Aironet 600シリーズOfficeExtendアクセスポイントの設定

内容

はじめに

このドキュメントでは、Cisco Aironet 600® シリーズ OfficeExtend アクセス ポイント（OEAP）とともに使用する Cisco Wireless LAN（WLAN; ワイヤレス LAN）コントローラを設定する際の要件について説明します。Cisco Aironet 600 シリーズ OEAP はスプリット モード操作をサポートしており、WLAN コントローラでの設定が必要な機能と、エンド ユーザがローカルで設定できる機能が組み込まれています。このドキュメントでは、適切な接続とサポートされている機能セットに必要な設定についても説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は Cisco Aironet 600 シリーズ OfficeExtend アクセス ポイント（OEAP）に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

表記法の詳細については、『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。

背景説明

設定ガイドライン

- Cisco Aironet 600シリーズOEAPは、Cisco 5508、WiSM-2、およびCisco 2504のコントローラでサポートされます。
- Cisco Aironet 600 シリーズ OEAP に対応しているコントローラの最初のリリースは 7.0.116.0 です。
- コントローラの管理インターフェイスがルーティング可能な IP ネットワーク上に存在している必要があります。
- UDP ポート番号 5246 および 5247 でトラフィックを許可するように、会社のファイアウォールの設定を変更する必要があります。

Office Extend ソリューション概要

- 会社のコントローラの IP アドレスを使用してプライミングされている Access Point（AP; アクセス ポイント）がユーザに提供されるか、またはユーザが設定画面（HTML 設定ページ）でコントローラの IP アドレスを入力できます。
- ユーザが AP をホーム ルータに接続します。
- AP がホーム ルータから IP アドレスを取得し、プライミングされているコントローラに接続し、セキュア トンネルを確立します。
- 次に Cisco Aironet 600 シリーズ OEAP が会社の SSID をアドバタイズします。これにより、会社と同じセキュリティ方式とサービスが WAN を介してユーザの自宅でも利用できるよ

うになります。

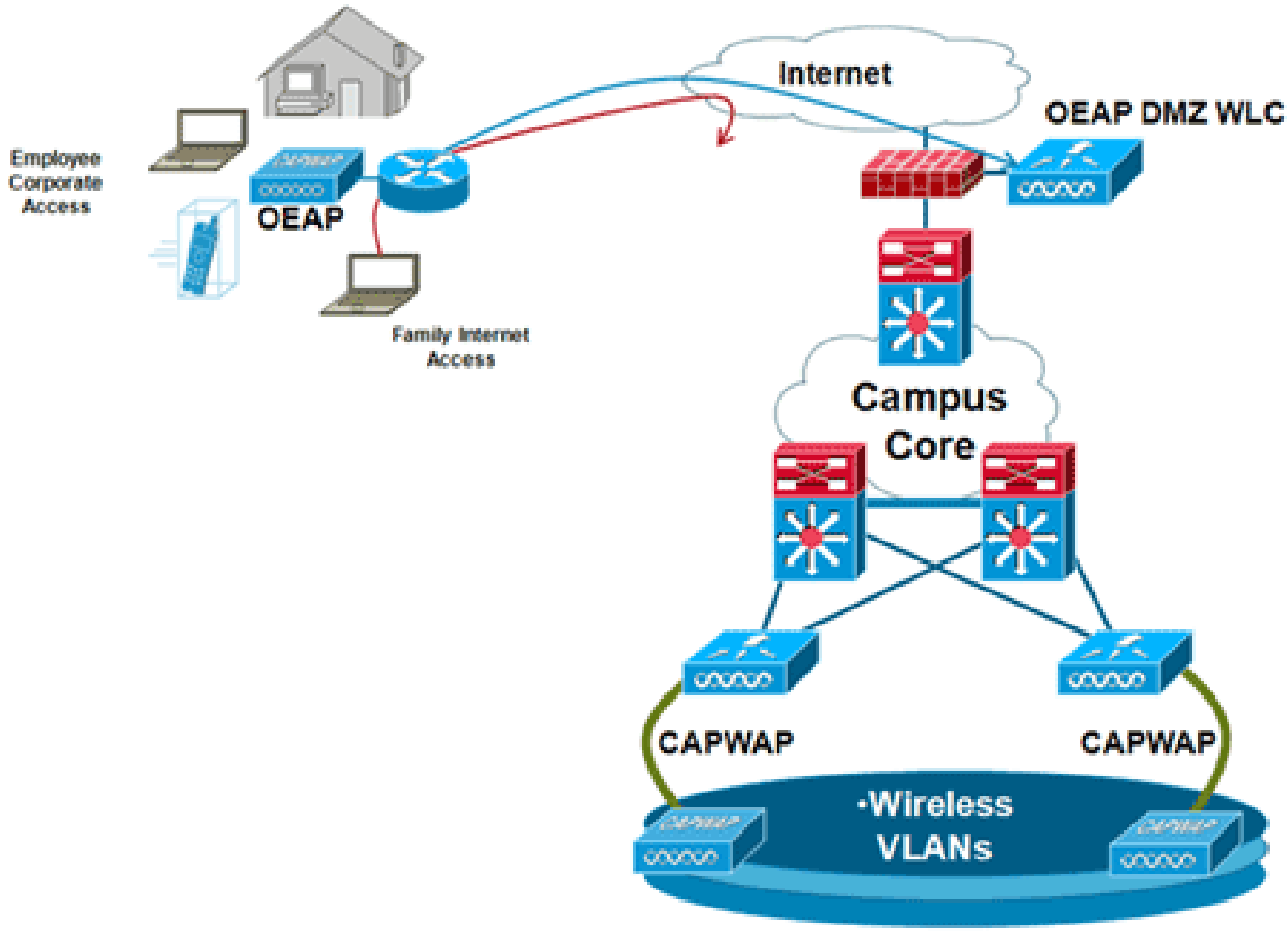
- リモート LAN を設定している場合は、AP の 1 つの有線ポートからコントローラへトンネルが確立されます。
- これで、ユーザが個人で使用するローカル SSID を有効にできます。

ファイアウォール設定ガイドライン

ファイアウォールの一般設定では、ファイアウォール経由での CAPWAP 制御および CAPWAP 管理ポート番号が許可されます。Cisco Aironet 600 シリーズ OEAP コントローラは DMZ ゾーンに設置できます。

注：WLANコントローラとCisco Aironet 600シリーズOEAPの間にあるファイアウォールでUDPポート5246および5247が開いている必要があります。

次の図に、DMZ における Cisco Aironet 600 シリーズ OEAP コントローラを示します。



ファイアウォール設定の例を次に示します。

```
interface Ethernet0/0
 nameif outside
```

```
 security-level 0
 ip address X.X.X.X 255.255.255.224

!--- X.X.X.X represents a public IP address

!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 172.16.1.2 255.255.255.0
!
access-list Outside extended permit udp any host X.X.X.Y eq 5246

!--- Public reachable IP of corporate controller

access-list Outside extended permit udp any host X.X.X.Y eq 5247

!--- Public reachable IP of corporate controller

access-list Outside extended permit icmp any any
!
global (outside) 1 interface
nat (dmz) 1 172.16.1.0 255.255.255.0
static (dmz,outside) X.X.X.Y 172.16.1.25 netmask 255.255.255.255
access-group Outside in interface outside
```

内部 AP マネージャの IP アドレスを CAPWAPP Discovery Response パケットの一部として OfficeExtend AP に送信するため、コントローラの管理者は AP マネージャ インターフェイスで NAT が有効になっており、正常な NAT により変換された IP アドレスが AP に送信されることを確認する必要があります。

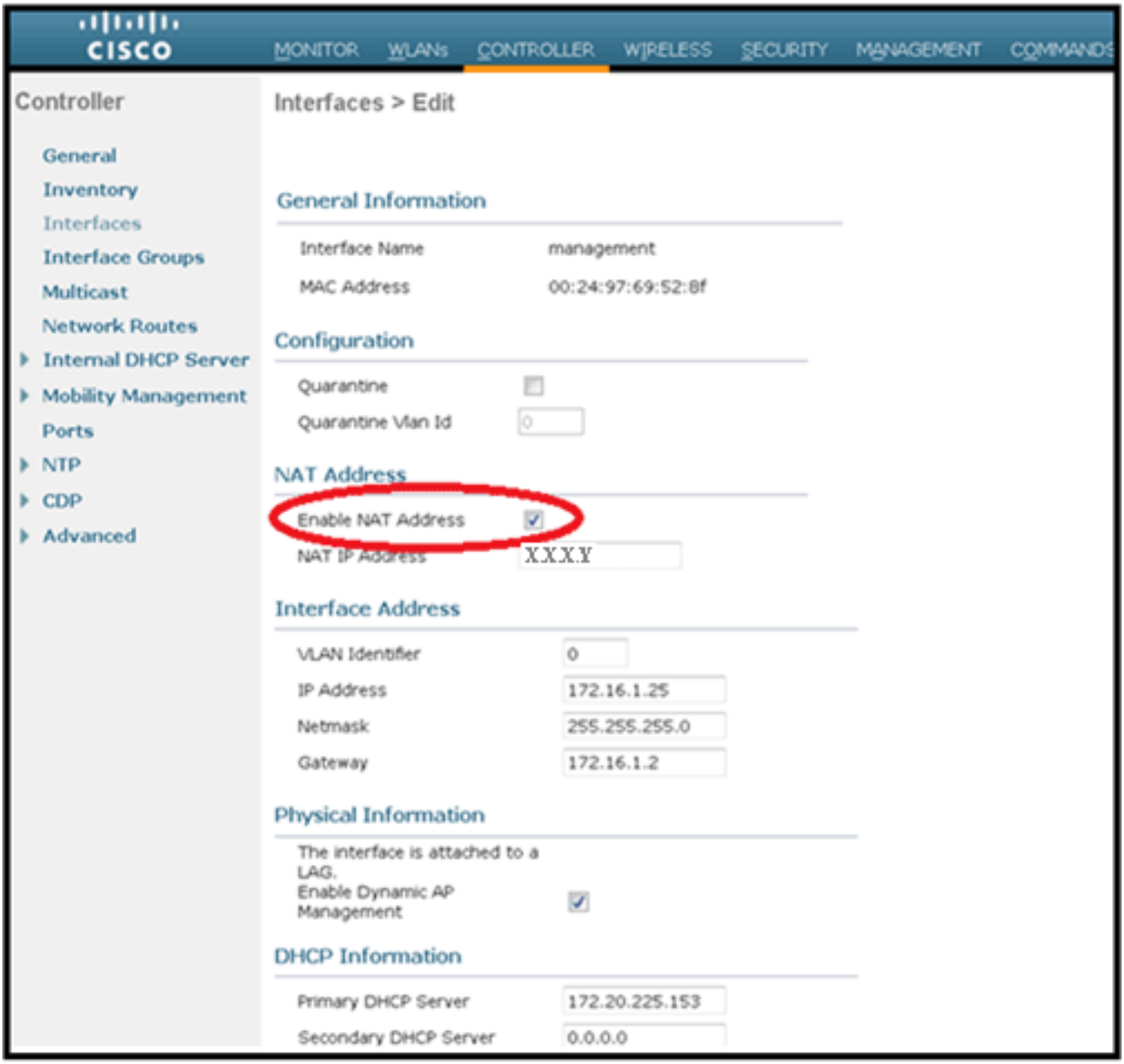
注：デフォルトでは、WLCは、NATが有効な場合にAPディスカバリ中にのみNAT IPアドレスで応答します。AP が NAT ゲートウェイの内部と外部に存在する場合、このコマンドを発行して WLC を NAT IP アドレスと非 NAT（内部）管理 IP アドレスで応答するように設定します。

<#root>

config network ap-discovery nat-ip-only disable

注：これは、WLCにNAT IPアドレスが設定されている場合にのみ必要です。

次の図に、WLC に NAT IP アドレスが設定されていることを前提として、NAT を有効にする方法を示します。



注：この設定は、インターネットでルーティング可能なIPアドレスが設定されていて、ファイアウォールの背後に設定されていない限り、コントローラでは必要ありません。

Office Extend AP-600 設定手順

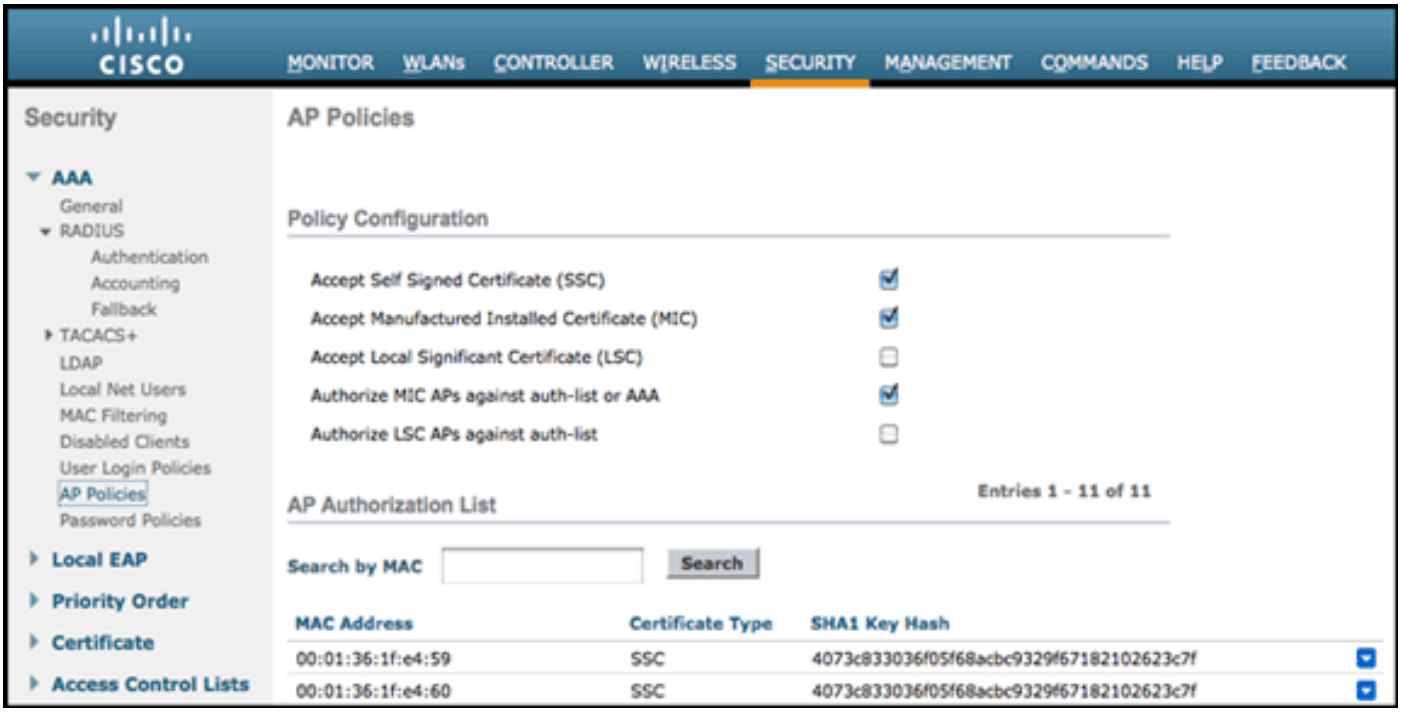
Cisco Aironet 600 シリーズ OEAP は、ローカル モード アクセス ポイントとして WLC に接続します。

注：モニタモード、H-REAPモード、スニファモード、不正検出モード、ブリッジモード、およびSE接続モードは600シリーズではサポートされておらず、設定できません。

注：1040、1130、1140、および3502iシリーズアクセスポイントでCisco Aironet 600シリーズOEAP機能を使用するには、APをHybrid REAP(H-REAP)用に設定し、APのサブモードをCisco Aironet 600シリーズOEAPに設定する必要があります。600 シリーズはローカル モードを使用し

、変更できないため、600 シリーズではこの設定を行うことはできません。

許可されていない Cisco Aironet 600 シリーズ OEAP 装置がコントローラに接続できないようにするため、初期接続プロセスで AP 認証に MAC フィルタリングを使用できます。次の図に、MAC フィルタリングを有効にし、AP セキュリティ ポリシーを設定する画面を示します。



この画面では（Radio MAC アドレスではなく）イーサネット MAC を入力します。MAC アドレスを Radius サーバに入力するときには必ず小文字を使用してください。イーサネット MAC アドレスの検出方法については、AP イベント ログで確認できます（詳しくは後述します）。

WLAN およびリモート LAN 設定

Cisco Aironet 600 シリーズ OEAP には 1 つの物理リモート LAN ポート（#4 の黄色のポート）が搭載されています。このポートの設定方法は、WLAN によく似ています。このポートはワイヤレスではなく、AP の背面にある有線 LAN ポートであるため、リモート LAN ポートとして管理されます。

このデバイスの物理ポートは 1 つだけですが、ハブやスイッチを使用する場合には最大 4 つの有線クライアントを接続できます。

注：リモートLANクライアントの制限では、スイッチまたはハブを複数のデバイスのリモートLANポートに接続するか、またはそのポートに接続されているCisco IP Phoneに直接接続することがサポートされています。

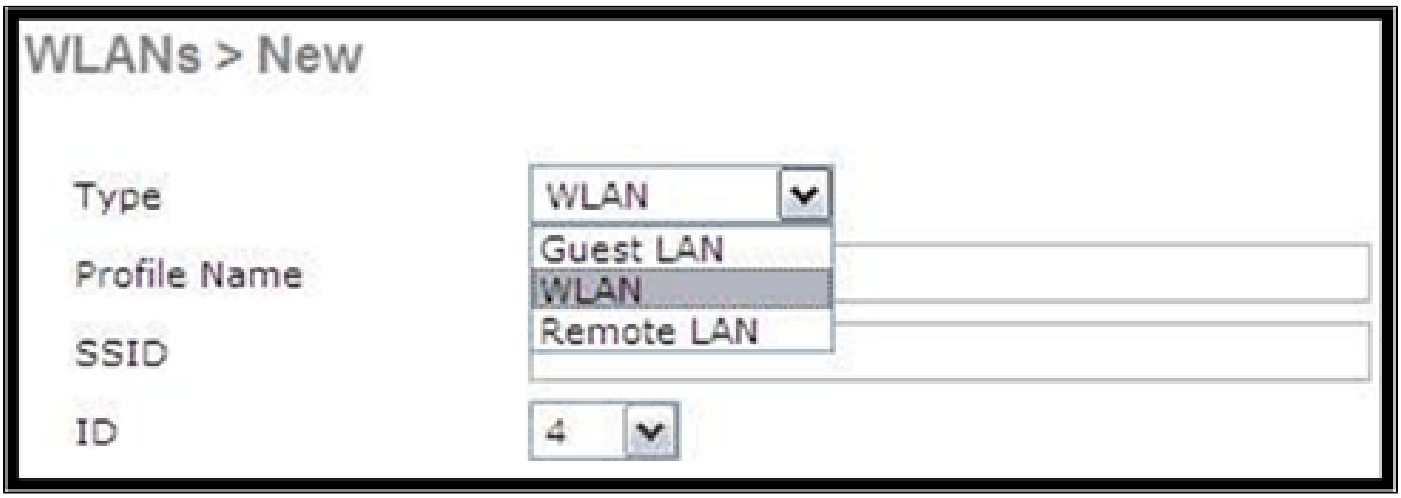
注：デバイスの1つが1分間以上アイドル状態になるまで、最初の4台のデバイスだけが接続できます。802.1x 認証を使用する際には、有線ポートで複数のクライアントを使用しようとすると問題が発生することがあります。

注：この数は、コントローラWLANに課せられている15の制限には影響しません。

リモート LAN は、コントローラで設定されている WLAN およびゲスト LAN と同様の方法で設定できます。

WLAN はワイヤレス セキュリティ プロファイルです。これは、会社のネットワークで使用されるプロファイルです。Cisco Aironet 600 シリーズ OEAP では最大 2 つの WLAN と 1 つの LAN がサポートされています。

