

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

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定ガイドライン](#)

[Office Extend ソリューション概要](#)

[ファイアウォール設定ガイドライン](#)

[Office Extend AP-600 設定手順](#)

[WLAN およびリモート LAN 設定](#)

[WLAN セキュリティ設定](#)

[MAC フィルタリング](#)

[サポートされるユーザ数](#)

[チャンネル管理および設定](#)

[追加の警告](#)

[OEAP-600 アクセス ポイント設定](#)

[OEAP-600 アクセス ポイント ハードウェアの設置](#)

[OEAP-600 のトラブルシューティング](#)

[クライアント アソシエーションの問題のデバッグ方法](#)

[イベント ログの解釈方法](#)

[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](#)

[追加のデバッグ コマンド](#)

[既知の問題および警告](#)

[関連情報](#)

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。

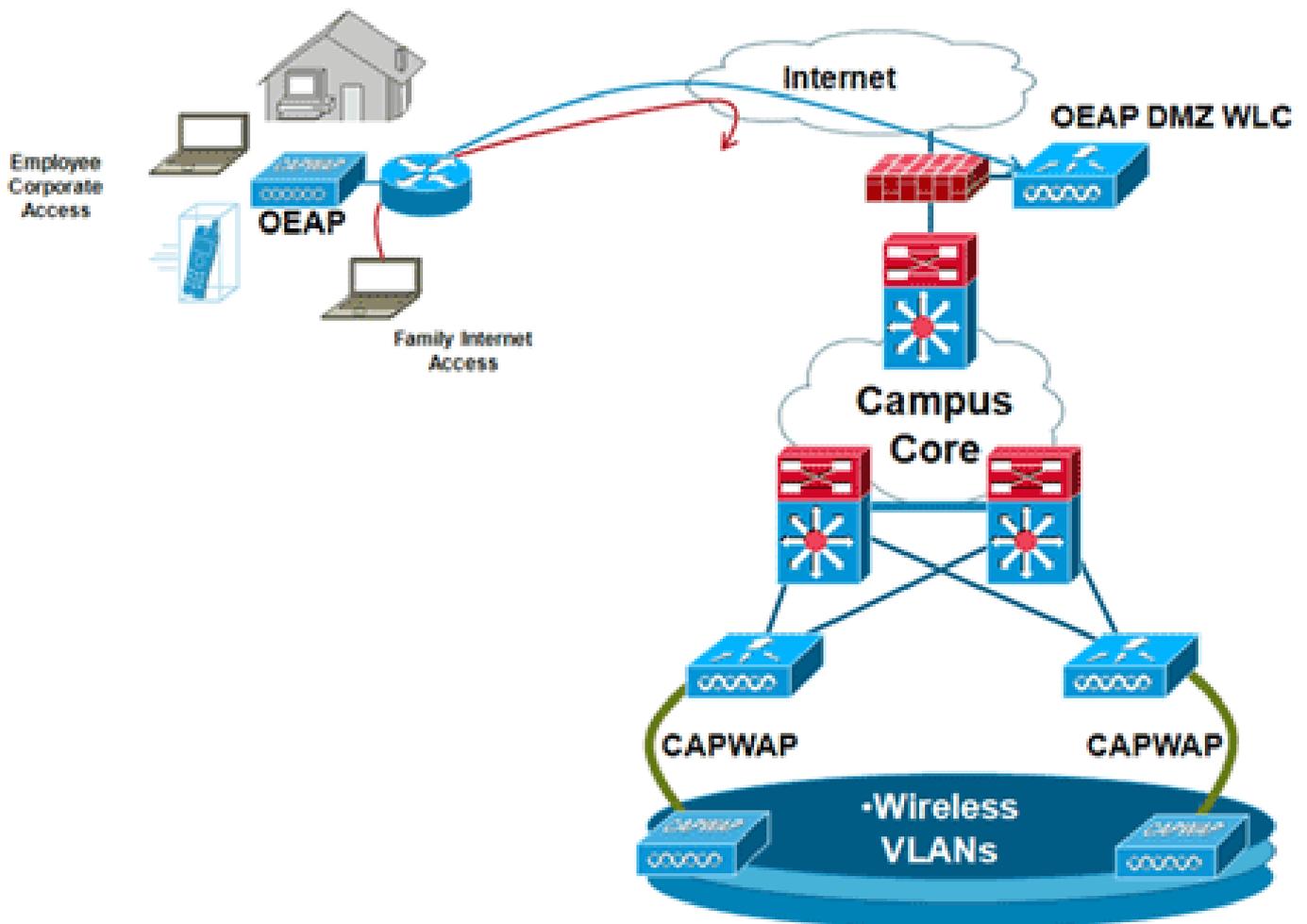
- リモート LAN を設定している場合は、AP の 1 つの有線ポートからコントローラへトンネルが確立されます。
- これで、ユーザが個人で使用するローカル SSID を有効にできます。

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ディスカバリ中にものみ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。

The screenshot shows the Cisco Controller configuration page for an interface named 'management'. The page is divided into several sections:

- General Information:** Interface Name: management, MAC Address: 00:24:97:69:52:8f
- Configuration:** Quarantine: , Quarantine Vlan Id: 0
- NAT Address:** Enable NAT Address: (circled in red), NAT IP Address: X.X.X.Y
- Interface Address:** VLAN Identifier: 0, IP Address: 172.16.1.25, Netmask: 255.255.255.0, Gateway: 172.16.1.2
- Physical Information:** The interface is attached to a LAG, Enable Dynamic AP Management:
- DHCP Information:** Primary DHCP Server: 172.20.225.153, Secondary DHCP Server: 0.0.0.0

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。

The screenshot shows the Cisco Aironet 600 Security configuration page for AP Policies. The left sidebar contains a navigation menu with categories like AAA, Local EAP, Priority Order, Certificate, and Access Control Lists. The main content area is titled 'AP Policies' and includes a 'Policy Configuration' section with several options: 'Accept Self Signed Certificate (SSC)' (checked), 'Accept Manufactured Installed Certificate (MIC)' (checked), 'Accept Local Significant Certificate (LSC)' (unchecked), 'Authorize MIC APs against auth-list or AAA' (checked), and 'Authorize LSC APs against auth-list' (unchecked). Below this is an 'AP Authorization List' section with a search box and a table of entries. The table has columns for MAC Address, Certificate Type, and SHA1 Key Hash. Two entries are shown, both with MAC Address 00:01:36:1f:e4:59 and 00:01:36:1f:e4:60, Certificate Type SSC, and SHA1 Key Hash 4073c833036f05f68acbc9329f67182102623c7f.

MAC Address	Certificate Type	SHA1 Key Hash
00:01:36:1f:e4:59	SSC	4073c833036f05f68acbc9329f67182102623c7f
00:01:36:1f:e4:60	SSC	4073c833036f05f68acbc9329f67182102623c7f

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。

WLANs > New

Type: WLAN

Profile Name: Guest LAN, WLAN, Remote LAN

SSID:

ID: 4

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。

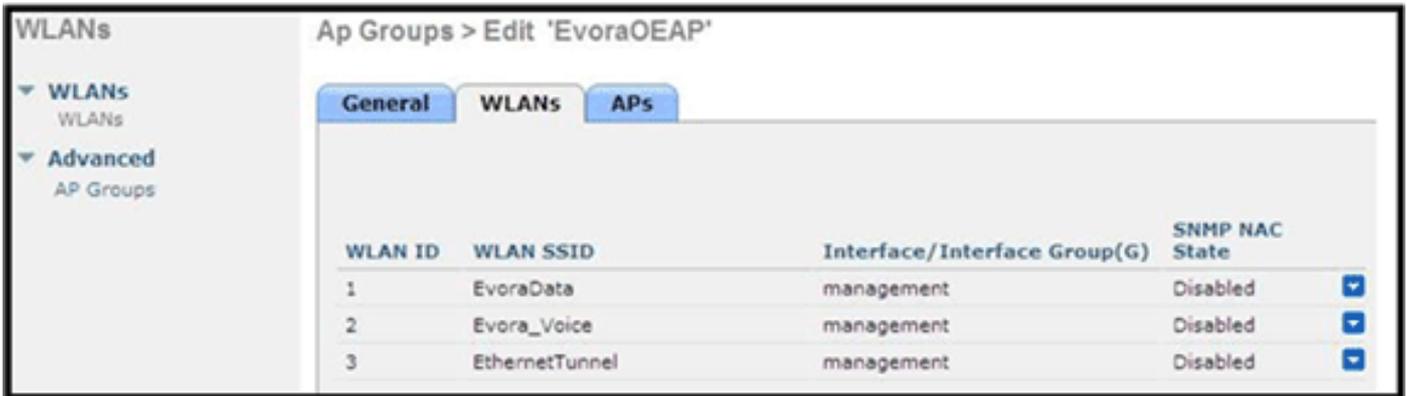
次の図に、WLAN とリモート LAN を設定する画面を示します。

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	EvoraData	EvoraData	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	EvoraVoice	Evora_Voice	Enabled	[WPA2][Auth(802.1X)]
3	Remote LAN	EthernetTunnel	---	Enabled	None

次の図に、OEAP グループ名の例を示します。

AP Group Name	AP Group Description
EvoraOEAP	Group for EvoraOEAPs
default-group	

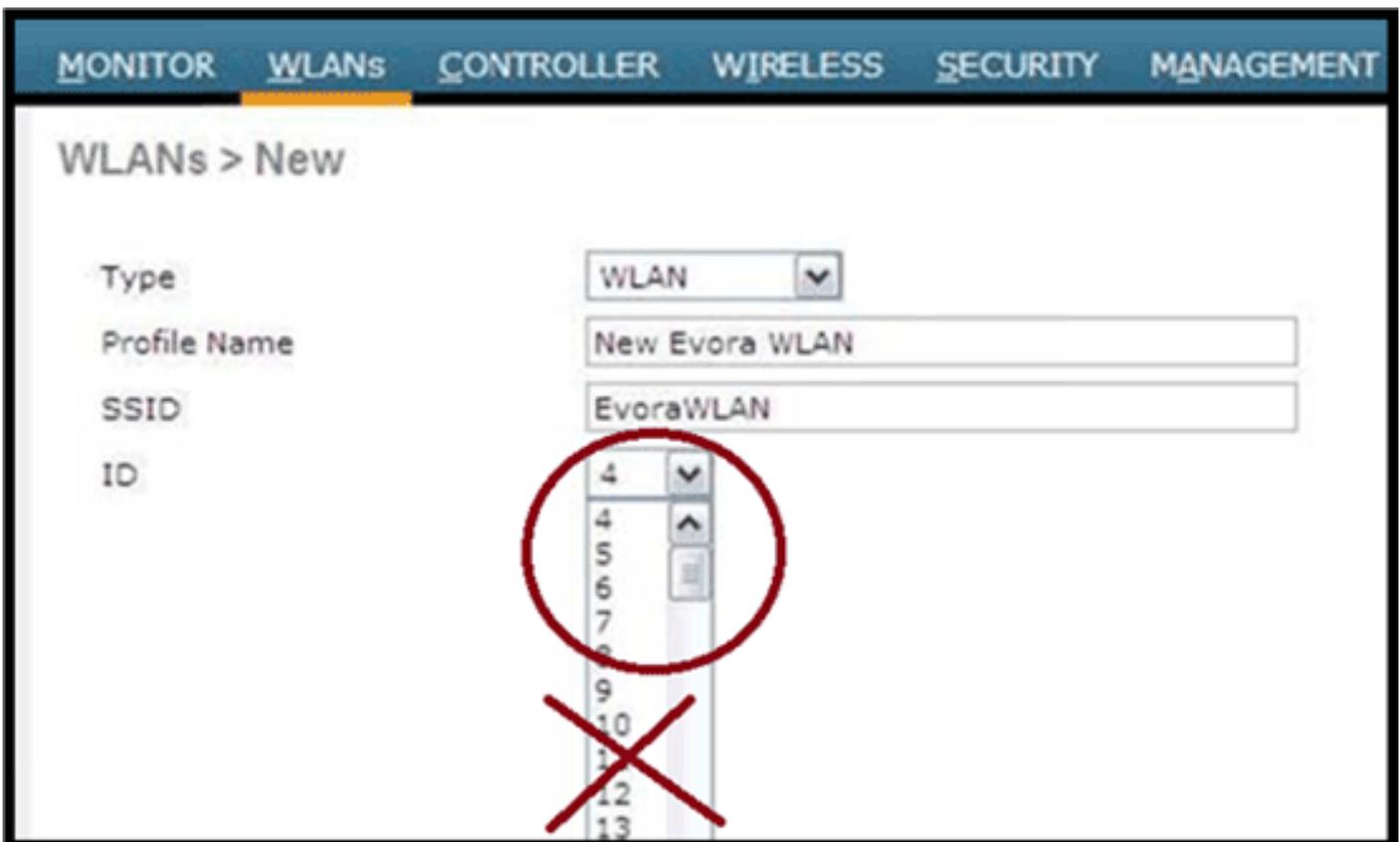
次の図に、WLAN SSID と RLAN の設定を示します。



WLAN ID	WLAN SSID	Interface/Interface Group(G)	SNMP NAC State
1	EvoraData	management	Disabled
2	Evora_Voice	management	Disabled
3	EthernetTunnel	management	Disabled

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。



MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT

WLANs > New

Type: WLAN

Profile Name: New Evora WLAN

SSID: EvoraWLAN

ID: 4 (highlighted with a red circle and a red X over it)

