



WLAN

- [WLAN について](#) (1 ページ)
- [WLAN の前提条件](#) (4 ページ)
- [WLAN の制約事項](#) (4 ページ)
- [WLAN の設定方法](#) (6 ページ)
- [WLAN プロパティの確認 \(CLI\)](#) (15 ページ)

WLAN について

この機能により、Lightweight アクセスポイントに対して WLAN を制御できます。各 WLAN には識別子である WLAN ID、プロファイル名、および WLAN SSID があります。アクセスポイントはすべて、最大 16 の WLAN をアドバタイズできます。ただし、最大 4096 の WLAN を作成し、作成した WLAN を（プロファイルとタグを使用して）別の AP に選択的にアドバタイズして、管理性を向上できます。

異なる SSID または同じ SSID で WLAN を設定できます。SSID は、コントローラがアクセスする必要がある特定の無線ネットワークを識別します。

バンドの選択

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、輻輳の少ない 5 GHz アクセスポイントに移動できます。2.4 GHz 帯域は、混雑していることがあります。この帯域のクライアントは一般に、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他のアクセスポイントからの同一チャンネル干渉も受けます。これは、802.11b/g では、重複しないチャンネルの数が 3 つに制限されているためです。このような干渉源を防ぎ、ネットワーク全体のパフォーマンスを向上させるには、device で帯域選択を設定します。

オフチャネル スキャンの保留

通常の動作状態では、Lightweight アクセスポイントは定期的にオフチャネルになり、別のチャンネルをスキャンします。これは、次のような RRM 動作を実行するためのものです。

- 他の AP を使用したネイバー探索プロトコル (NDP) パケットの送受信
- 不正 AP とクライアントの検出
- ノイズと干渉の測定

オフチャネル期間は通常は約 70 ミリ秒で、この期間は AP は対応するチャネル上でデータの送受信ができません。したがって、パフォーマンスに若干の影響が及び、一部のクライアント送信がドロップされることがあります。

AP が重要なデータを送受信している間はオフチャネルスキャンを保留するように設定して、AP がオフチャネルにならず、通常動作に影響を与えないようにすることができます。オフチャネルスキャンの保留は、指定した時間しきい値 (ミリ秒単位) で WMMUP クラス単位で WLAN ごとに設定できます。AP が指定されたしきい値内の所定の UP クラスでマークされたデータフレームを特定の WLAN 上で送受信している場合、その AP は次の RRM オフチャネルスキャンを保留します。たとえば、デフォルトでは、オフチャネルスキャンの保留は UP クラス 4、5、および 6 に対して 100 ミリ秒の時間しきい値で有効になります。したがって、RRM がオフチャネルスキャンを実行しようとしているときに直近の 100 ミリ秒内に UP 4、5、または 6 でマークされたデータフレームを受信すると、RRM はオフチャネルになるのを保留します。音声サンプルを送受信している音声コールがアクティブな 20 ミリ秒ごとに UP 6 としてマークされる場合、AP 無線はオフチャネルになりません。

オフチャネルスキャンの保留ではトレードオフが生じます。オフチャネルスキャンは、設定やトラフィックパターンなどに応じて 2% 以上の影響をスループットに与える可能性があります。すべてのトラフィッククラスに対してオフチャネルスキャンの保留を有効にし、時間しきい値を引き上げると、スループットが若干改善する可能性があります。ただし、オフチャネルにならないようにすることによって、RRM は AP ネイバーや不正を識別できず、セキュリティ、DCA、TPC、および 802.11k メッセージに悪影響が及びます。

DTIM 周期

802.11 ネットワークでは、Lightweight アクセスポイントは、Delivery Traffic Indication Map (DTIM) と一致するビーコンを定期的送信します。アクセスポイントでビーコンがブロードキャストされると、DTIM 期間で設定した値に基づいて、バッファされたブロードキャストフレームおよびマルチキャストフレームが送信されます。この機能により、ブロードキャストデータやマルチキャストデータが予想されると、適切なタイミングで省電力クライアントを再起動できます。