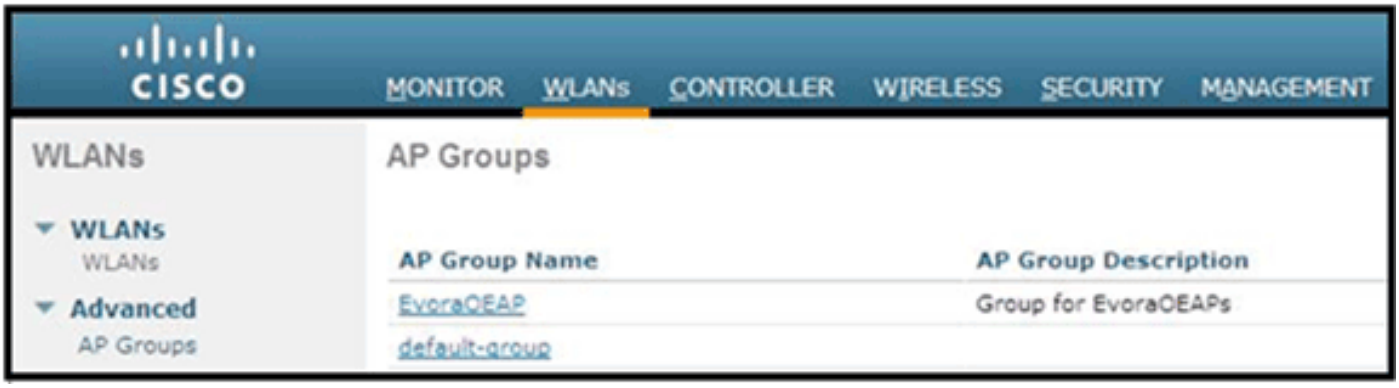
リモート LAN は WLAN に似ていますが、リモート LAN は次の図に示すようにアクセス ポイントの背面の有線ポート（黄色のポート #4）にマップされる点が異なります。



注：複数のWLANまたは複数のリモートLANがある場合は、すべてのWLANをAPグループに配置する必要があります。

次の図に、WLAN とリモート LAN を設定する画面を示します。

次の図に、OEAP グループ名の例を示します。



次の図に、WLAN SSID と RLAN の設定を示します。

Cisco Aironet 600 シリーズ OEAP を AP グループに含める場合、同じ制限（2 つの WLAN と 1 つのリモート LAN）が AP グループの設定にも適用されます。Cisco Aironet 600 シリーズ OEAP がデフォルト グループに含まれている場合、つまり定義される AP グループには含まれない場合は、WLAN/リモート LAN ID を 8 よりも小さい ID に設定する必要があります。これは、Cisco Aironet 600 シリーズ OEAP では 8 以上の ID 設定はサポートされていないためです。

次の図に示すように、ID を 8 未満に設定してください。

注：Cisco Aironet 600シリーズOEAPで使用されているWLANまたはリモートLANを変更するために追加の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を無効にしてください。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。

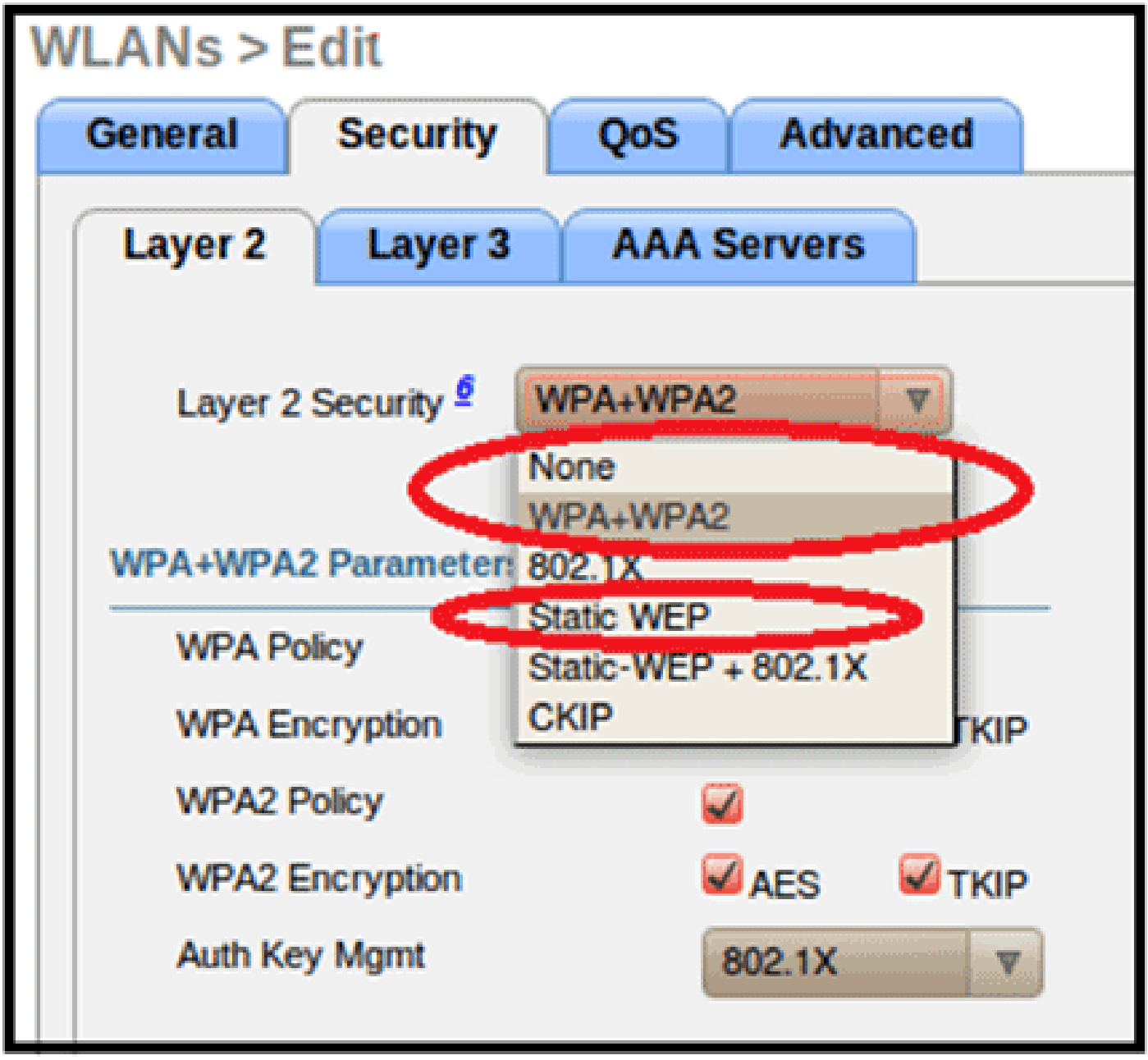
AP グループで 3 つ以上の WLAN が有効にされている場合は、すべての WLAN を無効にしてから 2 つの WLAN のみを有効にしてください。

WLAN セキュリティ設定

WLAN のセキュリティ設定では、600 シリーズではサポートされていない特定の機能があります。

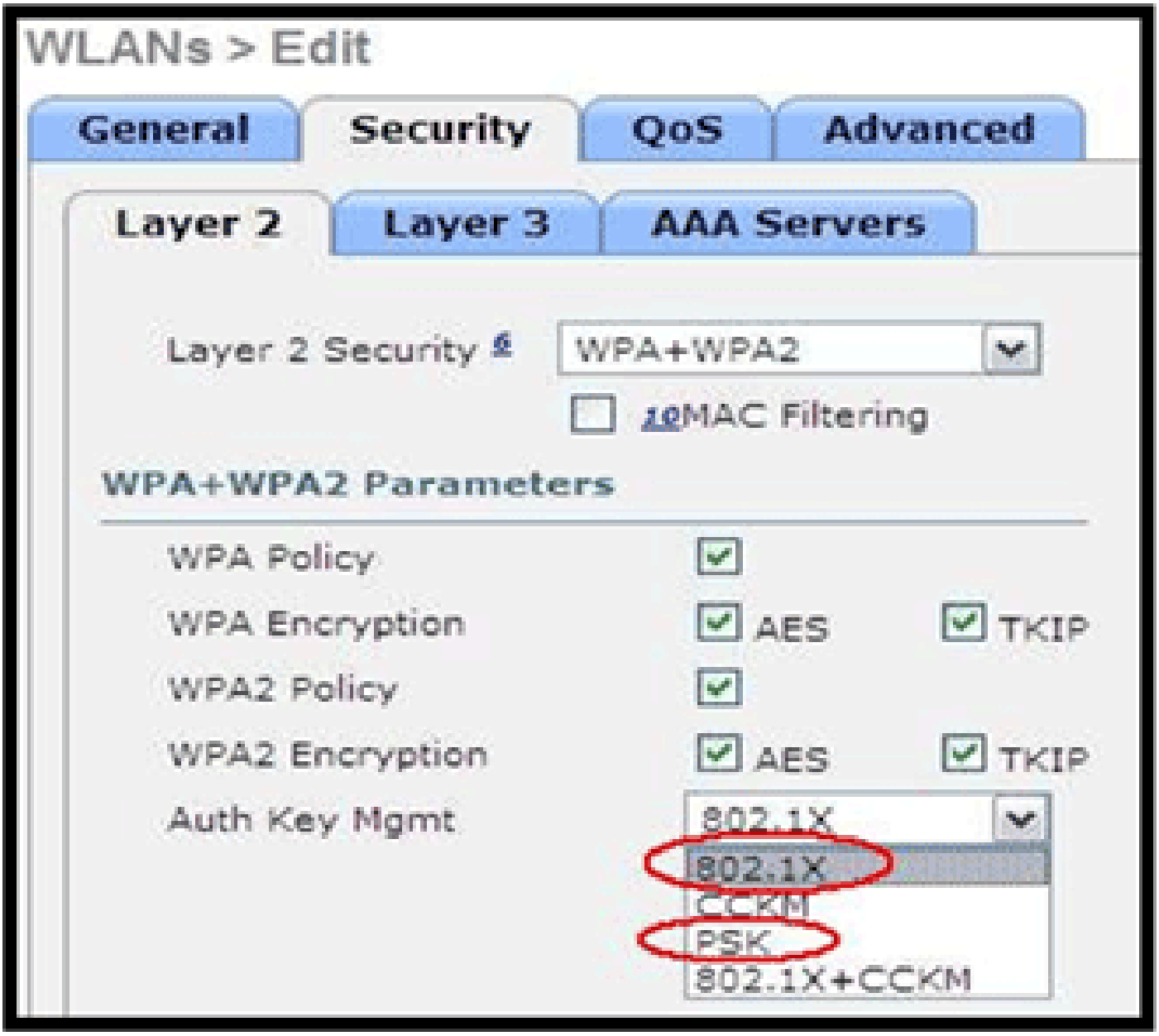
Cisco Aironet 600 シリーズ OEAP でサポートされているレイヤ 2 セキュリティのオプションは次のとおりです。

- なし
- [WPA+WPA2]
- [Static WEP] も使用できますが、.11n データ レートには使用できません。

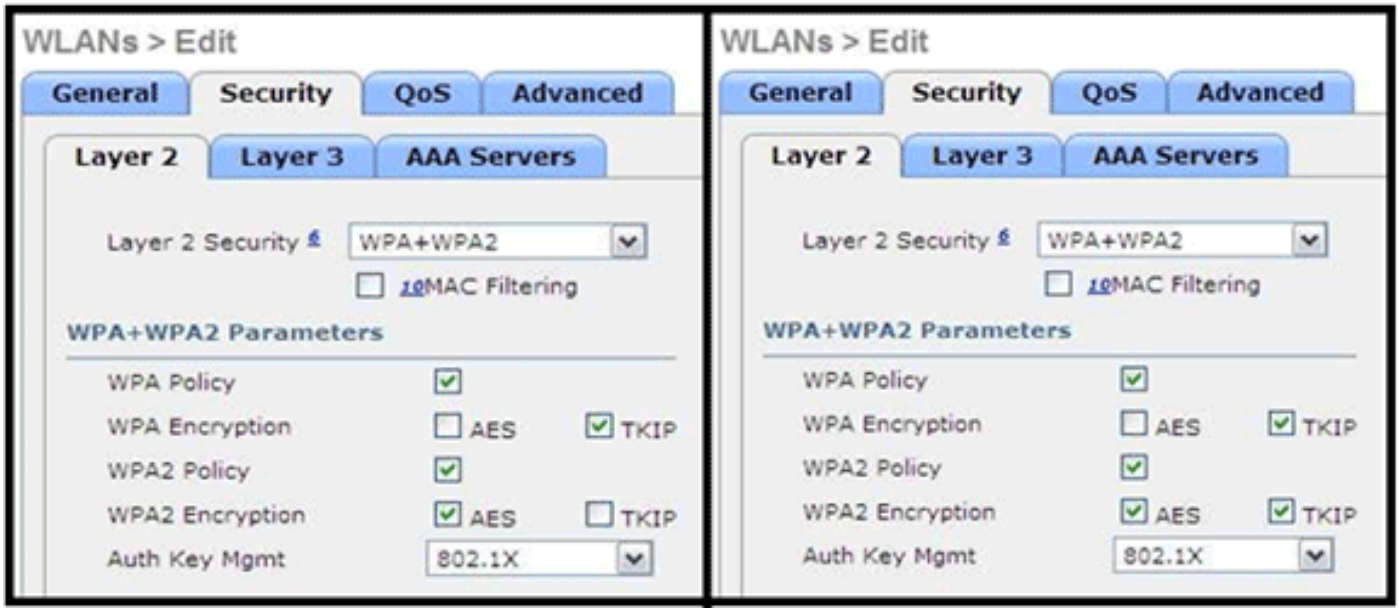


注：802.1xまたはPSKのみを選択してください。

次の図に示すように、WPA と WPA2 のセキュリティ暗号化設定では、TKIP と AES の設定を同じにする必要があります。

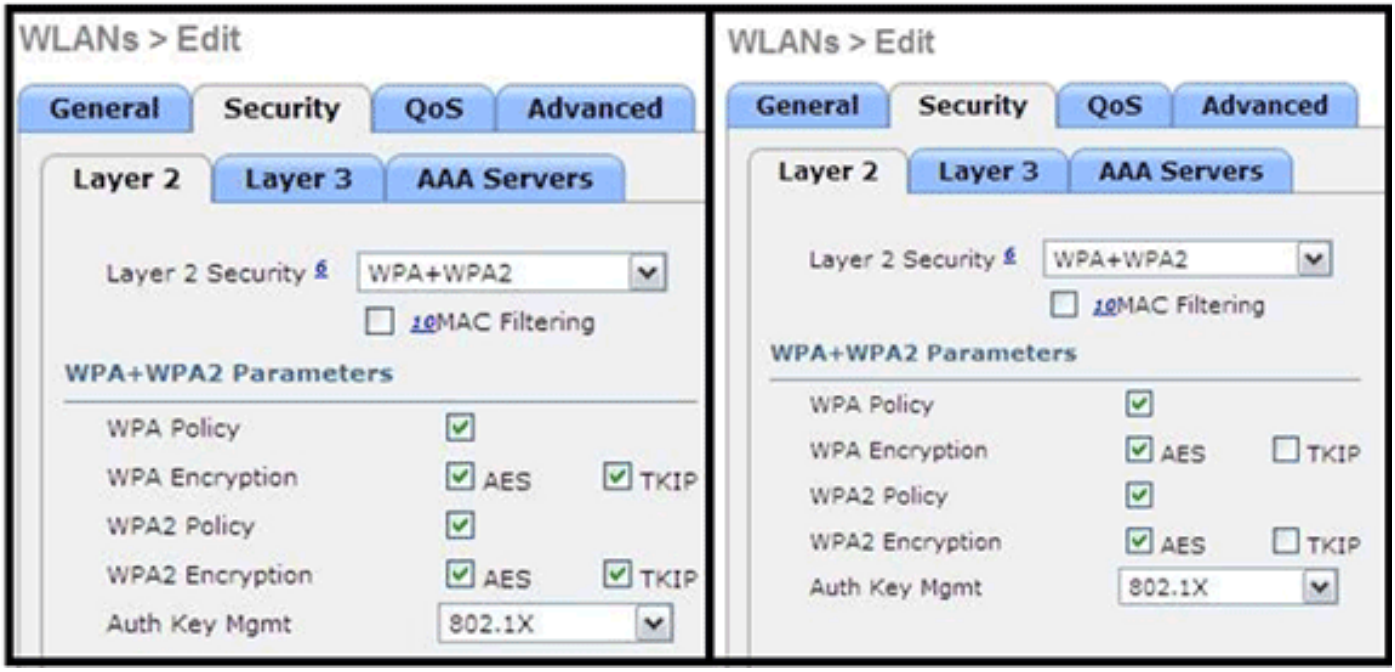


TKIP と AES の誤った設定の例を次の図に示します。



注：セキュリティ設定では、サポートされていない機能が許可されることに注意してください。

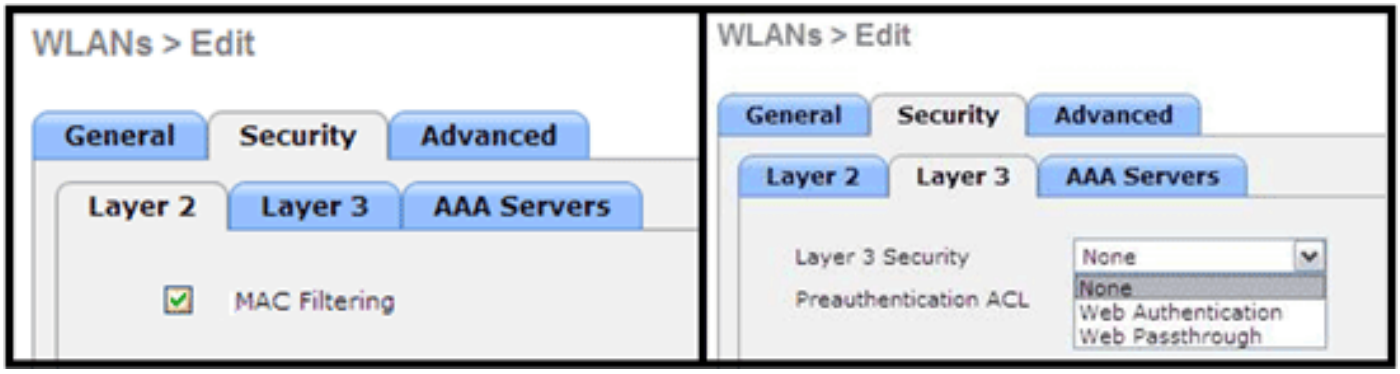
適切な設定の例を次の図に示します。



MAC フィルタリング

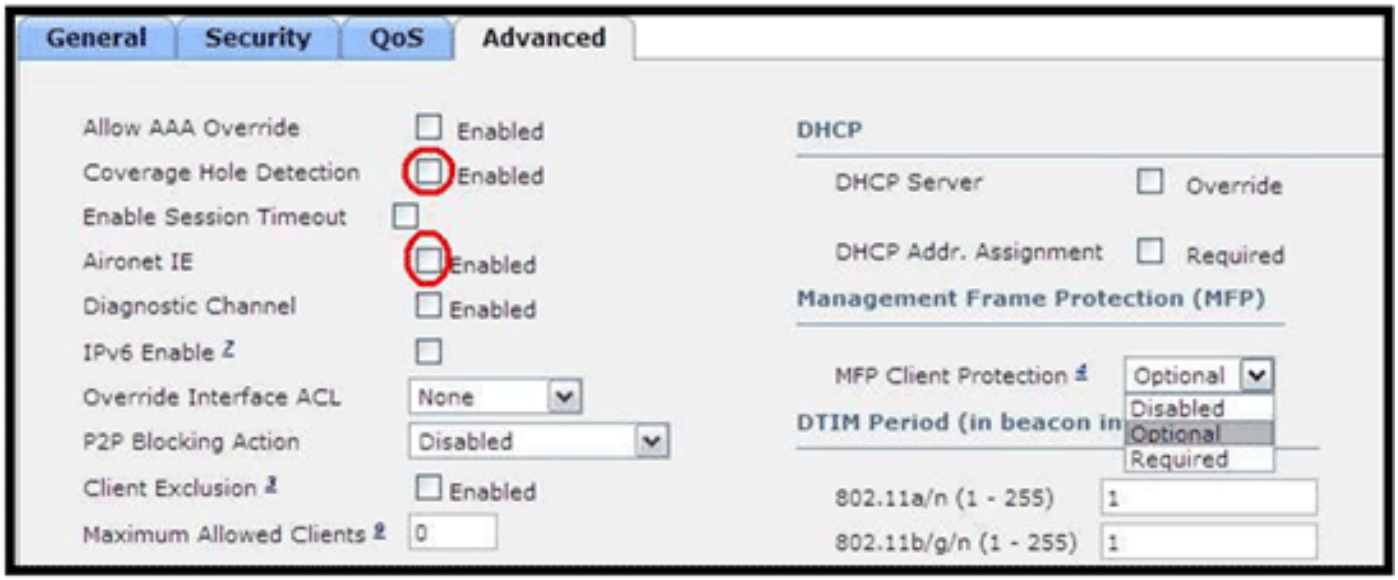
[Security] 設定を開いたままにし、MAC フィルタリングまたは Web 認証を設定することができます。デフォルトでは MAC フィルタリングが使用されます。

