Cisco Wireless LAN で Apple モバイル デバイスを使用する企業のためのベスト プラクティス

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目次

このマニュアルの目的

本書は、Cisco Wireless LAN（WLAN）の設計、導入、管理を担当する IT プロフェッショナルを対象としています。対象読者が Cisco WLAN の各コンポーネントと機能、および基本的な IP ネットワーキングに関して、実用的な知識を有していることを前提としています。インフラストラクチャのセキュリティを維持しながら、Apple デバイスおよび混合クライアント環境に考え得る最高のサービスを提供するための、実装の考慮事項、推奨されるネットワーク セットアップ、およびトラブルシューティングをカバーするベスト プラクティスを紹介します。

本書の各トピックには、さまざまな使用例における設定の全般的なガイドのほか、Wi-Fi 802.11r Fast Transition セキュア認証および 802.11k ネイバー リスト無線管理をサポートする iOS6 オペレーティング システム搭載の iPhone および iPad を対象とした、具体的なガイドが含まれています。

はじめに

この Bring Your Own Device（BYOD; 個人所有デバイスの持ち込み）の世界では、学生がワイヤレスの Apple iPhone や iPad をキャンパス内に持ち込んだりしますし、複数のデバイスを所有するユーザが人口構成の大半を占めています。こうした世界では、IT 管理者はネットワーク リソースのセキュリティを確保すると同時に、オープンなアクセス ネットワーク環境を用意することを求められます。

こうした環境では、セキュリティに関する懸念は元より、QoS、無線カバレッジ、ローミング シナリオ、セントラル スイッチングまたはローカル スイッチング アーキテクチャ、レガシー クライアントの混在など、数多くの課題が浮上します。ゲスト ユーザがワイヤレス プリンタを利用できるようにし、なおかつ会社のファイル サーバにはアクセスできないようにするには、どうすればよいでしょうか。信頼できる社内ユーザに対して優先度の高い帯域幅を保証するには、どうすればよいでしょうか。問題は安全なアクセスの確保だけではありません。良好なアプリケーション パフォーマンスを維持しながら、簡単にオンボーディングを実行でき、接続を維持できるようにすることも大切です。

本書では、考慮すべきさまざまな要素を加味した、考え得る限り最高のサービスを「iDevice」に提供するためのベスト プラクティスをいくつか紹介します。Apple は、ビジネス アプリケーションを利用できるモバイル デバイスの分野では最先端を走っています。iPhone5 は、5 GHz 帯域と、5 GHz 帯域向けの北米チャネル セットで 21 の Wi-Fi チャネルをサポートしています。そのおかげで iPhone5 の Wi-Fi デュアルバンド サポートが実現し、iPhone のビジネスでの採用に大きな影響を与えています。802.11k および 802.11r をサポートする Apple iOS6 は、Wi-Fi アクセス ポイント（AP）全体でローミングが強化されるように設計されたプロトコルのうち、2 つをサポートするようになりました。本書では、そのプロトコルを使用するように Cisco ワイヤレス LAN コントローラ（WLC）を設定する方法について説明します。

Wi-Fi チャネル カバレッジ

Wi-Fi チャネル カバレッジの概要

デュアルモードの iPhone5 および iPad は、米国で承認された 5 GHz チャネルをすべてサポートしています。デュアルモード機能により、これらのデバイスは追加の 21 Wi-Fi チャネルで動作できるようになっています。シスコは、5 GHz カバレッジ設計を推奨しています。5 GHz チャネルは、Bluetooth や電子レンジのような一般的な 2.4 GHz デバイスの影響を受けません。5 GHz チャネルのチャネル使用率は一般的に、2.4 GHz チャネルと比べるとはるかに低くなっています。5 GHz 帯域のチャネル使用率のほうが多くのチャネルを利用でき、チャネルの再使用（同一チャネル干渉）やオーバーラップが低減されるため、低くなります。

密集した 2.4 GHz ネットワークでは、チャネル使用率が高くなることが珍しくありません。WLC のレポートを使用して、チャネル使用率を入念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、新しい干渉源の出現、AP の停止、または新しい Wi-Fi デバイスの大量流入を示している可能性があります。

この他に監視が必要な条件として、チャネルを変更する AP が挙げられます。サイト内調査を実施すると、Wi-Fi のパフォーマンスに干渉する信号の固定発生源が見つかります。こうした条件の影響を受ける 5 GHz Wi-Fi チャネルは、Dynamic Channel Allocation（DCA）除外リストに追加することを推奨します。WLC の論理パラメータと設定パラメータ、および規制により、5 GHz チャネルが一時的に DCA リストに加えられる場合があります。これは正常な動作です。ただし、特定のチャネルが繰り返し DCA に追加される場合、その干渉を管理できないのであれば、当該のチャネルを DCA リストに追加するのが最善の方法であることも考えられます。

現在の 5 GHz AP のカバレッジが iPhone5 や iPad でアプリケーションを実行するのに十分であるかどうかを判断するための、使いやすいリンク テスト ツールが WLC には用意されています。

5 Ghz AP のカバレッジを確認するには：

ステップ 1 iPhone を AP にアソシエートし、クライアントに一致する MAC アドレスから、[WLC] > [Monitor] > [Clients] の順に選択します。クライアントの詳細画面が表示されます（図 1 を参照）。

ステップ 2 [Link Test] ボタンを選択してリンク テストを実行します。この操作により双方向リンク テストが実行され、クライアントの現在のカバレッジが判定されます。損失パケットが存在しない場合、クライアントを AP から遠ざけ、良好なアプリケーション パフォーマンスを維持できるだけの信号を得られる範囲をどこまで広げられるかを調べます。

図 1　　リンク テストのオプションが表示されたクライアントの詳細画面

カバレッジの 1 つの目標としては、AP に送信する信号の RSSI（Received Signal Strength Indicator; 受信信号強度）を -67 dBm 以上にします。2.4 GHz でカバレッジ テストを実行する際には、低いデータ レートを無効にすることを推奨します。これは、-67 dBm RSSI のカバレッジ領域が 1 Mbps データ レートで 12 Mbps を大きく上回るからです。範囲と帯域幅のいずれを重視した設計にするかは、この点を考慮して決めます。密集した 2.4 GHz ネットワークでは、チャネル使用率が高くなる可能性があります。チャネル使用率を下げる最も効率的な方法は、低いデータ レートを取り除くことです。

802.11n 無線技術を使用した現在の iPhone および iPad では、1 空間ストリームがサポートされます。1 空間ストリームとは、20 MHz ワイド Wi-Fi チャネルで 802.11n 対応のデータ レートが 6.5 Mbps ～ 72 Mbps の範囲になることを意味します。5 GHz 帯域では 802.11a データ レートより品質が良くなり、6 Mbps ～ 54 Mbps となります。11n テクノロジーにより、クライアントは 40 MHz ワイド Wi-Fi チャネルを利用できるようになります。クライアントが 802.11a クライアントとして動作している場合は、40 MHz ワイド チャネルのプライマリ 20 MHz の使用量を共有できます。

802.11n 無線を使用するクライアントの iPhone および iPad は、802.11n ビーム フォーミングをサポートします。シスコでは、802.11n ビーム フォーミング テクノロジーを ClientLink 2.0 と呼んでいます。シスコは、2.4 GHz で 802.11g の ClientLink、5 GHz で 802.11a の ClientLink をそれぞれ提供しています。ClientLink のメリットは、クライアント デバイスと AP 間の Wi-Fi 信号の品質が向上することにあります。クライアント デバイスと AP 間の高品質リンクそれぞれが、これらの Wi-Fi チャネルの帯域幅とカバレッジ品質を向上させます。

（注）　ClientLink 2.0 の詳細については、次の URL の『*Cisco Wireless ClientLink 2.0 Technology at a Glance*』を参照してください。
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps11983/at_a_glance_c45-691984.pdf

ビーム フォーミング（ClientLink）により 802.11a よりも高品質のリンクと音声品質が提供されるため、5 GHz 帯域では 802.11n を使用することを推奨します。ClientLink 2 を使用すると、Wi-Fi チャネルの帯域幅とカバレッジ領域が改善されます。そのため、カバレッジ領域内のすべてのデバイスのパフォーマンスが向上します。

シスコは、WLAN 設定で「BandSelect」を有効にすることも推奨しています。特定の状況で iPhone5 の 5 GHz 帯域に偏りが見られるような場合でも、BandSelect を有効にしておくと、電話機の信号強度が両方の帯域に対して適切な設定になっていれば 5 GHz での接続率を向上させることができます。

Wi-Fi 802.11e/WMM QoS

Wireless Multimedia（WMM）の WLAN 設定では別の使用例が見られます。WMM が無効に設定されている場合、WMM QoS はパケットのキュー設定やマーキングに使用されません。WLAN のすべてのパケットは、WLAN QoS 設定に基づいて転送されます。したがって、iPhone に送信される ping は、WLAN QoS 設定が voice または platinum になっていれば音声優先で送信されます。これは、ベスト エフォートの DSCP（Differentiated Services Code Point）値でマーキングされて WLC に送信される ping パケットも同様です。

上記の理由から、WMM の推奨設定は使用例に応じて「allowed」または「required」です。802.11e/WMM QoS 対応クライアントおよび WMM WLAN では、AP から転送される各パケットの 802.11 ヘッダーに QoS 値が含まれます。同様に、WMM クライアントから送信されるパケットにもすべて、802.11 ヘッダーに QoS 値が含まれます。WMM 以外のクライアントは、WMM ヘッダーを含むパケットを送受信できません。WMM ヘッダーを含まないパケットには、チャネル優先またはチャネル制御の機能はありません。このようなパケットのトラフィックはベスト エフォートとなります。

802.11e/WMM 仕様は、携帯電話で Wi-Fi が代替ワイヤレス メディアとして使用されている限り、またタブレットで Wi-Fi が使用されている限り、存続します。こうしたデバイスでは、必要に応じて WMM が設定された WLAN に接続できることが必要です。WLAN が「WMM 必須」に設定されている場合、WLAN にセキュリティが設定されていなくても、WMM ではないデバイスは WLAN に接続できません。セキュリティが設定された WLAN では、WMM 以外のクライアントの認証要求は承認されません。ハンドヘルド トランザクション コンピュータや旧式の単一用途型ラップトップなど、WMM に対応していないレガシー デバイスでは、WMM 設定を「allowed」にすることを検討する必要があります。iOS 4.0 以降を搭載した Apple デバイスでは、「WMM 必須」の設定がサポートされています。

「802.11n」（P.15）の図 5 は設定画面（[WLANs] > [Edit 11nSSID] > [QoS]）の図で、WMM の設定例を示しています。WLAN の使用例によって、この設定の内容が変わる場合があります。たとえば会社のポリシーにより、ゲスト アクセス WLAN の設定を allowed に、WMM QoS 値を silver または best effort にするように決められている場合もありえます。このような場合、特定のポリシーが設定されていない限り、AP ではすべてのトラフィックをベスト エフォートで転送します。

iPhone および iPad 用の企業 WLAN では、QoS 値を platinum または voice に、WMM の設定を required にすることを推奨します。この設定により、AP から送信されたイーサネット トラフィックが、Wi-Fi チャネルでの優先度を表す QoS 値を使用してスイッチ ポートに接続できます。その後、会社のポリシーで必要とされているなら、AP に接続されたポートのエッジ スイッチでヘッダーの再マーキングを実行できます。WLC コードのリリース 7.4 以降、Application Visibility and Control（AVC）を有効にすると、そのようなポリシーを WLC でアクティブにすることができます。AP ではアップストリーム パケットのディープ パケット インスペクションが実施され、WLC で設定されたポリシーに一致するアップストリーム パケットが再マーキングされます。

