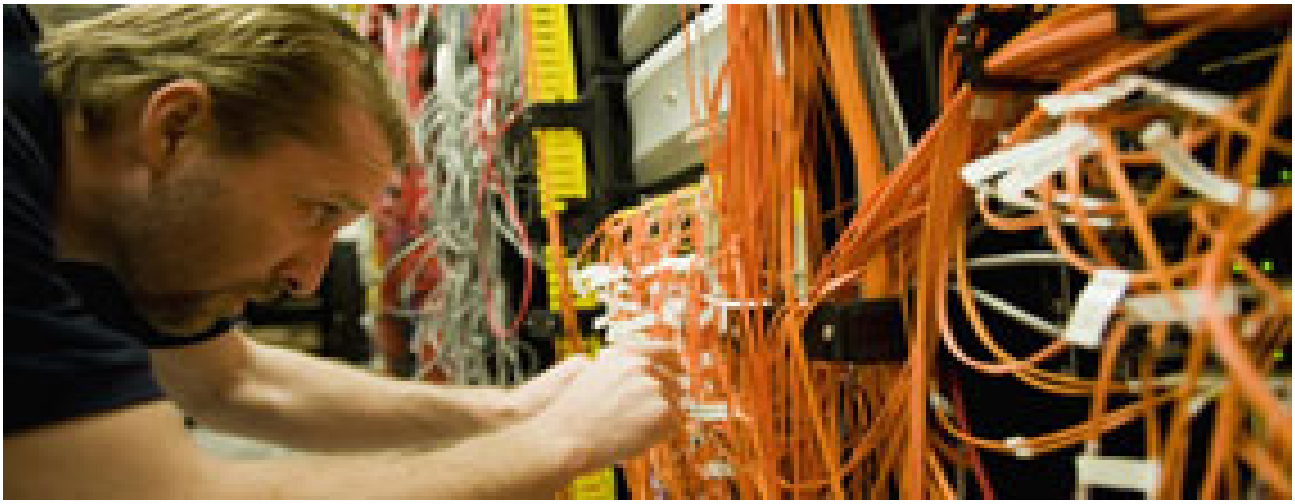


Wi-Fi 接続の最適化とビジネス アプリケーションの優先順位付け

目次

はじめに 3
要件 3
使用されるコンポーネント 3
表記法 4
Adaptive 11r 4
設定手順 4
debug コマンド 8
SNMP 8
11k および 11v の常時有効化 8
優先されるビジネス アプリケーション 10
機能概要 11
設定手順 12
debug コマンド 19
SNMP 20

はじめに

802.11r 対応 WLAN は、ワイヤレス クライアント デバイスのローミングを高速化します。ローミング エクスペリエンスを向上させるためには、iOS 10 を実行する iOS デバイスを 11r 対応 WLAN に接続できるようにすることをお勧めします。ただし、WLAN で 11r を有効にすると、FT AKM のビーコンおよびプローブ応答を認識しないレガシー デバイスを WLAN に接続することができなくなります。何らかの方法で、クライアント デバイスの機能を識別して 11r 対応デバイスを FT 対応デバイスとして WLAN に接続可能にし、同時に、レガシー デバイスを 11i/WPA2 デバイスとして接続できるようにする必要があります。Cisco WLC ソフトウェア リリース 8.3 は、802.11i 対応 WLAN 上の 802.11r を iOS デバイスに対して選択的に有効化することができます[1]。対応する iOS デバイスはこの機能を識別し、WLAN 上で FT アソシエーションを行います。シスコ ワイヤレス インフラストラクチャでは、非 FT WLAN で FT アソシエーションをネゴシエートできるデバイスから、WLAN 上で FT アソシエーションを行うことが、可能になります。

さらに、AireOS 8.3 が動作している WLC では、SSID 上で 802.11k および 11v 機能がデフォルトで有効になります。これらの機能により、ローミングすべきタイミングとネイバー AP に関する情報がクライアントに通知され、ローミングが必要な時にスキャニングして時間を無駄にすることがなくなるので、クライアントのローミング状況の改善に役立ちます。iOS デバイスはデュアルバンドをサポートするため、802.11k ネイバー リストは、iOS デバイスに適応してデュアルバンドで更新されます。

Apple iOS デバイスは、IETF の推奨に従って QoS マーキングを行います。AireOS 8.3 が動作している WLC では、Fastlane 機能を有効にすることにより、次のような便利な機能を活用することができます。

- WLC QoS 設定がグローバルに最適化され、リアルタイム アプリケーションのサポートが向上します。
- iOS 10 デバイスでは、WMM TSPEC/TCLAS ネゴシエーションを実行することなくアップストリーム音声トラフィックを送信できます。インフラストラクチャがこれらの端末の音声マーキングに対応します。
- QoS プロファイルを iOS 10 デバイスに適用して、アップストリームで QoS マーキングが適用されるアプリケーションと、ベスト エフォートまたはバックグラウンドで送信されるアプリケーションを決定することができます。

要件

AireOS 8.3 以上を実行する WLC、iOS 10 以上を実行するデバイス。

使用されるコンポーネント

このドキュメントの情報は、特定のラボ環境におけるテストに基づいて作成されました。本文書の作成に使用したデバイスはすべて、初期設定（デフォルト）の状態から作業が開始されています。これらの機能はテスト環境でテストすることをお推めします。稼働中のネットワークの場合は、コマンドによる影響の可能性について十分に理解したうえで作業してください。

[1] 最適化 Wi-Fi 接続ソリューションをサポートする iOS デバイスは、次のとおりです
iPhone 6s 以降
iPhone 6s Plus 以降
iPad Pro 以降
iPhone SE

表記法

文書中の表記方法の詳細については、『Cisco Technical Tips Conventions（シスコ テクニカル ティップスの表記法）』を参照してください。

Adaptive 11r

シスコのインフラストラクチャ側では、シスコの AP がビーコンとプローブで Adaptive 802.11r のサポートをアドバタイズし、Over-the-DS FT 機能が設定されます。

クライアント側では、iOS 10 以降を実行するデバイスが IE 上で Adaptive 11r 機能サポートを検索します。capability bit が設定されている場合は、機能ビットが AKM（dot1x または PSK）を検索し、それに応じて FT dot1x または FT PSK を使用します。Apple デバイスは、FT をサポートする IE をアソシエーション要求で送信します。それにはベンダー固有の OUI も含まれます。

Cisco WLAN は、アソシエーション要求を処理し、アソシエーション応答で 802.11r サポートに応答して FT アソシエーションを許可します。4 ウェイ ハンドシェイクには FT アソシエーションが含まれています。

この機能は、AireOS リリース 8.3 を実行する WLC で制御されるすべての 802.11n および 802.11ac Wave 1 AP に対応して、ローカル モードや FlexConnect モードの AP でサポートされます[2]。