次の図に、[Layer 2] と [Layer 3] の MAC フィルタリングの設定を示します。



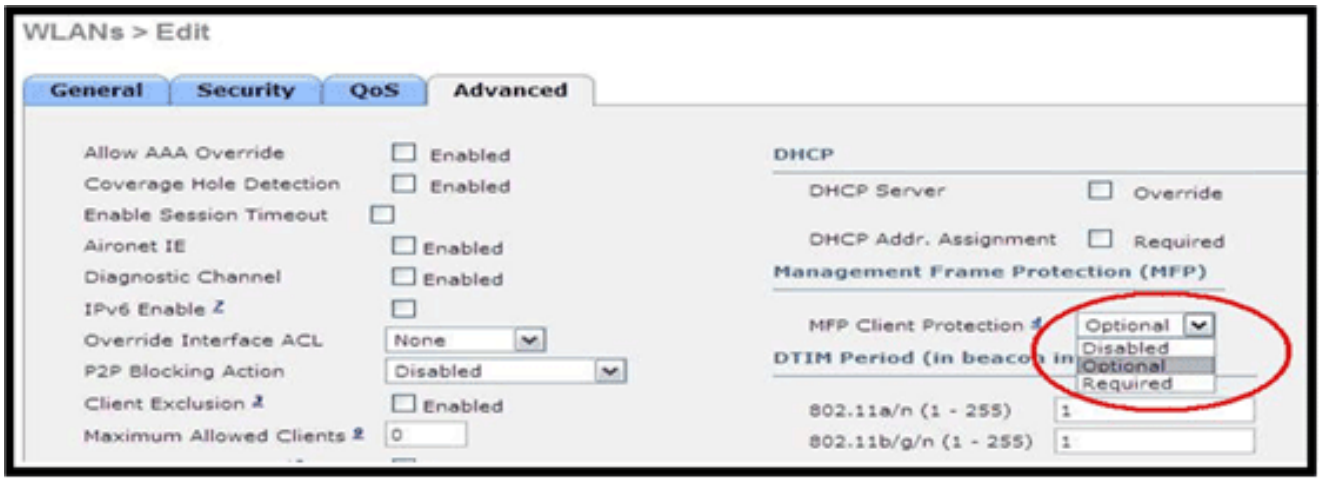
QoS 設定を管理します。

拡張設定も管理します。

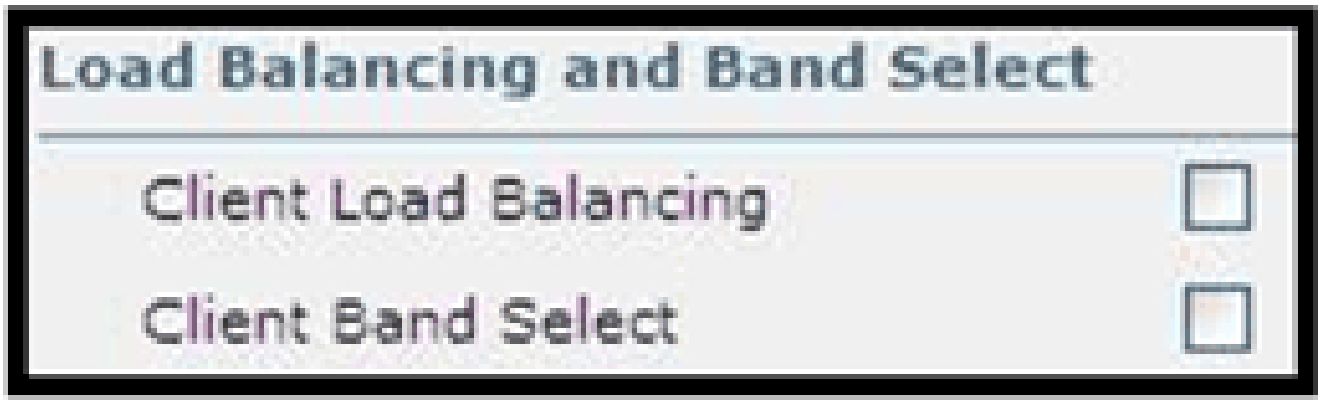


注：

- [Coverage Hole Detection] を有効にしないでください。
- [Aironet IE] (IE; Information Elements) は使用されないので、有効にしないでください。
- [Management Frame Protection (MFP)] もサポートされていないので、無効にするかまたは次の図に示すように [Optional] に設定してください。



- [Client Load Balancing] と [Client Band Select] はサポートされていないので、有効にしないでください。



サポートされるユーザ数

600 シリーズで WLAN コントローラを介して WLAN に同時接続できるユーザの最大数は 15 です。最初に接続したクライアントのいずれか 1 つが認証を解除するかまたはコントローラでタイムアウトが発生するまでは、16 番目のユーザは認証できません。

注：この数は、600シリーズのコントローラWLAN全体での累積数です。

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 シリーズではもう 1 つの WLAN にユーザが接続することができません。エンドユーザが 600 シリーズで設定する個人使用のローカル プライベート WLAN にはこの制限は適用されません。またこれらのプライベート WLAN または有線ポートに接続しているクライアントは、この制限に影響しません。

チャネル管理および設定

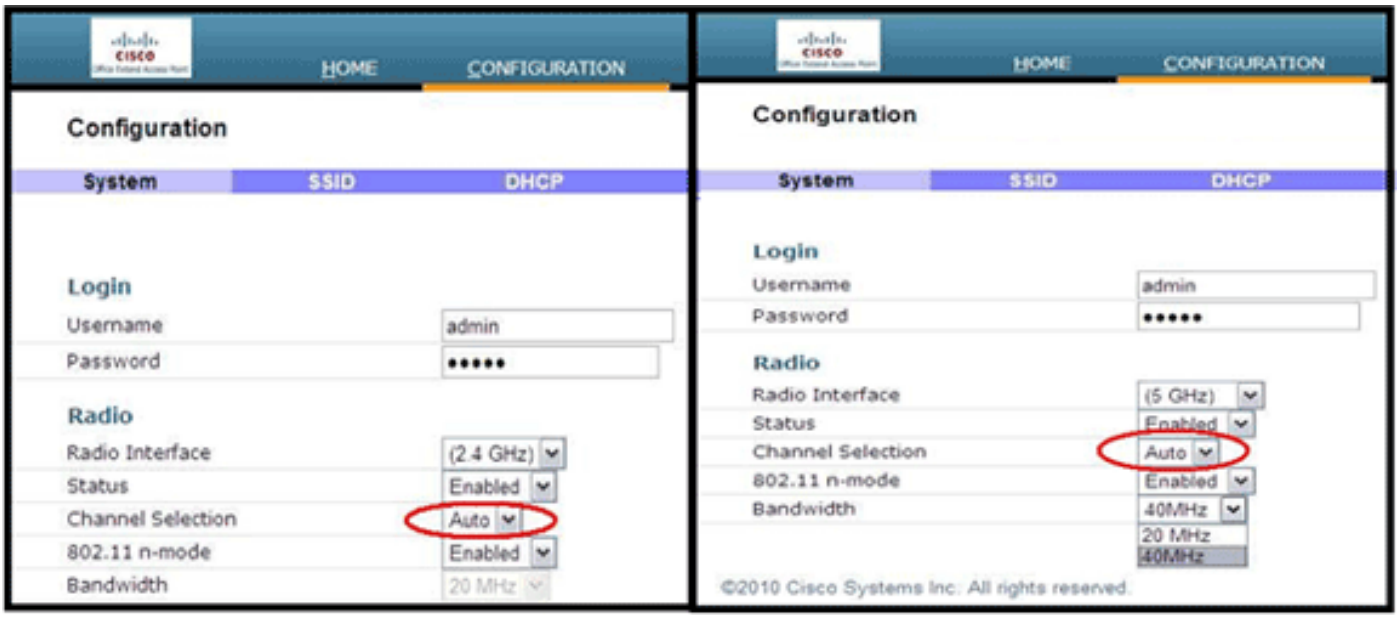
600 シリーズの無線は、ワイヤレス LAN コントローラではなく、600 シリーズのローカル GUI で管理されます。

スペクトラム チャネルと電力の管理や無線の無効化をコントローラから実行しても、600 シリーズには反映されません。

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 5.0 GHz のチャネルを選択します。

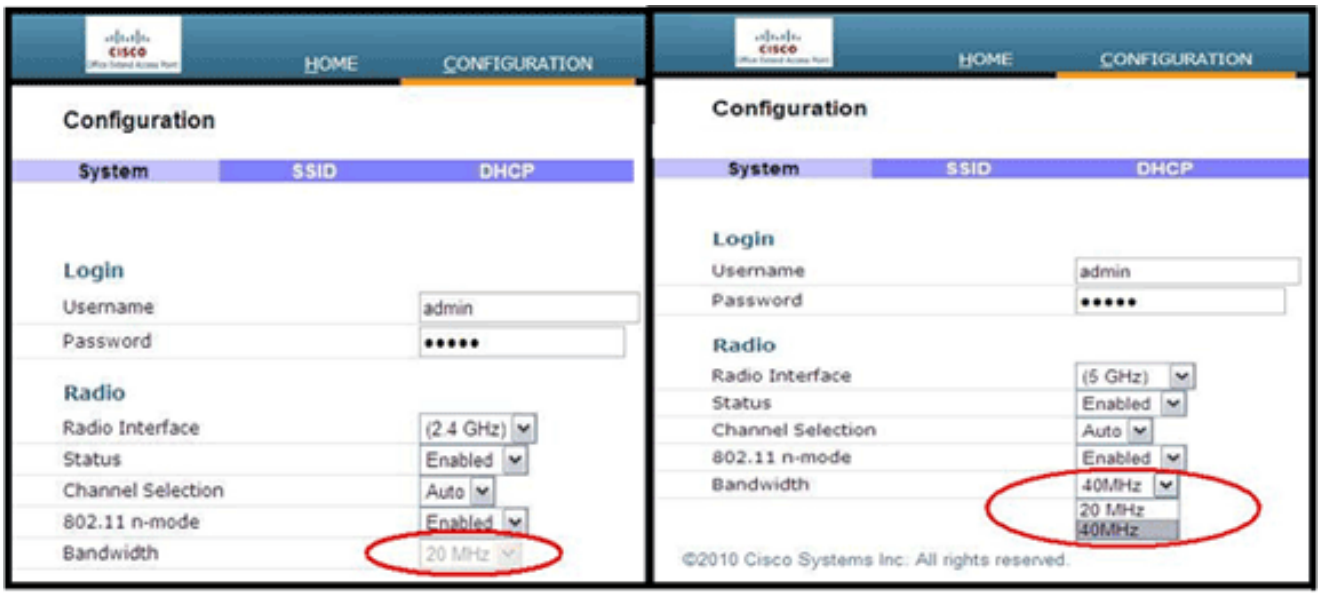
注：ユーザが一方または両方の無線をローカルで無効にする（その無線も社内アクセスに対して無効にする）と、前述したように、RRMと、モニタ、H-REAP、スニファなどの高度な機能は、自宅やテレワーカーが使用する場所に配置されたCisco Aironet 600シリーズOEAPの機能では利用できません。

5.0 GHz のチャネル選択と帯域幅は、Cisco Aironet 600 シリーズ OEAP のローカル GUI の次の画面で設定します。



注：

- 5 GHz に対して設定可能な帯域幅は 20 MHz と 40 MHz です。
- 2.4 GHz では帯域幅 40 MHz はサポートされておらず、20 MHz で固定されています。
- 2.4 GHz では帯域幅 40 MHz（チャネル ボンディング）はサポートされていません。



追加の警告

Cisco Aironet 600 シリーズ OEAP はシングル AP 展開向けに設計されています。したがって、600 シリーズ間でのクライアント ローミングはサポートされていません。

注：コントローラで802.11a/nまたは802.11b/g/nを無効にしても、ローカルSSIDが機能している可能性があるため、Cisco Aironet 600シリーズOEAPではこれらのスペクトルは無効にならない場合があります。

Cisco Aironet 600 シリーズ OEAP ではエンド ユーザが無線を有効または無効にできます。

有線ポートでの 802.1x のサポート

この初期リリースでは、802.1x は Command Line Interface (CLI; コマンド ライン インターフェイス) でのみサポートされています。

注：GUIサポートはまだ追加されていません。

これは Cisco Aironet 600 シリーズ OEAP の背面にある有線ポート (黄色のポート #4) であり、リモート LAN に関連付けられています (前述のリモート LAN の設定に関するセクションを参照)。

任意の時点で show コマンドを使用して現在のリモート LAN 設定を表示できます。

<#root>

show remote-lan <*remote-lan-id*>

リモート LAN 設定を変更するには、最初にこのリモート LAN 設定を無効にする必要があります。

<#root>

remote-lan disable <*remote-lan-id*>

リモート LAN の 802.1X 認証を有効にします。

<#root>

config remote-lan security 802.1X enable <*remote-lan-id*>

この操作を取り消すには、次のコマンドを使用します。

<#root>

config remote-lan security 802.1X disable <*remote-lan-id*>

リモート LAN の場合、「Encryption」は常に「None」であり、他の値には設定できません（この設定は show remote-lan を実行すると表示されます）。

コントローラのローカル EAP を認証サーバとして使用するには、次のコマンドを使用します。

<#root>

config remote-lan local-auth enable <*profile-name*> <*remote-lan-id*>

profile は、コントローラ GUI（[Security] > [Local EAP]）または CLI（config local-auth ）経由で定義されます。このコマンドの詳細については、コントローラのガイドを参照してください。

この操作を取り消すには、次のコマンドを使用します。

<#root>

config remote-lan local-auth disable <*remote-lan-id*>

外部 AAA 認証サーバを使用する場合は次のコマンドを使用します。

- config remote-lan radius_server auth add/delete <remote-lan-id> <server-id>
- config remote-lan radius_server auth enable/disable <remote-lan-id>

server は、コントローラ GUI（[Security] > [RADIUS] > [Authentication]）または CLI（config radius auth ）経由で設定されます。このコマンドの詳細については、コントローラのガイドを参照してください。

設定が完了したら、リモート LAN を有効にします。

<#root>

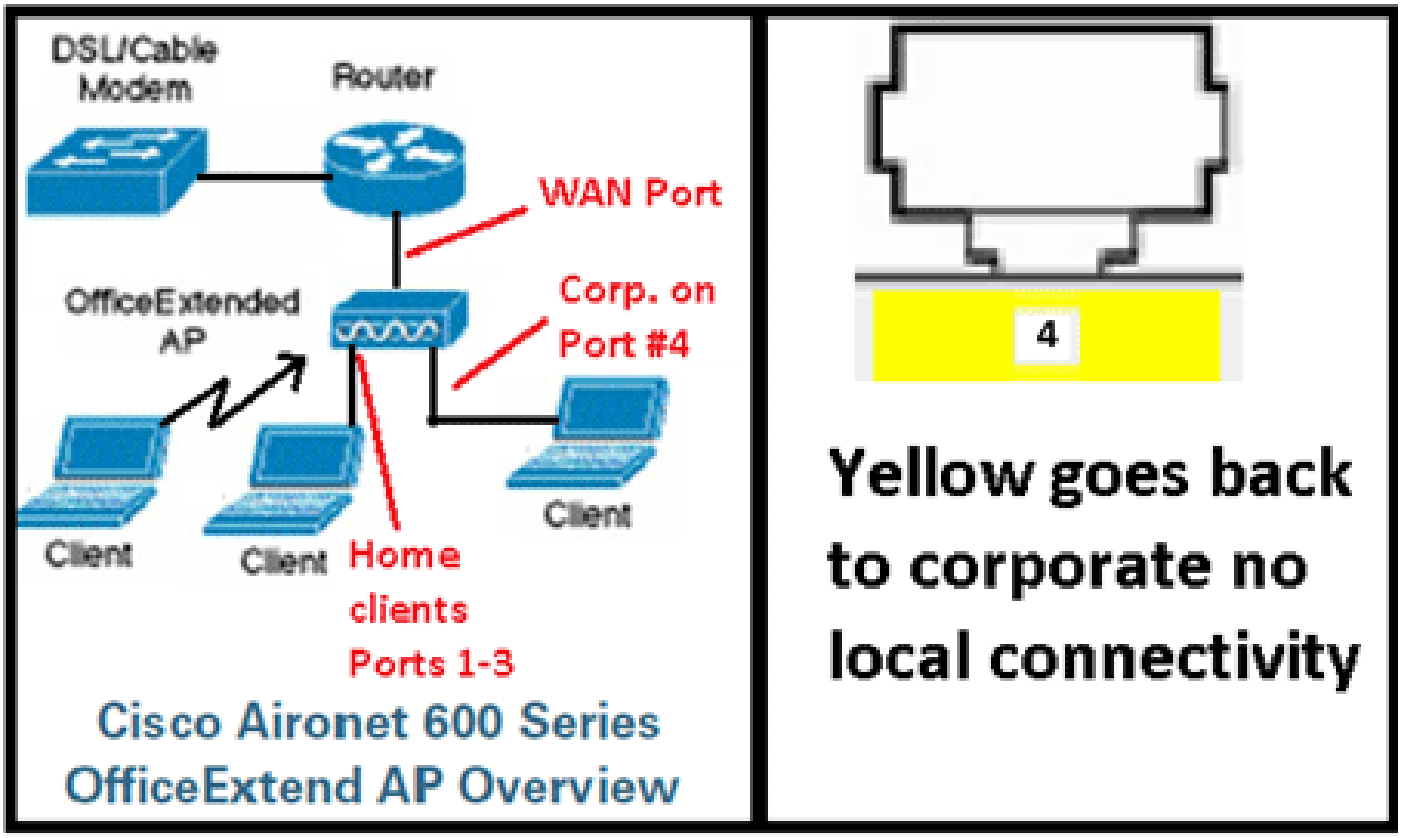
config remote-lan enable <*remote-lan-id*>

show remote-lan <remote-lan-id> コマンドを使用して設定を確認します。

リモート LAN クライアントでは、802.1X 認証を有効にし、これに合わせて設定を行います。デバイスのユーザ ガイドを参照してください。

OEAP-600 アクセス ポイント設定

次の図に、Cisco Aironet 600 シリーズ OEAP の接続配線図を示します。



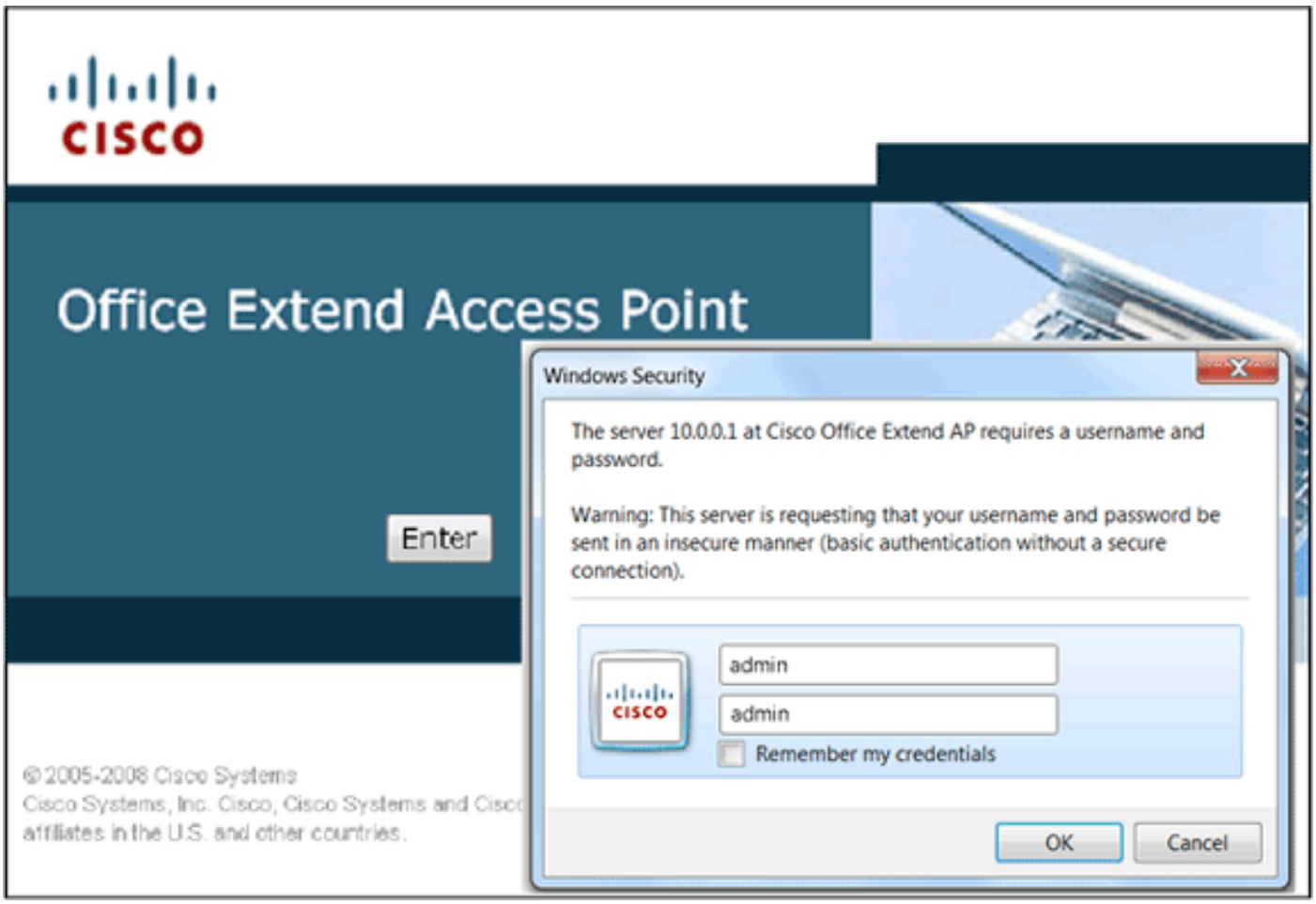
Cisco Aironet 600 シリーズ OEAP のデフォルトの DHCP スコープは 10.0.0.x であるため、アド

