Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（Cisco IOS XE Dublin 17.12.x）コマンドリファレンス

初版：2023 年 7 月 31 日

最終更新：2023 年 7 月 31 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.

目 次

はじめに

表記法

このマニュアルでは、以下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、およびユーザー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	**`太字の Courier`** フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3 つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。
|	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}]	角かっこまたは波かっこ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。角かっこ内の波かっこと縦棒は、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 安全上の重要な注意事項

装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。使用、設置、電源への接続を行う前にインストール手順を読んでください。各警告の最後に記載されているステートメント番号を基に、装置の安全についての警告を参照してください。ステートメント 1071

これらの注意事項を保存しておいてください

関連資料

（注） device をインストールまたはアップグレードする前に、https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-release-notes-list.html 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 9800-40 ワイヤレスコントローラのマニュアル：

  http://www.cisco.com/go/c9800
- 次の URL にある Cisco Catalyst 9800-80 ワイヤレスコントローラのマニュアル：

  http://www.cisco.com/go/c9800
- 次の URL にある Cisco Catalyst 9800-L ワイヤレスコントローラのマニュアル：

  http://www.cisco.com/go/c9800

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。

- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

シスコバグ検索ツール

Ciscoシスコバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

コマンドライン インターフェイスの使用

コマンドライン インターフェイスの使用に関する情報

（注） GUI および CLI の検索オプションでは、大文字と小文字が区別されます。

コマンド モード

Cisco IOS ユーザインターフェイスは、いくつかのモードに分かれています。使用可能なコマンドは、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。

CLIセッションを開始するには、コンソール接続、Telnet、SSH、またはブラウザを使用できます。

セッションを開始するときは、ユーザー モード（別名ユーザー 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、現在の設定ステータスを示す **show** コマンドや、カウンタまたはインターフェイスを消去する **clear** コマンドなど、ほとんどのユーザ EXEC コマンドは 1 回限りのコマンドです。ユーザー EXEC コマンドは、deviceをリブートするときには保存されません。

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

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

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

表 *1*: コマンドモードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	Telnet、SSH、またはコンソールを使用してセッションを開始します。	デバイス>	**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。	デバイス#	終了するには、**disable** と入力します。	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。	デバイス(config)#	終了して特権 EXEC モードに戻るには、**exit** または **end** を入力するか、**Ctrl+Z** を押します。	このモードは、device全体に適用するパラメータを設定する場合に使用します。

モード	アクセス方法	プロンプト	終了方法	モードの用途
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。	デバイス(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deviceのスタートアップ コンフィギュレーション ファイルに設定を保存できます。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、**interface** コマンドを入力し、インターフェイスを指定します。	デバイス(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 モードで回線を指定するには、**line vty** または **line console** コマンドを入力します。	デバイス(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。

コマンドの省略形

deviceでコマンドが一意に認識される長さまでコマンドを入力します。

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

```
デバイス# show conf
```

コマンドの no 形式および default 形式

ほとんどのコンフィギュレーション コマンドには、**no** 形式もあります。**no** 形式は一般に、特定の機能または動作を無効にする場合、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、インターフェイス コンフィギュレーション コマンド **no shutdown** 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。キーワード **no** なしでコマンドを使用すると、無効にされた機能を再度有効にしたり、デフォルトで無効になっている機能を有効にすることができます。

コンフィギュレーション コマンドには、**default** 形式もあります。コマンドの **default** 形式は、コマンド設定をデフォルトに戻します。ほとんどのコマンドはデフォルトで無効に設定されているため、**default** 形式を使用しても **no** 形式と同じ結果になります。ただし、デフォルトで有効に設定されていて、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。このような場合、**default** コマンドはそのコマンドを有効にし、変数をそのデフォルト値に設定します。

CLI のエラー メッセージ

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

表 *2 : CLI* の代表的なエラーメッセージ

エラーメッセージ	意味	ヘルプの表示方法
`% Ambiguous command: "show con"`	deviceがコマンドとして認識できるだけの文字数が入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを入れません。 コマンドとともに使用できるキーワードが表示されます。
`% Incomplete command.`	コマンドに必須のキーワードまたは値が、一部入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。

エラーメッセージ	意味	ヘルプの表示方法
`% 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

device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。この通知を syslog に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。

ヘルプ システムの使用

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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**help** 例： `デバイス# 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。

	コマンドまたはアクション	目的
ステップ 2	*abbreviated-command-entry* **?** 例： デバイス# **di?** dir disable disconnect	特定のストリングで始まるコマンドのリストを表示します。
ステップ 3	*abbreviated-command-entry* <Tab> 例： デバイス# **sh conf**<tab> デバイス# **show configuration**	特定のコマンド名を補完します。
ステップ 4	**?** 例： デバイス> **?**	特定のコマンドモードで使用可能なすべてのコマンドをリストします。
ステップ 5	*command* **?** 例： デバイス> **show ?**	コマンドに関連するキーワードを一覧表示します。
ステップ 6	*command keyword* **?** 例： デバイス(config)# **wireless management ?** certificate Configure certificate details interface Select an interface to configure transfer Active transfer profiles trustpoint Select a trustpoint to configure	キーワードに関連する引数を一覧表示します。

コンフィギュレーション コマンド：a ～ f

3gpp-info

ホットスポットで使用される 802.11u 第 3 世代パートナーシップ プロジェクト（3GPP）携帯電話ネットワークを設定するには、**3gpp-info** コマンドを使用します。ネットワークを削除するには、このコマンドの **no** 形式を使用します。

3gpp-info *country-code network-code*

構文の説明

country-code	携帯電話の国コード。
network-code	携帯電話ネットワーク コード。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、802.11u 3GPP 携帯電話ネットワークを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# 3gpp-info us mcc
```

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）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。最初のサーバーが利用できない場合、デバイスはバックアップサーバーのリストを使用して最初のサーバーを識別します。
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。 • *name*：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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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 モードを有効にするには、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。

```
デバイス# 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.

デバイス# configure terminal
デバイス(config)# aaa accounting identity default start-stop group radius
```

aaa accounting update periodic interval-in-minutes

アカウンティング更新レコード間隔を設定するには、 **aaa accounting update periodic** コマンドを使用します。

aaa accounting update periodic *interval-in-minutes*［**jitter maximum** *jitter-max-value*］

構文の説明

periodic	アカウンティングの更新レコードを定期的にサーバに送信します。
<1-71582>	アカウンティング更新レコードを送信するための定期間隔（分単位）
jitter	定期間隔のジッター パラメータを設定します
maximum	定期間隔の最大ジッター値を設定します（秒単位）
<0-2147483>	定期間隔の最大ジッター値（秒単位）。デフォルト値は300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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、アカウンティング レコードが更新される間隔を 5 分に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# aaa accounting update periodic 5
```

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、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。認証を無効にするには、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ストリングには他のキーワードも表示されますが、サポートされるのは **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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス(config)# aaa new-model
デバイス(config)# aaa authentication dot1x default group radius
```

aaa authentication login

ログイン時の認証、許可、およびアカウンティング（AAA）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 authentication login** コマンドを使用します。

aaa authentication login *authentication-list-name* {**group** }*group-name*

構文の説明

authentication-list-name	ユーザーがログインした時点でアクティブにされる認証方式のリスト名として使用するストリング。
group	サーバ コマンド **group-name** で定義されている RADIUS サーバのサブセットを認証に使用します。
group-name	サーバ グループ名。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、ローカル web 認証で **local_webauth** という名前の認証方式リストを **local** という名前のグループ タイプに設定する例を示します。

```
デバイス(config)# aaa authentication login local_webauth local
```

次に、ローカル web 認証で認証方式を RADIUS サーバー グループに設定する例を示します。

```
デバイス(config)# aaa authentication login webauth_radius group ISE_group
```

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** | **onep** | **policy-if** | **prepaid** | **radius-proxy** | **reverse-access** | **subscriber-service** | **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。
onep	ONEP サービスに許可を実行します。
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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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ー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** および **tacacs server** コマンドを使用します。特定のサーバグループを作成するには、**aaa group server radius**、**aaa group server ldap**、**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 *3 : 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 サーバー グループを調べて、特定の権限をユーザーに許可します。
- If-Authenticated：ユーザーが認証に成功した場合、ユーザー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 サーバーは、**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ーに許可します。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、認可情報を要求しません。認可は、この回線または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グループからの認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認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：ユーザが実行するEXECモードコマンドに適用されます。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されます。
- Network：ネットワーク接続に適用されます。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） **disable**、**enable**、**exit**、**help**、**logout** の 5 つのコマンドは特権レベル 0 と関連付けられています。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。

```
デバイス(config)#  aaa authorization network mygroup group radius local
```

aaa authorization credential download default

ローカル クレデンシャルを使用するように認証方式リストを設定するには、グローバル コンフィギュレーション モードで **aaa authorization credential download default** コマンドを使用します。

aaa authorization credential download default *group-name*

構文の説明

group-name	サーバ グループ名。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

次に、ローカル クレデンシャルを使用するように認証方式リストを設定する例を示します。

```
デバイス(config)# aaa authorization credential-download default local
```

aaa group server ldap

AAA サーバー グループを設定するには、**aaa group server ldap** コマンドを使用します。

aaa group server ldap *group-name*

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 Fuji 16.9.1	このコマンドが導入されました。

次の例では、AAA サーバー グループを設定する方法を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# aaa new-model
デバイス(config)# aaa group server ldap name1
デバイス(config-ldap-sg)# server server1
デバイス(config-ldap-sg)# exit
```

aaa group server radius

各種の RADIUS サーバー ホストを別個のリストおよび別個のメソッドのそれぞれに応じてグループ化するには、グローバル コンフィギュレーション モードで **aaa group server radius** コマンドを使用します。

aaa group server radius *group-name*

構文の説明

group-name	サーバ グループの名前の指定に使用する文字列です。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

認証、認可、およびアカウンティング（AAA）サーバ グループ機能には、既存のサーバ ホストをグループ化する方法が追加されています。この機能を使用して、設定されているサーバ ホストのサブセットを選択し、それらのホストを特定のサービスに使用できます。

グループ サーバは、特定のタイプのサーバ ホストのリストです。現在サポートされているサーバ ホスト タイプは RADIUS サーバ ホストです。グループ サーバは、グローバル サーバ ホスト リストと併せて使用されます。グループ サーバには、選択したサーバ ホストの IP アドレスが一覧表示されます。

次に、3 つのメンバ サーバーからなる **ISE_Group** という AAA グループ サーバーを設定する例を示します。

```
デバイス(config)# aaa group server radius ISE_Group
```

aaa local authentication default authorization

ローカル認証リストを設定するには、**aaa local authentication default authorization** コマンドを使用します。

aaa local authentication default authorization ［*method-list-name* | **default**］

構文の説明

method-list-name	方式リストの名前。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ローカル認証方式リストをデフォルト リストに設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# aaa local authentication default authorization default
```

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 **aaa new-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 Gibraltar 16.10.1	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で、かつ **aaa new-model** コマンドが削除されている場合は、デバイスをリロードして、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。デバイスをリロードしない場合、デバイスは、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。

```
デバイス(config)# aaa new-model
デバイス(config)# line vty 0 15
デバイス(config-line)# login local
デバイス(config-line)# exit
デバイス(config)# no aaa new-model
デバイス(config)# exit
デバイス# 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。

```
デバイス(config)# aaa new-model
デバイス(config)#
```

関連コマンド

コマンド	説明
aaa accounting	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。
aaa authentication arap	TACACS+ を使用する ARAP の AAA 認証方式を有効にします。
aaa authentication enable default	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。
aaa authentication login	ログイン時の AAA 認証を設定します。
aaa authentication ppp	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。
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します。

aaa server radius dynamic-author

デバイスを認証、許可、アカウンティング（AAA）サーバに設定し、外部ポリシー サーバとの相互作用を実行するには、グローバル コンフィギュレーション モードで **aaa server radius dynamic-author** コマンドを使用します。こ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。

aaa server radius dynamic-author
no aaa server radius dynamic-author

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

デバイスは、外部ポリシー サーバとの相互作用を実行するときにサーバとして機能しません。

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
12.2(28)SB	このコマンドが導入されました。
12.4	このコマンドが Cisco IOS Release 12.4 に統合されました。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。
12.2(5)SXI	このコマンドが Cisco IOS Release 12.2(5)SXI に統合されました。
15.2(2)T	このコマンドが、Cisco IOS Release 15.2(2)T に統合されました。
	このコマンドが導入されました。

使用上のガイドライン

ダイナミック認証では、外部ポリシー サーバは、デバイスに対して動的に更新を送信できます。**aaa server radius dynamic-author** コマンドを設定すると、ダイナミック認証ローカル サーバ コンフィギュレーション モードが開始されます。このモードでは、RADIUS アプリケーション コマンドを設定できます。