通常、DTIM の値は 1 (ビーコンのたびにブロードキャストフレームおよびマルチキャストフレームを送信) または 2 (ビーコン 1 回おきにブロードキャストフレームおよびマルチキャストフレームを送信) のいずれかに設定します。たとえば、802.11 ネットワークのビーコン間隔が 100 ミリ秒で DTIM 値が 1 に設定されている場合、アクセスポイントは、バッファされたブロードキャストフレームおよびマルチキャストフレームを毎秒 10 回送信します。ビーコン期間が 100 ミリ秒で DTIM 値が 2 に設定されている場合、アクセスポイントは、バッファされたブロードキャストフレームおよびマルチキャストフレームを毎秒 5 回送信します。これらの設定は、ブロードキャストフレームおよびマルチキャストフレームの頻度を想定する、Voice over IP (VoIP) を含むアプリケーションに適しています。

ただし、DTIM 値は 255 まで設定できます (255 回のビーコンごとにブロードキャストフレームおよびマルチキャストフレームを送信します)。推奨される DTIM 値は 1 と 2 のみです。DTIM の値を高くすると、通信の問題が発生する可能性があります。



- (注) ビーコン期間は、device でミリ秒単位で指定され、ソフトウェアによって、802.11 の時間単位 (TU) (1 TU=1.024 ミリ秒) に、内部的に変換されます。AP モデルによっては、実際のビーコン期間はわずかに異なる場合があります。たとえば、100 ミリ秒のビーコン期間は、実際には 104.448 ミリ秒に相当します。

セッションタイムアウト

WLAN にセッションタイムアウトを設定できます。セッションタイムアウトとは、クライアントセッションが再認証を要求することなくアクティブである最大時間を指します。

WLAN がレイヤ 2 セキュリティ (WPA2-PSK など) を使用して設定されていて、レイヤ 3 認証も設定されている場合、WLAN セッションタイムアウト値は 802.1X 再認証タイムアウト値で上書きされます。APF 再認証タイムアウト値が 65535 より大きい場合、WLAN セッションタイムアウトはデフォルトで 65535 に設定されます。65535 以下の場合、設定済みの 802.1X 再認証タイムアウト値が WLAN セッションタイムアウトとして適用されます。

ここでは、次の内容について説明します。

Cisco Client Extensions

Cisco Client Extensions (CCX) ソフトウェアは、サードパーティ製クライアントデバイスの製造業者およびベンダーに対してライセンスされます。これらのクライアント上の CCX コードにより、サードパーティ製クライアントデバイスは、シスコ製のアクセスポイントと無線で通信できるようになり、セキュリティの強化、パフォーマンスの向上、高速ローミング、電源管理などの、他のクライアントデバイスがサポートしていないシスコの機能もサポートできるようになります。

- ソフトウェアは、CCX バージョン 1 ~ 5 をサポートします。これによって、devices とそのアクセスポイントは、CCX をサポートするサードパーティ製クライアントデバイスと無線で通信できます。CCX サポートは、device 上の各 WLAN に対して自動的に有効になり、無効にすることはできません。ただし、Aironet Information Element (IE) を設定できません。
- Aironet IE のサポートが有効になっている場合、アクセスポイントは、Aironet IE 0x85 (アクセスポイント名、ロード、アソシエートされたクライアントの数などを含む) をこの WLAN のビーコンやプローブ応答に格納して送信します。また、アクセスポイントが再アソシエーション要求内の Aironet IE 0x85 を受信する場合、device は、Aironet IEs 0x85 および 0x95 (device の管理 IP アドレスおよびアクセスポイントの IP アドレスを含む) を再アソシエーション応答に格納して送信します。

ピアツーピア ブロック

ピアツーピアブロッキングは個別の WLAN に対して適用され、各クライアントが、アソシエート先の WLAN のピアツーピアブロッキング設定を継承します。ピアツーピアにより、トラフィックをリダイレクトする方法を制御できます。たとえば、トラフィックが device 内でローカルにブリッジされたり、device によってドロップされたり、またはアップストリーム VLAN に転送されるように選択することができます。

ピアツーピアブロッキングは、ローカルおよび中央スイッチングの WLAN にアソシエートされているクライアントに対してサポートされています。



(注) ピアツーピアブロッキング機能は VLAN ベースです。ピアツーピアブロッキング機能が有効になっている場合、同じ VLAN を使用する WLAN で影響が生じます。

