WLAN コンフィギュレーション ガイド、Cisco IOS XE Release 3SE（Catalyst 3850 スイッチ）

初版：2013 年 01 月 29 日

最終更新：2013 年 10 月 07 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Text Part Number: OL-27618-02-J

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します （ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
bold フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
Italic フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*italic* フォントで示しています。
`courier` フォント	システムが表示するターミナル セッションおよび情報は、`courier` フォントで示しています。
`太字の courier` フォント	**`太字の courier`** フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。

表記法	説明
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。 角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。 string の前後には引用符を使用しません。 引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

（注） 「注釈」です。 役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。 機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス　時間を節約する方法です。 ここに紹介している方法で作業を行うと、時間を短縮できます。

警告　「警告」の意味です。 人身事故を予防するための注意事項が記述されています。

関連資料

（注）　スイッチをインストールまたはアップグレードする前に、スイッチのリリース ノートを参照してください。

- 次の URL にある Cisco Catalyst 3850 スイッチ のマニュアル：

  http://www.cisco.com/go/cat3850_docs

- 次の URL にある Cisco SFP および SFP+ モジュールのマニュアル（互換性マトリクスを含む）：

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html

- 次の URL にある Cisco Validated Design（CVD）のマニュアル：

  http://www.cisco.com/go/designzone

- 次の URL にあるエラー メッセージ デコーダ:

  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。 RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

コマンドライン インターフェイスの使用

コマンドライン インターフェイスの使用に関する情報

コマンド モード

Cisco IOS ユーザ インターフェイスは、いくつかのモードに分かれています。 使用できるコマンドの種類は、現在のモードによって異なります。 システム プロンプトに疑問符（?）を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。

CLI セッションは、コンソール接続、Telnet、SSH、またはブラウザを使用することによって開始できます。

セッションを開始するときは、ユーザ モード（別名ユーザ EXEC モード）が有効です。 ユーザ EXEC モードでは、限られた一部のコマンドしか使用できません。 たとえばユーザ EXEC コマンドの大部分は、**show** コマンド（現在のコンフィギュレーション ステータスを表示する）、**clear** コマンド（カウンタまたはインターフェイスをクリアする）などのように、1 回限りのコマンドです。 ユーザ EXEC コマンドは、スイッチをリブートするときには保存されません。

すべてのコマンドにアクセスするには、特権EXECモードを開始する必要があります。 特権EXECモードを開始するには、通常、パスワードが必要です。 このモードでは、任意の特権 EXEC コマンドを入力でき、また、グローバルコンフィギュレーションモードを開始することもできます。

コンフィギュレーション モード（グローバル、インターフェイス、およびライン）を使用して、実行コンフィギュレーションを変更できます。 設定を保存した場合はこれらのコマンドが保存され、スイッチをリブートするときに使用されます。 各種のコンフィギュレーションモードにアクセスするには、まずグローバル コンフィギュレーション モードを開始する必要があります。 グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モードおよびライン コンフィギュレーション モードに移行できます。

次の表に、主要なコマンド モード、各モードへのアクセス方法、各モードで表示されるプロンプト、およびモードの終了方法を示します。

表 *1*：コマンド モードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	Telnet、SSH、またはコンソールを使用してセッションを開始します。	`Switch>`	**logout** または **quit** を入力します。	このモードを使用して次の作業を行います。 • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードで、**enable** コマンドを入力します。	`Switch#`	**disable** を入力して終了します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure** コマンドを入力します。	`Switch(config)#`	終了して特権 EXEC モードに戻るには、**exit** または **end** コマンドを入力するか、Ctrl+Z を押します。	このモードは、スイッチ全体に適用するパラメータを設定する場合に使用します。
VLAN コンフィギュレーション	グローバル コンフィギュレーション モードで、**vlan** *vlan-id* コマンドを入力します。	`Switch(config-vlan)#`	グローバル コンフィギュレーションモードに戻る場合は、**exit** コマンドを入力します。 特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	

モード	アクセス方法	プロンプト	終了方法	モードの用途
				このモードを使用して、VLAN（仮想LAN）パラメータを設定します。VTPモードがトランスペアレントであるときは、拡張範囲 VLAN（VLAN ID が 1006以上）を作成してスイッチのスタートアップコンフィギュレーションファイルに設定を保存できます。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、**interface** コマンドを入力し、インターフェイスを指定します。	`Switch(config-if)#`	終了してグローバル コンフィギュレーションモードに戻るには、**exit** を入力します。 特権EXECモードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、イーサネット ポートのパラメータを設定します。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードで、**line vty** または **line console** コマンドを使用して回線を指定します。	`Switch(config-line)#`	終了してグローバル コンフィギュレーションモードに戻るには、**exit** を入力します。 特権EXECモードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、端末回線のパラメータを設定します。

ヘルプ システムの使用

システム プロンプトで疑問符（?）を入力すると、各コマンド モードに使用できるコマンドのリストが表示されます。 また、任意のコマンドについて、関連するキーワードおよび引数の一覧を表示することもできます。

手順の概要

1. **help**
2. *abbreviated-command-entry* **?**
3. *abbreviated-command-entry* <Tab>
4. **?**
5. *command* **?**
6. *command keyword* **?**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**help** 例： `Switch# help`	コマンド モードのヘルプ システムの簡単な説明を表示します。

ステップ 2	*abbreviated-command-entry* **?**
	
	例：
	`Switch# di?`
	`dir disable disconnect`
		特定のストリングで始まるコマンドのリストを表示します。

ステップ 3	*abbreviated-command-entry* <Tab>
	
	例：
	`Switch# sh conf<tab>`
	`Switch# show configuration`
		特定のコマンド名を補完します。

ステップ 4	**?** 例： `Switch> ?`	特定のコマンド モードで使用可能なすべてのコマンドをリストします。
ステップ 5	*command* **?** 例： `Switch> show ?`	コマンドに関連するキーワードを一覧表示します。

	コマンドまたはアクション	目的

ステップ 6	*command keyword* **?**
	
	例：
	`Switch(config)# cdp holdtime ?`
	`  <10-255> Length of time (in sec) that receiver must keep this packet`
		キーワードに関連する引数を一覧表示します。

コマンドの省略形

スイッチでコマンドが一意に認識される長さまでコマンドを入力します。

show configuration 特権 EXEC コマンドを省略形で入力する方法を次に示します。

```
Switch# show conf
```

コマンドの no 形式および default 形式

大部分のコンフィギュレーション コマンドに、**no** 形式があります。 **no** 形式は一般に、特定の機能または動作をディセーブルにする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスのシャットダウンが取り消されます。 **no** キーワードなしでコマンドを使用すると、ディセーブルにされた機能を再度イネーブルにしたり、デフォルトでディセーブルになっている機能をイネーブルにすることができます。

コンフィギュレーション コマンドには、**default** 形式もあります。 コマンドの **default** 形式は、コマンドの設定値をデフォルトに戻します。 大部分のコマンドはデフォルトでディセーブルに設定されているので、**default** 形式は **no** 形式と同じになります。 ただし、デフォルトでイネーブルに設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。 これらのコマンドについては、**default** コマンドを使用すると、コマンドがイネーブルになり、変数がデフォルト値に設定されます。

CLI のエラー メッセージ

次の表に、CLI を使用してスイッチを設定するときに表示される可能性のあるエラー メッセージの一部を紹介します。

表 *2*：*CLI* の代表的なエラー メッセージ

エラー メッセージ	意味	ヘルプの表示方法
`% Ambiguous command: "show con"`	スイッチがコマンドとして認識できるだけの文字数が入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを入れません。 コマンドとともに使用できるキーワードが表示されます。
`% Incomplete command.`	コマンドに必須のキーワードまたは値が、一部入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。
`% Invalid input detected at '^' marker.`	コマンドの入力ミスです。 間違っている箇所をキャレット（^）記号で示しています。	疑問符（?）を入力すると、そのコマンド モードで利用できるすべてのコマンドが表示されます。 コマンドとともに使用できるキーワードが表示されます。

コンフィギュレーション ロギング

スイッチの設定変更を記録して表示させることができます。 Configuration Change Logging and Notification 機能を使用することで、セッションまたはユーザ ベースごとに変更内容をトラッキングできます。 ログに記録されるのは、適用された各コンフィギュレーション コマンド、コマンドを入力したユーザ、コマンドの入力時間、コマンドに対するパーサからのリターン コードです。 この機能には、登録しているアプリケーションの設定が変更されるときに通知される非同期通知方式もあります。 Syslog へこの通知を送信することも選択できます。

（注） CLI または HTTP の変更のみがログとして記録されます。

CLI を使用して機能を設定する方法

コマンド履歴の設定

入力したコマンドは、ソフトウェア側にコマンド履歴として残されます。 コマンド履歴機能は、アクセスコントロールリストの設定時など、長い複雑なコマンドまたはエントリを何度も入力しなければならない場合、特に便利です。 必要に応じて、この機能をカスタマイズできます。

コマンド履歴バッファ サイズの変更

デフォルトでは、スイッチは履歴バッファにコマンドライン10行を記録します。 現在の端末セッションまたは特定回線のすべてのセッションで、この数を変更できます。 この手順は任意です。

手順の概要

1. **terminal history** [**size** *number-of-lines*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal history** [**size** *number-of-lines*] 例： `Switch# terminal history size 200`	特権 EXEC モードで現在のターミナル セッション中にスイッチが記録するコマンドラインの数を変更します。 サイズは 0 から 256 までの間で設定できます。

コマンドの呼び出し

履歴バッファにあるコマンドを呼び出すには、次の表に示すいずれかの操作を行います。 これらの操作は任意です。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

手順の概要

1. **Ctrl+P** または**上矢印**キー
2. **Ctrl+N** または**下矢印**キー
3. **show history**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**Ctrl+P** または**上矢印**キー	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。 キーを押すたびに、より古いコマンドが順次表示されます。
ステップ 2	**Ctrl+N** または**下矢印**キー	**Ctrl+P** または上矢印キーでコマンドを呼び出した後で、履歴バッファ内のより新しいコマンドに戻ります。 キーを押すたびに、より新しいコマンドが順次表示されます。
ステップ 3	**show history** 例： `Switch# show history`	特権 EXEC モードで、直前に入力したコマンドをいくつか表示します。 表示されるコマンドの数は、**terminal history** グローバル コンフィギュレーション コマンドおよび **history** ライン コンフィギュレーション コマンドの設定値によって指定されます。

コマンド履歴機能のディセーブル化

コマンド履歴機能は、自動的にイネーブルになっています。 現在の端末セッションまたはコマンドラインでディセーブルにできます。 この手順は任意です。

手順の概要

1. **terminal no history**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal no history** 例： `Switch# terminal no history`	特権 EXEC モードで現在のターミナル セッションにおけるこの機能をディセーブルにします。

編集機能のイネーブル化およびディセーブル化

拡張編集モードは自動的に有効に設定されますが、ディセーブルにして、再度イネーブルにできます。

手順の概要

1. **terminal editing**
2. **terminal no editing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal editing** 例： `Switch# terminal editing`	特権 EXEC モードで現在のターミナル セッションにおける拡張編集モードを再びイネーブルにします。
ステップ 2	**terminal no editing** 例： `Switch# terminal no editing`	特権 EXEC モードで現在のターミナル セッションにおける拡張編集モードをディセーブルにします。

キー入力によるコマンドの編集

キーストロークは、コマンドラインの編集に役立ちます。 これらのキーストロークは任意です。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

表 *3*：編集コマンド

編集コマンド	説明
Ctrl-B または**左矢印**キー	カーソルを 1 文字後退させます。
Ctrl-F または**右矢印**キー	カーソルを 1 文字前進させます。
Ctrl+A	コマンドラインの先頭にカーソルを移動します。
Ctrl+E	カーソルをコマンド ラインの末尾に移動します。
Esc B	カーソルを 1 単語後退させます。
Esc F	カーソルを 1 単語前進させます。

Ctrl+T	カーソルの左にある文字を、カーソル位置の文字と置き換えます。
Delete キーまたは **Backspace** キー	カーソルの左にある文字を消去します。
Ctrl+D	カーソル位置にある文字を削除します。
Ctrl+K	カーソル位置からコマンドラインの末尾までのすべての文字を削除します。
Ctrl+U または Ctrl+X	カーソル位置からコマンドラインの先頭までのすべての文字を削除します。
Ctrl+W	カーソルの左にある単語を削除します。
Esc D	カーソルの位置から単語の末尾までを削除します。
Esc C	カーソル位置のワードを大文字にします。
Esc L	カーソルの場所にある単語を小文字にします。
Esc U	カーソルの位置から単語の末尾までを大文字にします。
Ctrl+V または Esc Q	特定のキーストロークを実行可能なコマンド（通常はショートカット）として指定します。
Return キー	1 行または 1 画面下へスクロールして、端末画面に収まりきらない表示内容を表示させます。 （注） **show** コマンドの出力など、端末画面に一度に表示できない長い出力では、More プロンプトが使用されます。More プロンプトが表示された場合は、Return キーおよび Space キーを使用してスクロールできます。
Space バー	1 画面分下にスクロールします。
Ctrl+L または Ctrl+R	スイッチから画面に突然メッセージが出力された場合に、現在のコマンドラインを再表示します。

画面幅よりも長いコマンドラインの編集

画面上で 1 行分を超える長いコマンドラインについては、コマンドのラップアラウンド機能を使用できます。 カーソルが右マージンに達すると、そのコマンドラインは 10 文字分だけ左へシフトされます。 コマンドラインの先頭から 10 文字までは見えなくなりますが、左へスクロールして、コマンドの先頭部分の構文をチェックできます。 これらのキー操作は任意です。

コマンドの先頭にスクロールして入力内容をチェックするには、Ctrl+B キーまたは←キーを繰り返し押します。 コマンドラインの先頭に直接移動するには、Ctrl+A を押します。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

次に、画面上で 1 行分を超える長いコマンドラインを折り返す例を示します。

手順の概要

1. **access-list**
2. **Ctrl+A**
3. **Return** キー

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**access-list**
	
	例：
	`Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35`
	`Switch(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25`
	`Switch(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq`
	`Switch(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45`
		1 行分を超えるグローバル コンフィギュレーション コマンド入力を表示します。
		最初にカーソルが行末に達すると、その行は 10 文字分だけ左へシフトされ、再表示されます。 ドル記号（$）は、その行が左へスクロールされたことを表します。 カーソルが行末に達するたびに、その行は再び10文字分だけ左へシフトされます。

ステップ 2	**Ctrl+A** 例： `Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$`	完全な構文をチェックします。 行末に表示されるドル記号（$）は、その行が右へスクロールされたことを表します。
ステップ 3	**Return** キー	コマンドを実行します。

	コマンドまたはアクション	目的
		ソフトウェアでは、端末画面は 80 カラム幅であると想定されています。 画面の幅が異なる場合は、**terminal width** 特権 EXEC コマンドを使用して端末の幅を設定します。 ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンドエントリを呼び出して変更できます。

show および more コマンド出力の検索およびフィルタリング

show および **more** コマンドの出力を検索およびフィルタリングできます。 この機能は、大量の出力をソートする場合や、出力から不要な情報を除外する場合に役立ちます。 これらのコマンドの使用は任意です。

手順の概要

1. {**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	{**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*
	
	例：
	`Switch# show interfaces | include protocol`
	`Vlan1 is up, line protocol is up`
	`Vlan10 is up, line protocol is down`
	`GigabitEthernet1/0/1 is up, line protocol is down`
	`GigabitEthernet1/0/2 is up, line protocol is up`
		出力を検索およびフィルタリングします。
		文字列では、大文字と小文字が区別されます。 たとえば、**| exclude output** と入力した場合、**output** を含む行は表示されませんが、**Output** を含む行は表示されます。

スイッチ スタックでの CLI へのアクセス

CLI にはコンソール接続、Telnet、SSH、またはブラウザを使用することによってアクセスできます。

スイッチ スタックおよびスタック メンバ インターフェイスは、を経由して管理します。 スイッチごとにスタック メンバを管理することはできません。 1 つまたは複数のスタック メンバのコンソール ポートまたはイーサネット管理ポートを経由してへ接続できます。 で複数の CLI セッションを使用する場合は注意してください。 1 つのセッションで入力したコマンドは、別のセッショ

ンには表示されません。 したがって、コマンドを入力したセッションを追跡できない場合があります。

（注） スイッチ スタックを管理する場合は、1 つの CLI セッションを使用することを推奨します。

特定のスタック メンバ ポートを設定する場合は、CLI コマンドインターフェイス表記にスタック メンバ番号を含めてください。

コンソール接続または Telnet 経由で CLI にアクセスする

CLI にアクセスするには、スイッチのハードウェア インストレーション ガイドに記載されている手順で、スイッチのコンソール ポートに端末または PC を接続するか、または PC をイーサネット管理ポートに接続して、スイッチの電源をオンにする必要があります。

スイッチがすでに設定されている場合は、ローカル コンソール接続またはリモート Telnet セッションによって CLI にアクセスできますが、このタイプのアクセスに対応できるように、先にスイッチを設定しておく必要があります。

次のいずれかの方法で、スイッチとの接続を確立できます。

- スイッチ コンソール ポートに管理ステーションまたはダイヤルアップ モデムを接続するか、またはイーサネット管理ポートに PC を接続します。 コンソール ポートまたはイーサネット管理ポートへの接続については、スイッチのハードウェア インストレーション ガイドを参照してください。
- リモート管理ステーションから任意の Telnet TCP/IP または暗号化 Secure Shell（SSH; セキュア シェル）パッケージを使用します。 スイッチは Telnet または SSH クライアントとのネットワーク接続が可能でなければなりません。また、スイッチにイネーブル シークレット パスワードを設定しておくことも必要です。
  - スイッチは同時に最大 16 の Telnet セッションをサポートします。 1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。
  - スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

コンソール ポート、イーサネット管理ポート、Telnet セッション、または SSH セッションを通じて接続すると、管理ステーション上にユーザ EXEC プロンプトが表示されます。

第 2 章

Web グラフィカル ユーザ インターフェイスの使用

Web GUI の使用に関する前提条件

- GUI を使用する PC では、Windows 7、Windows XP SP1 以降のリリースまたは Windows 2000 SP4 以降のリリースが稼働している必要があります。
- スイッチGUI は、Microsoft Internet Explorer バージョン 10.x、Mozilla Firefox 20.x、または Google Chrome 26.x. と互換性があります。

Web GUI の使用に関する情報

Web ブラウザ、つまり、グラフィカル ユーザ インターフェイス（GUI）は、各スイッチに組み込まれています。

サービス ポート インターフェイスまたは管理インターフェイスを使用して GUI にアクセスできますが、 サービス ポート インターフェイスの使用をお勧めします。 GUI のページ上部にある [Help] をクリックすると、オンライン ヘルプが表示されます。 オンライン ヘルプを表示するには、ブラウザのポップアップ ブロッカを無効にする必要があります。

Web GUI の機能

スイッチWeb GUI は次の機能をサポートします。

構成ウィザード : IP アドレスおよびローカルユーザ名/パスワードの初期設定、または認証サーバでの認証（必須特権 15）の後、ウィザードは最初の無線設定を完了するための手順を提供します。 [Configuration] > [Wizard] を起動し、次のことを設定するために、9 ステップの手順に従います。

