



トラブルシューティング

- [Mode ボタンの使用, on page 1](#)
- [Cisco コントローラへのアクセスポイント参加プロセスのトラブルシューティング, on page 2](#)
- [コントローラベースの導入に関する重要な情報, on page 3](#)
- [DHCP オプション 43 の設定, on page 3](#)

Mode ボタンの使用

Mode ボタン（コネクタとポートを備えた C9136I の上面図を参照）を使用して、次のタスクを実行できます。

- AP を工場出荷時のデフォルト設定にリセットする
- すべてのコンフィギュレーションファイルを含む、AP の内部ストレージをクリアする

Mode ボタンを使用するには、AP の起動サイクル中に、アクセスポイント上の Mode ボタンを押し続けます。AP コンソールに秒カウンタが表示されるまで待ちます。Mode ボタンが押された秒数がカウンタに表示されると、AP のステータス LED が赤色の点滅に変わります。次に AP を工場出荷時の初期状態にリセットします。Mode ボタンを押し続けたままにし、20 秒が経過する前にボタンを放します。AP のコンフィギュレーションファイルがクリアされます。

すべてのコンフィギュレーションファイルを含め、AP の内部ストレージをクリアします。Mode ボタンを 20 秒以上（60 秒未満）押し続けたままにします。これにより、パスワード、WEP キー、IP アドレス、SSID を含め、構成時のすべての設定が工場出荷時の初期状態にリセットされます。



Note Mode ボタンを 30 秒以上（60 秒未満）押し続けると、AP が工場出荷時設定にリセットされる際に FIPS モードフラグもクリアされます。FIPS フラグが設定されている場合、コンソールアクセスは無効になります。

AP のステータス LED が青から赤に変わり、AP のストレージディレクトリからすべてのファイルが削除されます。

Mode ボタンを押したまま 60 秒以上が経過した場合は、操作の誤りと見なされて、変更は行われません。

Cisco コントローラへのアクセス ポイント参加プロセスのトラブルシューティング



Note C9136I AP をサポートするには、『[Cisco Wireless Solutions Software Compatibility Matrix](#)』に記載されているように、コントローラでコントローラソフトウェア Cisco IOS-XE 17.7.1 以降のリリースが実行されていることを確認します。

アクセスポイントがコントローラへの接続を失敗する理由として、RADIUS の認可が保留の場合、コントローラで自己署名証明書が有効になっていない場合、アクセスポイントとコントローラ間の規制ドメインが一致しない場合など、多くの原因が考えられます。

コントローラ ソフトウェアの利用により、CAPWAP 関連のすべてのエラーを syslog サーバに送信するようにアクセスポイントを設定できます。すべての CAPWAP エラーメッセージは syslog サーバ自体から表示できるので、コントローラで **debug** コマンドを有効にする必要はありません。

アクセスポイントからの CAPWAP 接続要求を受信するまで、コントローラではアクセスポイントの状態は維持されません。したがって、特定のアクセスポイントからの CAPWAP 検出要求が拒否された理由を判断することは難しい場合があります。コントローラで CAPWAP **debug** コマンドを有効にせずにこのような接続問題のトラブルシューティングを行えるよう、コントローラでは検出メッセージを送信してきたすべてのアクセスポイントの情報を収集し、正常に接続したアクセスポイントの情報を維持します。

コントローラは、CAPWAP discovery request を送信してきた各アクセスポイントについて、join 関連のすべての情報を収集します。収集は、アクセスポイントから最初に受信した discovery メッセージから始まり、コントローラからアクセスポイントに送信された最後の設定ペイロードで終わります。

コントローラが最大数のアクセスポイントの join 関連情報を維持している場合、それ以上のアクセスポイントの情報は収集されません。

デフォルトでは、1 つのアクセスポイントからすべての syslog メッセージが IP アドレス 255.255.255.255 に送信されます。

DHCP サーバで syslog サーバの IP アドレスをアクセスポイントに返すよう設定することもできます。サーバ上でオプション 7 を使用します。それにより、アクセスポイントではすべての syslog メッセージがこの IP アドレスへ送信されるようになります。

アクセスポイントが最初にコントローラに接続される際に、コントローラはグローバルな syslog サーバの IP アドレス（デフォルトは 255.255.255.255）をアクセスポイントに送信します。