インテリジェント サービス ゲートウェイ（ISG）のダイナミック認証

ISG は、加入者別およびサービス別の情報が格納されたポリシー サーバと呼ばれる外部デバイスと連携動作します。ISG は、ISG デバイスと外部ポリシー サーバとの間で対話の 2 つのモデル（初期認可と動的認可）をサポートしています。

ダイナミック認証モデルでは、外部ポリシー サーバーは、ISG に対して動的にポリシーを送信できます。これらの処理は、（サービスの選択を通じて）加入者がインバンド方式で開始することも、管理者の操作を通じて開始することもできます。または、アプリケーションは、アルゴリズムに基づいてポリシーを変更できます（たとえば、1 日の特定の時間に、セッションの Quality of Service（QoS）を変更します）。このモデルは、Change of Authorization（CoA）RADIUS 拡張によって容易になります。CoA によりピアツーピア機能が RADIUS に導入され

ました。この機能により、ISGと外部ポリシーサーバがそれぞれRADIUSクライアントとサーバとして動作できます。

例

次に、IP アドレス 10.12.12.12 でクライアントとやり取りするときに、AAA サーバーとして機能するように ISG を設定する例を示します。

```
aaa server radius dynamic-author
 client 10.12.12.12 key cisco
 message-authenticator ignore
```

関連コマンド

コマンド	説明
auth-type (ISG)	サーバー認証タイプを指定します。
client	デバイスが CoA を受け取り、要求を取り外す RADIUS クライアントを指定します。
default	RADIUS アプリケーション コマンドをデフォルトに設定します。
domain	ユーザ名ドメイン オプションを指定します。
ignore	特定のパラメータを無視する動作を上書きします。
port	ローカルの RADIUS サーバがリッスンするポートを指定します。
server-key	RADIUS クライアントと共有する暗号キーを指定します。

aaa session-id

コール内の各認証、認可、アカウンティング（AAA）アカウンティング サービス タイプで同じセッション ID を使用するかどうか、または各アカウンティング サービス タイプに対して異なるセッション ID を割り当てるかどうかを指定するには、グローバル コンフィギュレーション モードで **aaa session-id** コマンドを使用します。**unique** キーワードの有効化後にデフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

aaa session-id [{**common** | **unique**}]
no aaa session-id [**unique**]

構文の説明

common	（オプション）特定のコールに対して送信されたすべてのセッション ID 情報が同じになるようにします。デフォルトの動作は **common** です。
unique	（オプション）対応するサービス アクセス要求およびアカウンティング要求だけが共通のセッション ID を維持するようにします。各サービスのアカウンティング要求には、異なるセッション ID が割り当てられます。

コマンド デフォルト

common キーワードが有効です。

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
12.2(4)B	このコマンドが導入されました。
12.2(8)T	このコマンドが Cisco IOS Release 12.2(8)T に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
	このコマンドが Cisco IOS XE 16.12.1 に統合されました。

使用上のガイドライン

common キーワード動作は、共有データベースに保存するコールの最初のセッション ID を許可します。それ以降のすべてのセッション ID 要求は最初のセッション ID の値を取得します。共有セッション ID はデフォルトの動作であるため、この機能は、**aaa new-model** コマンドの設定後にシステム設定に書き込まれます。

（注） ルータ設定では、**aaa session-id common** または **aaa session-id unique** のいずれかのコマンドを有効にします。2つのコマンド以外を有効にすることはできません。そのため、**no aaa session-id unique** コマンドはデフォルト機能に戻りますが、 **no aaa session-id common** コマンドはデフォルト機能のため影響を受けません。

unique キーワードの動作は、コール中に各アカウンティング タイプ（Auth-Proxy、Exec、Network、Command、System、Connection、Resource）に異なるセッション ID を割り当てます。この動作を指定するには、一意のキーワードを指定する必要があります。セッション ID は、**radius-server attribute 44 include-in-access-req** コマンドを設定することによって RADIUS アクセス要求に含めることができます。アクセス要求内のセッション ID は、同じサービスのアカウンティング要求のセッション ID と同じです。他のすべてのサービスは、同じコールに対して一意のセッション ID を提供します。

例

次に、一意のセッション ID を設定する例を示します。

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
aaa session-id unique
```

関連コマンド

コマンド	説明
aaa new model	AAA をイネーブルにします。
radius-server attribute 44 include-in-access-req	ユーザ認証（事前認証の要求も含む）の前にアクセス要求パケットで RADIUS 属性 44（Accounting Session ID）を送信します。

access-session wireless cui-enable

AAA サーバーに送信される認証およびアカウンティングのメッセージで Chargeable User Identity（CUI）属性を有効にするには、**access-session wireless cui-enable** コマンドを使用します。AAA サーバーに送信される認証およびアカウンティングのメッセージで CUI 属性を無効にするには、このコマンドの **no** 形式を使用します。

access-session wireless cui-enable

no access-session wireless cui-enable

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

CUI は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 Cupertino 17.9.1	このコマンドが導入されました。

使用上のガイドライン

CUI 属性の設定は、802.1x クライアントにのみ適用されます。

例

次に、AAA サーバーに送信される認証およびアカウンティングのメッセージで CUI 属性を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# access-session wireless cui-enable
```

aaa-override

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

ワイヤレス 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 Gibraltar 16.10.1	このコマンドが導入されました。

次の例では、AAA をイネーブルにする方法を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-test
Device(config-wireless-policy)# aaa-override
```

aaa-override vlan fallback

オーバーライドされた VLAN が使用できない場合にポリシープロファイル VLAN へのフォールバックを許可するには、ワイヤレス ポリシー コンフィギュレーション モードで **aaa-override vlan fallback** コマンドを使用します。ポリシープロファイル VLAN へのフォールバッ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。

aaa-override vlan fallback

no aaa-override vlan fallback

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

ワイヤレス ポリシー 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 Bengaluru 17.6.1	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

例

次に、オーバーライドされたVLANが使用できない場合にポリシープロファイルVLANへのフォールバックを許可する例を示します。

```
Device# configure terminal
Device(config)# wireless profile policy defalt-policy-profile
Device(config-wireless-policy)# aaa-override vlan fallback
```

aaa-policy

WLAN ポリシー プロファイルで AAA ポリシーをマッピングするには、**aaa-policy** コマンドを使用します。

aaa-policy *aaa-policy-name*

構文の説明

aaa-policy-name	AAA 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-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、WLAN ポリシー プロファイルで AAA ポリシーをマッピングする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-name
Device(config-wireless-policy)# aaa-policy aaa-policy-name
```

aaa-realm enable

レルムごとにAAA RADUIS選択を有効にするには、**aaa-realm enable** コマンドを使用します。

aaa-realm enable

コマンド デフォルト

なし

コマンド モード

config-aaa-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、レルムごとに AAA RADIUS 選択を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy aaa-profile-name
Device (config-aaa-policy)#  aaa-realm enable
```

absolute-timer

加入者セッションの絶対タイムアウトを有効にするには、サービステンプレート コンフィギュレーション モードで **absolute-timer** コマンドを使用します。タイマ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。

absolute-timer *minutes*
no absolute-timer

構文の説明

minutes	最大セッション時間（分）。範囲：1 ～ 65535。デフォルト：0、タイマーは無効になっています。

コマンド デフォルト

無効（絶対タイムアウトは 0）。

コマンド モード

サービス テンプレート コンフィギュレーション（config-service-template）

コマンド履歴

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

使用上のガイドライン

absolute-timer コマンドを使用すると、加入者セッションがアクティブなままになる時間を分単位で制限できます。このタイマーが期限切れになった後は、新しいリクエストの場合と同様、セッションで接続確立のプロセスを繰り返す必要があります。

例

次に、SVC_3 という名前のサービス テンプレートで絶対タイムアウトを 15 分に設定する例を示します。

```
service-template SVC_3
 description sample
 access-group ACL_2
 vlan 113
 inactivity-timer 15
 absolute-timer 15
```

関連コマンド

コマンド	説明
event absolute-timeout	条件が満たされた場合に制御ポリシーのアクションをトリガーするイベントのタイプを指定します。
inactivity-timer	加入者セッションに対する非アクティブ タイムアウトを有効にします。
show service-template	サービス テンプレートの設定情報を表示します。

access-list

アクセス リスト エントリを追加するには、**access-list** コマンドを使用します。

access-list {*1-99 100-199 1300-1999 2000-2699*}[*sequence-number*] {**deny** | **permit**} {*hostname-or-ip-addr* [{*wildcard-bits* | **log**}] | **any**[**log**] | **host** *hostname-or-ip-addr* **log**} | {**remark**[*line*]}

構文の説明

1 ～ 99	IP 標準アクセス リストを設定します。
100 ～ 199	IP 拡張アクセス リストを設定します。
1300-1999	IP 標準アクセス リスト（拡張範囲）を設定します。
2000 ～ 2699	IP 拡張アクセス リスト（拡張範囲）を設定します。
sequence-number	ACL エントリのシーケンス番号。有効な範囲は 1 ～ 2147483647 です。
deny	拒否されるパケットを設定します。
permit	転送されるパケットを設定します。
hostname-or-ip-addr	一致させるホスト名または IP アドレス。
wildcard-bits	IP アドレスに一致するワイルドカード ビット。
log	このエントリに対するログ一致を設定します。
any	任意のソース ホスト。
host	単一ホストのアドレス。
remark	ACL エントリのコメントを設定します。
line	ACL エントリのコメント。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、アクセス リスト エントリを追加する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# access-list 1 permit any
```

access-list acl-ace-limit

すべての ACL に設定可能な最大 ACE 制限を設定するには、**access-list acl-ace-limit** コマンドを使用します。

access-list acl-ace-limit *max-ace-limit*

構文の説明

max-ace-limit	すべての ACL の ace 制限の最大数。有効な範囲は 1 ～ 4294967295 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ACL の設定可能最大数を 100 に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# access-list acl-ace-limit 100
```

accounting-list

WLAN ポリシー プロファイル 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 ポリシー設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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 ポリシー プロファイル で RADIUS サーバー アカウンティングを設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless profile policy rr-xyz-policy-1
デバイス(config-wireless-policy)# accounting-list test
デバイス(config-wireless-policy)# no shutdown
```

次に、WLAN ポリシー プロファイル で RADIUS サーバー アカウンティングを無効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless profile policy rr-xyz-policy-1
デバイス(config-wireless-policy)# no accounting-list test
デバイス(config-wireless-policy)# no shutdown
```

acl-policy

アクセス コントロール リスト（ACL）を設定するには、**acl-policy** コマンドを使用します。

acl-policy *acl-policy-name*

構文の説明

acl-policy-name	ACL 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-wireless-flex-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ACL ポリシー名を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy my-acl-policy
```

action power-saving-mode power-profile

特定の電力プロファイルを特定のカレンダープロファイルにマッピングし、カレンダープロファイルの省電力モードアクションをマッピングするには、**action power-saving-mode power-profile** コマンドを使用します。このコマン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。

action power-saving-mode power-profile *power-profile-name*

[no] action power-saving-mode power-profile *power-profile-name*

構文の説明

power-profile-name	電力プロ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

AP カレンダー プロファイル 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 Cupertino 17.8.1	このコマンドが導入されました。

例

次に、特定の電力プロファイルを特定のカレンダープロファイルにマッピングし、カレンダープロファイルの省電力モードアクションをマッピングする例を示します。

```
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# calendar-profile ap-calendar-profile
Device(config-ap-profile-calendar)# action power-saving-mode power-profile power-profile1
```

address

キーリングで手動で設定するリモート ピアの Rivest, Shamir, and Adelman（RSA）公開キーの IP アドレスを指定するには、rsa-pubkey コンフィギュレーション モードで **address** コマンドを使用します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

address *ip-address*
no address *ip-address*

構文の説明

ip-address	リモート ピアの IP アドレス

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

Rsa-pubkey の設定

コマンド履歴

リリース	変更内容
11.3 T	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
Cisco IOS XE Release 2.6	このコマンドが Cisco IOS XE Release 2.6 に統合されました。

使用上のガイドライン

このコマンドを使用する前に、暗号キーリング モードで **rsa-pubkey** コマンドを入力する必要があります。

例

次に、IP セキュリティ（IPSec）ピアの RSA 公開キーを指定する例を示します。

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

関連コマンド

コマンド	説明
crypto keyring	IKE 認証時に使用する暗号化キーリングを定義します。
key-string	リモート ピアの RSA 公開キーを指定します。
rsa-pubkey	IKE 認証時の暗号化またはシグニチャに使用される RSA 手動キーを定義します。

address

Software-Defined Application Visibility and Control（SD-AVC）コントローラの IP アドレスを設定するには、**address** コマンドを使用します。SD-AVC コントローラの IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

address *ipv4-address*

no address

構文の説明

ipv4-address	SD-AVC コントローラの IPv4 アドレス。

コマンド デフォルト

コントローラの IP アドレスは設定されていません。

コマンド モード

SD サービス コントローラ コンフィギュレーション（config-sd-service-controller）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが導入されました。