診断チャネル

クライアントの WLAN による通信で問題が生じる理由についてトラブルシューティングする診断チャネルを選択できます。クライアントで発生している問題を識別し、ネットワーク上でクライアントを動作させるための修正措置を講じるために、クライアントとアクセスポイントをテストできます。診断チャネルを有効にするには、device の GUI または CLI を使用します。また、診断テストを実行するには、device **diag-channel** の CLI を使用します。



(注) 診断チャネル機能は、管理インターフェイスを使用するアンカーされていない SSID に対してのみ有効にすることをお勧めします。CCX 診断機能は Cisco ADU カードを持つクライアントでのみテストされています。

WLAN の前提条件

- 最大 16 個の WLAN を各のポリシータグに特定のアクセスポイントを割り当てることができます。
- devices が VLAN トラフィックを正常にルーティングできるように、WLAN と管理インターフェイスにはそれぞれ別の VLAN を割り当てておくことをお勧めします。

WLAN の制約事項

- WLAN で PSK と CCKM を設定しないでください。この設定はサポートされておらず、クライアントの接続フローに影響します。

- WPA1 設定で TKIP または AES 暗号が有効になっていることを確認してください。有効になっていない場合、アップグレードプロセス中に ISSU が壊れる可能性があります。
- WLAN のプロファイル名を変更すると、FlexConnect AP (AP 固有の VLAN マッピングを使用する) が WLAN 固有になります。FlexConnect グループが設定されている場合、VLAN マッピングはグループ固有になります。
- Flex ローカル認証が有効にされている WLAN では、Fast Transition 802.1X キー管理でクライアント関連付けがサポートされないため、IEEE 802.1X Fast Transition を有効にしないでください。
- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- FlexConnect では、特定の FlexConnect AP または一部の AP のみにピアツーピア ブロッキング設定を適用することはできません。SSID をブロードキャストするすべての FlexConnect AP に適用されます。
- WLAN 名と SSID は 32 文字以内にする必要があります。
- WLAN および SSID 名では、次の ASCII 文字のみサポートされます。
 - 数字 : 48 から 57 の 16 進数 (0 ~ 9)
 - アルファベット (大文字) : 65 から 90 の 16 進数 (A ~ Z)
 - アルファベット (小文字) : 97 から 122 の 16 進数 (a ~ z)
 - ASCII スペース : 20 の 16 進数
 - 印刷可能な特殊文字 : 21 から 2F, 3A から 40、および 5B から 60 の 16 進数。つまり、!"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~
- WLAN 名はキーワードにはできません。たとえば、**wlan s** コマンドを入力して、「s」という名前で WLAN を作成しようとする、と、「s」はシャットダウン用のキーワードとして使用されているため、すべての WLAN がシャットダウンします。
- WLAN を VLAN 0 にマッピングすることはできません。同様に、WLAN を VLAN 1002 ~ 1006 にマッピングすることはできません。
- 固定 IPv4 アドレスのデュアル スタック クライアントはサポートされません。
- Cisco 9800 コントローラで IPv4 と IPv6 が設定されているデュアルスタックでは、IPv4 トンネルが消去される前に AP が IPv6 トンネルを使用してコントローラに接続しようとする、と、トレースバックが表示され、AP の接続は失敗します。
- 同じ SSID を持つ WLAN を作成するときには、各 WLAN に対して一意のプロファイル名を作成する必要があります。
- 同じ SSID を持つ複数の WLAN を同じ AP 無線に割り当てる場合は、クライアントがその中から安全に選択できるように、一意のレイヤ 2 セキュリティ ポリシーを使用している必要があります。

- 新しく設定された SSID が 5 GHz DFS チャンネル上にある場合、ビーコンはすぐには開始されません。
- RADIUS サーバーの上書きは、WLAN ごとではなく、AAA サーバーグループごとに設定されます。
- ダウンロード可能な ACL (dACL) は、FlexConnect モードやローカルモードではサポートされていません。



注意 一部のクライアントが複数のセキュリティ ポリシーで同じ SSID を検出すると WLAN に正しく接続できない場合があります。この WLAN 機能を使用する際は注意してください。