- 管理ユーザ
- SNMP システムの概要
- Management Port
- ワイヤレス管理
- RF Mobility と国番号
- モビリティ設定
- WLAN
- 802.11 設定
- Set Time

[Monitor] タブ:

- 概要のスイッチ、クライアント、アクセス ポイントの詳細を表示します。
- すべての無線および AP 接続統計情報を表示します。
- アクセス ポイントの電波品質を表示します。
- すべてのインターフェイスおよび CDP トラフィック情報の Cisco Discovery Protocol (CDP) のすべてのネイバーの一覧を表示します。
- 分類 Friendly、Malicious、Ad hoc、Classified、および Unclassified に基づいて、すべての不正アクセス ポイントを表示します。

[Configuration] タブ:

- Web設定ウィザードを使用して、すべての初期操作のためにスイッチを設定できます。 ウィザードでは、ユーザの詳細、管理インターフェイスなどを設定できます。
- システム、内部 DHCP サーバ、管理、およびモビリティ管理パラメータを設定できます。
- スイッチ、WLAN、無線を設定できます。
- スイッチで、セキュリティ ポリシーを設定できます。
- オペレーティング システム ソフトウェアの管理コマンドスイッチにアクセスできます。

[Administration] タブで、システム ログを設定できます。

スイッチのコンソール ポートの接続

はじめる前に

基本的な動作ができるようにスイッチを設定するには、VT-100 ターミナル エミュレーション プログラム（HyperTerminal、ProComm、Minicom、Tip など）を実行する PC にコントローラを接続する必要があります。

ステップ 1 ヌルモデム シリアル ケーブルの一端をスイッチの RJ-45 コンソール ポートに接続し、もう一端を PC のシリアル ポートに接続します。

ステップ 2 AC 電源コードをスイッチに接続し、アース付き 100 ～ 240 VAC、50/60 Hz の電源コンセントに差し込みます。 電源を入れます。 起動スクリプトによって、オペレーティング システム ソフトウェアの初期化（コードのダウンロードおよび電源投入時自己診断テスト）および基本設定が表示されます。 スイッチの電源投入時自己診断テストに合格した場合は、起動スクリプトによって設定ウィザードが実行されます。画面の指示に従って、基本設定を入力してください。

ステップ 3 **yes** と入力します。 CLI セットアップ ウィザードの基本的な初期設定パラメータに進みます。 gigabitethernet 0/0 インターフェイスであるサービス ポートの IP アドレスを指定します。
構成ウィザードの設定パラメータを入力すると、Web GUI にアクセスできます。 これで、スイッチがサービス ポートの IP アドレスにより設定されます。

Web GUI へのログイン

ステップ 1 ブラウザのアドレス行にスイッチの IP アドレスを入力します。 接続をセキュリティで保護するには、https://**ip-address** と入力します。 接続をセキュリティで保護しない場合は、http://**ip-address** と入力します。

ステップ 2 [Accessing Cisco AIR-CT3850] ページが表示されます。

Web モードおよびセキュア Web モードの有効化

ステップ 1 [Configuration] > [Management] > [Protocol Management] > [HTTP-HTTPS]を選択します。

[HTTP-HTTPS Configuration] ページが表示されます。

ステップ 2 Web モード（ユーザが「http://ip-address」を使用してスイッチ GUI にアクセスできます）を有効にするには、[HTTP Access] ドロップダウン リストから [Enabled] を選択します。 有効にしない場合は、[Disabled] を選択します。 Web モード（HTTP）の接続は、セキュリティで保護されません。

ステップ 3 セキュア Web モード（ユーザが「https://ip-address」を使用してスイッチ GUI にアクセスできます）を有効にするには、[HTTPS Access] ドロップダウン リストから [Enabled] を選択します。 有効にしない場合は、[Disabled] を選択します。 セキュア Web モード（HTTPS）の接続は、セキュリティで保護されています。

ステップ 4 [IP Device Tracking] チェックボックスで、デバイスを追跡することを選択します。

ステップ 5 [Enable] チェックボックスでトラスト ポイントをイネーブルにすることを選択します。

ステップ 6 [Trustpoints] ドロップダウン リストからトラストポイントを選択します。

ステップ 7 [HTTP Timeout-policy (1 to 600 sec)] テキスト ボックスに、非アクティブ化により Web セッションがタイムアウトするまでの時間を秒単位で入力します。
有効な範囲は 1 ～ 600 秒です。

ステップ 8 [Server Life Time (1 to 86400 sec)] テキスト ボックスにサーバのライフタイムを入力します。
有効な範囲は 1 ～ 86400 秒です。

ステップ 9 [Maximum number of Requests (1 to 86400)] テキスト ボックスに、サーバが受け入れる最大接続要求数を入力します。
指定できる接続数の範囲は、1 ～ 86400 です。

ステップ 10 [Apply] をクリックします。

ステップ 11 [Save Configuration] をクリックします。

スイッチ Web GUI の設定

設定ウィザードでは、スイッチ上での基本的な設定を行うことができます。 このウィザードは、スイッチを購入した直後やスイッチを工場出荷時のデフォルトにリセットした後に実行します。 設定ウィザードは、GUI と CLI の両方の形式で使用できます。

ステップ 1 PC をサービス ポートに接続し、スイッチと同じサブネットを使用するように IPv4 アドレスを設定します。 スイッチが IOS XE イメージとともにロードされ、サービス ポート インターフェイスが gigabitethernet 0/0 として設定されます。

ステップ 2 PC で Internet Explorer 10 以降、Firefox 2.0.0.11 以降、または Google Chrome を開始し、ブラウザ ウィンドウに管理インターフェイスの IP アドレスを入力します。 管理インターフェイスの IP アドレスは、gigabitethernet 0/0（別名、サービス ポート インターフェイス）と同じです。 初めてログインするときに、

HTTP のユーザ名およびパスワードを入力する必要があります。 デフォルトでは、ユーザ名は **admin**、パスワードは **cisco** です。
サービス ポート インターフェイスを使用するときは、HTTP と HTTPS の両方を使用できます。 HTTPS はデフォルトでイネーブルであり、HTTP をイネーブルにすることもできます。

初めてログインすると、 <Model Number> <Hostname>] ページが表示されます。

ステップ 3 ページで、スイッチ Web GUI の [Home] ページにアクセスするために、[Wireless Web GUI] リンクをクリックします。

ステップ 4 最初にスイッチの設定に必要なすべての手順を実行するために、[Configuration] > [Wizard]を選択します。 [Admin Users] ページが表示されます。

ステップ 5 [Admin Users] ページで、このスイッチに割り当てる管理者のユーザ名を [User Name] テキスト ボックスに入力し、このスイッチに割り当てる管理パスワードを [Password] テキスト ボックスおよび [Confirm Password] テキスト ボックスに入力します。 [Next] をクリックします。
デフォルトのユーザ名は **admin** で、デフォルトのパスワードは **cisco** です。 またはスイッチの新しい管理者ユーザを作成できます。 ユーザ名とパスワードには、最大 24 文字の ASCII 文字を入力できます。

[SNMP System Summary] ページが表示されます。

ステップ 6 [SNMP System Summary] ページで、スイッチの次の SNMP システム パラメータを入力し、[Next] をクリックします。

- [Location] テキスト ボックスでユーザ定義可能なスイッチの場所。
- [Contact] テキスト ボックスで名前や電話番号などのユーザ定義可能な連絡先の詳細。
- SNMP 通知をさまざまな SNMP トラップで送信するには、[SNMP Global Trap] ドロップダウン リストで [Enabled] を選択し、さまざまな SNMP トラップに対して SNMP 通知を送信しないようにするには [Disabled] を選択します。
- システム ログ メッセージを送信するには [SNMP Logging] ドロップダウン リストから [Enabled] を選択し、システム ログ メッセージを送信しない場合は [Disabled] を選択します。

（注） SNMP トラップ サーバは、ディストリビューション ポートから到達可能であることが必要です（gigabitethernet0/0 サービスまたは管理インターフェイスは経由しません）。

[Management Port] ページが表示されます。

ステップ 7 [Management Port] ページで、管理ポートのインターフェイス（gigabitethernet 0/0）の次のパラメータを入力し、[Next] をクリックします。

- [IP Address] テキスト ボックスでサービス ポートに割り当てたインターフェイスの IP アドレス。
- [Netmask]テキスト ボックスで、管理ポートのインターフェイスのネットワーク マスクのアドレス。
- [IPv4 DHCP Server] テキスト ボックスで選択されたポートの IPv4 Dynamic Host Configuration Protocol (DHCP) のアドレス。

[Wireless Management] ページが表示されます。

ステップ 8 [Wireless Management] ページでは、次のワイヤレス インターフェイス管理の詳細を入力し、[Next] をクリックします。

- [Select Interface] ドロップダウン リストから、インターフェイスとして VLAN または 10 ギガビット イーサネットを選択します。
- [VLAN ID] テキスト ボックスで VLAN タグの ID。VLAN タグがない場合は 0。
- [IP Address] テキスト ボックスで、アクセス ポイントが接続されたワイヤレス管理インターフェイスの IP アドレス。
- [Netmask] テキスト ボックスで、ワイヤレス管理インターフェイスのネットワーク マスクのアドレス。
- [IPv4 DHCP Server] テキスト ボックスで DHCP IPv4 IP アドレス。

インターフェイスとして VLAN を選択すると、[Switch Port Configuration] テキスト ボックスで指定されたリストから、ポートとしてトランク ポートまたはアクセス ポートを指定できます。

[RF Mobility and Country Code] ページが表示されます。

ステップ 9 [RF Mobility and Country Code] ページで、RF モビリティ ドメイン名を [RF Mobility] テキスト ボックスに入力し、[Country Code] ドロップダウン リストから現在の国コードを選択して、[Next] をクリックします。GUI からは、1 つの国番号のみを選択できます。

（注） RF グループ化パラメータとモビリティ設定を設定する前に、必ず関連する概念のコンテンツを参照してから、設定に進むようにしてください。

[Mobility Configuration] ページが開き、モビリティのグローバル コンフィギュレーション設定が表示されます。

ステップ 10 [Mobility Configuration] ページで、次のモビリティのグローバル コンフィギュレーション設定を参照および入力し、[Next] をクリックします。

- [Mobility Role] ドロップダウン リストから、[Mobility Controller] または [Mobility Agent] を選択します。
  - [Mobility Agent] を選択した場合は、[Mobility Controller IP Address] テキスト ボックスにモビリティ コントローラの IP アドレス、[Mobility Controller Public IP Address] テキスト ボックスにモビリティ コントローラの IP アドレスを入力します。
  - [Mobility Controller] を選択すると、モビリティ コントローラの IP アドレスとモビリティ コントローラのパブリック IP アドレスがそれぞれのテキスト ボックスに表示されます。
- [Mobility Protocol Port] テキスト ボックスにモビリティ プロトコルのポート番号が表示されます。
- [Mobility Switch Peer Group Name] テキスト ボックスにモビリティ スイッチのピア グループ名が表示されます。
- [DTLS Mode] テキスト ボックスで、DTLS がイネーブルであるかどうかが示されます。

DTLS は、標準化過程にある TLS に基づくインターネット技術特別調査委員会（IETF）プロトコルです。

- [Mobility Domain ID for 802.11 radios] テキスト ボックスに、802.11 無線のモビリティ ドメイン ID が表示されます。
- [Mobility Keepalive Interval (1-30)sec] テキスト ボックスで、ピア スイッチに送信する各 ping 要求の間隔（秒単位）。

  有効範囲は 1 ～ 30 秒で、デフォルト値は 10 秒です。
- [Mobility Keep Alive Count（3-20）] テキスト ボックスで、ピア スイッチが到達不能と判断するまでに ping 要求を送信する回数。

  有効な範囲は 3 ～ 20 で、デフォルト値は 3 です。
- [Mobility Control Message DSCP Value (0-63)] テキスト ボックスで、モビリティ スイッチに設定される DSCP 値。

  有効な範囲は 0 ～ 63 で、デフォルト値は 0 です。
- [Switch Peer Group Members Configured] テキスト ボックスで設定したモビリティ スイッチ ピア グループ メンバーの数を表示します。

[WLANs] ページが表示されます。

ステップ 11 [WLANs] ページで、次の WLAN 設定パラメータを入力し、[Next] をクリックします。

- [WLAN ID] テキスト ボックスで WLAN 識別子。
- [SSID] テキスト ボックスで、クライアントに関連付けられている WLAN の SSID。
- [Profile Name] テキスト ボックスで、クライアントが使用する WLAN の名前。

[802.11 Configuration] ページが表示されます。

ステップ 12 [802.11 Configuration] ページで、[802.11a/n/ac] チェックボックスと [802.11b/g/n] チェックボックスのいずれかまたは両方をオンにして 802.11 無線をイネーブルにし、[Next] をクリックします。
[Set Time] ページが表示されます。

ステップ 13 [Set Time] ページで、次のパラメータに基づいてスイッチの日時を設定し、[Next] をクリックします。

- [Current Time] テキスト ボックスで、スイッチの現在のタイムスタンプが表示されます。
- [Mode] ドロップダウン リストから [Manual] または [NTP] を選択します。

  NTP サーバの使用時に、スイッチに接続されているすべてのアクセス ポイントが、使用可能な NTP サーバ設定に基づいて時間を同期します。
- [Year, Month, and Day] ドロップダウン リストからスイッチの日付を選択します。
- [Hours, Minutes, and Seconds] ドロップダウン リストから時間を選択します。
- 時間帯を [Zone] テキスト ボックスに入力し、スイッチで設定された現在の時刻と比較した場合に必要なオフセットを [Offset] ドロップダウン リストから選択します。

[Save Wizard] ページが表示されます。

ステップ 14 [Save Wizard] ページで、この手順を使用してスイッチで行った設定を確認できます。設定値を変更する場合は、[Previous] をクリックし、該当ページに移動します。
すべてのウィザードについて成功メッセージが表示された場合にのみ、ウィザードを使用して作成したスイッチ設定を保存できます。 [Save Wizard] ウィザード ページでエラーが表示された場合、スイッチの初期設定のためにウィザードを再実行する必要があります。

第 3 章

WLAN の設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

WLAN の前提条件

- 最大 16 個の WLAN を各アクセス ポイント グループにアソシエートし、各グループに個々のアクセス ポイントを割り当てることができます。 各アクセス ポイントは、有効化されている WLAN のうち、そのアクセス ポイント グループに属する WLAN だけをアドバタイズします。 アクセス ポイント グループで無効化されている WLAN または別のグループに属する WLAN はアドバタイズしません。
- コントローラが VLAN トラフィックを正常にルーティングできるよう、WLAN と管理インターフェイスにはそれぞれ別の VLAN を割り当てることをお勧めします。
- コントローラでは、同じ Service Set Identifier（SSID）の WLAN を区別するために、異なる属性が使用されます。
  - 同じ SSID、同じレイヤ 2 ポリシーの WLAN は、WLAN ID が 17 より小さい場合は作成できません。
  - WLAN が異なる AP グループに追加される場合、17 より大きい ID で、同じ SSID と同じレイヤ 2 ポリシーを持つ 2 つの WLAN を使用できます。

（注） この要件によって、クライアントが同じアクセスポイント無線のSSIDを検出することがないようにします。

関連トピック

WLAN の作成（CLI），（30 ページ）
WLAN の作成（GUI），（31 ページ）
汎用 WLAN プロパティの設定（CLI），（36 ページ）
汎用 WLAN プロパティの設定（GUI），（38 ページ）
WLAN の削除（CLI），（32 ページ）
高度な WLAN プロパティの設定（CLI），（40 ページ）
高度な WLAN プロパティの設定（GUI），（43 ページ）
帯域の選択，（26 ページ）
オフチャネル スキャンの延期
DTIM Period
セッションのタイムアウト
Cisco Client Extensions，（28 ページ）
ピアツーピア ブロッキング，（29 ページ）
診断チャネル
WLAN ごとのクライアント カウント

WLAN のイネーブル化（CLI），（34 ページ）
WLAN のディセーブル（CLI），（35 ページ）

WLAN の制約事項

- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- 最大 2000 台のクライアントを設定できます。
- WLAN 名と SSID は 32 文字以内にする必要があります。 スペースは WLAN プロファイル名と SSID では許可されません。
- WLAN から VLAN0 へのマッピング、VLAN 1002～1006 のマッピングはできません。
- 固定 IPv4 アドレスのデュアル スタック クライアントはサポートされません。
- 同じ SSID を持つ WLAN を作成するときには、各 WLAN に対して一意のプロファイル名を作成する必要があります。
- 同じ SSID を持つ複数の WLAN を同じ AP 無線に割り当てる場合は、クライアントがその中から安全に選択できるように、一意のレイヤ 2 セキュリティ ポリシーを使用している必要があります。

注意 一部のクライアントが複数のセキュリティ ポリシーで同じ SSID を検出すると WLAN に正しく接続できない場合があります。 この機能を使用する際は、十分注意してください。

関連トピック

WLAN の作成（CLI），（30 ページ）
WLAN の作成（GUI），（31 ページ）
汎用 WLAN プロパティの設定（CLI），（36 ページ）
汎用 WLAN プロパティの設定（GUI），（38 ページ）
WLAN の削除（CLI），（32 ページ）
高度な WLAN プロパティの設定（CLI），（40 ページ）
高度な WLAN プロパティの設定（GUI），（43 ページ）
帯域の選択，（26 ページ）
オフチャネル スキャンの延期
DTIM Period
セッションのタイムアウト
Cisco Client Extensions，（28 ページ）
ピアツーピア ブロッキング，（29 ページ）
診断チャネル

WLAN について

この機能により、Lightweight アクセス ポイント全体に対して、最大 64 の WLAN を制御できます。 各 WLAN には識別子である WLAN ID、プロファイル名、および WLAN SSID があります。 すべてのスイッチは接続している各アクセス ポイントに対して最大 16 の WLAN を公開しますが、管理しやすくするため、サポートされる最大数の WLAN を作成し、これらの WLAN を異なるアクセス ポイントに選択的に公開する（アクセス ポイント グループを使用）ことができます。

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

帯域の選択

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、混雑の少ない 5 GHz アクセス ポイントに移動できます。 2.4 GHz 帯域は、混雑していることがあります。 この帯域のクライアントは一般に、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他のアクセス ポイントからの同一チャネル干渉も発生します。802.11b/g では、重複しないチャネルが 3 つしかないからです。 これらの干渉の原因を防止して、ネットワーク全体のパフォーマンスを向上させるには、コントローラで帯域選択を設定できます。

帯域選択のしくみは、クライアントへのプローブ応答を規制するというものです。 5 GHz チャネルへクライアントを誘導するために、2.4 GHz チャネルでのクライアントへのプローブ応答を遅らせます。

関連トピック

オフチャネル スキャンの延期

特定の省電力モードのクライアントが展開される環境で、小容量クライアント（たとえば、省電力モードを使用し定期的にテレメトリ情報を送信する医療用デバイス）からの重要情報の欠落を防ぐために、場合によっては、無線リソース管理（RRM）の正常なオフチャネル スキャンを延期する必要があります。 この機能は、Quality of Service（QoS）と RRM スキャン延期機能との相互作用の方法を向上させます。