レス 10.0.0.1 を使用してポート 1 ~ 3 の AP にアクセスできます。工場出荷時のデフォルトのユーザ名およびパスワードは admin です。

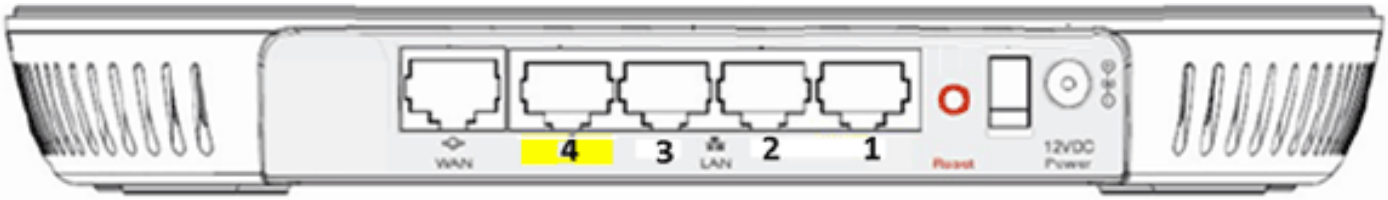
注：これは、ユーザ名およびパスワードとしてCiscoを使用したAP1040、1130、1140、および3502iとは異なります。

無線がオンになっていて、パーソナル SSID がすでに設定されている場合は、設定用画面にワイヤレスでアクセスできます。それ以外の場合は、ローカル イーサネット ポート 1 ~ 3 を使用する必要があります。

デフォルトのログイン ユーザ名とパスワードは admin です。



注：黄色のポート#4は、ローカルでの使用に対してアクティブではありません。コントローラでリモート LAN が設定されている場合、AP がコントローラに接続した後にこのポートがトンネルを確立します。デバイスにアクセスするには、ポート 1 ~ 3 をローカルに使用します。

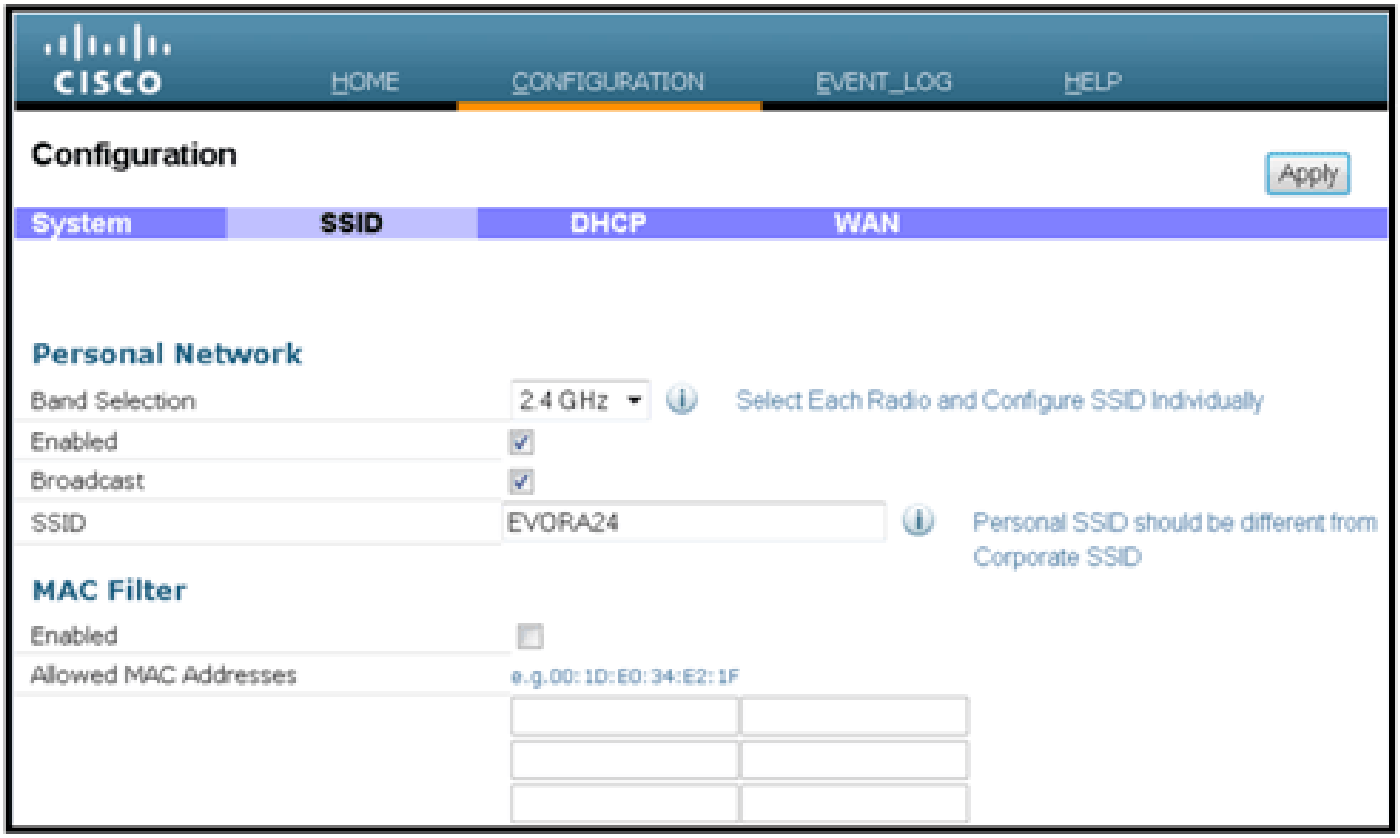


デバイスにアクセスすると、ホーム ステータス画面が表示されます。この画面には無線と MAC の統計が表示されます。無線が設定されていない場合、ユーザは設定画面で無線の有効化、チャ

ネルとモードの設定、ローカル SSID の設定、WLAN 設定の有効化を行うことができます。

SSID 画面ではユーザがパーソナル WLAN ネットワークを設定できます。会社の無線 SSID とセキュリティ パラメータが設定され、（コントローラの IP を使用して WAN を設定した後に）コントローラからプッシュダウンされ、正常に接続します。

次の図に、SSID ローカル MAC フィルタリング設定を示します。



ユーザがパーソナル SSID を設定した後に、以下の画面でプライベート ホーム SSID のセキュリティの設定と無線の有効化を行うことができます。また、必要に応じて MAC フィルタリングを設定できます。パーソナル ネットワークで 802.11n レートを使用する場合は、WPA2-PSK および AES を有効にするパスフレーズ、暗号化タイプ、および認証タイプをユーザが選択することをお勧めします。

注：これらのSSID設定は、ユーザがいずれかまたは両方の無線を無効にすることを選択した場合の企業設定とは異なります（どちらも企業使用に対しても無効になります）。

管理者がデバイスのパスワードの保護や設定をしていない場合には、管理制御設定にローカルにアクセスできるユーザが無線の有効化と無効化などのコア機能を制御できます。したがって、無線を無効にすると、デバイスがコントローラに接続できても接続が失われる可能性があるため、無線を無効にする際には十分に注意する必要があります。

次の図に、システム セキュリティ設定を示します。

Cisco Aironet 600 シリーズ OEAP はホーム ルータとして機能するように設計されていないため、在宅勤務者が Cisco Aironet 600 シリーズ OEAP をホーム ルータの後に設置することが想定されます。これは、本製品の現行バージョンではファイアウォール、PPPoE、ポート フォワーディングがサポートされていないためです。顧客はこれらの機能がホーム ルータに内蔵されているものと想定しています。

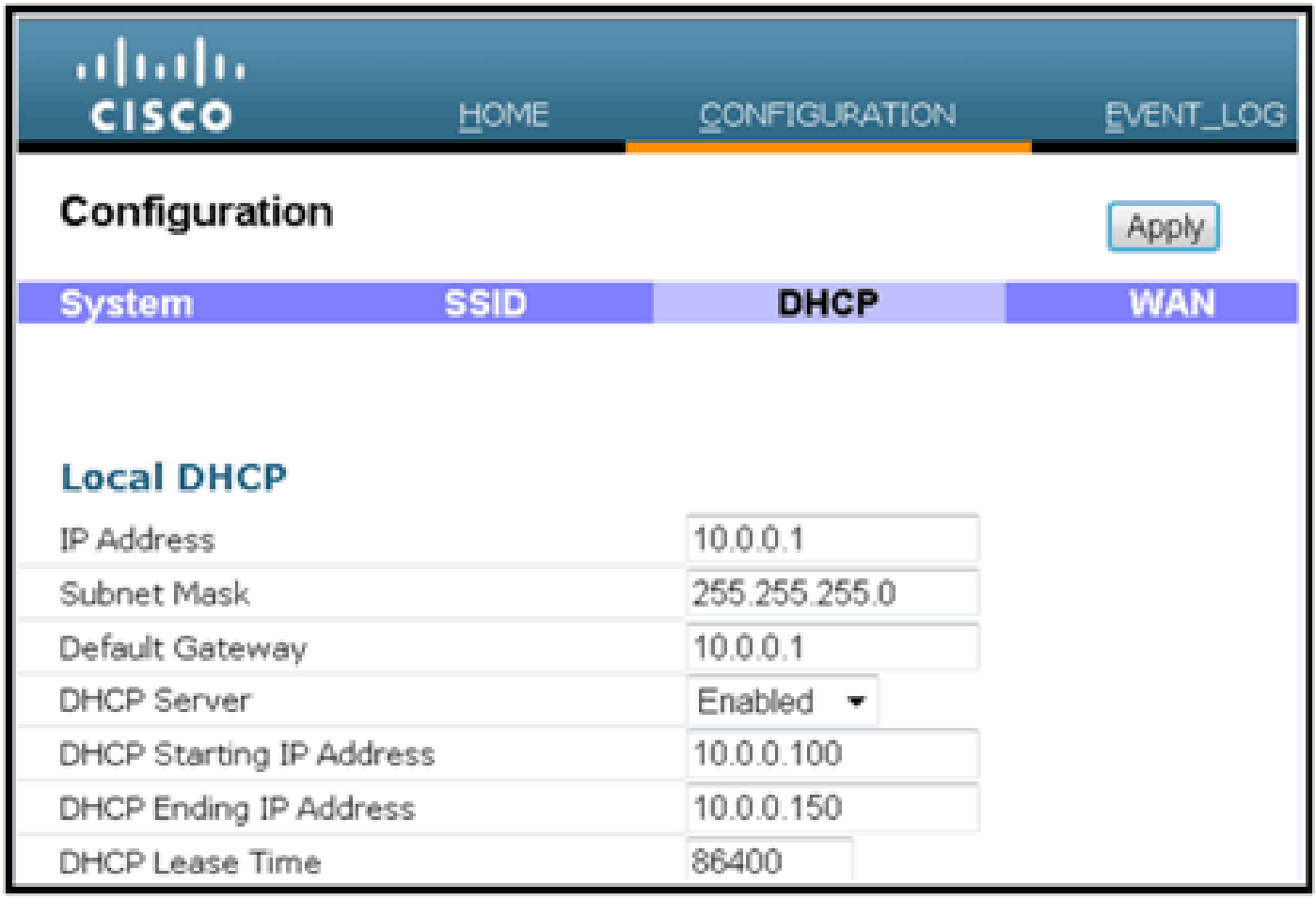
ホーム ルータを接続しなくても本製品は機能しますが、前述の理由からこのように配置しないことをお勧めします。一部のモデムに直接接続する場合に互換性の問題が生じることがあります。

ほとんどのホーム ルータでは DHCP スコープが 192.168.x.x で設定されていることから、このデバイスではデフォルト DHCP スコープは 10.0.0.x であり、DHCP スコープの設定を変更できます。

ホーム ルータでも 10.0.0.x が使用される場合は、ネットワーク競合を防ぐため、192.168.1.x または互換性のある IP アドレスを使用するように Cisco Aironet 600 シリーズ OEAP を設定する必

要があります。

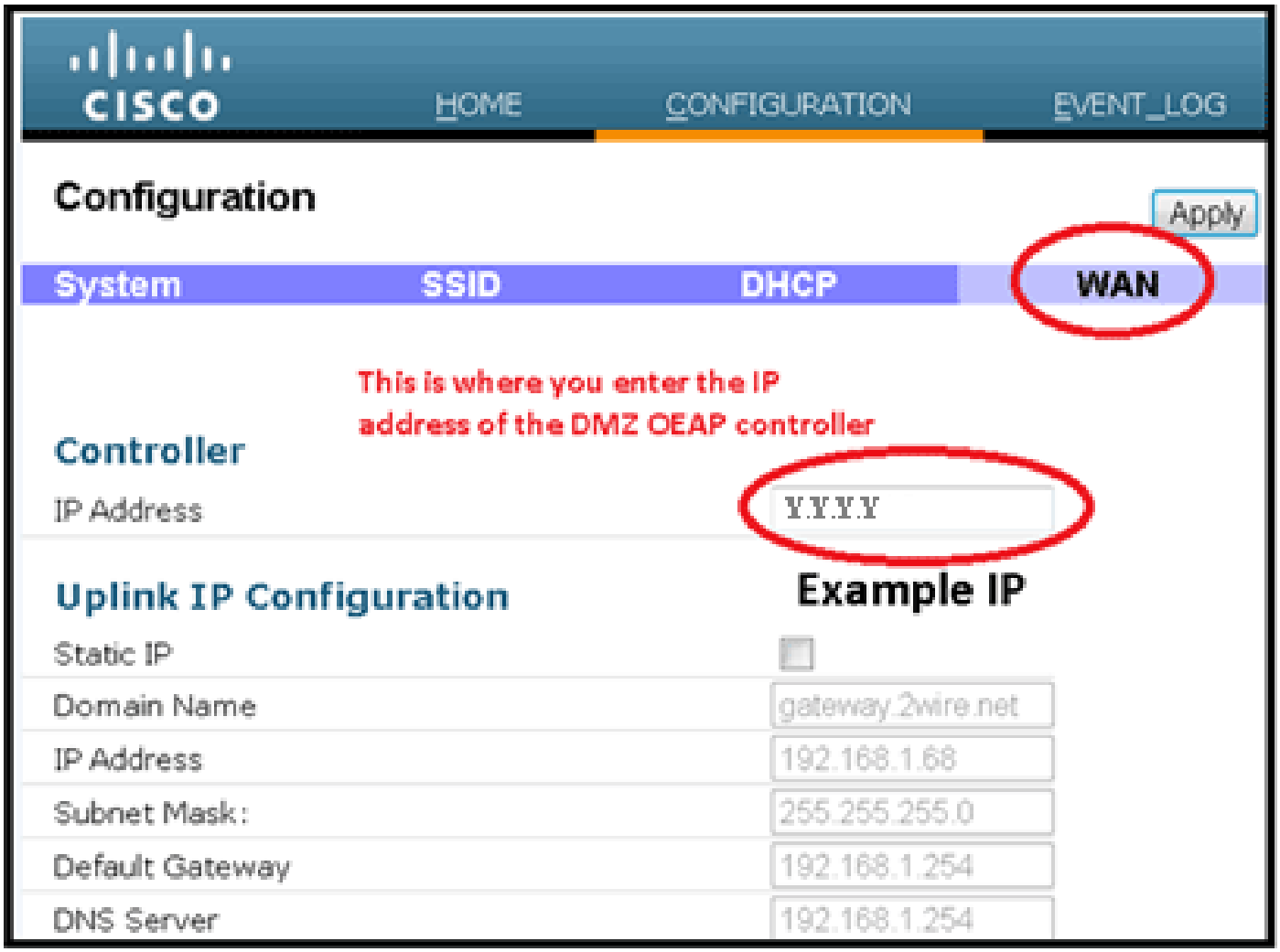
次の図に、DHCP スコープの設定を示します。



注意： IT 管理者が Cisco Aironet 600 シリーズ OEAP をステージングまたは設定していない場合、AP が会社のコントローラに接続できるようにするため、ユーザが会社のコントローラの IP アドレスを入力する必要があります（次の図を参照）。接続後、AP がコントローラから最新のイメージと会社の WAN 設定などのコンフィギュレーション パラメータをダウンロードします。設定されている場合には、Cisco Aironet 600 シリーズ OEAP の背面にある有線ポート #4 のリモート LAN 設定もダウンロードします。