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。

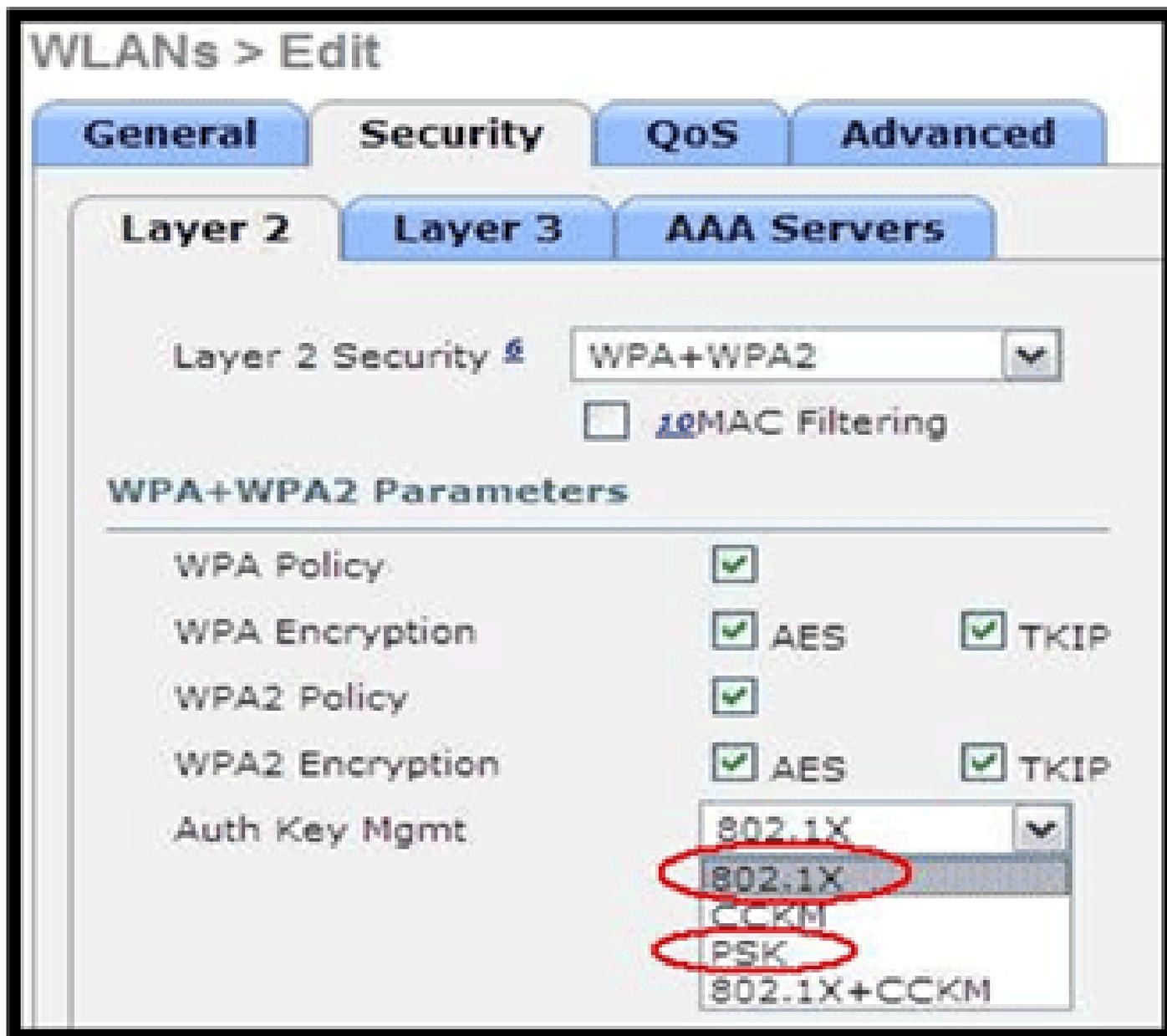
- なし
- [WPA+WPA2]
- [Static WEP] も使用できますが、.11nデータレートには使用できません。

The screenshot shows the 'WLANs > Edit' configuration page with the 'Security' tab selected. Under the 'Layer 2' sub-tab, the 'Layer 2 Security' dropdown menu is open, showing options: 'None', 'WPA+WPA2', 'Static WEP', 'Static-WEP + 802.1X', and 'CKIP'. The 'None' and 'Static WEP' options are circled in red. Below the dropdown, the 'WPA+WPA2 Parameter' is set to '802.1X'. The 'WPA2 Policy' checkbox is checked. The 'WPA2 Encryption' section has 'AES' and 'TKIP' checkboxes checked. The 'Auth Key Mgmt' dropdown is set to '802.1X'.

Setting	Value / Status
Layer 2 Security	WPA+WPA2 (dropdown menu open)
WPA+WPA2 Parameter	802.1X
WPA Policy	
WPA Encryption	
WPA2 Policy	<input checked="" type="checkbox"/>
WPA2 Encryption	<input checked="" type="checkbox"/> AES <input checked="" type="checkbox"/> TKIP
Auth Key Mgmt	802.1X (dropdown menu)

注：802.1xまたはPSKのみを選択してください。

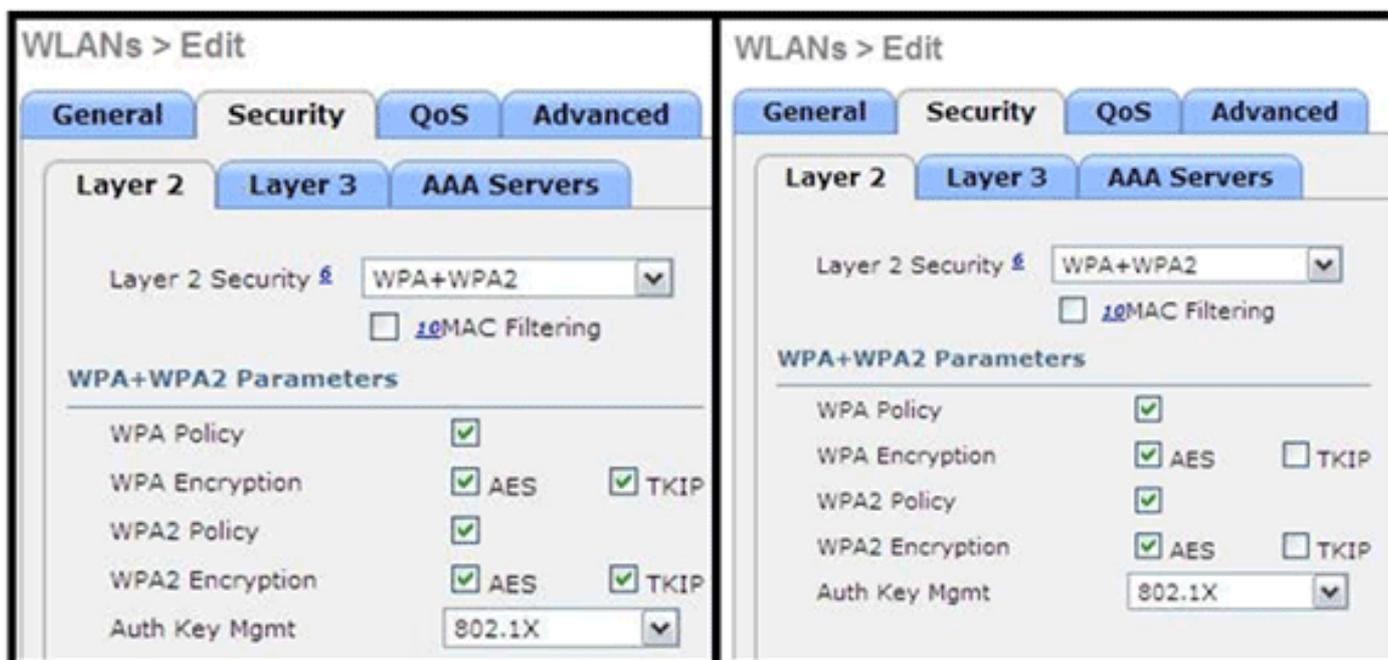
次の図に示すように、WPAとWPA2のセキュリティ暗号化設定では、TKIPとAESの設定を同じにする必要があります。



TKIPとAESの誤った設定の例を次の図に示します。



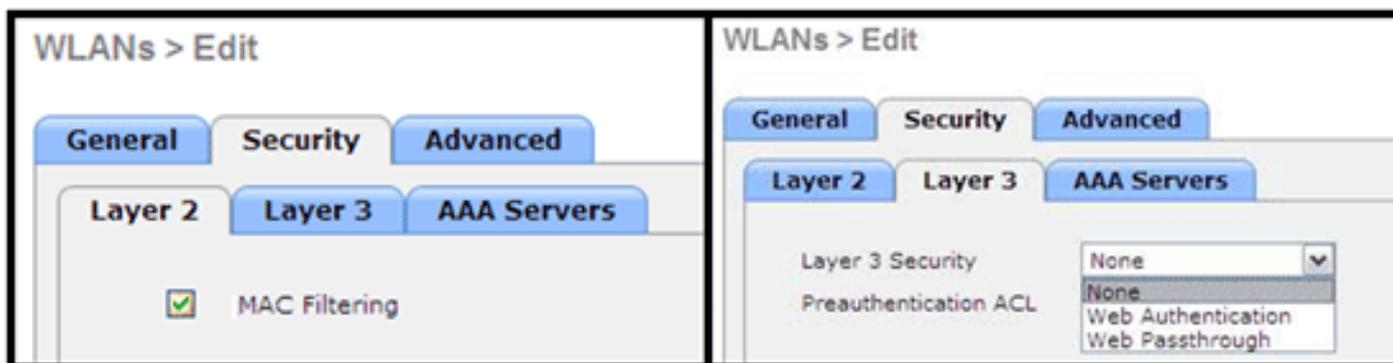
注：セキュリティ設定では、サポートされていない機能が許可されることに注意してください。
適切な設定の例を次の図に示します。



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。

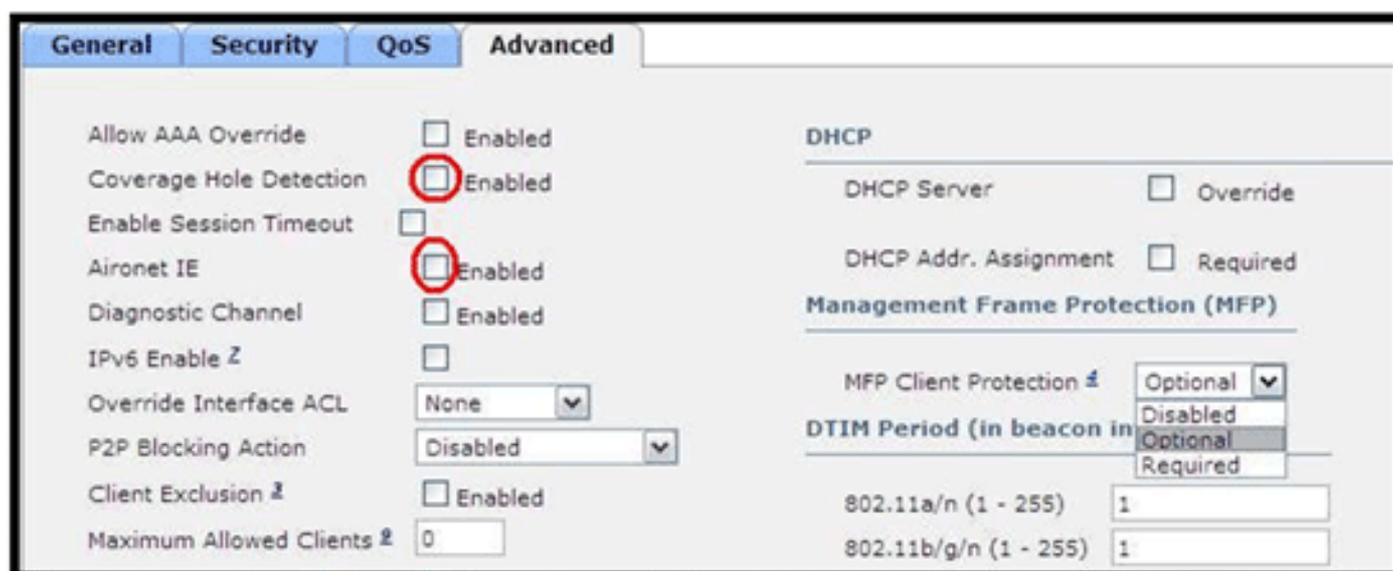
次の図に、[Layer 2] と [Layer 3] の MAC フィルタリングの設定を示します。