WLAN の設定方法

WLAN の作成 (GUI)

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [WLANs] ページで、[Add] をクリックします。

[Add WLAN] ウィンドウが表示されます。

ステップ 2 [General] タブで、[Profile Name] フィールドに WLAN の名前を入力します。名前には、32 ~ 126 文字の ASCII 文字を使用できます (先頭と末尾のスペースはなし)。

ステップ 3 [Save & Apply to Device] をクリックします。

WLAN の作成 (CLI)

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wlan profile-name wlan-id [ssid] 例 :	WLAN の名前と ID を指定します。

	コマンドまたはアクション	目的
	デバイス(config)# wlan mywlan 34 mywlan-ssid	<ul style="list-style-type: none"> • <i>profile-name</i> に、プロファイル名を入力します。入力できる範囲は英数字で 1 ~ 32 文字です。 • <i>wlan-id</i> に、WLAN ID を入力します。範囲は 1 ~ 512 です。 • <i>ssid</i> では、この WLAN に対する Service Set Identifier (SSID) を入力します。SSID を指定しない場合、WLAN プロファイル名は SSID として設定されます。 <p>(注)</p> <ul style="list-style-type: none"> • SSID は、GUI または CLI を使用して作成できますが、CLI を使用して作成することをお勧めします。 • WLAN はデフォルトでディセーブルにされています。
ステップ 3	end 例 : Device(config)# end	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WLAN の削除 (GUI)

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [WLANs] ページで、削除する WLAN の隣にあるチェックボックスをオンにします。

複数の WLAN を削除するには、複数の WLAN のチェックボックスをオンにします。

ステップ 2 [削除 (Delete)] をクリックします。

ステップ 3 確認ウィンドウで [Yes] をクリックして WLAN を削除します。

WLAN の削除

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no wlan wlan-name wlan-id ssid 例： デバイス (config)# no wlan test2	WLAN を削除します。引数は次のとおりです。 <ul style="list-style-type: none"> • <i>wlan-name</i> は WLAN プロファイル名です。 • <i>wlan-id</i> は、WLAN ID です。 • <i>ssid</i> は WLAN に設定された WLAN SSID 名前です。
ステップ 3	end 例： Device (config)# end	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WLAN の検索 (CLI)

コントローラで設定されているすべての WLAN のリストを確認するには、次の show コマンドを使用します。

```
Device# show wlan summary
Number of WLANs: 4
```

WLAN Profile Name	SSID	VLAN Status
1 test1	test1-ssid	137 UP
3 test2	test2-ssid	136 UP
2 test3	test3-ssid	1 UP
45 test4	test4-ssid	1 DOWN

ワイルドカードを使用して WLAN を検索するには、次の show コマンドを使用します。

```
Device# show wlan summary | include test-wlan-ssid
1 test-wlan test-wlan-ssid 137 UP
```


WLAN の有効化 (GUI)

手順

-
- ステップ 1 [Configuration] > [Tags & Profiles] > [WLANs] を選択します。
- ステップ 2 [WLANs] ページで、WLAN 名をクリックします。
- ステップ 3 [Edit WLAN] ウィンドウで、[Status] ボタンを [ENABLED] に切り替えます。
- ステップ 4 [Update & Apply to Device] をクリックします。
-

WLAN のイネーブル化 (CLI)

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wlan profile-name 例 : Device(config)# wlan test4	WLAN コンフィギュレーション サブモードを開始します。 <i>profile-name</i> は設定されている WLAN のプロファイル名です。
ステップ 3	no shutdown 例 : Device(config-wlan)# no shutdown	WLAN をイネーブルにします。
ステップ 4	end 例 : Device(config-wlan)# end	特権 EXEC モードに戻ります。

WLAN の無効化 (GUI)

手順

-
- ステップ 1 [Configuration] > [Tags & Profiles] > [WLANs] を選択します。
- ステップ 2 [WLANs] ウィンドウで、WLAN 名をクリックします。
- ステップ 3 [Edit WLAN] ウィンドウで、[Status] トグルボタンを [DISABLED] に設定します。

ステップ 4 [Update & Apply to Device] をクリックします。

WLAN のディセーブル (CLI)

