OfficeExtend アクセス ポイントの設定

- OfficeExtend アクセス ポイントについて，1 ページ
- OEAP 600 シリーズ アクセス ポイント，2 ページ
- セキュリティの実装，13 ページ
- OfficeExtend アクセス ポイントのライセンシング，13 ページ
- OfficeExtend アクセス ポイントの設定，13 ページ
- OEAP ACL の設定，20 ページ
- 600 シリーズ OEAP 以外の OfficeExtend アクセス ポイントでの個人用 SSID の設定，23 ページ
- OfficeExtend アクセス ポイント統計情報の表示，24 ページ
- OfficeExtend アクセス ポイントの音声メトリックの表示，25 ページ
- 連続したネットワーク診断，26 ページ

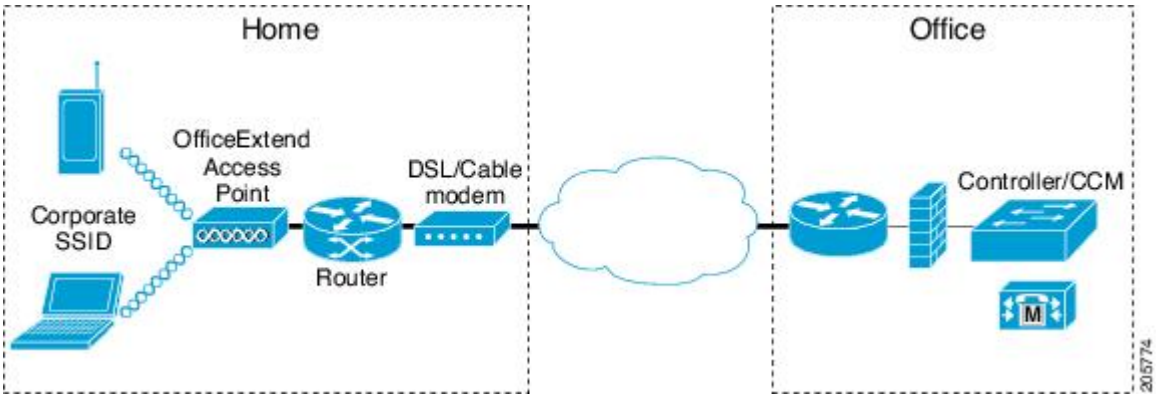
OfficeExtend アクセス ポイントについて

Cisco 600 シリーズ OfficeExtend アクセス ポイント（Cisco OEAP）はコントローラからリモートロケーションのアクセス ポイントへのセキュア通信を提供して、インターネットを通じて会社の WLAN を従業員の自宅にシームレスに拡張します。 ホーム オフィスにおけるユーザの使用感は、会社のオフィスとまったく同じです。 アクセス ポイントとコントローラの間の Datagram Transport Layer Security（DTLS; データグラム トランスポート層セキュリティ）による暗号化は、すべての通信のセキュリティを最高レベルにします。

（注） DTLS は Cisco OEAP で永続的に有効です。 このアクセス ポイントで、DTLS を無効にすることはできません。

次に、一般的な OfficeExtend アクセス ポイント セットアップを示します。

図 *1*：一般的な *OfficeExtend* アクセス ポイント セットアップ



（注） Cisco OEAP は、ルータまたはネットワーク アドレス変換（NAT）を使用するその他のゲートウェイ デバイスの背後で動作するように設計されています。 NAT により、ルータなどのデバイスはインターネット（パブリック）と個人ネットワーク（プライベート）間のエージェントとして動作でき、コンピュータのグループ全体を単一の IP アドレスで表すことができます。 NAT デバイスの背後に配置できる Cisco OEAP の数に制限はありません。 ローミングは Cisco 600 OEAP モデルではサポートされていません。

統合アンテナを備えたすべてのサポートされる屋内 AP モデルは、 AP-7001 および AP-700W シリーズ アクセスを除く OEAP としてアクセス ポイントを設定できます。

OEAP 600 シリーズ アクセス ポイント

ここでは、Cisco 600 シリーズ OfficeExtend アクセス ポイントと一緒に使用するように、Cisco 無線 LAN コントローラを設定するための要件について詳しく説明します。 600 シリーズ OfficeExtend アクセス ポイントは、スプリット モード動作をサポートしており、ローカル モードでの WLAN コントローラを介した設定を必要とします。 ここでは、適切に接続するために必要な設定と、サポートされている機能セットについて説明します。

（注） IPv6 は、Cisco 600 シリーズ OfficeExtend アクセス ポイントではサポートされません。

（注） WLAN コントローラと 600 シリーズ OfficeExtend アクセス ポイントの間にあるファイアウォールで、CAPWAP UDP 5246 および 5247 が開いている必要があります。

（注） マルチキャストは、Cisco 600 シリーズ OfficeExtend アクセス ポイントではサポートされません。

ローカル モードの OEAP

600 シリーズ OfficeExtend アクセス ポイントは、ローカル モードでコントローラに接続します。これらの設定は変更できません。

（注） Monitor モード、FlexConnect モード、Sniffer モード、Rogue Detector、Bridge、および SE-Connect は、600 シリーズ OfficeExtend アクセス ポイントではサポートされておらず、設定することはできません。

図 *2*：*OEAP* モード

600 シリーズ OfficeExtend アクセス ポイントに対してサポートされる WLAN の設定

600 シリーズ OfficeExtend アクセス ポイントでは、最大で 3 つの WLAN と 1 つのリモート LAN がサポートされます。 ネットワーク導入に 4 つ以上の WLAN が存在する場合は、600 シリーズ OfficeExtend アクセス ポイントを AP グループに入れる必要があります。 600 シリーズ OfficeExtend アクセス ポイントが AP グループに追加されると、3 つの WLAN と 1 つのリモート LAN に対する同一の制限が AP グループの設定に適用されます。

600 シリーズ OfficeExtend アクセス ポイントがデフォルト グループにある場合、つまり、定義された AP グループにない場合、WLAN/リモート LAN ID を ID 7 以下に設定する必要があります。

600 シリーズ OfficeExtend アクセス ポイントにより使用されている WLAN またはリモート LAN を変更する目的で、追加の WLAN またはリモート LAN を作成する場合は、新しい WLAN またはリモート LAN を 600 シリーズ OfficeExtend アクセス ポイントで有効にする前に、削除する現在の WLAN またはリモート LAN を無効にする必要があります。 AP グループで複数のリモート LAN が有効にされている場合は、すべてのリモート LAN を無効にしてから 1 つのリモート LAN のみを有効にしてください。

