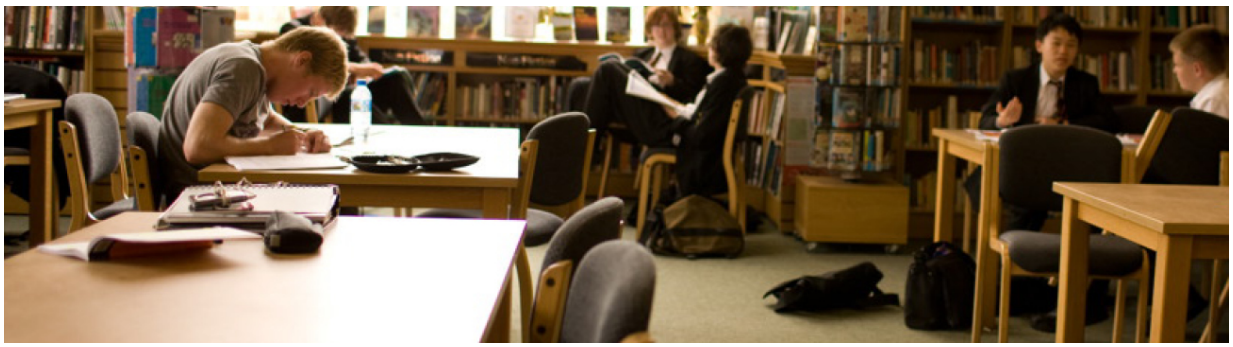
ホワイト ペーパー

Cisco Wireless LAN での iOS デバイス使用に関する企業向けベスト プラクティス



改訂: 2016 年 11 月

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

目次

対象範囲 4
背景....4
ワイヤレス LAN に関する考慮事項....5
Cisco WLAN での iOS デバイス使用に関する RF 設計ガイドライン 5
Cisco WLAN での iOS デバイス使用に関する RF 設計の推奨事項....6
Wi-Fi チャネル カバレッジ....7
ClientLink ビームフォーミング 9
Wi-Fi チャネル帯域幅....10
データ レート 12
QOS....14
ワイヤレス QoS 14
Wi-Fi マルチメディア....18
WLAN の QoS プロファイル 19
Fast lane の設定 21
最適化された EDCA（Enhanced Distribution Channel Access）....25
有線スイッチ ポートの設定....26
アプリケーションの可視化と制御 27
Cisco Jabber を使用する iOS デバイスの AVC 設定例....27
IOS デバイスのローミング拡張 30
802.11r – Fast Transition 31

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Adaptive 802.11r 34

802.11k - 無線測定とネイバー レポート 35

802.11v – Basic Service Set（BSS）移行管理 37

CISCO WLAN での IOS デバイスによる WI-FI コーリング 39

CISCO WLAN での BONJOUR.....40

ワイヤレス環境の把握.....41

接続したデバイスの監視.....43

チャネルの使用率 44

ピアツーピア アクティビティの監視.....46

CISCO WLAN での IOS デバイス使用に関するベスト プラクティスのまとめ.....47

追加情報 49

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

対象範囲

この文書は、Cisco Wireless LAN（WLAN）の設計、導入、管理を担当する IT 技術者を対象としています。このリファレンス設計ガイドは、コントローラ ベースの Cisco Wireless LAN の中央管理型設定を中心に、シスコと Apple が共同で推奨する事項を反映して更新されています。本文書は、読者が Cisco WLAN のコンポーネントと機能、基本的な IP ネットワーキング、Voice over IP（VoIP）に関する実務的知識をすでに備えていることを前提としています。ベスト プラクティスには、Cisco Wireless LAN で iOS デバイスを使用する場合に、インフラストラクチャのセキュリティを維持しながら可能なかぎり最良のサービスを提供するための、設計上の考慮事項、推奨されるネットワーク設定、設定ガイドラインが含まれます。

特に、さまざまな使用例向けの一般的なベスト プラクティスおよびコントローラの設定と、iOS 9 以降を実行する iOS デバイス特有のガイダンスを重点的に取り扱います。セクションによっては、iOS デバイスで実行する OS のバージョンとして iOS 10 が必要な場合があります。そのようなセクションでは、対応するソフトウェア コード バージョンとして Cisco AireOS 8.3（以降）および iOS 10（以降）が推奨されることを明確に示しています。

確立されている企業向けベスト プラクティスおよびシスコと Apple 両社の共同推奨事項では、ビジネス/ミッション クリティカルな企業アプリケーション向けニーズに 2.4 GHz 帯を使用することを最適とはみなしていません。シスコと Apple は、iOS デバイス用には 5 GHz（802.11a/n/ac）のワイヤレス ネットワークのみを使用することを強く推奨します。この文書では、すべての iOS デバイス向けのベスト プラクティスとして 5 GHz のネットワーク レイアウトに焦点を当てています。

背景

BYOD の傾向が広まった今の時代にあっては、エンドユーザが Wi-Fi ネットワークに接続できる個人デバイスを携帯することが積極的に奨励され、現在、大半の職場において、ユーザ 1 人あたりのワイヤレス対応デバイスの数は、少なくとも 2 ～ 3 台になっています。IT 管理者は、ネットワーク リソースのセキュリティを低下させることなく、適切なバランスでオープン アクセス ネットワーク環境に対応できるよう Wi-Fi インフラストラクチャを設計および構築することが求められています。

これらの環境は、セキュリティの懸念だけでなく、QoS、2.4 GHz と 5 GHz の無線カバレッジの比較、クライアントの AP ローミングのシナリオ、ワイヤレス ネットワーク上に存在するレガシーのクライアント デバイスなどに関する数多くの課題を抱えています。ビジネス クリティカルなアプリケーションが従業員の個人デバイスで使用されることが増えたのに伴い、アプリケーション パフォーマンスの向上と並行して広範なワイヤレス接続へのニーズが高まっています。

iOS ベースのスマートフォンとタブレットは、現在の企業環境において重要な存在となっています。可能なかぎり最良のサービスを iOS デバイスに提供するには、RF 状況、クライアントの接続性、ネットワークの可視性、QoS、ネットワーク監視など、数多くのさまざまな要素を考慮する必要があります。この文書には、これらの要素を考慮しながらシスコ ワイヤレス LAN コントローラ（WLC）を設定するための重要なガイドラインが含まれています。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

ワイヤレス LAN に関する考慮事項

実稼働環境において Wi-Fi のようなshared メディアに Voice over WLAN（VoWLAN）などのリアルタイム アプリケーションを導入するには、慎重な計画、検討、設計が必要です。多くの管理者が、元々まったく異なるニーズに合わせて設計された既存のワイヤレス インフラストラクチャに VoWLAN を追加することを要求されています。その一方、設計をゼロから始め、最初から VoWLAN を考慮に入れることのできる管理者もいます。どちらの場合でも、管理者は、自分の組織のシスコ ワイヤレス環境で最適なエンドユーザ エクスペリエンスを確保するにはどうしたらよいのかという重要な問題に直面します。

Apple は、Wi-Fi クライアントとしての接続を強化する業界標準テクノロジーのサポートを継続的に追加しています。ただし、特定の iOS デバイスおよびオペレーティング システム リリースでしかサポートされないものも含まれます。ネットワークの能力を最大限に活用できるような調整を行うには、組織のワイヤレス ネットワークでどんな iOS デバイス（および iOS リリース）の使用が想定されているかを把握することが重要です。このプロセスを支援するため、Apple は、『Apple Roaming on iOS（Apple の iOS でのローミング）』[英語] の中で、一連の技術情報記事を掲載し、さまざまなテクノロジーがどのデバイスでサポートされているか説明しています。

802.11r や 802.11k などのエンタープライズ機能の多くは iOS 6 アップデートから採用されていますが、Apple は、すべてのデバイスを最新の iOS（10 以降）にアップグレードすることを推奨しています。

注： 802.11 と iOS デバイス向けエンタープライズ機能の詳細については、デバイス分類チャートを参照してください。
http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/device_classification_guide.pdf [英語]

Cisco WLAN での iOS デバイス使用に関する RF 設計ガイドライン

ワイヤレス LAN（WLAN）導入の第一歩は、目的とする運用を確実に行うことができるように、特定の環境における無線周波数（RF）の挙動を評価するサイト サーベイを実行することです。不十分な計画とそれに起因するカバレッジ不足が原因となってワイヤレス ネットワークにさまざまな問題が発生する可能性もあります。既存のワイヤレス環境を分析すると、サイト サーベイが正しく行われていない、あるいはまったく行われていないケースが多いことがわかります。

成功を継続するための重要な要因の 1 つは、使用中のワイヤレス デバイスとアプリケーションの現在および将来のニーズを考慮したサイト サーベイを確実に行うことです。それには、使用例を含めるとともに、近い将来、ワイヤレス ネットワークに導入して使用することを計画しているさまざまなデバイス タイプを反映させる必要があります。使用例が異なれば、サイト サーベイの手法も違ってきます。たとえば、一般使用（データまたは音声）のみのサイト サーベイは、音声、ビデオ、データ、ロケーション ベースのサービスを必要とするミッション クリティカルなネットワークとは大きく異なることがあります。

ラップトップやスマートフォンなどのさまざまなデバイスのワイヤレス特性はそれぞれ異なっているので、ワイヤレス ネットワークの設計とサイト サーベイではそれを考慮に入れる必要があります。それはまた、ワイヤレス クライアント デバイスの送信電力特性を理解して、アクセス ポイントと接続デバイスからの送信に同等の RF 電力レベルを確保する上でも役立ちます。大半の iOS デバイスの一般的な最大送信電力は、モデルや AP チャネルによって異なりますが、9 ～ 14 dBm の範囲にあることがわかっています。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Cisco WLAN での iOS デバイス使用に関する RF 設計の推奨事項

- すべての iOS デバイスに関し、802.11a/n/ac 5 GHz ベースの設計を使用します
- iOS デバイス向けの最適セル エッジ推奨値は -67 dBm 以上です（一般的な高密度企業向け導入の場合は -65 dBm が望ましい）WLAN 環境を最適化するには、セル エッジにおいて、Apple クライアントの計測により -67 dBm で 5 GHz の AP が最低 2 つ必要です
- 平均チャネル使用率は 40 %未満とします
- 25 dB 以上の信号対雑音比（SNR）を維持します
- 802.11 再送信は 15 % 未満に維持します
- パケット損失は 1 %未満に維持し、ジッターは 100 ms 未満に維持します

これらは一般的な推奨事項であり、送信電力が変動する可能性がある状況には十分対応できないことがあります（たとえば、バッテリ レベルがフル、または少ない状況で、アクティブな状態のデバイスが使用中に手で覆われるか、あるいは直接使用されていないパッシブな状態で保管されている（ポケットの中など）場合に減衰の可能性がある場合など）

表 1. RF 設計を成功させるための基本的ステップ

ステップ	説明	目的
1	定義	導入対象のアプリケーションとクライアント、および関係者を定義します。
2	カバレッジ エリアおよびプロジェクト フェーズ	キャンパス内で、一般的なアプリケーションのみをサポートするエリアと、一般的なアプリケーションに加えてワイヤレス ネットワークで音声をサポートするエリアを定義します。
3	計画承認	すべての主要関係者の承認を得ます。
4	RF 監査とサイト サーベイ	設計を検証して調整します。
5	インフラストラクチャの導入	設計を実装します。
6	RF テスト	導入したインフラストラクチャで実装をテストします。
7	最終調整	アクセス ポイント設定を調整します。
8	継続的な運用サポート	使用状況の変更に対応しながら継続的サポートへと移行します。

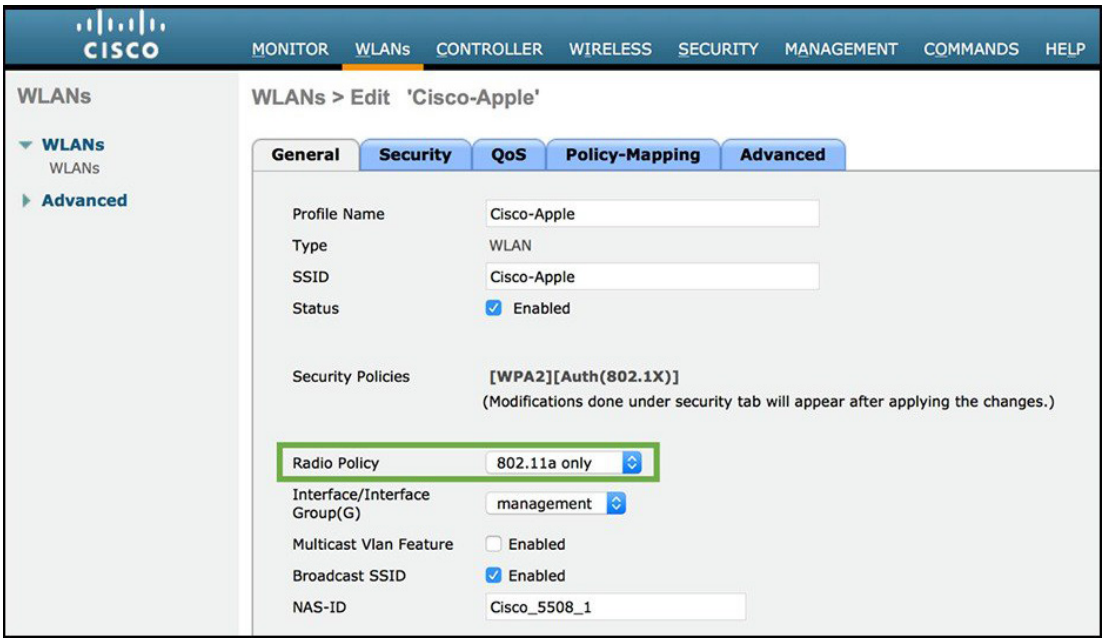
注： 詳細については、『Site Survey RF Design Validation Guide（サイト サーベイ RF 設計検証ガイド）』を参照してください。http://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html [英語]

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Wi-Fi チャネル カバレッジ

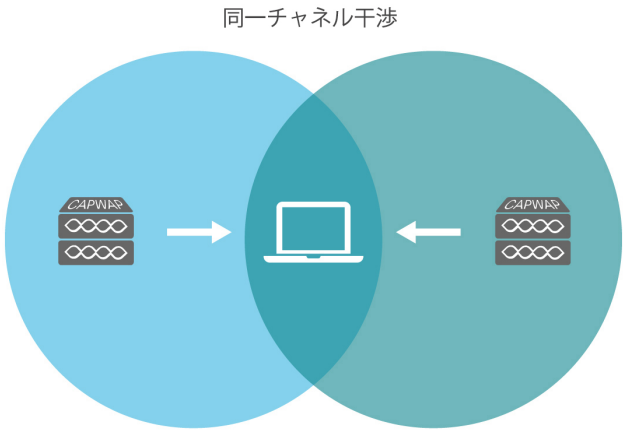
シスコと Apple は、シスコのワイヤレス ネットワーク上の iOS デバイス向けの設計をする際には5 GHz のみのカバレッジ設計を推奨しています。2.4 GHz 専用デバイスが存在する環境向けには、別のワイヤレス ネットワークを追加して、2.4 GHz のデバイスをネットワークに接続することもできます。

図 1. [無線ポリシー（Radio Policy）] を 5 GHz（[802.11a のみ（802.11a only）]）に設定する



5 GHz チャネルは、Bluetooth、ビデオ カメラ、電子レンジなど 2.4 GHz の周波数で動作する一般的なデバイスとは干渉しません。5 GHz ではより多くのチャネルを利用できるため、2.4 GHz と比較して、同一チャネル干渉が少なくチャネル オーバーラップ率が低いことにより、チャネルの使用率が一般的に低く、周波数再利用率が高くなります。

図 2. 同一チャネル上のアクセス ポイントによる同一チャネル干渉

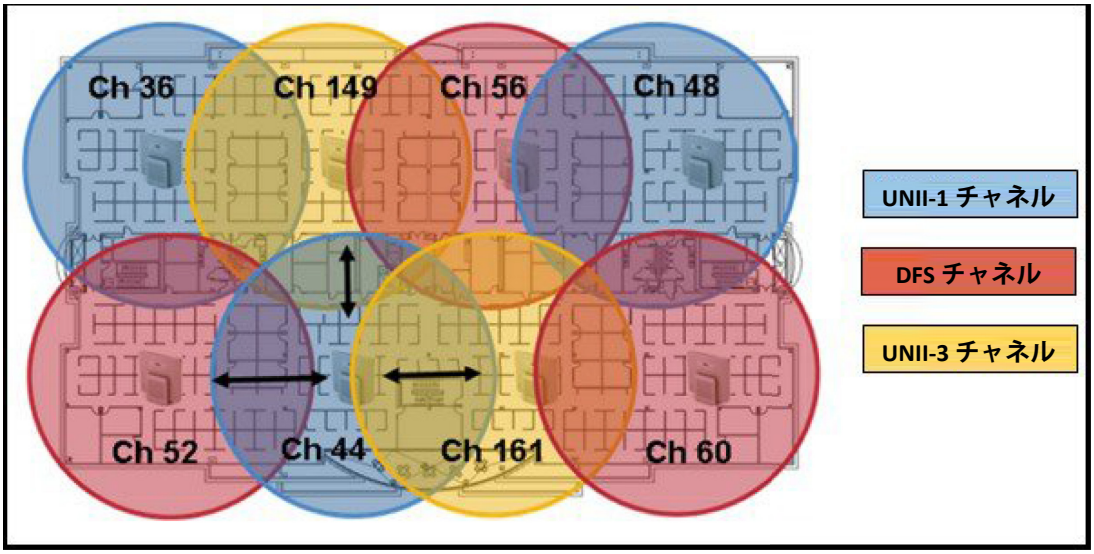


基本的な CCI：同じチャネル上の AP が相互に干渉

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

チャネル容量と同一チャネル干渉の状況から、動的周波数選択（DFS）チャネルの使用が必要になる場合があります。DFS は、Wi-Fi ネットワーク上の 5 GHz 無線との干渉を防ぐ必要のある軍事や気象といった分野で使用されている、レーダー信号検出プロセスです。信号が検出されると、AP は、5 GHz 無線の動作チャネルを切り換えて、レーダー システムに干渉しないチャネルに移動する必要があります。

図 3. 5 GHz ネットワーク設計におけるチャネル分配例



頻繁に DFS イベントが発生し、AP 間でチャネルが断続的に変更される事態を回避する計画を立てるため、シスコと Apple は、コントローラ トラップで DFS チャネルを注意深く監視してレーダー活動を確認することを推奨しています。

最適なアプリケーション パフォーマンスを考えた場合、一般にワイヤレス ネットワークは、平均使用率が 40 ～ 50 % に近づくとキャパシティ限界に達します。VoWLAN のように遅延の影響を受けやすいリアルタイム アプリケーションでは、チャネル使用率が 30 % を超えるとエンドユーザ エクスペリエンスに影響が出る可能性があります。チャネル使用率の値が高い場合、新たな干渉源、AP の停止、大量の Wi-Fi デバイスの追加を示している可能性があります。シスコでは、デバイスを追加する前に、既存のクライアント数、アクセス ポイントごとのクライアント数、設定済みチャネル数、現在のチャネル使用率のベースライン測定を作成することを、お客様に推奨しています。

シスコの無線リソース管理（RRM）は、コントローラ上でデフォルトで有効になっており、ユーザの関与をほとんど必要とせず RF 環境を動的に管理できるよう設計されています。RRM は、測定された Over-the-Air メトリックを使用して、チャネルと電力の最適な組み合わせを計算し、割り当てます。RRM は、すべてのチャネルで高使用率を追跡し、同一チャネル割り当てを軽減して電力を平均化します。利用できるオープン チャネルがない場合、または単に AP が近すぎる場合には、チャネルを既存のユーザと共有することが、唯一残された選択肢となります。これは、輻輳した環境で起こります。このようなときには、異なる 2 つのネットワークが同じ帯域幅を共有しなければならない場合があります。

シスコでは、継続的に高いチャネル使用状況の影響を受けている 5 GHz Wi-Fi チャネルを注意深く監視して、干渉が繰り返し発生する場合や管理不能な場合には動的チャネル割り当て（DCA）除外リストに追加することを推奨しています。DCA リストからチャネルを除外するのは最終手段と考えてください。チャネルを削除する場合、シスコでは、RF プロファイルを使用して、チャネルの削除をすべての AP でグローバルに適用するのではなく、該当する AP のみに効果的に適用することを推奨しています。