使用上のガイドライン

IPv4 アドレスのみをサポートしています。

例

次に、SD-AVC コントローラの IP アドレスを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
VM1(config)# avc sd-service
Device(config-sd-service)# controller
Device(config-sd-service-controller)# address 209.165.201.0
```

address prefix

アドレス割り当て用のアドレス プレフィックスを指定するには、インターフェイス コンフィギュレーション モードで **address prefix** コマンドを使用します。アドレス プレフィックスを削除するには、このコマンドの **no** 形式を使用します。

address prefix ipv6-prefix [**lifetime** {**valid-lifetime preferred-lifetime** | **infinite**}]
no address prefix

構文の説明

ipv6-prefix	IPv6 アドレス プレフィックス。
lifetime {valid-lifetime preferred-lifetime | infinite}]	（オプション）IPv6 アドレス プレフィックスが有効な状態を維持するタイム インターバル（秒）を指定します。**infinite** キーワードが指定されている場合、時間間隔は期限切れになりません。

コマンド デフォルト

IPv6 アドレス プレフィックスは割り当てられていません。

コマンド モード

DHCP プール設定（config-dhcpv6）

コマンド履歴

リリース	変更内容
12.4(24)T	このコマンドが導入されました。

使用上のガイドライン

address prefix コマンドを使用すると、IPv6 DHCP プール 設定で 1 つまたは複数のアドレス プレフィックスを設定できます。IPv6 DHCP アドレス プールが使用されるたびに、IPv6 DHCP プールに関連付けられている各アドレス プレフィックスからアドレスが割り当てられます。

例

次に、1 つの IPv6 アドレス プレフィックスを含む engineering という名前のプールを設定する例を示します。

```
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime infinite
```

関連コマンド

コマンド	説明
ipv6 dhcp pool	DHCPv6 サーバー設定情報プールを設定し、DHCPv6 プール コンフィギュレーション モードを開始します。

advice-charge

各ネットワークアクセス識別子（NAI）レルムのサービスセット識別子（SSID）の使用に対する課金通知を設定するには、**advice-charge** コマンドを使用します。課金通知を削除するには、このコマンドの **no** 形式を使用します。

advice-charge {**data** | **time** | **time-and-data** | **unlimited**}

構文の説明

data	データ量に基づいて料金を指定します。
time	時間に基づいて料金を指定します。
time-and-data	時間とデータ量に基づいて料金を指定します。
unlimited	無制限アクセスの料金を指定します。

コマンド デフォルト

課金通知は設定されていません。

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、各 NAI レルムの SSID の使用に対する課金通知を設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# advice-charge unlimited
```

airtime-fairness mode

（注） Cisco Air Time Fairness（ATF）は、2.4 または 5 GHz 無線で個別に有効にする必要があります。

異なるモードでの電波時間正常性を設定するには、**airtime-fairness mode** コマンドを使用します。

airtime-fairness mode {**enforce-policy** | **monitor**}

構文の説明

enforce-policy	このモードは、ATF が動作していることを示します。
monitor	このモードは、通信時間に関する情報を収集し、通信時間の使用状況を報告します。

コマンド デフォルト

なし

コマンド モード

RF プロファイルの設定（config-rf-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

次に、さまざまなモードで電波時間正常性を設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# ap dot11 24ghz rf-profile rfprof24_1
デバイス(config-rf-profile)# airtime-fairness mode enforce-policy
デバイス(config-rf-profile)# airtime-fairness optimization
デバイス(config-rf-profile)# end
```

allow at-least min-number at-most max-number

RA スロットラ ポリシーでスロットル期間ごとに、デバイスあたりのマルチキャスト RA の数を制限するには、**allow at-least** *min-number* **at-most** *max-number* コマンドを使用します。

allow at-least *min-number* **at-most** {*max-number* | **no-limit**}

構文の説明

at-least *min-number*	スロットリングの適用前に、ルータあたりのマルチキャストRAの最小保証数を入力します。有効な範囲は 0 ～ 32 です。
at-most *max-number*	スロットルを適用にするルータのマルチキャストRAの最大数を入力します。有効な範囲は 0 ～ 256 です。
at-most no-limit	ルータ レベルでの上限はありません。

コマンド デフォルト

なし

コマンド モード

config-nd-ra-throttle

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、RAスロットラポリシーのスロットル期間ごとに、デバイスあたりのマルチキャスト RA 数を制限する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ipv6 nd ra-throttler policy ra-throttler-policy-name
Device(config-nd-ra-throttle)# allow at-least 5 at-most 10
```

amsdu（メッシュ）

メッシュ AP プロファイルのバックホール集約 MAC サービス データ ユニット（A-MSDU）を設定するには、**amsdu** コマンドを使用します。

amsdu

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

amsdu は有効になっています。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、メッシュ AP プロファイルの A-MSDU を設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# amsdu
```

anqp

Generic Advertisement Service（GAS）または Access Network Query Protocol（ANQP）プロトコル設定を設定するには、**anqp** コマンドを使用します。プロトコル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。

anqp {**fragmentation-threshold** *fragmentation-threshold* | **gas-timeout** *gas-timeout*}

構文の説明

fragmentation-threshold	ANQP 応答フラグメンテーションしきい値（バイト単位）。有効な範囲は 16 ～ 1462 です。
gas-timeout	GAS 要求タイムアウト（ミリ秒単位）。有効な範囲は 100 ～ 10000 です。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、GAS 要求タイムアウトを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# anqp gas-timeout 100
```

anqp-domain-id

ホットスポット 2.0 Access Network Query Protocol（ANQP）ドメイン識別子を設定するには、**anqp-domain-id** コマンドを使用します。ドメイン識別子を削除するには、このコマンドの **no** 形式を使用します。

anqp-domain-id *domain-id*

構文の説明

domain-id	ANQP ドメイン ID。範囲は 0 ～ 65535 です。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、ホットスポット 2.0 ANQP ドメイン識別子を設定する例を示します。

```
Device(config)#wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# anqp-domain-id 100
```

antenna beam-selection

アンテナのビーム選択を設定するには、ワイヤレス無線プロファイル コンフィギュレーション モードで **antenna beam-selection** コマンドを使用します。この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。

antenna beam-selection { **narrow tilt** { **10** | **20** } | **wide** }

構文の説明

narrow tilt{**10**	**20**}	ナロービーム選択のチルト角度を設定します。10 度または 20 度のチルトに設定できます。
10	**20**	ナロービーム選択のチルト角度を 10 度または 20 度に設定します。
wide	ワイドビーム選択を設定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス無線プロファイル 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 Bengaluru 17.6.1	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

例

次に、アンテナのビーム選択を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
Device(config-wireless-profile)# antenna beam-selection narrow tilt 10
```

antenna count

無線プロファイルの下で有効にするアンテナの数を設定するには、無線プロファイル コンフィギュレーション モードで **antenna count** コマンドを使用します。設定されたアンテナの数を無効にするには、このコマンドの **no** 形式を使用します。

antenna count *0 - 8*

構文の説明

0-8	アンテナ数を指定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス無線プロファイル 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 Bengaluru 17.6.1	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

例

次に、無線プロファイルの下で有効にするアンテナの数を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
Device(config-wireless-radio-profile)# antenna count 4
```

antenna monitoring

アンテナの切断検知を設定するには、**antenna monitoring** コマンドを使用します。アンテナの切断検知を無効にするには、このコマンドの **no** 形式を使用します。

antenna monitoring [**rssi-failure-threshold** *threshold-value* | **weak-rssi** *weak-rssi-value* | **detection-time** *detect-time-in-mins*]

no antenna monitoring

構文の説明

rssi-failure-threshold *threshold-value*	RSSI 障害しきい値（dB 単位）を設定します。有効な値の範囲は 10 ～ 90 で、デフォルトは 40 です。 *threshold-value* が、AP の受信アンテナ間の信号強度の差分を決定します。
weak-rssi *weak-rssi-value*	低精度の RSSI 値（dBm 単位）を設定します。有効な値の範囲は -90 ～ -10 で、デフォルトは 60 です。 AP が受信した RSSI が設定された *weak-rssi-value* 以上である場合、アンテナが破損していると見なされます。*weak-rssi-value* の設定は、ネイバー AP の展開の距離に基づきます。
detection-time *detect-time-in-mins*	アンテナの切断検知時間（分単位）を設定します。有効な値の範囲は 9 ～ 180 で、デフォルトは 120 です。 *detect-time-in-mins* は、問題としてフラグ付けする前に信号強度（*weak-rssi-value* と *threshold-value* 両方の基準）をモニターするために使用されます。

コマンド デフォルト

アンテナモニタリングは有効になっていません。

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.4.1	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、次の AP でのみサポートされます。

- Cisco Catalyst 9120AX シリーズ アクセスポイント
- Cisco Catalyst 9130AX シリーズ アクセスポイント
- Cisco Aironet 2800e アクセスポイント
- Cisco Aironet 3800e アクセスポイント

例

次に、アンテナの切断検知を有効にする例を示します。

```
Device# configure terminal
Device(config)# ap profile xyz-ap-profile
Device(config-ap-profile)# antenna monitoring
```

ap

Cisco AP を設定するには、**ap** コマンドを使用します。

ap *mac-address*

構文の説明	
mac-address	AP のイーサネット MAC アドレス。

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 Everest 16.6.1	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。

例

次に、Cisco AP を設定する例を示します。

```
Device(config)# ap F866.F267.7DFB
```

ap audit-report

AP 監査レポートを有効にするか設定するには、**ap audit-report** コマンドを使用します。

ap audit-report {**enable** | **interval** *interval*}

構文の説明

enable	AP 監査レポートを有効にします。
interval	AP 監査レポートの間隔を設定します。
interval	AP監査レポート間隔（分単位）。デフォルトは1440です。有効な範囲は0～43200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 Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、AP 監査レポート間隔を設定する例を示します。

```
Device(config)# ap audit-report interval 1300
```

ap auth-list

AP 認証リストを設定するには、グローバル コンフィギュレーション モードで **ap auth-list** コマンドを使用します。AP 認証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。

ap auth-list {**authorize-mac** | **authorize-serialNum** | **method-list** *method-list-name*}

no ap auth-list {**authorize-mac** | **authorize-serialNum** | **method-list** *method-list-name*}

構文の説明

authorize-mac	MAC を使用して AP 認証ポリシーを設定します。
auhorize-serialNum	シリアル番号を使用してAP認証ポリシーを設定します。
method-list	AP 認証方式リストを設定します。
method-list-name	方式リスト名を示します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、シリアル番号を使用して AP 認証ポリシーを設定する例を示します。

```
Device(config) #ap auth-list authorize-serialNum
```

ap auth-list ap-cert-policy allow-mic-ap

CAPWAP-DTLS ハンドシェイク中の AP 証明書ポリシーを有効にするには、グローバル コンフィギュレーション モードで **ap auth-list ap-cert-policy allow-mic-ap** コマンドを使用します。CAPWAP-DTLS ハンドシェイク中の AP 証明書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-cert-policy allow-mic-ap

no ap auth-list ap-cert-policy allow-mic-ap

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

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 Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、CAPWAP-DTLS ハンドシェイク中の AP 証明書ポリシーを設定する例を示します。

```
Device# configure terminal
Device(config)# ap auth-list ap-cert-policy
Device(config)# ap auth-list ap-cert-policy allow-mic-ap
```

ap auth-list ap-cert-policy allow-mic-ap trustpoint

コントローラ証明書チェーンのトラストポイント名を設定するには、グローバル コンフィギュレーション モードで **ap auth-list ap-cert-policy allow-mic-ap trustpoint** 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。

ap auth-list ap-cert-policy allow-mic-ap trustpoint

no ap auth-list ap-cert-policy allow-mic-ap trustpoint

構文の説明

trustpoint-name	ワイヤレスコントローラ証明書チェーンのトラストポイント名を指定します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、コントローラ証明書チェーンのトラストポイント名を設定する例を示します。

```
Device# configure terminal
Device(config)# ap auth-list ap-cert-policy
Device(config)# ap auth-list ap-cert-policy allow-mic-ap trustpoint trustpoint-name
```

ap auth-list ap-cert-policy mac-address MAC-address | serial-number AP-serial-number policy-type mic

イーサネット MAC アドレスまたは AP のアセンブリシリアル番号に基づいて AP 証明書ポリシーを設定するには、**ap auth-list ap-cert-policy** {**mac-address** *H.H.H* | **serial-number** *AP-serial-number*} **policy-type mic** コマンドを使用します。この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 auth-list ap-cert-policy { **mac-address** *H.H.H* | **serial-number** *AP-serial-number* } **policy-type mic**

no ap auth-list ap-cert-policy { **mac-address** *H.H.H* | **serial-number** *AP-serial-number* } **policy-type mic**