AP グループで 4 つ以上の WLAN が有効にされている場合は、すべての WLAN を無効にしてから 3 つの WLAN のみを有効にしてください。

600 シリーズ OfficeExtend アクセス ポイントに対する WLAN のセキュリティ設定

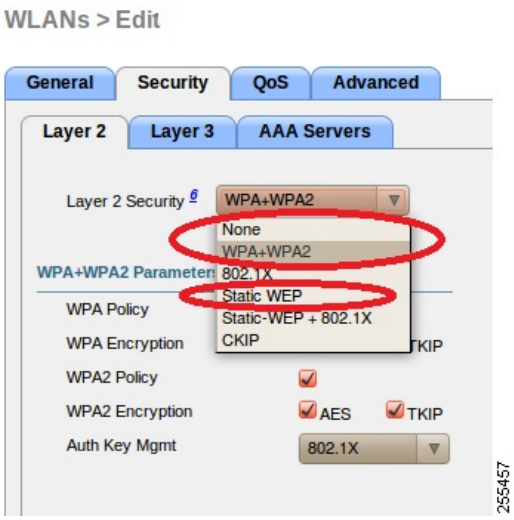
WLAN でセキュリティを設定（次の図を参照）する際は、600 シリーズ OfficeExtend アクセス ポイントでサポートされていない特定の要素があることに注意してください。 CCX は、600 シリーズ OfficeExtend アクセス ポイントではサポートされず、CCX に関連する要素もサポートされません。

レイヤ 2 セキュリティの場合、600 シリーズ OfficeExtend アクセス ポイントに対して次のオプションがサポートされます。

- なし
- WPA+WPA2
- Static WEP

- 802.1X（リモート LAN の場合のみ）

図 *3*：*WLAN* レイヤ *2* セキュリティ設定



[Security] タブ（次の図を参照）では、WPA+WPA2 設定の [CCKM] を選択しないでください。802.1X または PSK のみを設定します。

図 *4*：*WLAN* のセキュリティ設定 - 認証キー管理

TKIP および AES に対するセキュリティの暗号化設定は、WPA と WPA2 で同一であることが必要です。 次に、TKIP と AES に対する非互換の設定例を示します。

図 *5* : ***OEAP 600*** シリーズに対する非互換の ***WPA*** および ***WPA2*** セキュリティ暗号化設定

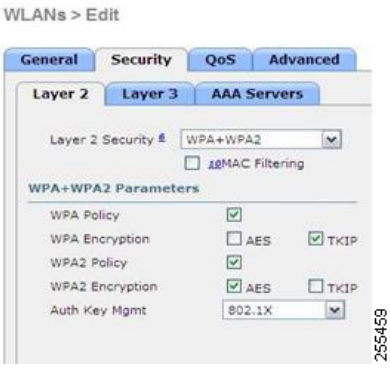


図 *6* : ***OEAP 600*** シリーズに対する非互換の ***WPA*** および ***WPA2*** セキュリティ暗号化設定

次に、互換性のある設定例を示します。

図 *7*：*OEAP* シリーズに対する互換性のあるセキュリティ設定

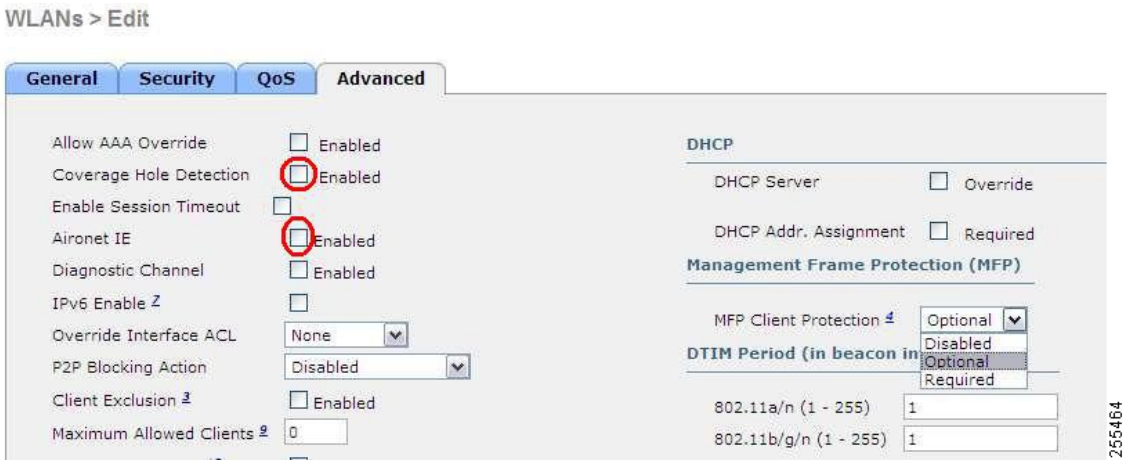
図 *8*：*OEAP* シリーズに対する互換性のあるセキュリティ設定

QoS 設定はサポートされています（次の図を参照）が、CAC 設定はサポートされていないため、有効にしないでください。

（注） カバレッジ ホールの検出は有効にしないでください。

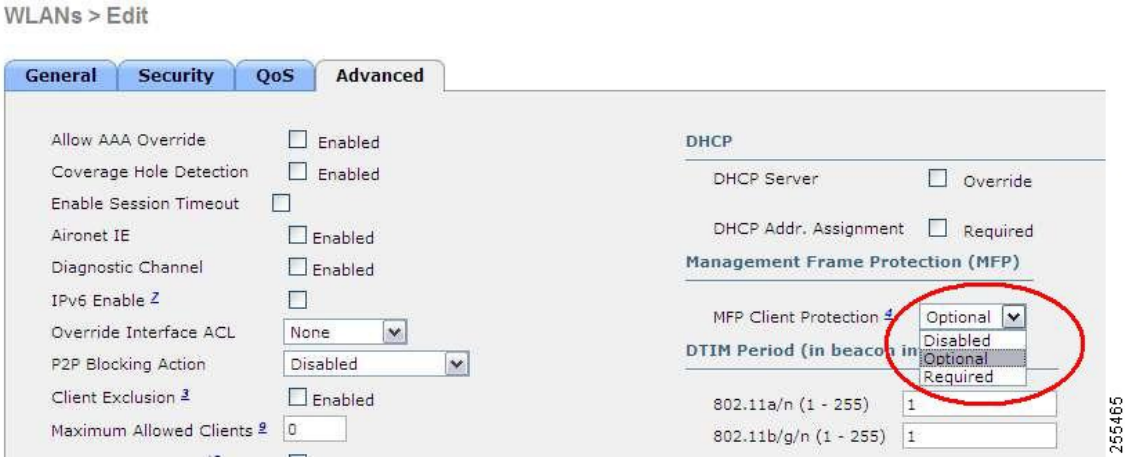
（注） Aironet IE は有効にしないでください。 このオプションはサポートされていません。