QoS マーキングの処理方法

パケットの QoS マーキングが WLAN での QoS 設定に一致しない場合、WLAN 設定ではパケット マーキングよりも転送が優先されます。iPhone から Wi-Fi チャネル経由で音声優先の音声パケットを送信した場合に、パケットのコリジョンが発生すると、音声の緊急再試行を優先させる音声優先キューイングおよび音声優先メディア アクセス（チャネル アクセス）が実行されます。この状態は、電話機を接続している WLAN で QoS が best effort または silver に設定されている場合にも発生します。

WMM の優先度が voice または platinum に設定された WLAN に電話機を接続している場合、そのパケットはイーサネット アップストリーム経由で音声優先のインフラストラクチャに転送されます。つまり、そのパケットの有線側ヘッダーの QoS 値を変更するオーバーライド ネットワーク ポリシーが設定されていない限り、転送されるということです。その iPhone が best effort 設定の WLAN または silver WLAN に接続されている場合、AP からは、best effort がマーキングされたパケットがイーサネットに転送されます。

シスコのソフトフォン アプリケーションである Jabber から送信されたオーディオ パケットの場合、Jabber アプリケーションによってオーディオ（G711/722）パケットに緊急転送値 46 の DSCP 値がマーキングされます。ただし、iPhone の WMM/iOS では、WMM の UP（ユーザ優先）フィールドが voice 値にマーキングされることはありません。そうではなく、ビデオ優先の値が使用されます。音声の WMM 値は UP=6 です。ビデオの WMM 値は UP=5 です。したがって、Jabber のオーディオ パケットには、Wi-Fi キューイング、再試行値、および Wi-Fi チャネルへの送信時のビデオ パケットの動作を示すメディア アクセス値が含まれます。WLAN の設定が voice、video、best effort のいずれであっても、それは変わりません。

そのパケットの宛先 WLAN が voice に設定されていて、オーバーライド ポリシーが存在しない場合、パケットは当該の WLAN から WMM UP 値 6 または voice で送信されます。この WLAN/WMM の動作により、他のポリシーを呼び出さなくてもコール品質を向上できます。iPhone で行われるオーディオ パケットのマーキングは、コールの最初のネットワーク ホップで QoS 値を引き下げるため、オーディオ コールの MOS（Mean Opinion Score）値に影響を与えます。ただし、WMM 値が platinum に設定された送信元 WLAN では、ネットワーク ポリシーで変更されない限り、Jabber のオーディオ パケットは最後のホップで音声優先となります。

Jabber アプリケーションでオーディオ パケットの DSCP 値が best effort に設定されている場合、iPhone から送信されるオーディオ パケットの WMM 値は、UP=0 または best effort となります。さらに、そのパケットの宛先が同一の WLAN 内の他の電話機である場合、WLAN の WMM 設定が platinum/voice であっても、AP でそのパケットは WMM UP=0 で転送されます。

WMM の QoS ロジックは DSCP 値をサポートします。Wi-Fi チャネルの利用率が過剰ではなく、したがって適度な帯域幅を維持している場合、高品質のアプリケーション パフォーマンスを期待できます。

この場合、使用するアプリケーションで適切な QoS 動作が維持されると、ある程度は信頼することができます。シスコのソフトフォン アプリケーションである Jabber のような特定のアプリケーションでは、オーディオ、ビデオ、およびその他のフレーム タイプを Cisco AVVID（Architecture for Voice, Video and Integrated Data）の QoS 基準にマーキングします。

（注） 「付録 A：IEEE IP DSCP - AVVID 値および 802.11e WMM」（P.35）の表を参照してください。

Jabber やその他のビジネス アプリケーションの場合、デバイスの WMM ドライバまたは QoS ポリシーによって WMM QoS 値が低下したパケットにおいてもアプリケーションに必要な QoS レベルを獲得できるように、QoS 値を platinum にすることを推奨します。iPhone、iPad、およびその他の類似デバイスで、ゲスト アクセスしか利用できないようにするか、ポリシーによってエンタープライズ レベルのアクセスを制限する場合、認証を行う WLAN で、WMM の QoS は該当デバイスの優先度を下げる設定にします。

WLAN に認証され、WMM が有効になった iDevice からは、そのデバイスの Wi-Fi 無線ドライバと QoS ポリシーで設定された WMM QoS レベルでパケットが送信されます。この場合、これらのデバイスで、WLC で WLAN 用に設定された QoS 値を含むパケットを送信する必要はありません。また、アプリケーションがパケット内に設定した DSCP IP 値を含むパケットを送信する必要もありません。WLAN の QoS 値は、AP でアップストリームおよびダウンストリーム トラフィックの転送に使用される高レベル マーキングの値より高くなります。WLAN WMM 設定に加えて、QoS 設定のオプションは多数用意されています。このオプションについては、最新の WLC コンフィグレーション ガイドを参照してください。

まとめると、iPhone および iPad の一般的な QoS 動作として、アップストリームおよびダウンストリーム パケットは DSCP 値を表す WMM 値を含んだ状態で送信されます。Wi-Fi iPhone および iPad トラフィックをさらに詳細に管理する必要がある場合は、AVC（Application Visibility and Control）を使用することを推奨します。Cisco WLAN リリース 7.4 以降、AVC は WLC に含まれています。

（注） その他の推奨事項については、『Voice over Wireless LAN 4.1 デザイン ガイド』（http://www.cisco.com/cisco/web/support/JP/docs/WL/WLLANMGMT/WLCntrlSystem/SDG/002/14684_01.html）、およびお使いのコードのバージョンに該当するワイヤレス LAN コントローラ コンフィギュレーション ガイド（cisco.com の該当ページ）を参照してください。

（注） サポートされる iDevice の各種機能については、「付録 B：対照表（概略）」（P.36）で簡単に説明しています。

ローミング

ローミングの概要

IEEE 802.11k および 802.11r は今後、展開するうえで、重要な業界標準であり、WLAN 環境でのシームレスな Basic Service Set（BSS）間のローミングを可能にします。Cisco WLAN リリース 7.4 以降、Apple iOS6 搭載の iPhone および iPad のエンタープライズ ローミングの推奨設定は、802.11k ネイバー リストです。IEEE 802.11k 仕様は、2008 年 6 月に批准されました。

（注） Wikipedia に掲載されている 802.11k の簡単な説明については、http://en.wikipedia.org/wiki/IEEE_802.11k-2008 を参照してください。

（注） IEEE 802.11k 仕様については、http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4544755 を参照してください。

（注） 802.11k については、本書の「無線リソース管理」（P.9）を参照してください。

ローミングを容易にするため、ある AP にアソシエートした iPhone は、ネイバー AP のリストを求める要求を送信します。この要求は、アクション パケットと呼ばれる 802.11 管理フレームの形式で送信されます。AP は、同一 WLAN 内のネイバー AP のリストで応答します。このリストには各 AP の Wi-Fi チャネル番号も含まれます。AP の応答もアクション パケットです。

iPhone は、応答フレームから次のローミングの候補となる AP を認識します。802.11k Radio Resource Management（RRM）プロセスを使用することで、iPhone は効率的かつ迅速なローミングを行うことができ、通話中にローミングを実行するのが一般的なエンタープライズ環境で良好なコール品質を確保するという要件を満たすことができます。

WLC 802.11k の推奨設定は、RRM を有効にすることです。これにより、ネイバー リスト応答パケットで 2.4 GHz と 5 GHz の両方の AP チャネル番号が提供されます。Voice over WLAN コールだけでなく、すべてのアプリケーションとデバイスで、5 GHz 帯域 Wi-Fi チャネルを使用することを推奨します。デュアルバンド iPhone5 および iPad は、5 GHz 帯域への偏向を示します。

ネイバー リストの情報があれば、iPhone はすべての 2.4 GHz および 5 GHz チャネルをプローブしてローミング先 AP を探す必要がなくなります。すべてのチャネルをプローブする必要がなければ、全チャネルのチャネル使用率が低下し、全チャネルの帯域幅が増加します。また、ローミング時間が短縮され、iPhone または iPad ですばやく切り替えができるようになります。さらに、各チャネルの無線設定を変更したり各チャネルでプローブ要求を送信したりすることもなくなるため、バッテリーの寿命が伸びます。すべてのプローブ応答フレームをデバイスで処理する必要もなくなります。

CLI を使用して 802.11k 向けに WLC を設定するための推奨コマンドを次に紹介します。

（注） WLC には、802.11k の設定を行うための GUI はありません。

- WLAN ネイバー リストを有効/無効にする：WLC からネイバー リストを有効または無効にします。また、AP の RRM および Power Constraint Information Elements（IEs）を有効または無効にします。

  config wlan assisted-roaming neighbor-list {enable|disable} *wlanId*

- WLAN ネイバー リストのデュアルバンド応答を有効/無効にする：両方の無線帯域のエントリを含むネイバー リストを有効または無効にします。デフォルトは、クライアントが現在アソシエートしている帯域です。

  config wlan assisted-roaming dual-list {enable|disable} *wlanId*

- 予測リスト ベースの支援ローミングを有効/無効にする：ローミング最適化の予測リストを使用した支援ローミング機能を有効または無効にします。すでに同一 WLAN 内でロードバランシングが有効になっている場合は、警告が出力され、WLAN のロードバランシングが無効になります。

  config wlan assisted-roaming prediction {enable|disable} *wlanId*

（注） コマンドを実行したら、設定を保存してください。

無線リソース管理

802.11k 標準は、利用できる最適な AP を見つけるための情報を提供します。

（注） 11r については、本書の「ローミング」（P.8）を参照してください。

iOS6 コードを利用する iPhone4s および iPhone5 では、802.11k 無線管理情報を使用してローミングを必要とする AP が判断されます。802.11k 仕様で定義されたプロセスの一部として、電話機から現在アソシエートしている AP にネイバー情報の要求を送信することができます。その AP は、最も近くにある AP およびその AP の Wi-Fi チャネル番号を含むネイバー情報を返します。この情報により、iPhone5 は 2.4 GHz 帯域のすべての Wi-Fi チャネルと 5 GHz 帯域のすべてのチャネルをスキャンする手間をかけずに AP を見つけることができます。時間にして数秒を短縮できるほか、バッテリーの節約にもつながります。

802.11k は、ネットワーク内でのトラフィックの分散方法を改善することを目指しています。WLAN では通常、個々のデバイスは最も強い信号を送信する AP に接続します。この調整方法の場合、クライアントの台数や位置によっては、1 台の AP に要求が集中する一方で他の AP では使用率が低下し、結

果としてネットワーク全体のパフォーマンスが低下する事態に陥ることがあります。802.11k に準拠するネットワークでは、信号強度が最も高い AP の負荷が限度一杯になると、使用率の低い AP のいずれかにワイヤレス デバイスは接続します。信号強度が低くても、ネットワーク リソースが効率的に使用されるため、全体的なスループットは向上します。

以下に、新しい AP に切り替わる前に 802.11k ネイバー リスト プロトコルが行う可能な動作の手順を示します。

1. AP は、クライアントが移動して離れていくと判断します。
2. AP はクライアントに、新しい AP への切り替え準備をするように知らせます。
3. クライアントは、ネイバー AP のリストを要求します。
4. AP が、サイト レポートを提供します。
5. クライアントは、そのレポートに基づいて最適な AP に移動します。

iOS6 搭載の iPhone5 および iPad では、これと同様に 802.11k ネイバー リスト機能が使用されます。AP とアソシエートすると間もなく、その AP から提供されるネイバー リストを要求します。ネイバー リスト レポートには、隣接する AP の Basic Service Set Identifier（BSSID）とチャネル番号が含まれています。

高速ローミング

高速ローミングの概要

Apple iOS6 搭載デバイスのエンタープライズ セキュリティの推奨設定は、802.11r Fast Transition（FT）です。IEEE 802.11r 仕様は 2008 年 7 月に批准されました。これは、2004 年 6 月の 802.11i 仕様の後継です。

802.11r では、標準ベースの Fast Transition が導入されています。

- クライアントは再アソシエートを実行する前に（またはその最中に）、対象 AP のセキュリティおよび QoS 状態を確立することが可能
- 方法 1：Over-the-Air：無線通信経由（クライアントから新しい AP へ）
  - 4 つのパケットが Wi-Fi チャネル経由で変更される
- 方法 2：Over-the-DS：分散システム経由（古い AP を経由）
  - 2 つのパケットが Wi-Fi チャネル経由で交換され、2 つはイーサネット経由で交換される