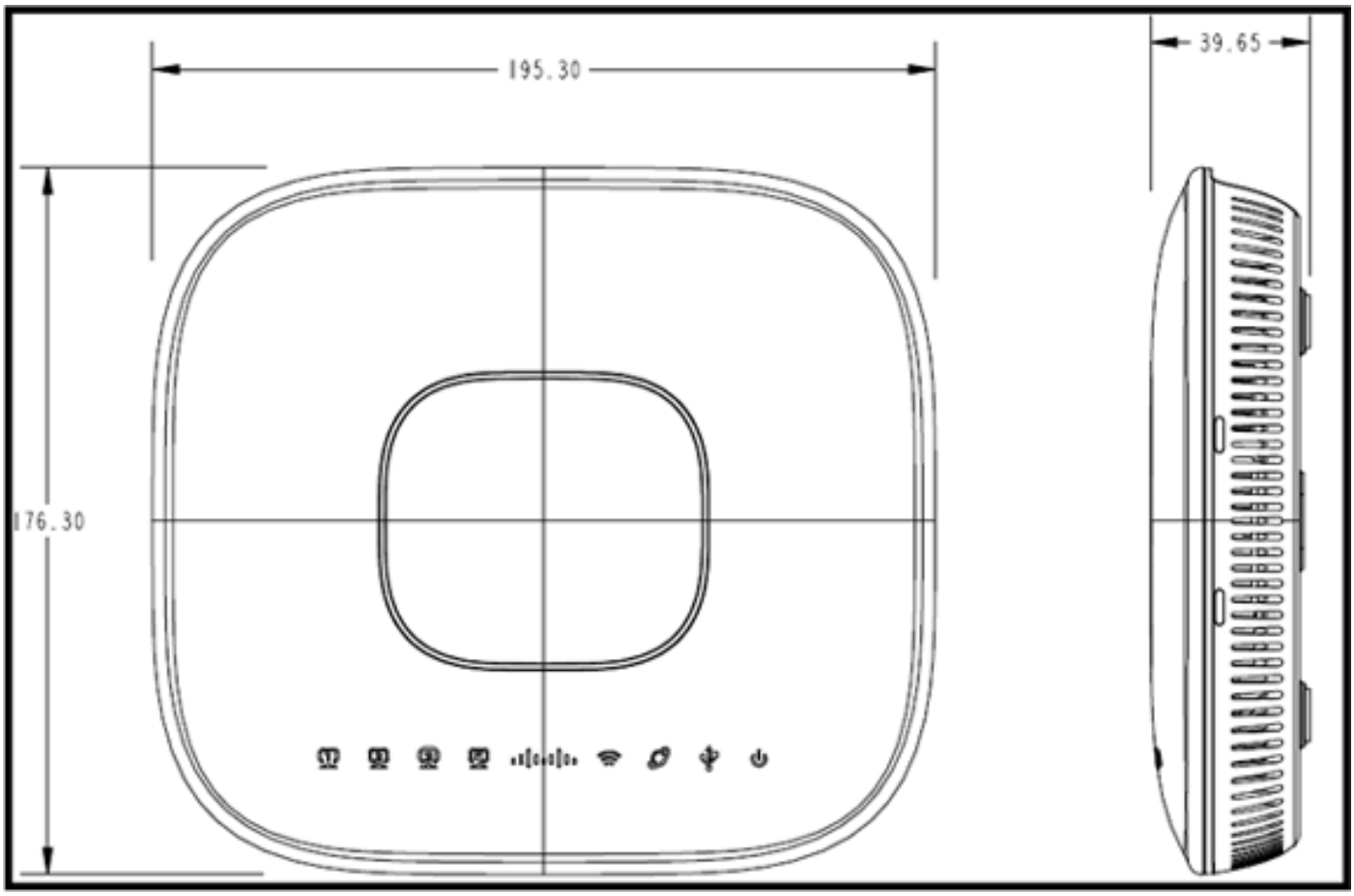
接続しない場合は、コントローラの IP アドレスがインターネット経由で到達可能であるかどうかを確認してください。MAC フィルタリングが有効な場合は、MAC アドレスがコントローラに適切に入力されているかどうかを確認してください。

次の図に、Cisco Aironet 600 シリーズ OEAP コントローラの IP アドレスを示します。



OEAP-600 アクセス ポイント ハードウェアの設置

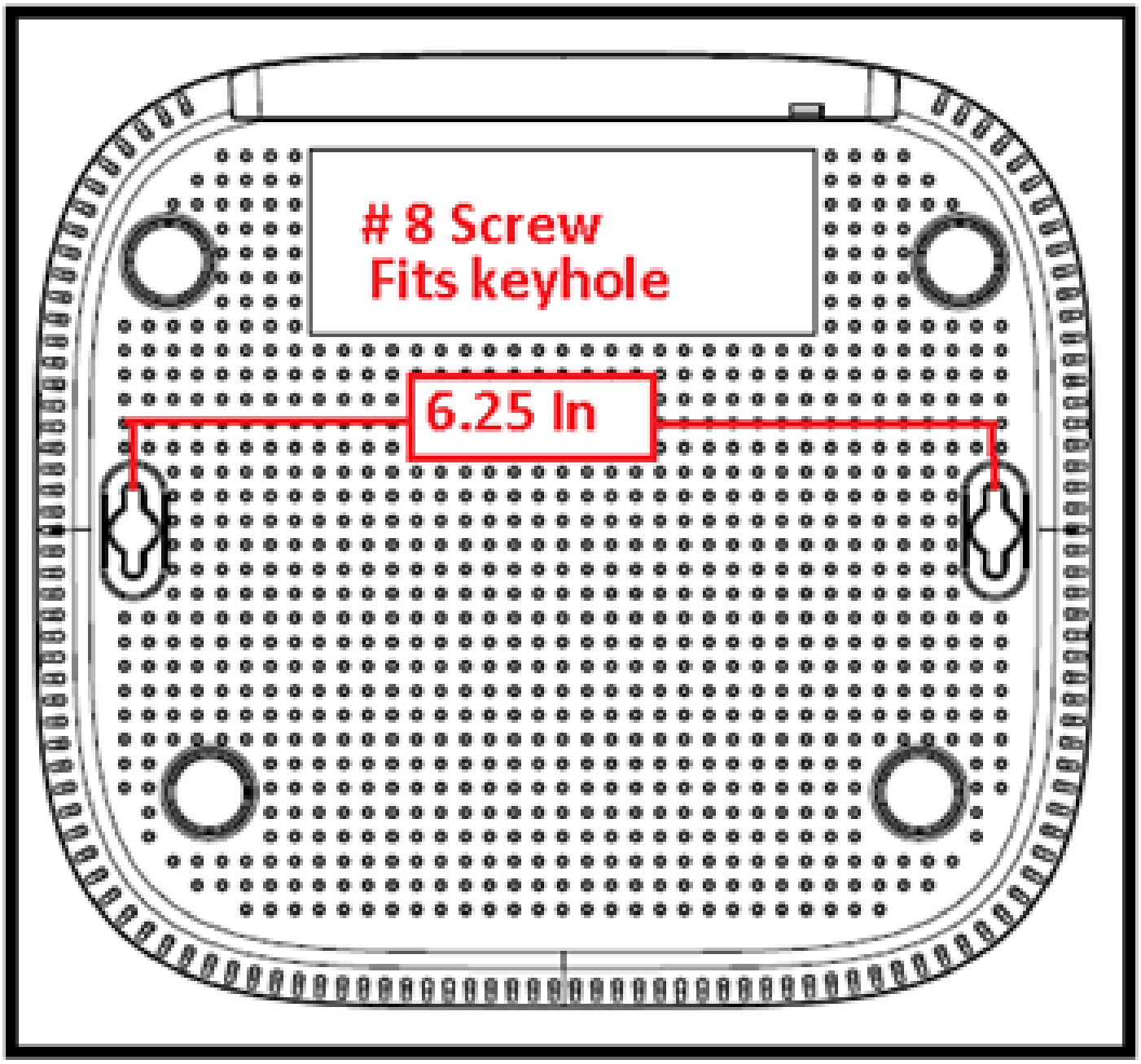
次の図に、Cisco Aironet 600 シリーズ OEAP の外観を示します。



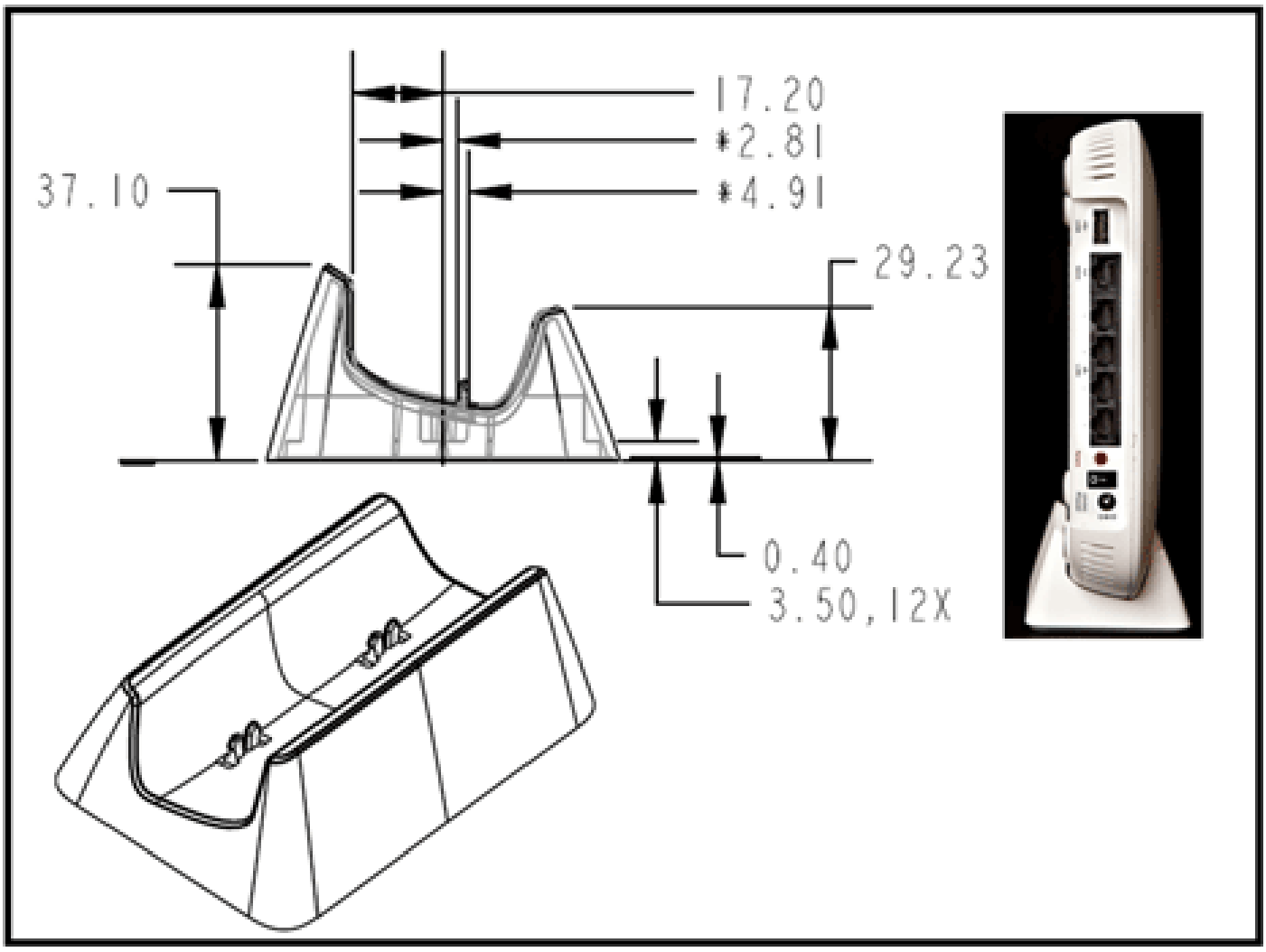
このAPは机の上に置くように設計されており、ゴム製の脚が付いています。壁に取り付けたり、付属のクレードルを使用して縦置きにしたりできます。使用するユーザにできるだけ近い場所にAPを設定してください。大きな金属面のある場所（金属製の机の上や大きな鏡の近く）には設置しないでください。APとユーザの間にある壁や障害物が多いほど信号強度が低くなり、パフォーマンスが低下する可能性があります。

注：このAPは+12ボルトの電源を使用し、Power over Ethernet(PoE)は使用しません。このデバイスにはPoEは組み込まれていません。APに正しい電源アダプタを使用していることを確認してください。ラップトップやIP電話など、他のデバイスのアダプタを使用しないでください。他のデバイスのアダプタを使用すると、APが損傷する恐れがあります。

壁に取り付けるには、プラスチック製のアンカーまたは木製のねじを使用します。



縦置きに設置するには、付属のクレードルを使用します。

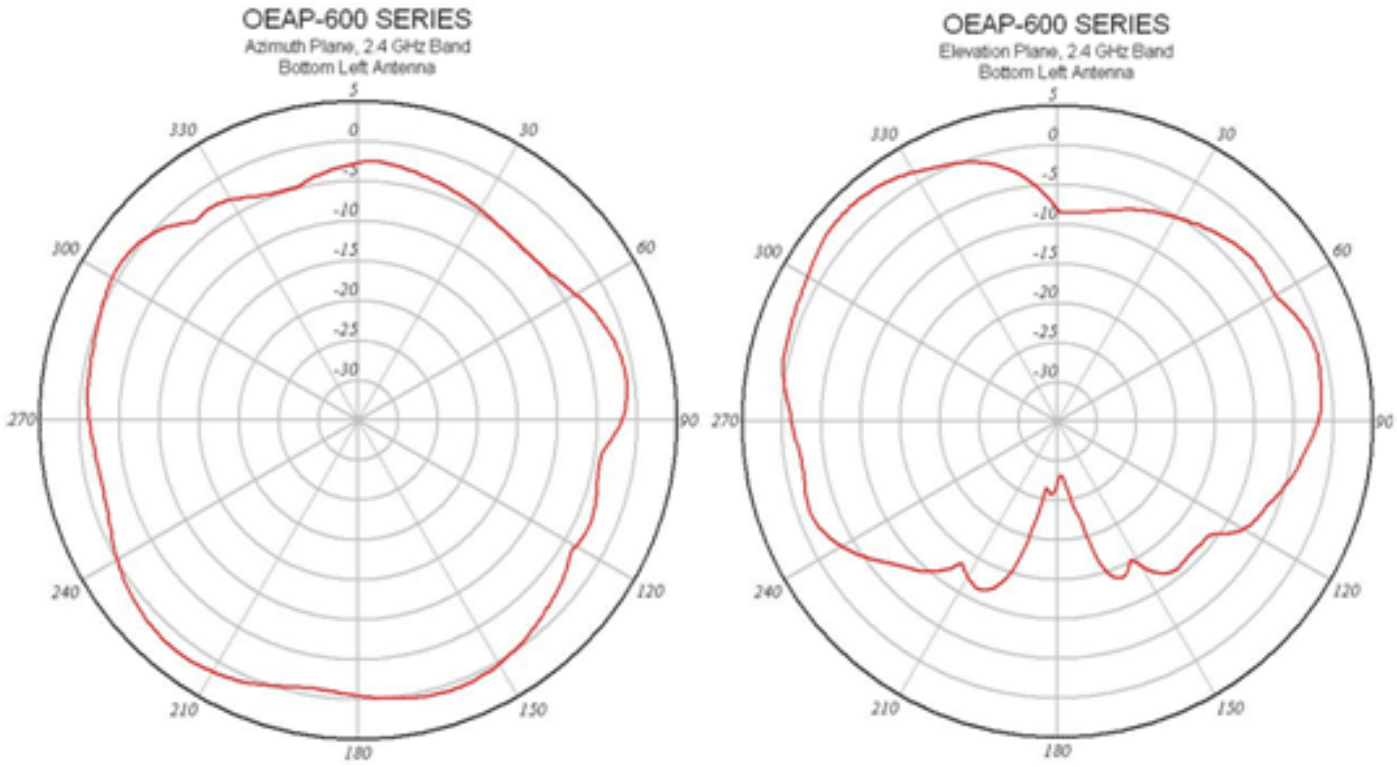


Cisco Aironet 600 シリーズ OEAP のアンテナは、AP の両端に位置しています。金属でできた物体や障害物の近くに AP を設置しないように十分注意してください。このように設置すると、信号に指向性が生じるか、または信号が低下する恐れがあります。アンテナ ゲインは両方の帯域で約 2 dBi であり、360 度パターンで放射するように設計されています。ランプシェードのない電球のように、すべての方向に放射することを目的としています。AP をランプとして考え、ユーザに近い場所に設置してください。

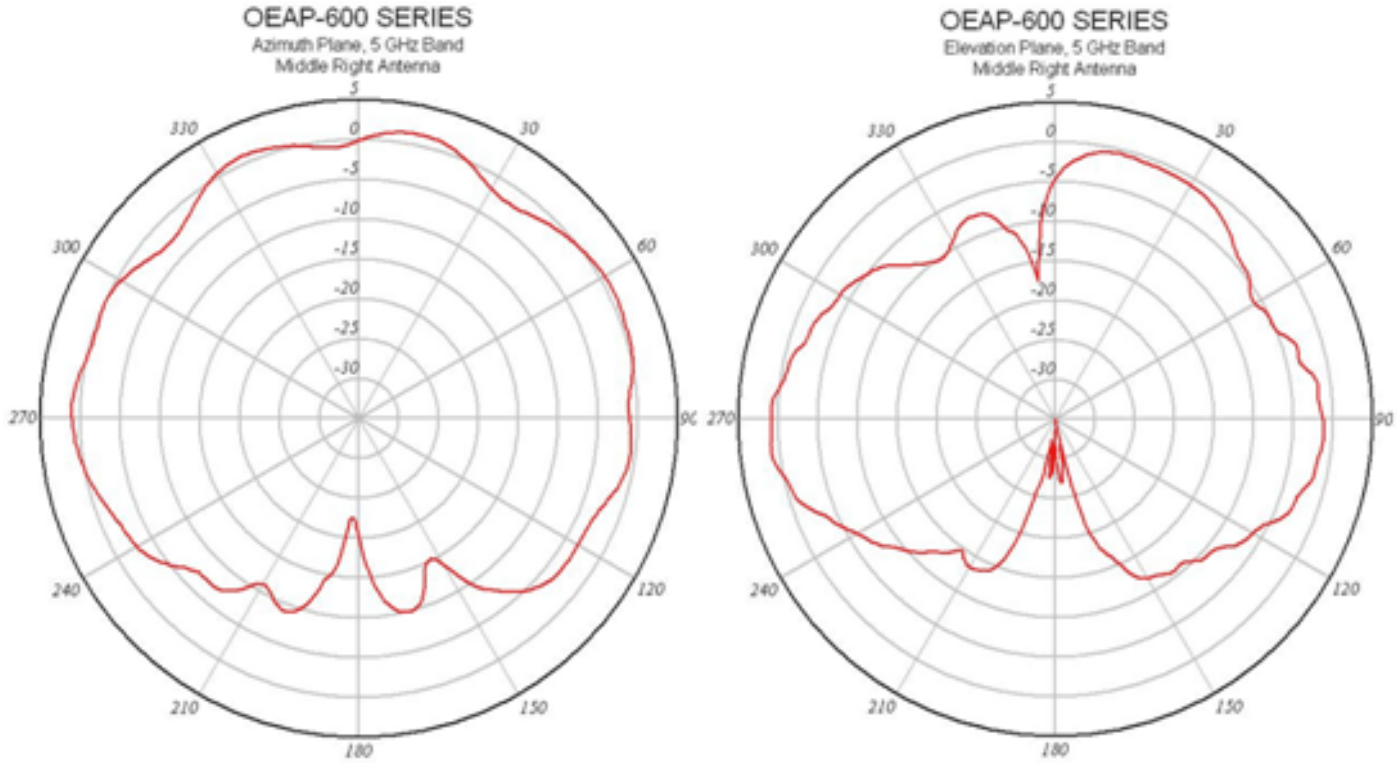
鏡などのような金属面を持つ物体は、ランプシェードの例えのように信号の障害となります。信号が固体を貫通しなければならない場合にはスループットまたはレンジが低下することがあります。たとえば 3 階建ての家で接続する場合には、AP を地下室に配置しないでください。AP は家の中央の場所に設置してください。

アクセス ポイントには 6 つのアンテナが内蔵されています（帯域幅あたり 3 つのアンテナ）。

次の図に、2.4 GHz アンテナ放射パターン（左下のアンテナ）を示します。



次の図に、5 GHz アンテナ放射パターン（右中央のアンテナ）を示します。



OEAP-600 のトラブルシューティング

最初の接続配線が正しいかどうかを確認します。これにより、Cisco Aironet 600 シリーズ OEAP の WAN ポートがルータに接続しており、IP アドレスを適切に受信できることを確認できます。AP がコントローラに接続していないようである場合は、PC をポート 1 ~ 3（ホーム クライアント ポート）に接続し、デフォルト IP アドレス 10.0.0.1 を使用して AP にアクセスできるかどう