図 *9*：*OEAP 600* に対する *QoS* の設定



MFP もサポートされていないので、無効にするか、[Optional] に設定してください。

図 *10*：*OEAP* シリーズ アクセス ポイントに対する *MFP* の設定



クライアント ロード バランシングおよびクライアント帯域の選択はサポートされていません。

認証の設定

600 シリーズ OfficeExtend アクセス ポイントの認証の場合、LEAP はサポートされません。 この設定については、EAP-Fast、EAP-TTLS、EAP-TLS、または PEAP に移行するように、クライアントおよび RADIUS サーバで対処する必要があります。

コントローラでローカル EAP が使用されている場合も、LEAP が使用されないように設定を変更する必要があります。

600 シリーズ OfficeExtend アクセス ポイントでサポートされるユーザ カウント

一度に 15 のユーザだけが Cisco 600 シリーズ OEAP で提供される WLAN に接続できます。クライアントのいずれかが認証を解除されるか、コントローラのタイムアウトが発生するまで、16 番目のユーザは認証できません。 この数は、600 シリーズ OfficeExtend アクセス ポイントでのコントローラ WLAN における累積数です。

たとえば、2 つのコントローラ WLAN が設定されており、1 つの WLAN に 15 ユーザが接続している場合、600 シリーズ OfficeExtend アクセス ポイントでは同時にもう 1 つの WLAN に別のユーザが join することができません。

この制限は、エンド ユーザが 600 シリーズ OfficeExtend アクセス ポイントで個人用に設定するローカル プライベート WLAN には適用されません。 これらのプライベート WLAN または有線ポートで接続されるクライアントは、これらの制限に影響しません。

（注） この制限は、OfficeExtend モードで動作する他の AP モデルには適用されません。

リモート LAN の設定

600 シリーズ OfficeExtend アクセス ポイントでは、リモート LAN ポートを介して 4 つのクライアントのみ接続できます。 この接続クライアントの数は、コントローラ WLAN でのユーザ制限数（15）には影響しません。 リモート LAN のクライアント制限では、リモート LAN ポートにスイッチまたはハブを接続して複数のデバイスを接続することや、このポートに接続している Cisco IP フォンに直接接続することは可能です。 接続できるデバイスは 4 つまでです。これは、この 4 つのデバイスの 1 つのアイドル時間が 1 分を超えるまで適用されます。

リモート LAN は、コントローラでの WLAN またはゲスト LAN の設定と同様に設定されます。

図 *11*：*OEAP 600* シリーズ *AP* に対するリモート *LAN* の設定

[Security] 設定を開いたままにし、MAC フィルタリングまたは Web 認証を設定することができます。 デフォルトでは MAC フィルタリングが使用されます。 さらに、802.1X レイヤ 2 セキュリティ設定を指定することもできます。

図 *12*：リモート *LAN* の *OEAP 600* シリーズ *AP* に対するレイヤ *2* セキュリティ設定

図 *13*：リモート *LAN* の *OEAP 600* シリーズ *AP* に対するレイヤ *3* セキュリティ設定

チャネルの管理と設定

600 シリーズ OfficeExtend アクセス ポイントの無線は、無線 LAN コントローラではなく、そのアクセス ポイントのローカル GUI で管理されます。 TX 電力およびチャネル設定はコントローラインターフェイスを使用して手動で設定できます。 RRM は、600 シリーズ OfficeExtend アクセス ポイントではサポートされません。

ローカル GUI で 2.4 GHz および 5.0 GHz の両方のデフォルト設定を変更していない限り、600 シリーズは起動時にチャネルをスキャンし、2.4 GHz および 5 GHz のチャネルを選択します。

図 *14*：*OEAP 600* シリーズ *AP* のチャネル選択

20 MHz または 40 MHz のワイド チャネルについても、600 シリーズ OfficeExtend アクセス ポイントのローカル GUI で 5.0 GHz 用のチャネル帯域幅が設定されます。 2.4 GHz のチャネル幅を 40 MHz に設定することはできず、20 MHz に固定されます。

図 *15*：*OEAP 600 AP* のチャネル幅

ファイアウォールの設定

ファイアウォールは Cisco 600 シリーズ OfficeExtend アクセス ポイントで有効にすることが可能で、フィルタリングと転送ルールを適用できます。 事前に設定された以下の 10 個のアプリケーションは、有効または無効にできます。

- FTP
- Telnet
- SMTP
- DNS
- TFTP
- HTTP
- POP3
- NNTP
- SNMP
- HTTPS

これらのアプリケーションは、プロトコル（TCP/UDP）、LAN クライアント IP 範囲、および宛先ポートの範囲を指定してブロック解除できます。

（注） ファイアウォールは、OEAP 600 AP 上のパーソナル トラフィックにのみ適用されます。コントローラと OEAP 600 AP 間のデータ トラフィックは、企業ネットワーク内のファイアウォールによってアドレスされます。

600 シリーズ OfficeExtend アクセス ポイントは、最大で 10 個のポートの転送ルールをサポートします。 すべてのルールは、パラメータとしてプロトコル（TCP/UDP）、WAN のポート範囲、ローカル LAN クライアント IP（トラフィックが転送される場合）、LAN のポート範囲、および有効/無効を使用します。

DMZ 機能により、ローカル LAN または WLAN に接続されている 1 つのネットワーク コンピュータを、特別な目的のサービス（インターネット ゲームなど）に使用するためにインターネットに公開することができます。 DMZ は、WAN IP で終了するすべてのポートを 1 つの PC へ同時に転送します。 ポート範囲の転送機能は、オープンすることを要求されているポートのみをオープンしますが、DMZ は 1 つのコンピュータのすべてのポートをオープンし、そのコンピュータをインターネットまたは WAN に公開します。 これは、受信するすべての WAN パケットを、ポートの転送ルールが設定されているいずれかのポートに転送します。 CAPWAP コントロールおよびデータ接続ポートは、DMZ IP に転送されません。

その他の注意事項

- Cisco 600 シリーズ OfficeExtend アクセス ポイント（OEAP）は、単一の AP 導入向けに設計されているので、Cisco 600 シリーズ OEAP 間のクライアント ローミングはサポートされません。