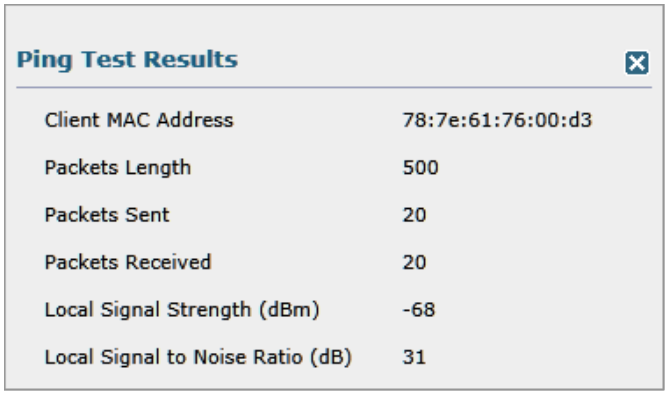
© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

注: 詳細については、『Enterprise Mobility Design Guide（エンタープライズ モビリティの設計ガイド）』の RRM ガイドラインを参照してください。http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide.pdf [英語]

iOS デバイスで実行しているアプリケーションに現在の 5 GHz AP カバレッジが十分かどうか評価するために、シスコ ワイヤレス LAN コントローラ（WLC）では、アクセス ポイントでのクライアント信号の認識を確認するための使いやすいリンク テスト ツールが提供されています。これに加えて、Apple が、同社の AirPort Utility アプリで iOS 向けワイヤレス ネットワーク スキャナを提供しています。信号対雑音比（SNR）は常に 25 以上に維持する必要があります。

コントローラ インターフェイスから Apple デバイスのリンク テストを実行する

1. コントローラ GUI で [監視（Monitor）] > [クライアント（Clients）] の順に選択し、[クライアント（Clients）] ページを開きます
2. カーソルを目的のクライアントの青いドロップダウン矢印の上に置いて、[リンク テスト（Link Test）] を選択します。リンク テスト ページが開き、結果が表示されます。

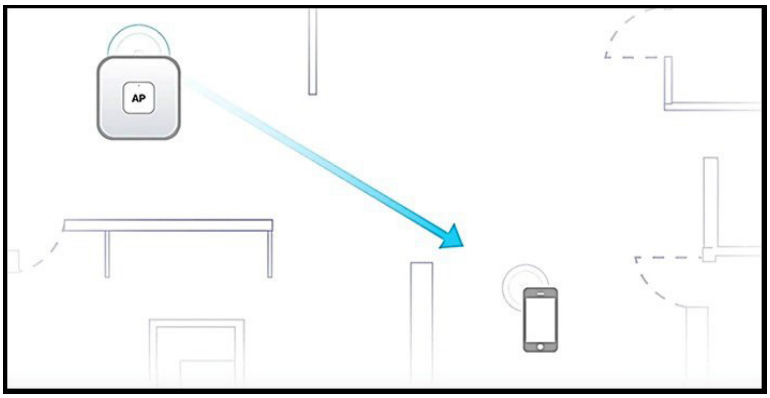


ClientLink ビームフォーミング

特許を取得したシスコのビームフォーミング テクノロジー、ClientLink は、Apple の iPhone や iPad といったモバイル デバイスの接続信頼性を最適化する機能を提供します。このテクノロジーは、アクセス ポイントのチップセットに対する信号処理の拡張機能をベースとしているので、ネットワーク パラメータを変更する必要はありません。現在ビームフォーミングは、最近の iOS デバイスのほとんどでサポートされていますが、ClientLink はすべてのワイヤレス クライアント デバイスにとって有益です。その機能はクライアント デバイスからの支援に依存しないので、クライアントのビームフォーミング対応の有無に関係なく、古いデバイスにも新しいデバイスにもメリットがあります。ClientLink はアルゴリズムを使用してワイヤレス チャネル状況を概算します。それにより、アクセス ポイントは、クライアント接続に有利になるようにトランスミッタ/レシーバ アンテナの RF を調整できます。この機能は Cisco AP ではデフォルトで有効になっており、常時、バックグラウンドで継続的に動作します。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

図 4. Cisco ClientLink テクノロジーは、各 iOS デバイスへの信号を最適化して接続性を向上させます。



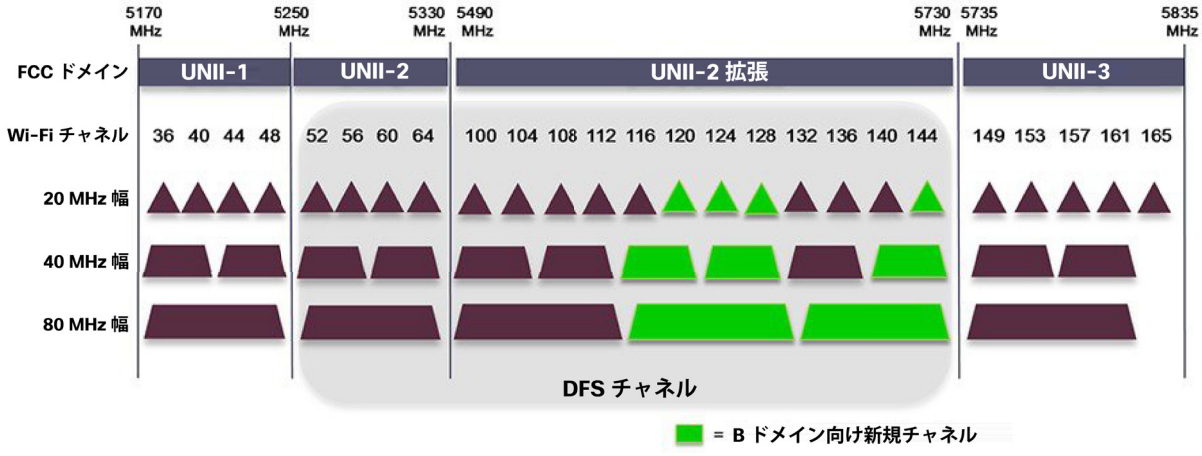
ClientLink テクノロジーの主なメリットは、AP とワイヤレス クライアント デバイス間の Wi-Fi 信号品質の向上です。その結果、AP とクライアント デバイス間のリンクの品質が高くなり、クライアントがより高いデータ レートで接続を維持する可能性が高まるとともに、Wi-Fi ネットワーク全体のすべてのワイヤレス クライアントのカバレッジ品質が向上します。ClientLink は、屋内のマルチパス環境でゲインを提供するだけでなく、屋外または大規模な屋内のオープン スペースなどのラインオブサイト（見通しの良い）環境のクライアントでも SNR を向上させます。

注: ClientLink 4.0 の詳細については、http://www.cisco.com/c/dam/en/us/products/collateral/wireless/aironet-3600-series/at_a_glance_c45-691984.pdf [英語] を参照してください。

Wi-Fi チャネル帯域幅

802.11a では、5 GHz チャネルが 20 MHz のチャネル幅を使用します。802.11n および 802.11ac の導入により、チャネル ボンディング機能が追加され、複数の 20 MHz チャネルを結合して、帯域幅の広い 1 つのチャネルを形成できるようになりました。チャネル帯域幅を倍にして 20 MHz から 40 MHz にすることにより、1 回の送信で同時に 2 倍の量のデータを送信して、ワイヤレス ネットワークのスループットを効果的に倍増させることができます。802.11ac では、5 GHz のチャネル幅モードを 20 MHz、40 MHz、80 MHz（802.11ac - wave 2 では 160 MHz）[英語] から選択できます。

図 5. 5 GHz ネットワークにおける 20 MHz、40 MHz、80 MHz チャネル幅のチャネル ボンディング例



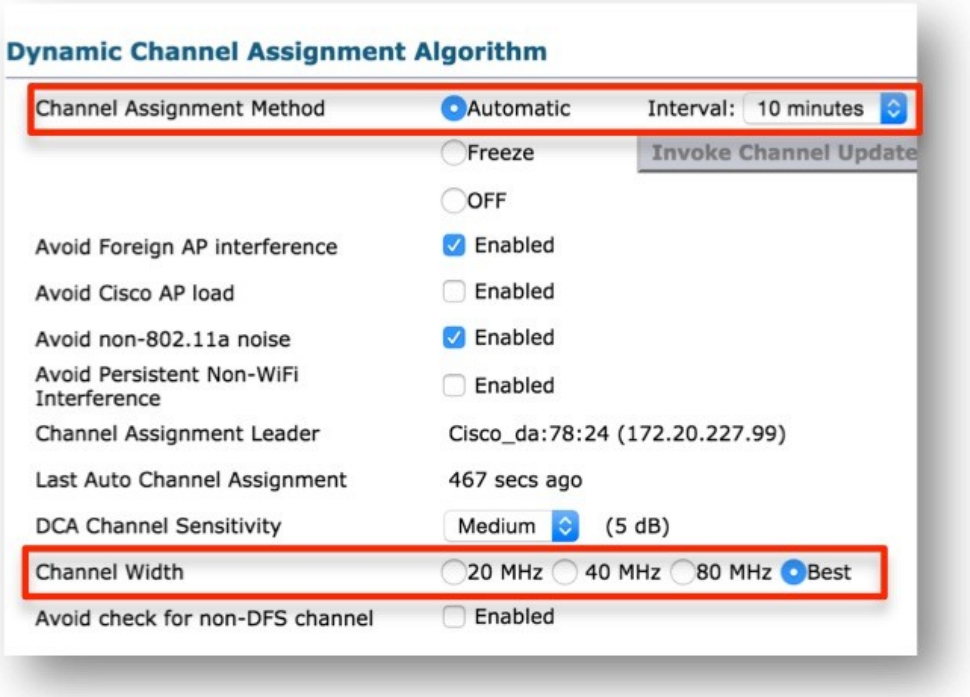
© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

シスコと Apple は、スループット パフォーマンスが要求される環境では 40 MHz チャネル幅を推奨し、AP 密度の高い導入環境では 20 MHz の使用を推奨しています。40 MHz 幅の導入を効率的に行うためには、DFS チャネルを使用して最適な周波数再利用を実現し、同一チャネル干渉の可能性を低くすることが必要になります。FCC の規制を受けるドメインで DFS チャネルを有効にしない場合は、4 つの 40 MHz チャネルが使用できます。DFS チャネルを有効にすると、使用可能な 40 MHz チャネルの数は 10 に増えます。

80 MHz 幅チャネル ボンディングを使用すると、最初は個々のクライアントのパフォーマンスが向上するように見えますが、高密度 AP 環境では、利用できるスペクトルが限られるため同一チャネル干渉が発生し、全体的なネットワーク パフォーマンスは低下する可能性があります。

したがって、80 MHz チャネル幅設計の使用は推奨していません。使用する必要がある場合は、同一チャネル干渉を簡単に回避できる低密度 AP 環境に限定して考慮すべきです。

図 6. コントローラ ユーザ インターフェイスからチャネル幅を設定する



[ワイヤレス（Wireless）] > [802.11a/n/ac] > [RRM] > [DCA] の順に移動して、使用するチャネル幅を指定します。

[20 MHz]、[40 MHz]、または [80 MHz] を選択します。あるいは、ネットワーク環境に基づいた最適なチャネル幅を RRM によって自動的に判定することもできます。このオプションを有効にするには、[チャネル幅（Channel Width）] で [最適（Best）] を選択します。

注: 詳細については、『Enterprise Mobility Design Guide（エンタープライズ モビリティの設計ガイド）』の DCA ガイドラインを参照してください。http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide.pdf [英語]

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

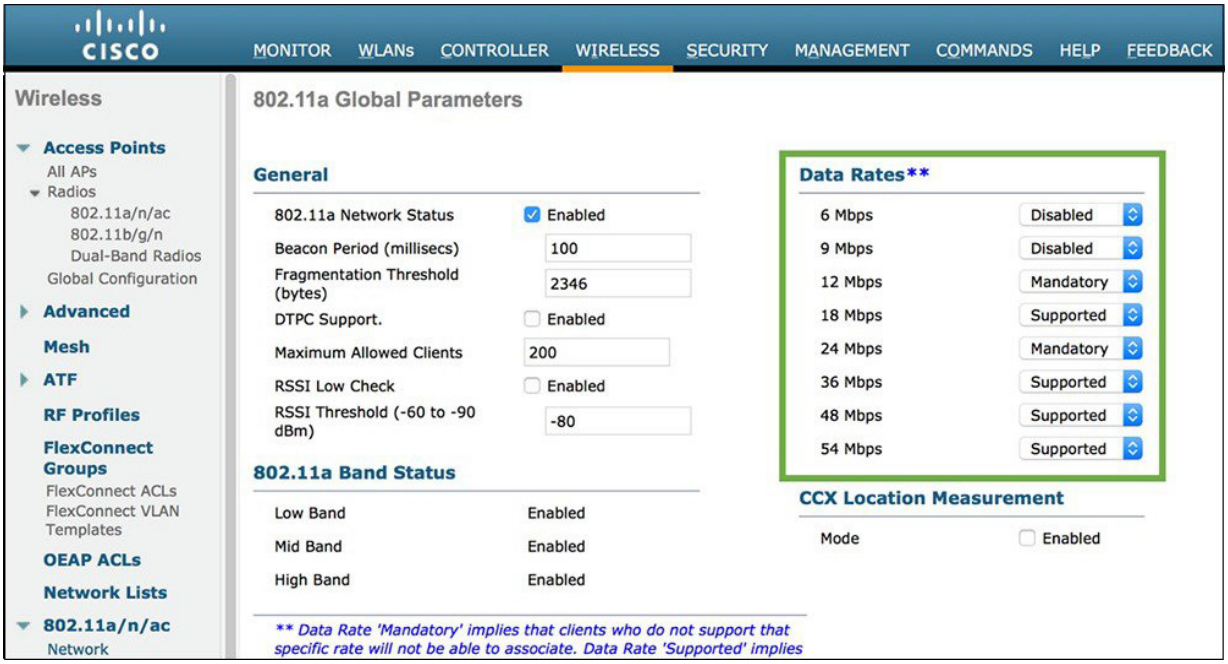
データ レート

ワイヤレス デバイスでのデータ伝送に使用するデータ レートを指定するには、データ レート設定を使用します。データ レート、パフォーマンス、範囲、および信頼性の間には、直接的な相関関係があります。iOS デバイスを使用するときの戦略は、ネットワーク接続する可能性のあるデバイスをすべて含めた包括的なものとし、環境の AP 密度を考慮する必要があります。方法は 2 つあります。

- **範囲の最大化**：範囲の拡大が必要な場合は、低データ レート化を検討します。データ レートを低くすると、受信側で信号を復号するために必要な信号レベルと SNR が低く抑えられるので、クライアント デバイスは遠い距離からでも信頼性を維持して AP に接続することができます。範囲を最大限に拡大すると、クライアント デバイスのアプリケーション パフォーマンスに影響を与える可能性があります。時間が重要視される音声/ビデオ タイプのアプリケーションでは特にその影響が大きくなります。一般的に、データ レートを低くすると、無線通信時間は長くなり、全体的なセル容量（ユーザ エクスペリエンス）が低下する可能性があります。
- **パフォーマンスの最大化**：高性能 WLAN の導入、ローミングの改善、セル カバレッジの削減による同一チャネル干渉の影響緩和を目指す場合は、データ レートを高くする設定を検討してください。最小データ レートで過剰にアグレッシブな動作をさせるのは避けてください。データ レートが低すぎると、クライアント デバイスが信頼性の高い接続を確立できなくなり、実質的にパフォーマンス低下という結果を招く恐れがあります。

IEEE 802.11a 規格では、6、9、12、18、24、36、48、54 Mbps のデータ レートを設定できます。54 Mbps が最大データ レートとなります。

図 7. 5 GHz ネットワークのデータ レートを設定する



[ワイヤレス（Wireless）] > [802.11a/n/ac] > [ネットワーク（Network）] の順に移動して、AP/クライアント間のデータ送信レートを指定します。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

個々のデータ レートは、次の 3 つのモードのいずれかに設定できます。

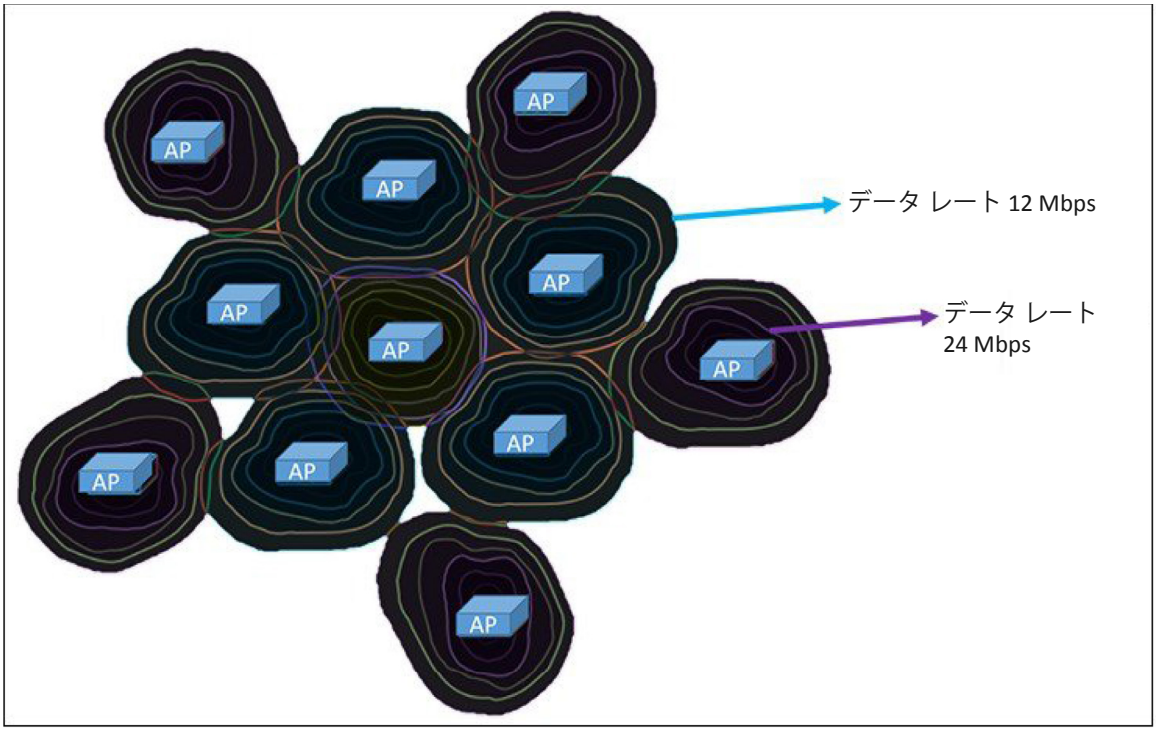
- [必須（Mandatory）]：全パケット（ユニキャストとマルチキャストの両方）にこのレートでの伝送を許可します。AP の少なくとも 1 つのデータ レートを [必須（Mandatory）] に設定する必要があります。また、この AP に接続したすべてのクライアントは、ネットワークを使用するための無線でこのデータ レートを物理的にサポートすることが必要となります。さらに、AP に接続したワイヤレス クライアントについては、現在最も低い必須データ レートで設定されているパケットを受信できる必要があります。また、無線は最大の必須データ レートを物理的にサポートする必要があります。現在最小の必須レート フレームが受信されないと、クライアントがビーコンを受信できず、接続解除につながる可能性があります。複数のデータ レートを [必須（Mandatory）] に設定すると、マルチキャストは、接続したすべてのクライアントに共通のレートの中で最も高い必須レートで送信されます。ブロードキャストは、常に最も低い必須レートで送信されます（最も高いレートではありません）。

- [サポート（Supported）]：ユニキャスト パケットのみこのレートでの伝送が許可されます。ワイヤレス クライアントは常に、可能なかぎり最も高いデータ レートで送受信しようとします。

- [無効（Disabled）]：AP はこのデータ レートでデータを伝送しません。

低いデータ レートを必須に設定すると、AP からのパケットを受信できる範囲が拡大します最小必須データ レートを低く設定するほど、AP からのビーコンおよびその他のパケットの範囲が広がります。これによってアクセス ポイントのセル サイズが増加するため、AP の数が少ないサイトでは望ましい状態かもしれませんが、モバイル クライアントの密度が高い場合には、サイトから帯域幅が奪われ、アプリケーション パフォーマンスの低下につながる可能性があります。

図 8. データ レートが AP のセル サイズに及ぼす影響をクライアント側の観点から示した例



© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

シスコと Apple は、Cisco Wireless LAN で iOS デバイスを使用する際の一般的なベスト プラクティスとして、最小データ レートを 12 Mbps とし、12 Mbps と 24 Mbps を 2 つの必須データ レートとして有効にすることを推奨します。5 GHz カバレッジでは余裕がないという場合には、最も低い必須レートとして 6 Mbps を設定することで問題を解決できる可能性があります。

クライアント デバイスが設定どおりのデータ レートでネットワークに接続していることを監視および確認するために、コントローラ ダッシュボードと Cisco Prime Infrastructure を使用して、管理ログ、トラップ、アラートを継続的に確認することをお勧めします。データ レートが正しく設定されていない可能性を示す兆候としては、次のような状態が挙げられます。