構文の説明

ap auth-list	アクセスポイントの承認リストを設定します。
ap-cert-policy	CAPWAP DTLS 中の AP 証明書ポリシーを指定します。
mac-address *MAC-address*	イーサネット MAC に基づいて AP 証明書ポリシーを設定します。
serial-number *AP-serial-number*	シリアル番号に基づいて AP 証明書ポリシーを設定します。
policy-type	AP 証明書ポリシータイプを設定します。
mic	MIC AP ポリシーを選択します。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、イーサネット MAC アドレスまたは AP のアセンブリシリアル番号に基づいて AP 証明書ポリシーを設定する例を示します。

```
Device# configure terminal
Device(config)# ap auth-list ap-cert-policy mac-address 10.1.1 policy-type mic

Device(config)# ap auth-list ap-cert-policy serial-number ap-serial-number policy-type
mic
```

ap auth-list ap-policy

device 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、 **ap auth-list ap-policy** コマンドを使用します。device 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 Gibraltar 16.10.1	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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(config)# ap auth-list ap-policy ssc
```

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 Gibraltar 16.10.1	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。

```
デバイス(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。

```
デバイス(config)# ap capwap multicast service-policy output tunnmulpolicy
```

ap capwap retransmit

AP プロファイルの下の 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 profile default-ap-profile

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

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# 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。

```
デバイス# ap capwap retransmit interval 5
```

ap capwap timers

AP プロファイルモードで高度なタイマー設定を指定するには、 **ap capwap timers** コマンドを使用します。

ap profile default-ap-profile

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device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-timeout local	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device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	device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device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 device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 device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、deviceへの接続が復元されるまで、device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

AP プロファイルモード（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス(config)# ap profile default-ap-profile

デバイス(config-ap-profile)# 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。

```
デバイス(config)# ap profile default-ap-profile

デバイス(config-ap-profile)# 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。

```
デバイス(config)# ap profile default-ap-profile

デバイス(config-ap-profile)# 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。

```
デバイス(config)# ap profile default-ap-profile

デバイス(config-ap-profile)# 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。

```
デバイス(config)# ap profile default-ap-profile

デバイス(config-ap-profile)# ap capwap timers primed-join-timeout 360
```

ap cisco-dna token

Cisco DNA のトークンを設定するには、**ap cisco-dna token** コマンドを使用します。この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 cisco-dna token { **0** | **8** } *<cisco-token-number>*

no ap cisco-dna token

構文の説明

Cisco-dna	Cisco DNA のパラメータを設定します。
token	Cisco DNA のトークンを設定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	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

例

次に、Cisco DNA のトークンを設定する例を示します。

```
Device(config)# ap cisco-dna token 0 <cisco-token-number>
```

ap country

device の 1 つ以上の国コードを設定するには、 **ap country** 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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.1	このコマンドはすでに廃止されています。 （注） Cisco IOS XE Amsterdam 17.3.1 以降、**ap country** コマンドは廃止され、**wireless country** <*1 country code*> に改名されます。このコマンドでは、20 を超える国の国コードを入力できます。既存の **ap country** コマンドは引き続き機能しますが、**wireless country** <*1 country code*> コマンドを使用することを推奨します。

使用上のガイドライン

Cisco device は、ネットワーク管理者または資格のある IT 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、device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。

```
デバイス(config)# ap country IN,FR
```

ap dot11 24ghz | 5ghz dot11ax spatial-reuse obss-pd

すべての 2.4 GHz または 5 GHz 無線で 802.11ax OBSS PD ベースの空間再利用を設定するには、**ap dot11** {**24ghz** | **5ghz**} **dot11ax spatial-reuse obss-pd** コマンドを使用します。OBSS ベースの空間再利用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 dot11 { **24ghz** | **5ghz** } **dot11ax spatial-reuse obss-pd**

no ap dot11 { **24ghz** | **5ghz** } **dot11ax spatial-reuse obss-pd**

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.4.1	このコマンドが導入されました。

例

次に、802.11ax OBSS PD ベースの空間再利用を設定する例を示します。

```
Device(config)# ap dot11 24ghz or 5ghz dot11ax spatial-reuse obss-pd
```

ap dot11 24ghz | 5ghz dot11ax spatial-reuse obss-pd non-srg-max

すべての 2.4 GHz または 5 GHz 無線で 802.11ax 非空間再利用グループ（SRG）OBSS PD の最大値を設定するには、**ap dot11** {**24ghz** | **5ghz**} **dot11ax spatial-reuse obss-pd non-srg-max** *-82 - -62* コマンドを使用します。すべての 2.4 GHz または 5 GHz 無線で 802.11ax 非空間再利用グループ（SRG）OBSS PD の最大値を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 { **24ghz** | **5ghz** } **dot11ax spatial-reuse obss-pd non-srg-max** *-82 - -62*

no ap dot11 { **24ghz** | **5ghz** } **dot11ax spatial-reuse obss-pd non-srg-max** *-82 - -62*

構文の説明

-82 - -62	非 SRG OBSS PD の最大値を dBm 単位で指定します

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.4.1	このコマンドが導入されました。

例

次に、すべての 2.4 GHz または 5 GHz 無線で 802.11ax 非 SRG OBSS PD の最大値を設定する例を示します。

```
Device(config)# ap dot11 24ghz or 5ghz dot11ax spatial-reuse obss-pd non-srg-max -80
```

ap dot11 24ghz | 5ghz rrm ndp-mode

802.11a ネイバー探索の動作モードを設定するには、**ap dot11** {**24ghz** | **5ghz**} **rrm ndp-mode** コマンドを使用します。

ap dot11 { **24ghz** | **5ghz** } **rrm ndp-mode** { **auto** | **off-channel** }

構文の説明

auto	auto モードを有効にします。
off-channel	RF ASIC 無線で NDP パケットを有効にします。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、802.11a ネイバー探索の動作モードを設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 24ghz or 5ghz rrm ndp-mode auto
```

ap dot11 24ghz cleanair

2.4 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 **ap dot11 24ghz cleanair** コマンドを使用します。2.4 GHz 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス(config)# ap dot11 24ghz cleanair
```

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 **default ap dot11 24ghz cleanair device** 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 Gibraltar 16.10.1	このコマンドが導入されました。
	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。

```
デバイス(config)# default ap dot11 24ghz cleanair device video
```

ap dot11 24ghz dot11g

Cisco Wireless LAN ソリューションの 802.11g ネットワークを有効または無効にするには、 **ap dot11 24ghz dot11g** 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

ap dot11 24ghz dot11g コマンドを入力する前に、**ap dot11 24ghz shutdown** コマンドでシスコの 802.11 対応無線を無効にします。

802.11g ネットワークのサポートを設定後、**no ap dot11 24ghz shutdown** コマンドを使用して 802.11 2.4 Ghz 無線を有効にします。

次に、802.11g ネットワークを有効にする例を示します。

```
デバイス(config)# ap dot11 24ghz dot11g
```

ap dot11 24ghz rate

802.11b 動作速度を設定するには、**ap dot11 24ghz rate** コマンドを使用します。

ap dot11 24ghz rate {**RATE_11M** | **RATE_12M** | **RATE_18M** | **RATE_1M** | **RATE_24M** | **RATE_2M** | **RATE_36M** | **RATE_48M** | **RATE_54M** | **RATE_5_5M** | **RATE_6M** | **RATE_9M**} {**disable** | **mandatory** | **supported**}

構文の説明

RATE_11M	11 Mbps のレートで送信されるデータを設定します
RATE_12M	12 Mbps のレートで送信されるデータを設定します
RATE_18M	18 Mbps のレートで送信されるデータを設定します
RATE_1M	1 Mbps のレートで送信されるデータを設定します
RATE_24M	24 Mbps のレートで送信されるデータを設定します
RATE_2M	2 Mbps のレートで送信されるデータを設定します
RATE_36M	36 Mbps のレートで送信されるデータを設定します
RATE_48M	48 Mbps のレートで送信されるデータを設定します
RATE_54M	54 Mbps のレートで送信されるデータを設定します
RATE_5_5M	5.5 Mbps のレートで送信されるデータを設定します
RATE_6M	6 Mbps のレートで送信されるデータを設定します
RATE_9M	9 Mbps のレートで送信されるデータを設定します
disable	指定したデータ レートを無効にします。クライアントが通信に使用するデータ レートも指定するように定義します。
mandatory	AP と関連付けるために、クライアントがこのデータ レートをサポートしていると定義します。
supported	関連付けたクライアントは、このデータ レートをサポートしていれば、このレートを使用して AP と通信することができます。ただし、クライアントは AP との関連付けにこのデータ レートを使用する必要はありません。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、802.11b 動作速度を 9 Mbps に設定し、必須にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz rate RATE_9M mandatory
```

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 **ap dot11 24ghz rrm channel cleanair-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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

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

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 **ap dot11 24ghz rrm channel device** 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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device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。

```
デバイス(config)# ap dot11 24ghz rrm channel device
```

ap dot11 24ghz rrm optimized-roam

802.11b ネットワークに最適化されたローミングを設定するには、**ap dot11 24ghz rrm optimized-roam** コマンドを使用します。

ap dot11 24ghz rrm optimized-roam ［**data-rate-threshold** {**11M** | **12M** | **18M** | **1M** | **24M** | **2M** | **36M** | **48M** | **54M** | **5_5M** | **6M** | **9M** | **disable**}］

構文の説明

data-rate-threshold	802.11b で最適化されたローミングのデータ レートしきい値を設定します。
11M	802.11b で最適化されたローミングのデータ レートしきい値を 11 Mbps に設定します
12M	802.11b で最適化されたローミングのデータ レートしきい値を 12 Mbps に設定します
18M	802.11b で最適化されたローミングのデータ レートしきい値を 18 Mbps に設定します
1M	802.11b で最適化されたローミングのデータ レートしきい値を 1 Mbps に設定します
24M	802.11b で最適化されたローミングのデータ レートしきい値を 24 Mbps に設定します
2M	802.11b で最適化されたローミングのデータ レートしきい値を 2 Mbps に設定します
36M	802.11b で最適化されたローミングのデータ レートしきい値を 36 Mbps に設定します
48M	802.11b で最適化されたローミングのデータ レートしきい値を 48 Mbps に設定します
54M	802.11b で最適化されたローミングのデータ レートしきい値を 54 Mbps に設定します
5_5M	802.11b で最適化されたローミングのデータ レートしきい値を 5.5 Mbps に設定します
6M	802.11b で最適化されたローミングのデータ レートしきい値を 6 Mbps に設定します
9M	802.11b で最適化されたローミングのデータ レートしきい値を 9 Mbps に設定します
disable	データ レートしきい値を無効にします。

コマンド デフォルト なし

コマンド モード 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、802.11b ネットワークの最適化されたローミングを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz rrm optimized-roam
```

ap dot11 24ghz rx-sop threshold

802.11b 無線受信機のパケット開始（RxSOP）を設定するには、**ap dot11 24ghz rx-sop threshold** コマンドを使用します。

ap dot11 24ghz rx-sop threshold {**auto** | **high** | **low** | **medium** | **custom** *rxsop-value*}

構文の説明

auto	RxSOP 値をデフォルト値に戻します。
high	RxSOP 値を高しきい値（–79 dBm）に設定します。
medium	RxSOP 値を中しきい値（–82 dBm）に設定します。
low	RxSOP 値を低しきい値（–85 dBm）に設定します。
custom *rxsop-value*	RxSOP 値をカスタムしきい値（–85 dBm ～ –60 dBm）に設定します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

RxSOP は、アクセス ポイントの無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。レベルが高いほど、無線機の感度が低く、レシーバ セル サイズが小さくなります。次の表に、2.4 GHz 帯域の高、中、低レベルの RxSOP しきい値およびカスタム レベルを示します。

表 *4 : 2.4 GHz* 帯域の *RxSOP* しきい値

高しきい値	中しきい値	低しきい値	カスタムしきい値
–79 dBm	–82 dBm	–85 dBm	–85 dBm ～ –60 dBm

例

次に、802.11b 無線受信機のパケット開始（RxSOP）値を auto に設定する例を示しています。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz rx-sop threshold auto
```

ap dot11 24ghz shutdown

802.11a ネットワークを無効にするには、**ap dot11 24ghz shutdown** コマンドを使用します。

ap dot11 24ghz shutdown

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、802.11a ネットワークを無効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# ap dot11 24ghz shutdown
```

ap dot11 5ghz channelswitch quiet

802.11h チャネル スイッチ静音モードを設定するには、**ap dot11 5ghz channelswitch quiet** コマンドを使用します。

ap dot11 5ghz channelswitch quiet

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、802.11h チャネル スイッチ静音モードを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz channelswitch quiet
```

ap dot11 5ghz cleanair

5GHz 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 **ap dot11 5ghz cleanair** 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス(config)# ap dot11 5ghz cleanair
```

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 **default ap dot11 5ghz cleanair device** 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 Gibraltar 16.10.1	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。

```
デバイス(config)# default ap dot11 5ghz cleanair device video
```

ap dot11 5ghz power-constraint

802.11h の電力制限値を設定するには、 **ap dot11 5ghz power-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 Gibraltar 16.10.1	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。