802.11r では、クレデンシャルをすでにキャッシュ済みの 11r クライアントと AP の間で交換されるパケットの数が減ります。

（注） Wikipedia に掲載されている 802.11r の簡単な説明については、http://en.wikipedia.org/wiki/IEEE_802.11r-2008 を参照してください。

（注） IEE 802.11r 仕様については、http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4573292 を参照してください。

（注） iPhone および iPad のモデル番号については、http://support.apple.com/kb/HT3939?viewlocale=ja_JP を参照してください。

Apple iOS 6.0 より前では、Fast Transition はサポートされていません。Apple iOS5 では Sticky Key Caching（SKC）がサポートされています。iOS5 と iOS6 ではどちらも、802.11e 認証タイプ、EAP-FAST、LEAP、EAP-TLS、EAP-TTLS、EAP-SIM、PEAP バージョン 1 および 2 がサポートされています。

このセキュリティ オプションにより、iPhone ではわずか 4 つのパケットを交換することで、AP への認証を安全に行うことができます。2 つのパケットは、AP 同士をつなぐイーサネット ケーブルで送信できます。残る 2 つのパケットは、各 AP の Wi-Fi チャネルで送信されます。これにより、実際のローミングを行う前に、iPhone からローミング先の AP に対して安全な認証を行うことができます。その結果、ローミング完了後に認証プロセスの遅延なく、iPhone でデータ、ビデオ、オーディオ パケットを送受信できます。

現在 802.11r FT に影響のあるガイドラインと制限事項は次のとおりです。

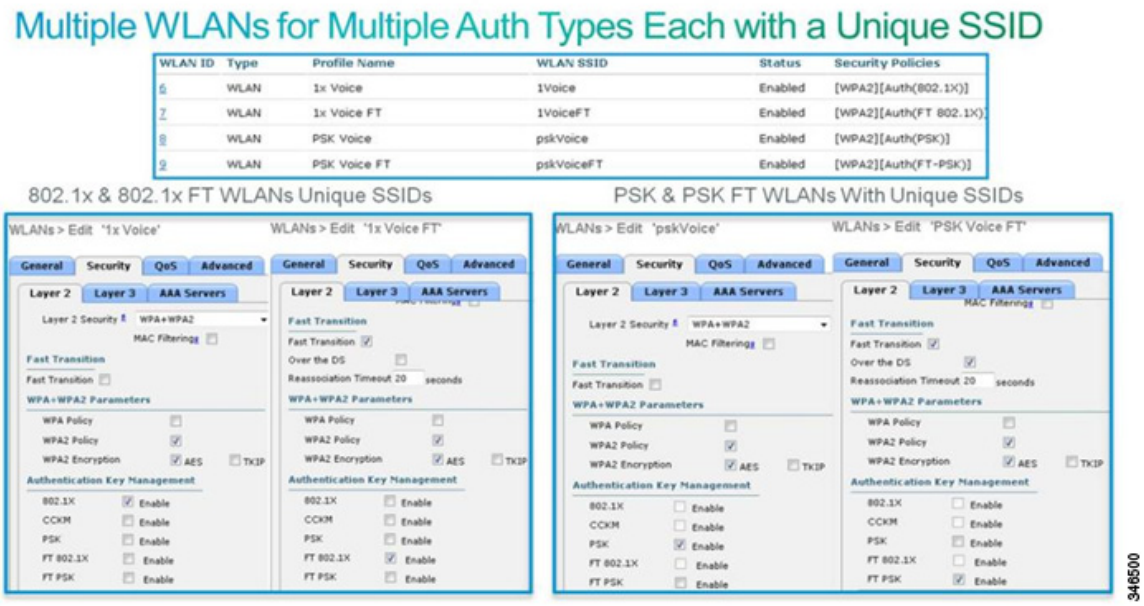
- 802.11r FT はメッシュ AP でサポートされません。
- FlexConnect モードの AP の場合：
  - 802.11r FT は、リリース 7.3 以降のセントラルおよびローカル スイッチング WLAN でサポートされます。
  - 802.11r FT は、ローカル認証が有効にされた WLAN ではサポートされません。
- 802.11r FT は、Cisco 600 シリーズ OfficeExtend アクセス ポイントではサポートされていません。
- 802.11r のクライアント アソシエーションは、スタンドアロン モードの AP ではサポートされません。
- 802.11r の高速ローミングは、スタンドアロン モードの AP ではサポートされません。
- ローカル認証 WLAN とセントラル認証 WLAN の間での 802.11r 高速ローミングはサポートされていません。
- 802.11r の高速ローミングは、クライアントがスタンドアロン モードで Over-the-DS 事前認証を使用している場合、サポートされません。Over-the-DS（Distribution System）とは、パケットが有線インフラストラクチャで送信される場合を指します。
- スタンドアロン AP からクライアントへ送信されるサービスは、セッション タイマーの期限が切れるまでの間のみサポートされます。
- Traffic Specification（TSpec）は、802.11r 高速ローミングではサポートされていません。WLAN リンクに遅延が存在する場合、高速ローミングも遅延します。音声またはデータの最大遅延を検証する必要があります。
- WLC では、Over-the-Air 方式と Over-the-DS 方式の両方で、ローミング中の 802.11r Fast Transition 認証要求が処理されます。
  - 必要なパケットのうち 2 つは AP の有線接続で送信され、2 つは Wi-Fi で送信されるため、Over-the-DS の使用を推奨します。DS オプションが選択されていない場合、4 つのパケットはすべて WLAN で送信されます。

WLC における Fast Transition の推奨設定

802.11r FT クライアントを WLAN ネットワークに追加する場合の、WLAN 設定の推奨事項は次のとおりです。図 2 に設定例を示します。下記のベスト プラクティスの推奨事項は、Apple とシスコ両社の共同作業によって導き出されたものです。

- Fast Transition 802.1x クライアント用に追加の WLAN を設定します。
- Fast Transition PSK クライアント用に追加の WLAN を設定します。
  - この推奨事項を挙げるのは、Fast Transition が設定された WLAN のアソシエーション応答パケットに追加される情報が、レガシーの無線ドライバでは認識されないためです。802.11r 仕様は 2008 年に批准されましたが、すべてのクライアントの無線ドライバが 802.11r に関する管理パケットの変更を処理するように更新されたわけではありません。この点は一部の Apple 製品も同様です。
  - Apple は、レガシー クライアントに別個の WLAN および SSID を使用することを推奨しています。

図 2　802.11r FT クライアントを追加するための WLAN 設定の推奨事項



（注）　Fast Transition に関する CLI または GUI での設定オプションの詳細については、WLC コードのインストールしたバージョンに該当する『Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド』を参照してください。

Sticky Key Caching（SKC）

SKC は広く採用されているものではありません。シスコでは、WLC リリース 7.2 でサポートを追加しました。SKC を使用したクライアントの制限事項は、アソシエートを行った直近 8 台の AP からの情報しかクライアントでキャッシュされないことです。新しい AP に対してローミングを行うたびに完全認証が実行され、同一の AP に対するローミングでもキャッシュされたエントリが使用されます。

WLC での制限事項は次のとおりです。

- 移動中、複数の WLC にまたがってキャッシュが動作することはありません。
- キャッシュは WPA2 Robust Security Network（RSN）設定の WLAN でのみ動作します。
- キャッシュはローカル モードの AP にのみ該当します。

SKC は、WLC の CLI で設定できます。使用するコマンドは次のとおりです。

config wlan security wpa wpa2 skc-cache {enable|disable} *wlan-id*

（注） SKC の詳細については、次の URL にある『Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド ソフトウェア リリース 7.2』を参照してください。
http://www.cisco.com/cisco/web/support/JP/docs/WL/WLLANCntrller/5500WLCntrllers/CG/002/cg.html

（注） コマンドを実行したら、設定を保存してください。

データ レート

データ レートの概要

データ レート設定を使用して、ワイヤレス デバイスのデータ伝送に使用されるデータ レートを選択します。データ レート、パフォーマンス、範囲、信頼性には、直接的な相関関係があります。Apple デバイスを使用する場合、ネットワークに接続する可能性のあるすべてのデバイスを対象に含め、導入環境の AP の密度を考慮した計画を立てる必要があります。

データ レートの選択には、次の 2 つの方法があります。

- 範囲を最大にする：範囲の拡大が要件となっている場合、低いデータ レートを有効にすることを検討します。それは、データ レートが低ければ、信号のデコードのためにレシーバで必要とされる信号レベルと SNR も低くなり、またクライアント デバイスと AP との間で信頼性の高い接続を維持できる距離も長くなるからです。適切なパフォーマンス レベルを維持できる程度のデータ レートに調整を行ってください。
- パフォーマンスを最大にする：高パフォーマンスの WLAN の導入、ローミングの改善、セルのカバレッジを狭めて同一チャネル干渉の影響を軽減することを目標とする場合、高いデータ レートの設定を検討します。ただし、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、実際上パフォーマンスの低下につながる場合があるため、あまり高すぎる値には設定しないでください。

次のガイドラインに従ってデータ レートを選択してください。

- 低いデータ レートを有効にすると、AP から送信されるパケットの範囲が拡大されます。データ レートの必須最低値を下げればそれだけ、ビーコンおよびその他のパケットの AP から送信可能な範囲が広がります。敷地内に AP があまり設置されておらず、レガシー クライアントが多数存在するような場合、低いデータ レートが適しています。現在のクライアント デバイスは、802.11b の

時代よりも無線の性能が向上しています。現在のクライアントの機能なら、802.11g レートで 802.11b レートと同じ範囲をカバーできます。したがって、低速のうえ帯域幅を多く消費する 802.11b には利用価値がありません。

- 敷地内に AP が多数設置されている場合は、データ レートを低くすると帯域幅の消費が増え、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。AP 密度が原因で発生する帯域幅の低下は、5 GHz よりも 2.4 GHz の場合のほうが顕著です。この場合の低下は、同一チャネル干渉によるチャネル使用率の増加が原因です。同一チャネル干渉の副作用として、パケットのコリジョンによるパケット エラー率の上昇がみられます。コリジョンが発生すると再試行が行われ、再試行によってチャネル使用率が高まります。

したがって、ベスト プラクティスとして、クライアント数に応じて、そのチャネル カバレッジで必要な帯域が提供されるように、データ レートを調整してください。

（注） 詳細については、次の URL にある『Enterprise Mobility 4.1 デザイン ガイド』を参照してください。http://www.cisco.com/cisco/web/support/JP/docs/WL/WLLANMGMT/WLCntrlSystem/SDG/001/14435_01.html