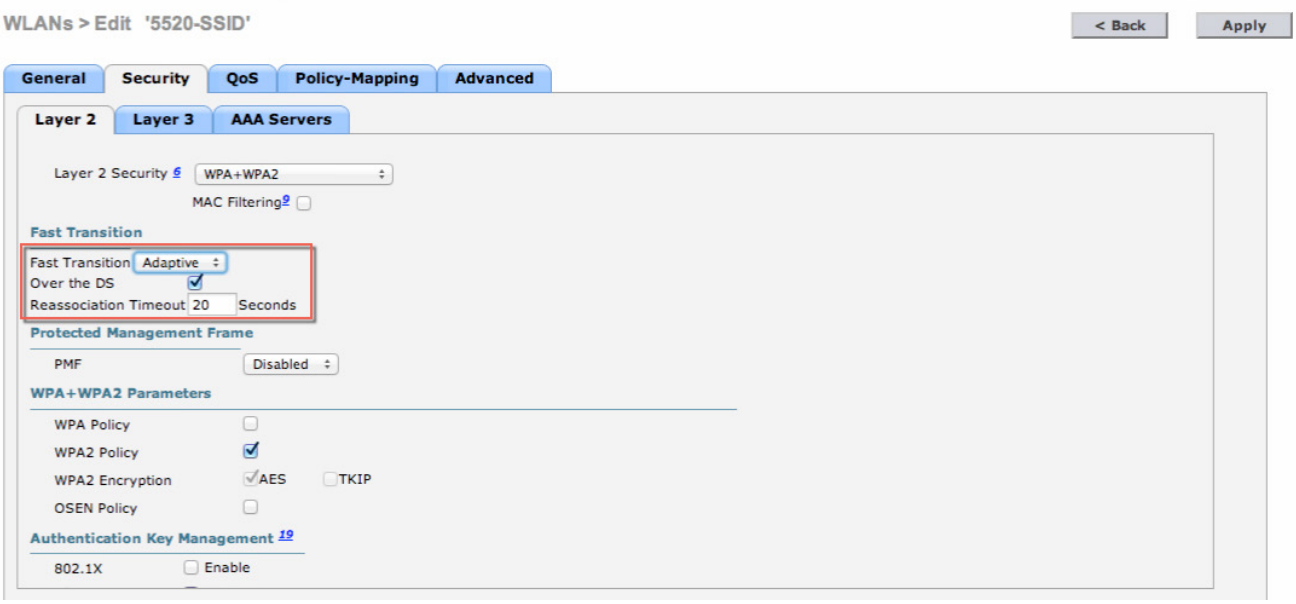
FT AKM のビーコンおよびプローブ応答を認識しないレガシー デバイスは、WLAN に接続できません。何らかの方法で、クライアント デバイスの機能を識別して 11r 対応デバイスを FT 対応デバイスとして WLAN に接続可能にし、同時に、レガシー デバイスを 11i/WPA2 デバイスとして接続できるようにする必要があります。Cisco WLC ソフトウェア リリース 8.3 は、802.11i 対応 WLAN 上の 802.11r を Apple デバイスに対して選択的に有効化することができます1。対応する Apple デバイスはこの機能を識別し、WLAN で FT アソシエーションを行います。

設定手順

1. PSK レイヤ 2 認証で新しい WLAN（SSID）を作成します（802.1x もサポートされます）。Adaptive 11r 機能はデフォルトで有効になっています。[Over the DS] がデフォルトで選択されており、再アソシエーションのタイムアウトが 20 秒に設定されています。

注：以前のリリースからアップグレードすると、Adaptive 11r 機能は既存の WLAN についてはデフォルトで無効になります。

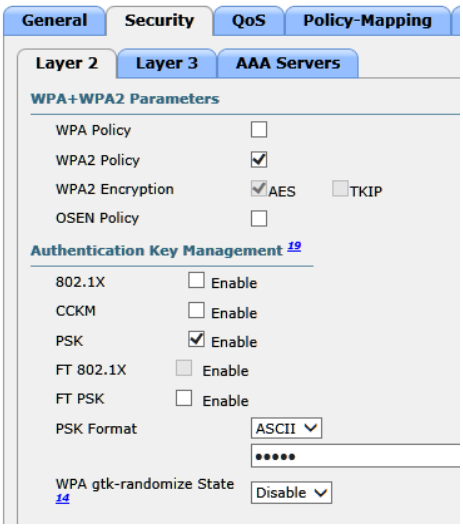
[2] AP1600/2600 シリーズ アクセス ポイント、AP1700/2700 シリーズ アクセス ポイント、AP3500 シリーズ アクセス ポイント、AP3600 シリーズ アクセス ポイント + 11ac モジュール、WSM、ハイパーロケーション モジュール、3602P、AP3700 シリーズ アクセス ポイント + WSM、3702P、OEAP600 シリーズ OfficeExtend アクセス ポイント、AP700 シリーズ アクセス ポイント、AP700W シリーズ アクセス ポイント、AP1530 シリーズ アクセス ポイント、AP1550 シリーズ アクセス ポイント、AP1570 シリーズ アクセス ポイント、AP1040/1140/1260 シリーズ アクセス ポイント。



この設定は、次の GUI または CLI コマンドを使用して変更できます。

- config wlan security ft adaptive enable/disable

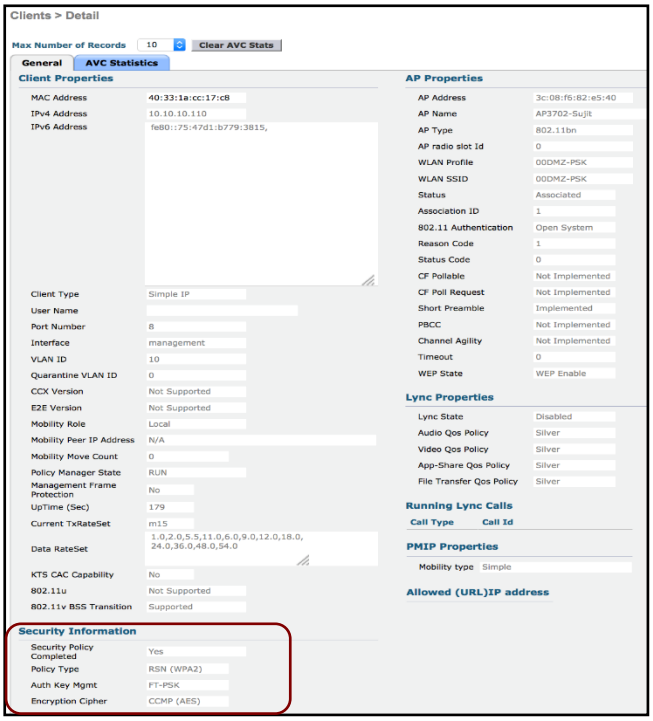
2. AKM を、FT 802.1x または FT PSK ではなく、802.1x または PSK として有効にします。

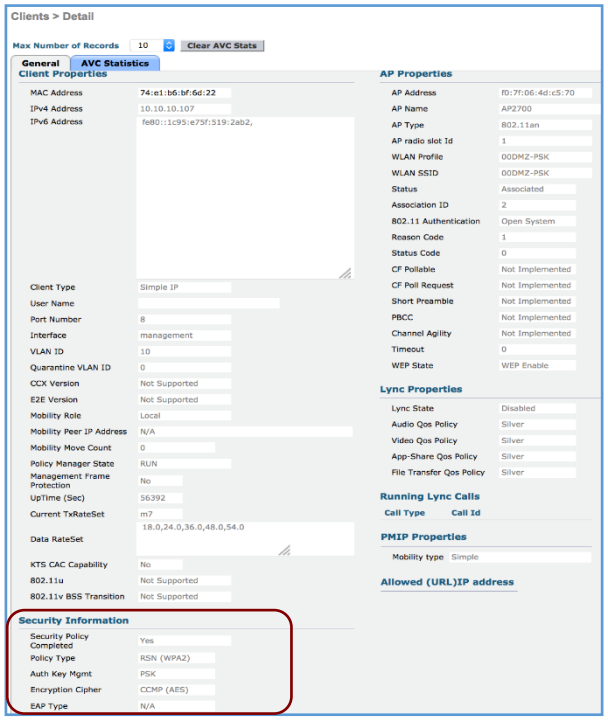


3. WLAN を有効にして、次の 3 種類のクライアントを SSID にアソシエーションさせます。
   - iOS 10 以降を実行する iPad および iPhone デバイス
   - iOS 9 以前を実行する iPad および iPhone デバイス
   - iOS 以外のデバイス

4. 以下の項目を確認します。
    - iOS 10 以降を実行する iPad または iPhone が 11r クライアントとしてアソシエーションしている
    - iOS 9 以前を実行する iPad または iPhone が通常の 802.11i クライアントとしてアソシエーションしている
    - Apple 以外のデバイスが通常の 802.11i クライアントとしてアソシエーションしている