QoS 設定を管理します。

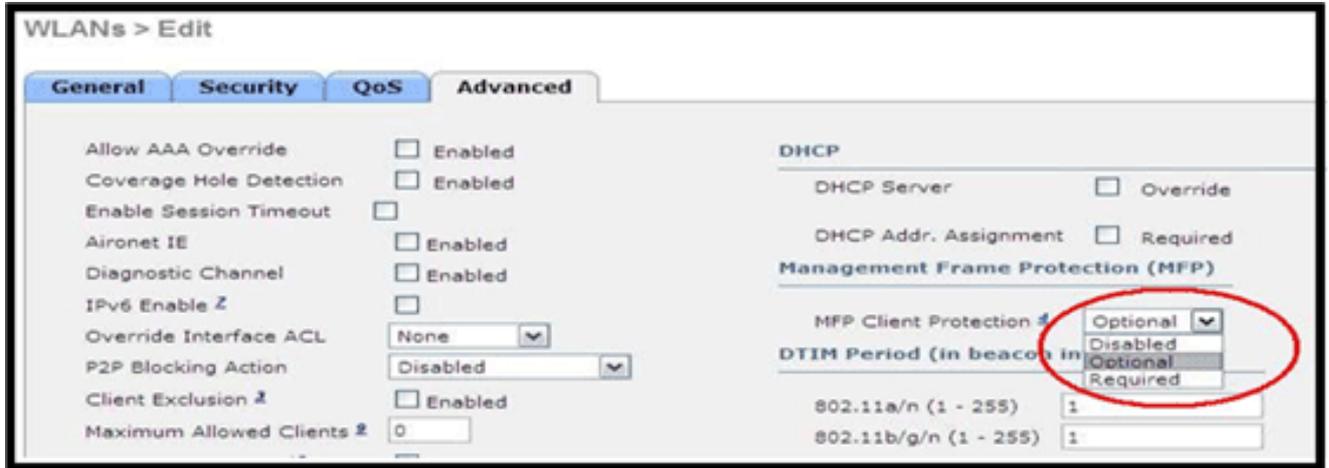


拡張設定も管理します。

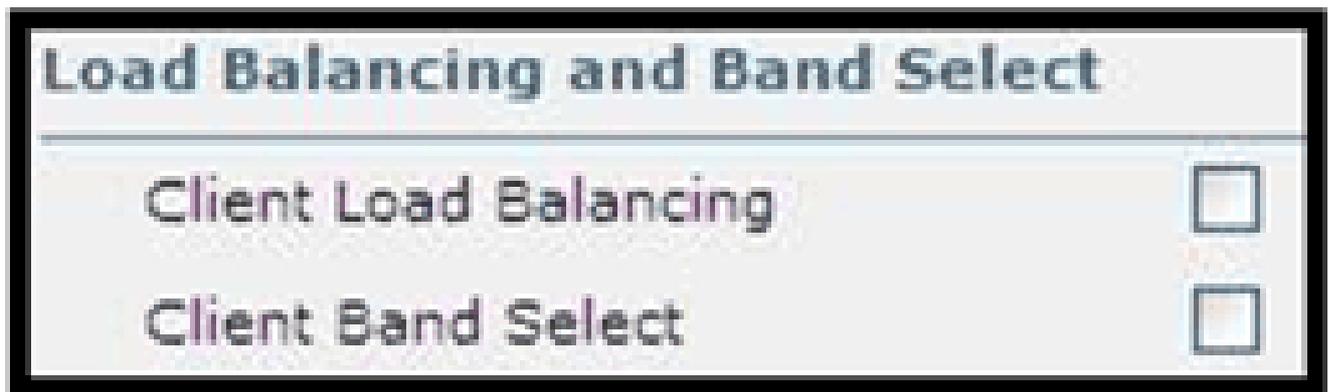


注：

- [Coverage Hole Detection] を有効にしないでください。
- [Aironet IE] (IE; Information Elements) は使用されないなので、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

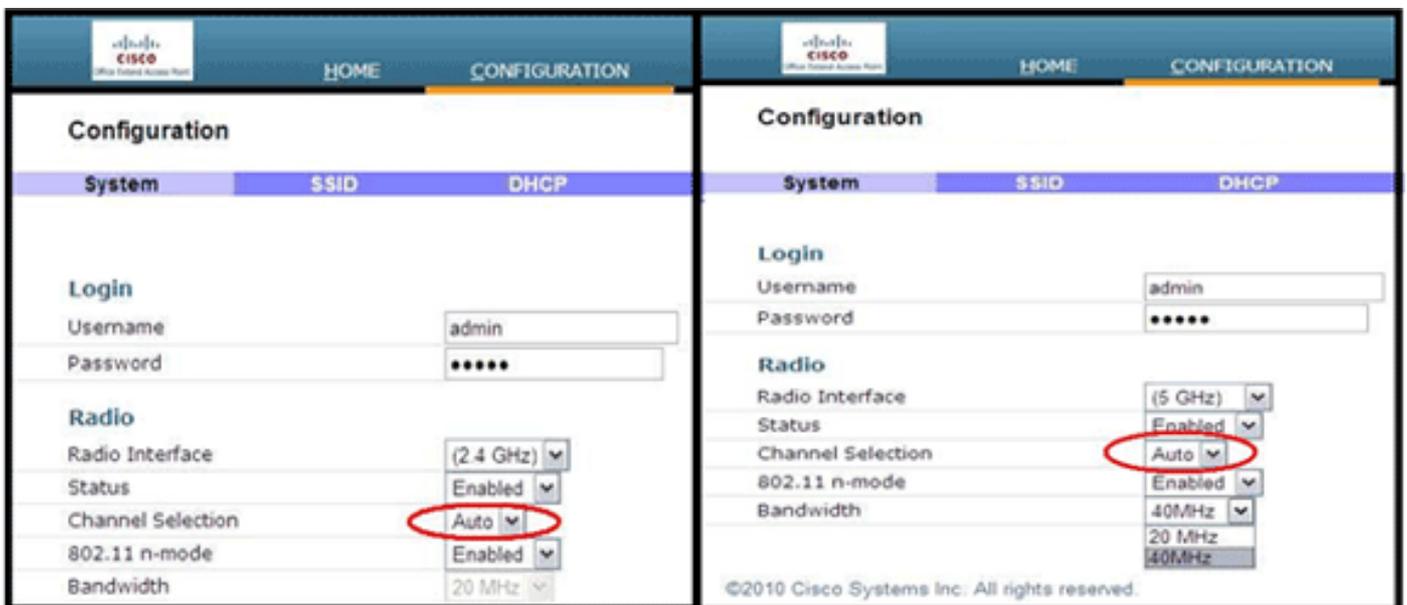
600 シリーズの無線は、ワイヤレス LAN コントローラではなく、600 シリーズのローカル GUI で管理されます。

スペクトラム チャン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ンネルをスキャンし、2.4 GHz および 5.0 GHz のチャンネルを選択します。

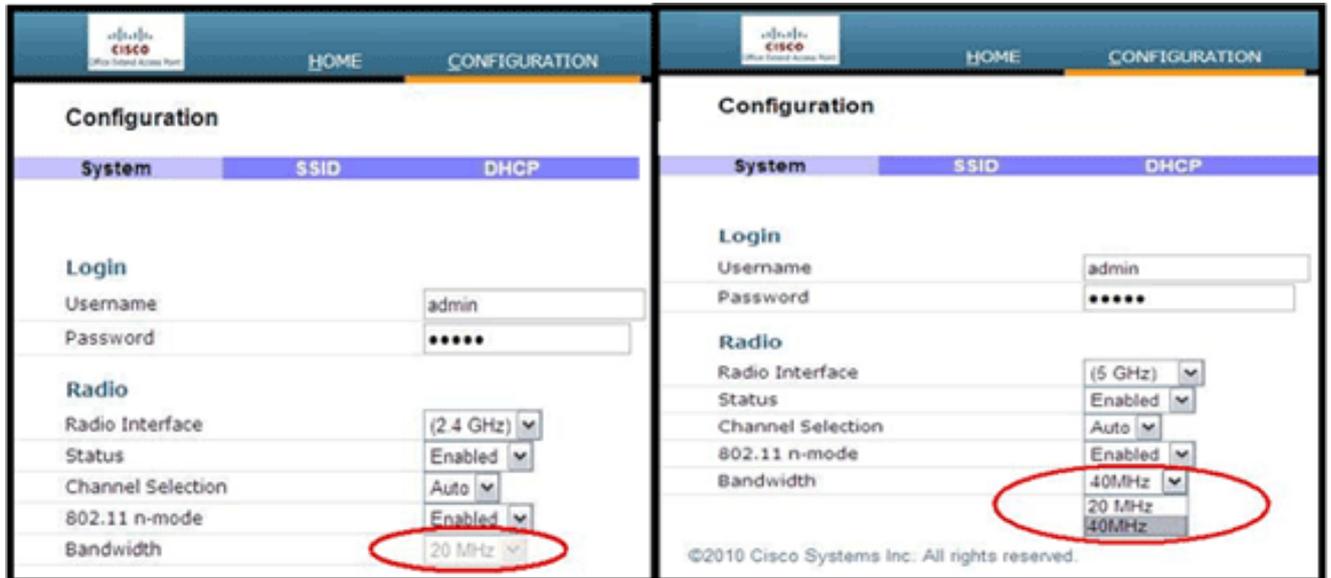
注：ユーザが一方または両方の無線をローカルで無効にする（その無線も社内アクセスに対して無効にする）と、前述したように、RRMと、モニタ、H-REAP、スニファなどの高度な機能は、自宅やテレワーカーが使用する場所に配置されたCisco Aironet 600シリーズOEAPの機能では利用できません。