- カバレッジ ホール アラーム
- 高チャネル使用率
- 過剰な再送信
- クライアントが接続不能、またはローミング問題が発生

QoS

Cisco WLAN に接続した iOS デバイス上で動作するアプリケーションの結果を最適化するには、正しいエンドツーエンドの QoS を実装することが不可欠です。Wi-Fi トラフィックは優先順位値を表示できます。この値は、802.11e 修正規格で定義されており、802.11 ヘッダーに存在するユーザ優先度（UP）タグによって表現されます。このユーザ優先度は、トラフィック識別子（TID）とも呼ばれます。0 ～ 7 の任意の値を受信できます。一般に、UP が高いトラフィックほど、Over-the-Air 処理の優先度が上がります。Wi-Fi Alliance によって、802.11 QoS マーキングを適用するベンダー間の相互運用性と、Wi-Fi マルチメディア（WMM）認定による優先順位付けが確保されます。シスコ コントローラでの SSID の設定によって、WLAN との間でやり取りされるトラフィックに認められる最高の優先順位が決まります。

ワイヤレス QoS

ベンダーによっては、使用する変換メカニズムや Wi-Fi QoS マーキング/有線 QoS マーキング間の値が異なっている可能性があります。シスコは DSCP マーキングをダウンストリームで使用しており、レイヤ 2 またはレイヤ 3 マーキングをアップストリームで使用できます。シスコでは、IETF マーキング変換推奨事項（例：DSCP トラフィック マーキングに関する最新の IETF ガイドラインである RFC 4594）および 802.11e マッピングに準拠しています。

表 2. 主なトラフィック カテゴリに適用されるデフォルトの QoS マーキング

Cisco 802.1p ユーザ優先度 トラフィック タイプ	IP DSCP（PHB 値）	IEEE 802.11e/WMM ユーザ優先度	名称（説明用）	シスコでの名称
予約済み	56 ～ 63	7（未使用）	—	—
予約済み	48 ～ 55	6（未使用）	—	—
音声	46（EF）	6	音声	プラチナ
インタラクティブ ビデオ	34、36、38（AF4x）	4	ビデオ	ゴールド

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

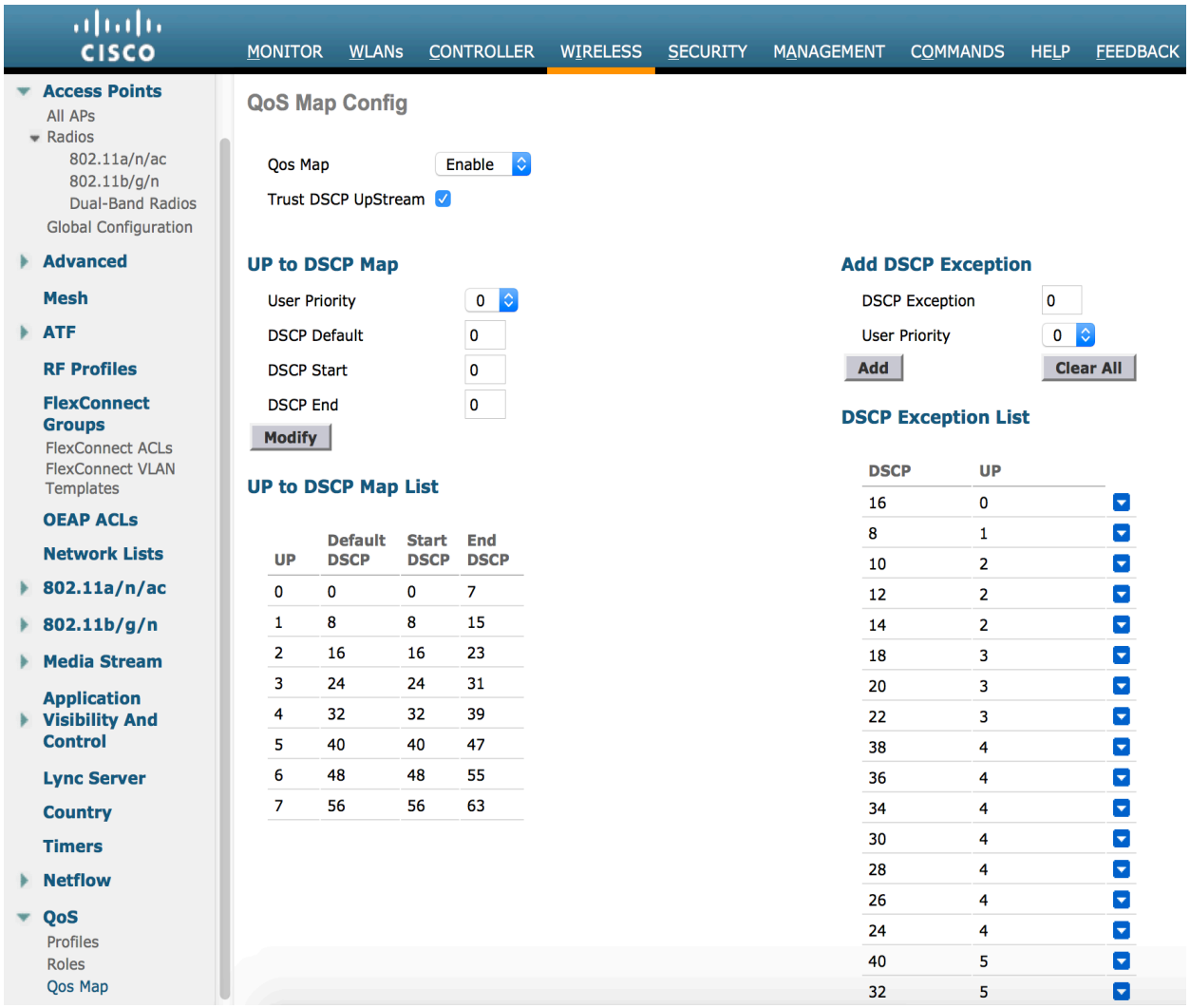
ビデオ ストリーミング	26、28、30（AF3x）	4	ビデオ	ゴールド
音声制御（シグナリング）	24（CS3）	4	ビデオ	ゴールド
バックグラウンド（トランザクショナル/インタラクティブ）	18、20、22（AF2x）	3	ベストエフォート	シルバー
バックグラウンド（バルク データ）	10、12、14（AF1x）	2	バックグラウンド	ブロンズ
ベストエフォート	0（BE）	0	ベストエフォート	シルバー
スカベンジャ	8（CS1）	1	バックグラウンド	ブロンズ

注： 表に記載されていない DSCP 値に対する IEEE 802.11e UP 値は、DSCP の上位（MSB）3 ビットを考慮して算出されます。たとえば、DSCP 32（バイナリ 100 000）に対する IEEE 802.11e UP 値は、MSB（100）と同等の 10 進数値、つまり 4 になります。DSCP 32 の 802.11e UP 値は 4 です。

AireOS コントローラ コード 8.1 以前では、上記の変換に、スタティック マッピング テーブルとアップストリーム マッピング用 UP 値が使用されます。AireOS 8.1MR リリースからは、ユーザが QoS マッピング オプションを使用してアップストリーム マッピング用カスタム DSCP 値を決めることができます。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

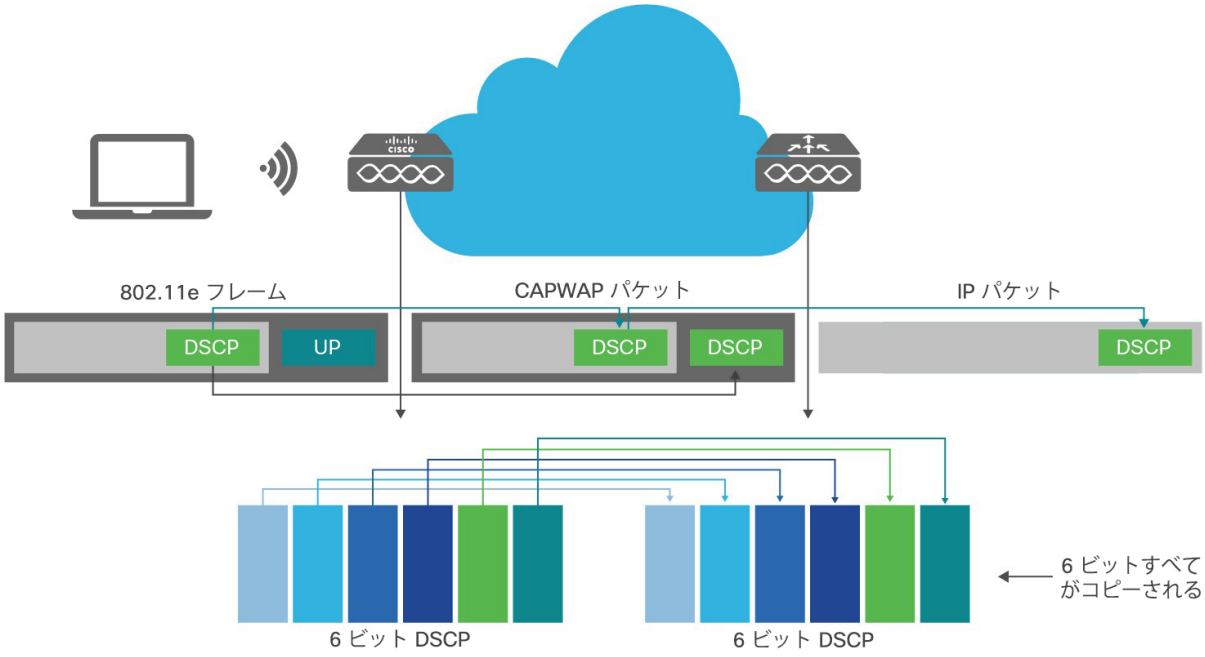
図 9. AireOS 8.1MR 以降で DSCP マッピング値にカスタム UP を適用する（AireOS 8.3 でさらにアップデート済み）



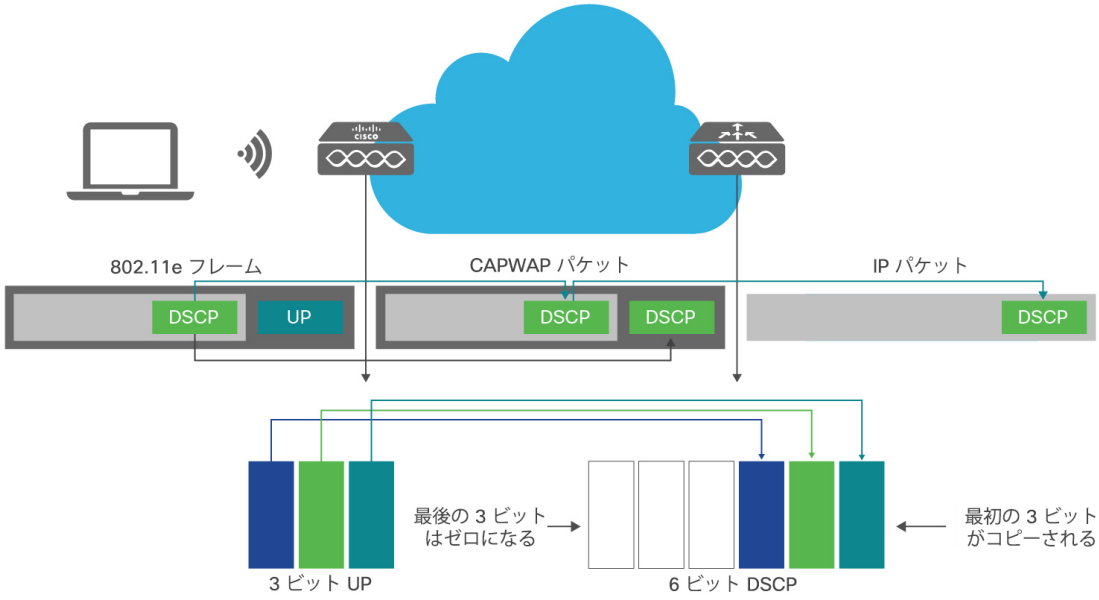
[ワイヤレス（Wireless）] > [QoS] > [QoS マップ（QoS Map）] の順に移動して、DSCP マッピング値に UP を設定します。

Wi-Fi 業界では、一般的にアップストリーム UP が信頼されています。しかし、その結果として、CAPWAP 外部ヘッダー DSCP（レイヤ3）QoS 値が UP 値（レイヤ2）から取得されます。一般に、レイヤ 2 の値はローカル セグメント上で有効であり、レイヤ 3 の値は複数のセグメント間で有効です。ローカルで有効な値からグローバル値を取得することはベスト プラクティスとは見なされません。さらに、UP 値から DSCP 値を取得するということは、QoS の 3 ビットだけが 6 ビット フィールドに変換されることを意味し、DSCP が十分に活用されないことになります。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.



AireOS code 8.1 MR によって、DSCP がアップストリームで信頼され、CAPWAP 外部ヘッダー DSCP（レイヤ3）QoS 値がワイヤレス クライアント DSCP（レイヤ3）値から取得される可能性が生じています。SSID QoS プロファイルは上限として使用され、QoS ポリシーの悪用を防止します。iOS デバイスは DSCP 値と UP 値をマークします。ワイヤレス クライアントが DSCP 値をマークする場合、シスコでは、アップストリーム DSCP の信頼を有効にして、インフラストラクチャが DSCP 6 ビットで詳細に設定できる機能を最大限に活用できるようにすることを推奨しています。



アップストリーム DSCP の信頼を有効にすると、カスタムの DSCP/UP マッピングを設定することもできます。デフォルトの DSCP/UP マッピングは、上記の表 2 に記載されたルールに従って行われます。カスタム マッピングにより、着信 DSCP 値と UP 値間の変換をより確定的に行うことができます。特に、次の点に注意してください。DSCP 値の中には、標準的なアクセス ネットワークで想定されていないものもあります。たとえば、すべて奇数の DSCP 値などがそれに当たります。標準的な DSCP 値は偶数と想定されています。DSCP 値が奇

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

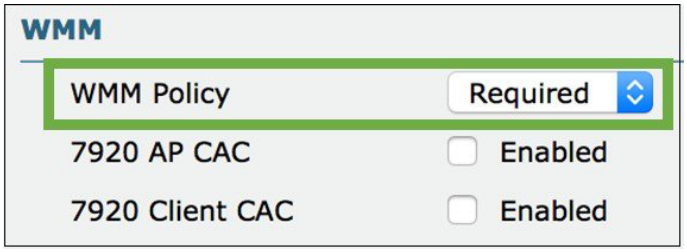
数ということは、MBZ（Must Be Zero：ゼロでなければならない）と呼ばれる DSCP フィールドの最下位ビットが 1 に設定されることを意味します。カスタム DSCP を UP マップに使用することにより、想定外のすべての DSCP 値がセル内でベスト エフォート送信に変換され、QoS ポリシー悪用のリスクが軽減されます。リストには最大 21 個の例外を設定できます。この設定により、3 つの MSB の値に関係なく、既知の DSCP 値を推奨 UP 値に確実に変換することが可能になります。

Wi-Fi マルチメディア

Wi-Fi マルチメディア（WMM）は、ワイヤレス ネットワーク向け QoS の標準形式で、802.11e 修正規格に基づいています。シスコと Apple の両社は、ネットワークおよびアプリケーション層で WMM を強力にサポートしています。

WMM の WLAN 設定にはさまざまな使用例があります。WMM が無効に設定されている場合、パケットのキューイングまたはマーキングに WMM QoS は使用されません。QoS を無効にすることにより、パケットのマーキングが一切なくなります。したがって、Apple iPhone デバイスに送られる ping は、たとえ WLAN QoS 設定が音声またはプラチナとなっていても、ベスト エフォート（BE）優先度として送られます。このような理由から、WMM の設定は、使用例に応じて [許可（Allowed）] または [必須（Required）] とするようお推めします。WLAN または SSID を iOS デバイスにしか使わないのであれば、[必須（Required）] に設定することを推奨します。

図 10. WLAN の WMM の設定



[WLAN] > [QoS] の順に移動し、WMM の設定として [必須（Required）] を選択します。

802.11e/WMM 仕様は、携帯電話が Wi-Fi を代替ワイヤレス メディアとして使用したり、タブレットが Wi-Fi を使用したりするようになって以来、広く使われてきました。これらのデバイスは、WMM が [必須（Required）] に設定されている WLAN に接続できることが必要です。

注： WMM 非対応クライアントは、WLAN の WMM ポリシーが [必須（Required）] に設定されている場合、セキュリティが設定されていなくても、WLAN に接続することはできません。一方、802.11n および 802.11ac 認定には WMM サポートが必須とされており、802.11n または 802.11ac クライアントはすべて WMM をサポートする必要があります。WMM 非対応クライアントをサポートする場合は、別のワイヤレス ネットワークでネットワーク接続を確保することを推奨します。

コントローラでの WMM 制御では、クライアントへのダウンストリーム パケットを定義済みとしてマークすることしか保証できないので、管理者は注意する必要があります。クライアントおよびアプリケーションは、アップストリーム トラフィック向けの WMM を適切にサポートする必要があります。iOS デバイスは、アプリケーション層サポートに加え、ネットワーク レベルの WMM 設定（たとえばプラチナまたは音声）をサポートできます。Apple は、特定のパケットを適切な WMM レベルに確実にキューイングできるように、アプリケーション層でパケット マーキングを行う機能をアプリケーション開発者に提供しています。アプリケーション開発者は、iOS アプリが適切な WMM マーキングのタグ付けを行うことでクライアントのアップストリーム トラフィックが正しくタグ付けされるようにする必要があります。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

WLAN の QoS プロファイル

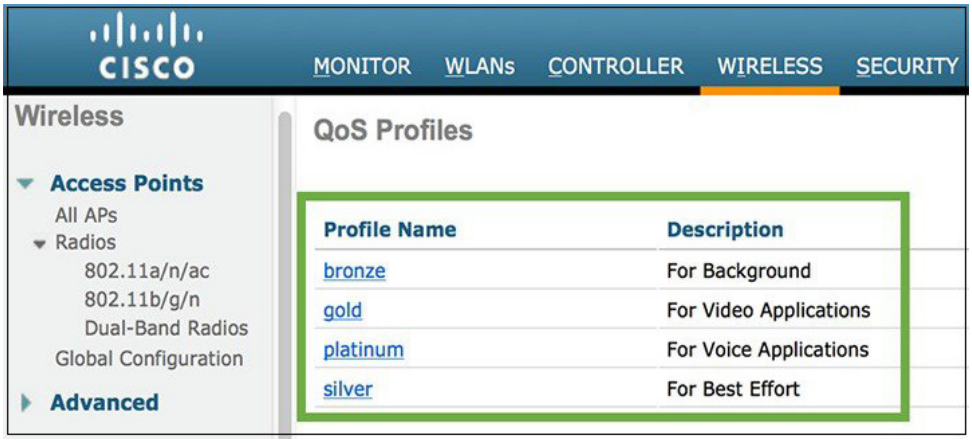
Cisco WLAN コントローラのユーザ インターフェイスから、各 SSID に QoS プロファイル（プラチナ、ゴールド、シルバー、ブロンズ）を割り当てることができます。このプロファイルによって、当該の SSID での使用を想定および許可される最高の QoS レベルが決まります。QoS プロファイルの役割は、上限（クライアントが使用できる最高 QoS レベル）を設定することです。たとえば、WLAN にシルバー プロファイルを設定すると、クライアントが送信できるのは、バックグラウンドなど優先度の低いトラフィックになります。高い QoS 値（たとえば音声やビデオ）をマークされたトラフィックは、マーキングがシルバー（BE、DSCP 18）に下げられます。

また、着信した非 WMM トラフィック、DSCP マーキングのないトラフィック、マルチキャスト トラフィックに使用されるマーキング動作も、プロファイルによって決まります。着信トラフィックがプロファイルの最高 QoS 値を超えている場合、そのトラフィックは、プロファイルに割り当てられている最高 QoS 値に一致するように再マーキングされます。マルチキャストおよび非 WMM トラフィックのターゲット QoS 値は設定によって変更できます。

同様に、プラチナを設定すると、クライアントは最高の QoS タグ/クラス（UP6/DSCP EF まで）を使用できます。ただし、すべてのトラフィックが音声トラフィックと見なされるわけではありません。つまり、たとえば iPad から音声トラフィックが送信された場合は、このトラフィックは音声として処理されますが、ベスト エフォート トラフィック（大半の非リアルタイム アプリケーションが送信するトラフィック）が送信された場合には、ベスト エフォートとして処理されます。

WLAN QoS パラメータの設定により、iOS デバイスが通信する WLAN 上の非 WMM または未知のトラフィックをきめ細かく処理できる設定を追加することができます。