5. 以下の項目を確認します。
    - iOS 10 以降を実行する iPad または iPhone は、新しい AP に高速ローミングする
    - iOS 9 以前を実行する iPad または iPhone は、新しい AP に低速ローミングする





設定ガイドラインの補足

1. FT 802.1x または FT PSK ではなく、802.1x または PSK を AKM として設定します。

CLI コマンド:

- config wlan security wpa akm 802.1x enable
  または
- config wlan security wpa akm psk enable

2. 必要に応じて、FT の [Over the DS] を有効または無効にし、再アソシエーションのタイムアウトを設定します。

CLI コマンド:

- config wlan security ft over-the-ds enable/disable
- config wlan security ft reassociation-timeout

debug コマンド

次のコマンドを使用してこの機能をデバッグできます。

- debug client <client-mac>
- debug snmp mib enable

SNMP

MIB CLWSecDot11EssCckmEntry の cLWSecDot11EssFtMode エントリは、WLAN 上の11r のステータスを、次のとおりに返します。

k_cLWSecDot11EssCckmEntry_get	戻り値	理由
	0	11r 無効/WLAN が存在しない
	1	11r モード有効
	2	**11r モード適応**

11k および 11v の常時有効化

リリース 8.3 では、802.11k および 11v 機能が SSID でデフォルトで有効になります。これらの機能により、ローミングすべきタイミングとネイバー AP に関する情報がクライアントに通知され、ローミングが必要な時にスキャニングして時間を無駄にすることがなくなるので、クライアントのローミング状況の改善に役立ちます。

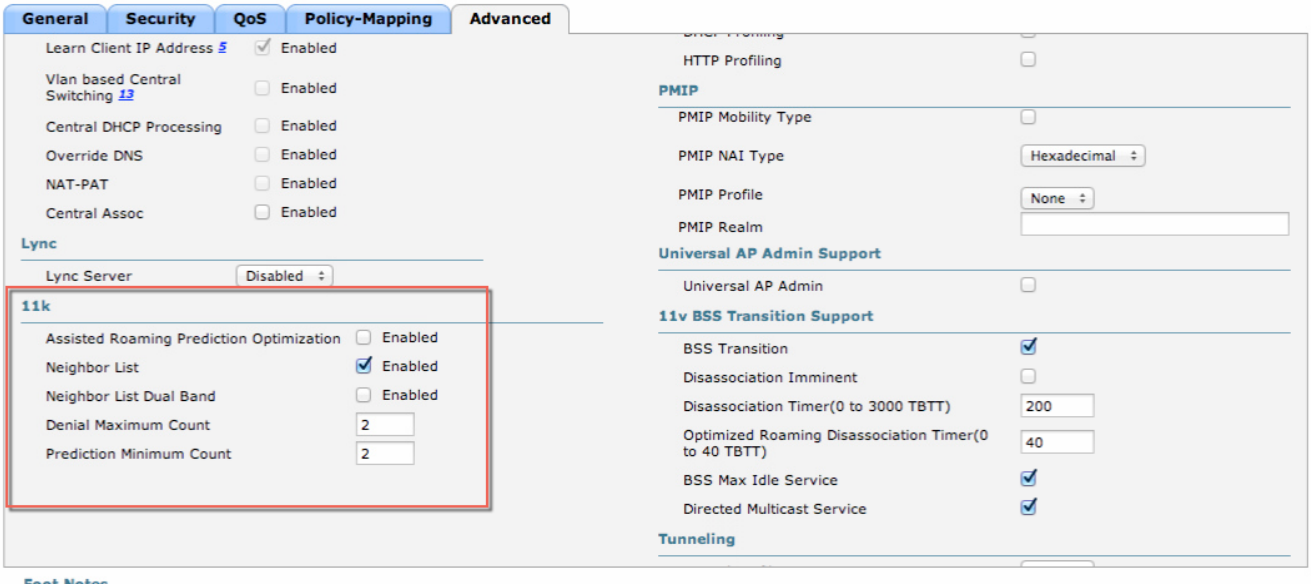
802.11kによる assisted roaming

802.11k では、11k 対応クライアントが、ローミングの候補となる既知のネイバー AP 情報を含むネイバー レポートを要求することができます。

AP にアソシエーションしている 11k 対応クライアントは、ローミングを容易にするために、ネイバー AP リストの要求を送信します。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。クライアントは、どの AP が次のローミング先候補となるのか、この応答フレームから知ることができます。802.11k 無線リソース管理（RRM）プロセスを使用することで、クライアントは効率的かつ高速にローミングを実行できます。

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 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 を検索する必要がありません。すべてのチャネルをプローブする必要がなくなれば、すべてのチャネルでチャネル利用率が減少するため、すべてのチャネルの帯域幅が増加します。また、ローミングにかかる時間が短縮され、クライアントによる判断が改善されます。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しないため、デバイスのバッテリ寿命が向上します。これにより、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。

手順 1 : [WLANs] をクリックします。
手順 2 : [WLAN ID] > [編集（Edit）] ページの順に選択します。
手順 3 : [詳細設定（Advanced）] タブをクリックします。
手順 4 : [11k] エリアでは、この機能が、新しく作成された SSID に対してデフォルトで有効になっています。

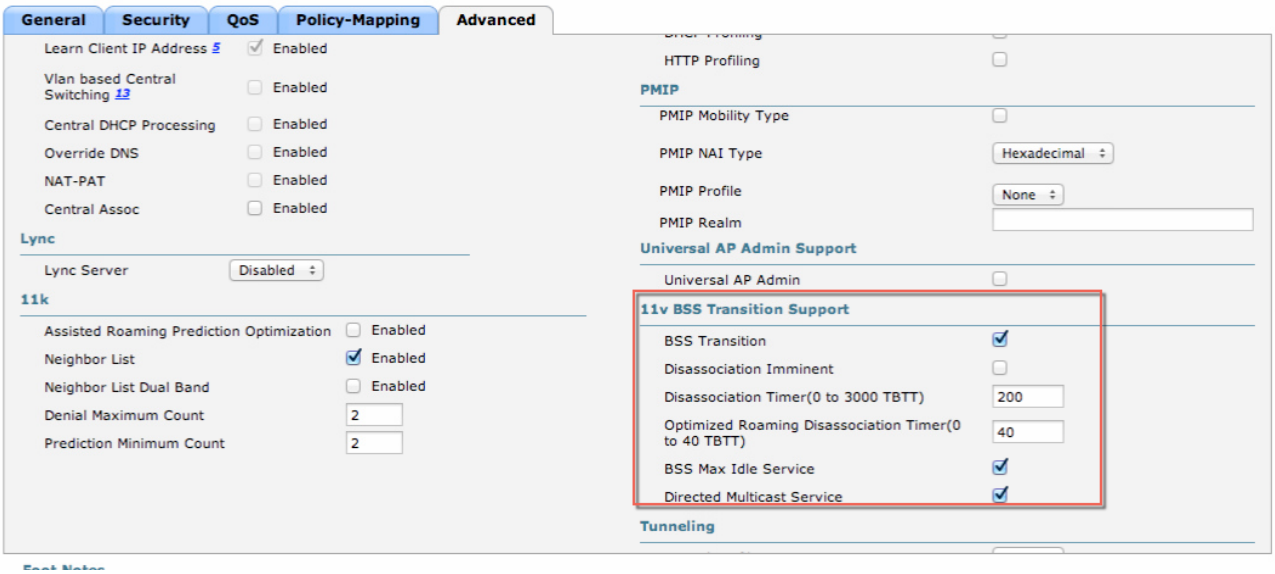


上図の設定では [ネイバー リスト デュアル バンド（Neighbor List Dual Band）] 設定が有効になっていませんが、Cisco WLAN インフラストラクチャとの間で適応機能をネゴシエートする Apple デバイスでは、デュアル バンド ネイバー リストが選択的に有効化され、クライアントは両帯域のメリットを活用することが可能になります。