各データ レートは、次の 3 つのモードのいずれかに設定できます。

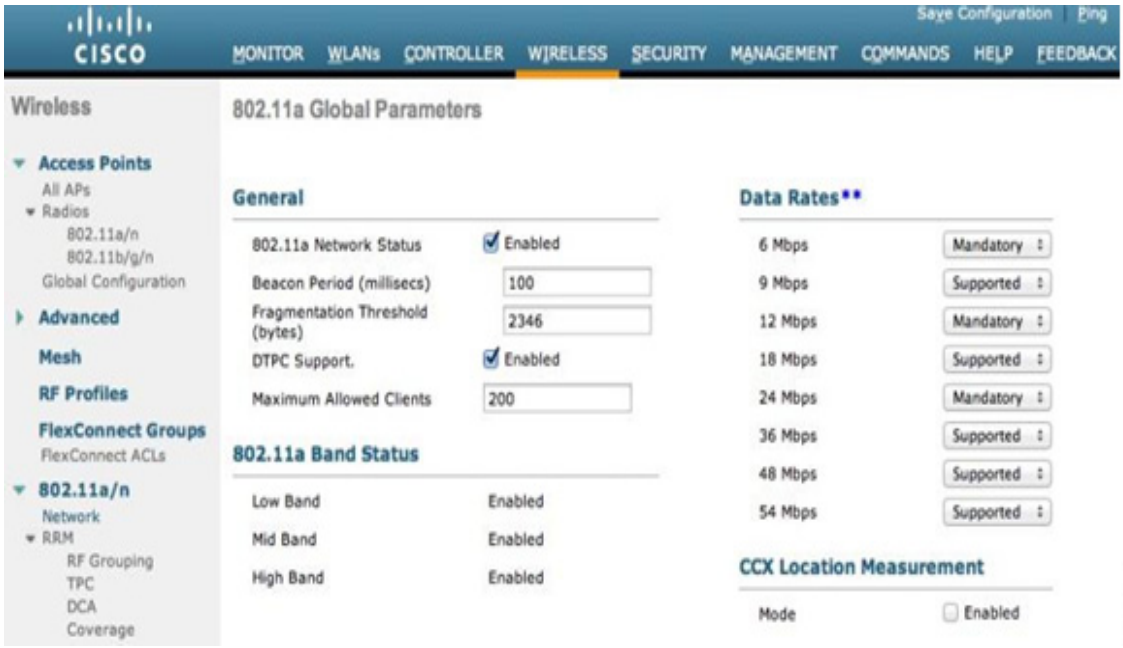
- [Mandatory]：ユニキャストとマルチキャストの両方で、全パケットのこのレートでの伝送が可能です。AP では、最低 1 つのデータ レートを [Mandatory] に設定する必要があります。AP にアソシエートするすべてのクライアントは、ネットワークを使用するための無線でこのデータ レートを物理的にサポートできる必要があります。さらに、AP にアソシエートするのがワイヤレス クライアントの場合、現状は最低値の必須レートでパケットを受信でき、無線で最大値の必須データ レートが物理的にサポートされている必要があります。複数のデータ レートが [Mandatory] に設定されている場合、マルチキャストおよびブロードキャスト フレームは、アソシエートされたすべてのクライアント共通の最大の必須伝送レートで送信されます。
- [Supported]：ユニキャスト パケットのみ、このレートでの伝送が可能です。ワイヤレス クライアントは常に、可能な範囲で最大のデータ レートでの送受信を試みます。
- [Disabled]：AP では、データはこのレートでは送信されません。

コントローラの GUI を使用してデータ レートを設定するには、[Wireless] > [802.11a/n] または [802.11b/g/n] > [Network] の順に選択し（図 3 を参照）、AP とクライアント間でのデータ伝送に使用するレートを指定します。

管理ログをチェックして、クライアント デバイスが指定したレートでネットワークに接続していることを確認します。データ レートが正しく設定されていない場合、次のような現象が発生します。

- カバレッジ ホール アラームが発生する
- チャネル使用率が高い
- 再送信が過剰に実行される
- クライアントが接続できない
- クライアントが正しくローミングされない

図 3　　データ レートの設定



802.11n

802.11n 標準により、Apple デバイスの大半（iPhone 4、iPod Touch 4、iPad および新バージョン）でワイヤレス ネットワークのパフォーマンス、信頼性、予測可能性が向上します。

ベスト プラクティスとして、802.11n を導入するときには次のガイドラインに従ってください。

- 集約 MAC サービス データ ユニット（A-MSDU）：パケット集約により、ファイル転送プロトコル（FTP）などのアプリケーションのスループットが高速化されます。ただし、チャネルの公平性はなくなります。同じカバレッジ領域内の複数の FTP プロセスで、音声アプリケーションのジッターが発生します。したがって、エンタープライズ ネットワークではパケット集約を無効にすることを推奨します。
- チャネル ボンディング：2.4 GHz の場合、802.11n には 20 MHz チャネルしか使用できないという制限がありますが、5 GHz の場合は、20 MHz と 40 MHz の両方のモードがサポートされます。チャネル密度が必要な場合（高密度環境など）は 20 MHz を使用し、クライアント トラフィックが多くの帯域幅を使用する場合（ビデオなど）は 40 MHz の使用を検討します。コントローラの GUI からチャネル ボンディングを設定するには、[Wireless] > [802.11a/n] > [RRM] > [DCA] の順に選択して、チャネルの帯域幅を図 4 のように指定します。
- 802.11n クライアントが使用する WLAN では、適切なセキュリティと QoS が有効になっていることが必要です。802.11n 標準では、セキュリティなしにするか Advanced Encryption Standard（AES）による WPA2 暗号化を設定するか、いずれかにする必要があります。また、Wi-Fi WMM を Allowed または Required に設定する必要もあります。図 5 を参照してください。
- 変調符号化方式（MCS）：WLC コード 7.3.101.0 以前では特定の MCS データ レートを有効/無効にすることができますが、図 6 に示すように、全項目を有効のままにしておくことを強く推奨します。802.11n 標準の場合、AP では 800 ns ガード インターバル（GI）の 20 MHz で MCS 0 ～ 15 が必須であり、全ステーションでは 800 ns GI の 20 MHz で MCS 0 ～ 7 が必須です（他の MCS およびモードはすべてオプションです）。これらのレートの一部を無効にすると、Mac OS 10.7 および 10.8 の 64 ビット ドライバの一部のバージョンとの互換性がなくなる可能性があります。

図 4　　DCA

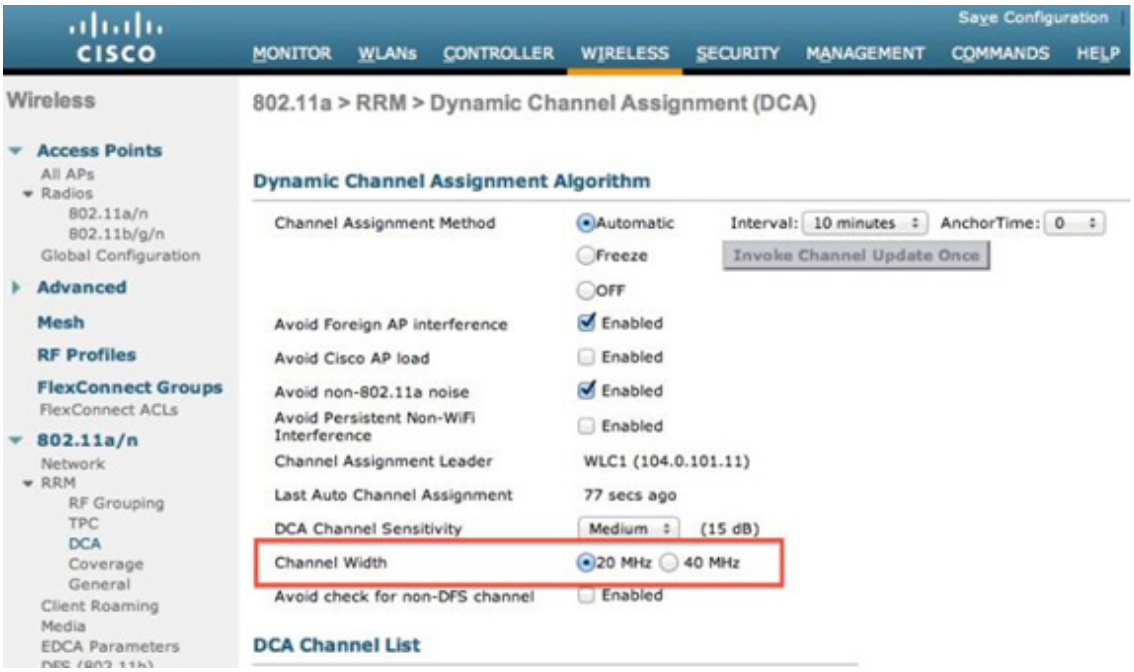


図 5　　セキュリティ

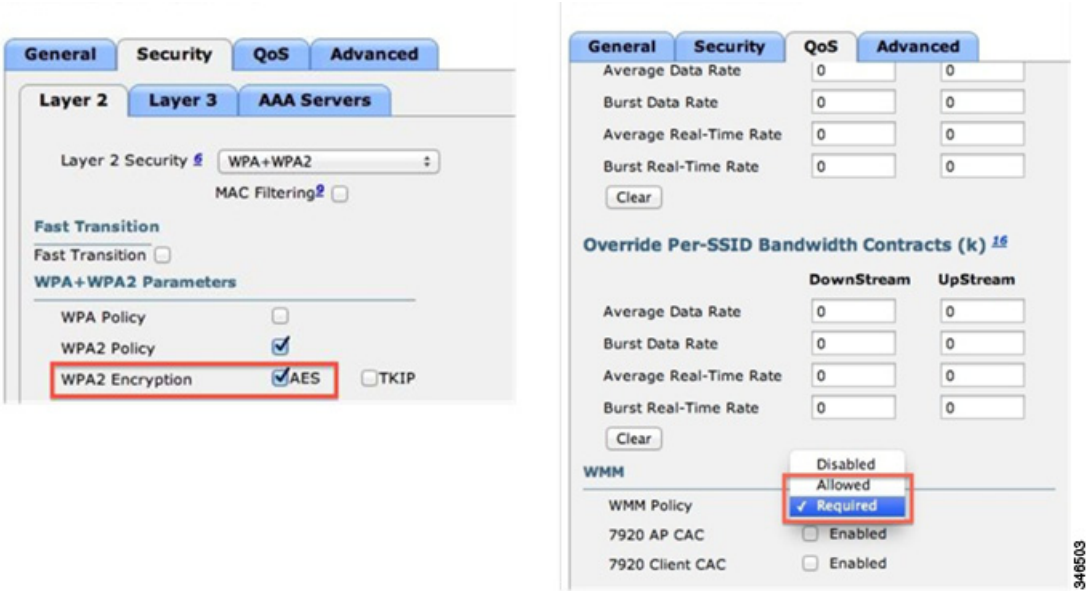
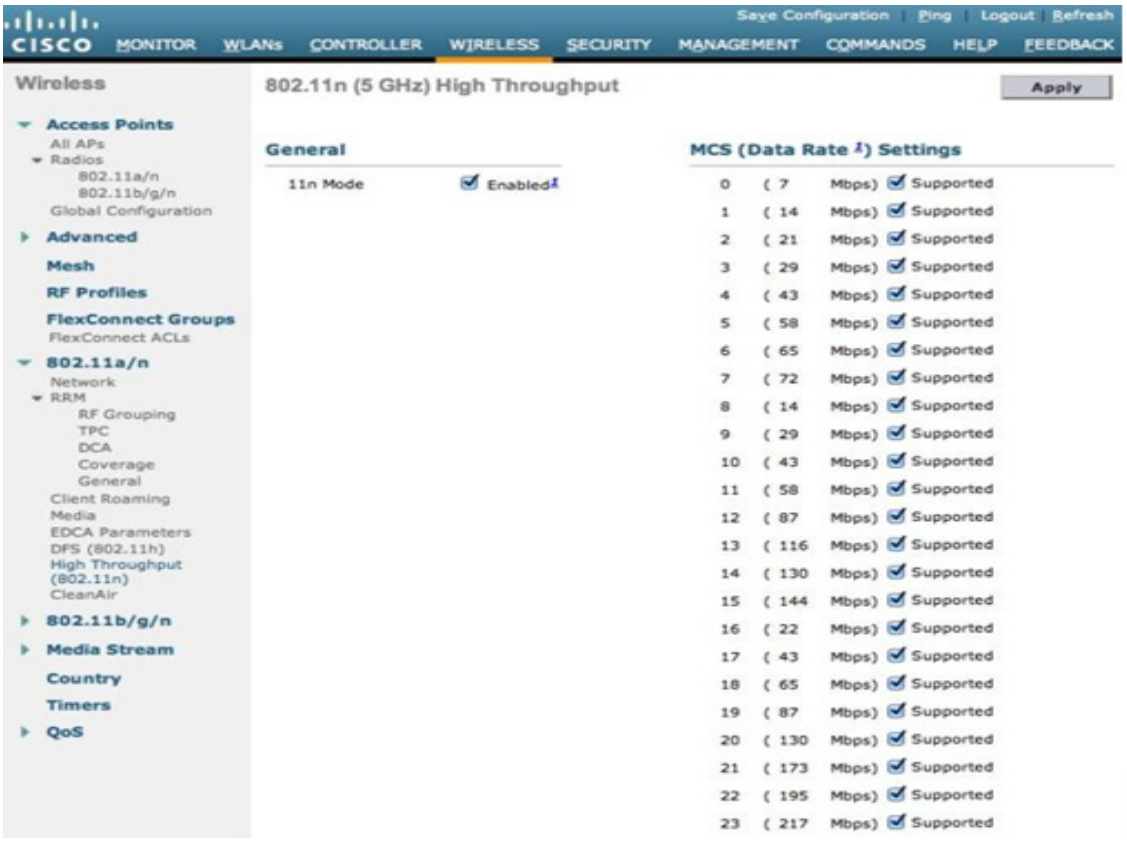