```
デバイス(config)# ap dot11 5ghz power-constraint 5
```

ap dot11 5ghz rate

802.11a 動作速度を設定するには、**ap dot11 5ghz rate** コマンドを使用します。

ap dot11 5ghz 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	12 Mbps のレートで送信されるデータを設定します
RATE_18M	18 Mbps のレートで送信されるデータを設定します
RATE_24M	24 Mbps のレートで送信されるデータを設定します
RATE_36M	36 Mbps のレートで送信されるデータを設定します
RATE_48M	48 Mbps のレートで送信されるデータを設定します
RATE_54M	54 Mbps のレートで送信されるデータを設定します
RATE_6M	6 Mbps のレートで送信されるデータを設定します
RATE_9M	9 Mbps のレートで送信されるデータを設定します
disable	指定したデータ レートを無効にします。クライアントが通信に使用するデータ レートも指定するように定義します。
mandatory	AP と関連付けるために、クライアントがこのデータ レートをサポートしていると定義します。
supported	関連付けたクライアントは、このデータ レートをサポートしていれば、このレートを使用して AP と通信することができます。ただし、クライアントは AP との関連付けにこのデータ レートを使用する必要はありません。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、802.11a の動作速度を 24 Mbps に設定し、サポートする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz rate RATE_24M supported
```

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 **ap dot11 5ghz rrm channel cleanair-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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

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

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 **ap dot11 5ghz rrm channel device** 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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device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。

```
デバイス(config)# ap dot11 5ghz rrm channel device
```

ap dot11 5ghz rrm channel zero-wait-dfs

5 GHz デバイスでゼロ待機動的周波数選択機能をグローバルに有効にするには、**ap dot11 5ghz rrm channel zero-wait-dfs** 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。

ap dot11 5ghz rrm channel zero-wait-dfs

no ap dot11 5ghz rrm channel zero-wait-dfs

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

ゼロ待機動的周波数選択機能は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 Cupertino 17.9.1	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 デバイスでのみ適用されます。

例

次に、5 GHz デバイスでゼロ待機動的周波数選択機能を有効にする例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz rrm channel zero-wait-dfs
```

ap dot11 5ghz rx-sop threshold

802.11a 無線受信機のパケット開始（RxSOP）を設定するには、**ap dot11 5ghz rx-sop threshold** コマンドを使用します。

ap dot11 5ghz rx-sop threshold {**auto** | **high** | **low** | **medium** | **custom** *rxsop-value*}

構文の説明

auto	RxSOP 値をデフォルト値に戻します。
high	RxSOP 値を高しきい値（–76 dBm）に設定します。
medium	RxSOP 値を中しきい値（–78 dBm）に設定します。
low	RxSOP 値を低しきい値（–80 dBm）に設定します。
custom *rxsop-value*	RxSOP 値をカスタムしきい値（–85 dBm ～ –60 dBm）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

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

RxSOP は、アクセス ポイントの無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。レベルが高いほど、無線機の感度が低く、レシーバ セル サイズが小さくなります。次の表に、5 GHz 帯域の高、中、低レベルの RxSOP しきい値およびカスタム レベルを示します。

表 *5 : 5 GHz* 帯域の *RxSOP* しきい値

高しきい値	中しきい値	低しきい値	カスタムしきい値
–76 dBm	-78 dBm	–80 dBm	–85 dBm ～ –60 dBm

例

次に、802.11b 無線受信機のパケット開始（RxSOP）値を –70 dBm のカスタム値に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 24ghz rx-sop threshold custom -70
```

ap dot11 5ghz shutdown

802.11a ネットワークを無効にするには、**ap dot11 5ghz shutdown** コマンドを使用します。

ap dot11 5ghz shutdown

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、802.11a ネットワークを無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz shutdown
```

ap dot11 5ghz smart-dfs

レーダー干渉チャネルに対して非占有時間を使用するように設定するには、**ap dot11 5ghz smart-dfs** コマンドを使用します。

ap dot11 5ghz smart-dfs

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、レーダー干渉チャネルに対して非占有時間を使用するように設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz smart-dfs
```

ap dot11 6ghz cleanair

6 GHz 無線の CleanAir 機能を設定するには、**ap dot11 6ghz cleanair** コマンドを使用します。この機能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。

ap dot11 6ghz cleanair

no ap dot11 6ghz 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

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 Cupertino 17.9.1	このコマンドが追加されました。

例

次に、6 GHz 無線の CleanAir 機能を設定する例を示します。

```
Device# ap dot11 6ghz cleanair
```

ap dot11 6ghz rf-profile

802.11 6 GHz パラメータの RF プロファイルを設定するには、**ap dot11 6ghz rf-profile** を使用します

ap dot11 6ghz rf-profile *rf-profile-name*

構文の説明

rf-profile-name	RFプロファイル名を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、802.11 6 GHz パラメータの RF プロファイルを設定する例を示します。

```
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
```

ap dot11

Qualcomm ベースの 2.4 GHz または 5 GHz 無線でスペクトル インテリジェンス（SI）を設定するには、**ap dot11 SI** コマンドを使用します。

ap dot11 {**24ghz** | **5ghz** } **SI**

構文の説明

24ghz	2.4 GHz 無線機
5ghz	5 GHz 無線機
SI	スペクトラムインテリジェンス（SI）を有効にします。コマンドに [no] を入力すると、SI が無効になります。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、5 GHz 無線で SI を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap dot11 5ghz SI
```

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、 **ap dot11 beaconperiod** 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

ビーコン期間を変更する前に、 **ap dot11** {**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ください。ビーコン期間を変更した後、 **no ap dot11** {**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ます。

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。

```
デバイス(config)# ap dot11 5ghz beaconperiod 120
```

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、**ap dot11 cac media-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**{**eighteen** | **eleven** | **fiftyFour** | **fivePointFive** | **fortyEight** | **nine** | **oneFifty** | **oneFortyFourPointFour** | **oneThirty** | **oneThirtyFive** | **seventyTwoPointTwo** | **six** | **sixtyFive** | **thirtySix** | **threeHundred** | **twelve** | **twentyFour** | **two** | **twoSeventy**}}

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。
- **ap dot11** {**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。
- **ap dot11** {**24ghz | 5ghz**} **cac voice acm** または **ap dot11** {**24ghz | 5ghz**} **cac video acm** 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。

```
デバイス(config)# ap dot11 5ghz cac media-stream multicast max-retry-percent 90
```

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、 **ap dot11 cac multimedia** コマンドを使用します。

ap dot11 {**24ghz** | **5ghz**} **cac multimedia max-bandwidth** *bandwidth*

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。
bandwidth	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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。
- **ap dot11** {**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。
- **ap dot11** {**24ghz | 5ghz**} **cac voice acm** または **ap dot11** {**24ghz | 5ghz**} **cac video acm** 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。

```
デバイス(config)# ap dot11 5ghz cac multimedia max-bandwidth 5
```

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、**ap dot11 cac voice** 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、**no ap dot11** {**24ghz	5ghz**} **cac voice acm** 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、**no ap dot11** {**24ghz	5ghz**} **cac voice load-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。
x	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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。
- **ap dot11** {**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。

- **ap dot11** {**24ghz** | **5ghz**} **cac voice acm** または **ap dot11** {**24ghz** | **5ghz**} **cac video acm** 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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(config)# ap dot11 24ghz cac voice tspec-inactivity-timeout enable
```

ap dot11 cleanair

802.11 ネットワークの CleanAir を設定するには、 **ap dot11 cleanair** 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 Gibraltar 16.10.1	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。

```
デバイス(config)# ap dot11 24ghz cleanair
```

ap dot11 cleanair alarm air-quality

2.4 GHz または 5 GHz 無線の電波品質の CleanAir アラームを設定するには、**ap dot11** {**24ghz** | **5ghz**} **cleanair alarm air-quality** を使用します

ap dot11 { **24ghz** | **5ghz** } **cleanair alarm air-quality**

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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、2.4 GHz または 5 GHz 無線の電波品質の CleanAir アラームを設定する例を示します。

```
Device(config)# ap dot11 24ghz cleanair alarm air-quality
```

ap dot11 cleanair alarm air-quality threshold

2.4 GHz または 5 GHz 無線の電波品質アラームしきい値を設定するには、**ap dot11** {**24ghz** | **5ghz**} **cleanair alarm air-quality threshold** を使用します

ap dot11 { **24ghz** | **5ghz** } **cleanair alarm air-quality threshold** *threshold-value*

構文の説明

threshold-value	電波品質アラームしきい値を指定します。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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、2.4 GHz または 5 GHz 無線の電波品質アラームしきい値を設定する例を示します。

```
Device(config)# ap dot11 24ghz cleanair alarm air-quality threshold 25
```

ap dot11 cleanair alarm device cont-tx

2.4 GHz または 5 GHz 無線の干渉デバイスの CleanAir アラームとして連続トランスミッタを設定するには、**ap dot11** {**24ghz** | **5ghz**} **cleanair alarm device cont-tx** を使用します

ap dot11 { **24ghz** | **5ghz** } **cleanair alarm device cont-tx**

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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、2.4 GHz または 5 GHz 無線の干渉デバイスの CleanAir アラームとして連続トランスミッタを設定する例を示します。

```
Device(config)# ap dot11 24ghz cleanair alarm device cont-tx
```

ap dot11 cleanair alarm unclassified

2.4 GHz および 5 GHz 無線で未分類カテゴリの重大度を超えた場合の電波品質のアラームを設定するには、**ap dot11** {**24ghz** | **5ghz**} **cleanair alarm unclassified** を使用します

ap dot11 { **24ghz** | **5ghz** } **cleanair alarm unclassified**

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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、2.4 GHz および 5 GHz 無線で未分類カテゴリの重大度を超えた場合の電波品質のアラームを設定する例を示します。

```
Device(config)# ap dot11 24ghz cleanair alarm unclassified
```

ap dot11 cleanair alarm unclassified threshold

2.4 GHz および 5 GHz 無線で未分類カテゴリの重大度を超えた場合の電波品質のアラームを設定するには、**ap dot11** {**24ghz** | **5ghz**} **cleanair alarm unclassified threshold** を使用します

ap dot11 { **24ghz** | **5ghz** } **cleanair alarm unclassified threshold** *threshold-value*

構文の説明

threshold-value	未分類のしきい値を超えた場合の電波品質のアラームを指定します。値の範囲は 1 ～ 100 で、1 は低干渉、100 は高干渉です。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、2.4 GHz および 5 GHz 無線で未分類カテゴリの重大度を超えた場合の電波品質のアラームを設定する例を示します。

```
Device(config)# ap dot11 24ghz cleanair alarm unclassified threshold 20
```

ap dot11 cleanair device

CleanAir 干渉デバイスのタイプを設定するには、 **ap dot11 cleanair device** 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 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

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 Gibraltar 16.10.1	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deviceを設定する例を示します。

```
デバイス(config)# ap dot11 24ghz cleanair device report
```

ap dot11 dot11n

802.11n ネットワークを設定するには、 **ap dot11 dot11n** 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-mpdu tx priority	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-msdu tx priority	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。
mcs tx *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。
rifs rx	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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(config)# ap dot11 24ghz dot11n mcs tx 5
```

次に、RIFS を有効にする例を示します。

```
デバイス(config)# ap dot11 24ghz dot11n rifs rx
```

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、 **ap dot11 dtpc** 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、**ap dot11** {**24ghz**	**5ghz**} **shutdown** コマンドでネットワークを無効にしてから使用します。
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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

CCX バージョン 5 Expedited Bandwidth Request 機能が有効になっている場合、device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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(config)# ap dot11 5ghz fragmentation 1500
```

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、**ap dot11 edca-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** { **client-load-based** | **custom-voice** | **optimized-video-voice** | **optimized-voice** | **svp-voice** | **wmm-default** }
no ap dot11 { **24ghz** | **5ghz** } **edca-parameters** { **client-load-based** | **custom-voice** | **fastlane** | **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。
fastlane	24GHz の Fastlane パラメータを有効にします。
client-load-based	802.11 無線のクライアントの負荷ベースの EDCA 設定を有効にします。
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 Gibraltar 16.10.1	このコマンドが導入されました。
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。
Cisco IOS XE Bengaluru 17.5.1	**client-load-based** キーワードが追加されました。

次に、SpectraLink 音声優先パラメータを有効にする例を示します。

```
デバイス(config)# ap dot11 24ghz edca-parameters svp-voice
```

ap dot11 load-balancing denial

ロードバランシングの拒否カウントを設定するには、**ap dot11 load-balancingdenial** コマンドを使用します。ロードバランシングの拒否カウン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 dot11 {**24ghz** | **5ghz**} **load-balancingdenial** *count*

構文の説明

count	ロードバランシングの拒否カウント。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、ロードバランシングの拒否カウントを設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz load-balancing denial 10
```

ap dot11 load-balancing window

アグレッシブ ロード バランシング クライアント ウィンドウのクライアント数を設定するには、**ap dot11 load-balancingwindow** コマンドを使用します。クライアント数を無効にするには、このコマンドの **no** 形式を使用します。

ap dot11 {**24ghz** | **5ghz**} **load-balancingwindow** クライアント

構文の説明

clients	クライアント数。有効な範囲は 0 ～ 20 です。

コマンド デフォルト

なし

コマンド モード

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 Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、アグレッシブ ロード バランシング クライアント ウィンドウのクライアント数を設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz load-balancing window 10
```