5.0 GHz のチャン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 (チャンネルボンディング) 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>
```

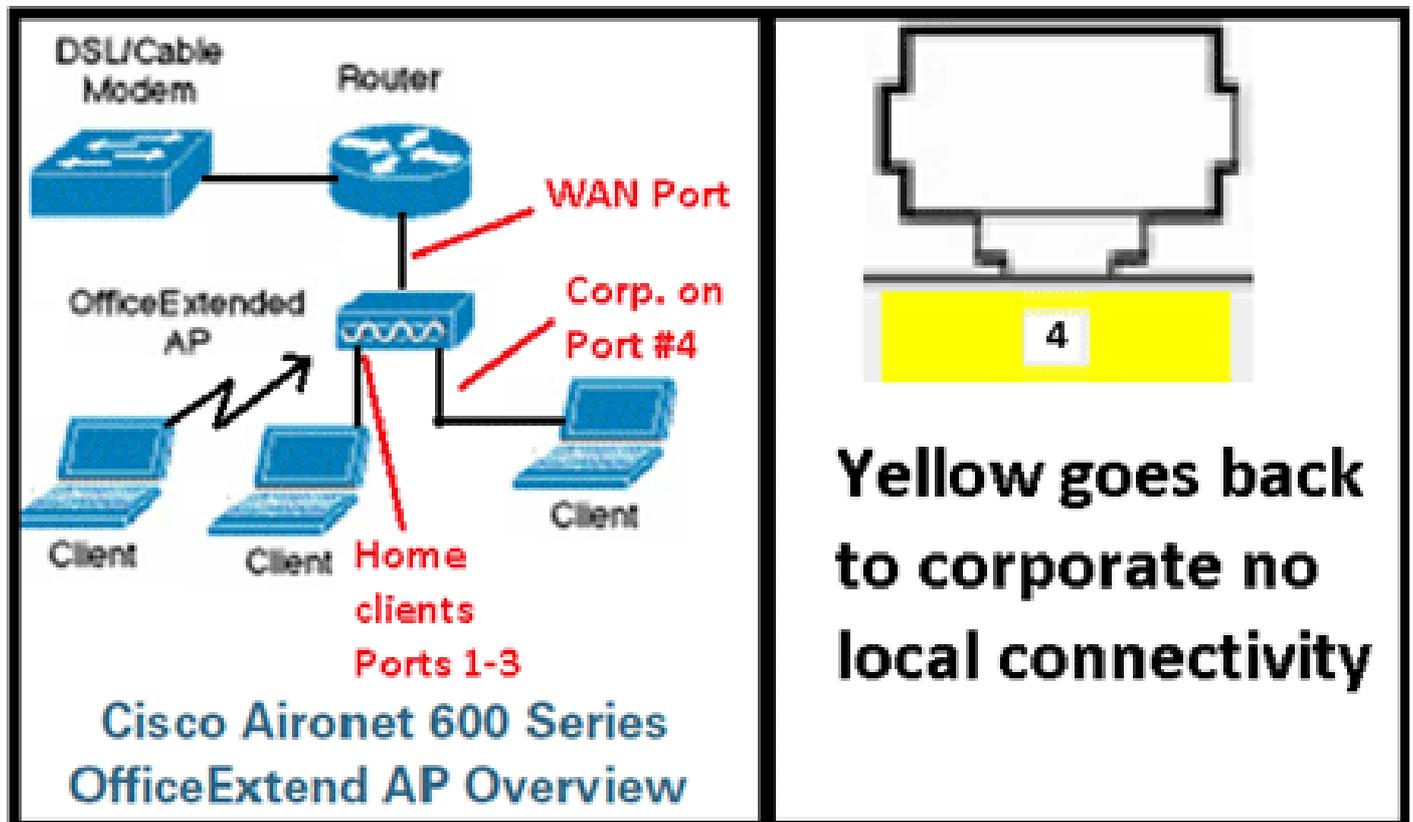
```
config remote-lan enable <remote-lan-id>
```

`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。



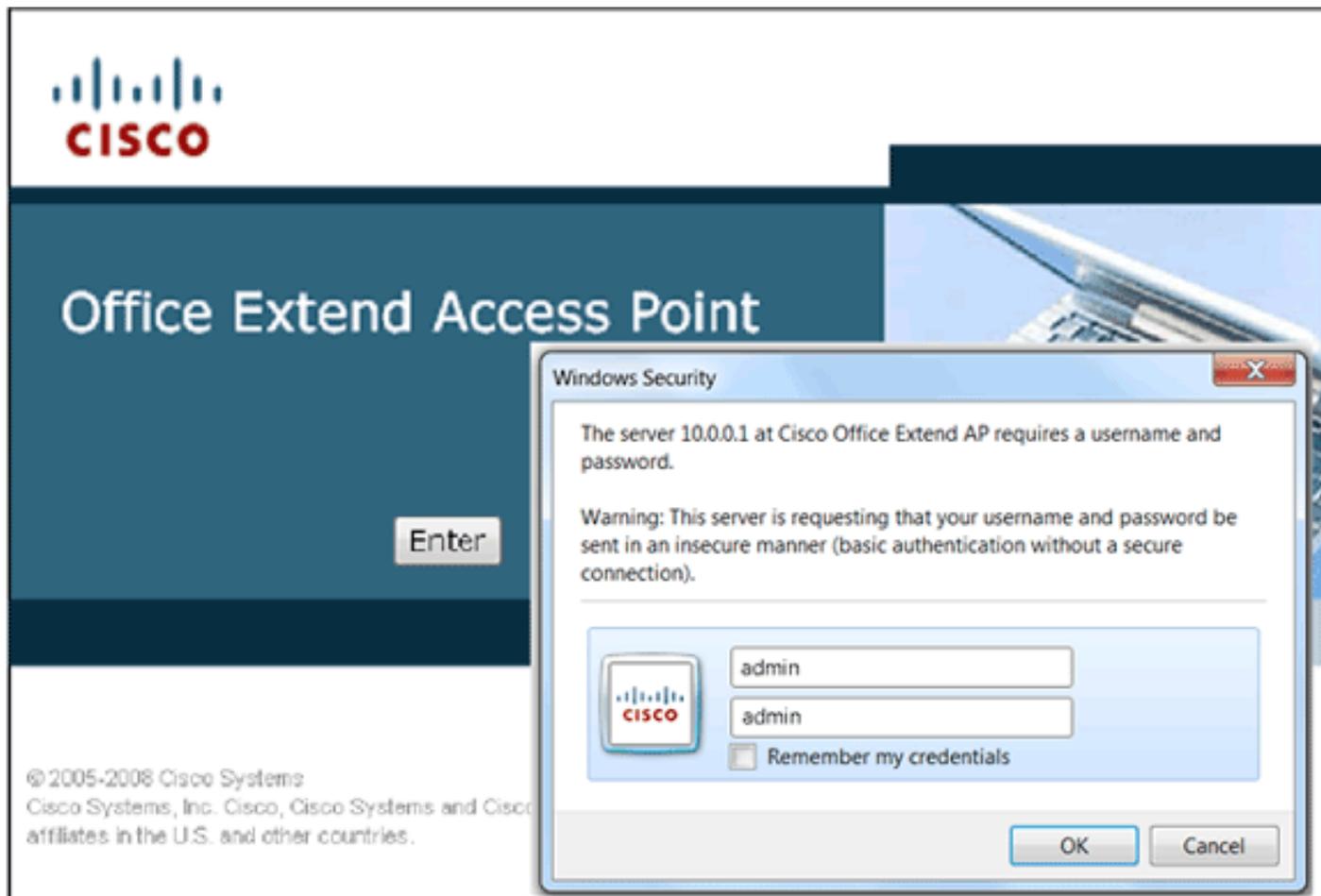
Cisco Aironet 600 シリーズ OEAP のデフォルトの DHCP スコープは 10.0.0.x であるため、アド

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。

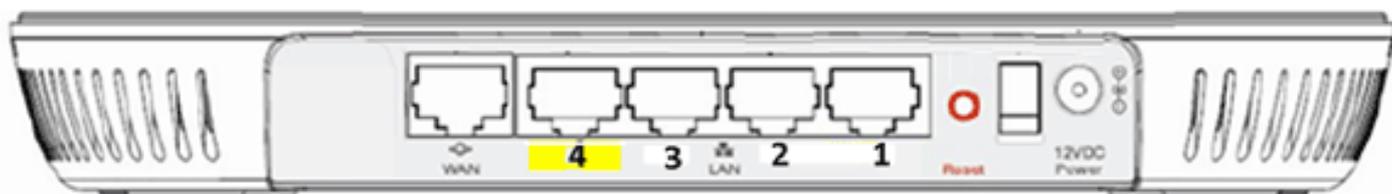
注：これは、ユーザ名およびパスワードとしてCiscoを使用したAP1040、1130、1140、および3502iとは異なります。

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。

The screenshot shows the Cisco Configuration page with the following details:

- Navigation: HOME, CONFIGURATION (selected), EVENT_LOG, HELP
- Section: Configuration (with an Apply button)
- Tabs: System, SSID, DHCP, WAN
- Section: Login
 - Username: admin
 - Password: ****
- Section: Radio
 - Radio Interface: 2.4 GHz (with info icon and text: Select Each Radio and Configure Independently)
 - Status: Enabled
 - Channel Selection: Auto
 - 802.11 n-mode: Enabled (with info icon and text: 802.11n is not supported with TKIP-only WPA Encryption)
 - Bandwidth: 20 MHz

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。

The screenshot shows the Cisco Configuration page with the following details:

- Navigation: HOME, CONFIGURATION (selected), EVENT_LOG, HELP
- Section: Configuration (with an Apply button)
- Tabs: System, SSID, DHCP, WAN
- Section: Personal Network
 - Band Selection: 2.4 GHz (with info icon and text: Select Each Radio and Configure SSID Individually)
 - Enabled:
 - Broadcast:
 - SSID: EVORA24 (with info icon and text: Personal SSID should be different from Corporate SSID)
- Section: MAC Filter
 - Enabled:
 - Allowed MAC Addresses: e.g. 00:1D:E0:34:E2:1F
 - Table with 3 rows and 2 columns for MAC addresses.

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 を有効にするパスワード、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。

Security	
WPA-PSK	Disabled ▼
WPA2-PSK	Enabled ▼
WEP Encryption	Disabled ▼
WPA Encryption	AES ▼
WPA passphrase	●●●●● Click here to display
Network Key 1	
Network Key 2	
Network Key 3	
Network Key 4	
Current Network Key	2 ▼

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。

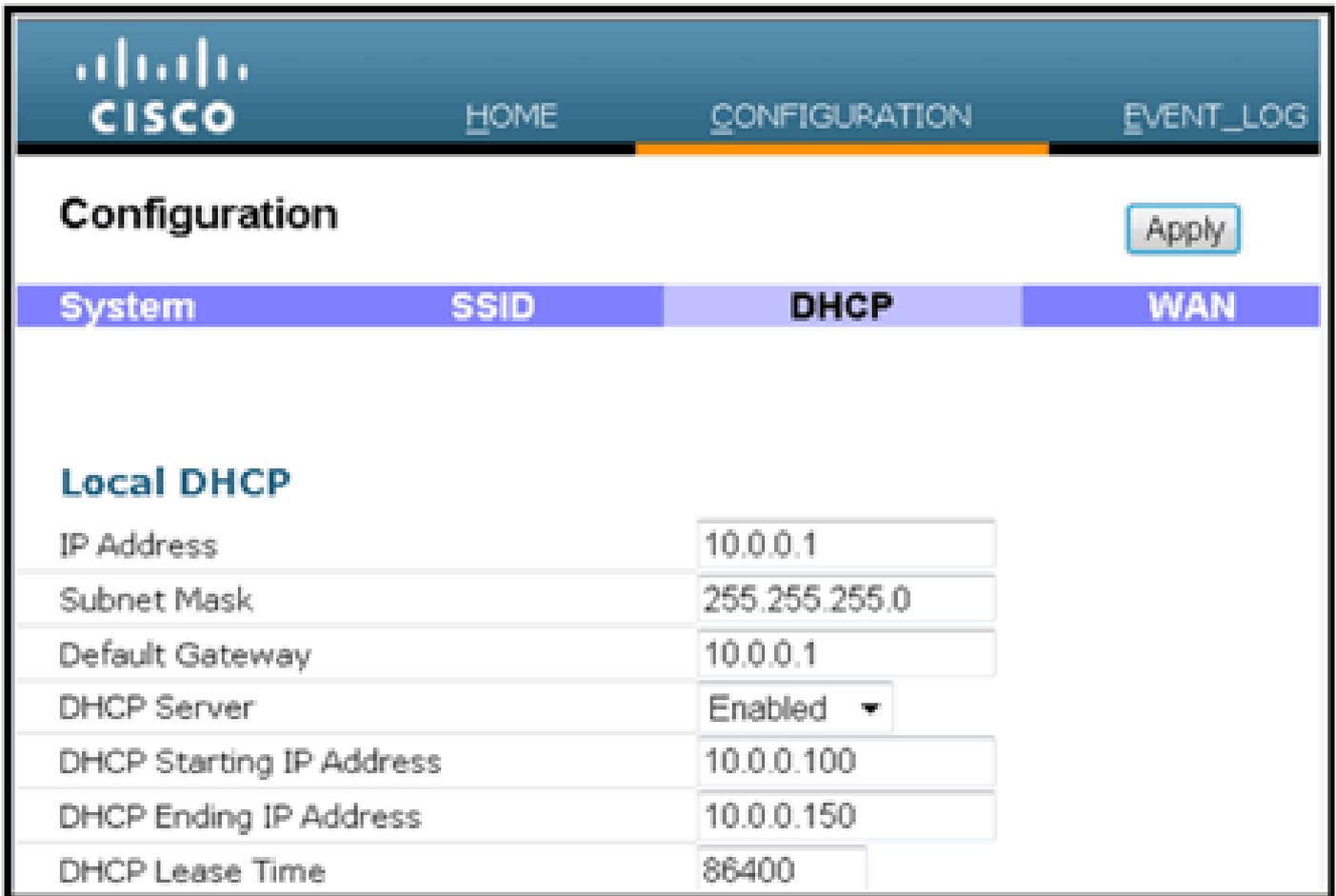
ホーム ルータを接続しなくても本製品は機能しますが、前述の理由からこのように配置しないことをお勧めします。一部のモデムに直接接続する場合に互換性の問題が生じることがあります。

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せん。

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

必要があります。

次の図に、DHCP スコープの設定を示します。



The screenshot shows the Cisco Aironet 600 Series OEAP configuration interface. The top navigation bar includes 'HOME', 'CONFIGURATION', and 'EVENT_LOG'. The 'CONFIGURATION' tab is active. Below the navigation bar, there is a 'Configuration' section with an 'Apply' button. The main content area is divided into four tabs: 'System', 'SSID', 'DHCP', and 'WAN'. The 'DHCP' tab is selected, displaying the 'Local DHCP' configuration table.