図 6　　高スループット


Save Configuration | Ping | Logout | Refresh
CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
802.11a/n
802.11b/g/n
Global Configuration
Advanced
Mesh
RF Profiles
FlexConnect Groups
FlexConnect ACLs
802.11a/n
Network
RRM
RF Grouping
TPC
DCA
Coverage
General
Client Roaming
Media
EDCA Parameters
DFS (802.11h)
High Throughput (802.11n)
CleanAir
802.11b/g/n
Media Stream
Country
Timers
QoS
802.11n (5 GHz) High Throughput
Apply
General
11n Mode
Enabled
MCS (Data Rate) Settings
0 (7 Mbps) Supported
1 (14 Mbps) Supported
2 (21 Mbps) Supported
3 (29 Mbps) Supported
4 (43 Mbps) Supported
5 (58 Mbps) Supported
6 (65 Mbps) Supported
7 (72 Mbps) Supported
8 (14 Mbps) Supported
9 (29 Mbps) Supported
10 (43 Mbps) Supported
11 (58 Mbps) Supported
12 (87 Mbps) Supported
13 (116 Mbps) Supported
14 (130 Mbps) Supported
15 (144 Mbps) Supported
16 (22 Mbps) Supported
17 (43 Mbps) Supported
18 (65 Mbps) Supported
19 (87 Mbps) Supported
20 (130 Mbps) Supported
21 (173 Mbps) Supported
22 (195 Mbps) Supported
23 (217 Mbps) Supported
346504

iOS デバイスに対応した Web 認証

ゲスト アクセス用の Web 認証

エンタープライズ ワイヤレス ネットワークで最もよく用いられるシナリオの 1 つが、ビジターにはゲスト アクセスを利用してもらうという方法です。ゲスト アクセスの場合、802.1x EAP 認証などのもっと安全な方式をセットアップするという複雑な手順を踏まなくても、ワイヤレス アクセスを簡単に利用できるようになります。

このセクションでは、WLC および iDevice のゲスト ソリューションの詳細について説明します。WLC にはゲスト サポート用の機能セットが用意されています。この機能については、次に示すシスコドキュメントを参照してください。

- ロビー アンバサダー アカウントの作成：

  http://www.cisco.com/cisco/web/support/JP/docs/WL/WLLANCntrller/5500WLCntrllers/CG/003/b_cg73_chapter_01011.html?bid=0900e4b182f76b39#d103195e96a1635

- ゲスト ユーザ用のダイナミック インターフェイスの作成：

  http://www.cisco.com/cisco/web/support/JP/110/1100/1100349_ext-web-auth-wlc-j.html#c3

- 外部 Web 認証用の WLC の設定：

  http://www.cisco.com/cisco/web/support/JP/110/1100/1100349_ext-web-auth-wlc-j.html#c5

（注） Identity Services Engine（ISE）/BYOD を使用したシナリオ、および ISE などのトピックの詳細については、次の URL にある『*Wireless BYOD with Identity Services Engine*』を参照してください。
http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bba10d.shtml

（注） BYOD の設計に関するトピックの詳細については、次の URL にある『Cisco Bring Your Own Device（BYOD）スマート ソリューション設計ガイド』を参照してください。
http://www.cisco.com/cisco/web/support/JP/docs/CVD/Borderless_Networks/001/byoddg-J.pdf

ゲスト アクセスには、通常は誤解されているセキュリティ関連事項がいくつかあり、これらを考慮に入れる必要があります。次にそれに関する情報を示します。

- 「レイヤ 3」ポリシーであるため、MAC/IP アドレス スプーフィングや傍受などのレイヤ 2 攻撃から自動的に保護されることはありません。セキュリティ ポリシーでレイヤ 2 の保護が必要とされている場合は、Web 認証と WPA/PSK、または Web 認証と WPA2/802.1x（リリース 7.4 以上）を組み合わせることを検討してください。ゲスト アクセスを使用する場合、お客様はレイヤ 2 セキュリティを問題視しない場合が多いため、ケース バイ ケースで実施してください。
- セッション タイムアウトが示す時間は、WLAN のセキュリティの再検証（再認証）が必要になるまでの時間としてクライアントで許容される「最大」時間です。つまり、セッション タイムアウトを長時間（24 時間など）に設定しても、その期間中クライアントの再認証が不要になるわけではありません。DHCP アクティビティ、アイドル タイムアウトなど、他の要因によってクライアントの接続が解除される可能性があります。

- 適切な証明書のセットアップ：後述するように、クライアント デバイスは信頼できないサーバとの HTTPS 接続を拒否することがあります。実装するゲスト アクセス ソリューションによっては、「サーバ」インフラストラクチャ（WLC、ISE、外部 Web サーバなど）にインストールされた証明書に適した信頼セットが、クライアント デバイス内に存在することが重要になります。

キャプティブ ポータルの検出

各種 iDevice には、最新のワイヤレス接続に必要な Web 認証の有無を検出するメカニズムが組み込まれています（インターネット アクセス検出）。この機能は、HTTP を介して apple.com アドレスに WiSPR 要求を送信して実行されます。

Web 認証のデフォルトでは、この接続は WLC がインターセプトしており、電話機がこのキャプティブ ポータル検出を開始するとすぐにログイン ページがユーザに表示されます。このため、クレデンシャルの入力画面がすばやく表示され、ユーザは直接認証を実行してネットワークにアクセスできます。

デバイス側のキャプティブ ポータル要求プロセスは、ユーザがデバイス上でトリガする通常の Web クライアントとは異なる方法で処理されます。このため、スプラッシュ ページのサポート、ログインのリダイレクト、または信頼できない証明書の処理などの機能が必要になります。

リリース 7.2 以降、**config network web-auth captive-bypass enable** コマンドを使用してリダイレクトを無効にできるようになりました。

これにより、WLC ではデバイスが想定する応答を「スプーフィング」し、クレデンシャルを入力しなくてもワイヤレス接続でインターネットにアクセスできるようになりました（図 7 を参照）。

図 7　　インターネット アクセスのスプーフィング

トラフィックは許可されませんが、デバイスではこの接続は「使用可能」とみなされます。
キャプティブ バイパスを有効にした場合の主な注意事項を次に示します。

- クライアント デバイスではすでにアクセス可能と「みなされて」いますが、クライアントが認証するまでトラフィックは許可されません。
- このキャプティブ バイパス機能の例外として、認証前のアクセス コントロール リスト（ACL）に許可ルールを追加すれば、認証前にトラフィックを明示的に許可できます。
- ユーザがデバイスを完全に認証するには（RUN 状態）、Safari を開き、HTTP ページに移動してログイン ページを表示する必要があります。
- クライアントは 5 分おきに削除されます。これは、クライアントが「WEBAUTH_REQ」状態になっているためで、言い換えると、アソシエーションと IP アドレスの設定は完了していても、認証が完全に完了していません。通常、クライアントはこのイベントの発生後に迅速に再アソシエーションを行います。

次のいずれかの機能を使用している場合、キャプティブ バイパスを使用する必要があります。

- スプラッシュ ページのリダイレクト：RADIUS から **url-redirect** AVP を送信します（Web 認証または条件付き Web 認証を使用している場合）。
- 外部サーバ Web 認証：外部サーバにページをホスティングして、WLC でローカル Web 認証を実行します。
- Web 認証に HTTPS を使用（信頼できる証明書を**使用しない**）：WLC ではデフォルトで自己署名証明書が使用されます。クライアント デバイスに手動で追加しない限り、自己署名証明書が信頼されることはありません。クライアントでキャプティブ リダイレクトが行われている場合、信頼できない証明書の処理が不完全になり、認証に失敗する可能性があります。したがって、Web 認証を使用する場合、Safari でのキャプティブ バイパス リダイレクトのバイパスと実行は、ユーザ要求を利用して行うことを推奨します。

信頼できる証明書

ほとんどの場合、Web 認証は HTTPS を介して実行され、Over-the-Air の場合に発生するユーザ名やパスワードのスニッフィングを防止します。したがって、サーバから提示された証明書とクライアントの間に、適切な「信頼チェーン」を構築することが重要になります。

Apple のドキュメントに記載されているように、iOS デバイスはデフォルトでいくつかの既知の証明書を信頼します。詳細については、次の URL にある「iOS 5 and iOS 6：信用できるルート証明書の一覧」を参照してください。http://support.apple.com/kb/HT5012?viewlocale=ja_JP

図 8 に、信頼できない証明書の例を示します。

図 8　信頼できない証明書の例

いずれかの認証局から WLC にインストールされた証明書は、クライアント デバイスで自動的に信頼されます。その結果、HTTPS リダイレクトの相互運用性に関する問題は防止されます。

別の方法として、Apple のエンタープライズ向け構成ツール（http://www.apple.com/jp/support/iphone/enterprise/ で入手可能）を使用してデバイス リストに信頼できる機関を追加することができます。この方法が有効なのは、デバイスを企業が完全管理しているか、ラボ テストに使用する場合のみです。

社内で公開キー インフラストラクチャ（PKI）システムが使用されている場合、このツールを使用して信頼済みリストに CA 証明書を追加できます（図 9 および図 10 を参照）。

図 9　　CA 証明書の追加

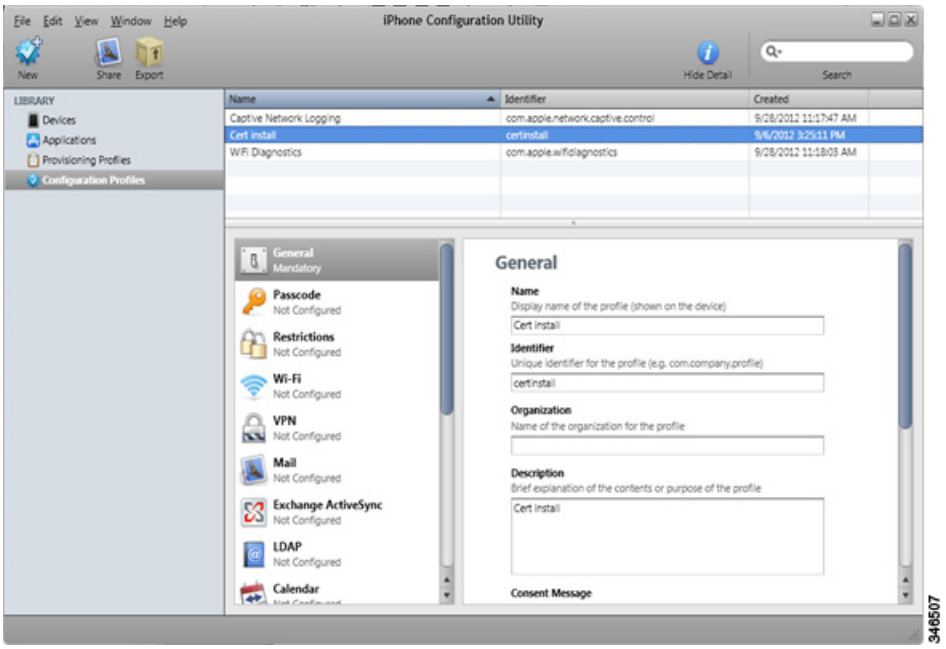
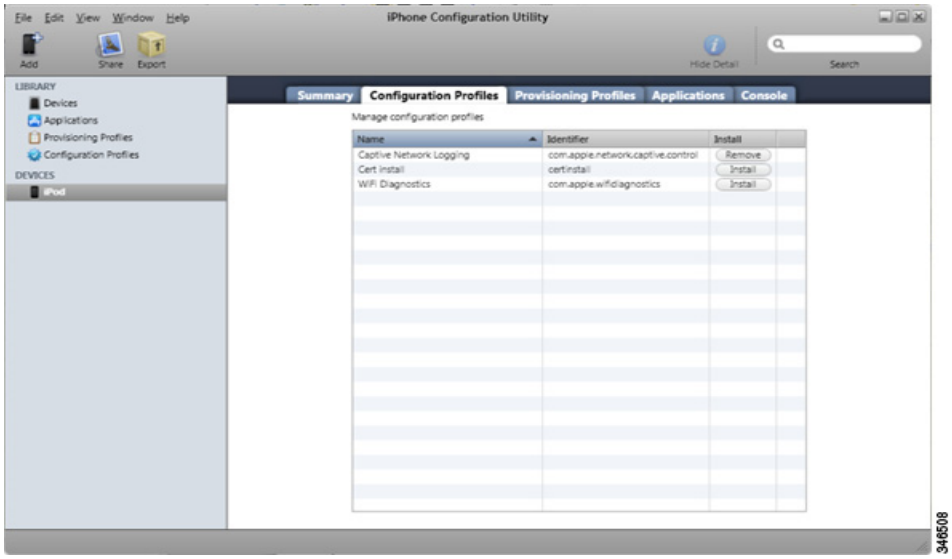