  コントローラで 802.11a/n/ac または 802.11b/g/n を無効にしても、ローカル SSID がまだ有効であるために、Cisco 600 シリーズ OEAP ではこれらのスペクトラムが無効にならない場合があります。

- ファイアウォールは、アクセス ポイントからの CAPWAP を使用するトラフィックを許可するよう設定されている必要があります。 UDP ポート 5246 および 5247 が有効であり、アクセス ポイントがコントローラに join できないようにする可能性のある中間デバイスによりブロックされていないことを確認してください。

- OEAP モードに変換され、ローカルでスイッチされる WLAN にマッピングされる 600 シリーズ OEAP 以外の Cisco Aironet AP は、AP 接続スイッチ上のローカル サブネットに DHCP 要求を転送します。 この状態を回避するには、ローカル スイッチングとローカル認証を無効にする必要があります。

- Cisco 仮想ワイヤレス LAN コントローラに関連付ける Cisco 600 シリーズ OEAP の場合は、次の手順を実行します。

  1. 7.5 以降のリリースを使用する物理コントローラに関連付ける OEAP を設定して、対応する AP イメージをダウンロードします。
  2. OEAP が物理コントローラに再び関連付けないように OEAP を設定します。たとえば、ネットワークに ACL を実装して、OEAP と物理コントローラ間の CAPWAP をブロックできます。

3 Cisco 仮想ワイヤレス LAN コントローラに関連付ける OEAP を設定します。

セキュリティの実装

（注） LSC の設定は要件ではなく、オプションです。 OfficeExtend 600 アクセス ポイントは、LSC をサポートしません。

1 「LSC を使用したアクセス ポイントの許可」の手順に従って、Local Significant Certificates（LSC）を使用して OfficeExtend アクセス ポイントを許可します。

2 次のコマンドを入力して、アクセス ポイントの MAC アドレス、名前、または両方を許可要求のユーザ名で使用して AAA サーバ検証を実装します。

config auth-list ap-policy authorize-ap username {*ap_mac* | *Cisco_AP* | **both**}

検証にアクセス ポイント名を使用すると、有効な従業員の OfficeExtend アクセス ポイントのみをコントローラに関連付けることができます。 このセキュリティ ポリシーを実装するには、各 OfficeExtend アクセス ポイントに、従業員の ID または番号で名前を付けます。 従業員が離職した場合は、AAA サーバ データベースからこのユーザを削除するスクリプトを実行して、その従業員の OfficeExtend アクセス ポイントがネットワークに join できないようにします。

3 次のコマンドを入力して、変更を保存します。

save config

（注） CCX は、600 OEAP ではサポートされません。 CCX に関連する要素はサポートされません。また、802.1X または PSK のみがサポートされます。 TKIP および AES セキュリティ暗号化の設定は、WPA と WPA2 で同一であることが必要です。

OfficeExtend アクセス ポイントのライセンシング

OfficeExtend アクセス ポイントを使用するには、コントローラに基本ライセンスがインストールされ、使用されている必要があります。 ライセンスのインストール後は、OfficeExtend モードに対応したサポート対象の Cisco Aironet AP モデルの OfficeExtend モードを有効にすることができます。

OfficeExtend アクセス ポイントの設定

Cisco Aironet アクセス ポイントがコントローラとアソシエートしている場合は、それを OfficeExtend アクセス ポイントとして設定できます。

OfficeExtend アクセス ポイントの設定（GUI）

ステップ 1 [Wireless] を選択して、[All APs] ページを開きます。

ステップ 2 目的のアクセス ポイントの名前をクリックして、[All APs > Details] ページを開きます。

ステップ 3 次の手順で、アクセス ポイントに対して FlexConnect を有効にします。

a) [General] タブで、[AP Mode] ドロップダウン リストから [FlexConnect] を選択し、このアクセス ポイントに対して FlexConnect を有効にします。

ステップ 4 次の手順で、アクセス ポイントに 1 つまたは複数のコントローラを設定します。

a) [High Availability] タブをクリックします

b) このアクセス ポイントのプライマリ コントローラの名前と IP アドレスを [Primary Controller Name] テキスト ボックスおよび [Management IP Address] テキスト ボックスに入力します。

（注） コントローラの名前および IP アドレスの両方を入力する必要があります。 入力しないと、アクセス ポイントはコントローラに join できません。

c) 必要に応じて、セカンダリまたはターシャリ コントローラ（または両方）の名前および IP アドレスを、対応する [Controller Name] テキスト ボックスおよび [Management IP Address テキスト ボックスに入力します。

d) [Apply] をクリックします。 アクセス ポイントはリブートしてからコントローラに再 join します。

（注） プライマリ、セカンダリ、およびターシャリ コントローラの名前および IP アドレスは一意である必要があります。

ステップ 5 次の手順で、OfficeExtend アクセス ポイントの設定を有効にします。

a) [FlexConnect] タブをクリックします。

b) [Enable OfficeExtend AP] チェックボックスをオンにして、このアクセス ポイントの OfficeExtend モードを有効にします。 デフォルト値はオンです。
このチェックボックスをオフにすると、このアクセス ポイントの OfficeExtend モードが無効になります。 アクセス ポイントの設定すべてが取り消されることはありません。 アクセス ポイントの設定をクリアして工場出荷時のデフォルト設定に戻す場合は、コントローラ CLI で **clear ap config***Cisco_AP* と入力します。 アクセス ポイントの個人の SSID のみをクリアする場合は、[Reset Personal SSID] をクリックします。

（注） OfficeExtend AP サポートがサポート対象のすべての Cisco Aironet 統合アンテナ アクセス ポイントに対して有効になります。

（注） アクセス ポイントに対して OfficeExtend モードを有効にした場合は、不正なアクセス ポイントの検出が自動的に無効になります。 ただし、[All APs > Details for]（Advanced）ページで [Rogue Detection] チェックボックスをオンまたはオフにして、特定のアクセス ポイントの不正検出を有効または無効にできます。 家庭の環境で展開されるアクセス ポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出はデフォルトでは無効です。

（注） アクセス ポイントに対して OfficeExtend モードを有効にした場合は、DTLS データ暗号化が自動的に有効になります。 ただし、[All APs > Details for]（[Advanced]）ページで [**Data Encryption**] チェックボックスをオンまたはオフにして、特定のアクセス ポイントの DTLS データ暗号化を有効または無効にできます。

（注） アクセス ポイントに対して OfficeExtend モードを有効にした場合は、Telnet および SSH アクセスが自動的に無効になります。 ただし、[All APs > Details for]（[Advanced]）ページで [**Telnet**] チェックボックスまたは [**SSH**] チェックボックスをオンまたはオフにして、特定のアクセス ポイントの Telnet アクセスまたは SSH アクセスを有効または無効にできます。