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** | **6ghz** } **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。
6ghz	6 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。
	Cisco IOS XE Cupertino 17.7.1 で 6 GHz 帯域が導入されました。

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。

```
デバイス#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、 **ap dot11 rrm** コマンドを使用します。

ap dot11 {**24ghz** | **5ghz**} **rrm** {**ccx location-measurement** *sec* | **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。
data fail-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。
data 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設定します。
data 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。
exception global *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。
level global *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 Gibraltar 16.10.1	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、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。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(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 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、 **ap dot11 rrm channel** 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 Gibraltar 16.10.1	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、**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。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(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 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、 **ap dot11 rrm channel cleanair-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 Gibraltar 16.10.1	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。

```
デバイス(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity high
```

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、 **ap dot11 rrm channel dca** 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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 *6 : 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
High	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deviceを設定する例を示します。

```
デバイス(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。

```
デバイス(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。

```
デバイス(config)# ap dot11 24ghz rrm channel dca sensitivity low
```

ap dot11 rrm channel-update mesh

すべてのメッシュ Cisco AP の 802.11a、802.11b、および 802.11 6GHz チャネル選択の更新を開始するには、**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm channel-update mesh** を使用します

AP

ap dot11 { **24ghz** | **5ghz** | **6ghz** } **rrm channel-update mesh**

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 Cupertino 17.9.1	このコマンドが導入されました。

例

次に、すべてのメッシュ Cisco AP の 802.11a、802.11b、および 802.11 6GHz チャネル選択の更新を開始する例を示します。

```
Device# ap dot11 5ghz rrm channel-update mesh
```

ap dot11 rrm channel-update mesh bridge-group

ブリッジグループのメッシュ AP の 802.11、802.11a、または 802.11b チャネル選択の更新を開始するには、**ap dot11** {**24ghz** | **5ghz** | **6ghz**} **channel-update mesh bridge-group** を使用します

ap dot11 { **24ghz** | **5ghz** | **6ghz** } **rrm channel-update mesh channel-update mesh bridge-group** *bridge-group-name*

構文の説明

bridge-group-name	ブリッジグループ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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、ブリッジグループのメッシュ AP の 802.11、802.11a、または 802.11b チャネル選択の更新を開始する例を示します。

```
Device# ap dot11 5ghz rrm channel-update mesh bridge-group cisco-bridge-group
```

ap dot11 rrm channel dca chan-width

IEEE 802.11 無線のチャネル幅を設定するには、**ap dot11 rrm channel dca chan-width** コマンドを使用します。

ap dot11 {**24ghz** | **5ghz**} **rrm channel dca chan-width** {**160** | **20** | **40** | **80** | **80+80** | **best** | **width-max**}

構文の説明

160	160 MHz。
20	20 MHz。
40	40 MHz。
80	80 MHz。
80+80	80+80 MHz。
best	最適なチャネル幅。
width-max	動的帯域幅選択で許可される最大チャネル幅。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

例

次に、IEEE 802.11 無線のチャネル幅を設定する例を示します。

```
Device(config)# ap dot11 5ghz rrm channel dca chan-width 160
```

ap dot11 rrm coverage

802.11 カバレッジ ホール検出を有効にするには、 **ap dot11 rrm coverage** 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。
exceptional global *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。
level global *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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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device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。device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。device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。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(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、 **ap dot11 rrm group-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deviceの名前。
controller-ip	追加するdevice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 Gibraltar 16.10.1	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deviceを追加する例を示します。

```
デバイス(config)# ap dot11 5ghz rrm group-member cisco-controller 192.0.2.54
```

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、 **ap dot11 rrm group-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** | **6ghz** } **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。
6ghz	6 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device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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Cupertino 17.7.1	このコマンドは、6 GHz 帯域を含むように変更されました。

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。

```
デバイス(config)# ap dot11 5ghz rrm group-mode auto
```

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、**ap dot11 rrm logging** 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 Gibraltar 16.10.1	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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(config)# ap dot11 5ghz rrm logging txpower
```

ap dot11 rrm monitor

802.11 ネットワークのモニタを設定するには、 **ap dot11 rrm monitor** 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-list all	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-list country	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-list dca	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 Gibraltar 16.10.1	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。

```
デバイス(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。

```
デバイス(config)# ap dot11 24ghz rrm monitor coverage 60
```

ap dot11 rrm ndp-type

802.11 アクセス ポイントの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、 **ap dot11 rrm ndp-type** コマンドを使用します。

ap dot11 { **24ghz** | **5ghz** | **6ghz** } **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。
6ghz	6 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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Cupertino 17.7.1	6 GHz 帯域の導入により、このコマンドが変更されました。

使用上のガイドライン

802.11 アクセスポイント RRM のネイバー探索プロトコルタイプを設定する前に、**ap dot11 {24ghz | 5ghz | 6ghz} 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。

```
デバイス(config)# ap dot11 5ghz rrm ndp-type protected
```

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、**ap dot11 rrm tpc-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 Gibraltar 16.10.1	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、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。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(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、 **ap dot11 rrm txpower** 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 Gibraltar 16.10.1	このコマンドが導入されました。
	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。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#ap dot11 5ghz rrm txpower once
```

ap dot11 rrm txpower

802.11 TX 電力レベルを設定するには、 **ap dot11 rrm txpower** 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 Gibraltar 16.10.1	このコマンドが導入されました。
	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。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#ap dot11 5ghz rrm txpower once
```

ap dot15 shutdown

グローバル dot 15 無線パラメータを設定するには、**ap dot15 shutdown** コマンドを使用します。この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 dot15 shutdown

no ap dot15 shutdown

構文の説明

dot15	グローバルDot15無線パラメータを設定します。
shutdown	すべての AP の Dot15 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

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 Amsterdam 17.3.1	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

例

次に、グローバル dot 15 無線パラメータを設定する例を示します。

```
Device(config)# ap dot15 shutdown
```

ap file-transfer https port

HTTPS経由でAPイメージをダウンロードするためのカスタムポート番号を設定するには、**ap file-transfer https port** コマンドを使用します。カスタムポート番号を削除するには、このコマンドの **no** 形式を使用します。

ap file-transfer https port *port-number*

構文の説明

port-number	ファイル転送用のカスタムポート番号。 有効な値の範囲は 0 ～ 65535 で、デフォルトは 8443 です。

コマンド デフォルト

デフォルトポートは 8443 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 Dublin 17.11.1	このコマンドが導入されました。

使用上のガイドライン

ポート 443 は他の HTTPS リクエストに使用されるデフォルトポートであるため、AP ファイル転送には使用しないでください。また、設定が失敗する可能性があるため、標準ポートとウェルノウンポートの設定も避けてください。

例

次に、HTTPS 経由で AP イメージをダウンロードするためのカスタムポート番号を設定する例を示します。

```
Device# configure terminal
Device(config)# ap file-transfer https port 8443
```

ap filter

AP フィルタを設定して優先順位を設定するには、**ap filter** コマンドを使用します。

ap filter { { **name** *filter-name* } **type** { **priming** | | **tag** } | { **priority** *priority-number* | **filter-name** *filter-name* } }

構文の説明

パラメータ	説明
priority	名前付きフィルタの優先順位を設定します。
priority-number	有効な AP フィルタの優先順位の範囲は 0 ～ 1023 です。
filter-name	ap フィルタの名前を入力します。
type	フィルタのタイプ。
priming	AP をプライミングするためのフィルタ。このフィルタは、AP で常に永続的です。
tag	AP タグを割り当てるためのフィルタ。タグフィルタは、グローバル コンフィギュレーションでのタグの永続化に基づいて永続化できます。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。
Cisco IOS XE Dublin 17.10.1	このコマンドが変更されました。**priming** キーワードが導入されました。

例

次に、ap フィルタを作成し、このフィルタの優先順位を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name test-filter
Device(config)# ap filter name test-filter type priming
Device(config)# ap filter priority 12 filter-name test-filter
```

ap fra

フレキシブル ラジオ アサインメント（FRA）とそのパラメータを設定するには、**ap fra** コマンドを使用します。

ap fra[{**interval** *no-of-hours* | **sensitivity** {**high** | **low** | **medium** } | **sensor-threshold** {**balanced** | **client-preferred** | **client-priority** | **sensor-preferred** | **sensor-priority** } | **service-priority** {**coverage** | **service-assurance**}}]

構文の説明

interval *no-of-hours*	FRA 間隔の時間数を入力します。有効な範囲は 1 ～ 24 時間です。
sensitivity {**high**	**low**	**medium**}	FRA カバレッジ オーバーラップ感度を高、低、または中に設定します。
sensor-threshold {**balanced**	**client-preferred**	**client-priority**	**sensor-preferred**	**sensor-priority**}	FRA センサーのしきい値を利用可能なオプションのいずれかに設定します。
service-priority {**coverage**	**service-assurance**}	FRA サービスの優先順位をカバレッジまたはサービス保証に設定します。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

802.11b/g および 802.11a 帯域の RF グループ リーダーが RF ドメイン全体で同じであることを確認し、RF グループ リーダーが FRA を有効にしていることを確認します。

例

次に、FRA 間隔を 8 時間に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap fra interval 8
```

ap fra 5-6ghz

すべての Cisco AP でフレキシブル ラジオ アサインメント（FRA）5/6GHz 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 **ap fra 5-6ghz** コマンドを使用します。この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 fra 5-6ghz

no ap fra 5-6ghz

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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、すべての Cisco AP でフレキシブル ラジオ アサインメント（FRA）5/6GHz を有効にする例を示します。

```
Device(config)# ap fra 5-6ghz
Device(config)# no ap fra 5-6ghz
```

ap fra 5-6ghz freeze

すべての Cisco AP で 5 ～ 6 GHz フレキシブル ラジオ アサインメント（FRA）凍結を有効にするには、グローバル コンフィギュレーション モードで **ap fra 5-6ghz freeze** コマンドを使用します。この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 fra 5-6ghz freeze

no ap fra 5-6ghz freeze

構文の説明

このコマンドに引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、すべての Cisco AP で 5 ～ 6 GHz フレキシブル ラジオ アサインメント（FRA）凍結を有効にする例を示します。

```
Device# ap fra 5-6ghz freeze
Device# no ap fra 5-6ghz freeze
```

ap fra 5-6ghz interval

フレキシブル ラジオ アサインメント（FRA）の 5/6 GHz 間隔を時間単位で設定するには、**ap fra 5-6ghz interval** コマンドを使用します。

ap fra 5-6ghz interval *number-of-hours*

構文の説明

number-of-hours	FRA の 5/6 GHz 間隔を時間単位で指定します。値の範囲は 1 ～ 24 時間です。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、フレキシブル ラジオ アサインメント（FRA）の 5/6 GHz 間隔を時間単位で設定する例を示します。

```
Device(config)# ap fra 5-6ghz interval 12
```

ap geolocation derivation ranging

地理位置情報導出レンジングを設定するには、**ap geolocation derivation ranging** コマンドを使用します。地理位置情報導出レンジ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。

ap geolocation derivation ranging

no ap geolocation derivation ranging

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

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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、AP 地理位置情報導出レンジングを設定する例を示します。

```
Device# configure terminal
Device(config)# ap geolocation derivation ranging
```

ap geolocation ranging all accurate

すべての AP で正確なレンジングを有効にするには、**ap geolocation ranging all accurate** コマンドを使用します。

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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.12.1	このコマンドが導入されました。

使用上のガイドライン

クライアント接続が中断される可能性があります。

例

次に、すべての AP で正確なレンジングを有効にする例を示します。

```
Device# ap geolocation ranging all accurate
```

ap geolocation ranging site accurate

設定したサイトタグの下の AP での正確なレンジングを有効にするには、**ap geolocation ranging site** *site-tag-name* **accurate** コマンドを使用します。

構文の説明

site-tag-name	サイトタグ名を指定します。

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 Dublin 17.12.1	このコマンドが導入されました。

使用上のガイドライン

クライアント接続が中断される可能性があります。

例

次に、設定したサイトタグの下の AP での正確なレンジングを有効にする例を示します。