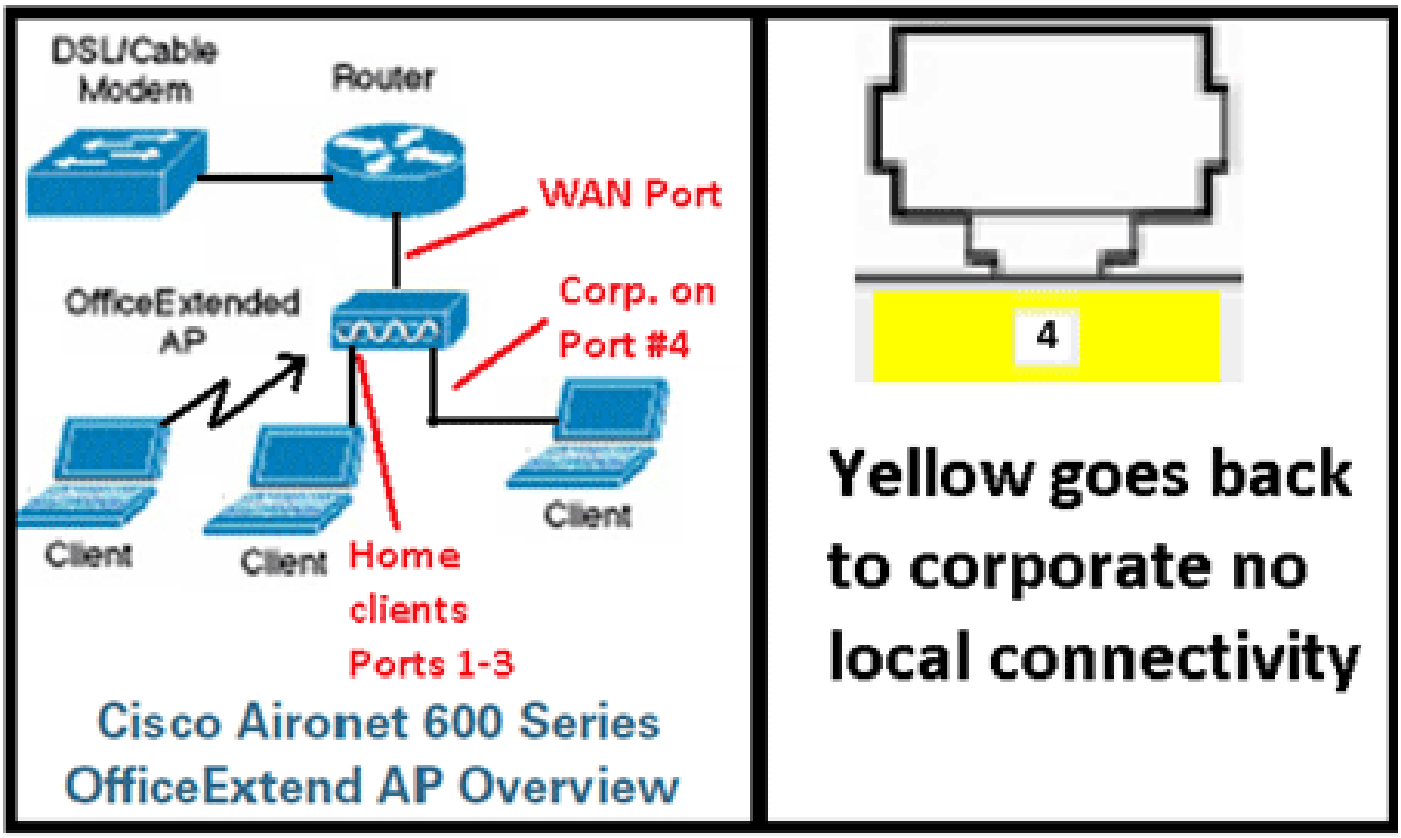
かを確認してください。デフォルトのユーザ名とパスワードは admin です。

会社のコントローラの IP アドレスが設定されているかどうかを確認します。設定されていない場合は IP アドレスを入力して Cisco Aironet 600 シリーズ OEAP をリブートします。これで、Cisco Aironet 600 シリーズ OEAP がコントローラへのリンクを確立する操作を試行できます。

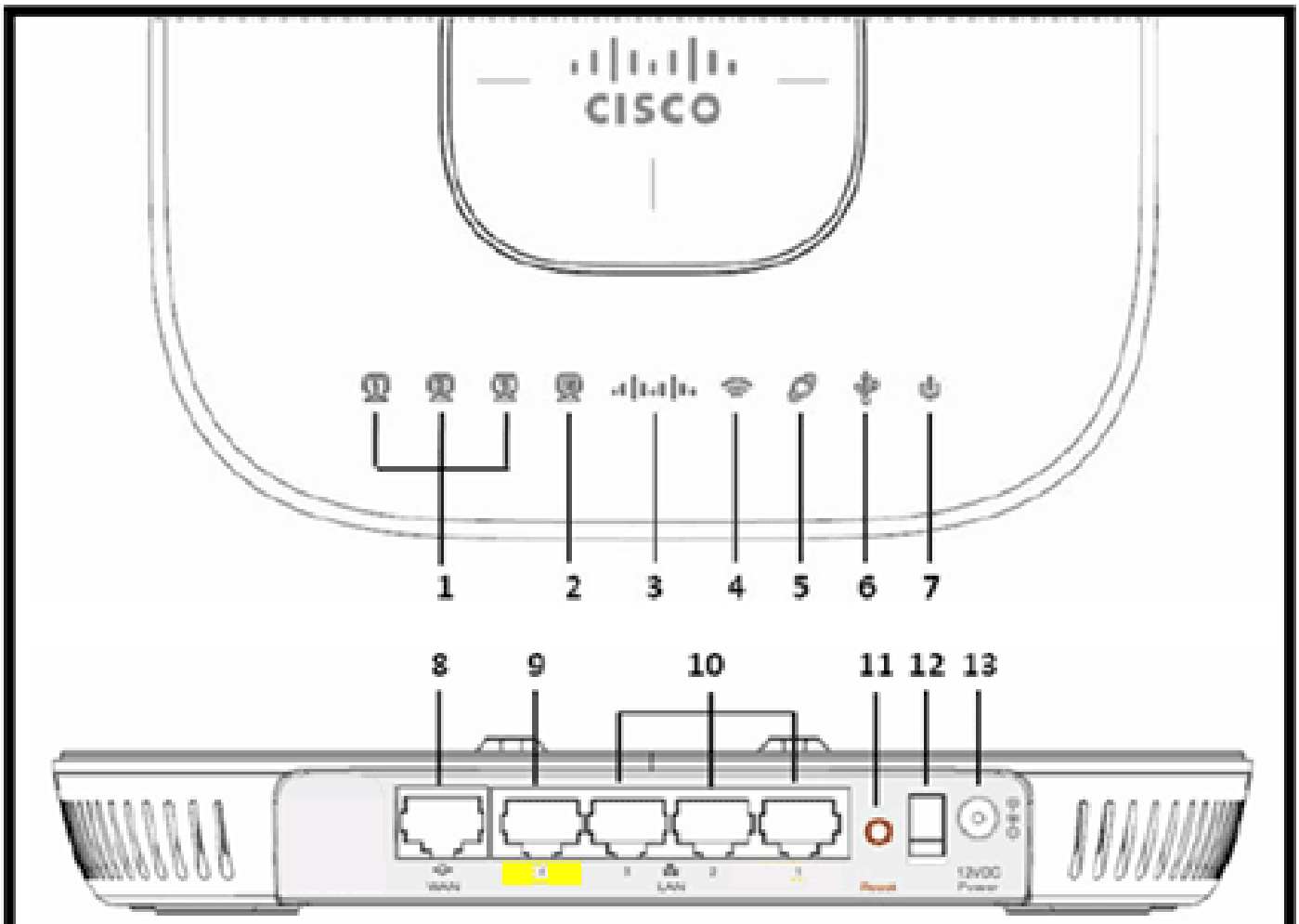
注：設定の目的でデバイスを参照するために、企業ポート#4（黄色）を使用することはできません。リモート LAN が設定されていない場合、これは実質的には「利用不可のポート」です。会社へのトンネルが確立されます（会社への有線接続に使用）。

イベント ログを調べ、アソシエーションの進行状況を確認します（詳細については後述します）。

次の図に、Cisco Aironet 600 シリーズ OEAP の接続配線図を示します。



次の図に、Cisco Aironet 600 シリーズ OEAP の接続ポートを示します。



1	Local Ethernet LEDs 1 through 3	8	WAN Port
2	Remote LAN LED	9	Remote LAN Port
3	Status LED	10	Local Ethernet Ports 1 through 3
4	Wireless LED	11	Reset Button
5	WAN LED	12	Power Toggle Switch
6	USB LED (future)	13	Power Connector
7	Power Indicator LED		

Cisco Aironet 600 シリーズ OEAP がコントローラに接続できない場合は、次の事項を確認することをお勧めします。

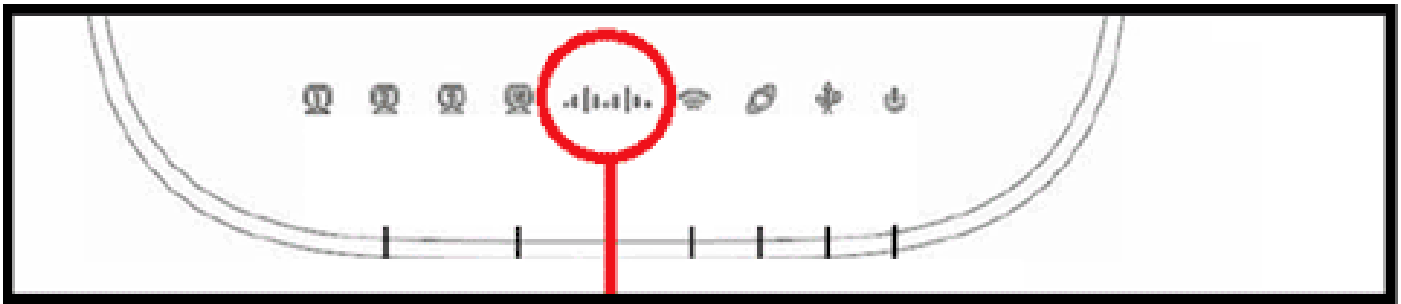
1. ルータが機能しており、Cisco Aironet 600 シリーズ OEAP の WAN ポートに接続しているかどうかを確認します。
2. Cisco Aironet 600 シリーズ OEAP のポート 1 ~ 3 のいずれかに PC を接続します。これでインターネットにアクセスできます。
3. 会社のコントローラの IP アドレスがこの AP に保存されているかどうかを確認します。
4. コントローラが DMZ に配置されており、インターネット経由で到達可能であるかどうかを確認します。

5. 接続を確認し、Cisco ロゴ LED が青色または紫色に点灯することを確認します。

6. AP で新しいイメージをロードして再起動する必要がある場合に備え、十分な時間をとります。

7. ファイアウォールを使用している場合は、UDP ポート 5246 および 5247 がブロックされていないかどうかを確認します。

次の図に、Cisco Aironet 600 シリーズ OEAP ロゴ LED のステータスを示します。

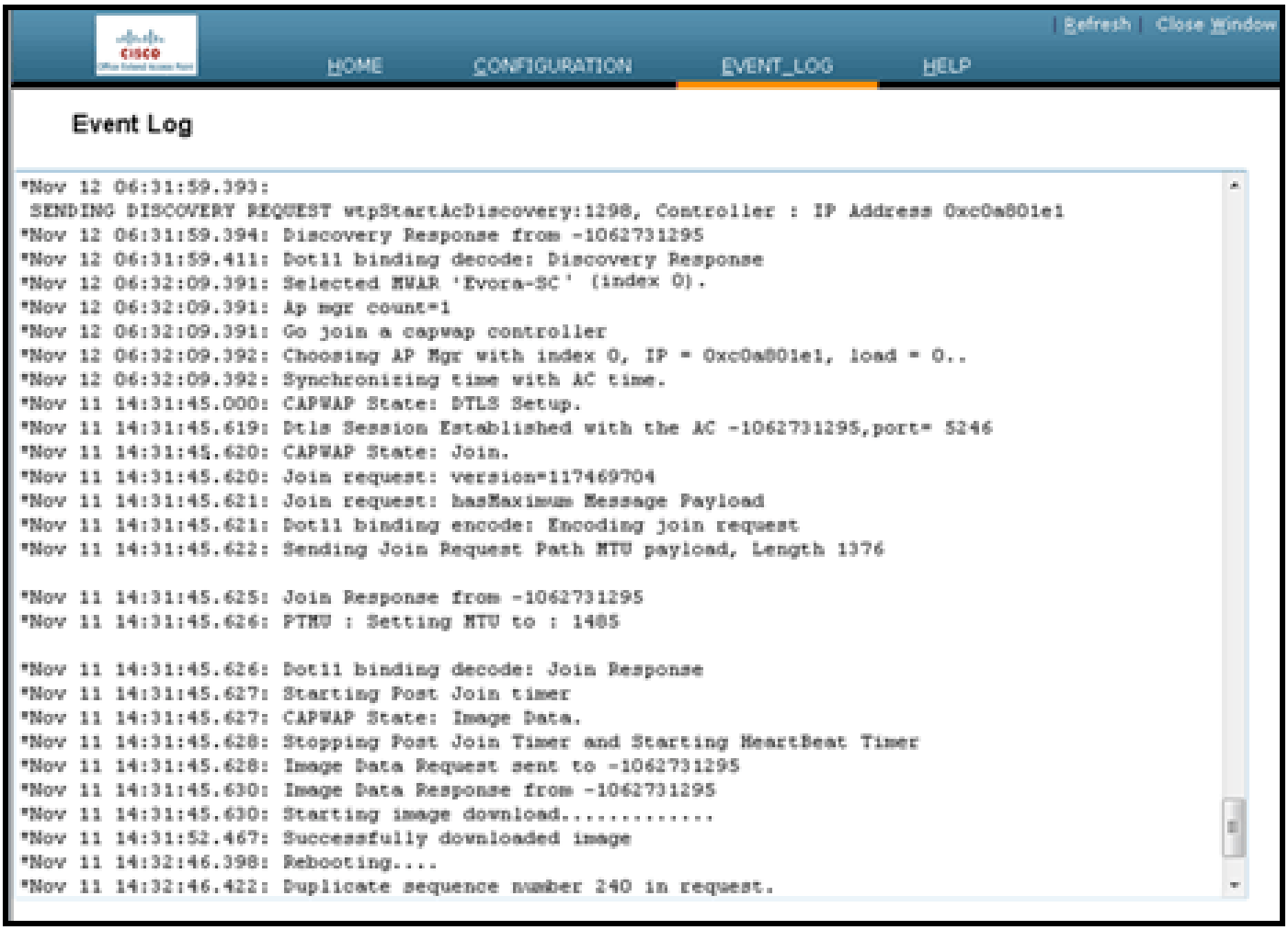


Understanding Cisco Aironet 600 Series OfficeExtend AP LEDs

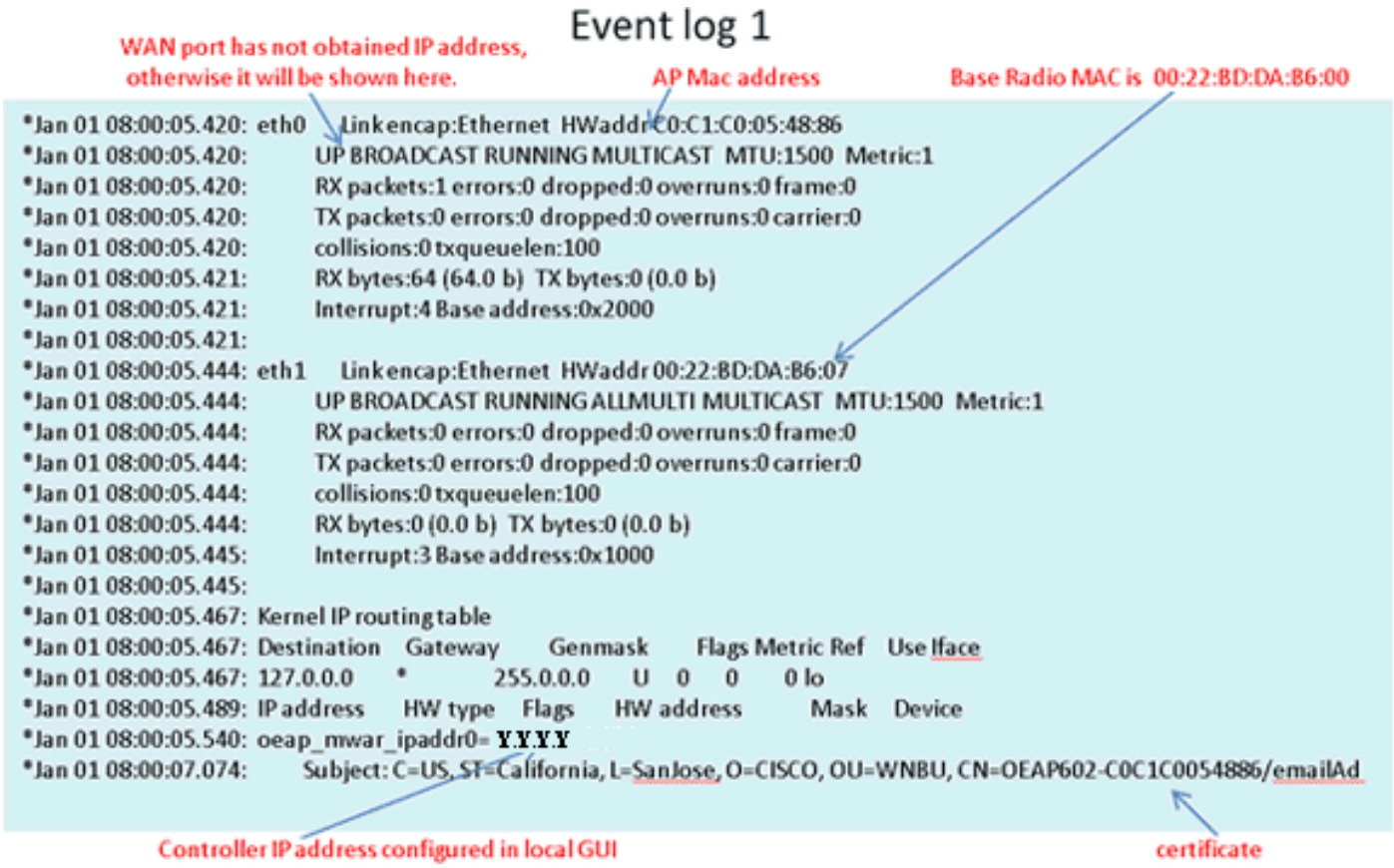
Status LED	Meaning
Purple	Association status, when CAPWAP is connected: Normal operating condition, but no wireless client associated.
Blue	Association status, when CAPWAP is connected: Normal operating condition, at least one wireless client association.
Flashing blue	Operating Status: Software upgrade in progress.
Flashing orange	Operating Status: No IP address, waiting for DHCP IP.
Cycling through purple, orange and blue	Operating Status: Discovery/join process in progress, no client associated.
Cycling through purple, orange	Operating Status: Discovery/join process in progress, with client associated.
Orange	Cisco IOS errors: Software failure; try disconnecting and reconnecting unit power.