クライアントの Wi-Fi マルチメディア（WMM）UP マーキングを使用して、UP がマークされたパケットを受信した場合に、設定可能な期間中オフチャネルスキャンを延期するアクセスポイントを設定することができます。

[Off-Channel Scanning Defer] は、ノイズや干渉など代替チャネル選択に関する情報を収集する RRM を使用するときに重要となります。 また、[Off-Channel Scanning Defer] は、不正検出を行います。 [Off-Channel Scanning Defer] を提供する必要があるデバイスは、可能な限り、同じ WLAN を使用する必要があります。 このようなデバイスが多くある場合（この機能を使用して Off-Channel Defer スキャンが完全に無効化されている可能性があります）、モニタ アクセス ポイントや、この WLAN が割り当てられていない同じ位置にあるその他のアクセスポイントなど、代わりにローカル AP で [Off-Channel Scanning Defer] を実装する必要があります。

QoS ポリシー（Bronze、Silver、Gold、Platinum）を WLAN に割り当てることで、クライアントからアップリンクでどのように受信されたかに関係なく、パケットがアクセス ポイントからのダウンリンク接続でどのようにマーキングされるかを制御できます。 UP=1,2 は最低の優先順位で、UP=0,3 はその次に高い優先順位です。 各 QoS ポリシーのマーキング結果は次のとおりです。

- Bronze は、すべてのダウンリンク トラフィックを UP= 1 にマーキングします。
- Silver は、すべてのダウンリンク トラフィックを UP=0 にマーキングします。
- Gold は、すべてのダウンリンク トラフィックを UP= 4 にマーキングします。
- Platinum は、すべてのダウンリンク トラフィックを UP= 6 にマーキングします。

DTIM Period

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

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

ただし、DTIM 値は、802.11 のすべてのクライアントで省電力モードがイネーブルである場合、255 まで設定できます（255 回のビーコンごとにブロードキャスト フレームおよびマルチキャスト フレームを送信します）。 クライアントは DTIM 期間に達したときのみリッスンする必要があるため、ブロードキャストとマルチキャストをリッスンする頻度を少なく設定することで、結果的にバッテリー寿命を長くできます。 たとえば、ビーコン期間が 100 ms、DTIM 値を 100 に設定すると、アクセスポイントは、バッファされたブロードキャストフレームおよびマルチキャストフレームを 10 秒ごとに 1 回送信します。 このレートにより省電力クライアントで、ブロードキャ

ストとマルチキャストをリッスンし、ウェイク アップするまでのスリープ状態が長くなり、バッテリ寿命を長くできます。

（注） ビーコン期間は、コントローラでミリ秒単位で指定され、ソフトウェアによって、802.11 単位時間（TU）（1 TU = 1.024 ミリ秒）に、内部的に変換されます。 Cisco の 802.11n アクセス ポイントでは、この値は直近の 17 TU の倍数に丸められます。 たとえば、100 ミリ秒に設定されたビーコン間隔は 104 ミリ秒の実際のビーコン間隔の結果です。

多くのアプリケーションでは、ブロードキャスト メッセージとマルチキャスト メッセージとの間隔を長くすると、プロトコルとアプリケーションのパフォーマンスが低下します。 このようなクライアントをサポートする 802.11 ネットワークでは、低い DTIM 値を推奨します。

セッション タイムアウト

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

Cisco Client Extensions

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

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

関連トピック

高度な WLAN プロパティの設定（CLI），（40 ページ）
高度な WLAN プロパティの設定（GUI），（43 ページ）
WLAN の前提条件，（24 ページ）

WLAN の制約事項, （25 ページ）

ピアツーピア ブロッキング

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

ローカル スイッチングの WLAN にアソシエートされたクライアントに対して、ピアツーピアブロッキングがサポートされます。

関連トピック

高度な WLAN プロパティの設定（CLI）, （40 ページ）
高度な WLAN プロパティの設定（GUI）, （43 ページ）
WLAN の前提条件, （24 ページ）
WLAN の制約事項, （25 ページ）

診断チャネル

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

（注） 診断チャネル機能は、管理インターフェイスを使用するアンカーされていない SSID に対してのみ有効にすることをお勧めします。

WLAN ごとの RADIUS 送信元サポート

デフォルトで、スイッチは、グローバル リストの代わりに、管理インターフェイスの IP アドレスがのすべての RADIUS トラフィックの送信元になります。つまり、設定されている特定の RADIUS サーバが WLAN に存在する場合でも、使用される ID は管理インターフェイスの IP アドレスです。

WLAN をフィルタする場合は RFC 3580 で APMAC SSID 形式に設定された callStationID を使用できます。 また、NAS-IP-Address 属性を使用することで、認証サーバ上のフィルタリングを WLAN ごとの送信元インターフェイス上にまで拡張できます。

WLAN ごとの RADIUS 送信元サポートを有効にすると、スイッチは、設定されている動的インターフェイスを使用して特定の WLAN のすべての RADIUS トラフィックを送信します。 また、それに応じて、RADIUS 属性が Identity に一致するように変更されます。 この機能は、各 WLAN が別個のレイヤ 3 Identity を持つ可能性がある場合に、WLAN ごとの RADIUS トラフィックでスイッチを効果的に仮想化します。 この機能は、ACS ネットワーク アクセス制限、およびネットワーク アクセス プロファイルと統合する展開に役立ちます。

アドレスの送信元として WLAN ごとの動的インターフェイスを用いる管理インターフェイスなどを使用するいくつかの WLAN および通常の RADIUS トラフィックの送信元と、WLAN ごとの RADIUS 送信元サポートを組み合わせることができます。

WLAN の設定方法

WLAN の作成（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name wlan-id* [*ssid*]
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name wlan-id* [*ssid*] 例： `Switch(config)# wlan mywlan 34 mywlan-ssid`	WLAN の名前と ID を指定します。 • [Profile Name] に、プロファイル名を入力します。 入力できる範囲は英数字で 1 ～ 32 文字です。 • WLAN ID に、wlan-id を入力します。 範囲は 1 ～ 512 です。 • *ssid* では、この WLAN に対する Service Set Identifier (SSID) を入力します。 SSID を指定しない場合、WLAN プロファイル名は SSID として設定されます。 （注） WLAN はデフォルトでディセーブルにされています。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN の前提条件, （24 ページ）
WLAN の制約事項, （25 ページ）

WLAN の作成（GUI）

ステップ 1 [Configuration] > [Wireless] をクリックします。
[WLANs] ページが表示されます。

ステップ 2 [New] をクリックして新しい WLAN を作成します。
[WLANs] > [Create New] ページが表示されます。

ステップ 3 次のパラメータを入力します。

パラメータ	説明
WLAN ID	WLAN 識別子。 値の範囲は 1 ～ 512 です。
SSID	WLAN のブロードキャスト名。
Profile	WLAN プロファイル名

ステップ 4 [Apply] をクリックします。

関連トピック

WLAN の前提条件, （24 ページ）
WLAN の制約事項, （25 ページ）

WLAN の削除（CLI）

手順の概要

1. **configure terminal**
2. **no wlan** *wlan-name wlan-id ssid*
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no wlan** *wlan-name wlan-id ssid* 例： `Switch(config)# no wlan test2`	WLAN を削除します。 引数は次のとおりです。 • *wlan-name*は WLAN プロファイル名です。 • *wlan-id*は、WLAN ID です。 • *ssid* は WLAN に設定された WLAN SSID 名前です。 （注） AP グループに属する WLAN を削除すると、WLAN は AP グループと AP の無線から削除されます。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN の前提条件, （24 ページ）
WLAN の制約事項, （25 ページ）

WLAN の削除（GUI）

ステップ 1 [Configuration] > [Wireless] をクリックします。
[WLANs] ページが表示されます。

ステップ 2 削除する WLAN に対応するチェックボックスをオンにします。

（注） AP グループに属する WLAN を削除すると、WLAN は AP グループと AP の無線から削除されます。

ステップ 3 [Remove] をクリックします。

WLAN の検索（CLI）

手順の概要

1. **show wlan summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show wlan summary** 例： `Switch# show wlan summary`	デバイスに設定されているすべての WLAN のリストを表示します。 出力内で WLAN を検索できます。

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

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

WLAN を検索するときにワイルドカードを使用できます。 たとえば、**show wlan summary include** | *variable* とすることができます。 variable は、出力内の検索文字列です。

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

WLAN の検索（GUI）

ステップ 1 [Configuration] > [Wireless] をクリックします。
[WLANs] ページが表示されます。

ステップ 2 検索する列の上部のテキスト ボックスに最初の数文字を入力します。 たとえば、プロファイルに基づいて WLAN を検索する場合は、プロファイル名の最初の数文字を入力します。

次の条件に基づいて WLAN を検索できます。

- Profile
- ID
- SSID
- VLAN
- Status

WLAN が存在する場合、一致精度に基づいて表示されます。

WLAN のイネーブル化（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **no shutdown**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**no shutdown** 例： `Switch(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバルコンフィギュレーションモードを終了できます。

関連トピック

WLAN の前提条件, （24 ページ）
WLAN の制約事項, （25 ページ）

WLAN のディセーブル（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **end**
5. **show wlan summary**

手順の詳細

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

関連トピック

WLAN の前提条件, （24 ページ）
WLAN の制約事項, （25 ページ）

汎用 WLAN プロパティの設定（CLI）

次のパラメータを設定できます。

- メディア ストリーム
- ブロードキャスト SSID
- コール スヌーピング
- Radio
- インターフェイス
- Status

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **broadcast-ssid**
5. **radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**}
6. **client vlan** *vlan-identifier*
7. **ip multicast vlan** *vlan-name*
8. **media-stream multicast-direct**
9. **call-snoop**
10. **no shutdown**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： `Switch# shutdown`	パラメータを設定する前に、WLAN をディセーブルにします。
ステップ 4	**broadcast-ssid** 例： `Switch(config-wlan)# broadcast-ssid`	この WLAN の SSID をブロードキャストします。 このフィールドは、デフォルトでイネーブルにされています。
ステップ 5	**radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**} 例： `Switch# radio all`	WLAN で無線をイネーブルにします。 キーワードは次のとおりです。 • **all**：すべての無線帯域で WLAN を設定します。 • **dot1a**：802.11a 無線帯域のみに WLAN を設定します。 • **dot11g**：802.11ag 無線帯域に WLAN を設定します。 • **dot11bg**：802.11b/g 無線帯域のみに WLAN を設定します（802.11g がディセーブルの場合は 802.11b のみ）。 • **dot11ag**：802.11g 無線帯域のみに無線 LAN を設定します。
ステップ 6	**client vlan** *vlan-identifier* 例： `Switch# client vlan test-vlan`	WLAN のインターフェイス グループをイネーブルにします。*vlan-identifier*：VLAN ID を指定します。 次に、VLAN 名、VLAN ID、または VLAN グループ名を指定できます。
ステップ 7	**ip multicast vlan** *vlan-name* 例： `Switch(config-wlan)# ip multicast vlan test`	WLAN のマルチキャストをイネーブルにします。 キーワードは次のとおりです。 • **vlan**：VLAN ID を指定します。 • *vlan-name*：VLAN の名前を指定します。
ステップ 8	**media-stream multicast-direct** 例： `Switch(config-wlan)# media-stream multicast-direct`	この WLAN では、マルチキャスト VLAN をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 9	**call-snoop** 例： `Switch(config-wlan)# call-snoop`	コール スヌーピング サポートをイネーブルにします。
ステップ 10	**no shutdown** 例： `Switch(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 11	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバルコンフィギュレーションモードを終了できます。

関連トピック

WLAN の前提条件, （24 ページ）
WLAN の制約事項, （25 ページ）

汎用 WLAN プロパティの設定（GUI）

WLAN の次の操作を行うには、次の手順を使用してください。

- WLAN ステータスを設定します
- 無線ポリシーを設定します
- インターフェイスまたはインターフェイス グループを割り当てます
- マルチキャスト VLAN 機能をイネーブルまたはディセーブルにします
- ブロードキャスト SSID 機能をイネーブルまたはディセーブルにします

はじめる前に

ステップ 1 [Configuration] > [Wireless] をクリックします。
[WLANs] ページが表示されます。

ステップ 2 ページの検索機能を使用して、設定する WLAN を検索します。

ステップ 3 WLAN の [WLAN Profile] をクリックします。

[WLAN] >[Edit] ページが表示されます。

ステップ 4 [General] タブをクリックします。 このタブは、デフォルトで表示されます。

ステップ 5 [General] パラメータを設定します。

パラメータ	説明
Profile Name	WLAN の設定済みプロファイル名を表示します。
Type	設定された LAN タイプを表示します。
SSID	WLAN の設定済み SSID を表示します。
Status	WLAN を有効にするチェックボックスです。 デフォルト値はイネーブルです。
Security Policies	[Security] タブを使用して設定された WLAN セキュリティ ポリシーです。
Radio Policy	WLAN の無線をイネーブルにするための LAN 無線ポリシーです。 値は次のとおりです。 • すべて（All） • 802.11a のみ • 802.11g のみ • 802.11a/g のみ • 802.11b/g のみ
Interface/Interface Group	この WLAN にマッピングするインターフェイスまたはインターフェイスのグループ。 [Interfaces] ページで設定されている非サービス ポートと非仮想インターフェイス名を表示します。 （注） このフィールドは、WLAN に対する VLAN が、コントローラの既存 VLAN の名前を使用してマッピングされている場合にのみ、ドロップ ダウンに表示されます。
Broadcast SSID	この SSID をブロードキャストするチェックボックスです。 デフォルトではイネーブルになっています。
Multicast VLAN Feature	マルチキャスト VLAN をイネーブルにするチェックボックスです。 デフォルトではディセーブルになっています。 （注） [Multicast Interface] フィールドは、[Multicast VLAN feature] テキスト ボックスをイネーブルにした後でのみ表示されます。 （注） マルチキャスト機能を使用する場合は、マルチキャスト VLAN 機能を 1 回だけ設定する必要があります。

ステップ 6　[Apply] をクリックします。

次の作業

セキュリティ、QoS、および詳細プロパティの設定に進みます。

関連トピック

WLAN の前提条件,（24 ページ）
WLAN の制約事項,（25 ページ）

高度な WLAN プロパティの設定（CLI）

次の高度なパラメータを設定できます。

- AAA オーバーライド
- Coverage Hole Detection
- セッションのタイムアウト
- Cisco Client Extensions
- 診断チャネル
- インターフェイス オーバーライド ACL
- P2P ブロッキング
- クライアント除外
- WLAN ごとの最大クライアント数
- オフ チャネル スキャンの延期

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **aaa-override**
4. **chd**
5. **session-timeout** *time-in-seconds*
6. **ccx aironet-iesupport**
7. **diag-channel**
8. **ip access-group** [web] *acl-name*
9. **peer-blocking** [**drop** | **forward-upstream**]
10. **exclusionlist** *time-in-seconds*
11. **client association limit** *max-number-of-clients*
12. **channel-scan defer-priority** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}}
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**aaa-override** 例： `Switch(config-wlan)# aaa-override`	AAA オーバーライドをイネーブルにします。
ステップ 4	**chd** 例： `Switch(config-wlan)# chd`	この WLAN のカバレッジホールの検出をイネーブルにします。このフィールドは、デフォルトでイネーブルにされています。
ステップ 5	**session-timeout** *time-in-seconds* 例： `Switch(config-wlan)# session-timeout 450`	セッション タイムアウトを秒単位で設定します。 範囲とデフォルト値は、セキュリティ設定によって異なります。 WLAN セキュリティが dot1x に設定されている場合、範囲は 300～86400 秒で、デフォルト値は 1800 秒です。 他のすべての WLAN セキュリティ設定では、有効範囲は 1～65535 秒であり、デフォルト値は 0 秒です。 値 0 は、セッション タイムアウトなしを示します。

	コマンドまたはアクション	目的
ステップ 6	**ccx aironet-iesupport** 例： `Switch(config-wlan)# ccx aironet-iesupport`	この WLAN の Aironet IE のサポートをイネーブルにします。 このフィールドは、デフォルトでイネーブルにされています。
ステップ 7	**diag-channel** 例： `Switch(config-wlan)# diag-channel`	WLAN でクライアントの通信の問題を修復するための診断チャネルのサポートをイネーブルにします。
ステップ 8	**ip access-group** [web] *acl-name* 例： `Switch(config)# ip access-group test-acl-name`	WLAN ACL グループを設定します。 可変 *acl* 名前はユーザ定義する IPv4 ACL の名前を指定します。 キーワード **web** は、IPv4 web ACL を指定します。
ステップ 9	**peer-blocking** [**drop** | **forward-upstream**] 例： `Switch(config)# peer-blocking drop`	ピアツーピア ブロッキング パラメータを設定します。 キーワードは次のとおりです。 • **drop**：ドロップ アクションのピアツーピア ブロッキングをイネーブルにします。 • **forward-upstream**：アップストリーム転送処理のピアツーピア ブロッキングをイネーブルにします。
ステップ 10	**exclusionlist** *time-in-seconds* 例： `Switch(config)# exclusionlist 10`	タイムアウトを秒単位で指定します。 0 ～ 2147483647 の範囲の値を指定できます。 タイムアウトなしでは、0 を入力します。 ゼロ（0）タイムアウトは、クライアントが除外リストに追加されたことを示しています。
ステップ 11	**client association limit** *max-number-of-clients* 例： `Switch(config)# client association limit 200`	WLAN で設定できる最大クライアント数を設定します。
ステップ 12	**channel-scan defer-priority** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}} 例： `Switch(config)# channel-scan defer-priority 6`	チャネルスキャンの延期プライオリティと延期時間を設定します。 引数は次のとおりです。 • **defer-priority**：オフチャネル スキャンを延期できるパケットのプライオリティ マーキングを指定します。 範囲は 0 ～ 7 です。 デフォルト値は 3 です。 • **defer-time**：ミリ秒単位の遅延時間です。 範囲は 0 ～ 6000 です。 デフォルトは 100 です。

	コマンドまたはアクション	目的
ステップ 13	**end** 例： `Switch(config)# end`	特権EXECモードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

帯域の選択，（26 ページ）
オフチャネル スキャンの延期
DTIM Period
セッションのタイムアウト
Cisco Client Extensions，（28 ページ）
ピアツーピア ブロッキング，（29 ページ）
診断チャネル
WLAN ごとのクライアント カウント
WLAN の前提条件，（24 ページ）
WLAN の制約事項，（25 ページ）
AAA Override について，（66 ページ）
レイヤ 2 セキュリティの前提条件，（65 ページ）