（注） アクセス ポイントに対して OfficeExtend モードを有効にした場合は、リンク遅延が自動的に有効になります。 ただし、[All APs > Details for]（[Advanced]）ページで [Enable Link Latency] チェックボックスをオンまたはオフにして、特定のアクセス ポイントのリンク遅延を有効または無効にできます。

c) join 時にアクセス ポイントに遅延の最も少ないコントローラを選択させたい場合は、[Enable Least Latency Controller Join] チェックボックスをオンにします。 有効にしない場合は、このチェックボックスをオフのままにします（デフォルト値）。 この機能を有効にすると、アクセス ポイントは discovery request と discovery response の間の時間を計算し、最初に応答した Cisco 5500 シリーズ コントローラに join します。

d) [Apply] をクリックします。
[All APs] ページの [OfficeExtend AP] テキスト ボックスには、どのアクセス ポイントが OfficeExtend アクセス ポイントとして設定されているかが表示されます。

ステップ 6 OfficeExtend アクセス ポイントに特定のユーザ名とパスワードを設定して、ホーム ユーザが OfficeExtend アクセス ポイントの GUI にログインできるようにします。

a) [Credentials] タブをクリックします。

b) [Override Global Credentials] チェックボックスをオンにし、このアクセス ポイントがコントローラからグローバルユーザ名、パスワード、イネーブルパスワードを継承しないようにします。 デフォルト値はオフです。

c) [Username]、[Password]、および [Enable Password] テキスト ボックスに、このアクセス ポイントに割り当てる独自のユーザ名、パスワード、およびイネーブル パスワードを入力します。

（注） 入力した情報は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに join された場合でも保持されます。

d) [Apply] をクリックします。

（注） このアクセスポイントで、コントローラのグローバル資格情報を強制的に使用する必要がある場合は、[Over-ride Global Credentials] チェックボックスをオフにします。

ステップ 7 OfficeExtend アクセス ポイントのローカル GUI、LAN ポート、およびローカル SSID へのアクセスを設定します。

a) [WIRELESS] > [Access Points] > [Global Configuration] の順に選択して [Global Configuration] ページを開きます。

b) [OEAP Config Parameters] の下の [Disable Local Access] チェックボックスをオンまたはオフにして、OfficeExtend アクセス ポイントのローカル アクセスを有効または無効にします。

（注） デフォルトでは、[Disable Local Access] チェックボックスはオフになるので、イーサネットポートおよび個人の SSID が有効になります。 この設定は、リモート LAN に影響しません。ポートは、リモート LAN を設定する場合のみ有効になります。

ステップ 8 次のように、OfficeExtend アクセス ポイントのスプリット トンネリングを設定します。

a) [Wireless] > [Access Points] > [Global Configuration] を選択します。

b) [OEAP Config Parameters] 領域で、[Disable Split Tunnel] チェックボックスをオンまたはオフにします。ここでスプリット トンネリングを無効にすると、すべての WLAN およびリモート LAN のスプリット トンネリングが無効になります。 特定の WLAN またはリモート LAN のスプリット トンネリングを無効にすることもできます。

c) [Apply] をクリックします。

ステップ 9 [Save Configuration] をクリックします。

ステップ 10 コントローラが OfficeExtend アクセス ポイントのみをサポートする場合は、「RRM の設定」の項で、DCA 間隔、チャネル スキャン間隔、およびネイバー パケット間隔に推奨される値を設定する手順を参照してください。

OfficeExtend アクセス ポイントの設定（CLI）

- 次のコマンドを入力して、アクセス ポイントで FlexConnect を有効にします。
  config ap mode flexconnect*Cisco_AP*
- アクセス ポイントに 1 つまたは複数のコントローラを設定するには、次のいずれか、またはすべてのコマンドを入力します。
  config ap primary-base *controller_name Cisco_APcontroller_ip_address*

  config ap secondary-base *controller_name Cisco_APcontroller_ip_address*

  config ap tertiary-base *controller_name Cisco_APcontroller_ip_address*

（注） コントローラの名前および IP アドレスの両方を入力する必要があります。 入力しないと、アクセス ポイントはコントローラに join できません。

（注） プライマリ、セカンダリ、およびターシャリ コントローラの名前および IP アドレスは一意である必要があります。

- 次のコマンドを入力して、このアクセス ポイントで OfficeExtend モードを有効にします。
  config flexconnect office-extend {**enable** | **disable**} *Cisco_AP*

  デフォルト値はイネーブルです。 **disable** パラメータは、このアクセス ポイントの OfficeExtend モードを無効にします。アクセス ポイントの設定すべてが取り消されることはありません。アクセス ポイントの設定をクリアして工場出荷時のデフォルト設定に戻す場合は、次のコマンドを入力します。

  clear ap config*cisco-ap*

  アクセス ポイントの個人の SSID のみをクリアする場合は、次のコマンドを入力します。

  config flexconnect office-extendclear-personalssid-config*Cisco_AP.*

（注） アクセス ポイントに対して OfficeExtend モードを有効にした場合は、不正なアクセス ポイントの検出が自動的に無効になります。 ただし、**config rogue detection** {**enable** | **disable**} {*Cisco_AP* | **all**} コマンドを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの不正検出を有効または無効にできます。 家庭の環境で展開されるアクセス ポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出はデフォルトでは無効です。

（注） アクセス ポイントに対して OfficeExtend モードを有効にした場合は、DTLS データ暗号化が自動的に有効になります。 ただし、**config ap link-encryption** {**enable** | **disable**} {*Cisco_AP* | **all**} コマンドを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの DTLS データ暗号化を有効または無効にできます。

（注） アクセス ポイントに対して OfficeExtend モードを有効にした場合は、Telnet および SSH アクセスが自動的に無効になります。 ただし、**config ap** {**telnet**| **ssh**} {**enable** | **disable**} *Cisco_AP* コマンドを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの Telnet または SSH アクセスを有効または無効にできます。

（注） アクセス ポイントに対して OfficeExtend モードを有効にした場合は、リンク遅延が自動的に有効になります。 ただし、**config ap link-latency** {**enable** | **disable**} {*Cisco_AP* | **all**} コマンドを使用して、コントローラに現在アソシエートされている特定のアクセス ポイントまたはすべてのアクセス ポイントのリンク遅延を有効または無効にできます。

- 次のコマンドを入力して、join 時にアクセス ポイントが遅延の最も少ないコントローラを選択できるようにします。
  config flexconnect join min-latency {**enable** | **disable**} *Cisco_AP*