図 10　　インストール済みの信頼できる証明書



信頼済みリストに CA 証明書を追加すると、インストール済みプロファイルとしてデバイスに表示されます（図 11 を参照）。

図 11　インストール済みの信頼できるプロファイル

Web 認証のセッション時間

前述のように、ユーザはセッション タイムアウトの最大期間、認証された状態を維持します。ただし、新しい認証プロセスが必要になるまでユーザがネットワーク内に存続できる期間は、その他の要因の影響を受ける可能性があります。セッション タイムアウトは一般に、ユーザ認証が必要になるまでの最大期間と定義できますが、次のような他の要因によって、認証要求が早期にトリガされることがあります。

- **アイドル タイムアウト**：デバイスがスリープ状態になる、カバレッジの外に出る、電源がオフになるなどの理由により、ユーザがアクティブでなくなると、コントローラはデフォルトで 5 分後にクライアントの接続を解除します。非アクティブ状態の期間を延長する必要がある場合は、このタイマー値を大きくすることができます。ただし、アクティブでないユーザが長時間存続することになるため、平均ユーザ数が増大します。
- **DHCP アクティビティ**：Web 認証の状態は IP/MAC アドレスの関係に関連付けられています。DHCP 更新プロセスが発生した場合、または DHCP 検出の試みがクライアントから行われた場合、そのプロセス中にクライアントによって IP アドレスが変更されると、WLC は Web 認証の状態をクリアすることがあります。
- **ローミング**：802.11 ネットワークでは非常に重要なプロセスです。ローミング イベント中に、クライアントが新しい AP または WLC に対するローミングを完全に完了できなかった場合、クライアントの状態はクリアされ、必要とされる新たな Web 認証の手順が途中で終了する可能性があります。

- **L2 ポリシー**：WPA2-PSK などのレイヤ 2 ポリシーと Web 認証などのレイヤ 3 ポリシーが混在している場合、クライアントはすべての要件に適合している必要があります。そうでないクライアントは終了します。これによってセキュリティは強化されますが、その副作用として、追加条件に応じてクライアントが削除される可能性があります。特に、Extensible Authentication Protocol over LAN（EAPoL）交換が完了していない場合や、デフォルトで 60 分おきに発生するブロードキャスト キー ローテーション中は、ローミングの失敗に注意する必要があります。クライアントには、AP から送信された EAP 要求に応答する機能が必要です。これにより、グループ キー ローテーション通知がトリガされて、クライアントの認証が解除されます。

Web 認証と WPA2-PSK を使用する場合、EAP の再試行回数およびブロードキャスト キー ローテーションをデフォルト値よりも大きくして、デバイスがスリープ状態になってもクライアントの Web 認証の状態がクリアされないようにすることを推奨します。Web 認証のセッション時間の設定を変更するコマンドは、**config advanced eap bcast-key-interval X** です。

デフォルトの間隔は 60 分です。

（注） セキュリティの厳格化という観点から見ると、タイマーの時間を長く設定することは望ましくありません。

EAP 要求のコマンドは、**config advanced eap request-retries X** です。

デフォルトの再試行回数は 2 回です。通常はこの設定に伴う副次的な影響はありませんが、例外として、EAP エラーが発生した場合にはクライアントの認証解除までの時間が長くなります。

トラブルシューティング

WLC を使用した iPhone の問題の診断

Cisco AP は、iPhone/iPad の接続に関する問題が生じた、まさにその場所にあります。それらは同じ Wi-Fi 状況を共有しています。したがって、AP と組み合わせた WLC は、初級レベルのデバッグに必要なリアルタイムかつ洗練された情報源になります。

AP で検出された内容は、リモートでグラフィカルに表示して確認できます。WLC では iPhone の周囲の Wi-Fi チャネル状況がレポートされます。iPhone のリモート テストを WLC で実行することもできます。また、電話機のリンク接続品質もレポートされます。さらに、Wi-Fi のリアルタイム品質、現在の干渉デバイス、AP に接続されているデバイス数、AP のコール数、Wi-Fi チャネルの利用率もレポートされます。この情報は、問題の原因を特定するうえで重要です。また、レポート機能の実行にあたって、エンド ユーザが直接操作する必要はありません。

Apple Web サイトの一部のドキュメントで、WLC を使用して低レベルのトラブルシューティングを行う方法が紹介されています。次に示すのはシスコの推奨事項です。ここでは、高品質の接続やアプリケーション パフォーマンスの妨げになる可能性のある問題について、環境および設定の面から考察します。

企業の導入環境では、Wi-Fi チャネルのデバイス数が多すぎるために帯域幅が不足し、それが原因で Wi-Fi ネットワーク接続の確立を試みるデバイスを追加接続できなくなることがあります。WLC のパラメータ設定によって、iPhone が接続できなくなる場合があります。WLC はこのような状況の判別に最適なツールです。

Csico AP には、十分なスペクトル分析機能を備えたモデルがあります。シスコが提供する PC ツールを使用して、このような AP の電話接続固有のスペクトル分析を離れた場所からリアルタイムで行うことができます。このツールを使用すれば診断プロセスの役に立ち、電話機やエンドユーザの関与がなくても、Wi-Fi チャネル状況に関連する問題を解決できる場合があります。

WLC のモニタリング機能を使用して、接続上の問題の原因となる可能性がある不正 AP やアドホック不正クライアントのリストを表示することもできます。モニタリング機能は Syslog サーバ（場合に応じて追加可能）に移行できます。ログは一般的なレベルおよびファシリティに設定できます。

Wi-Fi 環境の把握

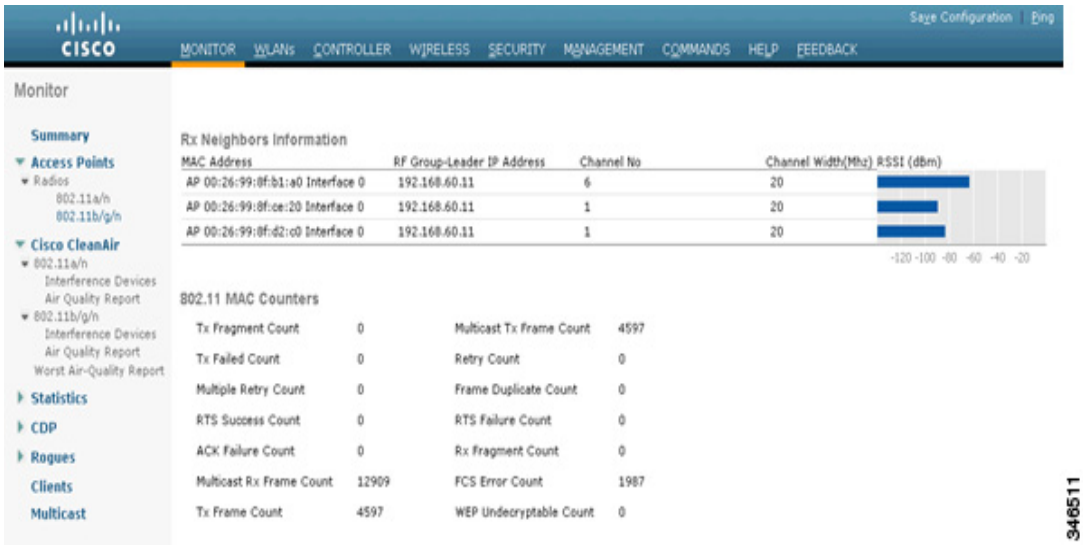
iPhone のコール品質およびローミング パフォーマンスは、AP カバレッジの広さおよび Wi-Fi チャネルの帯域幅に比例します。図 12 に示した WLC のグラフィック インターフェイスには、この 2 つの条件に関連するデータが示されています。[WLC] > [Monitor] > [Access Points] > [Radio(bands)] を選択すると、特定の AP を表示できます。このページには、AP の情報と、この AP のカバレッジ領域内の Wi-Fi 状況に関する情報が複数行にまたがって表示されます。各行の末尾に、ドロップダウン メニュー ボタンがあります。このメニュー ボタンを選択すると、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。表示されるデータは、Wi-Fi チャネル番号、このチャネルの干渉、現行チャネルの負荷に関する統計情報、Voice over IP（VoIP）コール数、およびその他の情報です。

また、このウィンドウには [Client Count vs RSSI] および [Client Count vs SNR] も表示されます。この情報を使用すると、電話機の機能上のデータ レートと、RSSI や SNR の影響で通話中に実際に使用されるデータ レートを特定して、iPhone のパケット送信速度を推察できます。

クライアントに関するこの情報の次に、[Rx Neighbors Information] が表示されます（図 13 を参照）。ネイバー情報を使用して、電話機をアソシエートした AP に隣接する複数の AP 間のカバレッジ オーバーラップの量をすばやく理解できます。ネイバー情報は 802.11k 仕様で使用します。この IEEE 仕様では無線管理情報を扱っています。

図 12　　AP および Wi-Fi の状況

図 13　　受信ネイバーの情報



（注）　シスコは、AP 隣接セル間の Wi-Fi 信号のオーバーラップ率として 15% を推奨しています。本書の「Wi-Fi チャネル カバレッジ」（P.3）を参照してください。

WLC クライアントの統計情報の詳細は、[Band Select Statistics] に表示されています。このデータは、AP に接続されているデュアルバンド デバイス（iPhone5 など）の数を示します。

iPhone の Wi-Fi 環境を把握するには、次に接続ステータスを調べます。同様に、個々の電話機の情報を示すウィンドウが表示されます。この情報は、電話機の Wi-Fi MAC アドレスをもとにアクセスするデータベースに格納されています。電話機でこの値を調べるには、電話機上で [設定] > [一般] > [情報] > [Wi-Fi アドレス] を選択します。

WLC の接続先 AP に現在アソシエートしているすべての電話機の MAC アドレスを WLC に表示するには、[Monitor] > [Clients] を選択します。クライアントの MAC アドレス、クライアントがアソシエートしている AP の名前、WLAN SSID、および 802.11 プロトコルが行別に表示されます。AP の名前のリンクをクリックすると、iPhone 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。表示される情報は、クライアントのプロパティ、およびそのクライアントがアソシエートしている AP のプロパティです。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、現在のデータ レート セット、セキュリティ情報、QoS プロパティなどが表示されます。