図 11. QoS プロファイル設定の確認

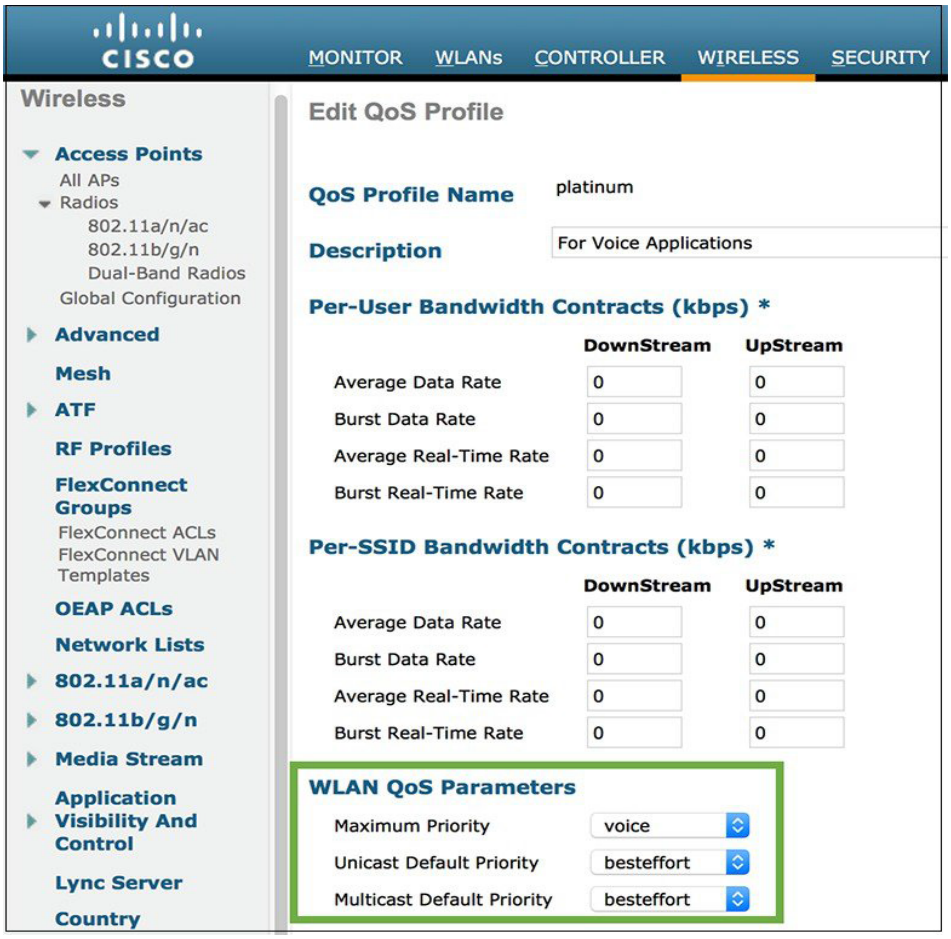


個々の QoS プロファイル設定は、[ワイヤレス（Wireless）] > [QoS] タブの順に移動して確認できます。

ユニキャストのデフォルト優先順位は、着信した未知のトラフィックのマーキングに割り当てられます。この設定によって、非 WMM トラフィックまたは未知のマーキングの付いたトラフィックに対して行う処理が決まります。ユニキャストのデフォルト優先順位とマルチキャストのデフォルト優先順位をベスト エフォートに設定すると、WLAN 上で意図しない優先順位付けが行われてしまうのを防ぐことができます。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

図 12. ユニキャストおよびマルチキャスト トラフィックの QoS プロファイル パラメータを設定する



[ワイヤレス（Wireless）] > [QoS] > [プロファイル（Profiles）] > [プラチナ（Platinum）] タブの順に移動して、[ユニキャストのデフォルト優先順位（Unicast Default Priority）] と [マルチキャストのデフォルト優先順位（Multicast Default Priority）] に [ベスト エフォート（best effort）] を選択します。iOS デバイス向けの WLAN に割り当てた QoS プロファイルに基づいて、パラメータの変更を適宜実施する必要があります。

音声としてマークされたトラフィックをすべての iOS デバイスで有効にするは、WLAN QoS を [プラチナ（Platinum）] に設定することを推奨します。

図 13. WLAN の QoS プロファイルの設定

WLAN に QoS プロファイルを割り当てるには、WLAN SSID の [WLANs] > [QoS] タブの順に移動します。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

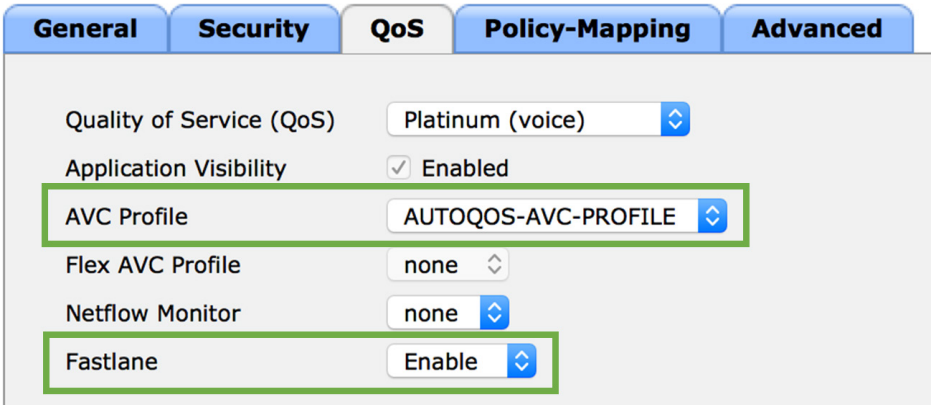
Fast lane の設定

この設定は、AireOS 8.3 以降を実行するシスコ コントローラおよび iOS 10 以降を実行するデバイスのみに適用されます。

Fast lane の設定は、WLAN コントローラでの最適な QoS 設定を簡単に確保できる方法です。特に、iOS 10 クライアントがワイヤレス クライアントのかなりの部分を占めることが予想される場合に有効です。QoS 関連の WLAN コントローラの設定には時間がかかることがあります。この設定には複数の複合的な要素の設定が伴うので、管理者にとっては困難な作業になる場合があります。

WLAN コントローラでの QoS 設定を容易に最適化できるように（特に iOS 10 を実行するデバイスがワイヤレス クライアント ベースのかなりの部分を占めることが予想される場合）、シスコは WLAN 設定ページの [QoS] タブに [Fast lane] オプションを設けました。

図 14. WLAN で Fast lane を設定する



注： Fast lane を（WLAN で初めて）有効にしたときには、すべての WLAN およびネットワークが自動的に無効になります。設定が完了すると、元のステータスに戻ります。また、AUTOQOS-AVC-PROFILE がまだ存在していない場合は、新たに作成されます。

WLAN の Fast lane QoS オプションを有効にすると、自動的に次の動作が行われます。

- 5 GHz および 2.4 GHz ネットワークが一時的に無効になります（これにより、下記の設定をアクティブ化できるようになります）。
- プラチナ QoS プロファイルで非 WMM およびマルチキャスト トラフィックがベスト エフォートに設定されます。
- プラチナ QoS プロファイルで UDP トラフィックの帯域幅制限が 0（制限なし）に設定されます。
- 設定された WLAN にプラチナ QoS プロファイルが適用されます。
- 新たに改訂された 802.11 規格の推奨事項に合致した Fast lane EDCA プロファイルが、両側でアクティブ化されます。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

- 負荷計算に基づき、音声トラフィック（両帯域）でワイヤレス CAC（ACM）が有効になります。帯域幅の 50 % が音声トラフィックに割り当てられ、6 % が音声トラフィックのローミングに割り当てられます。
- 上記の図 9 に示すように、DSCP がアップストリームで信頼され、カスタムの DSCP/UP マップが設定されます。
- Fast lane 機能が WLAN で有効になります。この機能は、次のセクションで説明する Fast lane プロファイルのコンテキストで使用されます。
- AUTOQOS-AVC-PROFILE という AVC プロファイルが作成されます。このプロファイルにより、代表的なアプリケーション（Jabber、Cisco Phone、WebEx、Lync などのアプリケーションからの音声およびビデオ トラフィックを含む）の適切な QoS マーキングが確保されます。
- 5 GHz および 2.4 GHz ネットワークが再び有効になります。

Fast lane では、ワイヤレス CAC が重要な要素となります。UP 6 キューは優先順位が非常に高く、音声トラフィック向けに設定されています。WLAN で QoS ポリシーが悪用されないようにするため、802.11 規格および WMM 認定では、どのトラフィック ステーションがこのキューを送信することになっているのかインフラストラクチャで確認できるようになっています。この確認は、UP 6 キューのアクセス制御強制（ACM）ビットを有効化することで行われます。このビットが有効になっている場合、UP 6 トラフィックを送信しようとするステーションは、最初に Add Traffic Stream（ADDTS）要求を AP に送信する必要があります。この要求には、対象トラフィックを記述する、トラフィック仕様（TSPEC）というフィールドが含まれます。AP は、ADDTS 応答で応答し、対象トラフィックを認可または拒否します。ACM が有効になっていると、ステーションは ADDTS を交換せずに UP 6 キューを使用することはできません。

ACM が有効なときにステーションが ADDTS 交換を経由せずに UP 6 でアップストリーム トラフィックを送信すると、リターン トラフィックはベスト エフォートになります。つまり、ワイヤレス インフラストラクチャはリターン パスで UP 6 を適用しないということです。

シスコと Apple は連携して、トラフィックが IETF の推奨に合った QoS マーキングを確実に受けられるよう力を注いできました。その結果、iOS 10 を実行するデバイスから着信したトラフィックは、AireOS コード8.3 以降を実行するシスコ ワイヤレス インフラストラクチャにおいて異なる扱いを受けるようになっています。iOS 10 を実行するデバイスから来た UP 6 トラフィックは、ADDTS 交換が行われない場合でも UP 6 として処理され、リターン トラフィックも特権的な UP 6 キューを経由します。この相互信頼を可能にするために、ビーコン、プローブ要求、プローブ応答、およびアソシエーション フレームには特別なビットが存在しており、クライアント側とインフラストラクチャ側が互いを確認し、この信頼を確立できるようになっています。

Fast lane で ACM を有効化したことによる実用上の効果として、ADDTS 交換を実行するステーションや、音声トラフィックを送信する iOS 10 実行デバイス（ADDTS 交換を行わない場合も含む）は、音声トラフィック向け UP 6 キューの特権を受けることができます。ただし、ADDTS を実行しない他のステーションは、別のキュー（通常はビデオまたはベスト エフォート）を使用しなければなりません。輻輳した環境では、この設定によってそのようなステーションのパフォーマンスが低下する可能性があります。シスコでは、UP 6 キューを使用する際には、ワイヤレス クライアントが ADDTS を正しく実行しているか確認することを推奨しています。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Fast lane プロファイル

AireOS 8.3 以降を実行するシスコ ワイヤレス インフラストラクチャおよび iOS 10 を実行するデバイスは、相互認識交換を実施します。WLAN で Fast lane を有効にすると（上記の「Fast lane の設定」セクションを参照）、ワイヤレス インフラストラクチャは、iOS 10 を実行するデバイスに対し、QoS マーキングを使用するアプリには特別な処理が適用できることを通知します。一部のアプリに QoS マーキングの使用が許可される一方、他のアプリはベスト エフォートまたはバックグラウンド キューで送信されます。

システム管理者は、EMM または MDM ソリューション、または Apple Configurator を使用して iOS デバイスに設定プロファイルを導入できます。iOS 10 では、これらのプロファイルをシンプルな QoS プロファイルにすることが可能です。このようなプロファイルでは、Fast lane ネットワークで QoS の使用が許されるアプリケーションをリストに記載します。これらのプロファイルは、iOS 10 実行デバイスのための標準プロファイル プロビジョニング手順に従って導入されます。ホワイトリストに入れるアプリケーションをリストに記載することにより、システム管理者は、ビジネス関連のアプリケーションには特権を与える一方で、ビジネスに関係のないアプリケーションはベスト エフォートあるいはバックグラウンド キューにプッシュすることができます。

Fast lane プロファイルにより、次の動作が実行されます。

- [WLAN QoS] 設定タブで [Fast lane] を有効にすることにより、8.3 以降を実行する Cisco WLAN コントローラ上で WLAN ごとに Fast lane がアクティブ化されます。
- デフォルトで、すべてのアプリケーションがホワイトリストに登録されています。Fast lane ネットワークにおいて、iOS 10 を実行するデバイスにプロファイルがプッシュされていない場合には、すべてのアプリケーションがアップストリーム QoS をマーキングできます。
- Fast lane ネットワークにおいて、QoS プロファイルが iOS 10 デバイスに適用されている場合は、ホワイトリストに登録されているアプリケーションのみがアップストリーム QoS をマーキングできます。ホワイトリストに登録されていないアプリケーションは、ベスト エフォートとして送信されます（または、QoS マーキングがベスト エフォートより低い場合はバックグラウンドとして送信されます）。
- Apple FaceTime と Wi-Fi Calling は特別なトラフィック カテゴリであり、デフォルトでホワイトリストに登録されます。QoS プロファイルで特定のビット（QoSMarkingAppleAudioVideoCalls）を非アクティブ化することにより、これらをベスト エフォート キューに送ることもできます。シスコでは、ほとんどのネットワークに関し、このビットを無効にすることは推奨していません。
- Fast lane でないネットワークにおいては、一般にアップストリーム DSCP にマーキングは行われず、ホワイトリストの概念も適用されません。

Systems Manager による Fast lane プロファイルの導入

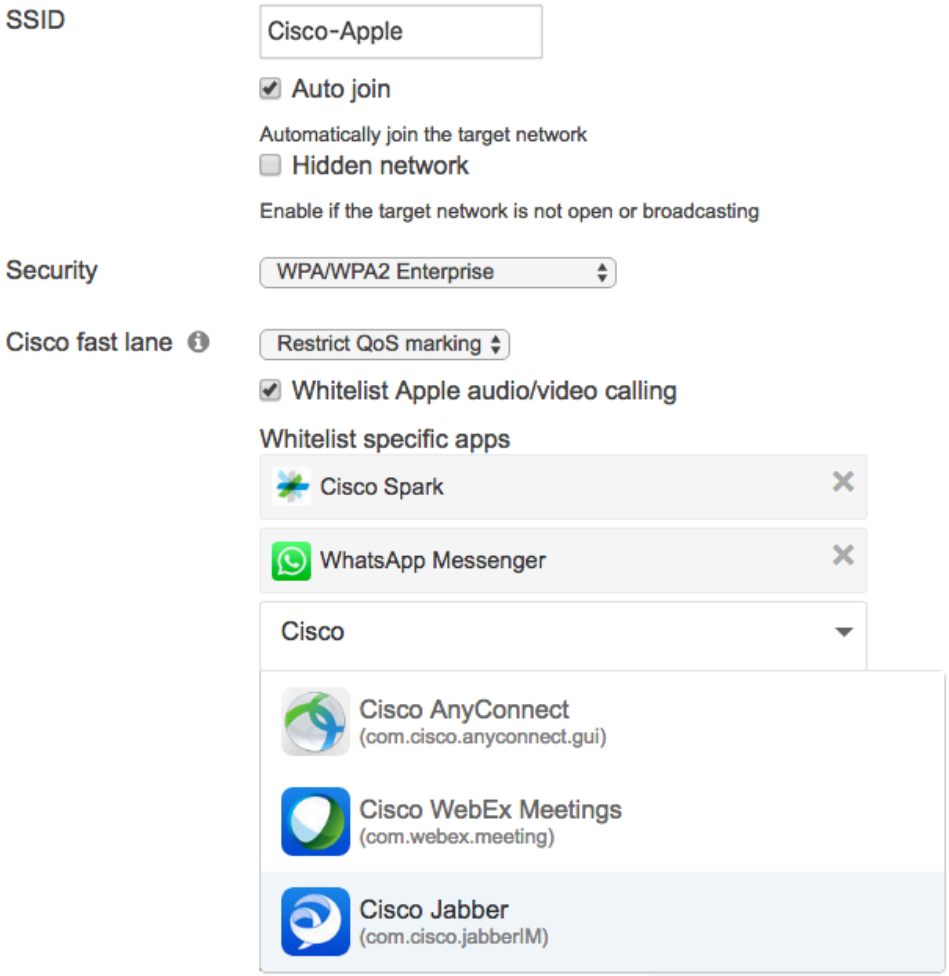
シスコのエンタープライズ モビリティ管理（EMM）ソリューション、Meraki Systems Manager を使用して、モバイル デバイスを管理できます。アップストリーム QoS マーキングを許可される特定のアプリケーションをホワイトリストに登録するために、iOS 10 を実行するデバイスを Fast lane プロファイルでプロビジョニングすることができます（上記の「Fast lane プロファイル」のセクションを参照）。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Fast lane プロファイルは、Meraki ダッシュボードで [システム マネージャ（Systems Manager）] > [MDM] > [設定（Settings）] > [Wi-Fi] の順に移動して、[QoS マーキングの制限（Restrict QoS marking）] オプションを選択することで設定できます。プロファイルは無線でプッシュされ、タグを使用して範囲指定することができます（タグ付けの詳細については以下の注を参照）。Fast lane プロファイルがワイヤレス プロファイルに追加されます。

Systems Manager は Apple App Store に直接統合されており、管理者は、以下の図に示すように、アプリケーションを検索してFast lane プロファイルに直接追加することができます。

図 15. Fast lane の設定とアプリケーションの追加



注: タグ付けに関する一般情報あるいは詳細については、次を参照してください。
https://meraki.cisco.com/products/systems-manager/ [英語]
https://documentation.meraki.com/SM/Tagging [英語]

注: Fast lane プロファイルは、旧バージョンの Systems Manager では使用できません。Systems Manager の新バージョンへのアップグレードに関する詳細については、次のページを参照してください。
https://documentation.meraki.com/zGeneral_Administration/Licensing/Systems_Manager_Licensing#Upgrading_from_Legacy_SM [英語]

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

最適化された EDCA（Enhanced Distribution Channel Access）

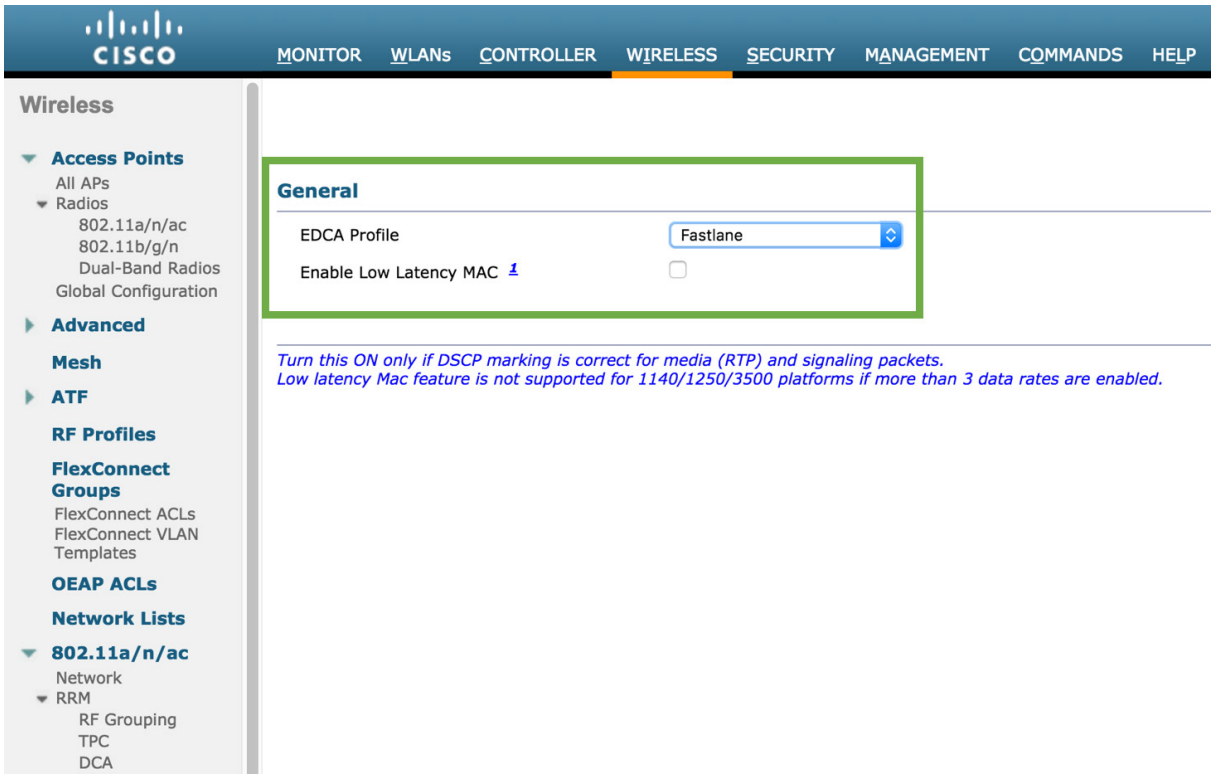
この設定は、AireOS 8.3 以降を実行するシスコ コントローラのみに適用されます。AireOS コントローラは、Fast lane と呼ばれる新しい EDCA プロファイルも実行します。この最適化された EDCA 機能は、802.11 規格における最新バージョンの EDCA に基づいており、シスコのインフラストラクチャに接続するすべてのデバイスにメリットを提供します。