802.11v BSS 移行（802.11v BSS Transition）の管理

802.11v BSS 移行は、次の 3 つのシナリオに適用されます。
要請要求（Solicited request）：クライアントは、ローミングする前に、クライアントの再アソシエーション先としてより適切な AP を見つけるため、802.11v BSS移行管理クエリ（802.11v BSS Transition Management Query）を送信できます。
非要請ロードバランシング要求（Unsolicited Load Balancing request）：AP の負荷が大きい場合、その AP は、アソシエーションされたクライアントに対して 802.11v BSS 移行管理要求（802.11v BSS Transition Management Request）を送信します。
非要請最適化ローミング要求：クライアントの RSSI とレートが要件を満たしていない場合、AP はこのクライアントに対して 802.11v BSS 移行管理要求（802.11v BSS Transition Management Request）を送信します。
802.11v BSS 移行管理要求（802.11v BSS Transition Management Request）とは、クライアントに対する提案です。クライアントは、提案を受け入れるか、拒否するかを自由に決定することができます。クライアントのアソシエーションを強制的に解除するには、関連付け解除通知機能（disassociation-imminent function）を利用できます。これは、クライアントが別の AP に再アソシエーションしない場合に、一定時間経過後にクライアントのアソシエーションを解除する機能です。

手順 1 : [WLANs] をクリックします。
手順 2 : [WLAN ID] > [編集（Edit）] ページの順に選択します。
手順 3 : [詳細設定（Advanced）] タブをクリックします。
手順 4 : 下図の [11v BSS 移行サポート（11v BSS Transition Support）] セクションに示すように、新しく作成された SSID については、この機能がデフォルトで有効になっています。



優先されるビジネス アプリケーション

QoS は、輻輳した環境でトラフィックを効率よく伝送するための主要なコンポーネントです。QoS を利用することで、ビジネス運営上の重要性を反映したマーキングをアプリケーションに適用できます。有線インフラストラクチャでは、このマーキングの使用により、マーキング値に基づいて異なる優先度を設定したり、アプリケーション カテゴリまたはマーキングに基づいて帯域幅の割り当てや制御を実施したりすることができます。ワイヤレス環境では、8 つのユーザ優先度キューのいずれか 1 つにアプリケーションをアソシエーションする目的でもマーキングが使用されます。また、キューへのアソシエーションを使用して、アプリケーションがワイヤレス メディアにアクセスする頻度を統計に基づいて変えることもできます。インフラストラクチャ レベルで適切なマーキングを行うことで、ダウンストリーム トラフィックが最適化され、ビジネスへの関連性が高いアプリケーションは、統計上優先的にトラフィックを受信でき、リアルタイム アプリケーションには非インタラクティブ アプリケーションより高い優先順位を付けることができます。クライアント端末が QoS マーキングを適切に運用していれば、同じ効果がアップストリームにも適用されます。
iOS デバイスは、IETF の推奨に従って QoS マーキングを行います。AireOS 8.3 が動作している WLC では、Fastlane 機能を有効にすることにより、次のような便利な機能を活用することができます。

- WLC QoS 設定がグローバルに最適化され、リアルタイム アプリケーションのサポートが向上します。
- iOS 10 を実行するデバイスでは、WMM TSPEC/TCLAS ネゴシエーションを実行することなく、アップストリーム音声トラフィックを送信できます。インフラストラクチャがこれらの端末の音声マーキングに対応します。
- QoS プロファイルを iOS 10 デバイスに適用して、アップストリームで QoS マーキングが適用されるアプリケーションと、ベスト エフォートまたはバックグラウンドで送信されるアプリケーションを決定することができます。

機能概要

シスコのインフラストラクチャ側では、ターゲット WLAN で機能が有効になり次第、シスコの AP が Fastlane のサポートをアドバタイズします。

クライアント側では、iOS 10 以降を実行している iOS デバイスが、AP 管理フレームで Fastlane サポートを検索します。また、iOS 10 デバイスがアップストリーム フレームで Fastlane のサポートをマーキングします。

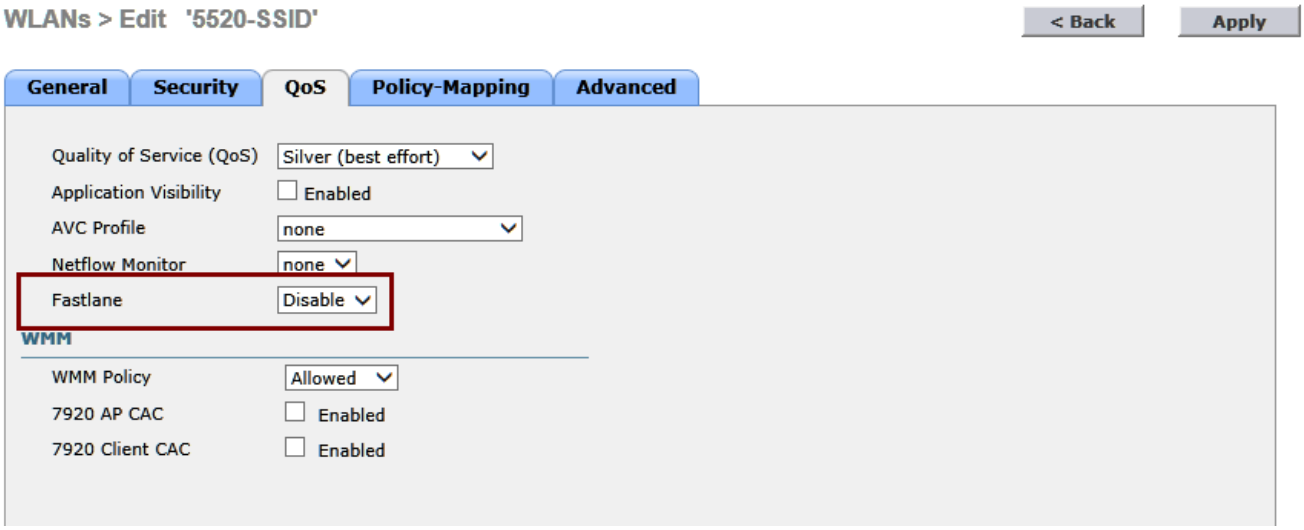
最初の WLAN で Fastlane を有効にすると、Wi-Fi デバイスの QoS サポートが最適になるようにコントローラが自動的に設定されます。特に、グローバル プラチナ プロファイルが音声へのトラフィックを許可するように設定されて、そのプロファイルにより、ユニキャスト デフォルト プライオリティやマルチキャスト デフォルト プライオリティのパラメータがベスト エフォートに設定されます。ユーザ単位での UDP 帯域幅契約はプロファイル上で無効になり、802.1p に準じたものとなります。プラチナ プロファイルは、ターゲットの WLAN に接続されます。ワイヤレス CAC（ACM）と優先帯域幅は、両方の帯域の音声キュー用に有効となっており、最大音声帯域幅が 50 % に設定されます。カスタマイズされた DSCP-to-UP マップと UP-to- DSCP マップは、IETF RFC 4594[3] および draft-szigetti-ieee-802-11-01[4] で推奨された値をマッピングするように設定されます。アップストリーム トラフィックには DSCP が信頼されています。AutoQoS プロファイルが作成され、差別化 QoS 処理を必要とすることの多い、広く普及した一般的な 32 のアプリケーションに対し、推奨されたマーキングが適用されます。ターゲット WLAN で、アプリケーションの可視性が有効になると、この自動 QoS プロファイルが自動的に適用されます。
iOS 10 デバイスは QoS プロファイルを受信できます（標準的な Apple プロファイル プロビジョニング テクニックを使用してプロビジョニングされます）。この QoS プロファイルでは、ホワイトリストに登録できるアプリケーションの一覧が示されます。ホワイトリストのアプリケーションには、Apple Service Type 方式を使用して、アップストリーム QoS マーキングを適用することが許可されます。ホワイトリストにないアプリケーションは、Fastlane 対応ネットワークではアップストリーム QoS マーキングを適用しません。デフォルトでは、すべてのアプリケーションがホワイトリスト化されています（例：QoS ホワイトリストのない状態では、すべてのアプリケーションで QoS マーキングが可能です。ホワイトリストが導入されると、ホワイトリスト内のアプリケーションのみが Service_Type 方式による QoS マーキング適用となり、他のアプリケーションは、ベスト エフォートもしくはバックグラウンドの QoS 処理を受けます）。iOS 10 デバイスがサポートされている場合は、Fastlane が設定された WLAN へのアソシエーションが行われ、以前受信した QoS プロファイルが適用されます。また、AP は iOS の QoS マーキングを信頼します。特に、音声としてマーキングされたトラフィックは、クライアントがアドミッション コントロール（ADDTS）を実行していなくとも信頼されます。