System	SSID	DHCP	WAN
Local DHCP			
IP Address		10.0.0.1	
Subnet Mask		255.255.255.0	
Default Gateway		10.0.0.1	
DHCP Server		Enabled ▾	
DHCP Starting IP Address		10.0.0.100	
DHCP Ending IP Address		10.0.0.150	
DHCP Lease Time		86400	

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。

CISCO HOME CONFIGURATION EVENT_LOG

Configuration

Apply

System SSID DHCP **WAN**

Controller

This is where you enter the IP address of the DMZ OEAP controller

IP Address **YYYY**

Uplink IP Configuration

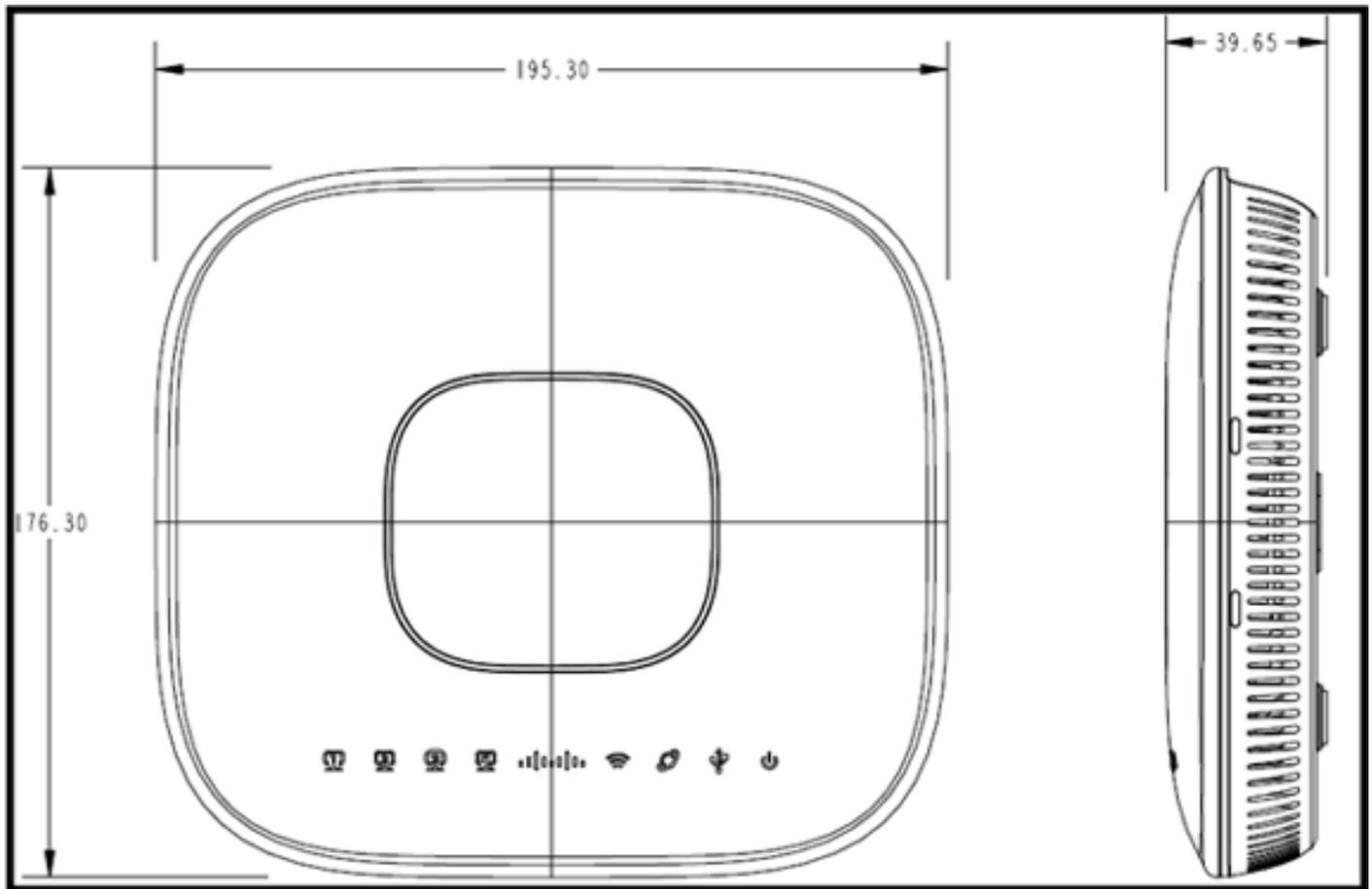
Example IP

Static IP

Domain Name	gateway.2wire.net
IP Address	192.168.1.68
Subnet Mask:	255.255.255.0
Default Gateway	192.168.1.254
DNS Server	192.168.1.254

OEAP-600 アクセス ポイント ハードウェアの設置

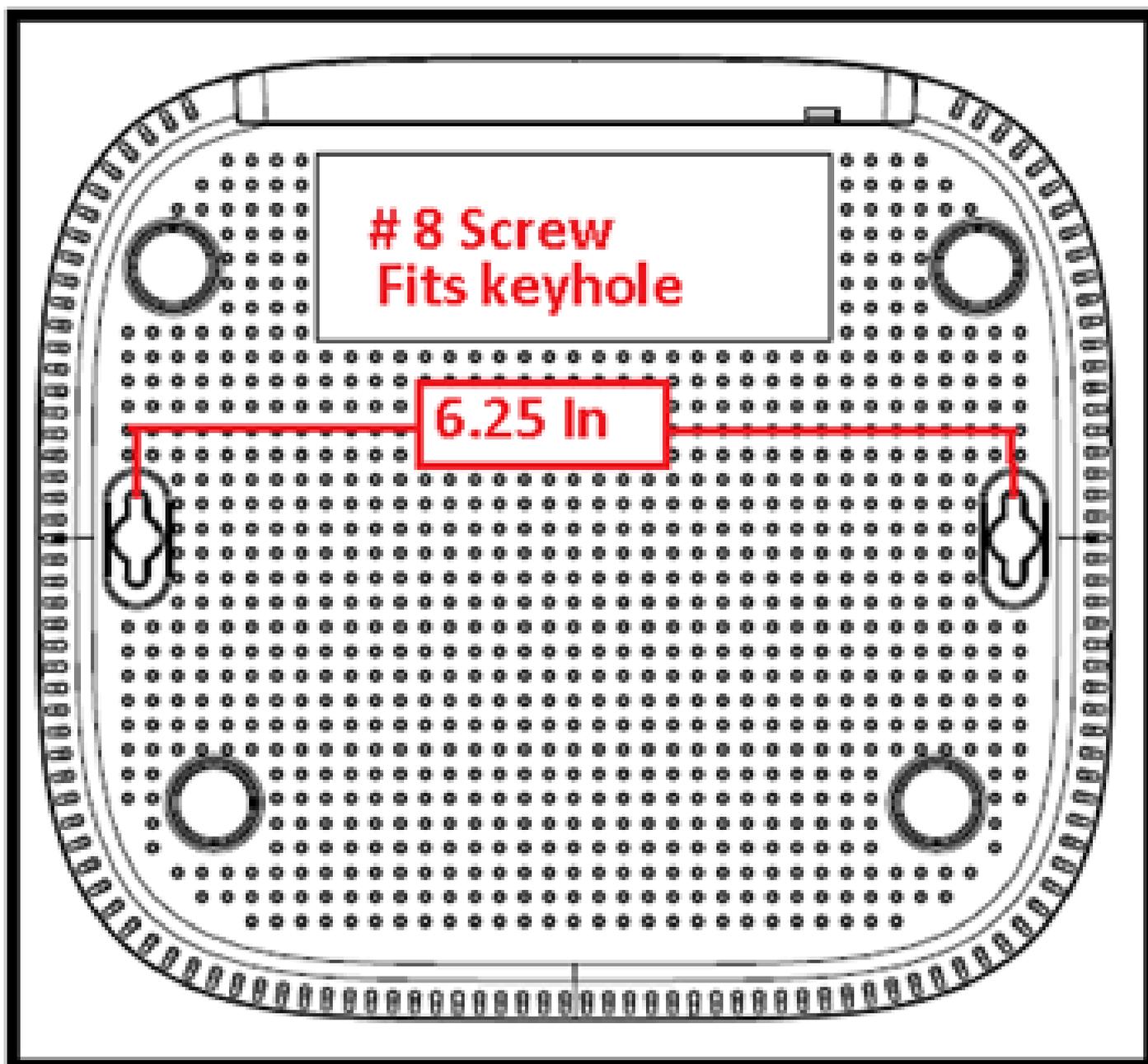
次の図に、Cisco Aironet 600 シリーズ OEAP の外観を示します。



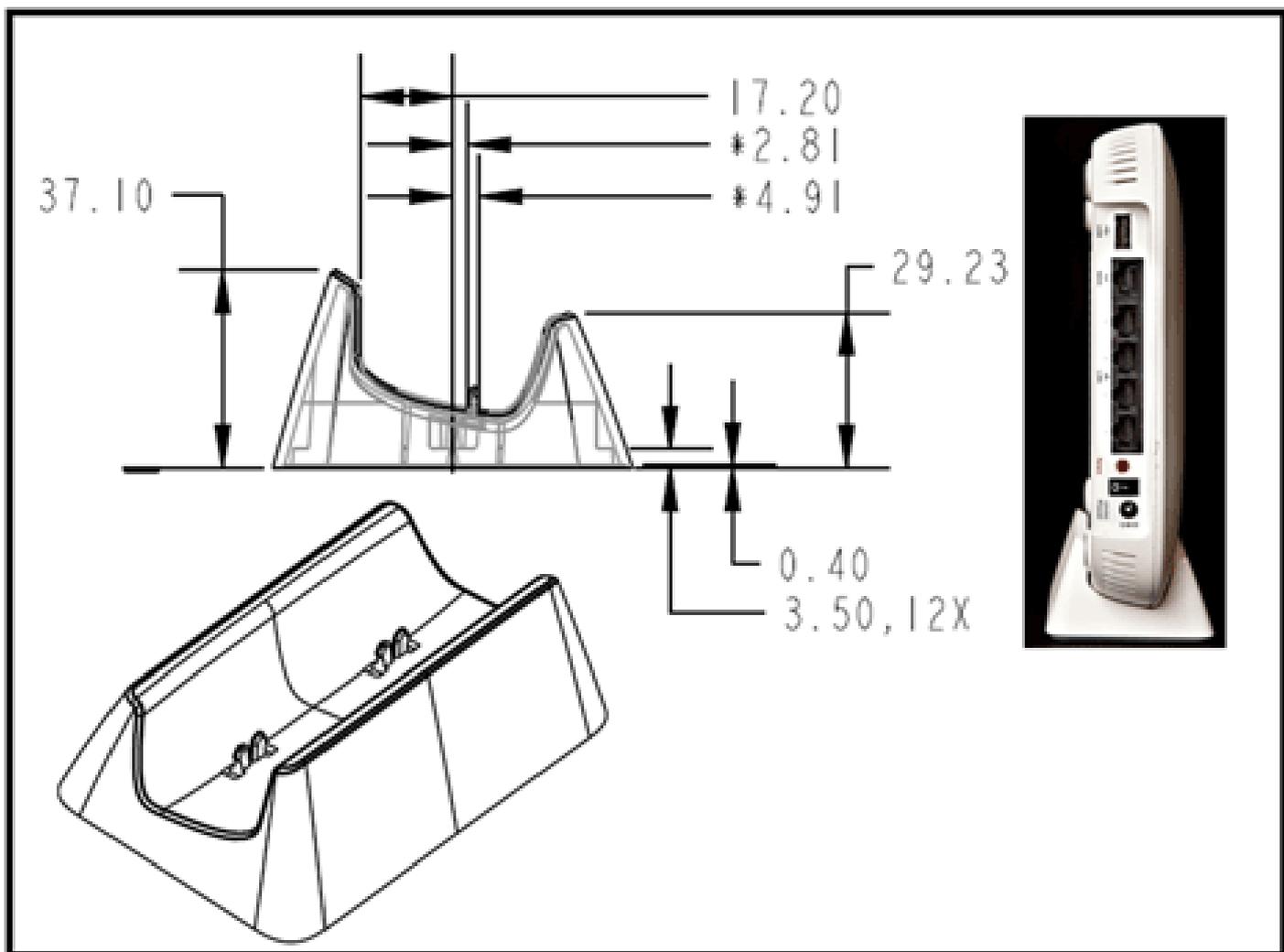
この AP は机の上に置くように設計されており、ゴム製の脚が付いています。壁に取り付けたり、付属のクレードルを使用して縦置きにしたりできます。使用するユーザにできるだけ近い場所に AP を設定してください。大きな金属面のある場所（金属製の机の上や大きな鏡の近く）には設置しないでください。AP とユーザの間にある壁や障害物が多いほど信号強度が低くなり、パフォーマンスが低下する可能性があります。

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。



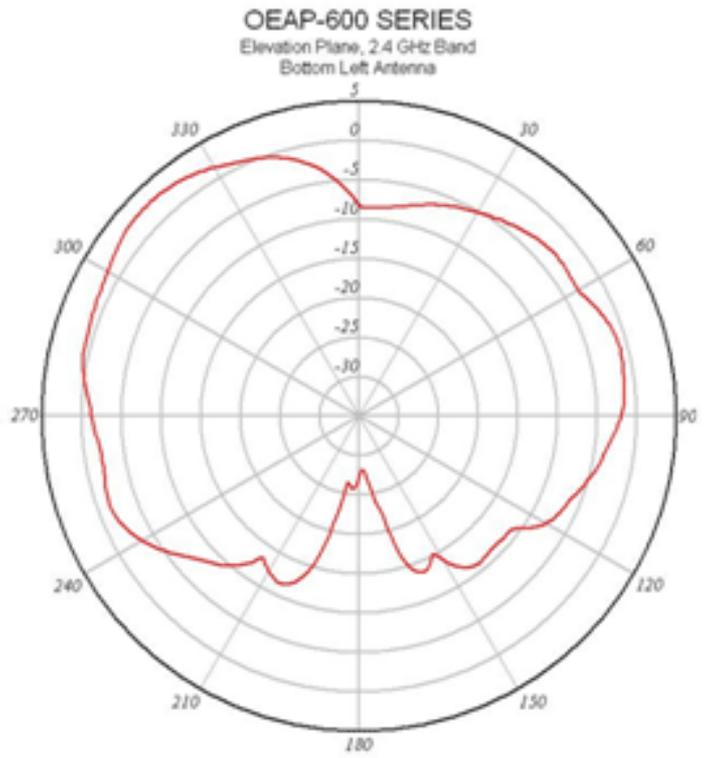
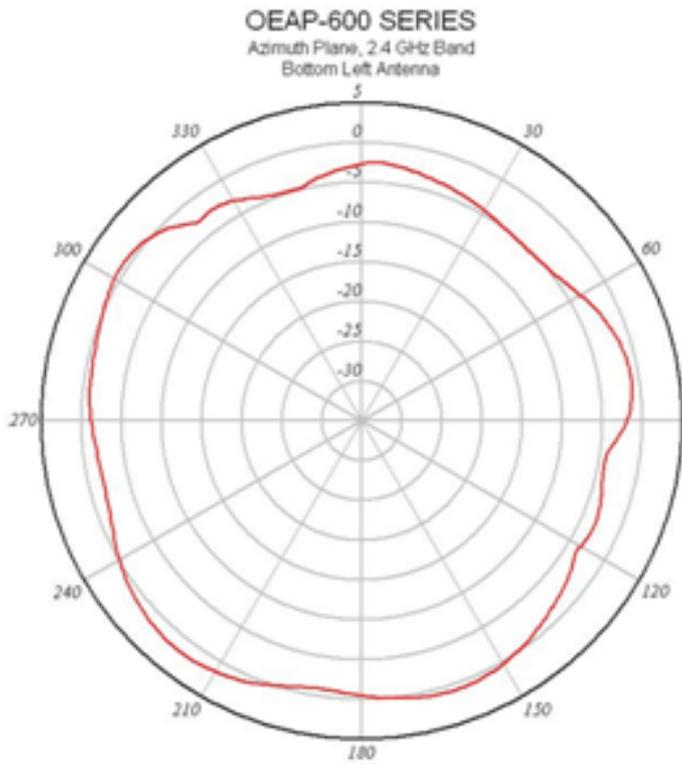
Cisco Aironet 600 シリーズ OEAP のアンテナは、AP の両端に位置しています。金属でできた物体や障害物の近くに AP を設置しないように十分注意してください。このように設置すると、信号に指向性が生じるか、または信号が低下する恐れがあります。アンテナ ゲインは両方の帯域で約 2 dBi であり、360 度パターンで放射するように設計されています。ランプシェードのない電球のように、すべての方向に放射することを目的としています。AP をランプとして考え、ユーザに近い場所に設置してください。

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。

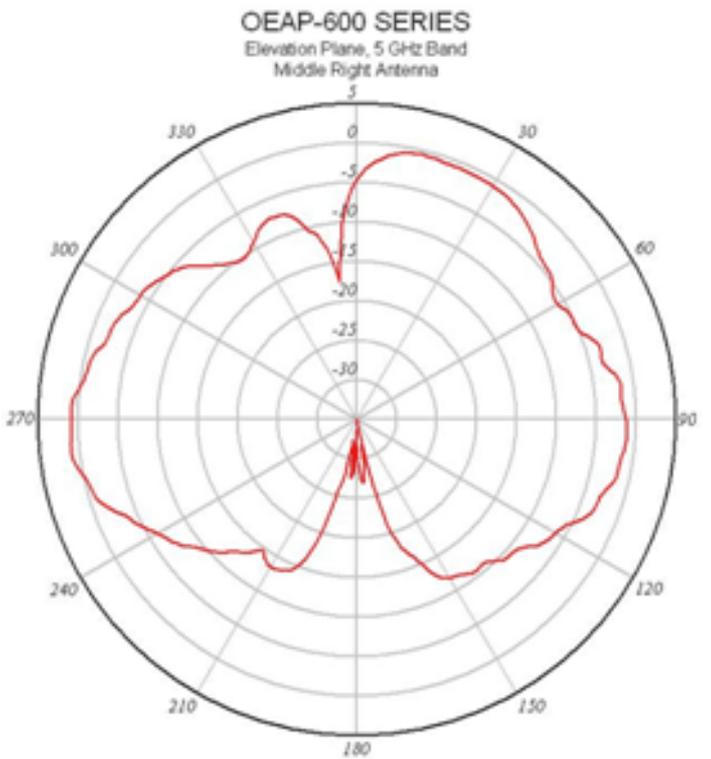
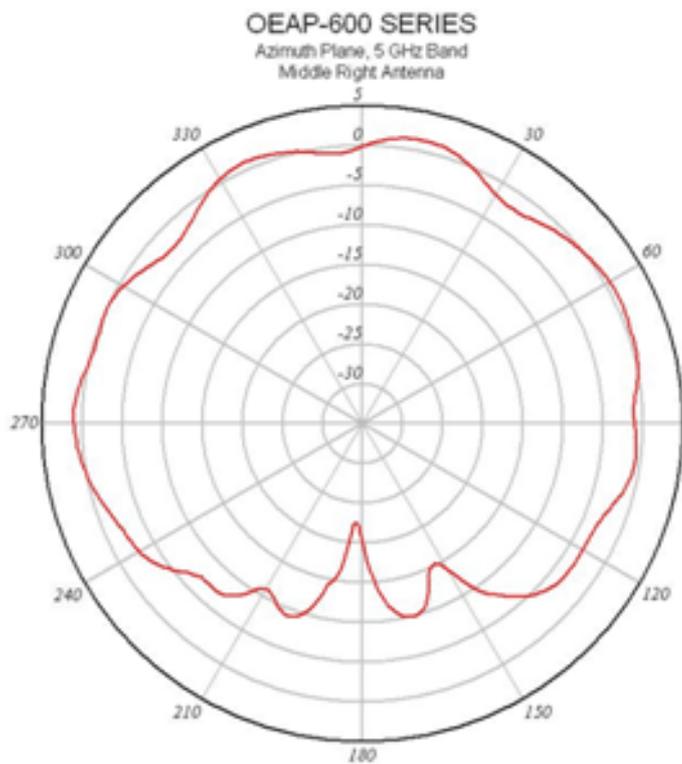
アクセス ポイントには 6 つのアンテナが内蔵されています (帯域幅あたり 3 つのアンテナ)。



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

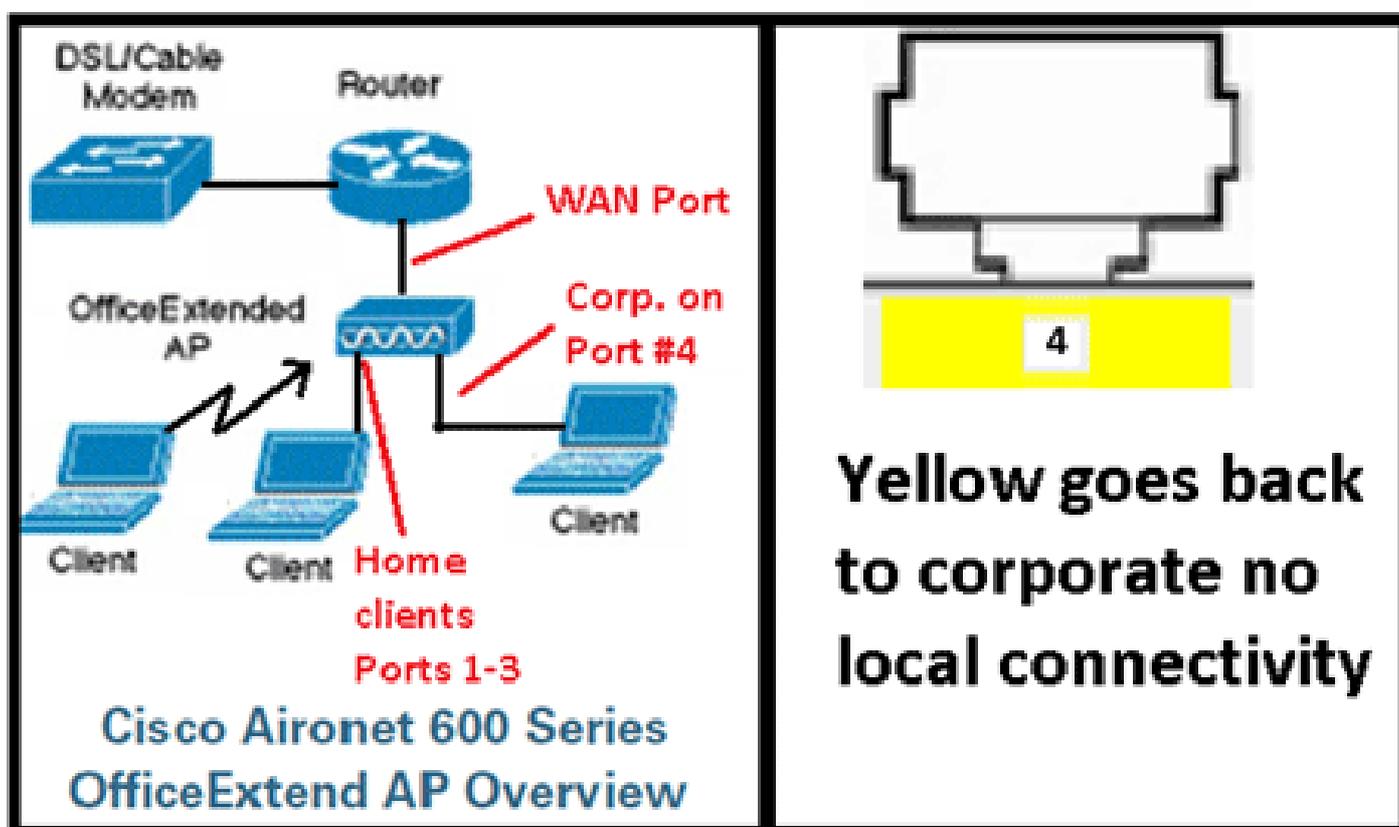
かを確認してください。デフォルトのユーザ名とパスワードは admin です。

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。

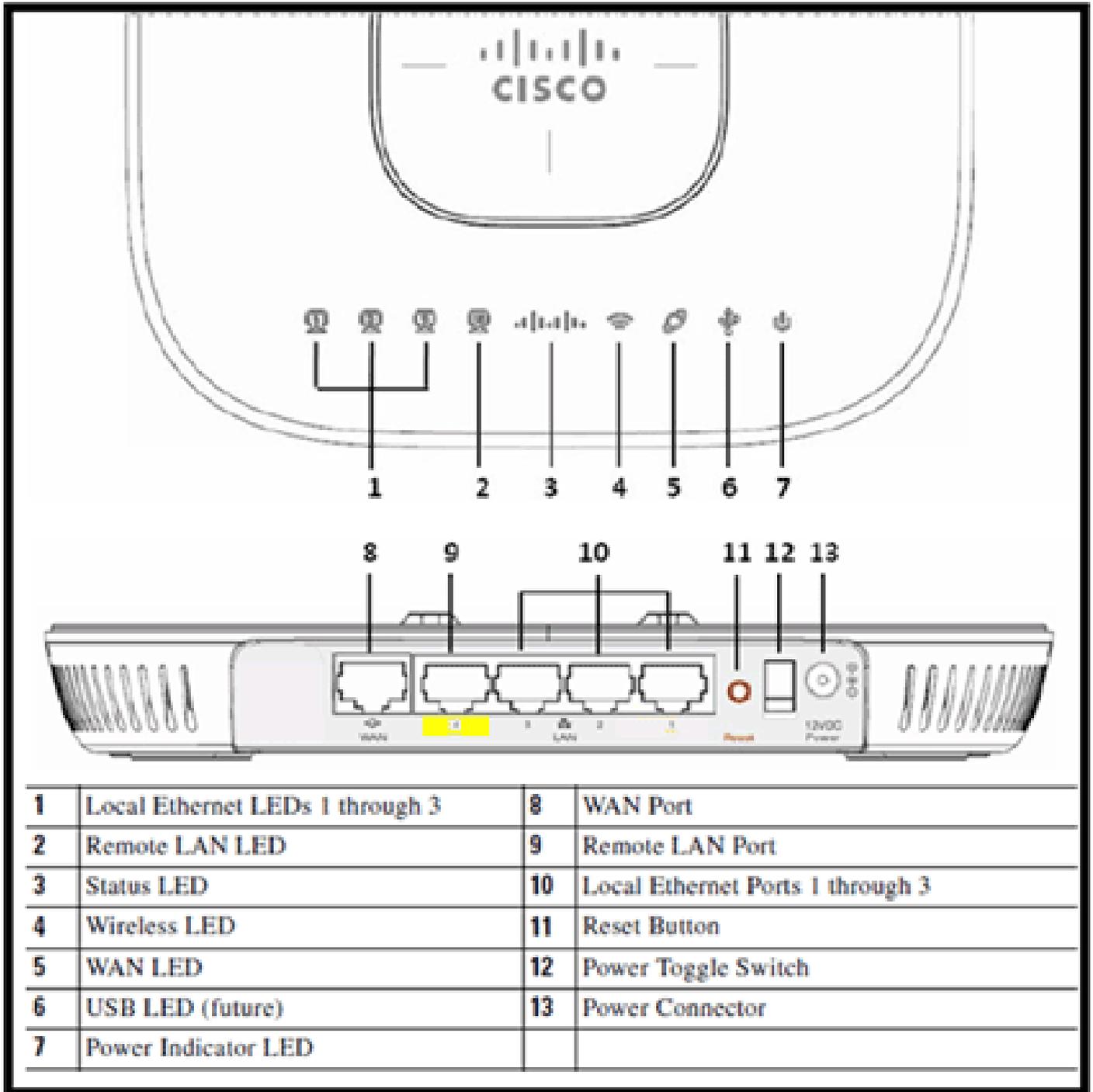
注：設定の目的でデバイスを参照するために、企業ポート#4（黄色）を使用することはできません。リモート LAN が設定されていない場合、これは実質的には「利用不可のポート」です。会社へのトンネルが確立されます（会社への有線接続に使用）。

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。

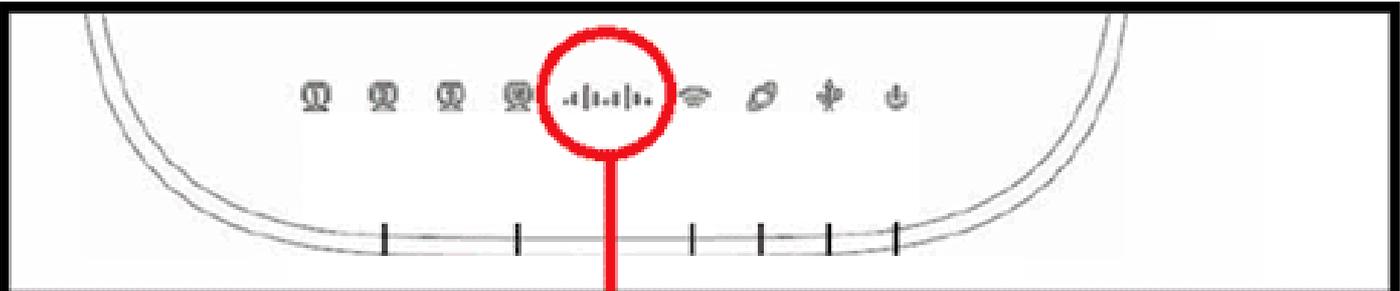


Cisco Aironet 600 シリーズ OEAP がコントローラに接続できない場合は、次の事項を確認することをお勧めします。

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 ログ LED のステータスを示します。



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。

The screenshot shows the Cisco Aironet 600 Event Log interface. At the top, there is a navigation bar with 'HOME', 'CONFIGURATION', 'EVENT_LOG', and 'HELP' tabs. The 'EVENT_LOG' tab is selected. Below the navigation bar, the title 'Event Log' is displayed. The main area contains a scrollable list of log entries. The entries show a sequence of events starting with a discovery request at 06:31:59.393, followed by a discovery response at 06:31:59.394, and a join request at 14:31:45.620. The process ends with a 'Duplicate sequence number 240 in request.' error at 14:32:46.422.

