip 10.134.0.0 0.0.255.255 any
 90 deny ip any 10.135.0.0 0.0.255.255
 100 deny ip 10.135.0.0 0.0.255.255 any
 110 deny ip any 10.136.0.0 0.0.255.255
 120 deny ip 10.136.0.0 0.0.255.255 any
 130 deny ip any 10.137.0.0 0.0.255.255
 140 deny ip 10.137.0.0 0.0.255.255 any
 150 permit ip any any
```

次のACLは、管理インターフェイスSVIに適用できます。

```
interface Vlan130
 ip access-group ACL_DENY_CLIENT_VLANS in
```

これは、レイヤ2 VLANデータベースにクライアントVLAN 131 ~ 137が作成されたWLC上で実行されますが、対応するSVIは存在せず、VLAN 130に対して存在するSVIは1つだけであるため、WLCはSVIを使用して管理されます。このACLにより、すべてのワイヤレスクライアントがWLC管理プレーンとコントロールプレーンにトラフィックを完全に送信できなくなります。すべてのAPへのCAPWAP接続も許可する必要があるため、SSHまたはWeb UI管理だけが許可する必要があることを忘れないでください。このACLにデフォルトの許可が設定されているものの、許可されたすべてのAPサブネット範囲と管理範囲の指定を必要とするデフォルトの「すべて拒否」アクションに依存するのではなく、ワイヤレスクライアント範囲をブロックするのはそのためです。

同様に、可能なすべての管理サブネットを指定する別のACLを作成できます。

```
ip access-list standard ACL_MGMT
 10 permit 10.128.0.0 0.0.255.255
 20 permit 10.127.0.0 0.0.255.255
 30 permit 10.100.0.0 0.0.255.255
```

```
 40 permit 10.121.0.0 0.0.255.255

 50 permit 10.141.0.0 0.0.255.255
```

次に、このACLをCLIアクセスに適用できます。

```
line vty 0 50

 access-class ACL_MGMT in

 exec-timeout 180 0

 ipv6 access-class ACL_IPV6_MGMT in

 logging synchronous

 length 0

 transport preferred none

 transport input ssh

 transport output ssh
```

同じACLをWeb管理アクセスにも適用できます。

トラフィックストームからの保護

マルチキャストとブロードキャストは、一部のアプリケーションによって他のアプリケーションよりも多く使用されます。有線のみのネットワークを検討する場合、ブロードキャストストームから保護することが唯一の予防策となることがよくあります。ただし、マルチキャストはブロードキャストと同様に負荷がかかるため、その理由を理解することが重要です。まず、すべてのワイヤレスクライアントに（ブロードキャストまたはマルチキャストを介して）送信されるパケットを想像してみてください。このパケットはすぐに多くの宛先に追加されます。各APは、可能な限り最も信頼性の高い方法（信頼性は保証されていません）でこのフレームを無線で送信する必要があります。この方法は、必須データレート（場合によっては最低データレート、場合によっては設定可能データレート）を使用して実行します。一般に、これはフレームがOFDM(802.11a/g)データレートを使用して送信されることを意味しますが、これは明らかに優れたデータレートではありません。

大規模なパブリックネットワークでは、通信時間を維持するためにマルチキャストに依存することはお勧めしません。ただし、大規模な企業ネットワークでは、特定のアプリケーションに対してマルチキャストを有効にしておく必要がありますが、その影響を抑えるためには可能な限りマルチキャストを制御する必要があります。アプリケーションの詳細、マルチキャストIPを文書化し、他の形式のマルチキャストを必ずブロックすることをお勧めします。マルチキャスト転送の有効化は、前述のようにIPv6を有効化するための要件ではありません。ブロードキャスト転送は、完全に無効のままにしておくことをお勧めします。ブロードキャストは、同じサブネット上の

他のデバイスを検出するためにアプリケーションによって使用されることがありますが、これは明らかに、大規模ネットワークのセキュリティ上の問題です。

グローバルマルチキャストフォワーディングを有効にする場合は、multicast-multicast AP CAPWAP設定を使用してください。これをイネーブルにすると、WLCは有線インフラストラクチャからマルチキャストパケットを受信すると、単一のマルチキャストパケットを使用して対象のすべてのAPにパケットを送信するため、パケットの重複が大幅に減少します。WLCごとに異なるCAPWAPマルチキャストIPを設定してください。設定しない場合、APは望ましくないマルチキャストトラフィックを他のWLCから受信します。

APがWLCのワイヤレス管理インターフェイス(WMM)の他のサブネットにある場合（大規模ネットワークの場合が多い）、有線インフラストラクチャでマルチキャストルーティングを有効にする必要があります。すべてのAPがマルチキャストトラフィックを正しく受信していることを確認するには、次のコマンドを使用します。

```
show ap multicast mom
```

マルチキャストに依存する必要がある場合は、すべてのケースでIGMP（IPv4マルチキャスト用）およびMLD（IPv6用）マルチキャストを有効にすることをお勧めします。対象のワイヤレスクライアント（対象のクライアントを持つAPのみ）のみがマルチキャストトラフィックを受信できるようにします。WLCは登録をマルチキャストトラフィックにプロキシし、登録を維持してクライアントをオフロードします。

結論

大規模なパブリックネットワークは複雑で、それぞれが固有の要件と成果を持っています。

このドキュメントのガイドラインを遵守することは出発点として最適であり、最も一般的な問題を回避しながら導入を成功に導きます。ただし、ガイドラインは単なるガイドラインであり、特定の場所のコンテキスト内で解釈または調整する必要があります。

Cisco CXには、大規模なワイヤレスの導入に特化したワイヤレス専門家チームがあり、スポーツイベントや会議など、多数の大規模イベントでの経験があります。詳細については、担当のアカウントチームにお問い合わせください。

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。