この機能は、AireOS リリース 8.3 を実行する WLC で制御されるすべての 802.11n および 802.11ac Wave 1 AP に対応して、ローカル モードや FlexConnect モードの AP でサポートされます[5]。

[3] https://tools.ietf.org/html/rfc4594
[4] https://tools.ietf.org/html/draft-szigeti-tsvwg-ieee-802-11-02
[5] AP1600/2600 シリーズ アクセス ポイント、AP1700/2700 シリーズ アクセス ポイント、AP3500 シリーズ アクセス ポイント、AP3600 シリーズ アクセス ポイント + 11ac モジュール、WSM、ハイパーロケーション モジュール、3602P、AP3700 シリーズ アクセス ポイント + WSM、3702P、OEAP600 シリーズ OfficeExtend アクセス ポイント、AP700 シリーズ アクセス ポイント、AP700W シリーズ アクセス ポイント、AP1530 シリーズ アクセス ポイント、AP1550 シリーズ アクセス ポイント、AP1570 シリーズ アクセス ポイント、AP1040/1140/1260 シリーズ アクセス ポイント。

設定手順

1. 新しい WLAN を作成します。Fastlane は、デフォルトでは有効化されていません。



この設定は、次の GUI または CLI コマンドを使用して変更できます。

- config qos Fastlane enable/disable wlan <wlan id>

WLAN で Fastlane を有効にすると、変更がグローバルに適用されて両方の帯域が一時的に無効になるので、そのことを伝える警告メッセージが表示されます（コマンドが完了すると自動的にどちらの帯域も再び有効になります）。

2. 以下を確認します。
   - WLAN の [QoS] タブで [Fastlane] が有効になっている。
   - WLAN の [QoS] プロファイルが [プラチナ（Platinum）] に設定されている。
   - [ワイヤレス（Wireless）] > [QoS] > [プロファイル（Profiles）] > [プラチナ（Platinum）] の順に移動すると、[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）] が [ベスト エフォート（Best Effort）] に設定されている。[有線 QoS プロトコル（Wired QoS protocol）] が [なし（None）] に設定されている。
   - [ワイヤレス（Wireless）] > [QoS] > [QoS マップ（QoS Map）] の順に移動すると、QoS マップが有効になっており、[アップストリームで DSCP を信頼する（Trust DSCP Upstream）] が選択されている。QoS マップは、既知の DSCP 値を IETF 推奨値にマッピングするための 19 個の例外を作成します。他の DSCP 値はすべて、その上位（MSB）3 ビットに合致する一般的な UP にマッピングされます。
   - [ワイヤレス（Wireless）] > [802.11a/n/ac] > [メディア（Media）] の順に移動すると、[コール アドミッション制御（Call Admission Control）] が有効になっており、[音声（Voice）] トラフィックに 50% の最大 RF 帯域幅が割り当てられている。[ワイヤレス（Wireless）] > [802.11b/g/n] > [メディア（Media）] ページでも、同じ設定が表示されます。

- [ワイヤレス（Wireless）] > [802.11a/n/ac] > [EDCA パラメータ（EDCA Parameters）] の順に移動すると、[EDCA プロファイル（EDCA Profile）] が [Fastlane] になっている。[ワイヤレス（Wireless）] > [802.11b/g/n] > [EDCA パラメータ（EDCA Parameters）] ページでも、同じ設定が表示されます。

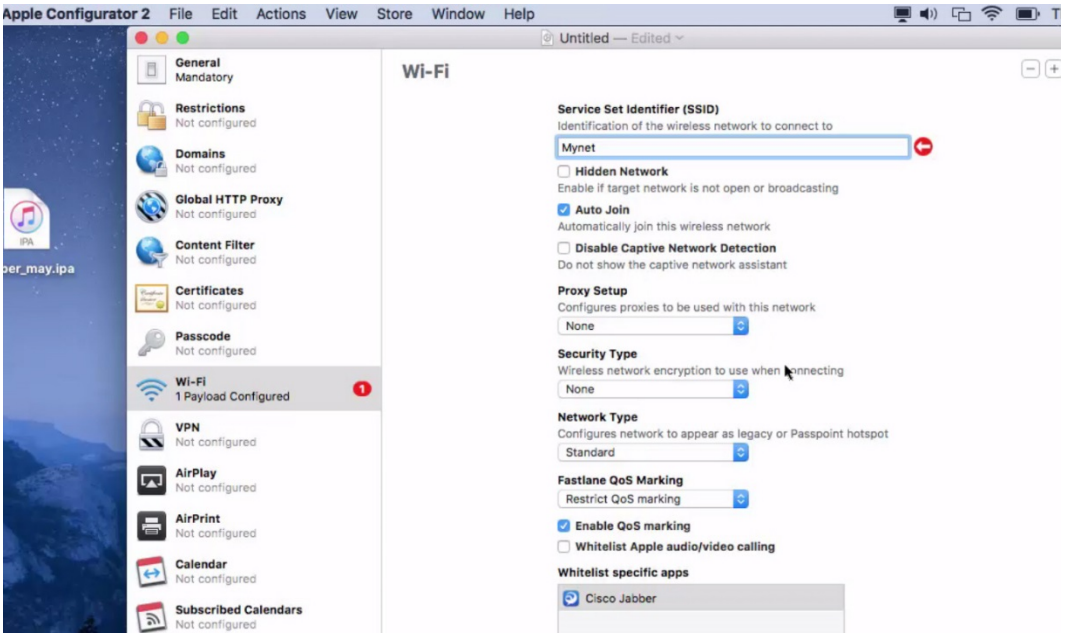
3. WLAN を有効にして、次の 3 種類のクライアントを SSID にアソシエーションさせます。
   - iOS 10 以降を実行する iPad および iPhone デバイス（ホワイトリスト登録アプリケーションをリストアップするプロファイルの有無は問わない）
   - iOS 9 以前を実行する iPad および iPhone デバイス
   - iOS 以外のデバイス

4. 以下の項目を確認します。
   - iOS 10 以降を実行する iPad および iPhone が Fastlane クライアントとしてアソシエーションされている
   - iOS 9 以前を実行する iPad および iPhone デバイスが通常のクライアントとしてアソシエーションされている
   - iOS 以外のデバイスが通常のクライアントとしてアソシエーションされている