高度な WLAN プロパティの設定（GUI）

はじめる前に

ステップ 1 [Configuration] > [Wireless] をクリックします。
[WLANs] ページが表示されます。

ステップ 2 ページの検索機能を使用して、設定する WLAN を検索します。

ステップ 3 WLAN の [WLAN Profile] をクリックします。
[WLAN] >[Edit] ページが表示されます。

ステップ 4 [Advanced Properties] タブをクリックします。

ステップ 5 詳細プロパティを設定します。

パラメータ	説明
Allow AAA Override	自身が有効または無効に設定できるグローバル WLAN パラメータの AAA オーバーライド。 スイッチ AAA Override が有効で、クライアントにおいて AAA と WLAN 認証パラメータが競合している場合、クライアント認証は AAA サーバにより行われます。この認証の一環として、オペレーティング システムはデフォルトの Cisco WLAN Solution WLAN VLAN から、AAA サーバによって返され、スイッチのインターフェイス設定で事前定義された VLAN にクライアントを移動します。 すべてのケースで、スイッチのインターフェイス構成で事前定義されている場合、オペレーティング システムは QoS、DSCP、802.1p 優先順位タグ値および AAA サーバで指定された ACLs を使用します（この AAA オーバーライドによる VLAN スイッチングは、ID ネットワーキングとも呼ばれます）。 企業の WLAN が主に VLAN 2 に割り当てられている管理インターフェイスを使用し、AAA オーバーライドが VLAN 100 へのリダイレクトを返す場合、VLAN 100 が割り当てられている物理ポートに関係なく、オペレーティング システムはすべてのクライアント送信を VLAN 100 にリダイレクトします。 AAA Override が無効の場合、すべてのクライアント認証はデフォルトのスイッチの認証パラメータ設定となり、スイッチの WLAN にクライアント固有の認証パラメータが含まれていない場合、認証のみ AAA サーバによって行われます。 AAA オーバーライド値は、たとえば RADIUS サーバから取り込まれます。
Coverage Hole Detection	自身でイネーブルまたはディセーブルにできるこの WLAN でのカバレッジ ホール検出 (CHD)。 デフォルトでは、CHD は、スイッチのすべての WLAN で有効です。 WLAN 上で CHD をディセーブルにすることができます。 WLAN で CHD を無効にした場合、カバレッジ ホールの警告はスイッチに送信されますが、カバレッジ ホールを解消するためのそれ以外の処理は行われません。 この機能については、ゲストのネットワーク接続時間は短く、モビリティが高いと考えられるようなゲスト WLAN に有用です。
Session Timeout	WLAN でセッション タイムアウト（秒単位）を設定します。 セッション タイムアウトとは、クライアント セッションが再認証を要求することなくアクティブである最大時間を指します。 ゼロを入力すると、セッションは期限切れになりません。
Aironet IE	自身がイネーブルまたはディセーブルにできる WLAN ごとの Aironet IE のサポート。 デフォルトではディセーブルになっています。
Diagnostic Channel	自身がイネーブルまたはディセーブルにできる WLAN 上の診断チャネルのサポート。 デフォルトではディセーブルになっています。

パラメータ	説明
P2P Blocking Action	次から選択できるピアツーピア ブロッキングの設定です。 • Disabled：（デフォルト）ピアツーピアブロッキングを無効にして、可能な場合にはコントローラ内でトラフィックをローカルにブリッジします。 • Drop：スイッチでパケットを破棄するようにします。 • [Forward-UpStream]：パケットがアップストリーム VLAN に転送されるようにします。 これらのパケットに対して行われる動作は、スイッチよりも上流にあるデバイスにより決定されます。
Client Exclusion	自身がイネーブルまたはディセーブルに設定できる無効なクライアント マシンのタイムアウト（秒単位）。 クライアントマシンは、MAC アドレスでディセーブルにされ、そのステータスを [Clients] > [Details] ページで監視できます。 0 のタイムアウト設定は、クライアントが永続的に無効であることを示します。 クライアントを再度有効にするには、管理制御が必要です。 デフォルトでイネーブルであり、タイムアウト設定は 60 秒として設定されます。
Timeout Value (secs)	
Max Allowed Client	各スイッチについて許可される最大クライアント数。 WLAN に接続できるクライアントの数に制限を設定できます。 この機能は、スイッチに接続できるクライアントの数に制限がある場合に役立ちます。 特定の WLAN にアクセス可能なゲスト クライアントの数に制限を設定できます。 WLAN ごとに設定できるクライアントの数は、使用しているプラットフォームによって異なります。 最大 12000 個のクライアントがサポートされます。 （注） WLAN ごとのクライアントの最大数機能は、接続モードのアクセス ポイントでのみサポートされます。
DHCP	
DHCP Server IP Address	WLAN に割り当てられたインターフェイスの DHCP サーバ アドレスを上書きする WLAN 上の DHCP サーバを入力します。
DHCP Address Assignment Required	DHCP アドレスの割り当てをイネーブルにし、クライアントが DHCP サーバから IP アドレスを取得できるようにすることを必須にします。
DHCP Option 82	WLAN で DHCP82 ペイロードをイネーブルにします。

パラメータ	説明
DHCP option 82 Format	DHCP オプション 82 の形式を指定します。 値は次のとおりです。 • add-ssid：AP 無線の MAC アドレスおよび SSID である RemoteID 形式を設定します。 • ap-ethmac：AP Ethernet MAC アドレスである RemoteID 形式を設定します。 （注） フォーマット オプションが設定されていない場合、AP 無線の MAC アドレスだけが使用されます。
DHCP Option ASCII Mode	DHCP オプション 82 の ASCII を設定します。 これが設定されていない場合、オプション 82 の形式は ASCII 形式に設定されます。
DHCP Option 82 RID Mode	DHCP オプション 82 に Cisco 2 バイト RID を追加します。
NAC	
NAC State	WLAN で NAC をイネーブルにします。
Off Channel Scanning Defer	
Scan Differ Priority	priority の引数をクリックし、割り当てることのできるチャネル スキャンのプライオリティを延期できます。 priority の有効範囲は 0 ～ 7 です。 priority は 0 ～ 7 です（この値は、クライアントおよび WLAN では 6 に設定する必要があります）。 複数の値を設定できます。 デフォルト値は、4、5、および 6 です。
Scan Differ Time	チャネル スキャンを割り当てることができる時間（ミリ秒）を延期します。 有効な範囲は 100（デフォルト）～60000（60 秒）です。 この設定は、お使いの無線 LAN の装置の要件に一致させる必要があります。
Override Interface ACL	
IPv4 ACL	WLAN IPv4 ACL のグループ。 値は次のとおりです。 • Un-configured • Pre-auth_ipv4_acl
IPv6 ACL	WLAN IPv6 ACL のグループ。 値は次のとおりです。 • Un-configured • Pre-auth_ipv6_acl

ステップ 6 [Apply] をクリックします。

関連トピック

帯域の選択，（26 ページ）
オフチャネル スキャンの延期
DTIM Period
セッションのタイムアウト
Cisco Client Extensions，（28 ページ）
ピアツーピア ブロッキング，（29 ページ）
診断チャネル
WLAN ごとのクライアント カウント
WLAN の前提条件，（24 ページ）
WLAN の制約事項，（25 ページ）
Dynamic Host Configuration Protocol について，（55 ページ）
内部 DHCP サーバ，（55 ページ）
外部 DHCP サーバ，（56 ページ）
DHCP 割り当て，（56 ページ）
DHCP オプション 82 について，（57 ページ）
DHCP スコープの設定，（58 ページ）
DHCP スコープについて，（59 ページ）
DHCP for WLANs を設定するための前提条件，（53 ページ）
DHCP for WLANs の設定に関する制約事項，（54 ページ）

WLAN での QoS ポリシーの適用（GUI）

ステップ 1 Choose [Configuration] > [Wireless] を選択します。

ステップ 2 WLAN ノードを左側のペインをクリックして拡大し、[WLANs] を選択します。
[WLANs] ページが表示されます。

ステップ 3 WLAN の [Profile] をクリックして QoS ポリシーを設定する WLAN を選択します。

ステップ 4 WLAN で QoS ポリシーを設定するには、[QoS] タブをクリックします。
次のオプションを使用できます。

パラメータ	説明
QoS SSID Policy	

パラメータ	説明
Downstream QoS Policy	QoS ダウンストリーム ポリシーの設定。 [Existing Policy] 列には、現在適用されているポリシーが表示されます。 既存のポリシーを変更するには、[Assign Policy] 列のドロップダウン リストからポリシーを選択します。
Upstream QoS Policy	QoS アップストリーム ポリシー設定。 [Existing Policy] 列には、現在適用されているポリシーが表示されます。 既存のポリシーを変更するには、[Assign Policy] 列のドロップダウン リストからポリシーを選択します。
QoS Client Policy	
Downstream QoS Policy	QoS ダウンストリーム ポリシーの設定。 [Existing Policy] 列には、現在適用されているポリシーが表示されます。 既存のポリシーを変更するには、[Assign Policy] 列のドロップダウン リストからポリシーを選択します。
Upstream QoS Policy	QoS アップストリーム ポリシー設定。 [Existing Policy] 列には、現在適用されているポリシーが表示されます。 既存のポリシーを変更するには、[Assign Policy] 列のドロップダウン リストからポリシーを選択します。
WMM	
WMM Policy	WMM ポリシー。 値は次のとおりです。 • Disabled：この WMM ポリシーをディセーブルにします。 • Allowed：クライアントがこの WLAN で通信できます。 • Required：WLAN との通信を可能にする WMM がクライアントに存在することが必須であることを確認します。

ステップ 5 [Apply] をクリックします。

WLAN プロパティの監視（CLI）

コマンド	説明
show wlan id *wlan-id*	WLAN ID に基づいて WLAN プロパティを表示します。
show wlan name *wlan-name*	WLAN 名に基づいて WLAN プロパティを表示します。
show wlan all	設定されているすべての WLAN の WLAN プロパティを表示します。
show wlan summary	すべての WLAN の要約を表示します。 サマリー詳細には、次の情報が含まれます。 • WLAN ID • プロファイル名 • SSID • VLAN • Status
show running-config wlan *wlan-name*	WLAN の名前に基づいて WLAN の実行コンフィギュレーションを表示します。
show running-config *wlan*	すべての WLAN の実行コンフィギュレーションを表示します。

WLAN プロパティの表示（GUI）

はじめる前に

- 管理者特権が必要です。

ステップ 1 [Configuration] > [WLAN] を選択します
[WLANs] ページが表示されます。

ステップ 2 [WLAN Profile] リンクをクリックします。
[WLANs] > [Edit] ページが表示されます。 [WLANs] ページは、次のタブで構成されます。

- [General]：WLAN の全般プロパティを表示します。
- [Security]: セキュリティ プロパティを表示します。 これらのプロパティには、レイヤ 2、レイヤ 3、および AAA のプロパティが含まれます。
- [QoS]: QoS 設定プロパティを表示します。
- [Advanced]：高度なプロパティを表示します。

次の作業

DHCP for WLANs の設定に進みます

その他の関連資料

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	*WLAN Command Reference, Cisco IOS XE Release 3SE*（*Catalyst 3850* スイッチ）
Mobility Anchor の設定	*Mobility Configuration Guide, Cisco IOS XE Release 3SE*（*Catalyst 3850* スイッチ）
WebAuth の設定	*Security Configuration Guide*（*Catalyst 3850* スイッチ）

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

WLANs の機能情報

次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能	リリース	変更内容
WLAN の機能	Cisco IOS XE 3.2SE	この機能が導入されました。

第 4 章

DHCP for WLANs の設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

DHCP for WLANs を設定するための前提条件

- DHCP オプション 82 を使用するには、Cisco IOS ソフトウェアで DHCP を設定します。 デフォルトでは、DHCP オプション 82 は、すべてのクライアントに対してイネーブルにされます。 WLAN サブオプションを使用して無線クライアントの動作を制御できます。

関連トピック

WLAN 用の DHCP 設定（CLI），（59 ページ）
高度な WLAN プロパティの設定（GUI），（43 ページ）
Dynamic Host Configuration Protocol について，（55 ページ）
内部 DHCP サーバ，（55 ページ）
外部 DHCP サーバ，（56 ページ）
DHCP 割り当て，（56 ページ）
DHCP オプション 82 について，（57 ページ）
DHCP スコープの設定，（58 ページ）
DHCP スコープについて，（59 ページ）

DHCP for WLANs の設定に関する制約事項

- WLAN で DHCP サーバをオーバーライドすると、DHCP サーバが到達可能であることを確認するために、基盤となる Cisco IOS 設定を行う必要があります。
- DHCP WLAN オーバーライドは DHCP サービスがコントローラ上で有効な場合にだけ動作します。

  次の方法で、DHCP サービスを設定できます。

  - コントローラで DHCP プールを設定します。
  - SVI で DHCP リレー エージェントを設定します。 注: SVI の VLAN は DHCP のオーバーライドが設定された WLAN にマッピングする必要があります。

関連トピック

WLAN 用の DHCP 設定（CLI），（59 ページ）
高度な WLAN プロパティの設定（GUI），（43 ページ）
Dynamic Host Configuration Protocol について，（55 ページ）
内部 DHCP サーバ，（55 ページ）
外部 DHCP サーバ，（56 ページ）
DHCP 割り当て，（56 ページ）
DHCP オプション 82 について，（57 ページ）
DHCP スコープの設定，（58 ページ）
DHCP スコープについて，（59 ページ）

Dynamic Host Configuration Protocol について

WLAN では、同じ Dynamic Host Configuration Protocol（DHCP）サーバまたは異なる DHCP サーバを使用するか、または DHCP サーバを使用しないように設定できます。 DHCP サーバには、内部 DHCP サーバと外部 DHCP サーバの 2 つのタイプがあります。

関連トピック

WLAN 用の DHCP 設定（CLI）, （59 ページ）
高度な WLAN プロパティの設定（GUI）, （43 ページ）
DHCP for WLANs を設定するための前提条件, （53 ページ）
DHCP for WLANs の設定に関する制約事項, （54 ページ）

内部 DHCP サーバ

スイッチは、内部 DHCP サーバを持っています。 このサーバは、一般的に、DHCP サーバを持たないブランチ オフィスで使用されます。 無線ネットワークには、通常、スイッチと同じ IP サブネット上にある最大 10 台のアクセス ポイントが含まれます。 内部サーバは、ワイヤレス クライアント、ダイレクトコネクト アクセス ポイント、およびアクセス ポイントからリレーされた DHCP 要求に対して DHCP アドレスを提供します。 Lightweight アクセス ポイントのみサポートされています。 内部 DHCP サーバを使用する場合は、スイッチの管理インターフェイスの IP アドレスを DHCP サーバの IP アドレスとして設定する必要があります。

内部サーバでは、DHCP オプション 43 はサポートされていません。 したがって、アクセス ポイントは、ローカル サブネット ブロードキャスト、ドメイン ネーム システム（DNS）、またはプライミングなどの別の方法を使用してスイッチの管理インターフェイスの IP アドレスを見つける必要があります。

内部 DHCP サーバ プールは、そのスイッチの無線クライアントだけをサポートし、他のスイッチのクライアントはサポートしません。 また、内部 DHCP サーバは、無線クライアントだけをサポートし、有線クライアントをサポートしません。

クライアントがスイッチの内部 DHCP サーバを使用する場合、IP アドレスは、再起動後には保持されません。 その結果、複数のクライアントに同じ IP アドレスが割り当てられることがあります。 IP アドレスの競合を解決するには、クライアントは既存の IP アドレスを解放し、新しいアドレスを要求する必要があります。 有線ゲストクライアントは常に、ローカルまたは外部コントローラに接続されたレイヤ 2 にあります。

（注） DHCPv6 は内部 DHCP サーバではサポートされません。

関連トピック

WLAN 用の DHCP 設定（CLI）, （59 ページ）

高度な WLAN プロパティの設定（GUI），（43 ページ）
DHCP for WLANs を設定するための前提条件，（53 ページ）
DHCP for WLANs の設定に関する制約事項，（54 ページ）

外部 DHCP サーバ

オペレーティング システムは、DHCP リレーをサポートする業界標準の外部 DHCP サーバを使用することにより、ネットワークに対しては DHCP リレーとして機能し、クライアントに対しては DHCP サーバとして機能するように設計されています。これは、各コントローラは、DHCP サーバに対しては DHCP リレー エージェントとして機能し、無線クライアントに対しては仮想 IP アドレスでの DHCP サーバとして機能することを意味します。

コントローラは DHCP サーバから取得したクライアント IP アドレスをキャプチャするため、スイッチ内、スイッチ間、およびサブネット間でのクライアント ローミング時に、各クライアントに対して同じ IP アドレスが保持されます。

（注） 外部 DHCP サーバは DHCPv6 をサポートします。

関連トピック

WLAN 用の DHCP 設定（CLI），（59 ページ）
高度な WLAN プロパティの設定（GUI），（43 ページ）
DHCP for WLANs を設定するための前提条件，（53 ページ）
DHCP for WLANs の設定に関する制約事項，（54 ページ）

DHCP 割り当て

DHCP はインターフェイスごとに、または WLAN ごとに設定できます。 特定のインターフェイスに割り当てられたプライマリ DHCP サーバのアドレスを使用することをお勧めします。

個々のインターフェイスに DHCP サーバを割り当てることができます。 プライマリおよびセカンダリ DHCP サーバの管理インターフェイス、AP マネージャ インターフェイス、動的インターフェイスの設定、DHCP サーバをイネーブルまたはディセーブルするためのサービス ポート インターフェイスの設定を行うことができます。 WLAN で DHCP サーバを定義することもできます。 この場合、サーバは、WLAN に割り当てられたインターフェイスの DHCP サーバアドレスを上書きします。

セキュリティに関する注意事項

高度なセキュリティが必要な場合は、すべてのクライアントが DHCP サーバから IP アドレスを取得するように設定してください。 この要件を適用するために、DHCP アドレスですべての WLAN を設定できます。 Assignment Required 設定で設定して、クライアントの固定 IP アドレスが禁止さ

れるようにします。 DHCP Addr. Assignment Required が選択されている場合、クライアントは DHCP を使って IP アドレスを取得する必要があります。 固定 IP アドレスを持つクライアントはすべて、ネットワーク上で許可されなくなります。 クライアントの DHCP プロキシとして動作するスイッチが、DHCP トラフィックを監視します。

（注） 無線による管理をサポートする WLAN では、管理（デバイスサービシング）クライアントが DHCP サーバから IP アドレスを取得できるようにする必要があります。

セキュリティが多少劣ってもかまわない場合は、DHCP Addr. Assignment Required を無効に設定して WLAN を作成できます。 その後クライアントは、固定 IP アドレスを使用するか、指定された DHCP サーバの IP アドレスを取得するかを選択できます。

（注） DHCP アドレス 有線ゲスト LAN に対する Assignment Required は、サポートされていません。

個別の WLAN は、 [DHCP アドレス割り当て必須（DHCP Address Assignment Required）] を無効にして作成できます。 これは、スイッチの DHCP プロキシがイネーブルの場合だけです。 DHCP プロキシをディセーブルにする必要があるプライマリ/セカンダリ コンフィギュレーションの DHCP サーバを定義しないでください。 このような WLAN では、すべての DHCP 要求がドロップするため、クライアントは固定 IP アドレスを使用しなければなりません。 これらの WLAN は、無線接続による管理をサポートしていません。