```
*Nov 12 06:31:59.393:
SENDING DISCOVERY REQUEST wtpStartAcDiscovery:1298, Controller : IP Address 0xc0a801e1
*Nov 12 06:31:59.394: Discovery Response from -1062731295
*Nov 12 06:31:59.411: Dot11 binding decode: Discovery Response
*Nov 12 06:32:09.391: Selected HWAR 'Evora-3C' (index 0).
*Nov 12 06:32:09.391: Ap mgr count=1
*Nov 12 06:32:09.391: Go join a capwap controller
*Nov 12 06:32:09.392: Choosing AP Mgr with index 0, IP = 0xc0a801e1, load = 0..
*Nov 12 06:32:09.392: Synchronizing time with AC time.
*Nov 11 14:31:45.000: CAPWAP State: DTLS Setup.
*Nov 11 14:31:45.619: Dtls Session Established with the AC -1062731295,port= 5246
*Nov 11 14:31:45.620: CAPWAP State: Join.
*Nov 11 14:31:45.620: Join request: version=117469704
*Nov 11 14:31:45.621: Join request: hasMaximum Message Payload
*Nov 11 14:31:45.621: Dot11 binding encode: Encoding join request
*Nov 11 14:31:45.622: Sending Join Request Path MTU payload, Length 1376