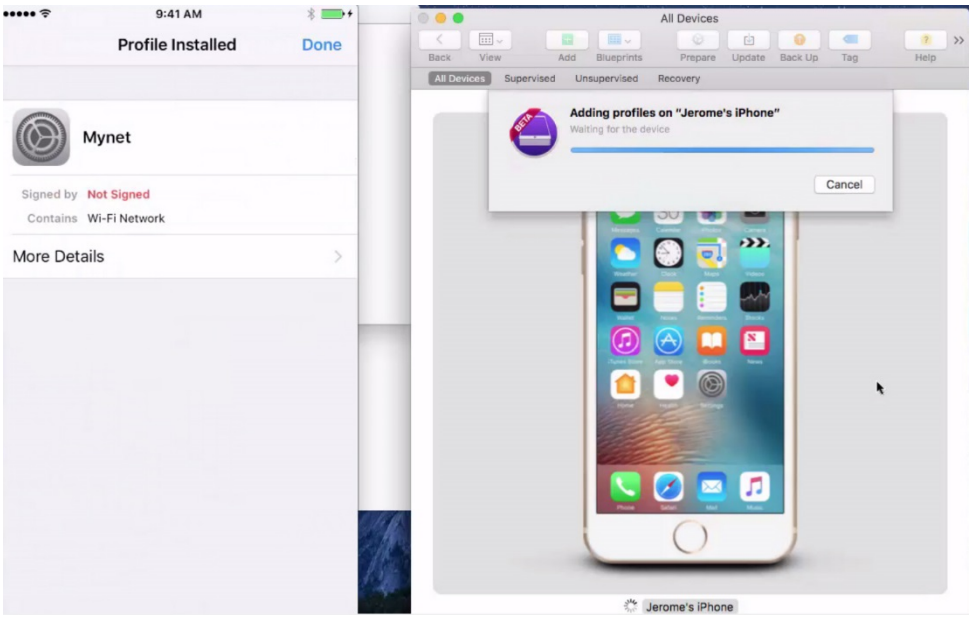
CLI コマンド:

- Show client details <mac address>
  …/..
  Fastlane Client: .....Yes

5. オプションで、Apple Configurator または使用中の MDM ソフトウェアを使用して QoS プロファイルを作成し、iOS 10 クライアントに導入します。QoS プロファイルはターゲット SSID 名と一致する必要があります。たとえば、Apple Configurator 2.3 以降を使用して MacOS にプロファイルを作成できます。プロファイルの Wi-Fi セクションでは、ターゲット SSID を設定し、ホワイトリストに登録するアプリケーションを選択することができます。次の例では、Mynet SSID のプロファイルを作成し、Cisco Jabber をホワイトリストに登録しています（Jabber は QoS マーキングを行います）。[アップル音声/ビデオ コーリング（Apple audio/video calling）] が無効になっているため、Wi-Fi コーリングと Facetime は QoS マーキングを適用しません（[アップル音声/ビデオ コーリング（Apple audio/video calling）] を無効にすることは推奨していませんが、説明のため、例として取り上げています）。



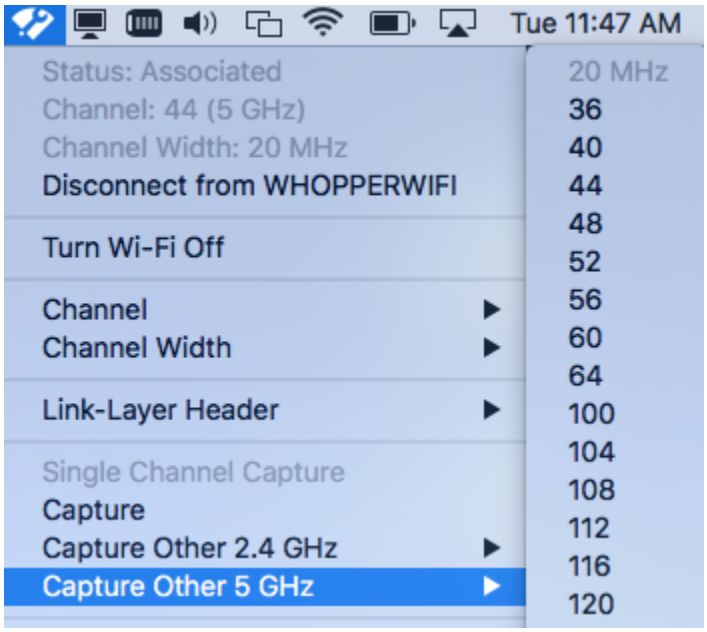
作成したプロファイルは、Apple Configurator を介して iOS 10 デバイスにプッシュできます。



6. QoS プロファイルを使用して iOS デバイスのプロビジョニングが完了したら、iOS 10 デバイスをターゲット SSID にアソシエーションします。ホワイトリストに登録されているアプリケーション（この例では Jabber）を起動してから、ホワイトリストにないアプリケーション（この例では Facetime）を起動します。

7. 以下の項目を確認します。

- iOS 10 以降を実行する iPad および iPhone デバイスが、ホワイトリスト登録アプリケーションには QoS をマーキングし、ホワイトリスト外のアプリケーションのトラフィックはベスト エフォートまたはバックグラウンドで送信している。
- iOS 10 以降を実行し、アップストリーム トラフィックに DSCP 46/UP6 をマーキングしている iPad および iPhone デバイスが、同じく DSCP46/UP6 マーキングを適用されたダウンストリーム トラフィックを受信している（ACM が有効で、なおかつ iOS 10 クライアントが TSPEC/ADDTS 経由でサービス レベルを要求していない場合でも同様）。
- iOS 9 以前を実行する iPhone および iPad デバイスがアップストリーム トラフィックのマーキングを実施できる。ただし、音声キューのリターン トラフィックは、WMM の仕様に従ってベスト エフォートとして送信されます。
- iOS 以外のデバイスがアップストリーム トラフィックのマーキングを実施できる。ただし、音声キューのリターン トラフィックは、WMM の仕様に従ってベスト エフォートとして送信されます（非 iOS デバイスが最初に ADDTS を要求し、それが受け入れられている場合を除く）。
- WLAN 上で [Application Visibility] が有効になっている場合、Jabber などのよく知られたアプリケーションには、アップストリーム マーキングにかかわらず、正しい（RFC 4594 および draft-szigetti-ieee-802-11-01 推奨）ダウンストリーム マーキングが適用される。
- これらのポイントを確認する最も良い方法は、WLAN チャネル トラフィックをキャプチャすることです。MacOS ラップトップでは、フレームをキャプチャする Wireshark と、キャプチャ対象チャネルを設定する Airtool を、組み合わせて使用することができます。



キャプチャでは、ホワイトリスト登録アプリケーションに適用された QoS マーキングが想定どおりであることを確認します。この例では、Jabber Audio に DSCP EF と UP 6 が与えられています[6]。

```
1639 13.198813    172.31.255.128    172.29.129.137    RTP      183 0x0006
1640 13.198886                      Apple_1e:d4:b9 (5c…  802.11   39
1641 13.198965    172.31.255.128    172.29.129.137    RTCP     147 0x0000
1642 13.199036                      Apple_1e:d4:b9 (5c…  802.11   39
1643 13.202159    CiscoInc_db:df:7a Broadcast          802.11   246
1644 13.212367    172.31.255.128    172.29.129.137    RTP      183 0x0006
1645 13.212442                      Apple_1e:d4:b9 (5c…  802.11   39
1646 13.231941    172.31.255.128    172.29.129.137    RTP      183 0x0006
1647 13.232014                      Apple_1e:d4:b9 (5c…  802.11   39
1648 13.241307    172.29.129.137    172.31.255.128    RTP      183 0x0006
Frame 1639: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 QoS Data, Flags: .......TC
Logical-Link Control
Internet Protocol Version 4, Src: 172.31.255.128, Dst: 172.29.129.137
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
▶ Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
```