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wlan profile-name 例： Device(config)# wlan test4	WLAN コンフィギュレーション サブ モードを開始します。 <i>profile-name</i> は設定されている WLAN のプロファイル名です。
ステップ 3	shutdown 例： Device(config-wlan)# shutdown	WLAN をディセーブルにします。
ステップ 4	end 例： Device(config-wlan)# end	特権 EXEC モードに戻ります。
ステップ 5	show wlan summary 例： Device# show wlan summary	デバイスに設定されているすべての WLAN のリストを表示します。出力内で WLAN を検索できます。

汎用 WLAN プロパティの設定 (CLI)

次のパラメータを設定できます。

- メディア ストリーム
- ブロードキャスト SSID
- Radio

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wlan profile-name 例： Device(config)# <code>wlan test4</code>	WLAN コンフィギュレーション サブ モードを開始します。 <i>profile-name</i> は設定されている WLAN のプロファイル名です。
ステップ 3	shutdown 例： Device(config-wlan)# <code>shutdown</code>	WLAN をディセーブルにします。
ステップ 4	broadcast-ssid 例： Device(config-wlan)# <code>broadcast-ssid</code>	この WLAN の SSID をブロードキャストします。
ステップ 5	radio {dot11a dot11ag dot11bg dot11g} 例： Device(config-wlan)# <code>radio dot11g</code>	WLAN で無線をイネーブルにします。キーワードは次のとおりです。 <ul style="list-style-type: none"> • dot11a : 802.11a の無線帯域だけに WLAN を設定します。 • dot11g : 802.11g の無線帯域でのみ WLAN を設定します。 • dot11bg : 802.11b/g の無線帯域でのみ WLAN を設定します (802.11g が無効の場合、802.11b のみ)。 • dot11ag : 802.11g の無線帯域だけに無線 LAN を設定します。
ステップ 6	media-stream multicast-direct 例： Device(config-wlan)# <code>media-stream multicast-direct</code>	この WLAN でマルチキャスト VLAN をイネーブルにします。
ステップ 7	no shutdown 例： Device(config-wlan)# <code>no shutdown</code>	WLAN をイネーブルにします。
ステップ 8	end 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device(config-wlan)# end	

高度な WLAN プロパティの設定 (CLI)

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wlan profile-name 例： Device(config)# wlan test4	WLAN コンフィギュレーション サブ モードを開始します。 <i>profile-name</i> は設定されている WLAN のプロファイル名です。
ステップ 3	chd 例： Device(config-wlan)# chd	この WLAN のカバレッジ ホールの検出をイネーブルにします。
ステップ 4	ccx aironet-iesupport 例： Device(config-wlan)# ccx aironet-iesupport	この WLAN の Aironet IE のサポートをイネーブルにします。
ステップ 5	client association limit { <i>clients-per-wlan</i> ap <i>clients-per-ap-per-wlan</i> radioclients-per-ap-radio--per-wlan } 例： Device(config-wlan)# client association limit ap 400	WLAN で設定できるクライアント、AP あたりのクライアント、または AP 無線あたりのクライアントの最大数を設定します。
ステップ 6	ip access-group web acl-name 例： Device(config-wlan)# ip access-group web test-acl-name	IPv4 WLAN の Web ACL を設定します。可変 <i>acl</i> 名前はユーザー定義する IPv4 ACL の名前を指定します。
ステップ 7	peer-blocking [drop forward-upstream] 例： Device(config-wlan)# peer-blocking drop	ピアツーピア ブロッキング パラメータを設定します。キーワードは次のとおりです。 <ul style="list-style-type: none">• drop : ドロップ アクションのピアツーピア ブロッキングをイネーブルにします。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • forward-upstream : 何もせず、パケットをアップストリームに転送します。
ステップ 8	channel-scan {defer-priority {0-7} defer-time {0 - 6000}} 例 : Device(config-wlan)# channel-scan defer-priority 6	チャンネルスキャンの延期プライオリティと延期時間を設定します。引数は次のとおりです。 <ul style="list-style-type: none"> • defer-priority : オフチャンネルスキャンを延期できるパケットのプライオリティ マーキングを指定します。範囲は 0～7 です。デフォルト値は 3 です。 • defer-time : 延期時間 (ミリ秒単位)。範囲は 0～6000 です。デフォルトは 100 です。
ステップ 9	end 例 : Device(config-wlan)# end	特権 EXEC モードに戻ります。