IEEE 802.11e-2005 に基づく前世代の EDCA 設定では、音声およびビデオ キューが消費できる時間には制限がありました。他のキューの消費時間は制限されていませんでした。最新バージョンではトラフィック キューを制御するメカニズムが改善されたことで高速化が可能になり、有効なプロトコルに基づいて消費時間制限値がすべてのキューに割り当てられるようになっています。Cisco WLAN コントローラで最適化された EDCA を有効にすることにより、接続された iOS デバイスおよびその他のクライアントは自動的に新しい 802.11 EDCA 推奨事項を実行し、すべてのセル デバイスにメリットが提供されます。これにより、実際の音声/ビデオ トラフィックに正確な優先順位付けがされ、マーキングのない他のトラフィックが制御される、より良い環境が整います。

最適化された EDCA の設定

AireOS 8.3 以上を実行するコントローラで EDCA パラメータに Fast lane プロファイルを選択することにより、新しい IEEE-802.11 EDCA パラメータを有効化できます。

図 16. EDCA に Fast lane パラメータを設定する



[ワイヤレス（Wireless）] > [802.11a/n/ac] > [EDCA パラメータ（EDCA Parameters）] の順に移動して、EDCA 設定に Fast lane 設定を割り当てます。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

有線スイッチ ポートの設定

インフラストラクチャの有線側も DSCP に対応させて、完全なエンド ツー エンドの優先順位構造を実現する必要があります。アクセス ポイントに接続するスイッチ ポートの QoS 設定では、アクセス ポイントとコントローラの間で交換されるパケットの DSCP を信頼する必要があります。

次の 3750X および 2960 スイッチ ポートの設定例では、ローカル QoS ポリシーに応じて追加できる分類コマンドとキューイング コマンドを示しています。

Cisco 3750X および 2960 の例

ワイヤレス LAN コントローラ EtherChannel スイッチ ポート:

```
interface GigabitEthernet1/0/1
description Wireless LAN Controller Connection port 1
!
interface GigabitEthernet2/0/1
description Wireless LAN Controller Connection port 2
interface range GigabitEthernet 1/0/1, GigabitEthernet 2/0/1
switchport
mls qos trust dscp
srr-queue bandwidth share 1 30 35 5
priority-queue out
channel-group 1 mode on
interface Port-channel 1
description EtherChannel to Wireless LAN Controller
switchport trunk allowed vlan 116, 120, 275
switchport mode trunk
spanning-tree portfast trunk
```

アクセス ポイントのスイッチ ポートの例:

```
interface GigabitEthernet1/0/2
description Access Point Connection Centralized Switching
switchport mode access
switchport access VLAN 100
switchport host
mls qos trust dscp
srr-queue bandwidth share 1 30 35 5
priority-queue out
```

アクセス ポイントの DSCP 値を信頼する上で、アクセス スイッチは WLC によってアクセス ポイントに設定されたポリシーを信頼します。クライアント トラフィックに割り当てられる最大 DSCP 値は、そのアクセス ポイントで WLAN に適用されている QoS ポリシーに基づきます。

注: 有線スイッチ ポートの設定例については、QoS ガイドを参照してください。

http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Oct2015/CVD-Campus_LAN_L2_Access_Simplified_Dist_Deployment-Oct2015.pdf [英語]

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

アプリケーションの可視化と制御

シスコの Application Visibility and Control（AVC）は、ディープ パケット インスペクション（DPI）手法と Network-Based Application Recognition（NBAR）エンジンを使用してアプリケーションを分類し、Wi-Fi ネットワークに対するアプリケーションレベルの可視化と制御を可能にします。コントローラは、AVC を使用して、音声/ビデオ、電子メール、ファイル共有、ゲーム、ピアツーピア アプリケーションなど 1,300 を超えるアプリケーションを検出できます。
AVC では、リアルタイムな分析を行い、ネットワークの輻輳、コストの高いネットワーク リンクの使用、インフラストラクチャのアップグレードを減らすためのポリシーを作成できます。

ビジネス アプリケーションの認識は、次世代 Network-Based Application Recognition（NBAR2）エンジン 13 以降が動作する AVC プロトコル パック 6.4 以降からサポートされます。この機能により、iOS デバイスで実行されるすべてのアプリケーションを正しく識別するとともに、トラフィックのうち、データ、音声、ビデオが占める部分をさらに分類して、それらに異なるポリシーを適用することができます。

注： AVC とプロトコル パックの詳細については、『Application Visibility Control FAQ（Application Visibility Control の FAQ）』ページを参照してください。http://products.mcisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/qa_c67-722538.pdf [英語]

アプリケーションの認識後は、AVC 機能によってデータ トラフィックのドロップ、マーキング、またはレート制限（方向ごと）を実施できます。DSCP がすでに設定されていても、AVC が分類したトラフィックを AVC の値によって可視化することができます。AVC を QoS と統合することにより、アプリケーションの識別に基づいて DSCP 値を使用したトラフィックのマーキングを行うポリシーを作成できます。

iOS デバイスからのトラフィックがワイヤレス コントローラに到達すると、コントローラはディープ パケット インスペクションを実行してフローを認識します。フローが AVC プロファイルに含まれるアプリケーションとして認識されると、トラフィックは AVC ポリシーに従ってマークされます。たとえば、ワイヤレス クライアントがアプリケーション トラフィックを送信する場合、このトラフィックが AP から WLAN コントローラに到達すると、NBAR2 エンジンによってただちに認識され、設定された AVC プロファイルに従って正しく再マーキングされます。

Cisco Jabber を使用する iOS デバイスの AVC 設定例

Cisco Jabber は、すべての iOS デバイスで、コラボレーション アプリケーションとして使用できます。ファイル転送、アプリケーション共有、SIP シグナリング、リアルタイム音声、リアルタイム ビデオ コミュニケーションなど、さまざまなタイプのサービスを提供します。シスコでは、リアルタイム音声には DSCP 46 を、ビデオには DSCP 34 を、シグナリングには 24 を、それぞれ推奨しています。

このセクションでは、例として Jabber トラフィックに対する AVC 設定について説明しています。このセクションでの設定例は、iOS デバイスで使用する WLAN プロファイル向けの Jabber トラフィックのみを対象にしています。Jabber トラフィックはすでに正しくマーキングされているものとします。

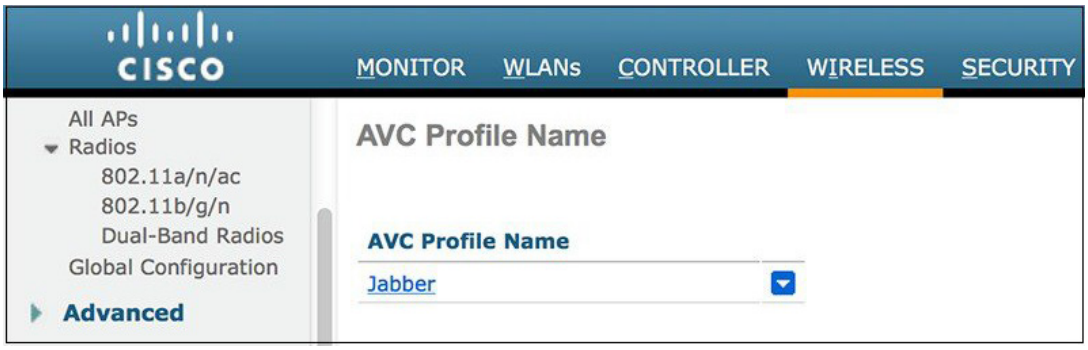
このポリシーにより、パケット パスでマーキングが変更された場合でも正しいマーキングが再確立されます。残りのトラフィックももちろん WLAN 上で許可されますが（同様に順位付けもされる）、残りのトラフィックのマーキングがそのまま据え置かれ、QoS プロファイルの最大値を超えないことが、前提とされます。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

注: AireOS 8.3 以降を実行する Cisco コントローラで Fast lane が有効になっている場合は、自動的に適用される AUTOQOS-AVC_PROFILE にすでに Jabber アプリケーションが含まれています。このセクションで示している手動設定よりも自動プロファイルを使用することを推奨します。

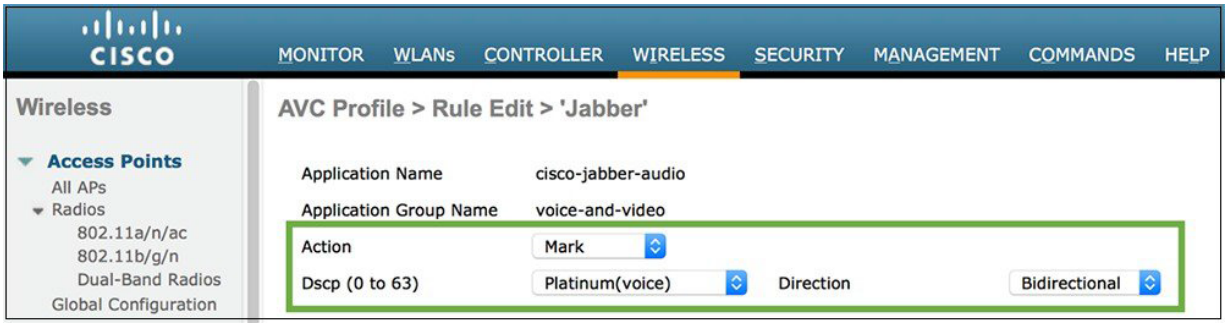
Cisco Jabber トラフィックに Application Visibility and Control を設定するには、次の手順を参照してください。

図 17. Jabber アプリケーション向けの AVC プロファイルの作成



[ワイヤレス（Wireless）] > [Application Visibility and Control] > [AVC プロファイル（AVC Profiles）] の順に移動して、[新規（New）] をクリックします。

図 18. アプリケーション トラフィック タイプをマークするルールを AVC プロファイルに追加する



[ワイヤレス（Wireless）] > [Application Visibility and Control] > [AVC プロファイル（AVC Profiles）] の順に移動して、アプリケーション マーキング ルールを追加するプロファイルをクリックします。

図 19. AVC プロファイルに関連付けるアプリケーション トラフィック タイプのすべてのルールを確認する

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

アプリケーション トラフィック タイプに正しい DSCP マーキングが関連付けられていることを確認します。AVC は、アクション、DSCP 値、トラフィック フローの方向に従ってトラフィックに優先順位を付けます。

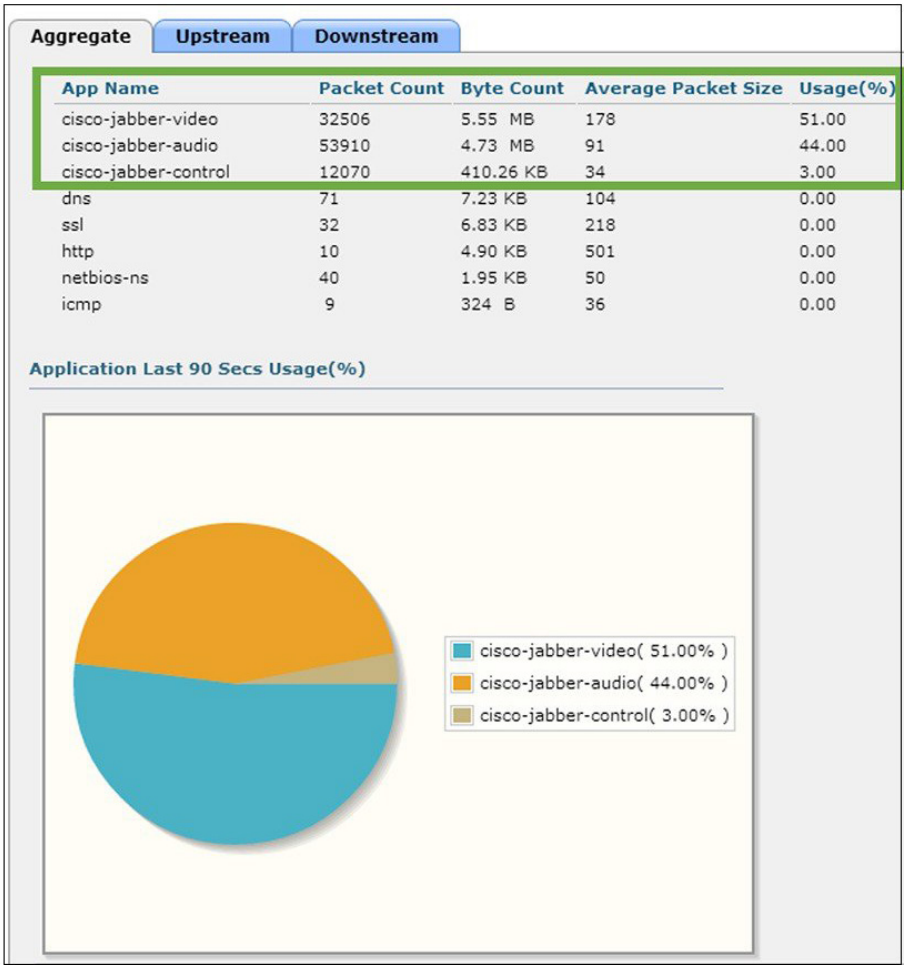
図 20. WLAN 上で AVC を有効にして、AVC プロファイルを適用する

WLAN SSID の [WLANs] > [QoS] タブの順に移動します。[Application Visibility] の [有効（Enabled）] をオンにし、この WLAN に割り当てる作成済み AVC プロファイルを選択します。

これで AVC が有効になり、Jabber AVC プロファイルが設定されるので、シスコ コントローラで、この WLAN のすべての Jabber トラフィックに対する完全な可視化とトラフィック制御が実現されます。設定をテストするには、iOS デバイスを WLAN に接続して、ネットワークで Jabber の音声およびビデオ通話を開始します。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

図 21. アプリケーション トラフィックが AVC によって正しく認識されていることを確認する



アプリケーション トラフィックが AVC によって正しく認識されていることを確認します。同じ WLAN 上の複数のアプリケーションの優先順位を制御するために、ほかのアプリケーションも同じ Jabber プロファイルに含めて、その QoS プライオリティを同様の方法で管理することができます。非常に密度の高い環境において 1 つの WLAN 上で複数のアプリケーションに対して AVC を有効にすると、パフォーマンスへの影響が出る可能性があります。

iOS デバイスのローミング拡張

ローミングは、企業のワイヤレス ネットワークに不可欠な要素です。スマートフォンやタブレットは、ユーザの移動に合わせて AP 間をローミングし、常に Wi-Fi 接続を維持します。企業のローミング拡張というのは、主に、ワイヤレス インフラストラクチャとクライアント デバイスの双方で IEEE 規格ベースの 802.11r、802.11k、および 802.11v 最適化に対応することを意味します。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

表 3. シスコと Apple でのローミング拡張規格のサポート

ローミング拡張規格	シスコでの実装	Apple での実装
802.11r – Fast Transition（FT）	AireOS v7.2	iOS 6
Adaptive 802.11r	AireOS v8.3	iOS 10
802.11k – ネイバー レポート	AireOS v7.4 （v8.0 MR3 以降推奨）	iOS 6 （iOS 8 以降推奨）
802.11v – BSS 移行管理	AireOS v8.0	iOS 7

ローミング動作強化のためのマイナーチェンジは、企業環境のローミング効率をさらに改善するために、iOS 8 から導入されました。これらの最適化により、クライアントは、アプリケーションの中断が最小限に抑えられた状態で、同じネットワーク内の AP 間を移動することが可能になります。

ローミング効率を考慮した企業環境を設定するために、シスコと Apple では、iOS デバイスをサポートするシスコ ワイヤレス LAN インフラストラクチャで、802.11r、802.11k、802.11v を有効にすることを推奨しています。ただし、この推奨が適用されるのは、WLAN 上で想定されるすべてのデバイスが少なくとも 802.11r ローミング拡張規格をサポートしている場合のみと考えてください。ローミング拡張規格をサポートしないクライアントは、ワイヤレス ネットワークへの接続が行われない可能性があります。使用している iOS デバイスの 11r、11k、11v サポート状況を確認するには、Apple のデバイス リスト [英語] を参照してください。

Wi-Fi の世界では、受信信号強度インジケータ（RSSI）が、RF 信号の重要な指標となります。RSSI 値は一般に、負の dBm 値（-72 dBm など）として表されます。RSSI 値が 0 に近づくほど Wi-Fi 信号が強いとみなされます。RSSI 測定値 -65 dBm は -73 dBm より強いので、-65 dBm で接続したクライアントは、-73 dBm で接続された場合よりも Wi-Fi 信号強度が高くなります。ただし、パフォーマンスに関与する要素はほかにも数多く存在するので、必ずしもこれがパフォーマンスやスループットの良し悪しに直結するわけではありません。

iOS デバイスは、特定の RSSI しきい値を使用してローミング スキャニング メカニズムをトリガーします。クライアントが現在の接続を維持するために必要な最小信号レベルが、このトリガーしきい値となります。Apple クライアントは、RSSI がしきい値 -70 dBm を超過するまで、現在の Wi-Fi 接続を監視して維持します。超過すると、iOS は、ローミング先として適切な AP を見つけるためのスキャンを開始します。Apple は、『Wireless Roaming Reference for Enterprise（企業向けワイヤレス ローミング リファレンス）』で、iOS デバイスのローミング ロジックについて詳しく説明しています。

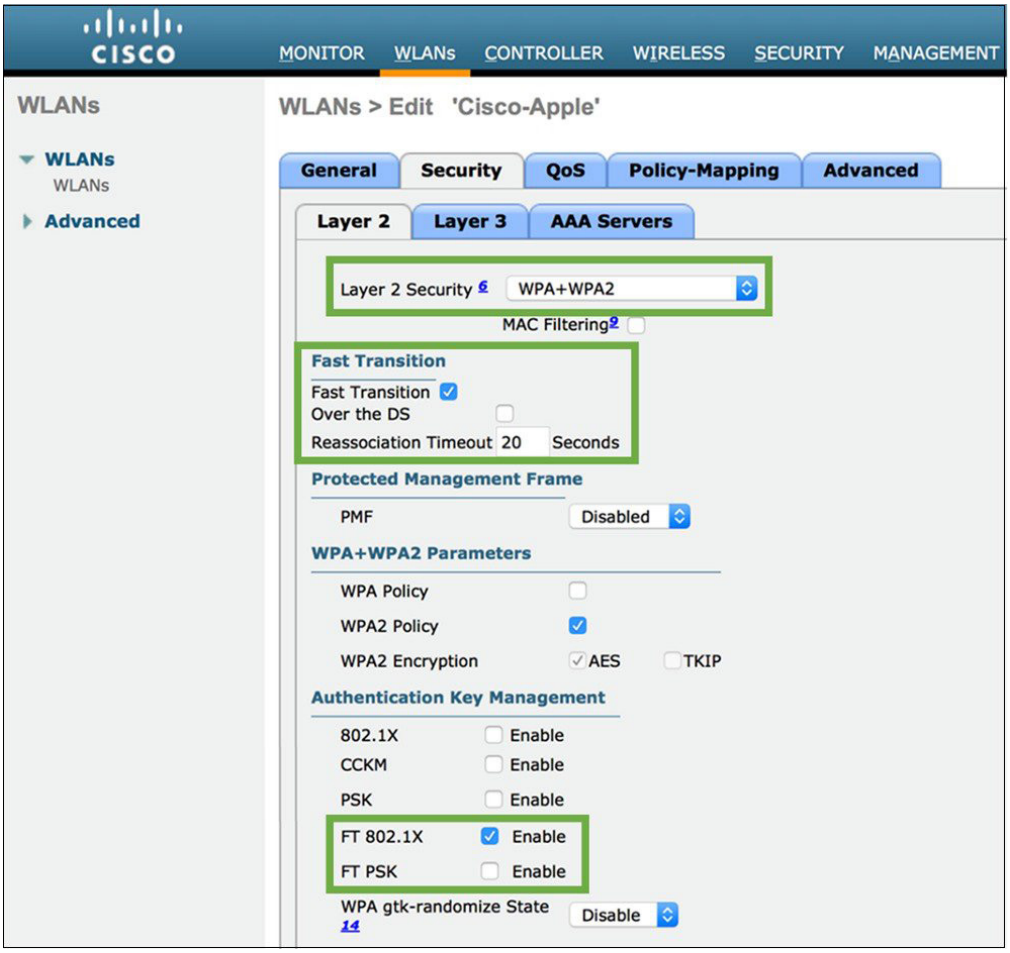
802.11r – Fast Transition

802.11 r は、クライアントが新しい AP に移動するよりも前に新しい AP とのクライアント/AP ハンドシェイクを実行できる拡張規格です。これを Fast Transition（高速移行、FT）と呼びます。この方式では、ワイヤレス クライアントは、最初の AP への接続が確立されたときに WLAN インフラストラクチャに対する初期認証を 1 回だけ行い、同じ FT モビリティドメインの AP 間を移動しながら高速で安全なローミングを実施します。これにより、ローミング中のハンドシェイクに要するオーバーヘッドが大幅に削減され、セキュリティと QoS を維持しながら、AP 間のハンドオフ時間が短縮されます。802.11r はローミング中の遅延の軽減に有効なため、Wi-Fi で音声やビデオなどのリアルタイム アプリケーションを実行するクライアント デバイスに有用です。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