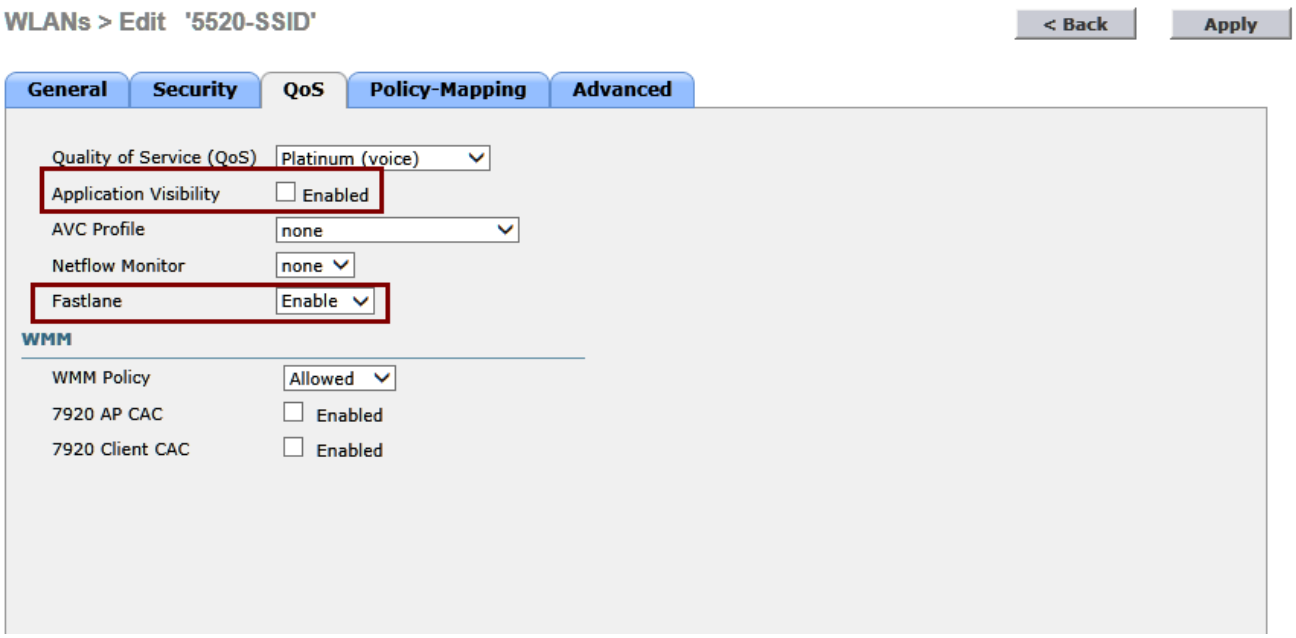
この例では、FaceTime はホワイトリストに登録されておらず、トラフィックをベスト エフォートとして送信します。

```
5712 32.356395    172.31.255.128    172.29.129.137    UDP      301 0x0000
  Receiver address: CiscoInc_db:ce:fc (a8:0c:0d:db:ce:fc)
  Destination address: CiscoInc_b8:dd:c3 (24:b6:57:b8:dd:c3)
  Transmitter address: Apple_1e:d4:b9 (5c:ad:cf:1e:d4:b9)
  Source address: Apple_1e:d4:b9 (5c:ad:cf:1e:d4:b9)
  BSS Id: CiscoInc_db:ce:fc (a8:0c:0d:db:ce:fc)
  STA address: Apple_1e:d4:b9 (5c:ad:cf:1e:d4:b9)
  .... .... .... 0000 = Fragment number: 0
  1101 0001 1010 .... = Sequence number: 3354
▶ Frame check sequence: 0xe6ef930e [correct]
▶ Qos Control: 0x0000
▶ Logical-Link Control
▼ Internet Protocol Version 4, Src: 172.31.255.128, Dst: 172.29.129.137
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
```

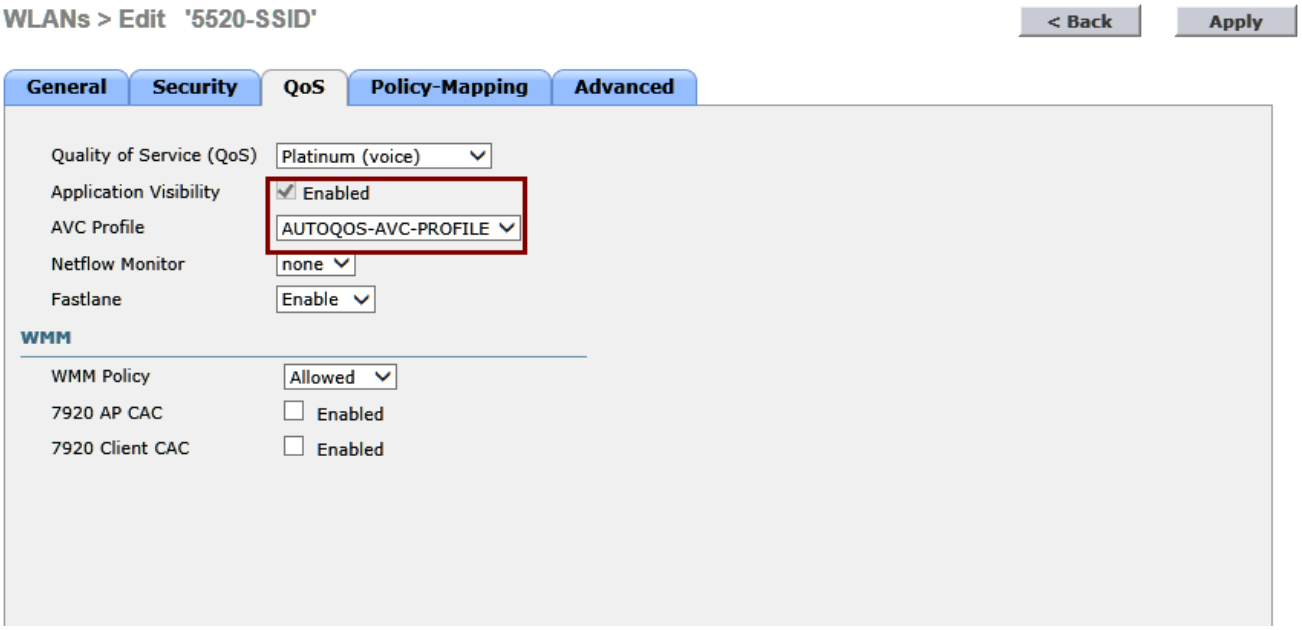
設定ガイドラインの補足

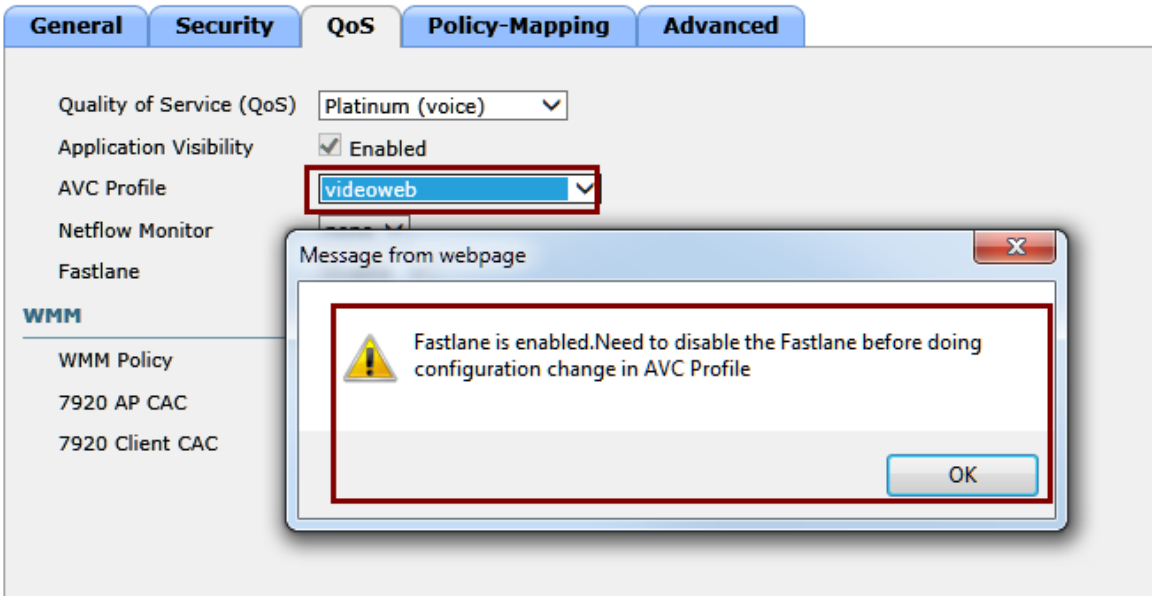
1. [Application Visibility] は Fastlane 設定のオプション要素です。[Application Visibility] を有効にしなくても、WLAN で Fastlane を有効にすることは可能です。