```
Device# ap geolocation ranging site site-tag-name accurate
```

ap hyperlocation

ハイパーロケーションおよび関連パラメータを設定するには、**ap hyperlocation** コマンドを使用します。ハイパーロケーションおよび関連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 hyperlocation ［**ble-beacon**{*beacon-id* | **interval** *interval-value*} | **threshold** {**detection** *value-in-dBm* | **reset** *value-btwn-0-99* | **trigger** *value-btwn-1-100*}］
[no] ap hyperlocation ［**ble-beacon**{*beacon-id* | **interval** *interval-value*}|**threshold** {**detection** *value-in-dBm* | **reset** *value-btwn-0-99* | **trigger** *value-btwn-1-100*}］

構文の説明

ble-beacon	BLE ビーコンのパラメータを有効にします。
beacon-id	BLE ビーコン ID。指定できる範囲は 1 ～ 4 です。
interval	BLE ビーコンの間隔を設定します。
interval-value	BLE ビーコンの間隔の値（ヘルツ単位）。値の範囲は 1 ～ 10 です。デフォルトは 1 です。
threshold detection *value-in-dBm*	低い RSSI を持つパケットを除外するためのしきい値を設定します。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。
threshold reset *value-btwn-0-99*	トリガー後のスキャン サイクルの値をリセットします。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。
threshold trigger *value-btwn-1-100*	BAR をクライアントに送信する前のスキャンサイクルの数を設定します。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。 （注） ハイパーロケーションしきい値のリセット値がしきい値のトリガー値より小さいことを確認してください。

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。
Cisco IOS XE Denali 16.3.1	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。

ap image

device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、**ap image** 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 Gibraltar 16.10.1	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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# ap image swap
```

ap image site-filter

サイト フィルタに基づいてソフトウェア メンテナンス アップデート（SMU）を使用してアクセス ポイント（AP）イメージをアップグレードするには、**ap image site-filter** コマンドを使用します。

ap image site-filter file *file-name* **any remove-all** { **add** *site-tag* | **apply** | **clear** | **remove** *site-tag* }

構文の説明

file-name	SMU イメージ名。
site-tag	サイト タグ名。
add	サイト フィルタにサイトを追加します。
apply	AP イメージを事前にダウンロードし、ローリング AP アップグレードを徐々に実行します。
clear	既存のサイト フィルタをクリアします。
remove	サイト フィルタからサイトを削除します。
any	
remove-all	

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 Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Cupertino 17.9.1	キーワード **any** および **remove-all** が追加されることで、このコマンドが変更されました。

例

次に、サイト フィルタに基づいて、SMU を使用して AP イメージをアップグレードする例を示します。

```
Device# ap image site-filter file vwlc_apsp_16.11.1.0_74.bin add bgl18
```

ap image upgrade

すべての AP がイメージ アップグレードを開始するように指示するには、**ap image upgrade** コマンドを使用します。

ap image upgrade [{**abort** | **destination** *controller-name* {*controller-ipv4-addr controller-ipv6-addr* } | **dry-run**}]

構文の説明

abort	AP イメージのアップグレードをキャンセルします。
destination *controller-name* {*controller-ipv4-addr* | *controller-ipv6-addr*}	名前と IP アドレスを入力する必要がある宛先コントローラに関連付けるようにすべての AP に指示します。
dry-run	ローリング AP イメージ アップグレードをドライラン モードで実行します。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP イメージのアップグレードをキャンセルする例を示します。

```
Device# ap image upgrade abort
```

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、 **ap link-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 Gibraltar 16.10.1	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。

```
デバイス(config)# ap link-encryption
```

ap name icap subscription ap rf spectrum

AP でのスペクトル解析を設定するには、**ap nameicap subscription ap rf spectrum** コマンドを使用します。スペクトル解析を無効にするには、このコマンドの **no** 形式を使用します。

ap name *ap_name* **icap subscription ap rf spectrum { enable** | *slot }*

構文の説明

enable	サブスクリプションを有効にします。
slot	RF スペクトル測定値を収集する無線スロットを設定します。
ap_name	AP 名

コマンド デフォルト

ディセーブル

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 Amsterdam 17.2.1	このコマンドが導入されました。

使用上のガイドライン

サブスクリプションを機能させるには、少なくとも 1 つの無線スロットを設定して、Cisco CleanAir を有効にし、動作状態をアップにする必要があります。

例

次に、AP でスペクトル解析を有効にする例を示します。

```
Device# ap name 4800AP icap subscription ap rf spectrum enable
Device# ap name 4800AP icap subscription ap rf spectrum slot 0
Device# show ap name 4800AP icap subscription ap rf spectrum chassis active
```

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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

デバイス**ap name <ap-name> antenna-band-mode single**

ap name ble

AP で ble ltx 状態を有効にするには、**ap name** *ap name* **ble** コマンドを使用します。

ap name *ap_name* **antena-band-mode {admin | ibeacon | interval | no-advertisement | sync | vibeacon}**

構文の説明

ap name	AP 名
admin	ble ltx 管理状態を有効にします。
ibeacon	BLE LTX iBeacon 設定を有効にします。
interval	BLE LTX スキャン設定間隔を有効にします。
no-advertisement	BLE LTX アドバタイズなしを有効にします。
Sync	BLE LTX 同期を有効にします。
vibeacon	BLE LTX viBeacon 設定を有効にします。

コマンド デフォルト

ディセーブル

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、AP で ble を有効にする例を示します。

```
Device# ap name test ble
```

ap name clear-personal-ssid

Cisco OfficeExtend アクセス ポイント（OEAP）からパーソナル SSID をクリアするには、**ap name clear-personal-ssid** コマンドを使用します。

ap name *ap-name* **clear-personal-ssid**

構文の説明

ap-name	AP 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、Cisco OEAP からパーソナル SSID をクリアする例を示します。

```
Device# ap name my-oeap clear-personal-ssid
```

ap name controller

AP でコントローラを設定するには、**ap name** *ap name* **controller** コマンドを使用します。

ap name *ap_name* **controller {primary | secondary | tertiary}** *name {A.B.C.D | X:X:X::XX}*

構文の説明

ap name	AP 名
controller	コントローラを設定します。
primary	プライマリコントローラを設定します。
secondary	セカンダリコントローラを設定します。
tertiary	ターシャリコントローラを設定します。
name	プライマリコントローラ、セカンダリコントローラ、またはターシャリコントローラの名前を指定します。
A.B.C.D	プライマリコントローラ、セカンダリコントローラ、またはターシャリコントローラの IPv4 アドレスを指定します。
X:X:X::XX	プライマリコントローラ、セカンダリコントローラ、またはターシャリコントローラの IPv6 アドレスを指定します。

コマンド デフォルト

ディセーブル

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、AP でコントローラを設定する例を示します。

```
Device# ap name cisco-ap controller primary cisco-primary-controller 10.1.1.1
```

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、 **ap name core-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）サーバーの 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# ap name AP2 core-dump 192.1.1.1 log compress
```

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、 **ap name country** 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

Cisco device は、ネットワーク管理者または資格のある IT 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。

```
デバイス# ap name AP2 country JP
```

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、**ap name crash-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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# 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。

```
デバイス# ap name AP02 crash-file get-radio-core-dump slot 0
```

ap name dot11 24ghz | 5ghz | 6ghz rrm channel update mesh

特定の AP の RRM DCA をトリガーするには、**ap name** *cisco-ap-name* **dot11** {**24ghz** | **5ghz** | **6ghz**} **rrm channel update mesh** を使用します

ap name *cisco-ap-name* **dot11** { **24ghz** | **5ghz** | **6ghz** } **rrm channel update mesh**

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 Cupertino 17.9.1	このコマンドが導入されました。

例

次に、特定の AP の RRM DCA をトリガーする例を示します。

```
Device# ap name Cisco-ap-name dot11 5ghz rrm channel update mesh
```

ap name dot11 24ghz slot 0 SI

特定のアクセス ポイントのスロット 0 でホストされている専用の 2.4-GHz 無線のスペクトル インテリジェンス（SI）を有効にするには、**ap name dot11 24ghz slot 0 SI** コマンドを使用します。

ap name *ap-name***dot11** {**24ghz** | **5ghz** | **dual-band** | **rx-dual-band**} **slot***slot ID***SI**

構文の説明

ap_name	Cisco アクセス ポイントの名前。
slot 0	特定のアクセス ポイントのスロット 0 でホストされている専用の 2.4 GHz 無線のスペクトル インテリジェンス（SI）を有効にします。 ここで、0 はスロット ID を示しています。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP のスペクトル インテリジェンスを設定する例を示します。

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 SI
```

ap name dot11 24ghz slot antenna

スロット 0 でホストされる 802.11b アンテナを設定するには、**ap name dot11 24ghz slot antenna** コマンドを使用します。

ap name *ap-name***dot1124ghzslot 0antenna**{**ext-ant-gain** *antenna-gain-value* | **selection**［**internal** | **external**}

構文の説明

ap-name	AP の名前。
24ghz	802.11b パラメータを設定します。
slot	Cisco アクセス ポイントのスロット ID を設定します。
antenna	802.11b アンテナを設定します。
ext-ant-gain	802.11b 外部アンテナ ゲインを設定します。値の範囲は 0 ～ 4294967295 です。 外部アンテナのゲイン値を .5 dBi 単位で入力します（整数値 4 は 4 x 0.5 = 2 dBi のゲインになります）。
selection	802.11b アンテナ選択の設定（内部/外部）

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

例

次に、AP のチャネル幅を設定する例を示します。

```
Device# ap name ax1 dot11 24ghz slot 0 antenna selection external
```

ap name dot11 24ghz slot beamforming

特定のアクセス ポイントのスロット 0 でホストされている 2.4 GHz 無線のビームフォーミングを設定するには、 **ap name dot11 24ghz slot beamforming** コマンドを使用します。

ap name *ap-name***dot1124ghzslot 0beamforming**

構文の説明

beamforming	802.11b tx ビームフォーミング（5 GHz）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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

例

次に、AP のビームフォーミングを設定する例を示します。

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 beamforming
```

ap name dot11 24ghz slot channel

Cisco AP の高度な 802.11 チャネル割り当てパラメータを設定するには、**ap name dot11 24ghz slot channel** コマンドを使用します。

ap name *ap-name* **dot11 24ghz slot 0 channel** { *channel_number* | **auto** }

構文の説明

channel_number	Cisco AP の高度な 802.11 チャネル割り当てパラメータ。1 ～ 14 のチャネル番号を入力します。
auto	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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

例

次に、AP のチャネルを設定する例を示します。

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 channel auto
```

ap name dot11 24ghz slot cleanair

特定のアクセス ポイントのスロット 0 でホストされている 802.11b 無線の CleanAir を有効にするには、**ap name dot11 24ghz slot cleanair** コマンドを使用します。

ap name *ap-name* **dot11 24ghz slot 0 cleanair**

構文の説明

cleanair	802.11b CleanAir 管理を有効にします

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。
Cisco IOS XE Cupertino 17.9.1	このコマンドはすでに廃止されています。

例

次に、AP の CleanAir を設定する例を示します。

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 cleanair
```

ap name dot11 24ghz slot dot11n antenna

特定のアクセス ポイントのスロット 0 でホストされている 2.4 GHz 無線の 802.11n アンテナを設定するには、**ap name dot11 24ghz slot dot11n antenna** コマンドを使用します。

ap name *ap-name* **dot11 24ghz slot 0 dot11n antenna** { **A** | **B** | **C** | **D** }

構文の説明

dot11n	特定のアクセス ポイントのスロット 0 でホストされている 2.4 GHz 無線の 802.11n アンテナを設定します。
antenna	アンテナポート A、B、C、および D の 802.11n - 2.4 GHz アンテナ選択を設定します。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP のチャネル幅を設定する例を示します。

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11n antenna A
```

ap name dot11 24ghz slot dot11ax bss-color

特定のアクセスポイントの 2.4 GHz、5 GHz、またはデュアルバンド無線の BSS カラーを設定するには、**ap name dot11 24ghz slot dot11ax bss-color** コマンドを使用します。

ap name *ap-name* **dot11 24ghz slot 0 dot11ax bss-color** *<1-63>*

構文の説明

bss-color	802.11ax-2.4GHz BSS カラーを設定します

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 16.12.1	このコマンドが導入されました。

例

次に、Cisco AP で 802.11b 無線を無効にする例を示します。

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11ax bss-color 3
```

ap name dot11 24ghz slot shutdown

特定のアクセス ポイントのスロット 0 でホストされている 802.11b 無線を無効にするには、**ap name dot11 24ghz slot shutdown** コマンドを使用します。

ap name *ap-name* **dot11 24ghz slot 0 shutdown**

構文の説明

shutdown	Cisco AP で 802.11b 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、Cisco AP で 802.11b 無線を無効にする例を示します。

```
Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 shutdown
```

ap name dot11 24ghz radio role manual sniffer channel

コントローラから AP での XOR 無線のスニファロールのサポートを有効にするには、**ap name dot11 24ghz radio role manual sniffer channel** コマンドを使用します。

ap name dot11 24ghz radio role manual sniffer channel *channel-number* **ip** *ip-address*

構文の説明

channel-number ip *ip-address*	チャネル番号と 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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.8.1	このコマンドが導入されました。

使用上のガイドライン

次に、コントローラから AP での XOR 無線のスニファロールのサポートを有効にする例を示します。