  デフォルト値は [disabled] です。 この機能を有効にすると、アクセス ポイントは discovery request と discovery response の間の時間を計算し、最初に応答した Cisco 5500 シリーズ コントローラに join します。

- 次のコマンドを入力して、ホーム ユーザが OfficeExtend アクセス ポイントの GUI にログインするために入力できる特定のユーザ名とパスワードを設定します。
  config ap mgmtuser add username*user***password***password***enablesecret***enable_password**Cisco_AP*

  このコマンドに入力した資格情報は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに join された場合でも保持されます。

（注） このアクセス ポイントで、コントローラのグローバル資格情報を強制的に使用する必要がある場合は、**config ap mgmtuser delete***Cisco_AP* コマンドを入力します。 このコマンドの実行後、「AP reverted to global username configuration」というメッセージが表示されます。

- Cisco 600 シリーズ OfficeExtend アクセス ポイントにローカル ネットワークへのアクセスを設定するには、次のコマンドを入力します。
  config network oeap-600 local-network {**enable** | **disable**}

  無効の場合は、ローカル SSID、ローカル ポートが機能せず、コンソールにアクセスできません。 リセットすると、デフォルトによってローカル アクセスが復元されます。 アクセス ポイントに設定する場合、この設定はリモート LAN 設定に影響しません。

- 次のコマンドを入力して、Cisco 600 シリーズ OfficeExtend アクセス ポイントのイーサネット ポート 3 がリモート LAN として動作できるようにする、デュアル R-LAN ポート機能を設定します。
  config network oeap-600 dual-rlan-ports {**enable** | **disable**}

  この設定は、コントローラに対してグローバルであり、AP および NVRAM 変数によって保存されます。 この変数が設定されていると、リモート LAN の動作が変わります。 この機能は、リモート LAN ポートごとに異なるリモート LAN をサポートします。

  リモート LAN マッピングは、デフォルト グループが使用されているか、または AP グループが使用されているかによって、次のように異なります。

  - デフォルト グループ：デフォルト グループを使用している場合、偶数のリモート LAN ID を持つ単一のリモート LAN がポート 4 にマッピングされます。 たとえば、リモート LAN ID 2 のリモート LAN は、ポート 4（Cisco 600 OEAP 上）にマッピングされます。 奇数のリモート LAN ID を持つリモート LAN は、ポート 3（Cisco 600 OEAP 上）にマッピングされます。 たとえば、リモート LAN ID 1 のリモート LAN は、ポート 3（Cisco 600 OEAP 上）にマッピングされます。

  - AP グループ：AP グループを使用する場合、OEAP-600 ポートへのマッピングは AP グループの順序によって決定します。 AP グループを使用するには、まず、AP グループからすべてのリモート LAN および WLAN を削除して、空にする必要があります。 次に、2 つのリモート LAN を AP グループに追加します。最初にポート 3 AP リモート LAN を追加してから、ポート 4 リモート グループを追加し、続けて WLAN を追加します。

- 次のコマンドを入力して、スプリット トンネリングを有効または無効にします。
  config network oeap-600 split-tunnel {**enable** | **disable**}
  ここでスプリット トンネリングを無効にすると、すべての WLAN およびリモート LAN のスプリット トンネリングが無効になります。 特定の WLAN またはリモート LAN のスプリット トンネリングを無効にすることもできます。

- 次のコマンドを入力し、ゲートウェイをオーバーライドせずにスプリット トンネリングを有効にします。
  config wlan split-tunnel*wlan-id***enabledapply-acl** *acl name*

- このコマンドを入力して、ゲートウェイのオーバーライドとプロセスのスプリット トンネリング:
  config wlan split-tunnel*wlan-id***enabled override gateway***gateway ip***mask***subnet mask***apply-acl** *acl name*
- 次のコマンドを入力して、変更を保存します。
  save config

（注） コントローラが OfficeExtend アクセス ポイントのみをサポートする場合は、「無線リソース管理の設定」の項で、DCA 間隔に推奨される値を設定する手順を参照してください。

WLAN またはリモート LAN のスプリット トンネリングの設定

WLAN またはリモート LAN のスプリット トンネリングの設定（GUI）

ステップ 1 [WLANs] を選択し、[WLAN ID] をクリックして、[WLANs > Edit] ページを開きます。
選択する WLAN はその設定によって WLAN またはリモート LAN を指定できます。

ステップ 2 [Advanced] タブをクリックします。

ステップ 3 [OEAP] 領域で、[Split Tunnel] チェックボックスをオンまたはオフにします。

ステップ 4 [Gateway Override] チェックボックスをオンにして、 [Gateway IP] と [Subnet Mask] を設定します。 このチェックボックスがオフの場合、WLAN または RLAN にマップされているインターフェイスが使用されます。

ステップ 5 ドロップダウン リストから [Associated ACL] を選択します。 [None] を選択すると、ACL を選択する必要があることを示すエラー メッセージが表示されます。

ステップ 6 [Apply] をクリックします。

ステップ 7 [Save Configuration] をクリックします。

WLAN またはリモート LAN のスプリット トンネリングの設定（CLI）

- 次のコマンドを入力して、WLAN のスプリット トンネリングを有効または無効にします。
  config wlan split-tunnel*wlan-id* {**enable** | **disable**}
- 次のコマンドを入力して、WLAN のスプリット トンネリングのステータスを表示します。
  show wlan*wlan-id*
- 次のコマンドを入力して、リモート LAN のスプリット トンネリングを有効または無効にします。
  config remote-lan split-tunnel*rlan-id* {**enable** | **disable**}

- 次のコマンドを入力して、リモート LAN のスプリット トンネリングのステータスを表示します。
  show remote-lan*rlan-id*

（注） 企業 SSID のリモート LAN または無線クライアントが、コミュニティ ポート間で通信する場合、企業 SSID およびリモート LAN 上のすべてのトラフィックがコントローラへのトンネルを説明しています。

OEAP ACL の設定

OEAP ACL の設定（GUI）

ステップ 1 [Wireless] > [OEAP ACLs] の順に選択します。
[OEAP ACL] ページが表示されます。

このページには、コントローラ上で設定したすべての OEAP ACL が一覧表示されます。 ACL を削除するには、該当する ACL 名の横にある青のドロップダウン矢印の上にカーソルを移動し、[Remove] を選択します。

ステップ 2 [New] をクリックして、新しい ACL を追加します。
[Access Control Lists > New] ページが表示されます。

ステップ 3 [Access Control List Name] テキスト ボックスに、新しい ACL の名前を入力します。 最大 32 文字の英数字を入力できます。