[6] マーキングを表示するには、アプリケーションが iOS 10 用にアップデートされ、QoS マーキングにネイティブで対応している必要があります。アプリケーションで iOS 10 Service_Type を使用して、iOS 10 で QoS マーキングを表示できるバージョンについては、アプリケーション プロバイダーに確認してください。



Fastlane WLAN で [Application Visibility] が有効になっている場合、推奨される Auto-QoS-AVC Profile が WLAN に適用されます。Fastlane を無効にしない限り、他の AVC プロファイルは適用できません。

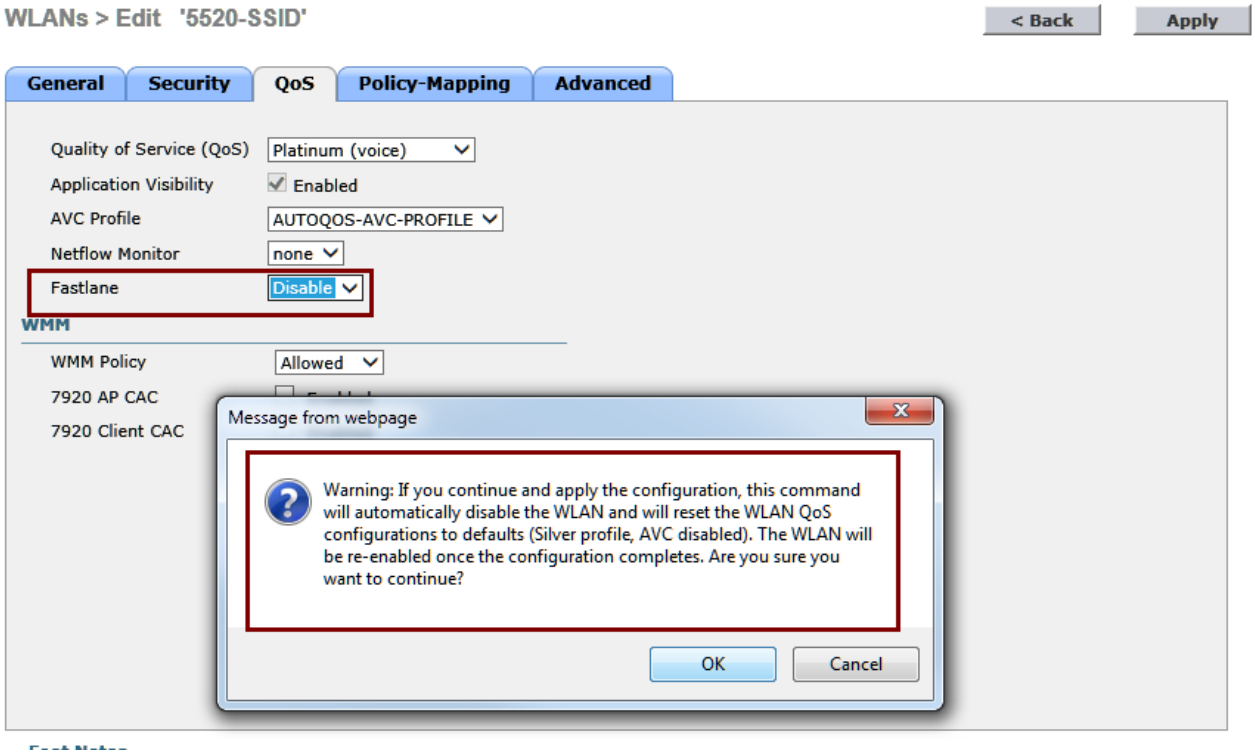




CLI コマンド:

- config wlan avc <wlan id> visibility enable

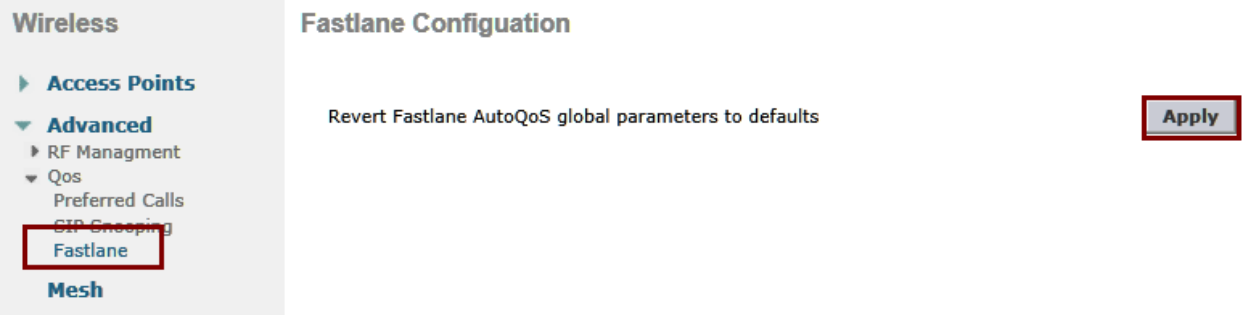
2. Fastlane は WLAN ごとに無効にすることができます。無効にすると、WLAN QoS ポリシーは [シルバー(Silver)](デフォルト)に戻り、[Application Visibility] がデフォルト([無効(Disabled)])にリセットされます。必要に応じて、コマンド完了後に WLAN を編集し、アソシエーションされた QoS プロファイルを手動で変更することで、[Application Visibility] を有効にすることができます。



CLI コマンド:

- Config qos Fastlane disable wlan <wlan id>

3. すべての WLAN で Fastlane を無効にすると、WLC のグローバル QoS 設定もデフォルトに戻すことができます。無効にするには、[Fastlane] グローバル設定ページを使用します。Fastlaneが有効な WLAN が 1 つでも残っている場合、Fastlane をグローバルで無効にすることはできません。Fastlane をグローバルで無効にすると、QoS プロファイル [プラチナ(Platinum)] がデフォルトにリセットされます([最高優先順位(Maximum Priority)] は [音声(Voice)] のままですが、[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)] は [音声(Voice)] にリセットされます)。[音声(Voice)] ではワイヤレス CAC(ACM)が無効になり、アソシエーションされた最大帯域幅がデフォルト値の 75 % に戻ります。QoS マップが無効になり、アップストリーム QoS は、DSCP ではなく UP を使用します。



CLI コマンド:

- Config qos Fastlane disable global

注:WLC のグローバル QoS 設定をデフォルトに戻すには Fastlane をグローバルで無効にする必要がありますが、Fastlaneをグローバルで有効に戻す必要はありません。最初の WLAN で Fastlane を有効にすると、Fastlane のグローバル パラメータも有効になります。

debug コマンド

次のコマンドを使用してこの機能をデバッグできます。

- debug client <client-mac>
- debug snmp mib enable

SNMP

cLQosFastlaneDisable エントリは、Fastlane のグローバル ステータスを次のとおりに返します。

cLQosFastlaneDisable_get	戻り値	理由
	0	予約済み
	1	**無効**
	2	**オペレーションなし**

cLWlanQosFastlane エントリは、各 WLAN の Fastlane のステータスを次のとおりに返します。

cLWlanQosFastlane_get	戻り値	理由
	True	**Fastlane が有効**
	False	**Fastlane が無効**