接続プロセスが失敗すると、LED の色が繰り返し変わるか、またはオレンジ色で点滅します。この状況が発生した場合は、イベント ログで詳細を確認してください。イベント ログを取得するには、パーソナル SSID または有線ポート 1 ~ 3 を使用して AP にアクセスし、IT 管理者が確認できるようにイベント ログを収集します。

次の図に、Cisco Aironet 600 シリーズ OEAP のイベント ログを示します。



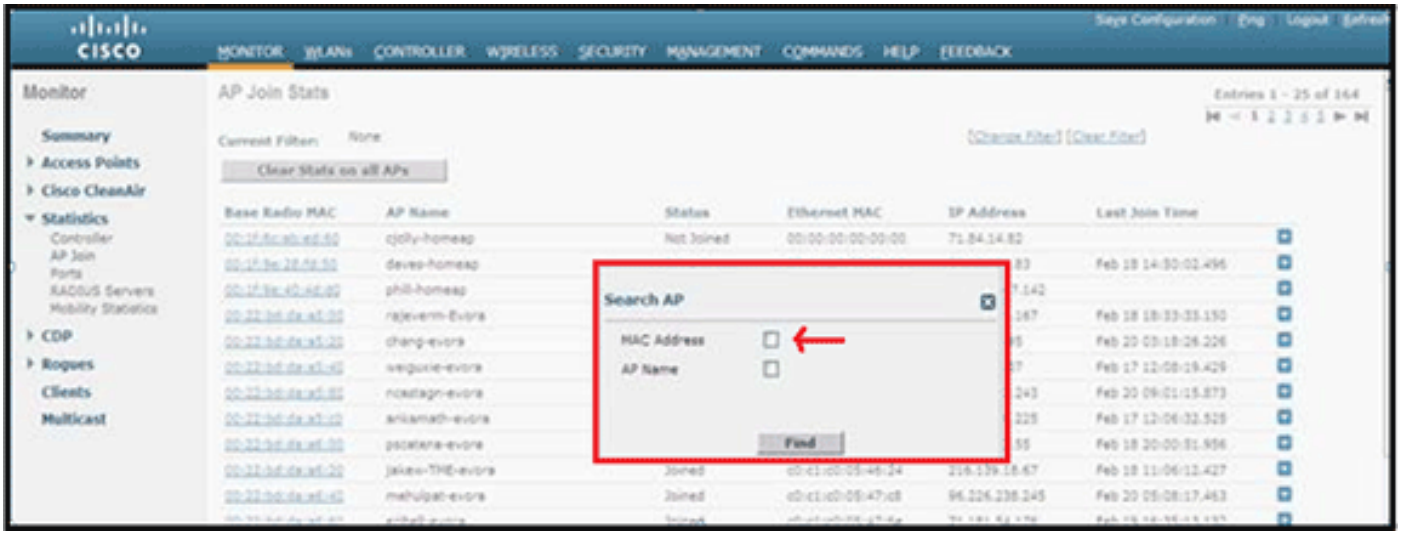
Cisco Aironet 600 シリーズ OEAP からコントローラへの初回接続時に接続プロセスが失敗した場合は、Cisco Aironet 600 シリーズ OEAP の AP 接続統計を確認します。この統計を確認するには、AP のベース Radio MAC が必要です。この情報はイベント ログで確認できます。イベント ログの例と、イベント ログについて説明するコメントを次に示します。



上の図の説明を理解したら、コントローラ モニタの統計を調べ、Cisco Aironet 600 シリーズ OEAP がコントローラに接続したかどうか、またこれまでにコントローラに接続したことがあるかどうかを確認できます。失敗の理由、または失敗したかどうかも確認できます。

AP 認証が必要な場合は、Cisco Aironet 600 シリーズ OEAP の（無線 MAC アドレスではなく）イーサネット MAC アドレスが Radius サーバに小文字で入力されているかどうかを確認します。イーサネット MAC アドレスもイベント ログで確認できます。

コントローラでの Cisco Aironet 600 シリーズ OEAP の検索



ローカル イーサネット ポートに接続している PC からインターネットにアクセスできることが判明しており、ローカル AP GUI で IP アドレスが設定されており、この IP アドレスに到達可能で

あることを確認しているが、AP がコントローラに接続できない場合は、AP がこれまでに正常に接続できていたかどうかを確認します。AP が AAA サーバにない可能性があります。DTLS ハンドシェークが失敗した場合は、AP に不適切な証明書がインストールされているか、コントローラの日付/時刻エラーの可能性があります。

どの Cisco Aironet 600 シリーズ OEAP ユニットからもコントローラにアクセスできない場合は、コントローラが DMZ に配置され到達可能であり、UDP ポート 5246 および 5247 が開いていることを確認します。

クライアント アソシエーションの問題のデバッグ方法

AP がコントローラに接続するが、ワイヤレス クライアントに会社の SSID を関連付けることができません。イベント ログで、アソシエーション メッセージが AP に到達しているかどうかを確認します。

次の図に、会社の SSID と WPA または WPA2 を使用したクライアント アソシエーションの標準的なイベントを示します。SSID とオープン認証または静的 WEP を使用する場合、ADD MOBILE イベントは 1 回だけ発生します。

イベント ログ – クライアント アソシエーション

```
*Feb 19 20:26:58.876: (Re)Assoc-Req from 00:24:d7:2a:72:c0 forwarded to WLC, wired: no

*Feb 19 20:26:58.941: received assoc-rsp for wireless client, status=0000

*Feb 19 20:26:58.942:
ADD_MOBILE from WLC,wmeEnabled=1,encrptPolicy=1

*Feb 19 20:26:58.942: ADD_MOBILE: client 00:24:d7:2a:72:c0, slot=0,vapid=1

*Feb 19 20:27:00.648:
ADD_MOBILE from WLC,wmeEnabled=1,encrptPolicy=4

*Feb 19 20:27:00.649: ADD_MOBILE: client 00:24:d7:2a:72:c0, slot=0,vapid=1
```

(Re)Assoc-Req イベントがログに記録されていない場合は、クライアントのセキュリティ設定が適切であるかどうかを確認してください。

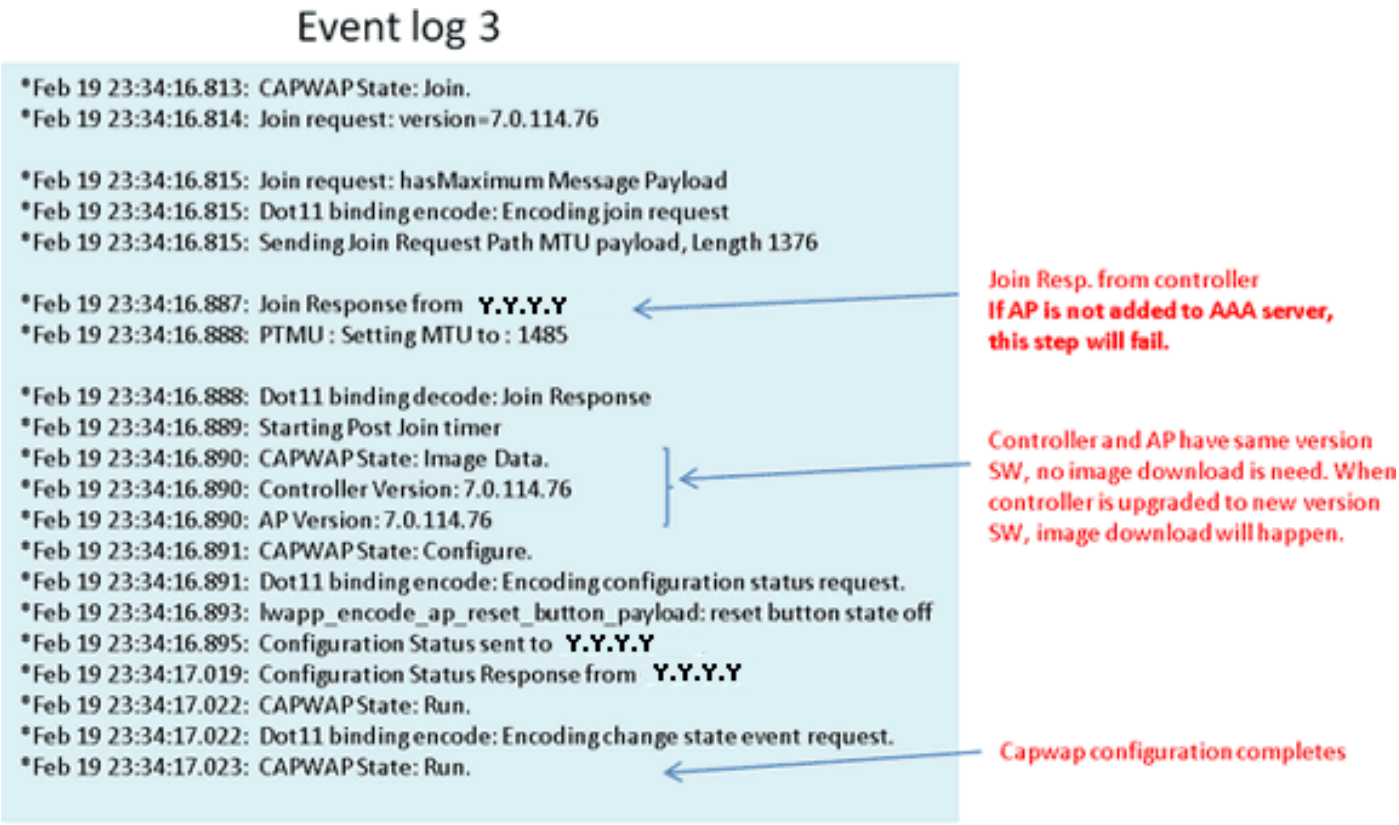
(Re)Assoc-Req イベントがログに記録されているが、クライアントが適切に関連付けられない場合は、コントローラでクライアントに対して debug client <MAC アドレス> コマンドを実行し、シスコの非 OEAP アクセス ポイントと連携するクライアントの場合と同様の方法で問題を調査します。

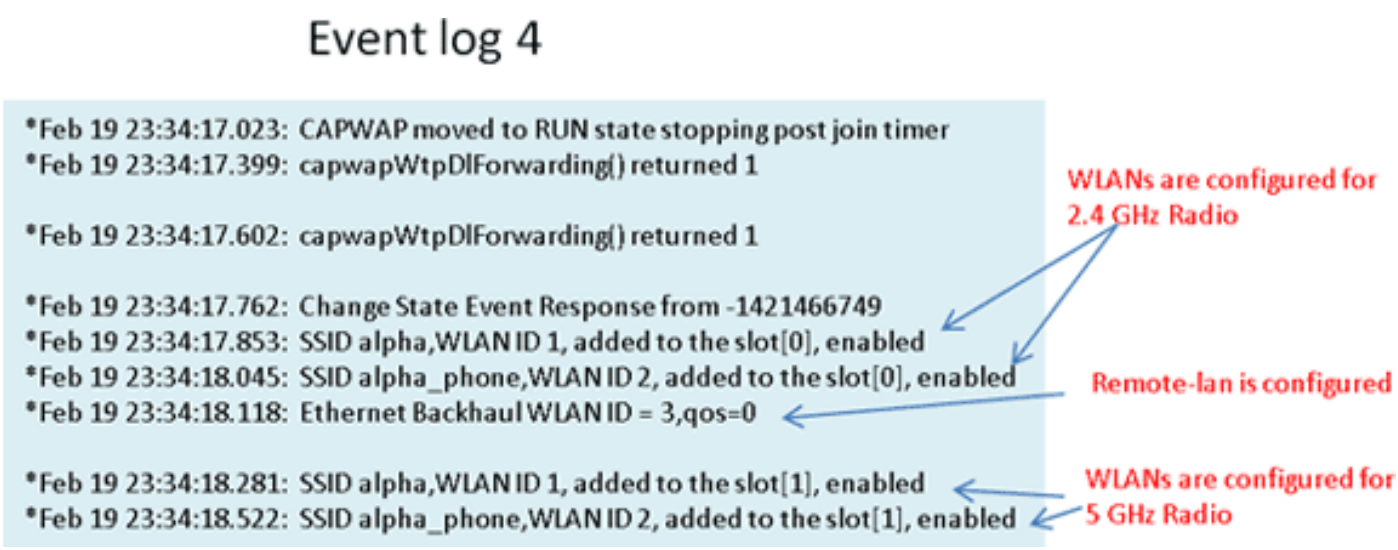
イベント ログの解釈方法

次に示すイベント ログには、Cisco Aironet 600 シリーズ OEAP のその他の接続に関連する問題

を解決する際に役立つコメントが付いています。

Cisco Aironet 600 シリーズ OEAP イベント ログ ファイルから収集したログの例と、イベント ログを解釈する際に役立つコメントを次に示します。





インターネット接続が信頼性のない接続である可能性がある場合

このセクションに示すイベント ログの例は、インターネット接続が失敗する場合、または最終的に低速または頻繁に停止する場合のログです。このような状況は通常、ISP ネットワーク、ISP モデム、またはホーム ルータが原因で発生します。ISP との接続がドロップするかまたは信頼性が低くなることがあります。このような状況が発生する場合は、CAPWAP リンク（会社へのトンネル）が失敗するか、または問題が発生している可能性があります。

次に、イベント ログに記録されているこのような失敗の例を示します。

```
*Feb 16 07:13:24.918: Re-Tx Count= 0, Max Re-Tx Value=5, NumofPendingMsgs=1
*Feb 16 07:13:36.919: Re-Tx Count= 4, Max Re-Tx Value=5, NumofPendingMsgs=2
*Feb 16 07:13:39.919: Max retransmission count exceeded going back to DISCOVER mode.
*Feb 16 07:13:39.919: Retransmission count for packet exceeded max(UNKNOWN_MESSAGE_TYPE (218103808)., 2)
*Feb 16 07:13:39.919: Retransmission count exceeded max, ignoring as the ethernet is overloaded
*Feb 16 07:13:42.918: Re-Tx Count= 6, Max Re-Tx Value=5, NumofPendingMsgs=2
Comment : This Retransmission continues on..... Multiple times..
*Feb 16 07:13:42.919: Max retransmission count exceeded going back to DISCOVER mode.
*Feb 16 07:13:42.919: Retransmission count for packet exceeded max(UNKNOWN_MESSAGE_TYPE (218103808)
*Feb 16 07:14:09.919: GOING BACK TO DISCOVER MODE
*Feb 16 07:14:09.920: CAPWAP State: DTLS Teardown.
*Feb 16 07:14:14.918: DTLS session cleanup completed. Restarting capwap state machine.
*Feb 16 07:14:14.919:
Lost connection to the controller, going to re-start evora...
```

追加のデバッグ コマンド

ホテルなどのような利用料金制の施設で Cisco Aironet 600 シリーズ OEAP を使用する際には、Cisco Aironet 600 シリーズ OEAP がコントローラへのトンネルを確立する前に、ウォールドガーデン内にアクセスする必要があります。このためには、ラップトップを有線ローカル ポート（ポート 1 ~ 3）の 1 つに接続するか、パーソナル SSID を使用してホテルにログインし、スプラッシュ スクリーンを表示します。

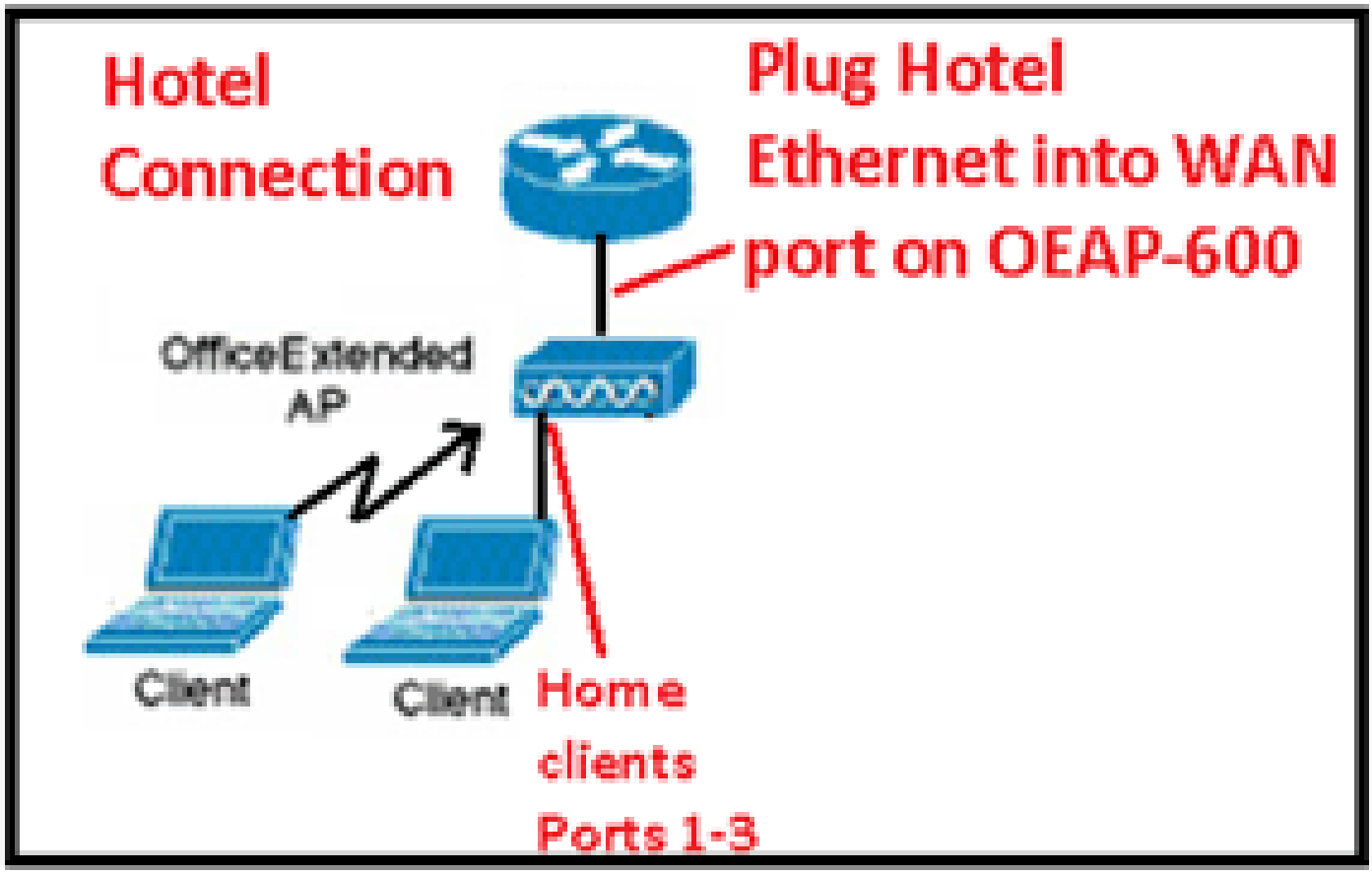
AP のホーム サイドからインターネットに接続すると、DTLS トンネルが確立され、会社の SSID が設定されます。有線ポート #4 がアクティブになります（リモート LAN が設定されていること

を前提とする）。

注：この処理には数分かかることがあります。CiscoロゴLEDが、接続が成功したことを示す青色または紫色で点灯することを確認します。この時点では、パーソナル接続と会社での接続の両方がアクティブです。

注：ホテルまたは別のISPが接続を解除すると（通常24時間）、トンネルが切断されます。このような場合、同じプロセスをやり直す必要があります。これは意図的に設計されたものであり、正常な操作です。

次の図に、利用料金制の施設での OfficeExtend の設定を示します。



次の図に、その他のデバッグ コマンド（無線インターフェイス情報）を示します。

Below are the new diagnostics commands for the OEAP 600

The WLC CLI of "show tech" is:

debug ap enable <apname>
then:
debug ap command "evoraTechSupport" <apname> → the information about system and radio slot 0/1
debug ap command "evoraTechSupport 2" <apname> → more info about radio slot 0 (2.4G)
debug ap command "evoraTechSupport 3" <apname> → more info about radio slot 1 (5G)

The "show eventlog" is the same as other APs:
show ap eventlog <apname>

既知の問題および警告

設定ファイルをコントローラから TFTP/FTP サーバにアップロードする場合、リモート LAN の設定は WLAN 設定としてアップロードされます。詳細については、『Cisco Wireless LAN Controller と Lightweight アクセス ポイント リリース 7.0.116.0 のリリース ノート』を参照してください。

OEAP-600で、CAPWAP 接続がコントローラの認証の失敗が原因で失敗した場合は、OEAP-600 が CAPWAP の試行を再開するまで OEAP-600 上の Cisco 口ゴ LED がしばらくオフになることがあります。これは通常の動作であるため、口ゴ LED がしばらく消灯しても AP がシャットダウンしたわけではないことを念頭に置いてください。