関連トピック

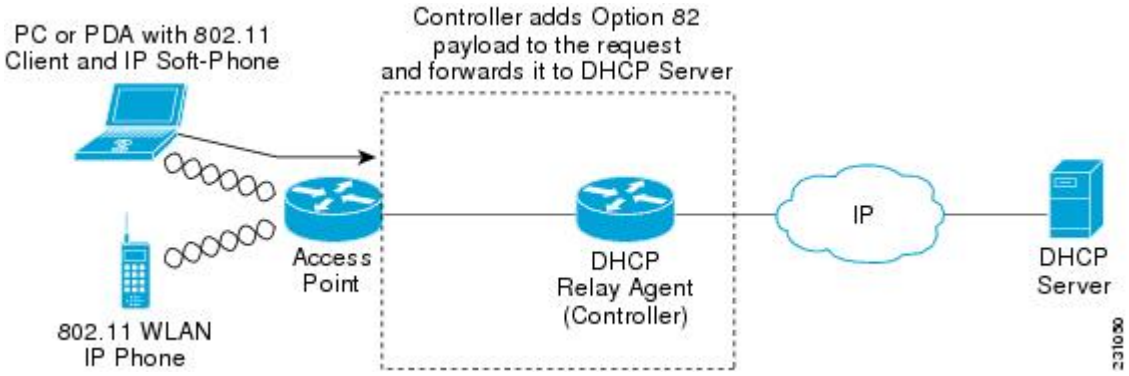
WLAN 用の DHCP 設定（CLI）, （59 ページ）
高度な WLAN プロパティの設定（GUI）, （43 ページ）
DHCP for WLANs を設定するための前提条件, （53 ページ）
DHCP for WLANs の設定に関する制約事項, （54 ページ）

DHCP オプション 82 について

DHCP オプション 82 では、DHCP を使用してネットワーク アドレスを割り当てる場合のセキュリティが強化されます。 スイッチが DHCP リレーエージェントとして動作して、信頼できないソー

スからの DHCP クライアント要求を阻止できるようにします。 DHCP サーバに転送するようにクライアントからの DHCP 要求にオプション 82 情報を追加するようにスイッチを設定できます。

図 *1*：*DHCP* オプション *82*



アクセス ポイントは、クライアントからのすべての DHCP 要求をスイッチに転送します。 スイッチは、DHCP オプション 82 ペイロードを追加してから要求を DHCP サーバに転送します。 このオプションの設定方法によって、ペイロードには MAC アドレス、または MAC アドレスとアクセス ポイントの SSID が含まれます。

（注） すでにリレー エージェント オプションが含まれている DHCP パケットは、スイッチでドロップされます。

DHCP オプション 82 が正しく動作するには、DHCP プロキシが有効でなければなりません。

関連トピック

WLAN 用の DHCP 設定（CLI），（59 ページ）
高度な WLAN プロパティの設定（GUI），（43 ページ）
DHCP for WLANs を設定するための前提条件，（53 ページ）
DHCP for WLANs の設定に関する制約事項，（54 ページ）

DHCP スコープの設定

関連トピック

WLAN 用の DHCP 設定（CLI），（59 ページ）
高度な WLAN プロパティの設定（GUI），（43 ページ）
DHCP for WLANs を設定するための前提条件，（53 ページ）
DHCP for WLANs の設定に関する制約事項，（54 ページ）

DHCP スコープについて

コントローラには組み込みの DHCP リレーエージェントがあります。 ただし、別個の DHCP サーバを持たないネットワークセグメントを求められる場合、コントローラに IP アドレスとサブネットマスクを無線クライアントに割り当てる組み込みの DHCP スコープを設定できます。 一般に、1 つのコントローラには、それぞれある範囲の IP アドレスを指定する複数の DHCP スコープを設定できます。

DHCP スコープは内部 DHCP が機能するために必要となります。 コントローラで DHCP が定義された後、管理インターフェイス、AP マネージャ インターフェイス、動的インターフェイスのプライマリ DHCP サーバの IP アドレスをコントローラの管理インターフェイスにポイントできます。

関連トピック

WLAN 用の DHCP 設定（CLI）, （59 ページ）
高度な WLAN プロパティの設定（GUI）, （43 ページ）
DHCP for WLANs を設定するための前提条件, （53 ページ）
DHCP for WLANs の設定に関する制約事項, （54 ページ）
DHCP スコープの設定（CLI）, （62 ページ）

DHCP for WLANs の設定方法

WLAN 用の DHCP 設定（CLI）

WLAN で次の DHCP パラメータを設定するには、次の手順に従います。

- DHCP オプション 82 ペイロード
- DHCP（必須）
- DHCP オーバーライド

はじめる前に

- WLAN を設定するには admin 権限がなければなりません。
- DHCP のオーバーライドを設定するには、DHCP サーバの IP アドレスが必要です。

手順の概要

1. **configure terminal**
2. **shutdown**
3. **wlan** *profile-name*
4. **ip dhcp opt82** {**ascii** | **format** {*add-ssid* | *ap-ethmac*} | **rid**}
5. **ip dhcp required**
6. **ip dhcp server** *ip-address*
7. **no shutdown**
8. **end**
9. **show wlan** *wlan-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**shutdown** 例： `Switch(config)# shutdown`	WLAN をシャットダウンします。
ステップ 3	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は、設定されている WLAN のプロファイル名です。

ステップ 4	**ip dhcp opt82** {**ascii**	**format** {*add-ssid*	*ap-ethmac*}	**rid**}
				
				例：
				`Switch(config)# ip dhcp opt82 format add-ssid`
					WLAN で DHCP82 ペイロードを指定します。 キーワードおよび引数は、次のとおりです。
					• **ascii**：DHCP オプション 82 の ASCII を設定します。 これが設定されていない場合、オプション 82 の形式は ASCII 形式に設定されます。
					• **format**：DHCP オプション 82 の形式を指定します。 次のオプションを使用できます。
					  • *add-ssid*：AP 無線の MAC アドレスおよび SSID である RemoteID 形式を設定します。
					  • *ap-ethmac*：AP Ethernet MAC アドレスである RemoteID 形式を設定します。

	コマンドまたはアクション	目的
		（注） フォーマット オプションが設定されていない場合、AP 無線の MAC アドレスだけが使用されます。 • **rid**：DHCP オプション 82 に Cisco 2 バイト RID を追加します。
ステップ 5	**ip dhcp required** 例： `Switch(config-wlan)# ip dhcp required`	DHCP サーバから IP アドレスをクライアントが取得することを必須にします。 スタティック クライアントは許可されません。
ステップ 6	**ip dhcp server** *ip-address* 例： `Switch(config-wlan)# ip dhcp server 200.1.1.2`	WLAN に割り当てられたインターフェイスの DHCP サーバ アドレスを上書きする WLAN 上の DHCP サーバを定義します。
ステップ 7	**no shutdown** 例： `Switch(config-wlan)# no shutdown`	WLAN を再起動します。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 9	**show wlan** *wlan-name* 例： `Switch(config-wlan)# show wlan test-wlan`	DHCP の設定を確認します。

関連トピック

Dynamic Host Configuration Protocol について，（55 ページ）
内部 DHCP サーバ，（55 ページ）
外部 DHCP サーバ，（56 ページ）
DHCP 割り当て，（56 ページ）
DHCP オプション 82 について，（57 ページ）
DHCP スコープの設定，（58 ページ）
DHCP スコープについて，（59 ページ）
DHCP for WLANs を設定するための前提条件，（53 ページ）
DHCP for WLANs の設定に関する制約事項，（54 ページ）

DHCP スコープの設定（CLI）

手順の概要

1. **configure terminal**
2. **ip dhcp pool** *pool-name*
3. **network** *network-name mask-address*
4. **dns-server** *hostname*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 2	**ip dhcp pool** *pool-name* 例： `Switch(config)#ip dhcp pool test-pool`	DHCP プール アドレスを設定します。
ステップ 3	**network** *network-name mask-address* 例： `Switch(dhcp-config)#network 209.165.200.224 255.255.255.0`	ドット付き 10 進表記とマスク アドレスでネットワーク番号を指定します。
ステップ 4	**dns-server** *hostname* 例： `Switch(dhcp-config)#dns-server example.com`	DNS ネーム サーバを指定します。 IP アドレスまたはホスト名を指定できます。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバルコンフィギュレーションモードを終了できます。

関連トピック

DHCP スコープについて，（59 ページ）

その他の関連資料

関連資料

関連項目	マニュアル タイトル
システム管理	*System Management Configuration Guide*（*Catalyst 3850* スイッチ）

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

DHCP for WLANs の機能情報

機能名	リリース	機能情報
WLAN の DHCP 機能	Cisco IOS XE 3.2SE	この機能が導入されました。

第 5 章

WLAN セキュリティの設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

レイヤ 2 セキュリティの前提条件

同じ SSID を持つ WLAN は、ビーコン応答とプローブ応答でアドバタイズされる情報に基づいてクライアントが WLAN を選択できるように、一意のレイヤ 2 セキュリティ ポリシーを使用している必要があります。 使用可能なレイヤ 2 セキュリティ ポリシーは、次のとおりです。

- なし（オープン WLAN）
- Static WEP または 802.1X

（注） Static WEP と 802.1X は両方とも、ビーコン応答とプローブ応答で同じビットによってアドバタイズされるので、クライアントはこれらを区別できません。したがって、同じ SSID を持つ複数の WLAN では、Static WEP と 802.1X の両方を使用できません。

- WPA/WPA2

（注） 同じ SSID を持つ複数の WLAN で WPA と WPA2 を使用することはできませんが、同じ SSID を持つ 2 つの WLAN は、PSK を使用する WPA/TKIP と 802.1X を使用する Wi-Fi Protected Access（WPA）/Temporal Key Integrity Protocol（WPA）で設定するか、802.1X を使用する WPA/TKIP または 802.1X を使用する WPA/AES で設定することができます。

関連トピック

静的 WEP と 802.1X レイヤ 2 セキュリティ パラメータの設定（CLI），（67 ページ）
レイヤ 2 パラメータの設定（GUI），（72 ページ）
静的 WEP レイヤ 2 セキュリティ パラメータの設定（CLI），（68 ページ）
レイヤ 2 パラメータの設定（GUI），（72 ページ）
WPA + WPA2 レイヤ 2 セキュリティ パラメータの設定（CLI），（69 ページ）
レイヤ 2 パラメータの設定（GUI），（72 ページ）
802.1X レイヤ 2 セキュリティ パラメータの設定（CLI），（71 ページ）
レイヤ 2 パラメータの設定（GUI），（72 ページ）
高度な WLAN プロパティの設定（CLI），（40 ページ）
AAA Override について，（66 ページ）

AAA Override について

WLAN の AAA Override オプションを使用すると、WLAN で Identity ネットワーキングを設定できます。 これにより、AAA サーバから返される RADIUS 属性に基づいて、個々のクライアントに VLAN タギング、Quality Of Service (QoS)、およびアクセス コントロール リスト (ACL) を適用することができます。

関連トピック

高度な WLAN プロパティの設定（CLI），（40 ページ）
レイヤ 2 セキュリティの前提条件，（65 ページ）

WLAN セキュリティの設定方法

静的 WEP と 802.1X レイヤ 2 セキュリティ パラメータの設定（CLI）

はじめる前に

管理者特権が必要です。

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **security static-wep-key** {**authentication** {**open** | **sharedkey**} | **encryption** {**104** | **40**} [**ascii** | **hex**] {**0**|**8**}} *wep-key wep-key-index1-4*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**security static-wep-key** {**authentication** {**open** | **sharedkey**} | **encryption** {**104** | **40**} [**ascii** | **hex**] {**0**|**8**}} *wep-key wep-key-index1-4* 例： `Switch(config-wlan)# security static-wep-key encryption 40 hex 0 test 2`	WLAN の静的 WEP セキュリティを設定します。 次のキーワードと引数があります。 • **authentication**：802.11 認証を設定します。 • **encryption**：静的 WEP キーとインデックスを設定します。 • **open**：オープン システム認証を設定します。 • **sharedkey**：共有キー認証を設定します。 • **104, 40**：WEP キーのサイズを指定します。 • **hex, ascii**：キーの入力形式を指定します。 • *wep-key-index*、*wep-key-index1-4* 指定するパスワードのタイプです。 値が 0 である場合は、暗号化されないパスワードを指定することを示します。 値が 8 である場合は、AES 暗号化を指定することを示します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

レイヤ 2 セキュリティの前提条件, （65 ページ）

静的 WEP レイヤ 2 セキュリティ パラメータの設定（CLI）

はじめる前に

管理者特権が必要です。

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **security static-wep-key** [**authentication** {**open** | **shared**} | **encryption** {**104** | **40**} {**ascii** | **hex**} [**0** | **8**]]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**security static-wep-key** [**authentication** {**open** | **shared**} | **encryption** {**104** | **40**} {**ascii** | **hex**} [**0** | **8**]] 例： `Switch(config-wlan)# security static-wep-key authentication open`	キーワードは次のとおりです。 • **static-wep-key**：静的 WEP キーの認証を設定します。 • **authentication**：ユーザが設定できる認証タイプを指定します。 値は、open および shared です。

	コマンドまたはアクション	目的
		• **encryption**：ユーザが設定できる暗号化タイプを指定します。有効な値は 104 と 40 です。 40 ビットキーには、ASCII テキスト文字が 5 文字と 16 進数文字が 10 文字必要です。 104 ビットキーには、ASCII テキスト文字が 13 文字と 16 進数文字が 26 文字必要です。 • **ascii**：ASCII としてキー形式を指定します。 • **hex**：HEX としてキー形式を指定します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

レイヤ 2 セキュリティの前提条件, （65 ページ）

WPA + WPA2 レイヤ 2 セキュリティ パラメータの設定（CLI）

（注） デフォルト セキュリティ ポリシーは、WPA2 です。

はじめる前に

管理者特権が必要です。

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **security wpa**
4. **security wpa wpa1**
5. **security wpa wpa1 ciphers** [**aes** | **tkip**]
6. **security wpa wpa2**
7. **security wpa wpa2 ciphers** [**aes** | **tkip**]
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**security wpa** 例： `Switch(config-wlan)# security wpa`	WPA をイネーブルにします。
ステップ 4	**security wpa wpa1** 例： `Switch(config-wlan)# security wpa wpa1`	WPA1 をイネーブルにします。
ステップ 5	**security wpa wpa1 ciphers** [**aes** | **tkip**] 例： `Switch(config-wlan)# security wpa wpa1 ciphers aes`	WPA1 暗号を指定します。 次のいずれかの暗号化タイプを選択します。 • **aes**：WPA/AES のサポートを指示します。 • **tkip**：WPA/TKIP のサポートを指示します。
ステップ 6	**security wpa wpa2** 例： `Switch(config-wlan)# security wpa`	WPA 2 をイネーブルにします。
ステップ 7	**security wpa wpa2 ciphers** [**aes** | **tkip**] 例： `Switch(config-wlan)# security wpa wpa2 ciphers tkip`	WPA2 暗号化を設定します。 次のいずれかの暗号化タイプを選択します。 • **aes**：WPA/AES のサポートを指示します。 • **tkip**：WPA/TKIP のサポートを指示します。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

レイヤ 2 セキュリティの前提条件, （65 ページ）

802.1X レイヤ 2 セキュリティ パラメータの設定（CLI）

はじめる前に

管理者特権が必要です。

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **security dot1x**
4. **security** [**authentication-list** *auth-list-name* | **encryption** {**0** | **104** | **40**}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**security dot1x** 例： `Switch(config-wlan)# security dot1x`	802.1X セキュリティを指定します。
ステップ 4	**security** [**authentication-list** *auth-list-name*	**encryption** {**0**	**104**	**40**} 例： `Switch(config-wlan)# security encryption 104`	次のキーワードと引数があります。 • **authentication-list**：IEEE 802.1X の認証リストを指定します。 • **encryption**：CKIP 暗号キーの長さを指定します。 有効な値は、0、40、および 104 です。 ゼロ（0）では暗号化されません。 これはデフォルトです。 （注） WLAN 内のすべてのキーは、同じサイズでなければなりません。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

レイヤ 2 セキュリティの前提条件, （65 ページ）

レイヤ 2 パラメータの設定（GUI）

はじめる前に

- 管理者特権が必要です。

ステップ 1 [Configuration] > [WLAN] > をクリックします。
[WLANs] ページが表示されます。

ステップ 2 設定する WLAN の WLAN プロファイルをクリックします。
[WLANs] > [Edit] > ページが表示されます。

ステップ 3 [Security] > [Layer 2] > タブをクリックします。

パラメータ	説明
Layer2 Security	選択した WLAN のレイヤ 2 セキュリティ。 値は次のとおりです。 • None—No：レイヤ 2 セキュリティは選択されていません。 • WPA+WPA2：Wi-Fi Protected Access。 • 802.1X：WEP 802.1X データ暗号化のタイプ。 これらの設定については、レイヤ 2 802.1X パラメータに関するトピックを参照してください。 • Static WEP：静的 WEP 暗号化パラメータ。 • Static WEP + 802.1x：静的 WEP および 802.1X の両パラメータ。
MAC Filtering	MAC アドレス フィルタリング [MAC Filters] > [New page] で、実際の MAC アドレスによってローカルにクライアントを設定できます。 そうでない場合は、RADIUS サーバのクライアントを構成します。 （注） MAC フィルタは、MAC Authentication By Pass（MAB）として知られています。
Fast Transition	アクセス ポイント間の高速移行をイネーブルまたはディセーブルにするチェックボックス。
Over the DS	分散システム上の高速移行をイネーブルまたはディセーブルにするチェックボックス。

パラメータ	説明
Reassociation Timeout	高速移行の再アソシエーションがタイムアウトになるまでの時間（秒単位）。

WPA + WPA2 パラメータを設定するには、次の詳細情報を提供します。

パラメータ	説明
WPA Policy	WPA Policy をイネーブルまたはディセーブルにするチェックボックス。
WPA Encryption	WPA2 encryption type: TKIP または AES。 WPA ポリシーがイネーブルな場合だけ使用可能です。
WPA2 Policy	WPA2 Policy をイネーブルまたはディセーブルにするチェックボックス。
WPA2 Encryption	WPA2 encryption type: TKIP または AES。 WPA2 ポリシーがイネーブルな場合だけ使用可能です。
Authentication Key Management（認証キー管理）	再生成メカニズム パラメータ。 値は次のとおりです。 • 802.1X • CCKM • PSK • 802.1x + CCKM
PSK Format	認証キー管理の PSK 値を選択するとイネーブルになります。 ASCII 形式または 16 進形式を選択し、事前共有キーを入力します。

802.1x パラメータを設定するには、次の詳細情報を入力します。

パラメータ	説明
802.11 data encryption	WEP 802.11 データ暗号化タイプ。
Type	セキュリティ タイプ。

パラメータ	説明
Key size	キー サイズ。 値は次のとおりです。 • なし • 40 ビット • 104 ビット サードパーティの AP WLAN（17）は 802.1X 暗号化としてのみ設定できます。 ドロップダウン設定可能な 802.1X パラメータは、この WLAN には使用できません。

静的 WEP を指定するには、次のパラメータを設定します。

パラメータ	説明
802.11 Data Encryption	静的 WEP 暗号化タイプ。
Current Key	現在選択されているキーの詳細を表示します。
Type	セキュリティ タイプ。
Key size	キー サイズ。 値は次のとおりです。 • 未設定 • 40 ビット • 104 ビット
Key Index	1～4 のインデックス。 各 WLAN に 1 つの一意な WEP キー インデックスを適用できます。 WEP キー インデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化には 4 つの WLAN しか設定できません。 WEP キー インデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化には 4 つの WLAN しか設定できません。
Encryption Key	暗号化キー。
Key Format	ASCII または 16 進の暗号キー形式を選択します。
Allow Shared Key Authentication	自身がイネーブルまたはディセーブルに設定できる認証キー。