このウィンドウには Wi-Fi の重要な統計情報が表示されます。最も重要なのは RSSI 値です。RSSI フィールドには、AP で受信されたパケットの信号強度が表示されます。この値は AP においてクライアント パケットがどれだけ良い状態で見れたかを示します。RSSI 値が -45 dBm の信号は、-67 dBm の信号よりも強力です。RSSI 値が重要なのは、カバレッジ品質を特定できるためです。この値が低すぎると、電話機のコール品質は低下します。またこの値から、AP 台数の追加の必要性や、より良い AP（への交換）の必要性もわかります。この RSSI 値は、クライアントの Wi-Fi パフォーマンスを示す重要な指標です。製品比較やサイト設計を行う際には、この値を使用する必要があります。

電話機のオーディオ パケットが AP で受信されない場合、そのコールの動作は片通話状態になります。RSSI 値が -45 ～ -67 dBm のパケットは、より高速なデータ レートで送信される可能性が高くなります。これは、両方とも強力な Wi-Fi 信号であるためです。電話機が AP から遠ざかると、RSSI 値は小さくなります。

電話機が AP から離れた場所に移動すると、それに伴って生じる信号強度の低下を補うために、各パケットのデータ レートは低くなります。このため、パケット配信の信頼性は高まりますが、電話機のスループットは低下し、使用帯域幅は大きくなります。電話機で必要とされる帯域幅が増加すると、その電話機と AP で使用される Wi-Fi チャネルの空き帯域幅が小さくなります。Wi-Fi チャネルの使用帯域幅が増えると、もう 1 つの Wi-Fi チャネルのパフォーマンス指標に当たる要素も増えます。ここで言うもう 1 つの指標とは、チャネル使用率のことです。

チャネル使用率は、AP の無線統計情報ページに表示される、チャネル負荷に関する統計情報の 1 つです。RSSI とチャネル使用率は、コールの品質を左右する主要な要素です。メディアとは、アソシエーションによって電話機と AP とで共有されることになる Wi-Fi チャネルです。Wi-Fi チャネルは、別の AP、別の電話機、および別のデバイス（Wi-Fi 対応と非 Wi-Fi 対応の両方）でも共有されます。チャネルを共有する別の Wi-Fi デバイスは、同一チャネル干渉としてチャネル使用率に影響します。非 Wi-Fi の干渉でもチャネル使用率に影響します。非 Wi-Fi 干渉をもたらすものには、Bluetooth デバイス、電子レンジ、監視カメラなど、802.11 プロトコルを使用しないけれど Wi-Fi チャネルと同じ無線周波数を使用するデバイスが含まれます。チャネル使用率の低下を防ぐには、不正 Wi-Fi デバイスおよび非 Wi-Fi 干渉をできるだけ効率的に管理する必要があります。

また、チャネル使用率を管理するうえでは、Wi-Fi チャネルで使用される有効なデバイス数および有効なアプリケーション数の管理も必要です。WLC の設定によって、AP で許可される（したがって AP の Wi-Fi チャネルで許可される）オーディオ コール、ビデオ コール、およびアプリケーションの数を制限することができます。この機能を管理する WLC の設定として、コール アドミッション制御（CAC）や AVC などがあります。

（注） これらの設定オプションの詳細については、次の URL にある『Cisco Wireless LAN Controller コンフィギュレーション ガイド』を参照してください。
http://www.cisco.com/cisco/web/support/JP/docs/WL/WLLANCntrller/5500WLCntrllers/CG/003/b_cg73.html

詳細については、次に示すコンテンツおよび Cisco Validated Design（CVD）のドキュメントの各セクションを参照してください。

- 音声用の Wi-Fi 設計の原則については、次の URL にある『Voice over Wireless LAN 4.1 デザイン ガイド』を参照してください。
  http://www.cisco.com/cisco/web/support/JP/docs/WL/WLLANMGMT/WLCntrlSystem/SDG/002/14684_01.html
- 高密度 Wi-Fi の導入：次の URL にあるドキュメントの「Design Point」と題された各セクションを参照してください。
  http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10981/design_guide_c07-693245.html
- Identity Services Engine（ISE）/Bring Your Own Device（BYOD; 個人所有デバイスの持ち込み）：次の URL にあるドキュメントの「ユーザ エクスペリエンス」-「Apple iOS デバイス」セクションを参照してください。
  http://www.cisco.com/cisco/web/support/JP/docs/CVD/Borderless_Networks/001/byoddg-J.pdf

WLC でのワイヤレス クライアントのデバッグ

コマンド **debug client <*MAC_Address*>** は、8 つのデバッグ コマンドと、指定した MAC アドレス上のフィルタを有効にして、指定した MAC アドレスを含むメッセージのみを表示するマクロです。8 つのデバッグ コマンドにより、クライアントのアソシエーションおよび認証に関する最も重要な情報が表示されます。ワイヤレス クライアントが複数存在する場合は、フィルタを使用すると便利です。

（注） リリース 7.2 以降では、**debug client** コマンドは次に示すように最大 3 つのクライアントを同時にサポートします。**debug client** <*MAC_Addr1*> <*MAC_Addr2*> <*MAC_Addr3*>

debug client を実行すると、次のデバッグが有効化されます。

```
(Cisco Controller) > show debug

MAC address.........................00:00:00:00:00:00
Debug Flags Enabled:
  dhcp packet enabled
  dot11 mobile enabled
  dot11 state enabled
  dot1x events enabled
  dot1x states enabled
  pem events enabled
  pem state enabled
```

以上のコマンドで、アドレス ネゴシエーション、802.11 クライアント ステート マシン、802.1x 認証、Policy Enforcement Module（PEM）、およびアドレス ネゴシエーション（DHCP）がカバーされます。

さまざまな状況に応じてトラブルシューティングを行う場合、次の **debug** コマンドを **debug client** に追加できます。

- 802.1X 認証：
  - **debug aaa events enable**
  - **debug aaa detail enable**
- Web 認証（リリース 7.2 以降）：
  - **debug web-auth redirect enable IPOFCLIENT**

次に、802.11k で使用する **debug** コマンドを示します。

- (Cisco Controller) > **debug 11k ?**
- **errors** 802.11k エラーのデバッグを設定
- **detail** 802.11k 詳細情報のデバッグを設定
- **history** 802.11k ローミング履歴のデバッグを設定
- **all** 802.11k の全イベントのデバッグを設定
- **>debug 11k {all/event/errors/detail] [enable|disable]**

次に、802.11r で使用する **debug** コマンドを示します。

- **11r / FT Debug**:
- (Cisco Controller) >**debug FT ?**
- **Events** 802.11r イベントのデバッグを設定
- **>debug ft events{enable|disable}**

（注） WLC でクライアントのデバッグを行う方法の詳細については、『Understanding Debug Client on Wireless LAN Controllers (WLCs)』またはビデオ「Troubleshooting Client Connection Issue on Cisco Wireless Controllers」を参照してください。

Apple iOS デバイスでのリモート パケット キャプチャの実行

iOS5 以降のリリースでは、Apple iOS デバイスのワイヤレス アダプタを介して送信されたパケットをリモートでキャプチャできます。この機能を使用すると、これらのプラットフォームのトラブルシューティングが飛躍的に向上します。Xcode 4.2 以降を実行している Mac OS X が必須です。Mac で Remote Virtual Interface（RVI）を設定する必要があります。これによりインターフェイスが作成され、Wireshark や他の推奨 OS X キャプチャ機能を通してキャプチャできるようになります。

iOS デバイスでキャプチャを開始する手順は、次のとおりです。

ステップ 1 USB ケーブルで Mac に iOS デバイスを接続します。

ステップ 2 次の URL から Apple Xcode 4.2 以降をダウロードして、インストールします。
http://developer.apple.com/xcode/

ステップ 3 iOS の Unique Identifier（UDID）を特定します。iTunes を起動し、左側の列の [デバイス] でお使いの iPhone を選択します。選択したら、[シリアル番号] をクリックすると表示が切り替わり、UDID が表示されます。この値はステップ 5 で使用します。

ステップ 4 [ユーティリティ] > [ターミナル] を選択して、ターミナルを起動します。

ステップ 5 iOS デバイスの UDID を使用して、RVI を作成します。

```
MacBookPro:~ client$ rvictl -s <UDID of iOS device>

Starting device UDID of iOS device
SUCCEEDED
```

（注） 現在のデバイスのリストを表示するには、**ifconfig –l** を使用します。

ステップ 6 Wireshark または推奨キャプチャ ツールを使用して、新しい rvi# インターフェイスでキャプチャを開始します。

ステップ 7 作業が終了したら、次のコマンドを実行して RVI を削除します。

```
MacBookPro:~ client$ rvictl -x <UDID of iOS device>

Stopped device UDID of iOS device
SUCCEEDED
```

（注） iOS デバイスでパケットをキャプチャする方法の詳細については、次の URL にある「Mac Developer Library」を参照してください。http://developer.apple.com/library/mac/#qa/qa1176/_index.html

ワイヤレス スニファ キャプチャの実行

802.11 Wi-Fi デバイスが通常どおりに動作する仕組みや理由を理解するには、ワイヤレス パケット キャプチャ（「スニファ」アクション）を実行すると非常に便利です。この機能は、Cisco Technical Assistance Centre（TAC）と連携して技術的な問題を解決する場合に、特に重要となります。ワイヤレス スニファの選択と使用の詳細については、次の記事を参照してください。

- 「Fundamentals of Wireless Sniffing」（いくつかの重要なガイドラインを参照できます）：https://supportforums.cisco.com/docs/DOC-19136
- 「Wireless Sniffing using a Mac with OS X 10.6 and Above」：https://supportforums.cisco.com/docs/DOC-19212
- 「Wireless Sniffing in Windows 7 with Netmon 3.4」：https://supportforums.cisco.com/docs/DOC-16398
- 「Collecting a Wireless Sniffer Trace using the Cisco Lightweight AP in Sniffer Mode」：https://supportforums.cisco.com/docs/DOC-19214
- OmniPeek Remote Assistant：http://www.wildpackets.com/products/omnipeek_remote_assistant

（注） Linksys USB600N がショート ガード インターバルの 802.11n パケットを収集する場合、高い信頼性は望めません。たとえば、ショート ガード インターバル パケットの 20 ～ 30% が損失します。必要に応じて、より低速なロング ガード インターバルのみを使用するように WLC の設定を変更してください。この設定変更は一時的に行う必要があります。使用するコマンドは、**config 802.11{a | b} 11n support guard-interval {any | long}** です。

なお、次のようなワイヤレス スニファ製品が市販されています。

- WildPackets 社の OmniPeek
- Fluke 社の AirMagnet Wi-Fi Analyzer
- TamoSoft 社の CommView for Wi-Fi
- Riverbed 社（旧 CACE 社）の AirPcap

Apple iOS デバイスでのデバッグとロギング

iPhone 構成ユーティリティ（IPCU）を使用すると、iPad、iPhone、または iPod Touch から一連の拡張ログを収集できます。

- Mac OS X の場合：http://support.apple.com/kb/DL1465?viewlocale=ja_JP
- Windows の場合：http://support.apple.com/kb/DL1466?viewlocale=ja_JP

お使いの iOS デバイスから拡張ログを収集する手順は、次のとおりです。

ステップ 1 IPCU をダウンロードして、iPhone、iPad、または iPod Touch と併用するコンピュータにインストールします。

ステップ 2 次の Shell コマンドを実行して、iPhone 構成ユーティリティのデバッグ ロギング オプションを有効にします。

Mac OS X の場合：

ターミナルを起動し（[ユーティリティ] > [ターミナル]）、次のように入力します。

```
defaults write com.apple.iPhoneConfigurationUtility
EnableDebugLoggingInterface YES
```

Windows OS の場合：

コマンド ラインで次のように入力します。

```
cd c:\Program Files\iPhone 構成ユーティリティ \ipcu.exe
-enableDeviceLogCapture
```