シスコ コントローラで 802.11r を設定する

図 22. WLAN 上で 802.11r - FT を有効にする



WLAN の [WLANs] > [セキュリティ(Security)] タブに移動します(レイヤ 2 のセキュリティは [WPA+WPA2] または [オープン(Open)] にします)。[Fast Transition] を選択して有効化します。[Over-the-DS] モードをオフにし、WLAN に必要なセキュリティ認証に応じて [FT 802.1X] または [FT PSK] を選択します。802.11r では、クレデンシャルがすでにキャッシュされている 11r クライアントと AP との間で交換されるパケットの数が減少します。802.11r を使用する場合、クライアント デバイスを再度接続する前に、次の 2 つのモードでセキュリティと QoS 状態を確立できます。

- Over-the-Air:クライアントが新しい AP と直接パケットを交換します
- Over-the-DS:クライアントは現在の AP を経由してパケットを交換します

[Over-the-DS] をオフにすると、FT は Over-the-Air モードを使用することになります。高密度企業環境の場合、11r - FT パフォーマンスを最適化するために、シスコと Apple は、802.11r を Over-the-Air 移行モードで使用することを推奨しています。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

802.11r を混合モードで設定する

WLC で Fast Transition を有効にすると、「Client that do not support 802.11r will be unable to join the network（802.11r をサポートしていないクライアントはネットワークに接続できません）」という警告を示すポップアップが表示されます。これは、802.11r をサポートしていない一部のラップトップおよびレガシー クライアントに当てはまります。これらのデバイスは、認証中に Fast Transition の情報要素（IE）を処理する方法を認識していないからです。したがって、このようなデバイスは、802.11r 対応 WLAN を確認したり、そこに参加したりすることができない可能性があります。

このような状況に対応するために、「混合モード」が開発されました。このモードは、同じ WLAN 上で FT 非対応と FT 対応の両バージョンの認証モードを有効にできる方式です。混合モードのサポートは、AireOS 8.0 で正式に導入され、これによって、802.11r 対応デバイス用に別の SSID を作成しなければならないという制約がなくなりました。

図 23. 802.11r 混合モードを有効にして、FT 非対応クライアントを同じ WLAN ネットワークに追加可能にする

WLAN の [WLANs] > [セキュリティ（Security）] タブに移動して、FT 認証と非 FT 認証の両方を選択します。たとえば、802.1X と 802.1X FT、あるいは PSK と FT-PSK などを選択します。「802.11r 互換」のアップデート済みワイヤレス LAN ドライバを備えた非 802.11r クライアントは、この 802.11r 混合モード WLAN に接続できます。重要なポイントとして、新しいワイヤレス LAN チップセットを備えたラップトップ クライアントと **11r 互換**のアップデート済みチップセット ドライバは、11r 混合モード SSID 設定に関しては、その重要性に変わりはないことに注意してください。たとえば、Apple は、OS X Maverick v10.9 を実行する MacBook ノート コンピュータ向けの 11r 互換ドライバを導入しました。これにより、MacBook が混合モード SSID（FT-PSK + PSK など）を正しく識別して関連付けできるようになりました。古いバージョンの MacOS を実行している MacBook は（たとえ同じチップセットを搭載していたとしても）、11r 混合モード SSID を確認することはできても接続はできない可能性があります。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

注: シスコと Apple では、11r 混合モード WLAN をネットワークで有効にする前にラボ テストを行うことを推奨しています。混合モードを有効にして新しく作成した WLAN を使用することにより、予期しない動作を回避することができます。既存の WLAN 設定を編集して通常モードまたは FT 限定モードから混合モードに変更すると、以前の接続からのキャッシュ情報が使用される可能性があるため、「11r 互換」クライアント（Apple MacBook など）を接続できない状態が続くという、想定外の結果が生じる可能性があります。既存の Wi-Fi ネットワークの設定を通常モードから混合モードに編集する方法を選択する場合は、回避策として、11r 互換クライアントでそのワイヤレス ネットワークに関する情報を「削除」してから、再接続してください。

11r 互換ドライバが存在していることを確認するために、混合モード SSID を使用する前に、各ベンダーのデバイスをチェックすることをお勧めします。どんなクライアントが 802.11r 対応 WLAN に参加するのか予測できない場合は、非 802.11r クライアント用に別の SSID を作成することをお勧めします。11r 互換とは、そのデバイスが 802.11r 対応であるということを意味するものではないことに注意してください。単に、混合モード SSID を正しく識別して接続ができる機能を備えていることを意味します。

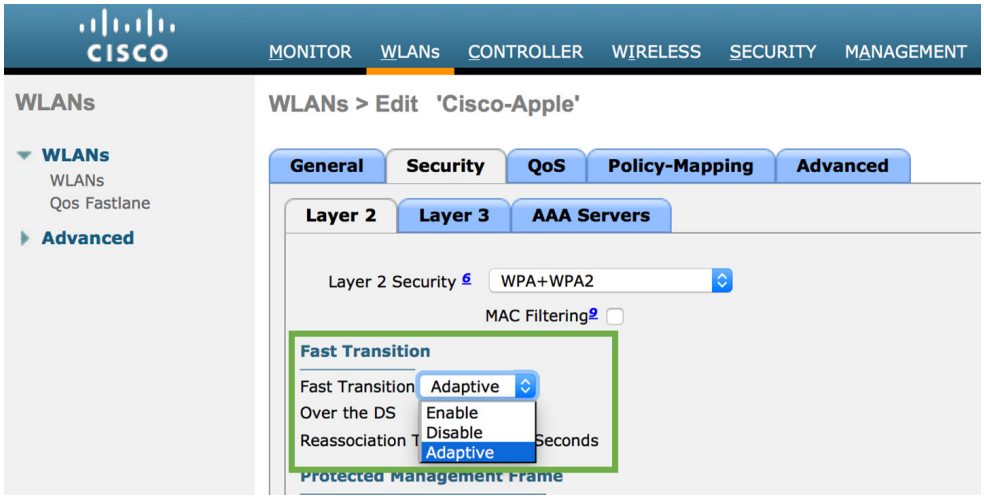
Adaptive 802.11r

設定はすべてのデバイスに適用されますが、Adaptive 802.11r の機能は、iOS 10 以降を実行する iOS デバイスにのみ適用されます。他のすべてのデバイスには、標準の WPA2 を使用した接続が可能です。

Adaptive 802.11r は、接続を最適化するために Cisco WLAN インフラストラクチャに接続する iOS デバイス用に特化して設計された拡張機能です。Adaptive 802.11r に Cisco AireOS 8.3 以上を設定すると、iOS 10 以降を実行するすべての iOS デバイスは、Cisco AP に接続すると同時に、自動的に 802.11r を実行します。ワイヤレス ネットワーク設定で 11r が有効化されていないときも同じです。

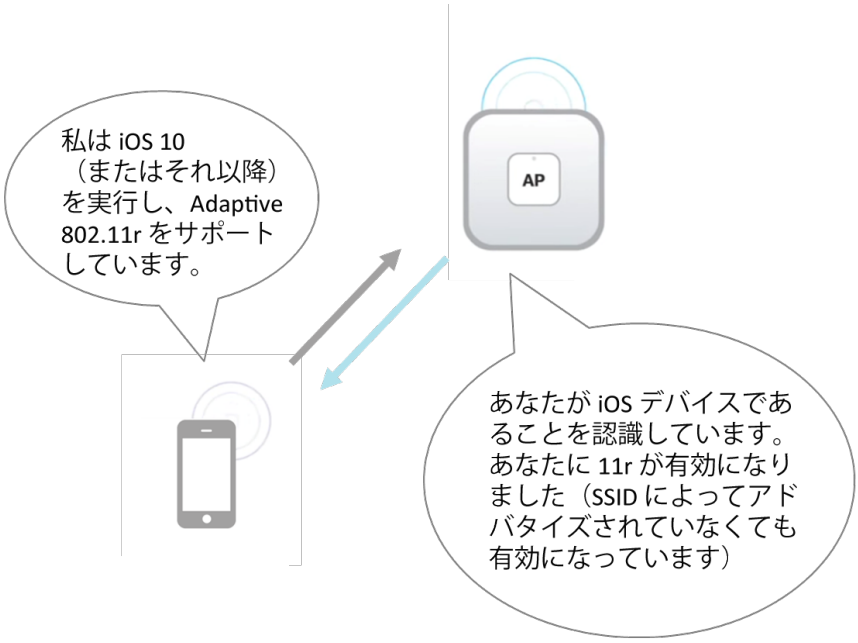
注: Adaptive 802.11r をサポートしている iOS デバイスは、iPhone 6S、6S Plus、iPhone 7、iPhone SE、iPad Pro です。

図 24. WLAN で Adaptive 802.11r を有効化



© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

図 25. iOS 10 以降を実行する iOS デバイスは、Adaptive 802.11r を設定された 8.3 以上を実行するコントローラから、Adaptive 802.11r 設定を自動的に受信



WLAN でAdaptive 802.11r が有効になると、AP はビーコンで情報を提供します。iOS 10 デバイスからのアソシエーション要求では、デバイスがアソシエーション要求を開始するよりも前に Adaptive 802.11r 設定を認識しているので、802.11r が自動的に要求されます。AP は、ドメインおよび Fast BSS 移行（802.11r）パラメータを示すことで 802.11r を確認するアソシエーション応答を提供します。

802.11k - 無線測定とネイバー レポート

802.11k 規格を使用すると、クライアントは、ローミングの候補となる既知のネイバー AP 情報を含むレポートを要求できます。要求は、アクション フレームと呼ばれる 802.11 管理フレームの形式になります。AP は、同じ WLAN 上にあるネイバー AP の Wi-Fi チャネル番号が付いたリストを使用して応答します。AP の応答もアクション フレームの形式で行われます。AP から 802.11k 応答フレームを受信すると、クライアントは、次回のローミングの前にスキャンする最適なチャネル候補を認識します。この便利なネイバー リストのおかげで、クライアントは、次のローミング機会にアプローチする際、報告されたこれらのチャネルを最初に戦略的に調査し、それによってスキャン時間を短縮して、どの AP に移動すべきかをすぐに判断することができます。

802.11k サポートが正式に導入されたのは、シスコでは AireOS 7.4、Apple では iOS 6 からでしたが、Apple に関しては、ネイバー リスト要求プロセスを改善するために Apple iOS 8 でいくつかの設計変更が実施されました。その変更は、シスコの AireOS v8.0 MR3 および v8.1 MR1 リリースに統合されています。シスコと Apple では、802.11k には AireOS v8.0 MR3 以上のコントローラ コードおよび iOS 8 以上にアップデート済みの iOS デバイスを使用することを推奨しています。AireOS 8.3 以上では、WLAN ネットワークで Fast lane を有効にすると、ネットワーク SSID で 802.11k が自動的に有効になります。

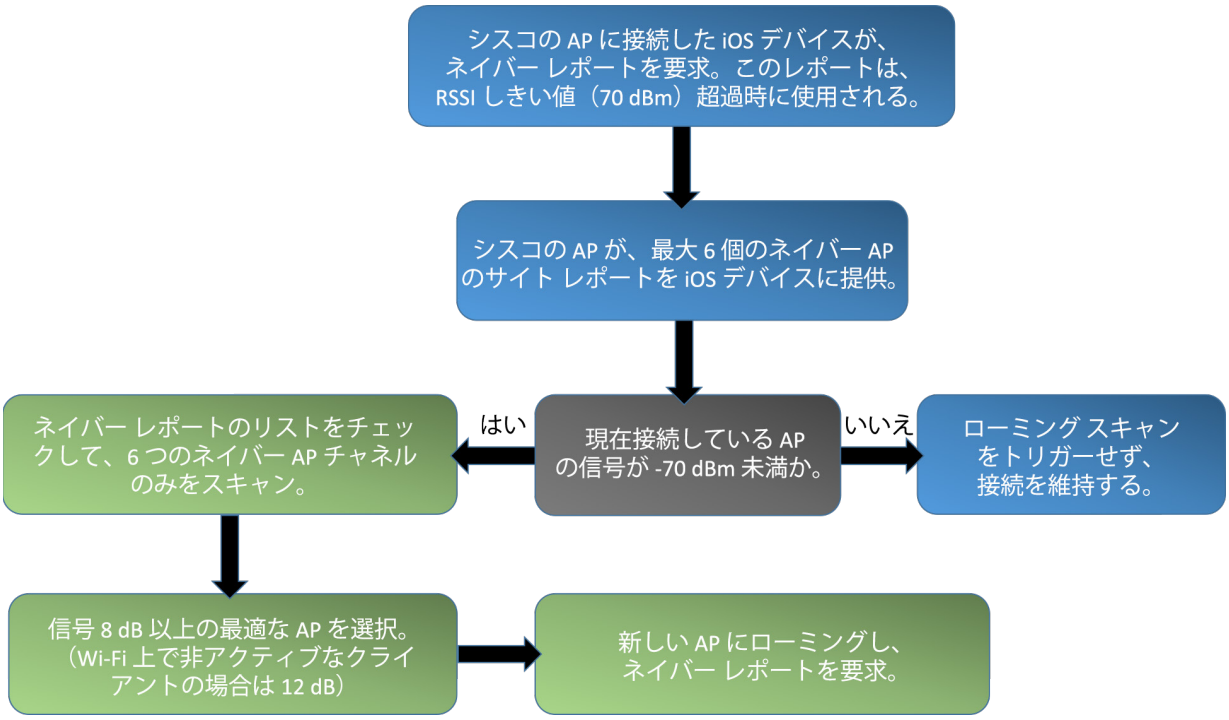
シスコのインフラストラクチャでは、802.11k アルゴリズムが RRM を使用して、クライアントが接続している AP のネイバーを判定し、どの AP がクライアントをヒアリングしたかチェックします。次に AP が、最適な 6 つの AP のリストをクライアントに返します。ネイバー リスト情報があるため、11k 対応クライアントは、すべてのチャネルをスキャンしてローミング先 AP を検索する必要がありません。すべてのチャネルをスキャンする必要がな

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

いためチャネル使用率も低下し、チャネルでの通信時間の短縮につながります。さらに、デバイスが各チャネルのスキャニングのために無線設定を頻繁に変更したり、各チャネルでプローブ要求を送信したりしないため、iOS デバイスのバッテリ寿命の面でもメリットがあります。

また、デバイスがすべてのプローブ応答フレームを処理する必要がなくなります。ビーコンをリスニングするオフチャネルのパッシブ スキャンによって接続が中断される時間も短縮されます。

図 26. 802.11k（iOS 8 以降）をサポートする iOS デバイスのネイバー レポート処理フロー



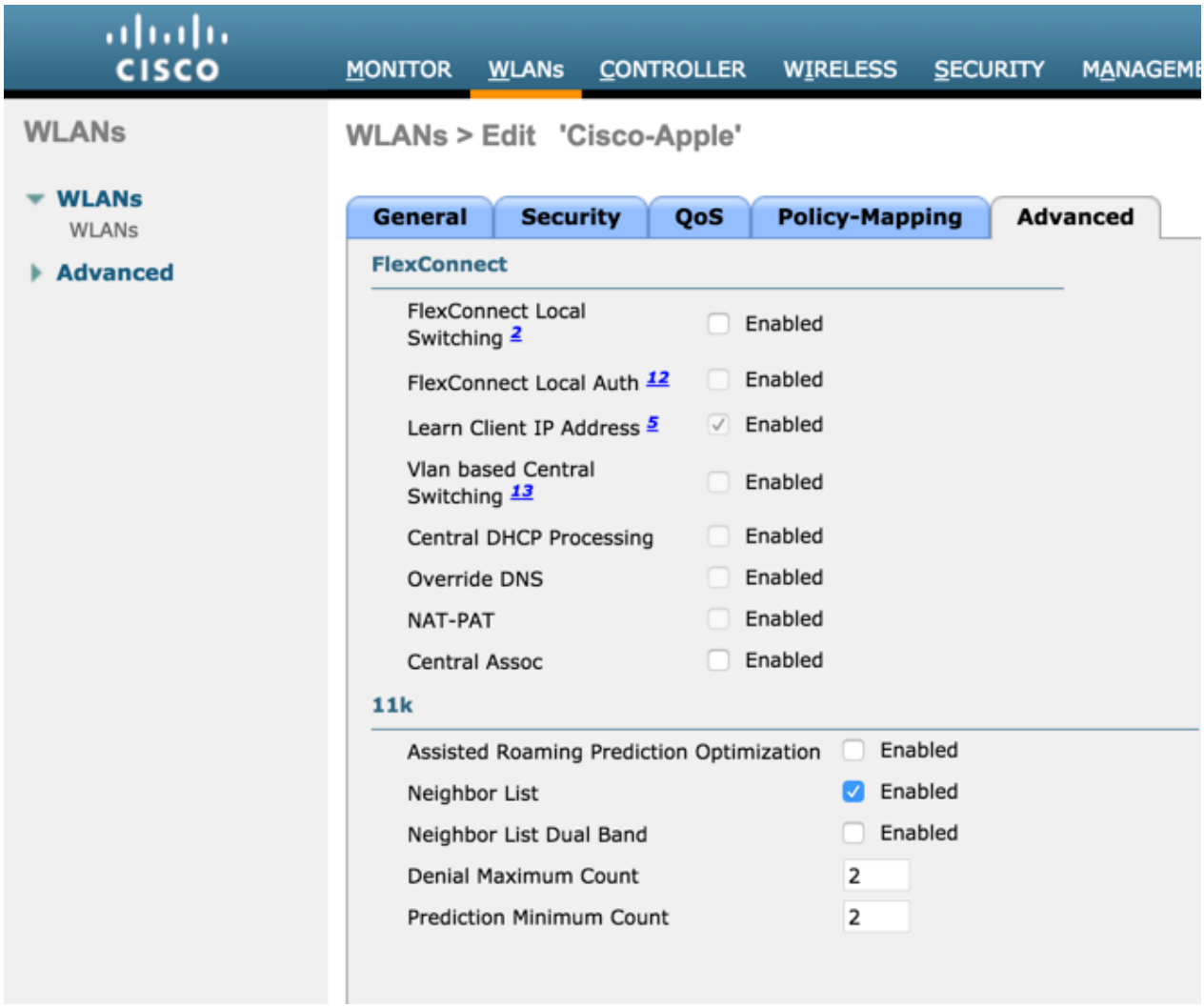
注: 詳細については、『Apple iPhone roaming behavior and optimization guide（Apple iPhone のローミング動作および最適化ガイド）』を参照してください。http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/iPhone_roam/b_iPhone-roaming.html [英語]

802.11k を使用して、デバイスの潜在的ローミング（接続）先とする AP を検出して確定することは、プロセスのほんの一部に過ぎません。この後 iOS デバイスは、ユーザ側のサービス中断が最小限に抑えられるよう、認証プロセスを迅速に完了する必要があります。このプロセスで、iOS デバイスは、新しい AP の認証を行い、現在の AP の認証を解除します。WLAN で 802.11r および 802.11k を同時に有効にすると、ローミング プロセスを迅速化する効果が得られます。11r および 11k を同時に実行することにより、iOS デバイスは、スキャン時間を短縮できるだけでなく、潜在的なアクセス ポイントに対する事前認証も実行できるため、認証時間が短縮され、新しい AP へのローミングが迅速に完了します。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

シスコ コントローラで 802.11k を設定する

図 27. WLAN でネイバー レポートを有効にする



WLAN の [WLANs] > [詳細設定（Advanced）] タブに移動した後、下方向にスクロールして [11k] セクションまで移動します。[ネイバー リスト（Neighbor List）] の [有効（Enabled）] を選択して 802.11k ネイバー レポートを有効にします。これは 5 GHz 限定の WLAN であるため、デュアル バンド ネイバー リストは必要ありません。802.11k は、AireOS コード リリース 8.3 以降ではデフォルトで有効になっています。