高度な WLAN プロパティの設定 (GUI)

始める前に

プライマリ コントローラとバックアップコントローラを設定する前に、AP 参加プロファイルがすでに設定済みであることを確認します。

手順

- ステップ 1 [Configuration] > [Wireless] > [WLANs] > [Wireless Networks] の順に選択します。
- ステップ 2 [Wireless Networks] ウィンドウで、[Add] をクリックします。
- ステップ 3 [Advanced] タブで、[Coverage Hole Detection] チェックボックスをオンにします。
- ステップ 4 [Aironet IE] チェック ボックスをオンにして、WLAN で Aironet IE を有効にします。
- ステップ 5 [Diagnostic Channel] チェック ボックスをオンにして、WLAN で診断チャンネルを有効にします。
- ステップ 6 [P2P Blocking Action] ドロップダウンリストから、必要な値を選択します。
- ステップ 7 [Multicast Buffer] トグルボタンを [enabled] または [disabled] に設定します。
- ステップ 8 [Media Stream Multicast-Direct] チェック ボックスをオンにして、この機能を有効にします。
- ステップ 9 [Max Client Connections] セクションで、次についてクライアント接続の最大数を指定します。

- [Per WLAN] フィールドに、値を入力します。有効な範囲は 1 ~ 10000 です。
- [Per AP Per WLAN] フィールドに、値を入力します。有効な範囲は、0 ~ 400 です。
- [Per AP Radio Per WLAN] フィールドに、値を入力します。有効な範囲は、0 ~ 200 です。

ステップ 10 [11v BSS Transition Support] セクションで、次の設定タスクを実行します。

- a) [BSS Transition] チェック ボックスをオンにして、802.11v BSS 移行サポートを有効にします。
- b) [Disassociation Imminent] フィールドに、値を入力します。有効な範囲は、0 ~ 3000 です。
- c) [Optimized Roaming Disassociation Timer] フィールドに、値を入力します。有効な範囲は、0 ~ 40 です。
- d) チェック ボックスをオンにして以下の項目を有効にします。
 - BSS Max Idle Service
 - BSS Max Idle Protected
 - Disassociation Imminent Service
 - Directed Multicast Service
 - Universal Admin
 - Load Balance
 - 帯域選択
 - IP ソース ガード

ステップ 11 [WMM Policy] ドロップダウンリストから、ポリシーとして [Allowed]、[Disabled]、または [Required] を選択します。デフォルトでは、WMM ポリシーが許可されています。

ステップ 12 [Off Channel Scanning Defer] セクションで、適切な [Defer Priority] 値を選択し、必要な [Scan Defer Time] の値をミリ秒単位で指定します。

ステップ 13 [Assisted Roaming (11k)] セクションで、次について適切なステータスを選択します。

- Prediction Optimization
- ネイバー リスト
- Dual-Band Neighbor List

ステップ 14 [DTIM Period (in beacon intervals)] セクションで、802.11a/n 無線と 802.11b/g/n 無線の値を指定します。有効な範囲は 1 ~ 255 です。

ステップ 15 [Save & Apply to Device] をクリックします。

WLAN プロパティの確認 (CLI)

WLAN ID に基づいて WLAN プロパティを確認するには、次の show コマンドを使用します。

```
Device# show wlan id wlan-id
```

WLAN 名に基づいて WLAN プロパティを確認するには、次の show コマンドを使用します。

```
Device# show wlan name wlan-name
```

設定されているすべての WLAN の WLAN プロパティを確認するには、次の show コマンドを使用します。

```
Device# show wlan all
```

すべての WLAN のサマリーを表示するには、次の show コマンドを使用します。

```
Device# show wlan summary
```

WLAN 名に基づいて WLAN の実行中コンフィギュレーションを確認するには、次の show コマンドを使用します。

```
Device# show running-config wlan wlan-name
```

すべての WLAN の実行中コンフィギュレーションを確認するには、次の show コマンドを使用します。

```
Device# show running-config wlan
```


翻訳について

このドキュメントは、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。