ステップ 4 [Apply] をクリックします。

ステップ 5 [Access Control Lists] ページが再度表示されたら、新しい ACL の名前をクリックします。
[Access Control Lists > Edit] ページが表示されたら、[Add New Rule] をクリックします。

[Access Control Lists > Rules > New] ページが表示されます。

ステップ 6 この ACL のルールを次のように設定します。

a) コントローラは各 ACL について最大 64 のルールをサポートします。 これらのルールは、1 から 64 の順にリストアップされます。 [Sequence] テキスト ボックスで、値（1 ～ 64）を入力し、この ACL に定義されている他のルールに対するこのルールの順番を決定します。

（注） ルール 1 ～ 4 がすでに定義されている場合にルール 29 を追加すると、これはルール 5 として追加されます。 ルールのシーケンス番号を追加または変更した場合は、順序を維持するために他のルールのシーケンス番号が自動的に調整されます。 たとえば、ルールのシーケンス番号を 7 から 5 に変更した場合、シーケンス番号 5 および 6 のルールはそれぞれ 6 および 7 へと自動的に番号が変更されます。

b) [Source] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL を適用するパケットの送信元を指定します。

- [Any]：任意の送信元（これはデフォルト値です）。
- [IP Address]：特定の送信元。 このオプションを選択する場合は、該当するテキスト ボックスに送信元の IP アドレスとネットマスクを入力します。

c) [Destination] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL を適用するパケットの宛先を指定します。

- [Any]：任意の宛先（これはデフォルト値です）。
- [IP Address]：特定の宛先。 このオプションを選択する場合は、テキスト ボックスに宛先の IP アドレスとネットマスクを入力します。
- [Network List]：特定のネットワーク リスト。 このオプションを選択した場合は、ネットワーク リストに設定されている、会社のサブネットを入力します。

d) [Protocol] ドロップダウン リストから、この ACL に使用する IP パケットのプロトコル ID を選択します。 使用できるプロトコル オプションは、次のとおりです。

- [Any]：任意のプロトコル（これは、デフォルト値です）
- TCP
- UDP
- [Other]：その他の Internet Assigned Numbers Authority（IANA）プロトコル

（注） Other を選択する場合は、[Protocol] テキスト ボックスに目的のプロトコルの番号を入力します。 使用可能なプロトコルのリストは IANA Web サイトで確認できます。

e) [Action] ドロップダウン リストから、この ACL でパケットをブロックする場合は [Deny] を選択し、この ACL でパケットを許可する場合は [Permit] を選択します。または、ルールと一致したすべてのパケットをローカル ネットワークにルートする場合は [Nat-route] を選択し、ルールと一致したパケットをインターネットへルートする場合は [NAT] を選択します。デフォルト値は [Deny] です。

f) [Apply] をクリックします。
[Access Control Lists > Edit] ページが表示され、この ACL のルールが示されます。

g) この ACL にさらにルールを追加するにはこの手順を繰り返します。

ステップ 7 [Save Configuration] をクリックします。

OEAP ACL の設定（CLI）

手順の概要

1. 次のコマンドを入力して、ACL を作成または削除します。
2. 次のコマンドを入力して、ACL ルールを作成します。
3. 次のコマンドを入力して、ACL ルールのアクションを指定します。
4. 次のコマンドを入力して、ACL ルールの宛先を指定します。
5. 次のコマンドを入力して、ACL ルールの宛先ポートを指定します。
6. 次のコマンドを入力して、ACL ルールの送信元アドレスを指定します。
7. 次のコマンドを入力して、ACL ルールの送信元ポートを指定します。
8. 次のコマンドを入力して、ACL ルールのプロトコルを指定します。
9. 次のコマンドを入力して、2 つの ACL ルールのインデックスまたは優先順位を交換します。
10. 次のコマンドを入力して、ACL ルールのインデックスまたは優先順位を変更します。
11. 次のコマンドを入力して、ACL ルールを削除します。
12. 次のコマンドを入力して、すべての ACL をリストします。
13. 次のコマンドを入力して、特定の ACL の詳細を表示します。

手順の詳細

ステップ 1 次のコマンドを入力して、ACL を作成または削除します。
config oeap-acl create|delete

ステップ 2 次のコマンドを入力して、ACL ルールを作成します。
config oeap-acl rule

ステップ 3 次のコマンドを入力して、ACL ルールのアクションを指定します。
config oeap-acl rule action

ステップ 4 次のコマンドを入力して、ACL ルールの宛先を指定します。
config oeap-acl rule destination mode address|local|network-list

ステップ 5 次のコマンドを入力して、ACL ルールの宛先ポートを指定します。
config oeap-acl rule destination port

ステップ 6 次のコマンドを入力して、ACL ルールの送信元アドレスを指定します。
config oeap-acl rule source address

ステップ 7 次のコマンドを入力して、ACL ルールの送信元ポートを指定します。
config oeap-acl rule source port

ステップ 8 次のコマンドを入力して、ACL ルールのプロトコルを指定します。
config oeap-acl rule protocol*protocol*

ここで *protocol* パラメータは、0 ～ 255 の間の値または any です。

ステップ 9 次のコマンドを入力して、2 つの ACL ルールのインデックスまたは優先順位を交換します。
config oeap-acl rule swap index

ステップ 10 次のコマンドを入力して、ACL ルールのインデックスまたは優先順位を変更します。
config oeap-acl rule change index

ステップ 11 次のコマンドを入力して、ACL ルールを削除します。
config oeap-acl rule delete

ステップ 12 次のコマンドを入力して、すべての ACL をリストします。
show oeap-acl summary

ステップ 13 次のコマンドを入力して、特定の ACL の詳細を表示します。
show oeap-acl detailed*ACL_name*

600 シリーズ OEAP 以外の OfficeExtend アクセス ポイントでの個人用 SSID の設定

ステップ 1 次のいずれかの手順で、OfficeExtend アクセス ポイントの IP アドレスを確認します。

- ホーム ルータにログインして OfficeExtend アクセス ポイントの IP アドレスを見つけます。
- 会社の IT 担当に OfficeExtend アクセス ポイントの IP アドレスを確認します。
- Network Magic などのアプリケーションを使用して、ネットワーク上のデバイスおよびデバイスの IP アドレスを検出します。

ステップ 2 OfficeExtend アクセス ポイントがホーム ルータに接続された状態で、インターネット ブラウザの [Address] テキスト ボックスに OfficeExtend アクセス ポイントの IP アドレスを入力して [Go] をクリックします。