ステップ 3 iPhone 構成ユーティリティを起動し、[デバイス]（左のサイドバー）で iPhone、iPad、または iPod Touch を選択します。

ステップ 4 [ファイル] > [書き出す] >（モバイル デバイスのプロファイル）を選択してデバイス プロファイルをエクスポートし、ローカル ディレクトリに保存します。

ステップ 5 [コンソール] タブをクリックし、[コンソールを別名で保存]（Mac）または [コンソールに名前をつけて保存]（Windows）を選択して、ステップ 4 で使用したのと同じ場所にコンソール出力を保存します。

（注） iOS デバイスのトラブルシューティングの詳細については、次の URL にあるエンタープライズ向け iOS サポート ページを参照してください。
http://www.apple.com/jp/support/iphone/enterprise/

Apple Mac OS X サプリカントでのデバッグとロギング

OS X 10.6 以前の場合：

ステップ 1 ターミナルを起動します（[ユーティリティ] > [ターミナル]）。

ステップ 2 get-mobility-info データを収集します。

```
MacBookPro:~ client$ sudo
/System/Library/Frameworks/SystemConfiguration.framework/Resources/get-mobility-info
Password: <Enter Password>
Please wait, collecting statistics
Network data collected to "/Users/client/Desktop/mobility-info-...tar.gz”
```

OS X 10.7 以降の場合：

OS X 10.7（Lion）には、さらに Wi-Fi のトラブルシューティングを実行できる Wi-Fi 診断ユーティリティが追加されています。Wi-Fi 診断ユーティリティでは、次のタスクを実行できます。

- パフォーマンスのモニタ（信号、ノイズ、BSSID など）
- Wi-Fi イベントの記録（アソシエーション、再アソシエーション、認証解除など）
- ワイヤレス スニファ キャプチャの実行
- デバッグ ロギングの有効化

Wi-Fi 診断ユーティリティを開く手順は、次のとおりです。

ステップ 1 Finder で [移動] > [フォルダへ移動] を選択します。

ステップ 2 「*/System/Library/CoreServices/*」と入力して、[移動] を選択します。

ステップ 3 [Wi-Fi 診断] を選択すると、画面が開きます。

OS X サプリカントでの 802.1x 認証の失敗に関するロギング

ステップ 1 ターミナルを起動します（[ユーティリティ] > [ターミナル]）。

ステップ 2 802.1x ロギングを有効にします。

```
MacBookPro:~ client$ sudo defaults write
Library/Preferences/SystemConfiguration/com.apple.eapolclient LogFlags -int -1
Password: <Enter Password>
```

ステップ 3 コンピュータを再起動（設定を適用）します。

ステップ 4 Finder で [移動] > [フォルダへ移動] を選択します。

ステップ 5 「*/var/log/*」と入力して、[移動] を選択します。

ステップ 6 サプリカント ログのタイトルは「eapolclient.<interface>.log」となります。

ステップ 7 作業が終了したら、ターミナルで次のように入力して、ロギングを無効にします。

```
MacBookPro:~ client$ sudo defaults write
/Library/Preferences/SystemConfiguration/com.apple.eapolclient LogFlags -int 0

Password: <Enter Password>
```

ステップ 8 コンピュータを再起動（設定を適用）します。

推奨事項のまとめ

本書ではいくつかの推奨事項を紹介しました。ここではそれらをまとめて示します。

- シスコは、デュアルバンド デバイスに 5 GHz カバレッジ設計を使用することを推奨しています。5 GHz チャネルのチャネル使用率は一般的に、2.4 GHz チャネルと比べるとはるかに低くなっています。

- WLC のレポートを使用して、チャネル使用率を入念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、新しい干渉源の出現、AP の停止、または新しい Wi-Fi デバイスの大量流入を示している可能性があります。
- シスコは、頻繁にチャネルが変更される AP をモニタし、既知の干渉源の影響を受ける 5 GHz Wi-Fi チャネルを特定して DCA 除外リストに追加することを推奨しています。
- 2.4 GHz でカバレッジ テストを実行する際には、低いデータ レートを無効にすることを推奨します。これは、-67 dBm RSSI のカバレッジ領域が 1 Mbps データ レートで 12 Mbps を大きく上回るからです。範囲と帯域幅のいずれを重視した設計にするかは、この点を考慮して決めます。
- ビーム フォーミング（ClientLink）により 802.11a よりも高品質のリンクと音声品質が提供されるため、5 GHz 帯域では 802.11n を使用することを推奨します。
- シスコは、WLAN 設定で「BandSelect」を有効にすることを推奨しています。特定の状況で iPhone5 の 5 GHz 帯域に偏りが見られるような場合でも、BandSelect を有効にしておくと、電話機の信号強度が両方の帯域に対して適切な設定になっていれば 5 GHz での接続率を向上させることができます。
- シスコは、QoS 値が platinum または voice で WMM が必須（required）に設定された WLAN に、iPhone および iPad を接続することを推奨しています。この設定により、AP から送信されたイーサネット トラフィックが、Wi-Fi チャネルでの優先度を表す QoS 値を使用してスイッチ ポートに接続できます。
- Jabber やその他のビジネス アプリケーションの場合、デバイスの WMM ドライバまたは QoS ポリシーによって WMM QoS 値が低下したパケットにおいてもアプリケーションに必要な QoS レベルを獲得できるように、QoS 値を platinum にすることを推奨します。
- シスコは、ネイバー リスト応答パケットで 2.4 GHz および 5 GHz の両方の AP チャネル番号が提示されるよう、WLC の設定で RRM を有効にすることを推奨しています（802.11k）。Voice over WLAN コールだけでなく、すべてのアプリケーションとデバイスで、5 GHz 帯域 Wi-Fi チャネルを使用することを推奨します。
- シスコおよび Apple は、Fast Transition 802.1x クライアント用に追加の WLAN を設定することを推奨しています。
- シスコおよび Apple は、Fast Transition PSK クライアント用に追加の WLAN を設定することを推奨しています。
- Apple は、レガシー クライアントに別個の WLAN および SSID を使用することを推奨しています。
- シスコは、チャネルのカバレッジで必要となるクライアント数に適したカバレッジが、チャネルのカバレッジで必要となる帯域幅で提供されるように、データ レートを調整することを推奨しています。
- シスコは、チャネル ボンディングでは、チャネル密度が必要な場合（高密度環境など）には 20 MHz を使用し、クライアント トラフィックが多くの帯域幅を使用する場合（ビデオなど）には 40 MHz の使用を検討することを推奨しています。
- シスコは、すべての MCS レートを有効のままにしておくことを強く推奨します。レートの一部を無効にすると、Mac OS 10.7 および 10.8 の 64 ビット ドライバの一部のバージョンとの互換性がなくなる可能性があります。
- シスコは、AP 隣接セル間の Wi-Fi 信号のオーバーラップ率として 15% を推奨しています。

詳細については、Apple 関連サービスおよび Cisco WLAN に関する次のリソースを参照してください。

- 『ワイヤレス LAN Apple Bonjour 導入ガイド』:
  - http://www.cisco.com/cisco/web/support/JP/111/1110/1110670_cuwn-apple-bonjour-dg-00-j.html
- 『Cisco Wireless LAN Controller System Management Guide, Release 7.4』:

  - http://www.cisco.com/en/US/docs/wireless/controller/7.4/configuration/guides/system_management/config_system_management.html

- Mac Wi-Fi アップデート 1.0：http://support.apple.com/kb/DL1620?viewlocale=ja_JP

（注） 本書および Apple Web サイトに記載された参照リンクについては、シスコの一般的なドキュメントと同様に定期的にチェックして、本書発行後に内容が更新されていないか確認することを推奨します。

付録 A：IEEE IP DSCP - AVVID 値および 802.11e WMM

AVVID 802.1pUP ベースのトラフィック タイプ	AVVID 802.1pUP	AVVID IP DSCP	IEEE IP DSCP	IEEE 802.eUP	注記
予約済み（ネットワーク制御）	7	56?	56	7	TBD
予約済み	6	48?			TBD
音声	5	46（EF）	48	6	
音声	4	34（AF41）	40	5	
音声制御	3	26（AF31）	32	4	
バックグラウンド（Gold）	2	18（AF21）	16	2	
バックグラウンド（Gold）	2	20（AF22）	16	2	
バックグラウンド（Gold）	2	22（AF23）	16	2	
バックグラウンド（Silver）	1	10（AF11）	8	1	
バックグラウンド（Silver）	1	12（AF12）	8	1	
バックグラウンド（Silver）	1	14（AF13）	8	1	
ベスト エフォート	0	0（BE）	0、24	0、3	
バックグラウンド	0	2	8	1	
バックグラウンド	0	4	8	1	
バックグラウンド	0	6	8	1	
有線からの未知の DSCP	アクセス ポート	D	任意	D>>3	AP 上

付録 B：対照表（概略）

	Wi-Fi 無線	11r Fast Transition 認証	11k ネイバーリスト	使用可能な Webex クライアント	使用可能な Jabber クライアント
iPhone iPhone3G iPhone 4 iPad	11g 20 MHz ワイド チャネル のみ	なし	なし	あり	あり
iPhone 4S iPad2	2.4 GHz 11g および 11n MCS 0 ～ 7 20 MHz ワイド チャネルのみ	iOS6 の場合：あり あり	iOS6 の場合：あり あり	あり	あり
iPhone 5 iPad Retina iPad Mini	2.4 および 5 GHz 11n MCS 0 ～ 7 2.4 GHz では 20 MHz ワイド 5 GHz では 20 または 40 MHz	あり	あり	あり	あり

付録 C：略語

A-MDSU	Aggregated MAC Service Data Unit（集約 MAC サービス データ ユニット）
ACL	Access Control List（アクセス コントロール リスト）
AP	Access Point（アクセス ポイント）
AVC	Application Visibility and Control
AVVID	Architecture for Voice Video and Integrated Data
BSS	Basic Service Set（基本サービス セット）
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device（個人所有デバイスの持ち込み）
CA	Certification Authority（認証局）
CAC	Call Admission Control（コール アドミッション制御）
CVD	Cisco Validation Design
DCA	Dynamic Channel Allocation
DS	Distribution System（分散システム）
DSCP	Differentiated Services Code Point（DiffServ コード ポイント）
FT	Fast Transition
FTP	File Transfer Protocol（ファイル転送プロトコル）
GHz	ギガヘルツ
GI	Guard Interval（ガード インターバル）
IEs	Information Element（情報要素）
IPCU	iPhone Configuration Utility（iPhone 構成ユーティリティ）
MAC	Medium Access Control（メディア アクセス コントロール）
Mbps	Megabits per second（メガビット / 秒）
MCS	Modulation Coding Schemes（変調符号化方式）
MOS	Mean Opionion Score
PKI	Public Key Infrastructure（公開キー インフラストラクチャ）
PSK	Pre-Shared Key（事前共有キー）
QoS	Quality of Service
RF	Radio Frequency（無線周波数）
RRM	Radio Resource Management（無線リソース管理）

RSSI	Received Signal Strenght Indicator（受信信号強度）
RToWLAN	Real-Time over Wireless LAN
RVI	Remote Virtual Interface
SKC	Sticky Key Caching
SNR	Singal-to-Noise Ratio（Singal-to-Noise 比）
SSID	System Set Indentifier
TAC	Technical Assistance Centre
TSpec	Traffic Specification（トラフィック仕様）
UDID	Unique Identifier（固有識別子）
VoWLAN	Voice over Wireless LAN
VPN	Virtual Private Network（バーチャル プライベート ネットワーク）
WiSPR	Wireless Internet Service Provider Roaming
WLAN	Wireless Local Area Network（ワイヤレス ローカル エリア ネットワーク）
WLC	Wireless LAN Controller（ワイヤレス LAN コントローラ）
WMM	Wireless Multimedia
WPA	Wi-Fi Protected Access

この資料の記載内容は2008年10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。

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
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/