静的 WEP と 802.1X パラメータを設定するには

パラメータ	説明
Static WEP Parameters	
802.11 Data Encryption	静的 WEP 暗号化タイプ。
Current Key	現在選択されているキーの詳細を表示します。
Type	セキュリティ タイプ。
Key size	キー サイズ。 値は次のとおりです。 • 未設定 • 40 ビット • 104 ビット
Key Index	1～4 のインデックス。 各 WLAN に 1 つの一意な WEP キー インデックスを適用できます。 WEP キー インデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化には 4 つの WLAN しか設定できません。 WEP キー インデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化には 4 つの WLAN しか設定できません。
Encryption Key	暗号化キー。
Key Format	ASCII または 16 進の暗号キー形式を選択します。
Allow Shared Key Authentication	自身がイネーブルまたはディセーブルに設定できる認証キー。
802.1x Parameters	
802.11 Data Encryption	静的 WEP 暗号化タイプ。
Current Key	表示のみ。 現在選択されているキーの詳細。
Type	セキュリティ タイプ。
Key size	キー サイズ。 値は次のとおりです。 • 未設定 • 40 ビット • 104 ビット

パラメータ	説明
Key Index	1～4 のインデックス。 各 WLAN に 1 つの一意な WEP キー インデックスを適用できることに注意してください。 WEP キー インデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化には 4 つの WLAN しか設定できません。
Encryption Key	暗号化キー。
Key Format	ASCII または 16 進の暗号キー形式を選択します。
Allow Shared Key Authentication	自身がイネーブルまたはディセーブルに設定できる認証キー。

ステップ 4 [Apply] をクリックします。

関連トピック

レイヤ 2 セキュリティの前提条件, （65 ページ）
レイヤ 2 セキュリティの前提条件, （65 ページ）
レイヤ 2 セキュリティの前提条件, （65 ページ）
レイヤ 2 セキュリティの前提条件, （65 ページ）

その他の関連資料

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	*WLAN Command Reference, Cisco IOS XE Release 3SE*（*Catalyst 3850* スイッチ）
セキュリティ コンフィギュレーション ガイド	*Security Configuration Guide*（*Catalyst 3850* スイッチ）

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

WLAN レイヤ 2 セキュリティに関する機能情報

次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能名	リリース	機能情報
WLAN のセキュリティ機能	Cisco IOS XE 3.2SE	この機能が導入されました。

第 6 章

WLAN ごとのクライアント カウントの設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

WLAN ごとのクライアント カウントの設定に関する制約事項

- WLAN が接続クライアントの最大数の制限に達しているか、AP 無線および新しいクライアントが WLAN に参加しようとしている場合、クライアントは既存のクライアントが切断されるまで WLAN に接続できません。

- ローミング クライアントは新しいクライアントと見なされます。 クライアントの接続数の最大制限に到達している WLAN に対して新しいクライアントは、既存のクライアントが切断されたときにのみ接続できます。

（注） サポートされているクライアント数の詳細については、スイッチの製品データ シートを参照してください。

関連トピック

WLAN ごとのクライアント カウントの設定（CLI），（81 ページ）
WLAN ごとの各 AP のクライアント数の設定（CLI），（82 ページ）
WLAN あたりの AP 無線ごとのクライアント数の設定（CLI），（83 ページ）
WLAN ごとのクライアント カウントの設定について，（80 ページ）

WLAN ごとのクライアント カウントの設定について

WLAN に接続できるクライアントの数に制限を設定できます。これは、スイッチに接続できるクライアントの数に制限があるシナリオで役立ちます。 たとえば、スイッチが WLAN 上の最大 256 個のクライアントに対応でき、これらのクライアントが企業ユーザ（従業員）およびゲスト ユーザ間で共有される場合について考えます。 特定の WLAN にアクセス可能なゲスト クライアントの数に制限を設定できます。 WLAN ごとに設定できるクライアントの数は、使用しているプラットフォームによって異なります。

関連トピック

WLAN ごとのクライアント カウントの設定（CLI），（81 ページ）
WLAN ごとの各 AP のクライアント数の設定（CLI），（82 ページ）
WLAN あたりの AP 無線ごとのクライアント数の設定（CLI），（83 ページ）
WLAN ごとのクライアント カウントの設定に関する制約事項，（79 ページ）
クライアントの接続の監視（CLI），（83 ページ）

WLAN ごとのクライアント カウントを設定する方法

WLAN ごとのクライアント カウントの設定（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **client association limit** *limit*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**client association limit** *limit* 例： `Switch(config-wlan)# client association limit 2000`	WLAN ごとのクライアント アソシエーションの最大数を設定します。 範囲は 0 ～ 2000 です。 デフォルト値は 0 です（制限なし）。
ステップ 4	**end** 例： `Switch(wlan-config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN ごとのクライアント カウントの設定について，（80 ページ）
WLAN ごとのクライアント カウントの設定に関する制約事項，（79 ページ）
クライアントの接続の監視（CLI），（83 ページ）

WLAN ごとの各 AP のクライアント数の設定（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **client association limit ap** *ap-limit*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**client association limit ap** *ap-limit* 例： `Switch(config-wlan)# client association limit ap 250`	WLAN ごとの AP あたりの最大クライアント数を設定します。 範囲は 1 ～ 400 です。
ステップ 4	**end** 例： `Switch(wlan-config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN ごとのクライアント カウントの設定について，（80 ページ）
WLAN ごとのクライアント カウントの設定に関する制約事項，（79 ページ）
クライアントの接続の監視（CLI），（83 ページ）

WLAN あたりの AP 無線ごとのクライアント数の設定（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **client association limit radio** *max-client-connections*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**client association limit radio** *max-client-connections* 例： `Switch(config-wlan)# client association limit radio 180`	WLAN あたりの AP 無線ごとのクライアント接続の最大数を設定します。 a、b、および g 無線でこの範囲は 0～200 です。
ステップ 4	**end** 例： `Switch(config-wlan)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

WLAN ごとのクライアント カウントの設定について, （80 ページ）
WLAN ごとのクライアント カウントの設定に関する制約事項, （79 ページ）
クライアントの接続の監視（CLI）, （83 ページ）

クライアントの接続の監視（CLI）

次のコマンドがスイッチクライアント接続の監視に使用できます。

コマンド	説明

show wlan name *wlan-name*	WLAN プロパティを表示します。 次に例を示します。
	`. . . .`
	`Max Associated Clients per WLAN :0`
	`Max Associated Clients per AP per WLAN :0`
	`Max Associated Clients per AP Radio per WLAN :0`
	`. . .`
	`. . .`

show wlan id *wlan-id*	WLAN プロパティを表示します。 次に例を示します。
	`. . . .`
	`Max Associated Clients per WLAN :0`
	`Max Associated Clients per AP per WLAN :0`
	`Max Associated Clients per AP Radio per WLAN :0`
	`. . .`
	`. . .`

関連トピック

WLAN ごとのクライアント カウントの設定（CLI），（81 ページ）
WLAN ごとの各 AP のクライアント数の設定（CLI），（82 ページ）
WLAN あたりの AP 無線ごとのクライアント数の設定（CLI），（83 ページ）
WLAN ごとのクライアント カウントの設定について，（80 ページ）

クライアント接続に関する追加情報

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	*WLAN Command Reference, Cisco IOS XE Release 3SE*（*Catalyst 3850* スイッチ）

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
このリリースのすべての MIB です。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

WLAN ごとのクライアント接続に関する機能情報

次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能名	リリース	機能情報
WLAN、AP、AP 無線ごとのクライアント接続	Cisco IOS XE 3.3SE	この機能が導入されました。

第 7 章

802.11w の設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

802.11w の前提条件

- オプションおよび必須の 802.11w 機能を設定するには、WPA および AKM を設定する必要があります。

（注） Robust Secure Network（RNS）IE は AES 暗号化とともにイネーブルにする必要があります。

- 必須として 802.11w を設定するには、WPA AKM に加えて PMF AKM を有効にします。

関連トピック

802.11w の設定（CLI），（89 ページ）
802.11w のディセーブル（CLI），（91 ページ）
802.11w に関する情報，（88 ページ）

802.11w の制約事項

- 802.11w はオープン WLAN、 WEP 暗号化 WLAN、または TKIP 暗号化 WLAN に適用されていません。
- 802.11w が設定された WLAN では、WPA2-PSK または WPA2-802.1x セキュリティを設定する必要があります。

関連トピック

802.11w の設定（CLI），（89 ページ）
802.11w のディセーブル（CLI），（91 ページ）
802.11w に関する情報，（88 ページ）

802.11w に関する情報

Wi-Fiは、正規のデバイスまたは不法なデバイスのいずれであっても、あらゆるデバイスで傍受または参加が可能なブロードキャスト メディアです。 認証/認証解除、アソシエーション/ディスアソシエーション、ビーコンおよびプローブなどの制御/管理フレームは、無線クライアントによって、AP を選択し、ネットワーク サービスのセッションを開始するために使用されます。

機密保持レベルを提供する暗号化可能なデータ トラフィックとは異なり、これらのフレームは、すべてのクライアントによって解釈されることが必要であり、したがってオープンまたは非暗号化形式で送信されます。 これらのフレームは暗号化できませんが、攻撃から無線メディアを保護するために偽造を防止することが必要になります。 たとえば、攻撃者はクライアントと AP の間のセッションを切断するために、AP から管理フレームをスプーフィングする可能性があります。

802.11w プロトコルは、管理フレーム保護（PMF）サービスによって保護された一連の強力な管理フレームにのみ適用されます。 これらには、ディスアソシエーション、認証解除、ロバストアクション フレームが含まれます。

したがって、ロバストアクションであり、保護されているものと見なされる管理フレームは次のとおりです。

- スペクトラム管理
- QoS
- ブロック ACK
- SA クエリー
- ベンダー固有保護

802.11w が無線メディアで実行されると、次のことが行われます。

- ディスアソシエーションフレームと認証解除フレームに対して、（MIC 情報要素を含めることにより）AP の暗号保護によるクライアント保護が追加されます。これによって、DoS 攻撃でのスプーフが防止されます。
- アソシエーションの復帰期間と SA クエリーの手順から構成されるセキュリティ アソシエーション（SA）ティアダウン保護メカニズムを追加することによって、インフラストラクチャの保護が追加され、スプーフィングされた要求によるすでに接続済みのクライアントの切断が防止されます。

関連トピック

802.11w の設定（CLI），（89 ページ）
802.11w のディセーブル（CLI），（91 ページ）
802.11w の前提条件，（87 ページ）
802.11w の制約事項，（88 ページ）
802.11w の監視（CLI），（93 ページ）

802.11w の設定方法

802.11w の設定（CLI）

はじめる前に

WPA および AKM を設定する必要があります。

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **security pmf** {**association-check** *association-comeback-time-in-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-in-milliseconds*}
5. **no shutdown**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： `Switch shutdown`	PMF を設定する前に WLAN をシャットダウンします。
ステップ 4	**security pmf** {**association-check** *association-comeback-time-in-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-in-milliseconds*} 例： `Switch(config-wlan)# security pmf saquery-retry-time 200`	次のオプションにより PMF パラメータを設定します。 • **association-comeback**：802.11w のアソシエーションの復帰期間を設定します。 範囲は、1 ～ 20 秒です。 • **mandatory**：クライアントが WLAN の 802.11w PMF 保護をネゴシエートすることを要求します。 • **optional**：WLAN の 802.11w PMF 保護を有効にします。 • **saquery**：SA のクエリー応答で想定される時間間隔（ミリ秒単位）です。スイッチが応答を受け取らなかった場合、別の SQ クエリーが試行されます。 範囲は 100 ～ 500 ミリ秒です。 値には 100 ミリ秒の倍数を指定する必要があります。

	コマンドまたはアクション	目的
ステップ 5	**no shutdown** 例： `Switch no shutdown`	変更内容を反映するために、WLAN サーバを再起動します。
ステップ 6	**end** 例： `Switch(config-wlan)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

802.11w に関する情報, （88 ページ）
802.11w の前提条件, （87 ページ）
802.11w の制約事項, （88 ページ）
802.11w の監視（CLI）, （93 ページ）

802.11w のディセーブル（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **shutdown**
4. **no security pmf [association-comeback** *association-check-comback-interval-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-interval-milliseconds*]
5. **no shutdown**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： `Switch shutdown`	PMF を設定する前に WLAN をシャットダウンします。
ステップ 4	**no security pmf [association-comeback** *association-check-comback-interval-seconds* | **mandatory** | **optional** | **saquery** *saquery-time-interval-milliseconds*] 例： `Switch(config-wlan)# no security pmf`	WLAN の PMF をディセーブルにします。 次の属性を使用できます。 • **association-comeback**：802.11w のアソシエーションの復帰期間をディセーブルにします。 • **mandatory**：クライアントが WLAN の 802.11w PMF 保護をネゴシエートすることをディセーブルにします。 • **optional**：WLAN の 802.11w PMF 保護をディセーブルにします。 • **saquery**：アソシエーションを再試行する前に、すでにアソシエートされているクライアントへのアソシエーション応答で特定される時間間隔。 アソシエーションの復帰期間中、この時間間隔により、クライアントが実際のクライアントであり、不正なクライアントではないかどうかが確認されます。 クライアントがこの時間内に応答しない場合は、クライアント アソシエーションがスイッチから削除されます。 範囲は 100 ～ 500 ミリ秒です。 値には 100 ミリ秒の倍数を指定する必要があります。
ステップ 5	**no shutdown** 例： `Switch no shutdown`	変更内容を反映するために、WLAN サーバを再起動します。
ステップ 6	**end** 例： `Switch(config-wlan)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

802.11w に関する情報, （88 ページ）

802.11w の前提条件, （87 ページ）
802.11w の制約事項, （88 ページ）
802.11w の監視（CLI）, （93 ページ）

802.11w の監視（CLI）

802.11w の監視に使用できるコマンドは次のとおりです。

コマンド	説明

show wlan name *wlan-profile-name*	WLAN の WLAN パラメータを表示します。PMF パラメータが表示されます。 次に例を示します。
	`. . . .`
	`. . . .`
	`Auth Key Management`
	`  802.1x :`
	` Disabled`
	`  PSK :`
	` Enabled`
	`  CCKM :`
	` Disabled`
	`  FT dot1x :`
	` Disabled`
	`  FT PSK :`
	` Disabled`
	`  PMF dot1x :`
	` Disabled`
	`  PMF PSK :`
	` Enabled`
	`  FT Support :`
	` Disabled`
	`  FT Reassociation Timeout :`
	` 20`
	`  FT Over-The-DS mode :`
	` Disabled`
	`  PMF Support :`
	` Required`
	`  PMF Association Comeback Timeout :`
	` 9`
	`  PMF SA Query Time :`
	` 200`
	`. . . .`
	`. . . .`

関連トピック

802.11w の設定（CLI）, （89 ページ）
802.11w のディセーブル（CLI）, （91 ページ）
802.11w に関する情報, （88 ページ）

802.11w に関する追加情報

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	*WLAN Command Reference, Cisco IOS XE Release 3SE*（*Catalyst 3850* スイッチ）
WLAN セキュリティ	このマニュアルの *WLAN*セキュリティの設定の章

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
802.11W	IEEE 802.11w 保護管理フレーム

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

802.11w の機能に関する情報

次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能名	リリース	機能情報
802.11w	Cisco IOS XE 3.3SE	この機能が導入されました。

第 8 章

Wi-Fi Direct クライアント ポリシーの設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

Wi-Fi Direct クライアント ポリシーの制限

Wi-Fi Direct クライアント ポリシーは、ローカル モードの AP が含まれる WLAN のみに適用できます。

Wi-Fi Direct クライアント ポリシーについて

Wi-Fi Direct 対応のデバイスは迅速な相互接続が可能で、印刷、同期、データ共有などのタスクを効率的に実行できます Wi-Fi Direct デバイスは、複数のピアツーピア（P2P）デバイスおよびインフラストラクチャ無線 LAN（WLAN）に同時にアソシエートしている場合があります。 コントローラを使用して、Wi-Fi Direct クライアント ポリシーを WLAN 単位で設定できます。その際、Wi-Fi デバイスとインフラストラクチャ WLAN のアソシエーションを許可または禁止するか、WLAN に対して Wi-Fi Direct クライアント ポリシーをすべて無効にすることができます。

関連トピック

Wi-Fi Direct クライアント ポリシーの設定（CLI），（98 ページ）
Wi-Fi Direct クライアント ポリシーのディセーブル（CLI），（100 ページ）
Wi-Fi Direct クライアント ポリシーの監視（CLI），（100 ページ）

Wi-Fi Direct クライアント ポリシーの設定方法

Wi-Fi Direct クライアント ポリシーの設定（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **wifidirect policy** {**permit** | **deny** }
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は、設定されている WLAN のプロファイル名です。

	コマンドまたはアクション	目的

ステップ 3	**wifidirect policy** {**permit** | **deny** }
	
	例：
	`Switch(config-wlan)#` **`wifidirect policy permit`**
		次のいずれかを使用して WLAN の Wi-Fi Direct クライアント ポリシーを設定します
		
		• **permit**：Wi-Fi Direct クライアントと WLAN のアソシエーションをイネーブルにします。
		
		• **deny**：Wi-Fi クライアント ポリシーが「拒否」に設定されている場合は、デバイス機能に基づいてスイッチが Wi-Fi Direct デバイスを許可または拒否します。 Wi-Fi Direct デバイスは、スイッチへのアソシエーション要求でこれらの機能をにレポートします。これは、このデバイスの Wi-Fi 機能に基づいて行われます。 次の作業を行います。
		
		  • 同時操作
		
		  • 相互接続
		
		（注） コマンド **no wifidirect policy** は、クライアントの Wi-Fi Direct ステータスを無視します。 さらに、アクセスポイントはビーコンおよびプローブをアドバタイズしません。 実際には、このコマンドの **no** 形式では、WLAN の Wi-Fi Direct 機能はディセーブルになります。
		
		Wi-Fi デバイスが同時操作または相互接続、あるいはその両方をサポートする場合は、クライアントの関連付けは拒否されます。 クライアントは、デバイスが同時操作と相互接続をサポートしない場合に関連付けることができます。

ステップ 4	**end** 例： `Switch(config-wlan)#` **`end`**	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

Wi-Fi Direct クライアント ポリシーについて，（98 ページ）
Wi-Fi Direct クライアント ポリシーの監視（CLI），（100 ページ）

Wi-Fi Direct クライアント ポリシーのディセーブル（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **no wifidirect policy**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**no wifidirect policy** 例： `Switch(config)# no wifidirect policy`	クライアントの Wi-Fi Direct ステータスを無視し、それによって Wi-Fi Direct クライアントのアソシエーションを許可します
ステップ 4	**end** 例： `Switch(config-wlan)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

Wi-Fi Direct クライアント ポリシーについて，（98 ページ）
Wi-Fi Direct クライアント ポリシーの監視（CLI），（100 ページ）

Wi-Fi Direct クライアント ポリシーの監視（CLI）

次のコマンドが Wi-Fi Direct クライアント ポリシーを監視するために使用できます。

コマンド	説明
show wireless client wifidirect stats	関連付けられたクライアントの総数と、Wi-Fi Direct クライアント ポリシーを有効にした場合に拒否されたアソシエーション要求の数が表示されます。
show wlan summary	WLAN での Wi-Fi Direct の状態を表示します。
show wireless cli mac-address *mac-address*	クライアントの詳細情報を表示します。

関連トピック

Wi-Fi Direct クライアント ポリシーの設定（CLI），（98 ページ）
Wi-Fi Direct クライアント ポリシーのディセーブル（CLI），（100 ページ）
Wi-Fi Direct クライアント ポリシーについて，（98 ページ）

Wi-Fi Direct クライアント ポリシーに関する追加リファレンス

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	*WLAN Command Reference, Cisco IOS XE Release 3SE（Catalyst 3850 スイッチ）*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Wi-Fi Direct クライアント ポリシーに関する機能情報

機能名	リリース	機能情報
Wi-Fi Direct の機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 9 章

802.11r BSS の高速移行の設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

802.11r 高速移行の制約事項

- 802.11r クライアント アソシエーションは、スタンドアロン モードのアクセス ポイントではサポートされません。
- 802.11r 高速ローミングは、スタンドアロン モードのアクセス ポイントではサポートされません。

- ローカル認証 WLAN と中央認証 WLAN 間の 802.11r 高速ローミングはサポートされていません。
- EAP LEAP 方式はサポートされません。
- TSpec は 802.11r 高速ローミングではサポートされません。 したがって、RIC IE の処理はサポートされません。
- WAN リンク遅延がある場合、高速ローミングも遅延します。 音声またはデータの最大遅延を確認する必要があります。 コントローラは、無線およびOver-the-DS DS 方式の両方をローミングする間、802.11r 高速移行の認証要求を処理します。
- この機能は、オープンで WPA2 設定の WLAN でのみサポートされます。
- レガシー クライアントは、Robust Security Network Information Exchange（RSN IE）の解析を担当するサプリカントのドライバが古く、IE 内の追加 AKM を認識しない場合、802.11r が有効にされている WLAN にアソシエートできません。 この制限のため、クライアントは、WLAN にアソシエーション要求を送信できません。 ただし、これらのクライアントは、非 802.11r WLAN とアソシエートできます。 802.11r 対応クライアントは、802.11r と 802.11i の両方の認証キー管理スイートが有効にされている WLAN の 802.11i クライアントとしてアソシエートできます。

  回避策は、レガシー クライアントのドライバを新しい 802.11r AKM で動作するようにするか、またはアップグレードすることです。そうすることで、レガシークライアントは、802.11r 対応 WLAN と正常にアソシエートできます。

  もう 1 つの回避策は、同じ名前で異なるセキュリティ設定（FT および非 FT）の 2 つの SSID を持つことです。
- 高速移行のリソース要求プロトコルは、クライアントがこのプロトコルをサポートしていないため、サポートされません。 また、リソース要求プロトコルはオプションのプロトコルです。
- サービス不能（DoS）攻撃を回避するため、各コントローラでは、異なる AP と最大 3 つの高速移行ハンドシェイクが可能です。

関連トピック

オープン WLAN での 802.11r 高速移行の設定（CLI），（108 ページ）

802.11r 高速移行のディセーブル（CLI），（114 ページ）

Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI），（110 ページ）

PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI），（111 ページ）

802.11 高速移行の設定（GUI），（113 ページ）

802.11r の高速移行について，（105 ページ）

802.11r の高速移行について

高速ローミングの IEEE 標準である 802.11r は、クライアントがターゲット AP にローミングする前でも、新しい AP との最初のハンドシェイクが実行される、高速移行（FT）と呼ばれるローミングの新しい概念が導入されています。 初期ハンドシェイクによって、クライアントと AP が事前に Pairwise Transient Key（PTK）計算をできるようになります。 これらの PTK キーは、クライアントが新しいターゲット AP の再アソシエーション要求または応答の交換をした後で、クライアントと AP に適用されます。

802.11r は、次の 2 通りのローミングを提供します。

- 無線
- Over-the-DS（分散システム）

FT キー階層は、クライアントが各 AP での再認証なしで、AP 間の高速 BSS 移行ができるように設計されています。 WLAN設定には、FT（高速移行）と呼ばれる、新しい認証キー管理（AKM）タイプが含まれています。

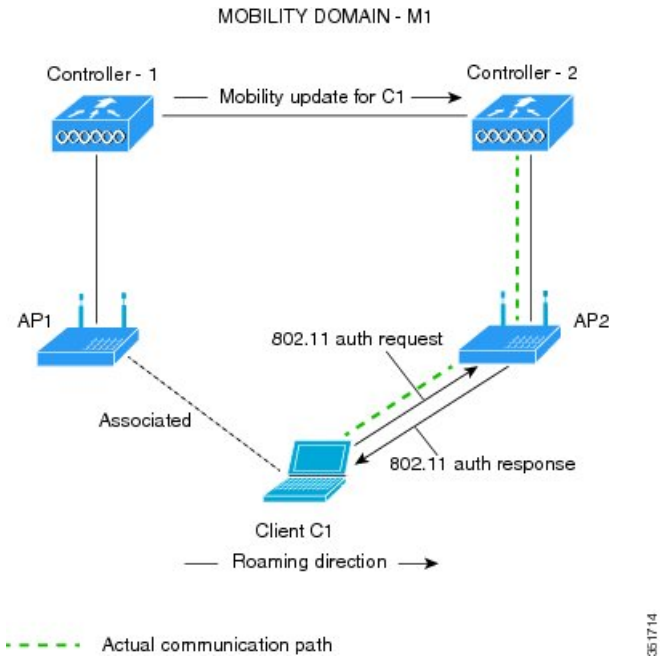
クライアントのローミング方法

FT プロトコルを使用して現在の AP からターゲット AP に移動するクライアントでは、メッセージ交換は次の 2 つの方法のいずれかを使用して行われます。

- 無線：クライアントは、FT 認証アルゴリズムを使用する IEEE 802.11 認証を使用して、ターゲット AP と直接通信を行います。
- Over-the-DS：クライアントは、現在の AP を介してターゲット AP と通信します。 クライアントとターゲット AP との間の通信は、クライアントと現在の AP 間の FT アクション フレームで実行されてから、コントローラによって送信されます。

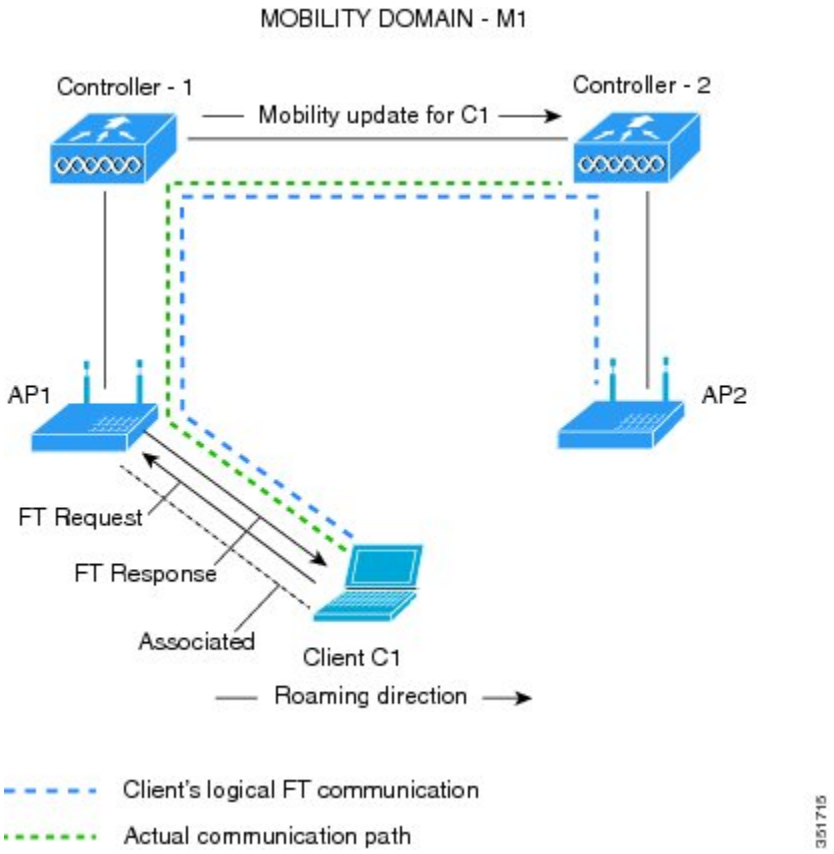
この図は、Over the Air クライアントのローミングを設定するときに実行されるメッセージ交換のシーケンスを示します。

図 *2*：***Over the Air*** クライアントのローミングの設定時にメッセージが交換されます



この図は、Over the DS クライアントのローミングを設定するときに実行されるメッセージ交換のシーケンスを示します。

図 *3*：***Over the DS*** クライアントのローミングの設定時にメッセージが交換されます



関連トピック

オープン WLAN での 802.11r 高速移行の設定（CLI），（108 ページ）
802.11r 高速移行のディセーブル（CLI），（114 ページ）
Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI），（110 ページ）
PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI），（111 ページ）
802.11 高速移行の設定（GUI），（113 ページ）
802.11r 高速移行の監視（CLI），（114 ページ）
802.11r 高速移行の制約事項，（103 ページ）

802.11r 高速移行を設定する方法

オープン WLAN での 802.11r 高速移行の設定（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **client vlan** *vlan-id*
4. **no security wpa**
5. **no security wpa akm dot1x**
6. **no security wpa wpa2**
7. **no wpa wpa2 ciphers aes**
8. **security ft**
9. **no shutdown**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-id* 例： `Switch(config-wlan)# client vlan 0120`	WLAN にクライアント VLAN を関連付けます。
ステップ 4	**no security wpa** 例： `Switch(config-wlan)# no security wpa`	WPA セキュリティをディセーブルにします。
ステップ 5	**no security wpa akm dot1x** 例： `Switch(config-wlan)# no security wpa akm dot1x`	dot1x に対して AKM セキュリティをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**no security wpa wpa2** 例： `Switch(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 7	**no wpa wpa2 ciphers aes** 例： `Switch(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化をディセーブルにします。
ステップ 8	**security ft** 例： `Switch(config-wlan)# security ft`	802.11r 高速移行パラメータを指定します。
ステップ 9	**no shutdown** 例： `Switch(config-wlan)# shutdown`	WLAN を停止します。
ステップ 10	**end** 例： `Switch(config-wlan)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

802.11r の高速移行について，（105 ページ）
802.11r 高速移行の監視（CLI），（114 ページ）
802.11r 高速移行の制約事項，（103 ページ）

Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **client vlan** *vlan-name*
4. **local-auth** *local-auth-profile-eap*
5. **security dot1x authentication-list default**
6. **security ft**
7. **security wpa akm ft dot1x**
8. **no shutdown**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-name* 例： `Switch(config-wlan)# client vlan 0120`	この WLAN にクライアント VLAN を関連付けます。
ステップ 4	**local-auth** *local-auth-profile-eap* 例： `Switch(config-wlan)# local-auth`	local auth EAP プロファイルをイネーブルにします。
ステップ 5	**security dot1x authentication-list default** 例： `Switch(config-wlan)# security dot1x authentication-list default`	dot1x セキュリティ用のセキュリティ認証リストをイネーブルにします。 この設定は、dot1x セキュリティ WLAN に似ています。
ステップ 6	**security ft** 例： `Switch(config-wlan)# security ft`	この WLAN で 802.11r 高速移行をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 7	**security wpa akm ft dot1x** 例： `Switch(config-wlan)# security wpa akm ft dot1x`	WLAN で 802.1x セキュリティをイネーブルにします。
ステップ 8	**no shutdown** 例： `Switch(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 9	**end** 例： `Switch(config-wlan)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

802.11r の高速移行について，（105 ページ）
802.11r 高速移行の監視（CLI），（114 ページ）
802.11r 高速移行の制約事項，（103 ページ）

PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **client vlan** *vlan-name*
4. **no security wpa akm dot1x**
5. **security wpa akm ft psk**
6. **security wpa akm psk set-key** {**ascii** {**0** | **8**} | **hex** {**0** | **8**}}
7. **security ft**
8. **no shutdown**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-name* 例： `Switch(config-wlan)# client vlan 0120`	この WLAN にクライアント VLAN を関連付けます。
ステップ 4	**no security wpa akm dot1x** 例： `Switch(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 5	**security wpa akm ft psk** 例： `Switch(config-wlan)# security wpa akm ft psk`	FT PSK サポートを設定します。
ステップ 6	**security wpa akm psk set-key {ascii {0 | 8} | hex {0 | 8}}** 例： `Switch(config-wlan)# security wpa akm psk set-key ascii 0 test`	PSK AKM の共有キーを設定します。
ステップ 7	**security ft** 例： `Switch(config-wlan)# security ft`	802.11r 高速移行を設定します。
ステップ 8	**no shutdown** 例： `Switch(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 9	**end** 例： `Switch(config-wlan)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバルコンフィギュレーションモードを終了できます。

関連トピック

802.11r の高速移行について，（105 ページ）
802.11r 高速移行の監視（CLI），（114 ページ）
802.11r 高速移行の制約事項，（103 ページ）

802.11 高速移行の設定（GUI）

ステップ 1 [Configuration] > [Wireless] > [WLANs] をクリックします。
[WLANs] ページが表示されます。

ステップ 2 ページの検索機能を使用して、設定する WLAN を検索します。

ステップ 3 WLAN の [WLAN Profile] をクリックします。
[WLAN > Edit] ページが表示されます。

ステップ 4 [Security] タブおよび[Layer 2] タブをクリックします。

ステップ 5 BSS の高速移行をイネーブルにするために [Fast Transition] チェックボックスをオンにします。
BSS の高速移行をディセーブルにするために [Fast Transition] チェックボックスをオフにします。

ステップ 6 分散システム上の BSS の高速移行をイネーブルにするには、[Over the DS] チェックボックスをオンにします。 この設定はデフォルトでイネーブルになっています。
（注） [Over the DS] をオフにすると、Over the Air の高速移行が有効になります。

ステップ 7 （任意） [Reassociation Timeout] テキスト ボックスに再アソシエーションのタイムアウト値（秒単位）を指定します。 指定できる範囲は 1 ～ 100 秒です。 デフォルト値は、20 秒です。

ステップ 8 [Apply] をクリックします。

関連トピック

802.11r の高速移行について，（105 ページ）
802.11r 高速移行の監視（CLI），（114 ページ）
802.11r 高速移行の制約事項，（103 ページ）

802.11r 高速移行のディセーブル（CLI）

手順の概要

1. **configure terminal**
2. **wlan** *profile-name*
3. **no security ft** [**over-the-ds** | **reassociation-timeout** *timeout-in-seconds*]
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 2	**wlan** *profile-name* 例： `Switch# wlan test4`	WLAN コンフィギュレーションサブモードを開始します。*profile-name* は、設定されている WLAN のプロファイル名です。
ステップ 3	**no security ft** [**over-the-ds** | **reassociation-timeout** *timeout-in-seconds*] 例： `Switch(config-wlan)# no security ft over-the-ds`	WLAN の 802.11r 高速移行をディセーブルにします。 （注） データ ソースに対して 802.11r 高速移行をディセーブルにすると、無線の高速移行がイネーブルになります。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバルコンフィギュレーションモードを終了できます。

関連トピック

802.11r の高速移行について，（105 ページ）
802.11r 高速移行の監視（CLI），（114 ページ）
802.11r 高速移行の制約事項，（103 ページ）

802.11r 高速移行の監視（CLI）

802.11r の高速移行を監視するために次のコマンドを使用できます。

コマンド	説明
show wlan name *wlan-name*	WLANに設定されているパラメータの要約を表示します。

show wireless cli mac-address *mac-address*	クライアントの 802.11r 認証キー管理の設定の概要を表示します。
	`. . .`
	`. . .`
	`Client Capabilities`
	`  CF Pollable : Not implemented`
	`  CF Poll Request : Not implemented`
	`  Short Preamble : Not implemented`
	`  PBCC : Not implemented`
	`  Channel Agility : Not implemented`
	`  Listen Interval : 15`
	`  Fast BSS Transition : Implemented`
	`Fast BSS Transition Details :`
	`Client Statistics:`
	`  Number of Bytes Received : 9019`
	`  Number of Bytes Sent : 3765`
	`  Number of Packets Received : 130`
	`  Number of Packets Sent : 36`
	`  Number of EAP Id Request Msg Timeouts : 0`
	`  Number of EAP Request Msg Timeouts : 0`
	`  Number of EAP Key Msg Timeouts : 0`
	`  Number of Data Retries : 1`
	`  Number of RTS Retries : 0`
	`  Number of Duplicate Received Packets : 1`
	`  Number of Decrypt Failed Packets : 0`
	`  Number of Mic Failured Packets : 0`
	`  Number of Mic Missing Packets : 0`
	`  Number of Policy Errors : 0`
	`  Radio Signal Strength Indicator : -48 dBm`
	`  Signal to Noise Ratio : 40 dB`
	`. . .`
	`. . .`

関連トピック

オープン WLAN での 802.11r 高速移行の設定（CLI），（108 ページ）
802.11r 高速移行のディセーブル（CLI），（114 ページ）
Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI），（110 ページ）
PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI），（111 ページ）
802.11 高速移行の設定（GUI），（113 ページ）
802.11r の高速移行について，（105 ページ）

802.11r 高速移行に関する追加情報

関連資料

関連項目	マニュアル タイトル
WLAN コマンド リファレンス	*WLAN Command Reference, Cisco IOS XE Release 3SE*（*Catalyst 3850* スイッチ）

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
IEEE 802.11r。	802.11r 用の IEEE 規格

MIB

MIB	MIB のリンク
このリリースでサポートされるすべての MIB です。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

802.11r 高速移行の機能に関する情報

次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能名	リリース	機能情報
802.11r の高速移行	Cisco IOS XE 3.3SE	この機能が導入されました。

第 10 章

経由ローミングの設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

経由ローミングの制約事項

- 経由ローミング機能は、複数のコントローラでサポートされます。

- この機能は、802.11n 対応の屋内アクセス ポイントでのみサポートされています。 1 つの帯域構成の場合、最大 6 のネイバーがネイバー リストに表示されます。 デュアル バンド構成の場合、最大 12 のネイバーが表示されます。
- スイッチ CLI をのみを使用して経由ローミングを設定できます。

関連トピック

経由ローミングについて, （120 ページ）
経由ローミングの設定（CLI）, （122 ページ）
経由ローミングの監視, （123 ページ）
経由ローミングの設定例, （124 ページ）

経由ローミングについて

802.11k 標準では、クライアントがサービス セットの移行の候補となる既知のネイバー アクセス ポイントに関する情報を含むネイバー レポートを要求することができます。 802.11k ネイバー リストを使用すると、アクティブおよびパッシブ スキャンの必要性を軽減できます。

経由ローミング機能は、インテリジェントでクライアントによって最適化されたネイバー リストに基づいています。

Cisco Client Extension（CCX）ネイバー リストとは異なり、802.11k ネイバー リストは動的かつオンデマンドで生成されます。スイッチ上では維持されません。 802.11k ネイバー リストは、クライアントのロケーションに基づくもので、Mobility Services Engine (MSE) を必要としません。 同じスイッチ上であっても異なる AP の 2 クライアントが、周囲の AP の個々の関係に応じて提供される異なるネイバー リストを設定できます。

デフォルトでは、ネイバー リストには、クライアントがアソシエートされている同じ帯域のネイバーだけが含まれます。 ただし、両方の帯域のネイバーを返すために、802.11k を可能にするスイッチが存在します。

クライアントは、ビーコン内の RRM（無線リソース管理）機能の情報要素（IE）をアドバタイズする AP に関連付けた後でのみ、ネイバー リストの要求を送信します。 ネイバー リストには、隣接する無線の BSSID、チャネル、および処理の詳細についての情報が含まれます。

ネイバー リストの作成と最適化

802.11k ネイバー リスト要求をスイッチが受信すると、次の処理が実行されます。

1. スイッチは、クライアントが現在関連付けられている AP と同じ帯域で、ネイバー リストについて RRM ネイバー テーブルを検索バンドします。
2. スイッチは、帯域ごとにネイバー リストを 6 つに削減するために、AP 間の RSSI（Received Signal Strength Indication）、現在の AP の現在のロケーション、Cisco Prime インフラストラクチャからのネイバー AP のフロア情報、スイッチ上でのローミング履歴情報に従ってネイバーをチェックします。 このリストは、同じフロアの AP に対して最適化されています。

非 802.11k クライアントの経由ローミング

非 802.11k クライアントのローミングを最適化することもできます。 クライアントが 802.11k ネイバーリスト要求を送信する必要なく、各クライアントの予測ネイバーリストを生成できます。 成功した各クライアント アソシエーション/再アソシエーションの後、WLAN でこれが有効である場合、ネイバー リストを生成し、モバイル ステーションのソフトウェア データ構造にリストを格納するために、同じネイバー リストの最適化を非 802.11k クライアントに適用する必要があります。 クライアントプローブが異なるネイバーによって異なる RSSI 値により認識されるため、異なるロケーションのクライアントが異なるリストを持ちます。 クライアントは、通常はアソシエーションまたは再アソシエーションの前にプローブするため、このリストは、更新されたほとんどのプローブ データによって構築され、クライアントがローミングする可能性が高い次の AP を予測します。

AP へのアソシエーション要求が保存された予測ネイバーリストのエントリに一致しない場合に、アソシエーションを拒否することによって、あまり望ましくないネイバーへのクライアントのローミングを抑止します。

アグレッシブ ロード バランシングに加えて、経由ローミング機能を ▪ WLAN ごとおよびグローバルにオンにするスイッチがあります。 次のオプションを使用できます。

- Denial count：クライアントでアソシエーションが拒否される最大回数です。
- Prediction threshold：経由ローミング機能をアクティブにするために、予測リスト内で必要なエントリの最小数です。

ロード バランシングおよび経由ローミングの両方で、クライアントがアソシエートする AP に影響を与えるように設計されているため、WLAN で両オプションを同時にイネーブルにすることはできません。

関連トピック

経由ローミングの設定（CLI），（122 ページ）
経由ローミングの監視，（123 ページ）
経由ローミングの設定例，（124 ページ）
経由ローミングの制約事項，（119 ページ）

経由ローミングの設定方法

経由ローミングの設定（CLI）

手順の概要

1. **configure terminal**
2. **wireless assisted-roaming floor-bias** *dBm*
3. **wlan** *wlan-id*
4. **assisted-roaming neighbor-list**
5. **assisted-roaming dual-list**
6. **assisted-roaming prediction**
7. **wireless assisted-roaming prediction-minimum** *count*
8. **wireless assisted-roaming denial-maximum** *count*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless assisted-roaming floor-bias** *dBm* 例： `Switch(config)# wireless assisted-roaming floor-bias 20`	ネイバー フロア ラベル バイアスを設定します。 有効な範囲は –5 ～ 25 dBm で、デフォルト値は –15 dBm です。
ステップ 3	**wlan** *wlan-id* 例： `Switch(config)# wlan wlan1`	WLAN コンフィギュレーション サブモードを開始します。 *wlan-name* は、設定した WLAN のプロファイル名です。
ステップ 4	**assisted-roaming neighbor-list** 例： `Switch(wlan)# assisted-roaming neighbor-list`	WLAN の 802.11k ネイバー リストを設定します。 WLAN を作成すると、デフォルトでネイバー リストで経由ローミングがイネーブルになります。 コマンドの **no** 形式では、経由ローミング ネイバー リストがディセーブルになります。

	コマンドまたはアクション	目的
ステップ 5	**assisted-roaming dual-list** 例： `Switch(wlan)# assisted-roaming dual-list`	WLAN のデュアル バンド 802.11k デュアル リストを設定します。 WLAN を作成すると、デフォルトでデュアル リストで経由ローミングがイネーブルになります。 コマンドの **no** 形式では、経由ローミング デュアル リストがディセーブルになります。
ステップ 6	**assisted-roaming prediction** 例： `Switch(wlan)# assisted-roaming prediction`	WLAN の経由ローミング予測リスト機能を設定します。 デフォルトでは、経由ローミング予測リストはディセーブルです。 （注） ロード バランシングが WLAN に対してすでにイネーブルである場合、警告メッセージが表示され、ロード バランシングが WLAN に対してディセーブルになります。
ステップ 7	**wireless assisted-roaming prediction-minimum** *count* 例： `Switch# wireless assisted-roaming prediction-minimum`	予測リスト機能が動作するために必要な予測 AP の最小数を設定します。 デフォルト値は 3 です。 （注） クライアントに割り当てられた Forecast、AP が指定した数よりもこの値が小さい場合、経由ローミング機能はこのルールに適用されません。
ステップ 8	**wireless assisted-roaming denial-maximum** *count* 例： `Switch# wireless assisted-roaming denial-maximum 8`	AP に送信されたアソシエーション要求が予測の AP に一致しない場合に、クライアントでアソシエーションを拒否できる最大回数を設定します。 有効な範囲は 1 ～ 10 で、デフォルト値は 5 です。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

経由ローミングについて，（120 ページ）
経由ローミングの制約事項，（119 ページ）

経由ローミングの監視

WLAN に設定された経由ローミングを監視するために次のコマンドが使用できます。 .

コマンド	説明
show wlan id *wlan-id*	WLAN の WLAN パラメータを表示します。

関連トピック

経由ローミングについて，（120 ページ）
経由ローミングの制約事項，（119 ページ）

経由ローミングの設定例

次に、ネイバー フロア ラベル バイアスを設定する例を示します。

```
Switch# configure terminal
Switch(config)# wireless assisted-roaming floor-bias 10
Switch(config)# end
Switch# show wlan id 23
```

次に、特定の WLAN のネイバー リストをディセーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# wlan test1
Switch(config (wlan)# no assisted-roaming neighbor-list
Switch(config)(wlan)# end
Switch# show wlan id 23
```

次に、特定の WLAN の予測リストを設定する例を示します。

```
Switch# configure terminal
Switch(config)# wlan test1
Switch(config)(wlan)# assisted-roaming prediction
Switch(config)(wlan)# end
Switch# show wlan id 23
```

次に、特定のWLANの経由ローミングの予測しきい値および最大の拒否数に基づいて予測リストを設定する例を示します。

```
Switch# configure terminal
Switch(config)# wireless assisted-roaming prediction-minimum 4
Switch(config)# wireless assisted-roaming denial-maximum 4
Switch(config)(wlan)# end
Switch# show wlan id 23
```

関連トピック

経由ローミングについて，（120 ページ）
経由ローミングの制約事項，（119 ページ）

経由ローミングに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference*（*Catalyst 3850* スイッチ）

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
802.11K	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

経由ローミング設定の機能履歴と情報

機能名	リリース	機能情報
経由ローミング	Cisco IOS XE 3.2SE	この機能が導入されました。

第 11 章

アクセス ポイント グループの設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

AP グループを設定するための前提条件

次に、スイッチでアクセス ポイント グループを作成するための前提条件を示します。

- VLAN またはサブネットにサービスを提供するルータ上で、必要なアクセス コントロール リスト（ACL）を定義する必要があります。

- アクセス ポイント グループ VLAN では、マルチキャスト トラフィックがサポートされます。 ただし、クライアントがあるアクセス ポイントから別のアクセス ポイントにローミングする場合、IGMP スヌーピングが有効になっていないと、クライアントによってマルチキャスト トラフィックの受信が停止されることがあります。

関連トピック

アクセス ポイント グループについて, （128 ページ）
アクセス ポイント グループの設定に関する制約事項, （128 ページ）

アクセス ポイント グループの設定に関する制約事項

- AP グループ テーブル内の WLAN に対するインターフェイス マッピングが、WLAN インターフェイスと同じであるとします。 WLAN インターフェイスが変更されると、AP グループ テーブル内の WLAN に対するインターフェイス マッピングも新しい WLAN インターフェイスに変わります。

  AP グループ テーブル内の WLAN に対するインターフェイス マッピングが、WLAN に定義されたインターフェイスと異なるとします。 WLAN インターフェイスが変更されても、AP グループ テーブル内の WLAN に対するインターフェイス マッピングは新しい WLAN インターフェイスに変わりません。

- スイッチ上の設定をクリアすると、アクセス ポイント グループのすべてが非表示となります。ただし、デフォルトのアクセス ポイント グループである「default-group」（自動的に作成される）は例外です。

- デフォルトのアクセス ポイント グループには、最大 16 の WLAN を関連付けることができます。 デフォルトのアクセス ポイント グループの WLAN ID は、16 以下である必要があります。 大規模なデフォルトのアクセス ポイント グループ内で ID が 16 以上の WLAN が作成されると、WLAN SSID はブロードキャストされません。 デフォルトのアクセス ポイント グループのすべての WLAN ID で ID が 16 以下であることが必要です。 16 を超える ID を含む WLAN は、カスタム アクセス ポイント グループに割り当てることができます。

関連トピック

アクセス ポイント グループについて, （128 ページ）
AP グループを設定するための前提条件, （127 ページ）

アクセス ポイント グループについて

スイッチ上に最大 512 の WLAN を作成した後では、さまざまなアクセス ポイントに WLAN を選択的に公開（アクセス ポイント グループを使用して）することで、ワイヤレス ネットワークをより適切に管理できます。 一般的な展開では、WLAN 上のすべてのユーザはスイッチ上の 1 つのインターフェイスにマップされます。 したがって、WLAN に関連付けられているすべてのユーザは、同じサブネットまたは VLAN に存在します。 しかし、複数のインターフェイス間で負荷を分

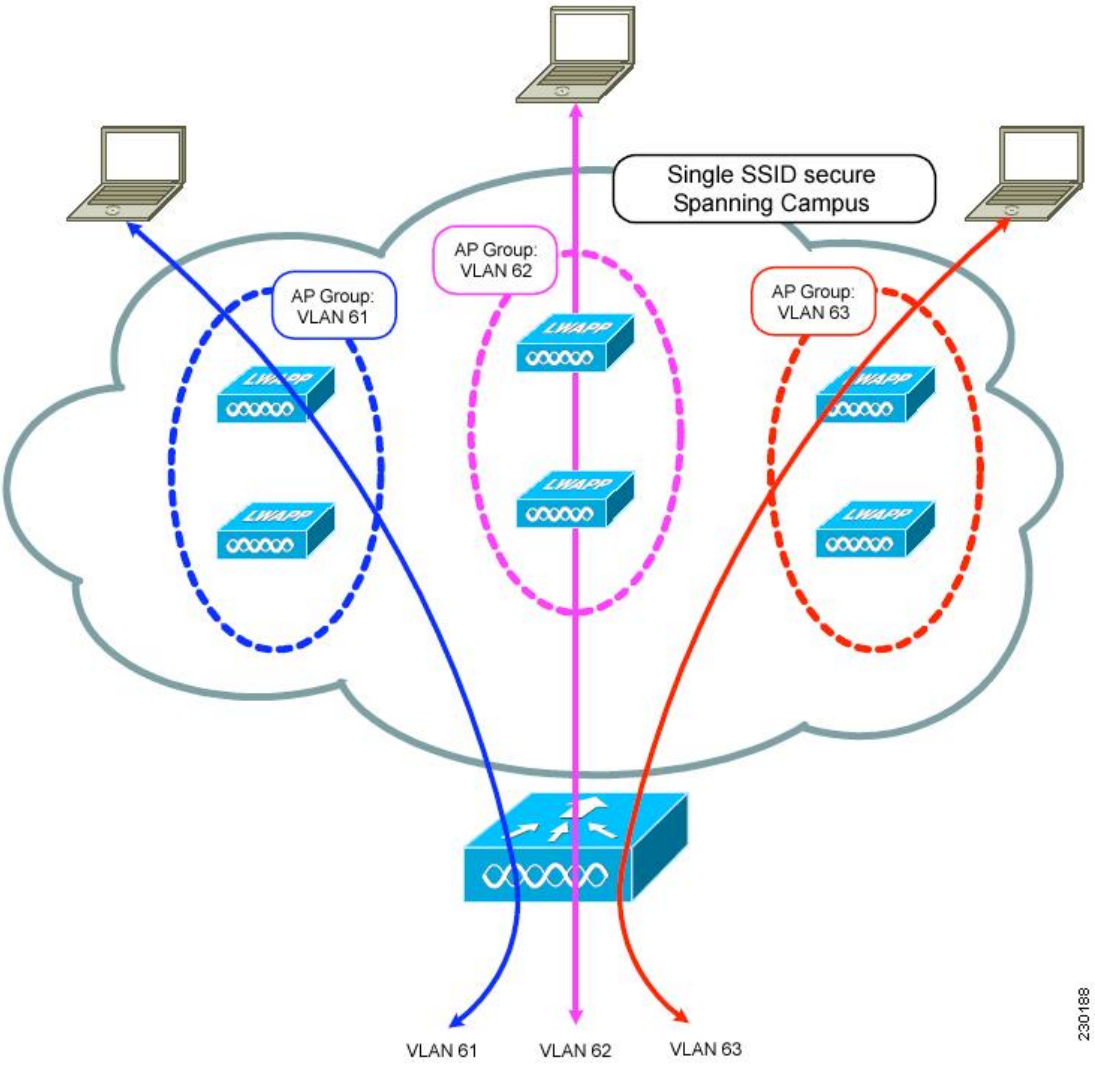
散すること、またはアクセスポイントグループを作成して、個々の部門（たとえばマーケティング部門）などの特定の条件に基づくグループユーザへと負荷を分配することを選択できます。 さらに、ネットワーク管理を簡素化するために、これらのアクセスポイントグループを別個のVLANで設定できます。

図では、3つの設定された動的インターフェイスが、3つの異なるVLAN（VLAN 61、VLAN 62、およびVLAN 63）にマップされています。 3つのアクセス ポイント グループが定義されており、各グループは異なる VLAN のメンバですが、すべてのグループが同じ SSID のメンバとなっています。 無線 SSID 内のクライアントには、そのアクセス ポイントがメンバとなっている VLAN サブネットからIPアドレスが割り当てられています。 たとえば、アクセス ポイント グループ VLAN 61のメンバであるアクセスポイントにアソシエートする任意のユーザには、そのサブネットから IP アドレスが割り当てられます。

図では、スイッチは内部的にレイヤ3ローミングイベントとしてアクセス ポイント間のローミングを扱っています。 こうすることで、WLAN クライアントは元の IP アドレスを保持します。

すべてのアクセス ポイントがスイッチに join された後は、アクセス ポイント グループを作成して、最大 16 の WLAN を各グループに割り当てることができます。 各アクセス ポイントは、有効化されている WLAN のうち、そのアクセス ポイント グループに属する WLAN だけをアドバタイズします。 アクセス ポイント グループで無効化されている WLAN または別のグループに属する WLAN はアドバタイズしません。

図 *4*：アクセス ポイント グループ



関連トピック

アクセス ポイント グループの作成，（131 ページ）
アクセス ポイント グループの表示，（133 ページ）
AP グループへのアクセス ポイントの割り当て，（132 ページ）
AP グループを設定するための前提条件，（127 ページ）
アクセス ポイント グループの設定に関する制約事項，（128 ページ）

アクセス ポイント グループの設定方法

アクセス ポイント グループの作成

はじめる前に

この操作を実行するには、管理者特権が必要です。

手順の概要

1. **configure terminal**
2. **ap group** *ap-group-name*
3. **wlan** *wlan-name*
4. （任意） **vlan** *vlan-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap group** *ap-group-name* 例： `Switch(config)# ap group my-ap-group`	アクセス ポイント グループを作成します。
ステップ 3	**wlan** *wlan-name* 例： `Switch(config-apgroup)# wlan wlan-name`	WLAN に AP グループを関連付けます。
ステップ 4	**vlan** *vlan-name* 例： `Switch(config-apgroup)# vlan test-vlan`	（任意） VLAN にアクセス ポイント グループを割り当てます。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

次に、AP グループを作成する例を示します。

```
Switch# configure terminal
Switch(config-apgroup)# ap group test-ap-group-16
Switch(config-wlan-apgroup)# wlan test-ap-group-16
Switch(config-wlan-apgroup)# vlan VLAN1300
```

関連トピック

アクセス ポイント グループについて，（128 ページ）

AP グループへのアクセス ポイントの割り当て

はじめる前に

この操作を実行するには、管理者特権が必要です。

手順の概要

1. **ap name** *ap-name* **ap-group-name** *ap-group*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap-name* **ap-group-name** *ap-group* 例： `Switch# ap name 1240-101 ap-groupname apgroup_16`	アクセス ポイント グループにアクセス ポイントを割り当てます。 次のキーワードと引数があります。 • **name**：このキーワードに続く引数がスイッチに関連付けられている AP の名前であることを指定します。 • *ap-name*：AP グループに関連付ける AP です。 • **ap-group-name**：このキーワードに続く引数が設定されてスイッチいる AP グループの名前を指定します。 • *ap-group*：スイッチ で設定するアクセス ポイント グループの名前です。

関連トピック

アクセス ポイント グループについて，（128 ページ）

アクセス ポイント グループの表示

はじめる前に

この操作を実行するには、管理者特権が必要です。

手順の概要

1. **show ap groups** [**extended**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ap groups** [**extended**] 例： `Switch# show ap groups`	スイッチで設定された AP グループを表示します。 **extended** キーワードは、システムで詳細に定義されているすべての AP グループ情報を表示します。

関連トピック

アクセス ポイント グループについて，（128 ページ）

その他の関連資料

関連資料

関連項目	マニュアル タイトル
WLAN コマンド	*WLAN Command Reference, Cisco IOS XE Release 3SE（Catalyst 3850 スイッチ）*
Lightweight アクセス ポイント コンフィギュレーション	*Lightweight Access Point Configuration Guide, Cisco IOS XE Release 3SE（Catalyst 3850 スイッチ）*
Lightweight アクセス ポイント コマンド	*Lightweight Access Point Command Reference, Cisco IOS XE Release 3SE（Catalyst 3850 スイッチ）*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

アクセス ポイント グループの機能履歴と情報

次の表で、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

機能名	リリース	機能情報
AP グループ数	Cisco IOS XE 3.2SE	この機能が導入されました。

索 引