（注） バーチャル プライベート ネットワーク（VPN）接続を使用して会社のネットワークに接続していないことを確認してください。

ステップ 3 プロンプトが表示されたら、ユーザ名とパスワードを入力してアクセス ポイントにログインします。

ステップ 4 [OfficeExtend Access Point Welcome] ページで、[Enter] をクリックします。 OfficeExtend アクセス ポイントの [Home] ページが表示されます。

ステップ 5 [Configuration] を選択して、[Configuration] ページを開きます。

ステップ 6 [SSID] テキスト ボックスに、このアクセス ポイントに割り当てる個人の SSID を入力します。 この SSID は、ローカルにスイッチされます。

（注） OfficeExtend アクセス ポイントを持つコントローラは、接続されたアクセス ポイントあたり 15 までの WLAN にのみ公開します。これは、個人の SSID ごとに WLAN を 1 つ確保するためです。

ステップ 7 [Security] ドロップダウン リストから [Open]、[WPA2/PSK (AES)]、または [104 bit WEP] を選択して、このアクセス ポイントが使用するセキュリティ タイプを設定します。

（注） [WPA2/PSK (AES)] を選択する場合は、クライアントに WPA2/PSK および AES 暗号化が設定されていることを確認してください。

ステップ 8 ステップ *8* で [WPA2/PSK (AES)] を選択した場合は、[Secret] テキスト ボックスに 8 ～ 38 文字の WPA2 パスフレーズを入力します。 104 ビット WEP を選択した場合、[Key] テキスト ボックスに 13 文字の ASCII キーを入力します。

ステップ 9 [Apply] をクリックします。

（注） 他のアプリケーションで OfficeExtend アクセス ポイントを使用する場合は、[Clear Config] をクリックしてこの設定をクリアし、アクセス ポイントを工場出荷時のデフォルトに戻せます。 コントローラ CLI から **clear ap config***Cisco_AP* コマンドを入力してアクセス ポイントの設定をクリアすることもできます。

これらの手順は、OfficeExtend アクセス ポイントの個人 SSID の設定のみに使用できます。 OEAP 600 AP の個人 SSID の設定については、『Aironet 600 Series OfficeExtend Access Point Configuration Guide』を参照してください。

OfficeExtend アクセス ポイント統計情報の表示

次の CLI コマンドを使用して、ネットワーク上の OfficeExtend アクセス ポイントの情報を表示します。

- 次のコマンドを入力して、すべての OfficeExtend アクセス ポイントのリストを表示します。

  show flexconnect office-extend summary

- 次のコマンドを入力して、OfficeExtend アクセス ポイントのリンク遅延を表示します。

  show flexconnect office-extend latency

- 次のコマンドを入力して、すべてのアクセス ポイントまたは特定のアクセス ポイントの暗号化状態を表示します。

  show ap link-encryption {**all** | *Cisco_AP*}

  このコマンドにより、整合性チェックのエラー数を追跡する認証エラー、およびアクセス ポイントが同じパケットを受信する回数を追跡する再送エラーも表示されます。 次のコマンドを入力して、すべてのアクセス ポイントまたは特定のアクセス ポイントのデータ プレーン ステータスを表示します。

  show ap data-plane {**all** | *Cisco_AP*}

OfficeExtend アクセス ポイントの音声メトリックの表示

次のコマンドを使用して、ネットワークの OfficeExtend アクセス ポイントの音声メトリックに関する情報を表示します。

show ap stats 802.11{a | b}*Cisco_AP*

以下に類似した情報が表示されます。

```
OEAP WMM Stats :
  Best Effort:
    Tx Frame Count............................. 0
    Tx Failed Frame Count...................... 0
    Tx Expired Count........................... 0
    Tx Overflow Count.......................... 0
    Tx Queue Count............................. 0
    Tx Queue Max Count......................... 0
    Rx Frame Count............................. 0
    Rx Failed Frame Count...................... 0
  Background:
    Tx Frame Count............................. 0
    Tx Failed Frame Count...................... 0
    Tx Expired Count........................... 0
    Tx Overflow Count......................... 0
    Tx Queue Count............................. 0
    Tx Queue Max Count..... 0
    Rx Frame Count............................. 0
    Rx Failed Frame Count...................... 0
  Video:
    Tx Frame Count............................. 0
    Tx Failed Frame Count...................... 0
    Tx Expired Count........................... 0
    Tx Overflow Count..... 0
    Tx Queue Count............................. 0
    Tx Queue Max Count..... 0
    Rx Frame Count............................. 0
    Rx Failed Frame Count...................... 0
  Voice:
    Tx Frame Count............................. 0
    Tx Failed Frame Count...................... 0
    Tx Expired Count..... 0
    Tx Overflow Count..... 0
    Tx Queue Count..... 0
    Tx Queue Max Count..... 0
    Rx Frame Count..... 0
    Rx Failed Frame Count..... 0
```

次のように WLC GUI を使用してネットワーク内の OfficeExtend アクセス ポイントの音質メトリックを表示します:

- [Wireless] > [Access Points] > [Radios] > [802.11a/n/ac] または [802.11b/g/n] の順に選択します。[802.11a/n/ac Radios] ページまたは [802.11b/g/n Radios] ページが表示されます。
- 目的のアクセス ポイントの青いドロップダウン矢印の上にカーソルを置いて [Detail] リンクをクリックし、[Radio > Statistics] ページを開きます。

  このページには、このアクセス ポイントの OEAP WMM カウンタが表示されます。

連続したネットワーク診断

ネットワーク診断の実行に関する情報

ネットワーク診断は、オンデマンドでスピード テストを実行することによって、システムの非 DTLS スループットを測定します。 ネットワーク診断により、主な障害の根本的な原因を解決することができます。 また、オンデマンドまたは定期的にテストを実行することによって、リンクの遅延およびジッターを測定します。

ネットワーク診断の実行（GUI）

ステップ 1 [WAN] > [Network Diagnostics] を選択します。
[Network Diagnostics] ページが表示されます。

ステップ 2 [Start Diagnostics] をクリックします。
診断ページが表示されます。

コントローラでのネットワーク診断の実行

ステップ 1 [Wireless] > [All APs] > [Details] の順に選択します。

ステップ 2 [Network Diagnostics] タブを選択します。
[Network Diagnostics] ページが表示されます。

ステップ 3 [Start Network Diagnostics] をクリックします。
診断ページが表示されます。

連続したネットワーク診断（CLI）

- ネットワーク診断を実行するには、Cisco WLC で次のコマンドを入力します。
  show ap network-diagnostics*Ap_Name*