802.11v – Basic Service Set（BSS）移行管理

802.11v Basic Service Set（BSS）移行管理はワイヤレス ネットワーク管理機能（WNM）の一部であり、クライアントとインフラストラクチャが運用情報を交換するためのプラットフォームとして機能し、どちらの側でも WLAN 状態の追加認識ができるようにしています。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

802.11v は、ネットワーク経由のローミング拡張機能をクライアント デバイスに提供します。この機能では、AP が、非要請推奨をクライアントへの要求という形で提供することによりローミングの決定をサポートしようとします。この要求には、クライアントのローミング先候補となる最適な AP の提案が含まれます。クライアント デバイスとインフラストラクチャはどちらも、WNM を使って運用情報を交換し、WLAN 状態を追加認識します。クライアントは AP からのアドバイスを受け入れることも、拒否することもできますが、追加認識によって、自己修正イベントおよびアクションを実行するための強固な基盤を構築する支援を受けることができます。

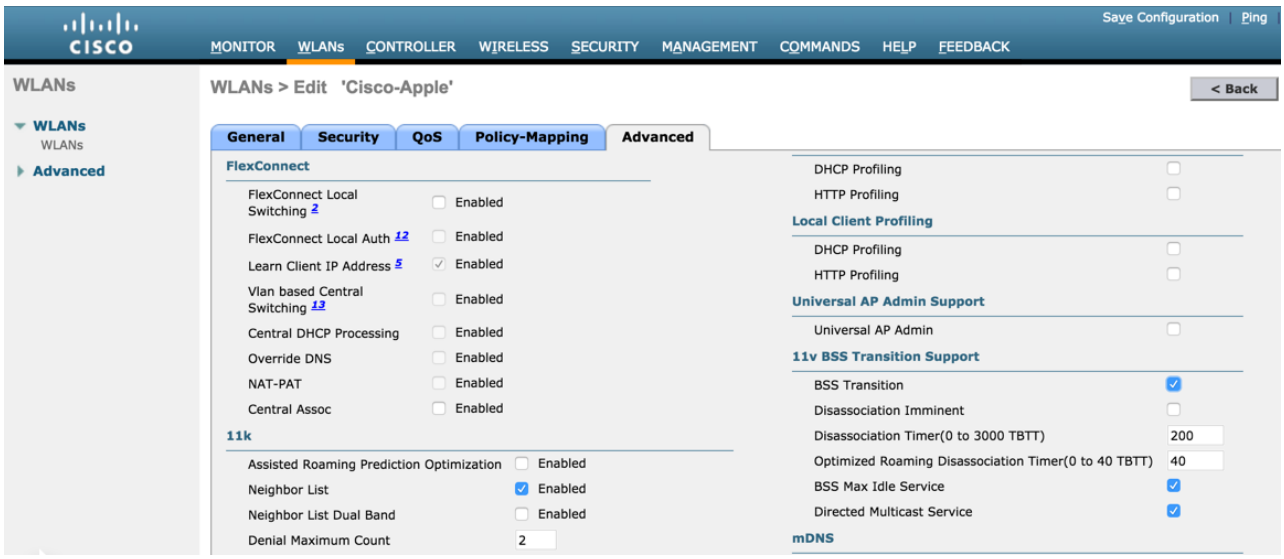
802.11v BSS 移行管理は 3 種類のフレーム セットで機能します。

- BSS 移行管理クエリ：クライアントから AP に送信されます
- BSS 移行管理要求：AP からクライアントに送信されます
- BSS 移行管理応答：クライアントから AP に送信されますが、これが実行されるのは、BSS 移行管理要求後に限られます

802.11v をサポートする iOS デバイスは、AP からの BSS 移行管理クエリに応答し、提供された優先 AP のリストを使用してローミング先を決めることができます。この優先 AP リストは 802.11k 交換で取得されるネイバー AP リストとは異なる可能性があるので注意してください。802.11k では、iOS デバイスがネイバー リストを要求するのは接続または再接続を実行する時だけですが、BSS 移行管理クエリはそれとは異なり、いつでも送信できます。まず、クライアントが、ローミング先として適している AP の推奨を要求するという、要請方式（BSS 移行管理クエリ経由）で行うか、接続状況が良くない場合には、特定の AP へのローミングを求めるクライアントに対して AP が応答、または非要請要求を提供するという方式（BSS 移行管理要求経由）で行うことができます。Cisco AP からの BSS 移行管理要求のトリガーは、ロードバランシング イベントなど、他の原因でも発生することがあります。この要求を受諾/拒否することが、BSS 移行管理応答の主要な役割です。クライアントは、受諾または拒否の理由コードを含めることもできます。重要なポイントとして、要求への応答は任意であるということに注意してください。

シスコ コントローラで 802.11v を設定する

図 28. シスコ コントローラで 802.11v BSS 移行管理を有効にする



WLAN の [WLANs] > [詳細設定（Advanced）] タブに移動した後、下方向にスクロールして [11v] セクションまで移動します。[BSS 移行（BSS Transition）] を選択して Cisco AP での 11v BSS 移行管理サポートを有効にします。802.11v BSS 移行は、AireOS コード リリース 8.3MR1 以降ではデフォルトで有効になっています。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

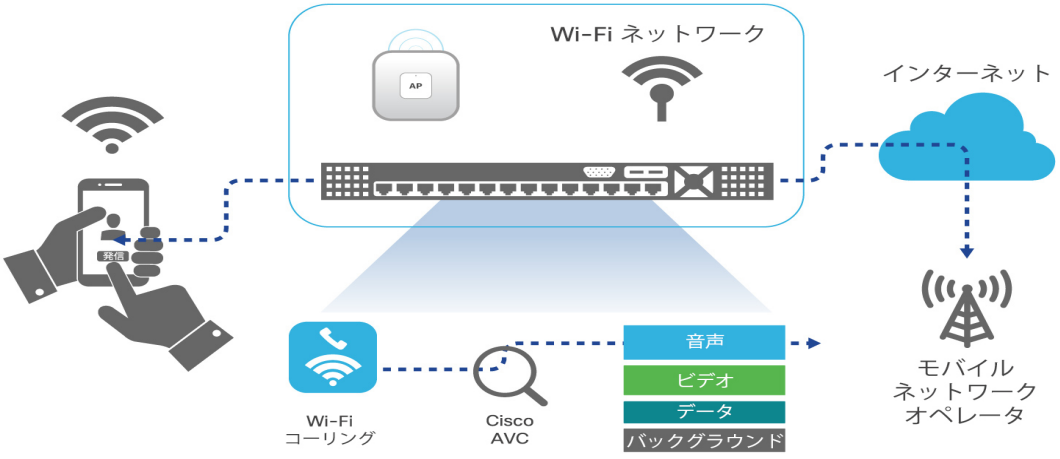
[接続解除通知（Disassociation Imminent）] は、BSS 移行サポート機能のオプションのアドオンです。これは、AP との接続が切れるまでの残り時間が [接続解除タイマー（Disassociation Timer）] フィールドで指定した時間に達したときにクライアントに通知を送るために使用されます。[接続解除タイマー（Disassociation Timer）] は、ビーコン間隔の数で表されます。[接続解除タイマー（Disassociation Timer）] がゼロに達すると、AP はその後いつでも強制的にクライアントの接続を解除できます。

Cisco WLAN での iOS デバイスによる Wi-Fi コーリング

Apple は、2014 年 9 月の iOS 8 アップデートで複数の iPhone モデル（iPhone 5c 以降）に Wi-Fi コーリングを導入し、それ以来、主要なネットワーク通信事業者を順次 Wi-Fi コーリング サービス提供者として追加しています。iOS 9 アップデートでは、さらに多くのネットワーク通信事業者が Wi-Fi コーリング サポート事業者のリストに追加されました。拡張 Wi-Fi コーリング サービスでは、ユーザが、別の iOS デバイスから直接 Wi-Fi コールを行うことができます。企業環境での Wi-Fi コーリングには、ワイヤレス ネットワークの最適化が重要になります。

Wi-Fi コーリングを有効にすると、iPhone は通信事業者のネットワーク サーバとの IPsec 接続を確立します。この初期接続トラフィックは、ベスト エフォート モードで送信されます。この後、iPhone からの音声トラフィックはすべて、音声優先順位（UP6）が設定され、暗号ペイロード（ESP）内で送信されます。iOS 10 以降を実行している iOS デバイスでは、アップストリーム Wi-Fi コーリング パケットも DSCP 46（EF）としてマーキングされます。

図 29. Cisco AVC による Cisco WLAN 経由の Wi-Fi コーリングの最適化



ほとんどのサービス プロバイダーのネットワークでは、iPhone へのダウンリンク トラフィックは、デフォルトのコントローラ設定により、ベスト エフォート優先順位で送信されます。WLAN にプラチナ QoS や AVC を使うと、すべての Wi-Fi コーリング音声トラフィックを効率的に分類して優先順位を付けることができます。Wi-Fi コーリングは、AVC Protocol Pack 15 に分類される新しいアプリケーションの 1 つです。

iOS 10 では、QoS プロファイルを使用すると、Wi-Fi コーリングは常にデフォルトでホワイトリスト登録されます。ホワイトリストからアプリケーションの名前を除いただけでは、Wi-Fi コーリングをベスト エフォート キューに送ることはできません。ネットワーク設定の関係上 Wi-Fi コーリングを音声トラフィックとして送信できない場合は、QoSMarkingAppleAudioVideoCalls を 0 に設定して QoS プロファイルを iOS 10 デバイスにプッシュす

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

ることにより、Wi-Fi コーリングの QoS を無効化できます。ほとんどのネットワークでは、Wi-Fi コーリングは有効な音声アプリケーションと見なされ、そのマーキングが維持されます。

Wi-Fi Calling の設計にあたっては、AP セル サイズ、データ レート、導入密度、ローミング拡張規格（802.11r/k/v）など、注意すべき重要な考慮事項があります。WLAN 設定に関しては、WLAN に WMM を設定し、QoS はプラチナ、分類は AVC をそれぞれ指定します。

注： 詳細については、『Cisco VoWi-Fi Network Design（Cisco VoWi-Fi ネットワーク設計）』を参照してください。http://www.cisco.com/c/en/us/solutions/collateral/service-provider/service-provider-wi-fi/white-paper-c11-733914.html [英語]

Cisco WLAN での Bonjour

Bonjour は、ゼロ コンフィギュレーション ネットワーキングとして知られ、プリンタなどのデバイスや他のコンピュータの場所、およびそれらのデバイスがローカル ネットワークで提供するサービスの場所を、マルチキャスト ドメイン ネーム システム（mDNS）サービス レコードを使用して特定することができます。

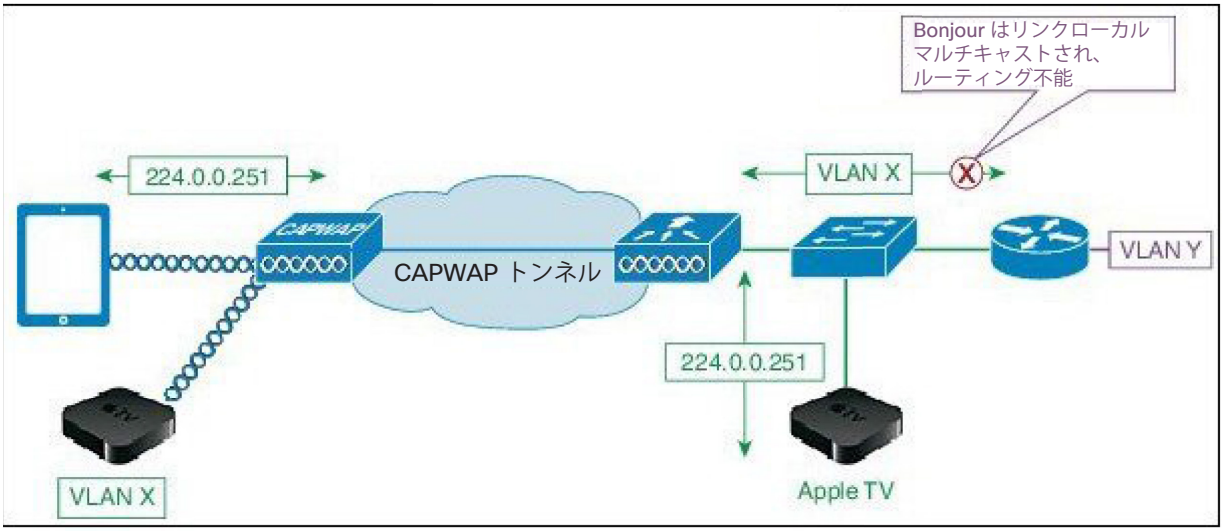
Bonjour プロトコルは、サービス通知やサービス クエリを受けて作動し、それによってデバイスは下記のような特定のアプリケーションに対するクエリとアドバタイズを行うことができます。

- 印刷サービス
- ファイル共有サービス
- リモート デスクトップ サービス
- iTunes ファイル共有
- iTunes ワイヤレス iOS デバイス同期（iOS v5 以降）
- AirPlay（下記のストリーミング サービスを提供）
    - 音楽ブロードキャスティング（iOS v4.2 以降）
    - ビデオ ブロードキャスティング（iOS v4.3 以降）
    - 全画面ミラーリング（iOS v5 以降、iPad 2、iPhone4s 以降）

各クエリまたはアドバタイズメントが Bonjour マルチキャスト アドレスに送信されると、サブネット上のすべてのクライアントに配信されます。Apple の Bonjour プロトコルは、UDP ポート 5353 で動作するマルチキャスト DNS（mDNS）を使用して、予約済みグループ アドレスに送信します。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

図 30. Cisco WLAN での Apple TV 向け Bonjour サービス



注: 詳細については、『Cisco v8.0 Bonjour Deployment Guide（Cisco v8.0 Bonjour 導入ガイド）』をご覧ください。http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/WLAN-Bonjour-DG.htmll [英語]

ワイヤレス環境の把握

iOS デバイス向けベスト プラクティスを参考にして Cisco WLAN を設計することに加え、ネットワークのメンテナンスおよび監視を行うことで、ネットワーク全体の健全性の追跡に役立ちます。iOS デバイスのアプリケーションおよびローミングのパフォーマンスは、AP カバレッジや Wi-Fi チャネル帯域幅に大きく依存します。シスコ コントローラのユーザ インターフェイスは、AP および RF 環境の重要な統計情報を細かく追跡するのに必要なデータを提供します。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

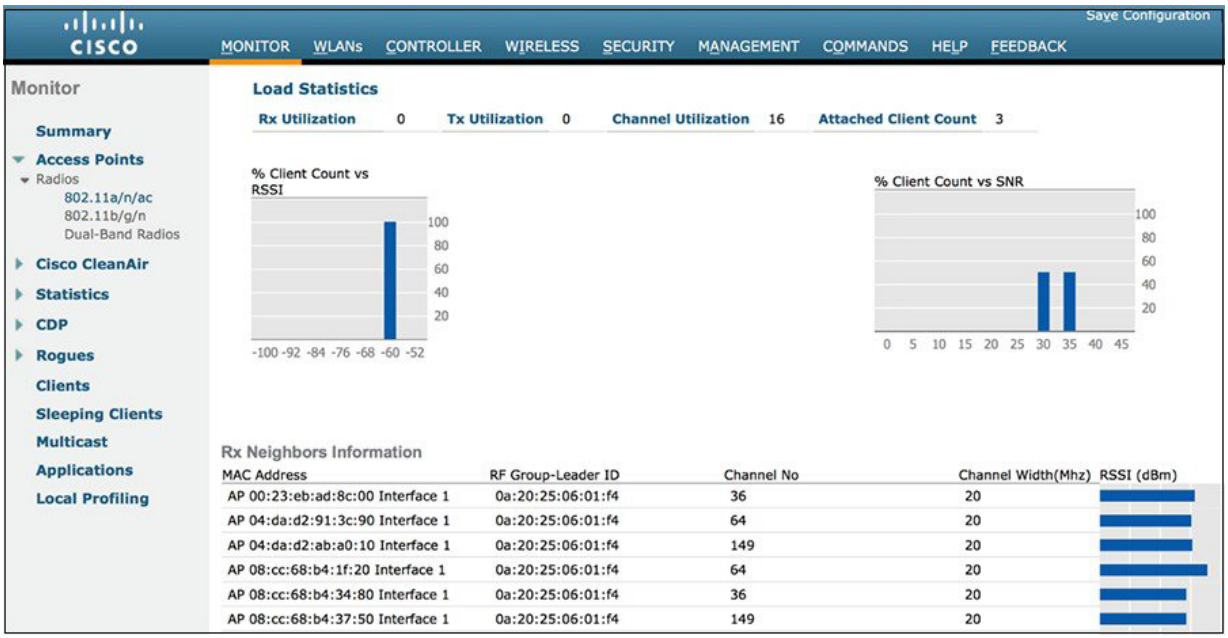
図 31. AP の統計情報をチェックして RF 環境を監視する

[監視（Monitor）] > [アクセス ポイント（Access Points）] > [無線（Radios）] > [802.11a/n/ac] の順に移動して、右側のオプション ボタンをクリックし、[ノイズ プロファイル（Noise Profile）]、[干渉（Interference）]、[カバレッジ（Coverage）] などの詳細を選択します。

データには、Wi-Fi チャネル番号、そのチャネルの干渉（赤）、現行チャネルの負荷に関する統計情報（青）、Voice over IP（VoIP）コール数などが含まれます。また、[RSSI に対するクライアント数（Client Count vs RSSI）] および [SNR に対するクライアント数（Client Count vs SNR）] といったその他のクライアント関連情報も含まれます。この情報を使用して、iOS デバイスのデータ レート能力や、関連付けられたクライアントの RSSI や SNR を考慮した実使用データ レート推定値などを分析できます。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

図 32. RSSI/SNR に対するクライアント数や AP ネイバー RSSI の監視



クライアントに関する情報としてはこのほかに [Rx ネイバー情報（Rx Neighbors Information）] もあり、この情報を使用して、iOS デバイスが接続している AP のネイバー AP 間にどの程度のカバレッジ オーバーラップがあるかを迅速に把握することができます。

接続したデバイスの監視

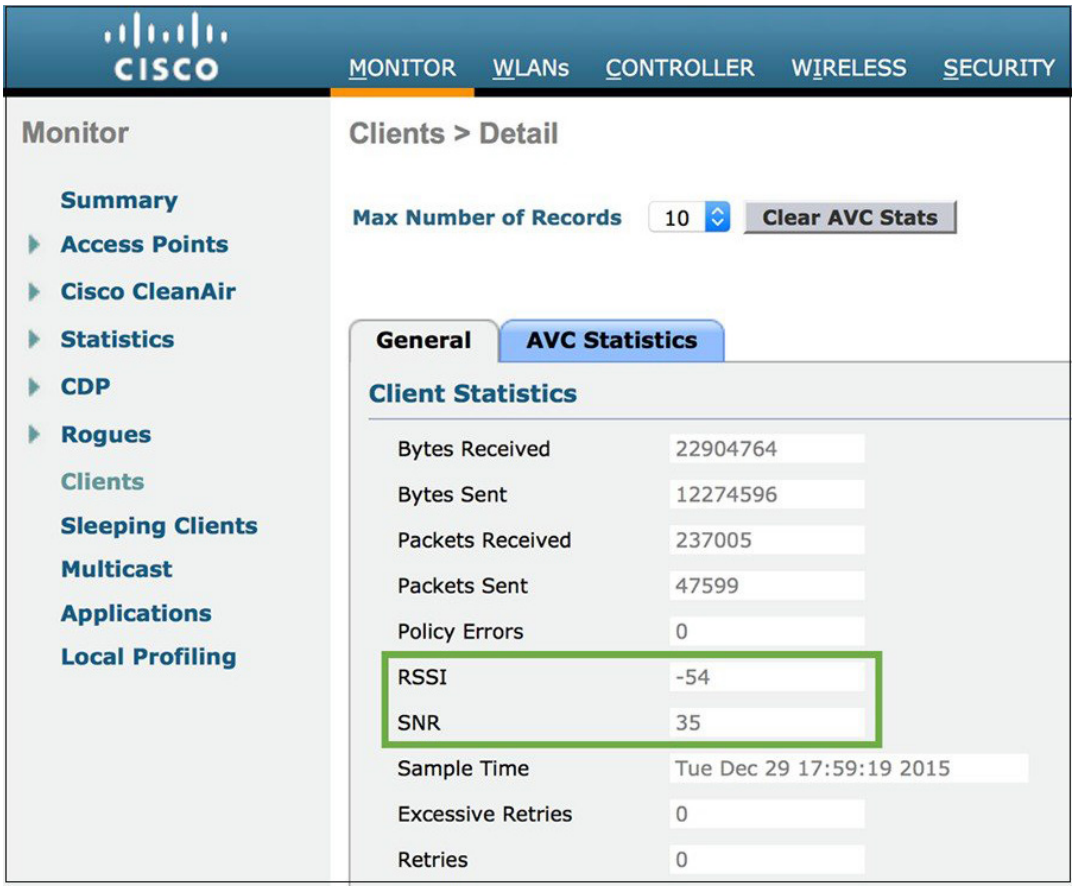
Wi-Fi 環境を把握するために次に確認すべき要素は、iOS デバイスの接続状態です。シスコ コントローラのユーザ インターフェイスでは、デバイスごとに情報ウィンドウが用意されています。この情報は、データベースで提供されており、デバイスの Wi-Fi MAC アドレスでアクセスできます。iOS デバイスの MAC アドレスの検索を行うには、iOS デバイスで [設定（Settings）] をタップして、[一般情報（General）] > [デバイスについて（About）] > [Wi-Fi アドレス（Wi-Fi Address）] の順に移動します。