- アクセスポイントはコントローラから接続を切断されており、別のコントローラに接続されている。この場合、新しいコントローラはそのグローバル syslog サーバの IP アドレスをアクセスポイントに送信します。
- 新しい syslog サーバの IP アドレスが既存の syslog サーバの IP アドレスを上書きするたびに、古いアドレスは固定記憶域から消去され、新しいアドレスがそこに保存される。アクセスポイントはその syslog サーバの IP アドレスに到達できれば、すべての syslog メッセージを新しい IP アドレスに送信するようになります。

**Note**

アクセスポイントの syslog サーバを設定して、アクセスポイントの接続情報をコントローラの CLI 以外では表示しないようにできます。

コントローラベースの導入に関する重要な情報

C9136I シリーズ AP を使用する場合は、次のガイドラインに留意してください。

- AP はシスコワイヤレスコントローラとのみ通信できます。
- AP は、無線ドメインサービス (WDS) をサポートしていないので、WDS デバイスとは通信できません。ただし、AP がコントローラに接続されると、コントローラが WDS に相当する機能を果たします。
- CAPWAP はレイヤ 2 をサポートしていません。この AP では、レイヤ 3、DHCP、DNS、または IP サブネットのブロードキャストを使用して IP アドレスを取得し、コントローラを検出する必要があります。
- AP のコンソールポートは、モニタリングおよびデバッグ用に有効になっています。
- AP がコントローラに接続されると、すべてのコンフィギュレーションコマンドが無効になります。

DHCP オプション 43 の設定

DHCP オプション 43 を使用すると、コントローラの IP アドレスのリストがアクセスポイントに提供されるため、アクセスポイントがコントローラを検出し、コントローラに接続できるようになります。

以下に、Windows 2003 エンタープライズ DHCP サーバを Cisco Catalyst Lightweight アクセスポイントと共に使用できるようにするための DHCP オプション 43 の設定例を示します。その他の DHCP サーバの実装に関する DHCP オプション 43 の設定については、製品マニュアルを参照してください。オプション 43 では、コントローラ管理インターフェイスの IP アドレスを使用する必要があります。



Note DHCP オプション 43 では、1 つの DHCP プールを 1 種類のアクセス ポイントだけに割り当てることができます。アクセス ポイントの種類別に、異なる DHCP プールを設定する必要があります。

C9136I AP では、DHCP オプション 43 に Type-Length-Value (TLV) 形式を使用します。DHCP サーバは、アクセス ポイントの DHCP Vendor Class Identifier (VCI; ベンダー クラス ID) 文字列 (DHCP オプション 43) に基づいてオプションを返すようにプログラミングされている必要があります。C9136I シリーズ アクセスポイントの VCI 文字列は、次のとおりです。

Cisco AP C9136I

TLV ブロックの形式は、次のとおりです。

- 型 : 0xf1 (十進数では 241)
- 長さ : コントローラの IP アドレス数 X 4
- 値 : 16 進数で順番にリストされているワイヤレスコントローラ管理インターフェイスの IP アドレス。

組み込みの Cisco IOS DHCP サーバに DHCP オプション 43 を設定する手順は、次のとおりです。

Procedure

ステップ 1 コンフィギュレーションモードを開始します。

ステップ 2 デフォルトのルータやネームサーバなどの必要なパラメータを指定して、DHCP プールを作成します。DHCP スコープの例を次に示します。

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>
```

ここで、各変数は次のように定義されます。

<pool name> : DHCP プールの名前 (AP など)

<IP Network> : コントローラがあるネットワーク IP アドレス (10.0.15.1 など)

<Netmask> : サブネットマスク (255.255.255.0 など)

<Default router> : デフォルトルータの IP アドレス (10.0.0.1 など)

<DNS Server> : DNS サーバの IP アドレス (10.0.10.2 など)

ステップ 3 次の構文に従って、オプション 43 の行を追加します。

```
option 43 hex <hex string>
```

hex string は、次の TLV 値を組み合わせて指定します。

型 + 長さ + 値

たとえば、管理インターフェイスの IP アドレスが 10.126.126.2 と 10.127.127.2 の 2 つのコントローラがある場合、タイプは f1 (16 進数)、長さは $2 \times 4 = 8 = 08$ (16 進数) であり、IP アドレスは 0a7e7e02 と 0a7f7f02 に変換されます。文字列を組み合わせると f1080a7e7e020a7f7f02 になります。DHCP スコープに追加される Cisco IOS のコマンドは、**option 43 hex f1080a7e7e020a7f7f02** となります。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。