*Nov 11 14:31:45.625: Join Response from -1062731295
*Nov 11 14:31:45.626: PTHU : Setting MTU to : 1485

*Nov 11 14:31:45.626: Dot11 binding decode: Join Response
*Nov 11 14:31:45.627: Starting Post Join timer
*Nov 11 14:31:45.627: CAPWAP State: Image Data.
*Nov 11 14:31:45.628: Stopping Post Join Timer and Starting HeartBeat Timer
*Nov 11 14:31:45.628: Image Data Request sent to -1062731295
*Nov 11 14:31:45.630: Image Data Response from -1062731295
*Nov 11 14:31:45.630: Starting image download.....
*Nov 11 14:31:52.467: Successfully downloaded image
*Nov 11 14:32:46.398: Rebooting....
*Nov 11 14:32:46.422: Duplicate sequence number 240 in request.
```

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。

Event log 1

WAN port has not obtained IP address, otherwise it will be shown here.

AP Mac address

Base Radio MAC is 00:22:BD:DA:B6:00

```

*Jan 01 08:00:05.420: eth0  Linkencap:Ethernet HWaddrC0:C1:C0:05:48:86
*Jan 01 08:00:05.420:      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
*Jan 01 08:00:05.420:      RX packets:1 errors:0 dropped:0 overruns:0 frame:0
*Jan 01 08:00:05.420:      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
*Jan 01 08:00:05.420:      collisions:0 txqueuelen:100
*Jan 01 08:00:05.421:      RX bytes:64 (64.0 b) TX bytes:0 (0.0 b)
*Jan 01 08:00:05.421:      Interrupt:4 Base address:0x2000
*Jan 01 08:00:05.444: eth1  Linkencap:Ethernet HWaddr00:22:BD:DA:B6:07
*Jan 01 08:00:05.444:      UP BROADCAST RUNNING ALLMULTI MULTICAST MTU:1500 Metric:1
*Jan 01 08:00:05.444:      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
*Jan 01 08:00:05.444:      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
*Jan 01 08:00:05.444:      collisions:0 txqueuelen:100
*Jan 01 08:00:05.444:      RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
*Jan 01 08:00:05.445:      Interrupt:3 Base address:0x1000
*Jan 01 08:00:05.467: Kernel IP routing table
*Jan 01 08:00:05.467: Destination Gateway Genmask Flags Metric Ref Use Iface
*Jan 01 08:00:05.467: 127.0.0.0 * 255.0.0.0 U 0 0 0 lo
*Jan 01 08:00:05.489: IP address HW type Flags HW address Mask Device
*Jan 01 08:00:05.540: oep_mwar_ipaddr= Y.Y.Y.Y
*Jan 01 08:00:07.074: Subject: C=US, ST=California, L=San Jose, O=CISCO, OU=WNBU, CN=OEAP602-C0C1C0054886/emailAd
  
```

Controller IP address configured in local GUI

certificate

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

The screenshot shows the Cisco Aironet 600 GUI. The main content area is titled 'AP Join Stats' and displays a table of AP join events. A search box is overlaid on the table, with a red box around it and a red arrow pointing to the 'MAC Address' field. The table columns include Base Radio MAC, AP Name, Status, Ethernet MAC, IP Address, and Last Join Time. The search box contains the following text:

```

Search AP
MAC Address 
AP Name 
Find
  
```

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 ハンドシェイ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もあります。

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。

Event log 2

```
*Jan 01 08:00:07.093: Build version 7.0.112.66 (compiled Feb 19 2011 at 16:29:58).
*Jan 01 08:00:08.975: CAPWAP State: Init.
*Jan 01 08:00:09.009: CAPWAP State: Discovery.
*Jan 01 08:00:09.042: Starting Discovery.
*Jan 01 08:00:09.044: CAPWAP State: Discovery.
*Jan 01 08:00:09.193: Discovery Request sent to Y.Y.Y.Y with discovery type set to 1
*Jan 01 08:00:09.194: Discovery Request sent to Y.Y.Y.Y with discovery type set to 1
*Jan 01 08:00:09.194:
SENDING DISCOVERY REQUEST wtpStartAcDiscovery:1338, Controller Cisco_7d:88:00: IP Address
*Jan 01 08:00:09.195: Discovery Request sent to Y.Y.Y.Y with discovery type set to 0
*Jan 01 08:00:09.256: Discovery Response from Y.Y.Y.Y
*Jan 01 08:00:09.272: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.272: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
*Jan 01 08:00:09.272: Discovery Response from Y.Y.Y.Y
*Jan 01 08:00:09.273: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.273: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
*Jan 01 08:00:09.273: Discovery Response from Y.Y.Y.Y
*Jan 01 08:00:09.274: Dot11 binding decode: Discovery Response
*Jan 01 08:00:09.274: wtpDecodeDiscoveryResponse Discovery Latency: 0, WLC: IP= Y.Y.Y.Y , name=Cisco_7d:88:00, index
*Jan 01 08:00:12.133: Dropping dtls packet since session is not established. ab462383, 147e, c0a80121, 147e, 0
*Jan 01 08:00:19.182: Selected MWAR 'Cisco_7d:88:00' (index 0).
*Jan 01 08:00:19.183: Selected MWAR 'Cisco_7d:88:00' (index 0).
*Jan 01 08:00:19.183: Ap mgr count=1
*Jan 01 08:00:19.183: Go join a capwap controller
*Jan 01 08:00:19.183: Choosing AP Mgr with index 0, IP = Y.Y.Y.Y , load=151.
*Jan 01 08:00:19.183: Synchronizing time with AC.
*Feb 19 23:33:56.000: CAPWAP State: DTLS Setup.
*Feb 19 23:34:16.813: Dtls Session Established with the AC: Y.Y.Y.Y , port= 5246
```

Discovery Request sent
If AP can not get IP address,
then Discovery Req. will not be sent

Discovery resp. received from
controller. If no response from
controller, then need to check
whether controller
is accessible

Selected controller to join, timestamp synced to the controller

DTLS handshaking with the controller
completed. If certificate has problem, then
the failure will happen here

Event log 3

```
*Feb 19 23:34:16.813: CAPWAP State: Join.
*Feb 19 23:34:16.814: Join request: version=7.0.114.76

*Feb 19 23:34:16.815: Join request: hasMaximum Message Payload
*Feb 19 23:34:16.815: Dot11 binding encode: Encoding join request
*Feb 19 23:34:16.815: Sending Join Request Path MTU payload, Length 1376

*Feb 19 23:34:16.887: Join Response from Y.Y.Y.Y
*Feb 19 23:34:16.888: PTMU : Setting MTU to : 1485

*Feb 19 23:34:16.888: Dot11 binding decode: Join Response
*Feb 19 23:34:16.889: Starting Post Join timer
*Feb 19 23:34:16.890: CAPWAP State: Image Data.
*Feb 19 23:34:16.890: Controller Version: 7.0.114.76
*Feb 19 23:34:16.890: AP Version: 7.0.114.76
*Feb 19 23:34:16.891: CAPWAP State: Configure.
*Feb 19 23:34:16.891: Dot11 binding encode: Encoding configuration status request.
*Feb 19 23:34:16.893: lwapp_encode_ap_reset_button_payload: reset button state off
*Feb 19 23:34:16.895: Configuration Status sent to Y.Y.Y.Y
*Feb 19 23:34:17.019: Configuration Status Response from Y.Y.Y.Y
*Feb 19 23:34:17.022: CAPWAP State: Run.
*Feb 19 23:34:17.022: Dot11 binding encode: Encoding change state event request.
*Feb 19 23:34:17.023: CAPWAP State: Run.
```

Join Resp. from controller
If AP is not added to AAA server,
this step will fail.

Controller and AP have same version
SW, no image download is need. When
controller is upgraded to new version
SW, image download will happen.

Capwap configuration completes

Event log 4

```
*Feb 19 23:34:17.023: CAPWAP moved to RUN state stopping post join timer
*Feb 19 23:34:17.399: capwapWtpDlForwarding() returned 1
*Feb 19 23:34:17.602: capwapWtpDlForwarding() returned 1
*Feb 19 23:34:17.762: Change State Event Response from -1421466749
*Feb 19 23:34:17.853: SSID alpha,WLAN ID 1, added to the slot[0], enabled
*Feb 19 23:34:18.045: SSID alpha_phone,WLAN ID 2, added to the slot[0], enabled
*Feb 19 23:34:18.118: Ethernet Backhaul WLAN ID = 3,qos=0
*Feb 19 23:34:18.281: SSID alpha,WLAN ID 1, added to the slot[1], enabled
*Feb 19 23:34:18.522: SSID alpha_phone,WLAN ID 2, added to the slot[1], enabled
```

WLANs are configured for 2.4 GHz Radio

Remote-lan is configured

WLANs are configured for 5 GHz Radio

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可能性があります。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: CAPWAPState: 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、ワ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。

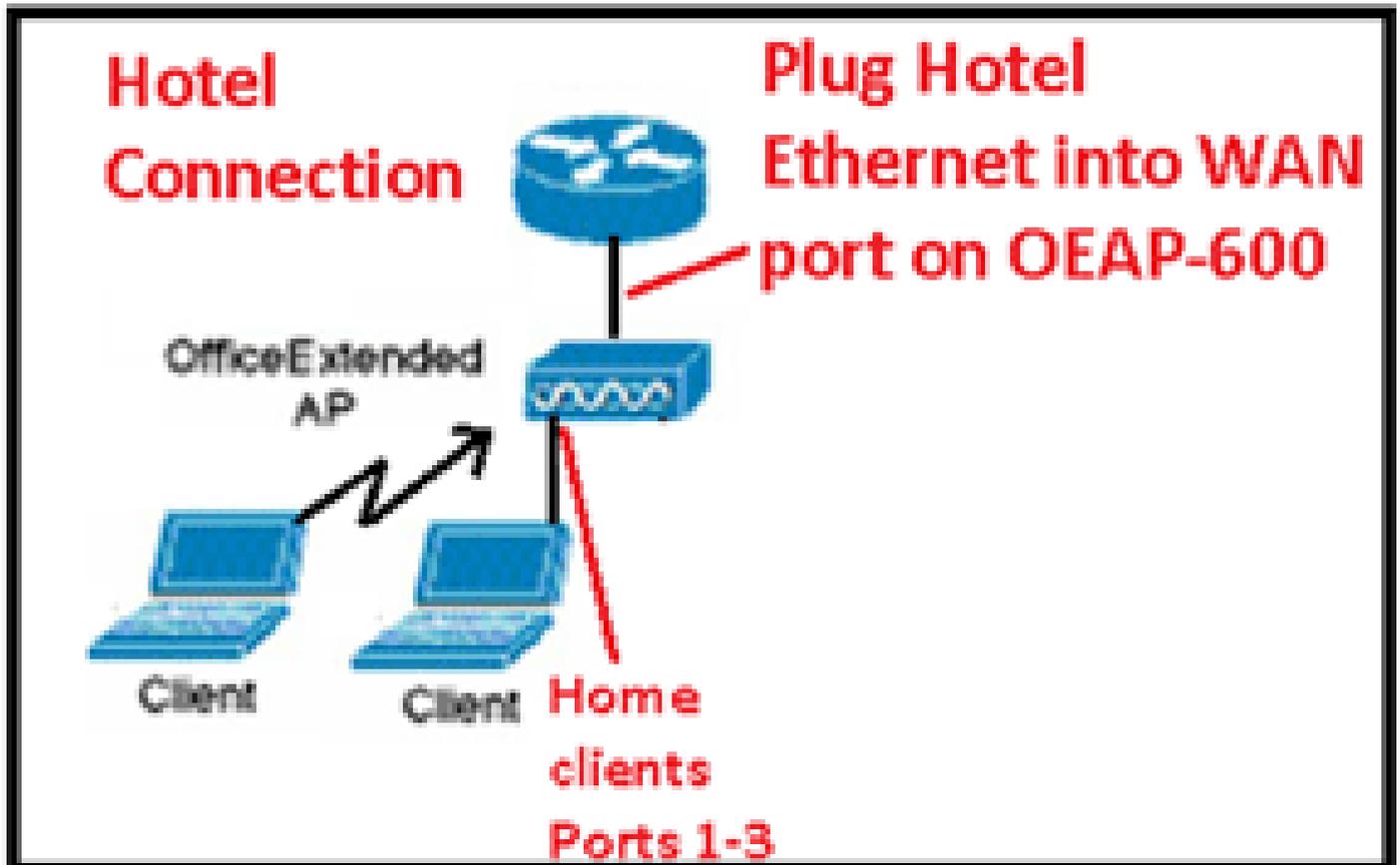
AP のホーム サイドからインターネットに接続すると、DTLS トンネルが確立され、会社の SSID が設定されます。有線ポート #4 がアクティブになります (リモート LAN が設定されていること

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:

```
debugap enable <apname>
```

then:

```
debugap command "evoraTechSupport" <apname> → the information about system and radio slot 0/1
```

```
debugap command "evoraTechSupport 2" <apname> → more info about radio slot 0 (2.4G)
```

```
debugap 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 ロゴ 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、ロゴ 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。