個々のクライアント情報のページには、クライアントの MAC アドレス、クライアントが接続している AP の名前、WLAN SSID、802.11 プロトコルが表示されます。各行の最後にドロップダウン メニュー ボタンがあります。このメニュー ボタンを選択すると、iOS デバイスの現在の接続ステータスを示す新しいウィンドウが表示されます。情報には、クライアントと AP のプロパティが含まれています。クライアントのプロパティには、IPv4 および IPv6 アドレス、VLAN ID、現行データ レート設定、セキュリティ情報、QoS プロパティが含まれます。

[クライアント（Clients）] ページでは、その他の重要な Wi-Fi 統計情報も収集できます。[RSSI] フィールドでは、AP で受信したパケットの信号強度が表示され、AP によるクライアント パケットの認識の程度が示されます。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

図 33. クライアントの RSSI および SNR 統計情報の監視



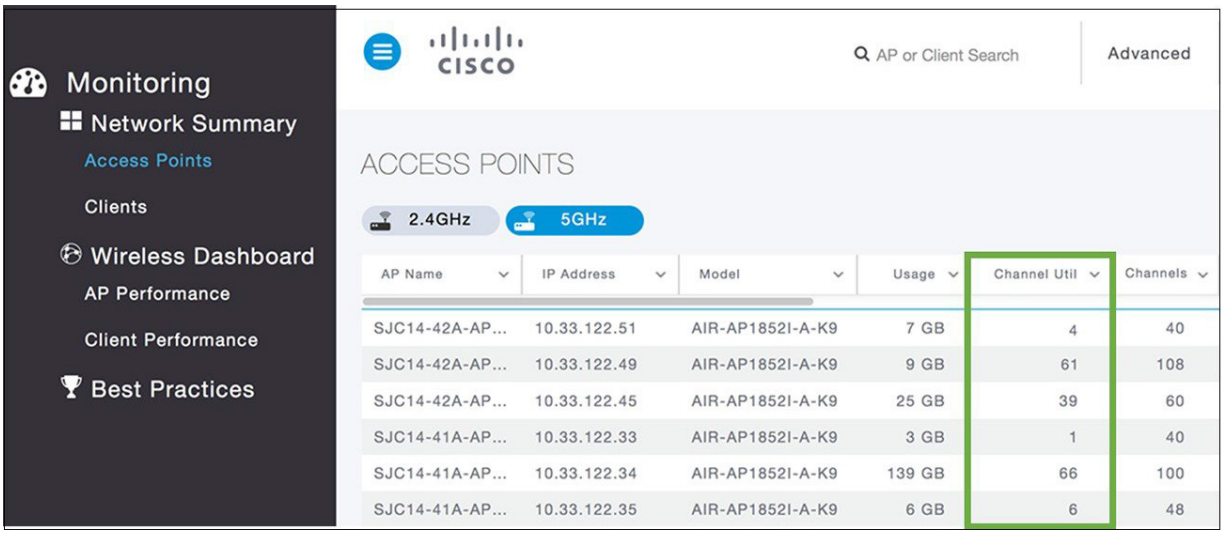
たとえば、RSSI 値が -45 dBm の場合、AP は、-67 dBm のときよりも強い信号でクライアントを認識できることになります。RSSI 値はカバレッジ品質を知るためにも重要です。値が低すぎる場合は、接続状態が悪いことを示している可能性があります。この値は、AP の数を増やす必要性や、AP の状態を改善する必要性を示す指標にもなります。

チャネルの使用率

電話が AP から離れると信号強度が低下しますが、それを補うためにデータ レートは低い値にシフトします。これは、より信頼性の高いパケット配信を実現できますが、その一方でデバイスのスループットは減少し、デバイスが使用する通信時間が増加します。消費する通信時間が増加すると、そのほかのデバイスが利用できる Wi-Fi セルの全体的な帯域幅が減少します。使用可能なチャネル帯域幅は、チャネル使用率を監視することで判定できます。RSSI とチャネル使用率は、iOS デバイスの全体的な接続性を評価する主要な要素です。Wi-Fi チャネルは、接続を通じて、デバイスと AP で共有されます。

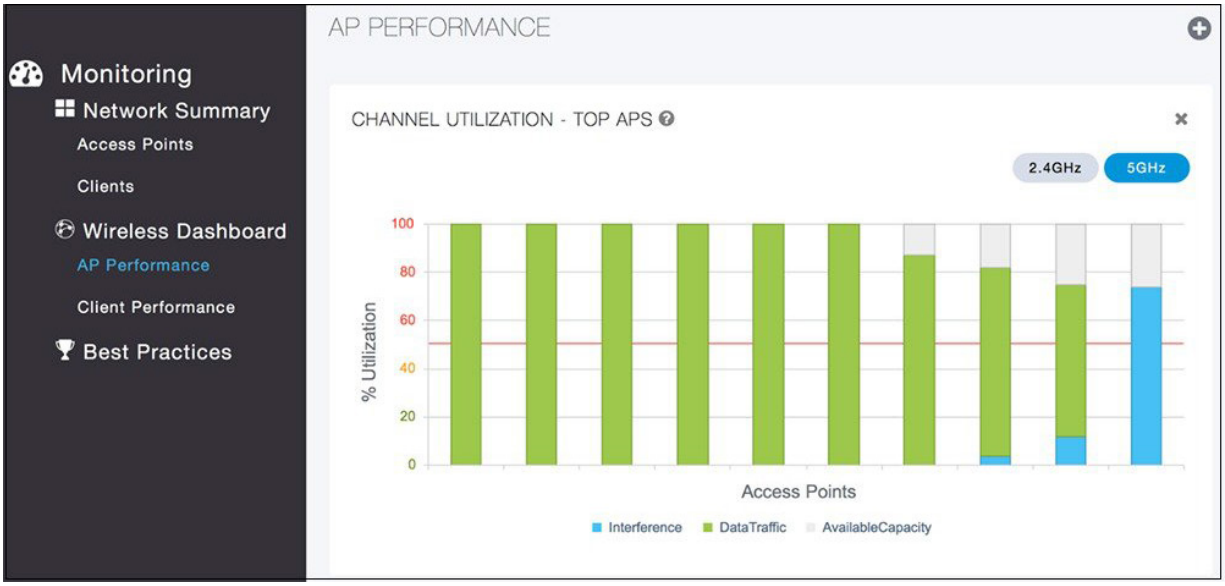
© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

図 34. AireOS v8.1 以降で監視ダッシュボードを使用して、すべての AP の [チャネル使用率（Channel Utilization）] を確認する



[チャネル使用率（Channel Utilization）] は、AP の無線統計情報のページに表示されるチャネル負荷統計情報の 1 つです。

図 35. [チャネル使用率（Channel Utilization）] を確認して、チャネル使用率の最も高い AP を特定する



AireOS 8.1 以上で、[監視（Monitoring）] > [ワイヤレス ダッシュボード（Wireless Dashboard）] > [AP パフォーマンス（AP Performance）] の順に移動して、チャネル使用率グラフを表示します。

Wi-Fi チャネルは、別の AP（自身の AP および同じチャネルで動作する他の AP の両方）や他のデバイス（Wi-Fi および非 Wi-Fi の両方を含む）とも共有されます。チャネルを共有する他の Wi-Fi デバイスはチャネル使用率に影響を与える要素となります。同一チャネル干渉のレベルが、同じチャネル上の AP からのヒアリングが可能な程度だからです。非 Wi-Fi 干渉源も、チャネル使用率に影響します。非 Wi-Fi 干渉源としては、Bluetooth デバイス、電子レンジ、DECT 方式の電話、監視ビデオ カメラなどのほか、802.11 プロトコルは使

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

用しないが Wi-Fi チャネルと同じ無線周波数を使用するあらゆるデバイスが挙げられます。チャネル使用率を適切な値に維持するためには、パーソナル ホットスポットおよび非 Wi-Fi 干渉源を含む不正 Wi-Fi デバイスを可能なかぎり管理する必要があります。

ピアツーピア アクティビティの監視

RF チャネルのレイアウト、計画、および関連する企業ワイヤレス ネットワーク設計に加えて、考慮すべきもう 1 つの要素があります。それは、新しい iOS デバイスの役割と潜在的影響、および、企業ネットワークにおけるデバイスのピアツーピア アクティビティです。Apple TV ソフトウェア バージョン 7 以降を実行する Apple TV の第 3 世代 Rev.A の時点で、AirPlay に新しい方式のピアツーピアが導入されています。これにより、互換性のある iOS および OS X デバイスは、AirPlay を使用して Apple TV と直接ワイヤレス通信を確立できます。このピアツーピア AirPlay 機能は、互換性のあるデバイスではデフォルトで有効になっており、確立されたネットワーク接続の有無にかかわらず、iOS デバイスの優先データ パスとなります。

互換性のある Apple TV とその他の Apple エンドポイントの間では、それぞれのデバイスが別々のワイヤレス ネットワーク上にある場合でも、あるいはネットワーク接続がまったくない場合でも、このピアツーピア機能が可能です。これは、Bluetooth Low Energy（BLE）などさまざまな方式を使用して、利用可能な Apple TV の初期検出を行うことにより実現され、その後、802.11 チャネルを使用した直接通信パスが 2 つのピア デバイス（たとえば AirPlay の送信側と AirPlay の受信側）の間に確立されます。したがって、互換性のある Apple TV が関与するピアツーピア AirPlay 接続が使用中のときは、チャネル 149+1 または 153-1（他の一部の国ではチャネル 36 と 404）に相応の影響が出る可能性があります。AirPlay の送信側または受信側のどちらかでピアツーピア AirPlay がサポートされていない場合は、AirPlay 通信ではなく、確立されたネットワーク インフラストラクチャ接続が使用されます。

互換性のある iOS または macOS デバイスが、Bluetooth アダプタを使用して第 3 世代 Rev A 以降の Apple TV を検出し、関与するすべてのエンドポイントがピアツーピア AirPlay 機能をサポートしている場合、接続の検出プロセスにおける次の段階として、互換性のある Apple エンド デバイスと Apple TV は、5 GHz 帯域で 802.11 チャネル 149+1 を使用して、ピアツーピア方式の直接通信を行います。Apple TV Rev.4（2015）を使用する場合、ピアツーピア通信にチャネル 149 ～ 161 を使用できることに注意してください。ただし、802.11ac と同様、チャネル幅はフレームごとに動的に決定されるので、チャネル幅が 40 MHz から 20 MHz にまで変わる可能性があります。

エンド ユーザは、検出フェーズ完了後、該当する Apple TV を選択して Airplay 通信を開始することができます。これにより、802.11 無線は、AirPlay 用チャネル 149+1 と、ワイヤレス ネットワーク インフラストラクチャへのアクティブな接続に使用されるインフラストラクチャ ワイヤレス チャネルとの間でタイムシェアされます。その時点でどちらのデバイスもワイヤレス ネットワークに接続されていない場合、デバイスは AirPlay 機能用のチャネル 149+1 を使用します。ワイヤレス ピアツーピア AirPlay 通信は、802.11 規格に準拠しています。

AirDrop は、Wi-Fi 経由でピアツーピア通信を使用する iOS デバイス同士の間でコンテンツを共有するのに使われる、Apple の機能です。AirPlay と同様、AirDrop も、5 GHz 帯域で 802.11 チャネル 149+1 または 153-1 を使用して、デバイス間のコンテンツ転送を行います。AirDrop アクティビティの間、デバイスは、接続している AP との Wi-Fi 接続とピアツーピア接続との間を行き来しながらコンテンツ転送を完了することで、Wi-Fi 接続とコンテンツ共有をタイム スライスします。

シスコでは、通常の Wi-Fi アクティビティとピアツーピア アクティビティの比較という観点から、UNII-3 帯域の高チャネル使用率を監視することを推奨しています。多くの iOS デバイスが継続的なピアツーピア接続を日常的に使用することが想定される場合、解決策として、輻輳を回避するために DCA リストからチャネル 149、153 を削除する方法が考えられます。チャネルを削除する場合、シスコでは、RF プロファイルを使用して、チャネルの削除をすべての AP でグローバルに適用するのではなく、該当する AP のみに効果的に適用することを強く推奨しています。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

注: DCA の設定に関する詳細については、『Enterprise Mobility Design Guide（エンタープライズ モビリティの設計ガイド）』のガイドラインを参照してください。http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide.pdf [英語]

Apple Watch は、ピアツーピア通信を利用して機能するもう 1 つのポータブル デバイスです。ペアの iOS デバイスとの通信に、Bluetooth と Wi-Fi 接続の両方をサポートしています。通信には 2 つのモードがありますが、Apple Watch と iPhone との間でデータをやり取りするための主要な接続モードは Bluetooth です。Bluetooth がオフの場合には、Apple Watch は Wi-Fi に切り換えて、ペアの iPhone との接続を維持します。現在 Apple Watch は、オープンまたは事前共有キーによるセキュリティ認証を伴う 2.4 GH z 帯域の 802.11b/g/n のみをサポートしています。

最新の watchOS 2 アップデートで、Apple Watch は、Tetherless Wi-Fi を使用した独自のインターネット接続もできるようになりました。つまり、Apple Watch は iPhone がなくても Wi-Fi ネットワークに接続できるということです。Apple Watch は 2.4 GHz 限定であるため、複数の Apple Watch が Wi-Fi ネットワークと通信していても、5 GHz ネットワークに影響することはありません。

Cisco WLAN での iOS デバイス使用に関するベスト プラクティスのまとめ

Cisco WLAN に関する推奨事項をまとめると、次のようになります。

- シスコは、すべての iOS デバイスに 5 GHz のみのネットワークおよびカバレッジ設計を推奨します。一般に、5 GHz 帯域では、2.4 GHz 帯域とくらべて、非 802.11 干渉源からの影響が少なくなります。
- シスコは、WLC ダッシュボードで提示されるチャネル使用率を綿密に監視することを推奨します。チャネル使用率の値が高い場合、新たな干渉源、AP の停止、大量の Wi-Fi デバイスの追加を示している可能性があります。
- シスコは、チャネル変更を頻繁に行っている AP を監視することを推奨します。既知の干渉源から定常的に最も大きな影響を受けている 5 GHz Wi-Fi チャネルを特定できたら、解決のための処置を行ってください。
- シスコは、WLAN に接続するすべての iOS デバイスについて、QoS 値をプラチナ（音声）に設定し、WMM を必須にすることを推奨します。これにより、AP からのイーサネット トラフィックを、Wi-Fi チャネルでの優先順位を表す QoS 値を付けて、スイッチ ポートに接続することができます。
- シスコと Apple は、802.11r 混合モード WLAN を設定して、Fast Transition 802.1X または WPA2 PSK 対応クライアント、および 802.11r 互換クライアントが同じネットワークに接続できるように設定することを推奨します。
- シスコと Apple は、高密度企業環境の場合、11r FT パフォーマンスを最適化するために、802.11r を Over-the-Air 移行モードで使用することを推奨します。
- シスコは、AireOS 8.3 以降を実行するコントローラには Adaptive 802.11r を設定することを推奨します。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

- シスコは、WLAN で 802.11k を設定して iOS デバイスにネイバー リスト応答を提供することを推奨します。802.11k には、Cisco v8.0 MR3 および v8.1.120.0 以上、iOS 8 以上のバージョンが推奨されます。
- シスコと Apple は、802.11v BSS 移行管理を使用してアクセス ポイント間のクライアント負荷を平均化することを推奨します。
- シスコは、チャネルのカバレッジに必要なクライアント数およびチャネルのカバレッジに必要な帯域幅に適したカバレッジが提供されるよう、データ レートを管理することを推奨します。
- シスコは、チャネル ボンディングに関し、チャネル密度が必要な場合（環境内に多数の AP がある場合など）には 20 MHz を使用し、クライアント トラフィックの帯域幅消費が多い場合（ビデオなど）および DFS チャネルが利用可能な場合には 40 MHz を考慮することを推奨します。
- シスコは、音声トラフィック ベースのアプリケーションには DSCP 46 を使用し、802.11e – UP 6 に変換することを推奨します。
- シスコと Apple は、Cisco Wireless LAN で iOS デバイスを使用する際の一般的なベスト プラクティスとして、最小データ レート 12 Mbps および 24 Mbps を必須データ レートとすることを推奨します。5 GHz カバレッジでは余裕がないという場合には、最も低い必須レートとして 6 Mbps を設定した上で、12 Mbps と 24 Mbps も有効になっていることを確認してください。
- シスコは、すべての MCS レートを有効化されたままにしておくことを強く推奨します。
- シスコは、Apple クライアント デバイスに RSSI 測定値 -67 dBm の AP を常に 2 つ以上チェックさせることをお勧めします。
- シスコは、高密度クライアント環境においては、UNII-3 帯域チャネルでのピアツーピア通信アクティビティを監視することを推奨します。多数の iOS デバイスがピアツーピア アクティビティを実行することが想定される場合には、最終手段として、DCA からチャネル 149、153 を除外することも考慮できます。
- Apple は、すべてのデバイスを最新バージョンの iOS にアップグレードすることを推奨します。
- RF 設計と監視に関する推奨事項のまとめ:
  - 全般的なチャネル使用率は 40 % 未満とします。
  - 最小信号対雑音比（SNR）25 dB とします。
  - 802.11 再送信は 15% 未満に維持します。
  - パケット損失は 1 %未満に抑え、ジッターは 100 ms 未満を維持します。

WLAN のベスト プラクティスには、高密度のアクセス ポイントと合わせて高可用性の WLC を導入し、常時利用可能な WLAN インフラストラクチャを推進することも含まれます。さらに、Cisco CleanAir、ClientLink、ローミングの最適化、無線リソース管理などのシスコの HDX テクノロジー スイートにより、カバレッジ ホールを低減し干渉を回避すると同時に、ネットワーク パフォーマンスを自動的に最適化することができます。

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

追加情報

『Cisco Wireless LAN Controller Deployment Guide v8.1（シスコ ワイヤレス LAN コントローラ導入ガイド v8.1）』
http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design-Guide/Enterprise_Mobility_8-1_Deployment_Guide.pdf [英語]

『Cisco Wireless LAN Controller Configuration Best Practices（シスコ ワイヤレス LAN コントローラの設定に関するベスト プラクティス）』
http://www.cisco.com/c/en/us/td/docs/wireless/technology/wlc/8-1/82463-wlc-config-best-practice.html [英語]

『Detailed overview on how 802.11r works on Cisco WLAN（Cisco WLAN における 802.11r 動作の詳細な総括）』
http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html#anc24 [英語]

『Cisco Device Classification Guide（シスコ デバイス分類ガイド）』
http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/device_classification_guide.html [英語]

『Cisco Application Visibility and Control (AVC) Q & A（Cisco Application Visibility and Control（AVC）の Q & A）』
http://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/qa_c67-722538.html [英語]

『Configuring Application Visibility and Control (WLC 7.6 or later)（Application Visibility and Control の設定（WLC 7.6 以降））』
http://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/115756-avc-guide-00.html [英語]

『Wi-Fi network roaming with 802.11k, 802.11r, and 802.11v on iOS（iOS での 802.11k、802.11r、802.11v による Wi-Fi ネットワーク ローミング）』
https://support.apple.com/en-us/HT203068 [英語]

『iOS 9 Deployment Reference Guide（iOS 9 導入リファレンス ガイド）』
https://help.apple.com/deployment/iOS/ [英語]

『iOS Voice Over IP (VoIP) Best Practices Guide（iOS Voice Over IP（VoIP）ベスト プラクティス ガイド）』
https://developer.apple.com/library/ios/documentation/Performance/Conceptual/EnergyGuide-iOS/OptimizeVoIP.html [英語]

『IEEE 802.11r/k/v standards（IEEE 802.11r/k/v 規格）』
http://ieeexplore.ieee.org/servlet/opac?punumber=4544752 [英語]
http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=4573290 [英語]
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5716530 [英語]

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

©2017 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)
この資料の記載内容は 2017 年 2 月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

お問い合せ先

シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp