Cisco IOS XE 3.6E（Catalyst 3850 スイッチ）統合プラットフォーム コマンド リファレンス

初版：2014 年 6 月 27 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/

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）。
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
Italic フォント	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、イタリック体で示しています。
`courier` フォント	システムが表示する端末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	ユーザが入力したテキストは、太字の courier フォントで示しています。
[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。
|	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。

表記法	説明
[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}	どれか 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に記載されていない参照資料を紹介しています。

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 IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger.You are in a situation that could cause bodily injury.Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.Statement 1071

SAVE THESE INSTRUCTIONS

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、SFP+、および QSFP+ 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/c/en/us/td/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。

コマンドライン インターフェイスの使用

この章は、次の内容で構成されています。

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

この章では、Cisco IOS コマンドライン インターフェイス（CLI）について説明し、CLI を使用してスイッチを設定する方法について説明します。

コマンド モードについて

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。使用可能なコマンドは、現在のモードによって異なります。各コマンドモードで使用できるコマンドのリストを取得するには、システム プロンプトで疑問符（?）を入力します。

スイッチとの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。スイッチの再起動時には、ユーザ EXEC コマンドは保存されません。

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。コンフィギュレーションを保存するとこれらのコマンドは保存され、スイッチの再起動時に使用されます。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 モードを開始できます。

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。表の例では、ホスト名として *Switch* を使用しています。

表 *1:* コマンド モードの概要

モード	Access Method	プロンプト	終了方法	モードの用途
ユーザ EXEC	スイッチとの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。	このモードを使用して、スイッチ全体に適用されるパラメータを設定します。
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。	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。

モード	Access Method	プロンプト	終了方法	モードの用途
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。

コマンド モードの詳細については、このリリースに対応するコマンド リファレンス ガイドを参照してください。

ヘルプ システムについて

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。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。

表 *2:* ヘルプの概要

コマンド	目的
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。

*abbreviated-command-entry***?**
 	
`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。

コマンド	目的

コマンドの先頭部分 <Tab>
 	
`Switch# sh conf<tab>`
`Switch# show configuration`
	特定のコマンド名を補完します。

? `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。
*command***?** `Switch> show ?`	コマンドに関連するキーワードを一覧表示します。

*command keyword***?**
 	
`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

コマンドの先頭から、スイッチが特定のコマンドとして認識できる文字数だけを入力し、後は省略できます。

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 形式の概要

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。ディセーブルにし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には、キーワード **no** を指定せずにコマンドを使用します。

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 メッセージについて

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 *3: 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 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。
`% 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 モードで使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 ロギングの使用方法

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。

コマンド履歴の使用

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、10のコマンドラインが履歴バッファに保存されます。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。これらの手順は任意です。

現在の端末セッションで保存されるコマンドライン数を変更するには、特権EXECモードで次のコマンドを入力します。

```
Switch# terminal history [size number-of-lines]
```

指定できる範囲は 0 ～ 256 です。

特定の回線に関するすべてのセッションで保存されるコマンドライン数を設定するには、ライン コンフィギュレーション モードで次のコマンドを入力します。

```
Switch(config-line)# history [size number-of-lines]
```

指定できる範囲は 0 ～ 256 です。

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。

表 *4:* コマンドの呼び出し

Action	結果
Ctrl+P キーまたは↑キーを押します。	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。
Ctrl+N キーまたは↓キーを押します。	Ctrl+P または↑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。

Action	結果
show history `Switch(config)# help`	特権EXECモードで、直前に入力したいくつかのコマンドを一覧表示します。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制御されます。

コマンド履歴機能の無効化

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。これらの手順は任意です。

現在の端末セッションでこの機能をディセーブルにするには、**terminal no history** 特権 EXEC コマンドを使用します。

回線に関するセッションでコマンド履歴をディセーブルにするには、**no history** ライン コンフィギュレーション コマンドを使用します。

編集機能の使用方法

ここでは、コマンドラインの操作に役立つ編集機能について説明します。

編集機能の有効化および無効化

拡張編集モードは自動的にイネーブルになりますが、ディセーブルにする、再びイネーブルにする、または特定の回線で拡張編集機能を使用できるように設定できます。これらの手順は任意です。

拡張編集モードをグローバルにディセーブルにするには、ライン コンフィギュレーション モードで次のコマンドを入力します。

```
Switch (config-line)# no editing
```

現在の端末セッションで拡張編集モードを再びイネーブルにするには、特権EXECモードで次のコマンドを入力します。

```
Switch# terminal editing
```

特定の回線について拡張編集モードを再び設定するには、ライン コンフィギュレーション モードで次のコマンドを入力します。

```
Switch(config-line)# editing
```

キーストロークによるコマンドの編集

このテーブルに、コマンドラインの編集に必要なキーストロークを示します。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 *5:* キーストロークによるコマンドの編集

機能	キーストローク	目的
コマンドライン上を移動して、変更または訂正を行います。	**Ctrl+B** または左矢印キーを押します。	カーソルを 1 文字後退させます。
	Ctrl+F または右矢印キーを押します。	カーソルを 1 文字前進させます。
	Ctrl+A を押します。	コマンドラインの先頭にカーソルを移動します。
	Ctrl+E を押します。	カーソルをコマンド ラインの末尾に移動します。
	Esc+B を押します。	カーソルを 1 単語後退させます。
	Esc+F を押します。	カーソルを 1 単語前進させます。
	Ctrl+T を押します。	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。
バッファからコマンドを呼び出し、コマンドラインにペーストします。最後に削除した 10 項目がバッファに保存されています。	Ctrl+Y を押します。	バッファ内の最新のエントリを呼び出します。
	Esc+Y を押します。	次のバッファ エントリを呼び出します。 バッファには、最後に削除またはカットした 10 項目しか保存されません。Esc+Y を 11 回以上押すと、最初のバッファ エントリに戻って表示されます。

機能	キーストローク	目的
不要なエントリを削除します。	Delete キーまたは Backspace キーを押します。	カーソルの左にある文字を消去します。
	Ctrl+D を押します。	カーソル位置にある文字を削除します。
	Ctrl+K を押します。	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 を押します。	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 を押します。	カーソルの左にある単語を削除します。
	Esc+D を押します。	カーソルの位置から単語の末尾までを削除します。
ワードを大文字または小文字にします。または、一連の文字をすべて大文字にします。	Esc+C を押します。	カーソル位置のワードを大文字にします。
	Esc+L を押します。	カーソルの場所にある単語を小文字にします。
	Esc+U を押します。	カーソルの位置から単語の末尾までを大文字にします。
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。	Ctrl+V または Esc+Q キーを押します。	

機能	キーストローク	目的
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。	Return キーを押します。	1 行下にスクロールします。
	Space キーを押します。	1 画面分下にスクロールします。
スイッチから画面にメッセージが突然送られた場合に、現在のコマンドラインを再表示します。	Ctrl+L または Ctrl+R を押します。	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。

次の例では、**access-list** グローバル コンフィギュレーション コマンドエントリが1行分よりも長くなっています。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。

```
Switch(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
Switch(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
Switch(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
```

```
Switch(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

コマンドの入力が終わった後、Ctrl+A を押して全体の構文をチェックし、その後 Return キーを押してコマンドを実行してください。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。

```
Switch(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

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。それ以外の幅の場合は、特権 EXEC コマンド **terminal width** を使用してターミナルの幅を設定します。

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。

この機能を使用するには、**show** または **more** コマンドを入力した後、パイプ記号（|）、**begin**、**include**、または **exclude** のいずれかのキーワード、および文字列（検索またはフィルタの条件）を指定します。

command | {**begin** | **include** | **exclude**} *regular-expression*

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。

次の例では、*protocol* が使用されている行だけを出力するように指定する方法を示します。

```
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
```

CLI のアクセス

CLI にはコンソール接続、Telnet、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、アクティブ スイッチ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 メンバーのコンソール ポートまたはイーサネット管理ポートを経由してアクティブ スイッチへ接続できます。複数の CLI セッションをアクティブ スイッチに使用する場合は注意が必要です。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。

特定のスタック メンバをデバッグする場合は、**session** *stack-member-number* 特権 EXEC コマンドでアクティブ スイッチからアクセスできます。スタック メンバ番号は、システム プロンプトに追加されます。たとえば、*Switch-2#* はスタック メンバ 2 の特権 EXEC モードのプロンプトであり、アクティブ スイッチ のシステム プロンプトは Switch です。特定のスタック メンバへの CLI セッションで使用できるのは、**show** コマンドと **debug** コマンドに限ります。

コンソール接続または Telnet による CLI アクセス

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。

CLI アクセスはスイッチのセットアップの前に使用できます。スイッチが設定された後は、リモート Telnet セッションまたは SSH クライアントで CLI にアクセスできます。

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。

- スイッチのコンソール 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、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 または暗号化セキュア シェル（SSH）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 I 部

CleanAir

CleanAir コマンド

ap dot11 5ghz cleanair

5 GHz デバイスを検出するために CleanAir を有効にするには、グローバル コンフィギュレーション モードで **apdot115ghzcleanair** コマンドを使用します。

ap dot11 5ghz cleanair

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

他の CleanAir コマンドを設定する前に、この CleanAir コマンドを有効にする必要があります。

次に、5 GHz デバイス用の CleanAir を有効にする例を示します。

```
Switch(config)# ap dot11 5ghz cleanair
```

関連トピック

ap dot11 5ghz cleanair alarm air-quality （19 ページ）
ap dot11 5ghz cleanair alarm device （20 ページ）
default ap dot11 5ghz cleanair device （22 ページ）
ap dot11 5ghz rrm channel cleanair-event （24 ページ）
ap dot11 5ghz rrm channel device （25 ページ）

ap dot11 5ghz cleanair alarm air-quality

電波品質（AQ）が 5 GHz デバイスのしきい値に達した場合のアラームを設定するには、**apdot115ghzcleanairalarmair-quality** コマンドを使用します。AQ が 5 GHz デバイスのしきい値に達した場合のアラームを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 5ghz cleanair alarm air-quality threshold *threshold _value*

構文の説明

threshold *threshold _value*	電波品質のしきい値を設定します。範囲は 1 ～ 100 です。

コマンド デフォルト

AQ のデフォルトのしきい値は 10 です。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 5ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、AQ のしきい値を設定する例を示します。

```
Switch(config)# ap dot11 5ghz cleanair alarm air-quality threshold 30
```

関連トピック

ap dot11 5ghz cleanair （18 ページ）
default ap dot11 5ghz cleanair device （22 ページ）

ap dot11 5ghz cleanair alarm device

5 GHz 干渉デバイスのアラームを設定するには、**apdot115ghzcleanairalarmdevice** コマンドを使用します。

ap dot11 5ghz cleanair alarm device {**canopy** | **cont-tx** | **dect-like** | **inv** | **jammer** | **nonstd** | **radar** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile**}

構文の説明

canopy	Canopy 干渉デバイスのアラームを設定します。
cont-tx	連続トランスミッタのアラームを設定します。
dect-like	Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話のアラームを設定します。
inv	スペクトル反転 Wi-Fi 信号を使用するデバイスのアラームを設定します。
jammer	電波妨害干渉デバイスのアラームを設定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスのアラームを設定します。
radar	レーダーのアラームを設定します。
superag	802.11 SuperAG 干渉デバイスのアラームを設定します。
tdd-tx	時分割複信（TDD）トランスミッタのアラームを設定します。
video	ビデオ カメラのアラームを設定します。
wimax-fixed	WiMax 固定干渉デバイスのアラームを設定します。
wimax-mobile	WiMax モバイル干渉デバイスのアラームを設定します。

コマンド デフォルト

Wi-Fi 反転デバイスのアラームが有効になっており、他のすべての干渉デバイスのアラームは無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 5ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、レーダーデバイスからの干渉を通知するアラームを有効にする例を示します。

```
Switch(config)# ap dot11 5ghz cleanair alarm device radar
```

関連トピック

ap dot11 5ghz cleanair （18 ページ）
ap dot11 5ghz cleanair alarm air-quality （19 ページ）

default ap dot11 5ghz cleanair device

5 GHz 干渉デバイスのアラームのデフォルト状態を設定するには、グローバル コンフィギュレーション モードで **defaultapdot115ghzcleanairdevice** コマンドを使用します。

default ap dot11 5ghz cleanair device {**canopy** |**cont-tx** |**dect-like** |**inv** |**jammer** |**nonstd** |**radar** |**report** |**superag** |**tdd-tx** |**video** |**wimax-fixed** |**wimax-mobile**}

構文の説明

canopy	Canopy 干渉デバイスのアラームを設定します。
cont-tx	連続トランスミッタのアラームを設定します。
dect-like	Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話のアラームを設定します。
inv	スペクトル反転 Wi-Fi 信号を使用するデバイスのアラームを設定します。
jammer	電波妨害干渉デバイスのアラームを設定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスのアラームを設定します。
radar	レーダーのアラームを設定します。
report	干渉デバイスのレポートを有効にします。
superag	802.11 SuperAG 干渉デバイスのアラームを設定します。
tdd-tx	時分割複信（TDD）トランスミッタのアラームを設定します。
video	ビデオ カメラのアラームを設定します。
wimax-fixed	WiMax 固定干渉デバイスのアラームを設定します。
wimax-mobile	WiMax モバイル干渉デバイスのアラームを設定します。

コマンド デフォルト

Wi-Fi 反転デバイスのアラームは有効になっています。その他の干渉デバイスのアラームはすべて無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 5ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、CleanAir によるビデオ カメラの干渉時のレポートを有効にする例を示します。

```
Switch(config)# default ap dot11 5ghz cleanair device video
```

ap dot11 5ghz rrm channel cleanair-event

イベント駆動型RRM（EDRRM）を有効にして5 GHzデバイスの感度を設定するには、グローバル コンフィギュレーション モードで **apdot115ghzrrmchannelcleanair-event** コマンドを使用します。EDRRM を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 5ghz rrm channel cleanair-event ［**sensitivity** {**high**|**low**|**medium**}］
no ap dot11 5ghz rrm channel cleanair-event ［**sensitivity** {**high**|**low**|**medium**}］

構文の説明

sensitivity	（任意）CleanAir イベントの EDRRM 感度を設定します。
high	（任意）電波品質（AQ）の値で示される、非 Wi-Fi 干渉に対する最も高い感度を指定します。
low	（任意）AQ の値で示される、非 Wi-Fi 干渉に対する最も低い感度を指定します。
medium	（任意）AQ の値で示される、非 Wi-Fi 干渉に対する中程度の感度を指定します。

コマンド デフォルト

EDRRM が無効になっており、EDRRM 感度は low になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

感度を設定する前に、**ap dot11 5ghz rrm channel cleanair-event** コマンドを使用して EDRRM を有効にする必要があります。

次に、EDRRM を有効にして EDRRM 感度を high に設定する例を示します。

```
Switch(config)# ap dot11 5ghz rrm channel cleanair-event
Switch(config)# ap dot11 5ghz rrm channel cleanair-event sensitivity high
```

関連トピック

ap dot11 5ghz cleanair （18 ページ）
ap dot11 5ghz rrm channel device （25 ページ）

ap dot11 5ghz rrm channel device

802.11aチャネルで永続型非Wi-Fiデバイス回避を設定するには、グローバル コンフィギュレーション モードで **apdot115ghzrrmchanneldevice** コマンドを使用します。永続型デバイス回避を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 5ghz rrm channel device
no ap dot11 5ghz rrm channel device

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

CleanAir 永続型デバイス ステートが無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

CleanAir 対応モニタ モード アクセス ポイントは、すべての設定済みチャネル上の永続型デバイスに関する情報を収集し、その情報をスイッチに保存します。ローカルモードおよびブリッジ モードのアクセス ポイントは、稼働チャネルでのみ干渉デバイスを検出します。

次に、802.11a デバイスで永続型デバイス回避を有効にする例を示します。

```
Switch(config)# ap dot11 5ghz rrm channel device
```

関連トピック

ap dot11 5ghz cleanair （18 ページ）
ap dot11 5ghz rrm channel cleanair-event （24 ページ）

ap dot11 24ghz cleanair

2.4GHz デバイスを検出するために CleanAir を有効にするには、グローバル コンフィギュレーション モードで **apdot1124ghzcleanair** コマンドを使用します。2.4GHz デバイスを検出するための CleanAir を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 24ghz cleanair

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

他の CleanAir コマンドを設定する前に、この CleanAir コマンドを有効にする必要があります。

次に、2.4 GHz デバイス用の CleanAir を有効にする例を示します。

```
Switch(config)# ap dot11 24ghz cleanair
```

関連トピック

ap dot11 24ghz cleanair alarm air-quality （27 ページ）
ap dot11 24ghz cleanair alarm device （28 ページ）
default ap dot11 24ghz cleanair device （30 ページ）
ap dot11 24ghz rrm channel cleanair-event （33 ページ）
ap dot11 24ghz rrm channel device （34 ページ）

ap dot11 24ghz cleanair alarm air-quality

すべての 2.4GHz デバイスの電波品質しきい値に関するアラームを設定するには、グローバル コンフィギュレーション モードで **apdot1124ghzcleanairalarmair-quality** コマンドを使用します。すべての 2.4GHz デバイスの AQ しきい値に関するアラームを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 24ghz cleanair alarm air-quality threshold *threshold_value*

構文の説明

threshold *threshold_value*	AQ のしきい値を設定します。範囲は 1 ～ 100 です。

コマンド デフォルト

AQ のデフォルトのしきい値は 10 です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 24ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、AQ のしきい値を設定する例を示します。

```
Switch(config)# ap dot11 24ghz cleanair alarm air-quality threshold 50
```

関連トピック

ap dot11 24ghz cleanair （26 ページ）
ap dot11 24ghz cleanair alarm device （28 ページ）
default ap dot11 24ghz cleanair device （30 ページ）

ap dot11 24ghz cleanair alarm device

2.4GHz 干渉デバイスのアラームを設定するには、グローバル コンフィギュレーション モードで **apdot1124ghzcleanairalarmdevice** コマンドを使用します。2.4GHz 干渉デバイスのアラームを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 24ghz cleanairalarm {**device** | **bt-discovery** | **bt-link canopy** | **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven** | **nonstd** | **superag** | **tdd-tx video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee**}

構文の説明

bt-discovery	Bluetooth 干渉デバイスのアラームを設定します。
bt-link	Bluetooth リンクのアラームを設定します。
canopy	Canopy 干渉デバイスのアラームを設定します。
cont-tx	連続トランスミッタのアラームを設定します。
dect-like	Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話のアラームを設定します。
fh	802.11 周波数ホッピング（FH）デバイスのアラームを設定します。
inv	スペクトル反転 Wi-Fi 信号を使用するデバイスのアラームを設定します。
jammer	電波妨害干渉デバイスのアラームを設定します。
mw-oven	電子レンジのアラームを設定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスのアラームを設定します。
superag	802.11 SuperAG 干渉デバイスのアラームを設定します。
tdd-tx	時分割複信（TDD）トランスミッタのアラームを設定します。
video	ビデオ カメラのアラームを設定します。
wimax-fixed	WiMax 固定干渉デバイスのアラームを設定します。
wimax-mobile	WiMax モバイル干渉デバイスのアラームを設定します。
xbox	Xbox 干渉デバイスのアラームを設定します。
zigbee	802.15.4 干渉デバイスのアラームを設定します。

コマンド デフォルト

Wi-Fi 反転デバイスのアラームが有効になっています。他のすべてのデバイスのアラームは無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 24ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、ZigBee デバイスからの干渉を通知するアラームを有効にする例を示します。

```
Switch(config)# ap dot11 24ghz cleanair alarm device zigbee
```

関連トピック

ap dot11 24ghz cleanair （26 ページ）
ap dot11 24ghz cleanair alarm air-quality （27 ページ）
default ap dot11 24ghz cleanair device （30 ページ）

default ap dot11 24ghz cleanair device

2.4 GHz 干渉デバイスのレポート生成のデフォルト状態を設定するには、グローバル コンフィギュレーション モードで **defaultapdot1124ghzcleanairdevice** コマンドを使用します。

default ap dot11 24ghz cleanair device {**ble-beacon**|**bt-discovery** |**bt-link** |**canopy** |**cont-tx** |**dect-like** |**fh** |**inv** |**jammer** |**mw-oven** |**nonstd** |**report** |**superag** |**tdd-tx** |**video** |**wimax-fixed** |**wimax-mobile** |**xbox** |**zigbee**}

構文の説明

ble-beacon	BLE ビーコン機能を設定します。
bt-discovery	Bluetooth 干渉デバイスのアラームを設定します。
bt-link	Bluetooth リンクのアラームを設定します。
canopy	Canopy 干渉デバイスのアラームを設定します。
cont-tx	連続トランスミッタのアラームを設定します。
dect-like	Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話のアラームを設定します。
fh	802.11 周波数ホッピング デバイスのアラームを設定します。
inv	スペクトル反転 Wi-Fi 信号を使用するデバイスのアラームを設定します。
jammer	電波妨害干渉デバイスのアラームを設定します。
mw-oven	電子レンジのアラームを設定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスのアラームを設定します。

superag	802.11 SuperAG 干渉デバイスのアラームを設定します。
tdd-tx	時分割複信（TDD）トランスミッタのアラームを設定します。
video	ビデオ カメラのアラームを設定します。
wimax-fixed	WiMax 固定干渉デバイスのアラームを設定します。
wimax-mobile	WiMax モバイル干渉デバイスのアラームを設定します。
xbox	Xbox 干渉デバイスのアラームを設定します。
zigbee	802.15.4 干渉デバイスのアラームを設定します。

コマンド デフォルト

Wi-Fi 反転デバイスのアラームが有効になっています。他のすべてのデバイスのアラームは無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE Denali 16.2.1	このコマンドが変更されました。**ble-beacon** キーワードが追加されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 24ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、CleanAir によるビデオ カメラの干渉時のレポートを有効にする例を示します。

```
Switch(config)# default ap dot11 24ghz cleanair device video
```

関連トピック

ap dot11 24ghz cleanair （26 ページ）
ap dot11 24ghz cleanair alarm air-quality （27 ページ）

ap dot11 24ghz cleanair alarm device （28 ページ）

ap dot11 24ghz rrm channel cleanair-event

イベント駆動型 RRM（EDRRM）を有効にして 2.4 GHz デバイスの感度を設定するには、グローバル コンフィギュレーション モードで **apdot1124ghzrrmchannelcleanair-event** コマンドを使用します。EDRRM を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 24ghz rrm channel cleanair-event sensitivity {**high** |**low** |**medium**}
no ap dot11 24ghz rrm channel cleanair-event [**sensitivity**{**high** | **low** | **medium**}]

構文の説明

sensitivity	（任意）CleanAir イベントの EDRRM 感度を設定します。
high	（任意）電波品質（AQ）の値で示される、非 Wi-Fi 干渉に対する最も高い感度を指定します。
low	（任意）AQ の値で示される、非 Wi-Fi 干渉に対する最も低い感度を指定します。
medium	（任意）AQ の値で示される、非 Wi-Fi 干渉に対する中程度の感度を指定します。

コマンド デフォルト

EDRRM が無効になっており、感度は low になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

感度を設定する前に、**ap dot11 24ghz rrm channel cleanair-event** コマンドを使用して EDRRM を有効にする必要があります。

次に、EDRRM を有効にして EDRRM 感度を low に設定する例を示します。

```
Switch(config)# ap dot11 24ghz rrm channel cleanair-event
Switch(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity low
```

関連トピック

ap dot11 24ghz cleanair （26 ページ）
ap dot11 24ghz rrm channel device （34 ページ）

ap dot11 24ghz rrm channel device

802.11bチャネルで永続型非Wi-Fiデバイス回避を設定するには、グローバル コンフィギュレーション モードで **apdot1124ghzrrmchanneldevice** コマンドを使用します。永続型デバイス回避を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 24ghz rrm channel device
no ap dot11 24ghz rrm channel device

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

永続型デバイス回避が無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

CleanAir 対応モニタ モード アクセス ポイントは、すべての設定済みチャネル上の永続型デバイスに関する情報を収集し、その情報をスイッチに保存します。ローカルモードおよびブリッジ モードのアクセス ポイントは、稼働チャネルでのみ干渉デバイスを検出します。

次に、永続型デバイス回避を有効にする例を示します。

```
Switch(config)# ap dot11 24ghz rrm channel device
```

関連トピック

ap dot11 24ghz cleanair （26 ページ）
ap dot11 24ghz rrm channel cleanair-event （33 ページ）

ap name mode se-connect

アクセス ポイントを SE-Connect モードに設定するには、特権 EXEC モードで **ap name** *ap_name* **mode se-connect** コマンドを使用します。

ap name *ap_name***mode se-connect**

構文の説明

ap_name	アクセス ポイントの名前。

コマンド デフォルト

どのアクセス ポイントも SE-Connect モードに設定されていません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

アクセス ポイントは、モードを変更した後に再起動します。

SE-Connect モードを使用すると、外部の Microsoft Windows XP または Vista PC で実行されている Spectrum Expert アプリケーションを Cisco CleanAir 対応のアクセス ポイントに接続して、詳細なスペクトラム データを表示および分析できるようになります。Spectrum Expert アプリケーションは、コントローラをバイパスしてアクセス ポイントに直接接続します。SE-Connect モードのアクセス ポイントからは、Wi-Fi、RF、スペクトラム データがコントローラに提供されません。すべての CleanAir システム機能は、AP がこのモードになっていて、クライアントが実行されていない間、一時停止状態になります。このモードは、リモート トラブルシューティングのみを対象としています。

次に、アクセス ポイントのモードを SE-Connect に変更する例を示します。

```
Switch# ap name AS-5508-5-AP3 mode se-connect

Changing the AP's mode will cause the AP to reboot.
Are you sure you want to continue? (y/n)[y]: y
% switch-1:wcm:Cisco AP does not support the seconnect mode
```

default ap dot11 5ghz cleanair device

5 GHz 干渉デバイスのアラームのデフォルト状態を設定するには、グローバル コンフィギュレーション モードで **defaultapdot115ghzcleanairdevice** コマンドを使用します。

default ap dot11 5ghz cleanair device {**canopy |cont-tx |dect-like |inv |jammer |nonstd |radar |report |superag |tdd-tx |video |wimax-fixed |wimax-mobile**}

構文の説明

canopy	Canopy 干渉デバイスのアラームを設定します。
cont-tx	連続トランスミッタのアラームを設定します。
dect-like	Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話のアラームを設定します。
inv	スペクトル反転 Wi-Fi 信号を使用するデバイスのアラームを設定します。
jammer	電波妨害干渉デバイスのアラームを設定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスのアラームを設定します。
radar	レーダーのアラームを設定します。
report	干渉デバイスのレポートを有効にします。
superag	802.11 SuperAG 干渉デバイスのアラームを設定します。
tdd-tx	時分割複信（TDD）トランスミッタのアラームを設定します。
video	ビデオ カメラのアラームを設定します。
wimax-fixed	WiMax 固定干渉デバイスのアラームを設定します。
wimax-mobile	WiMax モバイル干渉デバイスのアラームを設定します。

コマンド デフォルト

Wi-Fi 反転デバイスのアラームは有効になっています。その他の干渉デバイスのアラームはすべて無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 5ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、CleanAir によるビデオ カメラの干渉時のレポートを有効にする例を示します。

```
Switch(config)# default ap dot11 5ghz cleanair device video
```

default ap dot11 5ghz rrm channel cleanair-event

5 GHzデバイスのイベント駆動型無線リソース管理（EDRRM）のデフォルトの状態とEDRRM感度を設定するには、グローバル コンフィギュレーション モードで **default apdot115ghzrrmchannelcleanair-event** コマンドを使用します。

default ap dot11 5ghz rrm channel cleanair-event ［**sensitivity** {**high** |**low** |**medium**}］

構文の説明

sensitivity	（任意）CleanAir イベントの EDRRM 感度を設定します。
high	（任意）電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最高に指定します。
low	（任意）AQ の値で示される、非 Wi-Fi 干渉に対する最も低い感度を指定します。
medium	（任意）AQ の値で示される、非 Wi-Fi 干渉に対する中程度の感度を指定します。

コマンド デフォルト

EDRRM が無効になっており、感度は low になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

感度を設定する前に EDRRM を有効にする必要があります。

次に、デフォルトの EDRRM の状態と感度を設定する例を示します。

```
Switch(config)# default ap dot11 5ghz rrm channel cleanair-event
Switch(config)# default ap dot11 5ghz rrm channel cleanair-event sensitivity
```

default ap dot11 5ghz rrm channel device

802.11a チャネルに永続的非 WiFi デバイスの回避のデフォルト状態を設定するには、グローバル コンフィギュレーション モードで **default apdot115ghzrrmchannel device** コマンドを使用します。

default ap dot11 5ghz rrm channel device

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

永続的デバイスの状態は無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、802.11a チャネルに永続的非 WiFi デバイスの回避を設定する例を示します。

```
Switch(config)# default ap dot11 5ghz rrm channel device
```

default ap dot11 24ghz cleanair alarm device

2.4 GHz 干渉デバイスのアラームのデフォルト値を設定するには、グローバル コンフィギュレーション モードで **default apdot1124ghz cleanairalarm device** コマンドを使用します。

default ap dot11 24ghz cleanair alarm device {**bt-discovery** | **bt-link** | **canopy** | **cont-tx** | **dect-like | fh** | **inv** | **jammer | mw-oven** | **nonstd** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee**}

構文の説明

bt-discovery	Bluetooth 干渉デバイスのアラームを設定します。
bt-link	Bluetooth リンクのアラームを設定します。
canopy	Canopy 干渉デバイスのアラームを設定します。
cont-tx	連続トランスミッタのアラームを設定します。
dect-like	Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話のアラームを設定します。
fh	802.11 周波数ホッピング（FH）デバイスのアラームを設定します。
inv	スペクトル反転 Wi-Fi 信号を使用するデバイスのアラームを設定します。
jammer	電波妨害干渉デバイスのアラームを設定します。
mw-oven	電子レンジのアラームを設定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスのアラームを設定します。
superag	802.11 SuperAG 干渉デバイスのアラームを設定します。
tdd-tx	時分割複信（TDD）トランスミッタのアラームを設定します。
video	ビデオ カメラのアラームを設定します。
wimax-fixed	WiMax 固定干渉デバイスのアラームを設定します。
wimax-mobile	WiMax モバイル干渉デバイスのアラームを設定します。
xbox	Xbox 干渉デバイスのアラームを設定します。
zigbee	802.15.4 干渉デバイスのアラームを設定します。

コマンド デフォルト

Wi-Fi 反転デバイスのアラームは有効になっています。その他のデバイスのアラームはすべて無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 24ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、デフォルトの CleanAir 2.4 GHz 干渉デバイスのアラームを設定する例を示します。

```
Switch(config)# default ap dot11 24ghz cleanair alarm device inv
```

default ap dot11 24ghz cleanair device

2.4 GHz 干渉デバイスのレポート生成のデフォルト状態を設定するには、グローバル コンフィギュレーション モードで **defaultapdot1124ghzcleanairdevice** コマンドを使用します。

default ap dot11 24ghz cleanair device {**ble-beacon**|**bt-discovery** |**bt-link** |**canopy** |**cont-tx** |**dect-like** |**fh** |**inv** |**jammer** |**mw-oven** |**nonstd** |**report** |**superag** |**tdd-tx** |**video** |**wimax-fixed** |**wimax-mobile** |**xbox** |**zigbee**}

構文の説明

ble-beacon	BLE ビーコン機能を設定します。
bt-discovery	Bluetooth 干渉デバイスのアラームを設定します。
bt-link	Bluetooth リンクのアラームを設定します。
canopy	Canopy 干渉デバイスのアラームを設定します。
cont-tx	連続トランスミッタのアラームを設定します。
dect-like	Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話のアラームを設定します。
fh	802.11 周波数ホッピング デバイスのアラームを設定します。
inv	スペクトル反転 Wi-Fi 信号を使用するデバイスのアラームを設定します。
jammer	電波妨害干渉デバイスのアラームを設定します。
mw-oven	電子レンジのアラームを設定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスのアラームを設定します。

superag	802.11 SuperAG 干渉デバイスのアラームを設定します。
tdd-tx	時分割複信（TDD）トランスミッタのアラームを設定します。
video	ビデオ カメラのアラームを設定します。
wimax-fixed	WiMax 固定干渉デバイスのアラームを設定します。
wimax-mobile	WiMax モバイル干渉デバイスのアラームを設定します。
xbox	Xbox 干渉デバイスのアラームを設定します。
zigbee	802.15.4 干渉デバイスのアラームを設定します。

コマンド デフォルト

Wi-Fi 反転デバイスのアラームが有効になっています。他のすべてのデバイスのアラームは無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE Denali 16.2.1	このコマンドが変更されました。**ble-beacon** キーワードが追加されました。

使用上のガイドライン

このコマンドを設定する前に、**ap dot11 24ghz cleanair** コマンドを使用して CleanAir を有効にする必要があります。

次に、CleanAir によるビデオ カメラの干渉時のレポートを有効にする例を示します。

```
Switch(config)# default ap dot11 24ghz cleanair device video
```

関連トピック

ap dot11 24ghz cleanair （26 ページ）
ap dot11 24ghz cleanair alarm air-quality （27 ページ）

ap dot11 24ghz cleanair alarm device （28 ページ）

default ap dot11 24ghz rrm channel cleanair-event

2.4 GHzデバイスのデフォルトのイベント駆動型無線リソース管理（EDRRM）の状態と感度を設定するには、グローバル コンフィギュレーション モードで **default apdot1124ghzrrmchannelcleanair-event** コマンドを使用します。

default ap dot11 24ghz rrm channel cleanair-event ［**sensitivity** ｛**high** | **low** | **medium**｝］

構文の説明

sensitivity	CleanAir イベントの EDRRM 感度を設定します。
high	電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最高に指定します。
low	電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最低に指定します。
medium	電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を中間に指定します。

コマンド デフォルト

EDRRM は無効で、感度は low です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、EDRRM を有効にし、デフォルトの EDRRM 感度を設定する例を示します。

```
Switch(config)# default ap dot11 24ghz rrm channel cleanair-event
Switch(config)# default ap dot11 24ghz rrm channel cleanair-event sensitivity
```

show ap dot11 5ghz cleanair air-quality summary

5 GHz 帯域の CleanAir AQ データを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ap dot11 5ghz cleanair air-quality summary** コマンドを使用します。

show ap dot11 5ghz cleanair air-quality summary

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、5 GHz 帯域の CleanAir AQ データを表示する例を示します。

```
Switch# show ap dot11 5ghz cleanair air-quality summary

AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-----------------------------------------------------------------
AP270ca.9b86.4546   1         99      99      0            No
AP2894.0f26.22df    6         98      97      0            No
AP2894.0f58.cc6b    11        99      99      0            No
AP2894.0f39.1040    6         97      97      0            No
AP2894.0f63.c6da    11        99      99      0            No
AP2894.0f58.d013    6         97      97      0            No
```

show ap dot11 5ghz cleanair air-quality worst

5 GHz 帯域の最も深刻な AQ データを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ap dot11 5ghz cleanair air-quality worst** コマンドを使用します。

show ap dot11 5ghz cleanair air-quality worst

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、5 GHz 帯域の最も深刻な AQ データを表示する例を示します。

```
Switch# show ap dot11 5ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-----------------------------------------------------------------
AP2894.0f39.1040    6         97      97      0            No
```

show ap dot11 5ghz cleanair config

5 GHz 帯域の CleanAir 設定を表示するには、**show ap dot11 5ghz cleanair config** コマンドを使用します。

show ap dot11 5ghz cleanair config

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

リリース 3.3 SE では、モビリティ エージェント（MA）でこのコマンドを設定できます。

次に、モビリティ コントローラ上の 5 GHz 帯域の CleanAir 設定を表示する例を示します。

```
Switch# show ap dot11 5ghz cleanair config

CleanAir Solution................................ : Enabled
Air Quality Settings:
    Air Quality Reporting........................ : Enabled
    Air Quality Reporting Period (min)........... : 15
    Air Quality Alarms........................... : Enabled
    Air Quality Alarm Threshold.................. : 1
Interference Device Settings:
    Interference Device Reporting................ : Enabled
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
        WiMax Fixed.............................. : Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
```

```
        WiMax Fixed.............................. : Enabled
    Interference Device Alarms................... : Enabled
Additional CleanAir Settings:
    CleanAir Event-driven RRM State.............. : Enabled
    CleanAir Driven RRM Sensitivity.............. : HIGH
    CleanAir Persistent Devices state............ : Enabled
```

次に、モビリティ エージェント上の 5 GHz 帯域の CleanAir 設定を表示する例を示します。

```
Switch# show ap dot11 5ghz cleanair config

Mobility Controller Link Status.................. : UP
CleanAir Solution................................ : Enabled
Air Quality Settings:
    Air Quality Reporting........................ : Enabled
    Air Quality Reporting Period (min)........... : 15
    Air Quality Alarms........................... : Enabled
    Air Quality Alarm Threshold.................. : 10
Interference Device Settings:
    Interference Device Reporting................ : Enabled
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
        WiMax Fixed.............................. : Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter.......................... : Disabled
        Jammer................................... : Disabled
        Continuous Transmitter................... : Disabled
        DECT-like Phone.......................... : Disabled
        Video Camera............................. : Disabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Disabled
        WiMax Mobile............................. : Disabled
        WiMax Fixed.............................. : Disabled
    Interference Device Alarms................... : Enabled
Additional CleanAir Settings:
    CleanAir Event-driven RRM State.............. : Disabled
    CleanAir Driven RRM Sensitivity.............. : LOW
    CleanAir Persistent Devices state............ : Disabled
```

show ap dot11 5ghz cleanair device type

5 GHz 干渉源デバイスを表示するには、**showapdot115ghzcleanairdevicetype** コマンドを使用します。

show ap dot11 5ghz cleanair device type {**all** |**canopy** |**cont-tx** |**dect-like** |**inv** |**jammer** |**nonstd** |**persistent** |**superag** |**tdd-tx** |**video** |**wimax-fixed** |**wimax-mobile**}

構文の説明

all	5 GHz 帯域のすべての CleanAir 干渉源デバイスを表示します。
canopy	5 GHz 帯域の canopy タイプの CleanAir 干渉源を表示します。
cont-tx	5 GHz 帯域の continuous transmitter タイプの CleanAir 干渉源を表示します。
dect-like	5 GHz 帯域の Digital Enhanced Cordless Communication（DECT）と同様の電話機タイプの CleanAir 干渉源を表示します。
inv	5 GHz 帯域のスペクトラム反転 WiFi 信号を使用している CleanAir 干渉源デバイスを表示します。
jammer	5 GHz 帯域の jammer タイプの CleanAir 干渉源を表示します。
nonstd	5 GHz 帯域の非標準 Wi-Fi チャネルを使用している CleanAir 干渉源デバイスを表示します。
persistent	5 GHz 帯域の CleanAir 永続型デバイスの干渉源を表示します。
superag	5 GHz 帯域の SuperAG タイプの CleanAir 干渉源を表示します
tdd-tx	5 GHz 帯域の CleanAir 時分割複信（TDD）トランスミッタを表示します。
video	5 GHz 帯域の video camera タイプの CleanAir 干渉源を表示します。
winmax-fixed	5 GHz 帯域の WiMax fixed タイプの CleanAir 干渉源を表示します。
wimax-mobile	5 GHz 帯域の WiMax mobile タイプの CleanAir 干渉源を表示します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

干渉源デバイスは、5 GHz デバイスから干渉がある場合にのみ表示されます。

次に、すべての 5 GHz 干渉源デバイスを表示する例を示します。

```
Switch# show ap dot11 5ghz cleanair device type all

DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

No    ClusterID          DevID  Type           AP Name                 ISI  RSSI  DC
Channel
-------------------------------------------------------------------------------------------
```

show ap dot11 24ghz cleanair air-quality summary

2.4 GHz 帯域の CleanAir AQ データを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ap dot11 24ghz cleanair air-quality summary** コマンドを使用します。

show ap dot11 24ghz cleanair air-quality summary

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、2.4 GHz 帯域の CleanAir AQ データを表示する例を示します。

```
Switch# show ap dot11 24ghz cleanair air-quality summary

AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-----------------------------------------------------------------
AP270ca.9b86.4546   1         99      99      0            No
AP2894.0f26.22df    6         98      97      0            No
AP2894.0f58.cc6b    11        99      99      0            No
AP2894.0f39.1040    6         97      97      0            No
AP2894.0f63.c6da    11        99      99      0            No
```

show ap dot11 24ghz cleanair air-quality worst

2.4 GHz 帯域の最も深刻な AQ データを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ap dot11 24ghz cleanair air-quality worst** コマンドを使用します。

show ap dot11 24ghz cleanair air-quality worst

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、2.4 GHz 帯域の最も深刻な AQ データを表示する例を示します。

```
Switch# show ap dot11 24ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-----------------------------------------------------------------
AP2895.0f39.1040    6         97      97      0            No
```

show ap dot11 24ghz cleanair config

2.4 GHz 帯域の CleanAir AQ データを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ap dot11 24ghz cleanair config** コマンドを使用します。

show ap dot11 24ghz cleanair config

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

リリース 3.3 SE では、モビリティ エージェント（MA）でこのコマンドを設定できます。

次に、モビリティ コントローラ上の 2.4 GHz 帯域の CleanAir 設定を表示する例を示します。

```
Switch# show ap dot11 24ghz cleanair config

CleanAir Solution................................ : Enabled
Air Quality Settings:
    Air Quality Reporting........................ : Enabled
    Air Quality Reporting Period (min)........... : 15
    Air Quality Alarms........................... : Enabled
    Air Quality Alarm Threshold.................. : 1
Interference Device Settings:
    Interference Device Reporting................ : Enabled
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
        WiMax Fixed.............................. : Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
```

```
        WiMax Fixed.............................. : Enabled
    Interference Device Alarms................... : Enabled
Additional CleanAir Settings:
    CleanAir Event-driven RRM State.............. : Enabled
    CleanAir Driven RRM Sensitivity.............. : HIGH
    CleanAir Persistent Devices state............ : Enabled
```

次に、モビリティ エージェント上の 2.4 GHz 帯域の CleanAir 設定を表示する例を示します。

```
Switch# show ap dot11 24ghz cleanair config

Mobility Controller Link Status.................. : UP
CleanAir Solution................................ : Enabled
Air Quality Settings:
    Air Quality Reporting........................ : Enabled
    Air Quality Reporting Period (min)........... : 15
    Air Quality Alarms........................... : Enabled
    Air Quality Alarm Threshold.................. : 10
Interference Device Settings:
    Interference Device Reporting................ : Enabled
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
        WiMax Fixed.............................. : Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter.......................... : Disabled
        Jammer................................... : Disabled
        Continuous Transmitter................... : Disabled
        DECT-like Phone.......................... : Disabled
        Video Camera............................. : Disabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Disabled
        WiMax Mobile............................. : Disabled
        WiMax Fixed.............................. : Disabled
    Interference Device Alarms................... : Enabled
Additional CleanAir Settings:
    CleanAir Event-driven RRM State.............. : Disabled
    CleanAir Driven RRM Sensitivity.............. : LOW
    CleanAir Persistent Devices state............ : Disabled
```

show ap dot11 24ghz cleanair summary

2.4 GHz CleanAir デバイスのサマリーを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **showapdot1124ghzcleanairsummary** コマンドを使用します。

show ap dot11 24ghz cleanair summary

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、**show ap dot11 24ghz cleanair summary** コマンドの出力例を示します。

```
Switch# show ap dot11 24ghz cleanair summary

AP Name              MAC Address         Slot ID  Spectrum Capable  Spectrum Intelligence
   Spectrum Oper State
-----------------------------------------------------------------------------------------------
AP1cdf.0f95.1719      0817.35c7.1a60            0  Disabled          Disabled
      Down
AS-5508-5-AP3         0817.35dd.9f40            0  Disabled          Disabled
      Down
AP270ca.9b86.4546     0c85.259e.c350            0  Enabled           Enabled
      Up
AP2894.0f26.22df      0c85.25ab.cca0            0  Enabled           Enabled
      Up
AP2894.0f58.cc6b      0c85.25c7.b7a0            0  Enabled           Enabled
      Up
AP2894.0f39.1040      0c85.25de.2c10            0  Enabled           Enabled
      Up
AP2894.0f63.c6da      0c85.25de.c8e0            0  Enabled           Enabled
      Up
```

第 II 部

インターフェイスおよびハードウェア コンポーネント

インターフェイスおよびハードウェア コマンド

client vlan

WLAN インターフェイスまたはインターフェイス グループを設定するには、**clientvlan** コマンドを使用します。WLAN インターフェイスをディセーブルにするには、このコマンドの **no** 形式を使用します。

client vlan *interface-id-name-or-group-name*
no client vlan

構文の説明

interface-id-name-or-group-name	インターフェイス ID、名前、または VLAN グループ名。インターフェイス ID は、複数桁で指定することもできます。

コマンド デフォルト

デフォルト インターフェイスが設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN のクライアント VLAN をイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# client vlan client-vlan1
Switch(config-wlan)# end
```

次に、WLAN 上のクライアント VLAN をディセーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no client vlan
Switch(config-wlan)# end
```

関連トピック

wlan （1283 ページ）

debug ilpower

電源コントローラおよびPower over Ethernet（PoE）システムのデバッグをイネーブルにするには、特権 EXEC モードで **debug ilpower** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ilpower {**cdp**|**controller**|**event**|**ha**|**ipc**|**police**|**port**|**powerman**|**registries**| **scp** |**sense**|**upoe**}
no debug ilpower {**cdp**|**controller**|**event**|**ha**|**ipc**|**police**|**port**|**powerman**|**registries**| **scp** |**sense**|**upoe**}

構文の説明

cdp	PoE Cisco Discovery Protocol（CDP）デバッグ メッセージを表示します。
controller	PoE コントローラ デバッグ メッセージを表示します。
event	PoE イベント デバッグ メッセージを表示します。
ha	PoE ハイ アベイラビリティ メッセージを表示します。
ipc	PoE Inter-Process Communication（IPC）デバッグ メッセージを表示します。
police	PoE police デバッグ メッセージを表示します。
port	PoE ポート マネージャ デバッグ メッセージを表示します。
powerman	PoE 電力管理デバッグ メッセージを表示します。
registries	PoE レジストリ デバッグ メッセージを表示します。
scp	PoE SCP デバッグ メッセージを表示します。
sense	PoE sense デバッグ メッセージを表示します。
upoe	Cisco UPOE デバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**upoe** キーワードが追加されました。

使用上のガイドライン

このコマンドは、PoE 対応スイッチだけでサポートされています。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* EXEC コマンドを使用して、アクティブ スイッチからのセッションを開始できます。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。

debug interface

インターフェイス関連アクティビティのデバッグをイネーブルにするには、特権EXECモードで**debug interface**コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug interface {*interface-id*|**counters** {**exceptions**|**protocol memory**}|**states**}
no debug interface {*interface-id*|**counters** {**exceptions**|**protocol memory**}|**states**}

構文の説明

interface-id	物理インターフェイスの ID。タイプ スイッチ番号/モジュール番号/ポート（例：gigabitethernet 1/0/2）によって識別される指定された物理ポートのデバッグ メッセージを表示します。
counters	カウンタ デバッグ情報を表示します。
exceptions	インターフェイス パケットおよびデータ レート統計情報の計算中に回復可能な例外条件が発生したときにデバッグ メッセージを表示します。
protocol memory	プロトコル カウンタのメモリ操作のデバッグ メッセージを表示します。
states	インターフェイスの状態が移行するときに中間のデバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

キーワードを指定しない場合は、すべてのデバッグ メッセージが表示されます。

undebug interface コマンドは、**no debug interface** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* EXEC コマンドを使用して、アクティブ スイッチからのセッションを開始できます。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。

debug lldp packets

Link Layer Discovery Protocol（LLDP）パケットのデバッグをイネーブルにするには、特権 EXEC モードで **debug lldp packets** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug lldp packets
no debug lldp packets

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

undebug lldp packets コマンドは、**no debug lldp packets** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* EXEC コマンドを使用して、アクティブ スイッチからのセッションを開始できます。

debug nmsp

スイッチの Network Mobility Services Protocol（NMSP）のデバッグをイネーブルにするには、特権 EXEC モードで **debug nmsp** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug nmsp {**all**|**connection**|**detail**|**error**|**event**|**message** {**rx**|**tx**}|**packet**} [**switch** *switch-number*]
no debug nmsp {**all**|**connection**|**detail**|**error**|**event**|**message** {**rx**|**tx**}|**packet**} [**switch** *switch-number*]

構文の説明

all	すべての NMSP デバッグ メッセージを表示します。
connection	NMSP 接続イベントのデバッグ メッセージを表示します。
detail	NMSP の詳細なデバッグ メッセージを表示します。
error	NMSP エラー メッセージのデバッグ情報を表示します。
event	NMSP イベントのデバッグ メッセージを表示します。
message	NMSP メッセージのデバッグ情報を表示します。
rx	NMSP 受信メッセージのデバッグ情報を表示します。
tx	NMSP 送信メッセージのデバッグ情報を表示します。
packet	NMSP パケット イベントのデバッグ メッセージを表示します。
switch *switch-number*	（任意）NMSP デバッグ情報を表示するスイッチ番号を指定します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

undebug nmsp コマンドは、**no debug nmsp** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* EXEC コマンドを使用して、アクティブ スイッチからのセッションを開始できます。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。

debug platform poe

Power over Ethernet（PoE）ポートのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform poe** コマンドを使用します。デバッグを無効にするには、このコマンドの **no** 形式を使用します。

debug platform poe [{**error**|**info**}] [**switch** *switch-number*]
no debug platform poe [{**error**|**info**}] [**switch** *switch-number*]

構文の説明

error	（任意）PoE 関連エラーのデバッグ メッセージを表示します。
info	（任意）PoE 関連情報のデバッグ メッセージを表示します。
switch *switch-number*	（任意）スタック メンバを指定します。このキーワードは、スタック対応スイッチでのみサポートされています。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

undebug platform poe コマンドは、**no debug platform poe** コマンドと同じです。

duplex

ポートのデュプレックス モードで動作するように指定するには、インターフェイス コンフィギュレーション モードで **duplex** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

duplex {**auto**|**full**|**half**}
no duplex {**auto**|**full**|**half**}

構文の説明

auto	自動によるデュプレックス設定をイネーブルにします。接続されたデバイス モードにより、ポートが自動的に全二重モードか半二重モードで動作すべきかを判断します。
full	全二重モードをイネーブルにします。
half	半二重モードをイネーブルにします（10 または 100 Mb/s で動作するインターフェイスに限る）。1000 または 10,000 Mb/s で動作するインターフェイスに対して半二重モードを設定できません。

コマンド デフォルト

ギガビット イーサネット ポートに対するデフォルトは **auto** です。

10 ギガビット イーサネット ポートではデュプレックス モードを設定できません。常に **full** です。

二重オプションは、1000BASE-*x* または 10GBASE-*x*（-*x* は -BX、-CWDM、-LX、-SX、または -ZX）SFP モジュールではサポートされていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ギガビットイーサネットポートでは、接続装置がデュプレックスパラメータの自動ネゴシエーションを行わない場合にポートを **auto** に設定すると、**full** を指定するのと同じ効果があります。

（注） デュプレックスモードが **auto** で接続されている装置が半二重で動作している場合、半二重モードはギガビット イーサネット インターフェイスでサポートされます。ただし、これらのインターフェイスを半二重モードで動作するように設定することはできません。

特定のポートを全二重または半二重のいずれかに設定できます。このコマンドの適用可能性は、スイッチが接続されているデバイスによって異なります。

両方のラインの終端が自動ネゴシエーションをサポートしている場合、デフォルトの自動ネゴシエーションを使用することを強く推奨します。片方のインターフェイスが自動ネゴシエーションをサポートし、もう片方がサポートしていない場合、両方のインターフェイス上でデュプレックスと速度を設定し、サポートされている側で **auto** の設定を使用してください。

速度が **auto** に設定されている場合、スイッチはもう一方のリンクの終端にある装置と速度設定についてネゴシエートし、速度をネゴシエートされた値に強制的に設定します。デュプレックス設定はリンクの両端での設定が引き継がれますが、これにより、デュプレックス設定に矛盾が生じることがあります。

デュプレックス設定を行うことができるのは、速度が **auto** に設定されている場合です。

注意 インターフェイス速度およびデュプレックスモードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再びイネーブルになる場合があります。

設定を確認するには、**show interfaces** 特権 EXEC コマンドを入力します。

例

次の例では、インターフェイスを全二重動作に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# duplex full
```

関連トピック

show interfaces （132 ページ）

errdisable detect cause

特定の原因またはすべての原因に対して errdisable 検出をイネーブルにするには、グローバル コンフィギュレーション モードで **errdisable detect cause** コマンドを使用します。errdisable 検出機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

errdisable detect cause {all|arp-inspection|bpduguard shutdown vlan|dhcp-rate-limit|dtp-flap|gbic-invalid|inline-power|l2ptguard|link-flap|loopback|pagp-flap|pppoe-ia-rate-limit|security-violation shutdown vlan|sfp-config-mismatch}
no errdisable detect cause {all|arp-inspection|bpduguard shutdown vlan|dhcp-rate-limit|dtp-flap|gbic-invalid|inline-power|l2ptguard|link-flap|loopback|pagp-flap|pppoe-ia-rate-limit|security-violation shutdown vlan|sfp-config-mismatch}

構文の説明

all	すべての errdisable の原因に対して、エラー検出をイネーブルにします。
arp-inspection	ダイナミック アドレス解決プロトコル（ARP）インスペクションのエラー検出をイネーブルにします。
bpduguard shutdown vlan	BPDU ガードで VLAN ごとに errdisable をイネーブルにします。
dhcp-rate-limit	Dynamic Host Configuration Protocol（DHCP）スヌーピング用のエラー検出をイネーブルにします。
dtp-flap	ダイナミック トランキング プロトコル（DTP）フラップのエラー検出をイネーブルにします。
gbic-invalid	無効なギガビット インターフェイス コンバータ（GBIC）モジュール用のエラー検出をイネーブルにします。 （注） このエラーは、無効な Small Form-Factor Pluggable（SFP）モジュールを意味します。
inline-power	Power over Ethernet（PoE）の errdisable 原因に対して、エラー検出をイネーブルにします。 （注） このキーワードは、PoE ポートを備えたスイッチでのみサポートされています。
l2ptguard	レイヤ 2 プロトコル トンネルの errdisable 原因に対して、エラー検出をイネーブルにします。
link-flap	リンクステートのフラップに対して、エラー検出をイネーブルにします。
loopback	検出されたループバックに対して、エラー検出をイネーブルにします。

pagp-flap	ポート集約プロトコル（PAgP）フラップの errdisable 原因のエラー検出をイネーブルにします。
pppoe-ia-rate-limit	PPPoE 中継エージェントのレート制限 errdisable 原因に対して、エラー検出をイネーブルにします。
security-violation shutdown vlan	音声認識 IEEE 802.1x セキュリティをイネーブルにします。
sfp-config-mismatch	SFP 設定の不一致によるエラー検出をイネーブルにします。

コマンド デフォルト

検出はすべての原因に対してイネーブルです。VLAN ごとの errdisable を除くすべての原因について、ポート全体をシャットダウンするように設定されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

原因（link-flap、dhcp-rate-limit など）は、errdisable ステートが発生した理由です。原因がインターフェイスで検出された場合、インターフェイスは errdisable ステートとなり、リンクダウン ステートに類似した動作ステートとなります。

ポートが errdisable になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。ブリッジ プロトコル データ ユニット（BPDU）ガード、音声認識 802.1x セキュリティ、およびポート セキュリティ機能の場合は、違反の発生時にポート全体をシャットダウンする代わりに、ポートで問題となっている VLAN のみをシャットダウンするようにスイッチを設定できます。

errdisable recovery グローバル コンフィギュレーション コマンドを入力して、原因の回復メカニズムを設定する場合は、すべての原因がタイムアウトになった時点で、インターフェイスは errdisable ステートから抜け出して、処理を再試行できるようになります。回復メカニズムを設定しない場合は、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、インターフェイスを手動で errdisable ステートから回復させる必要があります。

設定を確認するには、**show errdisable detect** 特権 EXEC コマンドを入力します。

次の例では、リンクフラップ errdisable 原因に対して errdisable 検出をイネーブルにする方法を示します。

```
Switch(config)# errdisable detect cause link-flap
```

次のコマンドでは、VLAN ごとの errdisable ステートで BPDU ガードをグローバルに設定する方法を示します。

```
Switch(config)# errdisable detect cause bpduguard shutdown vlan
```

次のコマンドでは、VLAN ごとの errdisable ステートで音声認識 802.1x セキュリティをグローバルに設定する方法を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

show errdisable detect 特権 EXEC コマンドを入力すると、設定を確認できます。

関連トピック

show errdisable detect （128 ページ）

errdisable recovery cause

特定の原因から回復するようにerror-disabledメカニズムをイネーブルにするには、グローバル コンフィギュレーション モードで **errdisable recovery cause** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

errdisable recovery cause
{all | arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit | dtp-flap | gbic-invalid | inline-power | l2ptguard | link-flap | mac-limit | pagp-flap | psecure-violation | security-violation | sfp-config-mismatch | storm-control | udld | vmps}
no errdisable recovery cause
{all | arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit | dtp-flap | gbic-invalid | inline-power | l2ptguard | link-flap | mac-limit | pagp-flap | psecure-violation | security-violation | sfp-config-mismatch | storm-control | udld | vmps}

構文の説明

all	すべてのerrdisableの原因から回復するタイマーをイネーブルにします。
arp-inspection	アドレス解決プロトコル（ARP）検査による errdisable ステートから回復するためのタイマーをイネーブルにします。
bpduguard	ブリッジ プロトコル データ ユニット（BPDU）ガード errdisable ステートから回復するタイマーをイネーブルにします。
channel-misconfig	EtherChannel 設定の矛盾による errdisable ステートから回復するタイマーをイネーブルにします。
dhcp-rate-limit	DHCP スヌーピング errdisable ステートから回復するタイマーをイネーブルにします。
dtp-flap	ダイナミック トランキング プロトコル（DTP）フラップ errdisable ステートから回復するタイマーをイネーブルにします。
gbic-invalid	ギガビットインターフェイス コンバータ（GBIC）モジュールを無効な errdisable ステートから回復するタイマーをイネーブルにします。 （注） このエラーは無効な Small Form-Factor Pluggable（SFP）の errdisable ステートを意味します。
inline-power	Power over Ethernet（PoE）の errdisable ステートから回復するタイマーをイネーブルにします。 このキーワードは、PoE ポートを備えたスイッチでのみサポートされています。
l2ptguard	レイヤ2プロトコル トンネルによる errdisable ステートから回復するためのタイマーをイネーブルにします。

link-flap	リンクフラップ errdisable ステートから回復するタイマーをイネーブルにします。
loopback	ループバック errdisable ステートから回復するタイマーをイネーブルにします。
mac-limit	MAC 制限 errdisable ステートから回復するタイマーをイネーブルにします。
pagp-flap	ポート集約プロトコル（PAgP）フラップ errdisable ステートから回復するタイマーをイネーブルにします。
port-mode-failure	ポート モードの変更失敗の errdisable ステートから回復するタイマーをイネーブルにします。
pppoe-ia-rate-limit	PPPoE IA レート制限 errdisable ステートから回復するタイマーをイネーブルにします。
psecure-violation	ポート セキュリティ違反ディセーブル ステートから回復するタイマーをイネーブルにします。
security-violation	IEEE 802.1x 違反ディセーブル ステートから回復するタイマーをイネーブルにします。
sfp-config-mismatch	SFP設定の不一致によるエラー検出をイネーブルにします。
storm-control	ストーム制御エラーから回復するタイマーをイネーブルにします。
udld	単方向リンク検出（UDLD）errdisable ステートから回復するタイマーをイネーブルにします。
vmps	VLAN メンバーシップ ポリシー サーバ（VMPS）errdisable ステートから回復するタイマーをイネーブルにします。

コマンド デフォルト

すべての原因に対して回復はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

原因（all、BDPU ガードなど）は、errdisable ステートが発生した理由として定義されます。原因がインターフェイスで検出された場合、インターフェイスは errdisable ステート（リンクダウン ステートに類似した動作ステート）となります。

ポートが errdisable になっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。BPDU ガード機能およびポートセキュリティ機能の場合は、違反の発生時にポート全体をシャットダウンする代わりに、ポートで問題となっている VLAN だけをシャットダウンするようにスイッチを設定できます。

原因の回復をイネーブルにしない場合、インターフェイスは、**shutdown** 及び **no shutdown** インターフェイス コンフィギュレーション コマンドが入力されるまで error-disabled ステートのままです。原因の回復をイネーブルにした場合、インターフェイスは errdisable ステートから回復し、すべての原因がタイムアウトになったときに処理を再開できるようになります。

原因の回復をイネーブルにしない場合、まず **shutdown** コマンドを入力し、次に **no shutdown** コマンドを入力して、手動でインターフェイスを error-disabled ステートから回復させる必要があります。

設定を確認するには、**show errdisable recovery** 特権 EXEC コマンドを入力します。

例

次の例では、BPDU ガード errdisable 原因に対して回復タイマーをイネーブルにする方法を示します。

```
Switch(config)# errdisable recovery cause bpduguard
```

関連トピック

errdisable recovery interval （76 ページ）
show errdisable recovery （130 ページ）
show interfaces （132 ページ）

errdisable recovery interval

error-disabled ステートから回復する時間を指定するには、グローバル コンフィギュレーション モードで **errdisable recovery interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

errdisable recovery interval *timer-interval*
no errdisable recovery interval *timer-interval*

構文の説明

timer-interval	errdisable ステートから回復する時間。指定できる範囲は 30 ～ 86400 秒です。すべての原因に同じ間隔が適用されます。デフォルトの間隔は 300 秒です。

コマンド デフォルト

デフォルトの回復間隔は 300 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

errdisable recovery のタイマーは、設定された間隔値からランダムな差で初期化されます。実際のタイムアウト値と設定された値の差は、設定された間隔の 15% まで認められます。

設定を確認するには、**show errdisable recovery** 特権 EXEC コマンドを入力します。

例

次の例では、タイマーを 500 秒に設定する方法を示します。

```
Switch(config)# errdisable recovery interval 500
```

関連トピック

errdisable recovery cause （73 ページ）
show errdisable recovery （130 ページ）
show interfaces （132 ページ）

interface

インターフェイスを設定するには、**interface** コマンドを使用します。

interface {**Auto-Template** *Auto-Template interface-number*|**Capwap** *Capwap interface-number*|**GigabitEthernet** *Gigabit Ethernet interface number*| **Group VI** *Group VI interface number* **Internal Interface** *Internal Interface number* **Loopback** *Loopback interface number* **Null** *Null interface number* **Port-channel** *interface number* **Port-channel** *interface number* **TenGigabitEthernet** *interface number* **Tunnel** *interface number* **Vlan** *interface number*}

構文の説明

Auto-Template *Auto-template interface-number*	自動テンプレート インターフェイスを設定できます。指定できる範囲は 1 ～ 999 です。
Capwap *Capwap interface number*	Control And Provisioning of Wireless Access Points（CAPWAP）トンネル インターフェイスを設定できます。指定できる範囲は 0 ～ 2147483647 です。
GigabitEthernet *Gigabit Ethernet interface number*	ギガビット イーサネット IEEE 802.3z インターフェイスを設定できます。範囲は 0 ～ 9 です。
Group VI *Group VI interface number*	Group VI インターフェイスを設定できます。範囲は 0 ～ 9 です。
Internal Interface 内部インターフェイス	内部インターフェイスを設定できます。
Loopback *Loopback Interface number*	ループバック インターフェイスを設定できます。指定できる範囲は 0 ～ 2147483647 です。
Null *Null interface number*	ヌル インターフェイスを設定できます。デフォルト値は 0 です
Port-channel *interface number*	ポートチャネル インターフェイスを設定できます。有効な範囲は 1 ～ 128 です。
TenGigabitEthernet *interface number*	10 ギガビット イーサネット インターフェイスを設定できます。範囲は 0 ～ 9 です。
Tunnel *interface number*	トンネル インターフェイスを設定できます。指定できる範囲は 0 ～ 2147483647 です。
Vlan *interface number*	スイッチ VLAN を設定できます。範囲は 0 ～ 4098 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは「no」形式を使用できません。

次に、トンネル インターフェイスを設定する例を示します。

```
Switch# interface Tunnel 15
```

interface range

インターフェイス範囲を設定するには、**interfacerange** コマンドを使用します。

interface range {**Gigabit Ethernet** *interface-number*| **Loopback** *interface-number*| **Port Channel** *interface-number*| **TenGigabit Ethernet** *interface-number* **Tunnel** *interface-number* **Vlan** *interface-number* **Macro** *WORD*}

構文の説明

GigabitEthernet *interface-number*	ギガビット イーサネット IEEE 802.3z インターフェイスを設定します。値の範囲は 1 ～ 9 です。
Loopback *interface-number*	ループバック インターフェイスを設定します。値の範囲は 0 ～ 2147483647 です。
Port-Channel *interface-number*	インターフェイスの 10 ギガビット イーサネット チャネルを設定します。値の範囲は 1 ～ 128 です。
TenGigabit Ethernet *interface-number*	10 ギガビットイーサネットインターフェイスを設定します。値の範囲は 0 ～ 9 です。
Tunnel *interface-number*	トンネル インターフェイスを設定します。値の範囲は 0 ～ 2147483647 です。
VLAN *interface-number*	スイッチの VLAN インターフェイスを設定します。値の範囲は 1 ～ 4095 です。
Macro *WORD*	インターフェイスに対するキーワードを設定します。最大 32 文字までサポートされます。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、インターフェイス範囲を設定する例を示します。

```
Switch(config)# interface range vlan 1
```

ip mtu

スイッチまたはスイッチ スタックのすべてのルーテッド ポートのルーテッド パケットの IP 最大伝送ユニット（MTU）サイズを設定するには、インターフェイス コンフィギュレーション モードで **ip mtu** コマンドを使用します。デフォルトの IP MTU サイズに戻すには、このコマンドの **no** 形式を使用します。

ip mtu *bytes*
no ip mtu *bytes*

構文の説明

bytes	MTU サイズ（バイト単位）。指定できる範囲は 68 からシステム MTU 値（バイト単位）までです。

コマンド デフォルト

すべてのスイッチ インターフェイスで送受信されるフレームのデフォルト IP MTU サイズは、1500 バイトです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

IP 値の上限は、スイッチまたはスイッチ スタックの設定に基づき、現在適用されているシステム MTU 値を参照します。MTU サイズの設定に関する詳細については、**system mtu** グローバル コンフィギュレーション コマンドを参照してください。

デフォルトの IP MTU 設定に戻すには、インターフェイスで **default ip mtu** コマンドまたは **no ip mtu** コマンドを適用できます。

show ip interface *interface-id* または **show interfaces** *interface-id* 特権 EXEC コマンドを入力して設定を確認できます。

次に、VLAN 200 の最大 IP パケット サイズを 1000 バイト に設定する例を示します。

```
Switch(config)# interface vlan 200
Switch(config-if)# ip mtu 1000
```

次に、VLAN 200 の最大 IP パケット サイズをデフォルト設定の 1500 バイト に設定する例を示します。

```
Switch(config)# interface vlan 200
Switch(config-if)# default ip mtu
```

次に、**show ip interface** *interface-id* コマンドの出力の一部を示します。インターフェイスの現在の IP MTU 設定が表示されます。

```
Switch# show ip interface gigabitethernet4/0/1
GigabitEthernet4/0/1 is up, line protocol is up
  Internet address is 18.0.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set

<output truncated>
```

関連トピック

show interfaces （132 ページ）
system mtu （172 ページ）

ipv6 mtu

スイッチまたはスイッチ スタックのすべてのルーテッド ポートにルーテッド パケットの IPv6 最大伝送ユニット（MTU）サイズを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 mtu** コマンドを使用します。デフォルトの IPv6 MTU サイズに戻すには、このコマンドの **no** 形式を使用します。

ipv6 mtu *bytes*
no ipv6 mtu *bytes*

構文の説明

bytes	MTU サイズ（バイト単位）。指定できる範囲は 1280 からシステム MTU 値（バイト単位）までです。

コマンド デフォルト

すべてのスイッチ インターフェイスで送受信されるフレームのデフォルト IPv6 MTU サイズは、1500 バイトです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

IPv6 MTU 値の上限は、スイッチまたはスイッチ スタックの設定に基づき、現在適用されているシステム MTU 値を参照します。MTU サイズの設定に関する詳細については、**system mtu** グローバル コンフィギュレーション コマンドを参照してください。

デフォルトの IPv6 MTU 設定に戻すには、インターフェイスで **default ipv6 mtu** コマンドまたは **no ipv6 mtu** コマンドを適用できます。

show ipv6 interface *interface-id* または **show interface** *interface-id* 特権 EXEC コマンドを入力して設定を確認できます。

次に、インターフェイスの最大 IPv6 パケット サイズを 2000 バイトに設定する例を示します。

```
Switch(config)# interface gigabitethernet4/0/1
Switch(config-if)# ipv6 mtu 2000
```

次に、インターフェイスの最大 IPv6 パケット サイズをデフォルト設定の 1500 バイトに設定する例を示します。

```
Switch(config)# interface gigabitethernet4/0/1
Switch(config-if)# default ipv6 mtu
```

次に、**show ipv6 interface** *interface-id* コマンドの出力の一部を示します。インターフェイスの現在の IPv6 MTU 設定が表示されます。

```
Switch# show ipv6 interface gigabitethernet4/0/1
GigabitEthernet4/0/1 is up, line protocol is up
  Internet address is 18.0.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set

<output truncated>
```

関連トピック

show interfaces （132 ページ）
system mtu （172 ページ）

lldp（インターフェイス コンフィギュレーション）

インターフェイスのLink Layer Discovery Protocol（LLDP）をイネーブルにするには、インターフェイス コンフィギュレーション モードで **lldp** コマンドを使用します。インターフェイスでLLDP をディセーブルにするには、このコマンドの **no** 形式を使用します。

lldp {**med-tlv-select** *tlv*|**receive**|**tlv-select power-management**|**transmit**}
no lldp {**med-tlv-select** *tlv*|**receive**|**tlv-select power-management**|**transmit**}

構文の説明

med-tlv-select	LLDP Media Endpoint Discovery（LLDP-MED）の Time Length Value（TLV）要素を送信するように選択します。
tlv	TLV 要素を特定するストリング。有効な値は次のとおりです。 • **inventory-management**：LLDP MED インベントリ管理 TLV。 • **location**：LLDP MED ロケーション TLV。 • **network-policy**：LLDP MED ネットワーク ポリシー TLV。 • **power-management**：LLDP MED 電源管理 TLV。
receive	LLDP 伝送を受信するようにインターフェイスをイネーブルにします。
tlv-select	送信する LLDP TLV を選択します。
power-management	LLDP 電源管理 TLV を送信します。
transmit	インターフェイスで LLDP 伝送をイネーブルにします。

コマンド デフォルト

LLDP はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、802.1 メディア タイプでサポートされています。

インターフェイスがトンネル ポートに設定されていると、LLDP は自動的にディセーブルになります。

インターフェイスの LLDP 伝送をディセーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no lldp transmit
```

インターフェイスの LLDP 伝送をイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# lldp transmit
```

logging event power-inline-status

Power over Ethernet（PoE）イベントのロギングを有効にするには、インターフェイス コンフィギュレーション モードで **logging event power-inline-status** コマンドを使用します。PoE ステータス イベントのロギングを無効にするには、このコマンドの **no** 形式を使用します。

logging event power-inline-status
no logging event power-inline-status

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

PoE イベントのロギングはイネーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドの **no** 形式を使用しても、PoE エラー イベントは無効になりません。

例

次の例では、ポート上で PoE イベントのロギングをイネーブルにする方法を示します。

```
Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# logging event power-inline-status
Switch(config-if)#
```

関連トピック

power inline （97 ページ）
show power inline （154 ページ）

mdix auto

インターフェイスで Automatic Medium-Dependent Interface Crossover（Auto MDIX）機能をイネーブルにするには、インターフェイス コンフィギュレーション モードで **mdix auto** コマンドを使用します。Auto MDIX をディセーブルにするには、このコマンドの **no** 形式を使用します。

mdix auto
no mdix auto

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

Auto MDIX は、イネーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

Auto MDIX がイネーブルな場合、インターフェイスは自動的に必要なケーブル接続タイプ（ストレートまたはクロス）を検出し、接続を適切に設定します。

インターフェイスの Auto MDIX をイネーブルにする場合は、機能が正常に動作するように、インターフェイス速度とデュプレックスも **auto** に設定する必要があります。

Auto MDIX が（速度とデュプレックスの自動ネゴシエーションとともに）接続するインターフェイスの一方または両方でイネーブルの場合は、ケーブル タイプ（ストレートまたはクロス）が不正でもリンクがアップします。

インターフェイスの Auto-MDIX の動作ステートを確認するには、**show controllers ethernet-controller** *interface-id* **phy** 特権 EXEC コマンドを入力します。

次の例では、ポートの Auto MDIX をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

関連トピック

show controllers ethernet-controller （109 ページ）

mode（電源スタックの設定）

設定内容 電源スタックの電源スタックモードを設定するには、電源スタック コンフィギュレーション モードで **mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mode {**power-shared**|**redundant**} **[strict]**
no mode

構文の説明

power-shared	電源スタックが電源共有モードで動作するよう、設定します。これはデフォルトです。
redundant	電源スタックが冗長モードで動作するよう、設定します。他の電源の1つに障害が発生した場合のバックアップ電源として使用するため、最大の電源が電源プールから削除されます。
strict	（任意）電力バジェットが正確に実行されるよう、電源スタックモードを設定します。スタック電力は、使用可能電力を超えることができません。

コマンド デフォルト

デフォルト モードは **power-shared** および nonstrict です。

コマンド モード

電源スタックの設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、IP Base または IP Services フィーチャ セットが実行されているスイッチ スタックでのみ使用できます。

電源スタック コンフィギュレーション モードにアクセスするには、**stack-power stack** *power stack name* グローバル コンフィギュレーション コマンドを入力します。

no mode コマンドを入力すると、スイッチが、デフォルトの **power-shared** モードおよび non-strict モードに設定されます。

（注） スタック電源の場合、使用可能電力は、PoEで使用できる、電源スタックのすべての電源からの合計電力です。使用可能電力は、スタックのPoEポートに接続されているすべての受電デバイスに割り当てられている電力です。消費電力は、受電デバイスで実際に消費される電力です。

power-shared モードでは、すべての入力電力を負荷に使用でき、使用可能な合計電力は 1 つの大きな電源として扱われます。電力バジェットには、すべての電源から供給されるすべての電力が含まれます。電源障害の場合に除外される電力はありません。電源に障害が発生した場合、負荷制限（受電デバイスまたはスイッチのシャットダウン）が発生する場合があります。

redundant モードでは、他の電源の 1 つに障害が発生した場合のバックアップ電源として使用するため、最大の電源が電源プールから削除されます。使用可能な電力バジェットは、合計電力から最大の電源を差し引いたものです。これによって、スイッチおよび受電デバイスのプールで使用できる電力が減少しますが、障害または過剰な電力負荷が発生した場合に、スイッチまたは受電デバイスのシャットダウンの必要性が小さくなります。

strict モードでは、電源に障害が発生し、使用可能な電力が電力バジェットを下回った場合、システムによって、実際の電力が使用可能な電力よりも少ないかのように、受電デバイスの負荷制限を介してバジェットのバランスがとられます。nonstrict モードでは、電源スタックは割り当て超過状態で実行でき、実際の電力が使用可能な電力を超過しない限り、安定しています。このモードでは、受電デバイスが通常の電力を超えて電力を引き出すと、電源スタックが負荷制限を開始することがあります。ほとんどの装置は全出力電力では実行されないため、これは、通常、問題ではありません。スタック内で同時に最大電力を必要とする複数の受電デバイスが存在する可能性は、小さいからです。

strict モードと nonstrict モードの両方とも、電力バジェットに使用可能な電力がなくなった時点で、電力は拒否されます。

次に、power1 という名前のスタックの電源スタックモードを、電力バジェットを strict にした power-shared に設定する例を示します。スタック内のすべての電力は共有されますが、使用可能な電力全体が割り当てられた場合、電力を使用できる余分な装置はなくなります。

```
Switch(config)# stack-power stack power1
Switch(config-stackpower)# mode power-shared strict
Switch(config-stackpower)# exit
```

次に、power2 という名前のスタックの電源スタックモードを redundant に設定する例を示します。スタック内の最大の電源は電源プールから削除され、他の電源の 1 つが発生した場合に冗長性が提供されます。

```
Switch(config)# stack-power stack power2
Switch(config-stackpower)# mode redundant
Switch(config-stackpower)# exit
```

関連トピック

stack-power （165 ページ）

network-policy

インターフェイスにネットワークポリシー プロファイルを適用するには、インターフェイス コンフィギュレーション モードで **network-policy** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

network-policy *profile-number*
no network-policy

構文の説明

profile-number	インターフェイスに適用するネットワークポリシー プロファイル番号

コマンド デフォルト

ネットワークポリシー プロファイルは適用されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

インターフェイスにプロファイルを適用するには、**network-policy** *profile number* インターフェイス コンフィギュレーション コマンドを使用します。

最初にネットワークポリシー プロファイルを設定する場合、インターフェイスに **switchport voice vlan** コマンドを適用できません。ただし、**switchport voice vlan** *vlan-id* がすでにインターフェイス上に設定されている場合、ネットワークポリシープロファイルをインターフェイス上に適用できます。その後、インターフェイスは、適用された音声または音声シグナリング VLAN ネットワークポリシー プロファイルを使用します。

次の例では、インターフェイスにネットワークポリシー プロファイル 60 を適用する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# network-policy 60
```

関連トピック

network-policy profile（グローバル コンフィギュレーション） （91 ページ）
show network-policy profile （152 ページ）
voice-signaling vlan（ネットワークポリシー コンフィギュレーション） （173 ページ）
voice vlan（ネットワークポリシー コンフィギュレーション） （175 ページ）

network-policyprofile（グローバルコンフィギュレーション）

ネットワークポリシー プロファイルを作成し、ネットワークポリシー コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **network-policy profile** コマンドを使用します。ポリシーを削除して、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

network-policy profile *profile-number*
no network-policy profile *profile-number*

構文の説明

profile-number	ネットワークポリシー プロファイル番号。指定できる範囲は 1 ～ 4294967295 です。

コマンド デフォルト

ネットワークポリシー プロファイルは定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

プロファイルを作成し、ネットワークポリシー プロファイル コンフィギュレーション モードを開始するには、**network-policy profile** グローバル コンフィギュレーション コマンドを使用します。

ネットワークポリシー プロファイル コンフィギュレーション モードから特権 EXEC モードに戻る場合は、**exit** コマンドを入力します。

ネットワークポリシー プロファイル コンフィギュレーション モードの場合、VLAN、Class of Service（CoS）、Diffserv コード ポイント（DSCP）の値、およびタギング モードを指定することで、音声および音声シグナリング用のプロファイルを作成することができます。

これらのプロファイルの属性は、Link Layer Discovery Protocol for Media Endpoint Devices（LLDP-MED）の network-policy Time Length Value（TLV）に含まれます。

次の例では、ネットワークポリシー プロファイル 60 を作成する方法を示します。

```
Switch(config)# network-policy profile 60
Switch(config-network-policy)#
```

関連トピック

network-policy （90 ページ）

show network-policy profile （152 ページ）
voice-signaling vlan（ネットワークポリシー コンフィギュレーション） （173 ページ）
voice vlan（ネットワークポリシー コンフィギュレーション） （175 ページ）

nmsp attachment suppress

特定のインターフェイスからのアタッチメント情報のレポートを抑制するには、インターフェイス コンフィギュレーション モードで **nmsp attachment suppress** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

nmsp attachment suppress
no nmsp attachment suppress

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ロケーションおよびアタッチメント通知を Cisco モビリティ サービス エンジン（MSE）に送信しないようにインターフェイスを設定するには、**nmsp attachment suppress** インターフェイス コンフィギュレーション コマンドを使用します。

次の例では、アタッチメント情報を MSE に送信しないようにインターフェイスを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# nmsp attachment suppress
```

関連トピック

show nmsp

power efficient-ethernet auto

インターフェイスの EEE をイネーブルにするには、インターフェイス コンフィギュレーション モードで **power efficient-ethernet auto** コマンドを使用します。インターフェイスで EEE をディセーブルにするには、このコマンドの **no** 形式を使用します。

power efficient-ethernet auto
no power efficient-ethernet auto

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

EEE は、ディセーブルにされています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

低電力アイドル（LPI）モードをサポートするデバイスで EEE をイネーブルにできます。このようなデバイスは、低い使用率のときに LPI モードを開始して、電力を節約できます。LPI モードでは、リンクの両端にあるシステムは、特定のサービスをシャットダウンして、電力を節約できます。EEE は上位層プロトコルおよびアプリケーションに対して透過的であるように、LPI モードに移行したり、LPI モードから移行する必要があるプロトコルを提供します。

インターフェイスが EEE に対応している場合にのみ、**power efficient-ethernet auto** コマンドを使用できます。インターフェイスが EEE に対応しているかどうかを確認するには、**show eee capabilities** EXEC コマンドを使用します。

EEE がイネーブルの場合、スイッチはリンク パートナーに EEE をアドバタイズし、自動ネゴシエートします。インターフェイスの現在の EEE ステータスを表示するには、**show eee status** EXEC コマンドを使用します。

このコマンドにライセンスは必要ありません。

次に、インターフェイスで EEE をイネーブルにする例を示します。

```
Switch(config-if)# power efficient-ethernet auto
Switch(config-if)#
```

次に、インターフェイスで EEE をディセーブルにする例を示します。

```
Switch(config-if)# no power efficient-ethernet auto
Switch(config-if)#
```

power-priority

電源スタックのスイッチと高プライオリティおよび低プライオリティ PoE ポートに対して、Cisco StackPower の電源プライオリティ値を設定するには、スイッチ スタック電源コンフィギュレーション モードで **power-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

power-priority {**high** *value*|**low** *value*|**switch** *value*}
no power-priority {**high**|**low**|**switch**}

構文の説明

high *value*	ポートの電力プライオリティを高プライオリティ ポートとして設定します。値は1～27です。1が最高のプライオリティです。**high**の値は、低プライオリティ ポートに設定する値よりも小さく、スイッチに設定する値よりも大きくする必要があります。
low *value*	ポートの電力プライオリティを低プライオリティ ポートとして設定します。指定できる範囲は1～27です。**low**の値は、高プライオリティ ポートおよびスイッチに設定された値よりも大きくする必要があります。
switch *value*	スイッチの電力プライオリティを設定します。指定できる範囲は 1 ～ 27 です。**switch** の値は、低プライオリティ ポートおよび高プライオリティ ポートに設定された値よりも小さくする必要があります。

コマンド デフォルト

値が設定されていない場合、電源スタックでは、デフォルトプライオリティがランダムに決定されます。

デフォルトの範囲は、スイッチで 1 ～ 9、高プライオリティ ポートで 10 ～ 18、低プライオリティ ポートで 19 ～ 27 です。

非 PoE スイッチでは、（ポート プライオリティの）高い値と低い値は、影響がありません。

コマンド モード

スイッチのスタック電源設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スイッチ スタック電源コンフィギュレーション モードにアクセスするには、**stack-power switch** *switch-number* グローバル コンフィギュレーション コマンドを入力します。

Cisco StackPower の電源プライオリティ値によって、電源が失われ、負荷制限が発生した場合のスイッチとポートのシャットダウンの順序が決定されます。プライオリティ値は 1 ～ 27 です。最も高い数が最初にシャットダウンされます。

各スイッチ、その高プライオリティ ポート、および低プライオリティ ポートでは、異なるプライオリティ値を設定して、電源が失われている間に一度にシャットダウンされる装置数を制限することを推奨します。同じ電源スタックの異なるスイッチに同じプライオリティ値を設定しようとすると、設定は許可されますが、警告メッセージが表示されます。

（注） このコマンドは、IP Base または IP Services フィーチャ セットが実行されているスイッチ スタックでのみ使用できます。

例

次に、電源スタックの switch 1 の電源プライオリティを 7 に、高プライオリティ ポートを 11 に、低プライオリティ ポートを 20 に設定する例を示します。

```
Switch(config)# stack-power switch 1
Switch(config-switch-stackpower)# stack-id power_stack_a
Switch(config-switch-stackpower)# power-priority high 11
Switch(config-switch-stackpower)# power-priority low 20
Switch(config-switch-stackpower)# power-priority switch 7
Switch(config-switch-stackpower)# exit
```

関連トピック

stack-power （165 ページ）
show stack-power （160 ページ）

power inline

Power over Ethernet（PoE）ポートで電源管理モードを設定するには、インターフェイス コンフィギュレーション モードで **power inline** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

power inline {**auto** [**max** *max-wattage*]|**four-pair forced**|**never**|**port priority** {**high** |**low**} |**static** [**max** *max-wattage*]}
no power inline {**auto**|**four-pair forced**|**never**|**port priority** {**high** |**low**}|**static** [**max** *max-wattage*]}

構文の説明

auto	受電装置の検出をイネーブルにします。十分な電力がある場合は、装置の検出後に PoE ポートに電力を自動的に割り当てます。割り当ては、検出された順序で行われます。
max *max-wattage*	（任意）ポートに供給される電力を制限します。指定できる範囲は 4000 ～ 30000 mW です。値を指定しない場合は、最大電力が供給されます。
four-pair forced	（任意）L2 ネゴシエーションなしで 4 ペア PoE をイネーブルにします（Cisco UPOE スイッチのみ）。
never	装置の検出とポートへの電力供給をディセーブルにします。
port	ポートの電源プライオリティを設定します。デフォルトの優先度は [Low] です。
priority {**high** | **low**}	ポートの電源プライオリティを設定します。電源に障害が発生した場合には、低プライオリティとして設定されているポートが最初にオフになり、高プライオリティとして設定されたポートは最後にオフになります。デフォルトの優先度は [Low] です。

static	受電装置の検出をイネーブルにします。スイッチが受電デバイスを検出する前に、ポートへの電力を事前に割り当てます（確保します）。このアクションによって、インターフェイスに接続されたデバイスで十分な電力を受け取ることができます。

コマンド デフォルト

デフォルトの設定は **auto**（イネーブル）です。

最大ワット数は、30,000 mW です。

デフォルトのポート プライオリティは低です。

コマンド デフォルト

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**four-pair forced** キーワードが追加されました。

使用上のガイドライン

このコマンドは、PoE 対応ポートだけでサポートされています。PoE がサポートされていないポートでこのコマンドを入力すると、次のエラー メッセージが表示されます。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# power inline auto
                   ^
% Invalid input detected at '^' marker.
```

スイッチ スタックでは、このコマンドはPoEをサポートしているスタックの全ポートでサポートされます。

Cisco Universal Power Over Ethernet（Cisco UPOE）は、シグナル ペア（導線 1、2、3、6）付きの RJ-45 ケーブルのスペア ペア（導線 4、5、7、8）を使用して、IEEE 802.at PoE 標準を拡張するシスコ独自のテクノロジーで、標準のイーサネット ケーブル配線インフラストラクチャ（クラス D 以上）により最大 60 W の電力を供給する機能を提供します。スペア ペアの電力は、スイッチ ポートとエンドデバイスが Cisco UPOE 対応であることを CDP または LLDP を使用して相互に識別し、エンドデバイスがスペア ペアの電力のイネーブル化を要求したときにイネーブルになります。スペア ペアに給電されると、エンドデバイスは、CDP または LLDP を使用して、スイッチから最大 60 W の電力をネゴシエートできます。**power inline four-pair forced** コマンドは、信号ペアおよびスペア ペアの両方のエンド デバイスが PoE 対応の場合に使用します。ただし、Cisco UPOE に必要な CDP または LLDP 拡張はサポートしていません。

max *max-wattage* オプションを使用して、受電デバイスの電力が制限を超えないようにします。この設定によって、受電デバイスが最大ワット数より多い電力を要求する Cisco Discovery Protocol（CDP）メッセージを送信すると、スイッチはポートへ電力を供給しません。受電装置の IEEE クラスの最大値が最大ワット数を超えると、スイッチは装置に電力を供給しません。電力は、グローバル電力バジェットに送られます。

（注） **power inline max max-wattage** コマンドが 30 W 未満に設定されている場合、スイッチは Class 0 または Class 3 装置に電力を供給しません。

スイッチが受電デバイスへの電力供給を拒否する場合（受電デバイスが CDP メッセージを通じて制限を超えた電力を要求する場合、または IEEE クラスの最大値が最大ワット数を超えている場合）、PoE ポートは power-deny ステートになります。スイッチはシステム メッセージを生成し、**show power inline** 特権 EXEC コマンド出力の Oper カラムに *power-deny* が表示されます。

ポートに高いプライオリティを与えるには、 **power inline static max** *max-wattage* コマンドを使用します。スイッチは、auto モードに設定されたポートに電力を割り当てる前に、static モードに設定されたポートに PoE を割り当てます。スイッチは、装置検出より優先的に設定されている場合に、スタティック ポートの電力を確保します。接続された装置がない場合は、ポートがシャットダウン状態か否かに関係なく、スタティック ポートの電力が確保されます。スイッチは、設定された最大ワット数をポートに割り当てます。その値は、IEEE クラスまたは受電デバイスからの CDP メッセージによって調節されることはありません。電力が事前割り当てされているので、最大ワット数以下の電力を使用する受電デバイスは、スタティック ポートに接続されていれば電力が保証されます。ただし、受電デバイスの IEEE クラスが最大ワット数を超えると、スイッチは装置に電力を供給しません。CDP メッセージを通じて受電デバイスが最大ワット数を超えた量を要求していることをスイッチが認識すると、受電デバイスがシャットダウンします。

ポートが static モードの場合にスイッチが電力を事前割り当てできない場合（たとえば、電力バジェット全体がすでに別の自動ポートまたはスタティック ポートに割り当てられているなど）、次のメッセージが表示されます。Command rejected: power inline static: pwr not available。ポートの設定は、そのまま変更されません。

power inline auto または **power inline static** インターフェイス コンフィギュレーション コマンドを使用してポートを設定すると、ポートは設定された速度とデュプレックス設定を使用して自動ネゴシエーションします。これは、受電デバイスであるかどうかに関係なく、接続された装置の電力要件を判別するのに必要です。電力要件が判別された後、スイッチはインターフェイスをリセットすることなく、設定された速度とデュプレックス設定を使用してインターフェイスをハードコードします。

power inline never コマンドを使用してポートを設定すると、ポートは設定された速度とデュプレックス設定に戻ります。

ポートにシスコ製の受電デバイスが接続されている場合は、**power inline never** コマンドでポートを設定しないでください。不正なリンクアップが生じ、ポートが errdisable ステートになる可能性があります。

power inline port priority {high | low} コマンドを使用して、PoE ポートの電源プライオリティを設定します。電力が不足した場合には、低いポート プライオリティでポートに接続されている受電デバイスが、まず、シャットダウンされます。

設定を確認するには、**show power inline** EXEC コマンドを入力します。

例

次の例では、スイッチ上で受電デバイスの検出をイネーブルにし、PoE ポートに自動的に電力を供給する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline auto
```

次に、スイッチ ポート ギガビット イーサネット 1/0/1 から自動的に信号ペアおよびスペア ペアの両方の電力をイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# power inline four-pair forced
```

次の例では、Class 1 または Class 2 の受電デバイスを受け入れるように、スイッチ上で PoE ポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline auto max 7000
```

次の例では、受電装置の検出をディセーブルにし、スイッチ上で PoE ポートへの電力供給を停止する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline never
```

次の例では、電源に障害が発生した場合に最後のポートの 1 つがシャットダウンされるよう、ポートのプライオリティを高に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline port priority high
```

関連トピック

logging event power-inline-status （86 ページ）
show power inline （154 ページ）

power inline police

受電デバイスでリアルタイム電力消費のポリシングをイネーブルにするには、インターフェイス コンフィギュレーション モードで **power inline police** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

power inline police [**action** {**errdisable**|**log**}]
no power inline police

構文の説明

action errdisable	（任意）リアルタイムの電力消費がポートの最大電力割り当てを超過した場合、ポートへの電力をオフにするよう、スイッチを設定します。これがデフォルトのアクションになります。
action log	（任意）リアルタイムの電力消費がポートの最大電力割り当てを超過した場合、接続されているデバイスへの電力を供給しながら、スイッチが Syslog メッセージを生成するように設定します。

コマンド デフォルト

受電デバイスのリアルタイムの電力消費のポリシングは、ディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、LAN Base イメージのみでサポートされています。

このコマンドは、Power of Ethernet（PoE）対応ポートのみでサポートされています。PoE をサポートしていないスイッチまたはポートでこのコマンドを入力すると、エラー メッセージが表示されます。

スイッチ スタックでは、このコマンドは、PoEおよびリアルタイム電力消費モニタリングをサポートしているスタックの全スイッチまたはポートでサポートされます。

リアルタイムの電力消費のポリシングがイネーブルである場合、受電デバイスが割り当てられた最大電力より多くの量を消費すると、スイッチが対処します。

PoEがイネーブルである場合、スイッチは受電装置のリアルタイムの電力消費を検知します。この機能は、パワー モニタリングまたはパワー センシングといわれます。また、スイッチはパワー ポリシング機能を使用して消費電力をポリシングします。

パワー ポリシングがイネーブルである場合、スイッチは次の順のいずれかの方式で PoE ポートのカットオフ電力として、これらの値の 1 つを使用します。

1. **power inline auto max** *max-wattage* インターフェイス コンフィギュレーション コマンドまたは **power inline static max** *max-wattage* インターフェイス コンフィギュレーション コマンドを入力したときにポート上で許可される電力を制限するユーザ定義の電力レベル。
2. スイッチでは、CDP パワー ネゴシエーションまたは IEEE 分類および LLPD 電力ネゴシエーションを使用して、装置の消費使用量が自動的に設定されます。

カットオフ電力量の値を手動で設定しない場合、スイッチは、CDP電力ネゴシエーションまたはデバイスの IEEE 分類と LLDP 電力ネゴシエーションを使用して自動的に値を決定します。CDP または LLDP がイネーブルでない場合は、デフォルト値の 30 W が適用されます。ただし、CDP または LLDP がない場合は、15400 ～ 30000 mW の値が CDP 要求または LLDP 要求だけに基づいて割り当てられるため、装置で 15.4 W を超える電力の消費がスイッチから許可されません。受電デバイスが CDP または LLDP のネゴシエーションなしに 15.4 W を超える電力を消費する場合、装置は最大電流 *Imax* の制限に違反し、最大値を超える電流が供給されるという *Icut* 障害が発生する可能性があります。再び電源を入れるまで、ポートは障害状態のままになります。ポートで継続的に 15.4 W を超える電力が給電される場合、このサイクルが繰り返されます。

PoE+ ポートに接続されている受電デバイスが再起動し、電力 TLV で CDP パケットまたは LLDP パケットが送信される場合、スイッチは最初のパケットの電力ネゴシエーションプロトコルをロックし、その他のプロトコルからの電力要求に応答しません。たとえば、スイッチが CDP にロックされている場合、LLDP 要求を送信する装置に電力を供給しません。スイッチが CDP にロックされた後で CDP がディセーブルになった場合、スイッチは LLDP 電源要求に応答せず、アクセサリの電源がオンにならなくなります。この場合、受電デバイスを再起動する必要があります。

パワー ポリシングがイネーブルである場合、スイッチはリアルタイムの電力消費を PoE ポートに割り当てられた最大電力と比較して、消費電力をポリシングします。装置が最大電力割り当て（またはカットオフ電力）を超える電力をポートで使用している場合、スイッチでは、ポートへの電力供給がオフにされるか、または装置に電力を供給しながらスイッチは Syslog メッセージが生成して LED（ポート LED はオレンジ色に点滅）を更新します。

- ポートへの電力供給をオフにして、ポートを error-disabled ステートとするようスイッチを設定するには、**power inline police** インターフェイス コンフィギュレーション コマンドを使用します。
- 装置に電力を供給しながら、syslog メッセージを生成するようスイッチを設定するには、**power inline police action log** コマンドを使用します。

action log キーワードを入力しない場合のデフォルトのアクションは、ポートのシャット ダウン、ポートへの電力供給のオフ、およびポートを PoE error-disabled ステートに移行になります。PoE ポートを error-disabled ステートから自動的に回復するよう設定するには、**errdisable detect cause inline-power** グローバル コンフィギュレーション コマンドを使用して、PoE 原因に対する error-disabled 検出をイネーブルにして、**errdisable recovery cause inline-power interval** *interval* グローバル コンフィギュレーション コマンドを使用して、PoE error-disabled 原因の回復タイマーをイネーブルにします。

注意 ポリシングがディセーブルである場合、受電デバイスがポートに割り当てられた最大電力より多くの量を消費しても対処されないため、スイッチに悪影響を与える場合があります。

設定を確認するには、**show power inline police** 特権 EXEC コマンドを入力します。

例

次の例では、電力消費のポリシングをイネーブルにして、スイッチの PoE ポートで Syslog メッセージを生成するようスイッチを設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline police action log
```

関連トピック

power inline （97 ページ）
show power inline （154 ページ）

power supply

スイッチの内部電源を設定および管理するには、特権 EXEC モードで **power supply** コマンドを使用します。

power supply *stack-member-number* **slot** {**A**|**B**} {**off**|**on**}

構文の説明

stack-member-number	内部電源を設定するスタック メンバ番号。指定できる範囲は、スタック内のスイッチの数に応じて 1 ～ 9 です。 このパラメータは、スタック対応スイッチだけで使用できます。
slot	設定するスイッチの電源を選択します。
A	スロット A の電源を選択します。
B	スロット B の電源を選択します。 （注） 電源スロット B は、スイッチの外側エッジに最も近いスロットです。
off	スイッチの電源をオフに設定します。
on	スイッチの電源をオンに設定します。

コマンド デフォルト

スイッチの電源がオンになります。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**slot** キーワードが **frufep** キーワードに代わるものとして使用されるようになりました。

使用上のガイドライン

power supply コマンドは、スイッチまたはすべてのスイッチが同じプラットフォームであるスイッチ スタックに適用されます。

同じプラットフォーム スイッチを含むスイッチ スタックでは、**slot** {**A** | **B**} **off** or **on** キーワードを入力する前に、スタック メンバを指定する必要があります。

デフォルト設定に戻すには、**power supply** *stack-member-number***on** コマンドを使用します。

設定を確認するには、**show env power** 特権 EXEC コマンドを入力します。

例

次に、スロット A の電源装置をオフに設定する例を示します。

```
Switch> power supply 2 slot A off
Disabling Power supply A may result in a power loss to PoE devices and/or switches ...
Continue? (yes/[no]): yes
Switch
Jun 10 04:52:54.389: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered off
Jun 10 04:52:56.717: %PLATFORM_ENV-1-FAN_NOT_PRESENT: Fan is not present
```

次に、スロット A の電源装置をオンに設定する例を示します。

```
Switch> power supply 1 slot B on
Jun 10 04:54:39.600: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered on
```

次に、show env power コマンドの出力例を示します。

```
Switch> show env power
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
1A  PWR-1RUC2-640WAC    DCB1705B05B OK               Good     Good     250/390
1B  Not Present
```

関連トピック

show env （125 ページ）

show CAPWAP summary

アクセス ポイントおよびその他のモビリティ コントローラに対してコントローラが確立するすべての CAPWAP トンネルを表示するには、**show CAPWAP summary** コマンドを使用します。

show CAPWAP summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントなどに対して、コントローラの確立する CAPWAP トンネルを表示する例を示します。

```
Switch# show capwap summary
CAPWAP Tunnels General Statistics:
Number of Capwap Data Tunnels = 8
Number of Capwap Mobility Tunnels = 0
Number of Capwap Multicast Tunnels = 0
Name APName Type PhyPortIf Mode McastIf
------ -------------------------------- ---- --------- ---------
-------
Ca4 AP-Behind-Router data - unicast -
Ca0 AP1142-kat data - unicast -
Ca5 APRFCHAMBER2-EDISON data - unicast -
Ca6 KATANA_2_RF data - unicast -
Ca1 AP-1040-RF data - unicast -
Ca7 KATANA_1_RF data - unicast -
Ca2 AP3500-2027 data - unicast -
Ca3 AP-1040-out data - unicast -
```

show controllers cpu-interface

CPU ネットワーク インターフェイス ASIC の状態、および CPU に届くパケットの送受信の統計情報を表示するには、特権 EXEC モードで **show controllers cpu-interface** コマンドを使用します。

show controllers cpu-interface [{**switch** *stack-member-number*}]

構文の説明

switch *stack-member-number*	（任意）スタック メンバ番号を指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用することで、シスコのテクニカルサポート担当がスイッチのトラブルシューティングを行うのに役立つ情報が表示されます。

例

次に、**show controllers cpu-interface** コマンドの一部の出力例を示します。

```
Switch# show controllers cpu-interface switch 1
cpu-queue-frames  retrieved dropped invalid hol-block

----------------  --------- ------- ------- ---------

Routing Protocol          0         0     0     0
L2 Protocol          241567         0     0     0
sw forwarding             0         0     0     0
broadcast             68355         0     0     0
icmp                      0         0     0     0
icmp redirect             0         0     0     0
logging                   0         0     0     0
rpf-fail                  0         0     0     0
DOT1X authentication 328174         0     0     0
Forus Traffic             0         0     0     0
Forus Resolution          0         0     0     0
Wireless q5               0         0     0     0
Wireless q1               0         0     0     0
Wireless q2               0         0     0     0
Wireless q3               0         0     0     0
Wireless q4               0         0     0     0
Learning cache            0         0     0     0
Topology control     820408         0     0     0
Proto snooping            0         0     0     0
BFD Low latency           0         0     0     0
Transit Traffic           0         0     0     0
Multi End station         0         0     0     0
```

```
Health Check              0          0      0      0
Crypto control            0          0      0      0
Exception                 0          0      0      0
General Punt              0          0      0      0
NFL sampled data          0          0      0      0
STG cache                 0          0      0      0
EGR exception             0          0      0      0
show forward              0          0      0      0
Multicast data            0          0      0      0
Gold packet               0          0      0      0
```

関連トピック

show controllers ethernet-controller （109 ページ）
show interfaces （132 ページ）

show controllers ethernet-controller

キーワードでハードウェアから読み込んだインターフェイス単位の送受信の統計情報を表示するには、EXEC モードで **show controllers ethernet-controller** コマンドを使用します。

show controllers ethernet-controller [*interface-id*] [{**down-when-looped**|**phy** [**detail**]}] [**port-asic statistics** {**exceptions**|**interface** *interface-id* {**l2**|**l3**}|**l3-ifid** *if-id*|**port-ifid** *if-id*|**vlan-ifid** *if-id*} [**switch** *stack-member-number*] [**asic** *asic-number*]]

構文の説明

interface-id	（任意）物理インターフェイスの ID です。
down-when-looped	（任意）down-when-looped 検出に関連するステートを表示します。
phy	（任意）デバイス、またはインターフェイスのスイッチの物理層デバイス（PHY）の内部レジスタ ステータスを表示します。インターフェイスの Automatic Medium-Dependent Interface Crossover（Auto-MDIX）機能の動作ステートを表示に含めます。
detail	（任意）PHY 内部レジスタの詳細情報を表示します。
port-asic	（任意）ポートの ASIC 内部レジスタの情報を表示します。
statistics	ポートの ASIC 統計情報（Rx/Sup キューおよびその他の統計情報を含む）を表示します。
exceptions	ポートの ASIC 例外統計情報を表示します。
interface *interface-id*	ポートの ASIC 統計情報を表示するインターフェイスを指定します。
l2	レイヤ 2 インターフェイスの統計情報を表示します。
l3	レイヤ 3 インターフェイスの統計情報を表示します。
l3-ifid *if-id*	ポートの ASIC 統計情報を表示するレイヤ 3 IF インターフェイス ID を指定します。
port-ifid *if-id*	ポートの ASIC 統計情報を表示する PortIF インターフェイス ID を指定します。
vlan-ifid *if-id*	ポートの ASIC 統計情報を表示する VLANIF インターフェイス ID を指定します。
switch *stack-member-number*	（任意）送受信の統計情報を表示するスタック メンバ番号を指定します。
asic *asic-number*	（任意）ASIC 番号を指定します。

コマンド モード

ユーザ EXEC（ユーザ EXEC モードの *interface-id* キーワードを指定した場合だけサポート）

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

キーワードがない場合、このコマンドはすべてのインターフェイスまたは指定されたインターフェイスの RMON 統計情報を示します。

インターフェイスの内部レジスタを表示するには、**phy** キーワードを使用します。ポートの ASIC に関する情報を表示するには、**port-asic** キーワードを使用します。

phy または **port-asic** キーワードを入力すると、主にシスコ テクニカル サポート担当者によるスイッチのトラブルシューティングに役立つ情報が表示されます。

例

次に、あるインターフェイスに対する **show controllers ethernet-controller** コマンドの出力例を示します。

```
Switch# show controllers ethernet-controller gigabitethernet1/0/1
Transmit                  GigabitEthernet1/0/1          Receive
   19216827 Total bytes                                0 Total bytes
      41935 Unicast frames                             0 Unicast frames
    2683840 Unicast bytes                              0 Unicast bytes
     216662 Multicast frames                           0 Multicast frames
   16532987 Multicast bytes                            0 Multicast bytes
          0 Broadcast frames                           0 Broadcast frames
          0 Broadcast bytes                            0 Broadcast bytes
          0 System FCS error frames                    0 IpgViolation frames
          0 MacUnderrun frames                         0 MacOverrun frames
          0 Pause frames                               0 Pause frames
          0 Cos 0 Pause frames                         0 Cos 0 Pause frames
          0 Cos 1 Pause frames                         0 Cos 1 Pause frames
          0 Cos 2 Pause frames                         0 Cos 2 Pause frames
          0 Cos 3 Pause frames                         0 Cos 3 Pause frames
          0 Cos 4 Pause frames                         0 Cos 4 Pause frames
          0 Cos 5 Pause frames                         0 Cos 5 Pause frames
          0 Cos 6 Pause frames                         0 Cos 6 Pause frames
          0 Cos 7 Pause frames                         0 Cos 7 Pause frames
          0 Oam frames                                 0 OamProcessed frames
          0 Oam frames                                 0 OamDropped frames
     251598 Minimum size frames                        0 Minimum size frames
          0 65 to 127 byte frames                      0 65 to 127 byte frames
          0 128 to 255 byte frames                     0 128 to 255 byte frames
       6999 256 to 511 byte frames                     0 256 to 511 byte frames
          0 512 to 1023 byte frames                    0 512 to 1023 byte frames
          0 1024 to 1518 byte frames                   0 1024 to 1518 byte frames
          0 1519 to 2047 byte frames                   0 1519 to 2047 byte frames
          0 2048 to 4095 byte frames                   0 2048 to 4095 byte frames
          0 4096 to 8191 byte frames                   0 4096 to 8191 byte frames
          0 8192 to 16383 byte frames                  0 8192 to 16383 byte frames
          0 16384 to 32767 byte frame                  0 16384 to 32767 byte frame
          0 > 32768 byte frames                        0 > 32768 byte frames
          0 Late collision frames                      0 SymbolErr frames
          0 Excess Defer frames                        0 Collision fragments
          0 Good (1 coll) frames                       0 ValidUnderSize frames
```

```
          0 Good (>1 coll) frames                 0 InvalidOverSize frames
          0 Deferred frames                       0 ValidOverSize frames
          0 Gold frames dropped                   0 FcsErr frames
          0 Gold frames truncated
          0 Gold frames successful
          0 1 collision frames
          0 2 collision frames
          0 3 collision frames
          0 4 collision frames
          0 5 collision frames
          0 6 collision frames
          0 7 collision frames
          0 8 collision frames
          0 9 collision frames
          0 10 collision frames
          0 11 collision frames
          0 12 collision frames
          0 13 collision frames
          0 14 collision frames
          0 15 collision frames
          0 Excess collision frames

LAST UPDATE 850 msecs AGO
```

表 *6 : Transmit* のフィールドの説明

フィールド	説明
Total bytes	インターフェイス上で送信されたバイトの総数。
Unicast Frames	ユニキャスト アドレスに送信されたフレームの総数。
Unicast bytes	ユニキャスト アドレスに送信されたバイトの総数。
Multicast frames	マルチキャスト アドレスに送信されたフレームの総数。
Multicast bytes	マルチキャスト アドレスに送信されたバイトの総数。
Broadcast frames	ブロードキャスト アドレスに送信されたフレームの総数。
Broadcast bytes	ブロードキャスト アドレスに送信されたバイトの総数。
System FCS error frames	フレーム チェック シーケンス（FCS）に失敗したフレームの総数。
MacUnderrun frames	MAC アンダーラン エラーを持つフレームの総数。
Pause frames	インターフェイス上で送信されたポーズ フレームの総数。
Cos x Pause frames	インターフェイス上で送信されたサービス クラス（CoS）X ポーズ フレームの総数。
Oam frames	インターフェイス上で送信されたイーサネット OAM（オペレーション、アドミニストレーション、およびメンテナンス）フレームの総数。

フィールド	説明
Minimum size frames	最小許可フレーム サイズのフレームの数。
65 to 127 byte frames	インターフェイス上で送信された 65 ～ 127 バイトのフレームの総数。
128 to 255 byte frames	インターフェイス上で送信された 128 ～ 255 バイトのフレームの総数。
256 to 511 byte frames	インターフェイス上で送信された 256 ～ 511 バイトのフレームの総数。
512 to 1023 byte frames	インターフェイス上で送信された 512 ～ 1023 バイトのフレームの総数。
1024 to 1518 byte frames	インターフェイス上で送信された 1024 ～ 1518 バイトのフレームの総数。
1519 to 2047 byte frames	インターフェイス上で送信された 1519 ～ 2047 バイトのフレームの総数。
2048 to 4095 byte frames	インターフェイス上で送信された 2048 ～ 4095 バイトのフレームの総数。
4096 to 8191 byte frames	インターフェイス上で送信された 4096 ～ 8191 バイトのフレームの総数。
8192 to 16383 byte frames	インターフェイス上で送信された 8192 ～ 16383 バイトのフレームの総数。
16384 to 32767 byte frames	インターフェイス上で送信された 16384 ～ 32767 バイトのフレームの総数。
> 32768 byte frames	インターフェイス上で送信された 32768 バイトより大きいフレームの総数。
Late collision frames	フレームが送信された後で、フレームの送信時に検出されたレイト コリジョンのためにドロップされたフレームの数。
Excess defer frames	時間が最大パケット時間を超えた後で送信されなかったフレームの数。
Good (1 coll) frames	1 回の衝突後、インターフェイス上で正常に送信されたフレームの数。この値には 1 回の衝突後、インターフェイス上で正常に送信されなかったフレームの数は含まれません。
Good (>1 coll) frames	2 回以上の衝突後、インターフェイス上で正常に送信されたフレームの数。この値には 2 回以上の衝突後、正常に送信されなかったフレームの数は含まれません。

フィールド	説明
Deferred frames	時間が2*最大パケット時間を超えた後で送信されなかったフレームの数。
Gold frames dropped	ドロップされたゴールド フレームの数。
Gold frames truncated	切り捨てられたゴールド フレームの数。
Gold frames successful	成功したゴールド フレームの数。
1 collision frames	1 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
2 collision frames	2 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
3 collision frames	3 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
4 collision frames	4 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
5 collision frames	5 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
6 collision frames	6 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
7 collision frames	7 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
8 collision frames	8 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
9 collision frames	9 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
10 collision frames	10回の衝突後、インターフェイス上で正常に送信されたフレームの数。
11 collision frames	11回の衝突後、インターフェイス上で正常に送信されたフレームの数。
12 collision frames	12回の衝突後、インターフェイス上で正常に送信されたフレームの数。
13 collision frames	13回の衝突後、インターフェイス上で正常に送信されたフレームの数。

フィールド	説明
14 collision frames	14回の衝突後、インターフェイス上で正常に送信されたフレームの数。
15 collision frames	15回の衝突後、インターフェイス上で正常に送信されたフレームの数。
Excess collisions	16回の衝突後、インターフェイス上で送信できなかったフレームの数。

表 *7 : Transmit* のフィールドの説明

フィールド	説明
Bytes	インターフェイス上で送信されたバイトの総数。
Unicast Frames	ユニキャスト アドレスに送信されたフレームの総数。
Multicast frames	マルチキャスト アドレスに送信されたフレームの総数。
Broadcast frames	ブロードキャスト アドレスに送信されたフレームの総数。
Too old frames	パケットが有効期限切れのため出力ポートでドロップされたフレームの数。
Deferred frames	時間が 2* 最大パケット時間を超えた後で送信されなかったフレームの数。
MTU exceeded frames	最大許可フレーム サイズを超えたフレームの数。
1 collision frames	1 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
2 collision frames	2 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
3 collision frames	3 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
4 collision frames	4 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
5 collision frames	5 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
6 collision frames	6 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
7 collision frames	7 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
8 collision frames	8 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
9 collision frames	9 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
10 collision frames	10回の衝突後、インターフェイス上で正常に送信されたフレームの数。

フィールド	説明
11 collision frames	11 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
12 collision frames	12 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
13 collision frames	13 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
14 collision frames	14 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
15 collision frames	15 回の衝突後、インターフェイス上で正常に送信されたフレームの数。
Excessive collisions	16 回の衝突後、インターフェイス上で送信できなかったフレームの数。
Late collisions	フレームが送信された後で、フレームの送信時に検出されたレイトコリジョンのためにドロップされたフレームの数。
VLAN discard frames	CFI ビットが設定されたことによりインターフェイス上でドロップされたフレームの数。[1]。
Excess defer frames	時間が最大パケット時間を超えた後で送信されなかったフレームの数。
64 byte frames	インターフェイス上で送信された 64 バイトのフレームの総数。
127 byte frames	インターフェイス上で送信された 65 ～ 127 バイトのフレームの総数。
255 byte frames	インターフェイス上で送信された 128 ～ 255 バイトのフレームの総数。
511 byte frames	インターフェイス上で送信された 256 ～ 511 バイトのフレームの総数。
1023 byte frames	インターフェイス上で送信された 512 ～ 1023 バイトのフレームの総数。
1518 byte frames	インターフェイス上で送信された 1024 ～ 1518 バイトのフレームの総数。
Too large frames	インターフェイス上で送信された最大許可フレーム サイズを超えたフレームの数。
Good (1 coll) frames	1 回の衝突後、インターフェイス上で正常に送信されたフレームの数。この値には 1 回の衝突後、インターフェイス上で正常に送信されなかったフレームの数は含まれません。

[1] CFI = Canonical Format Indicator

表 *8 : Receive* のフィールドの説明

フィールド	説明
Total Bytes	インターフェイス上で受信されたフレームによって使用されたメモリ（バイト）の総量。FCS 値および正常形式でないフレームも含まれます。[2]。この値には、フレーム ヘッダー ビットが含まれません。
Unicast frames	インターフェイス上で正常に受信されたユニキャスト アドレスに向けられたフレームの総数。
Unicast bytes	インターフェイス上で受信されたユニキャストフレームによって使用されたメモリ（バイト）の総量。FCS 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。
Multicast frames	インターフェイス上で受信されたマルチキャスト フレームによって使用されたメモリ（バイト）の総量。FCS 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。
Multicast bytes	インターフェイス上で正常に受信されたマルチキャスト アドレスに向けられたバイトの総数。
Broadcast frames	インターフェイス上で正常に受信されたブロードキャスト アドレスに向けられたフレームの総数。
Broadcast bytes	インターフェイス上で受信されたブロードキャスト フレームによって使用されたメモリ（バイト）の総量。FCS 値および正常形式でないフレームも含まれます。この値には、フレーム ヘッダー ビットが含まれません。
IpgViolation frames	パケット間ギャップ（IPG）違反のフレームの総数。
MacOverrun frames	MacOverrun エラーのフレームの総数。
Pause frames	インターフェイス上で受信されたポーズ フレームの総数。
Cos x Pause frames	インターフェイス上で受信されたサービス クラス（CoS）X ポーズ フレームの総数。
OamProcessed	インターフェイス上で処理されたイーサネット OAM（オペレーション、アドミニストレーション、およびメンテナンス）フレームの総数。
OamDropped	インターフェイス上でドロップされたイーサネット OAM（オペレーション、アドミニストレーション、およびメンテナンス）フレームの総数。

フィールド	説明
Minimum size frames	最小フレーム サイズのフレームの総数。
65 to 127 byte frames	65 ～ 127 バイトのフレームの総数。
128 to 255 byte frames	128 ～ 255 バイトのフレームの総数。
256 to 511 byte frames	256 ～ 511 バイトのフレームの総数。
512 to 1023 byte frames	512 ～ 1023 バイトのフレームの総数。
1024 to 1518 byte frames	1024 ～ 1518 バイトのフレームの総数。
1519 to 2047 byte frames	1519 ～ 2047 バイトのフレームの総数。
2048 to 4095 byte frames	2048 ～ 4095 バイトのフレームの総数。
4096 to 8191 byte frames	4096 ～ 8191 バイトのフレームの総数。
8192 to 16383 byte frames	8192 ～ 16383 バイトのフレームの総数。
16384 to 32767 byte frames	16384 ～ 32767 バイトのフレームの総数。
> 32768 byte frames	32768 バイトより大きいフレームの総数。
Symbol error frames	インターフェイス上で受信されたシンボルエラーを持つフレームの数。
Collision fragments	インターフェイス上で受信されたコリジョン フラグメントの数。
Valid undersize frames	64 バイト（または VLAN タグ付きフレームでは 68 バイト）未満で、有効な FCS 値を持つインターフェイスで受信されたフレームの数。フレーム サイズには、FCS ビットが含まれ、フレーム ヘッダー ビットは含まれません。
Invalid oversize frames	許可される最大伝送単位（MTU）サイズ（FCS ビットを含み、フレーム ヘッダーを含まない）を超え、FCS エラーまたはアライメントエラーのいずれかを持つ、受信済みフレームの数。
Valid oversize frames	インターフェイス上で受信された最大許可フレーム サイズを超え、有効な FCS 値を持つフレームの数。フレーム サイズには、FCS 値が含まれ、VLAN タグは含まれません。
FcsErr frames	インターフェイス上で受信された有効な長さ（バイト）を持ち、正常な FCS 値を持たないフレームの総数。

[2] FCS = フレーム チェック シーケンス

次に、特定のインターフェイスに対する **show controllers ethernet-controller phy** コマンドの出力例を示します。

```
Switch# show controllers ethernet-controller gigabitethernet1/0/2 phy
Gi1/0/2 (gpn: 2, port-number: 2)
----------------------------------------------------------
 0000 : 1140  Control Register                  :  0001 0001 0100 0000
 0001 : 7949  Control STATUS                    :  0111 1001 0100 1001
 0002 : 0141  Phy ID 1                          :  0000 0001 0100 0001
 0003 : 0EE0  Phy ID 2                          :  0000 1110 1110 0000
 0004 : 03E1  Auto-Negotiation Advertisement    :  0000 0011 1110 0001
 0005 : 0000  Auto-Negotiation Link Partner     :  0000 0000 0000 0000
 0006 : 0004  Auto-Negotiation Expansion Reg    :  0000 0000 0000 0100
 0007 : 2001  Next Page Transmit Register       :  0010 0000 0000 0001
 0008 : 0000  Link Partner Next page Registe    :  0000 0000 0000 0000
 0010 : 3B60  PHY Specific Control              :  0011 1011 0110 0000
 0011 : 8010  PHY Specific Status               :  1000 0000 0001 0000
 0012 : 6404  PHY Specific Interrupt Enable     :  0110 0100 0000 0100
 0013 : 0000  PHY Specific Interrupt Status     :  0000 0000 0000 0000
```

関連トピック

show controllers cpu-interface （107 ページ）

show controllers utilization

帯域幅利用率を表示するには、EXEC モードで **show controllers utilization** コマンドを使用します。

show controllers [*interface-id*] **utilization**

構文の説明

interface-id	（任意）物理インターフェイスの ID です。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show controllers utilization** コマンドの出力例を示します。

```
Switch> show controllers utilization
Port       Receive Utilization  Transmit Utilization
Gi1/0/1            0                    0
Gi1/0/2            0                    0
Gi1/0/3            0                    0
Gi1/0/4            0                    0
Gi1/0/5            0                    0
Gi1/0/6            0                    0
Gi1/0/7            0                    0
<output truncated>
Gi2/0/1            0                    0
Gi2/0/2            0                    0
<output truncated>
Total Ports : 48
Switch Receive Bandwidth Percentage Utilization  : 0
Switch Transmit Bandwidth Percentage Utilization : 0

Average Switch Percentage Utilization : 0
```

次に、特定のポートでの **show controllers utilization** コマンドの出力例を示します。

```
Switch> show controllers gigabitethernet1/0/1 utilization
Receive Bandwidth Percentage Utilization   : 0
Transmit Bandwidth Percentage Utilization  : 0
```

表 *9 : show controllers utilization* のフィールドの説明

フィールド	説明
Receive Bandwidth Percentage Utilization	スイッチの受信帯域利用率を表示します。これは、すべてのポートの受信トラフィックの合計をスイッチの受信容量で割ったものです。
Transmit Bandwidth Percentage Utilization	スイッチの送信帯域利用率を表示します。これは、すべてのポートの送信トラフィックの合計をスイッチの送信容量で割ったものです。
Average Switch Percentage Utilization	スイッチの送信と受信の両方の帯域利用率の平均を表示します。

show eee

インターフェイスの EEE 情報を表示するには、EXEC モードで **show eee** コマンドを使用します。

show eee{**capabilities**| **status**}**interface***interface-id*

構文の説明

capabilities	指定インターフェイスの EEE 機能を表示します。
status	指定したインターフェイスの EEE ステータス情報を表示します。
interface *interface-id*	EEE 機能またはステータス情報を表示するためのインターフェイスを指定します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

低電力アイドル（LPI）モードをサポートするデバイスで EEE をイネーブルにできます。このようなデバイスは、低い電力使用率のときに LPI モードを開始して、電力を節約できます。LPI モードでは、リンクの両端にあるシステムは、特定のサービスをシャットダウンして、電力を節約できます。EEE は上位層プロトコルおよびアプリケーションに対して透過的であるように、LPI モードに移行したり、LPI モードから移行する必要があるプロトコルを提供します。

インターフェイスが EEE に対応しているかどうかを確認するには、**show eee capabilities** コマンドを使用します。**power efficient-ethernet auto** インターフェイス コンフィギュレーション コマンドを使用して、EEE に対応しているインターフェイスで EEE をイネーブルにできます。

インターフェイスの EEE ステータス、LPI ステータス、および wake エラー カウント情報を表示するには、**show eee status** コマンドを使用します。

次の例では、EEE がイネーブルのインターフェイスの **show eee capabilities**コマンドの出力を示します。

```
Switch# show eee capabilities interface gigabitethernet1/0/1
Gi1/0/1
        EEE(efficient-ethernet):  yes (100-Tx and 1000T auto)
```

```
        Link Partner          :  yes (100-Tx and 1000T auto)
```

次の例では、EEE がイネーブルでないインターフェイスの **show eee capabilities** コマンドの出力を示します。

```
Switch# show eee capabilities interface gigabitethernet2/0/1
Gi2/0/1
        EEE(efficient-ethernet):  not enabled
        Link Partner          :  not enabled
```

次の例では、EEE がイネーブルで機能しているインターフェイスの **show eee status** コマンドの出力を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
Switch# show eee status interface gigabitethernet1/0/4
Gi1/0/4 is up
        EEE(efficient-ethernet):  Operational
        Rx LPI Status         :  Received
        Tx LPI Status         :  Received
```

次の例では、EEE が機能していて、ポートが節電モードであるインターフェイスの **show eee status** コマンドの出力を示します。

```
Switch# show eee status interface gigabitethernet1/0/3
Gi1/0/3 is up
        EEE(efficient-ethernet):  Operational
        Rx LPI Status         :  Low Power
        Tx LPI Status         :  Low Power
        Wake Error Count      :  0
```

次の例では、リモート リンク パートナーが EEE と互換性がないために、EEE がイネーブルでないインターフェイスの **show eee status** コマンドの出力を示します。

```
Switch# show eee status interface gigabitethernet1/0/3
Gi1/0/3 is down
        EEE(efficient-ethernet):  Disagreed
        Rx LPI Status         :  None
        Tx LPI Status         :  None
        Wake Error Count      :  0
```

表 *10 : show eee status* のフィールドの説明

フィールド	説明
EEE (efficient-ethernet)	インターフェイスの EEE ステータス。このフィールドには、次のいずれかの値を使用できます。 • N/A：ポートは EEE に対応できません。 • Disabled：ポートの EEE はディセーブルです。 • Disagreed：リモート リンク パートナーが EEE に互換性がない可能性があるため、ポートの EEE は設定されていません。EEE 対応でないか、EEE の設定に互換性がありません。 • Operational：ポートの EEE がイネーブルで機能しています。 インターフェイスの速度が 10 Mbps として設定されていると、EEE は内部的にディセーブルになります。インターフェイスの速度が auto、100 Mbps または 1000 Mbps に戻ると、EEE は再びアクティブになります。

フィールド	説明
Rx/Tx LPI Status	リンク パートナーの低電力アイドル（LPI）ステータス。このフィールドには、次のいずれかの値を使用できます。 • N/A：ポートは EEE に対応できません。 • Interrupted：リンク パートナーは低電力モードへの移行中です。 • Low Power：リンク パートナーは低電力モードにあります。 • None：EEE がディセーブルであるか、リンク パートナー側で対応できません。 • Received：リンク パートナーは低電力モードにあり、トラフィック アクティビティがあります。 インターフェイスが半二重として設定されており、LPI ステータスが「None」の場合、インターフェイスが全二重として設定されるまで、インターフェイスは低電力モードにすることはできないことを意味します。
Wake Error Count	発生した PHY wake-up エラーの数EEE がイネーブルで、リンク パートナーへの接続が切断された場合に、wake-up エラーが発生します。 この情報は、PHY のデバッグに役立ちます。

show env

ファン、温度、、および電源情報を表示するには、EXEC モードで **show env** コマンドを使用します。

show env {**all**|**fan**|**power** [{**all**|**switch** [*stack-member-number*]}]|**stack** [*stack-member-number*] |**temperature** [**status**]}

構文の説明

all	ファンと温度環境の状態、および、内部電源を表示します。
fan	スイッチのファンの状態を表示します。
power	アクティブ スイッチの内部電源の状態を表示します。
all	（任意）スイッチでコマンドが入力された場合、スタンドアロン スイッチのすべての内部電源の状態が表示されます。アクティブ スイッチでコマンドが入力された場合は、すべてのスタック メンバのすべての内部電源の状態が表示されます。
switch	（任意）スタック内の各スイッチまたは指定したスイッチの内部電源装置のステータスを表示します。 このキーワードは、スタック構成対応スイッチでだけ使用できます。
stack-member-number	（任意）内部電源または環境ステータスの状態を表示するスタック メンバの数。 指定できる範囲は 1 ～ 9 です。
stack	スタックの各スイッチまたは指定されたスイッチのすべての環境ステータスを表示します。 このキーワードは、スタック構成対応スイッチでだけ使用できます。
temperature	スイッチの温度ステータスを表示します。
status	（任意）スイッチの内部温度（外部温度ではなく）およびしきい値を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

アクセスされているスイッチ（スタンドアロン スイッチまたはアクティブ スイッチ）の情報を表示するには、**show env** EXEC コマンドを使用します。**stack** および **switch** キーワードとともにこのコマンドを使用すると、スタックまたは指定されたスタック メンバのすべての情報が表示されます。

show env temperature status コマンドを入力すると、コマンド出力にスイッチの温度状態としきい値レベルが表示されます。

show env temperature コマンドを使用して、スイッチの温度状態を表示することもできます。コマンド出力では、GREEN および YELLOW ステートを *OK* と表示し、RED ステートを *FAULTY* と表示します。**show env all** コマンドを入力した場合のコマンド出力は、**show env temperature status** コマンド出力と同じです。

例

次に、**show env all** コマンドの出力例を示します。

```
Switch>show env all
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
Switch 1: SYSTEM TEMPERATURE is OK
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
1A  Not Present
1B  PWR-C1-715WAC       LIT150119Z1  OK              Good     Good     715
```

次に、**show env fan** コマンドの出力例を示します。

```
Switch>show env fan
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
```

次に、**show env power** コマンドの出力例を示します。

```
Switch>show env power
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
1A  Not Present
1B  PWR-C1-715WAC       LIT150119Z1  OK              Good     Good     715
```

次に、アクティブ スイッチ上での **show env power all** コマンドの出力例を示します。

```
Switch# show env power all
```

```
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
1A  Not Present
1B  PWR-C1-715WAC       LIT150119Z1  OK              Good     Good     715
```

次に、アクティブ スイッチ上での**show env stack** コマンドの出力例を示します。

```
Switch> show env stack
SWITCH: 1
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
Switch 1: SYSTEM TEMPERATURE is OK
Temperature Value: 28 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold    : 56 Degree Celsius
```

次の例では、スタンドアロン スイッチで温度値、ステート、およびしきい値を表示する方法を示します。表に、コマンド出力での温度ステートの説明を示します。

```
Switch> show env temperature status
Temperature Value: 33 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 65 Degree Celsius
Red Threshold    : 75 Degree Celsius
```

表 *11 : show env temperature status* コマンド出力のステート

状態	説明
グリーン	スイッチの温度が正常な動作範囲にあります。
黄色	温度が警告範囲にあります。スイッチの外の周辺温度を確認する必要があります。
赤	温度がクリティカル範囲にあります。温度がこの範囲にある場合、スイッチが正常に実行されない可能性があります。

show errdisable detect

error-disabled 検出ステータスを表示するには、EXEC モードで **show errdisable detect** コマンドを使用します。

show errdisable detect

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

gbic-invalid エラーの理由は、無効な Small Form-Factor Pluggable（SFP）モジュールを意味します。

コマンド出力内の errdisable の理由がアルファベット順に表示されます。Mode 列は、errdisable が機能ごとにどのように設定されているかを示します。

errdisable 検出は次のモードで設定できます。

- ポート モード：違反が発生した場合、物理ポート全体が errdisable になります。
- VLAN モード：違反が発生した場合、VLAN が errdisable になります。
- ポート/VLAN モード：一部のポートでは物理ポート全体が errdisable になり、その他のポートでは VLAN ごとに errdisable になります。

次の例では、**show errdisable detect** コマンドの出力を示します。

```
Switch> show errdisable detect
ErrDisable Reason    Detection    Mode
-----------------    ---------    ----
arp-inspection       Enabled      port
bpduguard            Enabled      vlan
channel-misconfig    Enabled      port
community-limit      Enabled      port
dhcp-rate-limit      Enabled      port
dtp-flap             Enabled      port
gbic-invalid         Enabled      port
inline-power         Enabled      port
invalid-policy       Enabled      port
l2ptguard            Enabled      port
link-flap            Enabled      port
```

```
loopback             Enabled      port
lsgroup              Enabled      port
pagp-flap            Enabled      port
psecure-violation    Enabled      port/vlan
security-violatio    Enabled      port
sfp-config-mismat    Enabled      port
storm-control        Enabled      port
udld                 Enabled      port
vmps                 Enabled      port
```

関連トピック

errdisable detect cause （70 ページ）
show errdisable recovery （130 ページ）

show errdisable recovery

error-disabled 回復タイマー情報を表示するには、EXEC モードで **show errdisable recovery** コマンドを使用します。

show errdisable recovery

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

gbic-invalid error-disable の理由は、無効な Small Form-Factor Pluggable（SFP）インターフェイスを意味します。

（注） unicast-flood フィールドは、出力に表示はされますが無効です。

次の例では、**show errdisable recovery** コマンドの出力を示します。

```
Switch> show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Enabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Disabled
loopback             Disabled
Timer interval:300 seconds
Interfaces that will be enabled at the next timeout:
Interface    Errdisable reason    Time left(sec)
```

```
---------    ------------------    --------------
Gi1/0/2        link-flap             279
```

関連トピック

errdisable recovery cause （73 ページ）
errdisable recovery interval （76 ページ）
show errdisable detect （128 ページ）

show interfaces

すべてのインターフェイスまたは指定したインターフェイスの管理ステータスおよび動作ステータスを表示するには、特権 EXEC モードで **show interfaces** コマンドを使用します。

show interfaces [{*interface-id*|**vlan** *vlan-id*}] [{**accounting**|**capabilities** [**module** *number*]|**debounce**|**description**|**etherchannel**|**flowcontrol**|**pruning**|**stats**|**status** [{**err-disabled**|**inactive**}]|**trunk**}]

構文の説明

interface-id	（任意）インターフェイスの ID です。有効なインターフェイスには、物理ポート（タイプ、スタック構成可能なスイッチのスタック メンバ、モジュール、およびポート番号を含む）やポート チャネルが含まれます。指定できるポート チャネルは 1 ～ 48 です。
vlan *vlan-id*	（任意）VLAN ID です。指定できる範囲は 1 ～ 4094 です。
accounting	（任意）インターフェイスのアカウント情報（アクティブ プロトコル、入出力のパケット、オクテットを含む）を表示します。 （注） ソフトウェアで処理されたパケットだけが表示されます。ハードウェアでスイッチングされるパケットは表示されません。
capabilities	（任意）すべてのインターフェイスまたは指定されたインターフェイスの性能（機能、インターフェイス上で設定可能なオプションを含む）を表示します。このオプションはコマンドラインのヘルプに表示されますが、VLAN ID に使用できません。
module *number*	（任意）スイッチまたは指定されたスタック メンバーのすべてのインターフェイスの機能を表示します。 指定できる範囲は 1 ～ 9 です。 このオプションは、特定のインターフェイス ID を入力したときは利用できません。
debounce	（任意）インターフェイスのポートデバウンス タイマー情報を表示します。
description	（任意）特定のインターフェイスに設定された管理ステータスおよび説明を表示します。

etherchannel	（任意）インターフェイス EtherChannel 情報を表示します。
flowcontrol	（任意）インターフェイスのフロー制御情報を表示します。
mtu	（任意）各インターフェイスまたは指定されたインターフェイスに対応する MTU を表示します。
pruning	（任意）インターフェイスのトランク VTP プルーニング情報を表示します。
stats	（任意）インターフェイスのパスを切り替えることによる入出力パケットを表示します。
status	（任意）インターフェイスのステータスを表示します。Type フィールドの unsupported のステータスは、他社製の Small Form-Factor Pluggable（SFP）モジュールがモジュール スロットに装着されていることを示しています。
err-disabled	（任意）errdisable ステートのインターフェイスを表示します。
inactive	（任意）非アクティブ ステートのインターフェイスを表示します。
trunk	（任意）インターフェイス トランク情報を表示します。インターフェイスを指定しない場合は、アクティブなトランキング ポートの情報だけが表示されます。

（注） **crb**、**fair-queue**、**irb**、**mac-accounting**、**precedence**、**random-detect**、および **rate-limit** キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

show interfaces capabilities コマンドに異なるキーワードを指定することで、次のような結果になります。

- **show interface capabilities module** *number* コマンドを使用して、スタックのスイッチ上のすべてのインターフェイスの機能を表示します。スタック内に該当するモジュール番号を持つスイッチがない場合、出力はありません。
- 指定されたインターフェイスの機能を表示するには、**show interfaces** *interface-id* **capabilities** を使用します。
- スタック内のすべてのインターフェイスの機能を表示するには、**show interfaces capabilities** を使用します（モジュール番号またはインターフェイス ID の指定なし）。

次の例では、スタック メンバ 3 のインターフェイスに対する **show interfaces** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet3/0/2
GigabitEthernet3/0/2 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is 2037.064d.4381 (bia 2037.064d.4381)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

次の例では、**show interfaces accounting** コマンドの出力を示します。

次の例では、インターフェイスに対する **show interfaces capabilities** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet1/0/2 capabilities
GigabitEthernet1/0/2
  Model:                 UA-3850-24-CR
  Type:                  10/100/1000BaseTX
  Speed:                 10,100,1000,auto
  Duplex:                full,half,auto
  Trunk encap. type:     802.1Q
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  Fast Start:            yes
  QoS scheduling:        rx-(not configurable on per port basis),
```

```
                        tx-(4q3t) (3t: Two configurable values and one fixed.)
  CoS rewrite:          yes
  ToS rewrite:          yes
  UDLD:                 yes
  Inline power:         no
  SPAN:                 source/destination
  PortSecure:           yes
  Dot1x:                yes
```

次の例では、**description** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスを *Connects to Marketing* として指定した場合の **show interfaces** *interface***description** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet1/0/2 description
Interface                      Status         Protocol Description
Gi1/0/2                        up             down     Connects to Marketing
```

次の例では、スイッチにポート チャネルが設定されている場合の **show interfaces etherchannel** コマンドの出力を示します。

```
Switch# show interfaces etherchannel
----
Port-channel34:
Age of the Port-channel   = 28d:18h:51m:46s
Logical slot/port   = 12/34          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Passive port list   =
Port state          = Port-channel L3-Ag Ag-Not-Inuse
Protocol            =    -
Port security       = Disabled
```

次の例では、VTP ドメイン内でプルーニングがイネーブルの場合の **show interfaces** *interface-id* **pruning** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3
```

次の例では、指定した VLAN インターフェイスの **show interfaces stats** コマンドの出力を示します。

```
Switch# show interfaces vlan 1 stats
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
     Processor    1165354   136205310      570800     91731594
   Route cache          0           0           0            0
         Total    1165354   136205310      570800     91731594
```

次の例では、**show interfaces status** コマンドの出力の一部を示します。すべてのインターフェイスのステータスが表示されます。

次に、**show interfaces** *interface-id***status** コマンドの出力例を示します。

```
Switch# show interfaces gigabitethernet1/0/20 status
Port      Name               Status       Vlan       Duplex  Speed       Type
Gi1/0/20                     notconnect   1            auto   auto 10/100/1000Ba
```

```
seTX
```

次の例では、**show interfaces status err-disabled** コマンドの出力を示します。errdisable ステートのインターフェイスのステータスを表示します。

```
Switch# show interfaces status err-disabled
Port      Name       Status         Reason
Gi1/0/2              err-disabled   gbic-invalid
Gi2/0/3              err-disabled   dtp-flap
```

次の例では、**show interfaces** *interface-id* **pruning** コマンドの出力を示します。

```
Switch# show interfaces gigabitethernet1/0/2 pruning
Port Vlans pruned for lack of request by neighbor
```

次の例では、**show interfaces** *interface-id* **trunk** コマンドの出力を示します。ポートのトランキング情報が表示されます。

```
Switch# show interfaces gigabitethernet1/0/1 trunk
Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/1     on               802.1q         other         10

Port        Vlans allowed on trunk
Gi1/0/1     none

Port        Vlans allowed and active in management domain
Gi1/0/1     none

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/1     none
```

関連トピック

show interfaces counters （137 ページ）
show interfaces switchport （140 ページ）
show interfaces transceiver （144 ページ）

show interfaces counters

スイッチまたは特定のインターフェイスのさまざまなカウンタを表示するには、特権 EXEC モードで **show interfaces counters** コマンドを使用します。

show interfaces [*interface-id*] **counters** [{**errors**|**etherchannel**|**module** *stack-member-number*|**protocol status**|**trunk**}]

構文の説明

interface-id	（任意）物理インターフェイスの ID（タイプ、スタック メンバ（スタック構成可能なスイッチのみ）、モジュール、ポート番号を含む）。
errors	（任意）エラー カウンタを表示します。
etherchannel	（任意）送受信されたオクテット、ブロードキャスト パケット、マルチキャスト パケット、およびユニキャスト パケットなど、EtherChannel カウンタを表示します。
module *stack-member-number*	（任意）指定されたスタック メンバのカウンタを表示します。 指定できる範囲は 1 ～ 9 です。 （注） このコマンドでは、**module** キーワードはスタック メンバ番号を参照しています。インターフェイス ID に含まれるモジュール番号は、常に 0 です。
protocol status	（任意）インターフェイスでイネーブルになっているプロトコルのステータスを表示します。
trunk	（任意）トランク カウンタを表示します。

（注） **vlan** *vlan-id* キーワードは、コマンドラインのヘルプ文字列には表示されますが、サポートされていません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

キーワードを入力しない場合は、すべてのインターフェイスのすべてのカウンタが表示されます。

次の例では、**show interfaces counters** コマンドの出力の一部を示します。スイッチのすべてのカウンタが表示されます。

```
Switch# show interfaces counters
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi1/0/1                0              0              0              0
Gi1/0/2                0              0              0              0
Gi1/0/3         95285341          43115        1178430           1950
Gi1/0/4                0              0              0              0

<output truncated>
```

次の例では、スタック メンバ 2 に対する **show interfaces counters module** コマンドの出力の一部を示します。スタック内で指定されたスイッチのすべてのカウンタが表示されます。

```
Switch# show interfaces counters module 2
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi1/0/1              520              2              0              0
Gi1/0/2              520              2              0              0
Gi1/0/3              520              2              0              0
Gi1/0/4              520              2              0              0

<output truncated>
```

次の例では、すべてのインターフェイスに対する **show interfaces counters protocol status** コマンドの出力の一部を示します。

```
Switch# show interfaces counters protocol status
Protocols allocated:
Vlan1: Other, IP
Vlan20: Other, IP, ARP
Vlan30: Other, IP, ARP
Vlan40: Other, IP, ARP
Vlan50: Other, IP, ARP
Vlan60: Other, IP, ARP
Vlan70: Other, IP, ARP
Vlan80: Other, IP, ARP
Vlan90: Other, IP, ARP
Vlan900: Other, IP, ARP
Vlan3000: Other, IP
Vlan3500: Other, IP
GigabitEthernet1/0/1: Other, IP, ARP, CDP
GigabitEthernet1/0/2: Other, IP
GigabitEthernet1/0/3: Other, IP
GigabitEthernet1/0/4: Other, IP
GigabitEthernet1/0/5: Other, IP
GigabitEthernet1/0/6: Other, IP
GigabitEthernet1/0/7: Other, IP
GigabitEthernet1/0/8: Other, IP
GigabitEthernet1/0/9: Other, IP
GigabitEthernet1/0/10: Other, IP, CDP

<output truncated>
```

次の例では、**show interfaces counters trunk** コマンドの出力を示します。すべてのインターフェイスのトランク カウンタが表示されます。

```
Switch# show interfaces counters trunk
Port        TrunkFramesTx   TrunkFramesRx   WrongEncap
Gi1/0/1                 0               0            0
Gi1/0/2                 0               0            0
Gi1/0/3             80678               0            0
Gi1/0/4             82320               0            0
Gi1/0/5                 0               0            0

<output truncated>
```

関連トピック

show interfaces （132 ページ）

show interfaces switchport

ポートブロッキング、ポート保護設定など、スイッチング（非ルーティング）ポートの管理ステータスおよび動作ステータスを表示するには、特権EXECモードで**show interfaces switchport**コマンドを使用します。

show interfaces [*interface-id*] **switchport** [{**backup** [**detail**]|**module** *number*}]

構文の説明

interface-id	（任意）インターフェイスのIDです。有効なインターフェイスには、物理ポート（タイプ、スタック構成可能なスイッチのスタック メンバ、モジュール、およびポート番号を含む）やポート チャネルが含まれます。指定できるポート チャネルは1 ～ 48です。
backup	（任意）指定したインターフェイスまたはすべてのインターフェイスのFlex Linkバックアップ インターフェイス コンフィギュレーションを表示します。
detail	（任意）スイッチまたはスタック上の指定したインターフェイスまたはすべてのインターフェイスの詳細なバックアップ情報を表示します。
module *number*	（任意）スイッチまたは指定されたスタック メンバのすべてのインターフェイスのスイッチポート設定を表示します。 指定できる範囲は1 ～ 9です。 このオプションは、特定のインターフェイスIDを入力したときは利用できません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スタックのスイッチ上のすべてのインターフェイスのスイッチ ポート特性を表示するには、**show interface switchport module** *number* コマンドを使用します。スタック内に該当するモジュール番号を持つスイッチがない場合、出力はありません。

次の例では、ポートの **show interfaces switchport** コマンドの出力を示します。次の表に、この出力で表示されるフィールドについて説明します。

（注） プライベート VLAN はこのリリースではサポートされないので、フィールドは適用されません。

```
Switch# show interfaces gigabitethernet1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 10 (VLAN0010)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 11-20
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

フィールド	説明
名前	ポート名を表示します。
Switchport	ポートの管理ステータスおよび動作ステータスを表示します。この出力の場合、ポートはスイッチポート モードです。
Administrative Mode 動作モード	管理モードおよび動作モードを表示します。
Administrative Trunking Encapsulation Operational Trunking Encapsulation Negotiation of Trunking	管理上および運用上のカプセル化方式、およびトランキング ネゴシエーションがイネーブルかどうかを表示します。
Access Mode VLAN	ポートを設定する VLAN ID を表示します。

フィールド	説明
Trunking Native Mode VLAN Trunking VLANs Enabled Trunking VLANs Active	ネイティブ モードのトランクの VLAN ID を一覧表示します。トランク上の許可 VLAN を一覧表示します。トランク上のアクティブ VLAN を一覧表示します。
Pruning VLANs Enabled	プルーニングに適格な VLAN を一覧表示します。
Protected	インターフェイス上で保護ポートがイネーブル（True）であるかまたはディセーブル（False）であるかを表示します。
Unknown unicast blocked Unknown multicast blocked	不明なマルチキャストおよび不明なユニキャスト トラフィックがインターフェイス上でブロックされているかどうかを表示します。
音声 VLAN	音声 VLAN がイネーブルである VLAN ID を表示します。
Appliance trust	IP Phone のデータ パケットのサービス クラス（CoS）設定を表示します。

次の例では、**show interfaces switchport backup** コマンドの出力を示します。

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface    Backup Interface    State
------------------------------------------------------------
Gi1/0/1              Gi1/0/2             Active Up/Backup Standby
Gi3/0/3              Gi4/0/5             Active Down/Backup Up
Po1                  Po2                 Active Standby/Backup Up
```

show interfaces switchport backup コマンドからの出力例では、スイッチに VLAN 1 ～ 50、60、および 100 ～ 120 が設定されています。

```
Switch(config)# interface gigabitethernet 2/0/6
Switch(config-if)# switchport backup interface gigabitethernet 2/0/8
prefer vlan 60,100-120
```

両方のインターフェイスが動作中の場合は、Gi2/0/8 が VLAN 60 および VLAN 100 ～ 120 のトラフィックを転送し、Gi2/0/6 が VLAN 1 ～ 50 のトラフィックを転送します。

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Up/Backup Up
Vlans on Interface Gi 2/0/6: 1-50
Vlans on Interface Gi 2/0/8: 60, 100-120
```

Flex Link インターフェイスがダウンすると（LINK_DOWN）、このインターフェイスで優先される VLAN は、Flex Link ペアのピア インターフェイスに移動します。この例では、インターフェイス Gi2/0/6 がダウンして、Gi2/0/8 が Flex Link ペアのすべての VLAN を引き継ぎます。

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Down/Backup Up
Vlans on Interface Gi 2/0/6:
Vlans on Interface Gi 2/0/8: 1-50, 60, 100-120
```

Flex Link インターフェイスがアップになると、このインターフェイスで優先される VLAN はピア インターフェイスでブロックされ、アップしたインターフェイスでフォワーディング ステートになります。この例では、インターフェイス Gi2/0/6 がアップになると、このインターフェイスで優先される VLAN はピア インターフェイス Gi2/0/8 でブロックされ、Gi2/0/6 で転送されます。

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet2/0/6    GigabitEthernet2/0/8    Active Up/Backup Up
Vlans on Interface Gi 2/0/6: 1-50
Vlans on Interface Gi 2/0/8: 60, 100-120
```

関連トピック

show interfaces （132 ページ）

show interfaces transceiver

SFP モジュール インターフェイスの物理インターフェイスを表示するには、EXEC モードで **show interfaces transceiver** コマンドを使用します。

show interfaces [*interface-id*] **transceiver** [{**detail**|**module** *number*|**properties**|**supported-list**|**threshold-table**}]

構文の説明

interface-id	（任意）物理インターフェイスの ID（タイプ、スタック メンバ（スタック構成可能なスイッチのみ）、モジュール、ポート番号を含む）。
detail	（任意）（スイッチにインストールされている場合）Digital Optical Monitoring（DoM）対応トランシーバの高低値やアラーム情報などの、調整プロパティを表示します。
module *number*	（任意）スイッチのモジュールのインターフェイスへの表示を制限します。 指定できる範囲は 1 ～ 9 です。 このオプションは、特定のインターフェイス ID を入力したときは利用できません。
properties	（任意）インターフェイスの速度、デュプレックス、およびインラインパワー設定を表示します。
supported-list	（任意）サポートされるトランシーバをすべて表示します。
threshold-table	（任意）アラームおよび警告しきい値テーブルを表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

例

次に、**show interfaces** *interface-id***transceiver properties** コマンドの出力例を示します。

```
Switch# show interfaces gigabitethernet1/1/1 transceiver properties
  Name : Gi1/1/1
  Administrative Speed: auto
  Operational Speed: auto
  Administrative Duplex: auto
  Administrative Power Inline: enable
  Operational Duplex: auto
  Administrative Auto-MDIX: off
```

```
  Operational Auto-MDIX: off
```

次に、**show interfaces** *interface-id***transceiver detail** コマンドの出力例を示します。

```
Switch# show interfaces gigabitethernet1/1/1 transceiver detail
  ITU Channel not available (Wavelength not available),
  Transceiver is internally calibrated.
  mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
  ++:high alarm, +:high warning, -:low warning, -- :low alarm.
  A2D readouts (if they differ), are reported in parentheses.
  The threshold values are uncalibrated.

                           High Alarm  High Warn  Low Warn   Low Alarm
           Temperature     Threshold   Threshold  Threshold  Threshold
  Port     (Celsius)      (Celsius)   (Celsius)  (Celsius)  (Celsius)
  -------  -------------- ----------  ---------  ---------  ---------
  Gi1/1/1  29.9           74.0        70.0       0.0        -4.0
                           High Alarm  High Warn  Low Warn   Low Alarm
           Voltage         Threshold   Threshold  Threshold  Threshold
  Port     (Volts)         (Volts)     (Volts)    (Volts)    (Volts)
  -------  ------------    ----------  ---------  ---------  ---------
  Gi1/1/1  3.28            3.60        3.50       3.10       3.00

           Optical         High Alarm  High Warn  Low Warn   Low Alarm
           Transmit Power  Threshold   Threshold  Threshold  Threshold
  Port     (dBm)           (dBm)       (dBm)      (dBm)      (dBm)
  -------  --------------  ----------  ---------  ---------  ---------
  Gi1/1/1  1.8             7.9         3.9        0.0        -4.0

           Optical         High Alarm  High Warn  Low Warn   Low Alarm
           Receive Power   Threshold   Threshold  Threshold  Threshold
  Port     (dBm)           (dBm)       (dBm)      (dBm)      (dBm)
  -------  --------------  ----------  ---------  ---------  ---------
  Gi1/1/1  -23.5           -5.0        -9.0       -28.2      -32.2
```

次に、**show interfaces transceiver threshold-table** コマンドの出力例を示します。

```
Switch# show interfaces transceiver threshold-table
              Optical Tx     Optical Rx    Temp     Laser Bias    Voltage
                                                    current
            -------------  -------------  ------   ------------  ---------

 DWDM GBIC
Min1             -4.00        -32.00        -4           N/A          4.65
Min2              0.00        -28.00        0            N/A          4.75
Max2              4.00         -9.00        70           N/A          5.25
Max1              7.00         -5.00        74           N/A          5.40
 DWDM SFP
Min1             -4.00        -32.00        -4           N/A          3.00
Min2              0.00        -28.00        0            N/A          3.10
Max2              4.00         -9.00        70           N/A          3.50
Max1              8.00         -5.00        74           N/A          3.60
 RX only WDM GBIC
Min1              N/A         -32.00        -4           N/A          4.65
Min2              N/A         -28.30        0            N/A          4.75
Max2              N/A          -9.00        70           N/A          5.25
Max1              N/A          -5.00        74           N/A          5.40
 DWDM XENPAK
Min1             -5.00        -28.00        -4           N/A          N/A
Min2             -1.00        -24.00        0            N/A          N/A
Max2              3.00         -7.00        70           N/A          N/A
```

```
Max1              7.00          -3.00         74            N/A           N/A
 DWDM X2
Min1             -5.00         -28.00         -4            N/A           N/A
Min2             -1.00         -24.00         0             N/A           N/A
Max2              3.00          -7.00         70            N/A           N/A
Max1              7.00          -3.00         74            N/A           N/A
 DWDM XFP
Min1             -5.00         -28.00         -4            N/A           N/A
Min2             -1.00         -24.00         0             N/A           N/A
Max2              3.00          -7.00         70            N/A           N/A
Max1              7.00          -3.00         74            N/A           N/A
 CWDM X2
Min1              N/A            N/A          0             N/A           N/A
Min2              N/A            N/A          0             N/A           N/A
Max2              N/A            N/A          0             N/A           N/A
Max1              N/A            N/A          0             N/A           N/A

<output truncated>
```

関連トピック

show interfaces （132 ページ）

show mgmt-infra trace messages ilpower

トレース バッファ内のインライン パワーのメッセージを表示するには、特権 EXEC モードで **show mgmt-infra trace messages ilpower** コマンドを使用します。

show mgmt-infra trace messages ilpower [**switch** *stack-member-number*]

構文の説明

switch *stack-member-number*	（任意）トレース バッファ内のインライン パワーのメッセージを表示するスタック メンバ番号を指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show mgmt-infra trace messages ilpower** コマンドの出力例を示します。

```
Switch# show mgmt-infra trace messages ilpower
[10/23/12 14:05:10.984 UTC 1 3] Initialized inline power system configuration fo
r slot 1.
[10/23/12 14:05:10.984 UTC 2 3] Initialized inline power system configuration fo
r slot 2.
[10/23/12 14:05:10.984 UTC 3 3] Initialized inline power system configuration fo
r slot 3.
[10/23/12 14:05:10.984 UTC 4 3] Initialized inline power system configuration fo
r slot 4.
[10/23/12 14:05:10.984 UTC 5 3] Initialized inline power system configuration fo
r slot 5.
[10/23/12 14:05:10.984 UTC 6 3] Initialized inline power system configuration fo
r slot 6.
[10/23/12 14:05:10.984 UTC 7 3] Initialized inline power system configuration fo
r slot 7.
[10/23/12 14:05:10.984 UTC 8 3] Initialized inline power system configuration fo
r slot 8.
[10/23/12 14:05:10.984 UTC 9 3] Initialized inline power system configuration fo
r slot 9.
[10/23/12 14:05:10.984 UTC a 3] Inline power subsystem initialized.
[10/23/12 14:05:18.908 UTC b 264] Create new power pool for slot 1
[10/23/12 14:05:18.909 UTC c 264] Set total inline power to 450 for slot 1
[10/23/12 14:05:20.273 UTC d 3] PoE is not supported on .
[10/23/12 14:05:20.288 UTC e 3] PoE is not supported on .
[10/23/12 14:05:20.299 UTC f 3] PoE is not supported on .
[10/23/12 14:05:20.311 UTC 10 3] PoE is not supported on .
[10/23/12 14:05:20.373 UTC 11 98] Inline power process post for switch 1
[10/23/12 14:05:20.373 UTC 12 98] PoE post passed on switch 1
[10/23/12 14:05:20.379 UTC 13 3] Slot #1: PoE initialization for board id 16387
[10/23/12 14:05:20.379 UTC 14 3] Set total inline power to 450 for slot 1
[10/23/12 14:05:20.379 UTC 15 3] Gi1/0/1 port config Initialized
[10/23/12 14:05:20.379 UTC 16 3] Interface Gi1/0/1 initialization done.
[10/23/12 14:05:20.380 UTC 17 3] Gi1/0/24 port config Initialized
```

```
[10/23/12 14:05:20.380 UTC 18 3] Interface Gi1/0/24 initialization done.
[10/23/12 14:05:20.380 UTC 19 3] Slot #1: initialization done.
[10/23/12 14:05:50.440 UTC 1a 3] Slot #1: PoE initialization for board id 16387
[10/23/12 14:05:50.440 UTC 1b 3] Duplicate init event
```

関連トピック

show mgmt-infra trace messages ilpower-ha （149 ページ）
show mgmt-infra trace messages platform-mgr-poe （150 ページ）

show mgmt-infra trace messages ilpower-ha

トレース バッファ内のインライン パワーのハイ アベイラビリティのメッセージを表示するには、特権 EXEC モードで **show mgmt-infra trace messages ilpower-ha** コマンドを使用します。

show mgmt-infra trace messages ilpower-ha [**switch** *stack-member-number*]

構文の説明

switch *stack-member-number*	（任意）トレース バッファ内のインライン パワーのメッセージを表示するスタック メンバ番号を指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show mgmt-infra trace messages ilpower-ha** コマンドの出力例を示します。

```
Switch# show mgmt-infra trace messages ilpower-ha
[10/23/12 14:04:48.087 UTC 1 3] NG3K_ILPOWER_HA: Created NGWC ILP CF client succ
essfully.
```

関連トピック

show mgmt-infra trace messages ilpower （147 ページ）
show mgmt-infra trace messages platform-mgr-poe （150 ページ）

show mgmt-infra trace messages platform-mgr-poe

トレース バッファ内のプラットフォーム マネージャの Power over Ethernet（PoE）メッセージを表示するには、**show mgmt-infra trace messages platform-mgr-poe** 特権 EXEC コマンドを使用します。

show mgmt-infra trace messages platform-mgr-poe [**switch** *stack-member-number*]

構文の説明

switch *stack-member-number*	（任意）トレース バッファ内のメッセージを表示するスタック メンバ番号を指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show mgmt-infra trace messages platform-mgr-poe** コマンドの一部の出力例を示します。

```
Switch# show mgmt-infra trace messages platform-mgr-poe
[10/23/12 14:04:06.431 UTC 1 5495] PoE Info: get power controller param sent:
[10/23/12 14:04:06.431 UTC 2 5495] PoE Info: POE_SHUT sent for port 1 (0:0)
[10/23/12 14:04:06.431 UTC 3 5495] PoE Info: POE_SHUT sent for port 2 (0:1)
[10/23/12 14:04:06.431 UTC 4 5495] PoE Info: POE_SHUT sent for port 3 (0:2)
[10/23/12 14:04:06.431 UTC 5 5495] PoE Info: POE_SHUT sent for port 4 (0:3)
[10/23/12 14:04:06.431 UTC 6 5495] PoE Info: POE_SHUT sent for port 5 (0:4)
[10/23/12 14:04:06.431 UTC 7 5495] PoE Info: POE_SHUT sent for port 6 (0:5)
[10/23/12 14:04:06.431 UTC 8 5495] PoE Info: POE_SHUT sent for port 7 (0:6)
[10/23/12 14:04:06.431 UTC 9 5495] PoE Info: POE_SHUT sent for port 8 (0:7)
[10/23/12 14:04:06.431 UTC a 5495] PoE Info: POE_SHUT sent for port 9 (0:8)
[10/23/12 14:04:06.431 UTC b 5495] PoE Info: POE_SHUT sent for port 10 (0:9)
[10/23/12 14:04:06.431 UTC c 5495] PoE Info: POE_SHUT sent for port 11 (0:10)
[10/23/12 14:04:06.431 UTC d 5495] PoE Info: POE_SHUT sent for port 12 (0:11)
[10/23/12 14:04:06.431 UTC e 5495] PoE Info: POE_SHUT sent for port 13 (e:0)
[10/23/12 14:04:06.431 UTC f 5495] PoE Info: POE_SHUT sent for port 14 (e:1)
[10/23/12 14:04:06.431 UTC 10 5495] PoE Info: POE_SHUT sent for port 15 (e:2)
[10/23/12 14:04:06.431 UTC 11 5495] PoE Info: POE_SHUT sent for port 16 (e:3)
[10/23/12 14:04:06.431 UTC 12 5495] PoE Info: POE_SHUT sent for port 17 (e:4)
[10/23/12 14:04:06.431 UTC 13 5495] PoE Info: POE_SHUT sent for port 18 (e:5)
[10/23/12 14:04:06.431 UTC 14 5495] PoE Info: POE_SHUT sent for port 19 (e:6)
[10/23/12 14:04:06.431 UTC 15 5495] PoE Info: POE_SHUT sent for port 20 (e:7)
[10/23/12 14:04:06.431 UTC 16 5495] PoE Info: POE_SHUT sent for port 21 (e:8)
[10/23/12 14:04:06.431 UTC 17 5495] PoE Info: POE_SHUT sent for port 22 (e:9)
[10/23/12 14:04:06.431 UTC 18 5495] PoE Info: POE_SHUT sent for port 23 (e:10)
```

関連トピック

show mgmt-infra trace messages ilpower （147 ページ）

show mgmt-infra trace messages ilpower-ha （149 ページ）

show network-policy profile

ネットワークポリシープロファイルを表示するには、特権 EXEC モードで **show network policy profile** コマンドを使用します。

show network-policy profile [*profile-number*]

構文の説明

profile-number	（任意）ネットワークポリシープロファイル番号を表示します。プロファイルが入力されていない場合、すべてのネットワーク ポリシープロファイルが表示されます。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、**show network-policy profile** コマンドの出力を示します。

```
Switch# show network-policy profile
Network Policy Profile 60
  Interface:
   none
```

関連トピック

network-policy （90 ページ）
network-policy profile（グローバル コンフィギュレーション） （91 ページ）

show platform CAPWAP summary

アクセス ポイントと他のモビリティ コントローラに対してコントローラが確立するすべてのCAPWAP トンネルのトンネル識別子およびタイプを表示するには、**show platform CAPWAP summary** コマンドを使用します。

show platform CAPWAP summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、トンネルの識別子と詳細を表示する例を示します。

```
Switch# show platform capwap summary
Tunnel ID | Type | Src IP | Dst IP | SPrt | DPrt | S | A
------------------------------------------------------------------------------

0x0088498000000983 data 9.6.44.61 9.12.138.101 5247 41894 1 1

0x00966dc000000010 data 9.6.44.61 9.6.47.101 5247 62526 1 2
0x00938e800000095b data 9.6.44.61 9.12.138.100 5247 45697 1 1

0x00ab1a8000000bd1 data 9.6.44.61 9.12.139.101 5247 38906 1 0

0x00896e40000000bd data 9.6.44.61 9.12.136.100 5247 1836 1 1
```

show power inline

指定されたPoEポート、指定されたスタック メンバ、またはスイッチ スタックのすべてのPoEポートのPoEステータスを表示するには、EXECモードで**show power inline**コマンドを使用します。

show power inline [{**police**|**priority**}] [{*interface-id*|**module** *stack-member-number*}] **[detail]**

構文の説明

police	（任意）リアルタイムの電力消費に関するパワー ポリシング情報を表示します。
priority	（任意）各ポートのパワー インライン ポート プライオリティを表示します。
interface-id	（任意）物理インターフェイスのID です。
module *stack-member-number*	（任意）指定されたスタック メンバのポートだけを表示します。 指定できる範囲は1 ～ 9 です。 このキーワードは、スタック対応スイッチでのみサポートされています。
detail	（任意）インターフェイスまたはモジュールの詳細な出力を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

例

次の例では、**show power inline**コマンドの出力を示します。次の表に、出力フィールドについて説明します。

```
Switch> show power inline
Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1             n/a        n/a         n/a
2             n/a        n/a         n/a
3          1440.0       15.4      1424.6
4           720.0        6.3       713.7
Interface Admin  Oper       Power   Device              Class Max
```

```
                            (Watts)
--------- ------ ---------- ------- -------------------- ----- ----
Gi3/0/1   auto   off        0.0     n/a                  n/a   30.0
Gi3/0/2   auto   off        0.0     n/a                  n/a   30.0
Gi3/0/3   auto   off        0.0     n/a                  n/a   30.0
Gi3/0/4   auto   off        0.0     n/a                  n/a   30.0
Gi3/0/5   auto   off        0.0     n/a                  n/a   30.0
Gi3/0/6   auto   off        0.0     n/a                  n/a   30.0
Gi3/0/7   auto   off        0.0     n/a                  n/a   30.0
Gi3/0/8   auto   off        0.0     n/a                  n/a   30.0
Gi3/0/9   auto   off        0.0     n/a                  n/a   30.0
Gi3/0/10  auto   off        0.0     n/a                  n/a   30.0
Gi3/0/11  auto   off        0.0     n/a                  n/a   30.0
Gi3/0/12  auto   off        0.0     n/a                  n/a   30.0
<output truncated>
```

次の例では、スイッチ ポートに対する **show power inline** *interface-id* コマンドの出力を示します。

```
Switch> show power inline gigabitethernet1/0/1
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi1/0/1   auto   off        0.0     n/a                 n/a   30.0
```

次の例では、スタック メンバ 3 での **show power inline module** *switch-number* コマンドの出力を示します。次の表に、出力フィールドについて説明します。

```
Switch> show power inline module 3
Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
3           865.0      864.0         1.0
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi3/0/1   auto   power-deny 4.0     n/a                 n/a   15.4
Gi3/0/2   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/3   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/4   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/5   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/6   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/7   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/8   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/9   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/10  auto   off        0.0     n/a                 n/a   15.4
<output truncated>
```

表 *12 : show power inline* のフィールドの説明

フィールド	説明
Available	スイッチ上の設定電力[3] の合計で、ワット数（W）です。
Used	PoE ポートに割り当てられている設定電力の合計で、ワット数です。
Remaining	システムで割り当てられていない設定電力の合計（ワット数）です。（Available - Used = Remaining）

フィールド	説明
Admin	管理モード：auto、off、static
Oper	動作モード： • on：受電デバイスが検出され、電力が適用されています。 • off：PoE が適用されていません。 • faulty：装置検出または受電デバイスが障害の状態です。 • power-deny：受電デバイスが検出されていますが、PoE が使用できない状態か、最大ワット数が検出された受電デバイスの最大数を超えています。
電源	受電デバイスに割り当てられている最大電力の合計で、ワット数です。この値は、**show power inline police** コマンドの出力の *Cutoff Power* フィールドの値と同じです。
デバイス	検出された装置のタイプ：n/a、unknown、Cisco受電装置、IEEE受電装置、または CDP からの名前。
クラス	IEEE 分類：n/a または 0 ～ 4 の値。
Max	受電デバイスに割り当てられている最大電力の合計で、ワット数です。
AdminPowerMax	スイッチがリアルタイム電力消費をポリシングする場合に、受電デバイスに割り当てられる電力の最大量です（ワット単位）。この値は、*Max*フィールドの値と同じです。
AdminConsumption	スイッチがリアルタイム電力消費をポリシングする場合に、受電デバイスに割り当てられる電力の消費量です（ワット単位）。ポリシングがディセーブルである場合、この値は *AdminPowerMax* フィールドの値と同じです。

[3] 設定電力とは、手動で指定する電力、または CDP 電力ネゴシエーションまたは IEEE 分類を使用してスイッチが指定する電力（電力検知機能によってモニタされるリアルタイムの電力とは異なります）です。

次の例では、スタッキング対応スイッチに対する **show power inline police** コマンドの出力を示します。

```
Switch> show power inline police
Module   Available     Used      Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1           370.0         0.0       370.0
3           865.0       864.0         1.0
          Admin  Oper        Admin      Oper       Cutoff Oper
Interface State  State       Police     Police     Power  Power
--------- ------ ----------- ---------- ---------- ------ ------
Gi1/0/1   auto   off         none       n/a        n/a    0.0
Gi1/0/2   auto   off         log        n/a        5.4    0.0
Gi1/0/3   auto   off         errdisable n/a        5.4    0.0
```

```
Gi1/0/4   off    off         none       n/a        n/a    0.0
Gi1/0/5   off    off         log        n/a        5.4    0.0
Gi1/0/6   off    off         errdisable n/a        5.4    0.0
Gi1/0/7   auto   off         none       n/a        n/a    0.0
Gi1/0/8   auto   off         log        n/a        5.4    0.0
Gi1/0/9   auto   on          none       n/a        n/a    5.1
Gi1/0/10  auto   on          log        ok         5.4    4.2
Gi1/0/11  auto   on          log        log        5.4    5.9
Gi1/0/12  auto   on          errdisable ok         5.4    4.2
Gi1/0/13  auto   errdisable  errdisable n/a        5.4    0.0
<output truncated>
```

上の例では、次のようになっています。

- Gi1/0/1 ポートはシャットダウンしていて、ポリシングは設定されていません。
- Gi1/0/2 ポートはシャットダウンしていますが、ポリシングはイネーブルであり、ポリシング アクションとして syslog メッセージを生成するよう設定されています。
- Gi1/0/3 ポートはシャットダウンしていますが、ポリシングはイネーブルであり、ポリシング アクションとしてポートをシャットダウンするよう設定されています。
- Gi1/0/4 ポートでは、デバイス検出がディセーブルであり、ポートに電力が供給されておらず、ポリシングがディセーブルです。
- Gi1/0/5 ポートでは、デバイス検出がディセーブルであり、ポートに電力が供給されていませんが、ポリシングはイネーブルであり、ポリシング アクションとして syslog メッセージを生成するよう設定されています。
- Gi1/0/6 ポートでは、デバイス検出がディセーブルであり、ポートに電力が供給されていませんが、ポリシングはイネーブルであり、ポリシング アクションとしてポートをシャットダウンするよう設定されています。
- Gi1/0/7 ポートはアップしていて、ポリシングはディセーブルですが、接続されている装置に対してスイッチから電力が供給されていません。
- Gi1/0/8 ポートはアップしていて、ポリシングはイネーブルであり、ポリシング アクションとして syslog メッセージを生成するよう設定されていますが、受電デバイスに対してスイッチから電力が供給されていません。
- Gi1/0/9 ポートはアップしていて、受電デバイスが接続されており、ポリシングはディセーブルです。
- Gi1/0/10 ポートはアップしていて、受電デバイスが接続されています。ポリシングはイネーブルであり、ポリシング アクションとして syslog メッセージを生成するよう設定されています。リアルタイム電力消費がカットオフ値より少ないため、ポリシング アクションは作動しません。
- Gi1/0/11 ポートはアップしていて、受電デバイスが接続されています。ポリシングはイネーブルであり、ポリシング アクションとして syslog メッセージを生成するよう設定されています。
- Gi1/0/12 ポートはアップしていて、受電デバイスが接続されています。ポリシングはイネーブルであり、ポリシング アクションとしてポートをシャットダウンするよう設定されています。リアルタイム電力消費がカットオフ値より少ないため、ポリシング アクションは作動しません。

- Gi1/0/13 ポートはアップしていて、受電デバイスが接続されています。ポリシングはイネーブルであり、ポリシング アクションとしてポートをシャットダウンするよう設定されています。

次の例では、スタンドアロン スイッチに対する **show power inline police** *interface-id* コマンドの出力を示します。次の表に、出力フィールドについて説明します。

```
Switch> show power inline police gigabitethernet1/0/1
Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi1/0/1   auto   off        none       n/a        n/a    0.0
```

表 *13 : show power inline police* のフィールドの説明

フィールド	説明
Available	スイッチ上の設定電力[4]
Used	PoE ポートに割り当てられている設定電力の合計で、ワット数です。
Remaining	システムで割り当てられていない設定電力の合計（ワット数）です。（Available - Used = Remaining）
Admin State	管理モード：auto、off、static
Oper State	動作モード： • errdisable：ポリシングはイネーブルです。 • faulty：受電デバイスでの装置検出が障害の状態です。 • off：PoE が適用されていません。 • on：受電デバイスが検出され、電力が適用されています。 • power-deny：受電デバイスが検出されていますが、PoE が使用できない状態か、リアルタイム電力消費が最大電力割り当てを超えています。 （注） 動作モードは、指定した PoE ポート、指定したスタック メンバ、またはスイッチのすべての PoE ポートの現在の PoE ステートです。
Admin Police	リアルタイム電力消費ポリシング機能のステータス： • errdisable：ポリシングがイネーブルで、リアルタイム電力消費が最大電力割り当てを超えるとスイッチはポートをシャットダウンします。 • log：ポリシングはイネーブルで、リアルタイム電力消費が最大電力割り当てを超えるとスイッチが Syslog メッセージを生成します。 • none：ポリシングはディセーブルです。

フィールド	説明
Oper Police	ポリシング ステータス： • errdisable：リアルタイム電力消費が最大電力割り当てを超えています。スイッチが PoE ポートをシャットダウンします。 • log：リアルタイム電力消費が最大電力割り当てを超えています。スイッチが Syslog メッセージを生成します。 • n/a：装置検出がディセーブルで、電力が PoE ポートに適用されていないか、ポリシング アクションが設定されていません。 • ok：リアルタイム電力消費が最大電力割り当てより少ない状態です。
Cutoff Power	ポートに割り当てられている最大電力です。リアルタイム電力消費がこの値を上回ると、スイッチは設定されたポリシング アクションを実行します。
Oper Power	受電デバイスのリアルタイム電力消費です。

[4] 設定電力とは、手動で指定する電力、または CDP 電力ネゴシエーションまたは IEEE 分類を使用してスイッチが指定する電力（電力検知機能によってモニタされるリアルタイムの電力とは異なります）です。

関連トピック

logging event power-inline-status （86 ページ）
power inline （97 ページ）

show stack-power

電源スタックのStackPower スタックまたはスイッチに関する情報を表示するには、EXEC モードで **show stack-power** コマンドを使用します。

show stack-power [*power-stack-name*]

構文の説明

power-stack-name	（任意）電源情報を表示する電源スタックの名前。名前は最大で 31 文字にできます。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、IP Base または IP Services イメージが実行されているスイッチ スタックでのみ使用できます。

負荷制限のためにスイッチがシャットダウンされた場合、**show stack-power** コマンドの出力には、シャットダウンされたネイバー スイッチの MAC アドレスが含まれています。コマンド出力は、スイッチに供給するために十分な電力がない場合でも、スタック電力トポロジを示します。

例

次の例では、**show stack-power** コマンドの出力を示します。

```
Switch# show stack-power
Power Stack           Stack   Stack    Total   Rsvd    Alloc   Unused  Num  Num
Name                  Mode    Topolgy  Pwr(W)  Pwr(W)  Pwr(W)  Pwr(W)  SW   PS
--------------------  ------  -------  ------  ------  ------  ------  ---  ---
Powerstack-1          SP-PS   Stndaln  715     509     190     16      1    1
```

関連トピック

mode（電源スタックの設定） （88 ページ）
power-priority （95 ページ）
stack-power （165 ページ）

show system mtu

グローバル最大伝送ユニット（MTU）、またはスイッチに設定されている最大パケット サイズを表示するには、特権 EXEC モードで **show system mtu** コマンドを使用します。

show system mtu

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

MTU 値および MTU 値に影響を与えるスタック設定の詳細については、**system mtu** コマンドを参照してください。

例

次の例では、**show system mtu** コマンドの出力を示します。

```
Switch# show system mtu
Global Ethernet MTU is 1500 bytes.
```

関連トピック

system mtu （172 ページ）

show wireless interface summary

ワイヤレス インターフェイスのステータスおよび設定を表示するには、**show wireless interfacesummary** 特権 EXEC コマンドを使用します。

show wireless interface summary

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

次に、ワイヤレス インターフェイスの要約を表示する例を示します。

```
Switch# show wireless interface summary
```

speed

10/100/1000/2500/5000 Mbps ポートの速度を指定するには、インターフェイス コンフィギュレーション モードで **speed** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

speed {**10**|**100**|**1000**|**2500**|**5000**|**auto** [{**10**|**100**|**1000**|**2500**|**5000**}]|**nonegotiate**}
no speed

構文の説明

10	ポートが 10 Mbps で稼働することを指定します。
100	ポートが 100 Mbps で稼働することを指定します。
1000	ポートが 1000 Mbps で稼働することを指定します。このオプションは、10/100/1000 Mb/s ポートでだけ有効になって表示されます。
2500	ポートが 2500 Mbps で稼働することを指定します。このオプションは、マルチギガビット対応のイーサネット ポートでのみ有効であり、表示されます。
5000	ポートが 5000 Mbps で稼働することを指定します。このオプションは、マルチギガビット対応のイーサネット ポートでのみ有効であり、表示されます。
auto	稼働時のポートの速度を、リンクのもう一方の終端のポートを基準にして自動的に検出します。**10**, **100**, **1000**, **1000**, **2500** キーワードまたは **5000** キーワードを **auto** キーワードとともに使用すると、ポートは指定した速度でのみ自動ネゴシエーションを実行します。
nonegotiate	自動ネゴシエーションをディセーブルにし、ポートは 1000 Mbps で稼働します。

コマンド デフォルト

デフォルトは **auto** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE Denali 16.3.1	このコマンドが変更されました。**2500** と **5000** のキーワードが追加されました。これらのキーワードは、マルチギガビット イーサネット ポート対応デバイスでのみ表示されます。

使用上のガイドライン

10 ギガビット イーサネット ポートでは速度を設定できません。

1000BASE-T Small Form-Factor Pluggable（SFP）モジュールを除き、SFP モジュール ポートが自動ネゴシエーションをサポートしていないデバイスに接続されている場合は、ネゴシエートしないように（**nonegotiate**）速度を設定できます。

新しいキーワードの **2500** および **5000** は、マルチギガビット（m-Gig）イーサネット対応デバイスでのみ表示されます。

速度が **auto** に設定されている場合、スイッチはもう一方のリンクの終端にあるデバイスと速度設定についてネゴシエートし、速度をネゴシエートされた値に強制的に設定します。デュプレックス設定はリンクの両端での設定が引き継がれますが、これにより、デュプレックス設定に矛盾が生じることがあります。

ラインの両端が自動ネゴシエーションをサポートしている場合、デフォルトの自動ネゴシエーション設定を使用することを強く推奨します。一方のインターフェイスでは自動ネゴシエーションをサポートし、もう一方の終端ではサポートしていない場合、サポートしている側には auto 設定を使用し、サポートしていない終端にはデュプレックスおよび速度を設定します。

⚠

注意 インターフェイス速度とデュプレックス モードの設定を変更すると、再設定中にインターフェイスがシャットダウンし、再びイネーブルになる場合があります。

スイッチの速度およびデュプレックスのパラメータの設定に関する注意事項は、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring Interface Characteristics」の章を参照してください。

show interfaces 特権 EXEC コマンドを使用して、設定を確認します。

例

次に、ポートの速度を 100 Mbps に設定する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed 100
```

次に、10 Mbps でだけポートが自動ネゴシエートするように設定する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto 10
```

次に、10 Mbps または 100 Mbps でだけポートが自動ネゴシエートするように設定する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto 10 100
```

関連トピック

duplex （68 ページ）
show interfaces （132 ページ）

stack-power

設定内容 電源スタックまたは電源スタックのスイッチに StackPower パラメータを設定するには、グローバル コンフィギュレーション モードで **stack power** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

stack-power {**stack** *power-stack-name*|**switch** *stack-member-number*}
no stack-power {**stack** *power-stack-name*|**switch** *stack-member-number*}

構文の説明

stack *power-stack-name*	電源スタックの名前を指定します。名前は最大で 31 文字にできます。これらのキーワードの後に改行を入力すると、電源スタック コンフィギュレーション モードが開始されます。
switch *stack-member-number*	スタックのスイッチ番号（1 ～ 4）を指定して、スイッチのスイッチ スタック電源コンフィギュレーション モードを開始します。

コマンド デフォルト

デフォルトはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

stack-power stack *power stack name* コマンドを入力すると、電源スタック コンフィギュレーション モードが開始され、次のコマンドが使用可能になります。

- **default**：コマンドをデフォルト設定に戻します。
- **exit**：ARP アクセスリスト コンフィギュレーション モードを終了します。
- **mode**：電源スタックの電源モードを設定します。**mode** コマンドを参照してください。
- **no**：コマンドを無効にするか、またはデフォルト設定に戻します。

StackPower に関係のないスイッチ番号を指定して **stack-power switch** *switch-number* コマンドを入力すると、エラー メッセージが表示されます。

StackPower に関係するスイッチの番号を指定して **stack-power switch** *switch-number* コマンドを入力すると、スイッチ スタック電源コンフィギュレーション モードが開始され、次のコマンドが使用可能になります。

- **default**：コマンドをデフォルト設定に戻します。
- **exit**：スイッチ スタック電源コンフィギュレーション モードを終了します。
- **no**：コマンドを無効にするか、またはデフォルト設定に戻します。
- **power-priority**：スイッチとスイッチ ポートの電源プライオリティを設定します。**power-priority** コマンドを参照してください。

- **stack-id** *name*：スイッチが属する電源スタックの名前を入力します。電源スタック ID を入力しない場合、スイッチはスタック パラメータを継承しません。名前は最大で 31 文字にできます。
- **standalone**：スイッチをスタンドアロン電源モードで動作させます。このモードに設定すると、両方の電源ポートがシャットダウンします。

例

次の例では、電源スタックに接続されたスイッチ 2 が電源プールから削除され、両方の電源ポートがシャットダウンされます。

```
Switch(config)# stack-power switch 2
Switch(config-switch-stackpower)# standalone
Switch(config-switch-stackpower)# exit
```

関連トピック

mode（電源スタックの設定） （88 ページ）
power-priority （95 ページ）
show stack-power （160 ページ）

switchport backup interface

Flex Link を設定するには、スイッチ スタックまたはスタンドアロン スイッチのレイヤ 2 インターフェイスで、インターフェイス コンフィギュレーション モードの **switchport backup interface** コマンドを使用します。Flex Link の設定を削除するには、このコマンドの **no** 形式を使用します。

switchport backup interface *interface-id* [{**mmu primary vlan** *vlan-id*|**multicast fast-convergence**|**preemption** {**delay** *seconds*|**mode** {**bandwidth**|**forced**|**off**}}|**prefer vlan** *vlan-id*}]
no switchport backup interface *interface-id* [{**mmu primary vlan**|**multicast fast-convergence**|**preemption** {**delay**|**mode**}|**prefer vlan**}]

構文の説明

interface-id	物理インターフェイスの ID。
mmu	（任意）バックアップ インターフェイス ペアの MAC Move Update（MMU）を設定します。
primary vlan *vlan-id*	（任意）プライマリ VLAN の VLAN ID です。指定できる範囲は 1 ～ 4094 です。
multicast fast-convergence	（任意）バックアップ インターフェイスのマルチキャスト高速コンバージェンスを設定します。
preemption	（任意）バックアップ インターフェイス ペアのプリエンプション スキームを設定します。
delay *seconds*	プリエンプション遅延を指定します。指定できる範囲は 1 ～ 300 秒です。デフォルト値は 35 秒です。
mode	プリエンプション モードを指定します。
bandwidth	より大きい帯域幅のインターフェイスを優先するように指定します。
forced	アクティブ インターフェイスを優先するように指定します。
off	バックアップからアクティブへのプリエンプションが発生しないことを指定します。
prefer vlan *vlan-id*	（任意）VLAN が Flex Link ペアのバックアップ インターフェイスで実行されるように指定します。VLAN ID 範囲は 1 ～ 4094 です。

コマンド デフォルト

デフォルトは、Flex Link が定義されていません。プリエンプション モードはオフです。プリエンプションを行いません。プリエンプション遅延は 35 秒に設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

Flex Link 相互バックアップを提供するインターフェイスのペアです。Flex Link を設定すると、1 つのリンクがプライマリ インターフェイスとして機能してトラフィックを転送し、もう一方のインターフェイスがスタンバイ モードになり、プライマリ リンクがシャットダウンされた場合に転送を開始できるように準備されます。設定されるインターフェイスはアクティブ リンクと呼ばれ、指定されたインターフェイスはバックアップ リンクとして識別されます。この機能はスパニングツリープロトコル（STP）の代わりに提供され、ユーザが STP をオフにしても基本的なリンク冗長性を維持できます。

このコマンドは、レイヤ 2 インターフェイスに対してだけ使用可能です。

任意のアクティブ リンクに対して設定可能な Flex Link バックアップ リンクは 1 つだけで、アクティブ インターフェイスとは異なるインターフェイスでなければなりません。

- インターフェイスが所属できる Flex Link ペアは 1 つだけです。インターフェイスは、1 つだけのアクティブ リンクのバックアップ リンクにすることができます。アクティブ リンクは別の Flex Link ペアに属することはできません。
- バックアップ リンクはアクティブ リンクと同じタイプ（たとえばファスト イーサネットやギガビット イーサネット）でなくてもかまいません。ただし、スタンバイ リンクがトラフィック転送を開始した場合にループが発生したり動作が変更したりしないように、両方の Flex Link を同様の特性で設定する必要があります。
- どちらのリンクも、EtherChannel に属するポートには設定できません。ただし、2 つのポート チャネル（EtherChannel 論理インターフェイス）を Flex Link として設定でき、ポート チャネルおよび物理インターフェイスを Flex Link として設定して、ポート チャネルか物理インターフェイスのどちらかをアクティブ リンクにすることができます。
- STP がスイッチに設定されている場合、Flex Link はすべての有効な VLAN で STP に参加しません。STP が動作していない場合、設定されているトポロジでループが発生していないことを確認してください。

次の例では、2 つのインターフェイスを Flex Link として設定する例を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)# switchport backup interface gigabitethernet1/0/2
Switch(conf-if)# end
```

次の例では、常にバックアップをプリエンプトするようにギガビットイーサネットインターフェイスを設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 preemption forced
Switch(conf-if)# end
```

次の例では、ギガビットイーサネットインターフェイスのプリエンプション遅延時間を設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 preemption delay 150
Switch(conf-if)# end
```

次の例では、MMU プライマリ VLAN としてギガビットイーサネットインターフェイスを設定する方法を示します。

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 mmu primary vlan 1021
Switch(conf-if)# end
```

設定を確認するには、**show interfaces switchport backup** 特権 EXEC コマンドを入力します。

関連トピック

show interfaces switchport （140 ページ）

switchport block

不明のマルチキャストまたはユニキャストパケットが転送されないようにするには、インターフェイス コンフィギュレーション モードで **switchport block** コマンドを使用します。不明のマルチキャストまたはユニキャスト パケットの転送を許可するには、このコマンドの **no** 形式を使用します。

switchport block {**multicast**|**unicast**}
no switchport block {**multicast**|**unicast**}

構文の説明

multicast 不明のマルチキャスト トラフィックがブロックされるように指定します。

（注） 純粋なレイヤ 2 マルチキャスト トラフィックだけがブロックされます。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。

unicast 不明のユニキャスト トラフィックがブロックされるように指定します。

コマンド デフォルト

不明なマルチキャストおよびユニキャスト トラフィックはブロックされていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、不明な MAC アドレスを持つすべてのトラフィックがすべてのポートに送信されます。保護ポートまたは非保護ポート上の不明なマルチキャストまたはユニキャスト トラフィックをブロックすることができます。不明なマルチキャストまたはユニキャスト トラフィックが保護ポートでブロックされない場合、セキュリティに問題のある場合があります。

マルチキャスト トラフィックでは、ポート ブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。

不明なマルチキャストまたはユニキャスト トラフィックのブロックは、保護ポート上で自動的にイネーブルにはなりません。明示的に設定する必要があります。

パケットのブロックに関する情報は、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

次の例では、インターフェイス上で不明なユニキャスト トラフィックをブロックする方法を示します。

```
Switch(config-if)# switchport block unicast
```

設定を確認するには、**show interfaces** *interface-id***switchport** 特権 EXEC コマンドを入力します。

関連トピック

show interfaces switchport （140 ページ）

system mtu

ギガビット イーサネットおよび 10 ギガビット イーサネット ポートのスイッチド パケットのグローバル最大パケット サイズまたはMTUサイズを設定するには、グローバル コンフィギュレーション モードで **system mtu** コマンドを使用します。グローバル MTU 値をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

system mtu *bytes*
no system mtu

構文の説明

bytes	グローバル MTU のサイズ（バイト単位）。指定できる範囲は、1500 ～ 9198 バイトです。デフォルトは 1500 バイトです。

コマンド デフォルト

すべてのポートのデフォルトの MTU サイズは 1500 バイトです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

設定を確認するには、**show system mtu** 特権 EXEC コマンドを入力します。

スイッチはインターフェイス単位では MTU をサポートしていません。

特定のインターフェイス タイプで許容範囲外の値を入力した場合、その値は受け入れられません。

例

次に、グローバル システム MTU サイズを 6000 バイトに設定する例を示します。

```
Switch(config)# system mtu 6000
Global Ethernet MTU is set to 6000 bytes.
Note: this is the Ethernet payload size, not the total
Ethernet frame size, which includes the Ethernet
header/trailer and possibly other tags, such as ISL or
802.1q tags.
```

関連トピック

show system mtu （161 ページ）

voice-signalingvlan（ネットワークポリシーコンフィギュレーション）

音声シグナリング アプリケーション タイプのネットワークポリシー プロファイルを作成するには、ネットワークポリシー コンフィギュレーション モードで **voice-signaling vlan** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

voice-signaling vlan {*vlan-id* [{**cos** *cos-value*|**dscp** *dscp-value*}]|**dot1p** [{**cos** *l2-priority*|**dscp** *dscp*}]|**none**|**untagged**}

構文の説明

vlan-id	（任意）音声トラフィック用の VLAN。指定できる範囲は 1 ～ 4094 です。
cos *cos-value*	（任意）設定された VLAN に対するレイヤ 2 プライオリティ Class of Service（CoS）を指定します。指定できる範囲は 0 ～ 7 です。デフォルト値は 5 です。
dscp *dscp-value*	（任意）設定された VLAN に対する Diffserv コード ポイント（DSCP）値を指定します。指定できる範囲は 0 ～ 63 です。デフォルト値は 46 です。
dot1p	（任意）IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話を設定します。
none	（任意）音声 VLAN に関して IP Phone に指示しません。電話は電話のキーパッドから入力された設定を使用します。
untagged	（任意）タグなしの音声トラフィックを送信するように電話を設定します。これが電話のデフォルトになります。

コマンド デフォルト

音声シグナリング アプリケーション タイプのネットワークポリシー プロファイルは定義されていません。

デフォルトの CoS 値は、5 です。

デフォルトの DSCP 値は、46 です。

デフォルトのタギング モードは、untagged です。

コマンド モード

ネットワークポリシー プロファイル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

プロファイルを作成し、ネットワークポリシー プロファイル コンフィギュレーション モードを開始するには、**network-policy profile** グローバル コンフィギュレーション コマンドを使用します。

voice-signaling アプリケーション タイプは、音声メディアと異なる音声シグナリング用のポリシーを必要とするネットワーク トポロジ用です。すべての同じネットワーク ポリシーが voice policy TLV にアドバタイズされたポリシーとして適用される場合、このアプリケーション タイプはアドバタイズしないでください。

ネットワークポリシー プロファイル コンフィギュレーション モードの場合、VLAN、Class of Service（CoS）、Diffserv コード ポイント（DSCP）の値、およびタギング モードを指定することで、音声シグナリング用のプロファイルを作成することができます。

これらのプロファイルの属性は、Link Layer Discovery Protocol for Media Endpoint Devices（LLDP-MED）の network-policy Time Length Value（TLV）に含まれます。

ネットワークポリシー プロファイル コンフィギュレーション モードから特権 EXEC モードに戻る場合は、**exit** コマンドを入力します。

次の例では、プライオリティ 2 の CoS を持つ VLAN 200 用の音声シグナリングを設定する方法を示します。

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice-signaling vlan 200 cos 2
```

次の例では、DSCP 値 45 を持つ VLAN 400 用の音声シグナリングを設定する方法を示します。

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice-signaling vlan 400 dscp 45
```

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声シグナリングを設定する方法を示します。

```
Switch(config-network-policy)# voice-signaling vlan dot1p cos 4
```

関連トピック

network-policy （90 ページ）
network-policy profile（グローバル コンフィギュレーション） （91 ページ）
voice vlan（ネットワークポリシー コンフィギュレーション） （175 ページ）

voicevlan（ネットワークポリシーコンフィギュレーション）

音声アプリケーション タイプのネットワークポリシー プロファイルを作成するには、ネットワークポリシー コンフィギュレーション モードで **voice vlan** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

voice vlan {*vlan-id* [{**cos** *cos-value*|**dscp** *dscp-value*}]|**dot1p** [{**cos** *l2-priority*|**dscp** *dscp*}]|**none**|**untagged**}

構文の説明

vlan-id	（任意）音声トラフィック用の VLAN。指定できる範囲は 1 ～ 4094 です。
cos *cos-value*	（任意）設定された VLAN に対するレイヤ 2 プライオリティ Class of Service（CoS）を指定します。指定できる範囲は 0 ～ 7 です。デフォルト値は 5 です。
dscp *dscp-value*	（任意）設定された VLAN に対する Diffserv コード ポイント（DSCP）値を指定します。指定できる範囲は 0 ～ 63 です。デフォルト値は 46 です。
dot1p	（任意）IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話を設定します。
none	（任意）音声 VLAN に関して IP Phone に指示しません。電話は電話のキーパッドから入力された設定を使用します。
untagged	（任意）タグなしの音声トラフィックを送信するように電話を設定します。これが電話のデフォルトになります。

コマンド デフォルト

音声アプリケーション タイプのネットワークポリシー プロファイルは定義されていません。

デフォルトの CoS 値は、5 です。

デフォルトの DSCP 値は、46 です。

デフォルトのタギング モードは、untagged です。

コマンド モード

ネットワークポリシー プロファイル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

プロファイルを作成し、ネットワークポリシー プロファイル コンフィギュレーション モードを開始するには、**network-policy profile** グローバル コンフィギュレーション コマンドを使用します。

voice アプリケーション タイプは IP Phone 専用であり、対話形式の音声サービスをサポートするデバイスに似ています。通常、これらのデバイスは、展開を容易に行えるようにし、データアプリケーションから隔離してセキュリティを強化するために、別個の VLAN に配置されます。

ネットワークポリシー プロファイル コンフィギュレーション モードの場合、VLAN、Class of Service（CoS）、Diffserv コード ポイント（DSCP）の値、およびタギング モードを指定することで、音声用のプロファイルを作成することができます。

これらのプロファイルの属性は、Link Layer Discovery Protocol for Media Endpoint Devices（LLDP-MED）の network-policy Time Length Value（TLV）に含まれます。

ネットワークポリシー プロファイル コンフィギュレーション モードから特権 EXEC モードに戻る場合は、**exit** コマンドを入力します。

次の例では、プライオリティ 4 の CoS を持つ VLAN 100 用の音声アプリケーション タイプを設定する方法を示します。

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 cos 4
```

次の例では、DSCP 値 34 を持つ VLAN 100 用の音声アプリケーション タイプを設定する方法を示します。

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 dscp 34
```

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声アプリケーション タイプを設定する方法を示します。

```
Switch(config-network-policy)# voice vlan dot1p cos 4
```

関連トピック

network-policy （90 ページ）
network-policy profile（グローバル コンフィギュレーション） （91 ページ）
voice-signaling vlan（ネットワークポリシー コンフィギュレーション） （173 ページ）

wireless ap-manager interface

ワイヤレス AP マネージャ インターフェイスを設定するには、**wireless ap-manager interface** コマンドを使用します。

wireless ap-managerinterface {**TenGigabitEthernet** *interface-number*|**Vlan** *interface-number*}

構文の説明

TenGigabitEthernet *interface-name*	10 ギガビット イーサネット インターフェイスを設定します。値の範囲は 0 ～ 9 です。
Vlan *interface-name*	VLAN を設定します。値の範囲は 1 ～ 4095 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例は、ワイヤレス AP-manager を設定する方法を示しています。

```
Switch# wireless ap-manager interface vlan
<1-4095>  Vlan interface number
```

次の例は、ワイヤレス AP-manager を設定する方法を示しています。

```
Switch# #wireless ap-manager interface vlan 10
```

wireless exclusionlist

除外リストエントリを管理するには、**wireless exclusionlist** グローバル コンフィギュレーション コマンドを使用します。除外リストエントリを削除するには、このコマンドの **no** 形式を使用します。

wireless exclusionlist *mac-addr* **description** *description*
no wireless exclusionlist *mac-addr*

構文の説明

mac-addr	ローカル除外リストエントリのMACアドレス。
description 説明	除外リスト エントリの説明を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、MAC アドレス xxx.xxx.xxx のローカル除外リスト エントリを作成する例を示します。

```
Switch# wireless exclusionlist xxx.xxx.xxx
```

次に、MAC アドレス xxx.xxx.xxx のローカル除外リスト エントリの説明を作成する例を示します。

```
Switch# wireless exclusionlist xxx.xxx.xxx description sample
```

wireless linktest

リンク テスト フレーム サイズおよび送信するフレーム数を設定するには、**wireless linktest** コマンドを使用します。

wireless linktest {**frame-size** *size*|**number-of-frames** *value*}

構文の説明

frame-size *size*	各パケットのリンク テスト フレームのサイズを指定します。値の範囲は 1 ～ 1400 です。
number-of-frames *value*	リンク テストに送信するフレーム数を指定します。値の範囲は 1 ～ 100 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、各フレーム リンクのテスト フレームのサイズを 10 に設定する例を示します。

```
Switch# wireless linktest frame-size 10
```

wireless management interface

インターフェイスのワイヤレス管理パラメータを設定するには、**wireless management interface** グローバル コンフィギュレーション コマンドを使用します。インターフェイスのワイヤレス管理パラメータを削除するには、このコマンドの **no** 形式を使用します。

wireless management interface *interface-name* {**TenGigabitEthernet** *interface-name*|**Vlan** *interface-name*}
no wireless management interface

構文の説明

interface-name	インターフェイス番号
TenGigabitEthernet *interface-name*	10 ギガビット イーサネット インターフェイス番号。値の範囲は 0 ～ 9 です。
Vlan *interface-name*	VLAN インターフェイス番号。値の範囲は 1 ～ 4095 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、ワイヤレス インターフェイスに VLAN 10 を設定する例を示します。

```
Switch# wireless management interface Vlan 10
```

wireless peer-blocking forward-upstream

アップストリーム転送のピアツーピア ブロッキングを設定するには、**wireless peer-blocking forward-upstream** コマンドを使用します。ピアツーピア ブロッキングを削除するには、このコマンドの **no** 形式を使用します。

wireless peer-blocking forward-upstream *interface*{**GigabitEthernet** *interface-number* **TenGigabitEthernet** *interface-number*}
no wireless peer-blocking forward-upstream {**GigabitEthernet** *interface-number* **TenGigabitEthernet** *interface-number*}

構文の説明

GigabitEthernet *interface*	ギガビット イーサネット インターフェイス番号。値の範囲は 0 ～ 9 です。
TenGigabitEthernet *interface*	10 ギガビット イーサネット インターフェイス番号。値の範囲は 0 ～ 9 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、インターフェイスの 10 ギガビット イーサネット インターフェイスについてピアツーピア ブロッキングを設定する例を示します。

```
Switch(config)# wireless peer-blocking forward-upstream TenGigabitEthernet 1/1/4
```

第 III 部

IPv6

IPv6 コマンド

ipv6 flow monitor

このコマンドは、着信または発信トラフィックを分析するためにインターフェイスに割り当てることで、作成済みのフロー モニタをアクティブにします。

以前に作成したフロー モニタをアクティブにするには、**ipv6flowmonitor** コマンドを使用します。フロー モニタを非アクティブにするには、このコマンドの **no** 形式を使用します。

ipv6 flow monitor *ipv6-monitor-name* [**sampler** *ipv6-sampler-name*] {**input**|**output**}
no ipv6 flow monitor *ipv6-monitor-name* [**sampler** *ipv6-sampler-name*] {**input**|**output**}

構文の説明

ipv6-monitor-name	着信または発信トラフィックを分析するためにインターフェイスに割り当てることで、作成済みのフロー モニタをアクティブにします。
sampler *ipv6-sampler-name*	フロー モニタ サンプラーを適用します。
input	入力トラフィックにフロー モニタを適用します。
output	出力トラフィックにフロー モニタを適用します。

コマンド デフォルト

IPv6 フロー モニタは、インターフェイスに割り当てられるまでアクティブになりません。

コマンド モード

インターフェイス コンフィギュレーション。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ポート チャネル インターフェイスには NetFlow モニタを接続できません。サービス モジュールの両方のインターフェイスが EtherChannel の一部である場合、両方の物理インターフェイスに監視を接続する必要があります。

次に、フロー モニタをインターフェイスに適用する例を示します。

```
Switch(config)# interface gigabitethernet 1/1/2
Switch(config-if)# ip flow monitor FLOW-MONITOR-1 input
Switch(config-if)# ip flow monitor FLOW-MONITOR-2 output
Switch(config-if)# end
```

ipv6 traffic-filter

このコマンドは、IPv6 トラフィック フィルタを有効にします。

インターフェイスでの IPv6 トラフィックのフィルタリングを有効にするには、**ipv6traffic-filter** コマンドを使用します。インターフェイスでの IPv6 トラフィックのフィルタリングを無効にするには、このコマンドの **no** 形式を使用します。

インターフェイス上で IPv6 トラフィックをフィルタ処理するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ipv6 traffic-filter** インターフェイス コンフィギュレーション コマンドを使用します。フィルタリングできるトラフィックのタイプと方向は、スイッチスタックで稼働するフィーチャ セットによって異なります。インターフェイスでの IPv6 トラフィックのフィルタリングを無効にするには、このコマンドの **no** 形式を使用します。

ipv6 traffic-filter [web] *acl-name*
no ipv6 traffic-filter [web]

構文の説明

web	（任意）WLAN Web ACL の IPv6 アクセス名を指定します。
acl-name	IPv6 アクセス名を指定します。

コマンド デフォルト

インターフェイス上での IPv6 トラフィックのフィルタリングは設定されません。

コマンド モード

wlan

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6 {default | vlan}** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

物理インターフェイス（レイヤ 2 またはレイヤ 3 ポート）、レイヤ 3 ポート チャネル、またはスイッチ仮想インターフェイス（SVI）で **ipv6 traffic-filter** コマンドを使用できます。

ACL をレイヤ 3 インターフェイス（ポート ACL）の発信または着信トラフィックに、またはレイヤ 2 インターフェイス（ルータ ACL）の着信トラフィックに適用できます。

いずれかのポート ACL（IPv4、IPv6、または MAC）がインターフェイスに適用された場合、そのポート ACL を使用してパケットをフィルタ処理し、ポート VLAN の SVI に適用されたルータ ACL は無視されます。**any**

次に、インターフェイスで IPv6 トラフィックをフィルタ処理する例を示します。

```
Switch(config-wlan)# ipv6 traffic-filter TestDocTrafficFilter
```

show wireless ipv6 statistics

このコマンドは、IPv6 パケット カウンタの統計を表示するために使用します。

IPv6 パケット カウンタの統計を表示するには、**show wireless ipv6 statistics** コマンドを使用します。

show wireless ipv6 statistics

コマンド デフォルト

なし。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、IPv6 パケット カウンタの統計の概要を表示する例を示します。

```
Switch# show wireless ipv6 statistics
NS Forwarding to wireless clients               : Enabled

RS count                                        : 0
RA count                                        : 0
NS count                                        : 0
NA count                                        : 0
Other NDP packet count                          : 0
-----------------------------------------------------
Non-IPv6 packets count                          : 0
Non-IPv6 Multicast Destination MAC packet count : 0
Invalid length packets count                    : 0
Null packets count                              : 0
Invalid Source MAC packets count                : 0
-----------------------------------------------------
TCP packets count                               : 0
UDP packets count                               : 0
Fragmented packets count                        : 0
No next header packets count                    : 0
Other type packets count                        : 0
-----------------------------------------------------
Total packets count                             : 0
-----------------------------------------------------
Blocked RA packets count                        : 0
Blocked NS packets count                        : 0
```

第 IV 部

レイヤ 2/3

レイヤ 2/3 コマンド

channel-group

EtherChannel グループにイーサネット ポートを割り当てたり、EtherChannel モードをイネーブルにしたり、この両方を行うには、インターフェイス コンフィギュレーション モードで **channel-group** コマンドを使用します。EtherChannel グループからイーサネット ポートを削除するには、このコマンドの **no** 形式を使用します。

channel-group { **auto** | *channel-group-number* **mode** {**active**|**auto** [**non-silent**]|**desirable** [**non-silent**]|**on**|**passive**}}
no channel-group

構文の説明

auto	個々のポート インターフェイスの auto-LAG 機能をイネーブルにします。 デフォルトでは、auto-LAG 機能は各ポート上でイネーブルになっています。
channel-group-number	チャネル グループ番号。指定できる範囲は 1 ～ 128 です。
mode	EtherChannel モードを指定します。
active	無条件に Link Aggregation Control Protocol（LACP）をイネーブルにします。
auto	Port Aggregation Protocol（PAgP）装置が検出された場合に限り、PAgP をイネーブルにします。
non-silent	（任意）PAgP 対応のパートナーに接続されたとき、インターフェイスを非サイレント動作に設定します。他の装置からのトラフィックが予想されている場合に PAgP モードで **auto** または **desirable** キーワードとともに使用されます。
desirable	無条件に PAgP をイネーブルにします。

on	オン モードをイネーブルにします。
passive	LACP装置が検出された場合に限り、LACPをイネーブルにします。

コマンド デフォルト

チャネル グループは割り当てることができません。

モードは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

レイヤ 2 の EtherChannel では、チャネル グループに最初の物理ポートが追加されると、**channel-group** コマンドがポートチャネルインターフェイスを自動的に作成します。ポートチャネル インターフェイスを手動で作成する場合は、グローバル コンフィギュレーション モードで **interface port-channel** コマンドを使用する必要はありません。最初にポートチャネル インターフェイスを作成する場合は、*channel-group-number* を *port-channel-number* と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポート チャネルを作成します。

EtherChannelを設定した後、ポートチャネルインターフェイスに加えられた設定の変更は、そのポートチャネルインターフェイスに割り当てられたすべての物理ポートに適用されます。物理ポートに適用された設定の変更は、設定を適用したポートだけに有効です。EtherChannel 内のすべてのポートのパラメータを変更するには、ポートチャネルインターフェイスに対してコンフィギュレーション コマンドを適用します。たとえば、spanning-tree コマンドを使用して、レイヤ 2 EtherChannel をトランクとして設定します。

active モードは、ポートをネゴシエーション ステートにします。このステートでは、ポートは LACP パケットを送信することによって、他のポートとのネゴシエーションを開始します。チャネルは、active モードまたは passive モードの別のポート グループで形成されます。

auto モードは、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。チャネルは、desirable モードの別のポート グループでだけ形成されます。auto がイネーブルの場合、サイレント動作がデフォルトになります。

desirable モードは、ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、他のポートとのネゴシエーションを開始します。EtherChannel は、desirable モードまたは auto モードの別のポート グループで形成されます。desirable がイネーブルの場合、サイレント動作がデフォルトになります。

auto モードまたは desirable モードとともに non-silent を指定しなかった場合は、サイレントが指定されているものと見なされます。サイレント モードを設定するのは、PAgP 非対応で、かつほとんどパケットを送信しない装置にスイッチを接続する場合です。サイレント パートナーの例は、トラフィックを生成しないファイル サーバ、またはパケット アナライザなどです。この場合、物理ポート上で稼働している PAgP は、そのポートを動作可能にしません。ただし、PAgP は動作可能で、チャネル グループにポートを付与したり、伝送用ポートを使用したりできます。リンクの両端はサイレントに設定することはできません。

on モードでは、使用可能な EtherChannel が存在するのは、両方の接続ポート グループが on モードになっている場合だけです。

注意 on モードの使用には注意が必要です。これは手動の設定であり、EtherChannel の両端のポートには、同一の設定が必要です。グループの設定を誤ると、パケット損失またはスパニングツリー ループが発生することがあります。

passive モードは、ポートをネゴシエーション ステートにします。この場合、ポートは受信した LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。チャネルは、active モードの別のポート グループでだけ形成されます。

EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP および LACP を実行している EtherChannel グループは、同一のスイッチ、またはスタックにある異なるスイッチ上で共存できます（クロススタック構成ではできません）。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。

channel-protocol インターフェイス コンフィギュレーション コマンドを使用してプロトコルを設定した場合、設定値は、**channel-group** インターフェイス コンフィギュレーション コマンドによっては優先されません。

アクティブまたはまだアクティブでない EtherChannel メンバとなっているポートを、IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x 認証はイネーブルになりません。

セキュア ポートを EtherChannel の一部として、または EtherChannel ポートをセキュア ポートとしては設定しないでください。

設定の注意事項の一覧については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

注意 物理 EtherChannel ポート上でブリッジ グループを割り当てることは、ループが発生する原因になるため、行わないでください。

この例では、スタック内の 1 つのスイッチに EtherChannel を設定する例を示します。VLAN 10 のスタティックアクセス ポート 2 つを PAgP モード desirable であるチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range GigabitEthernet 2/0/1 - 2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end
```

この例では、スタック内の 1 つのスイッチに EtherChannel を設定する例を示します。VLAN 10 のスタティックアクセス ポート 2 つを LACP モード active であるチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range GigabitEthernet 2/0/1 - 2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

次の例では、スイッチ スタックのクロススタック EtherChannel を設定する方法を示します。LACP パッシブ モードを使用して、VLAN 10 内のスタティックアクセス ポートとしてスタック メンバ 2 のポートを 2 つ、スタック メンバ 3 のポートを 1 つチャネル 5 に割り当てます。

```
Switch# configure terminal
Switch(config)# interface range GigabitEthernet 2/0/4 - 5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode passive
Switch(config-if-range)# exit
Switch(config)# interface GigabitEthernet 3/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# channel-group 5 mode passive
Switch(config-if)# exit
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連トピック

channel-protocol （197 ページ）
interface port-channel （214 ページ）
show etherchannel （230 ページ）
show lacp （233 ページ）
show pagp （238 ページ）

channel-protocol

ポート上で使用されるプロトコルを制限してチャネリングを管理するには、インターフェイス コンフィギュレーション モードで **channel-protocol** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

channel-protocol {**lacp**|**pagp**}
no channel-protocol

構文の説明

lacp	Link Aggregation Control Protocol（LACP）で EtherChannel を設定します。
pagp	Port Aggregation Protocol（PAgP）で EtherChannel を設定します。

コマンド デフォルト

EtherChannel に割り当てられているプロトコルはありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

channel-protocol コマンドは、チャネルを LACP または PAgP に制限するためだけに使用します。**channel-protocol** コマンドを使用してプロトコルを設定する場合、設定は **channel-group** インターフェイス コンフィギュレーション コマンドで上書きされることはありません。

channel-group インターフェイス コンフィギュレーション コマンドは、EtherChannel のパラメータ設定に使用してください。また、**channel-group** コマンドは、EtherChannel に対しモードを設定することもできます。

EtherChannel グループ上で、PAgP および LACP モードの両方をイネーブルにすることはできません。

PAgP と LACP には互換性がありません。両方ともチャネルの終端は同じプロトコルを使用する必要があります。

クロススタック構成の PAgP を設定できません。

次の例では、EtherChannel を管理するプロトコルとして LACP を指定する方法を示します。

```
Switch(config-if)# channel-protocol lacp
```

設定を確認するには、**show etherchannel** [*channel-group-number*] **protocol** 特権 EXEC コマンドを入力します。

関連トピック

channel-group （193 ページ）
show etherchannel （230 ページ）

clear lacp

Link Aggregation Control Protocol（LACP）チャネル グループ カウンタをクリアするには、特権 EXEC モードで **clear lacp** コマンドを使用します。

clear lacp [*channel-group-number*] **counters**

構文の説明

channel-group-number	（任意）チャネル グループ番号。指定できる範囲は 1 ～ 128 です。
counters	トラフィック カウンタをクリアします。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

すべてのカウンタをクリアするには、**clear lacp counters** コマンドを使用します。また、指定のチャネル グループのカウンタのみをクリアするには、**clear lacp** *channel-group-number* **counters** コマンドを使用します。

次の例では、すべてのチャネル グループ情報をクリアする方法を示します。

```
Switch# clear lacp counters
```

次の例では、グループ 4 の LACP トラフィックのカウンタをクリアする方法を示します。

```
Switch# clear lacp 4 counters
```

情報が削除されたことを確認するには、**show lacp counters** または **show lacp** *channel-group-number* **counters** 特権 EXEC コマンドを入力します。

関連トピック

show lacp （233 ページ）

clear pagp

Port Aggregation Protocol（PAgP）チャネル グループ情報をクリアするには、特権 EXEC モードで **clear pagp** コマンドを使用します。

clear pagp [*channel-group-number*] **counters**

構文の説明

channel-group-number	（任意）チャネル グループ番号。指定できる範囲は 1 ～ 128 です。
counters	トラフィック カウンタをクリアします。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

すべてのカウンタをクリアするには、**clear pagp counters** コマンドを使用します。また、**clear pagp** *channel-group-number* **counters** コマンドを使用すると、指定したチャネル グループのカウンタのみをクリアできます。

次の例では、すべてのチャネル グループ情報をクリアする方法を示します。

```
Switch# clear pagp counters
```

次の例では、グループ 10 の PAgP トラフィックのカウンタをクリアする方法を示します。

```
Switch# clear pagp 10 counters
```

情報が削除されたことを確認するには、**show pagp** 特権 EXEC コマンドを入力します。

関連トピック

debug pagp （207 ページ）
show pagp （238 ページ）

clear spanning-tree counters

スパニング ツリーのカウンタをクリアするには、特権 EXEC モードで **clear spanning-tree counters** コマンドを使用します。

clear spanning-tree counters ［**interface** *interface-id*］

構文の説明

interface *interface-id*	（任意）指定のインターフェイスのスパニングツリー カウンタをすべてクリアします。有効なインターフェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。 指定できる VLAN 範囲は 1 ～ 4094 です。 ポート チャネル範囲は 1 ～ 128 です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

interface-id が指定されていない場合は、すべてのインターフェイスのスパニングツリー カウンタがクリアされます。

次の例では、すべてのインターフェイスのスパニングツリー カウンタをクリアする方法を示します。

```
Switch# clear spanning-tree counters
```

関連トピック

clear spanning-tree detected-protocols （202 ページ）
debug spanning-tree （212 ページ）

clear spanning-tree detected-protocols

スイッチでプロトコル移行プロセスを再開して、強制的にネイバーと再ネゴシエーションするには、特権 EXEC モードで **clear spanning-tree detected-protocols** コマンドを使用します。

clear spanning-tree detected-protocols [**interface** *interface-id*]

構文の説明

interface *interface-id*	（任意）指定されたインターフェイスでプロトコル移行プロセスを再開します。有効なインターフェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。 指定できる VLAN 範囲は 1 ～ 4094 です。 ポート チャネル範囲は 1 ～ 128 です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

Rapid Per-VLAN Spanning-Tree Plus（Rapid PVST+）プロトコルまたは Multiple Spanning Tree Protocol（MSTP）が稼働するスイッチは、組み込み済みのプロトコル移行方式をサポートしています。それによって、スイッチはレガシー IEEE 802.1D スイッチと相互に動作できるようになります。Rapid PVST+ または MSTP スイッチが、プロトコルのバージョンが 0 に設定されているレガシー IEEE 802.1D コンフィギュレーション ブリッジ プロトコル データ ユニット（BPDU）を受信した場合、そのスイッチはそのポートで IEEE 802.1D BPDU だけを送信します。マルチ スパニング ツリー（MST）スイッチが、レガシー BPDU、別のリージョンに対応する MST BPDU（バージョン 3）、または高速スパニング ツリー（RST）BPDU（バージョン 2）を受信したときは、そのポートがリージョンの境界にあることを検知します。

スイッチは、IEEE 802.1D BPDU を受信しなくなった場合であっても、自動的には Rapid PVST+ モードまたは MSTP モードには戻りません。これは、レガシー スイッチが指定スイッチでなければ、リンクから削除されたかどうかを学習できないためです。この状況では、**clear spanning-tree detected-protocols** コマンドを使用します。

次の例では、ポートでプロトコル移行プロセスを再開する方法を示します。

```
Switch# clear spanning-tree detected-protocols interface gigabitethernet2/0/1
```

関連トピック

clear spanning-tree detected-protocols （202 ページ）
debug spanning-tree （212 ページ）

debug etherchannel

EtherChannel のデバッグをイネーブルにするには、特権 EXEC モードで **debug etherchannel** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug etherchannel [{**all** |**detail** |**error** |**event** |**idb** }]
no debug etherchannel [{**all** |**detail** |**error** |**event** |**idb** }]

構文の説明

all	（任意）EtherChannel デバッグ メッセージをすべて表示します。
detail	（任意）EtherChannel デバッグ メッセージの詳細を表示します。
error	（任意）EtherChannel エラー デバッグ メッセージを表示します。
event	（任意）EtherChannel イベント メッセージを表示します。
idb	（任意）PAgP インターフェイス記述子ブロック デバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

undebug etherchannel コマンドは、**no debug etherchannel** コマンドと同じです。

（注） **linecard** キー ワードは、コマンドラインのヘルプに表示されますが、サポートされていません。

あるスタック上でデバッグをイネーブルにした場合、アクティブ スイッチでのみイネーブルになります。スタンバイ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してアクティブ スイッチからセッションを開始します。スタンバイ スイッチのコマンドライン プロンプトで **debug** コマンドを入力します。

アクティブ スイッチで最初にセッションを開始せずにスイッチ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次の例では、すべての EtherChannel デバッグ メッセージを表示する方法を示します。

```
Switch# debug etherchannel all
```

次の例では、EtherChannel イベント関連のデバッグ メッセージを表示する方法を示します。

```
Switch# debug etherchannel event
```

関連トピック

show etherchannel （230 ページ）

debug lacp

Link Aggregation Control Protocol（LACP）アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug lacp** コマンドを使用します。LACP のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug lacp [{**all** |**event** |**fsm** |**misc** |**packet**}]
no debug lacp [{**all** |**event** |**fsm** |**misc** |**packet**}]

構文の説明

all	（任意）LACP デバッグ メッセージをすべて表示します。
event	（任意）LACP イベント デバッグ メッセージを表示します。
fsm	（任意）LACP有限状態マシン内の変更に関するメッセージを表示します。
misc	（任意）各種 LACP デバッグ メッセージを表示します。
packet	（任意）受信および送信 LACP 制御パケットを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

undebug etherchannel コマンドは、**no debug etherchannel** コマンドと同じです。

あるスタック上でデバッグをイネーブルにした場合、アクティブ スイッチでのみイネーブルになります。スタンバイ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してアクティブ スイッチからセッションを開始します。スタンバイ スイッチのコマンドライン プロンプトで **debug** コマンドを入力します。

アクティブ スイッチで最初にセッションを開始せずにスイッチ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次の例では、すべての LACP デバッグ メッセージを表示する方法を示します。

```
Switch# debug LACP all
```

次の例では、LACPイベントに関連するデバッグ メッセージを表示する方法を示します。

```
Switch# debug LACP event
```

debug pagp

Port Aggregation Protocol（PAgP）アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug pagp** コマンドを使用します。PAgP のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug pagp [{**all** |**dual-active** |**event** |**fsm** |**misc** |**packet**}]
no debug pagp [{**all** |**dual-active** |**event** |**fsm** |**misc** |**packet**}]

構文の説明

all	（任意）PAgP デバッグ メッセージをすべて表示します。
dual-active	（任意）デュアル アクティブ検出メッセージを表示します。
event	（任意）PAgP イベント デバッグ メッセージを表示します。
fsm	（任意）PAgP 有限状態マシン内の変更に関するメッセージを表示します。
misc	（任意）各種 PAgP デバッグ メッセージを表示します。
packet	（任意）送受信 PAgP 制御パケットを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

undebug pagp コマンドは、**no debug pagp** コマンドと同じです。

あるスタック上でデバッグをイネーブルにした場合、アクティブ スイッチでのみイネーブルになります。スタンバイ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してアクティブ スイッチからセッションを開始します。スタンバイ スイッチのコマンドライン プロンプトで **debug** コマンドを入力します。

アクティブ スイッチで最初にセッションを開始せずにスイッチ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次の例では、すべての PAgP デバッグ メッセージを表示する方法を示します。

```
Switch# debug pagp all
```

次の例では、PAgP イベントに関連するデバッグ メッセージを表示する方法を示します。

```
Switch# debug pagp event
```

debug platform pm

プラットフォーム依存ポート マネージャ ソフトウェア モジュールのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform pm** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug platform pm
{all|counters|errdisable|fec|if-numbers|l2-control|link-status|platform|pm-spi|pm-vectors [detail]|ses|vlans}
no debug platform pm
{all|counters|errdisable|fec|if-numbers|l2-control|link-status|platform|pm-spi|pm-vectors [detail]|ses|vlans}

構文の説明

all	すべてのポート マネージャ デバッグ メッセージを表示します。
counters	リモート プロシージャ コール（RPC）デバッグ メッセージのカウンタを表示します。
errdisable	error-disabled 関連イベント デバッグ メッセージを表示します。
fec	転送等価クラス（FEC）プラットフォーム関連イベント デバッグ メッセージを表示します。
if-numbers	インターフェイス番号移動イベントデバッグ メッセージを表示します。
l2-control	レイヤ 2 制御インフラ デバッグ メッセージを表示します。
link-status	インターフェイス リンク検出イベント デバッグ メッセージを表示します。
platform	ポート マネージャ関数イベント デバッグ メッセージを表示します。
pm-spi	ポート マネージャ ステートフル パケット インスペクション（SPI）イベント デバッグ メッセージを表示します。
pm-vectors	ポートマネージャ ベクトル関連イベントデバッグ メッセージを表示します。
detail	（任意）ベクトル関数の詳細を表示します。
ses	サービス拡張シェルフ（SES）関連イベント デバッグ メッセージを表示します。

vlans	VLAN 作成および削除イベント デバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

undebug platform pm コマンドは、**no debug platform pm** コマンドと同じです。

あるスタック上でデバッグをイネーブルにした場合、アクティブ スイッチでのみイネーブルになります。スタンバイ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してアクティブ スイッチからセッションを開始します。スタンバイ スイッチのコマンドライン プロンプトで **debug** コマンドを入力します。

アクティブ スイッチで最初にセッションを開始せずにスイッチ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次に、VLAN の作成および削除に関するデバッグ メッセージを表示する例を示します。

```
Switch# debug platform pm vlans
```

debug platform udld

プラットフォーム依存の単方向リンク検出（UDLD）ソフトウェアのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform udld** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug platform udld [{**error**|**event**}] [**switch** *switch-number*]
no debug platform udld [{**error**|**event**}] [**switch** *switch-number*]

構文の説明

error	（任意）エラー条件デバッグ メッセージを表示します。
event	（任意）UDLD 関連プラットフォーム イベント デバッグ メッセージを表示します。
switch *switch-number*	（任意）指定されたスタック メンバの UDLD デバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

undebug platform udld コマンドは、**no debug platform udld** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、アクティブ スイッチでのみイネーブルになります。スタック メンバのデバッグを有効にする場合は、**session** *switch-number* EXEC コマンドを使用して、アクティブ スイッチからのセッションを開始できます。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。

debug spanning-tree

スパニングツリー アクティビティのデバッグをイネーブルにするには、EXEC モードで **debug spanning-tree** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug spanning-tree {**all** |**backbonefast** |**bpdu** |**bpdu-opt** |**config** |**etherchannel** |**events** |**exceptions** |**general** |**ha** |**mstp** |**pvst+**|**root** |**snmp** |**synchronization** |**switch** |**uplinkfast**}
no debug spanning-tree {**all** |**backbonefast** |**bpdu** |**bpdu-opt** |**config** |**etherchannel** |**events** |**exceptions** |**general** |**mstp** |**pvst+**|**root** |**snmp** |**synchronization** |**switch** |**uplinkfast**}

構文の説明

all	スパニングツリーのデバッグ メッセージをすべて表示します。
backbonefast	BackboneFast イベント デバッグ メッセージを表示します。
bpdu	スパニングツリー ブリッジ プロトコル データ ユニット（BPDU）デバッグ メッセージを表示します。
bpdu-opt	最適化された BPDU 処理デバッグ メッセージを表示します。
config	スパニングツリー設定変更デバッグ メッセージを表示します。
etherchannel	EtherChannel サポート デバッグ メッセージを表示します。
events	スパニングツリー トポロジ イベント デバッグ メッセージを表示します。
exceptions	スパニングツリー例外デバッグ メッセージを表示します。
general	一般的なスパニングツリー アクティビティ デバッグ メッセージを表示します。
ha	高可用性スパニングツリー デバッグ メッセージを表示します。
mstp	Multiple Spanning Tree Protocol（MSTP）イベントをデバッグします。
pvst+	Per VLAN Spanning-Tree Plus（PVST+）イベント デバッグ メッセージを表示します。

root	スパニングツリー ルート イベント デバッグ メッセージを表示します。
snmp	スパニングツリーの Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）処理デバッグ メッセージを表示します。
switch	スイッチ シム コマンド デバッグ メッセージを表示します。このシムは、一般的なスパニングツリー プロトコル（STP）コードと、各スイッチ プラットフォーム固有コードとの間のインターフェイスとなるソフトウェア モジュールです。
synchronization	スパニングツリー同期イベント デバッグ メッセージを表示します。
uplinkfast	UplinkFast イベント デバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

undebug spanning-tree コマンドは、**no debug spanning-tree** コマンドと同じです。

あるスタック上でデバッグをイネーブルにした場合、アクティブ スイッチでのみイネーブルになります。スタンバイ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してアクティブ スイッチからセッションを開始します。スタンバイ スイッチのコマンドライン プロンプトで **debug** コマンドを入力します。

アクティブ スイッチで最初にセッションを開始せずにスイッチ スイッチ でデバッグをイネーブルにするには、特権 EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次の例では、すべてのスパニングツリー デバッグ メッセージを表示する方法を示します。

```
Switch# debug spanning-tree all
```

関連トピック

clear spanning-tree counters （201 ページ）
clear spanning-tree detected-protocols （202 ページ）

interface port-channel

ポート チャネルにアクセスするか、またはポート チャネルを作成するには、グローバル コンフィギュレーション モードで **interface port-channel** コマンドを使用します。ポート チャネルを削除するには、このコマンドの **no** 形式を使用します。

interface port-channel *port-channel-number*
no interface port-channel

構文の説明

port-channel-number	チャネル グループ番号。指定できる範囲は 1 ～ 128 です。

コマンド デフォルト

ポート チャネル論理インターフェイスは定義されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

レイヤ 2 EtherChannel では、物理ポートをチャネル グループに割り当てる前にポートチャネル インターフェイスを作成する必要はありません。代わりに、**channel-group** インターフェイス コンフィギュレーション コマンドを使用できます。このコマンドでは、チャネル グループが最初の物理ポートを獲得すると、ポートチャネル論理インターフェイスが自動的に作成されます。最初にポートチャネル インターフェイスを作成する場合は、*channel-group-number* を *port-channel-number* と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポート チャネルを作成します。

チャネル グループ内の 1 つのポート チャネルだけが許可されます。

interface port-channel コマンドを使用する場合は、次の注意事項に従ってください。

- Cisco Discovery Protocol（CDP）を使用する場合には、これを物理ポートで設定してください。ポートチャネル インターフェイスでは設定できません。
- EtherChannel のアクティブ メンバであるポートを IEEE 802.1x ポートとしては設定しないでください。まだアクティブになっていない EtherChannel のポートで IEEE 802.1x をイネーブルにしても、ポートは EtherChannel に加入しません。

設定の注意事項の一覧については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

次の例では、ポートチャネル番号 5 でポートチャネル インターフェイスを作成する方法を示します。

```
Switch(config)# interface port-channel 5
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel** *channel-group-number* **detail** 特権 EXEC コマンドを入力します。

関連トピック

channel-group （193 ページ）
show etherchannel （230 ページ）

lacp max-bundle

ポートチャネルで許可されるアクティブLACPポートの最大数を定義するには、インターフェイス コンフィギュレーション モードで **lacp max-bundle** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp max-bundle *max_bundle_number*
no lacp max-bundle

構文の説明

max_bundle_number	ポート チャネルのアクティブ LACP ポートの最大数。指定できる範囲は 1 ～ 8 です。デフォルト値は 8 です。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

LACP チャネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 個をアクティブに、最大 8 個をホットスタンバイ モードにできます。LACP チャネル グループに9つ以上のポートがある場合、リンクの制御側終端にあるスイッチは、ポートプライオリティを使用して、チャネルにバンドルするポートおよびホットスタンバイ モードに置くポートを判別します。他のスイッチ上のポートプライオリティ（リンクの非制御側終端）は無視されます。

lacp max-bundle コマンドには、**port-channel min-links** コマンドで指定される数より大きい数を指定する必要があります。

ホットスタンバイ モード（ポート ステート フラグの H で出力に表示）にあるポートを判断するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

次に、ポート チャネル 2 で最大 5 個のアクティブ LACP ポートを指定する例を示します。

```
Switch(config)# interface port-channel 2
Switch(config-if)# lacp max-bundle 5
```

関連トピック

port-channel min-links （229 ページ）

lacp port-priority

Link Aggregation Control Protocol（LACP）のポート プライオリティを設定するには、インターフェイス コンフィギュレーション モードで **lacp port-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp port-priority *priority*
no lacp port-priority

構文の説明

priority	LACP のポート プライオリティ。指定できる範囲は 1 ～ 65535 です。

コマンド デフォルト

デフォルトは 32768 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

lacp port-priority インターフェイス コンフィギュレーション コマンドは、LACP チャネル グループに 9 つ以上のポートがある場合、バンドルされるポートと、ホットスタンバイ モードに置かれるポートを判別します。

LACP チャネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。

ポート プライオリティの比較では、数値が小さいほどプライオリティが高くなります。LACP チャネル グループに 9 つ以上のポートがある場合、LACP ポート プライオリティの数値が小さい（つまり、高いプライオリティ値の）8 つのポートがチャネル グループにバンドルされ、それより低いプライオリティのポートはホットスタンバイ モードに置かれます。LACP ポート プライオリティが同じポートが 2 つ以上ある場合（たとえば、そのいずれもデフォルト設定の 65535 に設定されている場合）、ポート番号の内部値によりプライオリティが決定されます。

（注） LACP リンクを制御する スイッチ 上にポートがある場合に限り、LACP ポート プライオリティは有効です。リンクを制御する スイッチ の判別については、**lacp system-priority** グローバル コンフィギュレーション コマンドを参照してください。

LACP ポート プライオリティおよび内部ポート番号値を表示するには、**show lacp internal** 特権 EXEC コマンドを使用します。

物理ポート上での LACP の設定については、このリリースに対応する構成ガイドを参照してください。

次の例では、ポートで LACP ポート プライオリティを設定する方法を示します。

```
Switch# interface gigabitethernet2/0/1
Switch(config-if)# lacp port-priority 1000
```

設定を確認するには、**show lacp** [*channel-group-number*] **internal** 特権 EXEC コマンドを入力します。

関連トピック

channel-group （193 ページ）
lacp system-priority （219 ページ）
show lacp （233 ページ）

lacp system-priority

Link Aggregation Control Protocol（LACP）のシステム プライオリティを設定するには、スイッチのグローバル コンフィギュレーション モードで **lacp system-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp system-priority *priority*
no lacp system-priority

構文の説明

priority	LACP のシステム プライオリティ。指定できる範囲は 1 ～ 65535 です。

コマンド デフォルト

デフォルトは 32768 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

lacp system-priority コマンドでは、ポート プライオリティを制御する LACP リンクのスイッチが判別されます。

LACP チャネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。LACP チャネル グループに 9 つ以上のポートがある場合、リンクの制御側終端にあるスイッチは、ポート プライオリティを使用して、チャネルにバンドルするポートおよびホットスタンバイ モードに置くポートを判別します。他のスイッチ上のポート プライオリティ（リンクの非制御側終端）は無視されます。

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。したがって、LACP システム プライオリティの数値が小さい（プライオリティ値の高い）システムが制御システムとなります。どちらのスイッチも同じ LACP システム プライオリティである場合（たとえば、どちらもデフォルト設定の 32768 が設定されている場合）、LACP システム ID（スイッチの MAC アドレス）により制御するスイッチが判別されます。

lacp system-priority コマンドは、スイッチ上のすべての LACP EtherChannel に適用されます。

ホットスタンバイ モード（ポート ステート フラグの H で出力に表示）にあるポートを判断するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

次の例では、LACP のシステム プライオリティを設定する方法を示します。

```
Switch(config)# lacp system-priority 20000
```

設定を確認するには、**show lacp sys-id** 特権 EXEC コマンドを入力します。

関連トピック

channel-group （193 ページ）
lacp port-priority （217 ページ）
show lacp （233 ページ）

pagp learn-method

EtherChannelポートから受信した着信パケットの送信元アドレスを学習するには、インターフェイス コンフィギュレーション モードで**pagp learn-method** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pagp learn-method {**aggregation-port**|**physical-port**}
no pagp learn-method

構文の説明

aggregation-port	論理ポート チャネルでのアドレス ラーニングを指定します。スイッチ は、EtherChannelのいずれかのポートを使用して送信元にパケットを送信します。この設定は、デフォルトです。集約ポート ラーニングの場合、どの物理ポートにパケットが届くかは重要ではありません。
physical-port	EtherChannel 内の物理ポートでのアドレス ラーニングを指定します。スイッチ は、送信元アドレスを学習したEtherChannel内の同じポートを使用して送信元へパケットを送信します。チャネルのもう一方の終端では、特定の宛先 MAC または IP アドレスに対してチャネル内の同じポートが使用されます。

コマンド デフォルト

デフォルトは、aggregation-port（論理ポート チャネル）です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

学習方式は、リンクの両端で同一の設定にする必要があります。

コマンドライン インターフェイス（CLI）で**physical-port** キーワードが指定された場合でも、スイッチがサポートするのは集約ポートでのアドレス ラーニングのみです。**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドは スイッチ のハードウェアには影響を及ぼしませんが、物理ポートによるアドレス ラーニングのみをサポートしているデバイスと PAgP の相互運用性を確保するために必要です。

スイッチ のリンク パートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して物理ポート ラーナーとして スイッチ を設定することを推奨します。また、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用して、送信元MACアドレスに基づいて負荷分散方式を設定することを推奨します。**pagp learn-method** インターフェイス コンフィギュレーション コマンドは、このような場合にのみ使用してください。

次の例では、EtherChannel 内の物理ポート上のアドレスを学習するように学習方式を設定する方法を示します。

```
Switch(config-if)# pagp learn-method physical-port
```

次の例では、EtherChannel 内のポート チャネル上のアドレスを学習するように学習方式を設定する方法を示します。

```
Switch(config-if)# pagp learn-method aggregation-port
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp** *channel-group-number* **internal** 特権 EXEC コマンドを入力します。

関連トピック

pagp port-priority （223 ページ）
show pagp （238 ページ）

pagp port-priority

EtherChannel を経由してすべての Port Aggregation Protocol（PAgP）トラフィックが送信されるポートを選択するには、インターフェイス コンフィギュレーション モードで **pagp port-priority** コマンドを使用します。EtherChannel で使用されていないすべてのポートがホットスタンバイ モードにあり、現在選択されているポートやリンクに障害が発生した場合、これらのポートは稼働状態にできます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pagp port-priority *priority*
no pagp port-priority

構文の説明

priority	プライオリティ番号。有効な範囲は 0 ～ 255 です。

コマンド デフォルト

デフォルト値は 128 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

同じ EtherChannel 内で動作可能でメンバーシップを持つ物理ポートの中で最も高いプライオリティを持つポートが、PAgP 送信用として選択されます。

コマンドライン インターフェイス（CLI）で **physical-port** キーワードが指定された場合でも、スイッチがサポートするのは集約ポートでのアドレス ラーニングのみです。**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドは スイッチ のハードウェアには影響を及ぼしませんが、Catalyst 1900 スイッチなど、物理ポートによるアドレス ラーニングのみをサポートするデバイスと PAgP の相互運用性を確保するために必要です。

スイッチ のリンク パートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して物理ポート ラーナーとして スイッチ を設定することを推奨します。また、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用して、送信元 MAC アドレスに基づいて負荷分散方式を設定することを推奨します。**pagp learn-method** インターフェイス コンフィギュレーション コマンドは、このような場合にのみ使用してください。

次の例では、ポート プライオリティを 200 に設定する方法を示します。

```
Switch(config-if)# pagp port-priority 200
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp** *channel-group-number* **internal** 特権 EXEC コマンドを入力します。

関連トピック

- pagp learn-method （221 ページ）
- port-channel load-balance （225 ページ）
- show pagp （238 ページ）

port-channel load-balance

EtherChannelのポート間での負荷分散方式を設定するには、グローバル コンフィギュレーション モードで**port-channel load-balance** コマンドを使用します。ロードバランシング メカニズムをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel load-balance {**dst-ip**|**dst-mac**| **dst-mixed-ip-port**| **dst-port**| **extended**|**src-dst-ip**|**src-dst-mac**| **src-dst-mixed-ip-port**| **src-dst-port**|**src-ip**|**src-mac**| **src-mixed-ip-port**| **src-port**}
no port-channel load-balance

構文の説明

dst-ip	宛先ホストの IP アドレスに基づいた負荷分散を指定します。
dst-mac	宛先ホストの MAC アドレスに基づいた負荷分散を指定します。同一の宛先に対するパケットは同一のポートに送信され、異なる宛先のパケットはチャネルの異なるポートに送信されます。
dst-mixed-ip-port	宛先 IPv4 または IPv6 アドレスと TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。
dst-port	宛先 TCP/UDP（レイヤ 4）と IPv4 と IPv6 の両方のポート番号に基づいて負荷分散を指定します。
extended	EtherChannel のポート間の拡張ロード バランス方式を設定します。**port-channel load-balance extended** コマンドを参照してください。
src-dst-ip	送信元および宛先ホストの IP アドレスに基づいて負荷分散を指定します。
src-dst-mac	送信元および宛先ホストの MAC アドレスに基づいた負荷分散を指定します。
src-dst-mixed-ip-port	送信元および宛先のホストIPアドレスとTCP/UDP（レイヤ4）ポート番号に基づいて負荷分散を指定します。
src-dst-port	送信元および宛先の TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。
src-ip	送信元ホストの IP アドレスに基づいた負荷分散を指定します。
src-mac	送信元の MAC アドレスに基づいた負荷分散を指定します。異なるホストからのパケットは、チャネルで異なるポートを使用し、同一のホストからのパケットは同一のポートを使用します。
src-mixed-ip-port	送信元ホストIPアドレスとTCP/UDP（レイヤ4）ポート番号に基づいて負荷分散を指定します。
src-port	TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。

コマンド デフォルト

デフォルトは **src-mac** です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel load-balance** 特権 EXEC コマンドを入力します。

例

次の例では、負荷分散方式を dst-mac に設定する方法を示します。

```
Switch(config)# port-channel load-balance dst-mac
```

port-channel load-balance extended

EtherChannelのポート間での負荷分散方式の組み合わせを設定するには、グローバル コンフィギュレーション モードで **port-channel load-balance extended** コマンドを使用します。ロードバランシング メカニズムをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel load-balance extended[{**dst-ip**|**dst-mac**|**dst-port**|**ipv6-label**|**l3-proto**|**src-ip**|**src-mac**|**src-port**}]
no port-channel load-balance extended

構文の説明

dst-ip	（任意）宛先ホストの IP アドレスに基づいて負荷分散を指定します。
dst-mac	（任意）宛先ホストの MAC アドレスに基づいて負荷分散を指定します。同一の宛先に対するパケットは同一のポートに送信され、異なる宛先のパケットはチャネルの異なるポートに送信されます。
dst-port	（任意）IPv4 と IPv6 両方の宛先 TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。
ipv6-label	（任意）送信元MACアドレスとIPv6フローラベルに基づいて負荷分散を指定します。
l3-proto	（任意）送信元 MAC アドレスとレイヤ 3 プロトコルに基づいて負荷分散を指定します。
src-ip	（任意）送信元ホストの IP アドレスに基づいて負荷分散を指定します。
src-mac	（任意）送信元の MAC アドレスに基づいて負荷分散を指定します。異なるホストからのパケットは、チャネルで異なるポートを使用し、同一のホストからのパケットは同一のポートを使用します。
src-port	（任意）TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。

コマンド デフォルト

デフォルトは **src-mac** です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

どのような場合にこれらの転送方式を使用するかについては、このリリースの『*Layer 2/3 Configuration Guide (Catalyst 3850 Switches)*』を参照してください。

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel load-balance** 特権 EXEC コマンドを入力します。

例

次に、拡張負荷分散方式を設定する例を示します。

```
Switch(config)# port-channel load-balance extended dst-ip dst-mac src-ip
```

port-channel min-links

ポート チャネルがアクティブになるように、リンクアップ状態で、EtherChannel にバンドルする必要がある LACP ポートの最小数を定義するには、インターフェイス コンフィギュレーション モードで **port-channel min-links** を使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel min-links *min_links_number*
no port-channel min-links

構文の説明

min_links_number	ポート チャネル内のアクティブな LACP ポートの最小数。指定できる範囲は 2 ～ 8 です。デフォルトは 1 です。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

LACP チャネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 個をアクティブに、最大 8 個をホットスタンバイ モードにできます。LACP チャネル グループに 9 つ以上のポートがある場合、リンクの制御側終端にあるスイッチは、ポート プライオリティを使用して、チャネルにバンドルするポートおよびホットスタンバイ モードに置くポートを判別します。他のスイッチ上のポート プライオリティ（リンクの非制御側終端）は無視されます。

port-channel min-links コマンドには、**lacp max-bundle** コマンドで指定される数より少ない数を指定する必要があります。

ホットスタンバイ モード（ポート ステート フラグの H で出力に表示）にあるポートを判断するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

次に、ポート チャネル 2 がアクティブになる前に、少なくとも 3 個のアクティブな LACP ポートを指定する例を示します。

```
Switch(config)# interface port-channel 2
Switch(config-if)# port-channel min-links 3
```

関連トピック

lacp max-bundle （216 ページ）

show etherchannel

チャネルの EtherChannel 情報を表示するには、ユーザ EXEC モードで **show etherchannel** コマンドを使用します。

show etherchannel [{*channel-group-number*|{**detail** |**port** |**port-channel** |**protocol** |**summary** }}] | [{**auto**|**detail**|**load-balance** |**port**|**port-channel**|**protocol**|**summary**}]

構文の説明

channel-group-number	（任意）チャネル グループ番号。指定できる範囲は 1 ～ 128 です。
auto	（任意）Etherchannel が自動的に作成する情報を表示します。
detail	（任意）詳細な EtherChannel 情報を表示します。
load-balance	（任意）ポート チャネル内のポート間の負荷分散方式、またはフレーム配布方式を表示します。
port	（任意）EtherChannel ポートの情報を表示します。
port-channel	（任意）ポート チャネル情報を表示します。
protocol	（任意）EtherChannel で使用されるプロトコルを表示します。
summary	（任意）各チャネル グループのサマリーを 1 行で表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

チャネル グループ番号を指定しない場合は、すべてのチャネル グループが表示されます。

次の例では、**show etherchannel auto** コマンドの出力を示します。

```
スイッチ# show etherchannel auto
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
```

```
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SUA)        LACP      Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

次の例では、**show etherchannel** *channel-group-number* **detail** コマンドの出力を示します。

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:      LACP
                   Ports in the group:
                   -------------------
Port: Gi1/0/1
------------
Port state    = Up Mstr In-Bndl
Channel group = 1        Mode  = Active        Gcchange = -
Port-channel  =          Po1GC = -             Pseudo port-channel = Po1
Port index    =          0Load = 0x00          Protocol = LACP

Flags: S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDU
       A - Device is in active mode.        P - Device is in passive mode.

Local information:
                         LACP port   Admin   Oper   Port   Port
Port     Flags   State   Priority    Key     Key    Number State
Gi1/0/1   SA      bndl     32768      0x1     0x1    0x101  0x3D
Gi1/0/2    A      bndl     32768      0x0     0x1    0x0    0x3D

Age of the port in the current state: 01d:20h:06m:04s

                   Port-channels in the group:
                   ----------------------

Port-channel: Po1   (Primary Aggregator)

Age of the Port-channel = 01d:20h:20m:26s
Logical slot/port = 10/1          Number of ports = 2
HotStandBy port   = null
Port state        = Port-channel Ag-Inuse
Protocol          = LACP

Ports in the Port-channel:

Index  Load   Port      EC state        No of bits
------+------+------+------------------+-----------
 0      00    Gi1/0/1    Active           0
 0      00    Gi1/0/2    Active           0

Time since last port bundled:   01d:20h:24m:44s   Gi1/0/2
```

次の例では、**show etherchannel** *channel-group-number* **summary** コマンドの出力を示します。

```
Switch> show etherchannel 1 summary
Flags: D - down P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3 S - Layer2
       u - unsuitable for bundling
       U - in use f - failed to allocate aggregator
       d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
 1     Po1(SU)        LACP        Gi1/0/1(P) Gi1/0/2(P)
```

次の例では、**show etherchannel** *channel-group-number* **port-channel** コマンドの出力を示します。

```
Switch> show etherchannel 1 port-channel
Port-channels in the group:
----------------------
Port-channel: Po1 (Primary Aggregator)
------------
Age of the Port-channel = 01d:20h:24m:50s
Logical slot/port = 10/1 Number of ports = 2
Logical slot/port = 10/1 Number of ports = 2
Port state = Port-channel Ag-Inuse
Protocol = LACP

Ports in the Port-channel:

Index  Load   Port   EC state           No of bits
------+------+------+------------------+-----------
 0      00    Gi1/0/1 Active             0
 0      00    Gi1/0/2 Active             0

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2
```

次の例では、**show etherchannel protocol** コマンドの出力を示します。

```
Switch# show etherchannel protocol
Channel-group listing:
----------------------
Group: 1
----------
Protocol: LACP
Group: 2
----------
Protocol: PAgP
```

関連トピック

channel-group （193 ページ）
channel-protocol （197 ページ）
interface port-channel （214 ページ）

show lacp

Link Aggregation Control Protocol（LACP）チャネル グループ情報を表示するには、ユーザ EXEC モードで **show lacp** コマンドを使用します。

show lacp [*channel-group-number*] {**counters**|**internal**|**neighbor**|**sys-id**}

構文の説明

channel-group-number	（任意）チャネル グループ番号。指定できる範囲は 1 ～ 128 です。
counters	トラフィック情報を表示します。
internal	内部情報を表示します。
neighbor	ネイバーの情報を表示します。
sys-id	LACP によって使用されるシステム識別子を表示します。システム識別子は、LACP システム プライオリティと スイッチ MAC アドレスで構成されています。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

show lacp コマンドを入力すると、アクティブなチャネル グループの情報が表示されます。特定のチャネル情報を表示するには、チャネル グループ番号を指定して **show lacp** コマンドを入力します。

チャネル グループを指定しない場合は、すべてのチャネル グループが表示されます。

channel-group-number を入力すると、**sys-id** 以外のすべてのキーワードでチャネル グループを指定できます。

次の例では、**show lacp counters** ユーザ EXEC コマンドの出力を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
Switch> show lacp counters
              LACPDUs         Marker      Marker Response   LACPDUs
Port        Sent  Recv      Sent  Recv      Sent  Recv      Pkts  Err
--------------------------------------------------------------------
Channel group:1
Gi2/0/1      19    10         0    0          0    0         0
Gi2/0/2      14    6          0    0          0    0         0
```

表 *14 : show lacp counters* のフィールドの説明

フィールド	説明
LACPDUs Sent および Recv	ポートによって送受信された LACP パケット数
Marker Sent および Recv	ポートによって送受信された LACP Marker パケット数
Marker Response Sent および Recv	ポートによって送受信された LACP Marker 応答パケット数
LACPDUs Pkts および Err	ポートの LACP によって受信された、未知で不正なパケット数

次の例では、**show lacp internal** コマンドの出力を示します。

```
Switch> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port    Admin    Oper    Port     Port
Port      Flags   State     Priority     Key      Key     Number   State
Gi2/0/1    SA      bndl      32768         0x3     0x3       0x4    0x3D
Gi2/0/2    SA      bndl      32768         0x3     0x3       0x5    0x3D
```

次の表に、出力されるフィールドの説明を示します。

表 *15 : show lacp internal* のフィールドの説明

フィールド	説明
状態	特定のポートの状態。次に使用可能な値を示します。 • – : ポートの状態は不明です。 • **bndl** : ポートがアグリゲータに接続され、他のポートとバンドルされています。 • **susp** : ポートが中断されている状態で、アグリゲータには接続されていません。 • **hot-sby** : ポートがホットスタンバイの状態です。 • **indiv** : ポートは他のポートとバンドルできません。 • **indep** : ポートは独立状態です。バンドルされていませんが、データ トラフィックを処理することができます。この場合、LACP は相手側ポートで実行されていません。 • **down** : ポートがダウンしています。
LACP Port Priority	ポートのプライオリティ設定。ハードウェアの制限により互換性のあるすべてのポートを集約できない場合、LACP はポート プライオリティを使用してポートをスタンバイ モードにします。
Admin Key	ポートに割り当てられた管理用のキー。LACP は自動的に管理用のキー値を生成します（16 進数）。管理キーにより、他のポートとともに集約されるポートの機能が定義されます。ポートが他のポートと集約できるかどうかは、ポートの物理特性（たとえば、データ レートやデュプレックス機能）と設定に指定された制限によって決定されます。
Oper Key	ポートで使用される実行時の操作キー。LACP は自動的に値を生成します（16 進数）。
Port Number	ポート番号。

フィールド	説明
Port State	ポートの状態変数。1つのオクテット内で個々のビットとしてエンコードされ、次のような意味になります。 • bit0：LACP のアクティビティ • bit1：LACP のタイムアウト • bit2：集約 • bit3：同期 • bit4：収集 • bit5：配信 • bit6：デフォルト • bit7：期限切れ （注） 上のリストでは、bit7 が MSB で bit0 は LSB です。

次の例では、**show lacp neighbor** コマンドの出力を示します。

```
Switch> show lacp neighbor
Flags: S - Device is sending Slow LACPDUs  F - Device is sending Fast LACPDUs
       A - Device is in Active mode        P - Device is in Passive mode

Channel group 3 neighbors

Partner's information:

          Partner                Partner               Partner
Port      System ID              Port Number   Age     Flags
Gi2/0/1   32768,0007.eb49.5e80   0xC             19s    SP

          LACP Partner           Partner       Partner
          Port Priority          Oper Key      Port State
          32768                  0x3           0x3C

Partner's information:

          Partner                Partner               Partner
Port      System ID              Port Number   Age     Flags
Gi2/0/2   32768,0007.eb49.5e80   0xD             15s    SP

          LACP Partner           Partner       Partner
          Port Priority          Oper Key      Port State
          32768                  0x3           0x3C
```

次の例では、**show lacp sys-id** コマンドの出力を示します。

```
Switch> show lacp sys-id
32765,0002.4b29.3a00
```

システム ID は、システム プライオリティおよびシステム MAC アドレスで構成されています。最初の 2 バイトはシステム プライオリティ、最後の 6 バイトはグローバルに管理されているシステム関連の個々の MAC アドレスです。

関連トピック

clear lacp （199 ページ）
lacp port-priority （217 ページ）
lacp system-priority （219 ページ）

show pagp

Port Aggregation Protocol（PAgP; ポート集約プロトコル）のチャネル グループ情報を表示するには、EXEC モードで **show pagp** コマンドを使用します。

show pagp [*channel-group-number*] {**counters**|**dual-active**|**internal**|**neighbor**}

構文の説明

channel-group-number	（任意）チャネル グループ番号。指定できる範囲は 1 ～ 128 です。
counters	トラフィック情報を表示します。
dual-active	デュアルアクティブ ステータスが表示されます。
internal	内部情報を表示します。
neighbor	ネイバーの情報を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

show pagp コマンドを入力すると、アクティブなチャネル グループの情報が表示されます。非アクティブ ポート チャネルの情報を表示するには、チャネル グループ番号を指定して **show pagp** コマンドを入力します。

例

次の例では、**show pagp 1 counters** コマンドの出力を示します。

```
Switch> show pagp 1 counters
             Information        Flush
Port         Sent   Recv     Sent   Recv
---------------------------------------
Channel group: 1
  Gi1/0/1    45     42       0      0
  Gi1/0/2    45     41       0      0
```

次の例では、**show pagp dual-active** コマンドの出力を示します。

```
Switch> show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1

Channel group 1
          Dual-Active     Partner              Partner   Partner
```

```
Port      Detect Capable  Name                Port      Version
Gi1/0/1   No              スイッチ             Gi3/0/3   N/A
Gi1/0/2   No              スイッチ             Gi3/0/4   N/A

<output truncated>
```

次の例では、**show pagp 1 internal** コマンドの出力を示します。

```
Switch> show pagp 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Channel group 1
                                Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi1/0/1     SC    U6/S7   H       30s      1        128        Any      16
Gi1/0/2     SC    U6/S7   H       30s      1        128        Any      16
```

次の例では、**show pagp 1 neighbor** コマンドの出力を示します。

```
Switch> show pagp 1 neighbor

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.

Channel group 1 neighbors
            Partner             Partner          Partner           Partner Group
Port        Name                Device ID        Port         Age  Flags   Cap.
Gi1/0/1     スイッチ-p2          0002.4b29.4600   Gi01//1        9s SC      10001
Gi1/0/2     スイッチ-p2          0002.4b29.4600   Gi1/0/2       24s SC      10001
```

関連トピック

clear pagp （200 ページ）

show platform etherchannel

プラットフォーム依存 EtherChannel 情報を表示するには、特権 EXEC モードで **show platform etherchannel** コマンドを使用します。

show platform etherchannel *channel-group-number* {**group-mask**|**load-balance mac** *src-mac dst-mac* [**ip** *src-ip dst-ip* [**port** *src-port dst-port*]]} [**switch** *switch-number*]

構文の説明

channel-group-number	チャネル グループ番号。指定できる範囲は 1 ～ 128 です。
group-mask	EtherChannel グループ マスクを表示します。
load-balance	EtherChannel ロードバランシングのハッシュ アルゴリズムをテストします。
mac *src-mac dst-mac*	送信元と宛先の MAC アドレスを指定します。
ip *src-ip dst-ip*	（任意）送信元と宛先の IP アドレスを指定します。
port *src-port dst-port*	（任意）送信元と宛先のレイヤ ポート番号を指定します。
switch *switch-number*	（任意）スタック メンバを指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。

テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show platform pm

プラットフォーム依存のポート マネージャ情報を表示するには、特権 EXEC モードで **show platform pm** コマンドを使用します。

show platform pm {**etherchannel** *channel-group-number* **group-mask**|**interface-numbers**|**port-data** *interface-id*|**port-state**|**spi-info**|**spi-req-q**}

構文の説明

etherchannel *channel-group-number* **group-mask**	指定されたチャネル グループの EtherChannel グループ マスク テーブルを表示します。指定できる範囲は 1 ～ 128 です。
interface-numbers	インターフェイス番号情報を表示します。
port-data *interface-id*	指定されたインターフェイスのポート データ情報を表示します。
port-state	ポートの状態情報を表示します。
spi-info	ステートフル パケット インスペクション（SPI）情報を表示します。
spi-req-q	確認応答のためのステートフル パケット インスペクション（SPI）の最大待機時間を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。

テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show udld

すべてのポートまたは指定されたポートの単方向リンク検出（UDLD）の管理ステータスおよび運用ステータスを表示するには、ユーザ EXEC モードで **show udld** コマンドを使用します。

show udld ［**Auto-Template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan**］ *interface_number*
show udld neighbors

構文の説明

Auto-Template	（任意）自動テンプレート インターフェイスの UDLD 動作ステータスを表示します。範囲は 1 ～ 999 です。
Capwap	（任意）CAPWAP インターフェイスの UDLD 動作ステータスを表示します。指定できる範囲は 0 ～ 2147483647 です。
GigabitEthernet	（任意）GigabitEthernet インターフェイスの UDLD 動作ステータスを表示します。範囲は 0 ～ 9 です。
GroupVI	（任意）グループ仮想インターフェイスの UDLD 動作ステータスを表示します。範囲は 1 ～ 255 です。
InternalInterface	（任意）内部インターフェイスの UDLD 動作ステータスを表示します。範囲は 0 ～ 9 です。
Loopback	（任意）ループバック インターフェイスの UDLD 動作ステータスを表示します。指定できる範囲は 0 ～ 2147483647 です。
Null	（任意）null インターフェイスの UDLD 動作ステータスを表示します。
Port-channel	（任意）イーサネット チャネル インターフェイスの UDLD 動作ステータスを表示します。有効な範囲は 1 ～ 128 です。
TenGigabitEthernet	（任意）10 ギガビット イーサネット インターフェイスの UDLD 動作ステータスを表示します。範囲は 0 ～ 9 です。
Tunnel	（任意）トンネル インターフェイスの UDLD 動作ステータスを表示します。指定できる範囲は 0 ～ 2147483647 です。
Vlan	（任意）VLAN インターフェイスの UDLD 動作ステータスを表示します。指定できる範囲は 1 ～ 4095 です。

interface-id	（任意）インターフェイスの ID およびポート番号です。有効なインターフェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。
neighbors	（任意）ネイバー情報だけを表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

インターフェイス ID を入力しない場合は、すべてのインターフェイスの管理上および運用上の UDLD ステータスが表示されます。

次の例では、**show udld** *interface-id* コマンドの出力を示します。ここでは、UDLD はリンクの両端でイネーブルに設定されていて、リンクが双方向であることを UDLD が検出します。次の表に、この出力で表示されるフィールドについて説明します。

```
Switch> show udld gigabitethernet2/0/1
Interface gi2/0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
Entry 1
Expiration time: 146
Device ID: 1
Current neighbor state: Bidirectional
Device name: Switch-A
Port ID: Gi2/0/1
Neighbor echo 1 device: Switch-B
Neighbor echo 1 port: Gi2/0/2
Message interval: 5
CDP Device name: Switch-A
```

表 *16 : show udld* のフィールドの説明

フィールド	説明
インターフェイス	UDLD に設定されたローカル デバイスのインターフェイス。

フィールド	説明
Port enable administrative configuration setting	ポートでの UDLD の設定方法。UDLD がイネーブルまたはディセーブルの場合、ポートのイネーブル設定は運用上のイネーブル ステートと同じです。それ以外の場合、イネーブル動作設定は、グローバルなイネーブル設定によって決まります。
Port enable operational state	このポートで UDLD が実際に稼働しているかどうかを示す動作ステート。
Current bidirectional state	リンクの双方向ステート。リンクがダウンしているか、または UDLD 非対応デバイスに接続されている場合は、unknown ステートが表示されます。リンクが UDLD 対応デバイスに通常どおり双方向接続されている場合は、bidirectional ステートが表示されます。その他の値が表示されている場合は、正しく配線されていません。
Current operational state	UDLD ステート マシンの現在のフェーズ。通常の双方向リンクの場合、多くは、ステート マシンはアドバタイズ フェーズです。
Message interval	ローカル デバイスからアドバタイズ メッセージを送信する頻度。単位は秒です。
Time out interval	検出ウィンドウ中に、UDLD がネイバー デバイスからのエコーを待機する期間（秒）。
Entry 1	最初のキャッシュ エントリの情報。このエントリには、ネイバーから受信されたエコー情報のコピーが格納されます。
Expiration time	このキャッシュ エントリの期限が切れるまでの存続期間（秒）。
デバイス ID	ネイバー デバイスの ID。
Current neighbor state	ネイバーの現在の状態。ローカル デバイスおよびネイバー装置の両方で UDLD が通常どおり稼働している場合、ネイバー ステートおよびローカル ステートは双方向です。リンクがダウンしているか、またはネイバーが UDLD 対応でない場合、キャッシュ エントリは表示されません。

フィールド	説明
デバイス名	装置名またはネイバーのシステム シリアル番号。装置名が設定されていないか、またはデフォルト（Switch）に設定されている場合、システムのシリアル番号が表示されます。
Port ID	UDLD に対してイネーブルに設定されたネイバーのポート ID。
Neighbor echo 1 device	エコーの送信元であるネイバーのネイバー デバイス名。
Neighbor echo 1 port	エコーの送信元であるネイバーのポート番号 ID。
Message interval	ネイバーがアドバタイズ メッセージを送信する速度（秒）。
CDP device name	CDP デバイス名またはシステム シリアル番号。装置名が設定されていないか、またはデフォルト（Switch）に設定されている場合、システムのシリアル番号が表示されます。

次の例では、**show udld neighbors** コマンドの出力を示します。

```
Switch# show udld neighbors
Port     Device Name          Device ID  Port-ID  OperState
-------- -------------------- ---------- -------- --------------
Gi2/0/1  Switch-A             1          Gi2/0/1  Bidirectional
Gi3/0/1  Switch-A             2          Gi3/0/1  Bidirectional
```

関連トピック

udld （256 ページ）
udld port （258 ページ）
udld reset （260 ページ）

switchport

レイヤ 3 モードになっているインターフェイスをレイヤ 2 設定用のレイヤ 2 モードに配置するには、インターフェイス コンフィギュレーション モードで **switchport** コマンドを使用します。インターフェイスをレイヤ 3 モードに配置するには、このコマンドの **no** 形式を使用します。

switchport
no switchport

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、すべてのインターフェイスがレイヤ 2 モードです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

インターフェイスをルーテッドインターフェイスの状態に設定して、レイヤ2の設定をすべて削除するには、**no switchport** コマンド（パラメータの指定なし）を使用します。このコマンドは、ルーテッド ポートに IP アドレスを割り当てる前に使用する必要があります。

（注） このコマンドは、LAN Base 機能セットを実行しているスイッチではサポートされません。

no switchport コマンドを入力するとポートがシャットダウンされて、その後再び有効になります。その際に、ポートの接続先のデバイスでメッセージが生成されることがあります。

レイヤ 2 モードからレイヤ 3 モード（またはその逆）にインターフェイスを変更すると、影響を受けたインターフェイスに関連する以前の設定情報が失われる可能性があり、インターフェイスがデフォルト設定に戻ります。

（注） インターフェイスがレイヤ 3 インターフェイスとして設定されている場合、最初に **switchport** コマンドを入力して、そのインターフェイスをレイヤ 2 ポートとして設定する必要があります。その後、**switchport access vlan** コマンドと **switchport mode** コマンドを入力できます。

switchport コマンドは、シスコ ルーテッド ポートをサポートしないプラットフォームでは使用されません。このようなプラットフォーム上のすべての物理ポートは、レイヤ2のスイッチド インターフェイスとして想定されます。

インターフェイスのポート ステータスを確認するには、**show running-config** 特権 EXEC コマンドを入力します。

例

次の例では、インターフェイスをレイヤ 2 ポートとして運用することを中止し、シスコのルーテッド ポートにする方法を示します。

```
Switch(config-if)# no switchport
```

次の例では、ポートのインターフェイスをシスコのルーテッド ポートとして運用することを中止し、レイヤ 2 のスイッチド インターフェイスに変更する方法を示します。

```
Switch(config-if)# switchport
```

switchport access vlan

ポートをスタティック アクセス ポートとして設定するには、インターフェイス コンフィギュレーション モードで **switchport access vlan** コマンドを使用します。スイッチのアクセス モードをデフォルトの VLAN モードにリセットするには、このコマンドの **no** 形式を使用します。

switchport access vlan {*vlan-id*|**name** *vlan_name*}
no switchport access vlan

構文の説明

vlan-id	アクセス モード VLAN のVLAN ID。範囲は 1 ~ 4094。

コマンド デフォルト

デフォルトのアクセス VLAN およびトランク インターフェイス ネイティブ VLAN は、プラットフォームまたはインターフェイス ハードウェアに対応したデフォルト VLAN です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE Denali 16.2.1	**name** *vlan_name* キーワードが導入されました。

使用上のガイドライン

switchport access vlan コマンドを有効にするには、事前にポートをアクセス モードにする必要があります。

スイッチポートのモードが **access vlan** *vlan-id* に設定されている場合、ポートは指定された VLAN のメンバとして動作します。アクセス ポートを割り当てることができるのは、1 つの VLAN だけです。

no switchport access コマンドを使用すると、アクセス モード VLAN がデバイスに適したデフォルト VLAN にリセットされます。

例

次の例では、アクセス モードで動作するスイッチド ポート インターフェイスが、デフォルト VLAN ではなく VLAN 2 で動作するように変更します。

```
Switch(config-if)# switchport access vlan 2
```

例

次の例では、最初に VLAN ID と VLAN 名を対応させて、その情報を VLAN データベースに格納し、その後、アクセス モードにあるインターフェイス上の VLAN を設定します（名前を使用）。設定を確認するには、特権 EXEC コマンドで **show interfaces** *interface-id***switchport** を入力して、Access Mode VLAN: 行の情報を調べます。

手順 1：VLAN データベースでのエントリの作成

```
Switch# configure terminal
Switch(config)# vlan 33
Switch(config-vlan)# name test
Switch(config-vlan)# end
Switch#
```

手順 2：VLAN データベースの確認

```
Switch # show vlan id 33
VLAN  Name   Status   Ports
---- -------------------------------- --------- -------------------------------

33    test   active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
33   enet  100033     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary  Secondary Type              Ports
------- --------- -------------- -----------------------------------------
```

手順 3：VLAN 名を使用したインターフェイスへの VLAN の割り当て

```
Switch # configure terminal
Switch(config)# interface GigabitEthernet3/1/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan name test
Switch(config-if)# end
Switch#
```

手順 4：設定の確認

```
Switch # show running-config interface GigabitEthernet3/1/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet3/1/1
switchport access vlan 33
switchport mode access
Switch#
```

手順 5：インターフェイス スイッチポートの確認

```
Switch # show interface GigabitEthernet3/1/1 switchport
Name: Gi3/1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 33 (test)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: None
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
```

```
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#
```

関連トピック

switchport mode （251 ページ）

switchport mode

ポートの VLAN メンバーシップ モードを設定するには、インターフェイス コンフィギュレーション モードで **switchport mode** コマンドを使用します。モードをデバイスに適したデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

switchport mode {access|dynamic |{auto|desirable}|trunk}
noswitchport mode {access|dynamic |{auto|desirable}|trunk}

構文の説明

access	ポートをアクセス モードに設定します（**switchport access vlan** インターフェイス コンフィギュレーション コマンドの設定に応じて、スタティック アクセスまたはダイナミック アクセスのいずれか）。ポートは無条件にアクセスするように設定され、非カプセル化（タグなし）フレームを送受信する単一の非トランク VLAN インターフェイスとして動作します。アクセス ポートを割り当てることができるのは、1 つの VLAN だけです。
dynamic auto	ポート トランキング モードのダイナミック パラメータを auto に設定して、インターフェイスがリンクをトランク リンクに変換するように指定します。これがデフォルトのスイッチポート モードになります。
dynamic desirable	ポート トランキング モードのダイナミック パラメータを desirable に設定して、インターフェイスがリンクをトランク リンクにアクティブに変換するように指定します。
trunk	ポートを無条件にトランクに設定します。ポートはトランキング VLAN レイヤ 2 インターフェイスです。ポートは、送信元の VLAN を識別するカプセル化（タグ付き）フレームを送受信します。トランクは、2 つの スイッチ 間、または スイッチ とルータ間のポイントツーポイント リンクです。

コマンド デフォルト

デフォルト モードは **dynamic auto** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

（注） **dot1q-tunnel** キーワードは CLI に表示されますが、サポートされていません。

access または **trunk** キーワードによる設定が有効となるのは、**switchport mode** コマンドを使用して適切なモードでポートを設定した場合のみです。スタティック アクセスおよびトランクの設定は保存されますが、同時にアクティブにできるのはいずれかの設定だけです。

access モードを開始すると、インターフェイスは永続的な非トランキング モードになり、隣接インターフェイスがリンクから非トランク リンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

trunk モードを開始すると、インターフェイスは永続的なトランキング モードになり、接続先のインターフェイスがリンクからトランク リンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

dynamic auto モードを開始すると、隣接インターフェイスが **trunk** または **desirable** モードに設定された場合に、インターフェイスはリンクをトランク リンクに変換します。

dynamic desirable モードを開始すると、隣接インターフェイスが **trunk**、**desirable**、または **auto** モードに設定された場合に、インターフェイスはトランク インターフェイスになります。

トランキングを自動ネゴシエーションするには、インターフェイスが同じ VLAN トランキング プロトコル（VTP）ドメインに存在する必要があります。トランク ネゴシエーションは、ポイントツーポイント プロトコルである Dynamic Trunking Protocol（DTP）によって管理されます。ただし、一部のインターネットワーキング デバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。この問題を避けるには、DTP をサポートしないデバイスに接続されたインターフェイスが DTP フレームを転送しないように設定し、DTP をオフにします。

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスへのトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

アクセス ポートとトランク ポートは、互いに排他的な関係にあります。

IEEE 802.1x 機能は、次の方法でスイッチポート モードに作用します。

- トランク ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ポート設定で IEEE 802.1x を **dynamic auto** または **dynamic desirable** にイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートのモードを **dynamic auto** または **dynamic desirable** に変更しようとしても、ポート モードは変更されません。
- ダイナミック アクセス（VLAN Query Protocol（VQP））ポートで IEEE 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力して、*Administrative Mode* 行と *Operational Mode* 行の情報を調べます。

例

次の例では、ポートをアクセス モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode access
```

次の例では、ポートを dynamic desirable モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode dynamic desirable
```

次の例では、ポートをトランク モードに設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode trunk
```

関連トピック

switchport access vlan （248 ページ）

switchport nonegotiate

Dynamic Trunking Protocol（DTP）ネゴシエーション パケットがレイヤ 2 インターフェイス上で送信されないように指定するには、インターフェイス コンフィギュレーション モードで **switchport nonegotiate** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport nonegotiate
no switchport nonegotiate

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、トランキング ステータスを学習するために、DTP ネゴシエーションを使用します。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

no switchport nonegotiate コマンドは nonegotiate ステータスを解除します。

このコマンドが有効なのは、インターフェイス スイッチポート モードがアクセスまたはトランク（**switchport mode access** または **switchport mode trunk** インターフェイス コンフィギュレーション コマンドで設定）の場合だけです。dynamic（auto または desirable）モードでこのコマンドを実行しようとすると、エラーが返されます。

DTP をサポートしないインターネットワーキング デバイスでは、DTP フレームが正しく転送されず、設定に矛盾が生じることがあります。この問題を回避するには、**switchport nonegotiate** コマンドを使用して DTP をオフにし、DTP をサポートしていないデバイスに接続されたインターフェイスが DTP フレームを転送しないように設定します。

switchport nonegotiate コマンドを入力した場合、このインターフェイスでは DTP ネゴシエーション パケットが送信されません。デバイスがトランキングを実行するかどうかは、**mode** パラメータ（**access** または）によって決まります。 **trunk.**

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイス上のトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

次の例では、ポートに対してトランキング モードのネゴシエートを制限し、（モードの設定に応じて）トランク ポートまたはアクセス ポートとして動作させる方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport nonegotiate
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

関連トピック

switchport mode （251 ページ）

udld

単方向リンク検出（UDLD）で、アグレッシブモードまたは通常モードをイネーブルにし、設定可能なメッセージタイマーの時間を設定するには、グローバル コンフィギュレーション モードで **udld** コマンドを使用します。すべての光ファイバ ポート上でアグレッシブ モード UDLD または通常モード UDLDをディセーブルにするには、このコマンドの **no** 形式を使用します。

udld {**aggressive**|**enable**|**message time** *message-timer-interval*}
no udld {**aggressive**|**enable**|**message**}

構文の説明

aggressive	すべての光ファイバ インターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。
enable	すべての光ファイバインターフェイスにおいて、通常モードでUDLD をイネーブルにします。
message time *message-timer-interval*	アドバタイズメント フェーズにあり、双方向と判別されたポートにおける UDLD プローブ メッセージ間の時間間隔を設定します。指定できる範囲は 1 ～ 90 秒です。デフォルトは 15 秒です。

コマンド デフォルト

すべてのインターフェイスで UDLD はディセーブルです。

メッセージ タイマーは 15 秒に設定されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

UDLD は、2 つの動作モードをサポートしています。通常（デフォルト）とアグレッシブです。ノーマル モードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単一方向リンクを検出します。アグレッシブ モードでは、UDLD はまた、光ファイバおよびツイストペア リンクの単一方向トラフィックによる単一方向リンク、および光ファイバ リンクにおいて誤って接続されたインターフェイスによる単一方向リンクを検出します。通常モードおよびアグレッシブ モードについては、*Catalyst 2960-X* スイッチ *Layer 2* コンフィギュレーション ガイド*Catalyst 2960-XR Switch Layer 2 Configuration Guide*『*Layer 2/3 Configuration Guide (Catalyst 3850 Switches)*』を参照してください。

プローブ パケット間のメッセージ時間を変更する場合、検出速度と CPU 負荷との折り合いをつけることになります。時間を減少させると、検出応答を高速にすることができますが、CPU の負荷も高くなります。

このコマンドが作用するのは、光ファイバインターフェイスだけです。他のインターフェイスタイプで UDLD をイネーブルにする場合は、**udld** インターフェイス コンフィギュレーション コマンドを使用します。

UDLD によってシャットダウンされたインターフェイスをリセットするのに、次のコマンドを使用します。

- **udld reset** 特権 EXEC コマンド：UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- **shutdown** および **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。
- **no udld enable** グローバル コンフィギュレーション コマンドの後に **udld {aggressive | enable}** グローバル コンフィギュレーション コマンドを入力：グローバルに UDLD を再びイネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** または **udld port aggressive** インターフェイス コンフィギュレーション コマンドを入力：指定されたインターフェイスの UDLD を再びイネーブルにします。
- **errdisable recovery cause udld** および **errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンド：自動的に UDLD error-disabled ステートから回復します。

次の例では、すべての光ファイバインターフェイスで UDLD をイネーブルにする方法を示します。

```
Switch(config)# udld enable
```

設定を確認するには、**show udld** 特権 EXEC コマンドを入力します。

関連トピック

show udld （242 ページ）
udld port （258 ページ）
udld reset （260 ページ）

udld port

個々のインターフェイスで単方向リンク検出（UDLD）をイネーブルにするか、または光ファイバインターフェイスが **udld** グローバル コンフィギュレーション コマンドによってイネーブルになるのを防ぐには、インターフェース コンフィギュレーション モードで **udld port** コマンドを使用します。**udld** グローバル コンフィギュレーション コマンド設定に戻すか、または非光ファイバ ポートで入力された場合に UDLD をディセーブルにするには、このコマンドの **no** 形式を使用します。

udld port [aggressive]
no udld port [aggressive]

構文の説明

aggressive	（任意）指定されたインターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。

コマンド デフォルト

光ファイバ インターフェイスでは、UDLD はディセーブルになっていますが、光ファイバ インターフェイスは、**udld enable** または **udld aggressive** グローバル コンフィギュレーション コマンドのステートに応じて UDLD をイネーブルにします。

非光ファイバ インターフェイスでは、UDLD はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

UDLD 対応ポートが別のスイッチの UDLD 非対応ポートに接続されている場合、このポートは単一方向リンクを検出できません。

UDLD は、2 つの動作モードをサポートしています。通常（デフォルト）とアグレッシブです。ノーマル モードでは、UDLD は、光ファイバ接続において誤って接続されたインターフェイスによる単一方向リンクを検出します。アグレッシブ モードでは、UDLD はまた、光ファイバおよびツイストペア リンクの単一方向トラフィックによる単一方向リンク、および光ファイバ リンクにおいて誤って接続されたインターフェイスによる単一方向リンクを検出します。

UDLD を通常モードでイネーブルにするには、**udld port** インターフェイス コンフィギュレーション コマンドを使用します。UDLD をアグレッシブ モードでイネーブルにするには、**udld port aggressive** インターフェイス コンフィギュレーション コマンドを使用します。

UDLD の制御を **udld enable** グローバル コンフィギュレーション コマンドに戻したり、UDLD を非光ファイバ ポートでディセーブルにしたりする場合は、光ファイバ ポートで **no udld port** コマンドを使用します。

udld enable または **udld aggressive** グローバル コンフィギュレーション コマンドの設定を上書きする場合は、光ファイバ ポートで **udld port aggressive** コマンドを使用します。この設定を削除して UDLD イネーブル化の制御を **udld** グローバル コンフィギュレーション コマンドに戻したり、UDLD を非光ファイバ ポートでディセーブルにしたりする場合は、光ファイバ ポートで **no** 形式を使用します。

UDLD によってシャットダウンされたインターフェイスをリセットするのに、次のコマンドを使用します。

- **udld reset** 特権 EXEC コマンド：UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- **shutdown** および **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
- **no udld enable** グローバル コンフィギュレーション コマンドの後に **udld {aggressive | enable}** グローバル コンフィギュレーション コマンドを入力：グローバルに UDLD を再度イネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** または **udld port aggressive** インターフェイス コンフィギュレーション コマンドを入力：指定したインターフェイスで UDLD を再度イネーブルにします。
- **errdisable recovery cause udld** および **errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンド：自動的に UDLD errdisable ステートから回復します。

次の例では、ポート上で UDLD をイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet6/0/1
Switch(config-if)# udld port
```

次の例では、**udld** グローバル コンフィギュレーション コマンドの設定に関係なく、光ファイバ インターフェイス上で UDLD をディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet6/0/1
Switch(config-if)# no udld port
```

設定を確認するには、**show running-config** または **show udld** *interface* 特権 EXEC コマンドを入力します。

関連トピック

show udld （242 ページ）
udld （256 ページ）
udld reset （260 ページ）

udld reset

単方向リンク検出（UDLD）によりディセーブルにされたインターフェイスをすべてリセットし、インターフェイスのトラフィックを再開させるには、特権 EXEC モードで **udld reset** コマンドを使用します（イネーブルの場合には、スパニングツリー、Port Aggregation Protocol（PAgP）、Dynamic Trunking Protocol（DTP）などの他の機能を介することで有効になります）。

udld reset

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

インターフェイスの設定で、UDLDがまだイネーブルである場合、これらのポートは再びUDLDの稼働を開始し、問題が修正されていない場合には同じ理由でディセーブルになります。

次の例では、UDLDによってディセーブルにされたすべてのインターフェイスをリセットする方法を示します。

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

関連トピック

show udld （242 ページ）
udld （256 ページ）
udld port （258 ページ）

第 V 部

Lightweight アクセス ポイント

Cisco Lightweight アクセス ポイント コマンド

ap auth-list ap-policy

スイッチ に参加しているすべての Cisco Lightweight アクセス ポイントの認可ポリシーを設定するには、**apauth-listap-policy** コマンドを使用します。スイッチ に参加しているすべての Cisco Lightweight アクセス ポイントの認可ポリシーを無効にするには、このコマンドの **no** 形式を使用します。

ap auth-list ap-policy {**authorize-ap**|**lsc**|**mic**|**ssc**}
no ap auth-list ap-policy {**authorize-ap**|**lsc**|**mic**|**ssc**}

構文の説明

authorize-ap	許可ポリシーを有効にします。
lsc	ローカルで有効な証明書を持つアクセス ポイントの接続を有効にします。
mic	製造元でインストールされる証明書を持つアクセス ポイントの接続を有効にします。
ssc	自己署名証明書を持つアクセス ポイントの接続を有効にします。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの許可ポリシーを有効にする例を示します。

```
Switch(config)# ap auth-list ap-policy authorize-ap
```

次に、ローカルで有効な証明書を持つアクセス ポイントの接続を有効にする例を示します。

```
Switch(config)# ap auth-list ap-policy lsc
```

次に、製造元でインストールされる証明書を持つアクセス ポイントの接続を有効にする例を示します。

```
Switch(config)# ap auth-list ap-policy mic
```

次に、自己署名証明書を持つアクセス ポイントの接続を有効にする例を示します。

```
Switch(config)# ap auth-list ap-policy ssc
```

ap bridging

Cisco Lightweight アクセス ポイントでイーサネットと 802.11 の間のブリッジングを有効にするには、**apbridging** コマンドを使用します。Cisco Lightweight アクセス ポイントでイーサネットと 802.11 の間のブリッジングを無効にするには、このコマンドの **no** 形式を使用します。

ap bridging
no ap bridging

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、Lightweight アクセス ポイントでイーサネット間ブリッジングを有効にする例を示します。

```
Switch(config)# ap bridging
```

次に、Lightweight アクセス ポイントでイーサネット間ブリッジングを無効にする例を示します。

```
Switch(config)# no ap bridging
```

ap capwap multicast

マルチキャスト転送が有効のときにマルチキャスト トラフィックを受信するためにすべてのアクセス ポイントによって使用されるマルチキャスト アドレスを設定し、アクセス ポイントに送信されるマルチキャスト パケットの外部 Quality of Service（QoS）レベルを設定するには、**ap capwap multicast** コマンドを使用します。

ap capwap multicast {*multicast-ip-address*|**service-policy output** *pollicymap-name*}

構文の説明

multicast-ip-address	マルチキャスト IP アドレス。
service-policy	マルチキャスト アクセス ポイントのトンネル QoS ポリシーを指定します。
output	ポリシー マップ名を出力に割り当てます。
policymap-name	サービス ポリシー マップ名。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、マルチキャスト転送が有効のときにマルチキャスト トラフィックを受信するためにすべてのアクセス ポイントによって使用されるマルチキャスト アドレスを設定する例を示します。

```
Switch(config)# ap capwap multicast 239.2.2.2
```

次に、マルチキャスト アクセス ポイントのトンネル マルチキャスト QoS サービス ポリシーを設定する例を示します。

```
Switch(config)# ap capwap multicast service-policy output tunnmulpolicy
```

関連トピック

ap capwap retransmit （271 ページ）
ap capwap timers （272 ページ）

ap capwap retransmit

Control And Provisioning of Wireless Access Points（CAPWAP）制御パケットの再送信回数と制御パケットの再送信間隔を設定するには、**ap capwap retransmit** コマンドを使用します。

ap capwap retransmit {**count** *retransmit-count*|**interval** *retransmit-interval*}

構文の説明

count *retransmit-count*	アクセスポイントのCAPWAP 制御パケットの再送信回数を指定します。 （注） 回数は 3 ～ 8 です。
interval *retransmit-interval*	アクセスポイントのCAPWAP 制御パケットの再送信間隔を指定します。 （注） 間隔は 2 ～ 5 秒です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの CAPWAP 制御パケットの再送信回数を設定する例を示します。

```
Switch# ap capwap retransmit count 3
```

次に、アクセス ポイントの CAPWAP 制御パケットの再送信間隔を設定する例を示します。

```
Switch# ap capwap retransmit interval 5
```

ap capwap timers

高度なタイマー設定を指定するには、**apcapwaptimers** コマンドを使用します。

ap capwap timers {**discovery-timeout** *seconds*|**fast-heartbeat-timeout local** *seconds*|**heartbeat-timeout** *seconds*|**primary-discovery-timeout** *seconds*|**primed-join-timeout** *seconds*}

構文の説明

discovery-timeout	Cisco Lightweight アクセス ポイントの検出タイムアウトを指定します。 （注） Cisco Lightweight アクセス ポイントの検出タイムアウトは、アクセス ポイントが応答しなかったとみなす前にシスコのスイッチが応答のないアクセス ポイントの応答を待つ時間です。
seconds	Cisco Lightweight アクセス ポイントの検出タイムアウト（1 ～ 10 秒）。 （注） デフォルトは 10 秒です。
fast-heartbeat-timeoutlocal	ローカル アクセス ポイントまたはすべてのアクセス ポイントのスイッチ障害を検出するために要する時間を短縮する高速ハートビート タイマーを有効にします。
seconds	スイッチ障害を検出するために要する時間を短縮する小さい値のハートビート間隔（1～10 秒）。 （注） デフォルトでは高速ハートビート タイムアウト間隔が無効になっています。
heartbeat-timeout	Cisco Lightweight アクセス ポイントのハートビート タイムアウトを指定します。 （注） Cisco Lightweight アクセス ポイントのハートビート タイムアウトは、Cisco Lightweight アクセス ポイントがシスコのスイッチにハートビート キープアライブ信号を送信する頻度を制御します。 この値は、高速ハートビート タイマーの 3 倍以上の値である必要があります。
seconds	Cisco Lightweight アクセス ポイントのハートビート タイムアウト値（1 ～ 30 秒）。 （注） デフォルトは 30 秒です。

primary-discovery-timeout	アクセス ポイントのプライマリ ディスカバリ要求タイマーを指定します。このタイマーは、設定されているプライマリ、セカンダリ、またはターシャリ スイッチを検出するためにアクセス ポイントが取る時間を決定します。
seconds	アクセスポイントのプライマリ検出要求タイマー（30～3600秒）。 （注） デフォルトは 120 秒です。
primed-join-timeout	認証タイムアウトを指定します。プライマリ スイッチが応答不能になったと判断するためにアクセス ポイントが取る時間を決定します。アクセスポイントは、スイッチへの接続が復元されるまで、スイッチへの参加を試みなくなります。
seconds	認証応答タイムアウト（120 ～ 43200 秒）。 （注） デフォルトは 120 秒です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、タイムアウト値を 7 でアクセス ポイント検出タイムアウトを設定する例を示します。

```
Switch(config)# ap capwap timers discovery-timeout 7
```

次に、すべてのアクセスポイントを対象にファーストハートビート間隔を有効にする例を示します。

```
Switch(config)# ap capwap timers fast-heartbeat-timeout 6
```

次に、アクセスポイントのハートビートタイムアウトを20に設定する例を示します。

```
Switch(config)# ap capwap timers heartbeat-timeout 20
```

次に、アクセス ポイントのプライマリ検出要求タイマーを 1200 秒に設定する例を示します。

```
Switch(config)# ap capwap timers primary-discovery-timeout 1200
```

次に、認証タイムアウトを 360 秒に設定する例を示します。

```
Switch(config)# ap capwap timers primed-join-timeout 360
```

関連トピック

ap capwap multicast （270 ページ）
ap capwap retransmit （271 ページ）

ap cdp

Cisco Lightweight アクセス ポイントで Cisco Discovery Protocol（CDP）を有効にするには、**apcdp** コマンドを使用します。Cisco Lightweight アクセス ポイントで Cisco Discovery Protocol（CDP）を無効にするには、このコマンドの **no** 形式を使用します。

```
ap cdp [interface {ethernet ethernet-id|radio radio-id}]
no ap cdp [interface {ethernet ethernet-id|radio radio-id}]
```

構文の説明

interface	（任意）特定のインターフェイスの CDP を指定します。
ethernet	イーサネット インターフェイスの CDP を指定します。
ethernet-id	イーサネット インターフェイス番号（0 ～ 3）。
radio	無線インターフェイスの CDP を指定します。
radio-id	無線番号（0 ～ 3）。

コマンド デフォルト

すべてのアクセス ポイントで無効になっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

no apcdp コマンドは、スイッチに参加しているすべてのアクセス ポイントおよび今後参加するすべてのアクセス ポイントの CDP を無効にします。CDP は、スイッチまたはアクセス ポイントのリブート後も現在と将来のアクセス ポイントで無効のままになります。CDP を有効にするには、**apcdp** コマンドを入力します。

（注） イーサネット/無線インターフェイス上の CDP は、CDP が有効になっている場合にだけ使用できます。スイッチに参加しているすべてのアクセス ポイントで CDP を有効にした後は、**ap name** *Cisco-AP* **cdp** コマンドを使用して、個々のアクセス ポイントで CDP を無効にし、再度有効にすることができます。スイッチに参加しているすべてのアクセス ポイントで CDP を無効にした後は、個々のアクセス ポイントで CDP を有効にし、その後、無効にすることができます。

次に、すべてのアクセス ポイントで CDP を有効にする例を示します。

```
Switch(config)# ap cdp
```

次に、すべてのアクセス ポイントでイーサネット インターフェイス番号 0 の CDP を有効にする例を示します。

```
Switch(config)# ap cdp ethernet 0
```

関連トピック

show ap cdp （432 ページ）

ap core-dump

Cisco Lightweight アクセス ポイントのメモリ コア ダンプ設定を有効にするには、**apcore-dump** コマンドを使用します。Cisco Lightweight アクセス ポイントのメモリ コア ダンプ設定を無効にするには、このコマンドの **no** 形式を使用します。

ap core-dump *tftp-ip-addr filename* {**compress**|**uncompress**}
no ap core-dump

構文の説明

tftp-ip-addr	アクセス ポイントがコア ダンプ ファイルを送信する Trivial File Transfer Protocol（TFTP）サーバの IP アドレス。
filename	コア ファイルのラベルを付けるためにアクセス ポイントが使用する名前。
compress	コア ダンプ ファイルを圧縮します。
uncompress	コア ダンプ ファイルを圧縮解除します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

アクセス ポイントは TFTP サーバに到達できる必要があります。

次に、コア ダンプ ファイルを設定して圧縮する例を示します。

```
Switch(config)# ap core-dump 192.0.2.51 log compress
```

関連トピック

ap crash-file （279 ページ）
ap name crash-file （352 ページ）

ap country

スイッチの 1 つ以上の国コードを設定するには、**apcountry** コマンドを使用します。

ap country *country-code*

構文の説明

country-code	1 つ以上（複数の場合はカンマ区切り）の 2 文字または 3 文字の国番号。

コマンド デフォルト

US（米国の国コード）。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

Cisco スイッチは、ネットワーク管理者または資格のある IP プロフェッショナルがインストールしてください。その際、正しい国コードを選択する必要があります。インストール後は、法的な規制基準を遵守するためおよび、適切なユニット機能を保証するために、ユニットへのアクセスはパスワードで保護する必要があります。最新の国コードおよび規制区域については、関連する製品マニュアルを参照してください。

次に、スイッチで国コードを IN（インド）および FR（フランス）に設定する例を示します。

```
Switch(config)# ap country IN,FR
```

関連トピック

ap name country （351 ページ）

ap crash-file

クラッシュおよび無線コア ダンプ ファイルを削除するには、**apcrash-file** コマンドを使用します。

ap crash-file {**clear-all**|**delete** *filename*}

構文の説明

clear-all	クラッシュおよび無線コア ダンプ ファイルを削除します。
delete	単一のクラッシュおよび無線コア ダンプ ファイルを削除します。
filename	削除するファイルの名前を指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、すべてのクラッシュ ファイルを削除する例を示します。

```
Switch# ap crash-file clear-all
```

次に、クラッシュ ファイル 1 を削除する例を示します。

```
Switch# ap crash-file delete crash-file-1
```

関連トピック

ap name crash-file （352 ページ）
ap name core-dump （350 ページ）

ap dot11 24ghz preamble

サブクローズ 17.2.2.2 で定義されている短いプリアンブルだけを有効にするには、**apdot1124ghzpreamble** コマンドを使用します。長いプリアンブル（802.11b 以前のデバイスとの下位互換性のため、これらのデバイスが依然としてネットワーク上にある場合）または短いプリアンブル（従来の802.11b以前のデバイスがネットワークに存在しない場合の推奨）を有効にするには、このコマンドの **no** 形式を使用します。

ap dot11 24ghz preamble short
no ap dot11 24ghz preamble short

構文の説明

short	短い802.11bプリアンブルを指定します。

コマンド デフォルト

短いプリアンブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

（注） **apdot1124ghzpreamble** コマンドを使用するには、**Save** コマンドで Cisco スイッチをリブート（システムをリセット）する必要があります。

このパラメータは、SpectraLink NetLink 電話など一部のレガシー クライアントのためにこの Cisco スイッチを最適化するために、long に設定する必要があることがあります。

このコマンドは、CLI インターフェイスがアクティブなときはいつでも使用できます。

次に、長いプリアンブルと短いプリアンブルの両方を有効にする例を示します。

```
Switch(config)# no ap dot11 24ghz preamble short
```

ap dot11 24ghz dot11g

シスコ ワイヤレス LAN ソリューション 802.11g ネットワークを有効にするには、**apdot1124ghzdot11g** コマンドを使用します。シスコ ワイヤレス LAN ソリューション 802.11g ネットワークを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 24ghz dot11g
no ap dot11 24ghz dot11g

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

apdot1124ghzdot11g コマンドを入力する前に、**apdot1124ghzshutdown** コマンドを使用して 802.11 シスコ無線を無効にしてください。

802.11g ネットワークのサポートを設定した後、**noapdot1124ghzshutdown** コマンドを使用して 802.11 2.4 Ghz 無線を有効にしてください。

次に、802.11g ネットワークを有効にする例を示します。

```
Switch(config)# ap dot11 24ghz dot11g
```

関連トピック

show ap dot11 （444 ページ）

ap dot11 5ghz channelswitch mode

802.11h チャネル スイッチ アナウンスを設定するには、**apdot115ghzchannelswitchmode** コマンドを使用します。802.11h チャネル スイッチ アナウンスを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 5ghz channelswitch mode *value*
no ap dot11 5ghz channelswitch mode

構文の説明

value 802.11h チャネル スイッチ通知の値。

（注） 次の 2 つの値のどちらでも指定できます。

- 0：チャネル スイッチ アナウンスが無効であることを示します。
- 1：チャネル スイッチ アナウンスが有効であることを示します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、802.11h スイッチ アナウンスを無効にする例を示します。

```
Switch(config)# ap dot11 5ghz channelswitch mode 1
```

ap dot11 5ghz power-constraint

802.11h の電力制限値を設定するには、**apdot115ghzpower-constraint** コマンドを使用します。802.11h の電力制限値を削除するには、このコマンドの **no** 形式を使用します。

ap dot11 5ghz power-constraint *value*
no ap dot11 5ghz power-constraint

構文の説明

value	802.11h の電力制限値。 （注） 範囲は、0 ～ 30 dBm です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、802.11h 電力制限を 5 dBm に設定する例を示します。

```
Switch(config)# ap dot11 5ghz power-constraint 5
```

ap dot11 beaconperiod

2.4 GHz 帯域または 5 GHz 帯域のビーコン周期をグローバルに変更するには、**apdot11beaconperiod** コマンドを使用します。

（注） このコマンドを使用する前に、802.11 ネットワークを無効にします。「使用上のガイドライン」の項を参照してください。

ap dot11 {**24ghz**|**5ghz**} **beaconperiod** *time*

構文の説明

24ghz	2.4 GHz 帯域の設定を指定します。
5ghz	5 GHz 帯域の設定を指定します。
beaconperiod	ネットワークのビーコンをグローバルに指定します。
time	時間単位（TU）でのビーコン間隔。1 TU は 1024 マイクロ秒です。範囲は 20 ～ 1000 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

Cisco ワイヤレス LAN 802.11 ネットワークでは、すべての Cisco Lightweight アクセス ポイント（無線 LAN）が定期的にビーコンをブロードキャストします。このビーコンは、クライアントにワイヤレス サービスが使用可能なことを通知し、クライアントは Lightweight アクセス ポイントと同期できます。

ビーコン周期を変更する前に、**apdot11** {**24ghz | 5ghz**} **shutdown** コマンドを使用して 802.11 ネットワークを無効にしていることを確認してください。ビーコン周期を変更した後に、**noapdot11** {**24ghz | 5ghz**} **shutdown** コマンドを使用して 802.11 ネットワークを有効にしてください。

次に、120 時間単位のビーコン周期に合わせて 5 GHz 帯域を設定する例を示します。

```
Switch(config)# ap dot11 5ghz beaconperiod 120
```

ap dot11 beamforming

ネットワークまたは個別の無線に対してビームフォーミングを有効にするには、**apdot11beamforming** コマンドを使用します。

ap dot11 {24ghz|5ghz} beamforming

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
beamforming	ネットワークに対してビームフォーミングを指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ネットワークに対してビームフォーミングを有効にすると、そのネットワーク タイプに対応するすべての無線に対してビームフォーミングが自動的に有効になります。

ビームフォーミングを使用する際は、次のガイドラインに従ってください。

- ビームフォーミングは、レガシー直交周波数分割多重（OFDM）データ レート（6、9、12、18、24、36、48、および 54 Mbps）でサポートされています。

  （注） ビームフォーミングは、直接拡散方式のデータ レート（1 および 2 Mbps）および相補コード キー（CCK）のデータ レート（5.5 および 11 Mbps）ではサポートされません。

- ビームフォーミングは、802.11n に対応したアクセス ポイント（AP1260、AP3500、および AP3600）でだけサポートされます。
- 送信用に 2 本以上のアンテナを有効にする必要があります。
- 受信用に 3 本すべてのアンテナを有効にする必要があります。
- OFDM レートを有効にする必要があります。

  送信アンテナがアンテナ設定により 1 本に制限されている場合、あるいは OFDM レートが無効になっている場合、ビームフォーミングは使用されません。

次に、5 GHz 帯域に対してビームフォーミングを有効にする例を示します。

```
Switch(config)# ap dot11 5ghz beamforming
```

ap dot11 cac media-stream

2.4 GHz 帯域と 5 GHz 帯域のメディア ストリームのコール アドミッション制御（CAC）の音声およびビデオ品質パラメータを設定するには、**apdot11cacmedia-stream** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **cac media-stream multicast-direct** {**max-retry-percent**
retryPercent | **min-client-rate** {[illegible]}}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
multicast-direct	マルチキャスト直接メディア ストリーム用の CAC パラメータを指定します。
max-retry-percent	マルチキャスト直接メディア ストリームに許可される最大再試行回数の割合を指定します。
retryPercent	マルチキャスト直接メディア ストリームに許可される最大再試行回数の割合。 （注） 範囲は 0 ～ 100 です。
min-client-rate	マルチキャスト直接メディア ストリーム用にクライアントへの最小データ伝送レートを指定します（マルチキャスト直接ユニキャスト ストリームを受信するためにクライアントが送信する必要があるレート）。 伝送レートがこのレートを下回ると、ビデオが起動しないか、クライアントが不良クライアントとして分類される可能性があります。不良クライアント ビデオは、より良いエフォートの QoS のために降格されたり、拒否される可能性があります。

min-client-rate	次のレートを選択できます。 • **eighteen** • **eleven** • **fiftyFour** • **fivePointFive** • **fortyEight** • **nine** • **one** • **oneFifty** • **oneFortyFourPointFour** • **oneThirty** • **oneThirtyFive** • **seventyTwoPointTwo** • **six** • **sixtyFive** • **thirtySix** • **threeHundred** • **twelve** • **twentyFour** • **two** • **twoSeventy**

コマンド デフォルト

最大再試行回数の割合のデフォルト値は 80 です。80 を超えると、ビデオが開始されないか、クライアントが不良クライアントとして分類される場合があります。不良クライアント ビデオは、より良いエフォートの QoS のために降格されたり、拒否されたりします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **wlan** *wlan_name***shutdown** コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **apdot11** {**24ghz** | **5ghz**} **shutdown** コマンドを入力して、設定する無線ネットワークを無効にします。
- 新しい設定を保存します。
- **apdot11** {**24ghz** | **5ghz**} **cacvoiceacm** コマンドまたは **apdot11** {**24ghz** | **5ghz**} **cacvideoacm** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

次に、802.11a ネットワークの 90 としてマルチキャスト直接メディア ストリームの最大試行回数の割合を設定する例を示します。

```
Switch(config)# ap dot11 5ghz cac media-stream multicast max-retry-percent 90
```

関連トピック

ap dot11 cac multimedia （290 ページ）
ap dot11 cac video （292 ページ）
ap dot11 cac voice （294 ページ）

ap dot11 cac multimedia

2.4 GHz 帯域と 5 GHz 帯域のマルチメディアのコール アドミッション制御（CAC）の音声およびビデオ品質パラメータを設定するには、**apdot11cacmultimedia** コマンドを使用します。

ap dot11 {24ghz|5ghz} cac multimedia max-bandwidth 帯域幅

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
max-bandwidth	2.4 GHz 帯域または 5 GHz 帯域で音声およびビデオ アプリケーション用に Wi-Fi Multimedia（WMM）クライアントに割り当てられる最大帯域幅の割合を指定します。
帯域幅	802.11a または 802.11b/g ネットワークで音声およびビデオ アプリケーション用に WMM クライアントに割り当てられる最大帯域幅の割合。クライアントが指定値に達すると、アクセス ポイントはこの無線帯域での新しいマルチメディア フローを拒否します。範囲は 5 ～ 85% です。

コマンド デフォルト

デフォルト値は 75 % です

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **wlan** *wlan_name***shutdown** コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **apdot11 {24ghz | 5ghz} shutdown** コマンドを入力して、設定する無線ネットワークを無効にします。
- 新しい設定を保存します。
- **apdot11 {24ghz | 5ghz} cacvoiceacm** コマンドまたは **apdot11 {24ghz | 5ghz} cacvideoacm** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

次に、5 GHz 帯域で音声およびビデオ アプリケーション用に WMM クライアントに割り当てられる最大帯域幅の割合を設定する例を示します。

```
Switch(config)# ap dot11 5ghz cac multimedia max-bandwidth 5
```

関連トピック

ap dot11 cac media-stream （287 ページ）
ap dot11 cac video （292 ページ）
ap dot11 cac voice （294 ページ）

ap dot11 cac video

ビデオ カテゴリのコール アドミッション制御（CAC）パラメータを設定するには、**apdot11cacvideo** コマンドを使用します。ビデオ カテゴリの CAC パラメータを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**|**5ghz**} **cac video** {**acm**|**max-bandwidth** *value*|**roam-bandwidth** *value*}
no ap dot11 {**24ghz**|**5ghz**} **cac video** {**acm**|**max-bandwidth** *value*|**roam-bandwidth** *value*}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
acm	2.4 GHz 帯域または 5 GHz 帯域の帯域幅ベースのビデオ CAC を有効にします。 （注） 2.4 GHz 帯域または 5 GHz 帯域の帯域幅ベースのビデオ CAC を無効にするには、**noapdot11** {**24ghz**	**5ghz**} **cacvideoacm** コマンドを使用します。
max-bandwidth	2.4 GHz 帯域または 5 GHz 帯域でビデオ アプリケーション用にクライアントに割り当てられている最大帯域幅の割合を設定します。
value	5 ～ 85 % の帯域の割合値。
roam-bandwidth	2.4 GHz 帯域または 5 GHz 帯域での CAC の最大割り当て帯域幅のうち、ビデオ クライアントのローミング用に予約する割合を設定します。
value	0 ～ 85 % の帯域の割合値。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **wlan** *wlan_name***shutdown** コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。

- **apdot11 {24ghz | 5ghz} shutdown** コマンドを入力して、設定する無線ネットワークを無効にします。
- 新しい設定を保存します。
- **apdot11 {24ghz | 5ghz} cacvoiceacm** コマンドまたは **apdot11 {24ghz | 5ghz} cacvideoacm** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

次に、帯域幅ベースの CAC をイネーブルにする例を示します。

```
Switch(config)# ap dot11 24ghz cac video acm
```

次に、選択した無線帯域でビデオ アプリケーションに割り当てられる最大帯域幅の割合を指定する例を示します。

```
Switch(config)# ap dot11 24ghz cac video max-bandwidth 50
```

次に、選択した無線帯域でビデオ クライアントのローミング用に予約された最大割り当て帯域幅の割合を指定する例を示します。

```
Switch(config)# ap dot11 24ghz cac video roam-bandwidth 10
```

関連トピック

ap dot11 cac media-stream （287 ページ）
ap dot11 cac multimedia （290 ページ）
ap dot11 cac voice （294 ページ）

ap dot11 cac voice

音声カテゴリのコールアドミッション制御（CAC）パラメータを設定するには、**apdot11cacvoice** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **cac voice**{**acm**|**load-based**|**max-bandwidth** *value*|**roam-bandwidth** *value*|**sip** [**bandwidth** *bw*] **sample-interval** *value*|**stream-size** *x* **max-streams** *y*|**tspec-inactivity-timeout**{**enable**|**ignore**}}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
acm	2.4 GHz 帯域または 5 GHz 帯域の帯域幅ベースの音声 CAC を有効にします。 （注） 2.4 GHz 帯域または 5 GHz 帯域の帯域幅ベースの音声 CAC を無効にするには、**noapdot11** {**24ghz**	**5ghz**} **cacvoiceacm** コマンドを使用します。
load-based	音声アクセス カテゴリで負荷ベースの CAC を有効にします。 （注） 2.4 GHz 帯域または 5 GHz 帯域の音声アクセス カテゴリで負荷ベースの CAC を無効にするには、**noapdot11** {**24ghz**	**5ghz**} **cacvoiceload-based** コマンドを使用します。
max-bandwidth	2.4 GHz 帯域または 5 GHz 帯域で音声アプリケーション用にクライアントに割り当てられている最大帯域幅の割合を設定します。
value	5 ～ 85 % の帯域の割合値。
roam-bandwidth	2.4 GHz 帯域または 5 GHz 帯域での CAC の最大割り当て帯域幅のうち、音声クライアントのローミング用に予約する割合を設定します。
value	0 ～ 85 % の帯域の割合値。
sip	CAC のコーデック名とサンプル間隔をパラメータとして指定し、802.11 ネットワークのコールごとに必要な帯域幅を計算します。

bandwidth	（任意）SIP ベースのコールの帯域幅を指定します。
bw	帯域幅（kbps 単位）。次の帯域幅値は SIP コーデックのパラメータを指定します。 • 64kbps：SIP G711 コーデックに CAC パラメータを指定します。 • 8kbps：SIP G729 コーデックに CAC パラメータを指定します。 （注） デフォルト値は 64 Kbps です。
sample-interval	SIP コーデックのパケット化間隔を指定します。
value	ミリ秒単位のパケット化間隔。SIP コーデック値のサンプリング間隔は 20 秒です。
stream-size	2.4 GHz 帯域または 5 GHz 帯域で指定したデータ レートでの集約音声 Wi-Fi マルチメディア（WMM）トラフィック仕様（TSPEC）ストリームの数を指定します。
○	ストリームのサイズ。ストリーム サイズの範囲は 84000 ～ 92100 です。
max-streams	TSPEC ごとのストリームの最大数を指定します。
y	音声ストリームの数（1 ～ 5）。 （注） デフォルトのストリーム数は 2 で、ストリームの平均データ レートは 84 Kbps です。
tspec-inactivity-timeout	TSPEC 非アクティブ タイムアウトの処理モードを指定します。 （注） アクセス ポイントから受信した Wi-Fi マルチメディア（WMM）トラフィック仕様（TSPEC）非アクティブ タイムアウトを処理または無視するには、このキーワードを使用します。非アクティブ タイムアウトが無視された場合、アクセス ポイントがそのクライアントの非アクティブ タイムアウトを報告しても、クライアント TSPEC は削除されません。

enable	TSPEC 無活動タイムアウト メッセージを処理します。
ignore	TSPEC 無活動タイムアウト メッセージを無視します。 （注） デフォルトは **ignore**（無効）です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

CAC コマンドを使用するには、変更を予定している WLAN を Wi-Fi Multimedia（WMM）プロトコルに対応するように設定し、Quality of Service（QoS）レベルを Platinum に設定する必要があります。

ネットワーク上で CAC パラメータを設定するには、次の準備作業を完了しておく必要があります。

- **wlan** *wlan_name***shutdown** コマンドを入力して、WMM が有効になっているすべての WLAN を無効にします。
- **apdot11** {**24ghz** | **5ghz**} **shutdown** コマンドを入力して、設定する無線ネットワークを無効にします。
- 新しい設定を保存します。
- **apdot11** {**24ghz** | **5ghz**} **cacvoiceacm** コマンドまたは **apdot11** {**24ghz** | **5ghz**} **cacvideoacm** コマンドを入力して、設定するネットワークの音声またはビデオ CAC を有効にします。

次に、帯域幅ベースの CAC をイネーブルにする例を示します。

```
Switch(config)# ap dot11 24ghz cac voice acm
```

次に、音声アクセス カテゴリの負荷ベースの CAC を有効にする例を示します。

```
Switch(config)# ap dot11 24ghz cac voice load-based
```

次に、選択した無線帯域で音声アプリケーション用に割り当てられる最大帯域幅の割合を指定する例を示します。

```
Switch(config)# ap dot11 24ghz cac voice max-bandwidth 50
```

次に、選択した無線帯域で音声クライアントのローミング用に予約された最大割り当て帯域幅の割合を指定する例を示します。

```
Switch(config)# ap dot11 24ghz cac voice roam-bandwidth 10
```

次に、2.4 GHz 帯域の G729 SIP コーデックの帯域幅と音声パケット化間隔を設定する例を示します。

```
Switch(config)# ap dot11 24ghz cac voice sip bandwidth 8 sample-interval 40
```

次に、85000 のストリーム サイズと最大 5 ストリームで集約音声トラフィック仕様のストリームの数を設定する例を示します。

```
Switch(config)# ap dot11 24ghz cac voice stream-size 85000 max-streams 5
```

次に、アクセス ポイントから受信した音声 TSPEC 非アクティブ タイムアウト メッセージをイネーブルにする方法を示します。

```
Switch(config)# ap dot11 24ghz cac voice tspec-inactivity-timeout enable
```

関連トピック

ap dot11 cac media-stream （287 ページ）
ap dot11 cac multimedia （290 ページ）
ap dot11 cac video （292 ページ）

ap dot11 cleanair

802.11 ネットワークの CleanAir を設定するには、**apdot11cleanair** コマンドを使用します。802.11 ネットワークの CleanAir を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 {24ghz|5ghz} cleanair
no ap dot11 {24ghz|5ghz} cleanair

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
cleanair	2.4 GHz 帯域または 5 GHz 帯域の CleanAir を指定します。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、2.4 GHz 帯域の CleanAir 設定を有効にする例を示します。

```
Switch(config)# ap dot11 24ghz cleanair
```

関連トピック

ap dot11 cleanair alarm air-quality （299 ページ）
ap dot11 cleanair alarm device （300 ページ）
ap dot11 cleanair device （302 ページ）
ap name dot11 dual-band cleanair （363 ページ）
ap name dot11 dual-band shutdown （364 ページ）

ap dot11 cleanair alarm air-quality

Cisco Lightweight アクセス ポイントの CleanAir 電波品質アラームを設定するには、**apdot11cleanairalarmair-quality** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **cleanair alarm air-quality** [**threshold** *value*]

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
threshold	電波品質アラームのしきい値を指定します。
value	電波品質のアラームしきい値（1＝電波品質が悪い、100＝電波品質がよい）。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、2.4 GHz のCleanAir 電波品質しきい値を 90 に設定する例を示します。

```
Switch(config)# ap dot11 24ghz cleanair air-quality threshold 90
```

関連トピック

ap dot11 cleanair （298 ページ）
ap dot11 cleanair alarm device （300 ページ）
ap dot11 cleanair device （302 ページ）

ap dot11 cleanair alarm device

2.4 GHz 帯域または 5 GHz 帯域で CleanAir 干渉デバイスのアラームを設定するには、**apdot11cleanairalarmdevice** コマンドを使用します。802.11 ネットワークで CleanAir 干渉デバイスのアラームを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 {24ghz|5ghz} cleanair alarm device {all|bt-discovery|bt-link|canopy|cont-tx|dect-like|fh|inv|jammer|mw-oven|nonstd|superag|tdd-tx|video|wimax-fixed|wimax-mobile|xbox|zigbee}
no ap dot11 {24ghz|5ghz} cleanair

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
all	すべてのデバイス タイプを一度に指定します。
bt-discovery	ディスカバリ モードの Bluetooth デバイスを指定します。
bt-link	Bluetooth アクティブ リンクを指定します。
canopy	Canopy デバイスを指定します。
cont-tx	連続トランスミッタを指定します。
dect-like	Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話を指定します。
fh	周波数ホッピング デバイスを指定します。
inv	スペクトル反転 Wi-Fi 信号を使用するデバイスを指定します。
jammer	電波妨害装置を指定します。
mw-oven	電子レンジのデバイスを指定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスを指定します。
superag	802.11 SuperAG デバイスを指定します。
tdd-tx	TDD トランスミッタを指定します。
video	ビデオ カメラを指定します。
wimax-fixed	WiMax 固定デバイスを指定します。
wimax-mobile	WiMax モバイル デバイスを指定します。
xbox	Xbox デバイスを指定します。
zigbee	ZigBee デバイスを指定します。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、ZigBee 干渉検出のアラームを無効にする例を示します。

```
Switch(config)# no ap dot11 24ghz cleanair alarm device zigbee
```

次に、Bluetooth リンク検出アラームを有効にする例を示します。

```
Switch(config)# ap dot11 24ghz cleanair alarm device bt-link
```

関連トピック

ap dot11 cleanair alarm air-quality （299 ページ）
ap dot11 cleanair （298 ページ）
ap dot11 cleanair device （302 ページ）

ap dot11 cleanair device

CleanAir干渉デバイスのタイプを設定するには、**apdot11cleanairdevice**コマンドを使用します。

ap dot11 24ghz cleanair device
[{all|bt-discovery|bt-link|canopy|cont-tx|dect-like|fh|inv|jammer|mw-oven|nonstd|superag|tdd-tx|video|wimax-fixed|wimax-mobile|xbox|zigbee}]

構文の説明

all	すべてのデバイス タイプを指定します。
device	CleanAir 干渉デバイスのタイプを指定します。
bt-discovery	ディスカバリ モードのBluetoothデバイスを指定します。
bt-link	Bluetooth アクティブ リンクを指定します。
canopy	Canopy デバイスを指定します。
cont-tx	連続トランスミッタを指定します。
dect-like	Digital Enhanced Cordless Communication（DECT）デジタル コードレス電話を指定します。
fh	802.11 の周波数ホッピング デバイスを指定します。
inv	スペクトル反転 Wi-Fi 信号を使用するデバイスを指定します。
jammer	電波妨害装置を指定します。
mw-oven	電子レンジのデバイスを指定します。
nonstd	非標準 Wi-Fi チャネルを使用するデバイスを指定します。
superag	802.11 SuperAG デバイスを指定します。
tdd-tx	TDD トランスミッタを指定します。
video	ビデオ カメラを指定します。
wimax-fixed	WiMax 固定デバイスを指定します。
wimax-mobile	WiMax モバイル デバイスを指定します。
xbox	Xbox デバイスを指定します。
zigbee	ZigBee デバイスを指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、ZigBee の干渉をモニタするようにスイッチを設定する例を示します。

```
Switch(config)# ap dot11 24ghz cleanair device zigbee
```

関連トピック

ap dot11 cleanair alarm air-quality （299 ページ）
ap dot11 cleanair （298 ページ）
ap dot11 cleanair alarm device （300 ページ）

ap dot11 dot11n

802.11n ネットワークを設定するには、**apdot11dot11n** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **dot11n** {**a-mpdu tx priority** {*priority_value* **all** } | **scheduler timeout rt** *scheduler_value*}|**a-msdu tx priority** {*priority_value*|**all**}|**guard-interval** {**any**|**long**}|**mcs tx** *rate*|**rifs rx**}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
dot11n	802.11n サポートを有効にします。
a-mpdutxpriority	Aggregated MAC Protocol Data Unit（A-MPDU）伝送を使用する優先度レベルに関連するトラフィックを指定します。
priority_value	Aggregated MAC Protocol Data Unit（A-MPDU）の優先度レベル（0 ～ 7）。
all	すべての優先度レベルを一度に指定します。
a-msdutxpriority	Aggregated MAC Service Data Unit（A-MSDU）伝送を使用する優先度レベルに関連するトラフィックを指定します。
priority_value	Aggregated MAC Protocol Data Unit（A-MPDU）の優先度レベル（0 ～ 7）。
all	すべての優先度レベルを一度に指定します。
scheduler timeout rt	802.11n A-MPDU 伝送集約スケジューラのタイムアウト値（ミリ秒単位）を設定します。
scheduler_value	802.11n A-MPDU 伝送集約スケジューラのタイムアウト値（1 ～ 10000ミリ秒）。
guard-interval	ガード間隔を指定します。
any	短期または長期ガード間隔をイネーブルにします。
long	長期ガード間隔のみをイネーブルにします。
mcstx *rate*	データをアクセス ポイントとクライアント間で送信できる変調および符号化方式（MCS）レートを指定します。

rate	変調および符号化方式のデータ レートを指定します。 （注） 範囲は 0 ～ 23 です。
rifsrx	データ フレーム間の Reduced Interframe Space（RIFS）を指定します。

コマンド デフォルト

デフォルトでは 優先度 0 が有効になっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	scheduler、timeout、rt の各キーワードが追加されました。

使用上のガイドライン

集約は、パケット データ フレームを個別に伝送するのではなく、グループにまとめるプロセスです。集約には、次の 2 つの方法があります。

- A-MPDU：この集約はソフトウェアで実行されます。
- A-MSDU：この集約はハードウェアで実行されます。

トラフィック タイプごとに割り当てられた集約 MAC プロトコル データ ユニットの優先度は次のとおりです。

- 0：ベスト エフォート
- 1：バックグラウンド
- 2：スペア
- 3：エクセレント エフォート
- 4：制御ロード
- 5：ビデオ（100 ms 未満の遅延およびジッタ）
- 6：音声（10 ms 未満の遅延およびジッタ）
- 7：ネットワーク コントロール
- all：すべての優先度を一度に設定します。

（注） クライアントが使用する集約方法に合わせて優先度を設定します。

次に、2.4 GHz 帯域で 802.11n サポートを有効にする例を示します。

```
Switch(config)# ap dot11 24ghz dot11n
```

次に、優先度レベルに関連付けられたトラフィックがA-MSDU伝送を使用するようにすべての優先度レベルを設定する例を示します。

```
Switch(config)# ap dot11 24ghz dot11n a-msdu tx priority all
```

次に、長期ガード間隔だけを有効にする例を示します。

```
Switch(config)# ap dot11 24ghz dot11n guard-interval long
```

次に、MCS レートを指定する例を示します。

```
Switch(config)# ap dot11 24ghz dot11n mcs tx 5
```

次に、RIFS を有効にする例を示します。

```
Switch(config)# ap dot11 24ghz dot11n rifs rx
```

関連トピック

ap dot11 dtpc （307 ページ）

ap dot11 dtpc

Dynamic Transmit Power Control（DTPC）設定、Cisco Client eXtension（CCX）バージョン 5 Expedited Bandwidth Request 機能、および 802.11 ネットワークのフラグメンテーションしきい値を指定するには、**apdot11dtpc** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} {**dtpc**|**exp-bwreq**|**fragmentation** *threshold*}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
dtpc	Dynamic Transport Power Control（DTPC）設定を指定します。 （注） このオプションは、デフォルトで有効です。
exp-bwreq	Cisco Client eXtension（CCX）バージョン 5 Expedited Bandwidth Request 機能を指定します。 （注） Expedited Bandwidth Request 機能はデフォルトでは無効になっています。
fragmentation *threshold*	フラグメンテーションしきい値を指定します。 （注） このオプションは、**apdot11** {**24ghz** | **5ghz**} **shutdown** コマンドを使用してネットワークが無効になっている場合にだけ使用できます。
threshold	しきい値。指定できる範囲は 256 ～ 2346 バイトです（両端の値を含む）。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

CCX バージョン 5 Expedited Bandwidth Request 機能が有効になっている場合、スイッチは、この機能に関して、参加しているすべてのアクセス ポイントを設定します。

次に、5 GHz 帯域の DTPC を有効にする例を示します。

```
Switch(config)# ap dot11 5ghz dtpc
```

次に、CCX Expedited Bandwidth 設定をイネーブルにする例を示します。

```
Switch(config)# ap dot11 5ghz exp-bwrep
```

次に、5 GHz 帯域のフラグメンテーションしきい値を 1500 バイトのしきい値数で設定する例を示します。

```
Switch(config)# ap dot11 5ghz fragmentation 1500
```

関連トピック

ap dot11 beaconperiod （284 ページ）

ap dot11 edca-parameters

2.4 GHz 帯域または 5 GHz 帯域で特定の Enhanced Distributed Channel Access（EDCA）プロファイルを有効にするには、**apdot11edca-parameters** コマンドを使用します。2.4 GHz 帯域または 5 GHz 帯域で EDCA プロファイルを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**|**5ghz**} **edca-parameters** {**custom-voice**|**optimized-video-voice**|**optimized-voice**|**svp-voice**|**wmm-default**}
no ap dot11 {**24ghz**|**5ghz**} **edca-parameters** {**custom-voice**|**optimized-video-voice**|**optimized-voice**|**svp-voice**|**wmm-default**}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
edca-parameters	802.11 ネットワークで特定の Enhanced Distributed Channel Access（EDCA）プロファイルを指定します。
custom-voice	カスタム音声 EDCA パラメータを有効にします。
optimized-video-voice	EDCA 音声/ビデオ最適化パラメータを有効にします。ネットワーク上で音声サービスとビデオ サービスを両方とも展開する場合に、このオプションを選択します。
optimized-voice	EDCA 音声最適化パラメータを有効にします。ネットワーク上で SpectraLink 以外の音声サービスを展開する場合に、このオプションを選択します。
svp-voice	SpectraLink 音声優先パラメータを有効にします。コールの品質を向上させるためにネットワーク上で SpectraLink の電話を展開する場合に、このオプションを選択します。
wmm-default	Wi-Fi Multimedia（WMM）デフォルト パラメータを有効にします。音声サービスまたはビデオ サービスがネットワーク上に展開されていない場合に、このオプションを選択します。

コマンド デフォルト

wmm-default

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

リリース	変更内容
10.3	Cisco 5700 シリーズ WLC で **custom-voice** キーワードが削除されました。

次に、SpectraLink 音声優先パラメータを有効にする例を示します。

```
Switch(config)# ap dot11 24ghz edca-parameters svp-voice
```

ap dot11 rrm group-mode

802.11 の自動 RF グループ選択モードをオンに設定するには、**apdot11rrmgroup-mode** コマンドを使用します。802.11 の自動 RF グループ選択モードをオフに設定するには、このコマンドの **no** 形式を使用します。

ap dot11 {5ghz|24ghz} rrm group-mode {auto|leader|off|restart}
no ap dot11 {5ghz|24ghz} rrm group-mode

構文の説明

5ghz	2.4 GHz 帯域を指定します。
24ghz	5 GHz 帯域を指定します。
auto	802.11 RF グループ選択を自動更新モードに設定します。
leader	802.11 RF グループ選択をスタティック モードに設定し、グループ リーダーとしてこのスイッチを設定します。
off	802.11 RF グループ選択をオフに設定します。
restart	802.11 RF グループ選択を再起動します。

コマンド デフォルト

auto

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、5 GHz 帯域の自動 RF グループ選択モードをオンにする例を示します。

```
Switch(config)# ap dot11 5ghz rrm group-mode auto
```

関連トピック

ap dot11 rrm ccx location-measurement （317 ページ）
ap dot11 rrm channel cleanair-event （312 ページ）
ap dot11 rrm channel dca （318 ページ）
ap dot11 rrm group-member （321 ページ）
ap dot11 rrm logging （322 ページ）
ap dot11 rrm monitor （324 ページ）
ap dot11 rrm ndp-type （326 ページ）

ap dot11 rrm channel cleanair-event

すべての 802.11 Cisco Lightweight アクセス ポイントの CleanAir イベント駆動型無線リソース管理（RRM）パラメータを設定するには、**apdot11rrmchannelcleanair-event** コマンドを使用します。このパラメータが設定されている場合、CleanAir アクセス ポイントは、RRM 間隔が期限切れになっていなくても、干渉源によって動作が低下するとチャネルを変更できます。

ap dot11 {**24ghz**|**5ghz**} **rrm channel** {**cleanair-event sensitivity** *value*}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
sensitivity	CleanAir イベント駆動型 RRM の感度を設定します。
value	感度の値。次の3つの感度値オプションのいずれかを選択できます。 • **low**：低感度を指定します。 • **medium**：中間の感度を指定します。 • **high**：高感度を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、CleanAir イベント駆動型 RRM に高感度を設定する例を示します。

```
Switch(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity high
```

関連トピック

ap dot11 rrm ccx location-measurement （317 ページ）
ap dot11 rrm group-mode （311 ページ）
ap dot11 rrm channel dca （318 ページ）
ap dot11 rrm group-member （321 ページ）
ap dot11 rrm logging （322 ページ）
ap dot11 rrm monitor （324 ページ）
ap dot11 rrm ndp-type （326 ページ）

ap dot11 l2roam rf-params

2.4 GHz または 5 GHz のレイヤ 2 クライアント ローミング パラメータを設定するには、**apdot11l2roamrf-params** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **l2roam rf-params custom** *min-rssi roam-hyst scan-thresh trans-time*

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
custom	レイヤ 2 クライアントのカスタム ローミング RF パラメータを指定します。
min-rssi	クライアントをアクセス ポイントに関連付けるために必要な最小の受信信号強度インジケータ（RSSI）。クライアントの平均の受信信号の強度がこのしきい値より低い場合、通常、信頼できる通信はできません。したがって、最小の RSSI 値に達する前に、クライアントはより強い信号のある別のアクセス ポイントをすでに見つけてローミングしている必要があります。有効な範囲は -80 ～ -90 dBm で、デフォルト値は -85 dBm です。
roam-hyst	クライアントがローミングするために、周辺のアクセス ポイントの信号に必要な強度。このパラメータは、クライアントが 2 つのアクセス ポイント間のボーダー近くに物理的に存在している場合に、アクセス ポイント間のローミングの量を減らすことを意図しています。有効な範囲は 2 ～ 4 dB で、デフォルト値は 2 dB です。
scan-thresh	許容可能な最小 RSSI。この値を下回ると、クライアントはより適切なアクセス ポイントをローミングする必要があります。RSSI が指定された値より低い場合、クライアントは指定遷移時間内により強い信号のあるアクセス ポイントへローミングできる必要があります。このパラメータはまた、クライアントがアクティブまたはパッシブ スキャンで費やす時間を最小限に抑えるための節電方法も提供します。たとえば、クライアントは RSSI がしきい値よりも高いときにはゆっくりとスキャンし、しきい値よりも低いときにはより速くスキャンすることができます。有効な範囲は -70 ～ -77 dBm で、デフォルト値は -72 dBm です。
trans-time	クライアントのアソシエートされたアクセス ポイントからの RSSI がスキャンのしきい値を下回った場合に、クライアントがローミングに適したネイバー アクセス ポイントの検出と、ローミングの完了にかけられる最大許容時間。有効な範囲は 1 ～ 10 秒で、デフォルト値は 5 秒です。

コマンド デフォルト

min-rssi	-85
roam-hyst	2
scan-thresh	-72
trans-time	5

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、802.11a ネットワークにカスタム レイヤ 2 クライアント ローミング パラメータを設定する例を示します。

```
Switch(config)# ap dot11 5ghz l2roam rf-params custom -80 2 -70 7
```

ap dot11 media-stream

802.11 ネットワークのメディア ストリームのマルチキャスト ダイレクト設定とビデオ ダイレクト設定を指定するには、**apdot11media-stream** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **media-stream** {**multicast-direct** {**admission-besteffort**|**client-maximum** *value*|**radio-maximum** *value*}|**video-redirect**}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
multicast-direct	2.4 GHz 帯域または 5 GHz 帯域のマルチキャスト ダイレクトを指定します。
admission-besteffort	ベスト エフォート キューにメディア ストリームを許可します。
client-maximum *value*	クライアントで許可されるストリームの最大数を指定します。
radio-maximum *value*	2.4 GHz 帯域または 5 GHz 帯域で許可されるストリームの最大数を指定します。
video-redirect	2.4 GHz 帯域または 5 GHz 帯域のメディア ストリームのビデオ ダイレクトを指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

802.11 ネットワークのメディア ストリームのマルチキャスト ダイレクトまたはビデオ ダイレクトを設定する前に、ネットワークが非動作であることを確認します。

次に、5 GHz 帯域でメディア ストリームのマルチキャスト ダイレクト設定を有効にする例を示します。

```
Switch(config)# ap dot11 5ghz media-stream multicast-direct
```

次に、フローに順位付けするために十分な帯域幅がない場合に、ベストエフォート キューにメディア ストリームを許可さする例を示します。

```
Switch(config)# ap dot11 5ghz media-stream multicast-direct admission-besteffort
```

次に、クライアントで許可される最大ストリーム数を設定する例を示します。

```
Switch(config)# ap dot11 5ghz media-stream multicast-direct client-maximum 10
```

次に、5 GHz帯域でメディア ストリーム トラフィック リダイレクションを有効にする例を示します。

```
Switch(config)# ap dot11 5ghz media-stream video-redirect
```

ap dot11 rrm ccx location-measurement

2.4 GHz 帯域および 5 GHz 帯域の Cisco Client Extension（CCX）クライアント ロケーション測定を設定するには、**apdot11rrmccxlocation-measurement** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **rrm ccx location-measurement** {**disable**間隔}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
disable	CCX クライアント ロケーション測定のサポートを無効にします。
間隔	間隔（10 ～ 32400）。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、2.4 GHz の CCXクライアント ロケーション測定のサポートを無効にする例を示します。

```
Switch(config)# no ap dot11 24ghz rrm ccx location-measurement
```

関連トピック

ap dot11 rrm group-mode （311 ページ）
ap dot11 rrm channel cleanair-event （312 ページ）
ap dot11 rrm channel dca （318 ページ）
ap dot11 rrm group-member （321 ページ）
ap dot11 rrm logging （322 ページ）
ap dot11 rrm monitor （324 ページ）
ap dot11 rrm ndp-type （326 ページ）

ap dot11 rrm channel dca

802.11 ネットワークの動的チャネル割り当て（DCA）アルゴリズム パラメータを設定するには、**apdot11rrmchanneldca** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **rrm channel dca**{*channel_number*|**anchor-time** *value*|**global**{**auto**|**once**}|**interval** *value*|**min-metric** *value*|**sensitivity**{**high**|**low**|**medium**}}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
channel_number	DCA リストに追加するチャネル番号。 （注） 範囲は 1 ～ 14 です。
anchor-time	DCA アンカー時間を指定します。
value	時間（0 ～ 23）。この値は、午前 12 時から午後 11 時までの時間を表します。
global	802.11 ネットワークのアクセス ポイントに対してグローバルな DCA モードを指定します。
auto	自動 RF を有効にします。
once	ワンタイム自動 RF を有効にします。
interval	DCA の実行が許可される頻度を指定します。
value	DCA が実行できる時間の間隔。有効な値は 0、1、2、3、4、6、8、12、または 24 時間です。0 の場合は 10 分になります（600 秒）。デフォルト値は 0（10 分）です。
min-metric	DCA の最小 RSSI エネルギー メトリックを指定します。
value	最小 RSSI エネルギー メトリック値（-100 ～ -60）。
sensitivity	DCA アルゴリズムでチャネルを変更するかどうかを判断する際の、環境の変化（信号、負荷、ノイズ、干渉など）に対する感度を指定します。
high	環境の変化に対する DCA アルゴリズムの感度は特に高くないことを指定します。詳細については、「使用上のガイドライン」を参照してください。
low	環境の変化に対する DCA アルゴリズムの感度は中程度であることを指定します。詳細については、「使用上のガイドライン」を参照してください。
medium	環境の変化に対する DCA アルゴリズムの感度が高いことを指定します。詳細については、「使用上のガイドライン」を参照してください。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

DCA の感度のしきい値は、次の表で示すように、無線帯域によって異なります。

トラブルシューティングに役立つように、このコマンドの出力には失敗したコールすべてのエラー コードが示されます。次の表では、失敗したコールの考えられるエラー コードについて説明します。

表 *17 : DCA* 感度しきい値

感度	2.4 GHz DCA 感度しきい値	5 GHz DCA 感度しきい値
大きい	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

次に、2.4 GHz 帯域で午後 5 時に DCA の実行を開始するようにスイッチを設定する例を示します。

```
Switch(config)# ap dot11 24ghz rrm channel dca anchor-time 17
```

次に、2.4 GHz 帯域で 10 分ごとに実行するように DCA アルゴリズムを設定する例を示します。

```
Switch(config)# ap dot11 24ghz rrm channel dca interval 0
```

次に、2.4 GHz 帯域で DCA アルゴリズムの感度の値を low に設定する例を示します。

```
Switch(config)# ap dot11 24ghz rrm channel dca sensitivity low
```

関連トピック

ap dot11 rrm ccx location-measurement （317 ページ）
ap dot11 rrm channel cleanair-event （312 ページ）
ap dot11 rrm group-mode （311 ページ）
ap dot11 rrm group-member （321 ページ）
ap dot11 rrm logging （322 ページ）
ap dot11 rrm monitor （324 ページ）

ap dot11 rrm ndp-type （326 ページ）

ap dot11 rrm group-member

802.11 静的 RF グループのメンバを設定するには、**apdot11rrmgroup-member** コマンドを使用します。802.11 RF グループからメンバを削除するには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**|**5ghz**} **rrm group-member** *controller-name controller-ip*
no ap dot11 {**24ghz**|**5ghz**} **rrm group-member** *controller-name controller-ip*

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
controller-name	追加するスイッチの名前。
controller-ip	追加するスイッチの IP アドレス。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、5 GHz 帯域 RF グループにスイッチを追加する例を示します。

```
Switch(config)# ap dot11 5ghz rrm group-member cisco-controller 192.0.2.54
```

関連トピック

ap dot11 rrm ccx location-measurement （317 ページ）
ap dot11 rrm channel cleanair-event （312 ページ）
ap dot11 rrm channel dca （318 ページ）
ap dot11 rrm group-mode （311 ページ）
ap dot11 rrm logging （322 ページ）
ap dot11 rrm monitor （324 ページ）
ap dot11 rrm ndp-type （326 ページ）

ap dot11 rrm logging

サポートされている 802.11 ネットワークのレポート ログを設定するには、**apdot11rrmlogging** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **rrm logging** {**channel**|**coverage**|**foreign**|**load**|**noise**|**performance**|**txpower**}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
channel	チャネル変更ロギング モードをオンまたはオフにします。デフォルト モードはオフ（無効）です。
coverage	カバレッジ プロファイル ロギング モードをオンまたはオフにします。デフォルト モードはオフ（無効）です。
foreign	外部干渉プロファイル ロギング モードをオンまたはオフにします。デフォルト モードはオフ（無効）です。
load	負荷プロファイル ロギング モードをオンまたはオフにします。デフォルト モードはオフ（無効）です。
noise	ノイズ プロファイル ロギング モードをオンまたはオフにします。デフォルト モードはオフ（無効）です。
performance	パフォーマンス プロファイル ロギング モードをオンまたはオフにします。デフォルト モードはオフ（無効）です。
txpower	中継電力変更ロギング モードをオンまたはオフにします。デフォルト モードはオフ（無効）です。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、5 GHz ロギング チャネル選択モードをオンにする例を示します。

```
Switch(config)# ap dot11 5ghz rrm logging channel
```

次に、5 GHz カバレッジ プロファイル違反ロギング選択モードをオンにする例を示します。

```
Switch(config)# ap dot11 5ghz rrm logging coverage
```

次に、5 GHz 外部干渉プロファイル違反ロギング選択モードをオンにする例を示します。

```
Switch(config)# ap dot11 5ghz rrm logging foreign
```

次に、5 GHz 負荷プロファイル ロギング モードをオンにする例を示します。

```
Switch(config)# ap dot11 5ghz rrm logging load
```

次に、5 GHz ノイズ プロファイル ロギング モードをオンにする例を示します。

```
Switch(config)# ap dot11 5ghz rrm logging noise
```

次に、5 GHz パフォーマンス プロファイル ロギング モードをオンにする例を示します。

```
Switch(config)# ap dot11 5ghz rrm logging performance
```

次に、5 GHz 伝送パワー変更モードをオンにする例を示します。

```
Switch(config)# ap dot11 5ghz rrm logging txpower
```

関連トピック

ap dot11 rrm ccx location-measurement （317 ページ）
ap dot11 rrm channel cleanair-event （312 ページ）
ap dot11 rrm channel dca （318 ページ）
ap dot11 rrm group-member （321 ページ）
ap dot11 rrm group-mode （311 ページ）
ap dot11 rrm monitor （324 ページ）
ap dot11 rrm ndp-type （326 ページ）

ap dot11 rrm monitor

802.11 ネットワークのモニタを設定するには、**apdot11rrmmonitor** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **rrm monitor**{**channel-list**|{**all**|**country**|**dca**}|**coverage**|**load**|**noise**|**signal**} *seconds*

構文の説明

24ghz	802.11b パラメータを指定します。
5ghz	802.11a パラメータを指定します。
channel-listall	すべてのチャネルのノイズ、干渉、不正モニタリング チャネル リストをモニタします。
channel-listcountry	設定されている国で使用するチャネルのノイズ、干渉、不正モニタリング チャネル リストをモニタします。
channel-listdca	自動チャネル割り当てによって使用されるチャネルのノイズ、干渉、不正モニタリング チャネル リストをモニタします。
coverage	カバレッジ測定間隔を指定します。
load	負荷測定間隔を指定します。
noise	ノイズ測定間隔を指定します。
signal	信号測定間隔を指定します。
rssi-normalization	RRM ネイバー探索 RSSI 正規化を設定します。
seconds	測定間隔は 60 ～ 3600 秒です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、設定されている国で使用するチャネルを監視する例を示します。

```
Switch(config)# ap dot11 24ghz rrm monitor channel-list country
```

次に、カバレッジ測定間隔を 60 秒に設定する例を示します。

```
Switch(config)# ap dot11 24ghz rrm monitor coverage 60
```

関連トピック

- ap dot11 rrm ccx location-measurement （317 ページ）
- ap dot11 rrm channel cleanair-event （312 ページ）
- ap dot11 rrm channel dca （318 ページ）
- ap dot11 rrm group-member （321 ページ）
- ap dot11 rrm logging （322 ページ）
- ap dot11 rrm group-mode （311 ページ）
- ap dot11 rrm ndp-type （326 ページ）

ap dot11 rrm ndp-type

802.11 アクセスポイント無線リソース管理ネイバー ディスカバリ プロトコル タイプを設定するには、**apdot11rrmndp-type** コマンドを使用します。

ap dot11 {24ghz|5ghz} rrm ndp-type {protected|transparent}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
protected	Tx RRM で保護された（暗号化された）ネイバー ディスカバリ プロトコルを指定します。
transparent	Tx RRM の透過的な（暗号化されていない）ネイバー ディスカバリ プロトコルを指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

802.11 アクセス ポイント RRM のネイバー ディスカバリ プロトコル タイプを設定する前に、**apdot11 {24ghz | 5ghz} shutdown** コマンドを入力してネットワークを無効にしていることを確認してください。

次に、802.11a アクセス ポイント RRM ネイバー ディスカバリ プロトコル タイプを protected として有効にする例を示します。

```
Switch(config)# ap dot11 5ghz rrm ndp-type protected
```

関連トピック

ap dot11 rrm ccx location-measurement （317 ページ）
ap dot11 rrm channel cleanair-event （312 ページ）
ap dot11 rrm channel dca （318 ページ）
ap dot11 rrm group-member （321 ページ）
ap dot11 rrm logging （322 ページ）
ap dot11 rrm group-mode （311 ページ）
ap dot11 rrm monitor （324 ページ）

ap dot11 5ghz dot11ac frame-burst

802.11ac フレームバーストを設定するには、**apdot115ghzdot11acframe-burst** コマンドを使用します。802.11ac A-MPDU のバースティングを無効にするには、このコマンドの **no** 形式を使用します。

ap dot115ghzdot11acframe-burst

noap dot115ghzdot11acframe-burst

ap dot115ghzdot11acframe-burstautomatic

noap dot115ghzdot11acframe-burstautomatic

構文の説明

5ghz	802.11a パラメータを設定します。
frame-burst	802.11ac A-MPDU のバースティングを設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.6E	このコマンドが導入されました。

例

次に、802.11ac A-MPDU のバースティングを設定する例を示します。

```
Switchap dot11 5ghz
  dot11ac frame-burst
```

ap dot1x max-sessions

各アクセス ポイントに許可されている同時 802.1X セッションの最大数を設定するには、**apdot1xmax-sessions** コマンドを使用します。

ap dot1x max-sessions *num-of-sessions*

構文の説明

num-of-sessions	一度の AP あたりの 802.1X セッション開始の最大数。範囲は 0～255 で、0 は無制限を示します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

802.1Xメッセージを使用によって発生するフラッディング攻撃から保護するために、アクセスポイントごとに開始される同時 802.1X セッションの数を制限する必要があります。

次に、同時 802.1X セッションの最大数を設定する例を示します。

```
Switch(config)# ap dot1x max-sessions 100
```

ap dot1x username

現在スイッチに参加しているすべてのアクセスポイントと今後スイッチに参加するアクセスポイントの 802.1X ユーザ名およびパスワードを設定するには、**apdot1xusername** コマンドを使用します。現在スイッチに参加しているすべてのアクセスポイントの 802.1X ユーザ名およびパスワードを無効にするには、このコマンドの **no** 形式を使用します。

ap dot1x username *user-id* **password**{**0**|**8**} *password-string*
no ap dot1x username *user-id***password**{**0**|**8**} *password-string*

構文の説明

user-id	[Username]。
password	すべてのアクセス ポイントの 802.1X パスワードを指定します。
0	暗号化されていないパスワードを指定します。
8	AES 暗号化パスワードを指定します。
password_string	パスワード。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

強度が高いパスワードを入力する必要があります。強度が高いパスワードの特徴は次のとおりです。

- 少なくとも 8 文字の長さである。
- 小文字と大文字、数字、および記号の組み合わせを含む。
- どの言語の単語でもない。

特定のアクセス ポイントの値を設定できます。

次に、すべてのアクセス ポイントにグローバル認証ユーザ名およびパスワードを設定する例を示します。

```
Switch(config)# ap dot1x username cisco123 password 0 cisco2020
```

関連トピック

show ap summary （505 ページ）

ap ethernet duplex

Lightweight アクセス ポイントのイーサネット ポート デュプレックスおよび速度を設定するには、**apethernetduplex** コマンドを使用します。Lightweight アクセス ポイントのイーサネット ポート デュプレックスおよび速度を無効にするには、このコマンドの **no** 形式を使用します。

ap ethernet duplex *duplex* **speed** *speed*
no ap ethernet

構文の説明

duplex	イーサネット ポートのデュプレックス設定。次のオプションを指定してデュプレックスを設定できます。 • **auto**：イーサネット ポートの自動二重設定を指定します。 • **half**：イーサネット ポートの半二重設定を指定します。 • **full**：イーサネット ポートの全二重設定を指定します。
speed	イーサネット ポート速度の設定を指定します。
speed	イーサネット ポートの速度設定。次のオプションを指定して速度を設定できます。 • **auto**：イーサネット ポート速度を自動に指定します。 • **10**：イーサネット ポート速度を 10 Mbps に指定します。 • **100**：イーサネット ポート速度を 100 Mbps に指定します。 • **1000**：イーサネット ポート速度を 1000 Mbps に指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、すべてのアクセス ポイントで 1000 Mbps としてイーサネット ポートの全二重を設定する例を示します。

```
Switch(config)# ap ethernet duplex full speed 1000
```

関連トピック

show ap summary （505 ページ）

ap group

新しいアクセス ポイント グループを作成するには、**apgroup** コマンドを使用します。アクセス ポイント グループを削除するには、このコマンドの **no** 形式を使用します。

ap group *group-name*
no ap group *group-name*

構文の説明

group-name	アクセスポイントグループ名。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

1 つ以上のアクセス ポイントで使用しているアクセス ポイント グループを削除しようとすると、エラー メッセージが表示されます。AP グループを削除するには、まず、このグループのすべての AP を別のグループに移動します。アクセス ポイントが default-group アクセス ポイント グループに自動的に移動されることはありません。AP を表示するには、**showapsummary** コマンドを入力します。アクセス ポイントを移動するには、**apname** *Cisco-AP***ap-groupname** *Group-Name* コマンドを入力します。

次に、新しいアクセス ポイント グループを作成する例を示します。

```
Switch(config)# ap group sampleapgroup
```

関連トピック

ap name ap-groupname （341 ページ）

ap image

スイッチに関連付けられているすべてのアクセス ポイントでイメージを設定するには、**apimage** コマンドを使用します。

ap image {**predownload**|**reset**|**swap**}

構文の説明

predownload	すべてのアクセス ポイントにイメージのプレダウンロードを開始するように指示します。
reset	すべてのアクセス ポイントに再起動するように指示します。
swap	すべてのアクセス ポイントにイメージを切り替えるように指示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、すべてのアクセス ポイントにイメージをプレダウンロードする例を示します。

```
Switch# ap image predownload
```

次に、すべてのアクセス ポイントを再起動する例を示します。

```
Switch# ap image reset
```

次に、アクセス ポイントのプライマリ イメージとセカンダリ イメージを切り替える例を示します。

```
Switch# ap image swap
```

関連トピック

show ap image （455 ページ）

ap ipv6 tcp adjust-mss

すべてのシスコ AP の IPv6 TCP 最大セグメント サイズ（MSS）値を設定するには、**ap ipv6 tcp adjust-mss** コマンドを使用します。

ap ipv6 tcp adjust-mss *size*
no ap ipv6 tcp adjust-mss *size*

構文の説明

adjust-mss	すべてのシスコ AP の IPv6 TCP MSS を設定します。
size	MSS 値（500 ～ 1440）。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

MSS 値は 500 ～ 1440 の範囲でなければなりません。

次に、すべてのシスコ アクセス ポイントの IPv6 TCP MSS 値を 600 に設定する例を示します。

```
Switch(config)# ap ipv6 tcp adjust-mss 600
```

ap led

アクセス ポイントの LED ステートを有効にするには、**apled** コマンドを使用します。アクセス ポイントの LED ステートを無効にするには、このコマンドの **no** 形式を使用します。

ap led
no ap led

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの LED ステートを有効にする例を示します。

```
Switch(config)# ap led
```

ap link-encryption

アクセス ポイントの Datagram Transport Layer Security（DTLS）データ暗号化を有効にするには、**aplink-encryption** コマンドを使用します。アクセス ポイントの DTLS データ暗号化を無効にするには、このコマンドの **no** 形式を使用します。

ap link-encryption
no ap link-encryption

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、コントローラに参加しているすべてのアクセス ポイントのデータ暗号化を有効にする例を示します。

```
Switch(config)# ap link-encryption
```

関連トピック

ap link-latency （338 ページ）

ap link-latency

スイッチ に現在関連付けられているすべてのアクセス ポイントのリンク遅延を有効にするには、**aplink-latency** コマンドを使用します。スイッチ に現在関連付けられているすべてのアクセス ポイントのリンク遅延を無効にするには、このコマンドの **no** 形式を使用します。

ap link-latency ［**reset**］
no ap link-latency

構文の説明

reset	（任意）すべてのアクセスポイントのリンク遅延をリセットします。

コマンド デフォルト

リンク遅延は、デフォルトでは無効になります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、現在スイッチに参加しているアクセスポイントだけに対してリンク遅延を有効または無効にします。将来 join されるアクセス ポイントには適用されません。

次に、すべてのアクセス ポイントのリンク遅延を有効にする例を示します。

```
Switch(config)# ap link-latency
```

関連トピック

ap link-encryption （337 ページ）

ap mgmtuser username

アクセス ポイント管理用のユーザ名、パスワード、シークレット パスワードを設定するには、**apmgmtuserusername** コマンドを使用します。

ap mgmtuser username *username* **password** *password_type password* **secret** *secret_type secret*

構文の説明

username	アクセスポイント管理用のユーザ名を指定します。
password	アクセス ポイント管理用のパスワードを指定します。
password_type	パスワード タイプ。次の 2 つのパスワード タイプのいずれかを指定できます。 • **0**：暗号化されていないパスワードが後に続くことを示します。 • **8**：AES暗号化パスワードが続くことを指定します。
password	アクセス ポイント管理パスワード。 （注） パスワードは、サービス パスワード暗号化によって暗号化されません。
secret	特権アクセス ポイント管理用のシークレット パスワードを指定します。
secret_type	シークレット タイプ。次の 2 つのシークレット タイプのいずれかを指定できます。 • **0**：暗号化されていないシークレット パスワードが後に続くことを示します。 • **8**：AES 暗号化シークレット パスワードが続くことを指定します。
secret	アクセス ポイント管理シークレット パスワード。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

強力なパスワードを指定するには、次のパスワード要件を満たす必要があります。

- パスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスが含まれる必要があります。
- パスワード内で同じ文字を連続して 4 回以上繰り返すことはできません。
- パスワードに管理ユーザ名や逆にしたユーザ名を含めることはできません。
- パスワードに使用しないほうがよい文字には、Cisco、oscic、admin、nimda などの語のほか、大文字の代わりに 1 や |、！を、o の代わりに 0 を、s の代わりに $ を使用して置き換えた文字などがあります。

強力なシークレット パスワードを指定するには、次の要件を満たす必要があります。

- シークレット パスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスが含まれる必要があります。

次に、アクセス ポイント管理用のユーザ名、パスワード、シークレット パスワードを追加する例を示します。

```
Switch(config)# ap mgmtuser username glbusr password 0 Arc_1234 secret 0 Mid_1234
```

ap name ap-groupname

特定のアクセス ポイント グループに Cisco Lightweight アクセス ポイントを追加するには、**apnameap-groupname** コマンドを使用します。

ap name *ap-name* **ap-groupname** *group-name*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
group-name	アクセスポイントグループの内容がわかる名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

Cisco Lightweight アクセス ポイントを無効にしてから、このパラメータを変更する必要があります。

次に、アクセス ポイント AP01 をアクセス ポイント グループ スーパーユーザに追加する例を示します。

```
Switch# ap name AP01 ap-groupname superusers
```

関連トピック

ap group （333 ページ）
show ap summary （505 ページ）

ap name antenna band mode

アンテナ モードを設定するには、**ap name<AP name> antenna-band-mode{ single | dual }** コマンドを使用します。

ap name*ap-name***antenna-band-mode**{**single**|**dual**}

構文の説明

ap- name	Cisco Lightweight アクセス ポイントの名前。
antenna-band-mode	アクセス ポイントにアンテナのバンド モードを有効にするように指示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、アクセス ポイントのアンテナ バンド モードを設定する例を示します。

```
Switchap name <ap-name> antenna-band-mode single
```

ap name bhrate

Cisco Bridge Backhaul Tx Rate を設定するには、**apnamebhrate** コマンドを使用します。

ap name *ap-name* **bhrate** *kbps*

構文の説明

ap-name	Cisco アクセス ポイントの名前。
kbps	Cisco Bridge Backhaul Tx Rate（Kbps）。有効な値は、6000、12000、18000、24000、36000、48000、および 54000 です。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、Cisco Bridge Backhaul Tx Rate を 54000 kbps に設定する例を示します。

```
Switch# ap name AP02 bhrate 54000
```

ap name bridgegroupname

Cisco Lightweight アクセス ポイントでブリッジ グループ名を設定するには、**apnamebridgegroupname** コマンドを使用します。Cisco Lightweight アクセス ポイントでブリッジ グループ名を削除するには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **bridgegroupname** *bridge_group_name*
ap name *ap-name* **no bridgegroupname**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

同じブリッジ グループ名を持つアクセス ポイントだけが相互に接続できます。アクセス ポイントのブリッジ グループ名を変更すると、ブリッジ アクセス ポイントが機能しなくなる場合があります。

次に、Cisco アクセス ポイントのブリッジ グループ名 AP02 でブリッジ グループ名を設定する例を示します。

```
Switch# ap name AP02 bridgegroupname West
```

次に、Cisco アクセス ポイントのブリッジ グループ名 AP02 でブリッジ グループ名を削除する例を示します。

```
Switch# ap name AP02 no bridgegroupname
```

ap name bridging

Cisco Lightweight アクセス ポイントでイーサネット間ブリッジングを有効にするには、**apnamebridging** コマンドを使用します。Cisco Lightweight アクセス ポイントでイーサネット間ブリッジングを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **bridging**
ap name *ap-name* **no bridging**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントでイーサネット間ブリッジングを有効にする例を示します。

```
Switch# ap name TSIM_AP2 bridging
```

関連トピック

ap bridging （269 ページ）

ap name cdp interface

Cisco Lightweight アクセス ポイントで Cisco Discovery Protocol（CDP）を有効にするには、**apname** コマンドを使用します。Cisco Lightweight アクセス ポイントで Cisco Discovery Protocol（CDP）を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **cdp interface** {**ethernet** *ethernet-id*|**radio** *radio-id*}
ap name *ap-name* ［**no**］ **cdp interface** {**ethernet** *ethernet-id*|**radio** *radio-id*}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
ethernet	イーサネットインターフェイス上でCDPを有効にします。
ethernet-id	イーサネット インターフェイス番号（0 ～ 3）。
radio	無線インターフェイスの CDP を有効にします。
radio-id	無線 ID スロット番号（0 ～ 3）。

コマンド デフォルト

すべてのアクセス ポイントで無効になっています。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

イーサネット/無線インターフェイス上の CDP は、CDP が有効になっている場合にだけ使用できます。スイッチに参加しているすべてのアクセスポイントでCDPを有効にした後は、**apname** *ap-name***cdpinterfaceethernet** *ethernet-id* cisco_ap コマンドを使用して、個々のアクセス ポイントで CDP を無効にし、再度有効にすることができます。スイッチに参加しているすべてのアクセス ポイントで CDP を無効にした後は、個々のアクセス ポイントで CDP を有効にし、無効にすることはできません。

次に、アクセス ポイントでイーサネット インターフェイス番号 0 の CDP を有効にする例を示します。

```
Switch# ap name TSIM_AP2 cdp interface ethernet 0
```

ap name console-redirect

Cisco Lightweight アクセス ポイントのリモート デバッグ出力をコンソールにリダイレクトするには、**apnameconsole-redirect** コマンドを使用します。Cisco Lightweight アクセス ポイントのリモート デバッグ出力のコンソールへのリダイレクトを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **console-redirect**
ap name *ap-name* ［**no**］ **console-redirect**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、AP02 というシスコのアクセス ポイントのリモート デバッグ出力のコンソールへのリダイレクトを有効にする例を示します。

```
Switch# ap name AP02 console-redirect
```

ap name capwap retransmit

アクセス ポイント制御パケットの再送信間隔と制御パケットの再送信回数を設定するには、**apnamecapwapretransmit** コマンドを使用します。

ap name *ap-name* **capwap retransmit** {**count** *count-value*|**interval** *interval-time*}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
count	制御パケットが再送信される回数を設定します。
count-value	制御パケットが再送信される回数（3 ～ 8）。
interval	制御パケットの再送信タイムアウト間隔を設定します。
interval-time	制御パケットの再送信タイムアウト（2 ～ 5 秒）。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの再送信間隔を設定する例を示します。

```
Switch# ap name AP01 capwap retransmit interval 5
```

次に、特定のアクセス ポイントに対する再送信の再試行回数を設定する例を示します。

```
Switch# ap name AP01 capwap retransmit count 5
```

ap name command

特定のシスコのアクセス ポイントでコマンドをリモート実行するには、**apnamecommand** コマンドを使用します。

ap name *ap-name* **command "***command* **"**

構文の説明

ap-name	Cisco アクセス ポイントの名前。
command	シスコのアクセスポイントで実行するコマンド。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、TSIM_AP2 というシスコのアクセス ポイントに **show ip interface brief** コマンドをリモート入力する例を示します。

```
Switch# ap name AP2 command "show ip interface brief"
```

ap name core-dump

Cisco Lightweight アクセス ポイントのメモリ コア ダンプを設定するには、**apnamecore-dump** コマンドを使用します。Cisco Lightweight アクセス ポイントのメモリ コア ダンプを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **core-dump** *tftp-ip-addr filename* {**compress**|**uncompress**}
ap name *ap-name* [**no**]**core-dump**

構文の説明

ap-name	アクセス ポイントの名前。
tftp-ip-addr	アクセス ポイントがコア ダンプ ファイルを送信する Trivial File Transfer Protocol（TFTP）サーバの IP アドレス。
filename	コア ファイルのラベルを付けるためにアクセス ポイントが使用する名前。
compress	コア ダンプ ファイルを圧縮します。
uncompress	コア ダンプ ファイルを圧縮解除します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、アクセス ポイントが TFTP サーバに到達できる必要があります。

次に、コア ダンプ ファイルを設定して圧縮する例を示します。

```
Switch# ap name AP2 core-dump 192.1.1.1 log compress
```

関連トピック

ap core-dump （277 ページ）

ap name country

Cisco Lightweight アクセス ポイントを使用する国を設定するには、**apnamecountry** コマンドを使用します。

ap name *ap-name* **country** *country-code*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
country-code	2 文字または 3 文字の国コード。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

Cisco スイッチは、ネットワーク管理者または資格のある IP プロフェッショナルがインストールしてください。その際、正しい国コードを選択する必要があります。インストール後は、法的な規制基準を遵守するためおよび、適切なユニット機能を保証するために、ユニットへのアクセスはパスワードで保護する必要があります。最新の国コードおよび規制区域については、関連する製品マニュアルを参照してください。また、アクセス ポイントの規制区域は、アクセス ポイントの製造プロセス中に定義されます。アクセス ポイントの国コードは、アクセス ポイントの規制区域内で有効な国と一致する国コードに変更できます。アクセス ポイントの規制区域に対して有効でない国を入力しようとすると、コマンドは失敗します。

次に、Cisco Lightweight アクセス ポイントの国コードを DE に設定する例を示します。

```
Switch# ap name AP2 country JP
```

関連トピック

ap country （278 ページ）

ap name crash-file

シスコのアクセス ポイントのクラッシュ データおよび無線コア ファイルを管理するには、**apnamecrash-file** コマンドを使用します。

ap name *ap-name* **crash-file** {**get-crash-data**|**get-radio-core-dump** {**slot 0**|**slot 1**}}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
get-crash-data	Cisco Lightweight アクセス ポイントの最新のクラッシュ データを収集します。
get-radio-core-dump	Cisco Lightweight アクセス ポイントの無線コア ダンプを取得します。
slot	シスコのアクセス ポイントのスロット ID。
0	スロット 0 を指定します。
1	スロット 1 を指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイント A3 の最新のクラッシュ データを収集する例を示します。

```
Switch# ap name AP3 crash-file get-crash-data
```

次に、アクセス ポイント AP02 とスロット 0 の無線コア ダンプを収集する例を示します。

```
Switch# ap name AP02 crash-file get-radio-core-dump slot 0
```

関連トピック

ap crash-file （279 ページ）

ap name dot11 24ghz rrm coverage

2.4 GHz 帯域でカバレッジ ホール検出を設定するには、**apnamedot1124ghzrrmcoverage** コマンドを使用します。

ap name *ap-name* **dot11 24ghz rrm coverage** {**exception** *value*|**level** *value*}

構文の説明

ap-name	Cisco アクセス ポイントの名前。
exception	アクセスポイント上で、信号レベルが低くなっているにもかかわらず、別のアクセス ポイントにローミングできないクライアントの割合を指定します。
value	クライアントの割合。有効な値は 0 ～ 100 % です。 （注） デフォルトは 25% です。
level	アクセス ポイント上でデータまたは音声 RSSI しきい値以下の受信信号強度表示（RSSI）値を持つクライアントの最小数を指定します。
value	クライアントの最小数。有効な値は 1 ～ 75 です。 （注） デフォルトは 3 です。

コマンド デフォルト

exception パラメータのデフォルトは 25%、*level* パラメータのデフォルトは 3 です。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

カバレッジホール検出を有効にすると、カバレッジが不完全な領域に位置する可能性のあるクライアントを持つアクセス ポイントがあるかどうかを、アクセス ポイントから受信したデータに基づいてスイッチが自動的に判断します。

5 秒間で失敗したパケットの数と割合の両方が、**apdot1124ghzrrmcoveragedatapacket-count** *count* コマンドと **apdot1124ghzrrmcoveragedatafail-percentage** *percentage* コマンドに入力された値を超える場合、クライアントは事前アラーム状態と判断されます。スイッチは、この情報を使用してカバレッジ ホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。失敗したクライアントの数と割合の両方が、90 秒以上にわたって、**apdot1124ghzrrmcoverageexception** コマンドと **apdot1124ghzrrmcoveragelevel** コマンドで入力した値以上になると、カバレッジ ホールが検出されます。スイッチは、カバレッジ ホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、信号レベルが低くなっている 2.4 GHz 無線アクセス ポイントにクライアントの割合を指定する例を示します。

```
Switch# ap name AP2 dot11 24ghz rrm coverage exception 25%
```

次に、RSSI しきい値以下の RSSI 値を持つ 802.11b アクセス ポイントでクライアントの最小数を指定する例を示します。

```
Switch# ap name AP2 dot11 24ghz rrm coverage level 60
```

関連トピック

ap name dot11 49ghz rrm profile （355 ページ）
ap name dot11 5ghz rrm channel （357 ページ）

ap name dot11 49ghz rrm profile

4.9G Hz パブリック セーフティ チャネル上の Cisco Lightweight アクセス ポイントの無線リソース管理（RRM）パフォーマンス プロファイルを設定するには、**apnamedot1149ghzrrmprofile** コマンドを使用します。

ap name *ap-name* **dot11 49ghz rrm profile** {**clients** *value*|**customize**|**exception** *value*|**foreign** *value*|**level** *value*|**noise** *value*|**throughput** *value*|**utilization** *value*}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
clients	アクセス ポイント クライアントしきい値を設定します。
value	アクセス ポイント クライアントしきい値（1 ～ 75 クライアント）。 （注） デフォルトのクライアントしきい値は 12 です。
customize	アクセス ポイントのパフォーマンス プロファイルのカスタマイズをオンにします。 （注） デフォルトでは、パフォーマンス プロファイルのカスタマイズはオフになっています。
exception *value*	シスコの 802.11a 対応アクセス ポイントのカバレッジ例外レベルを設定します（0 ー 100 □）。
foreign	外部 802.11 トランスミッタ干渉しきい値を設定します。
value	外部 802.11 トランスミッタ干渉しきい値（0 ～ 100 %）。 （注） デフォルトは 10 % です。
level *value*	シスコの 802.11a 対応アクセス ポイントのクライアント最小例外レベルを設定します（1 ー 75 クライアント）。
noise	802.11 外部ノイズしきい値を設定します。
value	802.11 外部ノイズしきい値（-127 ～ 0 dBm）。 （注） デフォルトは -70 dBm です。
throughput	データ レート スループットしきい値を設定します。
value	802.11 スループットしきい値（1000 ～ 10000000 バイト/秒） （注） デフォルトは、1,000,000 バイト/秒です。

utilization	RF 使用率しきい値を設定します。 （注） オペレーティング システムがこのしきい値を超えた場合にトラップを生成します。
value	802.11 RF使用率しきい値（0 ～ 100 %）。 （注） デフォルトは 80% です。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、AP1 のクライアント数のしきい値を 75 個のクライアントに設定する例を示します。

```
Switch# ap name AP1 dot11 49ghz rrm profile clients 75
```

次に、4.9 GHz チャネル上の Cisco Lightweight アクセス ポイント AP1 のパフォーマンス プロファイルのカスタマイズをオンにする例を示します。

```
Switch# ap name AP1 dot11 49ghz rrm profile customize
```

次に、AP1 の外部トランスミッタ干渉しきい値を 0 パーセントに設定する例を示します。

```
Switch# ap name AP1 dot11 49ghz rrm profile foreign 0
```

次に、AP1 の外部ノイズしきい値を 0 dBm に設定する例を示します。

```
Switch# ap name AP1 dot11 49ghz rrm profile noise 0
```

次に、AP1 のデータ レートしきい値を 10,000,000 バイト/秒に設定する例を示します。

```
Switch# ap name AP1 dot11 49ghz rrm profile throughput 10000000
```

次に、AP1 の RF 利用率のしきい値を 100 パーセントに設定する例を示します。

```
Switch# ap name AP1 dot11 49ghz rrm profile utilization 100
```

関連トピック

ap name dot11 24ghz rrm coverage （353 ページ）
ap name dot11 5ghz rrm channel （357 ページ）

ap name dot11 5ghz rrm channel

802.11h チャネル アナウンスを使用して新しいチャネルを設定するには、**apnamedot115ghzrrmchannel** コマンドを使用します。

ap name *ap-name* **dot11 5ghz rrm channel** *channel*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
channel	新しいチャネル。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、802.11h チャネルを使用して新しいチャネルを設定する例を示します。

```
Switch# ap name AP01 dot11 5ghz rrm channel 140
```

関連トピック

ap name dot11 24ghz rrm coverage （353 ページ）
ap name dot11 49ghz rrm profile （355 ページ）

ap name dot11 antenna

異なる 802.11 ネットワーク上の Cisco Lightweight アクセス ポイントの無線アンテナを設定するには、**apnamedot11antenna** コマンドを使用します。

ap name *ap-name* **dot11** {**24ghz|5ghz**} **antenna** {**ext-ant-gain** ゲイン|**mode** {**omni|sectorA|sectorB**}|**selection** {**external|internal**}}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
ext-ant-gain	802.11 ネットワークの外部アンテナ ゲインを指定します。 （注） このコマンドを入力する前に、**apdot11** {**24ghz | 5ghz**} **shutdown** コマンドを使用してシスコの無線を無効にしてください。このコマンドを入力した後に、**noapdot11** {**24ghz | 5ghz**} **shutdown** コマンドを使用してシスコの無線を再度有効にできます。
ゲイン	0.5 dBm 単位でアンテナ ゲインを入力します（例：2.5 dBm = 5）。
mode	Cisco Lightweight アクセス ポイントが、802.11 の 180 度セクター化カバレッジ パターンに 1 つの内部アンテナを、または 802.11 の 360 度全方向性カバレッジ パターンに両方の内部アンテナを使用するように指定します。
omni	両方の内部アンテナを使用するように指定します。
sectorA	サイド A の内部アンテナだけを使用するように指定します。
sectorB	サイド B の内部アンテナだけを使用するように指定します。
selection	802.11 ネットワーク上の Cisco Lightweight アクセス ポイントの内部または外部アンテナ選択を指定します。
external	外部アンテナを指定します。
internal	内部アンテナを指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、5 GHz 外部アンテナ ゲインとして 0.5 dBm を AP1 に設定する例を示します。

```
Switch# ap name AP1 dot11 5ghz antenna ext-ant-gain 0.5
```

次に、2.4 GHz 帯域上でアクセス ポイント AP01 のアンテナを 360 度全方向性パターンに設定する例を示します。

```
Switch# ap name AP01 dot11 24ghz antenna mode omni
```

次に、2.4 GHz 帯域上のアクセス ポイント AP02 が内部アンテナを使用するように設定する例を示します。

```
Switch# ap name AP02 dot11 24ghz antenna selection interval
```

関連トピック

ap name dot11 antenna extantgain （360 ページ）

ap name dot11 antenna extantgain

4.9G Hz および 5.8 GHz パブリック セーフティ チャネル上の Cisco Lightweight アクセス ポイントの無線アンテナを設定するには、**apnamedot11antennaextantgain** コマンドを使用します。

ap name *ap-name* **dot11** {**49ghz|58ghz**} {**antenna extantgain** ゲイン}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
49ghz	4.9 GHz パブリック セーフティ チャネル設定を指定します。
58ghz	5.8 GHz パブリック セーフティ チャネル設定を指定します。
ゲイン	0.5 dBm 単位でアンテナ ゲインを入力します（例：2.5 dBm＝5）。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを入力する前に、**apdot11** {**24ghz** | **5ghz**} **shutdown** コマンドを使用してシスコの無線を無効にしてください。このコマンドを入力した後に、**noapdot11** {**24ghz** | **5ghz**} **shutdown** コマンドを使用してシスコの無線を再度有効にできます。

次に、外部アンテナ ゲインとして 0.5 dBm を 4.9 GHz パブリック セーフティ チャネル上の AP1 に設定する例を示します。

```
Switch# ap name AP1 dot11 49ghz antenna extantgain 0.5
```

関連トピック

ap name dot11 antenna （358 ページ）

ap name dot11 cleanair

802.11 ネットワーク上の特定の Cisco Lightweight アクセス ポイントの CleanAir を設定するには、**apnamedot11cleanair** コマンドを使用します。

ap name *ap-name* **dot11** {**24ghz**|**5ghz**} **cleanair**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。

コマンド デフォルト

ディセーブル

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、2.4 GHz 帯域で CleanAir を有効にする例を示します。

```
Switch# ap name AP01 dot11 24ghz cleanair
```

ap name dot11 dot11n antenna

特定のアンテナを使用するようにアクセスポイントを設定するには、**apnamedot11dot11nantenna** コマンドを使用します。

ap name *ap-name* **dot11** {**24ghz|5ghz**} **dot11n antenna** {**A|B|C|D**}

構文の説明

ap-name	アクセス ポイント名。
24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
A	アンテナ ポート A を指定します。
B	アンテナ ポート B を指定します。
C	アンテナ ポート C を指定します。
D	アンテナ ポート D を指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイント AP02 でアンテナ B を有効にする例を示します。

```
Switch# ap name AP02 dot11 5ghz dot11n antenna B
```

次に、アクセス ポイント AP02 でアンテナ C を無効にする例を示します。

```
Switch# ap name AP02 no dot11 5ghz dot11n C
```

ap name dot11 dual-band cleanair

デュアルバンド無線の CleanAir を設定するには、**ap name dot11 dual-band cleanair** コマンドを使用します。

ap name *ap-name* **dot11 dual-band cleanair**
ap name *ap-name* **no dot11 dual-band cleanair**

構文の説明

ap-name	Cisco AP の名前。
cleanair	CleanAir機能を指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、アクセス ポイント AP01 のデュアルバンド無線の CleanAir を有効にする例を示します。

```
Switch# ap name AP01 dot11 dual-band cleanair
```

関連トピック

ap name dot11 dual-band shutdown （364 ページ）
show ap dot11 cleanair config （441 ページ）
show ap name config dot11 （477 ページ）

ap name dot11 dual-band shutdown

シスコの AP でデュアルバンド無線を無効にするには、**ap name dot11 dual-band shutdown** コマンドを使用します。

ap name *ap-name* **dot11 dual-band shutdown**
ap name *ap-name* **no dot11 dual-band shutdown**

構文の説明

ap-name	Cisco AP の名前。
shutdown	シスコの AP でデュアルバンド無線を無効にします。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、シスコのアクセス ポイント AP01 でデュアルバンド無線を無効にする例を示します。

```
Switch# ap name AP01 dot11 dual-band shutdown
```

ap name dot11 rrm ccx

802.11 ネットワークで特定の Cisco Lightweight アクセス ポイントの Cisco Client eXtension（CCX）無線リソース管理（RRM）を設定するには、**apnamedot11rrmccx** コマンドを使用します。

ap name *ap-name* **dot11** {**24ghz**|**5ghz**} **rrm ccx** {**customize**|**location-measurement** 間隔}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
customize	802.11 CCX オプションを有効にします。
location-measurement	CCX クライアント ロケーション測定を設定します。
間隔	間隔（10 ～ 32400）。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、2.4 GHz 帯域のアクセス ポイントの CCX クライアント ロケーション測定を設定する例を示します。

```
Switch# ap name AP01 dot11 24ghz rrm ccx location-measurement 3200
```

関連トピック

ap name dot11 rrm profile （366 ページ）

ap name dot11 rrm profile

Cisco Lightweight アクセス ポイントの無線リソース管理（RRM）パフォーマンス プロファイルを設定するには、**apnamedot11rrmprofile** コマンドを使用します。

ap name *ap-name* **dot11** {**24ghz**|**5ghz**} **rrm profile** {**clients** *value*|**customize**|**foreign** *value*|**noise** *value*|**throughput** *value*|**utilization** *value*}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
clients	アクセス ポイント クライアントしきい値を設定します。
value	アクセス ポイント クライアントしきい値（1 ～ 75 クライアント）。 （注） デフォルトのクライアントしきい値は 12 です。
customize	アクセス ポイントのパフォーマンス プロファイルのカスタマイズをオンにします。 （注） デフォルトでは、パフォーマンスプロファイルのカスタマイズはオフになっています。
foreign	外部 802.11 トランスミッタ干渉しきい値を設定します。
value	外部 802.11 トランスミッタ干渉しきい値（0 ～ 100 %）。 （注） デフォルトは 10 % です。
noise	802.11 外部ノイズしきい値を設定します。
value	802.11 外部ノイズしきい値（-127 ～ 0 dBm）。 （注） デフォルトは -70 dBm です。
throughput	データ レート スループットしきい値を設定します。
value	802.11 スループットしきい値（1000 ～ 10000000 バイト/秒） （注） デフォルトは、1,000,000 バイト/秒です。
utilization	RF 使用率しきい値を設定します。 （注） オペレーティング システムがこのしきい値を超えた場合にトラップを生成します。

value	802.11 RF使用率しきい値（0 ～ 100 %）。 （注）　デフォルトは 80% です。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、AP1 のクライアント数のしきい値を 75 個のクライアントに設定する例を示します。

```
Switch# ap name AP1 dot11 24ghz rrm profile clients 75
```

次に、802.11a 対応 Cisco Lightweight アクセス ポイント AP1 のパフォーマンス プロファイルのカスタマイズをオンにする例を示します。

```
Switch# ap name AP1 dot11 5ghz rrm profile customize
```

次に、AP1 の外部 802.11a トランスミッタ干渉しきい値を 0 パーセントに設定する例を示します。

```
Switch# ap name AP1 dot11 5ghz rrm profile foreign 0
```

次に、AP1 の 802.11a 外部ノイズしきい値を 0 dBm に設定する例を示します。

```
Switch# ap name AP1 dot11 5ghz rrm profile noise 0
```

次に、AP1 のデータ レートしきい値を 10,000,000 バイト/秒に設定する例を示します。

```
Switch# ap name AP1 dot11 5ghz rrm profile throughput 10000000
```

次に、AP1 の RF 利用率のしきい値を 100 パーセントに設定する例を示します。

```
Switch# ap name AP1 dot11 5ghz rrm profile utilization 100
```

関連トピック

ap name dot11 rrm ccx （365 ページ）

ap name dot11 txpower

802.11 ネットワーク内の単一のアクセス ポイントの送信電力レベルを設定するには、**apnamedot11txpower** コマンドを使用します。

ap name *ap-name* **dot11** {**24ghz**|**5ghz**} {**shutdown**|**txpower** {**auto**|*power-level*}}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
shutdown	802.11 ネットワークを無効にします。
auto	シスコの 802.11 対応無線の電力レベルが無線リソース管理（RRM）によって自動的に設定されるように指定します。
power-level	アクセス ポイントに手動で設定する送信電力レベルの数値。

コマンド デフォルト

コマンドのデフォルト（txpower auto）は RRM による自動設定用です。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイント AP1 で 2.4 GHz 無線送信電力を自動的に設定する例を示します。

```
Switch# ap name AP1 dot11 24ghz txpower auto
```

関連トピック

show ap config dot11 （433 ページ）

ap name dot1x-user

現在スイッチ に参加しているアクセス ポイントのグローバル認証ユーザ名およびパスワードを設定するには、**apnamedot1x-user** コマンドを使用します。特定のアクセス ポイントの 802.1X 認証を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **dot1x-user** {**global-override**|**username** *user-id* **password** *passwd*}
ap name *ap-name* ［**no**］ **dot1x-user**

構文の説明

ap-name	アクセス ポイントの名前。
global-override	アクセス ポイントがスイッチのグローバル認証設定を使用するように強制します。
username	ユーザ名を追加することを指定します。
user-id	[Username]。
password	パスワードを追加することを指定します。
passwd	パスワード。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

強度が高いパスワードを入力する必要があります。強度が高いパスワードの特徴は次のとおりです。

- 少なくとも 8 文字の長さである。
- 小文字と大文字、数字、および記号の組み合わせを含む。
- どの言語の単語でもない。

特定のアクセス ポイントの値を設定できます。

特定のアクセス ポイントの 802.1X 認証は、グローバル 802.1X 認証が有効でない場合にだけ無効にできます。グローバル 802.1X 認証が有効な場合は、すべてのアクセス ポイントに対してだけ 802.1X を無効にできます。

次に、dot1x 認証用に特定のユーザ名とパスワードを設定する例を示します。

```
Switch# ap name AP02 dot1x-user username Cisco123 password Cisco2020
```

次に、アクセス ポイント cisco_ap1 の認証を無効にする例を示します。

```
Switch# ap name cisco_ap1 no dot1x-user
```

関連トピック

show ap summary （505 ページ）

ap name ethernet

Cisco Lightweight アクセス ポイントのイーサネット ポート設定を指定するには、**apnameethernet** コマンドを使用します。指定されたポート設定またはデフォルトの設定を削除には、このコマンドの **no** 形式を使用します。

ap name *ap-name* **ethernet** *intf-number* **mode** {**access** *vlan-id*|**trunk** [{**add**|**delete**}]} **native-vlan** *vlan-id*
ap name *ap-name* **no ethernet** *intf-number* **mode** {**access**|**trunk native-vlan**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
intf-number	イーサネット インターフェイス番号（0 ～ 3）。
mode	アクセス モードまたはトランク モードを設定します。
access	アクセス モードでポートを設定します。
vlan-id	VLAN 識別番号。
trunk	トランク モードでポートを指定します。
add	（任意）VLAN モードまたはトランク モードを追加します。
delete	（任意）VLAN モードまたはトランク モードを削除します。
native-vlan	ネイティブ VLAN を指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、シスコのアクセス ポイントのアクセス モードを設定する例を示します。

```
Switch# ap name AP2 ethernet 0 mode access 1
```

ap name ethernet duplex

Lightweight アクセス ポイントのイーサネット ポート デュプレックスおよび速度を設定するには、**apnameethernetduplex** コマンドを使用します。

ap name *ap-name* **ethernet duplex** {**auto**|**full**|**half**} **speed**{**10**|**100**|**1000**|**auto**}

構文の説明

ap-name	Cisco アクセス ポイントの名前。
auto	イーサネット ポートの自動二重設定を指定します。
full	イーサネット ポートの全二重設定を指定します。
half	イーサネット ポートの半二重設定を指定します。
speed	イーサネット ポート速度の設定を指定します。
10	イーサネット ポート速度を 10 Mbps に指定します。
100	イーサネット ポート速度を 100 Mbps に指定します。
1000	イーサネット ポート速度を 1000 Mbps に指定します。
auto	接続されているすべてのアクセス ポイントにイーサネット ポートの設定を指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントのイーサネット ポートを全二重および 1 Gbps に設定する例を示します。

```
Switch# ap name AP2 ethernet duplex full 1000
```

関連トピック

show ap summary （505 ページ）

ap name key-zeroize

アクセス ポイントで FIPS キー ゼロ化を有効にするには、**ap name<AP name> key-zeroize** コマンドを使用します。

ap name*ap-name***key-zeroize**

構文の説明

ap- name	Cisco Lightweight アクセス ポイントの名前。
key-zeroize	アクセス ポイントに、アクセス ポイントで FIPS キー ゼロ化を有効にするように指示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次の例では、FIPS キー ゼロ化を有効にする方法を示します。

```
Switchap name <AP Name> key-zeroize
```

ap name image

特定のアクセス ポイントでイメージを設定するには、**apnameimage** コマンドを使用します。

ap name *ap-name* **image** {**predownload**|**swap**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
predownload	アクセスポイントにイメージのプレダウンロードを開始するように指示します。
swap	アクセス ポイントにイメージを切り替えるように指示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントにイメージをプレダウンロードする例を示します。

```
Switch# ap name AP2 image predownload
```

次に、アクセスポイントのプライマリおよびセカンダリ イメージを切り替える例を示します。

```
Switch# ap name AP2 image swap
```

関連トピック

show ap image （455 ページ）
ap image （334 ページ）

ap name ipv6 tcp adjust-mss

シスコの AP の IPv6 TCP 最大セグメント サイズ（MSS）値を設定するには、**ap name ipv6 tcp adjust-mss** コマンドを使用します。

ap name *ap-name* **ipv6 tcp adjust-mss** *size*
ap name *ap-name* **no ipv6 tcp adjust-mss**

構文の説明

ap-name	Cisco AP の名前。
adjust-mss	すべてのシスコ AP の IPv6 TCP MSS を設定します。
size	MSS 値（500 ～ 1440）。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

MSS 値は 500 ～ 1440 の範囲でなければなりません。

次に、シスコのアクセス ポイント AP01 の IPv6 TCP MSS 値を 600 に設定する例を示します。

```
Switch# ap name AP01 ipv6 tcp adjust-mss 600
```

ap name jumbo mtu

ジャンボ MTU サポートを設定するには、**ap name<AP name>jumbo-mtu** コマンドを使用します。

ap name*ap-name*{**jumbo-mtu**|**no jumbo-mtu**}

構文の説明

ap- name	Cisco Lightweight アクセス ポイントの名前。
jumbo-mtu	アクセスポイントにジャンボMTUサポートを有効にするように指示します。
no jumbo-mtu	アクセスポイントにジャンボMTUサポートを無効にするように指示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、ジャンボ MTU サポートを設定する例を示します。

```
Switchap name <AP Name> jumbo-mtu
```

ap name lan

AP の LAN ポート設定を指定するには、**ap name lan** コマンドを使用します。AP の LAN ポート設定を削除するには、**ap name no lan** コマンドを使用します。

ap name *ap-name* **[no]lan port-id** *port-id* {**shutdown** | **vlan-access**}

構文の説明

no	LAN ポート設定を削除します。
port-id	ポートを設定します。
port-id	ポートの ID。範囲は 1 ～ 4 です。
shotdown	ポートを無効にします。
vlan-access	ポートへの VLAN アクセスを有効にします。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

次に、ポートへの VLAN アクセスを有効にする例を示します。

```
Switch# ap name AP1 lan port-id 1 vlan-access
```

ap name led

アクセス ポイントの LED ステートを有効にするには、**apnameled** コマンドを使用します。アクセス ポイントの LED ステートを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **led**
no ap name *ap-name* ［**led**］ **led**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
led	アクセスポイントのLEDステートを有効にします。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの LED ステートを有効にする例を示します。

```
Switch# ap name AP2 led
```

次に、アクセス ポイントの LED ステートを無効にする例を示します。

```
Switch# ap name AP2 no led
```

ap name link-encryption

特定の Cisco Lightweight アクセス ポイントの Datagram Transport Layer Security（DTLS）データ暗号化を有効にするには、**apname link-encryption** コマンドを使用します。Cisco Lightweight アクセス ポイントの DTLS データ暗号化を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **link-encryption**
ap name *ap-name* **no link-encryption**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントのデータ暗号化を有効にする例を示します。

```
Switch# ap name AP02 link-encryption
```

ap name link-latency

スイッチ に現在関連付けられている特定の Cisco Lightweight アクセス ポイントのリンク遅延を有効にするには、**apnamelink-latency** コマンドを使用します。スイッチ に現在関連付けられている特定の Cisco Lightweight アクセス ポイントのリンク遅延を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **link-latency**
ap name *ap-name* **no link-latency**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

リンク遅延は、デフォルトでは無効になります。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、現在スイッチに参加しているアクセス ポイントだけに対してリンク遅延を有効または無効にします。将来 join されるアクセス ポイントには適用されません。

次に、アクセス ポイントでリンク遅延を有効にする例を示します。

```
Switch# ap name AP2 link-latency
```

ap name location

Cisco Lightweight アクセス ポイントのロケーション説明を変更するには、**apnamelocation** コマンドを使用します。

ap name *ap-name* **location** *location*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
場所	アクセスポイントのロケーション名（二重引用符で囲みます）。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

Cisco Lightweight アクセス ポイントを無効にしてから、このパラメータを変更する必要があります。

次に、アクセス ポイント AP1 のロケーションの説明を設定する例を示します。

```
Switch# ap name AP1 location Building1
```

関連トピック

show ap summary （505 ページ）

ap name mgmtuser

アクセスポイント管理用のユーザ名、パスワード、シークレットパスワードを設定するには、**apnamemgmtuser** コマンドを使用します。特定のアクセス ポイントがスイッチのグローバル クレデンシャルを強制的に使用するには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **mgmtuser username** *username* **password** *password* **secret** *secret*
ap name *ap-name* **no mgmtuser**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
username	アクセス ポイント管理用のユーザ名を指定します。
username	管理ユーザ名。
password	アクセス ポイント管理用のパスワードを指定します。
password	アクセス ポイント管理パスワード。
secret	特権アクセスポイント管理用のシークレットパスワードを指定します。
secret	アクセス ポイント管理シークレット パスワード。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

強力なパスワードを指定するには、次の要件を満たす必要があります。

- パスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスが含まれる必要があります。
- パスワード内で同じ文字を連続して 4 回以上繰り返すことはできません。
- パスワードに管理ユーザ名や逆にしたユーザ名を含めることはできません。
- パスワードに使用できない文字には、Cisco、oscic、admin、nimda などの語のほか、大文字の代わりに 1 や |、！を、o の代わりに 0 を、s の代わりに $ を使用して置き換えた文字などがあります。

シークレット パスワードについて、次の要件が実施されます。

- シークレットパスワードは、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスを含むことができません。

次に、アクセスポイント管理用のユーザ名、パスワード、シークレットパスワードを追加する例を示します。

```
Switch# ap name AP01 mgmtuser username acd password Arc_1234 secret Mid_1234
```

ap name mode

個別の Cisco Lightweight アクセス ポイントの Cisco スイッチ 通信オプションを変更するには、**apnamemode** コマンドを使用します。

ap name *ap-name* **mode**{**local submode**{**none**|**wips**}|**monitor**
submode{**none**|**wips**}|**rogue**|**se-connect**|**sniffer**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
local	屋内メッシュ アクセス ポイント（MAP または RAP）から nonmesh Lightweight アクセス ポイント（ローカル モード）に変換します。
submode	アクセス ポイントで wIPS サブモードを指定します。
none	アクセス ポイントで wIPS を無効にします。
monitor	監視モードの設定を指定します。
wips	アクセス ポイントで wIPS サブモードを有効にします。
rogue	アクセスポイントで有線の不正なアクセスポイントの検出モードを有効にします。
se-connect	アクセス ポイントで Spectrum Expert モードを有効にします。
sniffer	アクセス ポイントで無線スニファ モードを有効にします。

コマンド デフォルト

ローカル

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スニファ モードは、そのチャネル上のクライアントからすべてのパケットを取得し、Airopeek を実行するリモート マシンまたはその他のサポート対象パケット アナライザ ソフトウェアに転送します。これには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。

次に、ローカル モードでアクセス ポイント AP01 と通信するようにスイッチを設定する例を示します。

```
Switch# ap name AP01 mode local submode none
```

次に、有線の不正なアクセス ポイントの検出モードでアクセス ポイント AP01 と通信するようにスイッチを設定する例を示します。

```
Switch# ap name AP01 mode rogue
```

次に、無線スニファ モードでアクセス ポイント AP02 と通信するようにスイッチを設定する例を示します。

```
Switch# ap name AP02 mode sniffer
```

関連トピック

show ap monitor-mode summary （461 ページ）

ap name monitor-mode

Cisco Lightweight アクセス ポイント チャネルの最適化を設定するには、**apnamemonitor-mode** コマンドを使用します。

ap name *ap-name* **monitor-mode** {**no-optimization**|**tracking-opt**|**wips-optimized**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
no-optimization	アクセス ポイントに対してチャネル スキャンの最適化を行わないことを指定します。
tracking-opt	アクセス ポイントに対してトラッキングが最適化されたチャネル スキャンを有効にします。
wips-optimized	アクセス ポイントに対して wIPS が最適化されたチャネル スキャンを有効にします。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイント AP01 に Cisco wireless Intrusion Prevention System（wIPS）監視モードを設定する例を示します。

```
Switch# ap name AP01 monitor-mode wips
```

関連トピック

show ap monitor-mode summary （461 ページ）
show ap config （436 ページ）

ap name monitor-mode dot11b

監視モード アクセス ポイントに対して 802.11b スキャン チャネルを設定するには、**apnamemonitor-modedot11b** コマンドを使用します。

ap name *ap-name* **monitor-mode dot11b fast-channel** *channel1* ［*channel2*］［*channel3*］［*channel4*］

構文の説明

ap-name	アクセス ポイントの名前。
fast-channel	監視モード アクセス ポイントに対して 2.4 GHz 帯域スキャン チャネル（単一または複数）を指定します。
channel1	channel1 のスキャン。
channel2	（任意）channel2 のスキャン。
channel3	（任意）channel3 のスキャン。
channel4	（任意）channel4 のスキャン。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、チャネル1、6、11をリッスンするようにトラッキング最適化モードのアクセス ポイントを設定する例を示します。

```
Switch# ap name AP01 monitor-mode dot11b fast-channel 1 6 11
```

関連トピック

show ap monitor-mode summary （461 ページ）

ap name name

Cisco Lightweight アクセス ポイントの名前を変更するには、**apnamename** コマンドを使用します。

ap name *ap-name* **name** *new-name*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの現在の名前。
new-name	Cisco Lightweight アクセス ポイントの新しい名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの名前を AP1 から AP2 に変更する例を示します。

```
Switch# ap name AP1 name AP2
```

関連トピック

show ap config （436 ページ）

ap name no dot11 shutdown

802.11 ネットワーク上の個別のシスコ無線の無線伝送を有効にするには、**apnamenodot11shutdown** コマンドを使用します。

ap name *ap-name* **no dot11**{**24ghz**|**5ghz**} **shutdown**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 無線を指定します。
5ghz	5 GHz 無線を指定します。

コマンド デフォルト

デフォルトでは、ネットワーク全体で伝送が有効化されています。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

（注） 802.11 を設定する場合は、このコマンドを **apname** *Cisco-AP***dot115ghzshutdown** コマンドとともに使用します。

このコマンドは、CLI インターフェイスがアクティブなときはいつでも使用できます。

次に、アクセス ポイント AP1 の 5 GHz 帯域での無線伝送を有効にする例を示します。

```
Switch# ap name AP1 no dot11 5ghz shutdown
```

ap name power

アクセス ポイントの Cisco Power over Ethernet（PoE）機能を有効にするには、**apnamepower** コマンドを使用します。アクセス ポイントの Cisco PoE 機能を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **power** {**injector**|**pre-standard**}
ap name *ap-name* **no power** {**injector**|**pre-standard**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
injector	アクセス ポイントのパワー インジェクタ ステートを指定します。
pre-standard	アクセス ポイントに対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効にします。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、すべてのアクセス ポイントのパワー インジェクタ ステートを有効にする例を示します。

```
Switch# ap name AP01 power injector
```

次に、アクセス ポイント AP02 に対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効にする例を示します。

```
Switch# ap name AP02 power pre-standard
```

ap name shutdown

特定の Cisco Lightweight アクセス ポイントを無効にするには、**apnameshutdown** コマンドを使用します。Cisco Lightweight アクセス ポイントを有効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **shutdown**
ap name *ap-name* **no shutdown**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、特定の Cisco Lightweight アクセス ポイントを無効にする例を示します。

```
Switch# ap name AP2 shutdown
```

ap name slot shutdown

特定の Cisco Lightweight アクセス ポイントでスロットを無効にするには、**apnameslotshutdown** コマンドを使用します。Cisco Lightweight アクセス ポイントでスロットを有効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **slot** {**0**|**1**|**2**|**3**} **shutdown**
ap name *ap-name* **no slot** {**0**|**1**|**2**|**3**} **shutdown**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
0	Cisco Lightweight アクセス ポイントでスロット番号 0 を有効にします。
1	Cisco Lightweight アクセス ポイントでスロット番号 1 を有効にします。
2	Cisco Lightweight アクセス ポイントでスロット番号 2 を有効にします。
3	Cisco Lightweight アクセス ポイントでスロット番号 3 を有効にします。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、TSIM_AP2 というシスコのアクセス ポイントでスロット 0 を有効にする例を示します。

```
Switch# ap name TSIM_AP2 no slot 0 shutdown
```

ap name sniff

アクセス ポイントでスニフィングを有効にするには、**apname sniff** コマンドを使用します。アクセス ポイントでスニフィングを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **sniff** {**dot11a**|**dot11b**}
ap name *ap-name* **no sniff** {**dot11a**|**dot11b**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
dot11a	2.4 GHz 帯域を指定します。
dot11b	5 GHz 帯域を指定します。
channel	スニファされる有効なチャネル。5 GHz 帯域の場合、範囲は 36 ～ 165 です。2.4 GHz 帯域の場合、範囲は 1 ～ 14 です。
server-ip-address	Omnipeek、Airopeek、AirMagnet、または Wireshark を実行するリモート マシンの IP アドレス。

コマンド デフォルト

チャネル 36

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

アクセス ポイントでスニフィング機能が有効になっている場合、そのアクセス ポイントは指定されたチャネルで信号のスニフィングを開始します。すべてのパケットが取得され、Omnipeek、Airopeek、AirMagnet、または Wireshark ソフトウェアを実行しているリモート コンピュータに転送されます。これには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。

アクセス ポイントをスニファとして機能させるには、そのアクセス ポイントが送信したパケットを、上記いずれかのパケット アナライザを実行しているリモート コンピュータが受信できるように設定しておく必要があります。

次に、プライマリ無線 LAN コントローラ上のアクセス ポイントの 5 GHz 帯域でのスニフィングを有効にする例を示します。

```
Switch# ap name AP2 sniff dot11a 36 192.0.2.54
```

ap name ssh

特定の Cisco Lightweight アクセス ポイントでセキュア シェル（SSH）接続を有効にするには、**apnamessh** コマンドを使用します。特定の Cisco Lightweight アクセス ポイントで SSH 接続を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **ssh**
ap name *ap-name* **no ssh**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

Cisco スイッチは、すべてのネットワーク操作に関して、およびハードウェア リセットが発生した場合に、Cisco ワイヤレス LAN コントローラと関連付けられます。

次に、アクセス ポイント Cisco_ap2 で SSH 接続を有効にする例を示します。

```
Switch# ap name Cisco_ap2 ssh
```

ap name telnet

アクセス ポイントで Telnet 接続を有効にするには、**apnametelnet** コマンドを使用します。アクセス ポイントで Telnet 接続を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **telnet**
ap name *ap-name* **no telnet**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイント cisco_ap1 で Telnet 接続を無効にする例を示します。

```
Switch# ap name cisco_ap1 no telnet
```

ap name power injector

アクセス ポイントのパワー インジェクタ ステートを設定するには、**apnamepowerinjector** コマンドを使用します。アクセス ポイントの Cisco Power over Ethernet（PoE）機能を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **power injector** {**installed**|**override**|**switch-mac-address** *switch-MAC-address*}
ap name *ap-name* **no power injector**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
installed	パワー インジェクタが設置された現在のスイッチ ポートの MAC アドレスを検出します。
override	安全性チェックを上書きし、パワー インジェクタが常にインストールされていることを前提とします。
switch-mac-address	パワー インジェクタが設置されたスイッチ ポートの MAC アドレスを指定します。
switch-MAC-address	パワー インジェクタが設置されたスイッチ ポートの MAC アドレス。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントのパワー インジェクタ ステートを有効にする例を示します。

```
Switch# ap name AP01 power injector switch-mac-address aaaa.bbbb.cccc
```

ap name power pre-standard

アクセス ポイントに対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効にするには、**apnamepowerpre-standard** コマンドを使用します。アクセス ポイントに対してインライン パワー搭載のシスコの先行標準スイッチ ステートを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **power pre-standard**
ap name *ap-name* **no power pre-standard**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイント AP02 に対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効にする例を示します。

```
Switch# ap name AP02 power pre-standard
```

次に、アクセス ポイント AP02 に対してインライン パワー搭載のシスコの先行標準スイッチ ステートを無効にする例を示します。

```
Switch# ap name AP02 no power pre-standard
```

ap name reset-button

アクセス ポイントの Reset ボタンを設定するには、**apnamereset-button** コマンドを使用します。

ap name *ap-name* **reset-button**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイント AP03 のリセット ボタンを有効にする例を示します。

```
Switch# ap name AP03 reset-button
```

ap name reset

特定の Cisco Lightweight アクセス ポイントをリセットするには、**apnamereset** コマンドを使用します。

ap name *ap-name* **reset**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、AP2 という Cisco Lightweight アクセス ポイントをリセットする例を示します。

```
Switch# ap name AP2 reset
```

関連トピック

show ap config （436 ページ）

ap name slot

さまざまなスロット パラメータを設定するには、**apnameslot** コマンドを使用します。Cisco Lightweight アクセス ポイントでスロットを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **slot** *slot-number* {**channel** {**global**|**number** *channel-number*|**width** *channel width*}|**rtsthreshold** *value*|**shutdown**|**txpower** {**global***channel-level*}}
ap name *ap-name* **no slot** {**0**|**1**|**2**|**3**} **shutdown**

構文の説明

ap-name	Cisco アクセス ポイントの名前。
slot-number	チャネルが割り当てられたスロットのダウンリンク無線。次のスロット番号を指定できます。 • **0**：Cisco Lightweight アクセス ポイントでスロット番号 0 を有効にします。 • **1**：Cisco Lightweight アクセス ポイントでスロット番号 1 を有効にします。 • **2**：Cisco Lightweight アクセス ポイントでスロット番号 2 を有効にします。 • **3**：Cisco Lightweight アクセス ポイントでスロット番号 3 を有効にします。
channel	スロットのチャネルを指定します。
global	スロットのチャネル グローバル プロパティを指定します。
number	スロットのチャネル番号を指定します。
channel-number	チャネル番号（1 ～ 169）。
width	スロットのチャネル幅を指定します。
channel-width	チャネル幅（20 ～ 40）。
rtsthreshold	アクセス ポイントの RTS/CTS しきい値を指定します。
value	RTS/CTS しきい値（0 ～ 65535）。
shutdown	スロットをシャット ダウンします。
txpower	スロットの Tx 電力を指定します。
global	スロットの自動-RF を指定します。
channel-level	スロットの送信電力レベル（1 ~ 7）電源レベル。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイント abc のスロット 3 を有効にする例を示します。

```
Switch# ap name abc slot 3
```

次に、アクセス ポイント abc の RTS を設定する例を示します。

```
Switch# ap name abc slot 3 rtsthreshold 54
```

ap name static-ip

Cisco Lightweight アクセス ポイントの静的 IP アドレス設定を指定するには、**apnamestatic-ip** コマンドを使用します。Cisco Lightweight アクセス ポイントの静的 IP アドレスを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **static-ip** {**domain** *domain-name*|**ip-address** *ip-address* **netmask** *netmask* **gateway** *gateway*|**nameserver** *ip-address*}
ap name *ap-name* **no static-ip**

構文の説明

ap-name	アクセス ポイントの名前。
domain	シスコのアクセス ポイントのドメイン名を指定します。
domain-name	特定のアクセス ポイントが属するドメイン。
ip-address	シスコのアクセス ポイントの静的 IP アドレスを指定します。
ip-address	シスコのアクセス ポイントの静的 IP アドレス。
netmask	シスコのアクセス ポイントの静的 IP ネットマスクを指定します。
netmask	シスコのアクセス ポイントの静的 IP ネットマスク。
gateway	シスコのアクセス ポイントのゲートウェイを指定します。
gateway	シスコのアクセス ポイントのゲートウェイの IP アドレス。
nameserver	特定のアクセス ポイントが DNS 解決を使用してスイッチを検出できるよう DNS サーバを指定します。
ip-address	DNS サーバの IP アドレス。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

静的 IP アドレスがアクセス ポイントに設定されている場合は、DNS サーバと、アクセス ポイントが属するドメインとを指定しない限り、アクセス ポイントはドメイン ネーム システム（DNS）解決を使用してスイッチを検出できません。

次に、アクセス ポイントの静的 IP アドレスを設定する例を示します。

```
Switch# ap name AP2 static-ip ip-address 192.0.2.54 netmask 255.255.255.0 gateway 192.0.2.1
```

ap name stats-timer

Cisco Lightweight アクセス ポイントがその DOT11 統計情報を Cisco スイッチに送信する時間（秒単位）を設定するには、**apnamestats-timer** コマンドを使用します。

ap name *ap-name* **stats-timer** *timer-value*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
timer-value	0 ～ 65535 の時間（秒単位）。ゼロの値を指定すると、タイマーが無効になります。

コマンド デフォルト

0（無効）。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

値 0 は、Cisco Lightweight アクセス ポイントが DOT11 統計情報を送信しないことを意味します。このタイマーには 0 ～ 65,535 秒を指定できます。Cisco Lightweight アクセス ポイントを無効にしてから、この値を設定する必要があります。

次に、アクセス ポイント AP2 で、統計情報タイマーを 600 秒に設定する例を示します。

```
Switch# ap name AP2 stats-timer 600
```

ap name syslog host

特定の Cisco Lightweight アクセス ポイントの syslog サーバを設定するには、**apnamesysloghost** コマンドを使用します。

ap name *ap-name* **syslog host** *syslog-host-ip-address*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
syslog-host-ip-address	Syslog サーバの IP アドレス。

コマンド デフォルト

255.255.255.255

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、各アクセス ポイントの syslog サーバ IP アドレスは 255.255.255.255 で、これはまだサーバが設定されていないことを示しています。このデフォルト値を使用すると、グローバル アクセス ポイント syslog サーバの IP アドレスがアクセス ポイントにプッシュされます。

次に、syslog サーバを設定する例を示します。

```
Switch# ap name AP2 syslog host 192.0.2.54
```

関連トピック

ap syslog （415 ページ）
show ap config （436 ページ）
show ap name config （475 ページ）

ap name syslog level

システム ログ レベルを設定するには、**apnamesysloglevel** コマンドを使用します。

ap name *ap-name* **syslog level**
{**alert**|**critical**|**debug**|**emergency**|**errors**|**information**|**notification**|**warning**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
alert	アラート レベルのシステム ログを指定します。
critical	クリティカル レベルのシステム ログを指定します。
debug	デバッグ レベルのシステム ログを指定します。
emergency	緊急レベルのシステム ログを指定します。
errors	エラー レベルのシステム ログを指定します。
information	情報レベルのシステム ログを指定します。
notification	通知レベルのシステム ログを指定します。
warning	警告レベルのシステム ログを指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アラート レベルのシステム ログを設定する例を示します。

```
Switch# ap name AP2 syslog level alert
```

ap name tcp-adjust-mss

特定のアクセス ポイントで TCP 最大セグメント サイズ（MSS）を有効または無効にするには、**apnametcp-adjust-mss** コマンドを使用します。特定のアクセス ポイントで TCP 最大セグメント サイズ（MSS）を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **tcp-adjust-mss size** *size*
ap name *ap-name* **no tcp-adjust-mss**

構文の説明

ap-name	アクセス ポイントの名前。
size	最大セグメント サイズ（536 ～ 1363 バイト）。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

この機能を有効にすると、アクセス ポイントがデータ パスの無線クライアントへの TCP パケットとデータ パスの無線クライアントからの TCP パケットをチェックします。これらのパケットの MSS が設定した値または Control And Provisioning of Wireless Access Points（CAPWAP）トンネルのデフォルト値よりも大きい場合、アクセス ポイントは MSS を、設定された新しい値に変更します。これらのパケットの MSS が設定した値または CAPWAP トンネルのデフォルト値よりも大きい場合、アクセス ポイントは MSS を、新しく設定された値に変更します。

次に、アクセス ポイント Cisco_ap1 で TCP MSS を有効にする例を示します。

```
Switch# ap name ciscoap tcp-adjust-mss size 1200
```

関連トピック

show ap name tcp-adjust-mss （500 ページ）

ap name tftp-downgrade

Lightweight アクセス ポイントを Autonomous アクセス ポイントにダウングレードするために使用される設定を指定するには、**apnametftp-downgrade** コマンドを使用します。

ap name *ap-name* **tftp-downgrade** *tftp-server-ip filename*

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
tftp-server-ip	TFTP サーバの IP アドレスです。
filename	TFTP サーバ上のアクセス ポイント イメージ ファイルのファイル名。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイント AP1 をダウングレードする設定を指定する例を示します。

```
Switch# ap name Ap01 tftp-downgrade 172.21.12.45 ap3g1-k9w7-tar.124-25d.JA.tar
```

ap power injector

スイッチ に参加しているすべての Cisco Lightweight アクセス ポイントのパワー インジェクタ ステートを設定するには、**appowerinjector** コマンドを使用します。すべてのアクセス ポイントのパワー インジェクタ ステートを削除するには、このコマンドの **no** 形式を使用します。

ap power injector {**installed**|**override**|**switch-mac-address** *switch-MAC-addr*}
no ap power injector

構文の説明

installed	パワー インジェクタが設置された現在のスイッチ ポートの MAC アドレスを検出します。
override	安全性チェックを上書きし、パワー インジェクタが常にインストールされていることを前提とします。
switch-mac-address	パワー インジェクタが設置されたスイッチ ポートの MAC アドレスを指定します。
switch-MAC-address	パワー インジェクタが設置されたスイッチ ポートの MAC アドレスを指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、スイッチに参加しているすべての Cisco Lightweight アクセス ポイントのパワー インジェクタ ステートを有効にする例を示します。

```
Switch(config)# ap power injector switch-mac-address aaaa.bbbb.cccc
```

ap power pre-standard

スイッチ に参加している Cisco Lightweight アクセス ポイントを、シスコのハイパワー スイッチによって電力が供給されるように設定するには、**appowerpre-standard** コマンドを使用します。すべてのアクセス ポイントの先行標準電力を無効にするには、このコマンドの **no** 形式を使用します。

ap power pre-standard
no ap power pre-standard

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイント AP02 に対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効にする例を示します。

```
Controller(config)# ap power pre-standard
```

ap reporting-period

アクセス ポイント不正/エラー レポート期間を設定するには、**apreporting-period** コマンドを使用します。アクセス ポイント不正/エラー レポート期間を無効にするには、このコマンドの **no** 形式を使用します。

ap reporting-period *value*
no ap reporting-period

構文の説明

value	秒単位の期間（10 ～ 120）。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイント不正/エラー レポートを設定する例を示します。

```
Switch(config)# ap reporting-period 100
```

次に、アクセス ポイント不正/エラー レポートを無効にする例を示します。

```
Switch(config)# no ap reporting-period 100
```

ap reset-button

スイッチ に参加しているすべての Cisco Lightweight アクセス ポイントの Reset ボタンを設定するには、**apreset-button** コマンドを使用します。すべてのアクセス ポイントの Reset ボタンを無効にするには、このコマンドの **no** 形式を使用します。

ap reset-button
no ap reset-button

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、コントローラに参加しているすべてのアクセス ポイントの Reset ボタンを設定する例を示します。

```
Switch(config)# ap reset-button
```

service-policy type control subscriber

グローバル サブスクライバ制御ポリシーを適用するには、**service-policy type control subscriber** <*subscriber-policy-name*> コマンドを使用します。

service-policytypecontrolsubscriber<*subscriber-policy-name*>

構文の説明

service-policy	アクセスポイントにグローバル サブスクライバ制御ポリシーを適用するように指示します。
<*subscriber-policy-name*>	サブスクライバ ポリシーの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、グローバル サブスクライバ制御ポリシーを無効にする例を示します。

```
Switchno service-policy type control subscriber
```

ap static-ip

Cisco Lightweight アクセス ポイントの静的 IP アドレスを設定するには、**apstatic-ip** コマンドを使用します。アクセス ポイントの静的 IP 設定を無効にするには、このコマンドの **no** 形式を使用します。

ap static-ip {**domain** *domain-name*|**name-server** *ip-address*}
no ap static-ip {**domain**|**name-server**}

構文の説明

domain	特定のアクセス ポイントまたはすべてのアクセス ポイントが属するドメインを指定します。
domain-name	ドメイン名。
name-server	特定のアクセス ポイントまたはすべてのアクセス ポイントが DNS 解決を使用してスイッチを検出できるよう DNS サーバを指定します。
ip-address	DNS サーバの IP アドレス。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

静的 IP アドレスがアクセス ポイントに設定されている場合は、DNS サーバと、アクセス ポイントが属するドメインとを指定しない限り、アクセス ポイントはドメイン ネーム システム（DNS）解決を使用してスイッチを検出できません。

次に、すべてのアクセス ポイントの静的 IP アドレスを設定する例を示します。

```
Switch(config)# ap static-ip domain cisco.com
```

ap syslog

スイッチ に参加しているすべての Cisco Lightweight アクセス ポイントのシステム ログを設定するには、**apsyslog** コマンドを使用します。

ap syslog {**host** *ipaddress*|**level**{**alert**|**critical**|**debug**|**emergency**|**errors**|**information**|**notification**|**warning**}}

構文の説明

host	スイッチに参加しているすべてのアクセス ポイントのグローバル syslog サーバを指定します。
ipaddress	Syslog サーバの IP アドレス。
level	スイッチに参加しているすべてのアクセス ポイントのシステム ログ レベルを指定します。
alert	シスコのアクセス ポイントのアラート レベルのシステム ログを指定します。
critical	シスコのアクセス ポイントのクリティカル レベルのシステム ログを指定します。
debug	シスコのアクセス ポイントのデバッグ レベルのシステム ログを指定します。
emergency	シスコのアクセス ポイントの緊急レベルのシステム ログを指定します。
errors	シスコのアクセス ポイントのエラー レベルのシステム ログを指定します。
information	シスコのアクセス ポイントの情報レベルのシステム ログを指定します。
notification	シスコのアクセス ポイントの通知レベルのシステム ログを指定します。
warning	シスコのアクセス ポイントの警告レベルのシステム ログを指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、すべてのアクセス ポイントのグローバル syslog サーバ IP アドレスは 255.255.255.255 です。スイッチ上の syslog サーバを設定する前に、アクセス ポイントがこのサーバが常駐するサブネットにアクセスできることを確認します。このサブネットにアクセスできない場合、アクセス ポイントは syslog メッセージを送信できません。

次に、すべてのアクセス ポイントにグローバル syslog サーバを設定する例を示します。

```
Switch(config)# ap syslog host 172.21.34.45
```

ap name no controller

設定済みのプライマリ、セカンダリ、およびターシャリ ワイヤレス LAN コントローラの順序を変更するには、次のコマンドを使用します。

ap name*ap-name* **no controller primary**

ap name*ap-name* **no controller secondary**

ap name*ap-name* **no controller tertiary**

構文の説明

ap- name	Cisco Lightweight アクセス ポイントの名前。
no controller primary	アクセス ポイントにプライマリ コントローラの構成解除を指示します。
no controller secondary	アクセス ポイントにセカンダリ コントローラの構成解除を指示します。
no controller tertiary	アクセス ポイントにターシャリ コントローラの構成解除を指示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

アクセス ポイントに対して設定されているプライマリ、セカンダリ、およびターシャリ ワイヤレス LAN コントローラがあり、コントローラの名前と対応する IP アドレスを交換する必要がある場合、プライマリ コントローラを構成解除して、セカンダリ コントローラを構成できます。

例

次に、プライマリ コントローラを構成解除する例を示します。

```
Switchap name <AP Name> no controller primary.
```

ap tcp-adjust-mss size

すべての Cisco Lightweight アクセス ポイントで TCP 最大セグメント サイズ（MSS）を有効にするには、**aptcp-adjust-msssize** コマンドを使用します。すべての Cisco Lightweight アクセス ポイントで TCP 最大セグメント サイズ（MSS）を無効にするには、このコマンドの **no** 形式を使用します。

ap tcp-adjust-mss size *size*
no ap tcp-adjust-mss

構文の説明

size	最大セグメント サイズ（536 ～ 1363 バイト）。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

この機能を有効にすると、アクセス ポイントがデータ パスの無線クライアントへの TCP パケットとデータ パスの無線クライアントからの TCP パケットをチェックします。これらのパケットの MSS が設定した値または Control And Provisioning of Wireless Access Points（CAPWAP）トンネルのデフォルト値よりも大きい場合、アクセス ポイントは MSS を、設定された新しい値に変更します。

次に、セグメント サイズが 1200 のすべてのアクセス ポイントで TCP MSS を有効にする例を示します。

```
Switch(config)# ap tcp-adjust-mss 1200
```

関連トピック

show ap name tcp-adjust-mss （500 ページ）

ap tftp-downgrade

Lightweight アクセス ポイントを Autonomous アクセス ポイントにダウングレードするために使用される設定を指定するには、**aptftp-downgrade** コマンドを使用します。Lightweight アクセス ポイントを Autonomous アクセス ポイントにダウングレードするために使用される設定を無効にするには、このコマンドの **no** 形式を使用します。

ap tftp-downgrade *tftp-server-ip filename*
no ap tftp-downgrade

構文の説明

tftp-server-ip	TFTP サーバの IP アドレスです。
filename	TFTP サーバ上のアクセス ポイント イメージ ファイルのファイル名。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、すべてのアクセス ポイントをダウングレードする設定を指定する例を示します。

```
Switch(config)# ap tftp-downgrade 172.21.23.45 ap3g1-k9w7-tar.124-25d.JA.tar
```

config wireless wps rogue client mse

不正 MSE クライアントを設定するには、**wirelesswps rogueclientmse** コマンドを使用します。

ワイヤレス クライアントの統計情報の概要を表示するには、**showwirelessclientclient-statisticssummary** コマンドを使用します。

wirelesswpsrogueclientmse

showwirelessclientclient-statisticssummary

構文の説明

rogueclientmse	不正 MSE クライアントの設定を有効にするようアクセス ポイントに命令します。
nowirelesswps	不正 MSE クライアントの設定を無効にするようアクセス ポイントに命令します。
client-statisticssummary	ワイヤレス クライアントの統計情報の概要を表示するよう命令します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、不正 MSE クライアントを設定する例を示します。

```
Switchwireless wps rogue client mse
```

clear ap name tsm dot11 all

特定のアクセス ポイントまたはすべてのアクセス ポイントのトラフィック ストリーム メトリック（TSM）統計情報をクリアするには、**clearapnametsmdot11all** コマンドを使用します。

clear ap name *ap-name* **tsm dot11** {**24ghz**|**5ghz**} **all**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
all	すべてのアクセス ポイントを指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、2.4 GHz 帯域のアクセス ポイントの TSM 統計情報をクリアする例を示します。

```
Switch# clear ap name AP1 tsm dot11 24ghz all
```

clear ap config

Lightweight アクセス ポイントの設定をクリア（デフォルト値にリセット）するには、**clearapconfig** コマンドを使用します。

clear ap config *ap-name* [{**eventlog**|**keep-ip-config**}]

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
eventlog	（任意）スイッチに参加している特定のアクセス ポイントまたはすべてのアクセス ポイントの既存のイベント ログ ファイルを削除して空のイベント ログ ファイルを作成します。
keep-ip-config	（任意）シスコのアクセス ポイントの静的 IP 設定を削除しないように指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを入力しても、アクセス ポイントの固定 IP アドレスはクリアされません。

次に、AP01 という名前のアクセス ポイント用のアクセス ポイントの設定をクリアする例を示します。

```
Switch# clear ap config AP01
```

関連トピック

show ap config （436 ページ）

clear ap eventlog-all

すべてのアクセス ポイントの既存のイベント ログを削除して空のイベント ログ ファイルを作成するには、**clearapeventlog-all** コマンドを使用します。

clear ap eventlog-all

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、すべてのアクセス ポイントのイベント ログを削除する例を示します。

```
Switch# clear ap eventlog-all
```

clear ap join statistics

すべてのアクセス ポイントまたは特定のアクセス ポイントの参加統計情報をクリアするには、**clearapjoinstatistics** コマンドを使用します。

clear ap join statistics

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、すべてのアクセス ポイントの参加統計情報をクリアする例を示します。

```
Switch# clear ap join statistics
```

clear ap mac-address

特定の Cisco Lightweight アクセス ポイントの参加統計情報の MAC アドレスをクリアするには、**clearapmac-address** コマンドを使用します。

clear ap mac-address *mac* **join statistics**

構文の説明

mac	アクセスポイントのMACアドレス。
joinstatistics	参加統計情報をクリックします。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの参加統計情報をクリアする例を示します。

```
Switch# clear ap mac-address aaaa.bbbb.cccc join statistics
```

clear ap name wlan statistics

WLAN 統計情報をクリアするには、**clearapnamewlanstatistics** コマンドを使用します。

clear ap name *ap-name* **wlan statistics**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイント cisco_ap の WLAN 設定要素をクリアする例を示します。

```
Switch# clear ap name cisco_ap wlan statistics
```

debug ap mac-address

MAC-アドレス上のアクセス ポイントのデバッグを有効にするには、**debugapmac-address** コマンドを使用します。

debug ap mac-address *mac-address*
no debug ap mac-address *mac-address*

構文の説明

mac-address	アクセス ポイント Ethernet MAC アドレス、または 802.11 無線インターフェイスの MAC アドレス。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
10.3Cisco IOS XE 3.3 SE	このコマンドが導入されました。

次に、AP での MAC アドレスのデバッグを有効にする例を示します。

```
Switch# debug ap mac-address
ap mac-address debugging is on
```

次に、AP での MAC アドレスのデバッグを無効にする例を示します。

```
Switch# no debug ap mac-address
ap mac-address debugging is off
```

show ap cac voice

使用されている帯域幅、使用可能な最大帯域幅、コール情報を含む簡潔な音声統計とともにすべてのアクセス ポイントの一覧を表示するには、**showapcacvoice** コマンドを使用します。

show ap cac voice

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、Cisco Lightweight アクセス ポイントに対応する音声 CAC の詳細を表示する例を示します。

```
controller# show ap cac voice

1) AP Name: AP01
============================

  Wireless Bandwidth (In MeanTime mt)

       Slot#  Radio         Calls  BW-Max  BW-Alloc  Bw-InUse (%age)
  ------------------------------------------------------------------
  1    0      802.11b/g     0      23437   0         0
  2    1      802.11a       0      23437   0         0

  Wired Bandwidth (in Kbps)

       Slot#  Wlan-ID  Wlan-Name             BW-Config   BW-Avail
  ------------------------------------------------------------------
  1    0      1        maria-open            0           0
  2    0      12       24                    0           0
  3    1      1        maria-open            0           0
  4    1      12       24                    0           0


2) AP Name: AP02
============================

  Wireless Bandwidth (In MeanTime mt)

       Slot#  Radio         Calls  BW-Max  BW-Alloc  Bw-InUse (%age)
  ------------------------------------------------------------------
  1    0      802.11b/g     0      23437   0         0
  2    1      802.11a       0      23437   0         0

  Wired Bandwidth (in Kbps)
```

```
      Slot#  Wlan-ID  Wlan-Name             BW-Config   BW-Avail
-------------------------------------------------------------------
1     0      1        maria-open            0           0
2     0      12       24                    0           0
3     1      1        maria-open            0           0
4     1      12       24                    0           0
```

show ap capwap

すべてのアクセス ポイントに適用される Control And Provisioning of Wireless Access Points（CAPWAP）設定を表示するには、**showapcapwap** コマンドを使用します。

show ap capwap {**retransmit**|**timers**|**summary**}

構文の説明

retransmit	アクセス ポイント CAPWAP 再送信パラメータを表示します。
timers	不正アクセス ポイント エントリ タイマーを表示します。
summary	シスコ スイッチのネットワーク設定を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイント CAPWAP 再送信パラメータを表示する例を示します。

```
Controller# show ap capwap retransmit

Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                          Retransmit Interval            Retransmit Count
-----------------------------------------------------------------------------------
AP01                              3                               5

AP02                              3                               5

AP03                              3                               5

AP04                              3                               5

AP05                              3                               5

AP07                              3                               5

AP08                              3                               5

AP09                              3                               5

AP10                              3                               5

AP11                              3                               5

AP12                              3                               5
```

次に、不正アクセス ポイント エントリ タイマーを表示する例を示します。

```
Controller# show ap capwap timers

AP Discovery timer       : 10
AP Heart Beat timeout    : 30
Primary Discovery timer  : 120
Primed Join timeout      : 0
Fast Heartbeat           : Disabled
Fast Heartbeat timeout   : 1
```

次に、シスコ スイッチのネットワーク設定を表示する例を示します。

```
Controller# show ap capwap summary

AP Fallback                      : Enabled
AP Join Priority                 : Disabled
AP Master                        : Disabled
Primary backup Controller Name   :
Primary backup Controller IP     : 0.0.0.0
Secondary backup Controller Name :
Secondary backup Controller IP   : 0.0.0.0
```

show ap cdp

スイッチ に結合されたすべての Cisco Lightweight アクセス ポイントの Cisco Discovery Protocol（CDP）情報を表示するには、**showapcdp** コマンドを使用します。

show ap cdp [**neighbors** [**detail**]]

構文の説明

neighbors	（任意）CDP を使用してネイバーを表示します。
detail	（任意）CDP を使用している特定のアクセス ポイントのネイバーに関する詳細情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、すべてのアクセス ポイントの CDP ステータスを表示する例を示します。

```
Switch# show ap cdp
```

次に、CDP を使用しているすべてのネイバーの詳細を表示する例を示します。

```
Switch# show ap cdp neighbors
```

関連トピック

ap cdp （275 ページ）

show ap config dot11

Cisco Lightweight アクセスポイントの 802.11-58G 無線の詳細な設定を表示するには、**showapconfigdot11** コマンドを使用します。

show ap config dot11 58ghz summary

構文の説明

58ghz	802.11-58G 無線を表示します。
summary	アクセスポイントの無線のサマリーを表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの 802.11a-58G の詳細な設定を表示する例を示します。

```
Switch# show ap config dot11 58ghz summary
```

show ap config dot11 dual-band summary

Cisco AP のデュアルバンド無線の設定のサマリーを表示するには、**show ap config dot11 dual-band summary** コマンドを使用します。

show ap config dot11 dual-band summary

構文の説明

dual-band	デュアルバンド無線を指定します。
summary	Cisco AP のデュアルバンド無線の設定のサマリーを表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

show ap config fnf

すべての Cisco AP の NetFlow 入出力モニタを表示するには、**show ap config fnf** コマンドを使用します。

show ap config fnf

構文の説明	**ff** すべての Cisco AP の NetFlow 入出力モニタ。
コマンド デフォルト	なし
コマンド モード	任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

show ap config

スイッチ に結合するすべてのアクセス ポイントの設定を表示するには、**showapconfig** コマンドを使用します。

show ap config {**ethernet**|**general**|**global**}

構文の説明

ethernet	すべてのCisco APのVLANタギング情報を表示します。
general	すべての Cisco AP に共通する情報を表示します。
global	すべての Cisco AP のグローバル設定を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、グローバル syslog サーバ設定を表示する例を示します。

```
Switch# show ap config global

AP global system logging host                  : 255.255.255.255
```

show ap crash-file

Lightweight アクセス ポイントによって生成されたクラッシュ ファイルおよび無線コア ダンプ ファイルの両方の一覧を表示するには、**showapcrash-file** コマンドを使用します。

show ap crash-file

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントで生成されたクラッシュ ファイルを表示する例を示します。

```
Switch# show ap crash-file
```

関連トピック

ap crash-file （279 ページ）

show ap data-plane

データ プレーンのステータスを表示するには、**showapdata-plane** コマンドを使用します。

show ap data-plane

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、すべてのアクセス ポイントのデータ プレーンのステータスを表示する例を示します。

```
Switch# show ap data-plane
```

show ap dot11 l2roam

802.11a または 802.11b/g レイヤ 2 クライアントのローミング情報を表示するには、**showapdot11l2roam** コマンドを使用します。

show ap dot11 {**24ghz**|**5ghz**} **l2roam** {**mac-address** *mac-address* **statistics**|**rf-param**|**statistics**}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
mac-address *mac-address***statistics**	Cisco Lightweight アクセス ポイントの MAC アドレスを指定します。
rf-param	レイヤ 2 周波数パラメータを指定します。
statistics	レイヤ 2 クライアントのローミング統計情報を指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、802.11b レイヤ 2 クライアントのローミング情報を表示する例を示します。

```
Switch# show ap dot11 24ghz l2roam rf-param

L2Roam 802.11bg RF Parameters
  Config Mode          : Default
  Minimum RSSI         : -85
  Roam Hysteresis      : 2
  Scan Threshold       : -72
  Transition time      : 5
```

show ap dot11 cleanair air-quality

802.11 ネットワークの電波品質のサマリー情報および最も深刻な電波品質の情報を表示するには、**showapdot11cleanairair-quality** コマンドを使用します。

show ap dot11 {24ghz|5ghz} cleanair air-quality {summary|worst}

構文の説明

24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。
summary	802.11 無線帯域電波品質情報のサマリーを表示します。
worst	802.11 ネットワークの最も深刻な電波品質の情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、5 GHz 帯域の最も深刻な電波品質の情報を表示する例を示します。

```
Switch# show ap dot11 5ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 36      95     70     0           40
```

次に、2.4 GHz 帯域の最も深刻な電波品質の情報を表示する例を示します。

```
Switch# show ap dot11 24ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 1       83     57     3           5
```

show ap dot11 cleanair config

802.11 ネットワークの CleanAir 設定を表示するには、**showapdot11cleanairconfig** コマンドを使用します。

show ap dot11 {24ghz|5ghz} cleanair config

構文の説明

24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、2.4 GHz 帯域の CleanAir 設定を表示する例を示します。

```
Switch# show ap dot11 24ghz cleanair config
Clean Air Solution................................ : Disabled
Air Quality Settings:
    Air Quality Reporting......................... : Disabled
    Air Quality Reporting Period (min)............ : 15
    Air Quality Alarms............................ : Enabled
    Air Quality Alarm Threshold................... : 10
Interference Device Settings:
    Interference Device Reporting................. : Enabled
        Bluetooth Link............................ : Enabled
        Microwave Oven............................ : Enabled
        802.11 FH................................. : Enabled
        Bluetooth Discovery....................... : Enabled
        TDD Transmitter........................... : Enabled
        Jammer.................................... : Enabled
        Continuous Transmitter.................... : Enabled
        DECT-like Phone........................... : Enabled
        Video Camera.............................. : Enabled
        802.15.4.................................. : Enabled
        WiFi Inverted............................. : Enabled
        WiFi Invalid Channel...................... : Enabled
        SuperAG................................... : Enabled
        Canopy.................................... : Enabled
        Microsoft Device.......................... : Enabled
        WiMax Mobile.............................. : Enabled
        WiMax Fixed............................... : Enabled
    Interference Device Types Triggering Alarms:
        Bluetooth Link............................ : Disabled
        Microwave Oven............................ : Disabled
        802.11 FH................................. : Disabled
        Bluetooth Discovery....................... : Disabled
        TDD Transmitter........................... : Disabled
```

```
        Jammer................................... : Disabled
        Continuous Transmitter................... : Disabled
        DECT-like Phone.......................... : Disabled
        Video Camera............................. : Disabled
        802.15.4................................. : Disabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Disabled
        Canopy................................... : Disabled
        Microsoft Device......................... : Disabled
        WiMax Mobile............................. : Disabled
        WiMax Fixed.............................. : Disabled
    Interference Device Alarms................... : Enabled
Additional Clean Air Settings:
    CleanAir Event-driven RRM State.............. : Disabled
    CleanAir Driven RRM Sensitivity.............. : LOW
    CleanAir Persistent Devices state............ : Disabled
```

show ap dot11 cleanair summary

すべての 802.11a Cisco AP の CleanAir 設定を表示するには、**show ap dot11 cleanair summary** コマンドを使用します。

show ap dot11 {**24ghz**|**5ghz**} **cleanair summary**

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
cleanair summary	すべての 802.11a Cisco AP の CleanAir 設定のサマリー

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

show ap dot11

802.11a および 802.11b の設定情報を表示するには、**showapdot11** コマンドを使用します。

show ap dot11{**24ghz**|**5ghz**}
{**channel**|**coverage**|**group**|**load-info**|**logging**|**media-stream**|**monitor**|**network**|**profile**|**receiver**|**service-policy**|**summary**|**txpower**|**ccx global**}

構文の説明

24ghz	2.4 GHz 帯域を指定します。
5ghz	5 GHz 帯域を指定します。
channel	自動チャネル割り当ての設定と統計情報を表示します。
coverage	カバレッジホール検出の設定と統計情報を表示します。
group	802.11a または 802.11b のシスコ無線 RF グループを表示します。
load-info	すべての Cisco AP のチャネルの使用率およびクライアント数の情報を表示します。
logging	802.11a または 802.11b の RF イベントとパフォーマンスのログを表示します。
media-stream	802.11a または 802.11b のメディア リソース予約制御の設定を表示します。
monitor	802.11a または 802.11b のデフォルトのシスコ無線モニタリングを表示します。
network	802.11a または 802.11b のネットワーク設定を表示します。
profile	802.11a または 802.11b の Lightweight アクセス ポイントのパフォーマンス プロファイルを表示します。
receiver	802.11a または 802.11b レシーバの設定と統計情報を表示します。
service-policy	すべてのシスコ アクセス ポイントの 802.11a または 802.11b 無線に関するサービス品質（QoS）ポリシーを表示します。

summary	802.11a または 802.11b の Cisco Lightweight アクセス ポイントの名前、チャネル、および送信レベルのサマリーを表示します。
txpower	802.11a または 802.11b の自動送信電力割り当てを表示します。
ccxglobal	スイッチに結合されたすべてのシスコ アクセス ポイントに関する 802.11a または 802.11b の Cisco Client eXtensions（CCX）情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**load-info** パラメータが追加されました。

次に、自動チャネル割り当ての設定および統計情報を表示する例を示します。

```
Switch# show ap dot11 5ghz channel
Automatic Channel Assignment
  Channel Assignment Mode                   : AUTO
  Channel Update Interval                   : 12 Hours
  Anchor time (Hour of the day)             : 20
  Channel Update Contribution               : SNI.
  Channel Assignment Leader                 : web (9.9.9.2)
  Last Run                                  : 13105 seconds ago
  DCA Sensitivity Level                     : MEDIUM (15 dB)
  DCA 802.11n Channel Width                 : 40 Mhz
  Channel Energy Levels
      Minimum                               : unknown
      Average                               : unknown
      Maximum                               : unknown
  Channel Dwell Times
      Minimum                               : unknown
      Average                               : unknown
      Maximum                               : unknown
  802.11a 5 GHz Auto-RF Channel List
  Allowed Channel List                      : 36,40,44,48,52,56,60,64,149,153,1
57,161
  Unused Channel List                       : 100,104,108,112,116,132,136,140,1
65
  802.11a 4.9 GHz Auto-RF Channel List
  Allowed Channel List                      :
  Unused Channel List                       : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24,25,26
  DCA Outdoor AP option                     : Disabled
```

次に、カバレッジ ホール検出の統計情報を表示する例を示します。

```
Switch# show ap dot11 5ghz coverage
Coverage Hole Detection
  802.11a Coverage Hole Detection Mode          : Enabled
  802.11a Coverage Voice Packet Count           : 100 packet(s)
  802.11a Coverage Voice Packet Percentage      : 50 %
  802.11a Coverage Voice RSSI Threshold         : -80dBm
  802.11a Coverage Data Packet Count            : 50 packet(s)
  802.11a Coverage Data Packet Percentage       : 50 %
  802.11a Coverage Data RSSI Threshold          : -80dBm
  802.11a Global coverage exception level       : 25
  802.11a Global client minimum exception level   : 3 clients
```

次に、シスコの無線 RF グループ設定を表示する例を示します。

```
Switch# show ap dot11 5ghz group
Radio RF Grouping

  802.11a Group Mode                 : STATIC
  802.11a Group Update Interval      : 600 seconds
  802.11a Group Leader               : web (10.10.10.1)
  802.11a Group Member               : web(10.10.10.1)
                                       nb1(172.13.21.45) (*Unreachable)
  802.11a Last Run                   : 438 seconds ago


  Mobility Agents RF membership information
  ------------------------------------------------------------
  No of 802.11a MA RF-members : 0
```

次に、802.11a RF イベント ログおよびパフォーマンス ログを表示する例を示します。

```
Switch# show ap dot11 5ghz logging
RF Event and Performance Logging

  Channel Update Logging              : Off
  Coverage Profile Logging            : Off
  Foreign Profile Logging             : Off
  Load Profile Logging                : Off
  Noise Profile Logging               : Off
  Performance Profile Logging         : Off
  TxPower Update Logging              : Off
```

次に、802.11a メディア ストリームの設定を表示する例を示します。

```
Switch# show ap dot11 5ghz media-stream
Multicast-direct                : Disabled
Best Effort                     : Disabled
Video Re-Direct                 : Disabled
Max Allowed Streams Per Radio     : Auto
Max Allowed Streams Per Client    : Auto
Max Video Bandwidth              : 0
Max Voice Bandwidth              : 75
Max Media Bandwidth              : 85
Min PHY Rate (Kbps)              : 6000
Max Retry Percentage             : 80
```

次に、802.11b ネットワークの無線監視を表示する例を示します。

```
Switch# show ap dot11 5ghz monitor
Default 802.11a AP monitoring
```

```
  802.11a Monitor Mode                            : Enabled
  802.11a Monitor Mode for Mesh AP Backhaul       : disabled
  802.11a Monitor Channels                        : Country channels
  802.11a RRM Neighbor Discover Type              : Transparent
  802.11a AP Coverage Interval                    : 180 seconds
  802.11a AP Load Interval                        : 60 seconds
  802.11a AP Noise Interval                       : 180 seconds
  802.11a AP Signal Strength Interval             : 60 seconds
```

次に、802.11a プロファイルのグローバル設定と統計情報を表示する例を示します。

```
Switch# show ap dot11 5ghz profile
Default 802.11a AP performance profiles
802.11a Global Interference threshold.............. 10%
802.11a Global noise threshold..................... -70 dBm
802.11a Global RF utilization threshold............ 80%
802.11a Global throughput threshold................ 1000000 bps
802.11a Global clients threshold................... 12 clients
802.11a Global coverage threshold.................. 12 dB
802.11a Global coverage exception level............ 80%
802.11a Global client minimum exception lev........ 3 clients
```

次に、802.11aプロファイルのネットワーク設定と統計情報を表示する例を示します。

```
Switch# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
  802.11a Low Band : Enabled
  802.11a Mid Band : Enabled
  802.11a High Band : Enabled

802.11a Operational Rates
  802.11a 6M : Mandatory
  802.11a 9M : Supported
  802.11a 12M : Mandatory
  802.11a 18M : Supported
  802.11a 24M : Mandatory
  802.11a 36M : Supported
  802.11a 48M : Supported
  802.11a 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
```

```
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

次に、802.11a プロファイルのグローバル設定と統計情報を表示する例を示します。

```
Switch# show ap dot11 5ghz receiver
Default 802.11a AP performance profiles
802.11a Global Interference threshold.............. 10%
802.11a Global noise threshold..................... -70 dBm
```

```
802.11a Global RF utilization threshold..... 80%
802.11a Global throughput threshold..... 1000000 bps
802.11a Global clients threshold..... 12 clients
802.11a Global coverage threshold..... 12 dB
802.11a Global coverage exception level..... 80%
802.11a Global client minimum exception lev..... 3 clients
```

次に、802.11a プロファイルのグローバル設定と統計情報を表示する例を示します。

```
Switch# show ap dot11 5ghz service-policy
```

次に、802.11b アクセス ポイント設定の要約を表示する例を示します。

```
Switch# show ap dot11 5ghz summary
AP Name MAC Address       Admin State Operation State Channel TxPower
------- ----------------- ----------- --------------- ------- -------
CJ-1240 00:21:1b:ea:36:60 ENABLED     UP              161     1( )
CJ-1130 00:1f:ca:cf:b6:60 ENABLED     UP              56*     1(*)
```

次に、802.11a 伝送パワー コストの設定と統計情報を表示する例を示します。

```
Switch# show ap dot11 5ghz txpower
Automatic Transmit Power Assignment

Transmit Power Assignment Mode          : AUTO
Transmit Power Update Interval          : 600 seconds
Transmit Power Threshold                : -70 dBm
Transmit Power Neighbor Count           : 3 APs
Min Transmit Power                      : -10 dBm
Max Transmit Power                      : 30 dBm
Transmit Power Update Contribution      : SNI.
Transmit Power Assignment Leader        : web (10.10.10.1)
Last Run                                : 437 seconds ago
```

次に、802.11a 伝送パワー コストの設定と統計情報を表示する例を示します。

```
Switch# show ap dot11 5ghz ccx global
 802.11a Client Beacon Measurements:
     disabled
```

関連トピック

ap dot11 rrm channel dca （318 ページ）

show ap env summary

AP 環境のサマリーを表示するには、**show ap env summary** コマンドを使用します。

キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

次に、AP 環境のサマリーを表示する例を示します。

```
Switch#show ap env summary
```

show ap ethernet statistics

すべての Cisco Lightweight アクセス ポイントに関するイーサネット統計情報を表示するには、**showapethernetstatistics** コマンドを使用します。

show ap ethernet statistics

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、すべてのアクセス ポイントのイーサネット情報を表示する例を示します。

```
Switch# show ap ethernet statistics
```

show ap gps-location summary

接続されているすべてのCisco APのGPS位置のサマリーを表示するには、**show ap gps-location summary** コマンドを使用します。

キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

次に、接続されているすべてのCisco APのGPS位置のサマリーを表示する例を示します。

```
Switch# show ap gps-location summary
```

show ap groups

システム内に定義されているすべてのアクセス ポイント グループに関する情報を表示するには、**showapgroups** コマンドを使用します。

show ap groups

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、すべてのアクセス ポイント グループの情報を表示する例を示します。

```
Switch# show ap groups
```

show ap groups extended

システム内に定義されているすべての AP グループの詳細情報を表示するには、**show ap groups extended** コマンドを使用します。

show ap groups extended

構文の説明	**extended** システム内に定義されているすべての AP グループの詳細情報を表示します。

コマンド デフォルト	なし

コマンド モード	特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

show ap image

Cisco Lightweight アクセス ポイントに存在しているイメージを表示するには、**showapimage** コマンドを使用します。

show ap image

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントに存在しているイメージを表示する例を示します。

```
Switch# show ap image
```

show ap is-supported

AP モデルがサポートされているかどうかを確認するには、**show ap is-supported** コマンドを使用します。

show ap is-supported *model-part-number*

構文の説明

model-part-number	AP モデルの部品番号。例：AIR-LAP1142N-N-K9。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0E	このコマンドが導入されました。

次に、AP モデルがサポートされているかどうかを確認する例を示します。

```
Switch# show ap is-supported AIR-LAP1142N-N-K9

AP Support: Yes
```

show ap join stats summary

特定のアクセス ポイントで最後に発生した結合エラーの詳細を表示するには、**show ap join stats summary** コマンドを使用します。

show ap join stats summary

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

802.11 無線インターフェイスの MAC アドレスを取得するには、アクセス ポイントで **show interface** コマンドを入力します。

次に、アクセス ポイントの結合情報を表示する例を示します。

```
Switch# show ap join stats summary
Number of APs : 1

Base MAC        Ethernet MAC    AP Name               IP Address       Status

--------------- --------------- --------------------- ---------------- -------------
-
c8f9.f91a.aa80  0000.0000.0000  N A                   0.0.0.0          Not Joined
```

show ap link-encryption

リンク暗号化ステータスを表示するには、**show ap link-encryption** コマンドを使用します。

show ap link-encryption

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、リンク暗号化ステータスを表示する例を示します。

```
Switch# show ap link-encryption
```

show ap mac-address

アクセスポイントに関して収集された結合関連の統計情報、および最後の結合エラーの詳細を表示するには、**showapmac-address** コマンドを使用します。

show ap mac-address *mac-address* **join stats** {**detailed**|**summary**}

構文の説明

mac-address	アクセス ポイント Ethernet MAC アドレス、または 802.11 無線インターフェイスの MAC アドレス。
joinstats	シスコのアクセス ポイントの結合情報と統計情報を表示します。
detailed	収集されたすべての結合関連の統計情報を表示します。
summary	最後の結合エラーの詳細を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、スイッチを結合しようしている特定のアクセス ポイントの結合情報を表示する例を示します。

```
Switch# show ap mac-address d0c2.8267.8b00 join stats detailed

Discovery phase statistics
  Discovery requests received                            : 6
  Successful discovery responses sent                    : 6
  Unsuccessful discovery request processing              : 0
  Reason for last unsuccessful discovery attempt         : Not applicable
  Time at last successful discovery attempt              : Nov 20 17:25:10.841
  Time at last unsuccessful discovery attempt            : Not applicable

Join phase statistics
  Join requests received                                 : 3
  Successful join responses sent                         : 3
  Unsuccessful join request processing                   : 0
  Reason for last unsuccessful join attempt              : Not applicable
  Time at last successful join attempt                   : Nov 20 17:25:20.998
  Time at last unsuccessful join attempt                 : Not applicable

Configuration phase statistics
  Configuration requests received                        : 8
  Successful configuration responses sent                : 3
  Unsuccessful configuration request processing          : 0
  Reason for last unsuccessful configuration attempt     : Not applicable
  Time at last successful configuration attempt          : Nov 20 17:25:21.177
  Time at last unsuccessful configuration attempt        : Not applicable
```

```
Last AP message decryption failure details
  Reason for last message decryption failure              : Not applicable

Last AP disconnect details
  Reason for last AP connection failure                   : Number of message
retransmission to the AP has reached maximum

Last join error summary
  Type of error that occurred last                      : AP got or has been disconnected

  Reason for error that occurred last                     : Number of message
retransmission to the AP has reached maximum
  Time at which the last join error occurred              : Nov 20 17:22:36.438
```

次に、アクセス ポイントの結合情報を表示する例を示します。

```
Switch# show ap mac-address d0c2.8267.8b00 join stats detailed

Is the AP currently connected to controller..... No
Time at which the AP joined this controller last time..... Aug 21 12:50:36:061
Type of error that occurred last..... Lwapp join request
rejected
Reason for error that occurred last..... RADIUS authorization
is pending for the AP
Time at which the last join error occurred..... Aug 21 12:50:34:374
```

show ap monitor-mode summary

チャネルに最適化されたモニタ モードの現在の設定を表示するには、**show ap monitor-mode summary** コマンドを使用します。

show ap monitor-mode summary

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、チャネルに最適化された監視モードの現在の設定を表示する例を示します。

```
Switch# show ap monitor-mode summary

AP Name Ethernet MAC      Status   Scanning Channel List
------- -------------     -------- -------- ----------------
AP_004  xx:xx:xx:xx:xx:xx Tracking 1,6,11,  4
```

show ap name auto-rf

Cisco Lightweight アクセス ポイントの自動 RF 設定を表示するには、**show ap name auto-rf** コマンドを使用します。

show ap name *ap-name* **auto-rf dot11** {**24ghz**|**5ghz**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの自動 RF 情報を表示する例を示します。

```
Switch# show ap name AP01 auto-rf dot11 24ghz

Number of Slots                                 : 2
AP Name                                         : TSIM_AP-1
MAC Address                                     : 0000.2000.02f0
Slot ID                                         : 0
Radio Type                                      : 802.11b/g
Subband Type                                    : All

Noise Information
  Noise Profile                                 : Failed
  Channel   1                                    :   24 dBm
  Channel   2                                    :   48 dBm
  Channel   3                                    :   72 dBm
  Channel   4                                    :   96 dBm
  Channel   5                                    :  120 dBm
  Channel   6                                    : -112 dBm
  Channel   7                                    :  -88 dBm
  Channel   8                                    :  -64 dBm
  Channel   9                                    :  -40 dBm
  Channel  10                                    :  -16 dBm
  Channel  11                                    :    8 dBm

Interference Information
  Interference Profile                          : Passed
  Channel   1                                    : -128 dBm @  0% busy
  Channel   2                                    :  -71 dBm @  1% busy
  Channel   3                                    :  -72 dBm @  1% busy
  Channel   4                                    :  -73 dBm @  2% busy
  Channel   5                                    :  -74 dBm @  3% busy
  Channel   6                                    :  -75 dBm @  4% busy
```

```
  Channel   7                                     :  -76 dBm @  5% busy
  Channel   8                                     :  -77 dBm @  5% busy
  Channel   9                                     :  -78 dBm @  6% busy
  Channel  10                                     :  -79 dBm @  7% busy
  Channel  11                                     :  -80 dBm @  8% busy

Rogue Histogram (20/40_ABOVE/40_BELOW)
    Channel  36                                   : 27/ 4/ 0
    Channel  40                                   : 13/ 0/ 0
    Channel  44                                   :  5/ 0/ 0
    Channel  48                                   :  6/ 0/ 1
    Channel  52                                   :  4/ 0/ 0
    Channel  56                                   :  5/ 0/ 0
    Channel  60                                   :  1/ 3/ 0
    Channel  64                                   :  3/ 0/ 0
    Channel 100                                   :  0/ 0/ 0
    Channel 104                                   :  0/ 0/ 0
    Channel 108                                   :  0/ 1/ 0

Load Information
  Load Profile                                  : Passed
  Receive Utilization                           : 10%
  Transmit Utilization                          : 20%
  Channel Utilization                           : 50%
  Attached Clients                              : 0 clients

Coverage Information
  Coverage Profile                              : Passed
  Failed Clients                                : 0 clients

Client Signal Strengths
  RSSI -100 dBm                                 : 0 clients
  RSSI  -92 dBm                                 : 0 clients
  RSSI  -84 dBm                                 : 0 clients
  RSSI  -76 dBm                                 : 0 clients
  RSSI  -68 dBm                                 : 0 clients
  RSSI  -60 dBm                                 : 0 clients
  RSSI  -52 dBm                                 : 0 clients

Client Signal to Noise Ratios
  SNR    0 dB                                   : 0 clients
  SNR    5 dB                                   : 0 clients
  SNR   10 dB                                   : 0 clients
  SNR   15 dB                                   : 0 clients
  SNR   20 dB                                   : 0 clients
  SNR   25 dB                                   : 0 clients
  SNR   30 dB                                   : 0 clients
  SNR   35 dB                                   : 0 clients
  SNR   40 dB                                   : 0 clients
  SNR   45 dB                                   : 0 clients

Nearby APs
  AP 0000.2000.0300 slot 0                      : -68 dBm on  11 (10.10.10.1)
  AP 0000.2000.0400 slot 0                      : -68 dBm on  11 (10.10.10.1)
  AP 0000.2000.0600 slot 0                      : -68 dBm on  11 (10.10.10.1)

Radar Information

Channel Assignment Information
  Current Channel Average Energy                : 0 dBm
  Previous Channel Average Energy               : 0 dBm
  Channel Change Count                          : 0
  Last Channel Change Time                      : Wed Oct 17 08:13:36 2012
  Recommended Best Channel                      : 11
```

```
RF Parameter Recommendations
  Power Level                                   : 1
  RTS/CTS Threshold                             : 2347
  Fragmentation Threshold                       : 2346
  Antenna Pattern                               : 0

Persistent Interference Devices
```

show ap name bhmode

Cisco ブリッジ バックホール モードを表示するには、**show ap name bhmode** コマンドを使用します。

show ap name *ap-name* **bhmode**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの Cisco ブリッジ バックホール モードを表示する例を示します。

```
Switch# show ap name TSIM_AP-1 bhmode
```

show ap name bhrate

Cisco ブリッジ バックホール レートを表示するには、**show ap name bhrate** コマンドを使用します。

show ap name *ap-name* **bhrate**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの Cisco ブリッジ バックホール レートを表示する例を示します。

```
Switch# show ap name AP01 bhrate
```

show ap name cac voice

特定の Cisco Lightweight アクセス ポイントの音声コール アドミッション制御の詳細を表示するには、**show ap name cacvoice** コマンドを使用します。

show ap name *ap-name* **cac voice**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、特定のアクセスポイントの音声コールアドミッション制御の詳細を表示する例を示します。

```
Switch# show ap name AP01 cac voice
1) AP Name: AP01
============================

  Wireless Bandwidth (In MeanTime mt)

       Slot#  Radio          Calls  BW-Max  BW-Alloc  Bw-InUse (%age)
  ------------------------------------------------------------------
  1    0      802.11b/g      0      23437   0         0
  2    1      802.11a        0      23437   0         0

  Wired Bandwidth (in Kbps)

       Slot#  Wlan-ID  Wlan-Name              BW-Config   BW-Avail
  ------------------------------------------------------------------
  1    0      1        maria-open             0           0
  2    0      12       24                     0           0
  3    1      1        maria-open             0           0
  4    1      12       24                     0           0
```

show ap name config fnf

Cisco AP の NetFlow の入出力モニタを表示するには、**show ap name config fnf** コマンドを使用します。

show ap name *ap-name* **config fnf**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
fnf	Cisco AP の NetFlow の入出力モニタ。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

show ap name dot11 call-control

成功したコールのコール制御情報とメトリックを表示するには、**show ap name dot11 call-control** コマンドを使用します。

show ap name *ap-name* **dot11** {**24ghz**|**5ghz**} **call-control** {**call-info**|**metrics**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。
call-info	コール情報を表示します。
metrics	コール メトリックを表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの成功したコールのメトリックを表示する例を示します。

```
Switch# show ap name AP01 dot11 24ghz call-control metrics

Slot#   Call Count      Call Duration
---------------------------------
0       0               0
```

show ap name cable-modem

特定の AP の AP CAPWAP CCX を表示するには、**show ap name cable-modem** コマンドを使用します。

show ap name *ap-name***cable-modem**

構文の説明

ap-name	特定の AP の名前。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0E	このコマンドが導入されました。

次に、AP1 の AP CAPWAP CCX を表示する例を示します。

```
Switch# show ap name ap1 cable-modem
```

show ap name capwap retransmit

Control And Provisioning of Wireless Access Points（CAPWAP）の再送信の設定を表示するには、**show ap name capwap retransmit** コマンドを使用します。

show ap name *ap-name* **capwap retransmit**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの CAPWAP の再送信の設定を表示する例を示します。

```
Switch# show ap name AP01 capwap retransmit

AP Name   Retransmit Interval Retransmit Count
--------  -------------------- ----------------
AP01      3                    5
```

show ap name ccx rm

アクセス ポイントの Cisco Client Extension（CCX）無線管理ステータス情報を表示するには、**show ap name ccx rm** コマンドを使用します。

show ap name *ap-name* **ccx rm status**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの CCX 無線管理情報を表示する例を示します。

```
Switch# show ap name AP01 ccx rm status

802.11b/g Radio
  Beacon Request                                : Disabled
  Channel Load Request                          : Disabled
  Frame Request                                 : Disabled
  Noise Histogram Request                       : Disabled
  Path Loss Request                             : Disabled
  Interval                                      : 60
  Iteration                                     : 0

802.11a Radio
  Beacon Request                                : Disabled
  Channel Load Request                          : Disabled
  Frame Request                                 : Disabled
  Noise Histogram Request                       : Disabled
  Path Loss Request                             : Disabled
  Interval                                      : 60
  Iteration                                     : 0
```

show ap name cdp

アクセス ポイントの Cisco Discovery Protocol（CDP）情報を表示するには、**show ap name cdp** コマンドを使用します。

show ap name *ap-name* **cdp** [**neighbors** [**detail**]]

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
neighbors	（任意）CDP を使用しているネイバーを表示します。
detail	（任意）CDP を使用している特定のアクセス ポイントのネイバーに関する詳細情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの CDP 情報を表示する例を示します。

```
Switch# show ap name AP01 cdp neighbors detail
```

show ap name channel

特定のメッシュアクセスポイントの使用可能なチャネルを表示するには、**show ap name channel** コマンドを使用します。

show ap name *ap-name* **channel**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、特定のアクセス ポイントの使用可能なチャネルを表示する例を示します。

```
Switch# show ap name AP01 channel

Slot ID                                    : 0
Allowed Channel List                       : 1, 2, 3, 4, 5, 6, 7, 8, 9
                                             10, 11
Slot ID                                    : 1
Allowed Channel List                       : 36, 40, 44, 48, 52, 56, 60, 64, 100
                                             104, 108, 112, 116, 132, 136, 140,
149, 153
                                             157, 161
```

show ap name config

特定の Cisco Lightweight アクセス ポイントの一般的な情報およびイーサネット VLAN タギング情報を表示するには、**show ap name config** コマンドを使用します。

show ap name *ap-name* **config** {**ethernet**|**general**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
ethernet	アクセスポイントのイーサネットタギング設定情報を表示します。
general	アクセス ポイントの一般的な情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントのイーサネット タギング情報を表示する例を示します。

```
Switch# show ap name AP01 config ethernet

VLAN Tagging Information for AP01
```

次に、アクセス ポイントの一般的な情報を表示する例を示します。

```
Switch# show ap name AP01 config general

Cisco AP Name                                   : AP01
Cisco AP Identifier                             : 5
Country Code                                    : US  - United States
Regulatory Domain Allowed by Country            : 802.11bg:-A     802.11a:-A
AP Country Code                                 : US  - United States
AP Regulatory Domain                            : Unconfigured
Switch Port Number                              : Te1/0/1
MAC Address                                     : 0000.2000.02f0
IP Address Configuration                        : Static IP assigned
IP Address                                      : 10.10.10.12
IP Netmask                                      : 255.255.0.0
Gateway IP Address                              : 10.10.10.1
Fallback IP Address Being Used                  : 10.10.10.12
Domain                                          : Cisco
Name Server                                     : 0.0.0.0
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Enabled
SSH State                                       : Disabled
Cisco AP Location                               : sanjose
Cisco AP Group Name                             : default-group
Primary Cisco Controller Name                   : CAPWAP Controller
Primary Cisco Controller IP Address             : 10.10.10.1
Secondary Cisco Controller Name                 :
```

```
Secondary Cisco Controller IP Address           : Not Configured
Tertiary Cisco Controller Name                  :
Tertiary Cisco Controller IP Address            : Not Configured
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : Local
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : informational
Software Version                                : 7.4.0.5
Boot Version                                    : 7.4.0.5
Stats Reporting Period                          : 180
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : Power Injector/Normal Mode
Number of Slots                                 : 2
AP Model                                        : 1140AG
AP Image                                        : C1140-K9W8-M
IOS Version                                     :
Reset Button                                    :
AP Serial Number                                : SIM1140K001
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : cisco
AP 802.1X User Mode                             : Not Configured
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 15 days 16 hours 19 minutes 57
 seconds
AP CAPWAP Up Time                               : 4 minutes 56 seconds
Join Date and Time                              : 10/18/2012 04:48:56
Join Taken Time                                 : 15 days 16 hours 15 minutes 0
seconds
Join Priority                                   : 1
Ethernet Port Duplex                            : Auto
Ethernet Port Speed                             : Auto
AP Link Latency                                 : Disabled
Rogue Detection                                 : Disabled
AP TCP MSS Adjust                               : Disabled
AP TCP MSS Size                                 : 6146
```

show ap name config dot11

特定の Cisco Lightweight アクセス ポイントに対応する 802.11 設定情報を表示するには、**show ap name config dot11** コマンドを使用します。

show ap name *ap-name* **config dot11** {**24ghz**|**49ghz**|**58ghz**|**5hgz**|**dual-band**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を表示します。
49ghz	802.11-4.9G ネットワークの設定を表示します。
58ghz	802.11-5.8G ネットワークの設定を表示します。
5hgz	5 GHz 帯域の設定を表示します。
dual-band	デュアル バンド無線の設定を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**dual-band** パラメータが追加されました。

次に、特定の Cisco Lightweight アクセス ポイントに対応する 802.11b 設定情報を表示する例を示します。

```
Switch# show ap name AP01 config dot11 24ghz

Cisco AP Identifier                             : 5
Cisco AP Name                                   : AP01
Country Code                                    : US  - United States
Regulatory Domain Allowed by Country            : 802.11bg:-A     802.11a:-A
AP Country Code                                 : US  - United States
AP Regulatory Domain                            : -A
Switch Port Number                              : Te1/0/1
MAC Address                                     : 0000.2000.02f0
IP Address Configuration                        : Static IP assigned
IP Address                                      : 10.10.10.12
IP Netmask                                      : 255.255.0.0
Gateway IP Address                              : 10.10.10.1
Fallback IP Address Being Used                  : 10.10.10.12
Domain                                          : Cisco
Name Server                                     : 0.0.0.0
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Enabled
SSH State                                       : Disabled
```

```
Cisco AP Location                               : sanjose
Cisco AP Group Name                             : default-group
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : Local
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : informational
Software Version                                : 7.4.0.5
Boot Version                                    : 7.4.0.5
Mini IOS Version                                : 3.0.51.0
Stats Reporting Period                          : 180
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : Power Injector/Normal Mode
Number of Slots                                 : 2
AP Model                                        : 1140AG
AP Image                                        : C1140-K9W8-M
IOS Version                                     :
Reset Button                                    :
AP Serial Number                                : SIM1140K001
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : cisco
AP 802.1X User Mode                             : Not Configured
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 15 days 17 hours 9 minutes 41
seconds
AP CAPWAP Up Time                               : 54 minutes 40 seconds
Join Date and Time                              : 10/18/2012 04:48:56
Join Taken Time                                 : 15 days 16 hours 15 minutes 0
seconds

Attributes for Slot 0
  Radio Type                                    : 802.11n - 2.4 GHz
  Administrative State                          : Enabled
  Operation State                               : Up
  Cell ID                                       : 0

  Station Configuration
    Configuration                               : Automatic
    Number of WLANs                             : 1
    Medium Occupancy Limit                      : 100
    CFP Period                                  : 4
    CFP Maximum Duration                        : 60
    BSSID                                       : 000020000200

    Operation Rate Set
       1000 Kbps                                : MANDATORY
       2000 Kbps                                : MANDATORY
       5500 Kbps                                : MANDATORY
      11000 Kbps                                : MANDATORY
       6000 Kbps                                : SUPPORTED
       9000 Kbps                                : SUPPORTED
      12000 Kbps                                : SUPPORTED
      18000 Kbps                                : SUPPORTED
      24000 Kbps                                : SUPPORTED
      36000 Kbps                                : SUPPORTED
      48000 Kbps                                : SUPPORTED
      54000 Kbps                                : SUPPORTED
```

```
  MCS Set
    MCS  0                                    : SUPPORTED
    MCS  1                                    : SUPPORTED
    MCS  2                                    : SUPPORTED
    MCS  3                                    : SUPPORTED
    MCS  4                                    : SUPPORTED
    MCS  5                                    : SUPPORTED
    MCS  6                                    : SUPPORTED
    MCS  7                                    : SUPPORTED
    MCS  8                                    : SUPPORTED
    MCS  9                                    : SUPPORTED
    MCS 10                                    : SUPPORTED
    MCS 11                                    : SUPPORTED
    MCS 12                                    : SUPPORTED
    MCS 13                                    : SUPPORTED
    MCS 14                                    : SUPPORTED
    MCS 15                                    : SUPPORTED
    MCS 16                                    : DISABLED
    MCS 17                                    : DISABLED
    MCS 18                                    : DISABLED
    MCS 19                                    : DISABLED
    MCS 20                                    : DISABLED
    MCS 21                                    : DISABLED
    MCS 22                                    : DISABLED
    MCS 23                                    : DISABLED

  Beacon Period                               : 100
  Fragmentation Threshold                     : 2346
  Multi Domain Capability Implemented         : True
  Multi Domain Capability Enabled             : True
  Country String                              : US

Multi Domain Capability
  Configuration                               : Automatic
  First Channel                               : 0
  Number of Channels                          : 0
  Country String                              : US

MAC Operation Parameters
  Configuration                               : Automatic
  Fragmentation Threshold                     : 2346
  Packet Retry Limit                          : 64
  Legacy Tx Beamforming Setting               : Disabled

Tx Power
  Number of Supported Power Levels            : 8
  Tx Power Level 1                            : 20 dBm
  Tx Power Level 2                            : 17 dBm
  Tx Power Level 3                            : 14 dBm
  Tx Power Level 4                            : 11 dBm
  Tx Power Level 5                            : 8 dBm
  Tx Power Level 6                            : 5 dBm
  Tx Power Level 7                            : 2 dBm
  Tx Power Level 8                            : -1 dBm
  Tx Power Configuration                      : Automatic
  Current Tx Power Level                      : 1

Phy OFDM Parameters
  Configuration                               : Automatic
  Current Channel                             : 11
  Extension Channel                           : None
  Channel Width                               : 20 MHz
  Allowed Channel List                        : 1, 2, 3, 4, 5, 6, 7, 8, 9
                                                10, 11
```

```
    TI Threshold                                : 0
    Antenna Type                                : Internal
    Internal Antenna Gain (in .5 dBi units)     : 0
    Diversity                                   : Diversity enabled

    802.11n Antennas
      Tx                                        : A, B, C
      Rx                                        : A, B, C

  Performance Profile Parameters
    Configuration                               : Automatic
    Interference Threshold                      : 10%
    Noise Threshold                             : -70 dBm
    RF Utilization Threshold                    : 80%
    Data Rate Threshold                         : 1000000 bps
    Client Threshold                            : 12 clients
    Coverage SNR Threshold                      : 15 dB
    Coverage Exception Level                    : 25%
    Client Minimum Exception Level              : 3 clients
    RTS/CTS Threshold                             : 2347
    Short Retry Limit                             : 7
    Long Retry Limit                              : 4
    Max Tx MSDU Lifetime                          : 512
    Max Rx Lifetime                               : 512

  CleanAir Management Information
    CleanAir Capable                            : Yes
    CleanAir Management Admin State             : Enabled
    CleanAir Management Operation State         : Up
    Rapid Udpate Mode                           : Disabled
    Spectrum Expert connection                  : Disabled
    CleanAir NSI Key                            : 377313C8F290E246E640C4EF177BED
88
    Spectrum Expert connections counter         : 0
    CleanAir Sensor State                       : Configured

  Rogue Containment Information
    Containment Count                           : 0
```

show ap name config slot

特定の Cisco Lightweight アクセス ポイント上のスロットの設定情報を表示するには、**show ap name config slot** コマンドを使用します。

show ap name *ap-name* **config slot** {**0**|**1**|**2**|**3**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
0	スロット番号 0 を表示します。
1	スロット番号 1 を表示します。
2	スロット番号 2 を表示します。
3	スロット番号 3 を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイント上のスロットの設定情報を表示する例を示します。

```
Switch# show ap name AP01 config slot 0

Cisco AP Identifier                             : 3
Cisco AP Name                                   : AP01
Country Code                                    : US  - United States
Regulatory Domain Allowed by Country            : 802.11bg:-A     802.11a:-A
AP Country Code                                 : US  - United States
AP Regulatory Domain                            : -A
Switch Port Number                              : Te1/0/1
MAC Address                                     : 0000.2000.02f0
IP Address Configuration                        : Static IP assigned
IP Address                                      : 10.10.10.12
IP Netmask                                      : 255.255.0.0
Gateway IP Address                              : 10.10.10.1
Fallback IP Address Being Used                  : 10.10.10.12
Domain                                          : Cisco
Name Server                                     : 0.0.0.0
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Enabled
SSH State                                       : Disabled
Cisco AP Location                               : sanjose
Cisco AP Group Name                             : default-group
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : Local
```

```
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : informational
Software Version                                : 7.4.0.5
Boot Version                                    : 7.4.0.5
Mini IOS Version                                : 3.0.51.0
Stats Reporting Period                          : 180
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : Power Injector/Normal Mode
Number of Slots                                 : 2
AP Model                                        : 1140AG
AP Image                                        : C1140-K9W8-M
IOS Version                                     :
Reset Button                                    :
AP Serial Number                                : SIM1140K001
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : cisco
AP 802.1X User Mode                             : Not Configured
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 15 days 16 hours 1 minute 19 s
econds
AP CAPWAP Up Time                               : 20 hours 21 minutes 37 seconds

Join Date and Time                              : 10/17/2012 08:13:36
Join Taken Time                                 : 14 days 19 hours 39 minutes 41
 seconds

Attributes for Slot 0
  Radio Type                                    : 802.11n - 2.4 GHz
  Administrative State                          : Enabled
  Operation State                               : Up
  Cell ID                                       : 0

  Station Configuration
    Configuration                               : Automatic
    Number of WLANs                             : 1
    Medium Occupancy Limit                      : 100
    CFP Period                                  : 4
    CFP Maximum Duration                        : 60
    BSSID                                       : 000020000200

    Operation Rate Set
       1000 Kbps                                : MANDATORY
       2000 Kbps                                : MANDATORY
       5500 Kbps                                : MANDATORY
      11000 Kbps                                : MANDATORY
       6000 Kbps                                : SUPPORTED
       9000 Kbps                                : SUPPORTED
      12000 Kbps                                : SUPPORTED
      18000 Kbps                                : SUPPORTED
      24000 Kbps                                : SUPPORTED
      36000 Kbps                                : SUPPORTED
      48000 Kbps                                : SUPPORTED
      54000 Kbps                                : SUPPORTED

    MCS Set
      MCS  0                                    : SUPPORTED
      MCS  1                                    : SUPPORTED
      MCS  2                                    : SUPPORTED
```

```
    MCS  3                                    : SUPPORTED
    MCS  4                                    : SUPPORTED
    MCS  5                                    : SUPPORTED
    MCS  6                                    : SUPPORTED
    MCS  7                                    : SUPPORTED
    MCS  8                                    : SUPPORTED
    MCS  9                                    : SUPPORTED
    MCS 10                                    : SUPPORTED
    MCS 11                                    : SUPPORTED
    MCS 12                                    : SUPPORTED
    MCS 13                                    : SUPPORTED
    MCS 14                                    : SUPPORTED
    MCS 15                                    : SUPPORTED
    MCS 16                                    : DISABLED
    MCS 17                                    : DISABLED
    MCS 18                                    : DISABLED
    MCS 19                                    : DISABLED
    MCS 20                                    : DISABLED
    MCS 21                                    : DISABLED
    MCS 22                                    : DISABLED
    MCS 23                                    : DISABLED

  Beacon Period                               : 100
  Fragmentation Threshold                     : 2346
  Multi Domain Capability Implemented         : True
  Multi Domain Capability Enabled             : True
  Country String                              : US

Multi Domain Capability
  Configuration                               : Automatic
  First Channel                               : 0
  Number of Channels                          : 0
  Country String                              : US

MAC Operation Parameters
  Configuration                               : Automatic
  Fragmentation Threshold                     : 2346
  Packet Retry Limit                          : 64

Tx Power
  Number of Supported Power Levels            : 8
  Tx Power Level 1                            : 20 dBm
  Tx Power Level 2                            : 17 dBm
  Tx Power Level 3                            : 14 dBm
  Tx Power Level 4                            : 11 dBm
  Tx Power Level 5                            : 8 dBm
  Tx Power Level 6                            : 5 dBm
  Tx Power Level 7                            : 2 dBm
  Tx Power Level 8                            : -1 dBm
  Tx Power Configuration                      : Automatic
  Current Tx Power Level                      : 1

Phy OFDM Parameters
  Configuration                               : Automatic
  Current Channel                             : 11
  Extension Channel                           : None
  Channel Width                               : 20 MHz
  Allowed Channel List                        : 1, 2, 3, 4, 5, 6, 7, 8, 9
                                                10, 11
  TI Threshold                                : 0
  Antenna Type                                : Internal
  Internal Antenna Gain (in .5 dBi units)     : 0
  Diversity                                   : Diversity enabled
```

```
  802.11n Antennas
    Tx                                    : A, B, C
    Rx                                    : A, B, C

Performance Profile Parameters
  Configuration                           : Automatic
  Interference Threshold                  : 10%
  Noise Threshold                         : -70 dBm
  RF Utilization Threshold                : 80%
  Data Rate Threshold                     : 1000000 bps
  Client Threshold                        : 12 clients
  Coverage SNR Threshold                  : 15 dB
  Coverage Exception Level                : 25%
  Client Minimum Exception Level          : 3 clients

Rogue Containment Information
  Containment Count                       : 0
```

show ap name core-dump

Lightweight アクセス ポイントのメモリ コア ダンプ情報を表示するには、**show ap name core-dump** コマンドを使用します。

show ap name *ap-name* **core-dump**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、メモリ コア ダンプ情報を表示する例を示します。

```
Switch# show ap name 3602a core-dump

TFTP server IP : 172.31.25.21
Memory core dump file : 3602a.dump
Memory core dump file compressed : Disabled
```

関連トピック

ap name core-dump （350 ページ）

show ap name data-plane

特定の Cisco Lightweight アクセス ポイントのデータ プレーンのステータスを表示するには、**show ap name data-plane** コマンドを使用します。

show ap name *ap-name* **data-plane**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントのデータ プレーンのステータスを表示する例を示します。

```
Switch# show ap name AP01 data-plane

                      Min Data          Data          Max Data     Last
AP Name              Round Trip     Round Trip     Round Trip    Update
------------------  -------------  -------------  ------------- --------
AP01                   0.000s          0.000s        0.000s       00:00:00
```

show ap name dot11

特定の Cisco Lightweight アクセス ポイントに対応する 802.11a または 802.11b 設定情報を表示するには、**show ap name dot11** コマンドを使用します。

show ap name *ap-name* **dot11** {**24ghz**|**5ghz**} {**ccx**|**cdp**|**profile**|**service-poicy output**|**stats**|**tsm** {**all***client-mac*}}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。
ccx	Cisco Client eXtensions（CCX）無線管理ステータス情報を表示します。
cdp	シスコ検出プロトコル（CDP）情報を表示します。
profile	802.11 プロファイルの設定と統計情報を表示します。
service-policyoutput	ダウンストリームのサービス ポリシー情報を表示します。
stats	Cisco Lightweight アクセス ポイントの統計情報を表示します。
tsm	802.11 トラフィック ストリーム メトリックの統計情報を表示します。
all	クライアントがアソシエーションを持つすべてのアクセス ポイントのリストを表示します。
client-mac	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、アクセス ポイントに関連付けられたサービス ポリシーを表示する方法を示します。

```
Switch# show ap name test-ap dot11 24ghz service-policy output

Policy Name  : test-ap1
Policy State : Installed
```

次の例では、特定のアクセス ポイントの CCX RRM 802.11 の設定を表示する例を示します。

```
Switch# show ap name AP01 dot11 24ghz ccx
```

次の例では、特定のアクセス ポイントの CDP 情報を表示する方法を示します。

```
Switch# show ap name AP01 dot11 24ghz cdp

AP Name               AP CDP State
--------------------- --------------
AP03                  Disabled
```

次の例では、特定のアクセス ポイントの 802.11b プロファイルの設定と統計情報を表示する方法を示します。

```
Switch# show ap name AP01 dot11 24ghz profile

 802.11b Cisco AP performance profile mode            : GLOBAL
 802.11b Cisco AP Interference threshold              : 10 %
 802.11b Cisco AP noise threshold                     : -70 dBm
 802.11b Cisco AP RF utilization threshold            : 80 %
 802.11b Cisco AP throughput threshold                : 1000000 bps
 802.11b Cisco AP clients threshold                   : 12 clients
```

次の例では、特定のアクセスポイントのダウンストリームのサービス ポリシー情報を表示する方法を示します。

```
Switch# show ap name AP01 dot11 24ghz service-policy output

Policy Name  : def-11gn
Policy State : Installed
```

次の例では、特定のアクセス ポイントの統計情報を表示する方法を示します。

```
Switch# show ap name AP01 dot11 24ghz stats

Number of Users................................: 0
TxFragmentCount................................: 0
MulticastTxFrameCnt............................: 0
FailedCount....................................: 0
RetryCount.....................................: 0
MultipleRetryCount.............................: 0
FrameDuplicateCount............................: 0
RtsSuccessCount................................: 0
RtsFailureCount................................: 0
AckFailureCount................................: 0
RxIncompleteFragment...........................: 0
MulticastRxFrameCnt............................: 0
FcsErrorCount..................................: 0
TxFrameCount...................................: 0
WepUndecryptableCount..........................: 0
TxFramesDropped................................: 0

Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw).....: 0
  Video Bandwidth in use(% of config bw).....: 0
  Total BW in use for Voice(%)...............: 0
  Total BW in use for SIP Preferred call(%)......: 0
```

```
Load based Voice Call Stats
  Total channel MT free.......................: 0
  Total voice MT free.........................: 0
  Na Direct...................................: 0
  Na Roam.....................................: 0

WMM TSPEC CAC Call Stats
  Total num of voice calls in progress........: 0
  Num of roaming voice calls in progress......: 0
  Total Num of voice calls since AP joined....: 0
  Total Num of roaming calls since AP joined..: 0
  Total Num of exp bw requests received.......: 0
  Total Num of exp bw requests admitted.......: 0
  Num of voice calls rejected since AP joined.: 0
  Num of roam calls rejected since AP joined..: 0
  Num of calls rejected due to insufficent bw.: 0
  Num of calls rejected due to invalid params.: 0
  Num of calls rejected due to PHY rate.......: 0
  Num of calls rejected due to QoS policy.....: 0

SIP CAC Call Stats
  Total Num of calls in progress..............: 0
  Num of roaming calls in progress............: 0
  Total Num of calls since AP joined..........: 0
  Total Num of roaming calls since AP joined..: 0
  Total Num of Preferred calls received.......: 0
  Total Num of Preferred calls accepted.......: 0
  Total Num of ongoing Preferred calls........: 0
  Total Num of calls rejected(Insuff BW)......: 0
  Total Num of roam calls rejected(Insuff BW).: 0

Band Select Stats
  Num of dual band client ....................: 0
  Num of dual band client added...............: 0
  Num of dual band client expired ............: 0
  Num of dual band client replaced............: 0
  Num of dual band client detected ...........: 0
  Num of suppressed client ...................: 0
  Num of suppressed client expired............: 0
  Num of suppressed client replaced...........: 0
```

次の例では、特定のアクセス ポイントに対応するすべてのクライアントのトラフィック ストリームの設定を表示する方法を示します。

```
Switch# show ap name AP01 dot11 24ghz tsm all
```

show ap name dot11 cleanair

アクセス ポイントに対応する CleanAir 設定情報を表示するには、**show ap name dot11 cleanair** コマンドを使用します。

show ap name *ap-name* **dot11** {**24ghz**|**5ghz**} **cleanair** {**air-quality**|**device**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。
cleanair	CleanAir 設定情報を表示します。
air-quality	CleanAir 電波品質（AQ）データを表示します。
device	5 GHz 帯域上にあるアクセス ポイントの CleanAir 干渉源を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、802.11b ネットワークのアクセス ポイントの CleanAir 電波品質情報を表示する例を示します。

```
Switch# show ap name AP01 dot11 24ghz cleanair air-quality

AQ = Air Quality
DFS = Dynamic Frequency Selection
```

次に、802.11b ネットワークのアクセス ポイントの CleanAir 干渉源情報を表示する例を示します。

```
Switch# show ap name AP01 dot11 24ghz cleanair device

DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

No ClusterID DevID Type AP Name ISI RSSI DC Channel
-- --------- ----- ---- ------- --- ---- ----------
```

show ap name env

特定の AP の AP 環境を表示するには、**show ap name env** コマンドを使用します。

show ap name *ap-name***env**

構文の説明

ap-name	特定の AP の名前。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

次に、AP1 の AP 環境を表示する例を示します。

```
Switch# show ap name ap1 env
```

show ap name ethernet statistics

特定の Cisco Lightweight アクセス ポイントのイーサネット統計情報を表示するには、**show ap name ethernet statistics** コマンドを使用します。

show ap name *ap-name* **ethernet statistics**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントのイーサネット統計情報を表示する例を示します。

```
Switch# show ap name 3602a ethernet statistics

Ethernet Stats for AP 3602a

Interface Name      Status   Speed       Rx Packets    Tx Packets    Discarded Packets

-------------------------------------------------------------------------------------
GigabitEthernet0    UP       1000 Mbps   3793          5036          0
```

show ap name eventlog

特定の Cisco Lightweight アクセス ポイントのイベント ログをダウンロードして表示するには、**show ap name eventlog** コマンドを使用します。

show ap name *ap-name* **eventlog**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、特定のアクセス ポイントのイベント ログを表示する例を示します。

```
Switch# show ap name AP01 eventlog
```

show ap gps-location summary

接続されているすべてのCisco APのGPS位置のサマリーを表示するには、**show ap gps-location summary** コマンドを使用します。

キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

次に、接続されているすべてのCisco APのGPS位置のサマリーを表示する例を示します。

```
Switch# show ap gps-location summary
```

show ap name image

指定されたアクセスポイントの事前にダウンロードされたイメージに関する詳細情報を表示するには、**show ap name image** コマンドを使用します。

show ap name *ap-name* **image**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、すべてのアクセス ポイント上に存在しているイメージの表示の例を示します。

```
Switch# show ap name 3602a image

Total number of APs  : 1

Number of APs
        Initiated                   : 0
        Predownloading              : 0
        Completed predownloading    : 0
        Not Supported               : 1
        Failed to Predownload       : 0

AP Name      Primary Image   Backup Image    Predownload Status    Predownload Ver...
Next Retry Time    Retry Count
-------------------------------------------------------------------------------------
3602a        10.0.1.234      0.0.0.0         Not supported         None
NA                           0
```

show ap name inventory

アクセス ポイントのインベントリ情報を表示するには、**show ap name inventory** コマンドを使用します。

show ap name *ap-name* **inventory**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントのインベントリ情報を表示する例を示します。

```
Switch# show ap name 3502b inventory

NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 1140AG  ,  VID: V01,  SN: SIM1140K001


NAME:     , DESCR:
PID: ,  VID: ,  SN:


NAME:     , DESCR:
PID: ,  VID: ,  SN:
NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 3502I  ,  VID: V01,  SN: FTX1525E94A


NAME: Dot11Radio0    , DESCR: 802.11N 2.4GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA


NAME: Dot11Radio1    , DESCR: 802.11N 5GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA
```

show ap name lan port

LAN 情報を表示するには、**show ap name lan port** コマンドを使用します。

show ap name lan portsummary | *port-id*

構文の説明

summary	LAN 情報の概要を表示します。
port-id	LAN情報が表示されるポートのポートID。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7SE	このコマンドが導入されました。

次に、LAN 情報の概要を表示する例を示します。

```
Switch# show ap name ap1 lan port summary
```

show ap name link-encryption

特定の Cisco Lightweight アクセス ポイントのリンク暗号化ステータスを表示するには、**show ap name link-encryption** コマンドを使用します。

show ap name *ap-name* **link-encryption**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、特定の Cisco Lightweight アクセス ポイントのリンク暗号化ステータスを表示する例を示します。

```
Switch# show ap name AP01 link-encryption

                    Encryption  Dnstream  Upstream    Last
AP Name                  State     Count     Count  Update
------------------  ----------  --------  --------  ------
AP01                 Disabled         0         0   Never
```

show ap name service-policy

特定の Cisco Lightweight アクセス ポイントのサービス ポリシー情報を表示するには、**show ap name service-policy** コマンドを使用します。

show ap name *ap-name* **service-policy**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、特定の Cisco Lightweight アクセス ポイントのサービス ポリシー情報を表示する方法を示します。

```
Switch# show ap name 3502b service-policy

NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 3502I  ,  VID: V01,  SN: FTX1525E94A


NAME: Dot11Radio0    , DESCR: 802.11N 2.4GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA


NAME: Dot11Radio1    , DESCR: 802.11N 5GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA
```

show ap name tcp-adjust-mss

アクセス ポイントの TCP 最大セグメント サイズ（MSS）を表示するには、**show ap name tcp-adjust-mss** コマンドを使用します。

show ap name *ap-name* **tcp-adjust-mss**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの TCP MSS を表示する例を示します。

```
Switch# show ap name AP01 tcp-adjust-mss

AP Name                    TCP State        MSS Size
-----------------------------------------------------------
AP01                       Disabled         6146
```

show ap name wlan

アクセス ポイントに定義された各 WLAN の基本サービス セット識別子（BSSID）値を表示し、WLAN の統計情報を表示するには、**show ap name wlan** コマンドを使用します。

show ap name *ap-name* **wlan** {**dot11** {**24ghz|5ghz**}|**statistic**}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
dot11	802.11 パラメータを表示します。
24ghz	802.11b ネットワークの設定を表示します。
5ghz	802.11a ネットワークの設定を表示します。
statistic	WLAN の統計情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、802.11b ネットワークのアクセス ポイントの BSSID 情報を表示する例を示します。

```
Switch# show ap name AP01 wlan dot11 24ghz

Site Name                                       : default-group
Site Description                                :

WLAN ID  Interface  BSSID
------------------------------------
1        default    00:00:20:00:02:00
12       default    00:00:20:00:02:0b
```

次に、アクセス ポイントの WLAN の統計情報を表示する例を示します。

```
Switch# show ap name AP01 wlan statistic

WLAN ID  : 1
WLAN Profile Name  : maria-open

   EAP Id Request Msg Timeouts           : 0
   EAP Id Request Msg Timeouts Failures  : 0
   EAP Request Msg Timeouts              : 0
   EAP Request Msg Timeouts Failures     : 0
   EAP Key Msg Timeouts                  : 0
   EAP Key Msg Timeouts Failures         : 0
```

```
WLAN ID  : 12
WLAN Profile Name  : 24

   EAP Id Request Msg Timeouts           : 0
   EAP Id Request Msg Timeouts Failures  : 0
   EAP Request Msg Timeouts              : 0
   EAP Request Msg Timeouts Failures     : 0
   EAP Key Msg Timeouts                  : 0
   EAP Key Msg Timeouts Failures         : 0
```

show ap name wlandot11 service policy

アクセスポイントの各基本サービスセット識別子（BSSID）のQoSポリシーを表示するには、次のコマンドを使用します。

show apname*ap -name***wlan dot1124ghzservice-policy**

show apname*ap -name***wlan dot115ghzservice-policy**

構文の説明

ap- name	Cisco Lightweight アクセス ポイントの名前。
service-policy	アクセスポイントのサービスポリシー情報。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、各 BSSID の QoS ポリシーを表示する例を示します。

```
Switchshow ap name <ap-name> wlan dot11 24ghz service-policy
```

show ap slots

接続されているすべての Cisco Lightweight アクセス ポイントのスロットの概要を表示するには、**show ap slots** コマンドを使用します。

show ap slots

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、接続されているすべての Cisco Lightweight アクセス ポイントのスロットの概要を表示する例を示します。

```
Controller# show ap slots

AP Name    Slots  AP Model    Slot0       Slot1      Slot2     Slot3
---------- ------ ----------- ----------- ---------- --------- --------
3602a      2      3502I       802.11b/g   802.11a    Unknown   Unknown
```

show ap summary

スイッチに接続されているすべてのCisco Lightweightアクセス ポイントのステータスの概要を表示するには、**show ap summary** コマンドを使用します。

show ap summary

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、各Lightweightアクセス ポイント名、スロット数、製造者、MACアドレス、ロケーション、スイッチのポート番号を含むリストを表示します。

次に、接続されているすべてのアクセス ポイントの要約を表示する例を示します。

```
Controller# show ap summary

Number of APs: 1

Global AP User Name: Cisco
Global AP Dot1x User Name: Not configured

AP Name                          AP Model  Ethernet MAC    Radio MAC       State

-------------------------------------------------------------------------------------
3602a                            3502I     003a.99eb.3fa8  d0c2.8267.8b00  Registered
```

show ap tcp-adjust-mss

Cisco Lightweight アクセス ポイントの TCP 最大セグメント サイズ（MSS）に関する情報を表示するには、**show ap tcp-adjust-mss** コマンドを使用します。

show ap tcp-adjust-mss

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクセス ポイントの TCP MSS 情報に関する情報を表示する例を示します。

```
Controller# show ap tcp-adjust-mss

AP Name                     TCP State        MSS Size
-------------------------------------------------------
3602a                       Disabled         0
```

show ap universal summary

接続されているすべての Cisco AP の一般的な概要を表示するには、**show ap universal summary** コマンドを使用します。

キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

次に、接続されているすべての Cisco AP の一般的な概要を表示する例を示します。

```
Switch# show ap universal summary
```

show ap uptime

接続されているすべてのCisco Lightweightアクセス ポイントの稼働時間を表示するには、**show ap uptime** コマンドを使用します。

show ap uptime

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、接続されているすべてのアクセス ポイントの稼働時間を表示する例を示します。

```
Controller# show ap uptime

Number of APs : 1

Global AP User Name : Cisco
Global AP Dot1x User Name : Not configured

AP Name Ethernet MAC    AP Up Time                      Association Up Time

------- --------------- ------------------------------- ------------------------------
3602a   003a.99eb.3fa8  5 hours 13 minutes 40 seconds  5 hours 12 minutes 15 seconds
```

show wireless ap summary

すべてのワイヤレス アクセス ポイントのステータスの概要を表示するには、**show wireless ap summary** コマンドを使用します。

show wirelessap summary

構文の説明

このコマンドには、キーワードおよび引数はありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
10.4	このコマンドが追加されました。

次に、すべてのワイヤレス アクセス ポイントの概要を表示する例を示します。

```
Controller# show wireless ap summary
Sub-Domain Access Point Summary

Maximum AP limit: 1010
Total AP Licence Installed: 1000
Total AP Licence Available: 1000
Total AP joined :0
```

show wireless client ap

Cisco Lightweight アクセス ポイント上のクライアントを表示するには、**show wireless client ap** コマンドを使用します。

show wireless client ap [**name** *ap-name*] **dot11** {**24ghz**|**5ghz**}

構文の説明

name *ap-name*	（任意）Cisco Lightweight アクセス ポイントの名前を表示します。
dot11	802.11 パラメータを表示します。
24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

show client ap コマンドでは自動的に無効にされたクライアントのステータスが表示されることがあります。除外リスト（ブラック リスト）のクライアントを表示するには、**show exclusionlist** コマンドを使用します。

次に、2.4 GHz 帯域の特定の Cisco Lghtweight アクセス ポイントのクライアント情報を表示する例を示します。

```
Switch# show wireless client ap name AP01 dot11 24ghz

MAC Address       AP Id  Status     WLAN Id Authenticated
----------------- ------ ---------- ------- -------------
xx:xx:xx:xx:xx:xx 1      Associated 1       No
```

test ap name

アクセス ポイントとスイッチ間のパスの最大伝送ユニット（MTU）の自動テストを有効にするには、**test ap name** コマンドを使用します。

test ap name *ap-name* **pmtu** {**disable size** *size*|**enable**}

構文の説明

ap-name	ターゲットの Cisco Lightweight アクセス ポイントの名前。
pmtu	アクセス ポイントの MTU 設定をテストします。
disable	パス MTU のテストを無効にし、MTU 値（バイト単位）を手動で設定します。
size *size*	パス MTU のサイズを指定します。 （注） 範囲は 576 ～ 1700 です。
enable	アクセス ポイントのパス MTU のテストを有効にします。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、スイッチに関連付けられているすべてのアクセス ポイントのパス MTU 設定を無効にする例を示します。

```
Controller# test ap name 3602a pmtu enable
```

test capwap ap name

特定の Cisco Lightweight アクセス ポイントの Control And Provisioning of Wireless Access Points（CAPWAP）パラメータをテストするには、**test capwap ap name** コマンドを使用します。

test capwap ap name *ap-name* {**encryption** {**enable**|**disable**}|**message** *token*}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
encryption	Datagram Transport Layer Security（DTLS）暗号化をテストします。
enable	DTLS 暗号化が有効になっているかどうかをテストします。
disable	DTLS 暗号化が無効になっているかどうかをテストします。
message *token*	送信する RRM ネイバー メッセージを指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、特定のアクセス ポイントで DTLS 暗号化が有効になっているかどうかをテストする例を示します。

```
Controller# test capwap ap name 3602a encryption enable
```

次に、特定のアクセス ポイントで DTLS 暗号化が無効になっているかどうかをテストする例を示します。

```
Controller# test capwap ap name 3602a encryption disable
```

trapflags ap

特定の Cisco lightweight アクセス ポイント トラップの送信を有効にするには、**trapflags ap** コマンドを使用します。特定の Cisco lightweight アクセス ポイント トラップの送信を無効にするには、このコマンドの no 形式を使用します。

trapflags ap {**register**|**interfaceup**}
no trapflags ap {**register**|**interfaceup**}

構文の説明

register	Cisco Lightweight アクセス ポイントを Cisco スイッチに登録する場合、トラップの送信を有効にします。
interfaceup	Cisco Lightweight アクセス ポイント インターフェイス（A または B）が表示された場合に、トラップの送信をイネーブルにします。

コマンド デフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、トラップで、アクセス ポイント関連トラップの送信が行われないようにする例を示します。

```
Switch(config)# no trapflags ap register
```

wireless wps rogue ap rldp alarm-only

不正が検出された場合のアラームを設定するには、**wirelesswps rogueaprldp alarm-only** コマンドを使用します。アラームを無効にするには、このコマンドの **no** 形式を使用します。

[no] wireless wps rogue ap rldp alarm-only monitor-ap-only

構文の説明

monitor-ap-only	モニタ AP のみで RLDP を実行します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.7.3E	コマンドの **no** 形式が導入されました。

例

次に、検出された不正に対するアラームを設定する例を示します。

```
Switchwireless wps rogue ap rldp alarm-only
```

wireless wps rogue ap rldp auto-contain

不正が検出された場合の RLDP、アラーム、自動阻止を設定するには **wirelesswps rogueaprldp auto-contain** コマンドを使用します。アラームを無効にするには、このコマンドの no 形式を使用します。

[no] wireless wps rogue ap rldp auto-contain monitor-ap-only

構文の説明

monitor-ap-only	モニタ AP のみで RLDP を実行します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.7.3E	コマンドの **no** 形式が導入されました。

例

次に、検出された不正に対するアラームを設定する例を示します。

```
Switchwireless wps rogue ap rldp auto-contain
```

第 VI 部

モビリティ

モビリティ コマンド

mobility anchor

モビリティ スティッキ アンカリングを設定するには、**mobility anchor sticky** コマンドを使用します。スティッキ アンカリングを無効にするには、このコマンドの **no** 形式を使用します。

ゲスト アンカリングを設定するには、**mobility anchor** *ip-address* コマンドを使用します。

ゲスト アンカーを削除するには、このコマンドの **no** 形式を使用します。

デバイスを自動アンカーとして設定するには、**mobility anchor** コマンドを使用します。

mobility anchor {*ip-address*|**sticky**}
no mobility anchor {*ip-address*|**sticky**}

構文の説明

sticky	クライアントは、関連付けられている最初のスイッチにアンカーされます。 （注） このコマンドはデフォルトで有効になっており、低ローミング遅延を保証します。これは、クライアントがモビリティ ドメインに参加し、ドメイン内をローミングする場合でも、クライアントの Point of Presence のが変更されないように確保します。
ip-address	ゲスト アンカー スイッチの IP アドレスをこの WLAN に設定します。

コマンド デフォルト

スティッキ設定は、デフォルトでは有効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	Cisco IOS XE 3.3SE リリースより前の自動アンカー設定ではデバイス IP アドレスを入力する必要がありました。このリリースでは、IP アドレスが指定されていない場合、デバイス自身がアンカーになります。明示的に IP アドレスを指定する必要はありません。

使用上のガイドライン

- wlan_id または guest_lan_id は必ず指定し、無効にする必要があります。
- 1 つ目のモビリティ アンカーを設定するときに、WLAN または有線ゲスト LAN で自動アンカー モビリティを有効にします。
- 最後のアンカーを削除すると、自動アンカーモビリティ機能は無効になり、新しいアソシエーションに対しては標準のモビリティが再度使用されるようになります。
- モビリティは、ファイアウォールの通過が許可されている次のポートを使用します。
  - 16666

- 16667
- 16668

次に、スティッキ モビリティ アンカーを有効にする例を示します。

```
Switch(config-wlan)# mobility anchor sticky
```

次に、ゲスト アンカリングを設定する例を示します。

```
Switch(config-wlan)# mobility anchor 209.165.200.224
```

次に、デバイスを自動アンカーとして設定する例を示します。

```
Switch(config-wlan)# mobility anchor
```

wireless mobility

switch 間のモビリティ マネージャを設定するには、**wireless mobility** コマンドを使用します。

wireless mobility {**dscp** *value*}

構文の説明

dscp *value*	モビリティの switch 間の DSCP 値を設定します。

コマンド デフォルト

デフォルトの DSCP 値は、48 です。

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、switch 間の DSCP 値が 20 のモビリティを設定する例を示します。

```
Switch(config)# wireless mobility dscp 20
```

wireless mobility controller

モビリティ コントローラの設定を構成するには、**wireless mobility controller** コマンドを使用します。モビリティ コントローラの設定を削除するには、このコマンドの **no** 形式を使用します。

wireless mobility controller peer-group *peer-group-name* [{ **bidge-domain-id** *id*| **member ip** *ip-address* [{**public-ip** *public-ip-address*}]| **multicast ip** *multicast-address*}]
no
wireless mobility controller peer-group *peer-group-name* [{ **bidge-domain-id** *id*| **member ip** *ip-address* [{**public-ip** *public-ip-address*}]| **multicast ip** *multicast-address*}]

構文の説明

peer-group *peer-group-name*	モビリティ ピア グループを作成します。
bidge-domain-id *id*	モビリティ ピア グループのブリッジ ドメイン ID を設定します。
memberip *ip-address***public-ip** *public-ip-address*	ピア グループ メンバーを追加または削除します。 （注） **public-ip** *public-ip-address* はオプションで、モビリティ ピアが NAT 処理されている場合にのみ使用します。
multicastip *multicast-address*	ピア グループのマルチキャスト設定を構成します。

コマンド デフォルト

なし。

コマンド モード

グローバル コンフィギュレーション。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

コンバージド アクセス ソリューションでは、WLAN は VLAN にマッピングされ、VLAN は通常サブネットにマッピングされます。シームレスなローミングのため、2 つのコントローラに設定されている同じ VLAN は、同じサブネットにマッピングされることが期待されます。ローミング イベントを処理するコントローラは、次の処理が必要かどうかを判断しなければならないため、1 つのコントローラから次のコントローラへのマッピングが一致していることは、ローミングの際に重要です。

- レイヤ 2 ローミング イベントの解決（WLAN から VLAN およびサブネットへのマッピングがアンカーと外部コントローラで一致している場合）、または
- レイヤ 3 ローミング イベントの解決（WLAN から VLAN およびサブネットへのマッピングがアンカーと外部コントローラで異なっている場合）。

この判断は、コントローラ間での WLAN SSID の文字列と VLAN ID の比較によって実行されます。WLAN SSID と VLAN ID が一致する場合、VLAN に関連付けられたサブネットも一致することが予想されます。

このマッピングが一致しない場合もあります。たとえば、コントローラ 1 の WLAN1 が VLAN 14 にマッピングされ、コントローラ 1 の VLAN 14 がサブネット 10.10.14.0/24 にマッピングされているとします。同時に、コントローラ 2 の WLAN 1 は VLAN 14 にマッピングされているものの、コントローラ 2 の VLAN 14 がサブネット 172.31.24.0/24 にマッピングされているとします。コントローラ 1 と 2 は、WLAN 1 と関連付けられた VLAN を比較してレイヤ 2 ローミング イベントを処理していると判断しますが、実際には、VLAN 14 が両コントローラに対して持つレイヤ 3 としての意味が異なるため、このローミング イベントはレイヤ 3 です。

VLAN と関連付けられたサブネットとの接続が解除された場合、さまざまなブリッジ ドメイン ID に対してコンバージドアクセス コントローラを設定することもできます。同じブリッジ ドメイン ID の 2 つのコントローラは、同じ VLAN でサブネット マッピングされると想定されます。サブネット マッピング用に同じ VLAN を共有し、ローミングが予想されるすべてのコントローラに、同じブリッジ ドメイン ID を設定することをお勧めします。

次に、switch ブリッジ ドメイン ID を設定する例を示します。

```
Switch (config)# wireless mobility controller peer-group SPG1 bridge-domain-id 111
```

次に、ブリッジ ID が 111 の switch ピア グループを作成し設定する例を示します。

```
Switch(config)# controller peer-group TestDocPeerGroup bridge-domain-id 111
```

次に、ブリッジ ID が 111 の switch ピア グループを無効にする例を示します。

```
Switch(config)# no controller peer-group TestDocPeerGroup bridge-domain-id 111
```

次に、NAT 処理されたメンバーを設定する例を示します（IP 172.19.13.15 は NAT の範囲 外）。

```
Switch (config)# wireless mobility group ip 1.4.91.2 public-ip 172.19.13.15
```

次に、NAT 処理されないメンバーを設定する例を示します（IP 1.4.91.2 は NAT の範囲内）。

```
Switch (config)# wireless mobility group ip 1.4.91.2
```

wireless mobility controller (ip_address)

モビリティ コントローラを設定するには、**wireless mobility controller** コマンドを使用します。

MC から MA にスイッチを変換するには、このコマンドの **no wireless mobility controller** 形式を使用します。

モビリティ コントローラの IP アドレスを削除するには、**no wirelessmobility controller** ip-address を使用します。

wireless mobility controller [**ip** *ip-address* [**public-ip** *public-ip-address*]]
no wireless mobility controller
no wireless mobility controllerip *ip-address*

構文の説明

ip *ip-address*	モビリティ コントローラの IP アドレス。
public-ip *public-ip-address*	

コマンド デフォルト

なし。

コマンド モード

グローバル コンフィギュレーション。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、コンバージド アクセス スイッチに対してのみ有効です。

NAted アドレスは通信の確立に使用され、設定済みのワイヤレス管理インターフェイスは、CAPWAP 交換時にピア コントローラを特定するために使用されます。

次に、コントローラがワイヤレス管理インターフェイスと通信する例を示します。

```
Switch (config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6
```

次に、ターゲット コントローラが NAT を使用する場合に、ワイヤレス管理インターフェイスとともに NAT オプションを追加する例を示します。

```
Switch (config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6
public-ip 10.21.21.2
```

wireless mobility controller peer-group

モビリティ ピア グループを設定するには **wireless mobility controller peer-group** コマンドを使用し、設定を削除するにはこのコマンドの **no** 形式を使用します。

wireless mobility controller peer-group *peer-group* **member IP** *ip-address***mode centralized**

構文の説明

peer group	ピア グループの名前。
member IP	ピア グループ メンバーを追加します。
ip-address	追加するピア グループ メンバーの IP アドレス。
mode centralized	集約的に管理されるピア グループ メンバーの管理モードを設定します。

コマンド デフォルト

集約型モードはオフです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

```
Switch enable
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wireless mobility controller peer-group peer1 member ip 10.0.0.1 mode
centralized
```

wireless mobility group keepalive

モビリティ グループ パラメータを設定し、その ping パラメータをキープアライブにするには、**wireless mobility group keepalive** コマンドを使用します。モビリティ グループ パラメータを削除するには、このコマンドの **no** 形式を使用します。

wireless mobility group keepalive {**count** *number*|**interval** 間隔}
no wireless mobility group keepalive {**count** 番号| **interval** 間隔}

構文の説明

count *number*	モビリティ グループ メンバに ping 要求を送信する回数。この回数を超えると、メンバにはアクセスできないと見なされます。有効な範囲は 3 ～ 20 です。デフォルトは 3 です。
interval 間隔	モビリティ グループ メンバへの ping 要求の送信間隔。範囲は 1 ～ 30 秒です。デフォルト値は 10 秒です。

コマンド デフォルト

カウントは 3秒、間隔は 10 秒です。

コマンド モード

グローバル コンフィギュレーション。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

interval のデフォルト値は 10 秒、*retries* のデフォルト値は 3 秒に設定されます。

次に、モビリティ グループ メンバに送信する各 ping 要求の間隔を 10 秒に指定する例を示します。

```
Switch(config)# wireless mobility group keepalive count 10
```

wireless mobility group member ip

モビリティ グループ メンバー リストでユーザの追加または削除を行うには、**wireless mobility group member ip** コマンドを使用します。モビリティ グループからメンバーを削除するには、このコマンドの **no** 形式を使用します。

wireless mobility group member ip *ip-address* [**public-ip** *public-ip-address*] [**group** *group-name*]
no wireless mobility group member ip *ip-address*

構文の説明

ip-address	メンバー コントローラの IP アドレス。
public-ip *public-ip-address*	（任意）メンバー コントローラのパブリック IP アドレス。 （注） このコマンドは、メンバーが NAT に関与する場合にのみ使用されます。サポートされているのは、スタティック IP NAT のみです。
group *group-name*	（任意）メンバー コントローラのグループ名。 （注） このコマンドは、メンバーがローカル モビリティ コントローラと同じグループに追加されない場合にのみ使用されます。

コマンド デフォルト

なし。

コマンド モード

グローバル コンフィギュレーション。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

モビリティ グループは、特定の導入に複数のモビリティ コントローラ（MC）がある場合に使用されます。モビリティ グループに任意の名前を割り当てることもできますし、デフォルト グループの名前を割り当てることもできます。モビリティ グループ メンバーは、グループ内でローミングするグループのすべてのメンバーに対して設定する必要があります。

次に、モビリティ グループにメンバーを追加する例を示します。

```
Switch(config)# mobility group member ip 10.104.171.101 group TestDocGroup
```

wireless mobility group name

モビリティ ドメイン名を設定するには、**wirelessmobilitygroupname** コマンドを使用します。モビリティ ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

（注） ネットワーク アドレス変換（NAT）が有効になっているネットワークのモビリティ グループを設定する際に、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。そうしないと、モビリティ グループ内のコントローラ間でモビリティが失敗します。

wireless mobility group name *domain-name*
no wireless mobility group name

構文の説明

domain-name	次のコマンドを入力して、新しいモビリティ グループを作成します。ドメイン名は最大 31 文字で、大文字と小文字を区別します。

コマンド デフォルト

これがデフォルトです。

コマンド モード

グローバル コンフィギュレーション。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、モビリティ ドメイン名 lab1 を設定する例を示します。

```
Switch(config)# mobility group domain lab1
```

wireless mobility load-balance

このコマンドは、少なくともロードされ、モバイル クライアントの Point of Presence として機能するよう選択されたスイッチ ピア グループ（SPG）のモビリティ アンカー（MA）でモバイル クライアントをロード バランシングするために使用されます。

モビリティ ロード バランスのステータスを設定するには、**wireless mobility load-balance** コマンドを使用します。

モビリティ ロード バランスを無効にするには、このコマンドの **no wirelessmobility load-balance** 形式を使用します。

モビリティ ロード バランスがオンになっているスイッチでクライアント ロードを設定するには、このコマンドの **no wirelessmobility load-balance** threshold 形式を使用します。

wireless mobility load-balance [**threshold** *threshold*]
[{**no**}]**wireless mobility load-balance [threshold]**

[{**no**}]**wireless mobility load-balance**

構文の説明

threshold *threshold*	ローカルで固定できるクライアント数のしきい値を設定します。

コマンド デフォルト

ロード バランスは有効で、値は 1000 に設定されます。

コマンド モード

グローバル コンフィギュレーション。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

- このコマンドは、モビリティ エージェントのみでサポートされます。
- デフォルトでは、しきい値はノードの総クライアント数の 50 パーセント以上を入力できます。設定されたしきい値に達した後にスイッチに追加されたクライアントは、同じスイッチ ピア グループ内の最小限のロード済みスイッチに自動的に固定されます。

次に、しきい値を 150 に設定したモビリティ ロード バランス ステータスを設定する例を示します。

```
Switch(config)# wireless mobility load-balance threshold 150
```

show wireless mobility

ワイヤレス モビリティの概要を表示するには、**show wireless mobility** コマンドを使用します。

show wireless mobility {**load-balance summary agent** *mobility-agent-ip***client summary** | **ap-list ip-address** *ip-address* | **controller client summary** | **dtls connections** | **statistics summary**}

構文の説明

load-balancesummary	モビリティのロードバランスのプロパティを表示します。
agent *mobility-agent-ip***clientsummary**	モビリティ エージェントのアクティブ クライアントを表示します。
ap-listip-address *ip-address*	モビリティ グループに認識されている Cisco AP のリストを表示します。
controllerclientsummary	サブドメインのアクティブ クライアントを表示します。
dtlsconnections	DTLS サーバのステータスを表示します。
statistics	Mobility Manager の統計を表示します。
summary	Mobility Manager のサマリーを表示します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、Mobility Manager のサマリーを表示する例を示します。

```
Switch (config)# show wireless mobility ap-list

AP name                              AP radio MAC      Controller IP     Learnt from
-------------------------------------------------------------------------------------------------
TSIM_AP-101                          0000.2000.6600    9.9.9.2           Self
TSIM_AP-102                          0000.2000.6700    9.9.9.2           Self
TSIM_AP-103                          0000.2000.6800    9.9.9.2           Self
TSIM_AP-400                          0000.2001.9100    9.9.9.2           Self
TSIM_AP-402                          0000.2001.9300    9.9.9.2           Self
TSIM_AP-403                          0000.2001.9400    9.9.9.2           Self
TSIM_AP-406                          0000.2001.9700    9.9.9.2           Self
TSIM_AP-407                          0000.2001.9800    9.9.9.2           Self
TSIM_AP-409                          0000.2001.9a00    9.9.9.2           Self
```

clear wireless mobility statistics

ワイヤレス統計情報をクリアするには、**clear wireless mobility statistics** コマンドを使用します。

clear wireless mobility statistics

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

clear wireless mobility statistics コマンドを使用すると、すべての情報をクリアできます。

次に、ワイヤレス モビリティ統計情報をクリアする例を示します。

```
Switch (config)# clear wireless mobility statistics
```

第 VII 部

ネットワーク管理

ネットワーク管理コマンド

ip wccp

Web キャッシュ サービスを有効にし、アプリケーション エンジンで定義されたダイナミック サービスに対応するサービス番号を指定するには、スイッチで **ip wccp** グローバル コンフィギュレーション コマンドを使用します。サービスを無効にするには、このコマンドの **no** 形式を使用します。

ip wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]
no ip wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]

構文の説明

web-cache	Web キャッシュ サービスを指定します（WCCP バージョン 1 とバージョン 2）。
service-number	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ～ 254 の範囲で指定できます。サービスの最大数（**web-cache** キーワードで指定する Web キャッシュ サービスを含む）は 256 です。
group-address *groupaddress*	（任意）サービス グループに参加するためにスイッチおよびアプリケーション エンジンが使用するマルチキャスト グループ アドレスを指定します。
group-list *access-list*	（任意）マルチキャスト グループ アドレスが使用されない場合、サービス グループに加入しているアプリケーション エンジンに対応する有効な IP アドレスのリストを指定します。
redirect-list *access-list*	（任意）ホストから特定のホストまたは特定のパケットのリダイレクト サービスを指定します。
password *encryption-number password*	（任意）暗号化番号を指定します。指定できる範囲は 0 ～ 7 です。暗号化しない場合は 0、独自の場合は 7 を使用します。また、7 文字以内でパスワード名を指定します。スイッチは、パスワードと MD5 認証値を組み合わせて、スイッチとアプリケーション エンジンとの接続にセキュリティを確保します。デフォルトでは、パスワードは設定されておらず、認証も実行されていません。

コマンド デフォルト

WCCP サービスがデバイスでイネーブルにされていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

シスコ エクスプレス フォワーディング スイッチングがイネーブルのとき、WCCP の透過的キャッシングはネットワーク アドレス変換（NAT）をバイパスします。この状況に対処するには、発信方向で WCCP 透過キャッシュを設定し、コンテンツ エンジン インターフェイスで Cisco Express Forwarding スイッチングを有効にし、**ip wccp web-cache redirect out** コマンドを指定します。キャッシュに面するルータ インターフェイスで **ip wccp redirect exclude in** コマンドを指定し、内部インターフェイスの着信方向に WCCP を設定します。この設定は、そのインターフェイスに到着したパケットのリダイレクションを回避します。

サービス グループを設定するときにリダイレクト リストを含めることもできます。指定されたリダイレクト リストは、NAT（送信元）IP アドレスを含むパケットを拒否して、リダイレクションを阻止します。

このコマンドは、指定されたサービス番号または Web キャッシュ サービス名のサポートをイネーブルまたはディセーブルにするようスイッチに指示します。サービス番号は 0 ～ 254 の範囲で指定できます。サービス番号または名前がイネーブルになると、ルータはサービス グループの確立に参加できます。

no ip wccp コマンドが入力されると、スイッチはサービス グループへの参加を終了し、引き続きサービスが設定されているインターフェイスがなければ領域の割り当てを解除し、他のサービスが設定されていなければ WCCP タスクを終了します。

web-cache に続くキーワードと *service-number* 引数はオプションで、任意の順序で指定できますが、1 回しか指定できません。

例

次に、Web キャッシュ、アプリケーション エンジンまたはサーバに接続されたインターフェイス、およびクライアントに接続するインターフェイスを設定する例を示します。

```
Switch(config)# ip wccp web-cache
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.10.30 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)#
*Dec  6 13:11:29.507: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to
down

Switch(config-if)# ip address 175.20.20.10 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# ip wccp web-cache group-listen
Switch(config-if)# exit
```

関連トピック

show platform ip wccp （573 ページ）

monitor capture (interface/control plane)

接続ポイントおよびパケット フロー方向を指定してモニタ キャプチャ ポイントを設定する、またはキャプチャ ポイントに接続ポイントを追加するには、特権 EXEC モードで **monitor capture** コマンドを使用します。指定した接続ポイントおよびパケット フロー方向でモニタ キャプチャを無効にする、またはキャプチャ ポイント上の複数の接続ポイントのいずれかを無効にするには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-nameinterface-typeinterface-id*}{**interface** | **control-plane**}{**in** | **out** | **both**}
no monitor capture {*capture-nameinterface-typeinterface-id*}{**interface** | **control-plane**}{**in** | **out** | **both**}

構文の説明

capture-name	定義するキャプチャの名前。
interface *interface-type interface-id*	*interface-type* および *interface-id* とのインターフェイスを接続ポイントとして指定します。引数の意味は次のとおりです。 • **GigabitEthernet** *interface-id*：ギガビット イーサネット IEEE 802.3z インターフェイス。 • **vlan** *vlan-id*：VLAN。*vlan-id*の範囲は 1 ～ 4095 です。 • **capwap** *capwap-id*：Control and Provisioning of Wireless Access Points（CAPWAP）プロトコル トンネリング インターフェイス。接続ポイントとして使用できるCAPWAP トンネルのリストを表示するには、**show capwap summary** コマンドを使用します。 （注） これはワイヤレス キャプチャに使用できる唯一の接続ポイントです。このインターフェイスを接続ポイントとして使用している場合、同じキャプチャ ポイントで他のインターフェイス タイプを接続ポイントとして使用することはできません。
control-plane	コントロール プレーンを接続ポイントとして指定します。
in | **out** | **both**	キャプチャするトラフィックの方向を指定します。

コマンド デフォルト

Wireshark キャプチャは設定されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

接続ポイントがこのコマンドを使用してキャプチャ ポイントに関連付けられると、方向を変更する唯一の方法は、このコマンドの **no** 形式を使用して接続ポイントを削除し、新しい方向に接続ポイントを再接続することです。接続ポイントの方向は上書きできません。

接続ポイントがキャプチャ ポイントから削除され、1 つの接続ポイントのみが関連付けられている場合、キャプチャ ポイントは効率的に削除されます。

このコマンドを別の接続ポイントで再実行することで、複数の接続ポイントをキャプチャ ポイントと関連付けることができます。次に例を示します。

複数のキャプチャ ポイントを定義できますが、一度にアクティブにできるのは1つだけです。つまり、1 つ開始するには 1 つ停止する必要があります。

インターフェイスの出力方向にキャプチャされたパケットは、スイッチの書き換えによって行われた変更（TTL、VLAN タグ CoS、チェックサム、および MAC アドレス、DSCP、プレシデント、UP など）が反映されないこともあります。

特定の順序はキャプチャ ポイントを定義する場合には適用されません。任意の順序でキャプチャ ポイント パラメータを定義できます。Wireshark CLI では、単一行のパラメータ数に制限はありません。これはキャプチャ ポイントを定義するために必要なコマンドの数を制限します。

VRF、管理ポート、プライベート VLAN はいずれも接続ポイントとして使用することはできません。

Wireshark は宛先 SPAN ポートでパケットをキャプチャできません。

VLAN が Wireshark の接続ポイントとして使用されている場合、パケットは、入力方向でのみキャプチャされます。

ワイヤレス（CAPWAP）使用上の注意事項

ワイヤレス キャプチャの唯一の形式は CAPWAP トンネル キャプチャです。

CAPWAP トンネルをキャプチャする場合、同じキャプチャ ポイント上で他のインターフェイス タイプを接続ポイントとして使用することはできません。また、同じキャプチャ ポイント上で可能な接続ポイントの唯一異なるタイプはコントロール プレーンです。コントロール プレーンおよび CAPWAP トンネル接続ポイントの組み合わせは、すべてのワイヤレス関連トラフィックをキャプチャできます。

複数の CAPWAP トンネルのキャプチャがサポートされています。各 CAPWAP トンネルの ACL は結合され、単一 ACL としてスイッチに送信されます。

コア フィルタは適用されず、CAPWAP トンネルをキャプチャする場合に省略できます。コントロール プレーンおよび CAPWAP トンネルが混在している場合、コア フィルタはコントロール プレーン パケットにも適用されません。

CAPWAP の非データ トンネルをキャプチャするには、管理 VLAN でトラフィックをキャプチャし、適切な ACL を適用してトラフィックをフィルタします。この ACL はコア フィルタ ACL と結合され、スイッチに単一の ACL として割り当てられることに注意してください。

例

物理インターフェイスを接続ポイントとして使用してキャプチャ ポイントを定義するには次を実行します。

```
Switch# monitor capture mycap interface GigabitEthernet1/0/1 in
Switch# monitor capture mycap match ipv4 any any
```

（注） 2 つ目のコマンドは、キャプチャ ポイントのコア フィルタを定義します。これは、キャプチャ ポイントで CAPWAP トンネリング接続ポイントを使用している場合を除いて、キャプチャ ポイントが機能するために必要です。

キャプチャ ポイントで CAPWAP トンネリング接続ポイントを使用している場合、コア フィルタを使用できません。

複数の接続ポイントを持つキャプチャ ポイントを定義するには次を実行します。

```
Switch# monitor capture mycap interface GigabitEthernet1/0/1 in
Switch# monitor capture mycap match ipv4 any any
Switch# monitor capture mycap control-plane in
Switch# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap control-plane in
```

複数の接続ポイントで定義されたキャプチャ ポイントから接続ポイントを削除するには次を実行します。

```
Switch# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap control-plane in
Switch# no monitor capture mycap control-plane
Switch# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
```

CAPWAP 接続ポイントでキャプチャ ポイントを定義するには次を実行します。

```
Switch# show capwap summary

CAPWAP Tunnels General Statistics:
  Number of Capwap Data Tunnels       = 1
  Number of Capwap Mobility Tunnels   = 0
  Number of Capwap Multicast Tunnels  = 0


Name   APName                           Type PhyPortIf Mode      McastIf
------ -------------------------------- ---- --------- --------- -------
Ca0    AP442b.03a9.6715                 data Gi3/0/6   unicast   -


Name   SrcIP           SrcPort DestIP          DstPort DtlsEn MTU   Xact
------ --------------- ------- --------------- ------- ------ ----- ----
Ca0    10.10.14.32     5247    10.10.14.2      38514   No     1449  0

Switch# monitor capture mycap interface capwap 0 both
Switch# monitor capture mycap file location flash:mycap.pcap
Switch# monitor capture mycap file buffer-size 1
Switch# monitor capture mycap start
```

```
*Aug 20 11:02:21.983: %BUFCAP-6-ENABLE: Capture Point mycap enabled.on

Switch# show monitor capture mycap parameter
   monitor capture mycap interface capwap  0 in
   monitor capture mycap interface capwap  0 out
   monitor capture mycap file location flash:mycap.pcap buffer-size 1
Switch#
Switch# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
    Ingress:
 0
    Egress:
 0
   Status : Active
  Filter Details:
    Capture all packets
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 1
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
Switch#
Switch# show monitor capture file flash:mycap.pcap
  1   0.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  2   0.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  3   2.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  4   2.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  5   3.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  6   4.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  7   4.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  8   5.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  9   5.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 10   6.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 11   8.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 12   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 13   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 14   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 15   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 16   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 17   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 18   9.236987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 19  10.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
```

```
 20  10.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 21  12.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 22  12.239993   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 23  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 24  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 25  12.250994   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 26  12.256990   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 27  12.262987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 28  12.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 29  12.802012   10.10.14.3 -> 10.10.14.255 NBNS Name query NB WPAD.<00>
 30  13.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
```

関連トピック

monitor capture buffer （545 ページ）
monitor capture file （548 ページ）
show monitor capture （571 ページ）

monitor capture buffer

モニタ キャプチャ（WireShark）のバッファを設定するには、特権 EXEC モードで **monitor capture buffer** コマンドを使用します。モニタ キャプチャ バッファを無効にする、またはバッファを循環バッファからデフォルトの線形バッファに戻すには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*} **buffer** {**circular** [**size** *buffer-size*] | **size** *buffer-size*}
no monitor capture {*capture-name*} **buffer** [**circular**]

構文の説明

capture-name	バッファが設定されるキャプチャの名前。
circular	バッファが循環タイプであることを指定します。循環タイプのバッファは、バッファが消費された後も以前にキャプチャされたデータを上書きすることでデータのキャプチャを継続します。
size *buffer-size*	（任意）バッファのサイズを指定します。範囲は 1 ～ 100 MB です。

コマンド デフォルト

線形バッファが設定されます。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

最初に WireShark のキャプチャを設定すると、小規模の循環バッファが提案されます。

例

1 MB のサイズの循環バッファを設定する場合は次を実行します。

```
Switch# monitor capture mycap buffer circular size 1
```

関連トピック

monitor capture (interface/control plane) （540 ページ）
monitor capture file （548 ページ）
show monitor capture （571 ページ）

monitor capture clear

モニタ キャプチャ（WireShark）バッファをクリアするには、特権 EXEC モードで **monitor capture clear** コマンドを使用します。

monitor capture {*capture-name*} **clear**

構文の説明

capture-name	バッファがクリアされるキャプチャの名前。

コマンド デフォルト

バッファのコンテンツはクリアされません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

キャプチャ中、または 1 つ以上の最終条件が満たされたか **monitor capture stop** コマンドを入力したためにキャプチャが停止された後に、**monitor capture clear** コマンドを使用します。キャプチャが停止した後に **monitor capture clear** コマンドを入力した場合、バッファにキャプチャされたパケットがないため、ファイルへのキャプチャされたパケットのコンテンツの保存に使用された **monitor capture export** コマンドには影響はありません。

パケットをバッファ内に保存する複数のキャプチャがある場合、メモリ ロスを避けるため、新しいキャプチャを開始する前にバッファをクリアしてください。

例

mycap をキャプチャするためにバッファ コンテンツをクリアするには次を実行します。

```
Switch#  monitor capture mycap clear
```

monitor capture export

ファイルにモニタ キャプチャ（WireShark）をエクスポートするには、特権 EXEC モードで **monitor capture export** コマンドを使用します。

monitor capture {*capture-name*} **export** *file-location* **:** *file-name*

構文の説明

capture-name	エクスポートするキャプチャの名前。
file-location : *file-name*	（任意）キャプチャ ストレージ ファイルの場所およびファイル名を指定します。*file-location* に使用可能な値は次のとおりです。 • flash：オンボード フラッシュ ストレージ • (usbflash0:)：USB ドライブ

コマンド デフォルト

キャプチャされたパケットは保存されません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

ストレージの宛先がキャプチャ バッファである場合にのみ **monitor capture export** コマンドを使用します。ファイルはリモートにもローカルにも保存できます。キャプチャ中またはパケット キャプチャ停止後にこのコマンドを使用します。パケット キャプチャは、1 つ以上の終了条件が満たされた場合、または **monitor capture stop** コマンドを入力すると停止します。

WireShark がスタック内のスイッチで使用される場合、パケット キャプチャは前述の *file-location* で指定されたアクティブ スイッチに接続されるデバイス上にのみ保存されます。例：flash1 はアクティブなスイッチに接続されています。flash2 はセカンダリ スイッチに接続されています。この場合、パケット キャプチャの保存に使用できるのは flash1 だけです。

（注） サポートされていないデバイスまたはアクティブなスイッチに接続されていないデバイスにパケット キャプチャを保存しようとするとエラーが発生する可能性があります。

例

キャプチャ バッファの内容を flash ドライブの mycap.pcap にエクスポートするには次を実行します。

```
Switch# monitor capture mycap export flash:mycap.pcap
```

monitor capture file

モニタ キャプチャ（WireShark）ストレージ ファイル属性を設定するには、特権 EXEC モードで **monitor capture file** コマンドを使用します。ストレージ ファイル属性を削除するには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*} **file**{ [**buffer-size** *temp-buffer-size*] [**location** *file-location* **:** *file-name*] [**ring** *number-of-ring-files*] [**size** *total-size*] }
no monitor capture {*capture-name*} **file**{ [**buffer-size**] [**location**] [**ring**] [**size**] }

構文の説明

capture-name	変更するキャプチャの名前。
buffer-size *temp-buffer-size*	（任意）一時バッファのサイズを指定します。*temp-buffer-size* の範囲は 1 ～ 100 MB です。これはパケット損失を削減するために指定されます。
location *file-location* : *file-name*	（任意）キャプチャ ストレージ ファイルの場所およびファイル名を指定します。*file-location* に使用可能な値は次のとおりです。 • flash：オンボード フラッシュ ストレージ • (usbflash0:)：USB ドライブ
ring *number-of-ring-files*	（任意）キャプチャが循環ファイル チェーンに保存されること、およびファイル リング内のファイル数を指定します。
size *total-size*	（任意）キャプチャ ファイルの合計サイズを指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

ストレージの宛先がファイルである場合にのみ **monitor capture file** コマンドを使用します。ファイルはリモートにもローカルにも保存できます。パケット キャプチャの停止後にこのコマンドを使用します。パケット キャプチャは、1 つ以上の終了条件が満たされた場合、または **monitor capture stop** コマンドを入力すると停止します。

WireShark がスタック内のスイッチで使用される場合、パケット キャプチャは前述の *file-location* で指定されたアクティブ スイッチに接続されるデバイス上にのみ保存されます。例：flash1 はアクティブなスイッチに接続されています。flash2 はセカンダリ スイッチに接続されています。この場合、パケット キャプチャの保存に使用できるのは flash1 だけです。

（注） サポートされていないデバイスまたはアクティブなスイッチに接続されていないデバイスにパケット キャプチャを保存しようとするとエラーが発生する可能性があります。

例

フラッシュ ドライブに保管されているファイル名が mycap.pcap であることを指定するには次を実行します。

```
Switch# monitor capture mycap file location flash:mycap.pcap
```

関連トピック

monitor capture (interface/control plane) （540 ページ）
monitor capture buffer （545 ページ）
show monitor capture （571 ページ）

monitor capture limit

キャプチャ制限を設定するには、特権 EXEC モードで **monitor capture limit** コマンドを使用します。キャプチャ制限を削除するには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-namesecondssizenum*} **limit** {[**duration**][**packet-length**][**packets**]}
no monitor capture {*capture-name*} **limit** [**duration**][**packet-length**][**packets**]

構文の説明

capture-name	キャプチャ制限を割り当てられるキャプチャの名前。
duration *seconds*	（任意）キャプチャ期間（秒）を指定します。範囲は 1 ～ 1000000 です。
packet-length *size*	（任意）パケット長（バイト）を指定します。実際のパケットが特定の長さより長い場合、数がバイト引数によって示される最初のセットのバイトのみが保存されます。
packets *num*	（任意）キャプチャに対して処理されるパケット数を指定します。

コマンド デフォルト

キャプチャ制限は設定されません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

60 秒のセッション制限および 400 バイトのパケット セグメント長を設定するには次を実行します。

```
Switch# monitor capture mycap limit duration 60 packet-len 400
```

monitor capture match

（注） CAPWAP トンネルをキャプチャする場合は、このコマンドを使用しないでください。また、コントロール プレーンおよびCAPWAP トンネルが混在している場合、このコマンドには効果がありません。

モニタ（Wireshark）キャプチャに対して明示的にインライン コア フィルタを定義するには、特権 EXEC モードで **monitor capture match** コマンドを使用します。このフィルタを削除するには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-namemac-match-string*} **match** {**any** | **mac** | **ipv4** {**any** | **host** | **protocol**}{**any** | **host**} | **ipv6** {**any** | **host** | **protocol**}{**any** | **host**}}
no monitor capture {*capture-name*} **match**

構文の説明

capture-name	コア フィルタを割り当てられるキャプチャの名前。
any	すべてのパケットを指定します。
mac *mac-match-string*	レイヤ 2 パケットを指定します。
ipv4	IPv4 パケットを指定します。
host	ホストを指定します。
protocol	プロトコルを指定します。
ipv6	IPv6 パケットを指定します。

コマンド デフォルト

コア フィルタは設定されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

ソースまたは宛先上の任意のIPバージョン4パケットに一致するキャプチャ ポイントに対してキャプチャ ポイントおよびコア フィルタを定義するには、次を実行します。

```
Switch# monitor capture mycap interface GigabitEthernet1/0/1 in
Switch# monitor capture mycap match ipv4 any any
```

monitor capture start

トラフィック トレース ポイントでパケット データのバッファへのキャプチャを開始するには、特権 EXEC モードで **monitor capture start** コマンドを使用します。

monitor capture {*capture-name*} **start**

構文の説明

capture-name	開始するキャプチャの名前。

コマンド デフォルト

バッファのコンテンツはクリアされません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

キャプチャ ポイントが定義された後にパケット データ キャプチャを有効にするには、**monitor capture clear** コマンドを使用します。パケット データのキャプチャを停止するには、**monitor capture stop** コマンドを使用します。

CPU およびメモリなどのシステム リソースがキャプチャの開始前に使用可能であることを確認します。

例

バッファ コンテンツのキャプチャを開始するには次を実行します。

```
Switch#  monitor capture mycap start
```

monitor capture stop

トラフィック トレース ポイントでパケット データのキャプチャを停止するには、特権 EXEC モードで **monitor capture stop** コマンドを使用します。

monitor capture {*capture-name*} **stop**

構文の説明

capture-name	停止するキャプチャの名前。

コマンド デフォルト

パケット データ キャプチャが進行中です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

monitor capture stop コマンドを使用して、**monitor capture start** コマンドによって開始したパケット データのキャプチャを停止します。線形および循環の 2 つのタイプのキャプチャ バッファを設定できます。線形バッファがいっぱいになった場合、データ キャプチャは自動的に停止します。循環バッファがいっぱいになると、データ キャプチャは最初から開始し、データは上書きされます。

例

バッファ コンテンツのキャプチャを停止するには次を実行します。

```
Switch#  monitor capture mycap stop
```

monitor session

ポート間のトラフィック分析のために、イーサネット スイッチド ポート アナライザ（SPAN）セッションまたはリモート スイッチド ポート アナライザ（RSPAN）セッションのコンフィギュレーションを新規作成するか、既存のセッションのコンフィギュレーションに追加するには、**monitor session** グローバル コンフィギュレーション コマンドを使用します。SPAN セッションまたは RSPAN セッションをクリアするには、このコマンドの **no** 形式を使用します。

monitor session *session-number* {**destination** | **filter** | **source**}
no monitor session {*session-number* [**destination** | **filter** | **source**] | **all** | **local** | **range** *session-range* | **remote**}

構文の説明

session-number	SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1 ～ 66 です。
all	すべてのモニタ セッションをクリアします。
local	すべてのローカル モニタ セッションをクリアします。
range *session-range*	指定された範囲のモニタ セッションをクリアします。
remote	すべてのリモート モニタ セッションをクリアします。

コマンド デフォルト

モニタ セッションは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

2 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチまたはスイッチ スタック上で、合計 66 の SPAN および RSPAN セッションを保有できます。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

例

次に、ローカル SPAN セッション 1 を作成して Po13（EtherChannel ポート）のトラフィックをモニタし、セッションの SPAN トラフィックを VLAN 1281 のみに限定する例を示します。出力トラフィックは送信元を複製します。入力転送はイネーブルになりません。

```
Switch(config)# monitor session 1 source interface Po13
Switch(config)# monitor session 1 filter vlan 1281
Switch(config)# monitor session 1 destination interface GigabitEthernet2/0/36 encapsulation
 replicate
Switch(config)# monitor session 1 destination interface GigabitEthernet3/0/36 encapsulation
 replicate
```

次に、これらのセットアップ手順を完了した後の **show monitor session all** コマンドの出力を示します。

```
Switch# show monitor session all

Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Po13
Destination Ports      : Gi2/0/36,Gi3/0/36
    Encapsulation      : Replicate
          Ingress      : Disabled
Filter VLANs           : 1281
...
```

関連トピック

monitor session destination （556 ページ）
monitor session filter （561 ページ）
monitor session source （563 ページ）
show monitor （568 ページ）

monitor session destination

新規にスイッチド ポート アナライザ（SPAN）セッションまたはリモート SPAN（RSPAN）宛先セッションを開始し、ネットワーク セキュリティ デバイス（Cisco IDS Sensor アプライアンスなど）の宛先ポート上の入力トラフィックをイネーブルにし、既存の SPAN または RSPAN セッションでインターフェイスを追加または削除するには、**monitor session destination** グローバル コンフィギュレーション コマンドを使用します。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから宛先インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

monitor session *session-number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**replicate** | **dot1q**}] {**ingress** [**dot1q** | **untagged**] } | {**remote**} **vlan** *vlan-id*
no monitor session *session-number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**replicate** | **dot1q**}] {**ingress** [**dot1q** | **untagged**] } | {**remote**} **vlan** *vlan-id*

構文の説明

session-number	SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1 ～ 66 です。
interface *interface-id*	SPAN または RSPAN セッションの宛先または送信元インターフェイスを指定します。有効なインターフェイスは物理ポート（タイプ、スタック メンバ、モジュール、ポート番号を含む）です。送信元インターフェイスの場合は、ポート チャネルも有効なインターフェイス タイプであり、指定できる範囲は 1 ～ 128 です。
,	（任意）複数のインターフェイスまたはVLANを指定します。または、前の範囲からインターフェイスまたは VLAN の範囲を分離します。カンマの前後にスペースを入れます。
-	（任意）インターフェイスまたは VLAN の範囲を指定します。ハイフンの前後にスペースを入れます。

encapsulation replicate	（任意）宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 次のキーワードは、ローカル SPAN にだけ有効です。RSPAN、RSPAN VLAN ID は元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。**encapsulation** オプションは、**no** 形式では無視されます。
encapsulation dot1q	（任意）宛先インターフェイスが IEEE 802.1Q カプセル化の送信元インターフェイスの着信パケットを受け入れるように指定します。 次のキーワードは、ローカル SPAN にだけ有効です。RSPAN、RSPAN VLAN ID は元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。**encapsulation** オプションは、**no** 形式では無視されます。
ingress	入力トラフィック転送をイネーブルにします。
dot1q	（任意）指定された VLAN をデフォルト VLAN として、IEEE 802.1Q カプセル化された着信パケットを受け入れます。
untagged	（任意）指定された VLAN をデフォルト VLAN として、タグなしカプセル化された着信パケットを受け入れます。
isl	ISL カプセル化を使用して入力トラフィックを転送するように指定します。
remote	RSPAN 送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。 RSPAN VLAN は VLAN 1（デフォルトの VLAN）、または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN に予約済）になることはできません。
vlan *vlan-id*	**ingress** キーワードとのみ使用された場合、入力トラフィックに対するデフォルトの VLAN を設定します。

コマンド デフォルト

モニタ セッションは設定されていません。

ローカル SPAN の宛先ポートで **encapsulation replicate** が指定されなかった場合、パケットはカプセル化のタグなしのネイティブ形式で送信されます。

入力転送は宛先ポートではディセーブルになっています。

all、**local**、**range**、*session-range*、**remote** を **no monitor session** コマンドに指定することで、すべての SPAN および RSPAN、すべてのローカル SPAN、範囲、すべての RSPAN セッションをクリアできます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

8 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチまたはスイッチ スタック上で、合計 66 の SPAN および RSPAN セッションを保有できます。

SPAN または RSPAN の宛先は物理ポートである必要があります。

スイッチ上またはスイッチ スタック上で、最大 64 の宛先ポートを保有できます。

各セッションには複数の入力または出力の送信元ポートまたは VLAN を含めることができますが、1 つのセッション内で送信元ポートと送信元 VLAN を組み合わせることはできません。各セッションは複数の宛先ポートを保有できます。

VLAN-based SPAN（VSPAN）を使用して、VLAN または一連の VLAN 内のネットワーク トラフィックを解析する場合、送信元 VLAN のすべてのアクティブ ポートが SPAN または RSPAN セッションの送信元ポートになります。トランク ポートは VSPAN の送信元ポートとして含まれ、モニタリングされた VLAN ID のパケットだけが宛先ポートに送信されます。

1 つのポート、1 つの VLAN、一連のポート、一連の VLAN、ポート範囲、VLAN 範囲でトラフィックをモニタできます。**[,|-]** オプションを使用して、複数または一定範囲のインターフェイスまたは VLAN を指定します。

一連の VLAN またはインターフェイスを指定するときは、カンマ（,）の前後にスペースが必要です。VLAN またはインターフェイスの範囲を指定するときは、ハイフン（-）の前後にスペースが必要です。

EtherChannel ポートは、SPAN または RSPAN 宛先ポートとして設定することは。EtherChannel グループのメンバである物理ポートは、宛先ポートとして使用できます。ただし、SPAN の宛先として機能する間は、EtherChannel グループに参加できません。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 宛先ポートであるポート上で IEEE 802.1x 認証をイネーブルにすることはできますが、ポートが SPAN 宛先として削除されるまで IEEE 802.1x 認証はディセーブルです。

IEEE 802.1x 認証がポート上で使用できない場合、スイッチはエラー メッセージを返します。SPAN または RSPAN 送信元ポートでは IEEE 802.1x 認証をイネーブルにすることができます。

入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。

宛先ポートは次のような動作を設定できます。

- **monitor session** *session_number***destination interface** *interface-id* を他のキーワードなしで入力すると、出力のカプセル化はタグなしとなり、入力転送はイネーブルになりません。
- **monitor session** *session_number***destinationinterface** *interface-id***ingress** を入力すると、出力のカプセル化はタグなしとなります。入力のカプセル化は **dot1q** または **untagged** に続くキーワードによって異なります。
- **monitor session** *session_number***destinationinterface** *interface-id***encapsulationreplicate** を他のキーワードなしで入力すると、出力のカプセル化はソースインターフェイスのカプセル化を複製し、入力転送はイネーブルになりません。（これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。
- **monitor session** *session_number***destinationinterface** *interface-id***encapsulationreplicate ingress** を入力すると、出力のカプセル化はソースインターフェイスのカプセル化を複製し、入力のカプセル化は **dot1q** または **untagged** に続くキーワードによって異なります。（これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバ 1 の送信元ポート 1 からスタック メンバ 2 の宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

次の例では、宛先ポートを既存のローカル SPAN セッションから削除する方法を示します。

```
Switch(config)# no monitor session 2 destination interface gigabitethernet1/0/2
```

次の例では、ある送信元インターフェイスをモニタリングする RSPAN 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 destination remote vlan 900
```

```
Switch(config)# end
```

次の例では、モニタリングされたトラフィックを受信するスイッチに、RSPAN 宛先セッション 10 を設定する方法を示します。

```
Switch(config)# monitor session 10 source remote vlan 900
Switch(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

次の例では、IEEE 802.1Q カプセル化をサポートするセキュリティ装置を使用して、VLAN 5 の入力トラフィックに対応する宛先ポートを設定する方法を示します。出力トラフィックは送信元のカプセル化を複製します。入力トラフィックは IEEE 802.1Q カプセル化を使用します。

```
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
 dot1q ingress dot1q vlan 5
```

次の例では、カプセル化をサポートしないセキュリティ デバイスを使用して、VLAN 5 上の入力トラフィックの宛先ポートを設定する方法を示します。出力トラフィックおよび入力トラフィックはタグなしです。

```
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress
untagged vlan 5
```

関連トピック

monitor session （554 ページ）
monitor session filter （561 ページ）
monitor session source （563 ページ）
show monitor （568 ページ）

monitor session filter

フローベース SPAN（FSPAN）セッションやフローベース RSPAN（FRSPAN）送信元または宛先セッションを新しく開始する、または特定の VLAN に対して SPAN 送信元トラフィックを制限（フィルタ処理）するには、**monitor session filter** グローバル コンフィギュレーション コマンドを使用します。SPAN または RSPAN セッションからフィルタを削除するには、このコマンドの **no** 形式を使用します。

monitor session *session-number* **filter** {**vlan** *vlan-id* [**,** | **-**] }
no monitor session *session-number* **filter** {**vlan** *vlan-id* [**,** | **-**] }

構文の説明

session-number	SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1 ～ 66 です。
vlan *vlan-id*	SPAN 送信元トラフィックを特定の VLAN に制限するため、トランクの送信元ポート上のフィルタとして VLAN のリストを指定します。*vlan-id* で指定できる範囲は 1 ～ 4094 です。
,	任意）複数の VLAN を指定します。または VLAN 範囲を前の範囲から区切ります。カンマの前後にスペースを入れます。
-	（任意）VLAN の範囲を指定します。ハイフンの前後にスペースを入れます。

コマンド デフォルト

モニタ セッションは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

2 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチまたはスイッチ スタック上で、合計 66 の SPAN および RSPAN セッションを保有できます。

1 つの VLAN、または複数のポートや VLAN、特定範囲のポートや VLAN でトラフィックをモニタできます。複数または一定範囲の VLAN を指定するには、[,|-] オプションを使用します。

複数の VLAN を指定するときは、カンマ（,）の前後にスペースが必要です。VLAN の範囲を指定するときは、ハイフン（-）の前後にスペースが必要です。

VLAN のフィルタリングは、トランクの送信元ポート上で選択された一連の VLAN のネットワーク トラフィック解析を参照します。デフォルトでは、すべての VLAN がトランクの送信元ポートでモニタリングされます。**monitor session** *session_number* **filter vlan** *vlan-id* コマンドを使用すると、トランク送信元ポートの SPAN トラフィックを指定された VLAN だけに限定できます。

VLAN のモニタリングおよび VLAN のフィルタリングは相互に排他的な関係です。VLAN が送信元の場合、VLANのフィルタリングはイネーブルにできません。VLANのフィルタリングが設定されている場合、VLAN は送信元になることができません。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

例

次の例では、既存のセッションの SPAN トラフィックを指定の VLAN だけに制限する方法を示します。

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

次に、ローカル SPAN セッション 1 を作成してスタック メンバ 1 の送信元ポート 1 とスタック メンバ 2 の宛先ポートの送受信両方のトラフィックをモニタし、FSPAN セッションでアクセス リスト番号 122 を使用して IPv4 トラフィックをフィルタする例を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 1 filter ip access-group 122
```

関連トピック

monitor session （554 ページ）
monitor session destination （556 ページ）
monitor session source （563 ページ）
show monitor （568 ページ）

monitor session source

スイッチド ポート アナライザ（SPAN）セッションまたはリモート SPAN（RSPAN）送信元セッションを開始する、または既存の SPAN または RSPAN セッションでインターフェイスを追加または削除するには、**monitor session source** グローバル コンフィギュレーション コマンドを使用します。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから送信元インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

monitor session *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [**,** | **-**] [**both** | **rx** | **tx**]}
no monitor session *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [**,** | **-**] [**both** | **rx** | **tx**]}

構文の説明

session_number	SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1 ～ 66 です。
interface *interface-id*	SPAN または RSPAN セッションの送信元インターフェイスを指定します。有効なインターフェイスは物理ポート（タイプ、スタック メンバ、モジュール、ポート番号を含む）です。送信元インターフェイスの場合は、ポートチャネルも有効なインターフェイスタイプであり、指定できる範囲は 1 ～ 48 です。
,	（任意）複数のインターフェイスまたはVLANを指定します。または、前の範囲からインターフェイスまたは VLAN の範囲を分離します。カンマの前後にスペースを入れます。
-	（任意）インターフェイスまたは VLAN の範囲を指定します。ハイフンの前後にスペースを入れます。
both | **rx** | **tx**	（任意）モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは送受信のトラフィックを送信します。

remote	（任意）RSPAN送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。 RSPAN VLAN は VLAN 1（デフォルトの VLAN）、または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN に予約済）になることはできません。
vlan *vlan-id*	**ingress** キーワードだけで使用された場合、入力トラフィックにデフォルトの VLAN を設定します。

コマンド デフォルト

モニタ セッションは設定されていません。

送信元インターフェイスのデフォルトでは、受信トラフィックと送信トラフィックの両方をモニタリングします。

送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタリングされます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

送信元ポートまたは送信元 VLAN を出入りするトラフィックは、SPAN または RSPAN を使用してモニタできます。送信元ポートまたは送信元 VLAN にルーティングされるトラフィックはモニタできません。

2 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチまたはスイッチ スタック上で、合計 66 の SPAN および RSPAN セッションを保有できます。

物理ポート、ポート チャネル、VLAN が送信元になることができます。

各セッションには複数の入力または出力の送信元ポートまたは VLAN を含めることができますが、1 つのセッション内で送信元ポートと送信元 VLAN を組み合わせることはできません。各セッションは複数の宛先ポートを保有できます。

VLAN-based SPAN（VSPAN）を使用して、VLAN または一連の VLAN 内のネットワーク トラフィックを解析する場合、送信元 VLAN のすべてのアクティブ ポートが SPAN または RSPAN セッションの送信元ポートになります。トランク ポートは VSPAN の送信元ポートとして含まれ、モニタリングされた VLAN ID のパケットだけが宛先ポートに送信されます。

1 つのポート、1 つの VLAN、一連のポート、一連の VLAN、ポート範囲、VLAN 範囲でトラフィックをモニタできます。[,|-] オプションを使用して、複数または一定範囲のインターフェイスまたは VLAN を指定します。

一連の VLAN またはインターフェイスを指定するときは、カンマ（,）の前後にスペースが必要です。VLAN またはインターフェイスの範囲を指定するときは、ハイフン（-）の前後にスペースが必要です。

個々のポートはそれらが EtherChannel に参加している間もモニタリングすることができます。また、RSPAN 送信元インターフェイスとして **port-channel** 番号を指定することで EtherChannel バンドル全体をモニタリングすることができます。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 送信元ポートでは IEEE 802.1x 認証をイネーブルにすることができます。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバ 1 の送信元ポート 1 からスタック メンバ 2 の宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

次の例では、複数の送信元インターフェイスをモニタリングする RSPAN 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

関連トピック

monitor session （554 ページ）
monitor session destination （556 ページ）
monitor session filter （561 ページ）
show monitor （568 ページ）

show ip sla statistics

Cisco IOS IP サービス レベル契約（SLA）のすべての動作または指定された動作の現在または集約された動作ステータスおよび統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip sla statistics** コマンドを使用します。

show ip sla statistics ［ *operation-number* ［**details**］ | **aggregated** ［ *operation-number* | **details**］ | **details**］

構文の説明

operation-number	（任意）動作ステータスおよび統計情報を表示する動作の番号。受け入れられる値の範囲は 1 ～ 2147483647 です。
details	（任意）詳細出力を指定します。
aggregated	（任意）IP SLA 集約統計を指定します。

コマンド デフォルト

稼働しているすべての IP SLA 動作の出力を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

動作の残りの継続時間、動作がアクティブかどうか、完了時刻など、IP SLA 動作の現在の状態を表示するには、**show ip sla statistics** を使用します。出力には、最後の（最近完了した）動作に対して返されたモニタリング データも含まれます。この生成された操作 ID は、基本マルチキャスト操作に対して、また操作全体の要約統計の一部として **show ip sla** コンフィギュレーション コマンドを使用すると表示されます。

あるレスポンダに関する詳細を表示するには、その特定の操作 ID に **show** コマンドを入力します。

例

次に、**show ip sla statistics** コマンドの出力例を示します。

```
Switch# show ip sla statistics

Current Operational State
Entry Number: 3
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
```

```
Operational State of Entry: active
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200  OK
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707
```

show monitor

すべての Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）およびリモート SPAN（RSPAN）セッションに関する情報を表示するには、EXEC モードで **show monitor** コマンドを使用します。

show monitor ［**session** {*session_number* | **all** | **local** | **range** *list* | **remote**} ［**detail**］］

構文の説明

session	（任意）指定された SPAN セッションの情報を表示します。
session_number	SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1 ～ 66 です。
all	（任意）すべての SPAN セッションを表示します。
local	（任意）ローカル SPAN セッションだけを表示します。
range リスト	（任意）一定範囲の SPAN セッションを表示します。*list* は有効なセッションの範囲です。range は単一のセッション、または 2 つの数字を小さい数字からハイフンで区切ったセッションの範囲です。カンマ区切りのパラメータ間、またはハイフン指定の範囲にスペースは入力しません。 （注） このキーワードは、特権 EXEC モードの場合だけ使用可能です。
remote	（任意）リモート SPAN セッションだけを表示します。
detail	（任意）指定されたセッションの詳細情報を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

show monitor コマンドと**show monitor session all** コマンドの出力は同じです。

SPAN 送信元セッションの最大数：2（送信元およびローカル セッションに適用）

例

次に、**show monitor** ユーザ EXEC コマンドの出力例を示します。

```
Switch# show monitor
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
Session 2
---------
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

次の例では、ローカル SPAN 送信元セッション 1 に対する **show monitor** ユーザ EXEC コマンドの出力を示します。

```
Switch# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

次の例では、入力トラフィック転送をイネーブルにした場合の **show monitor session all** ユーザ EXEC コマンドの出力を示します。

```
Switch# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
---------
Type : Local Session
Source Ports :
```

```
Both : Gi4/0/8
Destination Ports : Gi4/012
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

関連トピック

monitor session （554 ページ）
monitor session destination （556 ページ）
monitor session filter （561 ページ）
monitor session source （563 ページ）

show monitor capture

モニタ キャプチャ（WireShark）の内容を表示するには、特権 EXEC モードで **show monitor capture file** コマンドを使用します。

show monitor capture ［*capture-name* ［ **buffer** ］ | **file** *file-location* **:** *file-name* ］［ **brief** | **detailed** | **display-filter** *display-filter-string* ］

構文の説明

capture-name	（任意）表示するキャプチャの名前を指定します。
buffer	（任意）指定されたキャプチャに関連するバッファが表示されることを指定します。
file *file-location* : *file-name*	（任意）表示するキャプチャ ストレージファイルのファイル位置と名前を指定します。
brief	（任意）表示内容の概要を指定します。
detailed	（任意）詳細な表示内容を指定します。
display-filter *display-filter-string*	*display-filter-string* に従って表示内容をフィルタ処理します。

コマンド デフォルト

すべてのキャプチャの内容を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

none

例

mycap という名前のキャプチャのキャプチャを表示するには次を実行します。

```
Switch# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
    Ingress:
 0
    Egress:
 0
   Status : Active
  Filter Details:
    Capture all packets
```

```
Buffer Details:
 Buffer Type: LINEAR (default)
File Details:
 Associated file name: flash:mycap.pcap
 Size of buffer(in MB): 1
Limit Details:
 Number of Packets to capture: 0 (no limit)
 Packet Capture duration: 0 (no limit)
 Packet Size to capture: 0 (no limit)
 Packets per second: 0 (no limit)
 Packet sampling rate: 0 (no sampling)
```

関連トピック

monitor capture (interface/control plane) （540 ページ）
monitor capture buffer （545 ページ）
monitor capture file （548 ページ）

show platform ip wccp

プラットフォーム依存 Web Cache Communication Protocol（WCCP）情報を表示するには、**show platform ip wccp** 特権 EXEC コマンドを使用します。

show platform ip wccp {**cache-engines** |**interfaces** |**service-groups**} [**switch** *switch-number*]

構文の説明

cache-engines	WCCP キャッシュ エンジンを表示します。
interfaces	WCCP インターフェイスを表示します。
service-groups	WCCP サービス グループを表示します。
switch *switch-number*	（任意）指定された *switch-number* の WCCP 情報のみを表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

このコマンドは、スイッチが IP サービス フィーチャ セットを実行している場合だけ使用可能です。

次に、WCCP インターフェイスを表示する例を示します。

```
Switch# show platform ip wccp interfaces

WCCP Interfaces


**** WCCP Interface Gi1/0/3 iif_id:0x104a60000000087 (#SG:1), vrf:0 Ingress
le_handle:0x565dd208 IPv4 Sw-Label:3, Asic-Label:3

* Service group id:0 type: Well-known    token:126 vrf:0 (ref count:1)
Open service    prot: PROT_TCP  l4_type: Dest ports     priority: 240
port[0]: 80
```

関連トピック

ip wccp （537 ページ）

snmp-server enable traps

スイッチでネットワーク管理システム（NMS）にインフォーム要求やさまざまなトラップの Simple Network Management Protocol（SNMP）通知を送信可能にするには、グローバル コンフィギュレーション モードで **snmp-server enable traps** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps ［**auth-framework** ［**sec-violation**］ | **bridge** | **call-home** | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp** ］
no snmp-server enable traps ［**auth-framework** ［**sec-violation**］ | **bridge** | **call-home** | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp** ］

構文の説明

auth-framework	（任意）SNMP CISCO-AUTH-FRAMEWORK-MIB トラップをイネーブルにします。
sec-violation	（任意）SNMP camSecurityViolationNotif 通知をイネーブルにします。
bridge	（任意）SNMP STP ブリッジ MIB トラップをイネーブルにします。*
call-home	（任意）SNMP CISCO-CALLHOME-MIB トラップをイネーブルにします。*
cluster	（任意）SNMP クラスタ トラップをイネーブルにします。
config	（任意）SNMP 設定トラップをイネーブルにします。
config-copy	（任意）SNMP 設定コピー トラップをイネーブルにします。
config-ctid	（任意）SNMP設定CTIDトラップをイネーブルにします。
copy-config	（任意）SNMPコピー設定トラップをイネーブルにします。
cpu	（任意）CPU 通知トラップをイネーブルにします。*
dot1x	（任意）SNMP dot1x トラップをイネーブルにします。*

energywise	（任意）SNMP energywise トラップをイネーブルにします。*
entity	（任意）SNMP エンティティ トラップをイネーブルにします。
envmon	（任意）SNMP 環境モニタ トラップをイネーブルにします。*
errdisable	（任意）SNMP エラーディセーブル トラップをイネーブルにします。*
event-manager	（任意）SNMP 組み込みイベント マネージャ トラップをイネーブルにします。
flash	（任意）SNMP フラッシュ通知トラップをイネーブルにします。*
fru-ctrl	（任意）エンティティ現場交換可能ユニット（FRU）制御トラップを生成します。スイッチスタックでは、このトラップはスタックにおけるスイッチの挿入/取り外しを意味します。
license	（任意）ライセンス トラップをイネーブルにします。*
mac-notification	（任意）SNMP MAC 通知トラップをイネーブルにします。*
port-security	（任意）SNMP ポート セキュリティ トラップをイネーブルにします。*
power-ethernet	（任意）SNMP パワーイーサネット トラップをイネーブルにします。*
rep	（任意）SNMP レジリエント イーサネット プロトコル トラップをイネーブルにします。
snmp	（任意）SNMP トラップをイネーブルにします。*
stackwise	（任意）SNMP StackWise トラップをイネーブルにします。*
storm-control	（任意）SNMP ストーム制御トラップ パラメータをイネーブルにします。
stpx	（任意）SNMP STPX MIB トラップをイネーブルにします。*
syslog	（任意）SNMP syslog トラップをイネーブルにします。

transceiver	（任意）SNMP トランシーバ トラップをイネーブルにします。*
tty	（任意）TCP接続トラップを送信します。この設定はデフォルトでイネーブルになっています。
vlan-membership	（任意）SNMP VLAN メンバーシップ トラップをイネーブルにします。
vlancreate	（任意）SNMP VLAN作成トラップをイネーブルにします。
vlandelete	（任意）SNMP VLAN削除トラップをイネーブルにします。
vstack	（任意）SNMP スマートインストール トラップをイネーブルにします。*
vtp	（任意）VLAN トランキング プロトコル（VTP）トラップをイネーブルにします。

コマンド デフォルト

SNMP トラップの送信をディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

上記の表のアスタリスクが付いているコマンド オプションにはサブ コマンドがあります。これらのサブ コマンドの詳細については、関連コマンドの項を参照してください。

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

snmp-server enable traps コマンドは、トラップまたは情報がサポートされている場合に、これらの送信をイネーブルにします。

（注） コマンドラインのヘルプ ストリングに表示される場合でも、**fru-ctrl, insertion** および **removal** キーワードはスイッチでサポートされません。**snmp-server enable informs** グローバル コンフィギュレーション コマンドは、サポートされていません。SNMP情報の送信を有効にするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと **snmp-server host** *host-addr***informs** グローバル コンフィギュレーション コマンドを組み合わせて使用します。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、複数の SNMP トラップ タイプをイネーブルにする例を示します。

```
Switch(config)# snmp-server enable traps cluster
Switch(config)# snmp-server enable traps config
Switch(config)# snmp-server enable traps vtp
```

関連トピック

snmp-server enable traps bridge （578 ページ）
snmp-server enable traps call-home （580 ページ）
snmp-server enable traps cpu （582 ページ）
snmp-server enable traps envmon （583 ページ）
snmp-server enable traps errdisable （584 ページ）
snmp-server enable traps flash （585 ページ）
snmp-server enable traps license （587 ページ）
snmp-server enable traps mac-notification （588 ページ）
snmp-server enable traps port-security （592 ページ）
snmp-server enable traps power-ethernet （593 ページ）
snmp-server enable traps snmp （594 ページ）
snmp-server enable traps stackwise （595 ページ）
snmp-server enable traps storm-control （598 ページ）
snmp-server enable traps stpx （599 ページ）
snmp-server enable traps transceiver （600 ページ）
snmp-server enable traps vstack （602 ページ）
snmp-server host （604 ページ）
snmp-server enable traps bulkstat （579 ページ）
snmp-server enable traps cef （581 ページ）
snmp-server enable traps isis （586 ページ）
snmp-server enable traps ospf （589 ページ）
snmp-server enable traps pim （591 ページ）
snmp-server enable traps vrfmib （601 ページ）

snmp-server enable traps bridge

STP ブリッジ MIB トラップを生成するには、グローバル コンフィギュレーション モードで **snmp-server enable traps bridge** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps bridge ［**newroot**］［**topologychange**］
no snmp-server enable traps bridge ［**newroot**］［**topologychange**］

構文の説明

newroot	（任意）SNMP STP ブリッジ MIB 新規ルート トラップをイネーブルにします。
topologychange	（任意）SNMP STP ブリッジ MIB トポロジ変更トラップをイネーブルにします。

コマンド デフォルト

ブリッジ SNMP トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次の例では、NMS にブリッジ新規ルート トラップを送信する方法を示します。

```
Switch(config)# snmp-server enable traps bridge newroot
```

snmp-server enable traps bulkstat

データ収集 MIB トラップを有効にするには、グローバル コンフィギュレーション モードで **snmp-server enable traps bulkstat** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps bulkstat ［**collection** | **transfer**］
no snmp-server enable traps bulkstat ［**collection** | **transfer**］

構文の説明

collection	（任意）データ収集MIB収集トラップをイネーブルにします。
transfer	（任意）データ収集MIB送信トラップをイネーブルにします。

コマンド デフォルト

データ収集 MIB トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、データ収集 MIB 収集トラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps bulkstat collection
```

snmp-server enable traps call-home

SNMP CISCO-CALLHOME-MIB トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps call-home** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps call-home ［**message-send-fail** | **server-fail**］
no snmp-server enable traps call-home ［**message-send-fail** | **server-fail**］

構文の説明

message-send-fail	（任意）SNMP メッセージ送信失敗トラップをイネーブルにします。
server-fail	（任意）SNMP サーバ障害トラップをイネーブルにします。

コマンド デフォルト

SNMP CISCO-CALLHOME-MIB トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP メッセージ送信失敗トラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps call-home message-send-fail
```

snmp-server enable traps cef

SNMP Cisco Express Forwarding（CEF）トラップを有効にするには、グローバル コンフィギュレーション モードで **snmp-server enable traps cef** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]
no snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]

構文の説明

inconsistency	（任意）SNMP CEF 矛盾トラップをイネーブルにします。
peer-fib-state-change	（任意）SNMP CEF ピア FIB ステート変更トラップをイネーブルにします。
peer-state-change	（任意）SNMP CEF ピア ステート変更トラップをイネーブルにします。
resource-failure	（任意）SNMP リソース障害トラップをイネーブルにします。

コマンド デフォルト

SNMP CEF トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP CEF 矛盾トラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps cef inconsistency
```

snmp-server enable traps cpu

CPU通知をイネーブルにするには、グローバル コンフィギュレーション モードで**snmp-server enable traps cpu** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps cpu ［**threshold**］
no snmp-server enable traps cpu ［**threshold**］

構文の説明

threshold	（任意）CPU しきい値通知をイネーブルにします。

コマンド デフォルト

CPU 通知の送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、CPU しきい値通知を生成する例を示します。

```
Switch(config)# snmp-server enable traps cpu threshold
```

snmp-server enable traps envmon

SNMP 環境トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps envmon** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps envmon ［**fan**］［**shutdown**］［**status**］ ［**supply**］［**temperature**］
no snmp-server enable traps envmon ［**fan**］［**shutdown**］［**status**］ ［**supply**］［**temperature**］

構文の説明

fan	（任意）ファン トラップをイネーブルにします。
shutdown	（任意）環境シャットダウン モニタ トラップをイネーブルにします。
status	（任意）SNMP 環境ステータス変更トラップをイネーブルにします。
supply	（任意）環境電源モニタ トラップをイネーブルにします。
temperature	（任意）環境温度モニタ トラップをイネーブルにします。

コマンド デフォルト

環境 SNMP トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、ファン トラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps envmon fan
```

snmp-server enable traps errdisable

エラーディセーブルのSNMP通知をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps errdisable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps errdisable ［**notification-rate** *number-of-notifications*］
no snmp-server enable traps errdisable ［**notification-rate** *number-of-notifications*］

構文の説明

notification-rate *number-of-notifications*	（任意）通知レートとして 1 分当たりの通知の数を指定します。受け入れられる値の範囲は 0 ～ 10000 です。

コマンド デフォルト

エラー ディセーブルの SNMP 通知送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、エラー ディセーブルの SNMP 通知数を 2 に設定する例を示します。

```
Switch(config)# snmp-server enable traps errdisable notification-rate 2
```

snmp-server enable traps flash

SNMP フラッシュ通知をイネーブルにするには、グローバル コンフィギュレーション モードで**snmp-server enable traps flash** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps flash ［**insertion**］［**removal**］
no snmp-server enable traps flash ［**insertion**］［**removal**］

構文の説明

insertion	（任意）SNMP フラッシュ挿入通知をイネーブルにします。
removal	（任意）SNMP フラッシュ取り出し通知をイネーブルにします。

コマンド デフォルト

SNMP フラッシュ通知の送信はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP フラッシュ挿入通知を生成する例を示します。

```
Switch(config)# snmp-server enable traps flash insertion
```

snmp-server enable traps isis

Intermediate System-to-Intermediate System（IS-IS）リンクステート ルーティング プロトコル トラップを有効にするには、グローバル コンフィギュレーション モードで **snmp-server enable traps isis** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps isis ［**errors** | **state-change**］
no snmp-server enable traps isis ［**errors** | **state-change**］

構文の説明

errors	（任意）IS-IS エラー トラップをイネーブルにします。
state-change	（任意）IS-IS ステート変更トラップをイネーブルにします。

コマンド デフォルト

IS-IS のトラップ送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、IS-IS エラー トラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps isis errors
```

snmp-server enable traps license

ライセンス トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps license** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps license [**deploy**] [**error**] [**usage**]
no snmp-server enable traps license [**deploy**] [**error**] [**usage**]

構文の説明

deploy	（任意）ライセンス導入トラップをイネーブルにします。
error	（任意）ライセンスエラー トラップをイネーブルにします。
usage	（任意）ライセンス使用トラップをイネーブルにします。

コマンド デフォルト

ライセンス トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、ライセンス導入トラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps license deploy
```

snmp-server enable traps mac-notification

SNMP MAC 通知トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps mac-notification** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps mac-notification ［**change**］［**move**］［**threshold**］
no snmp-server enable traps mac-notification ［**change**］［**move**］［**threshold**］

構文の説明

change	（任意）SNMP MAC 変更トラップをイネーブルにします。
move	（任意）SNMP MAC 移動トラップをイネーブルにします。
threshold	（任意）SNMP MAC しきい値トラップをイネーブルにします。

コマンド デフォルト

SNMP MAC 通知トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP MAC 通知変更トラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps mac-notification change
```

snmp-server enable traps ospf

SNMP の Open Shortest Path First（OSPF）トラップを有効にするには、グローバル コンフィギュレーション モードで **snmp-server enable traps ospf** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time max-number-of-traps* | **retransmit** | **state-change**]
no snmp-server enable traps ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time max-number-of-traps* | **retransmit** | **state-change**]

構文の説明

cisco-specific	（任意）シスコ固有のトラップをイネーブルにします。
errors	（任意）エラー トラップをイネーブルにします。
lsa	（任意）リンクステート アドバタイズメント（LSA）トラップをイネーブルにします。
rate-limit	（任意）レート制限トラップをイネーブルにします。
rate-limit-time	（任意）レート制限トラップの時間の長さを秒数で指定します。指定できる値は 2 ～ 60 です。
max-number-of-traps	（任意）設定した時間内に送信するレート制限トラップの最大数を指定します。
retransmit	（任意）パケット再送信トラップをイネーブルにします。
state-change	（任意）状態変更トラップをイネーブルにします。

コマンド デフォルト

OSPF SNMP トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、LSA トラップをイネーブルにする例を示します。

```
Switch(config)# snmp-server enable traps ospf lsa
```

snmp-server enable traps pim

SNMP Protocol-Independent Multicast（PIM）トラップを有効にするには、グローバル コンフィギュレーション モードで **snmp-server enable traps pim** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps pim [**invalid-pim-message**] [**neighbor-change**] [**rp-mapping-change**]
no snmp-server enable traps pim
[**invalid-pim-message**] [**neighbor-change**] [**rp-mapping-change**]

構文の説明

invalid-pim-message	（任意）無効な PIM メッセージ トラップをイネーブルにします。
neighbor-change	（任意）PIM ネイバー変更トラップをイネーブルにします。
rp-mapping-change	（任意）ランデブー ポイント（RP）マッピング変更トラップをイネーブルにします。

コマンド デフォルト

PIM SNMP トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、無効な PIM メッセージ トラップをイネーブルにする例を示します。

```
Switch(config)# snmp-server enable traps pim invalid-pim-message
```

snmp-server enable traps port-security

SNMP ポート セキュリティ トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps port-security** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps port-security ［**trap-rate** *value*］
no snmp-server enable traps port-security ［**trap-rate** *value*］

構文の説明

trap-rate *value*	（任意）1 秒間に送信するポート セキュリティ トラップの最大数を設定します。指定できる範囲は 0 ～ 1000 です。デフォルトは 0 です（制限はなく、トラップは発生するたびに送信されます）。

コマンド デフォルト

ポート セキュリティ SNMP トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、1 秒当たり 200 の速度でポート セキュリティ トラップをイネーブルにする例を示します。

```
Switch(config)# snmp-server enable traps port-security trap-rate 200
```

snmp-server enable traps power-ethernet

SNMP の Power over Ethernet（PoE）トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps power-ethernet** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps power-ethernet {**group** *number* |**police**}
no snmp-server enable traps power-ethernet {**group** *number* |**police**}

構文の説明

group *number*	指定したグループ番号に対するインライン パワー グループベース トラップをイネーブルにします。受け入れられる値の範囲は 1 ～ 9 です。
police	インライン パワー ポリシング トラップをイネーブルにします。

コマンド デフォルト

Power over Ethernet の SNMP トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、グループ 1 の Power over Ethernet（PoE）トラップをイネーブルにする例を示します。

```
Switch(config)# snmp-server enable traps poower-over-ethernet group 1
```

snmp-server enable traps snmp

SNMP トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps snmp** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps snmp ［**authentication** ］［**coldstart** ］［**linkdown** ］［**linkup** ］［**warmstart**］
no snmp-server enable traps snmp ［**authentication** ］［**coldstart** ］［**linkdown** ］［**linkup** ］［**warmstart**］

構文の説明

authentication	（任意）認証トラップをイネーブルにします。
coldstart	（任意）コールドスタート トラップをイネーブルにします。
linkdown	（任意）リンクダウン トラップをイネーブルにします。
linkup	（任意）リンクアップ トラップをイネーブルにします。
warmstart	（任意）ウォームスタート トラップをイネーブルにします。

コマンド デフォルト

SNMP トラップの送信をディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、ウォーム スタートの SNMP トラップをイネーブルにする例を示します。

```
Switch(config)# snmp-server enable traps snmp warmstart
```

snmp-server enable traps stackwise

SNMP StackWise トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps stackwise** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps stackwise [**GLS**] [**ILS**] [**SRLS**]
[**insufficient-power**] [**invalid-input-current**]
[**invalid-output-current**] [**member-removed**] [**member-upgrade-notification**]
[**new-master**] [**new-member**] [**port-change**] [**power-budget-warning**] [**power-invalid-topology**]
[**power-link-status-changed**] [**power-oper-status-changed**]
[**power-priority-conflict**] [**power-version-mismatch**] [**ring-redundant**]
[**stack-mismatch**] [**unbalanced-power-supplies**] [**under-budget**] [**under-voltage**]
no snmp-server enable traps stackwise [**GLS**] [**ILS**] [**SRLS**]
[**insufficient-power**] [**invalid-input-current**]
[**invalid-output-current**] [**member-removed**] [**member-upgrade-notification**]
[**new-master**] [**new-member**] [**port-change**] [**power-budget-warning**] [**power-invalid-topology**]
[**power-link-status-changed**] [**power-oper-status-changed**]
[**power-priority-conflict**] [**power-version-mismatch**] [**ring-redundant**]
[**stack-mismatch**] [**unbalanced-power-supplies**] [**under-budget**] [**under-voltage**]

構文の説明

GLS	（任意）StackWise スタック電源 GLS トラップをイネーブルにします。
ILS	（任意）StackWise スタック電源 ILS トラップをイネーブルにします。
SRLS	（任意）StackWise スタック電源 SRLS トラップをイネーブルにします。
insufficient-power	（任意）Stackwise スタック電源の不平衡電源トラップをイネーブルにします。
invalid-input-current	（任意）Stackwise スタック電源の無効入力電流トラップをイネーブルにします。
invalid-output-current	（任意）Stackwise スタック電源の無効出力電流トラップをイネーブルにします。
member-removed	（任意）StackWise スタック メンバ削除トラップをイネーブルにします。
member-upgrade-notification	（任意）StackWise メンバのアップグレード用リロード トラップをイネーブルにします。
new-master	（任意）StackWise の新規マスター トラップをイネーブルにします。

new-member	（任意）StackWise の新規メンバ トラップをイネーブルにします。
port-change	（任意）StackWiseのスタック ポート変更トラップをイネーブルにします。
power-budget-warning	（任意）StackWise スタック電源バジェット警告トラップをイネーブルにします。
power-invalid-topology	（任意）Stackwise スタック電源の無効トポロジ トラップをイネーブルにします。
power-link-status-changed	（任意）StackWiseスタック電源リンク ステータス変更トラップをイネーブルにします。
power-oper-status-changed	（任意）StackWise スタック電源ポート動作ステータス変更トラップをイネーブルにします。
power-priority-conflict	（任意）StackWise スタック電源のプライオリティ競合トラップをイネーブルにします。
power-version-mismatch	（任意）StackWise スタック電源のバージョン不一致トラップをイネーブルにします。
ring-redundant	（任意）StackWise のリング冗長トラップをイネーブルにします。
stack-mismatch	（任意）StackWise スタック不一致トラップをイネーブルにします。
unbalanced-power-supplies	（任意）Stackwise スタック電源の不平衡電源トラップをイネーブルにします。
under-budget	（任意）StackWiseスタック電源の不足バジェット トラップをイネーブルにします。
under-voltage	（任意）Stackwise スタック電源の不足電圧トラップをイネーブルにします。

コマンド デフォルト

SNMP StackWise トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、StackWise スタック電源の GLS トラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps stackwise GLS
```

snmp-server enable traps storm-control

SNMP ストーム制御トラップ パラメータをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps storm-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps storm-control {**trap-rate** *number-of-minutes*}
no snmp-server enable traps storm-control {**trap-rate**}

構文の説明

trap-rate *number-of-minutes*	（任意）SNMP ストーム制御トラップ レートを分単位で指定します。受け入れられる値の範囲は 0 ～ 1000 です。

コマンド デフォルト

SNMP ストーム制御トラップ パラメータの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP ストーム制御トラップレートを 1 分あたり 10 トラップに設定する例を示します。

```
Switch(config)# snmp-server enable traps storm-control trap-rate 10
```

snmp-server enable traps stpx

SNMP STPX MIB トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps stpx** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps stpx [**inconsistency**] [**loop-inconsistency**] [**root-inconsistency**]
no snmp-server enable traps stpx [**inconsistency**] [**loop-inconsistency**] [**root-inconsistency**]

構文の説明

inconsistency	（任意）SNMP STPX MIB 矛盾更新トラップをイネーブルにします。
loop-inconsistency	（任意）SNMP STPX MIB ループ矛盾更新トラップをイネーブルにします。
root-inconsistency	（任意）SNMP STPX MIB ルート矛盾更新トラップをイネーブルにします。

コマンド デフォルト

SNMP STPX MIB トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP STPX MIB 矛盾更新トラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps stpx inconsistency
```

snmp-server enable traps transceiver

SNMP トランシーバ トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps transceiver** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps transceiver {**all**}
no snmp-server enable traps transceiver {**all**}

構文の説明

all	（任意）すべてのSNMP トランシーバ トラップをイネーブルにします。

コマンド デフォルト

SNMP トランシーバ トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、すべての SNMP トランシーバ トラップを設定する例を示します。

```
Switch(config)# snmp-server enable traps transceiver all
```

snmp-server enable traps vrfmib

SNMP vrfmib トラップを許可するには、グローバル コンフィギュレーション モードで **snmp-server enable traps vrfmib** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps vrfmib ［**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**］
no snmp-server enable traps vrfmib ［**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**］

構文の説明

vnet-trunk-down	（任意）vrfmib trunk ダウン トラップをイネーブルにします。
vnet-trunk-up	（任意）vrfmib trunk アップ トラップをイネーブルにします。
vrf-down	（任意）vrfmib vrf ダウン トラップをイネーブルにします。
vrf-up	（任意）vrfmib vrf アップ トラップをイネーブルにします。

コマンド デフォルト

SNMP vrfmib トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

この例は、vrfmib trunk ダウン トラップを生成する方法を示しています。

```
Switch(config)# snmp-server enable traps vrfmib vnet-trunk-down
```

snmp-server enable traps vstack

SNMP スマートインストール トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps vstack** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps vstack ［**addition**］［**failure**］［**lost**］［**operation**］
no snmp-server enable traps vstack ［**addition**］［**failure**］［**lost**］［**operation**］

構文の説明

addition	（任意）クライアントによって追加されたトラップをイネーブルにします。
failure	（任意）ファイルのアップロードとダウンロード障害トラップをイネーブルにします。
lost	（任意）クライアントの損失トラップをイネーブルにします。
operation	（任意）動作モード変更トラップをイネーブルにします。

コマンド デフォルト

SNMP スマート インストール トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP スマートインストール クライアント追加トラップを生成する例を示します。

```
Switch(config)# snmp-server enable traps vstack addition
```

snmp-server engineID

SNMP のローカル コピーまたはリモート コピーに名前を設定するには、グローバル コンフィギュレーション モードで **snmp-serverengineID** コマンドを使用します。

snmp-server engineID {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}

構文の説明

local *engineid-string*	SNMP コピーの名前に 24 文字の ID 文字列を指定します。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジン ID のうちゼロのみが続く箇所を除いた部分だけです。
remote *ip-address*	リモート SNMP コピーを指定します。SNMP のリモート コピーを含むデバイスの *ip-address* を指定します。
udp-port *port-number*	（任意）リモート デバイスのユーザ データグラム プロトコル（UDP）ポートを指定します。デフォルトは 162 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし

例

次の例では、ローカル エンジン ID 1234000000000000000000000 を設定します。

```
Switch(config)# snmp-server engineID local 1234
```

snmp-server host

Simple Network Management Protocol（SNMP）通知操作の受信者（ホスト）を指定するには、スイッチで **snmp-server host** グローバル コンフィギュレーション コマンドを使用します。指定されたホストを削除するには、このコマンドの **no** 形式を使用します。

snmp-server host {*host-addr*} [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }
no snmp-server host {*host-addr*} [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }

構文の説明

host-addr	ホスト（ターゲットとなる受信側）の名前またはインターネットアドレスです。
vrf *vrf-instance*	（任意）仮想プライベートネットワーク（VPN）ルーティング インスタンスとこのホストの名前を指定します。
informs | **traps**	（任意）このホストに SNMP トラップまたは情報を送信します。
version 1 | **2c** | **3**	（任意）トラップの送信に使用する SNMP のバージョンを指定します。 **1**：SNMPv1。情報の場合は、このオプションを使用できません。 **2c**：SNMPv2C。 **3**：SNMPv3。認証キーワードの 1 つ（次の表の行を参照）が、バージョン 3 キーワードに従っている必要があります。
auth | **noauth** | **priv**	**auth**（任意）：Message Digest 5（MD5）およびセキュア ハッシュ アルゴリズム（SHA）パケット認証をイネーブルにします。 **noauth**（デフォルト）：noAuthNoPriv セキュリティ レベル。**auth** | **noauth** | **priv** キーワードの選択が指定されていない場合、これがデフォルトとなります。 **priv**（任意）：データ暗号規格（DES）によるパケット暗号化（「プライバシー」ともいう）をイネーブルにします。
community-string	通知処理にともなって送信される、パスワードと類似したコミュニティ ストリングです。**snmp-server host** コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、**snmp-server community** グローバル コンフィギュレーション コマンドを使用してから、**snmp-server host** コマンドを使用することを推奨します。 （注） コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティ ストリングの一部として @ 記号を使用しないでください。

notification-type （任意）ホストに送信される通知のタイプです。タイプが指定されていない場合、すべての通知が送信されます。通知タイプには、次のキーワードの 1 つまたは複数を指定できます。

- **auth-framework**：SNMP CISCO-AUTH-FRAMEWORK-MIB トラップを送信します。
- **bridge**：SNMP スパニング ツリー プロトコル（STP）ブリッジ MIB トラップを送信します。
- **bulkstat**：データ収集 MIB 収集通知トラップを送信します。
- **call-home**：SNMP CISCO-CALLHOME-MIB トラップを送信します。
- **cef**：SNMP CEF トラップを送信します。
- **config**：SNMP 設定トラップを送信します。
- **config-copy**：SNMP config-copy トラップを送信します。
- **config-ctid**：SNMP config-ctid トラップを送信します。
- **copy-config**：SNMP コピー設定トラップを送信します。
- **cpu**：CPU 通知トラップを送信します。
- **cpu threshold**：CPU しきい値通知トラップを送信します。
- **eigrp**：SNMP EIGRP トラップを送信します。
- **entity**：SNMP エントリ トラップを送信します。

- **envmon**：環境モニタ トラップを送信します。
- **errdisable**：SNMP errdisable 通知トラップを送信します。
- **event-manager**：SNMP Embedded Event Manager トラップを送信します。
- **flash**：SNMP FLASH 通知を送信します。
- **flowmon**：SNMP flowmon 通知トラップを送信します。
- **ipmulticast**：SNMP IP マルチキャスト ルーティング トラップを送信します。
- **ipsla**：SNMP IP SLA トラップを送信します。
- **isis**：SNMP IS-IS トラップを送信します。
- **license**：ライセンス トラップを送信します。
- **local-auth**：SNMP ローカル認証トラップを送信します。
- **mac-notification**：SNMP MAC 通知トラップを送信します。
- **ospf**：Open Shortest Path First（OSPF）トラップを送信します。
- **pim**：SNMP プロトコル独立型マルチキャスト（PIM）トラップを送信します。
- **port-security**：SNMP ポートセキュリティ トラップを送信します。
- **power-ethernet**：SNMP パワー イーサネット トラップを送信します。
- **snmp**：SNMP タイプ トラップを送信します。
- **storm-control**：SNMP ストーム制御トラップを送信します。
- **stpx**：SNMP STP 拡張 MIB トラップを送信します。
- **syslog**：SNMP syslog トラップを送信します。
- **transceiver**：SNMP トランシーバ トラップを送信します。
- **tty**：TCP 接続トラップを送信します。
- **vlan-membership**：SNMP VLAN メンバーシップ トラップを送信します。
- **vlancreate**：SNMP VLAN 作成のトラップを送信します。
- **vlandelete**：SNMP VLAN 削除トラップを送信します。
- **vrfmib**：SNMP vrfmib トラップを送信します。
- **vstack**SNMP スマート インストール トラップを送信します。
- **vtp**：SNMP VLAN Trunking Protocol（VTP）トラップを送信します。
- **wireless**：ワイヤレス トラップを送信します。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。通知は送信されません。

キーワードを指定しないでこのコマンドを入力した場合は、デフォルトで、すべてのトラップタイプがホストに送信されます。情報はこのホストに送信されません。

version キーワードがない場合、デフォルトはバージョン 1 になります。

バージョン 3 を選択し、認証キーワードを入力しなかった場合は、デフォルトで、**noauth**（noAuthNoPriv）セキュリティ レベルになります。

（注） **fru-ctrl** キーワードは、コマンドラインのヘルプ ストリングには表示されていますが、サポートされていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

SNMP通知は、トラップまたは情報要求として送信できます。トラップを受信しても受信側は確認応答を送信しないため、トラップは信頼できません。送信側では、トラップが受信されたかどうかを判別できません。ただし、情報要求を受信したSNMPエンティティは、SNMP応答PDUを使用してメッセージに確認応答します。送信側が応答を受信しない場合、インフォーム要求を再送信して、インフォームが目的の宛先に到達する可能性を向上できます。

ただし、情報はエージェントおよびネットワークのリソースをより多く消費します。送信と同時に廃棄されるトラップと異なり、インフォーム要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持する必要があります。また、トラップの送信は1回限りですが、情報は数回にわたって再試行が可能です。再送信の回数が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因にもなります。

snmp-server host コマンドを入力しなかった場合は、通知が送信されません。SNMP 通知を送信するようにスイッチを設定するには、**snmp-server host** コマンドを少なくとも 1 つ入力する必要があります。キーワードを指定しないでこのコマンドを入力した場合、そのホストではすべてのトラップ タイプがイネーブルになります。複数のホストをイネーブルにするには、ホストごとに **snmp-server host** コマンドを個別に入力する必要があります。コマンドには複数の通知タイプをホストごとに指定できます。

ローカルユーザがリモートホストと対応させられていない場合、スイッチは **auth**（authNoPriv）および **priv**（authPriv）の認証レベルの情報を送信しません。

同じホストおよび同じ種類の通知（トラップまたは情報）に対して複数の **snmp-server host** コマンドを指定した場合は、後に入力されたコマンドによって前のコマンドが上書きされます。最後の **snmp-server host** コマンドだけが有効です。たとえば、ホストに **snmp-server host inform** コマンドを入力してから、同じホストに別の **snmp-server host inform** コマンドを入力した場合は、2 番目のコマンドによって最初のコマンドが置き換えられます。

snmp-server host コマンドは、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと組み合わせて使用します。グローバルに送信される SNMP 通知を指定するには、**snmp-server enable traps** コマンドを使用します。1 つのホストでほとんどの通知を受信する場合は、このホストに対して、少なくとも1つの **snmp-server enable traps** コマンドと **snmp-server host** コマンドをイネーブルにする必要があります。一部の通知タイプは、**snmp-server enable traps** コマンドで制御できません。たとえば、ある通知タイプは常にイネーブルですが、別の通知タイプはそれぞれ異なるコマンドによってイネーブルになります。

キーワードを指定しないで**no snmp-server host**コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。情報をディセーブルにするには、**no snmp-server host informs** コマンドを使用してください。

例

次の例では、トラップに対して一意の SNMP コミュニティ ストリング comaccess を設定し、このストリングによる、アクセス リスト 10 を介した SNMP ポーリング アクセスを禁止します。

```
Switch(config)# snmp-server community comaccess ro 10
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(config)# access-list 10 deny any
```

次の例では、名前 myhost.cisco.com で指定されたホストに SNMP トラップを送信する方法を示します。コミュニティ ストリングは、comaccess として定義されています。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

次の例では、コミュニティ ストリング public を使用して、すべてのトラップをホスト myhost.cisco.com に送信するようにスイッチをイネーブルにする方法を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連トピック

snmp-server enable traps

switchport mode access

トランキングなし、タグなしの単一VLANイーサネットインターフェイスとしてインターフェイスを設定するには、テンプレート コンフィギュレーション モードで **switchport mode access** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport mode access
no switchport mode access

構文の説明

switchport mode access	トランキングなし、タグなしの単一VLANイーサネットインターフェイスとして、インターフェイスを設定します。

コマンド デフォルト

アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。アクセス ポートは、デフォルトで、VLAN 1 のトラフィックを送受信します。

コマンド モード

テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、単一 VLAN インターフェイスを設定する例を示します。

```
Switch(config-template)# switchport mode access
```

switchport voice vlan

指定された VLAN からのすべての音声トラフィックを転送するように指定するには、テンプレート コンフィギュレーション モードで **switchport voice vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport voice vlan*vlan_id*
no switchport voice vlan

構文の説明

switchport voice vlan*vlan_id*	すべての音声トラフィックを指定された VLAN 経由で転送するように指定します。

コマンド デフォルト

1 ～ 4094 の値を指定できます。

コマンド モード

テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、指定された VLAN からのすべての音声トラフィックを転送するように指定する例を示します。

```
Switch(config-template)# switchport voice vlan 20
```

第 VIII 部

QoS

QoS コマンド

この章では、次の QoS コマンドについて説明します。

auto qos

自動 QoS ワイヤレス ポリシーを有効にするには、**auto QoS** コマンドを使用します。自動 QoS ワイヤレス ポリシーを削除するには、このコマンドの **no** 形式を使用します。

auto qos enterprise | guest | voice

構文の説明

enterprise	自動Qos ワイヤレス企業ポリシーを有効にします。
guest	自動 Qos ワイヤレス ゲスト ポリシーを有効にする
voice	自動 Qos ワイヤレス 音声ポリシーを有効にする

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

次に、自動 Qos ワイヤレス企業ポリシーを有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wlan wlan1
Switch(config-wlan)#auto qos enterprise
```

class

指定されたクラスマップ名のトラフィックを分類する一致基準を定義するには、ポリシーマップ コンフィギュレーション モードで **class** コマンドを使用します。既存のクラス マップを削除する場合は、このコマンドの **no** 形式を使用します。

class {*class-map-name*|**class-default**}
no class {*class-map-name*|**class-default**}

構文の説明

class-map-name	クラス マップ名。
class-default	分類されていないパケットに一致するシステムのデフォルト クラスを参照します。

コマンド デフォルト

ポリシー マップ クラス マップは定義されていません。

コマンド モード

ポリシー マップ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

class コマンドを使用する前に、**policy-map** グローバル コンフィギュレーション コマンドを使用してポリシー マップを識別し、ポリシーマップ 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。ポリシー マップを指定すると、ポリシー マップ内で新規クラスのポリシーを設定したり、既存クラスのポリシーを変更したりすることができます。**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、ポリシー マップをポートへ添付することができます。

class コマンドを入力すると、ポリシーマップ クラス コンフィギュレーション モードが開始されます。使用できるコンフィギュレーション コマンドは、次のとおりです。

- **admit**：コール アドミッション制御（CAC）の要求を許可します。
- **bandwidth**：クラスに割り当てられる帯域幅を指定します。
- **exit**：ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシー マップ コンフィギュレーション モードに戻ります。
- **no**：コマンドをデフォルト設定に戻します。
- **police**：分類したトラフィックにポリサーまたは集約ポリサーを定義します。ポリサーは、帯域幅の限度およびその限度を超過した場合に実行するアクションを指定します。このコマンドの詳細については、Cisco.com で入手可能な『*Cisco IOS Quality of Service Solutions Command Reference*』を参照してください。

- **priority**：ポリシー マップに属するトラフィックのクラスにスケジューリング プライオリティを割り当てます。
- **queue-buffers**：クラスのキュー バッファを設定します。
- **queue-limit**：ポリシー マップに設定されたクラス ポリシー用にキューが保持できる最大パケット数を指定します。
- **service-policy**：QoS サービス ポリシーを設定します。
- **set**：分類したトラフィックに割り当てる値を指定します。詳細については、次のサイトを参照してください。 set （639 ページ）
- **shape**：平均またはピーク レート トラフィック シェーピングを指定します。このコマンドの詳細については、Cisco.com で入手可能な『*Cisco IOS Quality of Service Solutions Command Reference*』を参照してください。

ポリシーマップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

class コマンドは、**class-map** グローバル コンフィギュレーション コマンドと同じ機能を実行します。他のポートと共有していない新しい分類が必要な場合は、**class** コマンドを使用します。多数のポート間でマップを共有する場合には、**class-map** コマンドを使用します。

classclass-default ポリシーマップ コンフィギュレーション コマンドを使用して、デフォルト クラスを設定できます。分類されていないトラフィック（トラフィック クラスで指定された一致基準を満たさないトラフィック）は、デフォルト トラフィックとして処理されます。

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

例

次に、policy1 という名前のポリシーマップを作成する例を示します。このコマンドが入力方向に添付された場合、class1 で定義されたすべての着信トラフィックの照合を行い、IP DiffServ コード ポイント（DSCP）を 10 に設定し、平均レート 1 Mb/s、バースト 20 KB のトラフィックをポリシングします。プロファイルを超えるトラフィックは、ポリシング設定 DSCP マップから取得した DSCP 値がマークされてから送信されます。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(config-pmap-c)# exit
```

次に、ポリシーマップにデフォルトのトラフィック クラスを設定する例を示します。また、**class-default** が最初に設定された場合でも、デフォルトのトラフィック クラスをポリシー マップ pm3 の終わりに自動的に配置する方法も示します。

```
Switch# configure terminal
Switch(config)# class-map cm-3
Switch(config-cmap)# match ip dscp 30
Switch(config-cmap)# exit

Switch(config)# class-map cm-4
```

```
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# exit

Switch(config)# policy-map pm3
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit

Switch(config-pmap)# class cm-3
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit

Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# set precedence 5
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit

Switch# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class cm-4
    set precedence 5
  Class class-default
    set dscp af11
```

関連トピック

class-map （618 ページ）
policy-map （625 ページ）
show policy-map （656 ページ）
set （639 ページ）

class-map

名前を指定したクラスとパケットの照合に使用するクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **class-map** コマンドを使用します。既存のクラス マップを削除し、グローバル コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

class-map [{**match-any***type*}] *class-map-name*
no class-map [{**match-any***type*}] *class-map-name*

構文の説明

match-any	（任意）このクラスマップ内の一致ステートメントの論理和をとります。1つ以上の条件が一致していなければなりません。
type	（任意）CPL クラス マップを設定します。
class-map-name	クラス マップ名。

コマンド デフォルト

クラス マップは定義されていません。

コマンド モード

グローバル コンフィギュレーション

ポリシー マップ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**type** キーワードが追加されました。

使用上のガイドライン

クラス マップ一致基準を作成または変更するクラスの名前を指定し、クラス マップ コンフィギュレーション モードを開始する場合は、このコマンドを使用します。

ポートごとに適用される、グローバルに名前が付けられたサービス ポリシーの一部として、パケットの分類、マーキング、および集約ポリシングを定義する場合は、**class-map** コマンドおよびそのサブコマンドを使用します。

Quality of Service（QoS）クラスマップ コンフィギュレーション モードでは、次のコンフィギュレーション コマンドを利用することができます。

- **description**：クラス マップを説明します（最大 200 文字）。**show class-map** 特権 EXEC コマンドは、クラス マップの説明と名前を表示します。
- **exit**：QoS クラスマップ コンフィギュレーション モードを終了します。
- **match**：分類基準を設定します。
- **no**：クラス マップから一致ステートメントを削除します。

match-any キーワードを入力した場合、**match access-group** クラスマップ コンフィギュレーション コマンドで名前付き拡張アクセス コントロール リスト（ACL）を指定するためにのみ使用できます。

物理ポート単位でパケット分類を定義するために、クラス マップごとに 1 つの **match** コマンドのみがサポートされています。

ACL には複数のアクセス コントロール エントリ（ACE）を含めることができます。

例

次に、クラス マップ class1 に 1 つの一致基準（アクセス リスト 103）を設定する例を示します。

```
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

次に、クラス マップ class1 を削除する例を示します。

```
Switch(config)# no class-map class1
```

設定を確認するには、**show class-map** 特権 EXEC コマンドを入力します。

関連トピック

policy-map （625 ページ）
show policy-map （656 ページ）

match（クラスマップ コンフィギュレーション）

トラフィックを分類するための一致基準を定義するには、クラスマップ コンフィギュレーション モードで **match** コマンドを使用します。一致基準を削除するには、このコマンドの **no** 形式を使用します。

match {**access-group**{**name***acl-nameacl-index*}|**class-map** *class-map-name*|**cos** *cos-value*|**dscp** *dscp-value*|**[ip] dscp** *dscp-list*|**[ip] precedence** *ip-precedence-list*|**precedence** *precedence-value1...value4*|**qos-group** *qos-group-value*|**vlan** *vlan-id*}
no match {**access-group**{**name***acl-nameacl-index*}|**class-map** *class-map-name*|**cos** *cos-value*|**dscp** *dscp-value*|**[ip] dscp** *dscp-list*|**[ip] precedence** *ip-precedence-list*|**precedence** *precedence-value1...value4*|**qos-group** *qos-group-value*|**vlan** *vlan-id*}

構文の説明

access-group	アクセス グループを指定します。
name *acl-name*	IP 標準または拡張アクセス コントロール リスト（ACL）または MAC ACL の名前を指定します。
acl-index	IP 標準または拡張アクセス コントロール リスト（ACL）または MAC ACL の番号を指定します。IP 標準 ACL の場合、ACL インデックス範囲は 1 ～ 99 および 1300 ～ 1999 です。IP 拡張 ACL の場合、ACL インデックス範囲は 100 ～ 199 および 2000 ～ 2699 です。
class-map *class-map-name*	トラフィック クラスを分類ポリシーとして使用し、使用するトラフィック クラスの名前を一致基準として指定します。
cos *cos-value*	レイヤ 2 サービス クラス（CoS）/Inter-Switch Link（ISL）マーキングに基づいてパケットを照合します。CoS 値は 0 ～ 7 です。1 つの **match cos** ステートメントに最大 4 つの CoS 値をスペースで区切って指定できます。
dscp *dscp-value*	各 DSCP 値のパラメータを指定します。DiffServ コード ポイント値を指定する 0 ～ 63 の範囲の値を指定できます。
ip dscp *dscp-list*	着信パケットとの照合を行うための、最大 8 つまでの IP DiffServ コード ポイント（DSCP）値の一覧を指定します。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。一般的に使用する値に対してはニーモニック名を入力することもできます。

ip precedence *ip-precedence-list*	着信パケットとの照合を行うための、最大 8 つの IP プレシデンス値の一覧を指定します。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。一般的に使用する値に対してはニーモニック名を入力することもできます。
precedence *precedence-value1...value4*	分類されたトラフィックに IP プレシデンス値を割り当てます。指定できる範囲は 0 ～ 7 です。一般的に使用する値に対してはニーモニック名を入力することもできます。
qos-group *qos-group-value*	特定の QoS グループ値を一致基準として識別します。指定できる範囲は 0 ～ 31 です。
vlan *vlan-id*	特定の VLAN を一致基準として指定します。指定できる範囲は 1 ～ 4095 です。

コマンド デフォルト

一致基準は定義されません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**class-map** *class-map-name*、**cos** *cos-value*、**qos-group** *qos-group-value*、および **vlan** *vlan-id* キーワードが追加されました。

使用上のガイドライン

パケットを分類するために着信パケットのどのフィールドを調べるのかを指定する場合は、**match** コマンドを使用します。IP アクセス グループまたは MAC アクセス グループの Ether Type/Len のマッチングだけがサポートされています。

class-mapmatch-any*class-map-name* グローバル コンフィギュレーション コマンドを入力した場合、次の **match** コマンドを入力できます。

- **matchaccess-groupname** *acl-name*

（注） ACL は、名前付き拡張 ACL にする必要があります。

- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

match access-group *acl-index* コマンドはサポートされていません。

物理ポート単位でパケット分類を定義するために、クラス マップごとに 1 つの **match** コマンドのみがサポートされています。この場合、**match-any** キーワードと同じです。

match ip dscp *dscp-list* コマンドまたは **match ip precedence** *ip-precedence-list* コマンドの場合は、よく使用される値のニーモニック名を入力できます。たとえば、**match ip dscp af11** コマンドを入力できます。このコマンドは、**match ip dscp 10** コマンドを入力した場合と同じ結果になります。また、**match ipprecedence critical** コマンドを入力できます。このコマンドは、**match ip precedence 5** コマンドを入力した場合と同じ結果になります。サポートされているニーモニックの一覧を表示するには、**match ip dscp ?** または **match ip precedence ?** コマンドを入力して、コマンドラインのヘルプ文字列を参照してください。

階層ポリシー マップ内にインターフェイス レベルのクラス マップを設定するときには、**input-interface** *interface-id-list* キーワードを使用します。*interface-id-list* には、最大 6 つのエントリを指定することができます。

例

次の例では、クラス マップ class2 を作成する方法を示します。このマップは、DSCP 値 10、11、および 12 を持つすべての着信トラフィックに一致します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

次の例では、クラス マップ class3 を作成する方法を示します。このマップは、IP precedence 値 5、6、および 7 を持つすべての着信トラフィックに一致します。

```
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

次の例では、IP precedence 一致基準を削除し、acl1 を使用してトラフィックを分類する方法を示します。

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# no match ip precedence
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
```

次の例では、階層ポリシー マップでインターフェイス レベルのクラス マップが適用する物理ポートのリストの指定方法を示しています。

```
Switch(config)# class-map match-any class4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
```

次の例では、階層ポリシー マップでインターフェイス レベルのクラス マップが適用する物理ポートの範囲の指定方法を示しています。

```
Switch(config)# class-map match-any class4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
```

設定を確認するには、**show class-map** 特権 EXEC コマンドを入力します。

match non-client-nrt

NRT（非リアルタイム）で非クライアントを照合するには、クラスマップ コンフィギュレーション モードで **matchnon-client-nrt** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

match non-client-nrt
no match non-client-nrt

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

クラスマップ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし

次に、NRT で非クライアントを設定する例を示します。

```
Switch(config)# class-map test_1000
Switch(config-cmap)# match non-client-nrt
```

match wlan user-priority

802.11 固有の値を照合するには、クラスマップ コンフィギュレーション モードで **matchwlanuser-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

match wlan user-priority *wlan-value* ［*wlan-value*］ ［*wlan-value*］ ［*wlan-value*］
no match wlan user-priority *wlan-value* ［*wlan-value*］ ［*wlan-value*］ ［*wlan-value*］

構文の説明

wlan-value	802.11 固有の値。ユーザ プライオリティ 802.11 TID user priority（0-7）を入力します。（任意）ユーザプライオリティ値を3つまで、空白文字区切りで入力します。

コマンド デフォルト

なし

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし

次に、ユーザ プライオリティ値を設定する例を示します。

```
Switch(config)# class-map test_1000
Switch(config-cmap)# match wlan user-priority 7
```

policy-map

複数の物理ポートまたはスイッチ仮想インターフェイス（SVI）に適用し、ポリシーマップ コンフィギュレーション モードを開始できるポリシーマップを作成または変更するには、グローバル コンフィギュレーション モードで **policy-map** コマンドを使用します。既存のポリシーマップを削除し、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

policy-map *policy-map-name*
no policy-map *policy-map-name*

構文の説明

policy-map-name	ポリシー マップ名です。

コマンド デフォルト

ポリシー マップは定義されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

policy-map コマンドを入力すると、ポリシーマップ コンフィギュレーション モードに入り、次のコンフィギュレーション コマンドが使用可能になります。

- **class**：指定したクラス マップの分類一致基準を定義します。
- **description**：ポリシー マップを説明します（最大 200 文字）。
- **exit**：ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
- **no**：定義済みポリシー マップを削除します。
- **sequence-interval**：シーケンス番号機能をイネーブルにします。

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** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

一致基準がクラス マップに定義されているクラスのポリシーを設定する前に、**policy-map** コマンドを使用して作成、追加または変更するポリシーマップの名前を指定します。**policy-map** コマンドを入力した場合も、ポリシーマップ コンフィギュレーション モードがイネーブルになり、このモードでポリシーマップのクラスポリシーを設定または変更することができます。

クラス ポリシーをポリシー マップ内で設定できるのは、クラスに一致基準が定義されている場合だけです。クラスの一致基準を設定するには、**class-map** グローバル コンフィギュレーショ

ン コマンドおよび **match** クラスマップ コンフィギュレーション コマンドを使用します。物理ポート単位でパケット分類を定義します。

入力ポートごとに 1 つのポリシー マップのみがサポートされます。同じポリシー マップを複数の物理ポート に適用できます。

物理ポートに非階層ポリシー マップを適用できます。非階層ポリシー マップは、スイッチのポート ベース ポリシー マップと同じです。

階層ポリシーマップには親子ポリシーの形式で2つのレベルがあります。親ポリシーは変更できませんが、子ポリシー（port-child ポリシー）は、QoS 設定に合わせて変更できます。

VLANベースのQoSでは、サービス ポリシーがSVIインターフェイスに適用されます。VLAN ポリシー マップに属するすべての物理インターフェイスは、ポートベースのポリシー マップの代わりに VLAN ベースのポリシー マップが表示されるように設定する必要があります。

（注） 有線およびワイヤレスポートですべての MQC QoS の組み合わせがサポートされているわけではありません。これらの制限の詳細については、サービス品質（QoS）構成ガイドの「有線ターゲットのQoSの制限」および「ワイヤレス ターゲットの QoS の制限」に関する章を参照してください。

例

次の例では、policy1 という名前のポリシー マップを作成する方法を示します。入力ポートに適用した場合、class1 で定義されたすべての着信トラフィックの照合を行い、IP DSCP を 10 に設定し、平均伝送速度 1 Mb/s、バースト 20 KB のトラフィックをポリシングします。プロファイル未満のトラフィックが送信されます。

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 1000000 20000 conform-action transmit
Switch(config-pmap-c)# exit
```

次に、階層ポリシーを設定する例を示します。

```
Switch# configure terminal
Switch(config)# class-map c1
Switch(config-cmap)# exit

Switch(config)# class-map c2
Switch(config-cmap)# exit

Switch(config)# policy-map child
Switch(config-pmap)# class c1
Switch(config-pmap-c)# priority level 1
Switch(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit

Switch(config-pmap)# class c2
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit

Switch(config-pmap)# class class-default
```

```
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit

Switch(config)# policy-map parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 1000000
Switch(config-pmap-c)# service-policy child
Switchconfig-pmap-c)# end
```

次に、ポリシー マップを削除する例を示します。

```
Switch(config)# no policy-map policymap2
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

関連トピック

class （615 ページ）
class-map （618 ページ）
service-policy（有線） （635 ページ）
show policy-map （656 ページ）

priority

ポリシーマップに属するトラフィックのクラスにプライオリティを割り当てるには、ポリシーマップ クラス コンフィギュレーション モードで **priority** コマンドを使用します。以前に指定したクラスのプライオリティを削除するには、このコマンドの **no** 形式を使用します。

priority ［*Kbps* ［*burst -in-bytes*］ | **level** *level-value* ［*Kbps* ［*burst -in-bytes*］］ | **percent** *percentage* ［*Kb/s* ［*burst -in-bytes*］］］
no priority ［*Kb/s* ［*burst -in-bytes*］ | **level** *level value* ［*Kb/s* ［*burst -in-bytes*］］ | **percent** *percentage* ［*Kb/s* ［*burst -in-bytes*］］］

構文の説明

Kb/s	（任意）プライオリティ トラフィック向けの保証帯域幅（キロビット/秒（kbps））。帯域幅の量は、使用中のインターフェイスとプラットフォームによって異なります。保証帯域幅を超えると、非プライオリティ トラフィックがなくならないようにするため、プライオリティ トラフィックが輻輳のイベントでドロップされます。値は 1 ～ 2,000,000 kbps である必要があります。
burst -in-bytes	（任意）バイト単位のバースト サイズ。バースト サイズは、トラフィックの一時的なバーストに対応するネットワークを設定します。デフォルトバースト値は、設定されている帯域幅レートで、200 ミリ秒のトラフィックとして計算され、burst引数が指定されていない場合に使用されます。バーストの範囲は 32 ～ 2000000 バイトです。
level *level-value*	（任意）プライオリティ レベルを割り当てます。*level-value* の有効値は 1 と 2 です。レベル 1 はレベル 2 よりもプライオリティが高くなります。レベル 1 は帯域幅を予約して最初に送信を行うため、遅延は非常に低くなります。
percent *percentage*	（任意）保証帯域幅の量が、使用可能な帯域幅の割合（%）によって指定されることを、指定します。

コマンド デフォルト

プライオリティは設定されません。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	*Kbps*、*burst -in-bytes* および **percent** *percentage* キーワードが追加されました。

使用上のガイドライン

priority コマンドを使用すると、（User Datagram Ports（UDP）ポートだけではなく）さまざまな基準に基づいてクラスと設定し、プライオリティを割り当てることができます。これは、シリアルインターフェイスとATM相手先固定接続（PVC）で使用できます。類似の**ip rtp priority**コマンドを使用すると、UDP ポート番号にだけ基づいてプライオリティ フローを決定することができ、ATM PVC は使用できません。

同じポリシーマップ内では、bandwidthコマンドおよびpriorityコマンドは、同じクラスに使用できません。ただし、これらのコマンドは、同じポリシーマップ内では一緒に使用できます。

ポリシーマップで、1つまたは複数のクラスにプライオリティ ステータスを指定できます。単一ポリシー マップ内の複数のクラスがプライオリティ クラスとして設定されると、これらのクラスからのすべてのトラフィックが、同じ単一のプライオリティ キューにキューイングされます。

クラス ポリシー設定が含まれているポリシー マップがインターフェイスに付加されて、そのインターフェイスのサービス ポリシーが決定される場合、使用可能な帯域幅が評価されます。インターフェイスの帯域幅が不十分なことが原因で、特定のインターフェイスにポリシーマップがアタッチできない場合、そのポリシーは、正常にアタッチされていたすべてのインターフェイスから削除されます。

例

次に、ポリシー マップ policy1 のクラスのプライオリティを設定する例を示します。

```
Switch(config)# class-map cm1
Switch(config-cmap)#match precedence 2
Switch(config-cmap)#exit

Switch(config)#class-map cm2
Switch(config-cmap)#match dscp 30
Switch(config-cmap)#exit

Switch(config)# policy-map policy1
Switch(config-pmap)# class cm1
Switch(config-pmap-c)# priority level 1
Switch(config-pmap-c)# police 1m
Switch(config-pmap-c-police)#exit
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit

Switch(config)#policy-map policy1
Switch(config-pmap)#class cm2
Switch(config-pmap-c)#priority level 2
Switch(config-pmap-c)#police 1m
```

qos queue-softmax-multiplier

softmax バッファの値を増やすには、グローバル コンフィギュレーション モードで **qos queue-softmax-multiplier** コマンドを使用します。

range-of-multiplier
no qos queue-softmax-multiplier *range-of-multiplier*

構文の説明

range-of-multiplier	値は、100～1200の範囲で指定できます。デフォルト値は 100 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.6.3 および Cisco IOS XE 3.7.2	このコマンドが導入されました。

使用上のガイドライン

（注） このコマンドは、ポリシー マップが対応付けられているポートでのみ有効です。1200 で設定されている場合、非プライオリティ キューおよび非プライマリ プライオリティ キュー（!=level 1）の softmax は、それぞれのデフォルト値に 12 を乗じた値になります。このコマンドは、プライオリティ キュー レベル 1 には適用されません。

queue-buffers ratio

クラスのキュー バッファを設定するには、ポリシーマップ クラス コンフィギュレーション モードで **queue-buffers ratio** コマンドを使用します。比率制限を削除するには、このコマンドの **no** 形式を使用します。

queue-buffers ratio *ratio limit*
no queue-buffers ratio *ratio limit*

構文の説明

ratio limit	（任意）クラスのキュー バッファを設定します。キュー バッファの比率制限（0 ～ 100）を入力します。

コマンド デフォルト

クラスのキュー バッファは定義されていません。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、**bandwidth**、**shape** または **priority** コマンドを使用する必要があります。これらのコマンドの詳細については、Cisco.com で入手可能な *Cisco IOS Quality of Service* ソリューションのコマンド リファレンスを参照してください。

スイッチを使用すると、キューにバッファを割り当てることができます。バッファが割り当てられていない場合、すべてのキューの間で均等に分割されます。queue-buffer ratio を使用して、特定の比率で分割できます。デフォルトでは、ダイナミックしきい値およびスケーリング（DTS）がすべてのキューでアクティブであるため、バッファはソフト バッファです。

（注） queue-buffer ratio は有線ポートと無線ポートの両方でサポートされますが、queue-buffer ratio は queue-limit とともに設定することはできません。

例

次にキュー バッファの比率を 10 % に設定する例を示します。

```
Switch(config)# policy-map policy_queuebuf01
Switch(config-pmap)# class-map class_queuebuf01
Switch(config-cmap)# exit
Switch(config)# policy policy_queuebuf01
Switch(config-pmap)# class class_queuebuf01
Switch(config-pmap-c)# bandwidth percent 80
Switch(config-pmap-c)# queue-buffers ratio 10
Switch(config-pmap)# end
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

関連トピック

show policy-map （656 ページ）

queue-limit

キューが保持できる、ポリシー マップ内に設定されたクラス ポリシーのパケットの最大数を指定または変更するには、**queue-limit** ポリシーマップ クラス コンフィギュレーション コマンドを使用します。クラスからキュー パケット制限を削除するには、このコマンドの **no** 形式を使用します。

queue-limit *queue-limit-size*[{**packets**}] {**cos** *cos-value*|**dscp** *dscp-value*} **percent** *percentage-of-packets*
no queue-limit *queue-limit-size*[{**packets**}] {**cos** *cos-value*|**dscp** *dscp-value*} **percent** *percentage-of-packets*

構文の説明

queue-limit-size	キューの最大サイズ。最大値は、オプションの指定される測定単位用キーワード（bytes、ms、または packets）の単位によって異なります。
cos *cos-value*	各 cos 値のパラメータを指定します。CoS 値の範囲は 0 ～ 7 です。
dscp *dscp-value*	各 DSCP 値のパラメータを指定します。 キュー制限のタイプに合わせて DiffServ コードポイント値を指定します。範囲は 0 ～63 です。
percent *percentage-of-packets*	このクラスのキューが蓄積できるパケットの最大割合を指定します。範囲は 1 ～ 100 です。

コマンド デフォルト

なし

コマンド モード

ポリシー マップ クラス コンフィギュレーション（policy-map-c）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

packets 測定単位は、コマンドラインのヘルプ文字列には表示されますが、サポートされていません。**percent** 測定単位を使用してください。

（注） このコマンドは、出力方向の有線ポートでのみサポートされています。

Weighted Fair Queueing（WFQ）により、クラス マップが定義される各クラスのキューが作成されます。クラスの一致条件を満たすパケットは、送信されるまで、このクラス専用のキューに蓄積されます。この処理は、均等化キューイング プロセスによってキューが処理される場合

に発生します。クラスに定義した最大パケットしきい値に達すると、クラス キューへのそれ以降のパケットのキューイングは、テール ドロップされます。

重み付けテール ドロップ（WTD）を設定するためにキュー制限を使用します。WTDを使用すると、キューごとに複数のしきい値を設定できます。各サービス クラスが異なるしきい値でドロップされて QoS 差別化が実現されます。

トラフィックの異なるサブクラス、つまり、DSCP と CoS に最大キューしきい値を設定し、各サブクラスに最大キューしきい値を設定できます。

例

次の例では、dscp-1 というクラスのポリシーを含めるために port-queue というポリシーマップを設定しています。このクラスのポリシーは、確保されているキューの最大パケット制限が 20 % になるように設定されています。

```
Switch(config)# policy-map policy11
Switch(config-pmap)# class dscp-1
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit dscp 1 percent 20
```

service-policy（有線）

物理ポートまたはスイッチ仮想インターフェイス（SVI）のにポリシー マップを適用するには、インターフェイス コンフィギュレーション モードで **service-policy** コマンドを使用します。ポリシー マップとポートの対応付けを削除するには、このコマンドの **no** 形式を使用します。

service-policy {**input** | **output**} *policy-map-name*
no service-policy {**input** | **output**} *policy-map-name*

構文の説明

input *policy-map-name*	物理ポートまたはSVIの入力に、指定したポリシーマップを適用します。
output *policy-map-name*	物理ポートまたはSVIの出力に、指定したポリシーマップを適用します。

コマンド デフォルト

ポートにポリシー マップは適用されていません。

コマンド モード

WLAN インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ポリシー マップは、**policy map** コマンドによって定義されます。

1 つのポートごとに入力と出力に関して 1 つのポリシー マップだけがサポートされます。つまり、いずれのポートにおいても、1 つの入力ポリシーと 1 つの出力ポリシーだけを使用できます。

ポリシー マップは、物理ポートまたは SVI 上の着信トラフィックに適用できます。『*QoS Configuration Guide (Catalyst 3850 Switches)*』。

（注） **history** キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。このキーワードが収集した統計情報は無視します。

例

次の例では、物理入力ポートに plcmap1 を適用する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# service-policy input plcmap1
```

次の例では、物理ポートから plcmap2 を削除する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config-if)# no service-policy input plcmap2
```

次の例では、VLANのポリサー設定を表示します。この設定の最後に、QoSのインターフェイスにVLANポリシー マップを適用します。

```
Switch# configure terminal
Switch(config)# class-map vlan100
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# exit
Switch(config)# policy-map vlan100
Switch(config-pmap)# policy-map class vlan100
Switch(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Switch(config-pmap-c-police)# end
Switch# configure terminal
Switch(config)# interface gigabitEthernet1/0/5
Switch(config-if)#  service-policy input vlan100
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連トピック

policy-map （625 ページ）
show policy-map （656 ページ）

service-policy（WLAN）

WLAN サービス品質（QoS）サービス ポリシーを設定するには、**service-policy** コマンドを使用します。WLAN の QoS ポリシーを無効にするには、このコマンドの **no** 形式を使用します。

service-policy [client] {**input**|**output**} *policy-name*
no service-policy [client] {**input**|**output**} *policy-name*

構文の説明

client	（任意）WLAN 上のすべてのクライアントにポリシーマップを割り当てます。
input	入力ポリシー マップを割り当てます。
output	出力ポリシー マップを割り当てます。
policy-name	ポリシー名。

コマンド デフォルト

ポリシーが割り当てられない場合、ポリシーに割り当てられる状態は [None] になります。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

例

次の例では、WLAN の入力 QoS サービス ポリシーを設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# service-policy input policy-test
```

次の例では、WLAN の入力 QoS サービス ポリシーをディセーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no service-policy input policy-test
```

次に、WLAN の出力 QoS サービス ポリシーを platinum（貴金属ポリシー）に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# service-policy output platinum
```

関連トピック

wlan （1283 ページ）

set

パケットで Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値または IP プレシデンス値を設定して IP トラフィックを分類するには、ポリシーマップ クラス コンフィギュレーション モードで **set** コマンドを使用します。トラフィックの分類を削除するには、このコマンドの **no** 形式を使用します。

set
cos|dscp|precedence|ip|qos-group|wlan
set cos
{*cos-value*} | {**cos|dscp|precedence|qos-group|wlan**} [{**table** *table-map-name*}]
set dscp
{*dscp-value*} | {**cos|dscp|precedence|qos-group|wlan**} [{**table** *table-map-name*}]
set ip {**dscp|precedence**}
set precedence {*precedence-value*} | {**cos|dscp|precedence|qos-group**} [{**table** *table-map-name*}]
set qos-group
{*qos-group-value*|**dscp** [{**table** *table-map-name*}]|**precedence** [{**table** *table-map-name*}]}
set wlan user-priority
user-priority-value|**costable** *table-map-name*|**dscptable** *table-map-name*|**qos-grouptable** *table-map-name*|**wlantable** *table-map-name*

構文の説明		
	cos	発信パケットのレイヤ 2 サービス クラス（CoS）値またはユーザ プライオリティを設定します。次の値を指定できます。 • *cos-value*：0 ～ 7 の CoS 値。一般的に使用する値に対してはニーモニック名を入力することもできます。 • パケットに CoS 値を設定するためのパケット マーキング カテゴリを指定します。パケット マーキング値をマッピングおよび変換するためのテーブル マップも設定している場合は、これによって「map from」パケットマーキング カテゴリが確立されます。パケットマーキングカテゴリのキーワードは次のとおりです。 • **cos**：CoS値またはユーザプライオリティからの値を設定します。 • **dscp**：DiffServ コード ポイント（DSCP）からの値を設定します。 • **precedence**：パケット優先順位からの値を設定します。 • **qos-group**：QoS グループからの値を設定します。 • **wlan**：WLANユーザプライオリティ値を設定します。 • （任意）**table** *table-map-name*：CoS 値の設定に使用される指定されたテーブル マップに設定されている値を示します。CoS 値の指定に使用されるテーブル マップの名前を入力します。テーブルマップ名には、最大64の英数字を使用できます。 パケットマーキング カテゴリを指定したが、テーブルマップを指定していない場合、デフォルトアクションは、パケットマーキング カテゴリに関連付けられた値をCoS値としてコピーすることです。たとえば、**set cos precedence** コマンドを入力する場合、precedence（パケットマーキング カテゴリ）値がコピーされ、CoS値として使用されます。

dscp	IP（v4）および IPv6 パケットの DiffServ コード ポイント（DSCP）を指定します。次の値を指定できます。 • *cos-value*：DSCP 値を設定する番号。範囲は 0 ～ 63 です。一般的に使用する値に対してはニーモニック名を入力することもできます。 • パケットに DSCP 値を設定するためのパケット マーキング カテゴリを指定します。パケット マーキング値をマッピングおよび変換するためのテーブルマップも設定している場合は、これによって「map from」パケットマーキング カテゴリが確立されます。パケットマーキングカテゴリのキーワードは次のとおりです。 • **cos**：CoS 値またはユーザ プライオリティからの値を設定します。 • **dscp**：DiffServ コード ポイント（DSCP）からの値を設定します。 • **precedence**：パケット優先順位からの値を設定します。 • **qos-group**：QoS グループからの値を設定します。 • **wlan**：WLAN から値を設定します。 • （任意）**table** *table-map-name*：DSCP 値の設定に使用される指定されたテーブル マップに設定されている値を示します。DSCP 値の指定に使用されるテーブル マップの名前を入力します。テーブルマップ名には、最大 64 の英数字を使用できます。 パケットマーキング カテゴリを指定したが、テーブルマップを指定していない場合、デフォルト アクションは、パケットマーキング カテゴリに関連付けられた値を DSCP 値としてコピーすることです。たとえば、**set dscp cos** コマンドを入力する場合、CoS 値（パケットマーキング カテゴリ）がコピーされ、DSCP 値として使用されます。

ip	分類されたトラフィックにIP値を設定します。次の値を指定できます。 • **dscp**：0 ～ 63 の IP DSCP 値またはパケットマーキング カテゴリを指定します。 • **precedence**：IP ヘッダーの precedence ビット値を指定します（有効な値は 0 ～ 7）。または、パケットマーキング カテゴリを指定します。
precedence	パケット ヘッダーに precedence 値を設定します。次の値を指定できます。 • *precedence-value*：パケット ヘッダーに precedence ビットを設定します。有効な値は0 ~7です。一般的に使用する値に対してはニーモニック名を入力することもできます。 • パケットの優先順位値を設定するためのパケットマーキング カテゴリを指定します。 • **cos**：CoSまたはユーザプライオリティからの値を設定します。 • **dscp**：DiffServ コード ポイント（DSCP）からの値を設定します。 • **precedence**：パケット優先順位からの値を設定します。 • **qos-group**：QoS グループからの値を設定します。 • （任意）**table** *table-map-name*：優先順位値の設定に使用される指定されたテーブル マップに設定されている値を示します。優先順位値の指定に使用されるテーブル マップの名前を入力します。テーブルマップ名には、最大64の英数字を使用できます。 パケットマーキング カテゴリを指定したが、テーブルマップを指定していない場合、デフォルトアクションは、パケットマーキング カテゴリに関連付けられた値を優先順位値としてコピーすることです。たとえば、**set precedence cos** コマンドを入力する場合、CoS 値（パケットマーキング カテゴリ）がコピーされ、優先順位値として使用されます。

qos-group	後でパケットを分類するために使用できる QoS グループ ID を割り当てます。 • *qos-group-value*：分類されたトラフィックに QoS 値を設定します。指定できる範囲は 0 ～ 31 です。一般的に使用する値に対してはニーモニック名を入力することもできます。 • **dscp**：パケットの元の DSCP フィールド値を QoS グループ値として設定します。 • **precedence**：パケットの元の precedence フィールド値を QoS グループ値として設定します。 • （任意）**table** *table-map-name*：DSCP 値または優先順位値の設定に使用される指定されたテーブル マップに設定されている値を示します。値の指定に使用されるテーブル マップの名前を入力します。テーブル マップ名には、最大 64 の英数字を使用できます。 パケットマーキング カテゴリ（**dscp** または **precedence**）を指定したが、テーブル マップを指定していない場合、デフォルト アクションは、パケットマーキング カテゴリに関連付けられた値を QoS グループ値としてコピーすることです。たとえば、**set qos-group precedence** コマンドを入力する場合、優先順位値（パケットマーキング カテゴリ）がコピーされ、QoS グループ値として使用されます。

wlanuser-priority *wlan-user-priority*	分類されたトラフィックにWLANユーザプライオリティを割り当てます。次の値を指定できます。 • *wlan-user-priority*：分類されたトラフィックにWLANユーザプライオリティを設定します。指定できる範囲は 0 ～ 7 です。 • **cos**：レイヤ2 CoSフィールド値をWLANユーザ プライオリティとして設定します。 • **dscp**：DSCP フィールド値を WLAN ユーザ プライオリティとして設定します。 • **precedence**：precedence フィールド値を WLAN ユーザ プライオリティとして設定します。 • **wlan**WLAN ユーザ プライオリティ フィールド値をWLANユーザプライオリティとして設定します。 • （任意）**table** *table-map-name*：WLANユーザプライオリティ値の設定に使用される指定されたテーブル マップに設定されている値を示します。値の指定に使用されるテーブル マップの名前を入力します。テーブル マップ名には、最大 64 の英数字を使用できます。 パケットマーキング カテゴリを指定したが、テーブルマップを指定していない場合、デフォルトアクションは、パケットマーキング カテゴリに関連付けられた値をWLANユーザプライオリティとしてコピーすることです。たとえば、**set wlan user-priority cos** コマンドを入力する場合、CoS 値（パケットマーキング カテゴリ）がコピーされ、WLANユーザプライオリティとして使用されます。

コマンド デフォルト

トラフィックの分類は定義されていません。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**cos**、**dscp**、**qos-group**、**wlantable** *table-map-name* の各キーワードが追加されました。

使用上のガイドライン

set dscp *dscp-value* コマンド、**set cos** *cos-value* コマンド、および **set ip precedence** *precedence-value* コマンドでは、一般的に使用される値にニーモニック名を入力できます。たとえば、**set dscp af11** コマンドを入力できます。これは **set dscp 10** コマンドの入力と同じです。**set ip precedence critical** コマンドを入力できます。これは **set ip precedence 5** コマンドの入力と同じです。サポートされているニーモニック名について、コマンドラインのヘルプ ストリングを表示するには、**set dscp ?** コマンドまたは **set ip precedence ?** コマンドを入力します。

set dscp cos コマンドを設定する場合は、CoS 値が 3 ビット フィールドで、DSCP 値は 6 ビット フィールドであり、CoS フィールドの 3 ビットのみが使用される点に注意してください。

set dscp qos-group コマンドを設定する場合は、次の点に注意してください。

- DSCP 値の有効な範囲は 0 ～ 63 の数字です。QoS グループの有効値の範囲は 0 ～ 99 です。
- QoS グループの値が両方の値の範囲内の場合（たとえば、44）、パケットマーキング値がコピーされ、パケットがマーク付けされます。
- QoS グループの値が DSCP の範囲を超える場合（たとえば、77）、パケットマーキング値はコピーされず、パケットはマーク付けされません。アクションは実行されません。

ポリシー マップ コンフィギュレーション モードでサービス ポリシーを作成し、インターフェイスまたは ATM 仮想回線（VC）にサービス ポリシーを付加するまで、**set qos-group** コマンドは適用できません。

ポリシーマップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

例

次の例では、ポリサーが設定されていないすべての FTP トラフィックに DSCP 値 10 を割り当てる方法を示します。

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class-map ftp_class
Switch(config-cmap)# exit
Switch(config)# policy policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap)# exit
```

設定を確認するには、**show policy-map** 特権 EXEC コマンドを入力します。

関連トピック

class （615 ページ）
policy-map （625 ページ）
show policy-map （656 ページ）

show ap name service-policy

特定の Cisco Lightweight アクセス ポイントのサービス ポリシー情報を表示するには、**show ap name service-policy** コマンドを使用します。

show ap name *ap-name* **service-policy**

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、特定の Cisco Lightweight アクセス ポイントのサービス ポリシー情報を表示する方法を示します。

```
Switch# show ap name 3502b service-policy

NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 3502I  ,  VID: V01,  SN: FTX1525E94A


NAME: Dot11Radio0    , DESCR: 802.11N 2.4GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA


NAME: Dot11Radio1    , DESCR: 802.11N 5GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA
```

show ap name dot11

特定の Cisco Lightweight アクセス ポイントに対応する 802.11a または 802.11b 設定情報を表示するには、**show ap name dot11** コマンドを使用します。

show ap name *ap-name* **dot11** {**24ghz**|**5ghz**} {**ccx**|**cdp**|**profile**|**service-poicy output**|**stats**|**tsm** {**all**|*client-mac*}}

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。
ccx	Cisco Client eXtensions（CCX）無線管理ステータス情報を表示します。
cdp	シスコ検出プロトコル（CDP）情報を表示します。
profile	802.11 プロファイルの設定と統計情報を表示します。
service-policyoutput	ダウンストリームのサービス ポリシー情報を表示します。
stats	Cisco Lightweight アクセス ポイントの統計情報を表示します。
tsm	802.11 トラフィック ストリーム メトリックの統計情報を表示します。
all	クライアントがアソシエーションを持つすべてのアクセス ポイントのリストを表示します。
client-mac	クライアントの MAC アドレス。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、アクセス ポイントに関連付けられたサービス ポリシーを表示する方法を示します。

```
Switch# show ap name test-ap dot11 24ghz service-policy output

Policy Name  : test-ap1
Policy State : Installed
```

次の例では、特定のアクセス ポイントの CCX RRM 802.11 の設定を表示する例を示します。

```
Switch# show ap name AP01 dot11 24ghz ccx
```

次の例では、特定のアクセス ポイントの CDP 情報を表示する方法を示します。

```
Switch# show ap name AP01 dot11 24ghz cdp

AP Name               AP CDP State
--------------------- --------------
AP03                  Disabled
```

次の例では、特定のアクセス ポイントの 802.11b プロファイルの設定と統計情報を表示する方法を示します。

```
Switch# show ap name AP01 dot11 24ghz profile

 802.11b Cisco AP performance profile mode             : GLOBAL
 802.11b Cisco AP Interference threshold               : 10 %
 802.11b Cisco AP noise threshold                      : -70 dBm
 802.11b Cisco AP RF utilization threshold             : 80 %
 802.11b Cisco AP throughput threshold                 : 1000000 bps
 802.11b Cisco AP clients threshold                    : 12 clients
```

次の例では、特定のアクセスポイントのダウンストリームのサービス ポリシー情報を表示する方法を示します。

```
Switch# show ap name AP01 dot11 24ghz service-policy output

Policy Name  : def-11gn
Policy State : Installed
```

次の例では、特定のアクセス ポイントの統計情報を表示する方法を示します。

```
Switch# show ap name AP01 dot11 24ghz stats

Number of Users................................: 0
TxFragmentCount................................: 0
MulticastTxFrameCnt............................: 0
FailedCount....................................: 0
RetryCount.....................................: 0
MultipleRetryCount.............................: 0
FrameDuplicateCount............................: 0
RtsSuccessCount................................: 0
RtsFailureCount................................: 0
AckFailureCount................................: 0
RxIncompleteFragment...........................: 0
MulticastRxFrameCnt............................: 0
FcsErrorCount..................................: 0
TxFrameCount...................................: 0
WepUndecryptableCount..........................: 0
TxFramesDropped................................: 0

Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw).....: 0
  Video Bandwidth in use(% of config bw).....: 0
  Total BW in use for Voice(%)...............: 0
  Total BW in use for SIP Preferred call(%)......: 0
```

```
Load based Voice Call Stats
  Total channel MT free.......................: 0
  Total voice MT free.........................: 0
  Na Direct...................................: 0
  Na Roam.....................................: 0

WMM TSPEC CAC Call Stats
  Total num of voice calls in progress........: 0
  Num of roaming voice calls in progress......: 0
  Total Num of voice calls since AP joined....: 0
  Total Num of roaming calls since AP joined..: 0
  Total Num of exp bw requests received.......: 0
  Total Num of exp bw requests admitted.......: 0
  Num of voice calls rejected since AP joined.: 0
  Num of roam calls rejected since AP joined..: 0
  Num of calls rejected due to insufficent bw.: 0
  Num of calls rejected due to invalid params.: 0
  Num of calls rejected due to PHY rate.......: 0
  Num of calls rejected due to QoS policy.....: 0

SIP CAC Call Stats
  Total Num of calls in progress..............: 0
  Num of roaming calls in progress............: 0
  Total Num of calls since AP joined..........: 0
  Total Num of roaming calls since AP joined..: 0
  Total Num of Preferred calls received.......: 0
  Total Num of Preferred calls accepted.......: 0
  Total Num of ongoing Preferred calls........: 0
  Total Num of calls rejected(Insuff BW)......: 0
  Total Num of roam calls rejected(Insuff BW).: 0

Band Select Stats
  Num of dual band client ....................: 0
  Num of dual band client added...............: 0
  Num of dual band client expired ............: 0
  Num of dual band client replaced............: 0
  Num of dual band client detected ...........: 0
  Num of suppressed client ...................: 0
  Num of suppressed client expired............: 0
  Num of suppressed client replaced...........: 0
```

次の例では、特定のアクセス ポイントに対応するすべてのクライアントのトラフィック ストリームの設定を表示する方法を示します。

```
Switch# show ap name AP01 dot11 24ghz tsm all
```

show class-map

トラフィックを分類するための一致基準を定義するサービス品質（QoS）クラスマップを表示するには、**show class-map** コマンドを EXEC モードで使用します。

show class-map [*class-map-name* | **type control subscriber** {**all** | *class-map-name*}]

構文の説明

class-map-name	（任意）クラス マップ名。
type control subscriber	（任意）コントロール クラス マップに関する情報を表示します。
all	（任意）すべてのコントロール クラス マップに関する情報を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

例

次の例では、**show class-map** コマンドの出力を示します。

```
Switch# show class-map
 Class Map match-any videowizard_10-10-10-10 (id 2)
   Match access-group name videowizard_10-10-10-10

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-any dscp5 (id 3)
   Match ip dscp 5
```

関連トピック

class-map （618 ページ）

show wireless client calls

スイッチのアクティブなコールまたは拒否されたコールの合計数を表示するには、特権EXECモードで **show wireless client calls** コマンドを使用します。

show wireless client calls {**active** | **rejected**}

構文の説明

active	アクティブなコールが表示されます。
rejected	拒否されたコールが表示されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless client calls** コマンドの出力例を示します。

```
スイッチ# show wireless client calls active

TSPEC Calls:

------------------------------------------------------------------------------
MAC Address     AP Name             Status               WLAN  Authenticated
------------------------------------------------------------------------------
0000.1515.000f    AP-2           Associated             1  Yes

SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a and 802.11b/g: 1
Number of Active SIP calls on 802.11a and 802.11b/g: 0
```

show wireless client dot11

特定の帯域（2.4 Ghz または 5 Ghz）のアクティブなコールまたは拒否されたコールの合計数を表示するには、特権 EXEC モードで **show wireless client dot11** コマンドを使用します。

show wireless client dot11 {**24ghz** | **5ghz**} **calls** {**active** | **rejected**}

構文の説明

24ghz	802.11b/g ネットワークを表示します。
5ghz	802.11a ネットワークを表示します。
calls	ワイヤレスクライアントのコールを表示します。
active	アクティブなコールが表示されます。
rejected	拒否されたコールが表示されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless client dot11** コマンドの出力例を示します。

```
Switch# show wireless client dot11 5ghz calls active

 TSPEC Calls:
------------------


SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a: 0
Number of Active SIP calls on 802.11a: 0
```

show wireless client mac-address（コール制御）

クライアントに関連するコール制御情報を表示するには、特権 EXEC モードで **show wireless client mac-address** コマンドを使用します。

show wireless client mac-address *mac-address* **call-control call-info**

構文の説明

mac-address	クライアントの MAC アドレス。
call-controlcall-info	クライアントに関するコール制御と IP 関連の情報を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、クライアントに関するコール制御および IP に関する情報を表示する方法を示します。

```
Switch# show wireless client mac-address  30e4.db41.6157 call-control call-info
Client MAC Address        : 30E4DB416157

Call 1 Statistics

Uplink IP Address         : 209.165.200.225
Downlink IP Address       : 209.165.200.226
Uplink Port               : 29052
Downlink Port             : 27538
Call ID                   : c40acb4d-3b3b0.3d27da1e-356bed03
Called Party              : sip:1011
Calling Party             : sip:1012
Priority                  : 6
Call On Hold              : false
Call Duration             : 30

Call 2 Statistics

No Active Call
```

show wireless client mac-address（TCLAS）

TCLAS およびユーザ プライオリティに関する情報を表示するには、特権 EXEC モードで **showwirelessclientmac-address** コマンドを使用します。

show wireless client mac-address *mac-address* **tclas**

構文の説明

mac-address	クライアントの MAC アドレス。
tclas	TCLAS およびクライアントに関するユーザ プライオリティ関連の情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

この例は、クライアントの TCLAS およびユーザ プライオリティ関連の情報を表示する方法を示しています。

```
Switch# show wireless client mac-address 30e4.db41.6157 tclas
MAC Address      UP TID Mask Source IP Addr  Dest IP Addr    SrcPort DstPort Proto
-------------------------------------------------------------------------------
30e4.db41.6157    4   4   95 167838052       2164326668      5060     5060      6
30e4.db41.6157    6   1   31 0               2164326668      0        27538    17
```

show wireless client voice diagnostics

ワイヤレス クライアントの音声診断パラメータを表示するには、特権 EXEC モードで **show wireless client voice diagnostics** コマンドを使用します。

show wireless client voice diagnostics {**qos-map** | **roam-history** | **rssi** | **status** | **tspec**}

構文の説明

qos-map	QoSおよびDSCPマッピングに関する情報と4つのキュー（VO、VI、BE、BK）それぞれのパケット統計を表示します。各種 DSCP 値も表示されます。
roam-history	既知の各クライアントの直前の 3 つのローミング履歴に関する情報を表示します。出力にはタイムスタンプ、ローミングに関連するアクセス ポイント、ローミングの理由が含まれ、ローミングに失敗した場合には失敗の理由も含まれます。
rssi	音声診断がイネーブルである場合に、直前の 5 秒間のクライアントの RSSI 値を表示します。
status	クライアントの音声診断の状態を表示します。
tspec	TSPEC クライアントに対して有効になっている音声診断を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

デバッグ音声診断は、音声診断を実行するにはイネーブルにする必要があります。

次に、**show wireless client voice diagnostics status** コマンドの出力例を示します。

```
Switch# show wireless client voice diagnostics status
Voice Diagnostics Status: FALSE
```

show policy-map

着信トラフィックの分類基準を定義するサービス品質（QoS）のポリシーマップを表示するには、EXEC モードで **show policy-map** コマンドを使用します。

show policy-map [{*policy-map-name*|**interface** *interface-id*}]

show policy-map interface {**Auto-template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Lspvif** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan** | **brief** | **class** | **input** | **output**

show policy-map type control subscriber detail

show policy-map interface wireless {**ap name** *ap_name* | **client mac** *mac_address* | **radio type** {**24ghz** | **5ghz**} **ap name***ap_name* | **ssid name** *ssid_name*{**ap name** *ap_name* | **radio type** {**24ghz** | **5ghz**} **ap name***ap_name*}}

構文の説明

policy-map-name	（任意）ポリシーマップの名前。
interface *interface-id*	（任意）インターフェイスに適用された入力ポリシーと出力ポリシーの統計情報と設定を表示します。
type control subscriber detail	（任意）QoS ポリシーのタイプと統計情報を特定します。
ap name *ap_name*	アクセス ポイントの SSID ポリシー設定を表示します。
client mac *mac_address*	すべてのクライアントターゲットのポリシーに関する情報を表示します。
radio type {**24ghz**	**5ghz**	指定された無線タイプのアクセスポイントのポリシー設定を表示します。
ssid name *ssid_name*	SSID のポリシー設定を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	The **interface** *interface-id* keyword was added.

使用上のガイドライン

ポリシーマップには、帯域幅制限および制限を超過した場合の対処法を指定するポリサーを格納できます。

（注） **control-plane**、**session**、および **type** キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。表示されている統計情報は無視してください。

TCAM（Ternary Content Addressable Memory）（マーキングまたはポリシング）の分類カウンタを表示するには、インターフェイス ID を入力します。分類カウンタには次の制限事項があります。

- フィルタベースの分類カウンタはサポートされません。
- 分類カウンタは有線ポートでのみサポートされます（イングレスとイーグレス方向）。
- 分類カウンタは、バイトの代わりにパケットをカウントします。
- マーキングまたはポリシングによる QoS 設定だけが、分類カウンタをトリガーします。
- ポリシー内にポリシングまたはマーキング アクションがある限り、クラス デフォルトは分類カウンタを保持します。
- 分類カウンタはポート ベースではありません。カウンタは同じポリシー マップを共有するターゲット間で共有されます。これは、分類カウンタが、異なるインターフェイスに接続し、同じポリシーの同じクラスに属するすべてのパケットを集約することを意味します。

次に、分類カウンタが表示されている **show policy-map interface** コマンドの出力例を示します。

```
Switch# show policy-map interface gigabitethernet1/0/1

  GigabitEthernet1/0/1

  Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

    Class-map: AutoQos-4.0-Voip-Data-CiscoPhone-Class (match-any)
      0 packets
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp ef
      police:
          cir 128000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Voip-Signal-CiscoPhone-Class (match-any)
      0 packets
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp cs3
      police:
```

```
        cir 32000 bps, bc 8000 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
      conformed 0000 bps, exceed 0000 bps

  Class-map: AutoQos-4.0-Default-Class (match-any)
    0 packets
    Match: access-group name AutoQos-4.0-Acl-Default
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp default

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
    0 packets
```

```
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
```

```
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

関連トピック

policy-map （625 ページ）

show wlan

WLAN パラメータを表示するには、**show wlan** コマンドを使用します。

show wlan {**all** |**id** *wlan-id*|**name** *wlan-name* |**summary**}

構文の説明

all	すべての設定済み WLAN のパラメータのサマリーを表示します。リストは WLAN ID の昇順に表示されます。
id *wlan-id*	無線 LAN の識別子を指定します。範囲は 1 ～ 512 です。
name *wlan-name*	WLAN プロファイル名を指定します。名前は 1 ～ 32 文字です。
summary	WLAN に設定されているパラメータのサマリーを表示します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、デバイスに設定されている WLAN のサマリーを表示する例を示します。

```
Switch# show wlan summary
Number of WLANs: 1

WLAN Profile Name                     SSID                           VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                        test-wlan-ssid                  1    UP
```

次に、特定の WLAN に設定されているパラメータのサマリーを表示する例を示します。

```
Switch# show wlan name test-wlan
WLAN Identifier                                 : 45
Profile Name                                    : test-wlan
Network Name (SSID)                             : test-wlan-ssid
Status                                          : Enabled
Broadcast SSID                                  : Enabled
Maximum number of Associated Clients            : 0
AAA Policy Override                             : Disabled
Network Admission Control
  NAC-State                                     : Disabled
Number of Active Clients                        : 0
Exclusionlist Timeout                           : 60
Session Timeout                                 : 1800 seconds
```

```
CHD per WLAN                                    : Enabled
Webauth DHCP exclusion                          : Disabled
Interface                                       : default
Interface Status                                : Up
Multicast Interface                             : test
WLAN IPv4 ACL                                   : test
WLAN IPv6 ACL                                   : unconfigured
DHCP Server                                     : Default
DHCP Address Assignment Required                : Disabled
DHCP Option 82                                  : Disabled
DHCP Option 82 Format                           : ap-mac
DHCP Option 82 Ascii Mode                       : Disabled
DHCP Option 82 Rid Mode                         : Disabled
QoS Service Policy - Input
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Service Policy - Output
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Client Service Policy
  Input  Policy Name                            : unknown
  Output Policy Name                            : unknown
WifiDirect                                      : Disabled
WMM                                             : Disabled
Channel Scan Defer Priority:
  Priority (default)                            : 4
  Priority (default)                            : 5
  Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Enabled
CCX - Gratuitous ProbeResponse (GPR)            : Disabled
CCX - Diagnostics Channel Capability            : Disabled
Dot11-Phone Mode (7920)                         : Invalid
Wired Protocol                                  : None
Peer-to-Peer Blocking Action                    : Disabled
Radio Policy                                    : All
DTIM period for 802.11a radio                   : 1
DTIM period for 802.11b radio                   : 1
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : Disabled
Accounting list name                            : Disabled
802.1x authentication list name                 : Disabled
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    802.1X                                      : Disabled
    Wi-Fi Protected Access (WPA/WPA2)           : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Enabled
            TKIP Cipher                         : Disabled
            AES Cipher                          : Enabled
        Auth Key Management
            802.1x                              : Enabled
            PSK                                 : Disabled
            CCKM                                : Disabled
    IP Security                                 : Disabled
    IP Security Passthru                        : Disabled
    L2TP                                        : Disabled
    Web Based Authentication                    : Disabled
    Conditional Web Redirect                    : Disabled
    Splash-Page Web Redirect                    : Disabled
    Auto Anchor                                 : Disabled
    Sticky Anchoring                            : Enabled
```

```
    Cranite Passthru                              : Disabled
    Fortress Passthru                             : Disabled
    PPTP                                          : Disabled
    Infrastructure MFP protection                 : Enabled
    Client MFP                                    : Optional
    Webauth On-mac-filter Failure                 : Disabled
    Webauth Authentication List Name              : Disabled
    Webauth Parameter Map                         : Disabled
    Tkip MIC Countermeasure Hold-down Timer       : 60
Call Snooping                                     : Disabled
Passive Client                                    : Disabled
Non Cisco WGB                                     : Disabled
Band Select                                       : Disabled
Load Balancing                                    : Disabled
IP Source Guard                                   : Disabled
Netflow Monitor                                   : test
        Direction                                 : Input
        Traffic                                   : Datalink

Mobility Anchor List
IP Address
-----------
```

trust device

インターフェイスに接続されているサポートデバイスに対する信頼を設定するには、インターフェイス コンフィギュレーション モードで **trust device** コマンドを使用します。接続デバイスに対する信頼を無効にするには、このコマンドの **no** 形式を使用します。

trust device {**cisco-phone** | **cts** | **ip-camera** | **media-player**}
no trust device {**cisco-phone** | **cts** | **ip-camera** | **media-player**}

構文の説明

cisco-phone	Cisco IP Phone を設定します。
cts	Cisco TelePresence System を設定します。
ip-camera	Video Surveillance IP カメラ（IPVSC）を設定します。
media-player	Cisco Digital Media Player（DMP）を設定します。

コマンド デフォルト

信頼はディセーブルに設定

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

trust device コマンドは、次のタイプのインターフェイスに使用します。

- **Auto**：自動テンプレート インターフェイス
- **Capwap**：Capwap トンネル インターフェイス
- **GigabitEthernet**：Gigabit Ethernet IEEE 802
- **GroupVI**：グループ仮想インターフェイス
- **Internal Interface**：内部インターフェイス
- **Loopback**：ループバック インターフェイス
- **Null**：ヌル インターフェイス
- **Port-channel**：イーサネット チャネル インターフェイス
- **TenGigabitEthernet**：10 ギガビット イーサネット
- **Tunnel**：トンネル インターフェイス
- **Vlan**：Catalyst VLAN
- **range**：**interface range** コマンド

例

次に、インターフェイス GigabitEthernet 1/0/1 で Cisco IP Phone の信頼を設定する例を示します。

```
Switch(config)# interface GigabitEthernet1/0/1
Switch(config-if)# trust device cisco-phone
```

設定を確認するには、**show interface status** 特権 EXEC コマンドを入力します。

Auto-QoS コマンド

この章では、次の auto-QoS コマンドについて説明します。

auto qos classify

QoS ドメイン内で信頼できないデバイスの Quality of Service（QoS）の分類を自動的に設定するには、インターフェイス コンフィギュレーション モードで **auto qos classify** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

auto qos classify [police]
no auto qos classify [police]

構文の説明

police	（任意）信頼できないデバイスの QoS ポリシングを設定します。

コマンド デフォルト

auto-QoS 分類は、すべてのポートでディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

QoS ドメイン内の信頼インターフェイスに QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、スイッチ、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジ デバイスなどが含まれます。

auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力/出力キューの設定を行います。

表 *18 :* 出力キューに対する *auto-QoS* の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キュー ウェイト（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
プライオリティ（シェイプド）	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

auto-QoS は、スイッチが信頼インターフェイスと接続するように設定します。着信パケットの QoS ラベルは信頼されます。非ルーテッド ポートの場合は、着信パケットの CoS 値が信頼されます。ルーテッド ポートでは、着信パケットの DSCP 値が信頼されます。

auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。auto-QoS をイネーブルにした後で、auto-QoS を調整できます。

（注） スイッチは、コマンドラインインターフェイス（CLI）からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシー マップや集約ポリサーを変更しないでください。ポリシーマップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシー マップやポリサーを変更します。生成されたポリシー マップの代わりに新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除して、新しいポリシー マップを適用します。

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。**debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッギングがイネーブルになります。

auto qos classify コマンドおよび **auto qos classify police** コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシーマップ（**auto qos classify police** コマンドの場合）：

- AutoQos-4.0-Classify-Police-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ：

- AutoQos-4.0-Multimedia-Conf-Class（match-any）
- AutoQos-4.0-Bulk-Data-Class（match-any）
- AutoQos-4.0-Transaction-Class（match-any）
- AutoQos-4.0-Scavanger-Class（match-any）
- AutoQos-4.0-Signaling-Class（match-any）
- AutoQos-4.0-Default-Class（match-any）
- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）

- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

ポートの auto-QoS を無効にするには、**no auto qos classify** インターフェイス コンフィギュレーション コマンドを使用します。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS を有効にした最後のポートで、**no auto qos classify** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS は無効と見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

例

次の例では、信頼できないデバイスの auto-QoS 分類をイネーブルにし、トラフィックをポリシングする方法を示します。

```
Switch(config)# interface gigabitEthernet1/0/6
Switch(config-if)# auto qos classify police
Switch(config-if)# end
Switch# show policy-map interface gigabitEthernet1/0/6

GigabitEthernet1/0/6

  Service-policy input: AutoQos-4.0-Classify-Police-Input-Policy

    Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp af41
      police:
          cir 5000000 bps, bc 156250 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-Bulk-Data
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp af11
      police:
          cir 10000000 bps, bc 312500 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
```

```
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Transaction-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Transactional-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af21
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Scavanger-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Scavanger
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs1
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Signaling-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Signaling
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
      cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Default
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp default
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: class-default (match-any)
```

```
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
    0 packets
    Match:  dscp af41 (34) af42 (36) af43 (38)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  4
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
    0 packets
    Match:  dscp af21 (18) af22 (20) af23 (22)
```

```
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

設定を確認するには、**show auto qos interface** *interface-id* 特権 EXEC コマンドを入力します。

auto qos trust

QoS ドメイン内の信頼インターフェイスのサービス品質（QoS）を自動的に設定するには、インターフェイス コンフィギュレーション モードで **auto qos trust** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

auto qos trust {**cos**|**dscp**}
no auto qos trust {**cos**|**dscp**}

構文の説明

cos	CoS パケット分類を信頼します。
dscp	DSCP パケット分類を信頼します。

コマンド デフォルト

auto-QoS 信頼は、すべてのポートでディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

QoS ドメイン内の信頼インターフェイスに QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、スイッチ、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジ デバイスなどが含まれます。auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力/出力キューの設定を行います。

表 *19:* トラフィック タイプ、パケット ラベル、およびキュー

	VoIP データ トラフィック	VOIP コントロール トラフィック	ルーティング プロトコル トラフィック	STP[5] BPDU[6] トラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラフィック	
DSCP[7]	46	24、26	48	56	34	–	
CoS[8]	5	3	6	7	3	–	
CoS から出力キューへのマッピング	4、5（キュー 1）	2、3、6、7（キュー 2）			0（キュー 3）	2（キュー 3）	0、1（キュー 4）

[5] STP = スパニング ツリー プロトコル
[6] BPDU = ブリッジ プロトコル データ ユニット
[7] DSCP = DiffServ コード ポイント

[8] CoS = サービス クラス

表 *20 :* 出力キューに対する *auto-QoS* の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キュー ウェイト（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
プライオリティ（シェイプド）	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

（注） スイッチは、コマンドライン インターフェイス（CLI）からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシー マップや集約ポリサーを変更しないでください。ポリシーマップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシー マップやポリサーを変更します。生成されたポリシー マップの代わりに新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除して、新しいポリシー マップを適用します。

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。**debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッギングがイネーブルになります。

auto qos trust cos コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ：

- class-default（match-any）

- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos trust dscp コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ：

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

ポートの auto-QoS をディセーブルにするには、**no auto qos trust** インターフェイス コンフィギュレーション コマンドを使用します。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos trust** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

例

次に、特定の CoS 分類を持つ信頼できるインターフェイスの auto-QoS を有効にする方法を示します。

```
Switch(config)# interface gigabitEthernet1/0/17
Switch(config-if)# auto qos trust cos
Switch(config-if)# end
Switch# show policy-map interface GigabitEthernet1/0/17

GigabitEthernet1/0/17

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
```

```
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      cos cos table AutoQos-4.0-Trust-Cos-Table

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
    0 packets
    Match:  dscp af41 (34) af42 (36) af43 (38)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  4
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
    0 packets
    Match:  dscp af21 (18) af22 (20) af23 (22)
```

```
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

次に、特定の DSCP 分類を持つ信頼できるインターフェイスの auto-QoS を有効にする方法を示します。

```
Switch(config)# interface GigabitEthernet1/0/18
Switch(config-if)# auto qos trust dscp
Switch(config-if)# end
Switch#show policy-map interface GigabitEthernet1/0/18

GigabitEthernet1/0/18

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

    Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
      0 packets
      Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue-limit dscp 16 percent 80
      queue-limit dscp 24 percent 90
      queue-limit dscp 48 percent 100
      queue-limit dscp 56 percent 100

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 10%

      queue-buffers ratio 10

    Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
      0 packets
```

```
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
```

```
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

設定を確認するには、**show auto qos interface** *interface-id* 特権 EXEC コマンドを入力します。

auto qos video

QoS ドメイン内のビデオのサービス品質（QoS）を自動的に設定するには、インターフェイス コンフィギュレーション モードで **auto qos video** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

auto qos video {**cts** | **ip-camera** | **media-player**}
no auto qos video {**cts** | **ip-camera** | **media-player**}

構文の説明

cts	Cisco TelePresence System に接続されるポートを指定し、自動的にビデオの QoS を設定します。
ip-camera	Cisco IP カメラに接続されるポートを指定し、自動的にビデオの QoS を設定します。
media-player	Cisco Digital Media Player に接続されるポートを指定し、自動的にビデオの QoS を設定します。

コマンド デフォルト

Auto-QoS ビデオは、ポート上でディセーブルに設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

QoS ドメイン内のビデオ トラフィックに適切な QoS を設定するには、このコマンドを使用します。QoS ドメインには、スイッチ、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジデバイスなどが含まれます。auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力/出力キューの設定を行います。詳細については、この項の最後にあるキューテーブルを参照してください。

auto-QoS は、Cisco TelePresence システム、Cisco IP カメラ、または Cisco Digital Media Player へのビデオ接続用にスイッチを設定します。

auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。auto-QoS をイネーブルにした後で、auto-QoS を調整できます。

スイッチは、コマンドライン インターフェイス（CLI）からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリ

に保存せずに、スイッチをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

これが auto-QoS をイネーブルにする最初のポートの場合は、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドに続いてインターフェイス コンフィギュレーション コマンドが実行されます。別のポートで auto-QoS をイネーブルにすると、そのポートに対して auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが実行されます。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシー マップや集約ポリサーを変更しないでください。ポリシーマップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシー マップやポリサーを変更します。生成されたポリシー マップの代わりに新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除して、新しいポリシー マップを適用します。

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。**debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッギングがイネーブルになります。

auto qos video cts コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos video ip-camera コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ：

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos video media-player コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ：

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

ポートの auto-QoS をディセーブルにするには、**no auto qos video** インターフェイス コンフィギュレーション コマンドを使用します。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS を有効にした最後のポートで、**no auto qos video** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS は無効と見なされます（グローバルコンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

表 *21 :* トラフィック タイプ、パケット ラベル、およびキュー

	VoIP データ トラフィック	VOIP コントロール トラフィック	ルーティング プロトコル トラフィック	STP[9] BPDU[10] トラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラフィック	
DSCP[11]	46	24、26	48	56	34	–	
CoS[12]	5	3	6	7	3	–	
CoS から出力キューへのマッピング	4、5（キュー 1）	2、3、6、7（キュー 2）	2、3、6、7（キュー 2）	2、3、6、7（キュー 2）	0（キュー 3）	2（キュー 3）	0、1（キュー 4）

[9] STP = スパニング ツリー プロトコル
[10] BPDU = ブリッジ プロトコル データ ユニット
[11] DSCP = DiffServ コード ポイント
[12] CoS = サービス クラス

表 *22 :* 出力キューに対する *auto-QoS* の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キュー ウェイト（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
プライオリティ（シェイプド）	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

例

次に、**auto qos video cts** コマンドと、適用されるポリシーとクラス マップの例を示します。

```
Switch(config)# interface gigabitEthernet1/0/12
Switch(config-if)# auto qos video cts
Switch(config-if)# end
Switch# show policy-map interface gigabitEthernet1/0/12

GigabitEthernet1/0/12
```

```
Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      cos cos table AutoQos-4.0-Trust-Cos-Table

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
    0 packets
    Match:  dscp af41 (34) af42 (36) af43 (38)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  4
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
```

```
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
```

```
    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

次に、**auto qos video ip-camera** コマンドと、適用されるポリシーとクラス マップの例を示します。

```
Switch(config)# interface GigabitEthernet1/0/9
Switch(config-if)# auto qos video ip-camera
Switch(config-if)# end
Switch# show policy-map interface GigabitEthernet1/0/9

GigabitEthernet1/0/9

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

    Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
      0 packets
      Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue-limit dscp 16 percent 80
      queue-limit dscp 24 percent 90
      queue-limit dscp 48 percent 100
      queue-limit dscp 56 percent 100

      (total drops) 0
```

```
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
```

```
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

次の例は、**auto qos video media-player** コマンドと、適用されるポリシーとクラス マップを示しています。

```
Switch(config)# interface GigabitEthernet1/0/7
Switch(config-if)# auto qos video media-player
Switch(config-if)# end
Switch# show policy-map interface GigabitEthernet1/0/7

GigabitEthernet1/0/7

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,
```

```
  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
```

```
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

設定を確認するには、**show auto qos video interface** *interface-id* 特権 EXEC コマンドを入力します。

auto qos voip

QoS ドメイン内の Voice over IP（VoIP）の Quality of Service（QoS）を自動的に設定するには、インターフェイス コンフィギュレーション モードで **auto qos voip** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

auto qos voip {**cisco-phone** | **cisco-softphone** | **trust**}
no auto qos voip {**cisco-phone** | **cisco-softphone** | **trust**}

構文の説明

cisco-phone	Cisco IP Phone に接続されるポートを指定し、自動的にビデオの VoIP を設定します。着信パケットの QoS ラベルが信頼されるのは、IP Phone が検知される場合に限ります。
cisco-softphone	Cisco SoftPhone が動作している装置に接続されるポートを指定し、自動的にビデオの VoIP を設定します。
trust	信頼できるスイッチに接続されるポートを指定し、自動的にビデオの VoIP を設定します。着信パケットの QoS ラベルは信頼されます。非ルーテッド ポートの場合は、着信パケットの CoS 値が信頼されます。ルーテッドポートでは、着信パケットの DSCP 値が信頼されます。

コマンド デフォルト

auto-QoS は、すべてのポートでディセーブルです。

auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力/出力キューの設定を行います。

コマンド デフォルト

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

QoS ドメイン内の VoIP トラフィックに適切な QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、スイッチ、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジ デバイスなどが含まれます。

Auto-QoS は、スイッチとルーテッド ポート上の Cisco IP Phone を使用した VoIP と、Cisco SoftPhone アプリケーションが動作する装置に対してスイッチを設定します。これらのリリースは Cisco IP SoftPhone バージョン 1.3(3)以降だけをサポートします。接続される装置は Cisco Call Manager バージョン 4 以降を使用する必要があります。

auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。auto-QoS をイネーブルにした後で、auto-QoS を調整できます。

（注） スイッチは、コマンドライン インターフェイス（CLI）からコマンドが入力された場合と同じように、auto-QoSによって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、スイッチをリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

これが auto-QoS をイネーブルにする最初のポートの場合は、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドに続いてインターフェイス コンフィギュレーション コマンドが実行されます。別のポートで auto-QoS をイネーブルにすると、そのポートに対して auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが実行されます。

Cisco IP Phone に接続されたネットワーク エッジのポートで **auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力すると、スイッチにより信頼境界の機能が有効になります。スイッチは、Cisco Discovery Protocol（CDP）を使用して、Cisco IP Phone の存在を検出します。Cisco IP Phone が検出されると、ポートの入力分類は、パケットで受け取ったQoS ラベルを信頼するように設定されます。また、スイッチはポリシングを使用してパケットがプロファイル内か、プロファイル外かを判断し、パケットに対するアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。Cisco IP Phone が存在しない場合、ポートの入力分類は、パケットで受け取った QoS ラベルを信頼しないように設定されます。ポリシングがポリシーマップ分類と一致したトラフィックに適用された後で、スイッチが信頼境界の機能をイネーブルにします。

-
- Cisco SoftPhone が動作するデバイスに接続されたネットワーク エッジにあるポートに **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを入力した場合、スイッチはポリシングを使用してパケットがプロファイル内かプロファイル外かを判断し、パケットに対するアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、スイッチは DSCP 値を 0 に変更します。
- ネットワーク内部に接続されたポート上で **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを入力すると、非ルーテッド ポートの場合は入力パケット内の CoS 値、ルーテッド ポートの場合は入力パケット内の DSCP 値がスイッチで信頼されます（前提条件は、トラフィックがすでに他のエッジデバイスによって分類されていることです）。

スタティック ポート、ダイナミック アクセス ポート、音声 VLAN アクセス ポート、およびトランク ポートで auto-QoS をイネーブルにすることができます。ルーテッド ポートで Cisco IP Phone の自動 QoS を有効にすると、スタティック IP アドレスを IP Phone に割り当てます。

（注） Cisco SoftPhone が稼働するデバイスがスイッチまたはルーテッド ポートに接続されている場合、スイッチはポートごとに 1 つの Cisco SoftPhone アプリケーションだけをサポートします。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシー マップや集約ポリサーを変更しないでください。ポリシーマップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシー マップやポリサーを変更します。生成されたポリシー マップの代わりに新しいポリシー マップを使用するには、生成したポリシー マップをインターフェイスから削除して、新しいポリシー マップを適用します。

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。**debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッギングがイネーブルになります。

auto qos voip trust コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ：

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos voip cisco-softphone コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- AutoQos-4.0-CiscoSoftPhone-Input-Policy
- AutoQos-4.0-Output-Policy

クラス マップ：

- AutoQos-4.0-Voip-Data-Class（match-any）

- AutoQos-4.0-Voip-Signal-Class（match-any）
- AutoQos-4.0-Multimedia-Conf-Class（match-any）
- AutoQos-4.0-Bulk-Data-Class（match-any）
- AutoQos-4.0-Transaction-Class（match-any）
- AutoQos-4.0-Scavanger-Class（match-any）
- AutoQos-4.0-Signaling-Class（match-any）
- AutoQos-4.0-Default-Class（match-any）
- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos voip cisco-phone コマンドを実行する場合、次のポリシーマップおよびクラス マップが作成され、適用されます。

ポリシー マップ：

- service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
- service-policy output AutoQos-4.0-Output-Policy

クラス マップ：

- class AutoQos-4.0-Voip-Data-CiscoPhone-Class
- class AutoQos-4.0-Voip-Signal-CiscoPhone-Class
- class AutoQos-4.0-Default-Class

ポートの auto-QoS をディセーブルにするには、 **no auto qos voip** インターフェイス コンフィギュレーション コマンドを使用します。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos voip** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

スイッチは、このテーブルの設定にしたがってポートの出力キューを設定します。

表 *23 :* 出力キューに対する *auto-QoS* の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キュー ウェイト（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
プライオリティ（シェイプド）	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

例

次に、**auto qos voip trust** コマンドと、適用されるポリシーとクラス マップの例を示します。

```
Switch(config)# interface gigabitEthernet1/0/31
Switch(config-if)# auto qos voip trust
Switch(config-if)# end
Switch# show policy-map interface GigabitEthernet1/0/31

GigabitEthernet1/0/31

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,
```

```
  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
```

```
    (bytes output) 0
    bandwidth remaining 4%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
    0 packets
    Match:  dscp cs1 (8)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
    0 packets
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

次に、**auto qos voip cisco-phone** コマンドと、適用されるポリシーとクラス マップの例を示します。

```
Switch(config)# interface gigabitEthernet1/0/5
Switch(config-if)# auto qos voip cisco-phone
Switch(config-if)# end
Switch# show policy-map interface gigabitEthernet1/0/5

GigabitEthernet1/0/5

  Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

    Class-map: AutoQos-4.0-Voip-Data-CiscoPhone-Class (match-any)
      0 packets
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp ef
      police:
          cir 128000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
```

```
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

  Class-map: AutoQos-4.0-Voip-Signal-CiscoPhone-Class (match-any)
    0 packets
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp cs3
    police:
        cir 32000 bps, bc 8000 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
      conformed 0000 bps, exceed 0000 bps

  Class-map: AutoQos-4.0-Default-Class (match-any)
    0 packets
    Match: access-group name AutoQos-4.0-Acl-Default
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp default

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
```

```
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
```

```
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
    0 packets
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

次に、**auto qos voip cisco-softphone** コマンドと、適用されるポリシーとクラス マップの例を示します。

```
Switch(config)# interface gigabitEthernet1/0/20
Switch(config-if)# auto qos voip cisco-softphone
Switch(config-if)# end
Switch# show policy-map interface gigabitEthernet1/0/20

 GigabitEthernet1/0/20

  Service-policy input: AutoQos-4.0-CiscoSoftPhone-Input-Policy

    Class-map: AutoQos-4.0-Voip-Data-Class (match-any)
      0 packets
      Match:  dscp ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp ef
      police:
          cir 128000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Voip-Signal-Class (match-any)
      0 packets
      Match:  dscp cs3 (24)
        0 packets, 0 bytes
```

```
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
      cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af41
  police:
      cir 5000000 bps, bc 156250 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Bulk-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af11
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Transaction-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Transactional-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af21
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Scavanger-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Scavanger
    0 packets, 0 bytes
    5 minute rate 0 bps
```

```
    QoS Set
      dscp cs1
    police:
        cir 10000000 bps, bc 312500 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        drop
      conformed 0000 bps, exceed 0000 bps

  Class-map: AutoQos-4.0-Signaling-Class (match-any)
    0 packets
    Match: access-group name AutoQos-4.0-Acl-Signaling
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp cs3
    police:
        cir 32000 bps, bc 8000 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        drop
      conformed 0000 bps, exceed 0000 bps

  Class-map: AutoQos-4.0-Default-Class (match-any)
    0 packets
    Match: access-group name AutoQos-4.0-Acl-Default
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp default
    police:
        cir 10000000 bps, bc 312500 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
      conformed 0000 bps, exceed 0000 bps

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,
```

```
  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
```

```
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

設定を確認するには、**show auto qos interface** *interface-id* 特権 EXEC コマンドを入力します。

debug auto qos

Automatic Quality of Service（auto-QoS; 自動 QoS）機能のデバッグをイネーブルにするには、特権 EXEC モードで **debug auto qos** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug auto qos
no debug auto qos

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

auto-QoS デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。デバッグをイネーブルにするには、**debug auto qos** 特権 EXEC コマンドを入力します。

undebug auto qos コマンドは、**no debug auto qos** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合、アクティブスイッチ でのみイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権 EXEC コマンドでアクティブ スイッチからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ スイッチのデバッグをイネーブルにするには、アクティブ スイッチ上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用することもできます。

例

次の例では、auto-QoS がイネーブルの場合に自動的に生成される QoS 設定を表示する方法を示します。

```
Switch# debug auto qos
AutoQoS debugging is on
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# auto qos voip cisco-phone
```

show auto qos

automatic QoS（auto-QoS）が有効になっているインターフェイスに入力された Quality of Service（QoS）コマンドを表示するには、特権 EXEC モードで **show auto qos** コマンドを使用します。

show auto qos [**interface** [*interface-id*]]

構文の説明

interface [*interface-id*]	（任意）指定されたポートまたはすべてのポートの auto-QoS 情報を表示します。有効なインターフェイスには、物理ポートが含まれます。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

show auto qos コマンド出力には、各インターフェイスに入力された **auto qos** コマンドだけが表示されます。**show auto qos interface** *interface-id* コマンド出力には、特定のインターフェイス上に入力された **auto qos** コマンドが表示されます。

auto-QoS 設定およびユーザ変更を表示する場合は、**show running-config** 特権 EXEC コマンドを使用します。

Cisco IOS リリース 12.2(40)SE 以降、**show auto qos** コマンドの出力には、Cisco IP Phone のサービス ポリシー情報が表示されます。

例

次の例では、**auto qos voip cisco-phone** および **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show auto qos** コマンドの出力を示します。

```
Switch# show auto qos
GigabitEthernet2/0/4
auto qos voip cisco-softphone

GigabitEthernet2/0/5
auto qos voip cisco-phone


GigabitEthernet2/0/6
auto qos voip cisco-phone
```

次に、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドが入力された場合の **show auto qos interface** *interface-id* コマンドの出力例を示します。

```
Switch# show auto qos interface gigabitethernet 2/0/5
GigabitEthernet2/0/5
```

```
auto qos voip cisco-phone
```

次に、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドが入力された場合の **show auto qos interface** *interface-id* コマンドの出力例を示します。

```
Switch# show auto qos interface gigabitethernet1/0/2
GigabitEthernet1/0/2
auto qos voip cisco-phone
```

次の例では、auto-QoS がインターフェイスでディセーブルになっている場合の **show auto qos interface** *interface-id* コマンドの出力を示します。

```
Switch# show auto qos interface gigabitethernet3/0/1
AutoQoS is disabled
```

第 IX 部

無線リソース管理

無線リソース管理コマンド

airtime-fairness dot11 mode（apgroup）

AP グループの ATF を設定するには、AP グループ サブモードで **airtime-fairness dot11 mode** コマンドを使用します。AP グループの ATF を無効にするには、このコマンドの **no** 形式を使用します。

airtime-fairness dot11 {**24ghz**|**5ghz**} **mode** {**enforce-policy**|**monitor**}

no airtime-fairness dot11 {**24ghz**|**5ghz**} **mode** {**enforce-policy**|**monitor**}

構文の説明

24ghz	802.11b パラメータを設定します。
5ghz	802.11a パラメータを設定します。
enforce-policy	強制ポリシー モードで Air Time Fairness を設定します。
monitor	モニタ モードで Air Time Fairness を設定します。

コマンド デフォルト

なし

コマンド モード

config apgroup

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、AP グループの ATF を設定する例を示します。

```
Switch#configure terminal
Switchconfig# ap group testap
Switchconfig-apgroup# airtime-fairness dot11 24ghz mode monitor
```

airtime-fairness dot11 optimization（apgroup）

AP グループの ATF 最適化を設定するには、**airtime-fairness dot11 optimization** コマンドを使用します。AP グループの ATF を無効にするには、このコマンドの **no** 形式を使用します。

airtime-fairness dot11 {**24ghz**|**5ghz**} **optimization**

no airtime-fairness dot11 {**24ghz**|**5ghz**} **optimization**

構文の説明

24ghz	802.11b パラメータを設定します。
5ghz	802.11a パラメータを設定します。

コマンド デフォルト

なし

コマンド モード

config apgroup

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、AP グループの ATF 最適化を設定する例を示します。

```
Switch#configure terminal
Switchconfig# ap group testap
Switchconfig-apgroup# airtime-fairness dot11 24ghz optimization
```

airtime-fairness dot11 policy

WLAN AP グループでグローバルに適用されているポリシーをオーバーライドするには、**airtime-fairness dot11 policy** コマンドを使用します。適用されているポリシーのオーバーライドを無効にするには、コマンドの **no** 形式を使用します。

airtime-fairness dot11 {**24ghz**|**5ghz**}**policy** *policy-name*

no airtime-fairness dot11 {**24ghz**|**5ghz**}**policy** *policy-name*

構文の説明

24ghz	2.4 GHz Air Time Fairness ポリシーを設定します。
5ghz	5 GHz Air Time Fairness ポリシーを設定します。
policy-name	割り当てる Air Time Fairness ポリシーの名前。

コマンド デフォルト

なし

コマンド モード

config wlan apgroup

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、WLAN AP グループで適用されているポリシーをオーバーライドする例を示します。

```
Switchconfig#ap group testapgroup
Switch(config-apgroup)# wlan testwlan
Switch(config-wlan-apgroup)# airtime-fairness dot11 24ghz policy testpolicy
```

airtime-fairness policy（wlan）

WLAN の ATF ポリシーを設定するには、 **airtime-fairness policy** コマンドを使用します。

airtime-fairness policy *policy-name*

構文の説明

policy-name	ポリシー名を入力します。

コマンド デフォルト

なし

コマンド モード

config wlan

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、WLAN の ATF ポリシーを設定する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wlan wlan-name
Switch(config-wlan)#airtime-fairness policy policy-name
```

ap dot11 rf-profile

選択した帯域の RF プロファイルを設定するには、**ap dot11 rf-profile** コマンドを使用します。RF プロファイルを削除するには、このコマンドの **no** 形式を使用します。

ap dot11 {**24GHz** | **5GHz**} **rf-profile** *profile name*

構文の説明

24ghz	2.4 GHz 帯域を表示します。
5ghz	5 GHz 帯域を表示します。
profile name	RF プロファイルの名前。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、選択した帯域の RF プロファイルを設定する例を示します。

```
Switch#ap dot11 24GHz rf-profile doctest
```

ap dot11 rrm

802.11 デバイスの無線リソース管理の基本設定および詳細設定を指定するには、**apdot11rrm** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **rrm** {**ccx location-measurement** 秒|**channel** {**cleanair-event**|**dca**|**device**|**foreign**|**load**|**noise**|**outdoor-ap-dca**}|**coverage** {**data fail-percentage** *pct*|**data packet-count** *count*|**data rssi-threshold** *threshold*}|**exception global** *percentage*|**level global** *number*|**voice** {**fail-percentage** *percentage*|**packet-count** *number*|**rssi-threshold** *threshold*}}

構文の説明

ccx	高度な（RRM）802.11 CCX オプションを設定します。
location-measurement	802.11 CCX クライアント ロケーション測定（秒単位）を指定します。値の範囲は 10 ～ 32400 秒です。
channel	高度な 802.11 チャネル割り当てパラメータを設定します。
cleanair-event	CleanAir のイベント駆動型 RRM パラメータを設定します。
dca	802.11 動的チャネル割り当てアルゴリズムのパラメータを設定します。
device	802.11 チャネル割り当てでの永続型非 Wi-Fi デバイス回避を設定します。
foreign	チャネル割り当てでの外部 AP の 802.11 干渉回避を有効にします。
load	チャネル割り当てでのシスコの AP の 802.11 負荷回避を有効にします。
noise	チャネル割り当てでの 802.11a 以外のノイズ回避を有効にします。
outdoor-ap-dca	屋外 AP の 802.11 DCA リスト オプションを設定します。

coverage	802.11 カバレッジ ホール検出を設定します。
datafail-percentage *pct*	アップリンク データ パケットの 802.11 カバレッジ障害率しきい値を設定します。範囲は 1 ～ 100 です。
datapacket-count *count*	アップリンク データ パケットの 802.11 カバレッジ最小障害数しきい値を設定します。
datarssi-threshold *threshold*	音声パケットの 802.11 最小受信カバレッジ レベルを設定します。
exceptionglobal *percentage*	802.11 シスコ AP カバレッジ例外レベルを設定します。範囲は 0 ～ 100 % です。
levelglobal *number*	802.11 シスコ AP クライアント最小例外レベルを設定します（1 ～ 75 クライアント）。
voice	音声パケットの 802.11 カバレッジ ホール検出を設定します。
fail-percentage *percentage*	音声パケットの 802.11 カバレッジ障害率しきい値を設定します。
packet-count *number*	音声パケットの 802.11 カバレッジ最小アップリンク障害数しきい値を設定します。
rssi-threshold *threshold*	音声パケットの 802.11 最小受信カバレッジ レベルを設定します。

コマンド デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、802.11a帯域と802.11b帯域の両方に適用されます。ただし、パラメータの設定には適切なコマンドを選択する必要があります。

次に、さまざまなRRM設定を指定する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ap dot11 5ghz rrm ?
  ccx            Configure Advanced(RRM) 802.11a CCX options
  channel        Configure advanced 802.11a channel assignment parameters
  coverage       802.11a Coverage Hole Detection
  group-member   Configure members in 802.11a static RF group
  group-mode     802.11a RF group selection mode
  logging        802.11a event logging
  monitor        802.11a statistics monitoring
  ndp-type       Neighbor discovery type Protected/Transparent
  profile        802.11a performance profile
  tpc-threshold  Configures the Tx Power Control Threshold used by RRM for auto
                 power assignment
  txpower        Configures the 802.11a Tx Power Level
```

ap dot11 rrm ccx

2.4 GHz デバイスおよび 5 GHz デバイスの無線リソース管理 CCX オプションを設定するには、**ap dot11 rrm ccx** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **rrm ccx location-measurement** 間隔

構文の説明

location-measurement 間隔	CCX クライアント ロケーション測定間隔値を指定します。値の範囲は 10 ～ 32400 秒です。

コマンド デフォルト

なし。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、5 GHz デバイスの CCX ロケーション測定間隔を設定する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ap dot11 5ghz rrm ccx location-measurement 10
```

ap dot11 rrm channel

2.4 GHz デバイスおよび 5 GHz デバイスの無線リソース管理チャネルを有効にするには、**apdot11rrmchannel** コマンドを使用します。2.4 GHz デバイスおよび 5 GHz デバイスの無線リソース管理を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz|5ghz**} **rrm channel** {**cleanair-event|dca|device|foreign|load|noise**}
no ap dot11 {**24ghz|5ghz**} **rrm channel** {**cleanair-event|dca|device|foreign|load|noise**}

構文の説明

cleanair-event	CleanAir のイベント駆動型 RRM パラメータを指定します。
dca	802.11 動的チャネル割り当てアルゴリズムのパラメータを指定します。
device	802.11 チャネル割り当てでの永続型非 Wi-Fi デバイス回避を指定します。
foreign	チャネル割り当てでの外部 AP の 802.11 干渉回避を有効にします。
load	チャネル割り当てでのシスコの AP の 802.11 負荷回避を有効にします。
noise	チャネル割り当てでの 802.11a 以外のノイズ回避を有効にします。

コマンド デフォルト

なし。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次の例は、**チャネル**の使用可能なすべてのパラメータを示しています。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ap dot11 24ghz rrm channel ?
  cleanair-event  Configure cleanair event-driven RRM parameters
  dca             Config 802.11b dynamic channel assignment algorithm
                  parameters
  device          Configure persistent non-WiFi device avoidance in the 802.11b
                  channel assignment
  foreign         Configure foreign AP 802.11b interference avoidance in the
                  channel assignment
  load            Configure Cisco AP 802.11b load avoidance in the channel
                  assignment
  noise           Configure 802.11b noise avoidance in the channel assignment
```

ap dot11 24ghz rrm channel cleanair-event rogue-contribution

CleanAir イベント駆動型 Radio Resource Management（RRM; 無線リソース管理）の不正寄与パラメータを設定するには、**ap dot11 24ghz rrm channel cleanair-event rogue-contribution** コマンドを使用します。

ap dot11 24ghz rrm channel cleanair-event rogue-contribution duty-cycle *threshold-value*

構文の説明

duty-cycle	イベント駆動型 RRM の不正寄与デューティ サイクルを設定します。
threshold-value	ED-RRM 不正寄与デューティ サイクルのしきい値をカスタマイズします。有効な値の範囲は 1 ~ -99 % です。

コマンド デフォルト

不正寄与デューティ サイクルは設定されていません。

コマンド履歴

リリース	変更内容
16.1	このコマンドが導入されました。

使用上のガイドライン

次のコマンドは、イベント駆動型 RRM の不正寄与デューティ サイクルを設定します。

例

次に、CleanAir イベント駆動型 RRM の不正寄与パラメータを設定する例を示します。

```
Cisco Controller(config)# ap dot11 24ghz rrm channel cleanair-event rogue-contribution
duty-cycle 1
```

ap dot11 24ghz または 5ghz rrm channel dca add

2.4 GHz デバイスまたは 5 GHz デバイスの DCA チャネル リストに非デフォルトの無線リソース管理 DCA チャネルを追加するには、**apdot11** {**24ghz** | **5ghz** } **rrm channel dca add** コマンドを使用します。DCA リストからデフォルトのチャネルを削除するには、このコマンドの **no** 形式を使用します。DCA チャネル リストには、使用する国に適合する標準チャネルが含まれています。たとえば、規制デフォルト チャネル リストにはチャネル 1、6、11 が含まれています。

ap dot11 [{**24ghz**|**5ghz**}] **rrm channel dca add** *number*
no ap dot11 [{**24ghz**|**5ghz**}] **rrm channel dca add** *number*

構文の説明

number	DCA チャネル番号。

コマンド デフォルト

なし。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、**ap dot11 24ghz rrm channel dca add 10** コマンドを使用して 2.4 GHz デバイスの DCA リストに非デフォルトの無線リソース管理 DCA チャネルを追加する例を示します。

```
Switch(config)# ap dot11 24ghz rrm channel dca add 10
```

ap dot11 24ghz または 5ghz rrm channel dca remove

2.4 GHz デバイスまたは 5 GHz デバイスの DCA チャネル リストからデフォルトの無線リソース管理 DCA チャネルを削除するには、**ap dot11**{**24ghz** | **5ghz**} **rrm channel dcaremove** *number* コマンドを使用します。デフォルトの DCA チャネルを DCA チャネル リストに戻すには、このコマンドの **no** 形式を使用します。

ap dot11 [{**24ghz**|**5ghz**}] **rrm channel dca remove** *number*
no ap dot11 [{**24ghz**|**5ghz**}] **rrm channel dca remove** *number*

構文の説明

number	無線リソース管理 DCA チャネルを指定します。

コマンド デフォルト

なし。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、**ap dot11 24ghz rrm channel dca remove** コマンドを使用して 2.4 GHz デバイスの DCA リストからデフォルトの無線リソース管理 DCA チャネルを削除する例を示します。

```
Switch(config)#ap dot11 24ghz rrm channel dca remove 11
```

ap dot11 5ghz rrm channel dca chan-width-11n

5 GHz 帯域のすべての 802.11n 無線に対して DCA チャネル幅を設定するには、**apdot115ghzrrmchanneldcachan-width-11n** *width* コマンドを使用します。5 GHz 帯域のすべての 802.11n 無線に対して DCA チャネル幅を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 5ghzrrm channel dca chan-width-11n {**20** | **40**}
noap dot11 5ghzrrm channel dca chan-width-11n {**20** | **40**}

構文の説明

chan-width-11n	5 GHz 帯域のすべての 802.11n 無線に対して DCA チャネル幅を指定します。
20	802.11n 無線のチャネル幅を 20 MHz に設定します。
40	802.11n 無線のチャネル幅を 40 MHz に設定します。

コマンド デフォルト

デフォルトのチャネル幅は 20 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、**ap dot11 5ghz rrm channel dca chan-width-11n** コマンドを使用して、802.11n 無線のチャネル幅を 40 MHzに設定する例を示します。

```
Switch(config)#ap dot11 5ghz rrm channel dca chan-width-11n 40
```

ap dot11 rrm coverage

802.11 カバレッジ ホール検出を有効にするには、**apdot11rrmcoverage** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **rrm coverage** [{**data** {**fail-percentage** *percentage*|**packet-count** *count*|**rssi-threshold** *threshold*}|**exceptional global** *value*|**level global** *value*|**voice** {**fail-percentage** *percentage*|**packet-count** *packet-count*|**rssi-threshold** *threshold*}}]

構文の説明

data	802.11 カバレッジ ホール検出のデータ パケットを指定します。
fail-percentage *percentage*	アップリンク データ パケットの 802.11 カバレッジ障害率しきい値を指定します。範囲は 1 ～ 100 です。
packet-count *count*	アップリンク データ パケットの 802.11 カバレッジ最小障害数しきい値を指定します。
rssi-threshold *threshold*	音声パケットの 802.11 最小受信カバレッジ レベルを指定します。
exceptionalglobal *value*	802.11 シスコ AP カバレッジ例外レベルを指定します。範囲は 0 ～ 100 % です。
levelglobal *value*	802.11 シスコ AP クライアント最小例外レベルを指定します（1 ～ 75 クライアント）。
voice	音声パケットの 802.11 カバレッジ ホール検出を指定します。
fail-percentage *percentage*	音声パケットの 802.11 カバレッジ障害率しきい値を指定します。
packet-count *packet-count*	音声パケットの 802.11 カバレッジ最小アップリンク障害数しきい値を指定します。
rssi-threshold *threshold*	音声パケットの 802.11 最小受信カバレッジ レベルを指定します。

コマンド デフォルト

なし。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

カバレッジ ホール検出を有効にすると、カバレッジが不完全な領域に位置する可能性のあるクライアントを持つアクセス ポイントがあるかどうかを、アクセス ポイントから受信したデータに基づいてスイッチが自動的に判断します。

5 秒間で失敗したパケットの数と割合の両方が、**ap dot11 {24ghz | 5ghz} rrm coverage packet-count** コマンドと **ap dot11 {24ghz | 5ghz} rrm coverage fail-percentage** コマンドに入力された値を超え

る場合、クライアントは事前アラーム状態と判断されます。スイッチは、この情報を使用してカバレッジ ホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。失敗したクライアントの数と割合の両方が、90 秒以上にわたって、**ap dot11 {24ghz | 5ghz} rrm coverage level-global** コマンドと **ap dot11 {24ghz | 5ghz} rrm coverage exceptional-global** コマンドで入力した値以上になると、カバレッジホールが検出されます。スイッチは、カバレッジ ホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、5 GHz 帯域で データの RSSI しきい値を設定する例を示します。

```
スイッチ#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
スイッチ(config)#ap dot11 5ghz rrm coverage data rssi-threshold -80
```

ap dot11 rrm group-member

802.11 静的 RF グループのメンバを設定するには、**apdot11rrmgroup-member** コマンドを使用します。メンバを削除するには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**|**5ghz**} **rrm group-member** *controller-name controller-ip*
no ap dot11 {**24ghz**|**5ghz**} **rrm group-member** *controller-name controller-ip*

構文の説明

controller-name	追加するコントローラの名前を指定します。
controller-ip	追加するコントローラのIPアドレスを指定します。

コマンド デフォルト

なし。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、5 GHz 自動 RF グループにコントローラを追加する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ap dot11 5ghz rrm group-member ABC 10.1.1.1
```

ap dot11 rrm monitor

802.11 帯域統計情報をモニタするには、**apdot11rrmmonitor** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

ap dot11 {24ghz|5ghz} rrm monitor {channel-list|{all|country|dca}|coverage|load|noise|signal}
no ap dot11 {24ghz|5ghz} rrm monitor {channel-list|coverage|load|noise|signal}

構文の説明

channel-list	802.11 ノイズ/干渉/不正モニタリング チャネル リストを設定します。
all	すべてのチャネルをモニタすることを指定します。
country	設定された国コードで使用するチャネルをモニタすることを指定します。
dca	動的チャネル割り当てで使用されるチャネルをモニタすることを指定します。
coverage	802.11 カバレッジ測定間隔を指定します。値の範囲は 60 ～ 3600（秒単位）です。
load	802.11 負荷測定間隔を指定します。値の範囲は 60 ～ 3600（秒単位）です。
noise	802.11 ノイズ測定間隔（チャネル スキャン間隔）を指定します。値の範囲は 60 ～ 3600（秒単位）です。
signal	802.11 信号測定間隔（ネイバー パケット周波数）を指定します。値の範囲は 60 ～ 3600（秒単位）です。

コマンド デフォルト

なし。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、すべての 5GHz 帯域チャネルのモニタリングを有効にする例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ap dot11 5ghz rrm monitor channel-list all
```

ap dot11 rrm profile

サポートされている 802.11 ネットワークの Cisco Lightweight アクセス ポイント プロファイルを設定するには、**apdot11rrmprofile** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **rrm profile** {**customize**|**foreign** *value*|**noise** *value*|**throughput** *value*|**utilization** *value*}

構文の説明

customize	パフォーマンス プロファイルを有効にします。
foreign *value*	802.11 外部 802.11 干渉しきい値を指定します。範囲は 0 ～ 100 % です。
noise *value*	802.11 外部ノイズしきい値を指定します。範囲は -127 ～ 0 dBm です。
throughput *value*	802.11a シスコ AP スループットしきい値を指定します。値の範囲は 1000 ～ 10000000 バイト/秒です。
utilization *value*	802.11a RF 使用率しきい値を指定します。範囲は 0 ～ 100 % です。

コマンド デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、ノイズ パラメータのしきい値を設定する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ap dot11 5ghz rrm profile noise -50
```

ap dot11 rrm tpc-threshold

自動電力割り当てのために RRM によって使用される TX 電力制御しきい値を設定するには、**apdot11rrmtpc-threshold** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**|**5ghz**} **rrm tpc-threshold** *value*
no ap dot11 {**24ghz**|**5ghz**} **rrm tpc-threshold**

構文の説明

value	電力値を指定します。範囲は -80 ～ -50 です。

コマンド デフォルト

なし。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、自動電力割り当てのために RRM によって使用される TX 電力制御しきい値を設定する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ap dot11 5ghz rrm tpc-threshold -60
```

ap dot11 rrm txpower

802.11 TX 電力レベルを設定するには、**apdot11rrmtxpower** コマンドを使用します。802.11 TX 電力レベルを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**|**5ghz**} **rrm txpower** {**auto**|**max** *powerLevel*|**min** *powerLevel*|**once***power-level*}
noap dot11 {**24ghz**|**5ghz**} **rrm txpower** {**auto**|**max** *powerLevel*|**min** *powerLevel*|**once***power-level*}

構文の説明

auto	自動 RF を有効にします。
max *powerLevel*	最大自動 RF TX 電力を設定します。範囲は -10 ～ -30 です。
min *powerLevel*	最小自動 RF TX 電力を設定します。範囲は -10 ～ -30 です。
once	ワンタイム自動 RF を有効にします。

コマンド デフォルト

なし。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	このコマンドの **no** 形式が導入されました。

使用上のガイドライン

なし。

次に、ワンタイム自動 RF を有効にする例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ap dot11 5ghz rrm txpower once
```

ap dot11 airtime-fairness mode

Air Time Fairness を強制ポリシー モードまたはモニタ モードで有効にするには、**ap dot11 airtime-fairness mode** コマンドを使用します。Air Time Fairness の強制ポリシー モードまたはモニタ モードを無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz**|**5ghz**}**airtime-fairness mode** {**enforce-policy**|**monitor**}

no ap dot11 {**24ghz**|**5ghz**}**airtime-fairness mode** {**enforce-policy**|**monitor**}

構文の説明

24ghz	802.11b パラメータを設定します。
5ghz	802.11a パラメータを設定します。
enforce-policy	強制ポリシー モードで Air Time Fairness を設定します。
monitor	モニタ モードで Air Time Fairness を設定します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次の例は、**Air Time Fairness モード**の使用可能なすべてのパラメータを示しています。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ap dot11 24ghz airtime-fairness mode ?
 enforce-policy  Configure airtime-fairness in enforce-policy mode
 monitor         Configure airtime-fairness in monitor mode
```

ap dot11 airtime-fairness policy-name

新しい Air Time Fairness（ATF）ポリシーを作成するには、**ap dot11 airtime-fairness policy-name** コマンドを使用します。

ap dot11 airtime-fairness policy-name *policy-name policy-id*

構文の説明

policy-name	ATF ポリシー名を入力します。
policy-id	新しいポリシーを作成するための ATF ポリシー ID を入力します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

すべての ATF ポリシーには、ポリシー ウェイト値が必要です。ポリシー ウェイトを追加するには、config-airtime-fairness ポリシー モードで **policy weight** コマンドを使用します。ポリシー ウェイトを追加しない場合は、デフォルト値の 10 が適用されます。ポリシー ウェイト追加の詳細については、policy-weight （737 ページ）を参照してください。

次に例を示します。

```
Switch#ap dot11 airtime-fairness policy-name testpolicy 12
```

policy-weight

Air Time Fairness（ATF）ポリシーにポリシー ウェイトを適用するには、**policy-weight** コマンドを使用します。

policy-weight *policy-weight*

構文の説明

policy-weight	ATF ポリシーのポリシー ウェイト。範囲は 5 ～ 100 です。デフォルト値は 10 です。

コマンド デフォルト

なし

コマンド モード

config-airtime-fairness policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

WLAN にポリシーを適用しない場合、ポリシー ウェイト 10 のデフォルト ポリシー（ID 0）が自動的に適用されます。ATF ポリシー作成の詳細については、ap dot11 airtime-fairness policy-name（737 ページ）を参照してください。

次に、ATF ポリシーにポリシー ウェイトを適用する例を示します。

```
Switch#ap dot11 airtime-fairness policy-name testpolicy 12
Switch(config-airtime-fairness policy)# policy-weight 35
```

ap group

AP グループを設定するには、**ap group** コマンドを使用します。

ap group *group-name*

構文の説明

group-name	AP グループの名前

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、AP グループを設定する例を示します。

```
Switchconfig# ap group docgroup
```

ap name dot11 airtime-fairness mode

特定の AP の Air Time Fairness を強制ポリシー モードまたはモニタ モードで有効にするには、**ap namedot11 airtime-fairness mode** コマンドを使用します。特定の AP の Air Time Fairness を 2 つのモードのいずれかから無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name***dot11** {**24ghz**|**5ghz**} **airtime-fairness mode** {**enforce-policy**|**monitor**}

ap name *ap-name***no dot11** {**24ghz**|**5ghz**} **airtime-fairness mode** {**enforce-policy**|**monitor**}

構文の説明

ap-name	アクセス ポイント名を入力します。
24ghz	802.11b パラメータを設定します。
5ghz	802.11a パラメータを設定します。
enforce-policy	強制ポリシー モードで Air Time Fairness を設定します。
monitor	モニタ モードで Air Time Fairness を設定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、特定の AP の Air Time Fairness を強制ポリシー モードまたはモニタ モードのいずれかから無効にする例を示します。

```
Switch# ap name testap no dot11 24ghz airtime-fairness mode
```

ap name dot11 airtime-fairness optimization

特定の AP の ATF 最適化を有効にするには、**ap name dot11 airtime-fairness optimization** コマンドを使用します。特定の AP の ATF 最適化を無効にするには、**no** を使用します。

ap name *ap-name***dot11** {**24ghz**|**5ghz**} **airtime-fairness optimization**

ap name *ap-name***no dot11** {**24ghz**|**5ghz**} **airtime-fairness optimization**

構文の説明

ap-name	アクセスポイント名を入力します。
24ghz	802.11b パラメータを設定します。
5ghz	802.11a パラメータを設定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、特定の AP の ATF 最適化を有効にする例を示します。

```
Switch#ap name doctestap dot11 24ghz airtime-fairness optimization
```

ap name no dot11 airtime-fairness wlan-name policy-name

WLAN 固有の WLAN で ATF ポリシー オーバーライドを無効にするには、**ap name no dot11 airtime-fairness wlan-name** コマンドを使用します。

ap name *ap-name***no dot11** {**24ghz**|**5ghz**}**airtime-fairness wlan-name** *wlan-name*

構文の説明

ap-name	アクセス ポイント名を入力します。
24ghz	802.11b パラメータを設定します。
5ghz	802.11a パラメータを設定します。
wlan-name	シスコの AP でこの WLAN の Air Time Fairness ポリシーを設定します。
wlan-name	WLAN プロファイル名を入力します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、WLAN 固有の WLAN で ATF ポリシー オーバーライドを無効にする例を示します。

```
Switch#ap name testap no dot11 24ghz airtime-fairness wlan-name testwlan
```

ap name dot11 airtime-fairness wlan-name policy

1 つの AP に固有の WLAN で ATF ポリシーをオーバーライドするには、**ap name dot11 airtime-fairness wlan-name policy-name** コマンドを使用します。

ap name *ap-name***dot11** {**24ghz**|**5ghz**} **airtime-fairness wlan-name** *wlan-name***policy-name** *policy-name*

構文の説明

ap-name	アクセス ポイント名。
24ghz	802.11b パラメータを設定します。
5ghz	802.11a パラメータを設定します。
wlan-name	シスコの AP でこの WLAN の Air Time Fairness ポリシーを設定します。
wlan-name	WLAN プロファイル名を入力します。
policy-name	Air Time Fairness ポリシーを設定します。
policy-name	Air Time Fairness ポリシー名を入力します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、1 つの AP に固有の WLAN で ATF ポリシーをオーバーライドする例を示します。

```
Switch# ap name testap dot11 24ghz airtime-fairness wlan-name testwlan policy-name
testpolicy
```

band-select client

選択した帯域のクライアントしきい値の最小 dB を設定するには、**band-select client** コマンドを使用します。選択した帯域のクライアントしきい値の最小 dB をリセットするには、このコマンドの **no** 形式を使用します。

band-select client {**mid-rssi** | **rssi** }*dBm value*

構文の説明

mid-rssi	クライアントRSSIがプローブへの応答を開始するための最小dBm。
rssi	クライアント RSSI がプローブへ応答するための最小 dBm。
dBm value	クライアント RSSI がプローブへ応答するための最小 dBm。有効な範囲は -90 ～ -20 dBm です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは 2.4 GHz 帯域でのみ有効です。

次に、選択した帯域のクライアントしきい値を最小 dB に設定する例を示します。

```
Switch(config-rf-profile)#band-select client rssi -50
```

band-select cycle

帯域選択のサイクル パラメータを設定するには、**band-select cycle** コマンドを使用します。しきい値をリセットするには、このコマンドの **no** 形式を使用します。

band-select cycle { **count** | **threshold** } *value*

構文の説明

count	帯域選択のプローブ サイクル カウントを設定します。
value	応答していないサイクルの最大数。範囲は 1 ～ 10 です。
threshold	新規スキャン サイクルの時間しきい値を設定します。
value	しきい値をミリ秒単位で設定します。有効な値は、1 ～ 1000 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、選択した帯域の RF プロファイルにプローブ サイクル カウントを設定する例を示します。

```
Switch(config-rf-profile)#band-select cycle count 5
```

band-select expire

選択した帯域の RF プロファイルの期限を設定するには、**band-select expire** コマンドを使用します。値をリセットするには、このコマンドの **no** 形式を使用します。

band-select expire { **dual-band** | **suppression** } *value*
no band-select expire { **dual-band** | **suppression** }

構文の説明

dual-band	RF プロファイルで帯域選択されたデュアル バンドの期限を設定します。
value	既知のデュアルバンドクライアントをプルーニングするための期限を設定します。範囲は 10 ～ 300 です。
suppression	RF プロファイルで帯域選択された抑制対象の期限を設定します。
value	既知の 802.11b/g クライアントをプルーニングするための期限を設定します。範囲は 10 ～ 200 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、選択した帯域の RF プロファイルのデュアルバンドに期限を設定する例を示します。

```
Switch(config-rf-profile)#band-select expire dual-band 15
```

band-select probe-response

選択した帯域でのクライアントへのプローブ応答を設定するには、**band-select probe-response** コマンドを使用します。プローブ応答を無効にするには、このコマンドの **no** 形式を使用します。

band-select probe-response

構文の説明

probe-response	クライアントへのプローブ応答。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、クライアントへのプローブ応答を有効にする例を示します。

```
Switch(config-rf-profile)#band-select probe-response
```

channel

RF プロファイルの DCA チャネル リストのチャネルを設定するには、**channel** コマンドを使用します。チャネルを無効にするには、このコマンドの **no** 形式を使用します。

channel { **add** |**remove** } *channel-number*

構文の説明

add	RF プロファイルの DCA チャネル リストにチャネルを追加します。
remove	RF プロファイルの DCA チャネル リストからチャネルを削除します。
channel-number	チャネル番号。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RF プロファイルの DCA チャネル リストにチャネルを追加する例を示します。

```
Switch(config-rf-profile)#channel add 3
```

channel foreign

RF プロファイルの外部 AP の寄与を設定するには、**channel foreign** コマンドを使用します。DCA 外部 AP の寄与を無効にするには、このコマンドの **no** 形式を使用します。

channel foreign

構文の説明

foreign	RF プロファイルの DCA 外部 AP の寄与を設定します。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RF プロファイルの DCA 外部 AP の寄与を設定する例を示します。

```
Switch(config-rf-profile)#channel foreign
```

channel width

RF プロファイルの DCA チャネル幅を設定するには、**channel width** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

channel width {**20** |**40** |**80** |**best** }

構文の説明

20	MHz 単位のチャネル幅。
40	MHz 単位のチャネル幅。
80	MHz 単位のチャネル幅。
best	MHz 単位のチャネル幅。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは 5 GHz 帯域でのみ有効です。

次に、チャネル幅を 40 MHzに設定する例を示します。

```
Switch(config-rf-profile)#channel width 40
```

coverage

音声とデータの対象範囲を設定するには、**coverage** コマンドを使用します。最小 RSSI 値をリセットするには、このコマンドの **no** 形式を使用します。

coverage {**data** |**voice**} **rssi threshold** *value*

構文の説明

data	データ パケットのカバレッジ ホール検出を設定します。
voice	音声パケットのカバレッジ ホール検出を設定します。
value	アクセスポイントが受信したパケットの最小 RSSI 値。有効な範囲は、-90 ～ -60 dBm です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、データ パケットのカバレッジ ホール検出を設定する例を示します。

```
Switch(config-rf-profile)#coverage data rssi threshold -85
```

coverage exception

Cisco AP カバレッジ例外レベルを設定するには、**coverage exception** コマンドを使用します。例外レベルのパーセンテージをリセットするには、このコマンドの **no** 形式を使用します。

coverage exception *exception-level*

構文の説明

exception-level	有効な範囲が 0 ~ 100 % の Cisco AP カバレッジ例外レベル。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、Cisco AP カバレッジ例外レベルを設定する例を示します。

```
Switch(config-rf-profile)#coverage exception 70
```

coverage level

Cisco AP クライアントの最低のカバレッジ レベルを設定するには、**coverage level** コマンドを使用します。カバレッジ クライアント値をリセットするには、このコマンドの **no** 形式を使用します。

coverage level クライアント

構文の説明

クライアント	最低のカバレッジ レベル。範囲は、1 ～ 200 クライアントです。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、Cisco AP クライアントの最低レベルを設定する例を示します。

```
Switch(config-rf-profile)#coverage level 180
```

clear wireless airtime-fairness statistics

ワイヤレス通信時間フェアネス統計情報をクリアするには、**clear wireless airtime-fairness statistics** コマンドを使用します。

clear clear wireless airtime-fairness statistics

構文の説明

airtime-fairness	通信時間フェアネス統計情報をクリアします。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、ワイヤレス通信時間フェアネス統計情報をクリアする例を示します。

```
Switch#clear wireless airtime-fairness statistics
```

dot11n-only

RF プロファイルの 802.11n クライアント専用モードを有効にするには、**dot11n-only** コマンドを使用します。802.11n クライアント専用モードを無効にするには、このコマンドの **no** 形式を使用します。

dot11n-only

構文の説明

dot11n-only	RF プロファイルの 802.11n クライアント専用モード。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RF プロファイルの 802.11n クライアント専用モードを有効にする例を示します。

```
Switch(config-rf-profile)#dot11n-only
```

load-balancing

RF プロファイルのロード バランスを設定するには、**load-balancing** コマンドを使用します。RF プロファイルのロード バランス値をリセットするには、このコマンドの **no** 形式を使用します。

load-balancing {**denial** | **window**} *value*

構文の説明

denial	ロード バランシングの拒否の数を設定します。
value	ロードバランシングの拒否回数を入力します。範囲は1～10です。
window	アグレッシブ ロード バランシング用のクライアント ウィンドウを設定します。
value	クライアント数。範囲は 0 ～ 20 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、ロード バランシングの拒否の数を設定する例を示します。

```
Switch#load-balancing denial 4
```

high-density clients count

RF プロファイルの最大クライアント数を設定するには、**high-density clients count** コマンドを使用します。RF プロファイルの最大クライアント数をリセットするには、このコマンドの **no** 形式を使用します。

high-density clients count *value*

構文の説明

value	AP 無線あたりの最大クライアント接続数。範囲は 0 ～ 200 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RF プロファイルの最大クライアント数を設定する例を示します。

```
Switch(config-rf-profile)#high-density clients count 25
```

high-density clients wlan

WLAN 上の AP あたりの最大クライアント数を設定するには、**high-density clients wlan** コマンドを使用します。最大数をリセットするには、このコマンドの **no** 形式を使用します。

high-density clients wlan *wlan name* **count** *count*

構文の説明

wlan name	AP あたりのクライアント数を制限するには、WLAN の名前を入力します。
count	WLAN ごとの AP あたりの最大クライアント接続数。範囲は 0 ～ 200 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、WLAN 上の AP あたりの最大クライアント数を設定する例を示します。

```
Switch(config-rf-profile)#high-density clients wlan doctest count 20
```

high-density multicast data-rate

RF プロファイルのマルチキャスト データ レートの値を設定するには、 **high-density multicast data-rate** コマンドを使用します。データレートを auto にリセットするには、このコマンドの **no** 形式を使用します。

high-density multicast data-rate
{RATE_12M|RATE_18M|RATE_24M|RATE_36M|RATE_48M|RATE_54M|RATE_6M|RATE_9M}

構文の説明

multicast	RF プロファイルのマルチキャストを設定します。
data-rate	RF プロファイルのマルチキャスト データ レートの値。
RATE_12M	802.11 12M レート
RATE_18M	802.11 18M レート
RATE_24M	802.11 24M レート
RATE_36M	802.11 36M レート
RATE_48M	802.11 48M レート
RATE_54M	802.11 54M レート
RATE_6M	802.11 6M レート
RATE_9M	802.11 9M レート

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RFプロファイルのマルチキャストデータ レートの値を設定する例を示します。

```
Switch(config-rf-profile)#high-density multicast data-rate RATE_9M
```

high-density rx-sop threshold

RF プロファイルの Rx SOPしきい値の値を設定するには、**high-density rx-sop threshold** コマンドを使用します。Rx SOP を auto に戻すには、このコマンドの **no** 形式を使用します。

high-density rx-sop threshold {**auto** |**high** |**low** |**medium** }

構文の説明

rx-sop	RF プロファイルの Rx SOP しきい値を設定します。
threshold	RF プロファイルの Rx SOP しきい値の値を設定します。
auto	無線レシーバ SOP しきい値を auto に戻します。
high	無線レシーバ SOP しきい値を high に設定します。
low	無線レシーバ SOP しきい値を low に設定します。
medium	無線レシーバ SOP しきい値を medium に設定します。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RFプロファイルの無線レシーバSOPしきい値をhighに設定する例を示します。

```
Switch(config-rf-profile)#high-density rx-sop threshold high
```

rate

802.11 動作速度を設定するには、**rate** コマンドを使用します。レートをデフォルト状態に戻すには、このコマンドの **no** 形式を使用します。

rate
{RATE_12M|RATE_18M|RATE_24M|RATE_36M|RATE_48M|RATE_54M|RATE_6M|RATE_9M}{disable|mandatory|supported}

構文の説明

RATE_12M	802.11 12M レート。
RATE_18M	802.11 18M レート。
RATE_24M	802.11 24M レート。
RATE_36M	802.11 36M レート。
RATE_48M	802.11 48M レート。
RATE_54M	802.11 54M レート。
RATE_6M	802.11 6M レート。
RATE_9M	802.11 9M レート。
disable	レートをディセーブルにします。
mandatory	レートを mandatory に設定します。
supported	レートを supported に設定します。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、802.11 9M 動作速度を無効にする例を示します。

```
Switch(config-rf-profile)#rate RATE_9M disable
```

rate mcs

RF プロファイルの MCS データ レートを有効にするには、**rate mcs** コマンドを使用します。RF プロファイルの MCS データ レートを無効にするには、このコマンドの **no** 形式を使用します。

rate mcs *index-number*

構文の説明

index-number	RF プロファイルの MCS データ レートのインデックス番号を入力します。範囲は 0 ～ 31 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RF プロファイルの MCS データ レートを有効にする例を示します。

```
Switch(config-rf-profile)#rate mcs 5
```

trap threshold

RF プロファイルのトラップしきい値パラメータを設定するには、**trap threshold** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

trap threshold {**clients** |**interference** |**noise** |**utilization** } *value*

構文の説明

clients	しきい値クライアントの RF プロファイル トラップを設定します。
value	トラップが送信された後に、アクセスポイントに関連付けるクライアントの数。範囲は 1 ～ 200 です。
interference	RF プロファイルの干渉のトラップしきい値を設定します。
value	RFプロファイルのトラップしきい値に干渉の割合値を設定します。範囲は 0 ～ 100 です。
noise	RF プロファイルのノイズのトラップしきい値を設定します。
value	RF プロファイルのトラップしきい値にノイズの値を dbm 単位で設定します。範囲は -127 ～ 0 です。
utilization	RF プロファイルの使用率のトラップしきい値を設定します。
value	RF プロファイルのトラップしきい値に使用率の割合値を設定します。範囲は 0 ～ 100 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、クライアントのRFプロファイルのしきい値トラップを設定する例を示します。

```
Switch(config-rf-profile)#trap threshold clients 10
```

tx-power

Tx 電力レベルを設定するには、 **tx-power** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

tx-power { **min** | **max** } *dBm value*

構文の説明

max	最大 Auto-RF 送信電力を設定します。
min	最小 Auto-RF 送信電力を設定します。
dBm value	dBm 単位で値を入力します。範囲は -10 ～ 30 です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、Tx 電力レベルを min に設定する例を示します。

```
Switch(config-rf-profile)#tx-power min -14
```

tx-power v1 threshold

伝送パワー コントロール（TPC）バージョン1のしきい値を設定するには、**tx-power v1 threshold** コマンドを使用します。デフォルトの dBm 値に戻すには、このコマンドの **no** 形式を使用します。

tx-power v1 threshold *dBm value*

構文の説明

dBm value	伝送パワー コントロール バージョン 1 のしきい値。範囲は -80 ～ -50 dBm です。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、TPCv1 しきい値を –75 dBm に設定する例を示します。

```
Switch#tx-power v1 threshold -75
```

no ap dot11 airtime-fairness policy-name

Air Time Fairness ポリシーを削除するには、**no ap dot11 airtime-fairness policy-name** コマンドを使用します。

no ap dot11 airtime-fairness policy-name *policy-name*

構文の説明

policy-name	Air Time Fairness ポリシー名を入力します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、Air Time Fairness ポリシーを削除する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch# no ap dot11 airtime-fairness policy-name testpol
```

remote-lan

AP グループにリモート LAN を設定するには、**remote-lan** コマンドを使用します。AP グループからリモート LAN を削除するには、このコマンドの **no** 形式を使用します。

remote-lan *name*

構文の説明

name	リモート LAN の名前を入力します。

コマンド デフォルト

なし

コマンド モード

config-apgroup

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、AP グループにリモート LAN を設定する例を示します。

```
Switch(config-apgroup)#remote-lan rlantest
```

rf-profile dot11 24ghz

2.4 GHz 帯域の AP グループに RF プロファイルを割り当てるには、**rf-profile dot11 24ghz** コマンドを使用します。

rf-profile dot11 24ghz *name*

構文の説明

name	現在の AP グループに割り当てられる RF プロファイルの名前を入力します。

コマンド デフォルト

なし

コマンド モード

config-apgroup

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、2.4 GHz 帯域の AP グループに RF プロファイルを割り当てる例を示します。

```
Switch(config-apgroup)#rf-profile dot11 24ghz doctest
```

rf-profile dot11 5ghz

5 GHz 帯域の AP グループに RF プロファイルを割り当てるには、**rf-profile dot11 5ghz** コマンドを使用します。

rf-profile dot11 5ghz *name*

構文の説明

name	現在の AP グループに割り当てられる RF プロファイルの名前を入力します。

コマンド デフォルト

なし

コマンド モード

config-apgroup

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、5GHz 帯域の AP グループに RF プロファイルを割り当てる例を示します。

```
Switch(config-apgroup)#rf-profile dot11 24ghz doc5test
```

show ap airtime-fairness ap-group

特定の AP グループの ATF 設定を表示するには、**show ap airtime-fairness ap-group** コマンドを使用します。

show ap airtime-fairness ap-group *group-name*

構文の説明

group-name	AP グループ名を入力します

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、特定の AP グループの ATF 設定の例を示します。

```
Switch#show ap airtime-fairness ap-group ?
Site Description:
Airtime-fairness 2.4GHz Mode:: Disable
Airtime-fairness 2.4GHz Optimization : n/a
Airtime-fairness 5GHz Mode:: Disable
Airtime-fairness 5GHz Optimization : n/a

WLAN ID   WLAN Name                        Interface            ATF Policy(2.4GHz)
ATF Policy(5GHz)
--------------------------------------------------------------------------------------------------
```

show ap airtime-fairness (ap)

特定の AP の ATF 設定を表示するには、**show ap airtime-fairness** コマンドを使用します。

show ap name*ap-name***airtime-fairness**

構文の説明

ap-name	アクセス ポイント名を入力します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、特定の AP の ATF 設定を表示する例を示します。

```
Switch# show ap name testap airtime-fairness
```

show ap airtime-fairness（無線別）

無線別の Air Time Fairness 設定がある AP リストを表示するには、**show ap airtime-fairness** コマンドを使用します。

show ap airtime-fairness

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、無線別の Air Time Fairness がある AP リストを表示する例を示します。

```
Switch#show ap airtime-fairness
```

show ap airtime-fairness policy（すべて）

すべての設定済みポリシーを表示するには、**show ap airtime-fairness policy** コマンドを使用します。

show ap airtime-fairness policy

構文の説明

policy	Air Time Fairness ポリシー情報を表示します。

コマンド デフォルト

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、設定済みのすべての Air Time Fairness ポリシーを表示する例を示します。

```
Switch#show ap airtime-fairness policy
Policy ID   Policy Name         Weight
----------------------------------------
23           f                    10
12           asd                  10
13           pol                  10
50           meaw                 45
20           pocy                 10
0            Default              10
```

show ap airtime-fairness wlan

Air Time Fairness ポリシーが適用されている設定済み WLAN の完全なリストを表示するには、**show ap airtime-fairness wlan** コマンドを使用します。

show ap airtime-fairness wlan

構文の説明

wlan	すべての WLAN の Air Time Fairness 設定を表示します。

コマンド デフォルト

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、ATF ポリシーが適用されている設定済み WLAN の完全なリストを表示する例を示します。

```
Switch#show ap airtime-fairness wlan

WLAN ID     Profile Name                        ATF Profile Name         Weight
-------------------------------------------------------------------------------
12          doctestlan                          Default                  10
```

show ap dot11 24ghz

2.4 GHz RRM パラメータを表示するには、**showapdot1124ghz** コマンドを使用します。

show ap dot11 24ghz
{ccx|channel|coverage|group|l2roam|logging|monitor|profile|receiver|summary|txpower}

構文の説明

ccx	すべての Cisco AP に対して 802.11b CCX 情報を表示します。
channel	802.11bチャネル割り当ての設定および統計情報を表示します。
coverage	802.11b カバレッジの設定と統計情報を表示します。
group	802.11b グループ化の設定と統計情報を表示します。
l2roam	802.11b l2roam 情報を表示します。
logging	802.11b イベント ロギングの設定と統計情報を表示します。
monitor	802.11b モニタリングの設定および統計情報を表示します。
profile	すべての Cisco AP の 802.11b プロファイル情報を表示します。
receiver	802.11b レシーバの設定と統計情報を表示します。
summary	802.11b Cisco AP の設定と統計情報を表示します。
txpower	802.11b 送信電力制御の設定と統計情報を表示します。

コマンド デフォルト

なし。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、802.11b カバレッジの設定と統計情報を表示する例を示します。

```
Switch#show ap dot11 24ghz coverage

Coverage Hole Detection
  802.11b Coverage Hole Detection Mode            : Enabled
  802.11b Coverage Voice Packet Count             : 100 packet(s)
  802.11b Coverage Voice Packet Percentage        : 50%
  802.11b Coverage Voice RSSI Threshold           : -80 dBm
  802.11b Coverage Data Packet Count              : 50 packet(s)
  802.11b Coverage Data Packet Percentage         : 50%
```

```
802.11b Coverage Data RSSI Threshold            : -80 dBm
802.11b Global coverage exception level         : 25 %
802.11b Global client minimum exception level   : 3 clients
```

show ap dot11 5ghz

5 GHz RRM パラメータを表示するには、**showapdot115ghz** コマンドを使用します。

show ap dot11 5ghz
{ccx|channel|coverage|group|l2roam|logging|monitor|profile|receiver|summary|txpower}

構文の説明

ccx	すべての Cisco AP の 802.11a CCX 情報を表示します。
channel	802.11a チャネル割り当ての設定および統計情報を表示します。
coverage	802.11a カバレッジの設定と統計情報を表示します。
group	802.11a グループ化の設定と統計情報を表示します。
l2roam	802.11a l2roam 情報を表示します。
logging	802.11a イベント ロギングの設定と統計情報を表示します。
monitor	802.11a モニタリングの設定および統計情報を表示します。
profile	すべての Cisco AP の 802.11a プロファイル情報を表示します。
receiver	802.11a レシーバの設定と統計情報を表示します。
summary	802.11a Cisco AP の設定と統計情報を表示します。
txpower	802.11a 送信電力制御の設定と統計情報を表示します。

コマンド デフォルト

なし。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、802.11a チャネル割り当ての設定と統計情報の例を示します。

```
Switch#show ap dot11 5ghz channel

Automatic Channel Assignment
  Channel Assignment Mode                   : AUTO
  Channel Update Interval                   : 12 Hours
  Anchor time (Hour of the day)             : 20
  Channel Update Contribution               : SNI..
  Channel Assignment Leader                 : web (9.9.9.2)
  Last Run                                  : 16534 seconds ago
```

```
DCA Sensitivity Level                        : MEDIUM (15 dB)
DCA 802.11n Channel Width                    : 40 Mhz
Channel Energy Levels
    Minimum                                  : unknown
    Average                                  : unknown
    Maximum                                  : unknown
Channel Dwell Times
    Minimum                                  : unknown
    Average                                  : unknown
    Maximum                                  : unknown
802.11a 5 GHz Auto-RF Channel List
Allowed Channel List                         : 36,40,44,48,52,56,60,64,149,153,1

                     57,161
Unused Channel List                          : 100,104,108,112,116,132,136,140,1

                     65
802.11a 4.9 GHz Auto-RF Channel List
Allowed Channel List                         :
Unused Channel List                          : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,

                     15,16,17,18,19,20,21,22,23,24,25,26
DCA Outdoor AP option                        : Disabled
```

show ap dot11 airtime-fairness（無線帯域）

ATF が設定された無線帯域がある AP リストを表示するには、**show ap dot11 airtime-fairness** コマンドを使用します。

show ap dot11 {**24ghz**|**5ghz**} **airtime-fairness**

構文の説明

24ghz	802.11b の設定を表示します。
5ghz	802.11a の設定を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、ATF が設定された無線帯域がある AP リストを表示する例を示します。

```
Switch#show ap dot 24ghz airtime-fairness
```

show ap dot11 24ghz rf-profile summary

2.4 GHz RF プロファイルのサマリーを表示するには、**show ap dot11 24ghz rf-profile summary** コマンドを使用します。

show ap dot11 24ghz rf-profile summary

構文の説明

summary	RF プロファイルのサマリーを表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に 24 GHz AP プロファイルのサマリーを表示する例を示します。

```
Switch(config-rf-profile)#show ap dot11 24ghz rf-profile summaryNumber of RF Profiles :
 1

RF Profile Name                  Band      Description           Applied   State
------------------------------------------------------------------------------
doctest                          2.4 GHz                         No        Down
```

show ap dot11 5ghz rf-profile summary

5 GHz AP の RF プロファイルを表示するには、**show ap dot11 5ghz rf-profile summary** コマンドを使用します。

show ap dot11 5ghz rf-profile summary

構文の説明

summary	RF プロファイルのサマリーを表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、5 GHz AP の RF プロファイルのサマリーを表示する例を示します。

```
Switch#show ap dot11 5ghz rf-profile summary
Number of RF Profiles : 1

RF Profile Name                  Band      Description           Applied   State
------------------------------------------------------------------------------
doc5test                         5 GHz                           No        Down
```

show ap name dot11 airtime-fairness summary

特定の AP の ATF 統計を表示するには、**show ap name dot11 airtime-fairness summary** コマンドを使用します。

show ap name *ap-name***dot11** {**24ghz**|**5ghz**} **airtime-fairness summary**

構文の説明

ap-name	24 GHz と 5 GHz の Air Time Fairness の統計を表示します。
24ghz	802.11b の設定を表示します。
5ghz	802.11a の設定を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、特定の AP の ATF 統計を表示する例を示します。

```
Switch#show ap ame testap dot11 24ghz airtime-fairness summary
```

show ap name dot11 airtime-fairness policy statistics

各 ATF ポリシーの統計を表示するには、**show ap name dot11 airtime-fairness policy statistics** コマンドを使用します。

show ap name *ap-name***dot11** {**24ghz**|**5hz**} **airtime-fairness policy** *policy-name***statistics**

構文の説明

ap-name	アクセス ポイント名を入力します。
24ghz	802.11b の設定を表示します。
5hz	802.11a の設定を表示します。
policy-name	ポリシー名を入力します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、各 ATF ポリシーの統計を表示する例を示します。

```
Switch#show ap name testap dot11 24ghz airtime-fairness policy testpolicy statistics
```

show ap name dot11 airtime-fairness wlan name statistics

特定の AP でアクティブな WLAN ごとの ATF の統計を表示するには、**show ap name dot11 airtime-fairness wlan name statistics** コマンドを使用します。

show ap name dot11 {**24ghz**|**5ghz**} **airtime-fairness wlan name** *wlan-name***statistics**

構文の説明

name	プロファイル名別の Air Time Fairness の統計を表示します。
wlan-name	WLAN 名を入力します。
statistics	24 GHz と 5 GHz の Air Time Fairness の統計を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

次に、特定の AP でアクティブな WLAN ごとの ATF の統計を表示する例を示します。

```
Switch#show ap name testap dot11 24ghz airtime-fairness wlan name testwlan statistics
```

show ap rf-profile summary

AP の RF プロファイルのサマリーを表示するには、**show ap rf-profile summary** コマンドを使用します。

show ap rf-profile summary

構文の説明

summary	RF プロファイルのサマリーを表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、AP の RF プロファイルのサマリーを表示する例を示します。

```
Switch#show ap rf-profile summary
Number of RF Profiles : 1

RF Profile Name                  Band      Description           Applied   State
------------------------------------------------------------------------------
doctest                          2.4 GHz                         No        Down
```

show ap rf-profile name

選択した AP の RF プロファイルの詳細を表示するには、**show ap rf-profile name** コマンドを使用します。

show ap rf-profile name *profile-name* **detail**

構文の説明

profile-name	RF プロファイルの名前。
detail	選択した RF プロファイルの詳細を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、選択した RF プロファイルの詳細を表示する例を示します。

```
Switch#show ap rf-profile name doctest detail
Description :
AP Group Names :
RF Profile Name : doctest
Band : 2.4 GHz
802.11n client only : Disabled
Transmit Power Threshold v1: -70 dBm
Min Transmit Power: -10 dBm
Max Transmit Power: 30 dBm
Operational Rates
  802.11b 1M Rate : Mandatory
  802.11b 2M Rate : Mandatory
  802.11b 5.5M Rate : Mandatory
  802.11b 11M Rate : Mandatory
  802.11b 6M Rate : Mandatory
  802.11b 9M Rate : Supported
  802.11b 12M Rate : Supported
  802.11b 18M Rate : Supported
  802.11b 24M Rate : Supported
  802.11b 36M Rate : Supported
  802.11b 48M Rate : Supported
  802.11b 54M Rate : Supported
Max Clients : 200
Wlan name                         Max Clients
---------------------------------------------

Trap Threshold
  Clients:  12 clients
  Interference:  10%
  Noise:  -70 dBm
```

```
  Utilization:  80%
Multicast Data Rate: auto
Rx SOP Threshold : auto
Band Select
  Probe Response:  Disabled
  Cycle Count:  2 cycles
  Cycle Threshold:  200 milliseconds
  Expire Suppression:  20 seconds
  Expire Dual Band:  60 seconds
  Client RSSI:  -80 dBm
  Client Mid RSSI:  -80 dBm
Load Balancing
  Window:  5 clients
  Denial:  3 count
Coverage Data
  Data: -80 dBm
  Voice: -80 dBm
 Minimum Client Level: 3 clients
  Exception Level: 25%
DCA Channel List  : 1,5,9,13
DCA Foreign AP Contribution : Enabled
802.11n MCS Rates
  MCS 0 : Enabled
  MCS 1 : Enabled
  MCS 2 : Enabled
  MCS 3 : Enabled
  MCS 4 : Enabled
  MCS 5 : Enabled
  MCS 6 : Enabled
  MCS 7 : Enabled
  MCS 8 : Enabled
  MCS 9 : Enabled
  MCS 10 : Enabled
  MCS 11 : Enabled
  MCS 12 : Enabled
  MCS 13 : Enabled
  MCS 14 : Enabled
  MCS 15 : Enabled
  MCS 16 : Enabled
  MCS 17 : Enabled
  MCS 18 : Enabled
  MCS 19 : Enabled
  MCS 20 : Enabled
  MCS 21 : Enabled
  MCS 22 : Enabled
  MCS 23 : Enabled
  MCS 24 : Enabled
  MCS 25 : Enabled
  MCS 26 : Enabled
  MCS 27 : Enabled
  MCS 28 : Enabled
  MCS 29 : Enabled
  MCS 30 : Enabled
  MCS 31 : Enabled
State : Down
```

show wireless mobility controller ap

サブドメインに参加したアクセスポイントの一覧を表示するには、**wireless mobility controller ap** コマンドを使用します。

show wireless mobility controller ap

構文の説明

ap	サブドメインに参加したアクセスポイントを表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、サブドメインに参加したアクセスポイントを一覧する例を示します。

```
Switch#show wireless mobility controller ap
Number of AP entries in the sub-domain     : 2

AP name                          AP radio MAC      Controller IP     Location
-------------------------------------------------------------------------------------------------
bos2kk                           00f2.8c42.f520    default-group     default-group
IosAP1                           34ed.522f.7e60    default-group     default-group
```

shutdown

RF プロファイルを閉じて、ネットワークを無効にするには、**shutdown** コマンドを使用します。シャットダウンの実行を無効にするには、このコマンドの **no** 形式を使用します。

shutdown

構文の説明

shutdown	プロファイルをシャットダウンし、ネットワークを無効にします。

コマンド デフォルト

なし

コマンド モード

config-rf-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、RF プロファイルを閉じて、ネットワークを無効にする例を示します。

```
Switch(config-rf-profile)#shutdown
```

wlan

AP グループに WLAN を設定するには、**wlan** コマンドを使用します。AP グループから VLAN を削除するには、このコマンドの **no** 形式を使用します。

wlan *wlan-name*

構文の説明

wlan-name	AP グループに設定される WLAN の名前を入力します。

コマンド デフォルト

なし

コマンド モード

config-apgroup

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

なし

次に、AP グループに VLAN を設定する例を示します。

```
Switch(config-apgroup)#wlan docwlan
```

第 X 部

セキュリティ

セキュリティ コマンド

aaa accounting dot1x

認証、認可、およびアカウンティング（AAA）アカウンティングをイネーブルにして、IEEE 802.1x セッションの特定のアカウンティング方式を、回線単位またはインターフェイス単位で定義する方式リストを作成するには **aaa accounting dot1x** グローバル コンフィギュレーション コマンドを使用します。IEEE 802.1x アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting dot1x {*name*| **default** } **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} **. . .**] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**}**. . .**]}
no aaa accounting dot1x {*name*| **default** }

構文の説明

name	サーバ グループ名。これは、**broadcast group** および **group** キーワードの後に入力する場合に使用するオプションです。
default	デフォルト リストにあるアカウンティング方式を、アカウンティング サービス用に指定します。
start-stop	プロセスの開始時に start accounting 通知を送信し、プロセスの終了時に stop accounting 通知を送信します。start アカウンティング レコードはバックグラウンドで送信されます。アカウンティング サーバが start accounting 通知を受け取ったかどうかには関係なく、要求されたユーザ プロセスが開始されます。
broadcast	複数の AAA サーバに送信されるアカウンティング レコードをイネーブルにして、アカウンティング レコードを各グループの最初のサーバに送信します。最初のサーバが利用できない場合、スイッチはバックアップ サーバのリストを使用して最初のサーバを識別します。
group	アカウンティング サービスに使用するサーバ グループを指定します。有効なサーバ グループ名は次のとおりです。 • 名前：サーバ グループの名前。 • **radius** ：すべての RADIUS ホストのリスト。 • **tacacs+** ：すべての TACACS+ ホストのリスト。 **broadcast group** および **group** キーワードの後に入力する場合、**group** キーワードはオプションです。オプションの **group** キーワードより多くの値を入力できます。
radius	（任意）RADIUS アカウンティングをイネーブルにします。
tacacs+	（任意）TACACS+ アカウンティングをイネーブルにします。

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、RADIUS サーバへのアクセスが必要です。

インターフェイスに IEEE 802.1x RADIUS アカウンティングを設定する前に、 **dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを入力することを推奨します。

次の例では、IEEE 802.1x アカウンティングを設定する方法を示します。

```
Switch(config)# aaa new-model
Switch(config)# aaa accounting dot1x default start-stop group radius
```

aaa accounting identity

IEEE 802.1x、MAC 認証バイパス（MAB）、および Web 認証セッションの認証、認可、およびアカウンティング（AAA）アカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで、**aaa accounting identity** コマンドを使用します。IEEE 802.1x アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting identity {*name*| **default** } **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} **. . .**] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} **. . .**] }
no aaa accounting identity {*name*| **default** }

構文の説明

name	サーバ グループ名。これは、**broadcast group** および **group** キーワードの後に入力する場合に使用するオプションです。
default	デフォルト リストにあるアカウンティング方式を、アカウンティング サービス用に使用します。
start-stop	プロセスの開始時に start accounting 通知を送信し、プロセスの終了時に stop accounting 通知を送信します。start アカウンティング レコードはバックグラウンドで送信されます。アカウンティング サーバが start アカウンティング通知を受け取ったかどうかには関係なく、要求されたユーザ プロセスが開始されます。
broadcast	複数の AAA サーバに送信されるアカウンティング レコードをイネーブルにして、アカウンティング レコードを各グループの最初のサーバに送信します。最初のサーバが利用できない場合、スイッチはバックアップ サーバのリストを使用して最初のサーバを識別します。
group	アカウンティング サービスに使用するサーバ グループを指定します。有効なサーバ グループ名は次のとおりです。 • 名前：サーバ グループの名前。 • **radius** ：すべての RADIUS ホストのリスト。 • **tacacs+** ：すべての TACACS+ ホストのリスト。 **broadcast group** および **group** キーワードの後に入力する場合、**group** キーワードはオプションです。オプションの **group** キーワードより多くの値を入力できます。
radius	（任意）RADIUS 認証をイネーブルにします。
tacacs+	（任意）TACACS+ アカウンティングをイネーブルにします。

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

AAA アカウンティング アイデンティティをイネーブルにするには、ポリシー モードをイネーブルにする必要があります。ポリシー モードをイネーブルにするには、特権 EXEC モードで **authentication display new-style** コマンドを入力します。

次の例では、IEEE 802.1x アカウンティング アイデンティティを設定する方法を示します。

```
Switch# authentication display new-style

Please note that while you can revert to legacy style
configuration at any time unless you have explicitly
entered new-style configuration, the following caveats
should be carefully read and understood.

(1) If you save the config in this mode, it will be written
    to NVRAM in NEW-style config, and if you subsequently
    reload the router without reverting to legacy config and
    saving that, you will no longer be able to revert.

(2) In this and legacy mode, Webauth is not IPv6-capable. It
    will only become IPv6-capable once you have entered new-
    style config manually, or have reloaded with config saved
    in 'authentication display new' mode.

Switch# configure terminal
Switch(config)# aaa accounting identity default start-stop group radius
```

aaa authentication dot1x

IEEE 802.1x 認証に準拠するポートで使用する認証、認可、およびアカウンティング（AAA）方式を指定するには、スイッチ スタックまたはスタンドアロン スイッチ上のグローバル コンフィギュレーション モードで **aaa authentication dot1x** コマンドを使用します。認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication dot1x {**default**} *method1*
no aaa authentication dot1x {**default**} *method1*

構文の説明

default	ユーザがログインするときのデフォルトの方法。この引数に続いてリストされた認証方式が使用されます。
method1	サーバ認証を指定します。認証用にすべてのRADIUSサーバの一覧を使用するには、**group radius** キーワードを入力します。 （注） コマンドラインのヘルプ文字列には他のキーワードが表示されますが、サポートされているのは **default** および **group radius** キーワードのみです。

コマンド デフォルト

認証は実行されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

method 引数には、認証アルゴリズムがクライアントからのパスワードを確認するために特定の順序で試みる方式を指定します。IEEE 802.1x に準拠している唯一の方式は、クライアントデータが RADIUS 認証サーバに対して確認される **group radius** 方式です。

group radius を指定した場合、**radius-server host** グローバル コンフィギュレーション コマンドを入力して RADIUS サーバを設定する必要があります。

設定された認証方式の一覧を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

次の例では AAA をイネーブルにして IEEE 802.1x 準拠の認証リストを作成する方法を示します。この認証は、最初に RADIUS サーバとの交信を試みます。この動作でエラーが返信された場合、ユーザはネットワークへのアクセスが許可されません。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
```

aaa authorization

ネットワークへのユーザアクセスを制限するパラメータを設定するには、グローバル コンフィギュレーション モードで **aaa authorization** コマンドを使用します。パラメータを削除するには、このコマンドの **no** 形式を使用します。

aaa authorization { **auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **credential-download** | **exec** | **multicast** | **network** | **reverse-access** | **template** } { **default** | *list_name* } [*method1* [*method2* . . .]]
no aaa authorization { **auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **credential-download** | **exec** | **multicast** | **network** | **reverse-access** | **template** } { **default** | *list_name* } [*method1* [*method2* . . .]]

構文の説明

auth-proxy	認証プロキシ サービスに許可を実行します。
cache	認証、許可、アカウンティング（AAA）サーバを設定します。
commands	指定した特権レベルですべてのコマンドの許可を実行します。
level	許可が必要な特定のコマンド レベル。有効な値は 0 ～ 15 です。
config-commands	コンフィギュレーション モードで入力されたコマンドを許可するかどうかを決定する許可を実行します。
configuration	AAA サーバから設定をダウンロードします。
console	AAA サーバのコンソール許可をイネーブルにします。
credential-download	Local/RADIUS/LDAP から EAP クレデンシャルをダウンロードします。
exec	AAA サーバのコンソール許可をイネーブルにします。
multicast	AAA サーバからマルチキャスト設定をダウンロードします。
network	シリアル ライン インターネット プロトコル（SLIP）、PPP（ポイントツーポイント プロトコル）、PPP ネットワーク コントロール プログラム（NCP）、AppleTalk Remote Access（ARA）など、すべてのネットワーク関連サービス要求について許可を実行します。
reverse-access	リバース Telnet などの逆アクセス接続の許可を実行します。
template	AAA サーバのテンプレート許可をイネーブルにします。
default	このキーワードに続く許可方式のリストを許可のデフォルト方式リストとして使用します。
list_name	許可方式リストの名前の指定に使用する文字列です。

method1［*method2...*］	（任意）許可に使用する 1 つまたは複数の許可方式を指定します。方式には、次の表に示すキーワードのどれでも指定できます。

コマンド デフォルト

すべてのアクションに対する許可がディセーブルになります（方式キーワード**none**と同等）。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

aaa authorization コマンドを使用して、許可をイネーブルにし、名前付きの方式リストを作成します。このリストにはユーザが特定の機能にアクセスするときに使用できる許可方式が定義されます。許可方式リストによって、許可の実行方法とこれらの方式の実行順序が定義されます。方式リストは、一定順序で使用する必要がある許可方式（RADIUS、TACACS+ など）を示す名前付きリストです。方式リストを使用すると、許可に使用するセキュリティ プロトコルを 1 つ以上指定できるため、最初の方式が失敗した場合のバックアップ システムを確保できます。Cisco IOS ソフトウェアでは、特定のネットワーク サービスについてユーザを許可するために最初の方式が使用されます。その方式が応答しない場合、方式リストの次の方式が選択されます。このプロセスは、リスト内の許可方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。

（注） Cisco IOS ソフトウェアでは、前の方式からの応答がない場合にのみ、リストの次の許可方式が試行されます。このサイクルの任意の時点で許可が失敗した場合（つまり、セキュリティ サーバまたはローカル ユーザ名データベースからユーザ サービスの拒否応答が返される場合）、許可プロセスは停止し、その他の許可方式は試行されません。

特定の許可の種類の **aaa authorization** コマンドを、名前付き方式リストを指定しないで発行した場合、名前付き方式リストが明示的に定義されているものを除いて、すべてのインターフェイスまたは回線（この許可の種類が適用される）にデフォルトの方式リストが自動的に適用されます（定義済みの方式リストは、デフォルトの方式リストに優先します）。デフォルトの方式リストが定義されていない場合、許可は実行されません。RADIUS サーバからの IP プールのダウンロードを許可するなどの発信許可は、デフォルトの許可方式リストを使用して実行する必要があります。

aaa authorization コマンドを使用して、*list-name* 引数および *method* 引数に値を入力してリストを作成します。*list-name* にはこのリストの名前として使用する任意の文字列（すべての方式名を除く）を指定し、*method* には特定の順序で試行される許可方式のリストを指定します。

（注） 次の表に、以前定義済みの RADIUS サーバまたは TACACS+ サーバのセットを参照する **group***group-name* 方式、**group ldap** 方式、**group radius** 方式、および **group tacacs+** 方式を示します。ホスト サーバを設定するには、**radius-server host** コマンドおよび **tacacs-server host** コマンドを使用します。サーバの名前付きグループを作成するには、**aaa group server radius** コマンド、**aaa group server ldap** コマンドおよび **aaa group server tacacs+** コマンドを使用します。

この表では、method キーワードについて説明します。

表 *24 : AAA* 許可方式

キーワード	説明
cache *group-name*	キャッシュ サーバ グループを許可に使用します。
group *group-name*	アカウンティングに、**server group** *group-name* コマンドで定義される RADIUS または TACACS+ サーバのサブセットを使用します。
group ldap	許可にすべての Lightweight Directory Access Protocol（LDAP）サーバのリストを使用します。
group radius	**aaa group server radius** コマンドで定義されるすべての RADIUS サーバのリストを認証に使用します。
grouptacacs+	**aaa group server tacacs+** コマンドで定義されるすべての TACACS+ サーバのリストを認証に使用します。
if-authenticated	許可された場合、ユーザは要求した機能にアクセスできます。 （注） **if-authenticated** 方式は終端の方式です。したがって、方式としてリストされている場合、その後にリストされたどの方式も評価されません。
local	許可にローカル データベースを使用します。
none	許可が行われないことを示します。

Cisco IOS ソフトウェアは、許可について次の方式をサポートします。

- Cache Server Groups：ルータはキャッシュ サーバ グループを調べて、特定の権限をユーザに許可します。

- If-Authenticated：ユーザが認証に成功した場合、ユーザは要求した機能にアクセスできます。
- Local：ルータまたはアクセス サーバは、**username** コマンドの定義に従ってローカル データベースに問い合わせ、特定の権限をユーザに許可します。ローカルデータベースでは制御できるのは、一部の機能だけです。
- None：ネットワーク アクセス サーバは、許可情報を要求しません。許可は、この回線/インターフェイスで実行されません。
- RADIUS：ネットワーク アクセス サーバは RADIUS セキュリティ サーバからの許可情報を要求します。RADIUS 認可では、属性を関連付けることでユーザに固有の権限を定義します。属性は適切なユーザとともに RADIUS サーバ上のデータベースに保存されます。
- TACACS+：ネットワーク アクセス サーバは、TACACS+ セキュリティ デーモンと許可情報を交換します。TACACS+ 許可は、属性値（AV）ペアを関連付けることでユーザに特定の権限を定義します。属性ペアは適切なユーザとともに TACACS+ セキュリティ サーバのデータベースに保存されます。

方式リストは、要求されている許可のタイプによって異なります。AAA は 5 種類の許可方式をサポートしています。

- Commands：ユーザが発行する EXEC モード コマンドに適用します。コマンドの認可は、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、認可を試行します。
- EXEC：ユーザ EXEC ターミナル セッションに関連付けられた属性に適用します。
- Network：ネットワーク接続に適用します。ネットワーク接続には、PPP、SLIP、または ARA 接続が含まれます。

（注） **aaa authorization config-commands** コマンドを設定して、先頭に **do** コマンドが追加される EXEC コマンドを含む、グローバル コンフィギュレーション コマンドを許可する必要があります。

- Reverse Access：リバース Telnet セッションに適用されます。
- Configuration：AAA サーバからダウンロードされた設定に適用されます。

名前付き方式リストを作成すると、指定した許可タイプに対して特定の許可方式リストが定義されます。

定義されると、方式リストを特定の回線またはインターフェイスに適用してから、定義済み方式のいずれかを実行する必要があります。

authorization コマンドにより、許可プロセスの一環として、一連の AV のペアを含む要求パケットが RADIUS または TACACS+ デーモンに送信されます。デーモンは、次のいずれかのアクションを実行できます。

- 要求をそのまま受け入れます。
- 要求を変更します。
- 要求および許可を拒否します。

サポートされるRADIUS属性のリストについては、RADIUS属性のモジュールを参照してください。サポートされる TACACS+ の AV ペアのリストについては、TACACS+ 属性値ペアのモジュールを参照してください。

（注） 次の5個のコマンドは、特権レベル0と対応しています。**disable**、**enable**、**exit**、**help**、**logout**。特権レベルの AAA 認証を 0 より大きい値に設定した場合、これらの 5 個のコマンドは特権レベル コマンド セットに含まれません。

次に、PPP を使用するシリアル回線に RADIUS の許可を使用するように指定する mygroup というネットワーク許可方式リストを定義する例を示します。RADIUS サーバが応答しない場合、ローカル ネットワークの許可が実行されます。

```
Switch(config)#  aaa authorization network mygroup group radius local
```

aaa new-model

認証、認可、およびアカウンティング（AAA）アクセス制御モデルを有効にするには、グローバル コンフィギュレーション モードで **aaanew-model** コマンドを使用します。AAA アクセス制御モデルを無効にするには、このコマンドの **no** 形式を使用します。

aaa new-model
no aaa new-model

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

AAA が有効になっていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2SE	このコマンドが Cisco Catalyst 3850 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドにより、AAA アクセス制御システムが有効になります。

仮想端末回線（VTY）に関して **login local** コマンドが設定されている場合、**aaa new-model** コマンドを削除するときは、スイッチをリロードしてデフォルト設定または **login** コマンドを取得する必要があります。スイッチをリロードしない場合、スイッチは、VTY ではデフォルトで **login local** コマンドに設定されます。

（注） **aaa new-model** コマンドを削除することは推奨されません。

次に、この制限の例を示します。

```
Switch(config)# aaa new-model
Switch(config)# line vty 0 15
Switch(config-line)# login local
Switch(config-line)# exit
Switch(config)# no aaa new-model
Switch(config)# exit
Switch# show running-config | b line vty

line vty 0 4
 login local  !<=== Login local instead of "login"
line vty 5 15
 login local
!
```

例

次に、AAA を初期化する例を示します。

```
Switch(config)# aaa new-model
Switch(config)#
```

関連コマンド

Command	Description
aaaaccounting	課金またはセキュリティ目的のために、要求されたサービスの AAA アカウンティングをイネーブルにします。
aaaauthenticationarap	TACACS+ を使用する ARAP の AAA 認証方式を有効にします。
aaaauthenticationenabledefault	ユーザが特権コマンド レベルにアクセスできるかどうかを決定する AAA 認証を有効にします。
aaaauthenticationlogin	ログイン時の AAA 認証を設定します。
aaaauthenticationppp	PPP を実行しているシリアル インターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
aaaauthorization	ネットワークへのユーザ アクセスを制限するパラメータを設定します。

access-session mac-move deny

スイッチ 上での MAC 移動をディセーブルにするには、**access-session mac-move deny** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

access-session mac-move deny
no access-session mac-move deny

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

MAC 移動はイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドの **no** 形式を使用すると、認証済みホストをスイッチ上の認証対応ポート（MAC 認証バイパス [MAB]、802.1x、または Web-auth）間で移動することができます。たとえば、認証されたホストとポートの間にデバイスがあり、そのホストが別のポートに移動した場合、認証セッションは最初のポートから削除され、ホストは新しいポート上で再認証されます。

MAC 移動がディセーブルで、認証されたホストが別のポートに移動した場合、そのホストは再認証されず、違反エラーが発生します。

次の例では、スイッチ上で MAC 移動をイネーブルにする方法を示します。

```
Switch(config)# no access-session mac-move deny
```

関連コマンド

コマンド	説明
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。

コマンド	説明
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポートプライオリティリストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウトパラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートにすでに最大数のデバイスが接続しているときに、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャイベントに関する情報を表示します。

action

VLAN アクセス マップ エントリのアクションを設定するには、アクセスマップ コンフィギュレーション モードで **action** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

action{**drop**|**forward**}
no action

構文の説明

drop	指定された条件に一致する場合に、パケットをドロップします。
forward	指定された条件に一致する場合に、パケットを転送します。

コマンド デフォルト

デフォルトのアクションは、パケットの転送です。

コマンド モード

アクセス マップ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

vlan access-map グローバル コンフィギュレーション コマンドを使用して、アクセス マップ コンフィギュレーション モードを開始します。

アクションが **drop** の場合は、一致条件でのアクセス コントロール リスト（ACL）名の設定など、アクセス マップを定義した後に、そのマップを VLAN に適用する必要があります。定義しない場合、すべてのパケットがドロップされることがあります。

アクセス マップ コンフィギュレーション モードでは、**match access-map** コンフィギュレーション コマンドを使用して、VLAN マップの一致条件を定義します。**action** コマンドを使用すると、パケットが条件に一致したときに実行するアクションを設定できます。

drop パラメータおよび forward パラメータは、このコマンドの **no** 形式では使用されません。

設定を確認するには、**show vlan access-map** 特権 EXEC コマンドを入力します。

次の例では、VLAN アクセス マップ vmap4 を指定し VLAN 5 と VLAN 6 に適用する方法を示します。このアクセス マップは、パケットがアクセス リスト al2 に定義された条件に一致する場合に、VLAN がその IP パケットを転送するように指定します。

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

authentication host-mode

ポートで認証マネージャ モードを設定するには、インターフェイス コンフィギュレーション モードで **authentication host-mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

authentication host-mode {**multi-auth** | **multi-domain** | **multi-host** | **single-host**}
no authentication host-mode

構文の説明

multi-auth	ポートのマルチ認証モード（multi-auth モード）をイネーブルにします。
multi-domain	ポートのマルチドメイン モードをイネーブルにします。
multi-host	ポートのマルチホスト モードをイネーブルにします。
single-host	ポートのシングルホスト モードをイネーブルにします。

コマンド デフォルト

シングルホスト モードがイネーブルにされています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

接続されているデータ ホストが 1 つだけの場合は、シングルホスト モードを設定する必要があります。シングルホスト ポートでの認証のために音声デバイスを接続しないでください。ポートで音声 VLAN が設定されていないと、音声デバイスの許可が失敗します。

データ ホストが IP フォン経由でポートに接続されている場合は、マルチドメイン モードを設定する必要があります。音声デバイスを認証する必要がある場合は、マルチドメインモードを設定する必要があります。

ハブの背後にデバイスを配置し、それぞれを認証してポートアクセスのセキュリティを確保できるようにするには、マルチ認証モードに設定する必要があります。音声 VLAN が設定されている場合は、このモードで認証できる音声デバイスは 1 つだけです。

マルチホストモードでも、ハブ越しの複数ホストのためのポートアクセスが提供されますが、マルチホスト モードでは、最初のユーザが認証された後でデバイスに対して無制限のポートアクセスが与えられます。

次の例では、ポートのマルチ認証モードをイネーブルにする方法を示します。

```
Switch(config-if)# authentication host-mode multi-auth
```

次の例では、ポートのマルチドメイン モードをイネーブルにする方法を示します。

```
Switch(config-if)# authentication host-mode multi-domain
```

次の例では、ポートのマルチホスト モードをイネーブルにする方法を示します。

```
Switch(config-if)# authentication host-mode multi-host
```

次の例では、ポートのシングルホスト モードをイネーブルにする方法を示します。

```
Switch(config-if)# authentication host-mode single-host
```

設定を確認するには、**show authentication sessions interface** *interface* **details** 特権 EXEC コマンドを入力します。

authentication mac-move permit

スイッチ上でのMAC移動をイネーブルにするには、グローバル コンフィギュレーション モードで **authentication mac-move permit** コマンドを使用します。MAC 移動をディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication mac-move permit
no authentication mac-move permit

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

MAC 移動は無効になっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

これはレガシー コマンドです。新しいコマンドは **access-session mac-move deny** です。

このコマンドを使用すると、スイッチ上の 認証対応ポート（MAC 認証バイパス [MAB]、802.1x、または Web-auth）間で認証ホストを移動できます。たとえば、認証されたホストとポートの間にデバイスがあり、そのホストが別のポートに移動した場合、認証セッションは最初のポートから削除され、ホストは新しいポート上で再認証されます。

MAC 移動がディセーブルで、認証されたホストが別のポートに移動した場合、そのホストは再認証されず、違反エラーが発生します。

次の例では、スイッチ上で MAC 移動をイネーブルにする方法を示します。

```
Switch(config)# authentication mac-move permit
```

関連コマンド

コマンド	説明
access-session mac-move deny	スイッチで MAC 移動をディセーブルにします。
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。

コマンド	説明
authentication host-mode	ポートで認証マネージャモードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートの再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポート プライオリティ リストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウト パラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートにすでに最大数のデバイスが接続しているときに、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

authentication priority

プライオリティ リストに認証方式を追加するには、インターフェイス コンフィギュレーション モードで **authentication priority** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

authentication priority ［**dot1x** | **mab**］｛**webauth**｝
no authentication priority ［**dot1x** | **mab**］｛**webauth**｝

構文の説明

dot1x	（任意）認証方式の順序に 802.1x を追加します。
mab	（任意）認証方式の順序にMAC認証バイパス（MAB）を追加します。
webauth	認証方式の順序に Web 認証を追加します。

コマンド デフォルト

デフォルトのプライオリティは、802.1x 認証、MAC 認証バイパス、Web 認証の順です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

順序付けでは、スイッチがポートに接続された新しいデバイスを認証しようとするときに試行する方式の順序を設定します。

ポートにフォールバック方式を複数設定するときは、Web 認証（webauth）を最後に設定してください。

異なる認証方式にプライオリティを割り当てることにより、プライオリティの高い方式を、プライオリティの低い進行中の認証方式に割り込ませることができます。

（注） クライアントがすでに認証されている場合に、プライオリティの高い方式の割り込みが発生すると、再認証されることがあります。

認証方式のデフォルトのプライオリティは、実行リストの順序におけるその位置と同じで、802.1x 認証、MAC 認証バイパス（MAB）、Web 認証の順です。このデフォルトの順序を変更するには、キーワード **dot1x**、**mab**、および **webauth** を使用します。

次の例では、802.1x を最初の認証方式、Web 認証を 2 番めの認証方式として設定する方法を示します。

```
Switch(config-if)# authentication priority dotx webauth
```

次の例では、MAB を最初の認証方式、Web 認証を 2 番めの認証方式として設定する方法を示します。

```
Switch(config-if)# authentication priority mab webauth
```

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event fail	認証マネージャが認証エラーを認識されないユーザ クレデンシャルの結果として処理する方法を指定します。
authentication event no-response action	認証マネージャが認証エラーを応答のないホストの結果として処理する方法を指定します。
authentication event server alive action reinitialize	以前に到達不能であった認証、許可、アカウンティング サーバが使用可能になったときに認証マネージャセッションを再初期化します。
authentication event server dead action authorize	認証、許可、アカウンティング サーバが到達不能になったときに認証マネージャ セッションを許可します。
authentication fallback	Web 認証のフォール バック方式をイネーブルにします。
authentication host-mode	ホストの制御ポートへのアクセスを許可します。
authentication open	ポートでオープン アクセスをイネーブルにします。
authentication order	認証マネージャがポート上のクライアントの認証を試みる順序を指定します。
authentication periodic	ポートの自動再認証をイネーブルにします。
authentication port-control	制御ポートの許可ステートを設定します。
authentication timer inactivity	機能しない認証マネージャ セッションを強制終了するまでの時間を設定します。

コマンド	説明
authentication timer reauthenticate	認証マネージャが許可ポートの再認証を試みる間隔を指定します。
authentication timer restart	認証マネージャが無許可ポートの認証を試みる間隔を指定します。
authentication violation	ポート上でセキュリティ違反が生じた場合に取るアクションを指定します。
mab	ポートのMAC認証バイパスをイネーブルにします。
show authentication registrations	認証マネージャに登録されている認証方式に関する情報を表示します。
show authentication sessions	現在の認証マネージャ セッションに関する情報を表示します。
show authentication sessions interface	特定のインターフェイスの認証マネージャに関する情報を表示します。

authentication violation

新しいデバイスがポートに接続されたとき、または最大数のデバイスがポートに接続されている状態で新しいデバイスがポートに接続されたときに発生する違反モードを設定するには、インターフェイス コンフィギュレーション モードで **authentication violation** コマンドを使用します。

authentication violation { **protect** | **replace** | **restrict** | **shutdown** }
no authentication violation { **protect** | **replace** | **restrict** | **shutdown** }

構文の説明

protect	予期しない着信 MAC アドレスをドロップします。syslog エラーは生成されません。
replace	現在のセッションを削除し、新しいホストによる認証を開始します。
restrict	違反エラーの発生時に Syslog エラーを生成します。
shutdown	エラーによって、予期しない MAC アドレスが発生するポートまたは仮想ポートがディセーブルになります。

コマンド デフォルト

Authentication violation shutdown モードがイネーブルにされています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ポート上でセキュリティ違反が発生したときに実行するアクションを指定するには、**authentication violation** コマンドを使用します。

次の例では、新しいデバイスがポートに接続する場合に、errdisable になり、シャットダウンするように IEEE 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# authentication violation shutdown
```

次の例では、新しいデバイスがポートに接続する場合に、システム エラー メッセージを生成して、ポートを制限モードに変更するように 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# authentication violation restrict
```

次の例では、新しいデバイスがポートに接続するときに、そのデバイスを無視するように 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# authentication violation protect
```

次の例では、新しいデバイスがポートに接続するときに、現在のセッションを削除し、新しいデバイスによる認証を開始するように 802.1x 対応ポートを設定する方法を示します。

```
Switch(config-if)# authentication violation replace
```

設定を確認するには、**show authentication** 特権 EXEC コマンドを入力します。

auto security

グローバルな自動セキュリティを設定するには、グローバル コンフィギュレーション モードで **auto security** コマンドを使用します。自動セキュリティを無効にするには、このコマンドの **no** 形式を使用します。

auto security
no auto security

このコマンドには、引数およびキーワードはありません。

コマンド デフォルト

自動セキュリティがグローバルに有効化されました。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(5)E	このコマンドは、Cisco IOS Release 15.2(5)E よりも前のリリースで導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードで自動セキュリティを設定すると、すべてのインターフェイスで自動セキュリティが有効になります。自動セキュリティを無効にすると、すべてのインターフェイスで無効になります。

特定のインターフェイスで自動セキュリティを有効にするには、インターフェイス コンフィギュレーション モードで **auto security-port** コマンドを使用します。

（注） Cisco IOS リリース 15.2(5)E では、グローバル コンフィギュレーション モードで **auto security** コマンドが設定されると、インターフェイス上で自動セキュリティが有効になります。ただし、**autosecurity-port** {**host** |**uplink**} コマンドはインターフェイスの設定には明示的に保存されません。自動セキュリティがあるインターフェイス上で設定され、**autosecurity-port** {**host** |**uplink**} コマンドがインターフェイスから削除されると、**no autosecurity-port** {**host** |**uplink**} コマンドはインターフェイスの設定に保存されます。

次に、自動セキュリティをグローバルで有効にする例を示します。

```
Switch(config)# auto security
```

関連コマンド

コマンド	説明
auto security-port	インターフェイス上で自動セキュリティを設定します。
show auto security	自動セキュリティ ステータスを表示します。

auto security-port

あるインターフェイスで自動セキュリティを有効にするには、インターフェイス コンフィギュレーション モードで **auto security-port** コマンドを使用します。インターフェイスで自動セキュリティを無効にするには、このコマンドの **no** 形式を使用します。

auto security {**host** | **uplink**}
no auto security

構文の説明

host	ホスト ポートの自動セキュリティを設定します。
uplink	アップリンク ポートの自動セキュリティを設定します。

コマンド デフォルト

自動セキュリティはすべてのインターフェイス上で無効です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(5)E	このコマンドは、Cisco IOS Release 15.2(5)E よりも前のリリースで導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードで **auto security** コマンドを使用して、自動セキュリティをグローバルに有効化できます。

（注） Cisco IOS リリース 15.2(5)E では、グローバル コンフィギュレーション モードで **auto security** コマンドが設定されると、インターフェイス上で自動セキュリティが有効になります。ただし、**autosecurity-port** {**host** | **uplink**} コマンドはインターフェイスの設定には明示的に保存されません。自動セキュリティがあるインターフェイス上で設定され、**autosecurity-port** {**host** | **uplink**} コマンドがインターフェイスから削除されると、**no autosecurity-port** {**host** | **uplink**} コマンドはインターフェイスの設定に保存されます。

次に、インターフェイスで自動セキュリティを設定する例を示します。

```
Switch(config)# interface gigabitethernet 1/0/2
Switch(config-if)# auto security-port host
```

関連コマンド

コマンド	説明
auto security	グローバルな自動セキュリティを設定します。
show auto security	自動セキュリティ ステータスを表示します。

cisp enable

スイッチ上で Client Information Signalling Protocol（CISP）を有効にして、サプリカント スイッチのオーセンティケータとして機能し、オーセンティケータ スイッチのサプリカントとして機能するようにするには、**cisp enable** グローバル コンフィギュレーション コマンドを使用します。

cisp enable
no cisp enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドはCisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされていませんでした。

使用上のガイドライン

オーセンティケータとサプリカント スイッチの間のリンクはトランクです。両方のスイッチで VTP をイネーブルにする場合は、VTP ドメイン名が同一であり、VTP モードがサーバである必要があります。

VTPモードを設定する場合にMD5チェックサムの不一致エラーにならないようにするために、次の点を確認してください。

- VLAN が異なる 2 台のスイッチに設定されていないこと。同じドメインに VTP サーバが 2 台存在することがこの状態の原因になることがあります。
- 両方のスイッチで、設定のリビジョン番号が異なっていること。

次の例では、CISP をイネーブルにする方法を示します。

```
Switch(config)# cisp enable
```

関連コマンド

コマンド	説明
dot1x credentialsプロファイル	プロファイルをサプリカント スイッチに設定します。
dot1x supplicant force-multicast	802.1Xサプリカントがマルチキャストパケットを送信するように強制します。
dot1x supplicant controlled transient	802.1X サプリカントによる制御アクセスを設定します。
show cisp	指定されたインターフェイスのCISP情報を表示します。

clear errdisable interface vlan

error-disabled 状態になっていた VLAN を再びイネーブルにするには、特権 EXEC モードで **clear errdisable interface** コマンドを使用します。

clear errdisable interface *interface-id* **vlan** ［*vlan-list*］

構文の説明

interface-id	インターフェイスを指定します。
vlan list	（任意）再びイネーブルにする VLAN のリストを指定します。VLAN リストを指定しない場合は、すべての VLAN が再びイネーブルになります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

shutdown および **no shutdown** のインターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにするか、**clear errdisable** インターフェイス コマンドを使用して VLAN の error-disabled をクリアできます。

次の例では、ギガビット イーサネット ポート 4/0/2 で errdisable になっているすべての VLAN を再びイネーブルにする方法を示します。

```
Switch# clear errdisable interface gigabitethernet4/0/2 vlan
```

関連コマンド

コマンド	説明
errdisable detect cause	特定の原因、またはすべての原因に対して errdisable 検出をイネーブルにします。
errdisable recovery	回復メカニズム変数を設定します。
show errdisable detect	errdisable 検出ステータスを表示します。
show errdisable recovery	errdisable 回復タイマーの情報を表示します。

コマンド	説明
show interfaces status err-disabled	errdisable ステートになっているインターフェイスのリストのインターフェイス ステータスを表示します。

clear mac address-table

特定のダイナミック アドレス、特定のインターフェイス上のすべてのダイナミック アドレス、スタック メンバ上のすべてのダイナミック アドレス、または特定の VLAN 上のすべてのダイナミック アドレスを MAC アドレス テーブルから削除するには、**clear mac address-table** コマンドを特権 EXEC モードで使用します。このコマンドはまた MAC アドレス通知グローバル カウンタもクリアします。

clear mac address-table {**dynamic** [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*] | **move update** | **notification**}

構文の説明

dynamic	すべてのダイナミック MAC アドレスを削除します。
address *mac-addr*	（任意）指定されたダイナミック MAC アドレスを削除します。
interface *interface-id*	（任意）指定された物理ポートまたはポート チャネル上のすべてのダイナミック MAC アドレスを削除します。
vlan *vlan-id*	（任意）指定された VLAN のすべてのダイナミック MAC アドレスを削除します。指定できる範囲は 1 ～ 4094 です。
move update	MAC アドレス テーブルの move-update カウンタをクリアします。
notification	履歴テーブルの通知をクリアし、カウンタをリセットします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

show mac address-table 特権 EXEC コマンドを入力することにより、情報が削除されたかどうかを確認できます。

次の例では、ダイナミック アドレス テーブルから特定の MAC アドレスを削除する方法を示します。

```
Switch# clear mac address-table dynamic address 0008.0070.0007
```

関連コマンド

コマンド	説明
mac address-table notification	MAC アドレス通知機能をイネーブルにします。
mac address-table move update {**receive** | **transmit**}	スイッチ上の MAC アドレス テーブル移行更新を設定します。
show mac address-table	MAC アドレス テーブルのスタティック エントリおよびダイナミック エントリを表示します。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。
show mac address-table notification	**interface** キーワードが追加されると、すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
snmp trap mac-notification change	特定のインターフェイスの SNMP MAC アドレス通知トラップをイネーブルにします。

deny（MAC アクセス リスト コンフィギュレーション）

条件が一致した場合に非 IP トラフィックが転送されるのを防止するには、スイッチ スタックまたはスタンドアロン スイッチ上で **deny** MAC アクセスリスト コンフィギュレーション コマンドを使用します。名前付き MAC アクセス リストから拒否条件を削除するには、このコマンドの **no** 形式を使用します。

deny {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**] [**cos** *cos*]
no deny {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**] [**cos** *cos*]

構文の説明

any	すべての送信元または宛先MACアドレスを拒否します。
host *src-MAC-addr* | *src-MAC-addr mask*	ホスト MAC アドレスと任意のサブネット マスクを定義します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP トラフィックは拒否されます。
host *dst-MAC-addr* | *dst-MAC-addr mask*	宛先 MAC アドレスと任意のサブネット マスクを定義します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。
type mask	（任意）パケットのEtherType番号と、Ethernet IIまたはSNAPカプセル化を指定して、パケットのプロトコルを識別します。 type には、0 ～ 65535 の 16 進数を指定できます。 mask は、一致をテストする前に EtherType に適用される don't care ビットのマスクです。
aarp	（任意）データリンク アドレスをネットワーク アドレスにマッピングする EtherType AppleTalk Address Resolution Protocol を指定します。

amber	（任意）EtherType DEC-Amber を指定します。
appletalk	（任意）EtherType AppleTalk/EtherTalk を指定します。
dec-spanning	（任意）EtherType Digital Equipment Corporation（DEC）スパニングツリーを指定します。
decnet-iv	（任意）EtherType DECnet Phase IV プロトコルを指定します。
diagnostic	（任意）EtherType DEC-Diagnostic を指定します。
dsm	（任意）EtherType DEC-DSM を指定します。
etype-6000	（任意）EtherType 0x6000 を指定します。
etype-8042	（任意）EtherType 0x8042 を指定します。
lat	（任意）EtherType DEC-LAT を指定します。
lavc-sca	（任意）EtherType DEC-LAVC-SCA を指定します。
lsap *lsap-number mask*	（任意）パケットの LSAP 番号（0 ～ 65535）と 802.2 カプセル化を使用して、パケットのプロトコルを指定します。 *mask* は、一致をテストする前に LSAP 番号に適用される don't care ビットのマスクです。
mop-console	（任意）EtherType DEC-MOP Remote Console を指定します。
mop-dump	（任意）EtherType DEC-MOP Dump を指定します。
msdos	（任意）EtherType DEC-MSDOS を指定します。
mumps	（任意）EtherType DEC-MUMPS を指定します。
netbios	（任意）EtherType DEC-Network Basic Input/Output System（NetBIOS）を指定します。
vines-echo	（任意）Banyan Systems による EtherType Virtual Integrated Network Service（VINES）Echo を指定します。

vines-ip	（任意）EtherType VINES IP を指定します。
xns-idp	（任意）10 進数、16 進数、または 8 進数の任意の Ethertype である EtherType Xerox Network Systems（XNS）プロトコル スイート（0 ～ 65535）を指定します。
cos *cos*	（任意）プライオリティを設定するため、0 ～ 7 までのサービス クラス（CoS）値を指定します。CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。**cos** オプションが設定されているかどうかを確認する警告メッセージが表示されます。

コマンド デフォルト

このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルト アクションは拒否です。

コマンド モード

MAC アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

MAC アクセス リスト コンフィギュレーション モードを開始するには、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。

host キーワードを使用した場合、アドレス マスクは入力できません。**host** キーワードを使用しない場合は、アドレス マスクを入力する必要があります。

アクセス コントロール エントリ（ACE）がアクセス コントロール リストに追加された場合、リストの最後には暗黙の **deny-any-any** 条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap** *lsap mask* キーワードを使用します。Novell 用語と Cisco IOS 用語での IPX カプセル化タイプに対応するフィルタ条件を表に一覧表示します。

表 *25 : IPX* フィルタ基準

IPX カプセル化タイプ		**フィルタ基準**
Cisco IOS 名	**Novel 名**	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137

IPX カプセル化タイプ		フィルタ基準
Cisco IOS 名	Novel 名	
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

次の例では、すべての送信元から MAC アドレス 00c0.00a0.03fa への NETBIOS トラフィックを拒否する名前付き MAC 拡張アクセス リストを定義する方法を示します。このリストに一致するトラフィックは拒否されます。

```
Switch(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

次の例では、名前付き MAC 拡張アクセス リストから拒否条件を削除する方法を示します。

```
Switch(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

次の例では、EtherType 0x4321 のすべてのパケットを拒否します。

```
Switch(config-ext-macl)# deny any any 0x4321 0
```

設定を確認するには、**show access-lists** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mac access-list extended	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
permit	MACアクセスリストコンフィギュレーションから許可します。 条件が一致した場合に非 IP トラフィックが転送されるのを許可します。
show access-lists	スイッチに設定されたアクセス コントロール リストを表示します。

device-role（IPv6 スヌーピング）

ポートに接続されているデバイスのロールを指定するには、IPv6 スヌーピング コンフィギュレーション モードで **device-role** コマンドを使用します。

device-role {**node** | **switch**}

構文の説明

node	接続されたデバイスのロールをノードに設定します。
switch	接続されたデバイスのロールをスイッチに設定します。

コマンド デフォルト

デバイスのロールはノードです。

コマンド モード

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

device-role コマンドは、ポートに接続されているデバイスのロールを指定します。デフォルトでは、デバイスのロールはノードです。

switch キーワードは、リモート デバイスがスイッチであり、ローカル スイッチがマルチスイッチ モードで動作していることを示します。ポートで学習したバインディング エントリは、trunk_port プリファレンス レベルでマークされます。ポートが trusted ポートに設定されている場合、バインディング エントリは trunk_trusted_port プリファレンス レベルでマークされます。

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、デバイスを IPv6 スヌーピング コンフィギュレーション モードにし、デバイスをノードとして設定する例を示します。

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# device-role node
```

device-role（IPv6 ND 検査）

ポートに接続されているデバイスのロールを指定するには、ネイバー探索（ND）インスペクション ポリシー コンフィギュレーション モードで **device-role** コマンドを使用します。

device-role {**host** | **monitor** | **router** | **switch**}

構文の説明

host	接続されたデバイスのロールをホストに設定します。
monitor	接続されたデバイスのロールをモニタに設定します。
router	接続されたデバイスのロールをルータに設定します。
switch	接続されたデバイスのロールをスイッチに設定します。

コマンド デフォルト

デバイスのロールはホストです。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

device-role コマンドは、ポートに接続されているデバイスのロールを指定します。デフォルトでは、デバイスのロールはホストであるため、すべての着信ルータ アドバタイズメントとリダイレクト メッセージはブロックされます。デバイス ロールが **router** キーワードを使用してイネーブルになっている場合、このポートですべてのメッセージ（ルータ送信要求（RS）、ルータ アドバタイズメント（RA）、またはリダイレクト）が許可されます。

router または **monitor** キーワードが使用されている場合、マルチキャストの RS メッセージは限定ブロードキャストがイネーブルかどうかに関係なく、ポート上でブリッジされます。ただし、monitor キーワードは着信 RA またはリダイレクト メッセージを許可しません。monitor キーワードを使用すると、これらのメッセージを必要とするデバイスがそれらを受け取ります。

switch キーワードは、リモートデバイスがスイッチであり、ローカル スイッチがマルチスイッチ モードで動作していることを示します。ポートで学習したバインド エントリは、trunk_port プリファレンス レベルでマークされます。ポートが trusted ポートに設定されている場合、バインディング エントリは trunk_trusted_port プリファレンス レベルでマークされます。

次に、Neighbor Discovery Protocol（NDP）ポリシー名を policy1 と定義し、デバイスを ND インスペクション ポリシー コンフィギュレーション モードにして、デバイスをホストとして設定する例を示します。

```
Switch(config)#  ipv6 nd inspection policy policy1
```

```
Switch(config-nd-inspection)# device-role host
```

device-tracking policy

スイッチ統合型セキュリティ機能（SISF）ベースの IP デバイス トラッキング ポリシーを設定するには、グローバル コンフィギュレーション モードで **device-tracking** コマンドを使用します。デバイス トラッキング ポリシーを削除するには、このコマンドの **no** 形式を使用します。

device -tracking policy *policy-name*
no device-tracking policy *policy-name*

構文の説明

policy-name	デバイス トラッキング ポリシーのユーザ定義名。ポリシー名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。

コマンド デフォルト

デバイス トラッキング ポリシーは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

デバイス トラッキング ポリシーを作成するには、SISF ベースの **device-tracking policy** コマンドを使用します。**device-tracking policy** コマンドがイネーブルの場合、コンフィギュレーション モードが デバイストラッキング コンフィギュレーション モードに変更されます。このモードでは、管理者が次のファーストホップ セキュリティ コマンドを設定できます。

- （任意）**device-role**{**node**] | **switch**}：ポートに接続されたデバイスの役割を指定します。デフォルトは **node** です。
- （任意）**limit address-count** *value*：ターゲットごとに許可されるアドレス数を制限します。
- （任意）**no**：コマンドを無効にするか、またはそのデフォルトに設定します。
- （任意）**destination-glean**{**recovery**| **log-only**}[**dhcp**]}：データ トラフィックの送信元アドレス グリーニングによるバインディング テーブルの回復をイネーブルにします。
- （任意）**data-glean**{**recovery**| **log-only**}[**dhcp** | **ndp**]}：送信元アドレスまたはデータ アドレスのグリーニングを使用したバインディング テーブルの回復をイネーブルにします。
- （任意）**security-level**{**glean**|**guard**|**inspect**}：この機能によって適用されるセキュリティのレベルを指定します。デフォルトは **guard** です。

  glean：メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。

  guard：アドレスを収集し、メッセージを検査します。さらに、RA および DHCP サーバ メッセージを拒否します。これがデフォルトのオプションです。

inspect：アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。

- （任意）**tracking** {**disable** | **enable**}：トラッキング オプションを指定します。
- （任意）**trusted-port**：信頼できるポートを設定します。これにより、該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。

次に、デバイストラッキング ポリシーを設定する例を示します。

```
Switch(config)# device-tracking policy policy1
Switch(config-device-tracking)# trusted-port
```

dot1x critical（グローバル コンフィギュレーション）

IEEE 802.1X クリティカル認証パラメータを設定するには、グローバル コンフィギュレーション モードで **dot1x critical** コマンドを使用します。

dot1x critical eapol

構文の説明

eapol	スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。

コマンド デフォルト

eapol はディセーブルです

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するよう指定する例を示します。

```
Switch(config)# dot1x critical eapol
```

dot1x max-start

もう一方の端で 802.1X が認識されないと判断されるまでにサプリカントがクライアントに送信する（応答が受信されないと想定）Extensible Authentication Protocol over LAN（EAPOL）開始フレームの最大数を設定するには、インターフェイス コンフィギュレーション モードで **dot1x max-start** コマンドを使用します。最大回数の設定を削除するには、このコマンドの **no** 形式を使用します。

dot1x max-start *number*
no dot1x max-start

構文の説明

number	ルータが EAPOL 開始フレームを送信する最大回数を指定します。1 ～ 10 の値を指定できます。デフォルトは 3 です。

コマンド デフォルト

デフォルトの最大数の設定は 3 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを入力する前に、スイッチポートで **switchport mode access** インターフェイス コンフィギュレーション コマンドを入力する必要があります。

次に、EAPOL 開始要求の最大数が 5 に設定されている例を示します。

```
Switch(config)# interface g1/0/3
Switch(config-if)# dot1x max-start 5
```

dot1x pae

Port Access Entity（PAE）タイプを設定するには、インターフェイス コンフィギュレーション モードで **dot1x pae** コマンドを使用します。設定された PAE タイプをディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x pae {**supplicant** | **authenticator**}
no dot1x pae {**supplicant** | **authenticator**}

構文の説明

supplicant	インターフェイスはサプリカントとしてだけ機能し、オーセンティケータ向けのメッセージに応答しません。
authenticator	インターフェイスはオーセンティケータとしてだけ動作し、サプリカント向けのメッセージに応答しません。

コマンド デフォルト

PAE タイプは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドはCisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされていませんでした。

使用上のガイドライン

IEEE 802.1x 認証をポート上でディセーブルにする場合は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

dot1x port-control インターフェイス コンフィギュレーション コマンドを入力するなどしてポート上で IEEE 802.1x 認証を設定した場合、スイッチは自動的にポートを IEEE 802.1x オーセンティケータとして設定します。オーセンティケータの PAE 動作は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを入力した後でディセーブルになります。

次に、インターフェイスがサプリカントとして動作するように設定されている例を示します。

```
Switch(config)# interface g1/0/3
Switch(config-if)# dot1x pae supplicant
```

dot1x supplicant force-multicast

サプリカント スイッチでマルチキャストまたはユニキャストの Extensible Authentication Protocol over LAN（EAPOL）パケットを受信した場合に、常にマルチキャスト EAPOL パケットのみを送信するように強制するには、グローバル コンフィギュレーション モードで **dot1x supplicant force-multicast** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x supplicant force-multicast
no dot1x supplicant force-multicast

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

サプリカント スイッチは、ユニキャスト EAPOL パケットを受信すると、ユニキャスト EAPOL パケットを送信します。同様に、マルチキャスト EAPOL パケットを受信すると、EAPOL パケットを送信します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドは Cisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされていませんでした。

使用上のガイドライン

Network Edge Access Topology（NEAT）がすべてのホスト モードで機能するようにするには、サプリカント スイッチ上でこのコマンドをイネーブルにします。

次の例では、サプリカント スイッチがオーセンティケータ スイッチにマルチキャスト EAPOL パケットを送信するように設定する方法を示します。

```
Switch(config)# dot1x supplicant force-multicast
```

関連コマンド

コマンド	説明
cisp enable	スイッチの Client Information Signalling Protocol（CISP）をイネーブルにすることで、スイッチがサプリカント スイッチに対するオーセンティケータとして動作するようにします。
dot1x credentials	ポートに 802.1x サプリカント資格情報を設定します。
dot1x pae supplicant	インターフェイスがサプリカントとしてだけ機能するように設定します。

dot1x test eapol-capable

すべてのスイッチ ポート上の IEEE 802.1x のアクティビティをモニタリングして、IEEE 802.1x をサポートするポートに接続しているデバイスの情報を表示するには、スイッチ スタックまたはスタンドアロン スイッチの特権 EXEC モードで **dot1x test eapol-capable** コマンドを使用します。

dot1x test eapol-capable ［**interface** *interface-id*］

構文の説明

interface *interface-id*	（任意）クエリー対象のポートです。

コマンド デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スイッチ上のすべてのポートまたは特定のポートに接続するデバイスの IEEE 802.1x 機能をテストするには、このコマンドを使用します。

このコマンドには、no 形式はありません。

次の例では、スイッチ上で IEEE 802.1x の準備チェックをイネーブルにして、ポートに対してクエリーを実行する方法を示します。また、ポートに接続しているデバイスを確認するためのクエリーの実行対象ポートから受信した応答が IEEE 802.1x 対応であることを示します。

```
Switch# dot1x test eapol-capable interface gigabitethernet1/0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL
 capable
```

関連コマンド

コマンド	説明
dot1x test timeout *timeout*	IEEE 802.1x 準備クエリーに対する EAPOL 応答を待機するために使用されるタイムアウトを設定します。

dot1x test timeout

IEEE 802.1x 準備状態を照会しているポートからの EAPOL 応答の待機に使用されるタイムアウトを設定するには、スイッチ スタックまたはスタンドアロン スイッチ上で、グローバル コンフィギュレーション モードで **dot1x test timeout** コマンドを使用します。

dot1x test timeout *timeout*

構文の説明

timeout	EAPOL応答を待機する時間（秒）。指定できる範囲は 1 ～ 65535 秒です。

コマンド デフォルト

デフォルト設定は 10 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

EAPOL 応答を待機するために使用されるタイムアウトを設定するには、このコマンドを使用します。

このコマンドには、no 形式はありません。

次の例では、EAPOL 応答を 27 秒間待機するようにスイッチを設定する方法を示します。

```
Switch# dot1x test timeout 27
```

タイムアウト設定のステータスを確認するには、**show run** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x test eapol-capable [**interface** *interface-id*]	すべての、または指定された IEEE 802.1x 対応ポートに接続するデバイスで IEEE 802.1x の準備が整っているかを確認します。

dot1x timeout

再試行タイムアウトの値を設定するには、グローバル コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで **dot1x timeout** コマンドを使用します。再試行タイムアウトをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

dot1x timeout {**auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds* | **ratelimit-period** *seconds* | **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds*}

構文の説明

auth-period *seconds*	サプリカントで保留ステートが維持される秒数（つまり、サプリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。
held-period *seconds*	サプリカントで保留ステートが維持される秒数（つまり、サプリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 60 です。
quiet-period *seconds*	認証情報の交換に失敗したあと、クライアントの再認証を試みるまでにオーセンティケータ（サーバ）が待機状態（HELD 状態）を続ける秒数を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 60 です。
ratelimit-period *seconds*	動作の不正なクライアント PC（たとえば、スイッチ処理電力の無駄につながる、EAP-START パケットを送信する PC）から送信される EAP-START パケットを抑制します。 • オーセンティケータはレート制限時間中、認証に成功したクライアントからの EAPOL-Start パケットを無視します。 • 有効な範囲は 1 ～ 65535 です。デフォルトでは、レート制限はディセーブルになっています。
server-timeout *seconds*	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 • 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。 サーバが指定時間内に 802.1X パケットへの応答を送信しない場合、パケットは再度送信されます。

start-period *seconds*	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。 Cisco IOS リリース 15.2(5)E では、サプリカント モードでのみこのコマンドを使用できます。その他のモードでこのコマンドを適用すると、設定からそのコマンドが失われます。
supp-timeout *seconds*	EAP 要求 ID 以外のすべての EAP メッセージについて、オーセンティケータからホストへの再送信時間を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。
tx-period *seconds*	クライアントに EAP 要求 ID パケットを再送信する間隔を（応答が受信されないものと仮定して）秒数で設定します。 • 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。 • 802.1X パケットがサプリカントに送信され、そのサプリカントが再試行期間後に応答しなかった場合、そのパケットは再度送信されます。

コマンド デフォルト

定期的な再認証と定期的なレート制限が行われます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

dot1x reauthentication インターフェイス コンフィギュレーション コマンドを使用して定期的な再認証をイネーブルにしただけの場合、**dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドは、スイッチの動作に影響します。

待機時間の間、スイッチはどのような認証要求も受け付けず、開始もしません。デフォルトよりも小さい数を入力することによって、ユーザへの応答時間を短縮できます。

ratelimit-period が 0（デフォルト）に設定された場合、スイッチは認証に成功したクライアントからの EAPOL パケットを無視し、それらを RADIUS サーバに転送します。

次に、さまざまな802.1X再送信およびタイムアウト時間が設定されている例を示します。

```
Switch(config)# configure terminal
Switch(config)# interface g1/0/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x timeout auth-period 2000
Switch(config-if)# dot1x timeout held-period 2400
Switch(config-if)# dot1x timeout quiet-period 600
Switch(config-if)# dot1x timeout start-period 90
Switch(config-if)# dot1x timeout supp-timeout 300
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x timeout server-timeout 60
```

epm access-control open

アクセス コントロール リスト（ACL）が設定されていないポートにオープン ディレクティブを設定するには、グローバル コンフィギュレーション モードで **epm access-control open** コマンドを使用します。オープン ディレクティブをディセーブルにするには、このコマンドの **no** 形式を使用します。

epm access-control open
no epm access-control open

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトのディレクティブが適用されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スタティック ACL が設定されたアクセス ポートに、認可ポリシーのないホストを許可するオープンディレクティブを設定するには、このコマンドを使用します。このコマンドを設定しない場合、ポートは設定された ACL のポリシーをトラフィックに適用します。ポートにスタティック ACL が設定されていない場合、デフォルトおよびオープンの両方のディレクティブがポートへのアクセスを許可します。

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

次の例では、オープン ディレクティブを設定する方法を示します。

```
Switch(config)# epm access-control open
```

関連コマンド

コマンド	説明
show running-config	現在実行されているコンフィギュレーション ファイルの内容を表示します

ip admission

Web 認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip admission** コマンドを使用します。このコマンドは、フォールバック プロファイル コンフィギュレーション モードでも使用できます。Web 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip admission *rule*
no ip admission *rule*

構文の説明

rule	IP アドミッション ルールの名前。

コマンド デフォルト

Web 認証はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

フォールバック プロファイル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ip admission コマンドにより、スイッチ ポートに Web 認証ルールが適用されます。

次の例では、スイッチ ポートに Web 認証ルールを適用する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip admission rule1
```

次の例では、IEEE 802.1x 対応のスイッチ ポートで使用するフォールバック プロファイルに Web 認証ルールを適用する方法を示します。

```
Switch# configure terminal
Switch(config)# fallback profile profile1
Switch(config-fallback-profile)# ip admission rule1
```

ip admission name

Web認証をイネーブルにするには、グローバル コンフィギュレーション モードで**ip admission name** コマンドを使用します。Web 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip admission name *name* {**consent** | **proxy http**} [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** {*acl* | *acl-name*} | **service-policy type tag** *service-policy-name*]
no ip admission name *name* {**consent** | **proxy http**} [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** {*acl* | *acl-name*} | **service-policy type tag** *service-policy-name*]

構文の説明

name	ネットワーク アドミッション制御ルールの名前。
consent	認証プロキシ同意 Web ページを *admission-name* 引数で指定された IP アドミッション ルールに対応させます。
proxy http	Web 認証のカスタム ページを設定します。
absolute-timer 分	（任意）外部サーバがタイム アウトするまでの経過時間（分）。
inactivity-time 分	（任意）外部ファイル サーバが到達不能であると見なされるまでの経過時間（分）。
list	（任意）指定されたルールをアクセス コントロール リスト（ACL）に関連付けます。
acl	標準、拡張リストを指定のアドミッション制御ルールに適用します。値の範囲は 1～199、または拡張範囲で 1300 から 2699 です。
acl-name	名前付きのアクセス リストを指定のアドミッション制御ルールに適用します。
service-policy type tag	（任意）コントロール プレーン サービス ポリシーを設定できます。
service-policy-name	**policy-map type control tag***policyname* コマンド、キーワード、および引数を使用して設定されたコントロール プレーン タグのサービス ポリシー。このポリシー マップは、タグを受信したときのホストでの処理を適用するために使用されます。

コマンド デフォルト

Web 認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ip admission name コマンドにより、スイッチ上で Web 認証がグローバルにイネーブルになります。

スイッチ上で Web 認証をイネーブルにしてから、**ip access-group in** および **ip admission web-rule** インターフェイス コンフィギュレーション コマンドを使用して、特定のインターフェイス上で Web 認証をイネーブルにします。

例

次に、スイッチ ポートで Web 認証のみを設定する例を示します。

```
Switch# configure terminal
Switch(config) ip admission name http-rule proxy http
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 101 in
Switch(config-if)# ip admission rule
Switch(config-if)# end
```

次の例では、スイッチ ポートでのフォールバック メカニズムとして、Web認証とともに IEEE 802.1x 認証を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip admission name rule2 proxy http
Switch(config)# fallback profile profile1
Switch(config)# ip access group 101 in
Switch(config)# ip admission name rule2
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback profile1
Switch(config-if)# end
```

関連コマンド

コマンド	説明
dot1x fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
fallback profile	Web 認証のフォールバック プロファイルを作成します。

コマンド	説明
ip admission	ポートで Web 認証をイネーブルにします。
show authentication sessions interface *interface* **detail**	Web 認証セッションのステータスに関する情報を表示します。
show ip admission	NAC のキャッシュされたエントリまたはNAC設定についての情報を表示します。

ip device tracking maximum

レイヤ 2 アクセス ポートで IP デバイス トラッキング パラメータを設定するには、インターフェイス コンフィギュレーション モードで **ip device tracking maximum** コマンドを使用します。最大値を削除するには、このコマンドの **no** 形式を使用します。

ip device tracking maximum *number*
no ip device tracking maximum

構文の説明

number	ポートの IP デバイス トラッキング テーブルに作成するバインディングの数。範囲は 0（ディセーブル）～ 65535 です。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

最大値を削除するには、**no ip device tracking maximum** コマンドを使用します。

IP デバイス トラッキングをディセーブルにするには、**ip device tracking maximum 0** コマンドを使用します。

（注） このコマンドは、設定されている場合は常に IPDT を有効にします。

例

次の例では、レイヤ 2 アクセス ポートで IP デバイス トラッキング パラメータを設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# end
```

ip device tracking probe

Address Resolution Protocol（ARP）プローブの IP デバイス トラッキング テーブルを設定するには、グローバル コンフィギュレーション モードで **ip device tracking probe** コマンドを使用します。ARP インスペクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip device tracking probe {**count** *number*|**delay** *seconds*|**interval** *seconds*|**use-svi** *address*}
no ip device tracking probe {**count** *number*|**delay** *seconds*|**interval** *seconds*|**use-svi** *address*}

構文の説明

count *number*	スイッチが ARP プローブを送信する回数を設定します。範囲は 1 ～ 255 です。
delay *seconds*	スイッチが ARP プローブを送信するまで待機する秒数を設定します。指定できる範囲は 1 ～ 120 です。
interval *seconds*	スイッチが応答を待ち、ARP プローブを再送信するまでの秒数を設定します。指定できる範囲は 30 ～ 1814400 秒です。
use-svi	スイッチ仮想インターフェイス（SVI）IP アドレスを ARP プローブのソースとして使用します。

コマンド デフォルト

カウント番号は 3 です。

遅延はありません。

30 秒間隔です。

ARP プローブのデフォルト ソース IP アドレスはレイヤ 3 インターフェイスで、スイッチポートでは 0.0.0.0 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スイッチ ポートのデフォルト ソース IP アドレス 0.0.0.0 が使用され、ARP プローブがドロップする場合に、IP デバイス トラッキング テーブルが SVI IP アドレスを ARP プローブに使用するように設定するには、**use-svi** キーワードを使用します。

例

次の例では、SVI を ARP プローブのソースとして設定する方法を示します。

```
Switch(config)# ip device tracking probe use-svi
```

ip dhcp snooping database

Dynamic Host Configuration Protocol（DHCP）のスヌーピング データベースを設定するには、グローバル コンフィギュレーション モードで **ip dhcp snooping database** コマンドを使用します。DHCP スヌーピング サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping database {**crashinfo:***url* | **flash:***url* | **ftp:***url* | **http:***url* | **https:***url* | **rcp:***url* | **scp:***url* | **tftp:***url* | **timeout** *seconds* | **usbflash0:***url* | **write-delay** *seconds*}
no ip dhcp snooping database [**timeout** | **write-delay**]

構文の説明

crashinfo:*url*	crashinfo を使用して、エントリを格納するためのデータベースの URL を指定します。
flash:*url*	flash を使用して、エントリを格納するためのデータベースの URL を指定します。
ftp:*url*	FTP を使用して、エントリを格納するためのデータベースの URL を指定します。
http:*url*	HTTP を使用して、エントリを格納するためのデータベースの URL を指定します。
https:*url*	セキュア HTTP（HTTPS）を使用して、エントリを格納するためのデータベースの URL を指定します。
rcp:*url*	リモート コピー（RCP）を使用して、エントリを格納するためのデータベースの URL を指定します。
scp:*url*	セキュア コピー（SCP）を使用して、エントリを格納するためのデータベースの URL を指定します。
tftp:*url*	TFTP を使用して、エントリを格納するためのデータベースの URL を指定します。

timeout *seconds*	中断タイムアウト インターバルを指定します。有効値は 0 ～ 86,400 秒です。
usbflash0:*url*	USB flash を使用して、エントリを格納するためのデータベースの URL を指定します。
write-delay *seconds*	ローカル DHCP スヌーピング データベースにデータが追加されてから、DHCP スヌーピング エントリを外部サーバに書き込みするまでの時間を指定します。有効値は 15 ～ 86,400 秒です。

コマンド デフォルト

DHCP スヌーピング データベースは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを入力する前に、インターフェイス上でDHCPスヌーピングをイネーブルにする必要があります。DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping** コマンドを使用します。

次に、TFTP を使用してデータベースの URL を指定する例を示します。

```
Switch(config)#  ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```

次に、DHCP スヌーピング エントリを外部サーバに書き込むまでの時間を指定する例を示します。

```
Switch(config)#  ip dhcp snooping database write-delay 15
```

ip dhcp snooping information option format remote-id

オプション 82 リモート ID サブオプションを設定するには、スイッチのグローバル コンフィギュレーション モードで **ip dhcp snooping information option format remote-id** コマンドを使用します。デフォルトのリモート ID サブオプションを設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping information option format remote-id {**hostname** | **string** *string*}
no ip dhcp snooping information option format remote-id {**hostname** | **string** *string*}

構文の説明

hostname	スイッチのホスト名をリモート ID として指定します。
string *string*	1 ～ 63 の ASCII 文字（スペースなし）を使用して、リモート ID を指定します。

コマンド デフォルト

スイッチの MAC アドレスは、リモート ID です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

DHCP スヌーピング設定を有効にするには、**ip dhcp snooping** グローバル コンフィギュレーション コマンドを使用して、DHCP スヌーピングをグローバルにイネーブルにする必要があります。

オプション 82 機能がイネーブルの場合、デフォルトのリモート ID サブオプションはスイッチの MAC アドレスです。このコマンドを使用すると、スイッチのホスト名または 63 個の ASCII 文字列（スペースなし）のいずれかをリモート ID として設定できます。

（注） ホスト名が 63 文字を超える場合、リモート ID 設定では 63 文字以降は省略されます。

次の例では、オプション 82 リモート ID サブオプションを設定する方法を示します。

```
Switch(config)# ip dhcp snooping information option format remote-id hostname
```

ip dhcp snooping verify no-relay-agent-address

DHCP クライアント メッセージのリレー エージェント アドレス（giaddr）が信頼できないポート上のクライアント ハードウェア アドレスに一致することを確認して、DHCP スヌーピング機能をディセーブルにするには、グローバル コンフィギュレーション モードで **ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。検証をイネーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping verify no-relay-agent-address
no ip dhcp snooping verify no-relay-agent-address

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

DHCP スヌーピング機能では、信頼できないポート上の DHCP クライアント メッセージのリレー エージェント IP アドレス（giaddr）フィールドが 0 であることを確認します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、DHCP スヌーピング機能では、信頼できないポート上の DHCP クライアント メッセージのリレー エージェントの IP アドレス（giaddr）フィールドが 0 であることを確認します。giaddr フィールドが 0 でない場合、メッセージはドロップされます。検証をディセーブルにするには、**ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。検証を再度イネーブルにするには、**no ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。

次に、DHCP クライアント メッセージの giaddr 検証をイネーブルにする例を示します。

```
Switch(config)# no ip dhcp snooping verify no-relay-agent-address
```

ip source binding

スタティック IP ソース バインディング エントリを追加するには、**ip source binding** コマンドを使用します。スタティック IP ソース バインディング エントリを削除するには、このコマンドの **no** 形式を使用します。

ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*
no ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

構文の説明

mac-address	バインディング対象MACアドレスです。
vlan *vlan-id*	レイヤ 2 VLAN ID を指定します。有効な値は 1～4094 です。
ip-address	バインディング対象 IP アドレスです。
interface *interface-id*	物理インターフェイスの ID。

コマンド デフォルト

IP 送信元バインディングは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、スタティック IP ソース バインディング エントリだけを追加するために使用できます。

no 形式は、対応する IP ソース バインディング エントリを削除します。削除が正常に実行されるためには、すべての必須パラメータが正確に一致しなければなりません。各スタティック IP バインディング エントリは MAC アドレスと VLAN 番号がキーであることに注意してください。コマンドに既存の MAC アドレスと VLAN 番号が含まれる場合、別のバインディング エントリが作成される代わりに既存のバインディングエントリが新しいパラメータで更新されます。

次の例では、スタティック IP ソース バインディング エントリを追加する方法を示します。

```
Switch# configure terminal
Switchconfig) ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/0/1
```

ip verify source

インターフェイス上の IP ソース ガードをイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip verify source** コマンドを使用します。IP ソース ガードをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip verify source [**mac-check**][**tracking**]
no ip verify source

構文の説明

mac-check	（任意）MAC アドレス検証による IP ソース ガードをイネーブルにします。
tracking	（任意）ポートで静的 IP アドレス を学習するために IP ポート セキュリティをイネーブルにします。

コマンド デフォルト

IP 送信元ガードはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、**ip verify source** インターフェイス コンフィギュレーション コマンドを使用します。

送信元 IP アドレス フィルタリングおよび MAC アドレス検証による IP ソース ガードをイネーブルにするには、**ip verify sourcemac-check** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、送信元 IP アドレス フィルタリングによる IP ソース ガードをインターフェイス上でイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source
```

次の例では、MAC アドレスの検証による IP ソース ガードをイネーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source mac-check
```

設定を確認するには、**show ip verify source** 特権 EXEC コマンドを入力します。

ipv6 snooping policy

（注） すべての既存の IPv6 スヌーピング コマンド（Cisco IOS XE Denali 16.1.1 より前）には、対応する SISF ベースのデバイス トラッキング コマンドが用意され、IPv4 と IPv6 の両方のアドレス ファミリに設定を適用できるようになりました。詳細については、「device-tracking policy」を参照してください。

IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 snooping policy** コマンドを使用します。IPv6 スヌーピング ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ipv6 snooping policy *snooping-policy*
no ipv6 snooping policy *snooping-policy*

構文の説明

snooping-policy	スヌーピング ポリシーのユーザ定義名。ポリシー名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。

コマンド デフォルト

IPv6 スヌーピング ポリシーは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

IPv6 スヌーピング ポリシーを作成するには、**ipv6 snooping policy** コマンドを使用します。**ipv6 snooping policy** コマンドがイネーブルの場合、コンフィギュレーション モードが IPv6 スヌーピング コンフィギュレーション モードに変更されます。このモードでは、管理者が次の IPv6 ファーストホップ セキュリティ コマンドを設定できます。

- **device-role** コマンドは、ポートに接続されているデバイスのロールを指定します。
- **limit address-count** *maximum* コマンドは、ポートで使用できる IPv6 アドレスの数を制限します。
- **protocol** コマンドは、アドレスを Dynamic Host Configuration Protocol（DHCP）または Neighbor Discovery Protocol（NDP）で収集する必要があることを指定します。
- **security-level** コマンドは、適用されるセキュリティのレベルを指定します。
- **tracking** コマンドは、ポートのデフォルトのトラッキング ポリシーに優先します。

- **trusted-port** コマンドは、ポートを信頼できるポートとして設定します。つまり、メッセージを受信したときに検証が限定的に実行されるか、まったく実行されません。

次に、IPv6 スヌーピング ポリシーを設定する例を示します。

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#
```

limit address-count

ポートで使用できるIPv6アドレスの数を制限するには、Neighbor Discovery Protocol（NDP）インスペクション ポリシー コンフィギュレーション モードまたはIPv6 スヌーピング コンフィギュレーション モードで **limit address-count** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

limit address-count *maximum*
no limit address-count

構文の説明

maximum	ポートで許可されているアドレスの数。範囲は1 ～ 10000 です。

コマンド デフォルト

デフォルト設定は無制限です。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

limit address-count コマンドは、ポリシーが適用されているポートで使用できるIPv6アドレスの数を制限します。ポート上のIPv6アドレスの数を制限すると、バインディング テーブル サイズの制限に役立ちます。範囲は 1 ～ 10000 です。

次に、NDP ポリシー名を policy1 と定義し、スイッチを NDP インスペクション ポリシー コンフィギュレーション モードにし、ポートで使用できるIPv6アドレスの数を25 に制限する例を示します。

```
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)# limit address-count 25
```

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、スイッチをIPv6 スヌーピング ポリシー コンフィギュレーション モードにし、ポートで使用できるIPv6アドレスの数を 25 に制限する例を示します。

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# limit address-count 25
```

mab request format attribute 32

スイッチ上でVLAN IDベースのMAC認証をイネーブルにするには、グローバル コンフィギュレーション モードで **mab request format attribute 32 vlan access-vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mab request format attribute 32 vlan access-vlan
no mab request format attribute 32 vlan access-vlan

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

VLAN-ID ベースの MAC 認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

RADIUS サーバがホスト MAC アドレスと VLAN に基づいて新しいユーザを認証できるようにするには、このコマンドを使用します。

Microsoft IAS RADIUS サーバを使用したネットワークでこの機能を使用します。Cisco ACS はこのコマンドを無視します。

次の例では、スイッチでVLAN-IDベースのMAC認証をイネーブルにする方法を示します。

```
Switch(config)# mab request format attribute 32 vlan access-vlan
```

関連コマンド

コマンド	説明
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1x 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャ モードを設定します。
authentication open	ポートでオープン アクセスをイネーブルまたはディセーブルにします。

コマンド	説明
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポートプライオリティリストに認証方式を追加します。
authentication timer	802.1x 対応ポートのタイムアウトパラメータと再認証パラメータを設定します。
authentication violation	新しいデバイスがポートに接続するか、ポートにすでに最大数のデバイスが接続しているときに、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
mab	ポートの MAC-based 認証をイネーブルにします。
mab eap	Extensible Authentication Protocol（EAP）を使用するようポートを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

match（アクセス マップ コンフィギュレーション）

1つまたは複数のアクセス リストをパケットと照合するようにVLANマップを設定するには、スイッチ スタックまたはスタンドアロン スイッチのアクセスマップ コンフィギュレーション モードで **match** コマンドを使用します。照合パラメータを削除するには、このコマンドの **no** 形式を使用します。

match {**ip address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]...|**ipv6 address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]...|**mac address** {*name*} [{*name*}] [{*name*}]...}
no match {**ip address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]...|**ipv6 address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]...|**mac address** {*name*} [{*name*}] [{*name*}]...}

構文の説明

ip address	パケットを IP アドレス アクセス リストと照合するようにアクセス マップを設定します。
ipv6 address	パケットを IPv6 アドレス アクセス リストと照合するようにアクセス マップを設定します。
mac address	パケットを MAC アドレス アクセス リストと照合するようにアクセス マップを設定します。
name	パケットを照合するアクセス リストの名前です。
number	パケットを照合するアクセス リストの番号です。このオプションは、MACアクセス リストに対しては無効です。

コマンド デフォルト

デフォルトのアクションでは、一致パラメータは VLAN マップに適用されません。

コマンド モード

アクセス マップ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

vlan access-map グローバル コンフィギュレーション コマンドを使用して、アクセス マップ コンフィギュレーション モードを開始します。

1 つのアクセス リストの名前または番号を入力する必要があります。その他は任意です。パケットは、1つまたは複数のアクセス リストに対して照合できます。いずれかのリストに一致すると、エントリの一致としてカウントされます。

アクセス マップ コンフィギュレーション モードでは、**match** コマンドを使用して、VLAN に適用されるVLANマップの一致条件を定義できます。**action** コマンドを使用すると、パケットが条件に一致したときに実行するアクションを設定できます。

パケットは、同じプロトコル タイプのアクセス リストに対してだけ照合されます。IP パケットは、IP アクセス リストに対して照合され、IPv6 パケットは IPv6 アクセス リストに対して照合され、その他のパケットはすべて MAC アクセス リストに対して照合されます。

同じマップ エントリに、IP アドレス、IPv6 アドレスおよび MAC アドレスを指定できます。

次の例では、VLAN アクセス マップ vmap4 を定義して VLAN 5 と VLAN 6 に適用する方法を示します。このアクセス マップでは、パケットがアクセス リスト al2 に定義された条件に一致すると、インターフェイスは IP パケットをドロップします。

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

設定を確認するには、**show vlan access-map** 特権 EXEC コマンドを入力します。

関連トピック

action （810 ページ）
show vlan access-map （903 ページ）
vlan access-map （937 ページ）

no authentication logging verbose

認証システム メッセージから詳細情報をフィルタリングするには、スイッチ スタックまたはスタンドアロン スイッチ上で **no authentication logging verbose** コマンドをグローバル コンフィギュレーション モードで使用します。

no authentication logging verbose

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

すべての詳細情報はシステム メッセージに表示されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、認証システムメッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose 認証システム メッセージをフィルタリングするには、次の手順に従います。

```
Switch(config)# no authentication logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
no authentication logging verbose	認証システム メッセージから詳細情報をフィルタリングします。
no dot1x logging verbose	802.1x システム メッセージから詳細情報をフィルタリングします。
no mab logging verbose	MAC認証バイパス（MAB）システム メッセージから詳細情報をフィルタリングします。

no dot1x logging verbose

802.1x システム メッセージから詳細情報をフィルタリングするには、スイッチ スタックまたはスタンドアロン スイッチのグローバル コンフィギュレーション モードで **no dot1x logging verbose** コマンドを使用します。

no dot1x logging verbose

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

すべての詳細情報はシステム メッセージに表示されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、802.1x システム メッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose 802.1x システム メッセージをフィルタリングするには、次の手順に従います。

```
Switch(config)# no dot1x logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
no authentication logging verbose	認証システム メッセージから詳細情報をフィルタリングします。
no dot1x logging verbose	802.1x システム メッセージから詳細情報をフィルタリングします。
no mab logging verbose	MAC 認証バイパス（MAB）システム メッセージから詳細情報をフィルタリングします。

no mab logging verbose

MAC認証バイパス（MAB）のシステムメッセージから詳細情報をフィルタリングするには、スイッチ スタックまたはスタンドアロン スイッチ上で、グローバル コンフィギュレーション モードで **no mab logging verbose** コマンドを使用します。

no mab logging verbose

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

すべての詳細情報はシステム メッセージに表示されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、MAC認証バイパス（MAB）システムメッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose MAB システム メッセージをフィルタリングするには、次の手順に従います。

```
Switch(config)# no mab logging verbose
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
no authentication logging verbose	認証システム メッセージから詳細情報をフィルタリングします。
no dot1x logging verbose	802.1x システム メッセージから詳細情報をフィルタリングします。
no mab logging verbose	MAC認証バイパス（MAB）システム メッセージから詳細情報をフィルタリングします。

permit（MACアクセス リストコンフィギュレーション）

条件が一致した場合に非 IP トラフィックの転送を許可するには、スイッチ スタックまたはスタンドアロン スイッチ上で **permit** MAC アクセスリスト コンフィギュレーション コマンドを使用します。拡張 MAC アクセス リストから許可条件を削除するには、このコマンドの **no** 形式を使用します。

{**permit** {**any** | **host***src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host***dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap***lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**] [**cos***cos*]
nopermit {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**] [**cos***cos*]

構文の説明

any	すべての送信元または宛先MACアドレスを拒否します。
host *src-MAC-addr* | *src-MAC-addr mask*	ホスト MAC アドレスと任意のサブネット マスクを指定します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP トラフィックは拒否されます。
host *dst-MAC-addr* | *dst-MAC-addr mask*	宛先 MAC アドレスと任意のサブネット マスクを指定します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。
type mask	（任意）パケットのEtherType番号と、Ethernet IIまたはSNAPカプセル化を指定して、パケットのプロトコルを識別します。 • *type* には、0 ～ 65535 の 16 進数を指定できます。 • *mask* は、一致をテストする前にEtherTypeに適用される don't care ビットのマスクです。

aarp	（任意）データリンク アドレスをネットワーク アドレスにマッピングする EtherType AppleTalk Address Resolution Protocol を指定します。
amber	（任意）EtherType DEC-Amber を指定します。
appletalk	（任意）EtherType AppleTalk/EtherTalk を指定します。
dec-spanning	（任意）EtherType Digital Equipment Corporation（DEC）スパニングツリーを指定します。
decnet-iv	（任意）EtherType DECnet Phase IV プロトコルを指定します。
diagnostic	（任意）EtherType DEC-Diagnostic を指定します。
dsm	（任意）EtherType DEC-DSM を指定します。
etype-6000	（任意）EtherType 0x6000 を指定します。
etype-8042	（任意）EtherType 0x8042 を指定します。
lat	（任意）EtherType DEC-LAT を指定します。
lavc-sca	（任意）EtherType DEC-LAVC-SCA を指定します。
lsap *lsap-number mask*	（任意）パケットの LSAP 番号（0 ～ 65535）と 802.2 カプセル化を使用して、パケットのプロトコルを指定します。 *mask* は、一致をテストする前に LSAP 番号に適用される don’t care ビットのマスクです。
mop-console	（任意）EtherType DEC-MOP Remote Console を指定します。
mop-dump	（任意）EtherType DEC-MOP Dump を指定します。
msdos	（任意）EtherType DEC-MSDOS を指定します。
mumps	（任意）EtherType DEC-MUMPS を指定します。

netbios	（任意）EtherType DEC-Network Basic Input/Output System（NetBIOS）を指定します。
vines-echo	（任意）Banyan Systems による EtherType Virtual Integrated Network Service（VINES）Echo を指定します。
vines-ip	（任意）EtherType VINES IP を指定します。
xns-idp	（任意）EtherType Xerox Network Systems（XNS）プロトコル スイートを指定します。
cos *cos*	（任意）プライオリティを設定するため、0～7 までの任意の Class of Service（CoS）値を指定します。CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。**cos** オプションが設定されているかどうかを確認する警告メッセージが表示されます。

コマンド デフォルト

このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルト アクションは拒否です。

コマンド モード

MAC アクセス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

appletalk は、コマンドラインのヘルプ ストリングには表示されますが、一致条件としてはサポートされていません。

MAC アクセス リスト コンフィギュレーション モードを開始するには、**mac access-list extended** グローバル コンフィギュレーション コマンドを使用します。

host キーワードを使用した場合、アドレス マスクは入力できません。 **any** キーワードまたは **host** キーワードを使用しない場合は、アドレス マスクを入力する必要があります。

アクセス コントロール エントリ（ACE）がアクセス コントロール リストに追加されると、リストの最後には暗黙の **deny-any-any** 条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap** *lsap mask* キーワードを使用します。Novell 用語と Cisco IOS 用語での IPX カプセル化タイプに対応するフィルタ条件を、次の表に一覧表示します。

表 *26 : IPX* フィルタ基準

IPX カプセル化タイプ		フィルタ基準
Cisco IOS 名	**Novell 名**	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

次の例では、あらゆる送信元からMACアドレス00c0.00a0.03faへのNetBIOSトラフィックを許可する名前付き MAC 拡張アクセス リストを定義する方法を示します。このリストに一致するトラフィックは許可されます。

```
Switch(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

次の例では、名前付き MAC 拡張アクセス リストから許可条件を削除する方法を示します。

```
Switch(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

次の例では、EtherType 0x4321 のすべてのパケットを許可します。

```
Switch(config-ext-macl)# permit any any 0x4321 0
```

設定を確認するには、**show access-lists** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
deny	MACアクセスリストコンフィギュレーションを拒否します。条件が一致した場合に非IPトラフィックが転送されるのを拒否します。
mac access-list extended	非IPトラフィック用にMACアドレス ベースのアクセス リストを作成します。
show access-lists	スイッチに設定されたアクセス コントロール リストを表示します。

protocol（IPv6 スヌーピング）

アドレスを Dynamic Host Configuration Protocol（DHCP）または Neighbor Discovery Protocol（NDP）で収集する必要があることを指定するか、プロトコルを IPv6 プレフィックス リストに対応させるには、**protocol** コマンドを使用します。DHCP または NDP によるアドレス収集をディセーブルにするには、このコマンドの **no** 形式を使用します。

protocol {**dhcp** | **ndp**}
no protocol {**dhcp** | **ndp**}

構文の説明

dhcp	アドレスをダイナミック ホスト コンフィギュレーション プロトコル（DHCP）パケットで収集する必要があることを指定します。
ndp	アドレスをネイバー探索プロトコル（NDP）パケットで収集する必要があることを指定します。

コマンド デフォルト

スヌーピングとリカバリは DHCP および NDP の両方を使用して試行します。

コマンド モード

IPv6 スヌーピング コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

アドレスが DHCP または NDP に対応するプレフィックス リストと一致しない場合は、制御パケットがドロップされ、バインディング テーブル エントリのリカバリはそのプロトコルに対しては試行されません。

- **no protocol** {**dhcp** | **ndp**} コマンドを使用すると、プロトコルはスヌーピングまたはグリーニングに使用されません。
- **no protocol dhcp** コマンドを使用すると、DHCP は依然としてバインディング テーブルのリカバリに使用できます。
- データ収集は DHCP および NDP でリカバリできますが、宛先ガードは DHCP によってのみリカバリできます。

次に、IPv6 スヌーピングポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、アドレスの収集に DHCP を使用するようにポートを設定する例を示します。

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# protocol dhcp
```

radius server

（注） Cisco IOS リリース 15.2(5)E より、**radius server** コマンドは、Cisco IOS リリース 15.2(5)E 以前のリリースで使用されていた **radius-server host** コマンドを置き換えます。古いコマンドは廃止されました。

RADIUS アカウンティングと RADIUS 認証を含む RADIUS サーバのパラメータを設定するには、スイッチ スタックまたはスタンドアロン スイッチで **radius server** コンフィギュレーション サブモード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius server *name*
address {ipv4 | ipv6} *ip{address | hostname}* **auth-port** *udp-port* **acct-port** *udp-port*
key *string*
automate tester *name* | **retransmit** *value* | **timeout** *seconds*
no radius server *name*

構文の説明

address {ipv4 | ipv6} *ip{address | hostname}*	RADIUS サーバの IP アドレスを指定します。
auth-port *udp-port*	（任意）RADIUS 認証サーバの UDP ポートを指定します。指定できる範囲は 0 ～ 65536 です。
acct-port *udp-port*	（任意）RADIUS アカウンティング サーバの UDP ポートを指定します。指定できる範囲は 0 ～ 65536 です。
key *string*	（任意）スイッチおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。 （注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。必ずこのコマンドの最終項目として key を設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。key にスペースが含まれる場合は、引用符が key の一部でない限り、key を引用符で囲まないでください。
automate tester *name*	（任意）RADIUS サーバ ステータスの自動サーバ テストをイネーブルにし、使用されるユーザ名を指定します。
retransmit *value*	（任意）サーバが応答しない、または応答が遅い場合に、RADIUS 要求をリセットする回数を指定します。指定できる範囲は 1 ～ 100 です。この設定は、radius-server retransmit グローバル コンフィギュレーション コマンドによる設定を上書きします。

timeout *seconds*	（任意）スイッチが要求を再送信する前にRADIUSサーバからの応答を待機する時間間隔を指定します。指定できる範囲は1～1000です。この設定は、radius-server timeout グローバル コンフィギュレーション コマンドによる設定を上書きします。
no radius server *name*	（任意）デフォルト設定に戻します。

コマンド デフォルト

- RADIUS アカウンティング サーバの UDP ポートは 1646 です。
- RADIUS 認証サーバの UDP ポートは 1645 です。
- 自動サーバ テストはディセーブルです。
- タイムアウトは 60 分（1 時間）です。
- 自動テストがイネーブルの場合、UDPポートのアカウンティングおよび認証時にテストが実行されます。
- 認証キーおよび暗号キー（string）は設定されていません。

コマンド モード

Radius サーバ サブモード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS 15.2(5)E	このコマンドは、コマンド**radius-server host** を置き換えるために導入されました。

使用上のガイドライン

- RADIUS アカウンティング サーバおよびRADIUS 認証サーバの UDP ポートをデフォルト以外の値に設定することを推奨します。
- **key** *string* サブモード コンフィギュレーション コマンドを使用して、認証キーおよび暗号キーを設定できます。必ずこのコマンドの最終項目として key を設定してください。
- RADIUS サーバ ステータスの自動サーバ テストを有効化し、使用されるユーザ名を指定するには、**automate-tester** *name* キーワードを使用します。

次に、認証サーバの UDP ポートを 1645、アカウンティング サーバの UDP ポートを 1646 に設定する例を示します。

```
Switch(config)# radius server ISE
Switch(config-radius-server)# address ipv4 10.1.1 auth-port 1645 acct-port 1646
Switch(config-radius-server)# key cisco123
```

security level（IPv6 スヌーピング）

適用されるセキュリティのレベルを指定するには、IPv6 スヌーピング ポリシー コンフィギュレーション モードで **security-level** コマンドを使用します。

security level {**glean** | **guard** | **inspect**}

構文の説明

glean	アドレスをメッセージから抽出し、検証を行わずにそれらをバインディング テーブルにインストールします。
guard	収集と検査の両方を実行します。さらに、信頼できるポートで受信されていない場合、または別のポリシーによって許可されていない場合、RA メッセージおよび DHCP サーバ メッセージは拒否されます。
inspect	メッセージの一貫性と準拠度を検証します。特に、アドレス所有権が強制されます。無効なメッセージはドロップされます。

コマンド デフォルト

デフォルトのセキュリティ レベルは guard です。

コマンド モード

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、デバイスを IPv6 スヌーピング コンフィギュレーション モードにし、セキュリティ レベルを inspect として設定する例を示します。

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# security-level inspect
```

security passthru

IPSec のパススルーを変更するには、**securitypassthru** コマンドを使用します。ディセーブルにするには、このコマンドの no 形式を使用します。

security passthru *ip-address*
no security passthru

構文の説明

ip-address	（任意）VPN トンネルの終端となる IPSec ゲートウェイ（ルータ）の IP アドレスです。

コマンド デフォルト

なし。

コマンド モード

wlan

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、IPSec のパススルーを変更する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#security passthrough 10.1.1.1
```

show aaa clients

AAA クライアントの統計情報を表示するには、**show aaa clients** コマンドを使用します。

show aaa clients ［**detailed**］

構文の説明

detailed	（任意）詳細なAAAクライアントの統計情報を示します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、**show aaa clients** コマンドの出力を示します。

```
Switch# show aaa clients
Dropped request packets: 0
```

show aaa command handler

AAA コマンド ハンドラの統計情報を表示するには、**show aaa command handler** コマンドを使用します。

show aaa command handler

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、**show aaa command handler** コマンドの出力を示します。

```
Switch# show aaa command handler

AAA Command Handler Statistics:
    account-logon: 0, account-logoff: 0
    account-query: 0, pod: 0
    service-logon: 0, service-logoff: 0
    user-profile-push: 0, session-state-log: 0
    reauthenticate: 0, bounce-host-port: 0
    disable-host-port: 0, update-rbacl: 0
    update-sgt: 0, update-cts-policies: 0
    invalid commands: 0
    async message not sent: 0
```

show aaa local

AAA ローカル方式オプションを表示するには、**show aaa local** コマンドを使用します。

show aaa local {**netuser** {*name* | **all** } | **statistics** | **user lockout**}

構文の説明

netuser	AAA ローカル ネットワークまたはゲスト ユーザ データベースを指定します。
name	ネットワーク ユーザ名。
all	ネットワークおよびゲスト ユーザ情報を指定します。
statistics	ローカル認証の統計情報を表示します。
user lockout	AAA ローカルのロックアウトされたユーザを指定します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、**show aaa local statistics** コマンドの出力を示します。

```
Switch# show aaa local statistics

Local EAP statistics

EAP Method         Success       Fail
---------------------------------------
Unknown                  0          0
EAP-MD5                  0          0
EAP-GTC                  0          0
LEAP                     0          0
PEAP                     0          0
EAP-TLS                  0          0
EAP-MSCHAPV2             0          0
EAP-FAST                 0          0

Requests received from AAA:                0
Responses returned from EAP:               0
Requests dropped (no EAP AVP):             0
Requests dropped (other reasons):          0
Authentication timeouts from EAP:          0

Credential request statistics
Requests sent to backend:                  0
Requests failed (unable to send):          0
Authorization results received

  Success:                                 0
```

```
Fail:                                    0
```

show aaa servers

AAA サーバの MIB によって認識されるすべての AAA サーバを表示するには、**show aaa servers** コマンドを使用します。

show aaa servers ［ **private** | **public** | ［**detailed**］］

構文の説明

detailed	（任意）AAA サーバの MIB によって認識されるプライベート AAA サーバを表示します。
public	（任意）AAA サーバの MIB によって認識されるパブリック AAA サーバを表示します。
detailed	（任意）詳細な AAA サーバの統計情報を表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、**show aaa servers** コマンドの出力を示します。

```
Switch# show aaa servers
RADIUS: id 1, priority 1, host 172.20.128.2, auth-port 1645, acct-port 1646
State: current UP, duration 9s, previous duration 0s
Dead: total time 0s, count 0
Quarantined: No
Authen: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Account: request 0, timeouts 0, failover 0, retransmission 0
Request: start 0, interim 0, stop 0
Response: start 0, interim 0, stop 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 0m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

show aaa sessions

AAA セッション MIB によって認識される AAA セッションを表示するには、**show aaa sessions** コマンドを使用します。

show aaa sessions

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、**show aaa sessions** コマンドの出力を示します。

```
Switch# show aaa sessions
Total sessions since last reload: 7
Session Id: 4007
   Unique Id: 4025
   User Name: *not available*
   IP Address: 0.0.0.0
   Idle Time: 0
   CT Call Handle: 0
```

show authentication history

デバイスで稼働中の認証セッションを表示するには、 **show authentication history** コマンドを使用します。

show authentication history ［**min-uptime** *seconds*］

構文の説明

min-uptime *seconds*	（任意）最小アップタイム内のセッションを表示します。有効範囲は 1 ～ 4294967295 秒です。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

デバイスで稼働中の認証セッションを表示するには、**show authentication history** コマンドを使用します。

次の例では、**show authentication history** コマンドの出力を示します。

```
Switch# show authentication history
Interface  MAC Address     Method  Domain  Status  Uptime
Gi3/0/2    0021.d864.07c0  dot1x   DATA    Auth    38s

Session count = 1
```

show authentication sessions

現在の認証マネージャ セッションに関する情報を表示するには、**show authentication sessions** コマンドを使用します。

show authentication sessions ［**database**］［**handle** *handle-id*［**details**］］［**interface** *type number*［**details**］［**mac** *mac-address*［**interface** *type number*］［**method** *method-name*［**interface** *type number*［**details**］［**session-id** *session-id* ［**details**］］

構文の説明

database	（任意）セッション データベースに格納されているデータだけを示します。
handle *handle-id*	（任意）認証マネージャ情報を表示する特定のハンドルを指定します。
details	（任意）詳細情報を表示します。
interface *type number*	（任意）認証マネージャ情報を表示する特定のインターフェイスのタイプと番号を指定します。
mac *mac-address*	（任意）情報を表示する特定の MAC アドレスを指定します。
method *method-name*	（任意）認証マネージャ情報を表示する特定の認証方法を指定します。方式を指定する場合（**dot1x**、**mab**、または **webauth**）、インターフェイスも指定できます。
session-id *session-id*	（任意）認証マネージャ情報を表示する特定のセッションを指定します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

現在のすべての認証マネージャ セッションに関する情報を表示するには、**show authentication sessions** コマンドを使用します。特定の認証マネージャ セッションに関する情報を表示するには、1 つ以上のキーワードを使用します。

このテーブルは、報告された認証セッションで想定される動作状態を示します。

表 *27 :* 認証方式のステート

状態	説明
Not run	このセッションの方式は実行されていません。
Running	このセッションの方式が実行中です。

状態	説明
Failed over	この方式は失敗しました。次の方式が結果を出すことが予期されています。
Success	この方式は、セッションの成功した認証結果を提供しました。
Authc Failed	この方式は、セッションの失敗した認証結果を提供しました。

次の表に、使用できる認証方式を示します。

表 *28* : 認証方式のステート

状態	説明
dot1x	802.1X
mab	MAC 認証バイパス
webauth	Web 認証

次に、スイッチ上のすべての認証セッションを表示する例を示します。

```
Switch# show authentication sessions
Interface    MAC Address     Method   Domain   Status         Session ID
Gi1/0/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/0/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/0/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

次に、インターフェイス上のすべての認証セッションを表示する例を示します。

```
Switch# show authentication sessions interface gigabitethernet2/0/47
            Interface:  GigabitEthernet2/0/47
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Guest Vlan
          Vlan Policy:  20
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000000002763C
      Acct Session ID:  0x00000002
               Handle:  0x25000000
Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Failed over
----------------------------------------
            Interface:  GigabitEthernet2/0/47
          MAC Address:  0005.5e7c.da05
```

```
            IP Address:  Unknown
             User-Name:  00055e7cda05
                Status:  Authz Success
                Domain:  VOICE
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000010002A238
      Acct Session ID:  0x00000003
               Handle:  0x91000001
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

show auto security

自動セキュリティ ステータスを表示するには、特権 EXEC モードで **show auto security** コマンドを使用します。

show auto-security

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS Release 15.2(5)E	このコマンドは、Cisco IOS Release 15.2(5)E よりも前のリリースで導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードで**auto security** コマンドを設定すると、グローバルに自動セキュリティが設定されます（すべてのインターフェイスを含む）。自動セキュリティを無効にすると、すべてのインターフェイスで無効になります。

特定のインターフェイスで自動セキュリティを有効にするには、**auto security-port** コマンドを使用します。

自動セキュリティがグローバルに有効である場合の **show auto security** コマンドの出力例を次に示します。

```
Switch# show auto security

Auto Security is Enabled globally

AutoSecurity is Enabled on below interface(s):
-----------------------------------------------
   GigabitEthernet1/0/2
   GigabitEthernet1/0/3
   GigabitEthernet1/0/4
   GigabitEthernet1/0/5
   GigabitEthernet1/0/7
   GigabitEthernet1/0/8
   GigabitEthernet1/0/10
   GigabitEthernet1/0/12
   GigabitEthernet1/0/23
```

自動セキュリティが特定のインターフェイスで有効である場合の **show auto security** コマンドの出力例を次に示します。

```
Switch# show auto security

Auto Security is Disabled globally

AutoSecurity is Enabled on below interface(s):
-----------------------------------------------
```

```
GigabitEthernet1/0/2
```

関連コマンド

コマンド	説明
auto security	グローバルな自動セキュリティを設定します。
auto security-port	インターフェイス上で自動セキュリティを設定します。

show cisp

指定されたインターフェイスの CISP 情報を表示するには、**show cisp** 特権 EXEC コマンドを使用します。

show cisp { [**clients** | **interface** *interface-id*] | **registrations** | **summary**}

構文の説明

clients	（任意）CISP クライアントの詳細を表示します。
interface *interface-id*	（任意）指定されたインターフェイスの CISP 情報を表示します。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。
registrations	CISP の登録情報を表示します。
summary	（任意）CISP のサマリー情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドはCisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされていませんでした。

次の例では、**show cisp interface** コマンドの出力を示します。

```
Switch# show cisp interface fast 0
CISP not enabled on specified interface
```

次の例では、**show cisp registration** コマンドの出力を示します。

```
Switch# show cisp registrations
Interface(s) with CISP registered user(s):
-----------------------------------------
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
```

```
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
Auth Mgr (Authenticator)
Gi2/0/13
Auth Mgr (Authenticator)
Gi3/0/3
Gi3/0/5
Gi3/0/23
```

関連コマンド

コマンド	説明
cisp enable	Client Information Signalling Protocol（CISP）をイネーブルにします。
dot1x credentials プロファイル	サプリカント スイッチでプロファイルを設定します。

show dot1x

スイッチまたは指定されたポートのIEEE 802.1x統計情報、管理ステータス、および動作ステータスを表示するには、ユーザ EXEC モードで **show dot1x** コマンドを使用します。

show dot1x ［**all** ［**count** | **details** | **statistics** | **summary**］］［**interface** *type number*［**details** | **statistics**］］［**statistics**］

構文の説明

all	（任意）すべてのインターフェイスの IEEE 802.1x 情報を表示します。
count	（任意）許可されたクライアントと無許可のクライアントの総数を表示します。
details	（任意）IEEE 802.1x インターフェイスの詳細を表示します。
statistics	（任意）すべてのインターフェイスの IEEE 802.1x 統計情報を表示します。
summary	（任意）すべてのインターフェイスの IEEE 802.1x サマリー情報を表示します。
interface *type number*	（任意）指定したポートの IEEE 802.1X ステータスを表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、**show dot1x all** コマンドの出力を示します。

```
Switch# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            3
```

次の例では、**show dot1x all count** コマンドの出力を示します。

```
Switch# show dot1x all count
Number of Dot1x sessions
------------------------------
Authorized Clients        = 0
UnAuthorized Clients      = 0
```

```
Total No of Client        = 0
```

次の例では、**show dot1x all statistics** コマンドの出力を示します。

```
Switch# show dot1x statistics
Dot1x Global Statistics for
-------------------------------------------
RxStart = 0     RxLogoff = 0    RxResp = 0      RxRespID = 0
RxReq = 0       RxInvalid = 0   RxLenErr = 0
RxTotal = 0

TxStart = 0     TxLogoff = 0    TxResp = 0
TxReq = 0       ReTxReq = 0     ReTxReqFail = 0
TxReqID = 0     ReTxReqID = 0   ReTxReqIDFail = 0
TxTotal = 0
```

show eap pac peer

拡張認証プロトコル（EAP）のセキュア トンネリングを介したフレキシブル認証（FAST）ピアの格納済み Protected Access Credential（PAC）を表示するには、特権 EXEC モードで **show eap pac peer** コマンドを使用します。

show eap pac peer

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例は、**show eap pac peers** 特権 EXEC コマンドの出力を示します。

```
Switch> show eap pac peers
No PACs stored
```

関連コマンド

コマンド	説明
clear eap sessions	スイッチまたは指定されたポートの EAP のセッション情報をクリアします。

show ip dhcp snooping statistics

DHCP スヌーピング統計情報を概要形式または詳細形式で表示するには、ユーザ EXEC モードで **show ip dhcp snooping statistics** コマンドを使用します。

show ip dhcp snooping statistics ［**detail** ］

構文の説明

detail	（任意）詳細な統計情報を表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スイッチ スタックでは、すべての統計情報がスタック マスターで生成されます。新しいアクティブ スイッチが選定された場合、統計カウンタはリセットされます。

次の例では、**show ip dhcp snooping statistics** コマンドの出力を示します。

```
Switch> show ip dhcp snooping statistics

 Packets Forwarded                                = 0
 Packets Dropped                                  = 0
 Packets Dropped From untrusted ports             = 0
```

次の例では、**show ip dhcp snooping statistics detail** コマンドの出力を示します。

```
Switch> show ip dhcp snooping statistics detail

 Packets Processed by DHCP Snooping               = 0
 Packets Dropped Because
   IDB not known                                  = 0
   Queue full                                     = 0
   Interface is in errdisabled                    = 0
   Rate limit exceeded                            = 0
   Received on untrusted ports                    = 0
   Nonzero giaddr                                 = 0
   Source mac not equal to chaddr                 = 0
   Binding mismatch                               = 0
   Insertion of opt82 fail                        = 0
   Interface Down                                 = 0
   Unknown output interface                       = 0
   Reply output port equal to input port          = 0
   Packet denied by platform                      = 0
```

次の表に、DHCP スヌーピング統計情報およびその説明を示します。

表 *29 : DHCP* スヌーピング統計情報

DHCP スヌーピング統計情報	**説明**
Packets Processed by DHCP Snooping	転送されたパケットおよびドロップされたパケットも含めて、DHCP スヌーピングによって処理されたパケットの合計数。
Packets Dropped Because IDB not known	パケットの入力インターフェイスを判断できないエラーの数。
Queue full	パケットの処理に使用される内部キューが満杯であるエラーの数。非常に高いレートでDHCPパケットを受信し、入力ポートでレート制限がイネーブルになっていない場合、このエラーが発生することがあります。
Interface is in errdisabled	errdisable としてマークされたポートでパケットを受信した回数。これが発生する可能性があるのは、ポートが errdisable ステートである場合にパケットが処理キューに入り、そのパケットが後で処理される場合です。
Rate limit exceeded	ポートで設定されているレート制限を超えて、インターフェイスが errdisable ステートになった回数。
Received on untrusted ports	信頼できないポートで DHCP サーバ パケット（OFFER、ACK、NAK、LEASEQUERY のいずれか）を受信してドロップした回数。
Nonzero giaddr	信頼できないポートで受信した DHCP パケットのリレー エージェント アドレス フィールド（giaddr）がゼロ以外だった回数。または **no ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを設定しておらず、信頼できないポートで受信したパケットにオプション 82 データが含まれていた回数。
Source mac not equal to chaddr	DHCP パケットのクライアント MAC アドレス フィールド（chaddr）がパケットの送信元 MAC アドレスと一致せず、**ip dhcp snooping verify mac-address** グローバル コンフィギュレーション コマンドが設定されている回数。

DHCP スヌーピング統計情報	説明
Binding mismatch	MACアドレスとVLANのペアのバインディングになっているポートとは異なるポートで、RELEASEパケットまたはDECLINEパケットを受信した回数。これは、誰かが本来のクライアントをスプーフィングしようとしている可能性があることを示しますが、クライアントがスイッチの別のポートに移動してRELEASEまたはDECLINEを実行したことを表すこともあります。MAC アドレスは、イーサネットヘッダーの送信元MACアドレスではなく、DHCP パケットの chaddr フィールドから採用されます。
Insertion of opt82 fail	パケットへのオプション82挿入がエラーになった回数。オプション82データを含むパケットがインターネットの単一物理パケットのサイズを超えた場合、挿入はエラーになることがあります。
Interface Down	パケットが DHCP リレー エージェントへの応答であるが、リレー エージェントの SVI インターフェイスがダウンしている回数。DHCP サーバへのクライアント要求の送信と応答の受信の間で SVI がダウンした場合に発生するエラーですが、めったに発生しません。
Unknown output interface	オプション 82 データまたは MAC アドレス テーブルのルックアップのいずれかで、DHCP 応答パケットの出力インターフェイスを判断できなかった回数。パケットはドロップされます。オプション82が使用されておらず、クライアントMACアドレスが期限切れになった場合に発生することがあります。ポートセキュリティ オプションで IPSG がイネーブルであり、オプション 82 がイネーブルでない場合、クライアントのMACアドレスは学習されず、応答パケットはドロップされます。
Reply output port equal to input port	DHCP 応答パケットの出力ポートが入力ポートと同じであり、ループの可能性の原因となった回数。ネットワークの設定の誤り、またはポートの信頼設定の誤用の可能性を示します。
Packet denied by platform	プラットフォーム固有のレジストリによってパケットが拒否された回数。

show radius server-group

RADIUS サーバ グループのプロパティを表示するには、**show radius server-group** コマンドを使用します。

show radius server-group {*name* | **all**}

構文の説明

name	サーバ グループの名前。サーバ グループの名前の指定に使用する文字列は、**the aaa group server radius** コマンドを使用して定義する必要があります。
all	すべてのサーバ グループのプロパティを表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

aaa group server radius コマンドで定義したサーバ グループを表示するには、**show radius server-group** コマンドを使用します。

次の例では、**show radius server-group all** コマンドの出力を示します。

```
Switch# show radius server-group all
Server group radius
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *30 : show radius server-groups* コマンドのフィールドの説明

フィールド	説明
サーバ グループ	サーバ グループの名前。
Sharecount	このサーバ グループを共有している方式リストの数。たとえば、1つの方式リストが特定のサーバ グループを使用する場合、sharecount は 1 です。2 つの方式リストが同じサーバ グループを使用する場合、sharecount は 2 です。
sg_unconfigured	サーバ グループが設定解除されました。

フィールド	説明
タイプ	タイプは、standard または nonstandard のいずれかです。タイプはグループ内のサーバが非標準の属性を受け入れるかどうかを示します。グループ内のすべてのサーバに非標準のオプションが設定されている場合、タイプは「nonstandard」と表示されます。
Memlocks	メモリ内にあるサーバ グループ構造の内部参照の数。この数は、このサーバ グループへの参照を保持している内部データ構造パケットまたはトランザクションがいくつあるかを表します。Memlocks はメモリ管理のために内部的に使用されます。

show storm-control

スイッチまたは指定のインターフェイス上で、ブロードキャスト、マルチキャストまたはユニキャスト ストーム制御の設定を表示する、またはストーム制御の履歴を表示するには、ユーザ EXEC モードで **show storm-control** コマンドを使用します。

show storm-control [{*interface-id*}] [{**broadcast**|**multicast**|**unicast**}]

構文の説明

interface-id	（任意）物理ポートのインターフェイス ID（タイプ、スタック構成可能なスイッチのスタック メンバ、モジュール、ポート番号を含む）。
broadcast	（任意）ブロードキャスト ストームのしきい値設定を表示します。
multicast	（任意）マルチキャスト ストームのしきい値設定を表示します。
unicast	（任意）ユニキャスト ストームのしきい値設定を表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

インターフェイス ID を入力すると、指定されたインターフェイスのストーム制御しきい値が表示されます。

インターフェイス ID を入力しない場合、スイッチ上のすべてのポートに対して 1 つのトラフィック タイプの設定が表示されます。

トラフィック タイプを入力しない場合は、ブロードキャスト ストーム制御の設定が表示されます。

次の例では、キーワードを指定せずに入力した **show storm-control** コマンドの出力の一部を示します。トラフィック タイプのキーワードが入力されてないため、ブロードキャスト ストーム制御の設定が表示されます。

```
Switch> show storm-control
Interface Filter State  Upper      Lower     Current
--------- ------------- ---------- --------- ---------
Gi1/0/1   Forwarding    20 pps     10 pps    5 pps
Gi1/0/2   Forwarding    50.00%     40.00%    0.00%
<output truncated>
```

次の例では、指定されたインターフェイスの **show storm-control** コマンドの出力を示します。トラフィック タイプのキーワードが入力されてないため、ブロードキャスト ストーム制御の設定が表示されます。

```
Switch> show storm-control gigabitethernet 1/0/1
Interface Filter State  Upper      Lower     Current
--------- ------------- ---------- --------- ---------
Gi1/0/1   Forwarding    20 pps     10 pps    5 pps
```

次の表に、show storm-control の出力に表示されるフィールドの説明を示します。

表 *31 : show storm-control* のフィールドの説明

フィールド	説明
インターフェイス	インターフェイスの ID を表示します。
Filter State	フィルタのステータスを表示します。 • blocking：ストーム制御はイネーブルであり、ストームが発生しています。 • forwarding：ストーム制御はイネーブルであり、ストームは発生していません。 • Inactive：ストーム制御はディセーブルです。
Upper	上限抑制レベルを利用可能な全帯域幅のパーセンテージとして、毎秒のパケット数または毎秒のビット数で表示します。
Lower	下限抑制レベルを利用可能な全帯域幅のパーセンテージとして、毎秒のパケット数または毎秒のビット数で表示します。
Current	ブロードキャスト トラフィックまたは指定されたトラフィック タイプ（ブロードキャスト、マルチキャスト、ユニキャスト）の帯域幅の使用状況を、利用可能な全帯域幅のパーセンテージで表示します。このフィールドは、ストーム制御がイネーブルの場合だけ有効です。

関連トピック

storm-control （906 ページ）

show vlan access-map

特定の VLAN アクセス マップまたはすべての VLAN アクセス マップに関する情報を表示するには、特権 EXEC モードで **show vlan access-map** コマンドを使用します。

show vlan access-map [*map-name*]

構文の説明

map-name	（任意）特定の VLAN アクセス マップ名。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、**show vlan access-map** コマンドの出力を示します。

```
Switch# show vlan access-map
Vlan access-map "vmap4"  10
  Match clauses:
    ip  address: al2
  Action:
    forward
Vlan access-map "vmap4"  20
  Match clauses:
    ip  address: al2
  Action:
    forward
```

関連トピック

show vlan filter （904 ページ）
vlan access-map （937 ページ）
vlan filter （939 ページ）

show vlan filter

すべての VLAN フィルタ、または特定の VLAN または VLAN アクセス マップに関する情報を表示するには、特権 EXEC モードで **show vlan filter** コマンドを使用します。

show vlan filter {**access-map** *name*|**vlan** *vlan-id*}

構文の説明

access-map *name*	（任意）指定された VLAN アクセス マップのフィルタリング情報を表示します。
vlan *vlan-id*	（任意）指定された VLAN のフィルタリング情報を表示します。指定できる範囲は 1 ～ 4094 です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、**show vlan filter** コマンドの出力を示します。

```
Switch# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

関連トピック

show vlan access-map （903 ページ）
vlan access-map （937 ページ）
vlan filter （939 ページ）

show vlan group

VLAN グループにマッピングされている VLAN を表示するには、特権 EXEC モードで **show vlan group** コマンドを使用します。

show vlan group [{**group-name** *vlan-group-name* **[user_count]**}]

構文の説明

group-name *vlan-group-name*	（任意）指定した VLAN グループにマッピングされている VLAN を表示します。
user_count	（任意）特定の VLAN グループにマッピングされている各 VLAN のユーザ数を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

show vlan group コマンドは既存の VLAN グループを表示し、各 VLAN グループのメンバである VLAN および VLAN の範囲を示します。**group-name** キーワードを入力すると、指定した VLAN グループのメンバのみが表示されます。

次の例では、特定の VLAN グループのメンバを表示する方法を示します。

```
Switch# show vlan group group-name group2
vlan group group1 :40-45
```

次に、グループ内の各 VLAN のユーザ数を表示する例を示します。

```
Switch# show vlan group group-name group2 user_count
  VLAN     : Count
-------------------
  40         : 5
  41         : 8
  42         : 12
  43         : 2
  44         : 9
  45         : 0
```

関連トピック

vlan group （941 ページ）

storm-control

ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御をイネーブルにして、インターフェイスのしきい値レベルを設定するには、インターフェイス コンフィギュレーション モードで **storm-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

storm-control {**action** {**shutdown**|**trap**}|{**broadcast**|**multicast**|**unicast**} **level** {*level* [*level-low*]|**bps** *bps* [*bps-low*]|**pps** *pps* [*pps-low*]}}
no storm-control {**action** {**shutdown**|**trap**}|{**broadcast**|**multicast**|**unicast**} **level**}

構文の説明

action	ポートでストームが発生した場合に実行されるアクションを指定します。デフォルト アクションは、トラフィックをフィルタリングし、簡易ネットワーク管理プロトコル（SNMP）トラップを送信しません。
shutdown	ストームの間、ポートをディセーブルにします。
trap	ストームが発生した場合に SNMP トラップを送信します。
broadcast	インターフェイス上でブロードキャスト ストーム制御をイネーブルにします。
multicast	インターフェイス上でマルチキャスト ストーム制御をイネーブルにします。
unicast	インターフェイス上でユニキャスト ストーム制御をイネーブルにします。
level	上限および下限抑制レベルをポートの全帯域幅の割合で指定します。
level	上限抑制レベル（小数点以下第 2 位まで）。指定できる範囲は 0.00 ～ 100.00 です。指定した level の値に達した場合、ストーム パケットのフラッディングをブロックします。
level-low	（任意）下限抑制レベル（小数点以下第 2 位まで）。指定できる範囲は 0.00 ～ 100.00 です。この値は上限抑制値より小さいか、または等しくなければなりません。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。
level bps	上限および下限抑制レベルを、ポートで受信するトラフィックの速度（ビット/秒）で指定します。
bps	上限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。指定した bps の値に達した場合、ストーム パケットのフラッディングをブロックします。 大きい数値のしきい値には、k、m、g などのメトリック サフィクスを使用できます。

bps-low	（任意）下限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。この値は上限抑制値に等しいか、または小さくなければなりません。 大きい数値のしきい値には、k、m、g などのメトリック サフィクスを使用できます。
level pps	上限および下限抑制レベルを、ポートで受信するトラフィックの速度（パケット/秒）で指定します。
pps	上限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。指定した pps の値に達した場合、ストーム パケットのフラッディングをブロックします。 大きい数値のしきい値には、k、m、g などのメトリック サフィクスを使用できます。
pps-low	（任意）下限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。この値は上限抑制値に等しいか、または小さくなければなりません。 大きい数値のしきい値には、k、m、g などのメトリック サフィクスを使用できます。

コマンド デフォルト

ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御はディセーブルです。

デフォルト アクションは、トラフィックをフィルタリングし、SNMP トラップを送信しません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ストーム制御抑制レベルは、ポートの全帯域幅の割合、またはトラフィックを受信する速度（1 秒あたりのパケット数、または 1 秒あたりのビット数）で入力できます。

全帯域幅の割合で指定した場合、100% の抑制値は、指定したトラフィック タイプに制限が設定されていないことを意味します。**level 0 0** の値は、ポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックをブロックします。ストーム制御は、上限抑制レベルが 100% 未満の場合にだけイネーブルになります。他のストーム制御設定が指定されていない場合、デフォルト アクションは、ストームの原因となっているトラフィックをフィルタリングし、SNMP トラップを送信しません。

（注） マルチキャスト トラフィックのストーム制御しきい値に達した場合、ブリッジプロトコルデータ ユニット（BPDU）および Cisco Discovery Protocol（CDP）フレームなどの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。ただし、スイッチは、Open Shortest Path First（OSPF）および通常のマルチキャスト データ トラフィック間のように、ルーティング アップデート間を区別しないため、両方のタイプのトラフィックがブロックされます。

trap および **shutdown** オプションは、互いに独立しています。

パケット ストームが検出されたときにシャットダウンを行う（ストームの間、ポートが error-disabled になる）ようにアクションを設定する場合、インターフェイスをこのステートから解除するには **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必要があります。**shutdown** アクションを指定しない場合、アクションを **trap**（ストーム検出時にスイッチがトラップを生成する）に指定してください。

ストームが発生し、実行されるアクションがトラフィックのフィルタリングである場合、下限抑制レベルが指定されていないと、トラフィック レートが上限抑制レベルより低くなるまでスイッチはすべてのトラフィックをブロックします。下限抑制レベルが指定されている場合、トラフィック レートがこのレベルより低くなるまでスイッチはトラフィックをブロックします。

（注） ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ブロードキャスト ストームが発生し、実行されるアクションがトラフィックのフィルタである場合、スイッチはブロードキャスト トラフィックだけをブロックします。

詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

次の例では、75.5% の上限抑制レベルでブロードキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control broadcast level 75.5
```

次の例では、87% の上限抑制レベルと 65% の下限抑制レベルのポートでユニキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control unicast level 87 65
```

次の例では、2000 パケット/秒の上限抑制レベルと 1000 パケット/秒の下限抑制レベルのポートでマルチキャスト ストーム制御をイネーブルにする方法を示します。

```
Switch(config-if)# storm-control multicast level pps 2k 1k
```

次の例では、ポートで **shutdown** アクションをイネーブルにする方法を示します。

```
Switch(config-if)# storm-control action shutdown
```

設定を確認するには、**show storm-control** 特権 EXEC コマンドを入力します。

関連トピック

show storm-control （901 ページ）

switchport port-security aging

セキュア アドレス エントリのエージング タイムおよびタイプを設定する、または特定のポートのセキュア アドレスのエージング動作を変更するには、インターフェイス コンフィギュレーション モードで **switchport port-security aging** コマンドを使用します。ポート セキュリティ エージングをディセーブルにする、またはパラメータをデフォルトの状態に設定するには、このコマンドの **no** 形式を使用します。

switchport port-security aging {**static**|**time** *time*|**type** {**absolute**|**inactivity**}}
no switchport port-security aging {**static**|**time**|**type**}

構文の説明

static	このポートに静的に設定されたセキュア アドレスのエージングをイネーブルにします。
time *time*	このポートのエージング タイムを指定します。指定できる範囲は0～1440分です。time が 0 の場合、このポートのエージングはディセーブルです。
type	エージング タイプを設定します。
absolute	absolute エージング タイプを設定します。このポートのすべてのセキュア アドレスは、指定された時間（分）が経過した後に期限切れとなり、セキュア アドレス リストから削除されます。
inactivity	inactivity エージング タイプを設定します。指定された時間内にセキュア送信元アドレスからのデータ トラフィックがない場合だけ、このポートのセキュア アドレスが期限切れになります。

コマンド デフォルト

ポート セキュリティ エージング機能はディセーブルです。デフォルトの時間は 0 分です。

デフォルトのエージング タイプは absolute です。

デフォルトのスタティック エージング動作はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

特定のポートのセキュア アドレス エージングをイネーブルにするには、ポート エージング タイムを 0 以外の値に設定します。

特定のセキュア アドレスに時間を限定してアクセスできるようにするには、エージング タイプを **absolute** に設定します。エージング タイムの期限が切れると、セキュア アドレスが削除されます。

継続的にアクセスできるセキュア アドレス数を制限するには、エージング タイプを **inactivity** に設定します。このようにすると、非アクティブになったセキュア アドレスが削除され、他のアドレスがセキュアになることができます。

セキュア アドレスへのアクセス制限を解除するには、セキュア アドレスとして設定し、**no switchport port-security aging static** インターフェイス コンフィギュレーション コマンドを使用して、静的に設定されたセキュア アドレスのエージングをディセーブルにします。

次の例では、ポートのすべてのセキュア アドレスに対して、エージング タイプを absolute、エージング タイムを 2 時間に設定します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport port-security aging time 120
```

次の例では、ポートに設定されたセキュア アドレスに対して、エージング タイプを inactivity、エージング タイムを 2 分に設定します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

次の例では、設定されたセキュア アドレスのエージングをディセーブルにする方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport port-security aging static
```

関連トピック

show interfaces switchport （140 ページ）
switchport port-security mac-address （912 ページ）
switchport port-security maximum （915 ページ）
switchport port-security violation （918 ページ）

switchport port-security mac-address

セキュアMACアドレスまたはスティッキMACアドレス ラーニングを設定するには、**switchport port-security mac-address** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security mac-address {*mac-address* [{**vlan** {*vlan-id* {**access**|**voice**}}}]|**sticky** [{*mac-address*|**vlan** {*vlan-id* {**access**|**voice**}}}]}
no switchport port-security mac-address {*mac-address* [{**vlan** {*vlan-id* {**access**|**voice**}}}]|**sticky** [{*mac-address*|**vlan** {*vlan-id* {**access**|**voice**}}}]}

構文の説明

mac-address	48 ビット MAC アドレスの入力によって指定するインターフェイスのセキュア MAC アドレス。設定された最大数まで、セキュア MAC アドレスを追加できます。
vlan *vlan-id*	（任意）トランク ポート上でだけ、VLAN ID および MAC アドレスを指定します。VLAN ID を指定しない場合は、ネイティブ VLAN が使用されます。
vlan access	（任意）アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。
vlan voice	（任意）アクセス ポートでだけ、VLAN を音声 VLAN として指定します。 （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合に限り利用可能です。
sticky	スティッキ ラーニングのインターフェイスをイネーブルにします。スティッキ ラーニングをイネーブルにすると、インターフェイスは動的に学習したすべてのセキュア MAC アドレスを実行コンフィギュレーションに追加して、これらのアドレスをスティッキ セキュア MAC アドレスに変換します。
mac-address	（任意）スティッキ セキュア MAC アドレスを指定する MAC アドレス。

コマンド デフォルト

セキュア MAC アドレスは設定されていません。

スティッキ ラーニングはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることはできますが、ダイナミック アクセス ポートには設定できません。

- セキュア ポートはルーテッド ポートにはできません。
- セキュア ポートは保護ポートにはできません。
- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。
- セキュア ポートをギガビットまたは 10 ギガビット EtherChannel ポート グループに含めることはできません。
- 音声 VLAN では、スタティック セキュアまたはスティッキ セキュア MAC アドレスを設定できません。
- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュア アドレスを設定する必要があります。
- 音声 VLAN はアクセス ポート上でだけサポートされます。トランク ポート上ではサポートされません。

スティッキ セキュア MAC アドレスには、次の特性があります。

- **switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイス上でスティッキ ラーニングをイネーブルにした場合、インターフェイスはすべてのダイナミック セキュア MAC アドレス（スティッキ ラーニングがイネーブルになる前に動的に学習されたアドレスを含む）を、スティッキ セキュア MAC アドレスに変換し、すべてのスティッキ セキュア MAC アドレスを実行コンフィギュレーションに追加します。
- **no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、スティッキ ラーニングをディセーブルする場合、または実行コンフィギュレーションを削除する場合は、スティッキ セキュア MAC アドレスは実行コンフィギュレーションの一部に残りますが、アドレス テーブルからは削除されます。削除されたアドレスはダイナミックに再設定することができ、ダイナミック アドレスとしてアドレス テーブルに追加されます。
- **switchport port-security mac-address sticky** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して、スティッキ セキュア MAC アドレスを設定する場合、これらのアドレスはアドレス テーブルおよび実行コンフィギュレーションに追加されます。ポート セキュリティがディセーブルの場合、スティッキ セキュア MAC アドレスは実行コンフィギュレーションに残ります。
- スティッキ セキュア MAC アドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時、またはインターフェイスのシャットダウン時に、インターフェイスはこれらのアドレスを再学習しなくてすみます。スティッキ セキュア アドレスを保存しない場合、アドレスは失われます。スティッキ ラーニングがディセーブルの場

合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

- スティッキ ラーニングをディセーブルにして、**switchport port-security mac-address sticky** *mac-address* インターフェイス コンフィギュレーション コマンドを入力した場合、エラー メッセージが表示され、スティッキ セキュア MAC アドレスは実行コンフィギュレーションに追加されません。

設定を確認するには、**show port-security** 特権 EXEC コマンドを入力します。

次の例では、ポートでセキュア MAC アドレスと VLAN ID を設定する方法を示します。

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

次の例では、スティッキ ラーニングをイネーブルにして、ポート上で 2 つのスティッキ セキュア MAC アドレスを入力する方法を示します。

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

関連トピック

show interfaces switchport （140 ページ）
switchport port-security aging （910 ページ）
switchport port-security maximum （915 ページ）
switchport port-security violation （918 ページ）

switchport port-security maximum

セキュアMACアドレスの最大数を設定するには、インターフェイス コンフィギュレーション モードで **switchport port-security maximum** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security maximum *value* [**vlan** [{*vlan-list*|[{**access**|**voice**}]}]]
no switchport port-security maximum *value* [**vlan** [{*vlan-list*|[{**access**|**voice**}]}]]

構文の説明

value	インターフェイスのセキュア MAC アドレスの最大数を設定します。 デフォルトの設定は 1 秒です。
vlan	（任意）トランク ポートの場合、VLAN ごとまたは一定範囲の VLAN のセキュア MAC アドレスの最大数を設定します。**vlan** キーワードが入力されていない場合、デフォルト値が使用されます。
vlan-list	（任意）カンマで区切られたVLANの範囲またはハイフンで区切られた一連のVLAN。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。
access	（任意）アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。
voice	（任意）アクセス ポートでだけ、VLAN を音声 VLAN として指定します。 （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。

コマンド デフォルト

ポートセキュリティをイネーブルにしてキーワードを入力しない場合、デフォルトのセキュア MAC アドレスの最大数は 1 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スイッチまたはスイッチ スタックに設定できるセキュアMACアドレスの最大数は、システムで許可されているMACアドレスの最大数によって決まります。この数字はアクティブなSwitch Database Management（SDM）テンプレートによって決められます。**sdm prefer** コマンドを参照してください。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他のセキュア MAC アドレスなど、利用可能な MAC アドレスの合計数を示します。

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることができます。

- セキュア ポートはルーテッド ポートにはできません。
- セキュア ポートは保護ポートにはできません。
- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。
- セキュア ポートをギガビットまたは 10 ギガビット EtherChannel ポート グループに含めることはできません。
- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュア アドレスを設定する必要があります。

  音声 VLAN はアクセス ポート上でだけサポートされます。トランク ポート上ではサポートされません。
- インターフェイスのセキュア アドレスの最大値を入力する場合、新しい値が前回の値より大きいと、新しい値によって前回の設定値が上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュア アドレス数が新しい値より大きい場合、コマンドは拒否されます。

  アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、確実にデバイスがポートの帯域幅を完全に使用できます。

インターフェイスのセキュア アドレスの最大値を入力すると、次の事象が発生します。

- 新しい値が前回の値より大きい場合、新しい値によって前回の設定値が上書きされます。
- 新しい値が前回の値より小さく、インターフェイスで設定されているセキュア アドレス数が新しい値より大きい場合、コマンドは拒否されます。

設定を確認するには、**show port-security** 特権 EXEC コマンドを入力します。

次の例では、ポートでポート セキュリティをイネーブルにし、セキュア アドレスの最大数を 5 に設定する方法を示します。違反モードはデフォルトで、セキュア MAC アドレスは設定されていません。

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
```

関連トピック

show interfaces switchport （140 ページ）
switchport port-security aging （910 ページ）
switchport port-security mac-address （912 ページ）

switchport port-security violation （918 ページ）

switchport port-security violation

セキュアMACアドレスの違反モード、またはポートセキュリティに違反した場合に実行するアクションを設定するには、インターフェイス コンフィギュレーション モードで **switchport port-security violation** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security violation {protect|restrict| shutdown|shutdown vlan}
no switchport port-security violation {protect|restrict| shutdown|shutdown vlan}

構文の説明

protect	セキュリティ違反保護モードを設定します。
restrict	セキュリティ違反制限モードを設定します。
shutdown	セキュリティ違反シャットダウン モードを設定します。
shutdown vlan	VLANごとのシャットダウンにセキュリティ違反モードを設定します。

コマンド デフォルト

デフォルトの違反モードは、**shutdown** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

セキュリティ違反保護モードでは、ポートのセキュアMACアドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。ドロップすることでセキュアMACアドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。セキュリティ違反が起こっても、ユーザには通知されません。

（注） トランクポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大数に達していなくてもVLANが保護モードの最大数に達すると、ラーニングがディセーブルになります。

セキュリティ違反制限モードでは、セキュアMACアドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。セキュアMACアドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。SNMPトラップが送信されます。Syslogメッセージがロギングされ、違反カウンタが増加します。

セキュリティ違反シャットダウンモードでは、違反が発生し、ポートのLEDがオフになると、インターフェイスが errdisable になります。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。セキュア ポートが error-disabled ステートの場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力してこのステートから回復させるか、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力して手動で再びイネーブルにすることができます。

セキュリティ違反モードが VLAN ごとのシャットダウンに設定されると、違反が発生した VLAN のみが errdisable になります。

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることができます。
- セキュア ポートはルーテッド ポートにはできません。
- セキュア ポートは保護ポートにはできません。
- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。
- セキュア ポートをギガビットまたは 10 ギガビット EtherChannel ポート グループに含めることはできません。

  セキュア MAC アドレスの最大値がアドレス テーブルに存在し、アドレス テーブルに存在しない MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合、または別のセキュア ポートのセキュア MAC アドレスとして設定された MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合に、セキュリティ違反が起こります。

  セキュア ポートが errdisable ステートの場合は、**errdisable recovery cause** *psecure-violation* グローバル コンフィギュレーション コマンドを入力して、このステートから回復させることができます。**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力するか、**clear errdisable interface** 特権 EXEC コマンドを使用して、ポートを手動で再びイネーブルにすることができます。

設定を確認するには、**show port-security** 特権 EXEC コマンドを入力します。

次の例では、MAC セキュリティ違反が発生した場合に VLAN のみをシャットダウンするようポートを設定する方法を示します。

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config)# switchport port-security violation shutdown vlan
```

関連トピック

show interfaces switchport （140 ページ）
switchport port-security aging （910 ページ）
switchport port-security mac-address （912 ページ）
switchport port-security maximum （915 ページ）

tracking（IPv6 スヌーピング）

ポートでデフォルトのトラッキング ポリシーを上書きするには、IPv6 スヌーピング ポリシー コンフィギュレーション モードで **tracking** コマンドを使用します。

tracking {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}

構文の説明

enable	トラッキングをイネーブルにします。
reachable-lifetime	（任意）到達可能という証明がない状態で、到達可能なエントリが直接的または間接的に到達可能であると判断される最大時間を指定します。 • **reachable-lifetime** キーワードを使用できるのは、**enable** キーワードが指定されている場合のみです。 • **reachable-lifetime** キーワードを使用すると、 **ipv6 neighbor binding reachable-lifetime** コマンドで設定されたグローバルな到達可能ライフタイムが上書きされます。
value	秒単位のライフタイム値。指定できる範囲は 1 ～ 86400 で、デフォルトは 300 です。
infinite	エントリを無限に到達可能状態またはステイル状態に維持します。
disable	トラッキングをディセーブルにします。
stale-lifetime	（任意）時間エントリをステイル状態に維持します。これによりグローバルの stale-lifetime 設定が上書きされます。 • ステイル ライフタイムは 86,400 秒です。 • **stale-lifetime** キーワードを使用できるのは、**disable** キーワードが指定されている場合のみです。 • **stale-lifetime** キーワードを使用すると、**ipv6 neighbor binding stale-lifetime** コマンドで設定されたグローバルなステイル ライフタイムが上書きされます。

コマンド デフォルト

時間のエントリは到達可能な状態に維持されます。

コマンド モード

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

tracking コマンドは、このポリシーが適用されるポート上で **ipv6 neighbor tracking** コマンドによって設定されたデフォルトのトラッキング ポリシーに優先します。この機能は、たとえば、エントリを追跡しないが、バインディング テーブルにエントリを残して盗難を防止する場合などに、信頼できるポート上で有用です。

reachable-lifetime キーワードは、到達可能という証明がない状態で、あるエントリがトラッキングにより直接的に、または IPv6 スヌーピングにより間接的に到達可能であると判断される最大時間を示します。**reachable-lifetime** 値に到達すると、エントリはステイル状態に移行します。tracking コマンドで **reachable-lifetime** キーワードを使用すると、**ipv6 neighbor binding reachable-lifetime** コマンドで設定されたグローバルな到達可能ライフタイムが上書きされます。

stale-lifetime キーワードは、エントリが削除されるか、直接または間接的に到達可能であると証明される前にテーブルに保持される最大時間です。**tracking** コマンドで **reachable-lifetime** キーワードを使用すると、**ipv6 neighbor binding stale-lifetime** コマンドで設定されたグローバルなステイル ライフタイムが上書きされます。

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、エントリを信頼できるポート上で無限にバインディング テーブルに保存するように設定する例を示します。

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# tracking disable stale-lifetime infinite
```

trusted-port

あるポートを信頼できるポートとして設定するには、IPv6 スヌーピング ポリシー モードまたはND 検査ポリシー コンフィギュレーション モードで **trusted-port** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

trusted-port
no trusted-port

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

どのポートも信頼されていません。

コマンド モード

ND インスペクション ポリシーの設定

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

trusted-port コマンドをイネーブルにすると、メッセージがこのポリシーを持つポートで受信された場合、限定的に実行されるか、まったく実行されません。ただし、アドレス スプーフィングから保護するために、メッセージは伝送するバインディング情報の使用によってバインディングテーブルを維持できるように分析されます。これらのポートで検出されたバインディングは、信頼できるものとして設定されていないポートから受信したバインディングよりも信頼性が高いものと見なされます。

次に、NDP ポリシー名を policy1 と定義し、スイッチを NDP インスペクション ポリシー コンフィギュレーション モードにし、ポートを信頼するように設定する例を示します。

```
Switch(config)# ipv6  nd inspection  policy1
Switch(config-nd-inspection)# trusted-port
```

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、ポートを信頼するように設定する例を示します。

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# trusted-port
```

wireless dot11-padding

Over-the-Air フレーム パディングをイネーブルにするには、**wirelessdot11-padding** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

wireless dot11-padding
no wireless dot11-padding

コマンド デフォルト

ディセーブル

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、Over-the-Air フレーム パディングをイネーブルにする例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless dot11-padding
```

wireless security dot1x

IEEE 802.1x のグローバル コンフィギュレーションを設定するには、**wirelesssecuritydot1x** コマンドを使用します。

wireless security dot1x [{**eapol-key** {**retries** *retries*|**timeout** *milliseconds*}|**group-key interval** 秒|**identity-request** {**retries** *retries*|**timeout** *seconds*}|**radius [call-station-id]** {**ap-macaddress**|**ap-macaddress-ssid**|**ipaddress**|**macaddress**}|**request** {**retries** *retries*|**timeout** *seconds*}|**wep key** {**index 0**|**index 3**}}]

構文の説明

eapol-key	eapol-key 関連パラメータを設定します。
retries *retries*	（任意）コントローラが無線クライアントに EAPOL（WPA）キー メッセージを再送信する最大回数（0～4）を指定します。 デフォルト値は 2 です。
timeout *milliseconds*	（任意）EAP または WPA/WPA-2 PSK を使用してコントローラが無線クライアントに EAPOL（WPA）キー メッセージを再送信するまでに待機する時間（200 ～ 5000 ミリ秒）を指定します。 デフォルト値は 1000 ミリ秒です。
group-keyinterval 秒	EAP ブロードキャスト キーを更新する間隔を秒で設定します（120～86400 秒）。
identity-request	EAP ID 要求の関連パラメータを設定します。
retries *retries*	（任意）コントローラが EAP ID を要求する最大試行回数（0～4）を指定します。 デフォルト値は 2 です。
timeout *seconds*	（任意）コントローラが無線クライアントに EAP ID 要求メッセージを再送信するまでに待機する時間（1 ～ 120 秒）を指定します。 デフォルト値は 30 秒です。
radius	RADIUS メッセージを設定します。
call-station-id	（任意）RADIUS メッセージで送信されるコール ステーション ID を設定します。
ap-macaddress	呼出端末 ID タイプを AP の MAC アドレスに設定します。
ap-macaddress-ssid	呼出端末 ID タイプを 'AP の MAC アドレス':'SSID' に設定します。
ipaddress	呼出端末 ID タイプをシステムの IP アドレスに設定します。
macaddress	呼出端末 ID タイプをシステムの MAC アドレスに設定します。

request	EAP 要求の関連パラメータを設定します。
retries *retries*	（任意）ID 要求または EAPOL（WPA）キー メッセージ以外の EAP メッセージについて、コントローラが無線クライアントにメッセージを再送信する最大回数（0 ～ 20）を指定します。 デフォルト値は 2 です。
timeout *seconds*	（任意）ID 要求または EAPOL（WPA）キー メッセージ以外の EAP メッセージについて、コントローラが無線クライアントにメッセージを再送信するまでに待機する時間（1 ～ 120 秒）を指定します。 デフォルト値は 30 秒です。
wepkey	802.1x WEP 関連パラメータを設定します。
index0	WEP キーのインデックス値を 0 として指定します。
index3	WEP キーのインデックス値を 3 として指定します。

コマンド デフォルト

eapol-key-timeout のデフォルト値：1 秒。

eapol-key-retries のデフォルト値：2 回。

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

この例では、**wirelesssecuritydot1x** の下のすべてのコマンドを示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless security dot1x ?
  eapol-key         Configure eapol-key related parameters
  group-key         Configures EAP-broadcast key renew interval time in seconds
  identity-request  Configure EAP ID request related parameters
  radius            Configure radius messages
  request           Configure EAP request related parameters
  wep               Configure 802.1x WEP related paramters
  <cr>
```

wireless security lsc

ローカルで有効な証明書を設定するには、**wirelesssecuritylsc** コマンドを使用します。

wireless security lsc {**ap-provision** [{**auth-list** *mac-addr*|**revert** *number*}]|**other-params** *key-size*|**subject-params** *country state city orgn dept email*|**trustpoint** トラストポイント}

構文の説明

ap-provision	アクセス ポイント プロビジョニング リストの設定を指定します。
auth-list *mac-addr*	プロビジョニング リストの許可設定を指定します。
revert *number*	デフォルトの証明書に戻る前にアクセス ポイントが LSC を使用してコントローラへの接続を試行する回数。最大試行回数は 255 以下にする必要があります。
other-params *key-size*	デバイスの証明書キーのサイズ設定を指定します。
subject-params *country state city orgn dept email*	デバイス証明書の設定を指定します。認証局の国、州、市、組織、部門、および電子メール。
trustpoint トラストポイント	LSC のトラスト ポイントを指定します。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

1 つの CA サーバだけを設定できます。別の CA サーバを設定するには、config certificate lsc ca-server delete コマンドを使用して設定済みの CA サーバを削除した後、別の CA サーバを設定します。

アクセス ポイント プロビジョニング リストを設定する場合は、AP プロビジョニングを有効にしたときに（手順8）プロビジョニング リストのアクセス ポイントだけがプロビジョニングされます。アクセス ポイント プロビジョン リストを設定しない場合、コントローラに接続する MIC または SSC 証明書を持つすべてのアクセス ポイントが LSC でプロビジョニングされます。

次の例に、ローカルで有効な証明書の設定方法を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless security lsc ?
  ap-provision    Provisioning the AP's with LSC's
  other-params    Configure Other Parameters for Device Certs
```

```
subject-params  Configure the Subject Parameters for Device Certs
trustpoint      Configure LSC Trustpoint
<cr>
```

wireless security strong-password

強力なパスワードの強制オプションを設定するには、**wirelesssecuritystrong-password** コマンドを使用します。強力なパスワードをディセーブルにするには、このコマンドの no 形式を使用します。

wireless security strong-password
no wireless security strong-password

コマンド デフォルト

なし。

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、ワイヤレス セキュリティのための強力なパスワードを設定する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless security strong-password
```

wireless wps ap-authentication

アクセス ポイントのネイバー認証を設定するには、**wirelesswpsap-authentication** コマンドを使用します。アクセス ポイントのネイバー認証を削除するには、このコマンドの no 形式を使用します。

wireless wps ap-authentication [**threshold** *value*]
no wireless wps ap-authentication [threshold]

構文の説明

threshold *value*	（任意）無線 LAN の WMM 対応クライアントであることを指定します。しきい値（1 ～ 255）。

コマンド デフォルト

なし。

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、WMM 対応クライアントのしきい値を設定する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless wps ap-authentication threshold 65
```

wireless wps auto-immune

サービス妨害（DoS）攻撃からの保護をイネーブルにするには、**wirelesswpsauto-immune** コマンドを使用します。ディセーブルにするには、このコマンドの no 形式を使用します。

wireless wps auto-immune
no wireless wps auto-immune

コマンド デフォルト

ディセーブル

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

潜在的な攻撃者は特別に作成したパケットを使用し、正規のクライアントを攻撃者として処理するように侵入検知システム（IDS）を誘導する場合があります。それによって、コントローラはこの正規のクライアントの接続を解除し、DoS 攻撃が開始されます。自己免疫機能は、有効な場合にこのような攻撃を防ぐように設計されています。ただし、自己免疫機能を有効にすると、Cisco 792x フォンを使用した会話が断続的に中断されることがあります。792x フォンを使用しているときに頻繁に中断されるようであれば、この機能を無効にしてください。

次の例では、サービス妨害（DoS）攻撃からの保護をイネーブルにする方法を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless wps auto-immune
```

wireless wps cids-sensor

Wireless Protection System（WPS）の侵入検知システム（IDS）センサーを設定するには、**wirelesswpscids-sensor** コマンドを使用します。Wireless Protection System（WPS）の侵入検知システム（IDS）センサーを削除するには、このコマンドの no 形式を使用します。

wireless wps cids-sensor *index* [**ip-address** *ip-addr* **username** *username* **password** *password_type password*]
no wireless wps cids-sensor *index*

構文の説明

index	IDS センサーの内部インデックスを指定します。
ip-address *ip-addr***username** *username***password** *password_type password*	IDS センサーの IP アドレス、IDS センサーのユーザ名、パスワード タイプ、および IDS センサーのパスワードを指定します。

コマンド デフォルト

ディセーブル

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし

次に、IDS インデックス、IDS センサーの IP アドレス、IDS ユーザ名およびパスワードを使用して侵入検知システムを設定する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless wps cids-sensor 1 10.0.0.51 Sensor_user0doc1 passowrd01
```

wireless wps client-exclusion

クライアント除外ポリシーを設定するには、**wireless wps client-exclusion** コマンドを使用します。クライアント除外ポリシーを削除するには、このコマンドの **no** 形式を使用します。

wireless wps client-exclusion {**all**|**dot11-assoc**|**dot11-auth**|**dot1x-auth**|**ip-theft**|**web-auth**}
no wireless wps client-exclusion {**all**|**dot11-assoc**|**dot11-auth**|**dot1x-auth**|**ip-theft**|**web-auth**}

構文の説明

dot11-assoc	コントローラが 802.11 アソシエーションに連続 5 回失敗すると、6 回目の試行を除外することを指定します。
dot11-auth	コントローラが 802.11 認証に連続 5 回失敗すると、6 回目の試行を除外することを指定します。
dot1x-auth	コントローラが 802.11X 認証に連続 5 回失敗すると、6 回目の試行を除外することを指定します。
ip-theft	IP アドレスがすでに別のデバイスに割り当てられている場合は、コントローラがクライアントを除外することを指定します。 詳細については、「使用上のガイドライン」セクションを参照してください。
web-auth	コントローラが Web 認証に連続 3 回失敗すると、4 回目の試行を除外することを指定します。
all	コントローラが上記のすべての理由でクライアントを除外することを指定します。

コマンド デフォルト

イネーブル

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

IP 窃盗シナリオに、古い Cisco IOS XE リリースと Cisco IOS XE Denali 16.x リリースの相違点があります。

古い Cisco IOS XE リリース	Cisco IOS XE Denali 16.x リリース
優先順位に従って、有線クライアントはワイヤレス クライアントよりも優先され、DHCP IP はスタティック IP よりも優先されます。クライアントのセキュリティ タイプはチェックされません。すべてのクライアント タイプのセキュリティが同じ優先順位で処理されます。 既存のバインドが優先順位の高いソースに由来する場合、新しいバインドは無視され、IP 窃盗の信号が送信されます。既存のバインドが新しいバインドと同じ優先順位のソースに由来する場合、新しいバインドは無視され、IP 窃盗の信号が送信されます。その結果、2 つのホストが同じ IP を使用してトラフィックを送信した場合、バインドは切り替わらないことになります。最初のバインドのみがソフトウェアに格納されます。新しいバインドが優先順位のより高いソースに由来する場合、既存のバインドは置き換えられます。その結果、既存のバインドの IP 窃盗通知と、新しいバインドの通知が送信されます。	有線とワイヤレスの間に基本的な相違はありません。重視されるのは、エントリの信頼性（優先度）、エントリの伝達経路となった機能（ARP、DHCP、ND など）、およびポートに付与されているポリシーです。優先度が等しい場合、古いエントリが到達可能であれば、IP テイクオーバーは拒否されます。IP テイクオーバーは、更新が信頼できるポートから発信され、新しいエントリが DHCP サーバから IP アドレスを取得した場合に発生します。そうでない場合には、明示的に許可する必要があります。古いエントリが新しいより信頼できるエントリに置き換えられた場合、IP 窃盗は報告されません。

次に、802.11 アソシエーションに連続 5 回失敗した場合にクライアントを無効にする例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless wps client-exclusion dot11-assoc
```

wireless wps mfp infrastructure

管理フレーム保護（MFP）を設定するには、**wirelesswpsmfpinfrastructure** コマンドを使用します。管理フレーム保護（MFP）を削除するには、このコマンドの no 形式を使用します。

wireless wps mfp infrastructure
no wireless wps mfp infrastructure

コマンド デフォルト

なし。

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、インフラストラクチャ MFP を有効にする例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless wps mfp infrastructure
```

wireless wps rogue

さまざまな不正パラメータを設定するには、**wirelesswpsrogue** コマンドを使用します。

wireless wps rogue {**adhoc**|**client**} [{**alert** *mac-addr*|**contain** *mac-addr no-of-aps*}]

構文の説明

adhoc	Independent Basic Service Set（IBSS またはアドホック）の不正なアクセス ポイントのステータスを設定します。
client	不正なクライアントを設定します。
alert *mac-addr*	アドホックの不正を検出すると SNMP トラップを生成し、システム管理者に即座にアラートを発信して、アドホックの不正アクセス ポイントの MAC アドレスに対し必要な措置を促します。
contain *mac-addr no-of-aps*	加害デバイスを阻止し、その信号が正規クライアントを阻害しないようにします。 アドホックの不正なアクセス ポイントをアクティブに阻止するために割り当てられた、シスコのアクセス ポイントの最大数（1 ～ 4）。

コマンド デフォルト

なし。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、システム管理者に即座にアラートを生成し、アドホックの不正アクセス ポイントの MAC アドレスに対し必要な措置を促す例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless wps rouge adhoc alert mac_addr
```

wireless wps shun-list re-sync

回避リストのコントローラをモビリティ グループ内の他のコントローラと同期させるには、**wirelesswpsshun-listre-sync** コマンドを使用します。

wireless wps shun-list re-sync

コマンド デフォルト

なし。

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

なし。

次に、回避リストのコントローラを他のコントローラと同期するように設定する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless wps shun-list re-sync
```

vlan access-map

VLAN パケット フィルタリング用の VLAN マップ エントリを作成または修正し、VLAN アクセス マップ コンフィギュレーション モードに変更するには、スイッチ スタックまたはスタンドアロン スイッチのグローバル コンフィギュレーション モードで **vlan access-map** コマンドを使用します。VLAN マップ エントリを削除するには、このコマンドの **no** 形式を使用します。

vlan access-map *name* [*number*]
no vlan access-map *name* [*number*]

（注） このコマンドは、LAN ベース フィーチャ セットを実行しているスイッチではサポートされません。

構文の説明

name	VLAN マップ名
number	（任意）作成または変更するマップエントリのシーケンス番号（0～65535）。VLAN マップを作成する際にシーケンス番号を指定しない場合、番号は自動的に割り当てられ、10 から開始して 10 ずつ増加します。この番号は、VLAN アクセス マップ エントリに挿入するか、または VLAN アクセス マップ エントリから削除する順番です。

コマンド デフォルト

VLAN に適用する VLAN マップ エントリまたは VLAN マップはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードでは、このコマンドは VLAN マップを作成または修正します。このエントリは、モードを VLAN アクセス マップ コンフィギュレーションに変更します。**match** アクセス マップ コンフィギュレーション コマンドを使用して、照合する IP または非 IP トラフィックのアクセス リストを指定できます。また、**action** コマンドを使用して、この照合によりパケットを転送またはドロップするかどうかを設定します。

VLAN アクセス マップ コンフィギュレーション モードでは、次のコマンドが利用できます。

- **action**：実行するアクションを設定します（転送またはドロップ）。
- **default**：コマンドをデフォルト値に設定します。
- **exit**：VLAN アクセス マップ コンフィギュレーション モードを終了します。
- **match**：照合する値を設定します（IP アドレスまたは MAC アドレス）。

- **no**コマンドを無効にするか、デフォルト値を設定します。

エントリ番号（シーケンス番号）を指定しない場合、マップの最後に追加されます。

VLAN ごとに VLAN マップは 1 つだけ設定できます。VLAN マップは、VLAN でパケットを受信すると適用されます。

シーケンス番号を指定して **no vlan access-map** *name* [*number*] コマンドを使用すると、エントリを個別に削除できます。

VLAN マップを 1 つまたは複数の VLAN に適用するには、**vlan filter** インターフェイス コンフィギュレーション コマンドを使用します。

VLANマップエントリの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

次の例では、vac1 という名の VLAN マップを作成し、一致条件とアクションをその VLAN マップに適用する方法を示します。他のエントリがマップに存在しない場合、これはエントリ 10 になります。

```
Switch(config)# vlan access-map vac1
Switch(config-access-map)# match ip address acl1
Switch(config-access-map)# action forward
```

次の例では、VLAN マップ vac1 を削除する方法を示します。

```
Switch(config)# no vlan access-map vac1
```

関連トピック

action （810 ページ）
match（アクセス マップ コンフィギュレーション） （865 ページ）
show vlan access-map （903 ページ）
vlan filter （939 ページ）

vlan filter

1 つ以上の VLAN に VLAN マップを適用するには、スイッチ スタックまたはスタンドアロン スイッチ上で、グローバル コンフィギュレーション モードで **vlan filter** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

vlan filter *mapname* **vlan-list** {リスト|**all**}
no vlan filter *mapname* **vlan-list** {リスト|**all**}

（注） このコマンドは、LAN ベース フィーチャ セットを実行しているスイッチではサポートされません。

構文の説明

mapname	VLAN マップ エントリ名
vlan-list	マップを適用する VLAN を指定します。
リスト	tt、uu-vv、xx、および yy-zz 形式での 1 つまたは複数の VLAN リスト。カンマとダッシュの前後のスペースは任意です。指定できる範囲は 1 ～ 4094 です。
all	マップをすべての VLAN に追加します。

コマンド デフォルト

VLAN フィルタはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

パケットを誤って過剰にドロップし、設定プロセスの途中で接続が無効になることがないように、VLAN アクセス マップを完全に定義してから VLAN に適用することを推奨します。

VLANマップエントリの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

次の例では、VLAN マップ エントリ map1 を VLAN 20 および 30 に適用します。

```
Switch(config)# vlan filter map1 vlan-list 20, 30
```

次の例では、VLAN マップ エントリ map1 を VLAN 20 から削除する方法を示します。

```
Switch(config)# no vlan filter map1 vlan-list 20
```

設定を確認するには、**show vlan filter** 特権 EXEC コマンドを入力します。

関連トピック

show vlan access-map （903 ページ）
show vlan filter （904 ページ）
vlan access-map （937 ページ）

vlan group

VLAN グループを作成または変更するには、グローバル コンフィギュレーション モードで**vlan group** コマンドを使用します。VLAN グループから VLAN リストを削除するには、このコマンドの **no** 形式を使用します。

vlan group *group-name* **vlan-list** *vlan-list*
no vlan group *group-name* **vlan-list** *vlan-list*

構文の説明

group-name	VLAN グループの名前。名前は最大 32 文字で、文字から始める必要があります。
vlan-list *vlan-list*	VLAN グループに追加される 1 つ以上の VLAN を指定します。*vlan-list* 引数には単一の VLAN ID、VLAN ID のリスト、または VLAN ID の範囲を指定できます。複数のエントリはハイフン（-）またはカンマ（,）で区切ります。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

指定された VLAN グループが存在しない場合、**vlan group** コマンドはグループを作成し、指定された VLAN リストをそのグループにマッピングします。指定された VLAN グループが存在する場合は、指定された VLAN リストがそのグループにマッピングされます。

vlan group コマンドの **no** 形式を使用すると、指定された VLAN リストが VLAN グループから削除されます。VLAN グループから最後の VLAN を削除すると、その VLAN グループは削除されます。

最大 100 の VLAN グループを設定でき、1 つの VLAN グループに最大 4094 の VLAN をマッピングできます。

次に、VLAN 7 ～ 9 と 11 を VLAN グループにマッピングする例を示します。

```
Switch(config)# vlan group group1 vlan-list 7-9,11
```

次の例では、VLAN グループから VLAN 7 を削除する方法を示します。

```
Switch(config)# no vlan group group1 vlan-list 7
```

関連トピック

show vlan group （905 ページ）

第 XI 部

スタック マネージャおよびハイ アベイラビリティ

スタック マネージャおよびハイ アベイラビリティ コマンド

- switch provision （1001 ページ）
- switch renumber （1003 ページ）

debug platform stack-manager

スタック マネージャ ソフトウェアのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform stack-manager** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug platform stack-manager {**level1**|**level2**|**level3**|**sdp**|**serviceability**|**sim**|**ssm**|**trace**} [{**switch** *switch-number*}]
no debug platform stack-manager {**level1**|**level2**|**level3**|**sdp**|**serviceability**|**sim**|**ssm**|**trace**} [{**switch** *switch-number*}]

構文の説明

level1	レベル 1 のデバッグ ログをイネーブルにします。
level2	レベル 2 のデバッグ ログをイネーブルにします。
level3	レベル 3 のデバッグ ログをイネーブルにします。
sdp	スタック ディスカバリ プロトコル（SDP）のデバッグ メッセージを表示します。
serviceability	スタック マネージャ サービスアビリティのデバッグ メッセージを表示します。
sim	スタック情報モジュールのデバッグ メッセージを表示します。
ssm	スタック ステートマシンのデバッグ メッセージを表示します。
trace	スタックマネージャの入口と出口のデバッグメッセージを追跡します。
switch *switch-number*	（任意）デバッグ オンをイネーブルにするスタック メンバー番号を指定します。指定できる範囲は 1 ～ 9 です。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、スタック対応スイッチのみでサポートされています。

undebug platform stack-manager コマンドは、**no debug platform stack-manager** コマンドと同じです。

main-cpu

冗長メイン コンフィギュレーション サブモードを開始し、スタンバイ スイッチを有効にするには、冗長コンフィギュレーション モードで **main-cpu** コマンドを使用します。

main-cpu

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

冗長コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

冗長メイン コンフィギュレーション サブモードから、**standby console enable** コマンドを使用してスタンバイ スイッチを有効にします。

次に、冗長メイン コンフィギュレーション サブモードを開始し、スタンバイ スイッチをイネーブルにする例を示します。

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)# standby console enable
Switch#
```

関連トピック

standby console enable （997 ページ）

mode sso

冗長モードをステートフル スイッチオーバー（SSO）に設定するには、冗長コンフィギュレーション モードで **mode sso** コマンドを使用します。

mode sso

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

冗長コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

mode sso コマンドは、冗長コンフィギュレーション モードでのみ入力できます。

システムを SSO モードに設定する場合は、次の注意事項に従ってください。

- SSO モードをサポートするために、スタック内のスイッチでは同一の Cisco IOS イメージを使用する必要があります。Cisco IOS リリース間の相違のために、冗長機能が動作しない場合があります。
- モジュールの活性挿抜（OIR）を実行する場合、モジュールの状態が移行状態（Ready 以外の状態）である場合にだけ、ステートフル スイッチオーバーの間にスイッチはリセットし、ポート ステートは再起動します。
- 転送情報ベース（FIB）テーブルはスイッチオーバー時に消去されます。ルーテッド トラフィックは、ルート テーブルが再コンバージェンスするまで中断されます。

次の例では、冗長モードを SSO に設定する方法を示します。

```
Switch(config)# redundancy
Switch(config-red)# mode sso
Switch(config-red)#
```

policy config-sync prc reload

Parser Return Code（PRC）の障害がコンフィギュレーションの同期中に発生した場合にスタンバイ スイッチをリロードするには、冗長コンフィギュレーション モードで **policy config-sync reload** コマンドを使用します。Parser Return Code（PRC）の障害が発生した場合にスタンバイ スイッチがリロードしないように指定するには、このコマンドの **no** 形式を使用します。

policy config-sync {bulk|lbl} prc reload
no policy config-sync {bulk|lbl} prc reload

構文の説明

bulk	バルク コンフィギュレーション モードを指定します。
lbl	1行ごと（lbl）のコンフィギュレーションモードを指定します。

コマンド デフォルト

このコマンドは、デフォルトではイネーブルです。

コマンド モード

冗長コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、Parser Return Code（PRC）の障害がコンフィギュレーションの同期化中に発生した場合に、スタンバイ スイッチがリロードされないように指定する例を示します。

```
Switch(config-red)# no policy config-sync bulk prc reload
```

redundancy

冗長コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **redundancy** コマンドを使用します。

redundancy

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

冗長コンフィギュレーション モードは、スタンバイ スイッチをイネーブルにするために使用されるメイン CPU サブモードを開始するために使用されます。

メイン CPU サブモードを開始するには、冗長コンフィギュレーション モードで **main-cpu** コマンドを使用します。

スタンバイ スイッチを有効にするには、メイン CPU サブモードから **standby console enable** コマンドを使用します。

冗長コンフィギュレーション モードを終了するには、**exit** コマンドを使用します。

次に、冗長コンフィギュレーション モードを開始する例を示します。

```
Switch(config)# redundancy
Switch(config-red)#
```

次の例では、メイン CPU サブモードを開始する方法を示します。

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)#
```

redundancy config-sync mismatched-commands

アクティブ スイッチとスタンバイ スイッチの間に設定の不一致があるときにスタンバイ スイッチのスタックへの参加を許可するには、特権 EXEC モードで **redundancy config-sync mismatched-commands** コマンドを使用します。

redundancy config-sync {ignore|validate} mismatched-commands

構文の説明

ignore	Mismatched Command List を無視します。
validate	修正した実行コンフィギュレーションに基づいて Mismatched Command List を再確認します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スタンバイ スイッチの起動中にアクティブ スイッチの実行コンフィギュレーションのコマンド構文チェックが失敗した場合、**redundancy config-sync mismatched-commands** コマンドを使用して、アクティブ スイッチの Mismatched Command List（MCL）を表示し、スタンバイ スイッチをリブートします。

次に、不一致コマンドのログ エントリの例を示します。

```
00:06:31: Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
 full list of mismatched commands via:
show redundancy config-sync failures mcl
00:06:31: Config Sync: Starting lines from MCL file:
interface GigabitEthernet7/7
! <submode> "interface"
- ip address 192.0.2.0 255.255.255.0
! </submode> "interface"
```

すべての不一致コマンドを表示するには、**show redundancy config-sync failures mcl** コマンドを使用します。

MCL を消去するには、次の手順を実行します。

1. アクティブ スイッチの実行コンフィギュレーションからすべての不一致コマンドを除外します。
2. **redundancy config-sync validate mismatched-commands** コマンドを使用して、修正した実行コンフィギュレーションに基づいて MCL を再確認します。
3. スタンバイ スイッチをリロードします。

次の手順に従って、MCL を無視することもできます。

1. **redundancy config-sync ignore mismatched-commands** コマンドを入力します。
2. スタンバイ スイッチをリロードします。システムは SSO モードに移行します。

（注） 不一致コマンドを無視する場合、アクティブ スイッチとスタンバイ スイッチの同期していないコンフィギュレーションは存在したままです。

3. 無視した MCL を **show redundancy config-sync ignored mcl** コマンドで確認します。

コンフィギュレーション ファイルの互換性の問題が原因で、アクティブ スイッチとスタンバイ スイッチ間で SSO モードを確立できない場合、Mismatched Command List（MCL）がアクティブ スイッチで生成され、スタンバイ スイッチに対して Route Processor Redundancy（RPR）モードへのリロードが強制されます。

（注） RPR モードはエラーの場合にフォール バックとして Catalyst 3850 スイッチでサポートされています。これは設定可能ではありません。

障害となっているコンフィギュレーションを削除し、スタンバイ スイッチを同じイメージで再起動した後に SSO の確立を試行する場合、ピア イメージが非互換としてリストされているため、C3K_REDUNDANCY-2-IOS_VERSION_CHECK_FAIL および ISSU-3-PEER_IMAGE_INCOMPATIBLE メッセージが表示されます。ピアが STANDBY COLD（RPR）状態のときに、**redundancy config-sync ignore mismatched-commands** EXEC コマンドで、非互換リストからピア イメージをクリアできます。このアクションによって、スタンバイ スイッチを、リロード時に STANDBY HOT（SSO）ステートで起動できます。

次の例に、変更したコンフィギュレーションとの Mismatched Command List を再検証する方法を示します。

```
Switch# redundancy config-sync validate mismatched-commands
Switch#
```

redundancy force-switchover

アクティブ スイッチとスタンバイ スイッチのスイッチオーバーを強制的に実行するには、スイッチ スタックの特権 EXEC モードで **redundancy force-switchover** コマンドを使用します。

redundancy force-switchover

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

手動で冗長スイッチに切り替えるには、**redundancy force-switchover** コマンドを使用します。冗長スイッチは Cisco IOS イメージを実行する新しいアクティブ スイッチになり、モジュールはデフォルト設定にリセットされます。

古いアクティブ スイッチは新しいイメージで再起動し、スタックに参加します。

アクティブ スイッチで **redundancy force-switchover** コマンドを使用すると、アクティブ スイッチのスイッチ ポートがダウン状態になります。

部分リング スタック内のスイッチにこのコマンドを使用すると、次の警告メッセージが表示されます。

```
Switch# redundancy force-switchover
Stack is in Half ring setup; Reloading a switch might cause stack split
This will reload the active unit and force switchover to standby[confirm]
```

次の例では、アクティブ スーパーバイザ エンジンからスタンバイ スーパーバイザ エンジンに手動で切り替える方法を示します。

```
Switch# redundancy force-switchover
Switch#
```

redundancy reload

スタック内のいずれか、またはすべてのスイッチを強制リロードするには、特権EXECモードで **redundancy reload** コマンドを使用します。

redundancy reload {**peer**|**shelf**}

構文の説明

peer	ピア ユニットをリロードします。
shelf	スタック内のすべてのスイッチが再起動します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、詳細情報について『*Stacking Configuration Guide (Catalyst 3850 Switches)*』の「Performing a Software Upgrade」の項を参照してください。

スタック内のすべてのスイッチをリブートするには、**redundancy reload shelf** コマンドを使用します。

次に、手動でスタック内のすべてのスイッチをリロードする例を示します。

```
Switch# redundancy reload shelf
Switch#
```

reload

スタック メンバをリロードし、設定変更を適用するには、特権 EXEC モードで **reload** コマンドを使用します。

reload [{**/noverify**|**/verify**}] [{*LINE*|**at**|**cancel**|**in**|**slot** *stack-member-number*|**standby-cpu**}]

構文の説明

/noverify	（任意）リロードの前にファイル シグニチャを確認しないように指定します。
/verify	（任意）リロードの前にファイル シグニチャを確認します。
LINE	（任意）リセットの理由。
at	（任意）リロードを実行する時間を hh:mm 形式で指定します。
cancel	（任意）保留中のリロードをキャンセルします。
in	（任意）リロードを実行する間隔を指定します。
slot	（任意）指定したスタック メンバーに変更を保存し、再起動します。
stack-member-number	（任意）変更を保存するスタック メンバ番号。指定できる範囲は 1 ～ 9 です。
standby-cpu	（任意）スタンバイ ルート プロセッサ（RP）をリロードします。

コマンド デフォルト

スタック メンバをただちにリロードし、設定の変更を有効にします。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スイッチ スタックに複数のスイッチがある場合に **reload slot** *stack-member-number* コマンドを入力すると、設定の保存を要求するプロンプトが表示されません。

例

次の例では、スイッチ スタックをリロードする方法を示します。

```
Switch# reload
System configuration has been modified. Save? [yes/no]: yes
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm] yes
```

次の例では、特定のスタック メンバをリロードする方法を示します。

```
Switch# reload slot 6
Proceed with reload? [confirm] y
```

次の例では、単一スイッチのスイッチ スタック（メンバ スイッチが 1 つだけ）をリロードする方法を示します。

```
Switch# reload slot 3
System configuration has been modified. Save? [yes/no]: y
Proceed to reload the whole Stack? [confirm] y
```

関連トピック

show switch （986 ページ）
switch priority （1000 ページ）
switch renumber （1003 ページ）

session

特定のスタック メンバの診断シェルまたはスタンバイ Switchの Cisco IOS プロンプトにアクセスするには、アクティブ Switch上の特権 EXEC モードで **session** コマンドを使用します。

session {**standby ios**|**switch** [{*stack-member-number*}]}

構文の説明

standby ios	スタンバイSwitchの Cisco IOS プロンプトにアクセスします。 （注） このコマンドを使用してスタンバイSwitchを設定することはできません。
switch	スタック メンバの診断シェルにアクセスします。
stack-member-number	（任意）アクティブ スイッチ からアクセスするスタック メンバの番号。範囲は 1 ～ 9 です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スタンバイSwitchで Cisco IOS プロンプトにアクセスした場合、システム プロンプトに `-stby` が付加されます。スタンバイSwitchを `Switch-stby>` プロンプトで設定することはできません。

スタック メンバの診断シェルにアクセスした場合、システム プロンプトに `(diag)` が付加されます。

例

次の例では、スタック メンバ 3 にアクセスする方法を示します。

```
Switch# session switch 3
Switch(diag)>
```

次の例では、スタンバイSwitchにアクセスする方法を示します。

```
Switch# session standby ios
Switch-stby>
```

関連トピック

reload （956 ページ）
show switch （986 ページ）
switch priority （1000 ページ）
switch renumber （1003 ページ）

set trace capwap ap ha

ワイヤレス アクセス ポイントの制御およびプロビジョニングのハイ アベイラビリティを追跡するには、**set trace capwap ap ha** 特権 EXEC コマンドを使用します。

set trace capwap ap ha [{**detail**|**event**|**dump** |{**filter** [{**none** [**switch** *switch*]|*filter_name* [*filter_value* [**switch** *switch*]]}]|**filtered***switch***level** {**default***trace_level*} [**switch** *switch*]}}]

構文の説明

detail	（任意）ワイヤレス CAPWAP HA の詳細を指定します。
event	（任意）ワイヤレス CAPWAP HA イベントを指定します。
dump	（任意）ワイヤレス CAPWAP HA の出力を指定します。
filter *mac*	MAC アドレスを指定します。
switch switch number	スイッチ番号を指定します。
none	（任意）フィルタ オプションを指定しません。
switch *switch*	（任意）スイッチ番号を指定します。
フィルタ名	適用されたフラグ フィルタ名を追跡します。
filter_value	（任意）フィルタの値。
switch *switch*	（任意）スイッチ番号を指定します。
filtered	フィルタ処理されたトレース メッセージを指定します。
switch	スイッチ番号を指定します。
level	トレース レベルを指定します。
default	解除されたトレース レベル値を指定します。
trace_level	トレース レベルを指定します。
switch *switch*	（任意）スイッチ番号を指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、ワイヤレス CAPWAP HA を表示する例を示します。

```
Switch# set trace capwap ap ha detail filter mac WORD switch number
```

set trace mobility ha

スイッチでワイヤレス モビリティ ハイ アベイラビリティをデバッグするには、**set trace mobility ha** 特権 EXEC コマンドを使用します。

set trace mobility ha [{**event**|**detail**|**dump**}] {**filter**[**mac** *WORD switch switch number*] [{**none** [**switch** *switch*]|*filter_name* [*filter_value* [**switch** *switch*]]}]|**level** {**default***trace_level*} [**switch** *switch*]{**filtered***switch*}}

構文の説明

event	（任意）ワイヤレス モビリティ ハイ アベイラビリティのイベントを指定します。
detail	（任意）ワイヤレス モビリティ ハイ アベイラビリティの詳細を指定します。
dump	（任意）ワイヤレス モビリティ ハイ アベイラビリティの出力を指定します。
filter	トレース適用フラグ フィルタを指定します。
mac	MACアドレスを指定します。
WORD switch	スイッチを指定します。
switch number	スイッチ番号を指定します。値の範囲は 1 ～ 4 です。
none	トレース適用フラグ フィルタを指定しません。
switch *switch*	（任意）スイッチ番号を指定します。
filter_name	適用されたフラグ フィルタ名を追跡します。
filter_value	適用されたフラグ フィルタの値を追跡します。
switch *switch*	スイッチ番号を指定します。
level	トレース レベル値を指定します。

default	解除されたトレース レベル値を指定します。
trace_level	トレース レベル値を指定します。
switch *switch*	スイッチ番号を指定します。
filtered	フィルタ処理されたトレース メッセージを指定します。
switch	スイッチを指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、ワイヤレス モビリティ ハイ アベイラビリティの詳細を表示する例を示します。

```
Switch# set trace mobility ha detail filter mac WORD
[08/27/13 10:38:35.349 UTC 1 8135] Invalid src ip: 169.254.1.1
[08/27/13 10:38:35.349 UTC 2 8135] Invalid sysIp: Skip plumbing MC-MA
tunnels.
[08/27/13 10:38:54.393 UTC 3 8135] Mobility version mismatch, v10
received, or m
sglen mismatch msglen=74 recvBytes=0, dropping
```

set trace qos ap ha

ワイヤレス サービス品質（QoS）ハイ アベイラビリティをトレースするには、**set trace qos ap ha** 特権 EXEC コマンドを使用します。

set trace QOS ap ha [{**event**|**error**}] {**filter** [{**MACnone** [**switch** *switch*]|*filter_name* [*filter_value* [**switch** *switch*]]}]|**level** {**default***trace_level*} [**switch** *switch*]}

構文の説明

event	（任意）トレース QoS ワイヤレス AP イベントを指定します。
event *mac*	AP の MAC アドレスを指定します。
event *none*	MAC アドレス値を指定しません。
error	（任意）トレース QoS ワイヤレス AP エラーを指定します。
error *mac*	AP の MAC アドレスを指定します。
error *none*	値を指定しません。
filter	トレース適用フラグ フィルタを指定します。
filter *mac*	AP の MAC アドレスを指定します。
filter *none*	値を指定しません。
switch *switch*	スイッチ番号を指定します。
filter_name	（任意）スイッチ フィルタの名前を指定します。
filter_value	（任意）スイッチ フィルタの値を指定します。値は 1 です。
switch *switch*	（任意）スイッチ番号を指定します。値は 1 です。
level	トレース レベルを指定します。
default	トレース QoS ワイヤレス AP デフォルトを指定します。
trace_level	トレース レベルです。
switch *switch*	（任意）スイッチ番号を指定します。値は 1 です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、ワイヤレス QoS ハイ アベイラビリティを追跡する例を示します。

```
Switch# set trace QOS ap ha
```

show checkpoint

チェックポイント ファシリティ（CF）のサブシステムに関する情報を表示するには、**show checkpoint** コマンドを使用します。

show checkpoint clients entities statistics

構文の説明

clients	チェックポイントクライアントに関する詳細情報を表示します。
entities	チェックポイントエンティティに関する詳細情報を表示します。
statistics	チェックポイント統計情報に関する詳細情報を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、すべての CF クライアントを表示する例を示します。

```
   Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_MOBILITY
    Client ID                   : 24105
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 6
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_DOT1X
    Client ID                   : 24106
    Total DB inserts            : 2
    Total DB updates            : 1312
    Total DB deletes            : 2
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_APFROGUE
    Client ID                   : 24107
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
--------------------------------------------------------------------------------
Checkpoint client: WCM_CIDS
```

```
    Client ID                   : 24110
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 0
    Client residing in process  : 8135
------------------------------------------------------------------------------
Checkpoint client: WCM_NETFLOW
    Client ID                   : 24111
    Total DB inserts            : 7
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
------------------------------------------------------------------------------
Checkpoint client: WCM_MCAST
    Client ID                   : 24112
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
------------------------------------------------------------------------------
Checkpoint client: wcm_comet
    Client ID                   : 24150
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 0
    Client residing in process  : 8135
------------------------------------------------------------------------------

All iosd checkpoint clients

------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
Network RF Client           3         --       Off

  Total API Messages Sent:                      0
  Total Transport Messages Sent:                0
  Length of Sent Messages:                      0
  Total Blocked Messages Sent:                  0
  Length of Sent Blocked Messages:              0
  Total Non-blocked Messages Sent:              0
  Length of Sent Non-blocked Messages:          0
  Total Bytes Allocated:                        0
  Buffers Held:                                 0
  Buffers Held Peak:                            0
  Huge Buffers Requested:                       0
  Transport Frag Count:                         0
  Transport Frag Peak:                          0
  Transport Sends w/Flow Off:                   0
  Send Errs:                                    0
  Send Peer Errs:                               0
  Rcv Xform Errs:                               0
  Xmit Xform Errs:                              0
  Incompatible Messages:                        0
  Client Unbundles to Process Memory:           T
```

```
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
SNMP CF Client             12         --       Off

  Total API Messages Sent:                      0
  Total Transport Messages Sent:                0
  Length of Sent Messages:                      0
  Total Blocked Messages Sent:                  0
  Length of Sent Blocked Messages:              0
  Total Non-blocked Messages Sent:              0
  Length of Sent Non-blocked Messages:          0
  Total Bytes Allocated:                        0
  Buffers Held:                                 0
  Buffers Held Peak:                            0
  Huge Buffers Requested:                       0
  Transport Frag Count:                         0
  Transport Frag Peak:                          0
  Transport Sends w/Flow Off:                   0
  Send Errs:                                    0
  Send Peer Errs:                               0
  Rcv Xform Errs:                               0
  Xmit Xform Errs:                              0
  Incompatible Messages:                        0
  Client Unbundles to Process Memory:           T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
Online Diags HA            14         --       Off

  Total API Messages Sent:                      0
  Total Transport Messages Sent:                0
  Length of Sent Messages:                      0
  Total Blocked Messages Sent:                  0
  Length of Sent Blocked Messages:              0
  Total Non-blocked Messages Sent:              0
  Length of Sent Non-blocked Messages:          0
  Total Bytes Allocated:                        0
  Buffers Held:                                 0
  Buffers Held Peak:                            0
  Huge Buffers Requested:                       0
  Transport Frag Count:                         0
  Transport Frag Peak:                          0
  Transport Sends w/Flow Off:                   0
  Send Errs:                                    0
  Send Peer Errs:                               0
  Rcv Xform Errs:                               0
  Xmit Xform Errs:                              0
  Incompatible Messages:                        0
  Client Unbundles to Process Memory:           T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
ARP                        22         --       Off

  Total API Messages Sent:                      0
  Total Transport Messages Sent:                0
  Length of Sent Messages:                      0
  Total Blocked Messages Sent:                  0
  Length of Sent Blocked Messages:              0
  Total Non-blocked Messages Sent:              0
```

```
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
Tableid CF                 27         --       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                 0
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
Event Manager              33          0       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                --
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
```

```
  Incompatible Messages:                          0
  Client Unbundles to Process Memory:             T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
LAN-Switch Port Mana       35          0       Off

  Total API Messages Sent:                        0
  Total Transport Messages Sent:                 --
  Length of Sent Messages:                        0
  Total Blocked Messages Sent:                    0
  Length of Sent Blocked Messages:                0
  Total Non-blocked Messages Sent:                0
  Length of Sent Non-blocked Messages:            0
  Total Bytes Allocated:                          0
  Buffers Held:                                   0
  Buffers Held Peak:                              0
  Huge Buffers Requested:                         0
  Transport Frag Count:                           0
  Transport Frag Peak:                            0
  Transport Sends w/Flow Off:                     0
  Send Errs:                                      0
  Send Peer Errs:                                 0
  Rcv Xform Errs:                                 0
  Xmit Xform Errs:                                0
  Incompatible Messages:                          0
  Client Unbundles to Process Memory:             T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
LAN-Switch PAgP/LACP       36          0       Off

  Total API Messages Sent:                        0
  Total Transport Messages Sent:                 --
  Length of Sent Messages:                        0
  Total Blocked Messages Sent:                    0
  Length of Sent Blocked Messages:                0
  Total Non-blocked Messages Sent:                0
  Length of Sent Non-blocked Messages:            0
  Total Bytes Allocated:                          0
  Buffers Held:                                   0
  Buffers Held Peak:                              0
  Huge Buffers Requested:                         0
  Transport Frag Count:                           0
  Transport Frag Peak:                            0
  Transport Sends w/Flow Off:                     0
  Send Errs:                                      0
  Send Peer Errs:                                 0
  Rcv Xform Errs:                                 0
  Xmit Xform Errs:                                0
  Incompatible Messages:                          0
  Client Unbundles to Process Memory:             T
------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
------------------------------------------------------------------------------
LAN-Switch VLANs           39          0       Off

  Total API Messages Sent:                        0
  Total Transport Messages Sent:                 --
  Length of Sent Messages:                        0
  Total Blocked Messages Sent:                    0
```

```
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
```

次に、すべての CF エンティティを表示する例を示します。

```
KATANA_DOC#show checkpoint entities
                        Check Point List of Entities

 CHKPT on ACTIVE server.

------------------------------------------------------------------------------
Entity ID         Entity Name
------------------------------------------------------------------------------
        0         CHKPT_DEFAULT_ENTITY

  Total API Messages Sent:             0
  Total Messages Sent:                 0
  Total Sent Message Len:              0
  Total Bytes Allocated:               0
  Total Number of Members:            10

  Member(s) of entity 0 are:
    Client ID          Client Name
-----------------------------------------
          168          DHCP Snooping
          167          IGMP Snooping
           41          Spanning-tree
           40          AUTH MGR CHKPT CLIEN
           39          LAN-Switch VLANs
           33          Event Manager
           35          LAN-Switch Port Mana
           36          LAN-Switch PAgP/LACP
          158          Inline Power Checkpoint
```

次に、CF の統計情報を表示する例を示します。

```
KATANA_DOC#show checkpoint statistics
        IOSd Check Point Status
 CHKPT on ACTIVE server.

Number Of Msgs In Hold Q:              0
CHKPT MAX Message Size:                0
TP MAX Message Size:               65503
CHKPT Pending Msg Timer:             100 ms

  FLOW_ON  total:                      0
  FLOW_OFF total:                      0
  Current FLOW status is:             ON
  Total API Messages Sent:             0
  Total Messages Sent:                 0
  Total Sent Message Len:              0
  Total Bytes Allocated:               0
```

```
Rcv  Msg Q Peak:                    0
Hold Msg Q Peak:                    0
Buffers Held Peak:                  0
Current Buffers Held:               0
Huge Buffers Requested:             0
```

show etherchannel summary

コントローラのポート、ポート チャネルおよびプロトコルの詳細を表示するには、**show etherchannel summary** コマンドを使用します。

show ethernet summary

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

特権モード。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、コントローラのポート、ポート チャネルおよびプロトコルの詳細を表示する例を示します。

```
controller#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SD)          -
23     Po23(SD)         -
```

show platform ses

プラットフォーム情報（コントローラのスタック イベント シーケンサ）を表示するには、特権 EXEC モードで **show platform ses** を使用します。

show platform ses clients states

構文の説明

clients	SES クライアント リストを表示します。
states	SES カードの状態を表示します。

コマンド デフォルト

なし。

コマンド モード

特権 EXEC モード。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

SES クライアントおよび状態の詳細を表示するには、特権 EXEC モードでこのコマンドを使用します。

次に、スタック イベント シーケンサの状態を表示する例を示します。

```
Card #  Card State
======  ==========
1       NG3K_SES_CARD_ADD_COMPLETED(51)
2       NG3K_SES_CARD_EMPTY(0)
3       NG3K_SES_CARD_EMPTY(0)
4       NG3K_SES_CARD_EMPTY(0)
5       NG3K_SES_CARD_EMPTY(0)
6       NG3K_SES_CARD_EMPTY(0)
7       NG3K_SES_CARD_EMPTY(0)
8       NG3K_SES_CARD_EMPTY(0)
9       NG3K_SES_CARD_EMPTY(0)
```

次に、スタック イベント シーケンサのすべての関連クライアントを表示する例を示します。

```
clientID  = 5
clientSeq = 5
clientName = "MATM"
clientCallback @ 0xF49F7300
next = 0x909194B4

clientID  = 6
clientSeq = 6
clientName = "L2 CONTROL"
clientCallback @ 0xF49CA3F0
next = 0x915E4E80

clientID  = 7
clientSeq = 7
```

```
clientName = "CDP"
clientCallback @ 0xF49C7220
next = 0x915E4F08

clientID  = 8
clientSeq = 8
clientName = "UDLD"
clientCallback @ 0xF49C75D0
next = 0x91854CA0

clientID  = 9
clientSeq = 9
clientName = "LLDP"
clientCallback @ 0xF49E62F0
next = 0x90919F90

clientID  = 10
clientSeq = 10
clientName = "L2M"
clientCallback @ 0xF49CE4D0
next = 0x90E35A5C

clientID  = 11
clientSeq = 11
clientName = "Storm-Control"
clientCallback @ 0xF4BA8080
next = 0x9089E9B4

clientID  = 12
clientSeq = 12
clientName = "Security Utils"
clientCallback @ 0xF466BFB0
next = 0x91855F14

clientID  = 13
clientSeq = 13
clientName = "BACKUP-INT"
clientCallback @ 0xF4A191B0
next = 0x91D3511C

clientID  = 14
clientSeq = 14
clientName = "SPAN"
clientCallback @ 0xF4A34F30
next = 0x90FFC8C8

clientID  = 15
clientSeq = 15
clientName = "NG3K_SES_CLIENT_SECURITY_CTRL"
clientCallback @ 0xF4CD1D80
next = 0x95AE5834

clientID  = 16
clientSeq = 16
clientName = "NG3K_SES_CLIENT_DAI"
clientCallback @ 0xF4CD0C50
next = 0x95AE4854

clientID  = 17
clientSeq = 17
clientName = "NG3K_SES_CLIENT_DHCPSN"
clientCallback @ 0xF4CA9D30
next = 0x91DF7728
```

```
clientID  = 18
clientSeq = 18
clientName = "NG3K_SES_CLIENT_IPSG"
clientCallback @ 0xF4CDED70
next = 0x9131DCD8

clientID  = 20
clientSeq = 20
clientName = "DTLS"
clientCallback @ 0xF49B2CB0
next = 0x9134508C

clientID  = 21
clientSeq = 21
clientName = "STATS"
clientCallback @ 0xF49BD750
next = 0x9134746C

clientID  = 22
clientSeq = 22
clientName = "PLATFORM_MGR"
clientCallback @ 0xF4AB2D40
next = 0x91323D20

clientID  = 23
clientSeq = 23
clientName = "LEARNING"
clientCallback @ 0xF49F93C0
next = 0x9091D52C

clientID  = 24
clientSeq = 24
clientName = "PLATFORM-SPI"
clientCallback @ 0xF4AAD6F0
next = 0x91F2AE14

clientID  = 25
clientSeq = 25
clientName = "EEM"
clientCallback @ 0xF5393370
next = 0x913474F4

clientID  = 26
clientSeq = 26
clientName = "NG3K_WIRELESS"
clientCallback @ 0xF4B130B0
next = 0x9131D144

clientID  = 27
clientSeq = 27
clientName = "NG3K Environment Variables"
clientCallback @ 0xF4C6DA80
next = 0x00000000

KATANA_DOC#
KATANA_DOC#
KATANA_DOC#show platform ses clients
Client list @ 0x915B312C

clientID  = 0
clientSeq = 0
clientName = "TM Shim"
clientCallback @ 0xF4C79A90
next = 0x91182F24
```

```
clientID  = 1
clientSeq = 1
clientName = "EM-HA"
clientCallback @ 0xF52CA730
next = 0x913245B8

clientID  = 2
clientSeq = 2
clientName = "IFM"
clientCallback @ 0xF4A3EB20
next = 0x934B80E4

clientID  = 3
clientSeq = 3
clientName = "PORT-MGR"
clientCallback @ 0xF49FD0A0
next = 0x91D36D08

clientID  = 4
clientSeq = 4
clientName = "IDBMAN"
clientCallback @ 0xF4AF6040
next = 0x92121224

clientID  = 5
clientSeq = 5
clientName = "MATM"
clientCallback @ 0xF49F7300
next = 0x909194B4

clientID  = 6
clientSeq = 6
clientName = "L2 CONTROL"
clientCallback @ 0xF49CA3F0
next = 0x915E4E80

clientID  = 7
clientSeq = 7
clientName = "CDP"
clientCallback @ 0xF49C7220
next = 0x915E4F08

clientID  = 8
clientSeq = 8
clientName = "UDLD"
clientCallback @ 0xF49C75D0
next = 0x91854CA0

clientID  = 9
clientSeq = 9
clientName = "LLDP"
clientCallback @ 0xF49E62F0
next = 0x90919F90

clientID  = 10
clientSeq = 10
clientName = "L2M"
clientCallback @ 0xF49CE4D0
next = 0x90E35A5C

clientID  = 11
clientSeq = 11
clientName = "Storm-Control"
```

```
clientCallback @ 0xF4BA8080
next = 0x9089E9B4

clientID  = 12
clientSeq = 12
clientName = "Security Utils"
clientCallback @ 0xF466BFB0
next = 0x91855F14

clientID  = 13
clientSeq = 13
clientName = "BACKUP-INT"
clientCallback @ 0xF4A191B0
next = 0x91D3511C

clientID  = 14
clientSeq = 14
clientName = "SPAN"
clientCallback @ 0xF4A34F30
next = 0x90FFC8C8

clientID  = 15
clientSeq = 15
clientName = "NG3K_SES_CLIENT_SECURITY_CTRL"
clientCallback @ 0xF4CD1D80
next = 0x95AE5834

clientID  = 16
clientSeq = 16
clientName = "NG3K_SES_CLIENT_DAI"
clientCallback @ 0xF4CD0C50
next = 0x95AE4854

clientID  = 17
clientSeq = 17
clientName = "NG3K_SES_CLIENT_DHCPSN"
clientCallback @ 0xF4CA9D30
next = 0x91DF7728

clientID  = 18
clientSeq = 18
clientName = "NG3K_SES_CLIENT_IPSG"
clientCallback @ 0xF4CDED70
next = 0x9131DCD8

clientID  = 20
clientSeq = 20
clientName = "DTLS"
clientCallback @ 0xF49B2CB0
next = 0x9134508C

clientID  = 21
clientSeq = 21
clientName = "STATS"
clientCallback @ 0xF49BD750
next = 0x9134746C

clientID  = 22
clientSeq = 22
clientName = "PLATFORM_MGR"
clientCallback @ 0xF4AB2D40
next = 0x91323D20

clientID  = 23
```

```
clientSeq = 23
clientName = "LEARNING"
clientCallback @ 0xF49F93C0
next = 0x9091D52C

clientID  = 24
clientSeq = 24
clientName = "PLATFORM-SPI"
clientCallback @ 0xF4AAD6F0
next = 0x91F2AE14

clientID  = 25
clientSeq = 25
clientName = "EEM"
clientCallback @ 0xF5393370
next = 0x913474F4

clientID  = 26
clientSeq = 26
clientName = "NG3K_WIRELESS"
clientCallback @ 0xF4B130B0
next = 0x9131D144

clientID  = 27
clientSeq = 27
clientName = "NG3K Environment Variables"
clientCallback @ 0xF4C6DA80
next = 0x00000000
```

show platform stack-manager

プラットフォーム依存スイッチ スタック情報を表示するには、特権 EXEC モードで **show platform stack-manager** コマンドを使用します。

show platform stack-manager {**oir-states**|**sdp-counters**|**sif-counters**} **switch** *stack-member-number*

構文の説明

oir-states	活性挿抜（OIR）状態の情報を表示します。
sdp-counters	スタック ディスカバリ プロトコル（SDP）カウンタ情報を表示します。
sif-counters	スタック情報（SIF）カウンタ情報を表示します。
switch *stack-member-number*	スタック マネージャ情報を表示するスタック メンバを指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スイッチ スタックのデータと統計を収集するには、**show platform stack-manager** コマンドを使用します。

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show redundancy

冗長ファシリティ情報を表示するには、特権 EXEC モードで **show redundancy** コマンドを使用します。

show redundancy [{**clients**|**config-sync**|**counters**|**history** [{**reload**|**reverse**}]|**slaves**[*slave-name*] {**clients**|**counters**}|**states**|**switchover history** [**domain default**]}]

構文の説明

clients	（任意）冗長ファシリティ クライアントに関する情報を表示します。
config-sync	（任意）コンフィギュレーション同期の失敗または無視された Mismatched Command List（MCL）を表示します。詳細については、show redundancy config-sync （984 ページ）を参照してください。
counters	（任意）冗長ファシリティ カウンタに関する情報を表示します。
history	（任意）冗長ファシリティの過去のステータスのログおよび関連情報を表示します。
history reload	（任意）冗長ファシリティの過去のリロード情報を表示します。
history reverse	（任意）冗長ファシリティの過去のステータスおよび関連情報のログを逆順で表示します。
slaves	（任意）冗長ファシリティのすべてのスレーブを表示します。
slave-name	（任意）特定の情報を表示する冗長ファシリティ スレーブの名前。指定スレーブのすべてのクライアントまたはカウンタを表示するには、追加でキーワードを入力します。
clients	指定スレーブのすべての冗長ファシリティ クライアントを表示します。
counters	指定スレーブのすべてのカウンタを表示します。
states	（任意）冗長ファシリティの状態（ディセーブル、初期化、スタンバイ、アクティブなど）に関する情報を表示します。
switchover history	（任意）冗長ファシリティのスイッチオーバー履歴に関する情報を表示します。
domain default	（任意）スイッチオーバー履歴を表示するドメインとしてデフォルト ドメインを表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、冗長ファシリティに関する情報を表示する方法を示します。

```
Switch# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 6 days, 9 hours, 23 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = not known

                 Hardware Mode = Simplex
    Configured Redundancy Mode = SSO
     Operating Redundancy Mode = SSO
              Maintenance Mode = Disabled
                Communications = Down      Reason: Simplex mode

Current Processor Information :
------------------------------
               Active Location = slot 1
        Current Software state = ACTIVE
       Uptime in current state = 6 days, 9 hours, 23 minutes
                 Image Version = Cisco IOS Software, IOS-XE Software, Catalyst 3
850 L3 Switch Software (CAT3850-UNIVERSALK9-M), Version 03.08.59.EMD EARLY DEPLO
YMENT ENGINEERING NOVA_WEEKLY BUILD, synced to DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_11
05
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 16-S
        Configuration register = 0x102

Peer (slot: 0) information is not available because it is in 'DISABLED' state
Switch#
```

次の例では、冗長ファシリティ クライアント情報を表示する方法を示します。

```
Switch# show redundancy clients
Group ID =     1
     clientID = 20002    clientSeq =     4    EICORE HA Client
     clientID = 24100    clientSeq =     5    WCM_CAPWAP
     clientID = 24101    clientSeq =     6    WCM RRM HA
     clientID = 24103    clientSeq =     8    WCM QOS HA
     clientID = 24105    clientSeq =    10    WCM_MOBILITY
     clientID = 24106    clientSeq =    11    WCM_DOT1X
     clientID = 24107    clientSeq =    12    WCM_APFROGUE
     clientID = 24110    clientSeq =    15    WCM_CIDS
     clientID = 24111    clientSeq =    16    WCM_NETFLOW
     clientID = 24112    clientSeq =    17    WCM_MCAST
     clientID = 24120    clientSeq =    18    wcm_comet
     clientID = 24001    clientSeq =    21    Table Manager Client
     clientID = 20010    clientSeq =    24    SNMP SA HA Client
     clientID = 20007    clientSeq =    27    Installer HA Client
     clientID =    29    clientSeq =    60    Redundancy Mode RF
     clientID =   139    clientSeq =    61    IfIndex
     clientID =  3300    clientSeq =    62    Persistent Variable
     clientID =    25    clientSeq =    68    CHKPT RF
     clientID = 20005    clientSeq =    74    IIF-shim
     clientID = 10001    clientSeq =    82    QEMU Platform RF
```

```
<output truncated>
```

出力には、次の情報が表示されます。

- clientID には、クライアントの ID 番号が表示されます。
- clientSeq には、クライアントの通知シーケンス番号が表示されます。
- 現在の冗長ファシリティ ステート。

次の例では、冗長ファシリティ カウンタ情報を表示する方法を示します。

```
Switch# show redundancy counters
Redundancy Facility OMs

               comm link up = 0
             comm link down = 0
          invalid client tx = 0
          null tx by client = 0
                tx failures = 0
      tx msg length invalid = 0

      client not rxing msgs = 0
 rx peer msg routing errors = 0
           null peer msg rx = 0
         errored peer msg rx = 0

                 buffers tx = 0
     tx buffers unavailable = 0
                 buffers rx = 0
      buffer release errors = 0

 duplicate client registers = 0
  failed to register client = 0
       Invalid client syncs = 0

Switch#
```

次の例では、冗長ファシリティ履歴情報を表示する方法を示します。

```
Switch# show redundancy history
00:00:00 *my state = INITIALIZATION(2) peer state = DISABLED(1)
00:00:00 RF_EVENT_INITIALIZATION(524) op=0 rc=0
00:00:00 *my state = NEGOTIATION(3) peer state = DISABLED(1)
00:00:01 client added: Table Manager Client(24001) seq=21
00:00:01 client added: SNMP SA HA Client(20010) seq=24
00:00:06 client added: WCM_CAPWAP(24100) seq=5
00:00:06 client added: WCM QOS HA(24103) seq=8
00:00:07 client added: WCM_DOT1X(24106) seq=11
00:00:07 client added: EICORE HA Client(20002) seq=4
00:00:09 client added: WCM_MOBILITY(24105) seq=10
00:00:09 client added: WCM_NETFLOW(24111) seq=16
00:00:09 client added: WCM_APFROGUE(24107) seq=12
00:00:09 client added: WCM RRM HA(24101) seq=6
00:00:09 client added: WCM_MCAST(24112) seq=17
00:00:09 client added: WCM_CIDS(24110) seq=15
00:00:09 client added: wcm_comet(24120) seq=18
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) First Slave(0) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6107) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6109) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6128) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8897) op=0 rc=0
```

```
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8898) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8901) op=0 rc=0
00:00:22 RF_EVENT_SLAVE_STATUS_DONE(523) First Slave(0) op=405 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Redundancy Mode RF(29) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) IfIndex(139) op=0 rc=0

<output truncated>
```

次の例では、冗長ファシリティ スレーブに関する情報を表示する方法を示します。

```
Switch# show redundancy slaves
Group ID =   1
Slave/Process ID =  6107   Slave Name = [installer]
Slave/Process ID =  6109   Slave Name = [eicored]
Slave/Process ID =  6128   Slave Name = [snmp_subagent]
Slave/Process ID =  8897   Slave Name = [wcm]
Slave/Process ID =  8898   Slave Name = [table_mgr]
Slave/Process ID =  8901   Slave Name = [iosd]

Switch#
```

次の例では、冗長ファシリティ ステートに関する情報を表示する方法を示します。

```
Switch# show redundancy states
         my state = 13 -ACTIVE
       peer state =  1 -DISABLED
            Mode = Simplex
         Unit ID = 1

  Redundancy Mode (Operational) = SSO
   Redundancy Mode (Configured) = SSO
               Redundancy State = Non Redundant
                      Manual Swact = disabled (system is simplex (no peer unit))

   Communications = Down      Reason: Simplex mode

     client count = 75
   client_notification_TMR = 360000 milliseconds
            keep_alive TMR = 9000 milliseconds
          keep_alive count = 0
      keep_alive threshold = 18
             RF debug mask = 0

Switch#
```

show redundancy config-sync

コンフィギュレーション同期障害情報または無視されたMismatched Command List（MCL）（存在する場合）を表示するには、EXEC モードで **show redundancy config-sync** コマンドを使用します。

show redundancy config-sync {failures {bem|mcl|prc}|ignored failures mcl}

構文の説明

failures	MCL エントリまたはベスト エフォート方式（BEM）/パーサー リターン コード（PRC）の障害を表示します。
bem	BEM 障害コマンド リストを表示し、スタンバイ スイッチを強制的にリブートします。
mcl	スイッチの実行コンフィギュレーションに存在するがスタンバイ スイッチのイメージでサポートされていないコマンドを表示し、スタンバイ スイッチを強制的にリブートします。
prc	PRC 障害コマンド リストを表示し、スタンバイ スイッチを強制的にリブートします。
ignored failures mcl	無視された MCL 障害を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

2 つのバージョンの Cisco IOS イメージが含まれている場合は、それぞれのイメージによってサポートされるコマンドセットが異なる可能性があります。このような不一致コマンドのいずれかがアクティブ スイッチで実行された場合、スタンバイ スイッチでそのコマンドを認識できない可能性があり、これにより設定の不一致状態が発生します。バルク同期中にスタンバイ スイッチでコマンドの構文チェックが失敗すると、コマンドはMCL に移動し、スタンバイ スイッチはリセットされます。すべての不一致コマンドを表示するには、**show redundancy config-sync failures mcl** コマンドを使用します。

MCL を消去するには、次の手順を実行します。

1. アクティブ スイッチの実行コンフィギュレーションから、不一致コマンドをすべて削除します。

2. **redundancy config-sync validate mismatched-commands** コマンドを使用して、修正した実行コンフィギュレーションに基づいて MCL を再確認します。
3. スタンバイ スイッチをリロードします。

または、次の手順を実行して MCL を無視することもできます。

1. **redundancy config-sync ignore mismatched-commands** コマンドを入力します。
2. スタンバイ スイッチをリロードします。システムは SSO モードに遷移します。

（注） 不一致コマンドを無視する場合、アクティブ スイッチとスタンバイ スイッチの同期していないコンフィギュレーションは存在したままです。

3. 無視した MCL は **show redundancy config-sync ignored mcl** コマンドで確認できます。

各コマンドでは、そのコマンドを実装するアクション機能において戻りコードが設定されます。この戻りコードは、コマンドが正常に実行されたかどうかを示します。アクティブ スイッチは、コマンドの実行後に PRC を維持します。スタンバイ スイッチはコマンドを実行し、アクティブ スイッチに PRC を返します。これら 2 つの PRC が一致しないと、PRC 障害が発生します。バルク同期または 1 行ごとの（LBL）同期中にスタンバイ スイッチで PRC エラーが生じた場合、スタンバイ スイッチはリセットされます。すべての PRC 障害を表示するには、**show redundancy config-sync failures prc** コマンドを使用します。

ベスト エフォート方式（BEM）エラーを表示するには、**show redundancy config-sync failures bem** コマンドを使用します。

次に、BEM 障害を表示する例を示します。

```
Switch> show redundancy config-sync failures bem
BEM Failed Command List
-----------------------

 The list is Empty
```

次に、MCL 障害を表示する例を示します。

```
Switch> show redundancy config-sync failures mcl
Mismatched Command List
-----------------------

The list is Empty
```

次に、PRC 障害を表示する例を示します。

```
Switch# show redundancy config-sync failures prc
PRC Failed Command List
-----------------------

 The list is Empty
```

show switch

スタック メンバまたはスイッチ スタックに関連した情報を表示するには、**show switch** コマンドを EXEC モードで使用します。

show switch [{*stack-member-number*|**detail**|**neighbors**|**stack-ports** [{**summary**}]}]

構文の説明

stack-member-number	（任意）スタック メンバ数。指定できる範囲は 1 ～ 9 です。
detail	（任意）スタック リングの詳細情報を表示します。
neighbors	（任意）スイッチ スタック全体のネイバーを表示します。
stack-ports	（任意）スイッチ スタック全体のポート情報を表示します。
summary	（任意）スタック ケーブルの長さ、スタック リンクのステータス、およびループバックのステータスを表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドでは、次のステートが表示されます。

- Initializing：スイッチはスタックに追加されたばかりで、ready 状態になるための基本的な初期化が完了していません。
- HA Sync in Progress：スタンバイが選出されると、同期が終了するまで対応するスイッチはこの状態のままになります。
- Syncing：既存のスタックに追加されたスイッチは、スイッチ追加シーケンスが完了するまでこの状態のままになります。
- Ready：メンバがシステム レベルおよびインターフェイス レベルの設定のロードを完了し、トラフィックを転送できるようになっています。

- V-Mismatch：Version-Mismatch モードのスイッチ。Version-Mismatch モードは、スタックに参加したスイッチのソフトウェア バージョンがアクティブ スイッチと非互換である場合です。
- Provisioned：スイッチ スタックのアクティブ メンバになる前にすでに設定されていたスイッチの状態です。プロビジョニングされたスイッチでは、MAC アドレスおよびプライオリティ番号は、常に 0 と表示されます。
- Unprovisioned：プロビジョニングされたスイッチ番号が **no switch** *switch-number* **provision** コマンドを使用してプロビジョニング解除された場合の状態です。
- Removed：スタックに存在していたスイッチが、**reload slot** コマンドを使用して除外された場合です。
- Sync not started：複数のスイッチが既存のスタックに同時に追加された場合、アクティブ スイッチが 1 台ずつ追加します。追加中のスイッチは Syncing 状態になります。まだ追加されていないスイッチは Sync not started 状態になります。
- Lic-Mismatch：スイッチのライセンス レベルがアクティブ スイッチと異なります。

スタック メンバ（アクティブ スイッチを含む）の代表的なステート遷移は、Waiting>Initializing > Ready です。

Version Mismatch（VM）モードのスタック メンバの代表的なステート遷移は、Waiting > Ver Mismatch です。

スイッチ スタックにプロビジョニングされたスイッチが存在するかどうかを識別するには、**show switch** コマンドを使用できます。**show running-config** および **show startup-config** 特権 EXEC コマンドでは、この情報は提供されません。

永続的 MAC アドレスがイネーブルになっている場合、スタックの MAC-persistency wait-time も表示されます。

例

次に、スタック情報の概要を表示する例を示します。

```
Switch# show switch
Switch/Stack Mac Address : 6400.f124.e900
                                            H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-----------------------------------------------------------
 1       Member   0000.0000.0000     0      0       Provisioned
 2       Member   0000.0000.0000     0      0       Removed
*3       Active   6400.f124.e900     2      0       Ready
 8       Member   0000.0000.0000     0      0       Unprovisioned
```

次に、スタック情報の詳細を表示する例を示します。

```
Switch# show switch detail
Switch/Stack Mac Address : 2037.06ce.3f80 - Local Mac Address
Mac persistency wait time: Indefinite
                                           H/W   Current
Switch#   Role   Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Active 2037.06ce.3f80     1      0       Ready
 2       Member 0000.000.0000      0      0       Provisioned
```

```
 6       Member 2037.06ce.1e00     1       0        Ready

           Stack Port Status             Neighbors
Switch#   Port 1     Port 2           Port 1   Port 2
--------------------------------------------------------
  1       Ok         Down              6        None
  6       Down       Ok                None       1
```

次に、メンバ 6 の要約情報を表示する例を示します。

```
Switch# show switch 6
Switch#  Role      Mac Address     Priority     State
-----------------------------------------------------------
 6       Member     0003.e31a.1e00     1          Ready
```

次に、スタックに関するネイバー情報を表示する例を示します。

```
Switch# show switch neighbors
  Switch #    Port A       Port B
  --------    ------       ------
      6         None          8
      8          6           None
```

次に、スタック ポート情報を表示する例を示します。

```
Switch# show switch stack-ports
  Switch #    Port A       Port B
  --------    ------       ------
    6          Down          Ok
    8           Ok          Down
```

次に、**show switch stack-ports summary** コマンドの出力例を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
Switch# show switch stack-ports summary
Switch#/  Stack   Neighbor   Cable    Link   Link   Sync      #         In
 Port#     Port              Length    OK   Active   OK    Changes   Loopback
           Status                                          To LinkOK
--------  ------  --------  --------  ----  ------  ----  ---------  --------
  1/1     Down       2       50 cm     No     NO      No      10         No
  1/2     Ok         3       1 m       Yes    Yes     Yes     0          No
  2/1     Ok         5       3 m       Yes    Yes     Yes     0          No
  2/2     Down       1       50 cm     No     No      No      10         No
  3/1     Ok         1       1 m       Yes    Yes     Yes     0          No
  3/2     Ok         5       1 m       Yes    Yes     Yes     0          No
  5/1     Ok         3       1 m       Yes    Yes     Yes     0          No
  5/2     Ok         2       3 m       Yes    Yes     Yes     0          No
```

表 *32 : show switch stack-ports summary* コマンドの出力

フィールド	説明
Switch#/Port#	メンバー番号と、そのスタック ポート番号

フィールド	説明
Stack Port Status	スタック ポートのステータス。 • Absent：スタック ポートにケーブルが検出されません。 • Down：ケーブルは検出されましたが、接続されたネイバーがアップになっていないか、スタック ポートがディセーブルになっています。 • OK：ケーブルが検出され、接続済みのネイバーが起動しています。
Neighbor	スタック ケーブルの接続先の、アクティブなメンバーのスイッチの数。
Cable Length	有効な長さは 50 cm、1 m、または 3 m です。 スイッチがケーブルの長さを検出できない場合は、値は *no cable* になります。ケーブルが接続されていないか、リンクが信頼できない可能性があります。
Link OK	スタック ケーブルが接続され機能しているかどうか。相手側には、接続されたネイバーが存在する場合も、そうでない場合もあります。 リンク パートナーは、ネイバー スイッチ上のスタック ポートのことです。 • No：このポートに接続されているスタック ケーブルがないか、スタック ケーブルが機能していません。 • Yes：このポートには正常に機能するスタック ケーブルが接続されています。
Link Active	スタック ケーブル相手側にネイバーが接続されているかどうか。 • No：相手側にネイバーが検出されません。ポートは、このリンクからトラフィックを送信できません。 • Yes：相手側にネイバーが検出されました。ポートは、このリンクからトラフィックを送信できます。
Sync OK	リンク パートナーが、スタック ポートに有効なプロトコル メッセージを送信するかどうか。 • No：リンク パートナーからスタック ポートに有効なプロトコル メッセージが送信されません。 • Yes：リンクの相手側は、ポートに有効なプロトコル メッセージを送信します。
# Changes to LinkOK	リンクの相対的安定性。 短期間で多数の変更が行われた場合は、リンクのフラップが発生することがあります。

フィールド	説明
In Loopback	スタック ケーブルがメンバのスタック ポートに接続されているかどうか。 • No：メンバ上の少なくとも 1 つのスタック ポートに接続済みのスタック ケーブルがあります。 • Yes：メンバーのどのスタック ポートにも、スタック ケーブルが接続されていません。

関連トピック

reload （956 ページ）
session （958 ページ）
stack-mac update force （995 ページ）
switch priority （1000 ページ）
switch provision （1001 ページ）
switch renumber （1003 ページ）

show trace messages capwap ap ha

ワイヤレス Control And Provisioning of Wireless Access Points（CAPWAP）ハイ アベイラビリティを表示するには、**show trace messagescapwap ap ha** 特権 EXEC コマンドを使用します。

show trace messages capwap ap ha [{**detail**|**event**|**dump**}] [**switch** *switch*]

構文の説明

detail	（任意）ワイヤレス CAPWAP ハイ アベイラビリティの詳細を表示します。
detail*switch number*	スイッチ番号を指定します。値は 1 です。
event	（任意）ワイヤレス CAPWAP ハイ アベイラビリティのイベントを表示します。
event*switch number*	スイッチ番号を指定します。値は 1 です。
dump	（任意）ワイヤレス CAPWAP ハイ アベイラビリティの出力を表示します。
dump *switch number*	スイッチ番号を指定します。値は 1 です。
switch	（任意）スイッチ番号を表示します。値は 1 です。
switch *switch number*	スイッチ番号を指定します。値は 1 です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、CAPWAP ハイ アベイラビリティ出力を表示する例を示します。

```
Switch# show trace messages mobility ha dump switch 1
|  Output modifiers
  <cr>
```

show trace messages mobility ha

ワイヤレス モビリティ ハイ アベイラビリティを表示するには、**show trace messages mobility ha** 特権 EXEC コマンドを使用します。

show trace messages mobility ha [{**event**|**detail**|**dump**}] [**switch** *switch*]

構文の説明

event	（任意）ワイヤレス モビリティ HA のイベントを表示します。
event *switch*	スイッチ番号を指定します。値は 1 です。
detail	（任意）ワイヤレス モビリティ HA の詳細を表示します。
detail *switch*	スイッチ番号を指定します。値は 1 です。
dump	（任意）ワイヤレスモビリティHAの出力デバッグを表示します。
dump *switch*	スイッチ番号を指定します。値は 1 です。
switch *switch*	（任意）スイッチ番号を表示します。
switch *switch*	スイッチ番号を指定します。値は 1 です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、ワイヤレス モビリティ ハイ アベイラビリティを表示する例を示します。

```
Switch# show trace messages mobility ha
```

stack-mac persistent timer

固定 MAC アドレス機能をイネーブルにするには、スイッチ スタックまたはスタンドアロン スイッチのグローバル コンフィギュレーション モードで **stack-mac persistent timer** コマンドを使用します。固定 MAC アドレス機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

stack-mac persistent timer [{**0***time-value*}]
no stack-mac persistent timer

構文の説明

0	（任意）現在のアクティブ スイッチの MAC アドレスの使用を無期限に継続し、新しいアクティブ スイッチが引き継いだ場合もそうします。
time-value	（任意）スタック MAC アドレスが新しいアクティブ スイッチの MAC アドレスに変わるまでの時間（分単位）。指定できる範囲は 1 ～ 60 分です。

コマンド デフォルト

固定 MAC アドレスはディセーブルに設定されています。スタックの MAC アドレスは常に、アクティブ スイッチの MAC アドレスです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、新しいアクティブ スイッチが引き継ぐ場合でも、スタック MAC アドレスは最初のアクティブ スイッチの MAC アドレスになります。同じ動作は、**stack-mac persistent timer** コマンドまたは **stack-mac persistent timer 0** コマンドを入力した場合にも発生します。

stack-mac persistent timer コマンドを *time-value* とともに入力すると、新しいスイッチがアクティブ スイッチになったときに、入力した時間の後にスタック MAC アドレスが新しいアクティブ スイッチのものに変わります。以前のアクティブ スイッチがこの時間内にスタックに再加入した場合、スタックはその MAC アドレスを持つスイッチがスタック内に存在する限り、その MAC アドレスを保持します。

スタック全体をリロードすると、アクティブ スイッチの MAC アドレスがスタックの MAC アドレスになります。

（注） スタック MAC アドレスを変更しない場合、レイヤ 3 インターフェイスのフラップが発生しません。これは、未知の MAC アドレス（スタック内のスイッチに属さない MAC アドレス）がスタック MAC アドレスになる可能性があることを意味します。この未知の MAC アドレスを持つスイッチが別のスタックにアクティブ スイッチとして参加すると、2 つのスタックが同じスタック MAC アドレスを持つことになります。**stack-mac update force** コマンドを使用して、この競合を解決する必要があります。

例

次に、固定 MAC アドレスをイネーブルにする例を示します。

```
Switch(config)# stack-mac persistent timer
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを入力します。イネーブルの場合、出力に **stack-mac persistent timer** が表示されます。

関連トピック

stack-mac update force （995 ページ）

stack-mac update force

スタック MAC アドレスをアクティブ スイッチの MAC アドレスに更新するには、アクティブ スイッチの EXEC モードで **stack-mac update force** コマンドを使用します。

stack-mac update force

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、ハイ アベイラビリティ（HA）フェールオーバー時に、スタックの MAC アドレスは新しいアクティブ スイッチの MAC アドレスに変更されません。スタック MAC アドレスが新しいアクティブ スイッチの MAC アドレスに強制的に変更されるようにするには、**stack-mac update force** コマンドを使用します。

スタック MAC アドレスと同じ MAC アドレスを持つスイッチが現在そのスタックのメンバーである場合、**stack-mac update force** コマンドは無効です。（スタック MAC アドレスはアクティブ スイッチの MAC アドレスに更新されません）

（注） スタック MAC アドレスを変更しない場合、レイヤ 3 インターフェイスのフラップが発生しません。これは、未知の MAC アドレス（スタック内のスイッチに属さない MAC アドレス）がスタック MAC アドレスになる可能性があることを意味します。この未知の MAC アドレスを持つスイッチが別のスタックにアクティブ スイッチとして参加すると、2 つのスタックが同じスタック MAC アドレスを持つことになります。**stack-mac update force** コマンドを使用して、この競合を解決する必要があります。

次に、スタック MAC アドレスをアクティブ スイッチの MAC アドレスに更新する例を示します。

```
Switch> stack-mac update force
Switch>
```

設定を確認するには、**show switch** 特権 EXEC コマンドを入力します。スタック MAC アドレスには、MAC アドレスがローカルと未知のどちらであるかも含まれます。

関連トピック

show switch （986 ページ）
stack-mac persistent timer （993 ページ）

standby console enable

スタンバイ コンソール スイッチへのアクセスを有効にするには、冗長メイン コンフィギュレーション サブモードで **standby console enable** コマンドを使用します。スタンバイ コンソール スイッチへのアクセスを無効にするには、このコマンドの **no** 形式を使用します。

standby console enable
no standby console enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

スタンバイ スイッチ コンソールへのアクセスはディセーブルです。

コマンド モード

冗長メイン コンフィギュレーション サブモード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、スタンバイ コンソールに関する特定のデータを収集し、確認するために使用されます。コマンドは、主にシスコのテクニカル サポート担当がスイッチのトラブルシューティングを行うのに役立ちます。

次に、冗長メイン コンフィギュレーション サブモードを開始し、スタンバイ コンソール スイッチへのアクセスをイネーブルにする例を示します。

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)# standby console enable
Switch(config-r-mc)#
```

関連トピック

main-cpu （948 ページ）

switch stack port

メンバの指定されたスタック ポートをディセーブルまたはイネーブルにするには、スタック メンバの特権 EXEC モードで **switch** コマンドを使用します。

switch *stack-member-number* **stack port** *port-number* {**disable**|**enable**}

構文の説明

stack-member-number	現在のスタック メンバ番号。指定できる範囲は 1 ～ 9 です。
stackport *port-number*	メンバ上のスタック ポートを指定します。指定できる範囲は 1 ～ 2 です。
disable	指定したポートをディセーブルにします。
enable	指定されたポートをイネーブルにします。

コマンド デフォルト

スタック ポートはイネーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スタックが full-ring 状態になるのは、すべてのスタック メンバがスタック ポートを使用して接続され、ready 状態になっている場合です。

スタックが partial-ring 状態になるのは、次が発生したときです。

- すべてのメンバがスタック ポートを通じて接続されたが、一部が ready ステートではない。
- スタック ポートを通じて接続されていないメンバーがある。

（注） **switch** *stack-member-number***stackport** *port-number***disable** コマンドを使用するときは注意してください。スタック ポートをディセーブルにすると、スタックは半分の帯域幅で稼働します。

switch *stack-member-number***stackport** *port-number***disable** 特権 EXEC コマンドを入力し、スタックが full-ring 状態にある場合、ディセーブルにできるスタック ポートは 1 つだけです。次のメッセージが表示されます。

```
Enabling/disabling a stack port may cause undesired stack changes. Continue?[confirm]
```

switch *stack-member-number* **stack port** *port-number* **disable** 特権 EXEC コマンドを入力し、スタックが partial-ring 状態にある場合、ポートはディセーブルにできません。次のメッセージが表示されます。

```
Disabling stack port not allowed with current stack configuration.
```

例

次に、member 4 上の stack port 2 をディセーブルにする方法の例を示します。

```
Switch# switch 4 stack port 2 disable
```

関連トピック

show switch （986 ページ）

switch priority

スタック メンバーのプライオリティ値を変更するには、アクティブ スイッチの EXEC モードで **switch priority** コマンドを使用します。

switch *stack-member-number* **priority** *new-priority-value*

構文の説明

stack-member-number	現在のスタック メンバ番号。指定できる範囲は 1 ～ 9 です。
new-priority-value	スタック メンバの新しいプライオリティ値指定できる範囲は 1 ～ 15 です。

コマンド デフォルト

デフォルトのプライオリティ値は 1 です。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

新しいプライオリティ値は、新しい アクティブ スイッチ 選定の要素になります。プライオリティ値を変更しても、アクティブ スイッチ がただちに変更されることはありません。

例

次の例では、スタック メンバ 6 のプライオリティ値を 8 に変更する方法を示します。

```
Switch# switch 6 priority 8
Changing the Switch Priority of Switch Number 6 to 8
Do you want to continue?[confirm]
```

関連トピック

reload （956 ページ）
session （958 ページ）
show switch （986 ページ）
switch renumber （1003 ページ）

switch provision

新しいスイッチがスイッチ スタックに追加される前に構成設定するには、アクティブ スイッチのグローバル コンフィギュレーション モードで **switch provision** コマンドを使用します。除外されたスイッチ（スタックを離れたスタック メンバ）に対応するすべての設定情報を削除するには、このコマンドの **no** 形式を使用します。

switch *stack-member-number* **provision** *type*
no switch *stack-member-number* **provision**

構文の説明

stack-member-number	スタック メンバの番号です。指定できる範囲は 1 ～ 9 です。
type	新しいスイッチがスタックに加入する前の、このスイッチのタイプ。

コマンド デフォルト

スイッチは、プロビジョニングされていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

type には、コマンドライン ヘルプ ストリングに示されたサポート対象のスイッチのモデル番号を入力します。

エラー メッセージを受信しないようにするには、このコマンドの **no** 形式を使用してプロビジョニングされた設定を削除する前に、スイッチ スタックから指定のスイッチを削除する必要があります。

スイッチ タイプを変更する場合も、スイッチ スタックから指定のスイッチを削除する必要があります。スイッチ タイプを変更しない場合でも、スイッチ スタック内に物理的に存在するプロビジョニングされたスイッチのスタック メンバ番号を変更できます。

プロビジョニングされたスイッチのタイプが、スタック上のプロビジョニングされた設定のスイッチ タイプと一致しない場合、スイッチ スタックはプロビジョニングされたスイッチにデフォルト設定を適用し、これをスタックに追加します。スイッチ スタックでは、デフォルト設定を適用する場合にメッセージを表示します。

プロビジョニング情報は、スイッチ スタックの実行コンフィギュレーションで表示されます。**copy running-config startup-config** 特権 EXEC コマンドを入力すると、プロビジョニングされた設定がスイッチ スタックのスタートアップ コンフィギュレーション ファイルに保存されます。

注意 **switch provision** コマンドを使用すると、プロビジョニングされた設定にメモリが割り当てられます。新しいスイッチ タイプが設定されたときに、以前割り当てられたメモリのすべてが解放されるわけではありません。そのため、このコマンドをおおよそ200回を超えて使用しないようにしてください。スイッチのメモリが不足し、予期せぬ動作が発生する可能性があります。

例

次に、スタック メンバー番号2が設定されたスイッチをスイッチ スタックに割り当てる例を示します。**show running-config** コマンドの出力は、プロビジョニングされたスイッチに関連付けられたインターフェイスを示します。

```
Switch(config)# switch 2 provision WS-xxxx
Switch(config)# end
Switch# show running-config | include switch 2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
<output truncated>
```

また、**show switch** ユーザ EXEC コマンドを入力すると、スイッチ スタックのプロビジョニングされたステータスを表示できます。

次の例では、スイッチがスタックから削除される場合に、スタック メンバ5についてのすべての設定情報が削除される方法を示します。

```
Switch(config)# no switch 5 provision
```

プロビジョニングされたスイッチが、実行コンフィギュレーションで追加または削除されたことを確認するには、**show running-config** 特権 EXEC コマンドを入力します。

関連トピック

show switch （986 ページ）

switch renumber

スタック メンバ番号を変更するには、**switch renumber** コマンドを アクティブ スイッチ の EXEC モードで使用します。

switch *current-stack-member-number* **renumber** *new-stack-member-number*

構文の説明

current-stack-member-number	現在のスタック メンバ番号。指定できる範囲は 1 ～ 9 です。
new-stack-member-number	スタック メンバの新しいスタック メンバ番号。指定できる範囲は 1 ～ 9 です。

コマンド デフォルト

デフォルトのスタック メンバ番号は 1 です。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

指定したメンバ番号をすでに他のスタック メンバが使用している場合、スタック メンバをリロードする際に アクティブ スイッチ は使用可能な一番低い番号を割り当てます。

（注） スタック メンバ番号を変更し、新しいスタック メンバ番号がどの設定にも関連付けされていない場合、そのスタック メンバは現在の設定を廃棄してリセットを行い、デフォルトの設定に戻ります。

プロビジョニングされたスイッチでは、**switch** *current-stack-member-number***renumber** *new-stack-member-number* コマンドを使用しないでください。使用すると、コマンドは拒否されます。

スタック メンバをリロードし、設定変更を適用するには、**reload slot** *current stack member number* 特権 EXEC コマンドを使用します。

例

次の例では、スタック メンバ 6 のメンバ番号を 7 に変更する方法を示しています。

```
Switch# switch 6 renumber 7
WARNING:Changing the switch number may result in a configuration change for that switch.
The interface configuration associated with the old switch number will remain as a
provisioned configuration.
Do you want to continue?[confirm]
```

関連トピック

- reload （956 ページ）
- session （958 ページ）
- show switch （986 ページ）
- switch priority （1000 ページ）

第 XII 部

システム管理

システム管理コマンド

arp

Address Resolution Protocol（ARP）テーブルの内容を表示するには、ブート ローダ モードで **arp** コマンドを使用します。

arp [*ip_address*]

構文の説明

ip_address	（任意）ARP テーブルまたは特定の IP アドレスのマッピングを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ARP テーブルには、IP アドレスと MAC アドレスのマッピングが示されます。

例

次に、ARP テーブルを表示する例を示します。

```
Switch: arp 172.20.136.8
arp'ing 172.20.136.8...
172.20.136.8 is at 00:1b:78:d1:25:ae, via port 0
```

関連トピック

set （1059 ページ）

boot

実行可能イメージをロードおよびブートして、コマンドライン インターフェイス（CLI）を表示するには、ブート ローダ モードで **boot** コマンドを使用します。

boot ［**-post** | **-n** | **-p** | *flag*］ *filesystem:/file-url...*

構文の説明

-post	（任意）拡張および総合POSTによってロードされたイメージを実行します。このキーワードを使用すると、POST の完了に要する時間が長くなります。
-n	（任意）起動後すぐに、Cisco IOS デバッガが休止します。
-p	（任意）イメージのロード後すぐに、JTAG デバッガが休止します。
filesystem:	ファイル システムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。USB メモリ スティックには **usbflash0:** を使用します。
/file-url	ブート可能なイメージのパス（ディレクトリ）および名前。各イメージ名はセミコロンで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

引数を何も指定しないで **boot** コマンドを入力した場合、スイッチは、BOOT 環境変数が設定されていればその中の情報を使用して、システムを自動的にブートしようとします。

file-url 変数にイメージ名を指定した場合、**boot** コマンドは指定されたイメージをブートしようとします。

ブート ローダ **boot** コマンドのオプションを設定した場合は、このコマンドがただちに実行され、現在のブート ローダ セッションだけに適用されます。

これらの設定が保存されて次回のブート処理に使用されることはありません。

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

例

次の例では、*new-image.bin* イメージを使用してスイッチをブートする方法を示します。

```
Switch: set BOOT flash:/new-images/new-image.bin
Switch: boot
```

このコマンドを入力すると、セットアップ プログラムを開始するように求められます。

cat

1 つ以上のファイルの内容を表示するには、ブート ローダ モードで **cat** コマンドを使用します。

cat *filesystem:/file-url...*

構文の説明

filesystem:	ファイル システムを指定します。
/file-url	表示するファイルのパス（ディレクトリ）と名前を指定します。ファイル名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

ファイルのリストを指定した場合は、各ファイルの内容が順に表示されます。

例

次の例では、イメージ ファイルの内容を表示する方法を示します。

```
Switch: cat flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

clear location

特定の無線 ID（RFID）タグまたはデータベース全体のすべての RFID タグ情報をクリアするには、EXEC モードで **clearlocation** コマンドを使用します。

clear location [mac-address *mac-address* | **rfid]**

構文の説明

mac-address *mac-address*	特定の RFID タグの MAC アドレス。
rfid	データベース上のすべての RFID タグを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、データベースからすべての RFID タグ情報をクリアする例を示します。

```
Switch> clear location rfid
```

clear location statistics

無線ID（RFID）統計情報をクリアするには、EXECモードで**clearlocationstatistics**コマンドを使用します。

clear location statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**clear location rfid**コマンドの出力例と、RFID統計情報をクリアする例を示します。

```
Switch> clear location statistics
```

clear nmsp statistics

Network Mobility Services Protocol（NMSP）統計情報をクリアするには、EXEC モードで **clearnmspstatistics** コマンドを使用します。

clear nmsp statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次は **clear nmsp statistics** コマンドのサンプル出力です。コントローラと接続中の Cisco モビリティ サービス エンジン（MSE）の間で交換される NMSP 情報に関するすべての統計情報をクリアする方法を示します。

```
Switch> clear nmsp statistics
```

clear wireless ccx statistics

CCX 統計情報をクリアするには、EXEC モードで **clearwirelessccxstatistics** コマンドを使用します。

clear wireless ccx statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**clear wireless ccx statistics** コマンドの出力例と、CCX クライアントに関して収集されたすべての統計情報をクリアする例を示します。

```
Switch> clear wireless ccx statistics
```

clear wireless client tsm dot11

特定のアクセス ポイント、またはこのクライアントが関連付けられているすべてのアクセス ポイントのトラフィック ストリーム メトリック（TSM）統計情報をクリアするには、EXEC モードで **clearwirelessclienttsmdot11** コマンドを使用します。

clear wireless client tsm dot11 {**24ghz**|**5ghz**} *client-mac-addr* {**all**| **name** *ap-name*}

構文の説明

24ghz	802.11a ネットワークを指定します。
5ghz	802.11b ネットワークを指定します。
client-mac-addr	クライアントの MAC アドレス。
all	すべてのアクセス ポイントを指定します。
name *ap-name*	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**clear wireless client tsm dot11** コマンドの出力例と、このクライアントが認識されているすべての 5-GHz 無線アクセス ポイント上の MAC アドレス 00:40:96:a8:f7:98 の TSM をクリアする例を示します。

```
Switch> clear wireless client tsm dot11 5ghz 00:40:96:a8:f7:98 all
```

clear wireless location s69 statistics

CCXv5 クライアントとの S69 交換に関する統計情報をクリアするには、EXEC モードで **clearwirelesslocations69statistics** コマンドを使用します。

clear wireless location s69 statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

S69 メッセージは、CCXv5 クライアントと無線インフラストラクチャとの間で交換されます。CCXv5 クライアントは S69 メッセージを使用してロケーション情報を要求します。これに対し、無線インフラストラクチャから S69 応答メッセージが返されます。

例

次に、**clear wireless location s69 statistics** コマンドの出力例と、CCXv5 クライアントとの S69 交換に関する統計情報をクリアする例を示します。

```
Switch> clear wireless location s69 statistics
```

copy

ファイルをコピー元からコピー先にコピーするには、ブート ローダ モードで **copy** コマンドを使用します。

copy *filesystem:/source-file-url filesystem:/destination-file-url*

構文の説明

filesystem:	ファイル システムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。
/source-file-url	コピー元のパス（ディレクトリ）およびファイル名です。
/destination-file-url	コピー先のパス（ディレクトリ）およびファイル名です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

スラッシュ（/）間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

指定できるファイル名は最大127文字です。ファイル名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

ファイルを別のディレクトリにコピーする場合は、そのディレクトリが存在していなければなりません。

例

次の例では、ルートにあるファイルをコピーする方法を示します。

```
Switch: copy usbflash0:test1.text usbflash0:test4.text
File "usbflash0:test1.text" successfully copied to "usbflash0:test4.text"
```

ファイルがコピーされたかどうかを確認するには、**dir** *filesystem:* ブート ローダ コマンドを入力します。

copy startup-config tftp:

スイッチから TFTP サーバに設定をコピーするには、特権 EXEC モードで **copy startup-config tftp:** コマンドを使用します。

copy startup-config tftp: *remote host {ip-address}/{name}*

構文の説明

remote host {ip-address}/{name}	リモートホストのホスト名またはIPアドレス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 16.1	このコマンドが導入されました。

使用上のガイドライン

スイッチから現在の設定をコピーするには、**copy startup-config tftp:** コマンドを実行し、続く指示に従います。設定が TFTP サーバにコピーされます。

次に、別のスイッチへログインし、**copy tftp: startup-config** コマンドを実行して、続く指示に従います。これで、設定は別のスイッチにコピーされます。

例

次に、TFTP サーバに設定をコピーする例を示します。

```
Switch: copy startup-config tftp:
Address or name of remote host []?
```

copy tftp: startup-config

TFTP サーバから新しいスイッチに設定をコピーするには、新しいスイッチ上で、特権 EXEC モードで **copy tftp: startup-config** コマンドを使用します。

copy tftp: startup-config *remote host {ip-address}/{name}*

構文の説明

remote host {ip-address}/{name}	リモートホストのホスト名またはIPアドレス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 16.1	このコマンドが導入されました。

使用上のガイドライン

設定をコピーした後、その設定を保存するには、**write memory** コマンドを使用し、その後スイッチをリロードするか、または **copy startup-config running-config** コマンドを実行します。

例

次に、TFTP サーバからスイッチに設定をコピーする例を示します。

```
Switch: copy tftp: startup-config
Address or name of remote host []?
```

debug call-admission wireless all

ワイヤレスコールアドミッション制御（CAC）機能のデバッグを有効にするには、特権EXECモードで **debugcall-admissionwirelessall** コマンドを使用します。デバッグを無効にするには、このコマンドの **no** 形式を使用します。

debug call-admission wireless all [**switch** *switch*]
no debug call-admission wireless all [**switch** *switch*]

構文の説明

switch	特定のスイッチに関連付けられるすべてのワイヤレス CAC メッセージのデバッグ オプションを設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**debug call-admission wireless switch** コマンドの出力例と、CAC メッセージのデバッグ オプションを有効にする例を示します。

```
Switch# debug call-admission wireless switch 1 all
```

debug rfid

無線 ID（RFID）デバッグを設定するには、特権 EXEC モードで **debugrfid** コマンドを使用します。デバッグを無効にするには、このコマンドの **no** 形式を使用します。

debug rfid {*debug_leaf_name* | **all** | **detail** | **error** | **nmsp** | **receive**} [**filter** | **switch** *switch*]
no debug rfid {*debug_leaf_name* | **all** | **detail** | **error** | **nmsp** | **receive**} [**filter** | **switch** *switch*]

構文の説明

debug_leaf_name	デバッグ リーフ名です。
all	すべての RFID のデバッグを設定します。
detail	RFID 詳細のデバッグを設定します。
error	RFID エラー メッセージのデバッグを設定します。
nmsp	RFID の Network Mobility Services Protocol（NMSP）メッセージのデバッグを設定します。
receive	入力 RFID タグ メッセージのデバッグを設定します。
filter	デバッグ フラグ フィルタ名です。
switch *switch*	スイッチの RFID デバッグを設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**debug rfid** コマンドの出力例と、RFID エラー メッセージのデバッグを有効にする例を示します。

```
Switch# debug rfid error switch 1
```

debug voice diagnostics mac-address

音声クライアントの音声診断のデバッグを有効にするには、特権 EXEC モードで **debugvoicediagnosticsmac-address** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug voice diagnostics mac-address *mac-address1* **verbose mac-address** *mac-address2* **verbose**
nodebug voice diagnostics mac-address *mac-address1* **verbose mac-address** *mac-address2* **verbose**

構文の説明

voice diagnostics	音声クライアントの音声のデバッグを設定します。
mac-address *mac-address1* **mac-address** *mac-address2*	音声クライアントのMACアドレスを指定します。
verbose	音声診断の冗長モードを有効にします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

以下は、**debug voice diagnostics mac-address** コマンドの出力例で、MAC アドレスが 00:1f:ca:cf:b6:60 である音声クライアントの音声診断のデバッグを有効にする手順を示しています。

```
Switch# debug voice diagnostics mac-address 00:1f:ca:cf:b6:60
```

debug wps mfp

WPS MFP デバッグ オプションを有効にするには、特権 EXEC モードで **debugwps mfp** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの no 形式を使用します。

debug wps mfp {**all** | **capwap** | **client** | **detail** | **mm** | **report**} [**switch** *switch*]

構文の説明

wps mfp	WPS MFP デバッグ オプションを設定します。
all	すべての WPS MFP デバッグ メッセージを表示します。
capwap	MFP メッセージを表示します。
client	クライアント MFP メッセージを表示します。
detail	詳細な MFP CAPWAP メッセージを表示します。
mm	MFP モビリティ（コントローラ間）メッセージを表示します。
report	MFP レポートを表示します。
switch *switch*	スイッチの WPS MFP デバッグを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、クライアントの WPS MFP デバッグ オプションを有効にする例を示します。

```
Switch# debug wps mfp client switch 1
```

delete

指定されたファイル システムから 1 つ以上のファイルを削除するには、ブート ローダ モードで **delete** コマンドを使用します。

delete *filesystem:/file-url...*

構文の説明

filesystem:	ファイル システムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。
/file-url...	削除するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

各ファイルを削除する前に確認を求めるプロンプトが スイッチ によって表示されます。

例

次の例では、2 つのファイルを削除します。

```
Switch: delete usbflash0:test2.text usbflash0:test5.text
Are you sure you want to delete "usbflash0:test2.text" (y/n)?y
File "usbflash0:test2.text" deleted
Are you sure you want to delete "usbflash0:test5.text" (y/n)?y
File "usbflash0:test2.text" deleted
```

ファイルが削除されたことを確認するには、**dir usbflash0:** ブート ローダ コマンドを入力します。

dir

指定されたファイル システムのファイルおよびディレクトリのリストを表示するには、ブート ローダ モードで **dir** コマンドを使用します。

dir *filesystem:/file-url*

構文の説明

filesystem:	ファイル システムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。USB メモリ スティックには **usbflash0:** を使用します。
/file-url	（任意）表示するコンテンツが格納されているパス（ディレクトリ）およびディレクトリの名前です。ディレクトリ名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブート ローダ

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ディレクトリ名では、大文字と小文字が区別されます。

例

次の例では、フラッシュ メモリ内のファイルを表示する方法を示します。

```
Switch: dir flash:
Directory of flash:/
    2  -rwx         561   Mar 01 2013 00:48:15  express_setup.debug
    3  -rwx     2160256   Mar 01 2013 04:18:48  c2960x-dmon-mz-150-2r.EX
    4  -rwx        1048   Mar 01 2013 00:01:39  multiple-fs
    6  drwx         512   Mar 01 2013 23:11:42  c2960x-universalk9-mz.150-2.EX
  645 drwx         512   Mar 01 2013 00:01:11  dc_profile_dir
  647 -rwx        4316   Mar 01 2013 01:14:05  config.text
  648 -rwx           5   Mar 01 2013 00:01:39  private-config.text

   96453632 bytes available (25732096 bytes used)
```

表 *33 : dir* のフィールドの説明

フィールド	説明
2	ファイルのインデックス番号

フィールド	説明
-rwx	ファイルのアクセス権（次のいずれか、またはすべて） • d：ディレクトリ • r：読み取り可能 • w：書き込み可能 • x：実行可能
1644045	ファイルのサイズ
<date>	最終変更日
env_vars	ファイル名。

関連トピック

mkdir （1050 ページ）
rmdir （1057 ページ）

emergency-install

システムで緊急インストールを実行するには、ブート ローダ モードで **emergency-install** コマンドを使用します。

emergency-install *url://<url>*

構文の説明

<url>	緊急インストール バンドル イメージが格納されているファイルの URL と名前です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

インストール操作時にブート フラッシュが消去されます。

例

次に、イメージ ファイルの内容を使用して緊急インストール操作を実行する例を示します。

```
Switch: emergency-install tftp:<url>
The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery (tftp:<url> ...
Reading full image into memory.....................done
Nova Bundle Image
--------------------------------------
Kernel Address    : 0x6042d5c8
Kernel Size       : 0x317ccc/3243212
Initramfs Address : 0x60745294
Initramfs Size    : 0xdc6774/14444404
Compression Format: .mzip

Bootable image at @ ram:0x6042d5c8
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range          \
[0x80180000, 0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)



Initiating Emergency Installation of bundle                                      \
tftp:<url>
```

```
Downloading bundle tftp:<url>...

Validating bundle tftp:<url>...
Installing bundle tftp:<url>...
Verifying bundle tftp:<url>...
Package cat3k_caa-base.SPA.03.02.00SE.pkg is Digitally Signed
Package cat3k_caa-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-infra.SPA.03.02.00SE.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg is Digitally Signed
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-wcm.SPA.10.0.100.0.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.\ufffd


Booting...(use DDR clock 667 MHz)Initializing and Testing RAM                      \
+++@@@@####...++@@++@@++@@++@@++@@++@@++@@++@@done.
Memory Test Pass!

Base ethernet MAC Address: 20:37:06:ce:25:80
Initializing Flash...

flashfs[7]: 0 files, 1 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 6784000
flashfs[7]: Bytes used: 1024
flashfs[7]: Bytes available: 6782976
flashfs[7]: flashfs fsck took 1 seconds....done Initializing Flash.

The system is not configured to boot automatically. The
following command will finish loading the operating system
software:

    boot
```

exit

以前のモードに戻るか、CLI EXEC モードを終了するには、**exit** コマンドを使用します。

exit

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、コンフィギュレーション モードを終了する例を示します。

```
Switch(config)# exit
Switch#
```

flash_init

flash: ファイル システムを再初期化するには、ブートローダ モードで **flash_init** コマンドを使用します。

flash_init

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

flash: ファイル システムは、通常のシステム動作中に自動的に初期化されます。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

flash: ファイル システムは、通常のブート プロセス中に自動的に初期化されます。

このコマンドは、flash: ファイル システムを手動で初期化します。たとえば、パスワードを忘れた場合には、回復手順中にこのコマンドを使用します。

help

利用可能なコマンドを表示するには、ブート ローダ モードで **help** コマンドを使用します。

help

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

例

次に、利用可能なブート ローダ コマンドのリストを表示する例を示します。

```
Switch:help
? -- Present list of available commands
arp -- Show arp table or arp-resolve an address
boot -- Load and boot an executable image
cat -- Concatenate (type) file(s)
copy -- Copy a file
delete -- Delete file(s)
dir -- List files in directories
emergency-install -- Initiate Disaster Recovery
...
...
...
unset -- Unset one or more environment variables
version -- Display boot loader version
```

license right-to-use

スイッチに使用権アクセス ポイント追加ライセンスを設定するには、特権 EXEC モードで **licenseright-to-use** コマンドを使用します。

license right-to-use {**activate | deactivate**} **apcount | ipbase | ipservices | lanbase**

構文の説明

activate	永久または評価 ap-count ライセンスをアクティブ化します。
deactivate	永久または評価 ap-count ライセンスを非アクティブ化します。
apcount *count*	追加する ap-count ライセンスの数を指定します。 設定できる追加ライセンス数は、5 ~ 50 です。
ipbase *count*	スイッチの ipbase ライセンスをアクティブ化します。
ipservices *count*	スイッチの ipservices ライセンスをアクティブ化します。
lanbase *count*	スイッチの lanbase ライセンスをアクティブ化します。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、ap-count 評価ライセンスをアクティブ化する例を示します。

```
Switch# license right-to-use activate apcount evaluation
Switch# end
```

次に、ap-count 永久ライセンスをアクティブ化する例を示します。

```
Switch# license right-to-use deactivate apcount evaluation
Switch# end
```

次に、新規 ap-count ライセンスを追加する例を示します。

```
Switch# license right-to-use activate apcount 500 slot 1
Switch# end
```

location

エンドポイントのロケーション情報を設定するには、グローバルコンフィギュレーションモードで **location** コマンドを使用します。ロケーション情報を削除するには、このコマンドの **no** 形式を使用します。

location {**admin-tag** *string*|**algorithm**|**civic-location identifier** {**host***id*}|**civic-location identifier** {**host***id*}|**elin-location** {*string* | **identifier** *id*}|**expiry**{**calibrating-client***timeout-value* | **client***timeout-value* | **rouge-aps***timeout-value* | **tags***timeout-value*}|**geo-location identifier** {**host***id*}|**notify-threshold**{**client***db* | **rouge-aps***db* | **tags***db*|**plm**{**calibrating**|{**multiband**|**uniband**}|**client***burst-interval*}|**prefer**{**cdp weight***priority-value* | **lldp-med weight***priority-value* | **static config weight***priority-value*} | **rfid**{**status** | **timeout***rfid-timeout-value* | **vendor-name***name*} | **rssi-half-life** { **calibrating-client***seconds* | **client***seconds* | **rogue-aps***seconds* | **tags***seconds*}
no location {**admin-tag** *string*|**algorithm**|**civic-location identifier** {**host***id*}|**civic-location identifier** {**host***id*}|**elin-location** {*string* | **identifier** *id*}|**expiry**{**calibrating-client***timeout-value* | **client***timeout-value* | **rouge-aps***timeout-value* | **tags***timeout-value*}|**geo-location identifier** {**host***id*}|**notify-threshold**{**client***db* | **rouge-aps***db* | **tags***db*|**plm**{**calibrating**|{**multiband**|**uniband**}|**client***burst-interval*}|**prefer**{**cdp weight***priority-value* | **lldp-med weight***priority-value* | **static config weight***priority-value*} | **rfid**{**status** | **timeout***rfid-timeout-value* | **vendor-name***name*} | **rssi-half-life** { **calibrating-client***seconds* | **client***seconds* | **rogue-aps***seconds* | **tags***seconds*}

構文の説明

admin-tag*string*	管理タグまたはサイト情報を設定します。英数字形式のサイト情報またはロケーション情報。
algorithm	平均 RSSI および SNR 値に使用されるアルゴリズムを設定します。
civic-location	都市ロケーション情報を設定します。
identifier	都市ロケーション、緊急ロケーション、地理的な場所の名前を指定します。
host	ホストの都市ロケーションや地理空間的な場所を定義します。
id	都市ロケーション、緊急ロケーション、地理的な場所の名前。 （注） LLDP-MED スイッチ TLV での都市ロケーションの ID は 250 バイト以下に制限されます。 スイッチ設定中に使用できるバッファ スペースに関するエラー メッセージを回避するには、各都市ロケーション ID に指定されたすべての都市ロケーション情報の全体の長さが 250 バイトを超えないようにします。
elin-location	緊急ロケーション情報 (ELIN) を設定します。

expiry {calibrating-client | client | rogue-aps | tags} *timeout-value*	調整クライアント、クライアント、不正アクセス ポイント、および RFID タグの RSSI タイムアウト値を設定します。 調整クライアントに有効なタイムアウトパラメータ値の範囲は 1 ～ 3600 秒です。デフォルト値は 5 秒です。 クライアント、不正アクセス ポイント、RFID タグに有効なタイムアウト パラメータ値の範囲は 5 ～ 3600 秒です。デフォルト値は 5 秒です。
geo-location	地理空間的なロケーション情報を設定します。
notify-threshold {client| rogue-aps| tags} *db*	RSSI 測定の NMSP 通知しきい値を設定します。 しきい値パラメータに有効な値の範囲は 0 ～ 10 dB です。デフォルト値は 0 dB です。
calibrating {multiband | uniband} | client *seconds*	調整クライアントのパス損失測定（CCX S60）要求およびクライアントのバースト間隔を設定します。 バースト間隔パラメータに有効な値の範囲は 0 ～ 3600 秒です。
prefer	ロケーション情報のソースのプライオリティを設定します。
rfid	ロケーションの RFID タグ トラッキングを設定します。
rssi-half-life	各種デバイスの RSSI 半減期を設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

location civic-location identifier グローバル コンフィギュレーション コマンドを入力後、都市ロケーション コンフィギュレーション モードが開始されます。**location geo-location identifier** グローバル コンフィギュレーション コマンドを入力後、ジオ ロケーション コンフィギュレーション モードが開始されます。

都市ロケーション ID は 250 バイトを超えてはなりません。

ホスト ID はホストの都市ロケーションや地理空間的な場所を設定します。ID がホストではない場合、ID はインターフェイスで参照できる地理空間的なテンプレートまたは都市ロケーションだけを定義します。

hostキーワードは、デバイスの場所を定義します。**identifier** と **host**キーワードを使用して設定可能な都市ロケーション オプションは同じです。都市ロケーション コンフィギュレーション モードで次の都市ロケーション オプションを指定できます。

- **additional-code**：追加都市ロケーション コードを設定します。
- **additional-location-information**：追加都市ロケーション情報を設定します。
- **branch-road-name**：ブランチのロード名を設定します。
- **building**：建物の情報を設定します。
- **city**：都市名を設定します。
- **country**：2 文字の ISO 3166 の国コードを設定します。
- **county**：郡名を設定します。
- **default**：コマンドをデフォルト値に設定します。
- **division**：市の地区の名前を設定します。
- **exit**：都市ロケーション コンフィギュレーション モードを終了します。
- **floor**：階数を設定します。
- **landmark**：目印となる建物の情報を設定します。
- **leading-street-dir**：町名番地に付与される方角を設定します。
- **name**：居住者名を設定します。
- **neighborhood**：ネイバーフッド情報を設定します。
- **no**：指定された都市ロケーション データを拒否し、デフォルト値を設定します。
- **number**：町名番地を設定します。
- **post-office-box**：私書箱を設定します。
- **postal-code**：郵便番号を設定します。
- **postal-community-name**：郵便コミュニティ名を設定します。
- **primary-road-name**：主要道路の名前を設定します。
- **road-section**：道路の区間を設定します。
- **room**：部屋の情報を設定します。
- **seat**：座席の情報を設定します。
- **state**：州の名前を設定します。
- **street-group**：町名番地のグループを設定します。
- **street-name-postmodifier**：町名番地の名前のポストモディファイアを設定します。
- **street-name-premodifier**：町名番地の名前のプレモディファイアを設定します。
- **street-number-suffix**：町名番地の番号のサフィックスを設定します。
- **street-suffix**：町名番地のサフィックスを設定します。
- **sub-branch-road-name**：支線からさらに分岐した道路名を設定します。
- **trailing-street-suffix**：後に続く町名番地のサフィクスを設定します。
- **type-of-place**：場所のタイプを設定します。
- **unit**：単位を設定します。

地理的ロケーション コンフィギュレーション モードで次の地理空間的なロケーション情報を指定できます。

- **altitude**：高さの情報を階数、メートル、またはフィート単位で設定します。

- **latitude**：度、分、秒の緯度情報を設定します。範囲は -90 ～ 90 度です。正の値は、赤道より北側の位置を示します。
- **longitude**：度、分、秒の経度の情報を設定します。範囲は -180 ～ 180 度です。正の値は、グリニッジ子午線の東側の位置を示します。
- **resolution**：緯度と経度の分解能を設定します。分解能値を指定しない場合、10 m のデフォルト値が緯度と経度の分解能パラメータに適用されます。緯度と経度の場合、分解能の単位はメートルで測定されます。分解能の値は小数単位でも指定できます。
- **default**：デフォルトの属性によって、地理的位置を設定します。
- **exit**：地理的ロケーション コンフィギュレーション モードを終了します。
- **no**：指定された地理的パラメータを拒否し、デフォルト値を設定します。

ロケーション TLV を無効にするには、**no lldp med-tlv-select location information** インターフェイス コンフィギュレーション コマンドを使用します。デフォルトでは、ロケーション TLV はイネーブルに設定されています。

次の例では、 スイッチに都市ロケーション情報を設定する方法を示します。

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(config-civic)# end
```

設定を確認するには、**show location civic-location** 特権 EXEC コマンドを入力します。

次の例では、 スイッチ上で緊急ロケーション情報を設定する方法を示します。

```
Switch(config)# location elin-location 14085553881 identifier 1
```

設定を確認するには、**show location elin** 特権 EXEC コマンドを入力します。

次に、スイッチに、地理空間ロケーション情報を設定する例を示します。

```
Switch(config)# location geo-location identifier host
Switch(config-geo)# latitude 12.34
Switch(config-geo)# longitude 37.23
Switch(config-geo)# altitude 5 floor
Switch(config-geo)# resolution 12.34
```

設定された地理空間的な場所の詳細を表示するには、**show location geo-location identifier** コマンドを使用します。

location algorithm

RSSI と SNR 値を平均するために使用するアルゴリズムを設定するには、グローバル コンフィギュレーション モードで **locationalgorithm** コマンドを使用します。RSSI と SNR 値を平均するために使用するアルゴリズムを削除するには、このコマンドの **no** 形式を使用します。

location algorithm {**rssi-average** |**simple**}
no location algorithm {**rssi-average** |**simple**}

構文の説明

rssi-average	より正確なアルゴリズムが指定されますが、CPU オーバーヘッドが増えます。
simple	CPU オーバーヘッドの少ない、より高速のアルゴリズムが指定されますが、精度が低くなります。

コマンド デフォルト

RSSI average

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、精度が高い一方、CPU オーバーヘッドが大きいアルゴリズムを設定する例を示します。

```
Switch# configure terminal
Switch(config)# location algorithm rssi-average
Switch(config)# end
```

location expiry

RSSI 値のタイムアウトを設定するには、グローバル コンフィギュレーション モードで **locationexpiry** コマンドを使用します。

location expiry {**calibrating-client |client |rogue-aps |tags** } *timeout-value*

構文の説明

calibrating-client	調整クライアントの RSSI タイムアウト値を指定します。
client	（任意）クライアントの RSSI タイムアウト値を指定します。
rogue-aps	不正アクセス ポイントの RSSI タイムアウト値を指定します。
tags	RFID タグの RSSI タイムアウト値を指定します。
timeout-value	調整クライアントに有効なタイムアウト パラメータ値の範囲は 1 ～ 3600 秒です。デフォルト値は 5 秒です。 クライアント、不正アクセス ポイント、RFID タグに有効なタイムアウト パラメータ値の範囲は 5 ～ 3600 秒です。デフォルト値は 5 秒です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、ワイヤレス クライアントの RSSI タイムアウト値を設定する例を示します。

```
Switch# configure terminal
Switch(config)# location expiry client 1000
Switch(config)# end
```

location notify-threshold

RSSI 測定の NMSP 通知しきい値を設定するには、グローバル コンフィギュレーション モードで **locationnotify-threshold** コマンドを使用します。RSSI 測定の NMSP 通知しきい値を削除するには、このコマンドの **no** 形式を使用します。

location notify-threshold {**client** |**rogue-aps** |**tags** } *db*
no location notify-threshold {**client** |**rogue-aps** |**tags** }

構文の説明

client	クライアントおよび不正クライアントの NMSP 通知しきい値（dB 単位）を指定します。 しきい値パラメータに有効な値の範囲は 0 ～ 10 dB です。デフォルト値は 0 dB です。
rogue-aps	不正アクセス ポイントの NMSP 通知しきい値（dB 単位）を指定します。 しきい値パラメータに有効な値の範囲は 0 ～ 10 dB です。デフォルト値は 0 dB です。
tags	RFID タグの NMSP 通知しきい値（dB 単位）を指定します。 しきい値パラメータに有効な値の範囲は 0 ～ 10 dB です。デフォルト値は 0 dB です。
db	しきい値パラメータに有効な値の範囲は 0 ～ 10 dB です。デフォルト値は 0 dB です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、クライアントの NMSP 通知しきい値を 10 dB に設定する例を示します。クライアント RSSI が差分 10 dB で変更されると同時に、通知 NMSP メッセージが MSE に送信されます。

```
Switch# configure terminal
Switch(config)# location notify-threshold client 10
Switch(config)# end
```

location plm calibrating

調整クライアントのパス損失測定（CCX S60）要求を設定するには、グローバル コンフィギュレーション モードで **locationplmcalibrating** コマンドを使用します。

location plm calibrating {**multiband** | **uniband**}

構文の説明

multiband	関連付けられた 802.11a または 802.11b/g 無線での調整クライアントのパス損失測定要求を指定します。
uniband	関連付けられた 802.11a/b/g 無線での調整クライアントのパス損失測定要求を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

単一の無線クライアントには、（無線がデュアルバンドで、2.4 GHz と 5 GHz の両方の帯域でも動作できるとしても）uniband が役立ちます。複数の無線クライアントには、multiband が役立ちます。

次に、関連付けられた 802.11a/b/g 無線での調整クライアントのパス損失測定要求を設定する例を示します。

```
Switch# configure terminal
Switch(config)# location plm calibrating uniband
Switch(config)# end
```

location rfid

ロケーションの RFID タグ トラッキングを設定するには、グローバル コンフィギュレーション モードで **locationrfid** コマンドを使用します。ロケーションの RFID タグ トラッキングを削除するには、このコマンドの **no** 形式を使用します。

location rfid { **status**|**timeout** *seconds*|**vendor-name** *name*}
no location rfid { **status**|**timeout** *seconds*|**vendor-name**}

構文の説明

status	RFID タグのロケーション トラッキングを有効にします。 **no location rfid status** コマンドはタグのロケーション トラッキングを無効にします。
timeout *seconds*	ロケーション RFID タイムアウト値を指定します。 この値は、検出された RFID ロケーション情報が有効と見なされる期間を決定します。設定された期間中に RSSI が変更されても（RSSI しきい値未満）、新しいロケーションは計算されず、メッセージが MSE に送信されます。 有効なタイムアウトの範囲は、60 ～ 7200 秒です。
vendor-name *name*	RFID タグ ベンダー名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

no location rfid status コマンドは、ロケーション RFID ステータスを無効にします。**no location rfid timeout** コマンドは、デフォルトのタイムアウト値に戻します。**no location rfid vendor-name** は、特定のベンダーのトラッキングを無効にします。

次に、スタティック RFID タグのデータ タイムアウトを設定する例を示します。

```
Switch# configure terminal
Switch(config)# location rfid timeout 1000
Switch(config)# end
```

location rssi-half-life

さまざまなデバイスのRSSI半減期を設定するには、グローバル コンフィギュレーション モードで **locationrssi-half-life** コマンドを使用します。さまざまなデバイスの RSSI 半減期を削除するには、このコマンドの **no** 形式を使用します。

location rssi-half-life {**calibrating-client |client |rogue-aps |tags** } *seconds*
no location rssi-half-life {**calibrating-client |client |rogue-aps |tags** }

構文の説明

calibrating-client	調整クライアントの RSSI 半減期を指定します。
client	クライアントの RSSI 半減期を指定します。
rogue-aps	不正アクセス ポイントの RSSI 半減期を指定します。
tags	RFID タグの RSSI 半減期を指定します。
seconds	半減期パラメータに有効な値は、0、1、2、5、10、20、30、60、90、120、180、または 300 秒です。デフォルト値は 0 秒です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、クライアントの RSSI 半減期値を 100 秒に設定する例を示します。

```
Switch# configure terminal
Switch(config)# location rssi-half-life client 100
Switch(config)# end
```

mac address-table move update

MACアドレステーブル移行更新機能を有効にするには、スイッチ スタックまたはスタンドアロン スイッチのグローバル コンフィギュレーション モードで **mac address-table move update** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac address-table move update {**receive** | **transmit**}
no mac address-table move update {**receive** | **transmit**}

構文の説明

receive	スイッチがMACアドレス テーブル移行更新メッセージを処理するように指定します。
transmit	プライマリ リンクがダウンし、スタンバイ リンクが起動した場合、スイッチがMACアドレス テーブル移行更新メッセージをネットワークの他のスイッチに送信するように指定します。

コマンド デフォルト

デフォルトでは、MACアドレステーブル移行更新機能はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

MACアドレステーブル移行更新機能により、プライマリ（フォワーディング）リンクがダウンし、スタンバイ リンクがトラフィックのフォワーディングを開始した場合、スイッチは高速双方向コンバージェンスを提供できます。

プライマリ リンクがダウンし、スタンバイ リンクが起動した場合、アクセス スイッチがMACアドレステーブル移行更新メッセージを送信するように設定できます。アップリンク スイッチが、MACアドレステーブル移行更新メッセージを受信および処理するように設定できます。

例

次の例では、アクセス スイッチがMACアドレス テーブル移行更新メッセージを送信するように設定する方法を示します。

```
Switch# configure terminal
Switch(config)# mac address-table move update transmit
Switch(config)# end
```

次の例では、アップリンク スイッチがMACアドレス テーブル移行更新メッセージを取得および処理するように設定する方法を示します。

```
Switch# configure terminal
```

```
Switch(config)# mac address-table move update receive
Switch(config)# end
```

show mac address-table move update 特権 EXEC コマンドを入力すると、設定を確認できます。

mgmt_init

イーサネット管理ポートを再初期化するには、ブートローダ モードで **mgmt_init** コマンドを使用します。

mgmt_init

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

イーサネット管理ポートのデバッグ中にのみ、**mgmt_init** コマンドを使用します。

例

次の例では、イーサネット管理ポートを初期化する方法を示します。

```
Switch: mgmt_init
```

mkdir

指定されたファイル システムに 1 つ以上のディレクトリを作成するには、ブート ローダ モードで **mkdir** コマンドを使用します。

mkdir *filesystem:/directory-url...*

構文の説明

filesystem:	ファイル システムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。
/directory-url...	作成するディレクトリの名前です。ディレクトリ名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ディレクトリ名では、大文字と小文字が区別されます。

スラッシュ（/）間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

例

次の例では、ディレクトリ Saved_Configs を作成する方法を示します。

```
Switch: mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```

関連トピック

dir （1028 ページ）
rmdir （1057 ページ）

more

1 つ以上のファイルの内容を表示するには、ブート ローダ モードで **more** コマンドを使用します。

more *filesystem:/file-url...*

構文の説明

filesystem:	ファイル システムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。
/file-url...	表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

ファイルのリストを指定した場合は、各ファイルの内容が順に表示されます。

例

次に、ファイルの内容を表示する例を示します。

```
Switch: more flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

nmsp notification interval

コントローラの Network Mobility Services Protocol（NMSP）通知間隔値をネットワークの遅延に対応するように変更するには、グローバル コンフィギュレーション モードで **nmspnotificationinterval** コマンドを使用します。

nmsp notification interval { **attachment** | **location** | **rssi** {**clients** | **rfid** | **rogues** {**ap** | **client** } } }

構文の説明

attachment	アタッチメント情報の集約に使用する時間を指定します。
location	ロケーション情報の集約に使用する時間を指定します。
rssi	RSSI 情報の集約に使用する時間を指定します。
clients	クライアントの時間間隔を指定します。
rfid	RFID タグの時間間隔を指定します。
rogues	不正APおよび不正クライアントの時間間隔を指定します。
ap	不正 AP の集約に使用する時間を指定します。
client	不正なクライアントの集約に使用する時間を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、アクティブな RFID タグの NMSP 通知間隔を 25 秒に設定する例を示します。

```
Switch# configure terminal
Switch(config)# nmsp notification-interval rfid 25
Switch(config)# end
```

次に、デバイスアタッチメント（ネットワークへの接続またはネットワークからの切断）の NMSP 通知間隔を 10 秒に変更する例を示します。

```
Switch# configure terminal
Switch(config)# nmsp notification-interval attachment 10
Switch(config)# end
```

次に、ロケーション パラメータ（ロケーション変更）の NMSP 通知間隔を 20 秒に設定する例を示します。

```
Switch# configure terminal
Switch(config)# nmsp notification-interval location 20
Switch(config)# end
```

no debug all

スイッチのデバッグを無効にするには、特権 EXEC モードで **no debug all** コマンドを使用します。

no debug all

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 16.1	このコマンドが導入されました。

例

次に、スイッチでデバッグを無効にする例を示します。

```
Switch: no debug all
All possible debugging has been turned off.
```

rename

ファイルの名前を変更するには、ブート コンフィギュレーション モードで**rename** コマンドを使用します。

rename *filesystem:/source-file-url filesystem:/destination-file-url*

構文の説明

filesystem:	ファイル システムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。
/source-file-url	元のパス（ディレクトリ）およびファイル名です。
/destination-file-url	新しいパス（ディレクトリ）およびファイル名です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

スラッシュ（/）間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

指定できるファイル名は最大127文字です。ファイル名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

例

次の例では、ファイル *config.text* の名前を *config1.text* に変更します。

```
Switch: rename usbflash0:config.text usbflash0:config1.text
```

ファイルの名前が変更されたかどうかを確認するには、**dir** *filesystem:* ブート ローダ コマンドを入力します。

reset

システムでハード リセットを実行するには、ブート ローダ モードで **reset** コマンドを使用します。ハードリセットを行うと、スイッチの電源切断後に電源を投入する手順と同様に、プロセッサ、レジスタ、およびメモリの内容が消去されます。

reset

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

例

次の例では、システムをリセットする方法を示します。

```
Switch: reset
Are you sure you want to reset the system (y/n)? y
System resetting...
```

関連トピック

reset （1056 ページ）
test cable-diagnostics tdr （1121 ページ）

rmdir

指定されたファイル システムから 1 つ以上の空のディレクトリを削除するには、ブート ローダ モードで **rmdir** コマンドを使用します。

rmdir *filesystem:/directory-url...*

構文の説明

filesystem:	ファイル システムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。
/directory-url...	削除する空のディレクトリのパス（ディレクトリ）および名前です。ディレクトリ名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スラッシュ（/）間に指定できるディレクトリ名は最大 45 文字で、大文字と小文字の区別があります。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、およびコロンは使用できません。

ディレクトリを削除する前に、まずディレクトリ内のファイルをすべて削除する必要があります。

スイッチは、各ディレクトリを削除する前に、確認を求めるプロンプトを出します。

例

次の例では、ディレクトリを 1 つ削除する方法を示します。

```
Switch: rmdir usbflash0:Test
```

ディレクトリが削除されたかどうかを確認するには、**dir** *filesystem:* ブート ローダ コマンドを入力します。

関連トピック

dir （1028 ページ）

sdm prefer

スイッチで使用する SDM テンプレートを指定するには、グローバル コンフィギュレーション モードで **sdm prefer** コマンドを使用します。

sdm prefer
{**advanced**}

構文の説明

advanced	NetFlow などの高度な機能をサポートします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スイッチ スタックでは、すべてのスタック メンバが、アクティブなスイッチに保存された同一の SDM テンプレートを使用する必要があります。

新規スイッチがスタックに追加されると、アクティブ スイッチに保存された SDM コンフィギュレーションは、個々のスイッチに設定されているテンプレートを上書きします。

例

次に、高度なテンプレートを設定する例を示します。

```
Switch(config)# sdm prefer advanced
Switch(config)# exit
Switch# reload
```

関連トピック

show sdm prefer （1086 ページ）

set

環境変数を設定または表示するには、ブート ローダ モードで**set**コマンドを使用します。環境変数は、ブートローダまたはスイッチで稼働している他のソフトウェアを制御するために使用できます。

set *variable value*

構文の説明

variable value	*variable* および *value* の適切な値には、次のいずれかのキーワードを使用します。
	MANUAL_BOOT：スイッチの起動を自動で行うか手動で行うかどうかを決定します。
	有効な値は 1/Yes と 0/No です。0 または No に設定されている場合、ブート ローダはシステムを自動的に起動します。他の値に設定されている場合は、ブート ローダ モードから手動でスイッチを起動する必要があります。
	BOOT *filesystem:/file-url*：自動起動時にロードおよび実行される実行可能ファイルのセミコロン区切りリストを識別します。
	BOOT 環境変数が設定されていない場合、システムは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT 変数が設定されていても、指定されたイメージをロードできなかった場合、システムはフラッシュ ファイル システムで最初に検出した起動可能なファイルを起動しようとします。
	ENABLE_BREAK：ユーザがコンソールの **Break** キーを押すと自動起動プロセスを中断できるようになります。
	有効な値は 1、Yes、On、0、No、および Off です。1、Yes、または On に設定されている場合は、フラッシュ ファイル システムの初期化後にコンソール上で Break キーを押すことで、自動起動プロセスを中断できます。
	HELPER *filesystem:/file-url*：ブート ローダの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストを識別します。ヘルパー ファイルは、ブートローダの機能を拡張したり、パッチを当てたりします。
	PS1 *prompt*：ブート ローダ モードの場合に、コマンドライン プロンプトとして使用する文字列を指定します。
	CONFIG_FILE flash: */file-url*：Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名を指定します。

BAUD *rate*：コンソールのボー レートに使用するビット数/秒（b/s）を指定します。コンフィギュレーションファイルに別の設定が指定されていない限り、Cisco IOS ソフトウェアはブートローダからボー レート設定を継承し、この値を引き続き使用します。指定できる範囲は 0 ～ 128000 b/s です。有効値は、50、75、110、150、300、600、1200、1800、2000、2400、3600、4800、7200、9600、14400、19200、28800、38400、56000、57600、115200、および 128000 です。

最も一般的な値は、300、1200、2400、9600、19200、57600、および 115200 です。

SWITCH_NUMBER *stack-member-number*：スタック メンバのメンバ番号を変更します。

SWITCH_PRIORITY *priority-number*：スタック メンバのプライオリティ値を変更します。

コマンド デフォルト

環境変数のデフォルト値は、次のとおりです。

MANUAL_BOOT: No (0)

BOOT：ヌル ストリング

ENABLE_BREAK：No（Off または 0）（コンソール上で Break キーを押して自動起動プロセスを中断することはできません）。

HELPER: デフォルト値はありません（ヘルパー ファイルは自動的にロードされません）。

PS1 スイッチ：

CONFIG_FILE: config.text

BAUD：9600 b/s

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1

（注） 値が設定された環境変数は、各ファイルのフラッシュ ファイル システムに保管されます。ファイルの各行には、環境変数名と等号に続いて、その変数の値が指定されます。

このファイルに表示されていない変数には値がありません。表示されていればヌル ストリングであっても値があります。ヌル ストリング（たとえば“”）が設定されている変数は、値が設定された変数です。

多くの環境変数は事前に定義されており、デフォルト値が設定されています。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

環境変数は大文字と小文字の区別があり、指定どおりに入力する必要があります。

値を持つ環境変数は、フラッシュ ファイル システムの外にあるフラッシュ メモリに保管されます。

通常の環境では、環境変数の設定を変更する必要はありません。

MANUAL_BOOT 環境変数は、**boot manual** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

BOOT 環境変数は、**boot system** *filesystem:/file-url* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

ENABLE_BREAK 環境変数は、**boot enable-break** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

HELPER 環境変数は、**boot helper** *filesystem: / file-url* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

CONFIG_FILE 環境変数は、**boot config-file flash:** */file-url* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

SWITCH_NUMBER 環境変数は、**switch** *current-stack-member-number***renumber** *new-stack-member-number* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

SWITCH_PRIORITY 環境変数は、スイッチ*stack-member-number***priority** *priority-number* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

ブート ローダのプロンプト ストリング（PS1）には、等号（=）を除く、出力可能な文字列を 120 文字まで指定できます。

例

次に、SWITCH_PRIORITY 環境変数を設定する例を示します。

```
Switch: set SWITCH_PRIORITY 2
```

設定を確認するには、**set** ブート ローダ コマンドを使用します。

関連トピック

reset （1056 ページ）
unset （1132 ページ）

show ap name config general

MA アクセス ポイントの詳細を表示するには、 **show ap name config general** コマンドを使用します。

show ap name *ap-name ma-ip***config general**

構文の説明

ap-name	アクセス ポイント名。
ma-ip	MA IPv4 アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.3E	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、MC でのみ動作します。

例

次に、MA アクセス ポイントの詳細を表示する例を示します。

```
Cisco controller# show ap name AP5 211.0.0.4 config general

Cisco AP Name                                   : AP5
Cisco AP Identifier                             : 0
Country Code                                    : US  - United States
Regulatory Domain Allowed by Country            : 802.11bg:-A     802.11a:-AB
AP Country Code                                 : US  - United States
AP Regulatory Domain
  Slot 0                                        : -A
  Slot 1                                        : -A
Switch Port Number                              : Gi1/0/5
MAC Address                                     : 6c20.56e1.4a57
IP Address Configuration                        : DHCP
IP Address                                      : 211.0.0.170
IP Netmask                                      : 255.255.255.0
Gateway IP Address                              : 211.0.0.100
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Disabled
SSH State                                       : Disabled
Jumbo MTU Status                                : Disabled
Cisco AP Location                               : default location
Cisco AP Group Name                             : default-group
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : Local
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : informational
Software Version                                : 10.3.123.92
Boot Version                                    : 12.4.23.0
```

```
Stats Reporting Period                          : 180
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : PoE/Full Power (normal mode)
Number of Slots                                 : 2
AP Model                                        : AIR-CAP3602I-A-K9
AP Image                                        : C3600-K9W8-M
IOS Version                                     : 15.3(20151222:165605)$
Reset Button                                    : Enabled
AP Serial Number                                : FGL1645W0W1
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : cisco
AP 802.1X User Mode                             : Not Configured
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 23 minutes 53 seconds
AP CAPWAP Up Time                               : 21 minutes 53 seconds
Join Date and Time                              : 01/18/2016 02:36:09
Join Taken Time                                 : 1 minute 59 seconds
Ethernet Port Duplex                            : Auto
Ethernet Port Speed                             : Auto
AP Link Latency                                 : Disabled
Rogue Detection                                 : Enabled
AP TCP MSS Adjust                               : Disabled
AP TCP MSS Size                                 : 0
AP IPv6 TCP MSS Adjust                          : Disabled
AP IPv6 TCP MSS Size                            : 1220
```

show avc client

上位アプリケーションの数に関する情報を表示するには、特権 EXEC モードで **show avc client** コマンドを使用します。

show avc client *client-mac* **top** *n* **application**［**aggregate** | **upstream** | **downstream**］

構文の説明

client*client-mac*	クライアントの MAC アドレスを指定します。
top*n***application**	特定のクライアントの上位「N」個のアプリケーションの数を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、**show avc client** コマンドの出力例を示します。

```
Switch# sh avc client 0040.96ae.65ec top 10 application aggregate

Cumulative Stats:

No.  AppName      Packet-Count    Byte-Count       AvgPkt-Size     usage%
---------------------------------------------------------------------------
1    skinny          7343           449860           61              94
2    unknown         99             13631            137             3
3    dhcp            18             8752             486             2
4    http            18             3264             181             1
5    tftp            9              534              59              0
6    dns             2              224              112             0

Last Interval(90 seconds) Stats:

No.  AppName     Packet-Count     Byte-Count       AvgPkt-Size      usage%
---------------------------------------------------------------------------
1    skinny          9               540              60               100
```

show avc wlan

上位のアプリケーションおよびそれらのアプリケーションを使用しているユーザに関する情報を表示するには、特権 EXEC モードで **show avc wlan** コマンドを使用します。

show avc wlan *ssid* **top** *n* **application**［**aggregate** | **upstream** | **downstream**］

構文の説明

wlan *ssid*	WLANのサービスセット識別子（SSID）を指定します。
top *n* **application**	上位「N」個のアプリケーションの数を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、**show avc wlan** コマンドの出力例を示します。

```
Switch# show avc wlan Lobby_WLAN top 10 application aggregate

Cumulative Stats:

No.  AppName            Packet-Count          Byte-Count          AvgPkt-Size  usage%
-------------------------------------------------------------------------------------
1    ssl                10598677              1979525706            997          42
2    vnc                5550900               3764612847            678          14
3    http               3043131               2691327197            884          10
4    unknown            1856297               1140264956            614          4
5    video-over-http    1625019               2063335150            1269         8
6    binary-over-http   1329115               1744190344            1312         6
7    webex-meeting      1146872               540713787             471          2
8    rtp                923900                635650544             688          2
9    unknown            752341                911000213             1210         3
10   youtube            631085                706636186             1119         3

Last Interval(90 seconds) Stats:

No.  AppName           Packet-Count          Byte-Count            AvgPkt-Size  usage%
-------------------------------------------------------------------------------------
1    vnc                687093                602731844             877          68
2    video-over-http    213272                279831588             1312         31
3    ssl                6515                  5029365               771          1
4    webex-meeting      3649                  1722663               472          0
5    http               2634                  1334355               506          0
6    unknown            1436                  99412                 69           0
7    google-services    722                   378121                523          0
8    linkedin           655                   393263                600          0
9    exchange           432                   167390                387          0
10   gtalk-chat         330                   17330                 52           0
```

show cable-diagnostics tdr

タイム ドメイン反射率計（TDR）の結果を表示するには、特権 EXEC モードで **show cable-diagnostics tdr** コマンドを使用します。

show cable-diagnostics tdr interface *interface-id*

構文の説明

interface-id	TDR が実行されているインターフェイスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

TDR は、銅線のイーサネット 10/100/100 ポートだけでサポートされます。10 ギガビット イーサネット ポート、および Small Form-Factor Pluggable（SFP）モジュール ポートではサポートされません。

例

次の例では、スイッチ での **show cable-diagnostics tdr interface** *interface-id* コマンドの出力を示します。

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/0/23
  TDR test last run on: March 01 00:04:08
  Interface  Speed  Local pair  Pair length         Remote pair   Pair status
  ---------- ----- ---------- ------------------ ----------- --------------------
  Gi1/0/23   1000M  Pair A      1    +/- 1 meters   Pair A        Normal
                    Pair B      1    +/- 1 meters   Pair B        Normal
                    Pair C      1    +/- 1 meters   Pair C        Normal
                    Pair D      1    +/- 1 meters   Pair D        Normal
```

表 *34 : show cable-diagnostics tdr* コマンドで出力されるフィールドの説明

フィールド	説明
インターフェイス	TDR が実行されているインターフェイス。
速度	接続速度。
Local pair	ローカル インターフェイスで TDR がテストを実行するワイヤ ペア名。

フィールド	説明
Pair length	スイッチ に関するケーブルの問題の場所。次のいずれかの場合に限り、TDR は場所を特定できます。 • ケーブルが正しく接続され、リンクがアップ状態で、インターフェイス速度が 1000 Mb/s である場合 • ケーブルが断線している場合 • ケーブルがショートしている場合
Remote pair	ローカル ペアが接続されたワイヤ ペア名。ケーブルが正しく接続されリンクがアップ状態である場合だけ、TDR はリモート ペアについて確認します。
Pair status	TDR が実行されているワイヤ ペアのステータス • Normal：ワイヤ ペアが正しく接続されています。 • Not completed：テストは実行中で、完了していません。 • Not supported：インターフェイスは TDR をサポートしません。 • Open：ワイヤ ペアが断線しています。 • Shorted：ワイヤ ペアがショートしています。 • ImpedanceMis：インピーダンスが一致しません。 • Short/Impedance Mismatched：インピーダンスが一致しないかケーブルがショートしています。 • InProgress：診断テストが進行中です。

次の例では、TDR が実行されているときの **show interface** *interface-id* コマンドの出力を示します。

```
Switch# show interface gigabitethernet1/0/2
  gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

次の例では、TDR が実行されているときの **show cable-diagnostics tdr interface** *interface-id* コマンドの出力を示します。

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/0/2
  % TDR test was never issued on gigabitethernet1/0/2
```

インターフェイスでTDRがサポートされない場合、次のメッセージが表示されます。

```
% TDR test is not supported on スイッチ 1
```

関連トピック

test cable-diagnostics tdr （1121 ページ）

show debug

スイッチで使用できるすべての debug コマンドを表示するには、特権 EXEC モードで **show debug** コマンドを使用します。

show debug

show debug condition *Condition identifier* | *All conditions*

構文の説明

Condition identifier	使用される条件識別子の値を設定します。範囲は、1 ～ 1000 です。
All conditions	使用可能なすべての条件付きデバッグ オプションを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 16.1	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、debug コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、debug コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用するのが最良です。このような時間帯を選んでデバッグを実行すると、debug コマンドの処理の負担によってシステム利用が影響を受ける可能性が少なくなります。

例

次に、**show debug** コマンドの出力例を示します。

```
Switch# show debug condition all
```

デバッグを無効にするには、**no debug all** コマンドを使用します。

show env

スイッチ（スタンドアロンスイッチ、スタックマスター、またはスタックメンバ）のファン、温度、および電源情報を表示するには、EXEC モードで **show env** コマンドを使用します。

show env { **all** | **fan** | **power** [**all** | **switch** [*switch-number*]] | **stack** [*stack-number*] | **temperature** [**status**] }

構文の説明

all	ファン、温度、および電源環境のステータスを表示します。
fan	スイッチのファンの状態を表示します。
power	電源装置のステータスを表示します。
all	（任意）すべての電源装置のステータスを表示します。
switch *switch-number*	（任意）特定のスイッチの電源装置のステータスを表示します。
stack *switch-number*	（任意）スタックの各スイッチまたは指定されたスイッチのすべての環境ステータスを表示します。指定できる範囲は、スタック内のスイッチメンバ番号に従って 1 ～ 9 です。
temperature	スイッチの温度ステータスを表示します。
status	（任意）温度ステータスとしきい値を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

任意のメンバスイッチからスタック内のスイッチに関する情報を表示するには、**show env stack** [*switch-number*] コマンドを使用します。

スイッチの温度ステータスとしきい値レベルを表示するには、**show env temperature status** コマンドを使用します。

例

次の例では、マスター スイッチからスタック メンバ 1 に関する情報を表示する方法を示します。

```
Switch> show env stack 1
Switch :1
Switch 1 Fan 1 is OK
Switch 1 Fan 2 is OK
Switch 1 Fan 3 is OK
FAN-PS1 is OK
FAN-PS2 is NOT PRESENT
Switch 1: SYSTEM TEMPERATURE is OK
Inlet Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 46 Degree Celsius
Red Threshold : 56 Degree Celsius

Hotspot Temperature Value: 43 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 105 Degree Celsius
Red Threshold : 125 Degree Celsius

Switch>
```

次に、温度値、状態、およびしきい値を表示する例を示します。

```
Switch> show env temperature status
Temperature Value: 26 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 46 Degree Celsius
Red Threshold : 56 Degree Celsius

Hotspot Temperature Value: 43 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 105 Degree Celsius
Red Threshold : 125 Degree Celsius

Switch>
```

例

次の例では、マスター スイッチからスタック メンバ 1 に関する情報を表示する方法を示します。

```
Switch> show env stack 1
Switch 1:
Switch Fan 1 is OK
Switch Fan 2 is OK
Switch Fan 3 is OK
FAN-PS1 is OK
FAN-PS2 is NOT PRESENT
Switch 1: SYSTEM TEMPERATURE is OK
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
```

```
Red Threshold : 56 Degree Celsius

Switch>
```

次に、温度値、状態、およびしきい値を表示する例を示します。

```
Switch> show env temperature status
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius

Switch>
```

表 *35 : show env temperature status* コマンド出力のステート

状態	説明
グリーン	スイッチの温度が正常な動作範囲にあります。
黄色	温度が警告範囲にあります。スイッチの外の周辺温度を確認する必要があります。
赤	温度がクリティカル範囲にあります。温度がこの範囲にある場合、スイッチが正常に実行されない可能性があります。

show flow monitor

Flexible NetFlow フロー モニタのステータスと統計情報を表示するには、特権 EXEC モードで **showflowmonitor** コマンドを使用します。

show flow monitor [{**broker** [{**detail**|**picture**}]|[**name**] *monitor-name* [{**cache** [**format** {**csv**|**record**|**table**}]}]|**provisioning**|**statistics**}]

構文の説明

broker	（任意）フロー モニタのブローカの状態に関する情報を表示します。
detail	（任意）フロー モニタのブローカに関する詳細情報を表示します。
picture	（任意）ブローカ状態の画像を表示します。
name	（任意）フロー モニタの名前を指定します。
monitor-name	（任意）事前に設定されたフロー モニタの名前。
cache	（任意）フロー モニタのキャッシュの内容を表示します。
format	（任意）ディスプレイ出力のフォーマット オプションのいずれかを使用することを指定します。
csv	（任意）フロー モニタのキャッシュの内容をカンマ区切り値（CSV）形式で表示します。
record	（任意）フロー モニタのキャッシュの内容をレコード形式で表示します。
table	（任意）フロー モニタのキャッシュの内容を表形式で表示します。
provisioning	（任意）フロー モニタのプロビジョニング情報を表示します。
statistics	（任意）フロー モニタの統計情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

cache キーワードでは、デフォルトでレコード形式が使用されます。

showflowmonitor *monitor-name* **cache** コマンドのディスプレイ出力に含まれる大文字のフィールド名は、フローの識別に Flexible NetFlow が使用するキー フィールドです。**showflowmonitor** *monitor-name* **cache** コマンドのディスプレイ出力に含まれる小文字のフィールド名は、Flexible NetFlow がキャッシュの追加データとして値を収集する非キー フィールドです。

例

次の例では、フロー モニタのステータスを表示します。

```
Switch# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic traffic analysis
  Flow Record:       flow-record-1
  Flow Exporter:     flow-exporter-1
                     flow-exporter-2
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 311316 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *36 : show flow monitor monitor-name* フィールドの説明

フィールド	説明
フロー モニタ	設定したフロー モニタの名前。
説明	モニタに設定した説明、またはユーザ定義のデフォルトの説明。
フロー レコード	フロー モニタに割り当てられたフロー レコード。
Flow Exporter	フロー モニタに割り当てられたエクスポータ。
Cache	フロー モニタのキャッシュに関する情報。
タイプ	フロー モニタのキャッシュ タイプ。この値は常に normal となります。これが唯一サポートされているキャッシュ タイプです。
Status（ステータス）	フロー モニタのキャッシュのステータス。 次の値が可能です。 • allocated：キャッシュが割り当てられています。 • being deleted：キャッシュが削除されています。 • not allocated：キャッシュが割り当てられていません。
サイズ	現在のキャッシュ サイズ。
Inactive Timeout	非アクティブ タイムアウトの現在の値（秒単位）。
Active Timeout	アクティブ タイムアウトの現在の値（秒単位）。

次の例では、FLOW-MONITOR-1 という名前のフロー モニタのステータス、統計情報、およびデータを表示します。

```
Switch# show flow monitor FLOW-MONITOR-1 cache
  Cache type:                               Normal (Platform cache)
  Cache size:                               Unknown
  Current entries:                                1

  Flows added:                                    3
  Flows aged:                                     2
    - Active timeout      (   300 secs)           2

DATALINK MAC SOURCE ADDRESS INPUT:       0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:  6400.F125.59E6
IPV6 SOURCE ADDRESS:                     2001:DB8::1
IPV6 DESTINATION ADDRESS:                2001:DB8:1::1
TRNS SOURCE PORT:                        1111
TRNS DESTINATION PORT:                   2222
IP VERSION:                              6
IP PROTOCOL:                             6
IP TOS:                                  0x05
IP TTL:                                  11
tcp flags:                               0x20
counter bytes long:                      132059538
counter packets long:                    1158417
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *37 : show flow monitor monitor-name cache* フィールドの説明

フィールド	説明
Cache type	フローモニタのキャッシュ タイプ。この値は常にnormalとなります。これが唯一サポートされているキャッシュ タイプです。
Cache Size	キャッシュ内のエントリ数。
Current entries	キャッシュ内の使用中のエントリ数。
Flows added	キャッシュの作成後にキャッシュに追加されたフロー
Flows aged	キャッシュの作成後に期限切れになったフロー
Active timeout	アクティブ タイムアウトの現在の値（秒単位）。
Inactive timeout	非アクティブ タイムアウトの現在の値（秒単位）。
DATALINK MAC SOURCE ADDRESS INPUT	入力パケットの MAC 送信元アドレス。
DATALINK MAC DESTINATION ADDRESS INPUT	入力パケットの MAC 宛先アドレス。
IPV6 SOURCE ADDRESS	IPv6 送信元アドレスです。
IPV6 DESTINATION ADDRESS	IPv6 宛先アドレス。
TRNS SOURCE PORT	トランスポート プロトコルの送信元ポート。

フィールド	説明
TRNS DESTINATION PORT	トランスポート プロトコルの宛先ポート。
IP VERSION	IP バージョン。
IP PROTOCOL	プロトコル番号。
IP TOS	IP タイプ オブ サービス（ToS）の値。
IP TTL	IP 存続可能時間（TTL）の値。
tcp flags	TCP フラグの値。
counter bytes	カウントされたバイト数。
counter packets	カウントされたパケット数。

次の例では、FLOW-MONITOR-1 という名前のフロー モニタのステータス、統計情報、およびデータを表形式で表示します。

```
Switch# show flow monitor FLOW-MONITOR-1 cache format table
  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               1

  Flows added:                                   3
  Flows aged:                                    2
    - Active timeout      (   300 secs)          2

DATALINK MAC SRC ADDR INPUT  DATALINK MAC DST ADDR INPUT  IPV6 SRC ADDR  IPV6 DST ADDR
 TRNS SRC PORT  TRNS DST PORT  IP VERSION  IP PROT  IP TOS  IP TTL  tcp flags  bytes
long  pkts long
===========================  ===========================  =============  =============
 =============  =============  ==========  =======  ======  ======  =========  ==========
  =========
0000.0000.1000               6400.F125.59E6               2001:DB8::1    2001:DB8:1::1
          1111           2222           6        6  0x05        11  0x20        132059538
    1158417
```

次の例では、FLOW-MONITOR-IPv6 という名前のフロー モニタ（キャッシュに IPv6 データを格納）のステータス、統計情報、およびデータをレコード形式で表示します。

```
Switch# show flow monitor name FLOW-MONITOR-IPv6 cache format record
  Cache type:                                Normal (Platform cache)
  Cache size:                               Unknown
  Current entries:                                1

  Flows added:                                    3
  Flows aged:                                     2
    - Active timeout      (   300 secs)           2

DATALINK MAC SOURCE ADDRESS INPUT:       0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:  6400.F125.59E6
IPV6 SOURCE ADDRESS:                     2001::2
IPV6 DESTINATION ADDRESS:                2002::2
TRNS SOURCE PORT:                        1111
TRNS DESTINATION PORT:                   2222
```

```
IP VERSION:                             6
IP PROTOCOL:                            6
IP TOS:                                 0x05
IP TTL:                                 11
tcp flags:                              0x20
counter bytes long:                     132059538
counter packets long:                   1158417
```

次の例では、フロー モニタのステータスと統計情報を表示します。

```
Switch# show flow monitor FLOW-MONITOR-1 statistics
  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               1

  Flows added:                                   3
  Flows aged:                                    2
    - Active timeout      (   300 secs)          2
```

show license right-to-use

スイッチにインストールされている apcount adder ライセンスの詳細情報を表示するには、EXEC モードで **show license right-to-use** コマンドを使用します。

show license right-to-use {**default** |**detail** |**eula** |**mismatch** |**slot** |**summary** |**usage**}

構文の説明

default	デフォルトのライセンス情報を表示します。
detail	スタック内のすべてのライセンスの詳細を表示します。
eula	EULA テキストを表示します。
mismatch	一致しないライセンス情報を表示します。
slot	スイッチ番号を指定します。
summary	スタック全体の統合ライセンス情報を表示します。
usage	すべてのライセンスの使用状況の詳細を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show license right-to-use usage** コマンドの出力例として、すべての詳細情報を表示します。

```
Switch# show license right-to-use usage

 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
--------------------------------------------------------------------------
 1      ipservices     permanent    0 :0 :1                yes   yes
 1      ipbase         permanent    0 :0 :0                no    no
 1      ipbase         evaluation   0 :0 :0                no    no
 1      lanbase        permanent    0 :0 :7                no    yes
 1      apcount        evaluation   0 :0 :0                no    no
 1      apcount        base         0 :0 :0                no    no
 1      apcount        adder        0 :0 :0                no    yes
 1      apcount        adder        0 :0 :0                no    yes
 1      apcount        adder        0 :0 :0                no    yes
 1      apcount        adder        0 :0 :0                no    yes
```

```
 1      apcount        adder        0 :0 :0               no     yes

Switch#
```

次に、**show license right-to-use detail** コマンドの出力例として、ライセンスの詳細情報を表示します。

```
Switch# show license right-to-use detail

Index 1:  License Name: apcount
           Period left: 16
           License Type: evaluation
           License State: Not Activated
           License Count: 1000
           License Location: Slot 1
Index 2:  License Name: apcount
           Period left: Lifetime
           License Type: adder
           License State: Active, In use
           License Count: 125
           License Location: Slot 1
```

次に、評価ライセンスがアクティブな場合の **show license right-to-use summary** コマンドの出力例を示します。

```
Switch# show license right-to-use summary
  License Name    Type     Count   Period left
-----------------------------------------------
  apcount      evaluation  1000     50

-----------------------------------------------

Evaluation AP-Count: Enabled
Total AP Count Licenses: 1000
AP Count Licenses In-use: 100
AP Count Licenses Remaining: 900
```

次に、adder ライセンスがアクティブな場合の **show license right-to-use summary** コマンドの出力例を示します。

```
Switch# show license right-to-use summary
  License Name    Type     Count   Period left
-----------------------------------------------
apcount      adder       125      Lifetime

-----------------------------------------------

Evaluation AP-Count: Disabled
Total AP Count Licenses: 125
AP Count Licenses In-use: 100
AP Count Licenses Remaining: 25
```

show location

ロケーション情報を表示するには、特権 EXEC モードで **show location** コマンドを使用します。

show location {**detail** *mac-addr*|**plm**|**statistics**| **summary** **rfid**|**rfid** {**client**|**config**|**detail** *mac-addr*|**summary**}}

構文の説明

detail *mac-addr*	特定のクライアントの RSSI テーブルとともに詳細なロケーション情報を表示します。
plm	ロケーション パス損失測定（CCX S60）の設定を表示します。
statistics	ロケーションベースのシステム統計情報を表示します。
summary	ロケーションベースのシステム概要情報を表示します。
rfid	RFID タグ トラッキング情報を表示します。
client	クライアントである RFID タグの概要を表示します。
config	RFID タグ トラッキングの設定オプションを表示します。
detail *mac-addr*	1 つの RFID タグの詳細情報を表示します。
summary	既知のすべての RFID タグの概要情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show location plm** コマンドの出力例を示します。

```
Switch# show location plm
Location Path Loss Configuration

Calbration client      : Disabled, Radio: Multiband
Normal clients         : Disabled
Burst interval         : 60
```

show location ap-detect

指定されたアクセスポイントで検出されたロケーション情報を表示するには、特権EXECモードで **show location ap-detect** コマンドを使用します。

show location ap-detect {**all**|**client**|**rfid**|**rogue-ap**|**rogue-client**} *ap-name*

構文の説明

all	クライアント、RFID、不正アクセスポイント、不正クライアントの情報を表示します。
client	クライアント情報を表示します。
rfid	RFID 情報を表示します。
rogue-ap	不正アクセス ポイントの情報を表示します。
rogue-client	不正クライアントの情報を表示します。
ap-name	特定のアクセス ポイント名。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show location ap-detect client** コマンドの出力例を示します。

```
Switch# show location ap-detect client AP02
Clients

MAC Address       Status            Slot  Antenna     RSSI
------------------------------------------------------------
2477.0389.96ac    Associated           1        0      -60
2477.0389.96ac    Associated           1        1      -61
2477.0389.96ac    Associated           0        0      -46
2477.0389.96ac    Associated           0        1      -41


RFID Tags


Rogue AP's


Rogue Clients

MAC Address         State               Slot     Rssi
------------------------------------------------------------
```

```
0040.96b3.bce6      Alert               1        -58
586d.8ff0.891a      Alert               1        -72
```

show mac address-table move update

スイッチ上のMACアドレステーブル移動更新情報を表示するには、EXECモードで**show mac address-table move update** コマンドを使用します。

show mac address-table move update

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

例

次の例では、**show mac address-table move update** コマンドの出力を示します。

```
Switch# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

show nmsp

Network Mobility Services Protocol（NMSP）構成の設定を表示するには、**shownmsp** コマンドを使用します。

show nmsp {**attachment** |{**suppress interfaces**}|**capability**|**notification interval**|**statistics** {**connection**|**summary**}|**status**|**subscription detail** ［*ip-addr* ］|**summary**}

構文の説明

attachmentsuppressinterfaces	アタッチメント抑制インターフェイスを表示します。
capability	NMSP 機能を表示します。
notificationinterval	NMSP 通知間隔を表示します。
statisticsconnection	すべての接続別カウンタを表示します。
statisticssummary	NMSP カウンタを表示します。
status	アクティブな NMSP 接続のステータスを表示します。
subscriptiondetail *ip-addr*	特定の IP アドレスでサブスクライブされている NMSP サービスについてのみ詳細を表示します。
subscriptionsummary	コントローラがサブスクライブされているすべての NMSP サービスの詳細を表示します。特定の IP アドレスでサブスクライブされている NMSP サービスについてのみ詳細を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show nmsp notification interval** コマンドの出力例を示します。

```
Switch#  show nmsp notification interval
NMSP Notification Intervals
---------------------------

RSSI Interval:
 Client               : 2 sec
 RFID                 : 2 sec
 Rogue AP             : 2 sec
```

```
 Rogue Client          : 2 sec
Attachment Interval    : 30 sec
Location Interval      : 30 sec
```

show sdm prefer

特定の機能用のシステム リソースを最大にするために使用できるテンプレートに関する情報を表示するには、特権 EXEC モードで **show sdm prefer** コマンドを使用します。現在のテンプレートを表示するには、キーワードを指定せずにコマンドを使用します。

show sdm prefer［**advanced**］

構文の説明

advanced	（任意）高度なテンプレートに関する情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

sdm prefer グローバル コンフィギュレーション コマンドを入力後にスイッチをリロードしていない場合、**show sdm prefer** 特権 EXEC コマンドでは、新しく設定されたテンプレートでなく現在使用中のテンプレートが表示されます。

各テンプレートで表示される番号は、各機能のリソースにおけるおおよその最大数になります。他に設定された機能の実際の数字にもよるため、実際の数字とは異なる場合があります。たとえば、スイッチに 16 を超えるルーテッド インターフェイス（サブネット VLAN）がある場合、デフォルトのテンプレートでは、可能なユニキャスト MAC アドレスの数は 6000 未満になることがあります。

例

次に、**show sdm prefer** コマンドの出力例を示します。

```
Switch# show sdm prefer

Showing SDM Template Info

This is the Advanced template.
 Number of VLANs:                                4094
 Unicast MAC addresses:                          32768
 Overflow Unicast MAC addresses:                 512
 IGMP and Multicast groups:                      8192
 Overflow IGMP and Multicast groups:             512
 Directly connected routes:                      32768
 Indirect routes:                                7680
 Security Access Control Entries:                3072
 QoS Access Control Entries:                     3072
 Policy Based Routing ACEs:                      1024
 Netflow ACEs:                                   1024
 Input Microflow policer ACEs:                   256
```

```
 Output Microflow policer ACEs:                  256
 Flow SPAN ACEs:                                 256
 Tunnels:                                        256
 Control Plane Entries:                          512
 Input Netflow flows:                           8192
 Output Netflow flows:                         16384
 SGT/DGT entries:                               4096
 SGT/DGT Overflow entries:                       512
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.

Switch#
```

関連トピック

sdm prefer （1058 ページ）

show tech-support wireless

Cisco Technical Assistance Center（TAC）によって頻繁に要求されるシスコ ワイヤレス LAN コントローラの変数を表示するには、特権 EXEC モードで **show tech-support wireless** コマンドを使用します。

show tech-support wireless

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show tech-support wireless** コマンドの出力例を示します。

```
Switch# show tech-support wireless
 *** show ap capwap timers ***

Cisco AP CAPWAP timers

AP Discovery timer       : 10
AP Heart Beat timeout    : 30
Primary Discovery timer  : 120
Primed Join timeout      : 0
Fast Heartbeat           : Disabled
Fast Heartbeat timeout   : 1
*** show ap capwap retransmit ***
Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                          Retransmit Interval             Retransmit Count
-----------------------------------------------------------------------------------------
TSIM_AP-2                        3                               5
TSIM_AP-3                        3                               5
*** show ap dot11 24ghz cleanair air-quality summary ***

AQ = Air Quality
DFS = Dynamic Frequency Selection

*** show ap dot11 24ghz cleanair air-quality worst ***

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-------------------------------------------------------------
                    0         0       0       0            No
*** show ap dot11 24ghz cleanair config ***

Clean Air Solution................................ : Disabled
Air Quality Settings:
    Air Quality Reporting........................ : Disabled
```

```
    Air Quality Reporting Period (min)..... : 15
    Air Quality Alarms..................... : Enabled
    Air Quality Alarm Threshold............ : 10
Interference Device Settings:
    Interference Device Reporting.......... : Enabled
        Bluetooth Link..................... : Enabled
        Microwave Oven..................... : Enabled
        802.11 FH.......................... : Enabled
        Bluetooth Discovery................ : Enabled
        TDD Transmitter.................... : Enabled
        Jammer............................. : Enabled
        Continuous Transmitter............. : Enabled
        DECT-like Phone.................... : Enabled
        Video Camera....................... : Enabled
        802.15.4........................... : Enabled
        WiFi Inverted...................... : Enabled
        WiFi Invalid Channel............... : Enabled
        SuperAG............................ : Enabled
        Canopy............................. : Enabled
        Microsoft Device................... : Enabled
        WiMax Mobile....................... : Enabled
        WiMax Fixed........................ : Enabled
    Interference Device Types Triggering Alarms:
        Bluetooth Link..................... : Disabled
        Microwave Oven..................... : Disabled
        802.11 FH.......................... : Disabled
        Bluetooth Discovery................ : Disabled
        TDD Transmitter.................... : Disabled
        Jammer............................. : Disabled
        Continuous Transmitter............. : Disabled
        DECT-like Phone.................... : Disabled
        Video Camera....................... : Disabled
  802.15.4............................... : Disabled
        WiFi Inverted...................... : Enabled
        WiFi Invalid Channel............... : Enabled
        SuperAG............................ : Disabled
        Canopy............................. : Disabled
        Microsoft Device................... : Disabled
        WiMax Mobile....................... : Disabled
        WiMax Fixed........................ : Disabled
    Interference Device Alarms............. : Enabled
Additional Clean Air Settings:
    CleanAir Event-driven RRM State........ : Disabled
    CleanAir Driven RRM Sensitivity........ : LOW
    CleanAir Persistent Devices state...... : Disabled
```

show wireless ap summary (MA)

ワイヤレス アクセス ポイント モビリティ エージェント（MA）の概要情報を表示するには、**show wireless ap summary** コマンドを使用します。

show wireless ap *ma-ip***summary**

構文の説明

ma-ip	MA IPv4 アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.3E	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、MC でのみ動作します。

例

次に、ワイヤレス アクセス ポイント MA の概要を表示する例を示します。

```
Cisco controller# show wireless ap 211.0.0.4 summary

Mobility Agent Access Point Summary:

Mobility Role                                  : Mobility Agent
Mobility Agent IP                              : 211.0.0.4
Mobility Switch Peer Group Name                : SPG1
Multicast Group IP Address                     : 0.0.0.0
Capwap Multicast Iif-Id                        : NA
Link Encryption                                : Disabled
Total AP Joined                                : 1
IOS Version                                    : Not Available
AP software version                            : 10.3.123.92

Codes U - Up, UR - Unregistered, D - Downloading, R - Registered
AP Up Time in hours:minutes:seconds

AP Name           AP Model  Port      IP Address      Radio(Ghz) State Radio MAC
AP UpTime   Clients
-------------------------------------------------------------------------------------------------
AP5               3602I     Gi1/0/5   211.0.0.170     2.4, 5     R     1ce6.c75b.3e70
00:21:06    0
```

show wireless ap summary

コントローラに認識されているアクセス ポイントの数を表示するには、**show wireless ap summary** コマンドを使用します。

show wireless ap summary

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.3E	このコマンドが導入されました。

次に、コントローラに認識されているアクセス ポイントの数を表示する例を示します。

```
Cisco controller# show wireless ap summary

Sub-Domain Access Point Summary

Maximum AP Limit: 100
Total AP License Installed: 60
Total AP License Available: 59
Total AP Joined: 1

AP UpTime in hours:minutes:seconds

HostName        Controller IP   AP name           AP Group        AP Model AP IP
    AP UpTime   Clients
-------------------------------------------------------------------------------------------------------
Switch          52.2.2.1        APd48c.b5e1.05bd  default-group   1142N    52.2.2.155
    452:37:01   0
```

show wireless band-select

バンドセレクト設定のステータスを表示するには、特権 EXEC モードで **show wireless band-select** コマンドを使用します。

show wireless band-select

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless band-select** コマンドの出力例を示します。

```
Switch# show wireless band-select
Band Select Probe Response    : per WLAN enabling
Cycle Count                   : 2
Cycle Threshold (millisec)    : 200
Age Out Suppression (sec)     : 20
Age Out Dual Band (sec)       : 60
Client RSSI (dBm)             : 80
```

show wireless client calls

スイッチのアクティブなコールまたは拒否されたコールの合計数を表示するには、特権EXECモードで **show wireless client calls** コマンドを使用します。

show wireless client calls {**active** | **rejected**}

構文の説明

active	アクティブなコールが表示されます。
rejected	拒否されたコールが表示されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless client calls** コマンドの出力例を示します。

```
スイッチ# show wireless client calls active

TSPEC Calls:

------------------------------------------------------------------------------
MAC Address     AP Name             Status               WLAN  Authenticated
------------------------------------------------------------------------------
0000.1515.000f    AP-2           Associated             1  Yes

SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a and 802.11b/g: 1
Number of Active SIP calls on 802.11a and 802.11b/g: 0
```

show wireless client dot11

特定の帯域（2.4 Ghz または 5 Ghz）のアクティブなコールまたは拒否されたコールの合計数を表示するには、特権 EXEC モードで **show wireless client dot11** コマンドを使用します。

show wireless client dot11 {**24ghz** | **5ghz**} **calls** {**active** | **rejected**}

構文の説明

24ghz	802.11b/g ネットワークを表示します。
5ghz	802.11a ネットワークを表示します。
calls	ワイヤレスクライアントのコールを表示します。
active	アクティブなコールが表示されます。
rejected	拒否されたコールが表示されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless client dot11** コマンドの出力例を示します。

```
Switch# show wireless client dot11 5ghz calls active

 TSPEC Calls:
------------------


SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a: 0
Number of Active SIP calls on 802.11a: 0
```

show wireless client location-calibration

ロケーションキャリブレーションを実行するために現在使用されているクライアントのリストを表示するには、特権 EXEC モードで **show wireless client location-calibration** コマンドを使用します。

show wireless client location-calibration

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless client location-calibration** コマンドの出力例を示します。

```
Switch# show wireless client location-calibration
```

show wireless client probing

プロービング クライアントの数を表示するには、特権 EXEC モードで **show wireless client probing** コマンドを使用します。

show wireless client probing

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless client probing** コマンドの出力例を示します。

```
Switch# show wireless client probing
MAC Address
------------------
000b.cd15.0001
000b.cd15.0002
000b.cd15.0003
000b.cd15.0004
000b.cd15.0005
000b.cd15.0006
```

show wireless client summary

コントローラと関連付けられているアクティブ クライアントの概要を表示するには、特権 EXEC モードで **show wireless client summary** コマンドを使用します。

show wireless client summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

次に、**show wireless client summary** コマンドの出力例を示します。

除外リスト（ブラック リスト）のクライアントを表示するには、**show wireless exclusionlist** コマンドを使用します。

```
Switch# show wireless client summary
Number of Local Clients : 1

MAC Address    AP Name                          WLAN State              Protocol
-------------------------------------------------------------------------------
0000.1515.000f  AP-2                         1    UP                 11a
```

show wireless client timers

802.11 システム タイマーを表示するには、特権 EXEC モードで **show wireless client timers** コマンドを使用します。

show wireless client timers

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless client timers** コマンドの出力例を示します。

```
Switch# show wireless client timers
 Authentication Response Timeout (seconds)      : 10
```

show wireless client voice diagnostics

ワイヤレス クライアントの音声診断パラメータを表示するには、特権 EXEC モードで **show wireless client voice diagnostics** コマンドを使用します。

show wireless client voice diagnostics {**qos-map** | **roam-history** | **rssi** | **status** | **tspec**}

構文の説明

qos-map	QoSおよびDSCPマッピングに関する情報と4つのキュー（VO、VI、BE、BK）それぞれのパケット統計を表示します。各種 DSCP 値も表示されます。
roam-history	既知の各クライアントの直前の 3 つのローミング履歴に関する情報を表示します。出力にはタイムスタンプ、ローミングに関連するアクセス ポイント、ローミングの理由が含まれ、ローミングに失敗した場合には失敗の理由も含まれます。
rssi	音声診断がイネーブルである場合に、直前の 5 秒間のクライアントの RSSI 値を表示します。
status	クライアントの音声診断の状態を表示します。
tspec	TSPEC クライアントに対して有効になっている音声診断を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

デバッグ音声診断は、音声診断を実行するにはイネーブルにする必要があります。

次に、**show wireless client voice diagnostics status** コマンドの出力例を示します。

```
Switch# show wireless client voice diagnostics status
Voice Diagnostics Status: FALSE
```

show wireless country

サポートされる設定済みの国タイプと無線タイプを表示するには、特権 EXEC モードで **show wireless country** コマンドを使用します。

show wireless country {**channels**|**configured**|**supported** [**tx-power**]}

構文の説明

channels	帯域ごとに使用可能なチャネルのリストと、設定されている国で許容されるチャネルのリストを表示します。
configured	設定されている国を表示します。
supportedtx-power	サポートされている各国で許容される Tx 電源のリストを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless country channels** コマンドの出力例を示します。

```
Switch# show wireless country channels
  Configured Country...........................: US  - United States
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
         (-,-) = (indoor, outdoor) regulatory domain allowed by this country.
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
    802.11bg     :
    Channels     :                  1 1 1 1 1
                 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 (-A   ,-AB  )  US  :  A * * * * A * * * * A . . .
 Auto-RF         : . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11a         :                        1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
 Channels        : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
                 : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 (-A   ,-AB  )  US  :  . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 Auto-RF         : . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 4.9GHz 802.11a  :
   Channels      :                  1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
                 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-A   ,-AB  ): * * * * * * * * * * * * * * * * * * A * * * * * A
 Auto-RF         : . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

次に、**show wireless country configured** コマンドの出力例を示します。

```
Switch# show wireless country configured
 Configured Country.............................: US  - United States
 Configured Country Codes
        US  - United States : 802.11a Indoor,Outdoor/ 802.11b / 802.11g
```

次に、**show wireless country supported tx-power** コマンドの出力例を示します。

```
Switch# show wireless country supported tx-power
      KEY: ##    = Tx Power in dBm.
           ##*   = Channel supports radar detection .
           .     = Channel is not legal in this country.
           (-)   = Regulatory Domains allowed by this country.
           (-,-) = (indoor, outdoor) regulatory Domains allowed by this country.
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+
    802.11bg     :
    Channels     :                   1 1 1 1 1
                 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+
 (-CE  ,-CE  )  AE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  AL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AR  )  AR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  AT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-NA  )  AU  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  BA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  BE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  BG  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-    )  BH  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-A   )  BO  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-A   ,-AR  )  BR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  BY  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-ABN )  CA  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-A   ,-ABN )  CA2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  CH  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-AER ,-AR  )  CL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  CM  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-CE  ,-CE  )  CN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AR  )  CO  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-A   ,-AB  )  CR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  CY  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  CZ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  DE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  DK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-ABN )  DO  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  DZ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-AB  )  EC  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-E   )  EE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  EG  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  ES  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  FI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  FR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  GB  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  GI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  GR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-A   ,-NA  )  HK  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
 (-E   ,-    )  HR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  HU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-ER  )  ID  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-E   ,-E   )  IE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
 (-EI  ,-IE  )  IL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
```

```
(-I   ,-I   )  ILO :   .  .  .  . 20 20 20 20 20 20 20 20 20  .
(-A   ,-AN  )  IN  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  IQ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  IS  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  IT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-JPU ,-JPU )  J2  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-JPU ,-JPU )  J3  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-JPQU,-PQ  )  J4  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-E   ,-    )  JO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-JPU ,-JPU )  JP  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-ACE ,-ACEK)  KE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-ACE ,-ACEK)  KR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KW  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KZ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LB  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,     )  LK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LV  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MC  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  ME  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,     )  MO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-NA  )  MX  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-ACE ,-AEC )  MY  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  NL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  NO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-NA  )  NZ  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  OM  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-AR  )  PA  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AR  )  PE  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-ABN )  PH  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-ABN )  PH2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  PK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  PL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-A   )  PR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  PT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-A   )  PY  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  QA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  RO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  RS  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-AER ,-ER  )  RU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-AE  ,-AE  )  SA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  SE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-SE  )  SG  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E   ,-E   )  SI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  SK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-ER  )  TH  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  TN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-EI  ,-E   )  TR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-ANT )  TW  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  UA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-AB  )  US  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AB  )  US2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AB  )  USL :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-    )  USX :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-A   )  UY  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AR  )  VE  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  VN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  ZA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
```

show wireless detail

設定済みのワイヤレス パラメータの詳細を表示するには、特権 EXEC モードで **show wireless detail** コマンドを使用します。

show wireless detail

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

次のようなパラメータが表示されます。

- ワイヤレス ユーザ アイドル タイムアウト
- コントローラで設定されている RF グループ名
- Fast SSID change

次に、**show wireless detail** コマンドの出力例を示します。

```
Switch# show wireless detail
User Timeout               : 300
RF network                 : default
Fast SSID                  : Disabled
```

show wireless dtls connections

Datagram Transport Layer Security（DTLS）サーバのステータスを表示するには、特権 EXEC モードで **show wireless dtls connections** コマンドを使用します。

show wireless dtls connections

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless dtls connections** コマンドの出力例を示します。

```
Switch# show wireless dtls connections
 AP Name         Local Port   Peer IP    Peer Port  Ciphersuite
------------------------------------------------------------------------
  AP-2       Capwap_Ctrl   10.0.0.16     52346      TLS_RSA_WITH_AES_128_CBC_SHA
  AP-3       Capwap_Ctrl   10.0.0.17     52347      TLS_RSA_WITH_AES_128_CBC_SHA
```

show wireless flow-control

特定のチャネルのフロー制御に関する情報を表示するには、特権 EXEC モードで **showwirelessflow-control** コマンドを使用します。

show wireless flow-control *channel-id*

構文の説明

channel-id	フロー制御がモニタされるチャネルの識別番号。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、**show wireless flow-control** *channel-id* コマンドの出力例を示します。

```
Switch# show wireless flow-control 3
Channel Name                            : CAPWAP
FC State                                : Disabled
Remote Server State                     : Enabled
Pass-thru Mode                          : Disabled
EnQ Disabled                            : Disabled
Queue Depth                             : 2048
Max Retries                             : 5
Min Retry Gap (mSec)                    : 3
```

show wireless flow-control statistics

特定のチャネルのフロー制御に関する完全な情報を表示するには、特権 EXEC モードで **show wireless flow-control statistics** コマンドを使用します。

show wireless flow-control *channel-id* **statistics**

構文の説明

channel-id	フロー制御がモニタされるチャネルの識別番号。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

次に、**show wireless flow-control** *channel-id* **statistics** コマンドの出力例を示します。

```
Switch# show wireless flow-control 3 statistics
 Channel Name                                : CAPWAP
# of times channel went into FC              : 0
# of times channel came out of FC            : 0
Total msg count received by the FC Infra     : 1
Pass-thru msgs send count                    : 0
Pass-thru msgs fail count                    : 0
# of msgs successfully queued                : 0
# of msgs for which queuing failed           : 0
# of msgs sent thru after queuing            : 0
# of msgs sent w/o queuing                   : 1
# of msgs for which send failed              : 0
# of invalid EAGAINS received                : 0
Highest watermark reached                    : 0
# of times Q hit max capacity                : 0
Avg time channel stays in FC (mSec)          : 0
```

show wireless load-balancing

ロード バランシング機能のステータスを表示するには、特権 EXEC モードで **show wireless load-balancing** コマンドを使用します。

show wireless load-balancing

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless load-balancing** コマンドの出力例を示します。

```
 > show wireless load-balancing
Aggressive Load Balancing.........................: per WLAN enabling
Aggressive Load Balancing Window (clients)..................:: 5
Aggressive Load Balancing Denial Count......................:: 3

Statistics
Total Denied Count (clients)................................:: 0
Total Denial Sent (messages)................................:: 0
Exceeded Denial Max Limit Count (times).....................:: 0
None 5G Candidate Count (times).............................:: 0
None 2.4G Candidate Count (times)...........................:: 0
```

show wireless mobility summary

モビリティマネジメントコンフィギュレーションの概要を表示するには、**show wireless mobility summary** コマンドを使用します。

show wireless mobility *ma-ip***summary**

構文の説明

ma-ip	MA IPv4 アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.3E	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、MC でのみ動作します。

例

次に、モビリティマネジメントコンフィギュレーションの概要を表示する例を示します。

```
Cisco controller# show wireless mobility 211.0.0.4 summary

Mobility Agent Summary:

Mobility Role                                 : Mobility Agent
Wireless Management VLAN                      : 211
Wireless Management IP Address                : 211.0.0.4
Mobility Switch Peer Group Name               : SPG1
Multicast IP Address                          : 0.0.0.0
DTLS Mode                                     : Enabled
Mobility Keepalive Interval/Count             : 10/3
Mobility Control Message DSCP Value           : 48
Switch Peer Group Members Configured          : 1
Central Management                            : Enabled

Link Status is Control Link Status : Data Link Status

The status of Mobility Controller:

Host Name         IP              Public IP            Link Status
------------------------------------------------------------------
ct3850-62         211.0.0.8       211.0.0.8            UP   : UP

Switch Peer Group members:

Host Name          IP              Public IP            Data Link Status
-------------------------------------------------------------------------
ct3850-63         211.0.0.4       211.0.0.4            N/A
```

show wireless performance

アグレッシブ ロード バランシングの設定を表示するには、特権 EXEC モードで **showwirelessperformance** コマンドを使用します。

show wireless performance {ap|client} summary

構文の説明

apsummary	コントローラに対して設定されているアクセス ポイントのアグレッシブ ロード バランシングの設定を表示します。
client summary	クライアントのアグレッシブ ロードバランシングの設定の詳細を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless performance ap summary** コマンドの出力例を示します。

```
Switch# show wireless performance ap summary
Number of APs:
```

次に、**show wireless performance client summary** コマンドの出力例を示します。

```
Switch# show wireless performance client summary
Number of Clients:

MAC Address        AP Name           Status        WLAN/Guest-Lan Auth Protocol Port
Wired
-------------------------------------------------------------------------------------
```

show wireless pmk-cache

ペアワイズ マスター キー（PMK）キャッシュに関する情報を表示するには、特権 EXEC モードで **show wireless pmk-cache** コマンドを使用します。

show wireless pmk-cache[**mac-address** *mac-addr*]

構文の説明

mac-address *mac-addr*	（任意）PMK キャッシュの単一エントリに関する情報。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless pmk-cache mac-address** コマンドの出力例を示します。

```
Switch# show wireless pmk-cache mac-address H.H.H
Number of PMK caches in total : 0
```

show wireless probe

拡張プローブ要求フィルタリングの設定と、各クライアントのアクセスポイントごとのWLANコントローラに送信されたプローブ数およびプローブ間隔（ミリ秒）を表示するには、特権EXECモードで **showwirelessprobe** コマンドを使用します。

show wireless probe

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless probe** コマンドの出力例を示します。

```
Switch# show wireless probe
Probe request filtering                          : Enabled
Number of probes per client per radio fwd from AP: 2
Probe request rate-limiting interval             : 500 msec
Aggregate probe request interval                 : 500 msec
```

show wireless sip preferred-call-no

SIP 優先コール番号を表示するには、特権 EXEC モードで **show wireless sip preferred-call-no** コマンドを使用します。

show wireless sip preferred-call-no

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless sip preferred-call-no** コマンドの出力例を示します。

```
Switch# show wireless sip preferred-call-no
Index Preferred-Number
----------------------
1     1031
2     1032
4     1034
```

show wireless summary

コントローラに認識されているアクセス ポイント、無線クライアントとワイヤレス クライアントの数を表示するには、特権EXECモードで**show wireless summary**コマンドを使用します。

show wireless summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、**show wireless summary** コマンドの出力例を示します。

```
Switch# show wireless summary

Access Point Summary

               Total    Up    Down
------------------------------------
802.11a/n          2     2       0
802.11b/g/n        2     2       0
All APs            2     2       0

Client Summary

Current Clients : 1
Excluded Clients: 0
Disabled Clients: 0
```

show wireless wlan summary

ワイヤレス WLAN の詳細を表示するには、**show wireless wlan summary** コマンドを使用します。

show wireless wlan summary

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.3E	このコマンドが導入されました。

次に、ワイヤレス WLAN の概要を表示する例を示します。

```
Cisco controller# show wireless WLAN summary

Total WLAN Configured: 2

Total Client Count: 0


ID    Profile Name          SSID                 Security    Radio       VLAN
Client   Status
-----------------------------------------------------------------------------------------------
1     benimr3               benimr3              NONE        All         602         0
        UP
2     Proton_2              Proton_2             NONE        All         202         0
        UP
```

show wlan name

MA WLAN 設定を名前で表示するには、**show wlan name** コマンドを使用します。

show wlan name *name ma-ip*

構文の説明

name	アクセス ポイント名。
ma-ip	MA IPv4 アドレス。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.3E	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、MC でのみ動作します。

例

次に、MA VLAN 設定を名前で表示する例を示します。

```
Cisco controller# show wlan name anu_mcma 211.0.0.4

WLAN Profile Name     : anu_mcma
================================================
Identifier                                    : 1
Network Name (SSID)                           : anu_mcma
Status                                        : Disabled
Broadcast SSID                                : Enabled
Max Associated Clients per WLAN               : 0
Max Associated Clients per AP per WLAN        : 0
Max Associated Clients per AP Radio per WLAN  : 0
AAA Policy Override                           : Disabled
Network Admission Control
  NAC-State                                   : Disabled
Number of Active Clients                      : 0
Exclusionlist Timeout                         : 60
Session Timeout                               : 1800 seconds
CHD per WLAN                                  : Enabled
Webauth DHCP exclusion                        : Disabled
Interface                                     : 211
Interface Status                              : Up
Multicast Interface                           : Unconfigured
WLAN IPv4 ACL                                 :
WLAN IPv6 ACL                                 : unconfigured
DHCP Server                                   : Default
DHCP Address Assignment Required              : Disabled
DHCP Option 82                                : Disabled
DHCP Option 82 Format                         : ap-mac
DHCP Option 82 Ascii Mode                     : Disabled
DHCP Option 82 Rid Mode                       : Disabled
Local Profiling -Policy Name                  : Disabled
```

```
Device Classification                          : Disabled
QoS Service Policy - Input
  Policy Name                                  : unknown
  Policy State                                 : None
QoS Service Policy - Output
  Policy Name                                  : unknown
  Policy State                                 : None
QoS Client Service Policy
  Input  Policy Name                           : unknown
  Output Policy Name                           : unknown
WMM                                            : Allowed
WifiDirect                                     : Disabled
Channel Scan Defer Priority:
  Priority (default)                           : 4
  Priority (default)                           : 5
  Priority (default)                           : 6
Scan Defer Time (msecs)                        : 100
Media Stream Multicast-direct                  : Disabled
CCX - AironetIe Support                        : Enabled
CCX - Gratuitous ProbeResponse (GPR)           : Disabled
CCX - Diagnostics Channel Capability           : Disabled
Dot11-Phone Mode (7920)                        : Invalid
Wired Protocol                                 : None
Peer-to-Peer Blocking Action                   : Disabled
Radio Policy                                   : All
DTIM period for 802.11a radio                  : 1
DTIM period for 802.11b radio                  : 1
Local EAP Authentication                       : Disabled
Mac Filter Authorization list name             : MACFILTER
Accounting list name                           : Disabled
802.1x authentication list name                : wcm_dot1x
Security
    802.11 Authentication                      : Open System
    Static WEP Keys                            : Disabled
    802.1X                                     : Disabled
    Wi-Fi Protected Access (WPA/WPA2)          : Enabled
        WPA (SSN IE)                           : Disabled
        WPA2 (RSN IE)                          : Enabled
            TKIP Cipher                        : Disabled
            AES Cipher                         : Enabled
        Auth Key Management
            802.1x                             : Enabled
            PSK                                : Disabled
            CCKM                               : Disabled
            FT dot1x                           : Disabled
            FT PSK                             : Disabled
            PMF dot1x                          : Disabled
            PMF PSK                            : Disabled
    FT Support                                 : Disabled
        FT Reassociation Timeout               : 20
        FT Over-The-DS mode                    : Enabled
    PMF Support                                : Disabled
        PMF Association Comeback Timeout       : 1
        PMF SA Query Time                      : 200
    CKIP                                       : Disabled
    IP Security                                : Disabled
    L2TP                                       : Disabled
    Web Based Authentication                   : Disabled
    Conditional Web Redirect                   : Disabled
    Splash-Page Web Redirect                   : Disabled
    Auto Anchor                                : Disabled
    Sticky Anchoring                           : Enabled
    Cranite Passthru                           : Disabled
    Fortress Passthru                          : Disabled
```

```
    PPTP                                          : Disabled
    Infrastructure MFP protection                 : Enabled
    Client MFP                                    : Optional
    Webauth On-mac-filter Failure                 : Disabled
    Webauth Authentication List Name              : Disabled
    Webauth Parameter Map                         : Disabled
    Tkip MIC Countermeasure Hold-down Timer       : 60
Call Snooping                                     : Disabled
Passive Client                                    : Disabled
Non Cisco WGB                                     : Disabled
Band Select                                       : Disabled
Load Balancing                                    : Disabled
IP Source Guard                                   : Disabled
Local HTTP Profiling Status                       : Disabled
Radius HTTP Profiling Status                      : Disabled
Assisted-Roaming
    Neighbor List                                 : Disabled
    Prediction List                               : Disabled
    Dual Band Support                             : Disabled
AVC Visibility                                    : Disabled
Universal Ap Admin                                : Disabled
11ac Mu Mimo                                      : Disabled
```

shutdown

VLAN スイッチングをシャットダウンするには、グローバル コンフィギュレーション モードで**shutdown** コマンドを使用します。設定セットを無効化するには、このコマンドの**no**形式を使用します。

shutdown [**vlan** *vlan-id*]
no shutdown

構文の説明

vlan *vlan-id*	シャットダウンする VAN の VLAN ID。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

例

次に、VLAN をシャットダウンする方法の例を示します。

```
Switch(config)# vlan open1
Switch(config-wlan)# shutdown
```

次に、アクセス ポイントがシャットダウンされない例を示します。

```
Switch# configure terminal
Switch(config)# ap name 3602a no shutdown
```

system env temperature threshold yellow

イエローのしきい値を決定する、イエローとレッドの温度しきい値の差を設定するには、グローバル コンフィギュレーション コマンドで **system env temperature threshold yellow** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

system env temperature threshold yellow *value*
no system env temperature threshold yellow *value*

構文の説明

value イエローとレッドのしきい値の差を指定します（摂氏）。指定できる範囲は 10 ～ 25 です。

コマンド デフォルト

デフォルト値は次のとおりです。

表 *38* : 温度しきい値のデフォルト値

Switch	イエローとレッドの差	レッド[13]
Catalyst 3850	14 °C	60 °C

[13] レッドの温度しきい値を設定することはできません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

グリーンとレッドのしきい値を設定することはできませんが、イエローのしきい値を設定することはできます。イエローとレッドのしきい値の差を指定して、イエローのしきい値を設定するには、**system env temperature threshold yellow** *value* グローバル コンフィギュレーション コマンドを使用します。たとえば、レッドしきい値が 66 °C の場合に、イエローしきい値を 51 °C に設定するには、しきい値の差を 15 に設定するために、**system env temperature threshold yellow 15** コマンドを使用します。たとえば、レッドしきい値が 60 °C の場合に、イエローしきい値を 51 °C に設定するには、しきい値の差を 15 に設定するために、**system env temperature threshold yellow 9** コマンドを使用します。

（注） スイッチ内部の温度センサーでシステム内の温度を測定するため、±5 °Cの差が生じる可能性があります。

例

次の例では、イエローとレッドのしきい値の差を 15 に設定する方法を示します。

```
Switch(config)# system env temperature threshold yellow 15
Switch(config)#
```

test cable-diagnostics tdr

インターフェイス上でタイム ドメイン反射率計（TDR）機能を実行するには、特権 EXEC モードで **test cable-diagnostics tdr** コマンドを使用します。

test cable-diagnostics tdr interface *interface-id*

構文の説明

interface-id	TDR を実行するインターフェイス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

TDR は、銅線のイーサネット 10/100/100 ポートだけでサポートされます。10 ギガビット イーサネット ポートまたは Small Form-Factor Pluggable（SFP）モジュール ポートではサポートされません。

test cable-diagnostics tdr interface *interface-id* コマンドを使用して TDR を実行した後、**show cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを使用して結果を表示します。

次の例では、インターフェイス上で TDR を実行する方法を示します。

```
Switch# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results
```

インターフェイスのリンク ステータスがアップ状態で速度が 10 Mb/s または 100 Mb/s である場合、**test cable-diagnostics tdr interface** *interface-id* コマンドを入力すると、次のメッセージが表示されます。

```
Switch# test cable-diagnostics tdr interface gigabitethernet1/0/3
TDR test on Gi1/0/9 will affect link state and traffic
TDR test started on interface Gi1/0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

関連トピック

show cable-diagnostics tdr （1067 ページ）

traceroute mac

指定の送信元 MAC アドレスから指定の宛先 MAC アドレスまでをパケットが通過するレイヤ 2 パスを表示するには、特権 EXEC モードで **traceroute mac** コマンドを使用します。

traceroute mac [**interface** *interface-id*] *source-mac-address* [**interface** *interface-id*] *destination-mac-address* [**vlan** *vlan-id*] **[detail]**

構文の説明

interface*interface-id*	（任意）送信元または宛先スイッチ上のインターフェイスを指定します。
source-mac-address	送信元スイッチの 16 進形式の MAC アドレス。
destination-mac-address	宛先スイッチの 16 進形式の MAC アドレス。
vlan *vlan-id*	（任意）送信元スイッチから宛先スイッチまでをパケットが通過するレイヤ2のパスをトレースするVLANを指定します。指定できるVLAN ID の範囲は 1 ～ 4094 です。
detail	（任意）詳細情報を表示するよう指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

レイヤ 2 の traceroute を適切に機能させるには、Cisco Discovery Protocol（CDP）がネットワークのすべてのスイッチで有効になっている必要があります。CDP をディセーブルにすることは避けてください。

スイッチがレイヤ 2 パス内でレイヤ 2 traceroute をサポートしていないデバイスを検知した場合、スイッチはレイヤ 2 trace クエリを送信し続け、タイムアウトにします。

パス内で識別可能な最大ホップ数は 10 です。

レイヤ 2 traceroute はユニキャスト トラフィックだけをサポートします。マルチキャストの送信元または宛先 MAC アドレスを指定しても、物理的なパスは識別されず、エラー メッセージが表示されます。

指定された送信元および宛先アドレスが同じ VLAN にある場合、**traceroute mac** コマンド出力はレイヤ 2 パスを表示します。

異なる VLAN にある送信元および宛先アドレスを指定した場合、レイヤ2パスは識別されず、エラー メッセージが表示されます。

送信元または宛先 MAC アドレスが複数の VLAN に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。

VLAN を指定しないと、パスは識別されず、エラー メッセージが表示されます。

複数の装置がハブを介して 1 つのポートに接続されている場合（たとえば、複数の CDP ネイバーがポートで検出されるなど）、レイヤ 2 traceroute 機能はサポートされません。

複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。

この機能は、トークンリング VLAN ではサポートされません。

例

次の例では、送信元および宛先 MAC アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                 (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

次の例では、**detail** キーワードを使用することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201 detail
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 / WS-C3750E-24PD / 2.2.6.6 :
          Gi0/0/2 [auto, auto] => Gi0/0/3 [auto, auto]
  con5 / WS-C2950G-24-EI / 2.2.5.5 :
          Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
  con1 / WS-C3550-12G / 2.2.1.1 :
          Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
          Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

次の例では、送信元および宛先スイッチのインターフェイスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
 0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                 (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
```

```
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

次の例では、スイッチが送信元スイッチに接続されていない場合のレイヤ 2 のパスを示します。

```
Switch# traceroute mac 0000.0201.0501 0000.0201.0201 detail
  Source not directly connected, tracing source .....
  Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
  con5 / WS-C3750E-24TD / 2.2.5.5 :
          Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
  con1 / WS-C3550-12G / 2.2.1.1 :
          Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
          Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

次の例では、スイッチが送信元 MAC アドレスの宛先ポートを検出できない場合のレイヤ 2 のパスを示します。

```
Switch# traceroute mac 0000.0011.1111 0000.0201.0201
  Error:Source Mac address not found.
  Layer2 trace aborted.
```

次の例では、送信元および宛先デバイスが異なる VLAN にある場合のレイヤ 2 のパスを示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0301.0201
  Error:Source and destination macs are on different vlans.
  Layer2 trace aborted.
```

次の例では、宛先 MAC アドレスがマルチキャスト アドレスの場合のレイヤ 2 のパスを示します。

```
Switch# traceroute mac 0000.0201.0601 0100.0201.0201
  Invalid destination mac address
```

次の例では、送信元および宛先スイッチが複数の VLAN にある場合のレイヤ 2 のパスを示します。

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
  Error:Mac found on multiple vlans.
  Layer2 trace aborted.
```

関連トピック

traceroute mac ip （1126 ページ）

traceroute mac ip

指定の送信元 IP アドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名を通過するパケットのレイヤ 2 パスを表示するには、特権 EXEC モードで **traceroute mac ip** コマンドを使用します。

traceroute mac ip {*source-ip-address source-hostname*} {*destination-ip-address destination-hostname*} **[detail]**

構文の説明

source-ip-address	32 ビットの値（ドット付き 10 進表記）で指定された送信元スイッチの IP アドレス。
source-hostname	送信元スイッチの IP ホスト名。
destination-ip-address	32 ビットの値（ドット付き 10 進表記）で指定された宛先スイッチの IP アドレス。
destination-hostname	宛先スイッチの IP ホスト名。
detail	（任意）詳細情報を表示するよう指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

レイヤ 2 の traceroute を適切に機能させるには、Cisco Discovery Protocol（CDP）がネットワークの各スイッチでイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。

スイッチがレイヤ 2 パス内でレイヤ 2 traceroute をサポートしていないデバイスを検知した場合、スイッチはレイヤ 2 trace クエリを送信し続け、タイムアウトにします。

パス内で識別可能な最大ホップ数は 10 です。

指定された送信元および宛先の IP アドレスが同一のサブネット内にある場合、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。

IP アドレスを指定した場合、スイッチは Address Resolution Protocol（ARP）を使用し、IP アドレスとそれに対応する MAC アドレスおよび VLAN ID を対応させます。

- 指定の IP アドレスの ARP のエントリが存在している場合、スイッチは対応する MAC アドレスを使用して、物理パスを識別します。

- ARP のエントリが存在しない場合、スイッチは ARP クエリを送信し、IP アドレスを解決しようと試みます。IP アドレスは同一のサブネットにある必要があります。IP アドレスが解決されない場合は、パスは識別されず、エラー メッセージが表示されます。

複数の装置がハブを介して 1 つのポートに接続されている場合（たとえば、複数の CDP ネイバーがポートで検出されるなど）、レイヤ 2 traceroute 機能はサポートされません。

複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。

この機能は、トークンリング VLAN ではサポートされません。

例

次の例では、**detail** キーワードを使用して、送信元と宛先の IP アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C3750E-24TD / 2.2.6.6 :
        Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先ホスト名を指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Switch# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5                (2.2.5.5        )  :    Gi0/0/3 => Gi0/1
con1                (2.2.1.1        )  :    Gi0/0/1 => Gi0/2
con2                (2.2.2.2        )  :    Gi0/0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

次の例では、ARP が送信元 IP アドレスと対応する MAC アドレスを関連付けられない場合の、レイヤ 2 のパスを示します。

```
Switch# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

関連トピック

traceroute mac （1122 ページ）

trapflags

不正アクセス ポイント検出トラップの送信を有効にするには、特権 EXEC モードで **trapflags** コマンドを使用します。不正アクセスポイント検出トラップの送信を無効にするには、このコマンドの **no** 形式を使用します。

trapflags rogueap
no trapflags rogueap

構文の説明

rogueap	不正アクセスポイント検出トラップの送信を有効にします。

コマンド デフォルト

イネーブル

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、不正なアクセス ポイント検出トラップの送信をディセーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# no trapflags rogueap
Switch(config)# end
```

trapflags client

クライアント関連の DOT11 トラップの送信を有効にするには、特権 EXEC モードで **trapflags client** コマンドを使用します。クライアント関連の DOT11 トラップの送信を無効にするには、このコマンドの **no** 形式を使用します。

trapflags client [{**dot11** {**assocfail**|**associate**|**authfail**|**deauthenticate**|**disassociate**}|**excluded**}]
no trapflags client [{**dot11** {**assocfail**|**associate**|**authfail**|**deauthenticate**|**disassociate**}|**excluded**}]

構文の説明

dot11	クライアント関連の DOT11 トラップ。
assocfail	クライアントへの Dot11 アソシエーション エラー トラップの送信をイネーブルにします。
associate	クライアントへの Dot11 アソシエーション トラップの送信をイネーブルにします。
authfail	クライアントへの Dot11 認証エラー トラップの送信をイネーブルにします。
deauthenticate	クライアントへの Dot11 認証解除トラップの送信をイネーブルにします。
disassociate	クライアントへの Dot11 ディスアソシエーション トラップの送信をイネーブルにします。
excluded	除外したトラップのクライアントへの送信をイネーブルにします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、クライアントへの Dot11 アソシエーション解除トラップの送信をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# trapflags client dot11 disassociate
Switch(config)# end
```

type

一つ以上のファイルの内容を表示するには、ブート ローダ モードで **type** コマンドを使用します。

type *filesystem:/file-url...*

構文の説明

filesystem:	ファイル システムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。USB メモリ スティックには **usbflash0:** を使用します。
/file-url...	表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

ファイルのリストを指定すると、各ファイルの内容が順次表示されます。

例

次に、ファイルの内容を表示する例を示します。

```
Switch: type flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

unset

1 つ以上の環境変数をリセットするには、ブート ローダ モードで **unset** コマンドを使用します。

unset *variable...*

構文の説明

variable	*variable* には、次に示すキーワードのいずれかを使用します。
	MANUAL_BOOT：スイッチの起動を自動で行うか手動で行うかどうかを指定します。
	BOOT：自動起動時に、実行可能ファイルのリストをリセットして、ロードおよび実行します。BOOT環境変数が設定されていない場合、システムは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT変数が設定されていても、指定されたイメージをロードできなかった場合、システムはフラッシュ ファイル システムで最初に検出した起動可能なファイルを起動しようとします。
	ENABLE_BREAK：フラッシュ ファイル システムの初期化後に、コンソール上の **Break** キーを使用して自動ブート プロセスを中断できるかどうかを指定します。
	HELPER：ブート ローダの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストを識別します。ヘルパー ファイルは、ブートローダの機能を拡張したり、パッチを当てたりします。
	PS1：ブート ローダ モードの場合に、コマンドライン プロンプトとして使用する文字列を指定します。
	CONFIG_FILE：Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名をリセットします。
	BAUD：コンソールで使用される速度（ビット/秒（b/s）単位）をリセットします。コンフィギュレーション ファイルに別の設定が指定されていない限り、Cisco IOS ソフトウェアはブートローダからボー レート設定を継承し、この値を引き続き使用します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

通常の環境では、環境変数の設定を変更する必要はありません。

MANUAL_BOOT 環境変数は、**no boot manual** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

BOOT 環境変数は、**no boot system** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

ENABLE_BREAK 環境変数は、**no boot enable-break** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

HELPER 環境変数は、**no boot helper** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

CONFIG_FILE 環境変数は、**no boot config-file** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

例

次に、SWITCH_PRIORITY 環境変数をリセットする例を示します。

```
Switch: unset SWITCH_PRIORITY
```

関連トピック

set （1059 ページ）
reset （1056 ページ）

version

ブートローダのバージョンを表示するには、ブート ローダ モードで **version** コマンドを使用します。

version

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

例

次に、スイッチのブート ローダのバージョンを表示する例を示します。

```
Switch: version
CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 1.3, RELEASE SOFTWARE (P)
Compiled Sun Jun 16 18:31:15 PDT 2013 by rel
```

wireless client

クライアント パラメータを設定するには、グローバル コンフィギュレーション モードで **wirelessclient** コマンドを使用します。

wireless client {**association limit** *assoc-number* **interval** *interval*|**band-select** {**client-rssi** *rssi*|**cycle-count** *count*|**cycle-threshold** *threshold*|**expire dual-band** *timeout*|**expire suppression** *timeout*}|**max-user-login** *max-user-login*|**timers auth-timeout** *seconds*|**user-timeout** *user-timeout*}

構文の説明

associationlimit *assoc-number***interval** *interval*	所定の間隔での1つのアクセスポイントスロットあたりの関連付け要求制限を有効にし、関連付け要求制限間隔を設定します。 所定の間隔での1つのアクセスポイントスロットあたりの関連付け要求の数は、1～100の範囲で設定できます。 クライアント関連付け要求制限間隔は、100～10000ミリ秒の範囲で設定できます。
band-select	クライアントのバンド選択オプションを設定します。
client-rssi *rssi*	バンド選択のクライアント受信信号強度インジケータ（RSSI）しきい値を設定します。 -90 ～ -20 のプローブに応答するクライアントRSSIの最小dBm。
cycle-count *count*	バンド選択プローブ周期カウントを設定します。 周期カウントは、1～10の範囲で設定できます。
cycle-threshold *threshold*	新規スキャン周期の時間しきい値を設定します。 周期しきい値は、1～1000ミリ秒の範囲で設定できます。
expiredual-band *timeout*	特定のクライアントを5 GHz帯域にプッシュする試行を停止するまでのタイムアウトを設定します。 タイムアウトは10～300秒の範囲で設定できます。デフォルト値は60秒です。
expiresuppression *timeout*	既知のデュアルバンドクライアントが失効してプルーニングされるまでの時間を設定します。 抑止時間は10～200秒の範囲で設定できます。デフォルトのタイムアウト値は20秒です。
max-user-login *max-user-login*	ユーザのログイン セッションの最大数を設定します。
timersauth-timeout *seconds*	クライアント タイマーを設定します。
user-timeout *user-timeout*	アイドル クライアント タイムアウトを設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、帯域幅選択のプローブ サイクルカウントを 8 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# wireless client band-select cycle-count 8
Switch(config)# end
```

次に、しきい値が 700 ミリ秒の新しいスキャン サイクルの時間のしきい値を設定する例を示します。

```
Switch# configure terminal
Switch(config)# wireless client band-select cycle-threshold 700
Switch(config)# end
```

次に、70 秒後にデュアルバンド データベースのデュアルバンド クライアントを抑止する例を示します。

```
Switch# configure terminal
Switch(config)# wireless client band-select expire suppression 70
Switch(config)# end
```

wireless client mac-address deauthenticate

ワイヤレス クライアントへの接続を解除するには、グローバル コンフィギュレーション モードで **wireless client mac-address deauthenticate** コマンドを使用します。

wirelessclientmac-address *mac-addr***deauthenticate**

構文の説明

mac-address *mac-addr*	ワイヤレス クライアントのMACアドレス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、ワイヤレス クライアントを接続解除する例を示します。

```
Switch# configure terminal
Switch(config)# wireless client mac-address 00:1f:ca:cf:b6:60 deauthenticate
Switch(config)# end
```

wireless client mac-address

ワイヤレス クライアントの設定を構成するには、グローバル コンフィギュレーション モードで **wirelessclientmac-address** コマンドを使用します。

wireless client mac-address *mac-addr* **ccx** {**clear-reports**|**clear-results**|**default-gw-ping**|**dhcp-test**|**dns-ping**|**dns-resolve hostname** *host-name*|**get-client-capability**|**get-manufacturer-info**|**get-operating-parameters**|**get-profiles**|**log-request** {**roam**|**rsna**|**syslog**}|**send-message** *message-id*|**stats-request** *measurement-duration* {**dot11**|**security**}|**test-abort**|**test-association** *ssid bssid dot11 channel*|**test-dot1x** [*profile-id*] *bssid dot11 channel*|**test-profile** {**any***profile-id*}}

構文の説明

mac-addr	クライアントの MAC アドレス。
ccx	Cisco Client Extension（CCX）。
clear-reports	クライアント レポートの情報をクリアします。
clear-results	コントローラのテスト結果をクリアします。
default-gw-ping	デフォルト ゲートウェイ pingテストの実行要求をクライアントに送信します。
dhcp-test	DHCP テストの実行要求をクライアントに送信します。
dns-ping	ドメイン ネーム システム（DNS）サーバ IP アドレス ping テストの実行要求をクライアントに送信します。
dns-resolvehostname *host-name*	指定されたホスト名に対するドメイン ネーム システム（DNS）解決テストの実行要求をクライアントに送信します。
get-client-capability	クライアントにその機能情報を送信するよう指示する要求を送信します。
get-manufacturer-info	製造元の情報を送信するよう指示する要求をクライアントに送信します。
get-operating-parameters	クライアントに現在の動作パラメータを送信するよう指示する要求を送信します。
get-profiles	クライアントにプロファイルを送信するよう指示する要求を送信します。
log-request	指定されたクライアント デバイスに対する CCX ログ要求を設定します。
roam	（任意）クライアント CCX ローミング ログを指定する要求を指定します。

rsna	（任意）クライアント CCX RSNA ログを指定する要求を指定します。
syslog	（任意）クライアント CCX システム ログを指定する要求を指定します。

send-message *message-id*

メッセージをクライアントに送ります。

次のいずれかを含むメッセージ タイプ。

- 1：SSID が無効です。
- 2：ネットワーク設定が無効です。
- 3：WLAN の信頼性に不一致があります。
- 4：ユーザの資格情報が間違っています。
- 5：サポートにお問い合わせください。
- 6：問題は解決されました。
- 7：問題は解決されていません。
- 8：もう一度後で作業を行ってください。
- 9：示された問題を修正してください。
- 10：ネットワークにより、トラブルシューティングが拒否されました。
- 11：クライアント レポートを取得中です。
- 12：クライアント ログを取得中です。
- 13：取得が完了しました。
- 14：アソシエーション テストを開始します。
- 15：DHCP テストを開始します。
- 16：ネットワーク接続テストを開始します。
- 17：DNS ping テストを開始します。
- 18：名前解決テストを開始します。
- 19：802.1X 認証テストを開始します。
- 20：クライアントを特定のプロファイルにリダイレクトしています。
- 21：テストが完了しました。
- 22：テストに合格しました。
- 23：テストに失敗しました。
- 24：通常の操作を再開するには、診断チャネル操作をキャンセルするか、WLAN プロファイルを選択してください。
- 25：クライアントにより、ログの取得が拒否されました。

- 26：クライアントにより、クライアント レポートの取得が拒否されました。
- 27：クライアントにより、テスト要求が拒否されました。
- 28：無効なネットワーク（IP）設定です。
- 29：ネットワークで機能停止または問題が発生しています。
- 30：予定された保守期間です。
- 31：WLAN セキュリティ方式が正しくありません。
- 32：WLAN 暗号化方式が正しくありません。
- 33：WLAN 認証方式が正しくありません。

stats-request *measurement-duration*	統計情報の要求を送信します。
dot11	（任意）dot11 カウンタを指定します。
security	（任意）セキュリティ カウンタを指定します。
test-abort	現在のテストを中止するよう指示する要求をクライアントに送信します。
test-association *ssid bssid dot11 channel*	関連付けテストの実行要求をクライアントに送信します。
test-dot1x	802.1x テストの実行要求をクライアントに送信します。
profile-id	（任意）テストのプロファイル名。
bssid	Basic SSID。
dot11	802.11a、802.11b、または 802.11g ネットワークを指定します。
channel	チャネル番号。
test-profile	プロファイル リダイレクト テストの実行要求をクライアントに送信します。
any	プロファイル リダイレクト テストの実行要求をクライアントに送信します。
profile-id	テスト プロファイル名。 （注） プロファイル ID には、必ずクライアント レポートが有効なクライアント プロファイルのプロファイル ID を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

default-gw-ping テストでは、クライアントは診断チャネルを使用する必要はありません。

次に、クライアントの MAC アドレス 00:1f:ca:cf:b6:60 のレポート情報をクリアする例を示します。

```
Switch# configure terminal
Switch(config)# wireless client mac-address 00:1f:ca:cf:b6:60 ccx clear-reports
Switch(config)# end
```

wireless load-balancing

コントローラでアグレッシブ ロード バランシングを設定するには、グローバル コンフィギュレーション モードで **wirelessload-balancing** を使用します。

wireless load-balancing {**denial** *denial-count*|**window** *client-count*}

構文の説明

denial *denial-count*	ロードバランシング時に拒否されるアソシエーションの数を指定します。 ロードバランシング時の関連付け拒否の最大数は、1～10 の範囲で指定できます。デフォルト値は 3 です。
window *client-count*	アグレッシブ ロード バランシング クライアント ウィンドウと、特定のアクセス ポイントに対するアグレッシブ ロード バランシングをトリガーするのに必要なクライアント数を指定します。 クライアント数を指定するアグレッシブ ロード バランシング クライアント ウィンドウは、0～20 の範囲で指定できます。デフォルト値は 5 です。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

負荷分散が有効になっている WLAN は、音声およびビデオなどの時間依存型アプリケーションをサポートしません。これは、ローミングでの遅延が存在するためです。

コントローラとともに Cisco 7921 および 7920 Wireless IP Phone を使用する場合、各コントローラの音声 WLAN でアグレッシブなロードバランシングが無効化されていることを確認します。無効化されていない場合、電話による初期ローミングが失敗し、オーディオパスが中断されることがあります。

次に、ロード バランシング中の関連付け拒否を設定する例を示します。

```
Switch# configure terminal
Switch(config)# wireless load-balancing denial 5
Switch(config)# end
```

wireless sip preferred-call-no

新しい優先コールを追加したり、音声優先制御を設定したりするには、グローバル コンフィギュレーション モードで **wirelesssippreferred-call-no** コマンドを使用します。優先コールを削除するには、このコマンドの **no** 形式を使用します。

wireless sip preferred-call-no *callIndex call-no*
no wireless sip preferred-call-no *callIndex*

構文の説明

callIndex	1～6の間の有効な値を持つコールインデックス。
call-no	27 文字まで使用できる優先コール数。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

音声優先制御を設定する前に、次の前提条件を実行する必要があります。

- 音声コールがパススルーできるように WLAN QoS を設定します。
- 無線の ACM を有効にします。
- WLAN 上で SIP コール スヌーピングを有効にします。

次に、新しい優先コールを追加するか、または音声優先制御を設定する例を示します。

```
Switch# configure terminal
Switch(config)# wireless sip preferred-call-no 2 0123456789
Switch(config)# end
```

第 XIII 部

VideoStream

VideoStream コマンド

ap dot11 media-stream multicast-direct

2.4 GHz/5 GHz 帯域のマルチキャスト ダイレクトを設定するには、**ap dot11 media-stream multicast-direct** コマンドを使用します。

ap dot11 {**24ghz**|**5ghz**} **media-stream** {**multicast-direct** {**admission-besteffort**|**client-maximum** *value*|**radio-maximum** *value*}|**video-redirect**}

構文の説明

multicast-direct	802.11 帯域のマルチキャスト ダイレクトを設定します。
admission-besteffort	ベスト エフォート キューにメディア ストリームを許可します。
client-maximum *value*	クライアントで許可されるストリームの最大数を指定します。
radio-maximum *value*	2.4 GHz または 5 GHz 帯域で許可されるストリームの最大数を指定します。
video-redirect	非マルチキャスト ダイレクト ビデオを無線で BestEffort キューにリダイレクトします。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

802.11 ネットワークのメディア ストリーム マルチキャスト ダイレクト パラメータを設定する前に、ネットワークが非動作であることを確認します。

例

次に、2.4 GHz 帯域のマルチキャスト ダイレクトを設定する例を示します。

```
(Cisco Controller) >Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ap dot11 24ghz media-stream multicast-direct
```

関連トピック

wireless media-stream multicast-direct （1153 ページ）

show ap dot11

802.11 帯域パラメータを表示するには、**showapdot11** コマンドを使用します。

show ap dot11 {24ghz|5ghz} {media-stream rrc|network|profile|summary}

構文の説明

media-streamrrc	メディア ストリーム設定を表示します。
network	ネットワーク設定を表示します。
profile	すべての Cisco AP のプロファイル情報を表示します。
summary	802.11b および 802.11a Cisco AP の設定と統計情報を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC コマンド モードまたは特権 EXEC コマンド モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

なし。

次に、**show ap dot11 24ghz media-stream rrc** コマンドの出力例を示します。

```
Switch#show ap dot11 24ghz media-stream rrc

Multicast-direct                : Disabled
Best Effort                     : Disabled
Video Re-Direct                 : Disabled
Max Allowed Streams Per Radio     : Auto
Max Allowed Streams Per Client    : Auto
Max Video Bandwidth              : 0
Max Voice Bandwidth              : 75
Max Media Bandwidth              : 85
Min PHY Rate (Kbps)              : 6000
Max Retry Percentage             : 80
```

関連トピック

wireless media-stream （1154 ページ）

show wireless media-stream group

ワイヤレス メディア ストリーム グループ情報を表示するには、**show wireless media-stream group** コマンドを使用します。

show wireless media-stream group {**detail** *GroupName*|**summary**}

構文の説明

detail *GroupName*	コマンドで指定されているグループのメディア ストリーム グループの設定の詳細を表示します。
summary	メディア ストリーム グループの設定の概要を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC モードまたは特権 EXEC モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

なし。

次に、**show wireless media-stream group detail GRP1** コマンドの出力例を示します。

```
Switch#show wireless media-stream group detail GRP1
```

関連トピック

wireless media-stream （1154 ページ）

wireless media-stream multicast-direct

マルチキャストダイレクトのステータスを設定するには**media-streammulticast-direct** コマンドを使用します。マルチキャストダイレクトのステータスを削除するには、このコマンドの no 形式を使用します。

no wireless media-stream multicast-direct

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。WLAN Quality of Service（QoS）を gold または platinum のいずれかに設定する必要があります。

例

次に、ワイヤレス LAN メディア ストリームのマルチキャストダイレクトを設定する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless media-stream multicast-direct
```

wireless media-stream

さまざまなパラメータを設定するには、**wirelessmedia-stream** コマンドを使用します。

wireless media-stream group *groupName* [*startipAddr endipAddr*]

wireless media-stream group{ avg-packet-size default exit max-bandwidth no policy qos}

wireless media-stream {**multicast-direct**|**message** [{**phone** *phone*|**URL** *URL*|**Notes** 注|**Email** *Email*}]}

構文の説明

group *groupName*	グループのマルチキャスト ダイレクト ステータスを設定します。
startipAddr	グループの開始 IP アドレスを設定します。
endipAddr	グループの終了 IP アドレスを設定します。
group *avg-packet-size*	平均パケット サイズを設定します。
group デフォルト	コマンドをデフォルト値に設定します。
group *exit*	サブモードを終了します。
group *max-bandwidth*	予想されるストリームの最大帯域幅を Kbps 単位で設定します。
group *no*	コマンドを無効にするか、そのデフォルトに設定します。
group ポリシー	メディア ストリームのアドミッション ポリシーを設定します。
group *qos*	エア QoS クラスを <'video'> ONLY に設定します。
multicast-direct	マルチキャスト ダイレクト ステータスを設定します。
message	セッション アナウンス メッセージを設定します。
phone *phone*	セッション アナウンスの電話番号を設定します。
URL *URL*	セッション アナウンス URL を設定します。
Notes 注	セッション アナウンス メモを設定します。
Email *Email*	セッション アナウンス電子メールを設定します。

コマンド デフォルト

ディセーブル

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

コマンド履歴

リリース	変更内容
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。

例

次に、予想されるマルチキャスト宛先アドレス、ストリームの帯域幅の使用量およびストリームの優先順位のパラメータなど、各メディア ストリームとそのパラメータを設定する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wireless media-stream group GROUP1 231.1.1.1 231.1.1.10
```

第 XIV 部

VLAN

VLAN コマンド

client vlan

WLAN インターフェイスまたはインターフェイス グループを設定するには、**clientvlan** コマンドを使用します。WLAN インターフェイスをディセーブルにするには、このコマンドの **no** 形式を使用します。

client vlan *interface-id-name-or-group-name*
no client vlan

構文の説明

interface-id-name-or-group-name	インターフェイス ID、名前、または VLAN グループ名。インターフェイス ID は、複数桁で指定することもできます。

コマンド デフォルト

デフォルト インターフェイスが設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN のクライアント VLAN をイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# client vlan client-vlan1
Switch(config-wlan)# end
```

次に、WLAN 上のクライアント VLAN をディセーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no client vlan
Switch(config-wlan)# end
```

関連トピック

wlan （1283 ページ）

clear vtp counters

VLAN Trunking Protocol（VTP）およびプルーニング カウンタをクリアするには、特権 EXEC モードで **clear vtp counters** コマンドを使用します。

clear vtp counters

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次の例では、VTP カウンタをクリアする方法を示します。

```
Switch# clear vtp counters
```

情報が削除されたことを確認するには、**show vtp counters** 特権 EXEC コマンドを入力します。

関連トピック

show vtp （1178 ページ）

debug platform vlan

VLAN マネージャ ソフトウェアのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform vlan** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug platform vlan [{**error**|**event**}] [**switch** *switch-number*]
no debug platform vlan [{**error**|**event**}] [**switch** *switch-number*]

構文の説明

error	（任意）VLAN エラー デバッグ メッセージを表示します。
event	（任意）VLAN プラットフォーム イベント デバッグ メッセージを表示します。
switch *switch-number*	（任意）VLANマネージャ ソフトウェアのデバッグをイネーブルにするスタック メンバ番号を指定します。 このキーワードは、スタック対応スイッチでのみサポートされています。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

undebug platform vlan コマンドは、**no debug platform vlan** コマンドと同じです。

次の例では、VLAN エラー デバッグ メッセージを表示する方法を示します。

```
Switch# debug platform vlan error
```

debug sw-vlan

VLAN マネージャ アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sw-vlan {**badpmcookies**|**cfg-vlan** {**bootup**|**cli**}|**events**|**ifs**|**management**|**mapping**|**notification**|**packets**|**redundancy**|**registries**|**vtp**}
no debug sw-vlan {**badpmcookies**|**cfg-vlan** {**bootup**|**cli**}|**events**|**ifs**|**management**|**mapping**|**notification**|**packets**|**redundancy**|**registries**|**vtp**}

構文の説明

badpmcookies	不良ポート マネージャ クッキーの VLAN マネージャ インシデントに関するデバッグ メッセージを表示します。
cfg-vlan	VLAN 設定デバッグ メッセージを表示します。
bootup	スイッチが起動すると、メッセージが表示されます。
cli	コマンドライン インターフェイス（CLI）が VLAN コンフィギュレーション モードである場合のメッセージを表示します。
events	VLAN マネージャ イベントのデバッグ メッセージを表示します。
ifs	VLAN マネージャ IOS ファイル システム（IFS）のデバッグ メッセージを表示します。詳細については、「debug sw-vlan ifs （1165 ページ）」を参照してください。
management	内部 VLAN の VLAN マネージャ管理のデバッグ メッセージを表示します。
mapping	VLAN マッピングのデバッグ メッセージを表示します。
notification	VLAN マネージャ通知のデバッグ メッセージを表示します。詳細については、「debug sw-vlan notification （1167 ページ）」を参照してください。
packets	パケット処理およびカプセル化プロセスのデバッグ メッセージを表示します。
redundancy	VTP VLAN 冗長性のデバッグ メッセージを表示します。
registries	VLAN マネージャ レジストリのデバッグ メッセージを表示します。
vtp	VLAN Trunking Protocol（VTP）コードのデバッグ メッセージを表示します。詳細については、「debug sw-vlan vtp （1169 ページ）」を参照してください。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

undebug sw-vlan コマンドは、**no debug sw-vlan** コマンドと同じです。

スイッチ スタック上でデバッグをイネーブルにした場合、アクティブ スイッチ でのみイネーブルになります。特定のスタック メンバをデバッグする場合は、**session switch***stack-member-number* 特権 EXEC コマンドを使用してアクティブ スイッチから CLI セッションを開始できます。

次に、VLAN マネージャ イベントのデバッグ メッセージを表示する例を示します。

```
Switch# debug sw-vlan events
```

関連トピック

debug sw-vlan ifs （1165 ページ）
debug sw-vlan notification （1167 ページ）
debug sw-vlan vtp （1169 ページ）
show vlan （1174 ページ）
show vtp （1178 ページ）

debug sw-vlan ifs

VLAN マネージャ IOS File System（IFS）エラー テストのデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan ifs** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sw-vlan ifs {**open** {**read**|**write**}|**read** {**1**|**2**|**3**|**4**}|**write**}
no debug sw-vlan ifs {**open** {**read**|**write**}|**read** {**1**|**2**|**3**|**4**}|**write**}

構文の説明

open read	VLAN マネージャ IFS ファイル読み取り動作のデバッグ メッセージを表示します。
open write	VLAN マネージャ IFS ファイル書き込み動作のデバッグ メッセージを表示します。
read	指定されたエラー テスト（**1**、**2**、**3**、または **4**）に関するファイル読み取り動作のデバッグ メッセージを表示します。
write	ファイル書き込み動作のデバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

undebug sw-vlan ifs コマンドは、**no debug sw-vlan ifs** コマンドと同じです。

ファイルの読み取り処理に処理 **1** を選択すると、ヘッダー検証ワードおよびファイル バージョン番号が格納されたファイル ヘッダーが読み込まれます。処理 **2** を指定すると、ドメインおよび VLAN 情報の大部分が格納されたファイル本体が読み取られます。処理 **3** を指定すると、Type Length Version（TLV）記述子構造が読み取られます。処理 **4** を指定すると、TLV データが読み取られます。

スイッチ スタック上でデバッグをイネーブルにした場合、アクティブ スイッチ でのみイネーブルになります。特定のスタック メンバをデバッグする場合は、**session switch***stack-member-number* 特権 EXEC コマンドを使用してアクティブ スイッチから CLI セッションを開始できます。

次の例では、ファイル書き込み動作のデバッグ メッセージを表示する方法を示します。

```
Switch# debug sw-vlan ifs write
```

関連トピック

show vlan （1174 ページ）

debug sw-vlan notification

VLANマネージャ通知のデバッグをイネーブルにするには、特権EXECモードで**debug sw-vlan notification** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sw-vlan notification
{accfwdchange|allowedvlancfgchange|fwdchange|linkchange|modechange|pruningcfgchange|statechange}
no debug sw-vlan notification
{accfwdchange|allowedvlancfgchange|fwdchange|linkchange|modechange|pruningcfgchange|statechange}

構文の説明

accfwdchange	集約アクセス インターフェイス スパニングツリー転送変更に関するVLAN マネージャ通知のデバッグ メッセージを表示します。
allowedvlancfgchange	許可 VLAN の設定変更に関する VLAN マネージャ通知のデバッグ メッセージを表示します。
fwdchange	スパニングツリー転送変更に関する VLAN マネージャ通知のデバッグ メッセージを表示します。
linkchange	インターフェイス リンクステート変更のVLANマネージャ通知のデバッグ メッセージを表示します。
modechange	インターフェイス モード変更の VLAN マネージャ通知のデバッグ メッセージを表示します。
pruningcfgchange	プルーニング設定変更の VLAN マネージャ通知のデバッグ メッセージを表示します。
statechange	インターフェイス ステート変更のVLANマネージャ通知のデバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

undebug sw-vlan notification コマンドは、**no debug sw-vlan notification** コマンドと同じです。

スイッチ スタック上でデバッグをイネーブルにした場合、アクティブ スイッチ でのみイネーブルになります。特定のスタック メンバをデバッグする場合は、**session switch** *stack-member-number* 特権 EXEC コマンドを使用してアクティブ スイッチから CLI セッションを開始できます。

次に、インターフェイス モード変更の VLAN マネージャ通知のデバッグ メッセージを表示する例を示します。

```
Switch# debug sw-vlan notification
```

関連トピック

show vlan （1174 ページ）

debug sw-vlan vtp

VLAN Trunking Protocol（VTP）コードのデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan vtp** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sw-vlan vtp {**events**|**packets**|**pruning** [{**packets**|**xmit**}]|**redundancy**|**xmit**}
no debug sw-vlan vtp {**events**|**packets**|**pruning**|**redundancy**|**xmit**}

構文の説明

events	汎用の論理フローのデバッグ メッセージおよびVTP コード内の VTP_LOG_RUNTIME マクロによって生成された VTP メッセージの詳細を表示します。
packets	Cisco IOS VTP プラットフォーム依存層から VTP コードに渡されたすべての着信 VTP パケット（プルーニング パケットを除く）の内容のデバッグ メッセージを表示します。
pruning	VTP コードのプルーニング セグメントによって生成されるデバッグ メッセージを表示します。
packets	（任意）Cisco IOS VTP プラットフォーム依存層から VTP コードに渡されたすべての着信VTPプルーニング パケットの内容のデバッグ メッセージを表示します。
xmit	（任意）VTP コードが Cisco IOS VTP プラットフォーム依存層に送信するように要求したすべての発信 VTP パケットの内容のデバッグ メッセージを表示します。
redundancy	VTP 冗長性のデバッグ メッセージを表示します。
xmit	VTP コードが Cisco IOS VTP プラットフォーム依存層に送信するように要求したすべての発信VTPパケット（プルーニング パケットを除く）の内容のデバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

undebug sw-vlan vtp コマンドは、**no debug sw-vlan vtp** コマンドと同じです。

pruning キーワードの後に追加のパラメータを入力しない場合は、VTP プルーニング デバッグ メッセージが表示されます。これらのメッセージは、VTP プルーニング コード内の

VTP_PRUNING_LOG_NOTICE、VTP_PRUNING_LOG_INFO、VTP_PRUNING_LOG_DEBUG、VTP_PRUNING_LOG_ALERT、および VTP_PRUNING_LOG_WARNING マクロによって生成されます。

スイッチ スタック上でデバッグをイネーブルにした場合、アクティブ スイッチ でのみイネーブルになります。特定のスタック メンバをデバッグする場合は、**session switch***stack-member-number* 特権 EXEC コマンドを使用してアクティブ スイッチから CLI セッションを開始できます。

次に、VTP 冗長性のデバッグ メッセージを表示する例を示します。

```
Switch# debug sw-vlan vtp redundancy
```

関連トピック

show vtp （1178 ページ）

interface vlan

ダイナミック スイッチ仮想インターフェイス（SVI）を作成するか、既存のダイナミック SVI にアクセスし、インターフェイス コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **interface vlan** コマンドを使用します。SVI を削除するには、このコマンドの **no** 形式を使用します。

interface vlan *vlan-id*
no interface vlan *vlan-id*

構文の説明

vlan-id	VLAN 番号。指定できる範囲は 1 ～ 4094 です。

コマンド デフォルト

デフォルトの VLAN インターフェイスは VLAN 1 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

SVI は、特定の VLAN に対して最初に **interface vlan** *vlan-id* コマンドを入力したときに作成されます。*vlan-id* は、IEEE 802.1Q カプセル化トランク上のデータ フレームに対応する VLAN タグ、またはアクセス ポート用に設定された VLAN ID に対応します。

（注） 物理ポートと関連付けられていない場合、SVI を作成してもアクティブにはなりません。

no interface vlan *vlan-id* コマンドを使用して削除した SVI は、**show interfaces** 特権 EXEC コマンドの出力に表示されなくなります。

（注） VLAN 1 インターフェイスを削除することはできません。

削除されたインターフェイスに対して **interface vlan** *vlan-id* コマンドを入力すると、削除された SVI を元に戻すことができます。インターフェイスはバックアップとなりますが、それまでの設定は削除されます。

スイッチまたはスイッチ スタック上で設定された SVI の数と、設定された他の機能の数の相互関係によっては、ハードウェア制限により、CPU 使用率に影響が出る可能性があります。**sdm prefer** グローバル コンフィギュレーション コマンドを使用して、システムのハードウェア リソースを、テンプレートおよび機能テーブルに基づいて再度割り当てることができます。

設定を確認するには、**show interfaces** および **show interfaces vlan** *vlan-id* 特権 EXEC コマンドを入力します。

次の例では、VLAN ID 23 の新しい SVI を作成し、インターフェイス コンフィギュレーション モードを開始する方法を示します。

```
Switch(config)# interface vlan 23
Switch(config-if)#
```

関連トピック

show interfaces （132 ページ）

show platform vlan

プラットフォーム依存 VLAN 情報を表示するには、**show platform vlan** 特権 EXEC コマンドを使用します。

show platform vlan [*vlan-id*] [**switch** *switch-number*]

構文の説明

vlan-id	（任意）VLAN の ID。指定できる範囲は 1 ～ 4094 です。
switch *switch-number*	（任意）指定されたスタック メンバの VLAN のみを表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

次の例では、プラットフォーム依存 VLAN 情報を表示する方法を示します。

```
Switch# show platform vlan
```

show vlan

設定されたすべてのVLANまたはスイッチ上のVLAN（VLAN IDまたは名前を指定した場合）のパラメータを表示するには、特権 EXEC モードで **show vlan** コマンドを使用します。

show vlan [{**brief**|**dot1q tag native**|**group**|**id** *vlan-id*|**mtu**|**name** *vlan-name*|**remote-span**|**summary**}]

構文の説明

brief	（任意）VLANごとにVLAN名、ステータス、およびポートを 1 行で表示します。
dot1q tag native	（任意）IEEE 802.1Q ネイティブ VLAN タギング ステータスを表示します。
group	（任意VLAN グループについての情報を表示します。
id *vlan-id*	（任意）VLAN ID 番号で特定された 1 つの VLAN に関する情報を表示します。*vlan-id* に指定できる範囲は 1 ～ 4094 です。
mtu	（任意）VLAN のリストと、VLAN のポートに設定されている最小および最大伝送単位（MTU）サイズを表示します。
name *vlan-name*	（任意）VLAN 名で特定された 1 つの VLAN に関する情報を表示します。VLAN 名は、1 ～ 32 文字の ASCII 文字列です。
remote-span	（任意）Remote SPAN（RSPAN）VLAN に関する情報を表示します。
summary	（任意）VLAN サマリー情報を表示します。

（注） **ifindex** キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

show vlan mtu コマンド出力では、MTU_Mismatch 列に VLAN 内のすべてのポートに同じ MTU があるかどうかを示します。この列に yes が表示されている場合、VLAN の各ポートに別々の MTU があり、パケットが、大きい MTU を持つポートから小さい MTU を持つポートにスイッチングされると、ドロップされることがあります。VLAN に SVI がない場合、ハイフン（-）記号が SVI_MTU 列に表示されます。MTU-Mismatch 列に yes が表示されている場合、MiniMTU と MaxMTU を持つポート名が表示されます。

次の例では、**show vlan** コマンドの出力を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
Switch> show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                Gi1/0/23, Gi1/0/24, Gi1/0/25
                                                Gi1/0/26, Gi1/0/27, Gi1/0/28
                                                Gi1/0/29, Gi1/0/30, Gi1/0/31
                                                Gi1/0/32, Gi1/0/33, Gi1/0/34
                                                Gi1/0/35, Gi1/0/36, Gi1/0/37
                                                Gi1/0/38, Gi1/0/39, Gi1/0/40
                                                Gi1/0/41, Gi1/0/42, Gi1/0/43
                                                Gi1/0/44, Gi1/0/45, Gi1/0/46
                                                Gi1/0/47, Gi1/0/48
2    VLAN0002                         active
40   vlan-40                          active
300  VLAN0300                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
300  enet  100300     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
2000 enet  102000     1500  -      -      -        -    -        0      0
3000 enet  103000     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
2000,3000

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

表 *39 : show vlan* コマンドの出力フィールド

フィールド	説明
VLAN	VLAN 番号。
名前	VLAN の名前（設定されている場合）。
Status（ステータス）	VLAN のステータス（active または suspend）。
ポート	VLAN に属するポート。
タイプ	VLAN のメディア タイプ。
SAID	VLAN のセキュリティ アソシエーション ID 値。
MTU	VLAN の最大伝送単位サイズ。
親	親 VLAN（存在する場合）。
RingNo	VLAN のリング番号（該当する場合）。
BrdgNo	VLAN のブリッジ番号（該当する場合）。
Stp	VLAN で使用されるスパニングツリー プロトコル タイプ。
BrdgMode	この VLAN のブリッジング モード：可能な値はソースルート ブリッジング（SRB）およびソースルート トランスペアレント（SRT）で、デフォルトは SRB です。
Trans1	トランスレーション ブリッジ 1。
Trans2	トランスレーション ブリッジ 2。
Remote SPAN VLANs	設定されている RSPAN VLAN を識別します。

次の例では、**show vlan dot1q tag native** コマンドの出力を示します。

```
Switch> show vlan dot1q tag native
dot1q native vlan tagging is disabled
```

次の例では、**show vlan summary** コマンドの出力を示します。

```
Switch> show vlan summary
Number of existing VLANs              : 45
 Number of existing VTP VLANs         : 45
 Number of existing extended VLANS    : 0
```

次の例では、**show vlan id** コマンドの出力を示します。

```
Switch# show vlan id 2
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    VLAN0200                         active    Gi1/0/7, Gi1/0/8
```

```
2    VLAN0200                         active    Gi2/0/1, Gi2/0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
Disabled
```

関連トピック

switchport mode

vlan （1192 ページ）

show vtp

VLAN Trunking Protocol（VTP）管理ドメイン、ステータス、およびカウンタに関する一般情報を表示するには、EXEC モードで **show vtp** コマンドを使用します。

show vtp {**counters**|**devices** [**conflicts**]|**interface** [*interface-id*]|**password**|**status**}

構文の説明

counters	スイッチの VTP 統計情報を表示します。
devices	ドメイン内のすべての VTP バージョン 3 デバイスに関する情報を表示します。このキーワードは、スイッチが VTP バージョン 3 を実行していない場合だけ適用されます。
conflicts	（任意）競合するプライマリ サーバを持つ VTP バージョン 3 デバイスに関する情報を表示します。スイッチが VTP トランスペアレント モードまたは VTP オフ モードにある場合、このコマンドは無視されます。
interface	すべてのインターフェイスまたは指定されたインターフェイスに対する VTP のステータスおよび設定を表示します。
interface-id	（任意）VTP ステータスおよび設定を表示するインターフェイス。ここには物理インターフェイスまたはポート チャネルを指定できます。
password	設定された VTP パスワードを表示します（特権 EXEC モードでのみ使用可能）。
status	VTP 管理ドメインのステータスに関する一般情報を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スイッチが VTP バージョン 3 を実行中に **show vtp password** コマンドを入力すると、表示は次のルールに従います。

- **password** *password* グローバル コンフィギュレーション コマンドで **hidden** キーワードを指定せず、スイッチ上で暗号化がイネーブルでない場合、パスワードはクリアテキストで表示されます。

- **password** *password* コマンドで **hidden** キーワードを指定せず、スイッチ上で暗号化がイネーブルの場合、暗号化されたパスワードが表示されます。
- **password** *password* コマンドに **hidden** キーワードが含まれていた場合、16 進数の秘密キーが表示されます。

次の例では、**show vtp devices** コマンドの出力を示します。**Conflict** 列の **Yes** は、応答するサーバがその機能のローカル サーバと競合していることを示します。つまり、同じドメイン内の 2 つのスイッチは、データベースに対して同じプライマリ サーバを持ちません。

```
Switch# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf スイッチ ID      Primary Server Revision   System Name
             lict
------------ ---- -------------- -------------- ---------- ----------------------
VLAN         Yes  00b0.8e50.d000 000c.0412.6300 12354      main.cisco.com
MST          No   00b0.8e50.d000 0004.AB45.6000 24         main.cisco.com
VLAN         Yes  000c.0412.6300=000c.0412.6300 67         qwerty.cisco.com
```

次の例では、**show vtp counters** コマンドの出力を示します。次の表に、この出力で表示される各フィールドについて説明します。

```
Switch> show vtp counters
VTP statistics:
Summary advertisements received    : 0
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 0
Subset advertisements transmitted  : 0
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Gi1/0/47              0                0                0
Gi1/0/48              0                0                0
Gi2/0/1               0                0                0
Gi3/0/2               0                0                0
```

表 *40 : show vtp counters* のフィールドの説明

フィールド	説明
Summary advertisements received	トランク ポート上でこのスイッチが受信するサマリー アドバタイズメントの数。サマリー アドバタイズには、管理ドメイン名、コンフィギュレーション リビジョン番号、更新タイムスタンプと ID、認証チェックサム、および関連するサブセット アドバタイズの数が含まれます。
Subset advertisements received	トランク ポート上でこのスイッチが受信するサブセットアドバタイズメントの数。サブセット アドバタイズには、1 つ以上の VLAN に関する情報がすべて含まれています。
Request advertisements received	トランク ポート上でこのスイッチが受信するアドバタイズメント要求の数。アドバタイズ要求は、通常、すべての VLAN 上に関する情報を要求します。また、VLAN のサブセットに関する情報も要求できます。
Summary advertisements transmitted	トランク ポート上でこのスイッチが送信するサマリー アドバタイズメントの数。サマリー アドバタイズには、管理ドメイン名、コンフィギュレーション リビジョン番号、更新タイムスタンプと ID、認証チェックサム、および関連するサブセット アドバタイズの数が含まれます。
Subset advertisements transmitted	トランク ポート上でこのスイッチが送信するサブセットアドバタイズメントの数。サブセット アドバタイズには、1 つ以上の VLAN に関する情報がすべて含まれています。
Request advertisements transmitted	トランク ポート上でこのスイッチが送信するアドバタイズメント要求の数。アドバタイズ要求は、通常、すべての VLAN 上に関する情報を要求します。また、VLAN のサブセットに関する情報も要求できます。

フィールド	説明
Number of configuration revision errors	リビジョン エラーの数。 新しい VLAN の定義、既存 VLAN の削除、中断、または再開、あるいは既存 VLAN のパラメータ変更を行うと、スイッチのコンフィギュレーション リビジョン番号が増加します。 リビジョン番号がスイッチのリビジョン番号と一致するにもかかわらず、MD5 ダイジェスト値が一致しないアドバタイズメントをスイッチが受信すると、リビジョン エラーが増加します。このエラーは、2 つのスイッチの VTP パスワードが異なるか、またはスイッチの設定が異なることを意味します。 これらのエラーは、スイッチが受信アドバタイズメントをフィルタしていて、これにより VTP データベースがネットワーク全体で同期されていない状態になっていることを示しています。
Number of configuration digest errors	MD5 ダイジェスト エラーの数。 サマリー パケット内の MD5 ダイジェストと、スイッチによって計算された受信済みアドバタイズメントの MD5 ダイジェストが一致しない場合は、ダイジェストエラーが増加します。このエラーは、通常、2 つのスイッチの VTP パスワードが異なることを意味します。この問題を解決するには、すべてのスイッチで VTP パスワードが同じになるようにします。 これらのエラーは、スイッチが受信アドバタイズメントをフィルタしていて、これにより VTP データベースがネットワーク全体で同期されていない状態になっていることを示しています。

フィールド	説明
Number of V1 summary errors	バージョン 1 エラーの数。 VTP V2 モードのスイッチが VTP バージョン 1 フレームを受信すると、バージョン 1 サマリーエラーが増加します。これらのエラーは、少なくとも 1 つの近接スイッチで、V2 モードがディセーブルにされた VTP バージョン 1、または VTP バージョン 2 が実行されていることを示しています。この問題を解決するには、VTP V2 モードのスイッチの設定をディセーブルに変更します。
Join Transmitted	トランク上で送信された VTP プルーニング メッセージの数。
Join Received	トランク上で受信された VTP プルーニング メッセージの数。
Summary Advts Received from non-pruning-capable device	トランク上で受信された、プルーニングをサポートしていないデバイスからの VTP サマリー メッセージの数。

次の例では、**show vtp status** コマンドの出力を示します。次の表に、この出力で表示される各フィールドについて説明します。

```
Switch> show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 2037.06ce.3580
Configuration last modified by 192.168.1.1 at 10-10-12 04:34:02
Local updater ID is 192.168.1.1 on interface LIIN0 (first layer3 interface found
)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 2
MD5 digest                        : 0xA0 0xA1 0xFE 0x4E 0x7E 0x5D 0x97 0x41
                                    0x89 0xB9 0x9B 0x70 0x03 0x61 0xE9 0x27
```

表 *41 : show vtp status* のフィールドの説明

フィールド	説明
VTP Version capable	スイッチ上で動作できる VTP バージョンを表示します。

フィールド	説明
VTP Version running	スイッチ上で動作中の VTP バージョンを表示します。デフォルトでは、スイッチはバージョン 1 を実行しますが、バージョン 2 に設定することもできます。
VTP Domain Name	スイッチの管理ドメインを特定する名前。
VTP Pruning Mode	プルーニングがイネーブルかまたはディセーブルかを表示します。VTP サーバでプルーニングをイネーブルにすると、管理ドメイン全体でプルーニングが有効になります。プルーニングを使用すると、トラフィックが適切なネットワーク デバイスにアクセスするために使用しなければならないトランク リンクへのフラッディング トラフィックが制限されます。
VTP Traps Generation	VTP トラップをネットワーク管理ステーションに送信するかどうかを表示します。
デバイス ID	ローカル デバイスの MAC アドレスを表示します。
Configuration last modified	最後に行った設定変更の日付と時刻を表示します。データベースの設定変更の原因となったスイッチの IP アドレスを表示します。

フィールド	説明
VTP Operating Mode	VTP 動作モード（サーバ、クライアント、またはトランスペアレント）を表示します。 **Server**：VTP サーバ モードのスイッチは VTP に対してイネーブルであり、アドバタイズメントを送信します。スイッチで VLAN を設定できます。このスイッチを使用すると、起動後に、現在の VTP データベース内のすべての VLAN 情報を、NVRAM から復元できます。デフォルトでは、すべてのスイッチが VTP サーバです。 （注） スイッチが設定をNVRAMに書き込んでいる間に障害を検出し、NVRAMが機能するまでサーバモードに戻ることができない場合、スイッチは VTP サーバ モードから VTP クライアント モードに自動的に変わります。 **Client**：VTP クライアント モードのスイッチは VTP に対してイネーブルであり、アドバタイズメントを送信できますが、VLAN 設定を格納するために十分な不揮発性ストレージがありません。スイッチでは VLAN を設定できません。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。 **Transparent**：VTP トランスペアレント モードのスイッチは、VTP に対してディセーブルであり、アドバタイズメントの送信や、他のデバイスから送信されたアドバタイズメントの学習を行いません。また、ネットワーク内の他のデバイスのVLAN設定にも影響しません。スイッチは VTP アドバタイズメントを受信し、アドバタイズメントを受信したトランク ポートを除くすべてのトランク ポートにこれを転送します。
Maximum VLANs Supported Locally	ローカルにサポートされている VLAN の最大数。
Number of Existing VLANs	既存の VLAN 数。

フィールド	説明
Configuration Revision	このスイッチの現在のコンフィギュレーション リビジョン番号。
MD5 Digest	VTP 設定の 16 バイト チェックサム。

次の例では、VTP バージョン 3 を実行するスイッチに対する **show vtp status** コマンドの出力を示します。

```
Switch> show vtp status
VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : Cisco
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0021.1bcd.c700

Feature VLAN:
--------------
VTP Operating Mode : Server
Number of existing VLANs : 7
Number of existing extended VLANs : 0
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature MST:
--------------
VTP Operating Mode : Client
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature UNKNOWN:
----------------
```

関連トピック

clear vtp counters （1161 ページ）

show wireless vlan group

VLAN グループ内の VLAN の詳細リストと DHCP に失敗した VLAN のステータスを表示するには、特権 EXEC モードで **showwirelessvlangroup** コマンドを使用します。

show wireless vlan group *group-name*

構文の説明

group-name	ワイヤレス VLAN グループの名前。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、グローバル コンフィギュレーション モードでのみ使用してください。

次の例では、VLAN グループのサマリーを表示する方法を示します。

```
Switch# show wireless vlan group grp1

Member Vlans Configured
------------------------------------------------------------
VLAN        VLAN Name                           DHCP Failed
100         VLAN0100                            No
101         VLAN0101                            Yes
102         VLAN0102                            No
103         VLAN0103                            No
104         VLAN0104                            Yes
105         VLAN0105                            No
```

switchport priority extend

着信したタグなしフレームのポート プライオリティ、または指定されたポートに接続された IP Phone が受信するフレームのプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **switchport priority extend** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport priority extend {**cos** *value*|**trust**}
no switchport priority extend

構文の説明

cos *value*	PC から受信したか、または指定した Class of Service（CoS）値を持つ接続装置から受信した IEEE 802.1p プライオリティを上書きするよう IP Phone ポートを設定します。指定できる範囲は 0 ～ 7 です。7 が最も高いプライオリティです。デフォルトは 0 です。
trust	PC または接続装置から受信した IEEE 802.1p プライオリティを信頼するように IP Phone のポートを設定します。

コマンド デフォルト

ポートで受信したタグなしフレームには、デフォルト ポート プライオリティは、CoS 値 0 で設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

音声 VLAN をイネーブルにした場合、スイッチを設定して、Cisco Discovery Protocol（CDP）パケットを送信し、Cisco IP Phone のアクセス ポートに接続される装置からデータ パケットを送信する方法を IP Phone に指示できます。Cisco IP Phone に設定を送信するには、Cisco IP Phone に接続しているスイッチポートの CDP をイネーブルにする必要があります（デフォルトでは、CDP はすべてのスイッチ インターフェイスでグローバルにイネーブルです）。

スイッチ アクセス ポート上で音声 VLAN を設定する必要があります。音声 VLAN は、レイヤ 2 ポート上にだけ設定できます。

音声 VLAN をイネーブルにする前に、**trust device cisco-phone** インターフェイス コンフィギュレーション コマンドを入力してインターフェイス上でサービス品質（QoS）をイネーブルに設定しておくことを推奨します。Auto QoS 機能を使用すると、これらは自動的に設定されます。

次の例では、受信した IEEE 802.1p プライオリティを信頼するように、指定されたポートに接続された IP Phone を設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport priority extend trust
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

switchport trunk

インターフェイスがトランキング モードの場合、トランクの特性を設定するには、インターフェイス コンフィギュレーション モードで **switchport trunk** コマンドを使用します。トランキング特性をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

switchport trunk {**allowed vlan** *vlan-list*|**native vlan** *vlan-id*|**pruning vlan** *vlan-list*}
no switchport trunk {**allowed vlan**|**native vlan**|**pruning vlan**}

構文の説明

allowed vlan *vlan-list*	トランキング モードの場合に、このインターフェイス上でタグ付き形式のトラフィックを送受信できる許可 VLAN のリストを設定します。*vlan-list* の選択については、「使用上のガイドライン」を参照してください。
native vlan *vlan-id*	インターフェイスが IEEE 802.1Q トランキング モードの場合に、タグなしトラフィックを送受信するようにネイティブ VLAN を設定します。指定できる範囲は 1 ～ 4094 です。
pruning vlan *vlan-list*	トランキング モードの場合に、VTP プルーニングに適格な VLAN のリストを設定します。*vlan-list* の選択については、「使用上のガイドライン」を参照してください。

コマンド デフォルト

VLAN 1 は、ポートのデフォルトのネイティブ VLAN ID です。

すべての VLAN リストのデフォルトには、すべての VLAN が含まれます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

vlan-list の形式は、**all | none | [add | remove | except]** *vlan-atom* [,*vlan-atom...*] です。各キーワードの意味は、次のとおりです。

- **all** 1 ～ 4094 のすべての VLAN を指定します。これはデフォルトです。このキーワードは、リストのすべての VLAN を同時に設定することを許可しないコマンド上では使用できません。
- **none** 空のリストを指定します。特定の VLAN を設定するか、または少なくとも 1 つの VLAN を設定する必要があるコマンドでは、このキーワードを使用できません。
- **add** リストを置き換えるのではなく、現在設定されている VLAN に VLAN の定義済みリストを追加します。有効な ID は 1 ～ 1005 です。場合によっては、拡張範囲 VLAN（VLAN ID が 1005 より上）を使用できます。

（注） 許可 VLAN リストに拡張範囲 VLAN を追加できますが、プルーニング適格 VLAN リストには追加できません。

カンマを使い、連続しない VLAN ID を区切ります。ID の範囲を指定するには、ハイフンを使用します。

- **remove** リストを置き換えるのではなく、現在設定されている VLAN から VLAN の定義済みリストを削除します。有効な ID は 1 ～ 1005 です。場合によっては、拡張範囲 VLAN ID を使用できます。

（注） 許可 VLAN リストから拡張範囲 VLAN を削除できますが、プルーニング適格リストからは削除できません。

- **except** 定義済み VLAN リスト以外の、計算する必要がある VLAN を示します。（指定されている VLAN 以外の VLAN が追加されます）。有効な ID の範囲は 1 ～ 1005 です。カンマを使い、連続しない VLAN ID を区切ります。ID の範囲を指定するには、ハイフンを使用します。
- *vlan-atom* は、1 ～ 4094 内の単一の VLAN 番号、または 2 つの VLAN 番号で指定された連続した範囲の VLAN で、小さい方の値を先頭にハイフンで区切ります。

ネイティブ VLAN：

- IEEE 802.1Q トランク ポートで受信されたすべてのタグなしトラフィックは、ポートに設定されたネイティブ VLAN によって転送されます。
- パケットの VLAN ID が送信側ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信します。
- **native vlan** コマンドの **no** 形式は、ネイティブ モード VLAN を、デバイスに適したデフォルト VLAN にリセットします。

許可 VLAN：

- スパニングツリー ループまたはストームのリスクを減らすには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートの VLAN 1 をディセーブルにできます。トランク ポートから VLAN 1 を削除した場合、インターフェイスは管理トラフィック（Cisco Discovery Protocol（CDP）、ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、ダイナミック トランキング プロトコル（DTP）、および VLAN 1 の VLAN トランキング プロトコル（VTP））を送受信し続けます。
- リストをデフォルト リスト（すべての VLAN を許可）にリセットするには、**allowed vlan** コマンドの **no** 形式を使用します。

トランク プルーニング：

- プルーニング適格リストは、トランク ポートだけに適用されます。
- トランク ポートごとに独自の適格リストがあります。
- VLANをプルーニングしない場合は、プルーニング適格リストからVLANを削除します。プルーニング不適格のVLANは、フラッディング トラフィックを受信します。
- VLAN 1、VLAN 1002 ～ 1005、および拡張範囲 VLAN（VLAN 1006 ～ 4094）は、プルーニングできません。

次の例では、すべてのタグなしトラフィックを送信するポートのデフォルトとして、VLAN 3 を設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk native vlan 3
```

次の例では、許可リストに VLAN 1、2、5、および 6 を追加する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

次の例では、プルーニング適格リストから VLAN 3 および 10 ～ 15 を削除する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk pruning vlan remove 3,10-15
```

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

関連トピック

show interfaces （132 ページ）
switchport mode

vlan

VLAN を追加して、VLAN コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **vlan** コマンドを使用します。VLAN を削除するには、このコマンドの **no** 形式を使用します。

vlan *vlan-id*
no vlan *vlan-id*

構文の説明

vlan-id	追加および設定する VLAN の ID。指定できる範囲は 1 ～ 4094 です。1 つの VLAN ID、それぞれをカンマで区切った一連の VLAN ID、またはハイフンを間に挿入した VLAN ID の範囲を入力できます。
group **word** **vlan-list**	VLAN グループの作成をイネーブルにします。VLAN グループ名は最大 32 文字であり、文字で始める必要があります。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

通常範囲の VLAN（VLAN ID 1 ～ 1005）や拡張範囲 VLAN（VLAN ID 1006 ～ 4094）を追加するには、**vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。通常範囲の VLAN の設定情報は常に VLAN データベースに保存されます。この情報を表示するには、**show vlan** 特権 EXEC コマンドを入力します。VTP モードがトランスペアレントである場合、通常範囲の VLAN の VLAN 設定情報もスイッチの実行コンフィギュレーション ファイルに保存されます。拡張範囲の VLAN ID は VLAN データベースに保存されず、スイッチの実行コンフィギュレーション ファイルに保存されます。また、設定をスタートアップ コンフィギュレーション ファイルに保存できます。

VTP バージョン 3 は拡張範囲 VLAN の伝播をサポートしているため、。VTP バージョン 1 および 2 で伝播する範囲は、VLAN 1 ～ 1005 だけです。

VLAN および VTP 設定をスタートアップ コンフィギュレーション ファイルに保存してスイッチをリブートすると、設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。

- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

無効な VLAN ID を入力すると、エラー メッセージが表示され、VLAN コンフィギュレーション モードを開始できません。

VLAN ID を指定して **vlan** コマンドを入力すると、VLAN コンフィギュレーション モードがイネーブルになります。既存の VLAN の VLAN ID を入力すると、新しい VLAN は作成されませんが、その VLAN の VLAN パラメータを変更できます。指定された VLAN は、VLAN コンフィギュレーションモードを終了したときに追加または変更されます。（VLAN 1 ～ 1005 の）**shutdown** コマンドだけがただちに有効になります。

（注） すべてのコマンドが表示されますが、拡張範囲 VLAN でサポートされる VLAN コンフィギュレーション コマンドは **remote-span** だけです。拡張範囲 VLAN の場合、他のすべての特性はデフォルト ステートのままにしておく必要があります。

次のコンフィギュレーション コマンドを VLAN コンフィギュレーション モードで利用できます。各コマンドの **no** 形式を使用すると、特性がそのデフォルト ステートに戻ります。

- **are** *are-number*：この VLAN の全ルート エクスプローラ（ARE）ホップの最大数を定義します。このキーワードは、TrCRF VLAN だけに適用されます。指定できる範囲は 0 ～ 13 です。デフォルト値は 7 です。値が入力されない場合、最大数は 0 であると見なされます。
- **backupcrf**：バックアップ CRF モードを指定します。このキーワードは、TrCRF VLAN だけに適用されます。
  - **enable**：この VLAN のバックアップ CRF モード。
  - **disable**：この VLAN のバックアップ CRF モード（デフォルト）。
- **bridge** {*bridge-number* | **type**}：論理分散ソース ルーティング ブリッジ、つまり、FDDI-NET、トークンリング NET、および TrBRF VLAN 内で親 VLAN としてこの VLAN を持つすべての論理リングと相互接続するブリッジを指定します。指定できる範囲は 0 ～ 15 です。FDDI-NET、TrBRF、およびトークン リング NET VLAN については、デフォルトのブリッジ番号は 0（ソース ルーティング ブリッジなし）です。**type** キーワードは、TrCRF VLAN だけに適用され、次のうちのいずれかです。
  - **srb**：ソースルート ブリッジング。
  - **srt**：（ソースルート トランスペアレント）ブリッジング VLAN
- **exit**：変更を適用し、VLAN データベース リビジョン番号（VLAN 1 ～ 1005）を増加させ、VLAN コンフィギュレーション モードを終了します。
- **media**：VLAN メディア タイプを定義します。タイプは次のいずれかになります。

（注） スイッチは、イーサネット ポートだけをサポートします。FDDI およびトークン リング メディア固有の特性は、別のスイッチに対する VLAN Trunking Protocol（VTP）グローバル アドバタイズメントにかぎって設定します。これらのVLANはローカルに停止されます。

- **ethernet**：イーサネット メディア タイプ（デフォルト）。
- **fd-net**：FDDI ネットワーク エンティティ タイトル（NET）メディア タイプ。
- **fddi**：FDDI メディア タイプ。
- **tokenring**：VTP v2 モードがディセーブルの場合は、トークン リング メディア タイプ。VTP バージョン 2（v）モードがイネーブルの場合は、TrCRF。
- **tr-net**：VTP v2 モードがディセーブルの場合は、トークン リング ネットワーク エンティティ タイトル（NET）メディア タイプ。VTP v2 モードがイネーブルの場合は、TrBRF メディア タイプ。

さまざまなメディア タイプで有効なコマンドおよび構文については、下の表を参照してください。

- **name** *vlan-name*：管理ドメイン内で一意である 1 ～ 32 文字の ASCII 文字列で VLAN に名前を付けます。デフォルトは VLANxxxx です。ここで、xxxx は VLAN ID 番号と同じ 4 桁の数字（先行ゼロを含む）です。
- **no**：コマンドを無効にするか、またはデフォルト設定に戻します。
- **parent** *parent-vlan-id*：既存の FDDI、トークンリング、または TrCRF VLAN の親 VLAN を指定しますこのパラメータは、TrCRF が所属する TrBRF を識別するもので、TrCRF を定義するときに必要です。指定できる範囲は 0 ～ 1005 です。デフォルトの親 VLAN ID は、FDDI およびトークンリング VLAN では 0（親 VLAN なし）です。トークンリングおよび TrCRF VLAN の両方で、親 VLAN ID はデータベースにすでに存在していて、トークンリング NET または TrBRF VLAN と関連付けられている必要があります。
- **remote-span**：VLAN をリモート SPAN（RSPAN）VLAN として設定します。RSPAN 機能が既存の VLAN に追加される場合、まず VLAN は削除され、次に RSPAN 機能とともに再生されます。RSPAN 機能が削除されるまで、どのアクセス ポートも非アクティブになります。VTP がイネーブルの場合、新しい RSPAN VLAN は、1024 より小さい数字の VLAN ID の VTP により伝播されます。ラーニングは VLAN 上でディセーブルになります。

（注） RSPAN 機能は、LAN Base イメージが稼働しているスイッチでだけサポートされます。

- **ring** *ring-number*：FDDI、トークンリング、またはTrCRF VLANの論理リングを定義します。指定できる範囲は1 ～ 4095です。トークンリング VLANのデフォルト値は0です。FDDI VLANには、デフォルト設定はありません。
- **said** *said-value*：IEEE 802.10に記載されているセキュリティアソシエーションID（SAID）を指定します。指定できるIDは、1 ～ 4294967294です。この数字は、管理ドメイン内で一意である必要があります。デフォルト値は、100000にVLAN ID番号を加算した値です。
- **shutdown**：VLAN上でVLANスイッチングをシャットダウンします。このコマンドはただちに有効になります。他のコマンドは、VLANコンフィギュレーション モードを終了したときに有効になります。
- **state**：VLANの状態を指定します。
  - **active** VLANが稼働中であることを意味します（デフォルト）。
  - **suspend** VLANが停止していることを意味します。停止しているVLANはパケットを通過させません。
- **ste** *ste-number*：スパニングツリーエクスプローラ（STE）ホップの最大数を定義します。このキーワードは、TrCRF VLANだけに適用されます。指定できる範囲は0 ～ 13です。デフォルト値は7です。
- **stp type**：FDDI-NET、トークンリング NET、またはTrBRF VLANのスパニングツリー タイプを定義します。FDDI-NET VLANの場合、デフォルトのSTPタイプはieeeです。トークン リング NET VLANの場合、デフォルトのSTPタイプはibmです。FDDIおよびトークン リング VLANの場合、デフォルトのタイプは指定されていません。
  - **ieee**：ソースルート トランスペアレント（SRT）ブリッジングを実行しているIEEEイーサネットSTP。
  - **ibm**：ソースルート ブリッジング（SRB）を実行しているIBM STP。
  - **auto**：ソースルート トランスペアレント（SRT）ブリッジング（IEEE）およびソースルート ブリッジング（IBM）の組み合わせを実行しているSTP。
- **tb-vlan1** *tb-vlan1-id* and **tb-vlan2** *tb-vlan2-id*：このVLANにトランスレーショナル ブリッジングが行われる最初および2番目のVLANを指定します。トランスレーショナルVLANは、たとえばFDDIまたはトークンリングをイーサネットに変換します。指定できる範囲は0～1005です。値が指定されないと、0（トランスレーショナルブリッジングなし）と見なされます。

表 *42*：さまざまなメディア タイプで指定できるコマンドと構文

メディア タイプ	指定できる構文
イーサネット	**name** *vlan-name*, **media ethernet**, **state** {**suspend** | **active**}, **said** *said-value*, **remote-span**, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*

メディア タイプ	指定できる構文
FDDI	**name** *vlan-name*, **media fddi**, **state** {**suspend** | **active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
FDDI-NET	**name** *vlan-name*, **media fd-net** , **state** {**suspend** | **active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee** | **ibm** | **auto**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id* VTP v2 モードがディセーブルの場合は、**stp type** を次に設定しないでください： **auto.**
Token Ring	VTP v1 モードはイネーブルです。 **name** *vlan-name*, **media tokenring**, **state** {**suspend** | **active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
トークンリング コンセントレータ リレー機能（TrCRF）	VTP v2 モードはイネーブルです。 **name** *vlan-name*, **media tokenring**, **state** {**suspend** | **active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **bridge type** {**srb** | **srt**}, **are** *are-number*, **ste** *ste-number*, **backupcrf** {**enable** | **disable**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
トークンリング NET	VTP v1 モードはイネーブルです。 **name** *vlan-name*, **media tr-net**, **state** {**suspend** | **active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee** | **ibm**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
トークンリング ブリッジ リレー機能（TrBRF）	VTP v2 モードはイネーブルです。 **name** *vlan-name*, **media tr-net**, **state** {**suspend** | **active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee** | **ibm** | **auto**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*

次の表に、VLAN の設定ルールを示します。

表 *43 : VLAN* 設定ルール

設定	ルール
VTP v2 モードがイネーブルで、TrCRF VLAN メディア タイプを設定している場合	すでにデータベースに存在している TrBRF の親 VLAN ID を指定します。 リング番号を指定します。このフィールドを空白のままにしないでください。 TrCRF VLAN に同じ親 VLAN ID がある場合には一意のリング番号を指定します。1 つのバックアップ コンセントレータ リレー機能（CRF）だけをイネーブルにすることができます。
VTP v2 モードがイネーブルで、TrCRF メディア タイプ以外の VLAN を設定している場合	バックアップ CRF を指定しないでください。
VTP v2 モードがイネーブルで、TrBRF VLAN メディア タイプを設定している場合	ブリッジ番号を指定します。このフィールドを空白のままにしないでください。
VTP v1 モードはイネーブルです。	VLAN の STP タイプを auto に設定しないでください。 このルールは、イーサネット、FDDI、FDDI-NET、トークンリング、およびトークンリング NET VLAN に適用されます。

設定	ルール
トランスレーショナル ブリッジングが必要な VLAN を追加する場合（値は 0 に設定されない）	使用されるトランスレーショナル ブリッジング VLAN ID は、すでにデータベースに存在している必要があります。 （たとえば、イーサネットは FDDI をポイントし、FDDI はイーサネットをポイントするというように）コンフィギュレーションがポイントしているトランスレーショナル ブリッジング VLAN ID にも、トランスレーショナル ブリッジング パラメータの 1 つに元の VLAN へのポインタが含まれている必要があります。 コンフィギュレーションがポイントするトランスレーショナル ブリッジング VLAN ID は、（たとえば、イーサネットはトークンリングをポイントすることができるというように）元の VLAN とは異なるメディア タイプである必要があります。 両方のトランスレーショナル ブリッジング VLAN ID が設定されている場合、（たとえば、イーサネットは FDDI およびトークンリングをポイントすることができるというように）これらの VLAN は異なるメディア タイプである必要があります。

次の例では、デフォルトのメディア特性を持つイーサネット VLAN を追加する方法を示します。デフォルトには VLAN *xxxx* の *vlan-name* が含まれています。ここで、xxxx は VLAN ID 番号と同じ 4 桁の数字（先行ゼロを含む）です。デフォルトの media は ethernet です。state は active です。デフォルトの said-value は、100000 に VLAN ID を加算した値です。mtu-size 変数は 1500、stp-type は ieee です。**exit** VLAN コンフィギュレーション コマンドを入力した場合、VLAN がまだ存在していなかった場合にはこれが追加されます。そうでない場合、このコマンドは何も作用しません。

次に、新しい VLANをすべてデフォルトの特性で 作成し、VLAN コンフィギュレーション モードを開始する例を示します。

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
Switch(config)#
```

次に、新しい拡張範囲 VLANをすべてデフォルトの特性で作成して、VLAN コンフィギュレーション モードを開始し、新しい VLAN をスイッチのスタートアップ コンフィギュレーション ファイルに保存する例を示します。

```
Switch(config)# vlan 2000
Switch(config-vlan)# end
```

```
Switch# copy running-config startup config
```

次に、VLAN グループを作成する例を示します。

```
Switch(config)#  vlan group xyz vlan-list 50-60
```

次に、リモート VLAN グループを作成する例を示します。

```
Switch(config)#  no vlan group xyz vlan-list 50-60
```

次に、1 つの VLAN を VLAN グループから削除する例を示します。

```
Switch(config)#    no vlan group xyz vlan-list 51
```

次に、複数の VLAN を VLAN グループから削除する例を示します。

```
Switch(config)#    no vlan group xyz vlan-list 52-55
```

次に、1 つの VLAN と複数の VLAN を VLAN グループから削除する例を示します。

```
Switch(config)#    no vlan group xyz vlan-list 56, 58-60
```

設定を確認するには、**show vlan** 特権 EXEC コマンドを入力します。

関連トピック

show vlan （1174 ページ）

vlan dot1q tag native

すべての IEEE 802.1Q トランク ポートでネイティブ VLAN フレームのタギングをイネーブルにするには、グローバル コンフィギュレーション モードで **vlan dot1q tag native** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

vlan dot1q tag native
no vlan dot1q tag native

（注） このコマンドは、LAN Base イメージを実行しているスイッチではサポートされません。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IEEE 802.1Q ネイティブ VLAN タギングはディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

イネーブルの場合は、すべての IEEE 802.1Q トランク ポートから出るネイティブ VLAN パケットがタグ付けされます。

ディセーブルの場合は、すべての IEEE 802.1Q トランク ポートから出るネイティブ VLAN パケットがタグ付けされません。

IEEE 802.1Q トンネリングに関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

次の例では、ネイティブ VLAN フレームの IEEE 802.1Q タギングをイネーブルにする方法を示します。

```
Switch# configure terminal
Switch (config)# vlan dot1q tag native
Switch (config)# end
```

設定を確認するには、**show vlan dot1q tag native** 特権 EXEC コマンドを入力します。

関連トピック

show vlan （1174 ページ）

vtp（グローバル コンフィギュレーション）

VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）設定の特性を設定するか、または変更するには、グローバル コンフィギュレーション モードで **vtp** コマンドを使用します。この設定を削除したりデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

vtp {**domain** *domain-name*|**file** *filename*|**interface** *interface-name* [**only**]|**mode** {**client**|**off**|**server**|**transparent**} [{**mst**|**unknown**|**vlan**}]|**password** *password* [{**hidden**|**secret**}]|**pruning**|**version** *number*}
no vtp {**file**|**interface**|**mode** [{**client**|**off**|**server**|**transparent**}] [{**mst**|**unknown**|**vlan**}]|**password**|**pruning**|**version**}

構文の説明

domain *domain-name*	VTP ドメイン名をスイッチの VTP 管理ドメインを識別する 1 ～ 32 文字の ASCII 文字列で指定します。ドメイン名では大文字と小文字が区別されます。
file *filename*	VTP VLAN 設定が保存されている Cisco IOS ファイル システム ファイルを指定します。
interface *interface-name*	このデバイスで更新された VTP ID を提供するインターフェイスの名前を指定します。
only	（任意）VTP IP アップデータとしてこのインターフェイスの IP アドレスだけを使用します。
mode	VTP デバイス モードをクライアント、サーバ、またはトランスペアレントに指定します。
client	スイッチを VTP クライアント モードにします。VTP クライアント モードのスイッチは VTP に対してイネーブルであり、アドバタイズメントを送信できますが、VLAN 設定を格納するための十分な不揮発性メモリがありません。VTP クライアントでは、VLAN を設定できません。VLAN は、ドメインに含まれる、他のサーバ モードのスイッチで設定します。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。
off	スイッチを VTP オフ モードにします。VTP オフ モードのスイッチは、トランク ポート上で VTP アドバタイズメントを転送しないことを除いて、VTP トランスペアレント デバイスと同様に機能します。
server	スイッチを VTP サーバ モードにします。VTP サーバ モードのスイッチは VTP に対してイネーブルであり、アドバタイズを送信します。スイッチでは VLAN を設定できます。スイッチは、再起動後に、不揮発性メモリから現在の VTP データベース内のすべての VLAN 情報を回復できます。

transparent	スイッチを VTP トランスペアレント モードにします。VTP トランスペアレントモードのスイッチは、VTP に対してディセーブルであり、アドバタイズメントの送信や、他のデバイスから送信されたアドバタイズメントからの学習を行いません。また、ネットワーク内の他のデバイスの VLAN 設定に影響を与えることはありません。スイッチは VTP アドバタイズメントを受信し、アドバタイズメントを受信したトランク ポートを除くすべてのトランク ポートにこれを転送します。 VTP モードがトランスペアレントである場合、モードおよびドメイン名はスイッチの実行コンフィギュレーション ファイルに保存されます。この情報をスイッチのスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup config** 特権 EXEC コマンドを入力します。
mst	（任意）マルチ スパニングツリー（MST）VTP データベース（VTP バージョン 3 に限る）にモードを設定します。
unknown	（任意）未知の VTP データベース（VTP バージョン 3 に限る）にモードを設定します。
vlan	（任意）VLAN VTP データベースにモードを設定します。これがデフォルトです（VTP バージョン 3 に限る）。
password *password*	VTP アドバタイズメントで送信され、受信 VTP アドバタイズメントを確認するための MD5 ダイジェスト計算で使用される 16 バイトの秘密値を生成するための管理ドメイン パスワードを設定します。パスワードは、1 ～ 32 文字の ASCII 文字列です。パスワードでは大文字と小文字が区別されます。
hidden	（任意）パスワード文字列から生成されたキーが VLAN データベース ファイルに保存されることを指定します。**hidden** キーワードを指定しない場合、パスワード文字列はクリア テキストに保存されます。hidden パスワードを入力した場合、そのパスワードを再入力し、ドメイン内でコマンドを実行する必要があります。このキーワードは、VTP バージョン 3 だけでサポートされています。
secret	（任意）ユーザがパスワードの秘密キーを直接設定できるようにします（VTP バージョン 3 に限る）。
pruning	スイッチ上で VTP プルーニングをイネーブルにします。
version *number*	VTP バージョンをバージョン 1、バージョン 2、またはバージョン 3 に設定します。

コマンド デフォルト

デフォルトのファイル名は *flash:vlan.dat* です。

デフォルト モードはサーバ モードで、デフォルトのデータベースは VLAN です。

VTP バージョン 3 では、MST データベースのデフォルト モードはトランスペアレントです。

ドメイン名またはパスワードは定義されていません。

パスワードは設定されていません。

プルーニングはディセーブルです。

デフォルトのバージョンはバージョン 1 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

VTP モード、ドメイン名、および VLAN 設定をスイッチのスタートアップ コンフィギュレーション ファイルに保存して、スイッチを再起動すると、VTP および VLAN 設定は次の条件によって選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

新規データベースをロードするのに **vtp file** *filename* を使用することはできません。これは、既存のデータベースが保存されているファイルの名前を変更するだけです。

VTP ドメイン名を設定するときには、次の注意事項に従ってください。

- ドメイン名を設定するまで、スイッチは非管理ドメイン ステートの状態です。非管理ドメイン ステートの間は、ローカル VLAN 設定に変更が生じても、スイッチは VTP アドバタイズメントを送信しません。スイッチは、トランキングを行っているポートで最初の VTP サマリー パケットを受信した後、または **vtp domain** コマンドでドメイン名を設定した後で、非管理ドメイン ステートから抜け出します。スイッチは、サマリー パケットからドメインを受信した場合、そのコンフィギュレーション リビジョン番号を 0 にリセットします。スイッチが非管理ドメイン ステートから抜け出したあと、NVRAM（不揮発性 RAM）をクリアしてソフトウェアをリロードするまで、スイッチがこのステートに再び入るよう設定することはできません。
- ドメイン名では、大文字と小文字が区別されます。
- 設定したドメイン名は、削除できません。別のドメインに再度割り当てるしかありません。

VTP モードを設定するときには、次の注意事項に従ってください。

- **no vtp mode** コマンドを使用すると、スイッチを VTP サーバ モードに戻すことができます。
- **vtp mode server** コマンドは、スイッチがクライアント モードまたはトランスペアレント モードでない場合にエラーを返さないことを除けば、**no vtp mode** と同じです。
- 受信スイッチがクライアント モードである場合、クライアント スイッチはその設定を変更して、サーバの設定をコピーします。クライアントモードのスイッチがある場合には、必ずサーバ モードのスイッチですべての VTP または VLAN 設定変更を行ってください。サーバ モードのスイッチの方が、保持している VTP コンフィギュレーション リビジョン番号が大きいためです。受信スイッチがトランスペアレントモードの場合、そのスイッチの設定は変更されません。
- トランスペアレントモードのスイッチは、VTPに参加しません。トランスペアレントモードのスイッチで VTP または VLAN 設定の変更を行った場合、その変更はネットワーク内の他のスイッチには伝播されません。
- サーバ モードのスイッチで VTP または VLAN 設定を変更した場合、その変更は同じ VTP ドメインのすべてのスイッチに伝播されます。
- **vtp mode transparent** コマンドは、ドメインの VTP をディセーブルにしますが、スイッチからドメインを削除しません。
- VTP バージョン 1 および 2 では、VTP および VLAN 情報を実行コンフィギュレーション ファイルに保存する場合には、VTP モードはトランスペアレントに設定してください。
- VTP バージョン 1 および 2 では、拡張範囲 VLAN がスイッチで設定されている場合には、VTP モードをクライアントまたはサーバに変更できません。VTP モードは、VTP バージョン 3 で拡張 VLAN を使用することにより変更できます。
- 拡張範囲 VLAN を追加したり、VTP および VLAN 情報を実行コンフィギュレーション ファイルに保存したりする場合には、VTP モードはトランスペアレントに設定してください。
- ダイナミック VLAN 作成がディセーブルの場合、VTP に設定できるモードは、サーバ モードまたはクライアント モードのいずれかに限ります。
- **vtp mode off** コマンドを使用すると、デバイスをオフに設定します。**no vtp mode off** コマンドを使用すると、デバイスを VTP サーバ モードにリセットします。

VTP パスワードを設定するときには、次の注意事項に従ってください。

- パスワードは大文字と小文字が区別されます。パスワードは、同じドメイン内のすべてのスイッチで一致している必要があります。
- スイッチをパスワードが設定されていない状態に戻す場合は、このコマンドの **no vtp password** 形式を使用します。
- **hidden** および **secret** キーワードは、VTP バージョン 3 だけでサポートされています。VTP バージョン 2 から VTP バージョン 3 に変換する場合、変換前に hidden または secret キーワードを削除する必要があります。

VTP プルーニングを設定するときには、次の注意事項に従ってください。

- VTP プルーニングは、プルーニング適格 VLAN に所属するステーションがない場合、その VLAN の情報を VTP 更新から削除します。
- VTP サーバでプルーニングをイネーブルにすると、プルーニングは VLAN ID 1 ～ 1005 の管理ドメイン全体でイネーブルになります。
- プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。
- プルーニングは、VTP バージョン 1 およびバージョン 2 でサポートされています。

VTP バージョンを設定するときには、次の注意事項に従ってください。

- バージョン 2（v2）モード ステートを切り替えると、ある一定のデフォルト VLAN のパラメータが変更されます。
- 各 VTP スイッチは他のすべての VTP デバイスの機能を自動的に検出します。VTP バージョン 2 を使用するには、ネットワーク内のすべての VTP スイッチでバージョン 2 がサポートされている必要があります。そうでない場合、VTP バージョン 1 モードで稼働するよう設定する必要があります。
- ドメイン内のすべてのスイッチが VTP バージョン 2 対応である場合、1 つのスイッチでバージョン 2 を設定すれば、バージョン番号は、VTP ドメイン内の他のバージョン 2 対応スイッチに伝播されます。
- トークンリング環境で VTP を使用している場合、VTP バージョン 2 もイネーブルである必要があります。
- Token Ring Bridge Relay Function（TrBRF）または Token Ring Concentrator Relay Function（TrCRF）VLAN メディア タイプを設定している場合には、バージョン 2 を使用してください。
- トークンリングまたはトークンリング NET VLAN メディア タイプを設定している場合には、バージョン 1 を使用してください。
- VTP バージョン 3 では、VLAN データベース情報だけでなく、すべてのデータベース VTP 情報がその VTP ドメイン全体に伝播します。
- VTP バージョン 3 の 2 つのリージョンが、VTP バージョン 1 または VTP バージョン 2 のリージョン経由で通信できるのは、トランスペアレントモードの場合に限られます。

スイッチ コンフィギュレーション ファイルにパスワード、プルーニング、およびバージョン コンフィギュレーションを保存することはできません。

次の例では、VTP コンフィギュレーション ストレージのファイル名を vtpfilename に変更する方法を示します。

```
Switch(config)# vtp file vtpfilename
```

次の例では、デバイス ストレージのファイル名をクリアする方法を示します。

```
Switch(config)# no vtp file vtpconfig
Clearing device storage filename.
```

次の例では、このデバイスの VTP アップデータ ID を提供するインターフェイスの名前を指定する方法を示します。

```
Switch(config)# vtp interface gigabitethernet
```

次の例では、スイッチの管理ドメインを設定する方法を示します。

```
Switch(config)# vtp domain OurDomainName
```

次の例では、スイッチを VTP トランスペアレント モードにする方法を示します。

```
Switch(config)# vtp mode transparent
```

次の例では、VTP ドメイン パスワードを設定する方法を示します。

```
Switch(config)# vtp password ThisIsOurDomainsPassword
```

次の例では、VLAN データベースでのプルーニングをイネーブルにする方法を示します。

```
Switch(config)# vtp pruning
Pruning switched ON
```

次の例では、VLAN データベースのバージョン 2 モードをイネーブルにする方法を示します。

```
Switch(config)# vtp version 2
```

設定を確認するには、**show vtp status** 特権 EXEC コマンドを入力します。

関連トピック

show vtp （1178 ページ）
vtp（インターフェイス コンフィギュレーション） （1207 ページ）

vtp（インターフェイス コンフィギュレーション）

ポート単位で VLAN Trunking Protocol（VTP）をイネーブルにするには、インターフェイス コンフィギュレーション モードで **vtp** コマンドを使用します。インターフェイスで VTP をディセーブルにするには、このコマンドの **no** 形式を使用します。

vtp
no vtp

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、トランキング モードのインターフェイスでのみ入力してください。

このコマンドは、スイッチが VTP バージョン 3 を実行している場合にのみサポートされます。

次の例では、インターフェイス上で VTP をイネーブルにする方法を示します。

```
Switch(config-if)# vtp
```

次の例では、インターフェイス上で VTP をディセーブルにする方法を示します。

```
Switch(config-if)# no vtp
```

関連トピック

switchport trunk （1189 ページ）
vtp（グローバル コンフィギュレーション） （1201 ページ）

vtp primary

スイッチをVLAN Trunking Protocol（VTP）プライマリ サーバとして設定するには、特権EXECモードで **vtp primary** コマンドを使用します。

vtp primary [{**mst**|**vlan**}] **[force]**

構文の説明

mst	（任意）スイッチをマルチスパニングツリー（MST）機能のプライマリ VTP サーバとして設定します。
vlan	（任意）スイッチ を VLAN のプライマリ VTP サーバとして設定します。
force	（任意）プライマリ サーバを設定するときにスイッチが競合するデバイスをチェックしないように設定します。

コマンド デフォルト

スイッチ は VTP セカンダリ サーバです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

VTP プライマリ サーバはデータベース情報をアップデートし、システム内のすべてのデバイスによって行われるアップデートを送信します。VTP セカンダリ サーバは、プライマリ サーバから受信したアップデートされた VTP のコンフィギュレーションを NVRAM にバックアップすることだけができます。

デフォルトでは、すべてのデバイスはセカンダリ サーバとして起動します。プライマリ サーバのステータスは、管理者がドメイン内のテイクオーバー メッセージを発行する場合のデータベース アップデートのためだけに必要です。プライマリ サーバなしで実用 VTP ドメインを持つことができます。

デバイスがリロードするかドメイン パラメータが変更された場合、プライマリ サーバのステータスは失われます。

（注） このコマンドは、スイッチがVTPバージョン3を実行している場合にのみサポートされます。

次の例では、スイッチ を VLAN のプライマリ VTP サーバとして設定する方法を示します。

```
Switch# vtp primary vlan
Setting device to VTP TRANSPARENT mode.
```

設定を確認するには、**show vtp status** 特権 EXEC コマンドを入力します。

関連トピック

show vtp （1178 ページ）
vtp（グローバル コンフィギュレーション） （1201 ページ）

wireless broadcast vlan

VLAN 上でブロードキャストのサポートをイネーブルにするには、グローバル コンフィギュレーション モードで **wireless broadcast vlan** コマンドを使用します。イーサネット ブロードキャストのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

wireless broadcast vlan [*vlan-id*]
no wireless broadcast vlan [*vlan-id*]

構文の説明

vlan-id	（任意） VLAN ID を指定して、その VLAN に対するブロードキャスト サポートをイネーブルにします。値の範囲は 1 ～ 4095 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、グローバル コンフィギュレーション モードのみで使用してください。

次の例では、VLAN 20 でブロードキャスティングをイネーブルにする方法を示します。

```
Switch(config)# wireless broadcast vlan 20
```

第 XV 部

WLAN

WLAN コマンド

aaa-override

WLAN で AAA オーバーライドを有効にするには、**aaa-override** コマンドを使用します。AAA オーバーライドを無効にするには、このコマンドの **no** 形式を使用します。

aaa-override
no aaa-override

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

デフォルトでは AAA が無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN で AAA を有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# aaa-override
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

次に、WLAN で AAA を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# no aaa-override
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

関連トピック

wlan （1283 ページ）

accounting-list

WLAN でRADIUS アカウンティング サーバを設定するには、**accounting-list** コマンドを使用します。RADIUS サーバ アカウンティングを無効にするには、このコマンドの **no** 形式を使用します。

accounting-list *radius-server-acct*
no accounting-list

構文の説明

radius-server-acct	アカウンティングRADIUSサーバ名。

コマンド デフォルト

デフォルトでは RADIUS サーバ アカウンティングが無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN で RADIUS サーバ アカウンティングを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# accounting-list test
Switch(config-wlan)# end
```

次に、WLAN で RADIUS サーバ アカウンティングを無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no accounting-list test
Switch(config-wlan)# end
```

関連トピック

wlan （1283 ページ）

assisted-roaming

WLAN で 802.11k を使用して経由ローミングを設定するには、**assisted-roaming** コマンドを使用します。経由ローミングを無効にするには、このコマンドの **no** 形式を使用します。

assisted-roaming {**dual-list**|**neighbor-list**|**prediction**}

no assisted-roaming {**dual-list**|**neighbor-list**|**prediction**}

構文の説明

dual-list	WLANのデュアルバンド802.11kネイバーリストを設定します。デフォルトは、クライアントが現在関連付けられている帯域です。
neighbor-list	WLAN の 802.11k ネイバー リストを設定します。
prediction	WLAN の経由ローミング最適化の予測を設定します。

コマンド デフォルト

ネイバー リストとデュアル バンドのサポートはデフォルトで有効になっています。デフォルトは、クライアントが現在関連付けられている帯域です。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

経由ローミングの予測のリストを有効にすると、警告が表示されます。また、WLANでロードバランシングがすでに有効になっている場合、ロード バランシングはその WLAN で無効になります。WLAN に変更を加えるには、WLAN が無効状態になっている必要があります。

例

次に、WLAN で 802.11k ネイバー リストを設定する例を示します。

```
Switch(config-wlan)#assisted-roaming neighbor-list
```

次に、WLAN で ロード バランシングが有効になっている場合の警告メッセージの例を示します。経由ローミングを設定するときにロード バランシングがすでに有効になっている場合は、ロード バランシングを無効にする必要があります。

```
Switch(config)#wlan test-prediction 2 test-prediction
Switch(config-wlan)#client vlan 43
Switch(config-wlan)#no security wpa
Switch(config-wlan)#load-balance
Switch(config-wlan)#assisted-roaming prediction
WARNING: Enabling neighbor list prediction optimization may slow association and impact
 VOICE client perform.
Are you sure you want to continue? (y/n)[y]: y
```

```
% Request aborted - Must first disable Load Balancing before enabling Assisted Roaming
Prediction Optimization on this WLAN.
```

ap name ap-name lan port-id port-id poe

AP の LAN ポートで PoE を有効にするには、特権 EXEC モードで **ap name ap-name lan port-id port-id poe** コマンドを使用します。AP の LAN ポートで PoE を無効にするには、このコマンドの **no** 形式を使用します。

（注） PoE はポート 1 に対してのみ設定できます。

ap name *ap-name* **lan port-id** *port-id* **poe**

ap name *ap-name* **no lan port-id** *port-id* **poe**

構文の説明

ap-name	AP の名前。
port-id	ポートの ID。

コマンド デフォルト デフォルトでは、PoE は無効です。

コマンド モード 特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、AP の LAN ポートで PoE を有効にする例を示します。

```
Switch # ap name AP00FE.C82D.DFB0 lan port-id 1 poe
```

ap name ap-name lan override

AP グループの LAN ポート設定をオーバーライドするには、特権 EXEC モードで **ap name ap-name lan override** コマンドを使用します。AP グループの LAN ポート設定でオーバーライドを無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap-name* **lan override**

ap name *ap-name* **no lan override**

構文の説明

ap-name	AP の名前。

コマンド デフォルト

デフォルトでは、LAN オーバーライドはディセーブルに設定されています。

（注） 各AP の LAN ポート設定は、LAN のオーバーライドが有効な場合にのみ許可されます。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、AP グループの LAN ポート設定でオーバーライドを有効にする例を示します。

```
Switch # ap name AP00FE.C82D.DFB0 lan override
```

band-select

WLAN で帯域選択を設定するには、**band-select** コマンドを使用します。帯域選択を無効にするには、このコマンドの **no** 形式を使用します。

band-select
no band-select

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

デフォルトでは、帯域選択は無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

WLAN で帯域選択を有効にすると、アクセス ポイントによって 2.4 GHz でのクライアント プローブが抑制され、デュアル バンド クライアントが 5 GHz スペクトルに移動されます。帯域選択アルゴリズムによるデュアルバンドクライアントの誘導は、同じアクセス ポイントの 2.4 GHz 無線から 5 GHz 無線へに限られます。このアルゴリズムが機能するのは、アクセス ポイントで 2.4 GHz と 5 GHz の両方の無線が稼働している場合のみです。

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN で帯域選択を有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# band-select
Switch(config-wlan)# end
```

次に、WLAN で帯域選択を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no band-select
Switch(config-wlan)# end
```

関連トピック

wlan （1283 ページ）

broadcast-ssid

WLANでサービスセット識別子（SSID）を有効にするには、**broadcast-ssid**コマンドを使用します。SSIDのブロードキャスティングを無効にするには、このコマンドの**no**形式を使用します。

broadcast-ssid
no broadcast-ssid

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

WLANのSSIDはデフォルトでブロードキャストされます。

コマンド モード

WLANの設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLANでブロードキャストSSIDを有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# broadcast-ssid
Switch(config-wlan)# end
```

次に、WLANでブロードキャストSSIDを無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no broadcast-ssid
Switch(config-wlan)# end
```

関連トピック

wlan （1283ページ）

call-snoop

WLAN で Voice over IP（VoIP）スヌーピングを有効にするには、**call-snoop** コマンドを使用します。Voice over IP（VoIP）を無効にするには、このコマンドの **no** 形式を使用します。

call-snoop
no call-snoop

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

デフォルトでは VoIP スヌーピングは無効になっています。

コマンド モード

WLN 設定

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN を無効にする方法の詳細については、「関連コマンド」の項を参照してください。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

コール スヌーピングが設定される WLAN は、Platinum QoS で設定されている必要があります。このコマンドを使用する前に、QoS を無効にする必要があります。QoS サービス ポリシーの設定の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN で VoIP を有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# call-snoop
Switch(config-wlan)# end
```

次に、WLAN で VoIP を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no call-snoop
Switch(config-wlan)# end
```

関連トピック

service-policy（WLAN） （637 ページ）
wlan （1283 ページ）

channel-scan defer-priority

オフチャネルスキャンを延期できるパケットの優先順位マーキングに対して、延期するようにデバイスを設定するには、**channel-scandefer-priority** コマンドを使用します。オフチャネル スキャンを延期できるパケットの優先順位マーキングに対して、延期するデバイスを無効にするは、このコマンドの **no** 形式を使用します。

channel-scan defer-priority *priority*
no channel-scan defer-priority *priority*

構文の説明

priority	チャネル優先順位値。指定できる範囲は0～7です。デフォルトは3です。

コマンド デフォルト

チャネル スキャン延期が有効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、WLAN でチャネル スキャン延期優先順位を有効にして、それを優先順位値 4 に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# channel-scan defer-priority 4
Switch(config-wlan)# end
```

次に、WLAN でチャネル スキャン延期優先順位を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no channel-scan defer-priority 4
Switch(config-wlan)# end
```

channel-scan defer-time

チャネル スキャン延期時間を割り当てるには、**channel-scandefer-time** コマンドを使用します。チャネル スキャン延期時間を無効にするには、このコマンドの **no** 形式を使用します。

channel-scan defer-time *msecs*
no channel-scan defer-time

構文の説明

msecs 延期時間（ミリ秒単位）。範囲は 0 ～ 60000 です。デフォルトは 100 です。

コマンド デフォルト

チャネル スキャン延期時間が有効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ミリ秒単位の時間値は、WLAN 機器の要件を満たす必要があります。

次に、WLAN でチャネル スキャンを有効にして、スキャン延期時間を 300 ミリ秒に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# channel-scan defer-time 300
Switch(config-wlan)# end
```

次に、WLAN でチャネル スキャン延期時間を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no channel-scan defer-time
Switch(config-wlan)# end
```

chd

WLAN でカバレッジ ホール検出を有効にするには、**chd** コマンドを使用します。カバレッジ ホール検出を無効にするには、このコマンドの **no** 形式を使用します。

chd
no chd

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

カバレッジ ホール検出が有効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、WLAN でカバレッジ ホール検出を有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# chd
Switch(config-wlan)# end
```

次に、WLAN でカバレッジ ホール検出を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no chd
Switch(config-wlan)# end
```

client association limit

WLAN のクライアント接続、アクセス ポイントあたりのクライアント、または無線アクセス ポイントあたりのクライアントの最大数を設定するには、**clientassociationlimit** コマンドを使用します。WLAN のクライアント アソシエーションの上限を無効にするには、このコマンドの **no** 形式を使用します。

client association limit {*association-limit*|**ap** *ap-limit*|**radio** *max-ap-radio-limit*}
no client association limit {*association-limit*|**ap** *ap-limit*|**radio** *max-ap-radio-limit*}

構文の説明

association-limit	許可されるクライアント接続の数。有効な範囲は 0 ～ 2000 です。値がゼロ（0）の場合、上限が設定されていないことを示します。
ap	アクセス ポイントあたりのクライアントの最大数。
ap-limit	無線アクセス ポイントあたりに許可されるクライアント接続の最大数を設定します。有効な範囲は 0 ～ 400 です。
radio	無線 AP あたりのクライアントの最大数を設定します。
max-ap-radio-limit	無線アクセス ポイントあたりに許可されるクライアント接続の最大数。有効な範囲は 0 ～ 200 です。

コマンド デフォルト

クライアント接続の最大数は 0 （上限なし）に設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	コマンドが変更されました。**ap** キーワードと **radio** キーワードが追加されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLANのクライアントアソシエーションの制限を設定し、クライアントの上限を 200 に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# client association limit 200
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

次に、WLANのクライアントアソシエーションの制限をディセーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# no client association limit
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

次に、WLANの無線あたりのクライアントアソシエーションの制限を設定し、クライアントの上限を 200 に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# client association limit radio 200
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

次に、WLAN の AP あたりのクライアント アソシエーションの制限を設定し、クライアントの上限を 300 に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# client association limit ap 300
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

関連トピック

wlan （1283 ページ）

client vlan

WLAN インターフェイスまたはインターフェイス グループを設定するには、**clientvlan** コマンドを使用します。WLAN インターフェイスをディセーブルにするには、このコマンドの **no** 形式を使用します。

client vlan *interface-id-name-or-group-name*
no client vlan

構文の説明

interface-id-name-or-group-name	インターフェイス ID、名前、または VLAN グループ名。インターフェイス ID は、複数桁で指定することもできます。

コマンド デフォルト

デフォルト インターフェイスが設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN のクライアント VLAN をイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# client vlan client-vlan1
Switch(config-wlan)# end
```

次に、WLAN 上のクライアント VLAN をディセーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no client vlan
Switch(config-wlan)# end
```

関連トピック

wlan （1283 ページ）

ccx aironet-iesupport

WLAN で Aironet 情報要素（IE）を有効にするには、**ccxaironet-iesupport** コマンドを使用します。Aironet 情報要素（IE）を無効にするには、このコマンドの **no** 形式を使用します。

ccx aironet-iesupport
no ccx aironet-iesupport

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

Aironet IE サポートは有効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN で Aironet IE を有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# ccx aironet-iesupport
Switch(config-wlan)# end
```

次に、WLAN で Aironet IE を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no ccx aironet-iesupport
Switch(config-wlan)# end
```

関連トピック

wlan （1283 ページ）

datalink flow monitor

WLAN での NetFlow モニタリングを有効にするには、**datalinkflowmonitor** コマンドを使用します。NetFlow モニタリングを無効にするには、このコマンドの **no** 形式を使用します。

datalink flow monitor *datalink-monitor-name* {**input**|**output**}
no datalink flow monitor *datalink-monitor-name* {**input**|**output**}

構文の説明

datalink-monitor-name	フロー モニタ名。データリンク モニタ名には最大 31 文字を含めることができます。
input	入力トラフィックの NetFlow モニタを指定します。
output	出力トラフィックの NetFlow モニタを指定します。

コマンド デフォルト

なし。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN での NetFlow モニタリングを有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# datalink flow monitor test output
Switch(config-wlan)# end
```

次に、WLAN での NetFlow モニタリングを無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no datalink flow monitor test output
Switch(config-wlan)# end
```

関連トピック

wlan （1283 ページ）

device-classification

WLAN でクライアント デバイスの分類を有効にするには、**device-classification** コマンドを使用します。デバイスの分類を無効にするには、このコマンドの **no** 形式を使用します。

device-classification
no device-classification

構文の説明

device-classification	クライアントデバイスの分類を有効または無効にします。

コマンド デフォルト

なし。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# device-classification
Switch(config-wlan)# end
```

default

パラメータをデフォルト値に設定するには、**default** コマンドを使用します。

default {**aaa-override**|**accounting-list**|
[illegible]

構文の説明

aaa-override	AAA オーバーライド パラメータをデフォルト値に設定します。
accounting-list	アカウンティング パラメータとその属性をデフォルト値に設定します。
band-select	帯域選択パラメータをデフォルト値に設定します。
broadcast-ssid	ブロードキャストのサービスセット識別子（SSID）パラメータをデフォルト値に設定します。
call-snoop	コール スヌープ パラメータをデフォルト値に設定します。
ccx	Cisco Client Extension（Cisco Aironet IE）のパラメータと属性をデフォルト値に設定します。
channel-scan	チャネル スキャンのパラメータと属性をデフォルト値に設定します。
chd	カバレッジ ホール検出パラメータをデフォルト値に設定します。
client	クライアントのパラメータと属性をデフォルト値に設定します。
datalink	データリンクのパラメータと属性をデフォルト値に設定します。
diag-channel	診断チャネルのパラメータと属性をデフォルト値に設定します。
dtim	Delivery Traffic Indicator Message（DTIM）パラメータをデフォルト値に設定します。
exclusionlist	クライアント除外タイムアウト パラメータをデフォルト値に設定します。
ip	IP パラメータをデフォルト値に設定します。
ipv6	IPv6 のパラメータと属性をデフォルト値に設定します。

load-balance	ロードバランシング パラメータをデフォルト値に設定します。
local-auth	Extensible Authentication Protocol（EAP）プロファイルのパラメータと属性をデフォルト値に設定します。
mac-filtering	MACフィルタリングのパラメータと属性をデフォルト値に設定します。
media-stream	メディア ストリームのパラメータと属性をデフォルト値に設定します。
mfp	管理フレーム保護（MPF）のパラメータと属性をデフォルト値に設定します。
mobility	モビリティのパラメータと属性をデフォルト値に設定します。
nac	RADIUSネットワーク アドミッション コントロール（NAC）パラメータをデフォルト値に設定します。
passive-client	パッシブ クライアント パラメータをデフォルト値に設定します。
peer-blocking	ピアツーピア ブロッキングのパラメータと属性をデフォルト値に設定します。
radio	ワイヤレス ポリシーのパラメータと属性をデフォルト値に設定します。
roamed-voice-client	ローミングされた音声クライアントのパラメータと属性をデフォルト値に設定します。
security	セキュリティ ポリシーのパラメータと属性をデフォルト値に設定します。
service-policy	WLAN サービス品質（QoS）ポリシーのパラメータと属性をデフォルト値に設定します。
session-timeout	クライアント セッション タイムアウト パラメータをデフォルト値に設定します。
shutdown	シャットダウン パラメータをデフォルト値に設定します。
sip-cac	Session Initiation Protocol（SIP）のコール アドミッション制御（CAC）のパラメータと属性をデフォルト値に設定します。
static-ip	スタティック IP クライアント トンネリングのパラメータと属性をデフォルト値に設定します。

uapsd	Wi-Fi マルチメディア（WMM）不定期自動省電力配信（UAPSD）のパラメータと属性をデフォルト値に設定します。
wgb	ワークグループブリッジ（WGB）パラメータをデフォルト値に設定します。
wmm	WMM のパラメータと属性をデフォルト値に設定します。

コマンド デフォルト

なし。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、Cisco Client Extensio パラメータをデフォルト値に設定する例を示します。

```
Switch(config-wlan)# default ccx aironet-iesupport
```

関連トピック

wlan （1283 ページ）

dtim dot11

WLAN の Delivery Traffic Indicator Message（DTIM）期間を設定するには、**dtimdot11** コマンドを使用します。DTIM を無効にするには、このコマンドの **no** 形式を使用します。

dtim dot11 {**5ghz**|**24ghz**} *dtim-period*
no dtim dot11 {**5ghz**|**24ghz**} *dtim-period*

構文の説明

5ghz	5 GHz 帯域の DTIM 期間を設定します。
24ghz	2.4 GHz 帯域の DTIM 期間を設定します。
dtim-period	DTIM 期間の値。範囲は 1 ～ 255 です。

コマンド デフォルト

DTIM 期間は 1 に設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN で DTIM 期間を有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# dtim dot11 24ghz 3
```

次に、2.4 GHz 帯域の WLAN で DTIM 期間を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no dtim dot11 24ghz 3
```

関連トピック

wlan （1283 ページ）

exclusionlist

無線 LAN で除外リストを設定するには、**exclusionlist** コマンドを使用します。除外リストを無効にするには、このコマンドの **no** 形式を使用します。

exclusionlist [**timeout** *seconds*]
no exclusionlist [timeout]

構文の説明

timeout *seconds*	（任意）除外リスト タイムアウトを秒単位で指定します。指定できる範囲は 0 ～ 2147483647 です。値ゼロ（0）はタイムアウトなしを示します。

コマンド デフォルト

除外リストは 60 秒に設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN のクライアント除外リストを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# exclusionlist timeout 345
```

次に、WLAN のクライアント除外リストを無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no exclusionlist timeout 345
```

exit

WLAN コンフィギュレーション サブモードを終了するには、**exit** コマンドを使用します。

exit

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、WLAN コンフィギュレーション サブモードを終了する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# exit
Switch(config)#
```

exit（WLAN AP グループ）

WLAN アクセスポイント グループ サブモードを終了するには、**exit** コマンドを使用します。

exit

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

WLAN AP グループ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、WLAN AP グループ サブモードを終了する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ap group test
Switch(config-apgroup)# exit
```

ip access-group

WLAN アクセス コントロール グループ（ACL）を設定するには、**ipaccess-group** コマンドを使用します。WLAN ACL グループを削除するには、このコマンドの **no** 形式を使用します。

ip access-group [web] *acl-name*
no ip access-group [web]

構文の説明

web	（任意）IPv4 Web ACL を設定します。
acl-name	セキュリティ タイプ値を webauth として、WLAN に使用する preauth ACL を指定します。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、WLAN ACL を設定する例を示します。

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wlan wlan1
Switch(config-wlan)#ip access-group test-acl
```

次に、IPv4 WLAN Web ACL を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# ip access-group web test
Switch(config-wlan)#
```

関連トピック

wlan （1283 ページ）

ip flow monitor

IP NetFlow モニタリングを設定するには、**ipflowmonitor** コマンドを使用します。IP NetFlow モニタリングを削除するには、このコマンドの **no** 形式を使用します。

ip flow monitor *ip-monitor-name* {**input**|**output**}
no ip flow monitor *ip-monitor-name* {**input**|**output**}

構文の説明

ip-monitor-name	フロー モニタ名。
input	入力トラフィックのフローモニタを有効にします。
output	出力トラフィックのフローモニタを有効にします。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、入力トラフィックに IP フロー モニタを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# ip flow monitor test input
```

次に、IP フロー モニタを無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no ip flow monitor test input
```

ip verify source mac-check

WLAN の IPv4 ソース ガード（IPSG）を有効にするには、**ipverifysourcemac-check** コマンドを使用します。IPSG を無効にするには、このコマンドの **no** 形式を使用します。

ip verify source mac-check
no ip verify source mac-check

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

IPSG は無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

ホストの IP アドレスに基づいて、ホストから特定のインターフェイスへのトラフィックを制限するには、この機能を使用します。機能は、IP スプーフィングを防ぐために、ホストの送信元 MAC と IP をバインドするように設定することもできます。

DHCP スヌーピング、ARP および Dataglean から受信した情報に基づいて、ワイヤレス ホストの IP アドレスと MAC アドレスをバインドするには、この機能を使用します。Dataglean は、DHCP リレーエージェントによってDHCPメッセージが転送された場合に、それらのメッセージからホスト ハードウェア アドレス、ホストに接続されているポートなどのロケーション情報を抽出するプロセスです。ワイヤレス ホストが、スイッチによって学習されていない IP アドレスとMACアドレスの組み合わせを持つトラフィックの送信を試みた場合、このトラフィックはハードウェアでドロップされます。IPSG は、DHCPパケットではサポートされていません。IPSG は、外部スイッチの外部クライアントではサポートされていません。

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。

次に、IPSG を有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# ip verify source mac-check
```

次に、IPSG を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no ip verify source mac-check
```

load-balance

WLANのロードバランシングを有効にするには、**load-balance**コマンドを使用します。ロードバランシングを無効にするには、このコマンドの **no** 形式を使用します。

load-balance
no load-balance

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

ロード バランシングはデフォルトではディセーブルになっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN でロード バランシングを有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# shutdown
Switch(config)# wlan wlan1
Switch(config-wlan)# load-balance
Switch(config)# no shutdown
Switch(config-wlan)# end
```

次に、WLAN でロード バランシングを無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# shutdown
Switch(config)# wlan wlan1
Switch(config-wlan)# no load-balance
Switch(config)# no shutdown
Switch(config-wlan)# end
```

関連トピック

wlan （1283 ページ）

mobility anchor

モビリティ スティッキ アンカリングを設定するには、**mobility anchor sticky** コマンドを使用します。スティッキ アンカリングを無効にするには、このコマンドの **no** 形式を使用します。

ゲスト アンカリングを設定するには、**mobility anchor** *ip-address* コマンドを使用します。

ゲスト アンカーを削除するには、このコマンドの **no** 形式を使用します。

デバイスを自動アンカーとして設定するには、**mobility anchor** コマンドを使用します。

mobility anchor {*ip-address*|**sticky**}
no mobility anchor {*ip-address*|**sticky**}

構文の説明

sticky	クライアントは、関連付けられている最初のスイッチにアンカーされます。 （注） このコマンドはデフォルトで有効になっており、低ローミング遅延を保証します。これは、クライアントがモビリティ ドメインに参加し、ドメイン内をローミングする場合でも、クライアントの Point of Presence のが変更されないように確保します。
ip-address	ゲスト アンカー スイッチの IP アドレスをこの WLAN に設定します。

コマンド デフォルト

スティッキ設定は、デフォルトでは有効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。
Cisco IOS XE 3.3SE	Cisco IOS XE 3.3SE リリースより前の自動アンカー設定ではデバイス IP アドレスを入力する必要がありました。このリリースでは、IP アドレスが指定されていない場合、デバイス自身がアンカーになります。明示的に IP アドレスを指定する必要はありません。

使用上のガイドライン

- wlan_id または guest_lan_id は必ず指定し、無効にする必要があります。
- 1 つ目のモビリティ アンカーを設定するときに、WLAN または有線ゲスト LAN で自動アンカー モビリティを有効にします。
- 最後のアンカーを削除すると、自動アンカーモビリティ機能は無効になり、新しいアソシエーションに対しては標準のモビリティが再度使用されるようになります。
- モビリティは、ファイアウォールの通過が許可されている次のポートを使用します。
  - 16666

- 16667
- 16668

次に、スティッキ モビリティ アンカーを有効にする例を示します。

```
Switch(config-wlan)# mobility anchor sticky
```

次に、ゲスト アンカリングを設定する例を示します。

```
Switch(config-wlan)# mobility anchor 209.165.200.224
```

次に、デバイスを自動アンカーとして設定する例を示します。

```
Switch(config-wlan)# mobility anchor
```

nac

WLAN 対応の RADIUS ネットワーク アドミッション コントロール（NAC）サポートを有効にするには、**nac** コマンドを使用します。NAC アウトオブバンド サポートを無効にするには、このコマンドの **no** 形式を使用します。

nac
no nac

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

NAC は無効です。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

RADIUS NAC 状態を有効にする前に、AAA オーバーライドを有効にする必要があります。

次に、WLAN に RADIUS NAC を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# aaa-override
Switch(config-wlan)# nac
```

次に、WLAN で RADIUS NAC を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no nac
Switch(config-wlan)# no aaa-override
```

関連トピック

aaa-override （1215 ページ）

passive-client

WLANのパッシブクライアント機能を有効にするには、**passive-client**コマンドを使用します。パッシブ クライアント機能を無効にするには、このコマンドの **no** 形式を使用します。

passive-client
no passive-client

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

パッシブ クライアント機能は無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを入力する前に、グローバル マルチキャスト モードとマルチキャスト-マルチキャスト モードを有効にする必要があります。マルチキャスト-マルチキャスト モードとマルチキャスト-ユニキャストモードの両方がサポートされています。マルチキャスト-マルチキャスト モードが推奨されます。

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN でパッシブ クライアント機能を有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wireless multicast
Switch(config)# wlan test-wlan
Switch(config-wlan)# passive-client
```

次に、WLAN でパッシブ クライアント機能を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wireless multicast
Switch(config)# wlan test-wlan
Switch(config-wlan)# no passive-client
```

関連トピック

wlan （1283 ページ）

peer-blocking

WLAN にピアツーピア ブロッキング機能を設定するには、**peer-blocking** コマンドを使用します。ピアツーピア ブロッキング機能を無効にするには、このコマンドの **no** 形式を使用します。

peer-blocking {**drop**|**forward-upstream**}
no peer-blocking

構文の説明

drop	スイッチでパケットを破棄するように指定します。
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指定します。スイッチの次に上の階層のデバイスが、パケットに関して実行するアクションを決定します。

コマンド デフォルト

ピア ブロッキングは無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、ピアツーピア ブロッキングの drop オプションと forward-upstream オプションを有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# peer-blocking  drop
Switch(config-wlan)# peer-blocking forward-upstream
```

次に、ピアツーピア ブロッキングの drop オプションと forward-upstream オプションを無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no peer-blocking  drop
Switch(config-wlan)# no peer-blocking forward-upstream
```

関連トピック

wlan （1283 ページ）

port

AP グループのポート ID を設定するには、インターフェイス コンフィギュレーション モードで **port** コマンドを使用します。

port *port-id*

構文の説明

port-id	ポートの ID。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション（config-apgroup）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、AP グループのポート ID を設定する例を示します。

```
Switch(config-apgroup)# port 1
```

poe

ポートで PoE を有効にするには、インターフェイス コンフィギュレーション モードで **poe** コマンドを使用します。

（注） PoE はポート 1 に対してのみ設定できます。

poe
no poe

コマンド デフォルト デフォルトでは、PoE は無効です。

コマンド モード インターフェイス コンフィギュレーション（config-port-apgroup）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、ポートで PoE を有効にする方法を示します。

```
Switch(config-port-apgroup)# poe
```

radio

WLANのシスコ無線ポリシーを有効にするには、**radio**コマンドを使用します。WLANのシスコ無線ポリシーを無効にするには、このコマンドの**no**形式を使用します。

radio {**all**|**dot11a**|**dot11ag**|**dot11bg**|**dot11g**}
no radio

構文の説明

all	すべての無線帯域でWLANを設定します。
dot11a	802.11aの無線帯域だけにWLANを設定します。
dot11ag	802.11a/gの無線帯域にWLANを設定します。
dot11bg	802.11b/g無線帯域だけに無線LANを設定します（802.11gが無効な場合は802.11bだけに設定）。
dot11g	802.11gの無線帯域だけに無線LANを設定します。

コマンド デフォルト

無線ポリシーは、すべての帯域で有効になっています。

コマンド モード

WLANの設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLANをディセーブルにする必要があります。WLANをディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、すべての無線帯域に無線LANを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# radio all
```

次に、WLAN上のすべての無線帯域を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no radio all
```

関連トピック

wlan （1283 ページ）

radio-policy

WLANアクセス ポイント グループに無線ポリシーを設定するには、**radio-policy** コマンドを使用します。WLAN の無線ポリシーを無効にするには、このコマンドの **no** 形式を使用します。

radio-policy {**all**|**dot11a**|**dot11bg**|**dot11g**}
no radio{**all**|**dot11a**|**dot11bg**|**dot11g**}

構文の説明

all	すべての無線帯域で無線 LAN を設定します。
dot11a	802.11a 無線帯域だけに無線 LAN を設定します。
dot11bg	802.11b/g だけに無線 LAN を設定します（802.11g が無効な場合は 802.11b だけに設定）。
dot11g	802.11g 無線帯域だけに無線 LAN を設定します。

コマンド デフォルト

無線ポリシーは、すべての帯域で有効になっています。

コマンド モード

WLAN AP グループ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

変更を有効にするには、NTP サービスを再起動する必要があります。WLAN をシャットダウンする方法の詳細については、「関連コマンド」の項を参照してください。

次に、AP グループの 802.11b 帯域で無線ポリシーを有効にする例を示します。

```
Switch(config)# ap group test
Switch(config-apgroup)# wlan test-wlan
Switch(config-wlan-apgroup)# radio-policy dot11b
```

次に、AP グループの 802.11b 帯域で無線ポリシーを無効にする例を示します。

```
Switch(config)# ap group test
Switch(config-apgroup)# wlan test-wlan
Switch(config-wlan-apgroup)# no radio-policy dot11bg
```

関連トピック

wlan （1283 ページ）
wlan shutdown （1284 ページ）

remote-lan

リモート LAN プロファイル名を指定するには、グローバル コンフィギュレーション モードで **remote-lan** コマンドを使用します。設定したプロファイル名を無効にするには、このコマンドの **no** 形式を使用します。

remote-lan *profile-name id*
no remote-lan *profile-name id*

構文の説明

profile-name	リモート LAN プロファイル名。
id	リモート LAN の識別子。範囲は 1 ～ 64 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、リモート LAN プロファイル名を指定する例を示します。

```
Switch(config)# remote-lan test-lan 3
```

remote-lan

リモート LAN を AP グループに追加するには、インターフェイス コンフィギュレーション モードで **remote-lan** コマンドを使用します。AP グループ内のリモート LAN を無効にするには、このコマンドの **no** 形式を使用します。

remote-lan *remote-lan-name*
no remote-lan *remote-lan-name*

（注） **remote-lan remote-lan-name** コマンドは、リモート LAN をポートにマッピングする際にも必要です。

構文の説明

remote-lan-name	リモート LAN の名前。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション（config-apgroup）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、リモート LAN を AP グループに追加する例を示します。

```
Switch(config-apgroup)# remote-lan test-lan
```

roamed-voice-client re-anchor

ローミングしている音声クライアントのリアンカー機能を有効にするには、**roamed-voice-clientre-anchor** コマンドを使用します。ローミングしている音声クライアントのリアンカー機能を向こうにするには、このコマンドの **no** 形式を使用します。

roamed-voice-client re-anchor
no roamed-voice-client re-anchor

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

ローミングしている音声クライアントのリアンカー機能は無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次にローミングしている音声クライアントのリアンカー機能を有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# roamed-voice-client re-anchor
```

次にローミングしている音声クライアントのリアンカー機能を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no roamed-voice-client re-anchor
```

関連トピック

wlan （1283 ページ）

security ft

802.11r Fast Transition パラメータを設定するには、**security ft** コマンドを使用します。**over the air**（無線）の Fast Transition を設定するには、**no security ft over-the-ds** コマンドを使用します。

security ft [{**over-the-ds**|**reassociation-timeout** *timeout-jn-seconds*}]
no security ft [{**over-the-ds**|**reassociation-timeout**}]

構文の説明

over-the-ds	（任意）802.11r Fast Transition が分散システムを介して発生するように指定します。このパラメータを指定したコマンドの no 形式は、無線を介したセキュリティ Fast Transition を設定します。
reassociation-timeout	（任意）再アソシエーションのタイムアウト間隔を設定します。
timeout-in-seconds	（任意）再アソシエーションのタイムアウト間隔を秒単位で指定します。有効な範囲は 1 ～ 100 です。デフォルト値は 20 です。

コマンド デフォルト

機能はディセーブルです。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

なし

WLAN セキュリティを有効にする必要があります。

例

次に、オープンな WLAN のセキュリティ FT を設定する例を示します:

```
Switch#wlan test
Switch(config-wlan)# client vlan 0140
Switch(config-wlan)# no mobility anchor sticky
Switch(config-wlan)# no security wpa
Switch(config-wlan)# no security wpa akm dot1x
Switch(config-wlan)# no security wpa wpa2
Switch(config-wlan)# no security wpa wpa2 ciphers aes
Switch(config-wlan)# security ft
Switch(config-wlan)# shutdown
```

次に、WPA 対応の WLAN のセキュリティ FT を表示する例を示します。

```
Switch# wlan test
Switch(config-wlan)# client vlan 0140
Switch(config-wlan)# no security wpa akm dot1x
```

```
Switch(config-wlan)# security wpa akm ft psk
Switch(config-wlan)# security wpa akm psk set-key ascii 0 test-test
Switch(config-wlan)# security ft
Switch(config-wlan)# no shutdown
```

security pmf

WLAN に 802.11w 管理フレーム保護（PMF）を設定するには、**security pmf** コマンドを使用します。管理フレーム保護を無効にするには、このコマンドの **no** 形式を使用します。

security pmf {**association-comeback** *association-comeback-time-seconds*|**mandatory**|**optional**|**saquery-retry-time** *saquery-retry-time-milliseconds*}
no security pmf [{**association-comeback** *association-comeback-time-seconds*|**mandatory**|**optional**|**saquery-retry-time** *saquery-retry-time-milliseconds*}]

構文の説明

association-comeback	802.11w アソシエーション復帰時間を設定します。
association-comeback-time-seconds	アソシエーション復帰間隔（秒単位）。アソシエーションがステータス コード 30 によって拒否された後に、アソシエートされているクライアントがアソシエーションを再試行するまでに待機する必要がある時間間隔。ステータス コード 30 のメッセージは、「Association request rejected temporarily; Try again later」です。 有効範囲は 1 ～ 20 秒です。
mandatory	クライアントが WLAN の 802.1w PMF 保護をネゴシエートする必要があることを指定します。
optional	WLAN がクライアントでの 802.11w サポートを必要としていないことを指定します。802.11w 機能のないクライアントも、参加可能です。
saquery-retry-time	SA クエリの応答を受け取るまでの時間。スイッチが応答を受け取らなかった場合、別の SA クエリーが試行されます。
saquery-retry-time-milliseconds	SA クエリの再試行時間は、ミリ秒単位で指定します。指定できる範囲は 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 デフォルト

PMF は無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

この機能を使用するには、WPA（Wi-Fi Protected Access）と AKM（認証キー管理）が設定されている必要があります。セキュリティ パラメータの設定の詳細については、「関連コマンド」の項を参照してください。

802.11w では、ブロードキャストまたはマルチキャストの堅牢な管理フレームを保護するために使用される Integrity Group Temporal Key（IGTK）が導入されています。IGTK は、ソース STA からの MAC 管理プロトコル データ ユニット（MMPDU）を保護するために使用するオーセンティケータ ステーション（スイッチ）によって割り当てられる、ランダムな値です。802.11w IGTK キーは、4 ウェイ ハンドシェイクを使用して取得され、レイヤ 2 で WPA2 セキュリティが設定されている WLAN でのみ使用されます。

次に、アソシエーション復帰時間値を 15 秒で有効にする例を示します。

```
Switch(config-wlan)# security pmf association-comeback 15
```

次に、WLAN のクライアントに必須の 802.11w MPF 保護を設定する例を示します。

```
Switch(config-wlan)# security pmf mandatory
```

次に、WLAN のクライアントにオプションの 802.11w MPF 保護を設定する例を示します。

```
Switch(config-wlan)# security pmf optional
```

次に、saquery パラメータを設定する例を示します。

```
Switch(config-wlan)# security pmf saquery-retry-time 100
```

次に、PMF 機能を無効にする例を示します。

```
Switch(config-wlan)# no security pmf
```

関連トピック

security wpa akm （1261 ページ）

security web-auth

WLAN で使用する Web 認証のステータスを変更するには、**securityweb-auth** コマンドを使用します。WLAN で Web 認証を無効にするには、このコマンドの **no** 形式を使用します。

security web-auth [{**authentication-list** *authentication-list-name*|**on-macfilter-failure**|**parameter-map** *parameter-map-name*}]
no security web-auth [{**authentication-list [authentication-list-name]**|**on-macfilter-failure**|**parameter-map [parameter-name]**}]

構文の説明

authentication-list *authentication-list-name*	IEEE 802.1x の認証リストを設定します。
on-macfilter-failure	MAC の失敗時の Web 認証を有効にします。
parameter-map *parameter-map-name*	パラメータ マップを設定します。

コマンド デフォルト

Web 認証はディセーブルです。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

例

次に、WLAN に認証リストによる Web 認証を設定する例を示します。

```
Switch(config-wlan)# security web-auth authentication-list test
```

security wpa akm

Cisco Centralized Key Management（CCKM）を使用して認証キー管理を設定するには、**security wpa akm** コマンドを使用します。Cisco Centralized Key Management の認証キー管理を無効にするには、このコマンドの **no** 形式を使用します。

security wpa [{**akm** {**cckm**|**dot1x**|**ft**|**pmf**|**psk**}|**wpa1** [**ciphers** {**aes**|**tkip**}]|**wpa2** [**ciphers** {**aes**|**tikp**}]}]
no security wpa [{**akm** {**cckm**|**dot1x**|**ft**|**pmf**|**psk**}|**wpa1** [**ciphers** {**aes**|**tkip**}]|**wpa2** [**ciphers** {**aes**|**tikp**}]}]

構文の説明

akm	認証キー管理（AKM）パラメータを設定します。
aes	AES（Advanced Encryption Standard）暗号化サポートを設定します。
cckm	Cisco Centralized Key Management のサポートを設定します。
ciphers	WPA 暗号方式を設定します。
dot1x	802.1x のサポートを設定します。
ft	802.11r を使用して Fast Transition を設定します。
pmf	802.11w 管理フレーム保護を設定します。
psk	802.11r Fast Transition の事前共有キー（PSK）のサポートを設定します。
tkip	Temporal Key Integrity Protocol（TKIP）暗号化のサポートを設定します。
wpa2	Wi-Fi Protected Access 2（WPA2）のサポートを設定します。

コマンド デフォルト

デフォルトではWi-Fi Protected Access2、802.1xは有効になっています。WPA2、PSK、CCKM、FT dot1x、FT PSK、PMF dot1x、PMF PSK、FT のサポートは無効になっています。FT の再アソシエーションのタイムアウトは 20 秒、PMF SA クエリ時間は 200 に設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、WLAN に CCKM を設定する例を示します。

```
Switch(config-wlan)#security wpa akm cckm
```

service-policy（WLAN）

WLAN サービス品質（QoS）サービス ポリシーを設定するには、**service-policy** コマンドを使用します。WLAN の QoS ポリシーを無効にするには、このコマンドの **no** 形式を使用します。

service-policy [client] {**input**|**output**} *policy-name*
no service-policy [client] {**input**|**output**} *policy-name*

構文の説明

client	（任意）WLAN 上のすべてのクライアントにポリシーマップを割り当てます。
input	入力ポリシー マップを割り当てます。
output	出力ポリシー マップを割り当てます。
policy-name	ポリシー名。

コマンド デフォルト

ポリシーが割り当てられない場合、ポリシーに割り当てられる状態は [None] になります。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

例

次の例では、WLAN の入力 QoS サービス ポリシーを設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# service-policy input policy-test
```

次の例では、WLAN の入力 QoS サービス ポリシーをディセーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no service-policy input policy-test
```

次に、WLAN の出力 QoS サービス ポリシーを platinum（貴金属ポリシー）に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# service-policy output platinum
```

関連トピック

wlan （1283 ページ）

session-timeout

WLAN に関連付けられたクライアントのセッション タイムアウトを設定するには、**session-timeout** コマンドを使用します。WLAN に関連付けられたクライアントのセッション タイムアウトを無効にするには、このコマンドの **no** 形式を使用します。

session-timeout seconds
no session-timeout

構文の説明

seconds	タイムアウトまたはセッション時間（秒）。値 0 は、タイムアウトなしに相当します。範囲は 300 ～ 86400 です。

コマンド デフォルト

dot1x セキュリティが設定された WLAN の場合、クライアントのタイムアウトは 1800 秒に設定されます。オープンな WLAN の場合、クライアントのタイムアウトは 0 に設定されます。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、セッション タイムアウトを 300 秒に設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# session-timeout 300
```

次に、セッション タイムアウトを無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no session-timeout
```

show remote-lan all

設定済みのすべてのリモートLANのリモートLANプロパティを表示するには、**show remote-lan all** コマンドを使用します。

show remote-lan all

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、設定済みのすべてのリモート LAN のリモート LAN プロパティを表示する例を示します。

```
Switch#show remote-lan all
Remote-LAN Profile Name : test
================================================
Identifier : 1
Status : Disabled
Universal AP Admin : Disabled
Max Associated Clients per Remote-LAN : 0
AAA Policy Override : Disabled
Number of Active Clients : 0
Exclusionlist Timeout : 60
Session Timeout : 1800 seconds
Interface : default
Interface Status : Up
Remote-LAN ACL : unconfigured
DHCP Server : 0.0.0.0
DHCP Address Assignment Required : Disabled
Local EAP Authentication : Disabled
Mac Filter Authorization list name : Disabled
Accounting list name : Disabled
802.1x authentication list name : Disabled
Security
802.11 Authentication : Open System
802.1X : Disabled
Web Based Authentication : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : Disabled
Webauth Parameter Map : Disabled
```

show remote-lan id

ID 別にリモート LAN 設定を表示するには、**show remote-lan id** コマンドを使用します。

show remote-lan id *id*

構文の説明

id	リモート LAN の識別子。範囲は 1 ～ 64 です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、ID 別にリモート LAN 設定を表示する例を示します。

```
Switch #show remote-lan id 2
Remote-LAN Profile Name     : test
================================================
Identifier                                    : 2
Status                                        : Disabled
Universal AP Admin                            : Disabled
Max Associated Clients per Remote-LAN         : 0
AAA Policy Override                           : Enabled
Number of Active Clients                      : 0
Exclusionlist Timeout                         : 21474
Session Timeout                               : 864 seconds
Interface                                     : default
Interface Status                              : Up
Remote-LAN ACL                                 : testacl
DHCP Server                                   : 10.5.7.9
DHCP Address Assignment Required              : Disabled
Local EAP Authentication                      : testeapprofile
Mac Filter Authorization list name            : testmaclist
Accounting list name                          : testlist
802.1x authentication list name               : dotxauth
Security
    802.11 Authentication                     : Open System
    802.1X                                    : Enabled
        Encryption                            : 104-bit WEP
```

show remote-lan name

プロファイル名別にリモート LAN 設定を表示するには、**show remote-lan name** コマンドを使用します。

show remote-lan name *name*

構文の説明

name	リモートLANプロファイル名。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、プロファイル名別にリモート LAN 設定を表示する例を示します。

```
Switch# show remote-lan name test
Remote-LAN Profile Name : test
================================================
Identifier : 1
Status : Disabled
Universal AP Admin : Disabled
Max Associated Clients per Remote-LAN : 0
AAA Policy Override : Disabled
Number of Active Clients : 0
Exclusionlist Timeout : 60
Session Timeout : 1800 seconds
Interface : default
Interface Status : Up
Remote-LAN ACL : unconfigured
DHCP Server : 0.0.0.0
DHCP Address Assignment Required : Disabled
Local EAP Authentication : Disabled
Mac Filter Authorization list name : Disabled
Accounting list name : Disabled
802.1x authentication list name : Disabled
Security
802.11 Authentication : Open System
802.1X : Disabled
Web Based Authentication : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : Disabled
Webauth Parameter Map : Disabled
```

show remote-lan summary

すべてのリモート LAN のサマリーを表示するには、**show remote-lan summary** コマンドを使用します。

show remote-lan summary

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、すべてのリモート LAN のサマリーを表示する例を示します。

```
Switch # show remote-lan summary
Number of Remote-LANs: 1

Remote-LAN Profile Name                      VLAN Status
------------------------------------------------------
2          test                              1    DOWN
```

show running-config remote-lan

リモート LAN 設定を表示するには、**show running-config remote-lan** コマンドを使用します。

show running-config remote-lan *name*

構文の説明	*name* リモートLANプロファイル名。
コマンド デフォルト	なし
コマンド モード	特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、リモート LAN 設定を表示する例を示します。

```
Switch# show running-config remote-lan test
remote-lan test 1
aaa-override
accounting-list test-all-list
exclusionlist timeout 100
ip access-group test-acl
ip dhcp server 10.100.12.5
mac-filtering test-mac-list
security dot1x authentication-list test-dot1x-list
session-timeout 100
shutdown
```

show wlan

WLAN パラメータを表示するには、**show wlan** コマンドを使用します。

show wlan {**all** |**id** *wlan-id*|**name** *wlan-name* |**summary**}

構文の説明

all	すべての設定済み WLAN のパラメータのサマリーを表示します。リストは WLAN ID の昇順に表示されます。
id *wlan-id*	無線 LAN の識別子を指定します。範囲は 1 ～ 512 です。
name *wlan-name*	WLAN プロファイル名を指定します。名前は 1 ～ 32 文字です。
summary	WLAN に設定されているパラメータのサマリーを表示します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、デバイスに設定されている WLAN のサマリーを表示する例を示します。

```
Switch# show wlan summary
Number of WLANs: 1

WLAN Profile Name                     SSID                           VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                        test-wlan-ssid                  1    UP
```

次に、特定の WLAN に設定されているパラメータのサマリーを表示する例を示します。

```
Switch# show wlan name test-wlan
WLAN Identifier                                 : 45
Profile Name                                    : test-wlan
Network Name (SSID)                             : test-wlan-ssid
Status                                          : Enabled
Broadcast SSID                                  : Enabled
Maximum number of Associated Clients            : 0
AAA Policy Override                             : Disabled
Network Admission Control
  NAC-State                                     : Disabled
Number of Active Clients                        : 0
Exclusionlist Timeout                           : 60
Session Timeout                                 : 1800 seconds
```

```
CHD per WLAN                                    : Enabled
Webauth DHCP exclusion                          : Disabled
Interface                                       : default
Interface Status                                : Up
Multicast Interface                             : test
WLAN IPv4 ACL                                   : test
WLAN IPv6 ACL                                   : unconfigured
DHCP Server                                     : Default
DHCP Address Assignment Required                : Disabled
DHCP Option 82                                  : Disabled
DHCP Option 82 Format                           : ap-mac
DHCP Option 82 Ascii Mode                       : Disabled
DHCP Option 82 Rid Mode                         : Disabled
QoS Service Policy - Input
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Service Policy - Output
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Client Service Policy
  Input  Policy Name                            : unknown
  Output Policy Name                            : unknown
WifiDirect                                      : Disabled
WMM                                             : Disabled
Channel Scan Defer Priority:
  Priority (default)                            : 4
  Priority (default)                            : 5
  Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Enabled
CCX - Gratuitous ProbeResponse (GPR)            : Disabled
CCX - Diagnostics Channel Capability            : Disabled
Dot11-Phone Mode (7920)                         : Invalid
Wired Protocol                                  : None
Peer-to-Peer Blocking Action                    : Disabled
Radio Policy                                    : All
DTIM period for 802.11a radio                   : 1
DTIM period for 802.11b radio                   : 1
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : Disabled
Accounting list name                            : Disabled
802.1x authentication list name                 : Disabled
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    802.1X                                      : Disabled
    Wi-Fi Protected Access (WPA/WPA2)           : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Enabled
            TKIP Cipher                         : Disabled
            AES Cipher                          : Enabled
        Auth Key Management
            802.1x                              : Enabled
            PSK                                 : Disabled
            CCKM                                : Disabled
    IP Security                                 : Disabled
    IP Security Passthru                        : Disabled
    L2TP                                        : Disabled
    Web Based Authentication                    : Disabled
    Conditional Web Redirect                    : Disabled
    Splash-Page Web Redirect                    : Disabled
    Auto Anchor                                 : Disabled
    Sticky Anchoring                            : Enabled
```

```
    Cranite Passthru                              : Disabled
    Fortress Passthru                             : Disabled
    PPTP                                          : Disabled
    Infrastructure MFP protection                 : Enabled
    Client MFP                                    : Optional
    Webauth On-mac-filter Failure                 : Disabled
    Webauth Authentication List Name              : Disabled
    Webauth Parameter Map                         : Disabled
    Tkip MIC Countermeasure Hold-down Timer       : 60
Call Snooping                                     : Disabled
Passive Client                                    : Disabled
Non Cisco WGB                                     : Disabled
Band Select                                       : Disabled
Load Balancing                                    : Disabled
IP Source Guard                                   : Disabled
Netflow Monitor                                   : test
        Direction                                 : Input
        Traffic                                   : Datalink

Mobility Anchor List
IP Address
-----------
```

show wireless wlan summary

ワイヤレス WLAN のサマリーを表示するには、**show wireless wlan summary** コマンドを使用します。

show wireless wlan summary

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド履歴

リリース	変更内容
15.2(3)E	このコマンドが導入されました。

次に、**show wireless wlan summary** コマンドの出力例を示します。

```
Cisco-Controller# show wireless wlan summary

Total WLAN Configured: 3

Total Client Count: 0


ID    Profile Name          SSID                 Security    Radio       VLAN
Client   Status
-----------------------------------------------------------------------------------------------
1     Test1                 xxx                  WPA1/WPA2   All         1           0
        DOWN
2     wlan1                 wlan2-ssid           WPA1/WPA2   All         1           0
        DOWN
3     wlan3                 mywlan3              WPA1/WPA2   All         1           0
        DOWN
```

shutdown

WLAN を無効にするには、**shutdown** コマンドを使用します。WLAN フェイスを有効にするには、このコマンドの **no** 形式を使用します。

shutdown
no shutdown

（注） AP グループ設定とリモート LAN プロファイルの LAN ポートを有効にするには、このコマンドの **no** 形式を使用します。

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、WLAN を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan test-wlan
Switch(config-wlan)# shutdown
Switch(config-wlan)# end
Switch# show wlan summary
Number of WLANs: 1

WLAN Profile Name                     SSID                           VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                         test-wlan-ssid                   1    DOWN
```

次に、WLAN を有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan test-wlan
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
Switch# show wlan summary
Number of WLANs: 1

WLAN Profile Name                     SSID                           VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                         test-wlan-ssid                   1    UP
```

sip-cac

WLAN の Session Initiation Protocol（SIP）コール アドミッション制御（CAC）機能を設定するには、**sip-cac** コマンドを使用します。SIP CAC 機能を無効にするには、このコマンドの **no** 形式を使用します。

sip-cac {**disassoc-client**|**send-486busy**}
no sip-cac {**disassoc-client**|**send-486busy**}

構文の説明

disassoc-client	CACに障害が発生した場合に、クライアント関連付けの解除を有効にします。
send-486busy	CAC に障害が発生した場合に、SIP 486 ビジー メッセージを送信します。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN 上でクライアント関連付けの解除および 486 ビジー メッセージを有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# sip-cac disassoc-client
Switch(config-wlan)# sip-cac send-486busy
```

次に、WLAN 上でクライアント関連付けおよび 486 ビジー メッセージを無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no sip-cac disassoc-client
Switch(config-wlan)# no sip-cac send-486busy
```

関連トピック

wlan （1283 ページ）

static-ip tunneling

WLAN のスタティック IP トンネリング機能を有効にするには、**static-ip tunneling** コマンドを使用します。スタティック IP トンネリング機能を無効にするには、このコマンドの **no** 形式を使用します。

static-ip tunneling
no static-ip tunneling

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

次に、スタティック IP トンネリングを有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# static-ip tunneling
```

次に、スタティック IP トンネリングを無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no static-ip tunneling
```

vlan

AP グループに VLAN を割り当てるには、**vlan** コマンドを使用します。VLAN ID を削除するには、このコマンドの **no** 形式を使用します。

vlan *interface-name*
no vlan

構文の説明

interface-name	VLANインターフェイス名。

コマンド デフォルト

VLAN が AP グループに割り当てられていません。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

コマンド モード

WLAN AP グループの設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。

次の例では、AP グループで VLAN を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ap group ap-group-1
Switch(config-apgroup)# wlan test-wlan
Switch(config-wlan-apgroup)# vlan 3
```

関連トピック

wlan （1283 ページ）

universal-admin

WLAN をユニバーサル管理として設定するには、**universal-admin** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

universal-admin

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

```
Switchenable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#wlan wlan1
Switch(config-wlan)#universal-admin
```

wgb non-cisco

WLAN でシスコ以外のワークグループ ブリッジ（WGB）クライアントを有効にするには、**wgbnon-cisco** コマンドを使用します。シスコ以外の WGB クライアントのサポートを無効にするには、このコマンドの **no** 形式を使用します。

wgb non-cisco
no wgb non-cisco

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

シスコ以外の WGB クライアントは無効です。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN でシスコ以外の WGB を有効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# wgb non-cisco
Switch(config-wlan)# no shutdown
```

次に、WLAN でシスコ以外の WGB クライアントのサポートを無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# no wgb non-cisco
Switch(config-wlan)# no shutdown
```

wifidirect policy

WLAN で Wi-Fi Direct クライアント ポリシーを設定するには、**wifidirect policy** コマンドを使用します。Wi-Fi Direct クライアント ポリシーを無効にするには、このコマンドの **no** 形式を使用します。

wifidirect policy {**permit**|**deny**}

構文の説明

permit	Wi-Fi Direct クライアントを有効にして WLAN と関連付けます。
deny	Wi-Fi Direct 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、関連付け要求でこれらの機能をスイッチにレポートします。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 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。

コマンド デフォルト

Wi-Fi Direct を無効にします。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、Wi-Fi Direct を有効にし、Wi-Fi Direct クライアントを設定して WLAN に関連付ける例を示します。

```
Switch(config-wlan)# wifidirect policy permit
```

wlan（AP グループの設定）

アクセスポイント（AP）グループの WLAN の WLAN パラメータを設定するには、**wlan** コマンドを使用します。AP グループから WLAN を削除するには、このコマンドの **no** 形式を使用します。

wlan *wlan-name*
no wlan *wlan-name*

構文の説明

wlan-name	WLANプロファイル名入力できる範囲は英数字で1～32文字です。

コマンド デフォルト

WLAN パラメータは、APグループに対して設定されていません。

コマンド モード

AP グループの設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、AP グループ コンフィギュレーション モードで WLAN 関連パラメータを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ap group test
Switch(config-apgroup)# wlan qos-wlan
```

関連トピック

wlan （1283 ページ）

wlan

無線 LAN を作成するには、**wlan** コマンドを使用します。無線 LAN をディセーブルにするには、このコマンドの **no** 形式を使用します。

wlan [{*wlan-name*|*wlan-name wlan-id*|*wlan-name wlan-id wlan-ssid*}]
no wlan [{*wlan-name*|*wlan-name wlan-id*|*wlan-name wlan-id wlan-ssid*}]

構文の説明

wlan-name	WLANプロファイル名名前には、1～32文字の英数字を使用できます。
wlan-id	無線 LAN の ID。範囲は 1 ～ 512 です。
wlan-ssid	SSID。入力できる範囲は英数字で 1 ～ 32 文字です。

コマンド デフォルト

WLAN はディセーブルになっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

SSID を指定しない場合は、プロファイル名パラメータがプロファイル名と SSID の両方に使用されます。管理インターフェイスおよびAPマネージャ インターフェイスが同じポートにマップされており、いずれも同じ VLAN のメンバである場合は、WLAN を無効にしてから、ポートマッピングをいずれかのインターフェイスに変更する必要があります。管理インターフェイスと AP マネージャ（アクセス ポイント マネージャ）インターフェイスが別々の VLAN に割り当てられている場合は、WLAN を無効にする必要はありません。

アクセス ポイント グループに割り当てられている WLAN を削除しようとすると、エラー メッセージが表示されます。そのまま続行すると、アクセス ポイント グループとアクセス ポイントの無線から WLAN が削除されます。

次の例では、WLAN を作成する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config)# wlan test-wlan-cr 67 test-wlan-cr-ssid
```

次の例では、WLAN を削除する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config)# no wlan test-wlan-cr 67 test-wlan-cr-ssid
```

wlan shutdown

WLAN を無効にするには、**wlanshutdown** コマンドを使用します。WLAN フェイスを有効にするには、このコマンドの **no** 形式を使用します。

wlan shutdown
no wlan shutdown

コマンド デフォルト

WLAN は無効になっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN をシャット ダウンする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
```

関連トピック

wlan （1283 ページ）

wmm

WLAN で Wi-Fi マルチメディア（WMM）を有効にするには、**wmm** コマンドを使用します。WLAN で WMM を無効にするには、このコマンドの **no** 形式を使用します。

wmm {**allowed**|**require**}
no wmm

構文の説明

allowed	WLAN での WMM の使用を許可します。
require	クライアントが WLAN で WMM を使用することを要求します。

コマンド デフォルト

WMM は有効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.2SE、、、、、	このコマンドが導入されました。

使用上のガイドライン

スイッチがレイヤ2モードで、WMMが有効化されている場合にアクセス ポイントをスイッチに結合できるようにするには、これらのアクセス ポイントをトランク ポート上に配置する必要があります。

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN で WMM を有効にする例を示します。

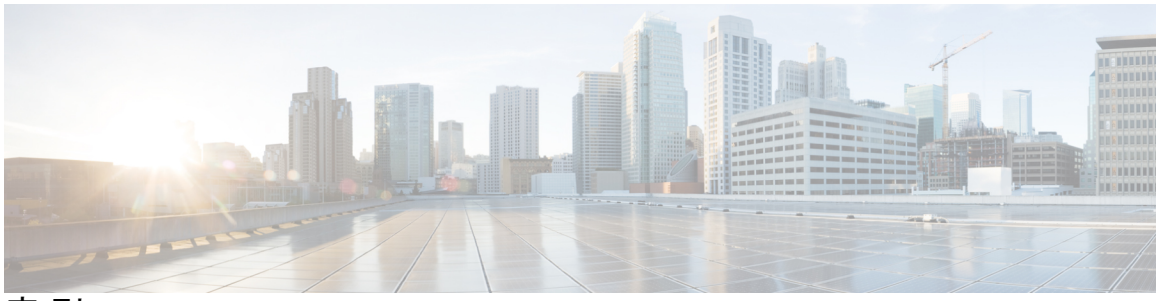
```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# wmm allowed
```

次に、WLAN で WMM を無効にする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no wmm
```

関連トピック

wlan （1283 ページ）



索引

A

B

C

D

E

F

H

I

L

M

N

P

Q

R

S

T

U

V

W

す

は

ふ

り