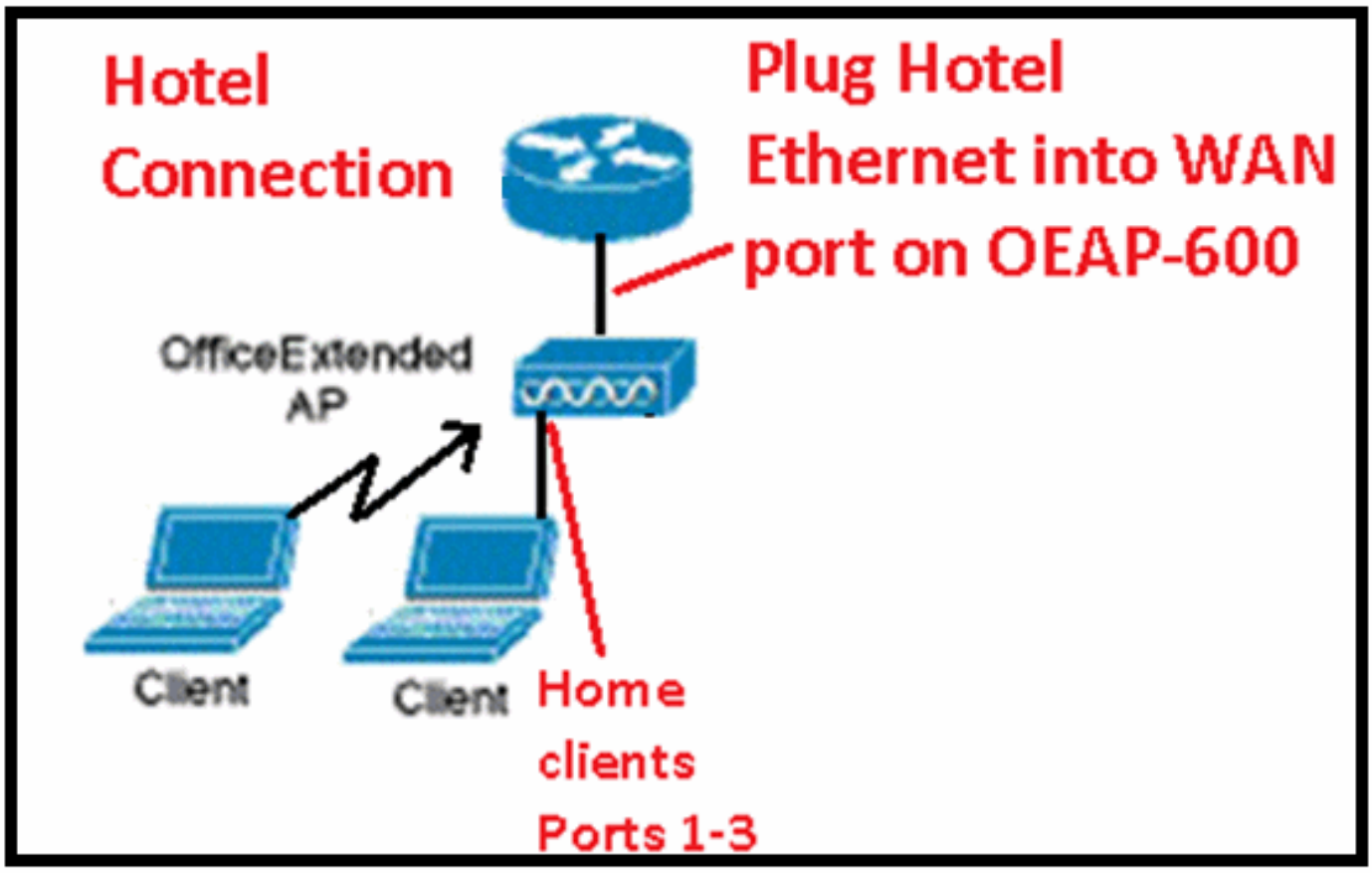
この OEAP-600 製品は、以前の OEAP アクセス ポイントとはログイン名が異なるため、Linksys などのホーム製品と一貫性を保つためにデフォルトのユーザ名はadmin 、パスワードは admin となっています。AP-1130 および AP-1140 などのその他の Cisco OEAP アクセス ポイントのデフォルトのユーザ名は Cisco で、パスワードは Cisco です。

OEAP-600 の最初のリリースでは 802.1x がサポートされていますが、CLI でのみサポートされます。GUI の変更を試行したユーザの設定が失わる場合があります。

ホテルなどのような利用料金制の施設で OEAP-600 を使用する際には、OEAP-600 がコントローラへのトンネルを確立する前に、ウォールドガーデン内にアクセスする必要があります。単にラップトップを有線ローカル ポート (ポート 1 ~ 3) の 1 つに接続するか、パーソナル SSID を使用してホテルにログインし、スプラッシュ スクリーンを表示します。AP のホーム サイドからインターネットに接続すると、DTLS トンネルが確立され、会社の SSID および有線ポート #4 が設定されます。これによりリモート LAN が設定されたとみなされ、アクティブになります。この処理には数分間かかることがあることに注意してください。Cisco 口ゴ LED が、接続が成功したことを示す青色または紫色で点灯することを確認します。この時点では、パーソナル接続と会社での接続の両方がアクティブです。

注：ホテルや他のISPが接続を解除すると（通常は24時間）、トンネルが切断される場合があり、同じプロセスを再起動する必要があります。これは意図的に設計されたものであり、正常な操作です。

利用料金制の施設での Office Extend の使用

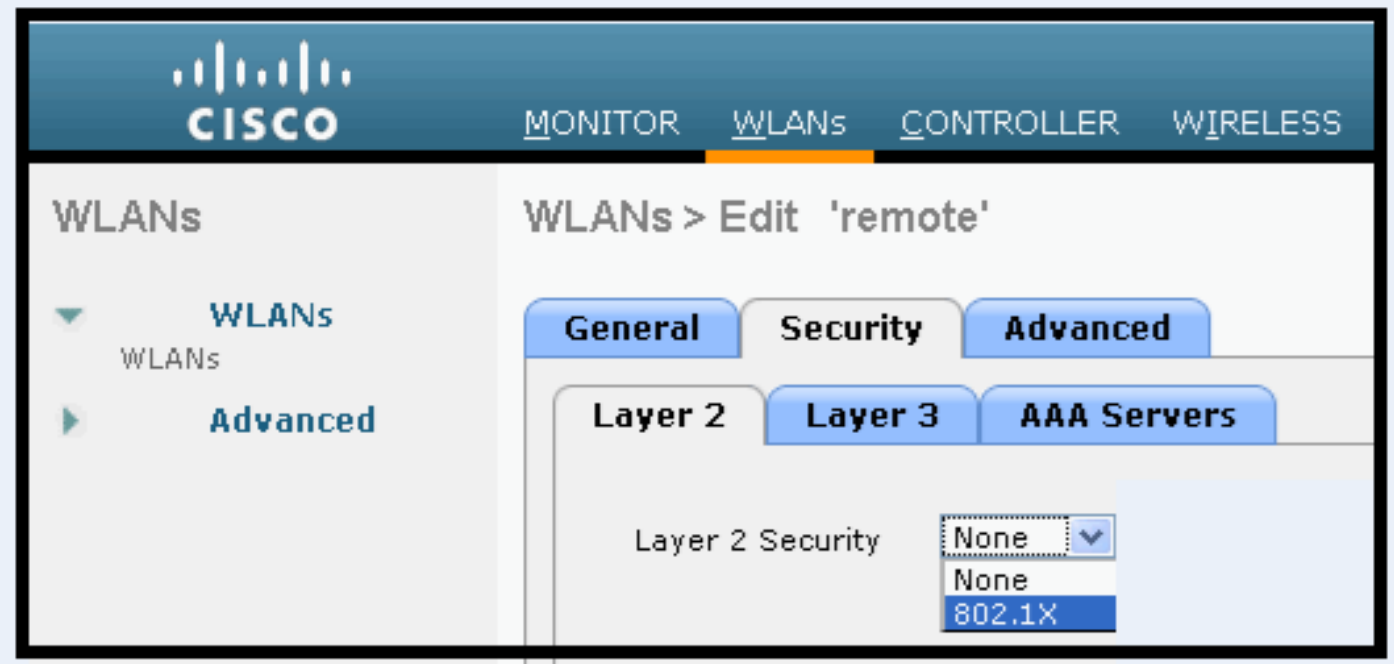


次に Cisco 7.2 リリースで導入された拡張の一部を示します。

- GUI への 802.1x セキュリティの追加
- コントローラから AP 上のローカル WLAN アクセスを無効にする機能：パーソナル SSID を無効にして企業設定のみを許可
- チャネル割り当ての選択可能なオプション
- サポートが 2 つの企業 SSID から 3 つの SSID に変更
- デュアル RLAN ポート機能のサポート

GUI への 802.1x セキュリティの追加

802.1x が GUI に追加されました



リモート LAN ポートに対する認証に関する注記。

802.1x authentication for remote-LAN port

WCS shall be provided to enable 802.1x Layer 2 Security and configure AAA server for remote-LAN. WEP encryption shall be always disabled.

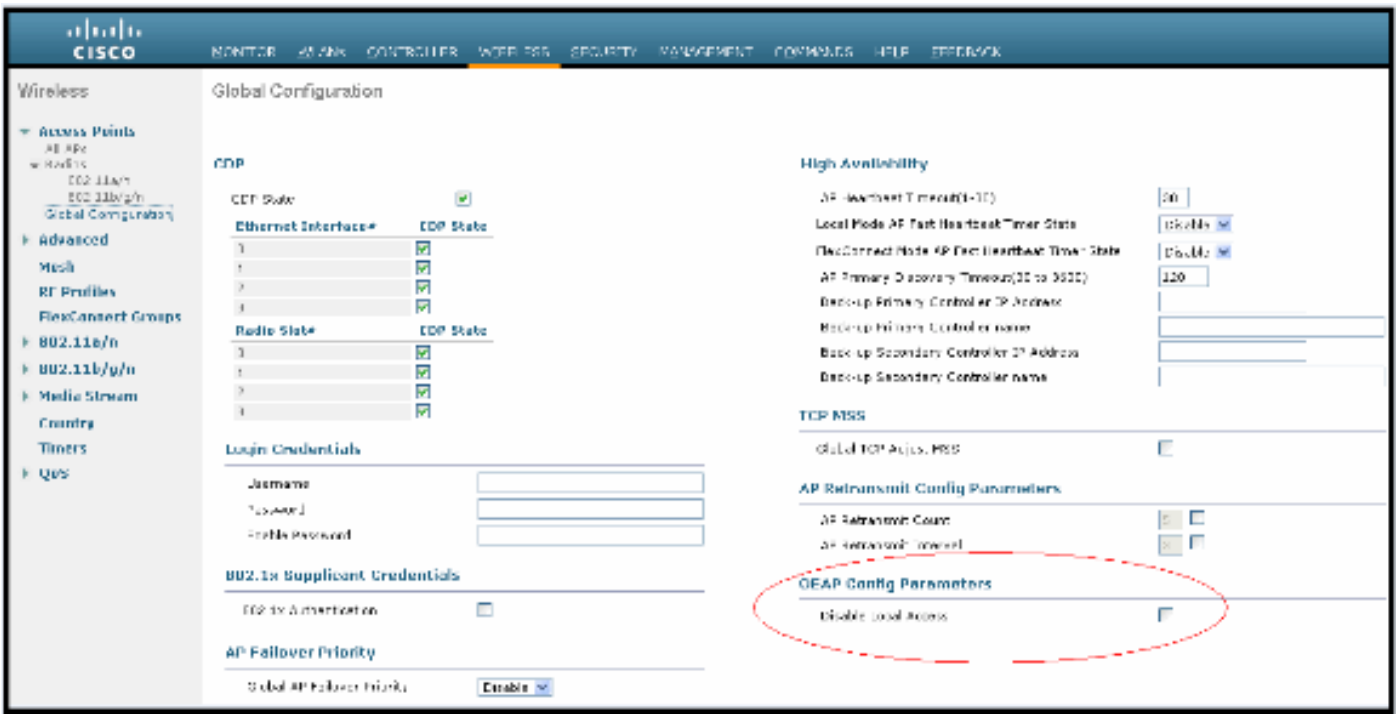
Same as 802.1x authentication for wireless clients, in 802.1x authentication for remote-LAN client, WLC acts as authenticator. Evora AP just forwards the EAPOL packets. AP converts EAPOL Ethernet packet to 802.11 data frame before sending it to WLC. The destination address in the 802.11 data frame shall be set to BSSID for remote-LAN. There is no data encryption for the Ethernet packets transferred on remote-LAN port. So there is no key exchange on EAPOL. The data security is provided by DTLS on CAPWAP data channel.

Following EAP methods are supported:

- EAP-TLS
- PEAP
- EAP-TTLS.

コントローラから AP 上のローカル WLAN アクセスを無効にする機能：パーソナル SSID を無効にして企業設定のみを許可

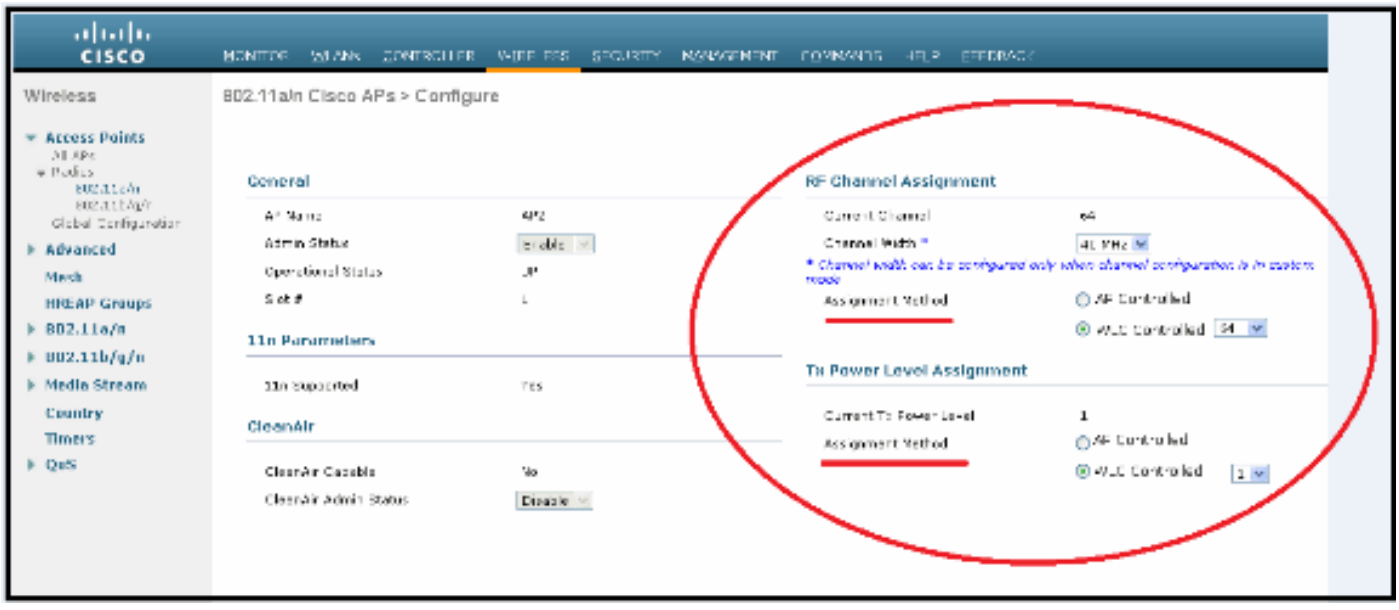
ローカル WLAN アクセスの無効化

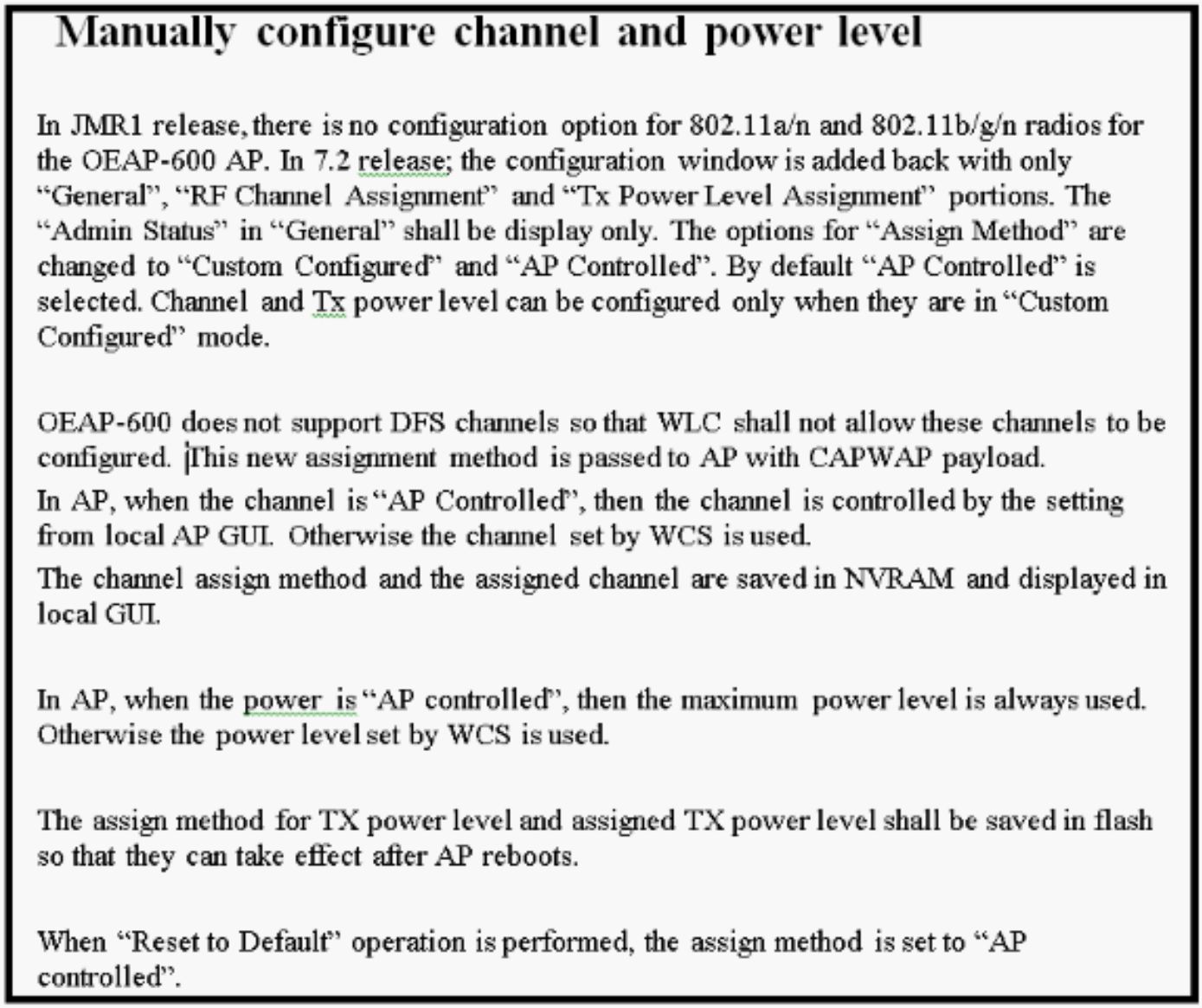


チャネル割り当ての選択可能なオプションは次のとおりです。

- ローカル制御の AP
- WLC 制御

RF のチャネルおよび電源割り当てはローカルまたは WLC 制御になりました





デュアル RLAN ポート機能（CLI のみ）のサポート

この注記は、OEAP-600 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 RLAN ポート機能を使用する OEAP-600 シリーズ AP に適用されます。設定は CLI からのみ許可されます。次に例を示します。

```
Config network oeap-600 dual-rlan-ports enable|disable
```

この機能が設定されていない場合は、単一ポート 4 のリモート LAN が引き続き機能します。各ポートは、ポートごとに固有のリモート LAN を使用します。リモート LAN マッピングは、デフォルト グループまたは AP グループが使用されるかどうかによって異なります。

Default-group

default-groupを使用すると、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が2のリモートLANは、（OEAP-600の）ポート4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（OEAP-600 上）にマッピングされます。

たとえば、次の 2 つのリモート LAN を想定します。

```
(Cisco Controller) >show remote-lan summary

Number of Remote LANS.......................... 2

RLAN ID  RLAN Profile Name    Status    Interface Name
-------  -----------------------------------  --------  --------------------
2        rlan2                                Enabled   management
3        rlan3                                Enabled   management
```

rlan2 には偶数のリモート LAN ID 2 があり、ポート 4 にマッピングされます。rlan3 は奇数のリモート LAN ID 3 があるため、ポート 3 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と、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、AP グループに 2 つのリモート LAN を追加します。最初に、ポート 3 AP リモート LAN を追加し、次にポート 4 リモート グループ、最後に任意の WLAN を追加します。

次の例に示すように、リスト内の最初の位置のリモート LAN はポート 3 にマッピングし、次のリモート LAN はポート 4 にマッピングします。

```
RLAN ID  RLAN Profile Name      Status    Interface Name
-------  -----------------------------------  --------  --------------------
2        rlan2                                Enabled   management
3        rlan3                                Enabled   management
```

関連情報

- Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 7.0
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。