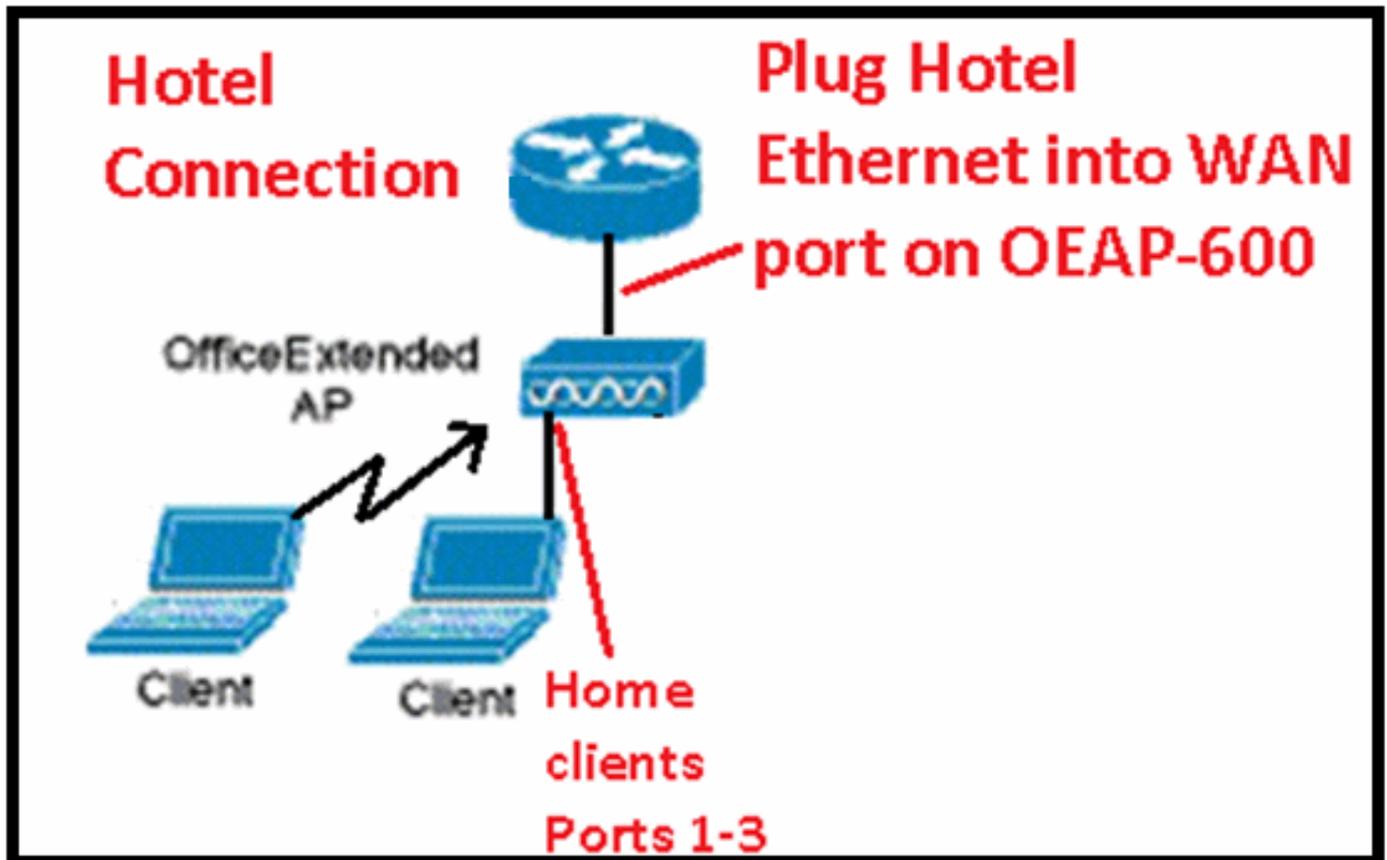
この OEAP-600 製品は、以前の OEAP アクセス ポイントとはログイン名が異なるため、Linksys などのホーム製品と一貫性を保つためにデフォルトのユーザ名は admin 、パスワードは admin となっています。AP-1130 および AP-1140 などのその他の Cisco OEAP アクセス ポイントのデフォルトのユーザ名は Cisco で、パスワードは Cisco です。

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れる場合があります。

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 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ます、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

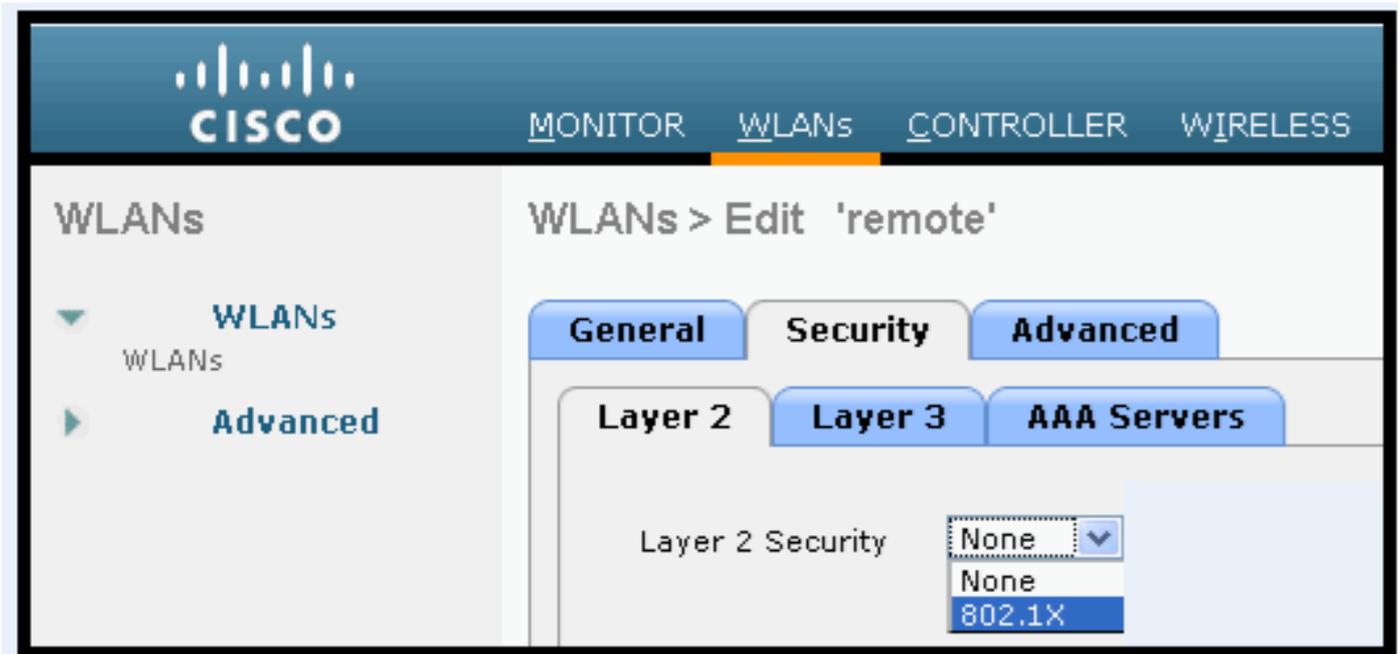


次に Cisco 7.2 リリースで導入された拡張の一部を示します。

- 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
- チャン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.

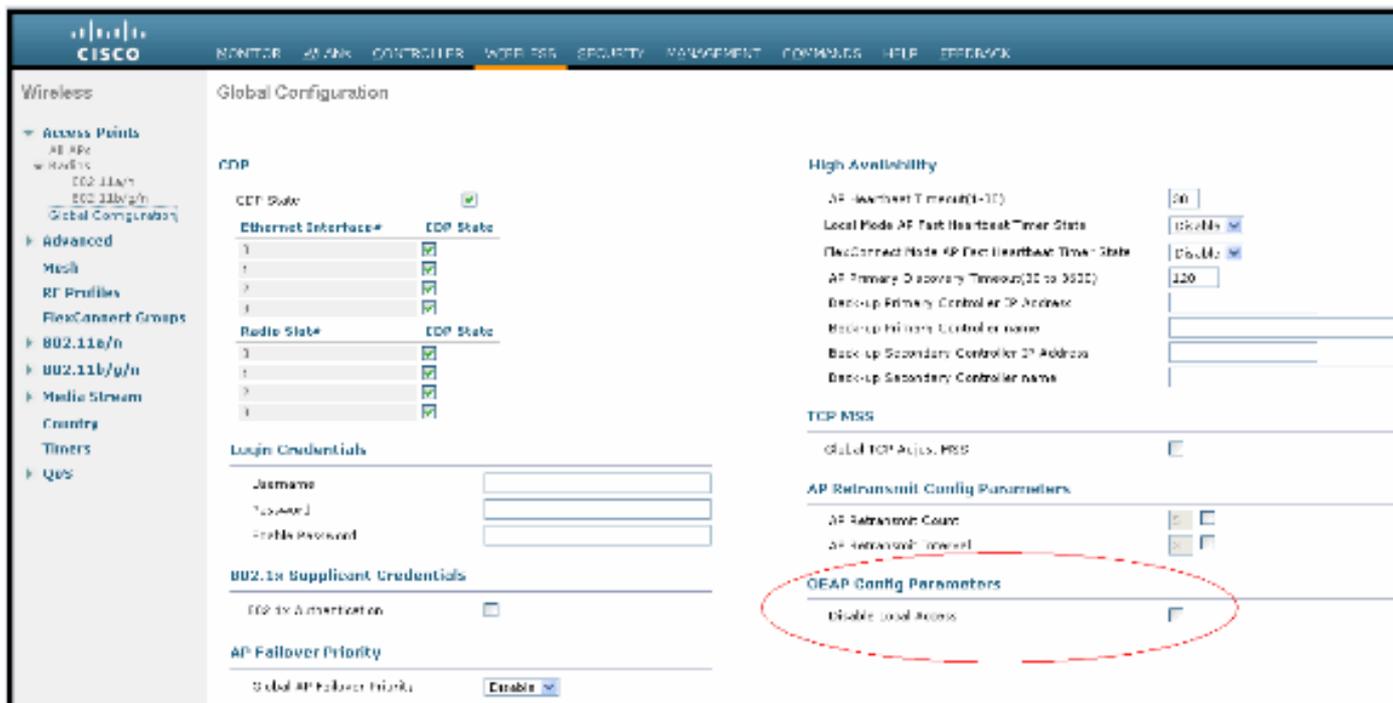
Same as 802.1x authentication for wireless clients, in 802.1x authentication for remote-LAN client, WLC acts as authenticator. Evora AP just forwards the EAPOL packets. AP converts EAPOL Ethernet packet to 802.11 data frame before sending it to WLC. The destination address in the 802.11 data frame shall 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

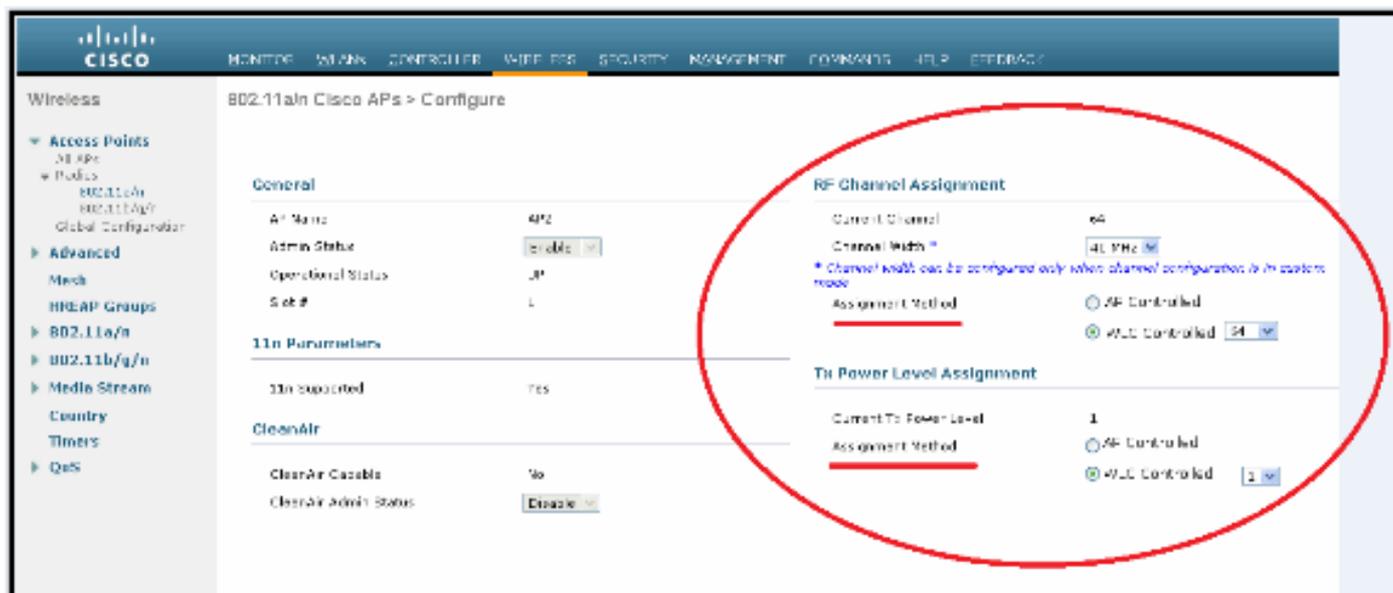
ローカル WLAN アクセスの無効化



チャン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 のチャン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



Manually configure channel and power level

In JMR1 release, there is no configuration option for 802.11a/n and 802.11b/g/n radios for the OEAP-600 AP. In 7.2 release; the configuration window is added back with only “General”, “RF Channel Assignment” and “Tx Power Level Assignment” portions. The “Admin Status” in “General” shall be display only. The options for “Assign Method” are changed to “Custom Configured” and “AP Controlled”. By default “AP Controlled” is selected. Channel and Tx power level can be configured only when they are in “Custom Configured” mode.

OEAP-600 does not support DFS channels so that WLC shall not allow these channels to be configured. [This new assignment method is passed to AP with CAPWAP payload.

In AP, when the channel is “AP Controlled”, then the channel is controlled by the setting from local AP GUI. Otherwise the channel set by WCS is used.

The channel assign method and the assigned channel are saved in NVRAM and displayed in local GUI.

In AP, when the power is “AP controlled”, then the maximum power level is always used. Otherwise the power level set by WCS is used.

The assign method for TX power level and assigned TX power level shall be saved in flash so that they can take effect after AP reboots.

When “Reset to Default” operation is performed, the assign method is set to “AP controlled”.

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 oep-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	r1an2	Enabled	management
3	r1an3	Enabled	management

r1an2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。r1an3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	r1an2	Enabled	management
3	r1an3	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。