```
Device# enable
Device# ap name AP687D.B45C.189C dot11 24ghz shutdown
Device# ap name AP687D.B45C.189C dot11 24ghz radio role manual sniffer channel 100 ip
9.4.197.85
Device# ap name AP687D.B45C.189C no dot11 24ghz shutdown
Device# end
```

ap name dot11 5ghz radio role manual sniffer channel

コントローラから AP での XOR 無線のスニファロールのサポートを有効にするには、**ap name dot11 5ghz radio role manual sniffer channel** コマンドを使用します。

ap name dot11 5ghz radio role manual sniffer channel *channel-number* **ip** *ip-address*

構文の説明

channel-number ip *ip-address*	チャネル番号と 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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.8.1	このコマンドが導入されました。

使用上のガイドライン

次に、コントローラから AP での XOR 無線のスニファロールのサポートを有効にする例を示します。

```
Device# enable
Device# ap name AP687D.B45C.189C dot11 5ghz shutdown
Device# ap name AP687D.B45C.189C dot11 5ghz radio role manual sniffer channel 100 ip
9.4.197.85
Device# ap name AP687D.B45C.189C no dot11 5ghz shutdown
Device# end
```

ap name dot11 5ghz slot 1 dual-radio mode

AP で 802.11a デュアル無線を設定するには、**ap name** *ap-name* **dot11 5ghz slot 1 dual-radio mode** を使用します

ap name *ap-name* **dot11 5ghz slot 1 dual-radio mode** {**enable** | **disable**}

構文の説明

dual-radio mode	AP で 802.11a デュアル無線を設定します。

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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、AP で 802.11a デュアル無線を設定する例を示します。

```
Device#ap name ap-name dot11 5ghz slot 1 dual-radio mode enable
```

ap name dot11 5ghz slot radio role

手動の無線のロールをクライアントサービスまたはモニターに設定するには、**ap name** *ap-name* **dot11 5ghz slot** {**1** | **2**} **radio role** コマンドを使用します。

ap name *ap-name* **dot11 5ghz slot** { **1** | **2** } **radio role** { **auto** | **manual** { **client-serving** | **monitor** } }

構文の説明

radio role	802.11a 無線のロール（手動または自動）を設定します。
manual	クライアントサービスの手動ロールまたはモニターの手動ロールを設定します。

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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、手動の無線ロールをクライアントサービスまたはモニターに設定する例を示します。

```
Device# ap name ap-name dot11 5ghz slot 2 radio role manual monitor
```

ap name dot11 channel width

AP のチャネル幅を設定するには、**ap name dot11 channel width** コマンドを使用します。

ap name *ap-name* **dot11** { **24ghz** | **5ghz** | **dual-band** | **rx-dual-band** } **channel width** { **160** | **20** | **40** | **80** | **80+80** }

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
160	160 MHz。
20	20 MHz。
40	40 MHz。
80	80 MHz。
80+80	80+80 MHz。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP のチャネル幅を設定する例を示します。

```
Device# ap name ax1 dot11 5ghz channel width 80+80
```

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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Cupertino 17.9.1	このコマンドは廃止されました。

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。

```
デバイス# ap name AP01 dot11 dual-band cleanair
```

ap name dot11 dual-band shutdown

Cisco 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 Gibraltar 16.12.1	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。

```
デバイス# ap name AP01 dot11 dual-band shutdown
```

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、 **ap name dot11 rrm profile** 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# ap name AP1 dot11 5ghz rrm profile utilization 100
```

ap name export support-bundle mode

APサポートバンドルをAPからコントローラにエクスポートするには、**ap name** *Cisco-AP-name* **export support-bundle mode** を使用します

ap name *Cisco-AP-name* **export support-bundle mode** { **scp** | **tftp**} **target ip-address** { *A.B.C.D* | *X:X:X:X::X*} **path** *file-path*

構文の説明

scp	SCP モードでサポートバンドルを転送します。
tftp	TFTP モードでサポートバンドルを転送します。
target	TFTP を使用したファイル転送のターゲットの詳細を示します。
ip-address	SCP または TFTP を使用したファイル転送のターゲット IP アドレス（IPv4 または IPv6）を示します。
A.B.C.D	ターゲット IPv4 アドレスを示します。
X:X:X:X::X	ターゲット IPv6 アドレスを示します。
path	ターゲットファイルパスを示します。
file-path	ファイルパスを示します。

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 Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、AP サポートバンドルを AP からコントローラにエクスポートする例を示します。

```
Device> ap name Cisco-AP-name export support-bundle mode scp target ip-address 10.1.1.1
 path file-path
```

ap name floor

AP のフロア ID を設定するには、**ap name** *cisco-ap-name* **floor** *floor-id* コマンドを使用します。

ap name *cisco-ap-name* **floor** *floor-id*

構文の説明

cisco-ap-name	Cisc を指定します
floor-id	AP のフロア ID を指定します。フロア ID の値は、-2147483648 ～ 2147483647 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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、AP のフロア ID を設定する例を示します。

```
Device# ap name cisco-ap-name floor 20
```

ap name hyperlocation

アクセス ポイント（AP）のハイパーロケーションおよび関連パラメータを設定するには、**ap name hyperlocation** コマンドを使用します。ハイパーロケーションおよび関連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 name *ap-name* **hyperlocation ble-beacon** *beacon-id* {**major** *major-value* | **minor** *minor-value* | **txpwr** *att-value* }

構文の説明

ap-name	アクセス ポイント名。
ble-beacon	BLE ビーコンのパラメータを設定します。
beacon-id	BLE ビーコン ID。
major	BLE ビーコンの major パラメータを設定します。
major-value	BLE ビーコンの major 値。範囲は 0 ～ 65535 です。デフォルトは 0 です。
minor	BLE ビーコンの minor パラメータを設定します。
minor-value	BLE ビーコンの minor 値。範囲は 0 ～ 65535 です。デフォルトは 0 です。
txpwr	BLE ビーコン減衰レベルを設定します。
att-value	BLE ビーコン減衰値（dBm 単位）。範囲は 0 ～ 52 です。デフォルトは 0 です。

コマンド デフォルト

BLE ビーコンの詳細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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、AP のハイパーロケーションおよび関連パラメータを設定する例を示します。

```
Device# ap name test-ap hyperlocation ble-beacon 3 txpwr 50
```

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、**ap name image** 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# 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。

```
デバイス# ap name AP2 image swap
```

ap name icap subscription client anomaly-detection report-individual enable aggregate

クライアント サブスクリプションの異常検出を設定し、個々のレポート集約を有効にするには、**ap name icap subscription client anomaly-detection report-individual enable aggregate** コマンドを使用します。

ap name *ap name* **icap subscription client anomaly-detection report-individual enable aggregate**

構文の説明

ap name	Cisco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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.12.1	このコマンドが導入されました。

例

次に、クライアント サブスクリプションの異常検出を設定し、個々のレポート集約を有効にする例を示します。

```
Device# ap name cisco-AP icap subscription client anomaly-detection report-individual
enable aggregate
```

ap name icap subscription client anomaly-detection report-individual per-client throttle

AP で 5 分ごとにクライアント別の個別レポートを設定するには、**ap name icap subscription client anomaly-detection report-individual per-client throttle** コマンドを使用します。

ap name *ap name* **icap subscription client anomaly-detection report-individual per-client throttle** *throttle-value*

構文の説明

ap name	Cisco アクセス ポイントの名前。
throttle-value	クライアントごとのイベントレポートの数。有効な値の範囲は 0 ～ 50 です。値が 0 の場合、スロットルはありません。

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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、AP で 5 分ごとにクライアント別の個別レポートを設定する例を示します。

```
Device# ap name cisco-AP icap subscription client anomaly-detection report-individual
per-client throttle 10
```

ap name icap subscription client anomaly-detection report-individual per-type throttle

AP でタイプ別の個別レポートを設定するには、**ap name icap subscription client anomaly-detection report-individual per-type throttle** コマンドを使用します。

ap name *ap name* **icap subscription client anomaly-detection report-individual per-type throttle** *throttle*

構文の説明

ap name	Cisco アクセス ポイントの名前。
throttle-value	クライアントごとのイベントレポートの数。有効な値の範囲は 0 ～ 100 です。値が 0 の場合、スロットルはありません。

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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、AP でタイプ別の個別レポートを設定する例を示します。

```
Device# ap name cisco-AP icap subscription client anomaly-detection report-individual
per-type throttle 50
```

ap name indoor

屋内モードでアクセスポイントを有効にするには、**ap name** *ap name* **indoor** コマンドを使用します。

ap name *ap_name* **indoor**

構文の説明

ap name	AP 名
indoor	屋内モードでアクセスポイントを有効にします。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、屋内モードでアクセスポイントを有効にする例を示します。

```
Device# ap name test indoor
```

ap name ipsla

AP で ipsla を設定するには、**ap name** *ap name* **ipsla** コマンドを使用します。

ap name *ap_name* **ipsla**

構文の説明

ap name	AP 名
ipsla	アクセスポイントで ipsla 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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、アクセスポイントで ipsla を設定する例を示します。

```
Device# ap name test ipsla
```

ap name keepalive

AP でキープアライブオプションを有効にするには、**ap name** *ap name* **keepalive** コマンドを使用します。

ap name *ap_name* **keepalive**

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 Gibraltar 17.03.1	このコマンドが導入されました。

例

次に、AP でキープアライブオプションを有効にする例を示します。

```
Device# ap name test keepalive
```

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 Gibraltar 16.10.1	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。

```
デバイス# 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、 **ap name led** 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# 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。

```
デバイス# ap name AP2 no led
```

ap name led-brightness-level

AP で LED の明るさレベルを設定するには、**ap name** *ap name* **led-brightness-level** コマンドを使用します。

ap name *ap_name* **led-brightness-level {1–8}**

構文の説明

ap name	AP 名
led brightness level	LED の明るさレベルを設定します。 （注） 有効な LED の明るさレベルは 1 ～ 8 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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、アクセスポイントでの LED の明るさレベルの例を示します。

```
Device# ap name cisco-ap led-brightness-level2
```

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、 **ap name location** 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。
location	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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス# ap name AP1 location Building1
```

ap name mesh backhaul rate dot11abg

メッシュバックホール dot11abg レートを設定するには、**ap name** *ap-name* **mesh backhaul rate dot11abg** コマンドを使用します。

ap name *ap-name* **mesh backhaul rate dot11abg** { **RATE_11M** | **RATE_12M** | **RATE_18M** | **RATE_1M** | **RATE_24M** | **RATE_2M** | **RATE_36M** | **RATE_48M** | **RATE_54M** | **RATE_5DOT5M** | **RATE_6M** | **RATE_9M** }

構文の説明		
	RATE_11M | **RATE_12M** | **RATE_18M** | **RATE_1M** | **RATE_24M** | **RATE_2M** | **RATE_36M** | **RATE_48M** | **RATE_54M** | **RATE_5DOT5M** | **RATE_6M** | **RATE_9M**	メッシュバックホールレートを設定します。

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 Bengaluru 17.6.1	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

例

次に、AP メッシュバックホール dot11abg レートを設定する例を示します。

```
Device# ap name cisco-ap mesh backhaul rate dot11abg RATE_11M
```

ap name mdsn-ap

AP で mdsn-ap を設定するには、**ap name** *ap name* **mdsn-ap** コマンドを使用します。

ap name *ap_name* **mdsn-ap {disable | enable | vlan}** *add delete*

構文の説明

ap name	AP 名
disable	mDNS アクセスポイントを無効にします。
enable	mDNS アクセスポイントを有効にします。
vlan	mDNSアクセスポイントのVLANを追加または削除します。
add	mDNS AP に vlan を追加します。
add	mDNS AP から vlan を削除します。

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、AP で mdns を有効にする例を示します。

```
Device# Device# ap name test mdns enable
```

ap name mesh backhaul rate dot11ac

メッシュバックホール dot11ac レートを設定するには、**ap name** *ap-name* **mesh backhaul rate dot11ac** コマンドを使用します。

ap name *ap-name* **mesh backhaul rate dot11ac mcs** *0-9* **ss** *1-4*

構文の説明

mcs *0-9*	メッシュバックホール 11ac の MCS レートを設定します。
0-9	メッシュバックホールレート 11ac の mcs インデックスを示します。
ss	メッシュバックホール 11ac の空間ストリームを設定します。
1-4	メッシュバックホール 11ac の空間ストリーム値を示します。

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 Bengaluru 17.6.1	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

例

次に、AP メッシュバックホール dot11ac レートを設定する例を示します。

```
Device# ap name cisco-ap mesh backhaul rate dot11ac mcs 5 ss 3
```

ap name name mesh backhaul rate dot11ax

メッシュバックホール dot11ax レートを設定するには、**ap name** *ap-name* **mesh backhaul rate dot11ax** コマンドを使用します。

ap name *ap-name* **mesh backhaul rate dot11ax mcs** *0-11* **ss** *1-8*

構文の説明

mcs	メッシュバックホール 11ax の MCS レートを設定します。
0-11	メッシュバックホール 11ax の MCS インデックスを示します。
ss	メッシュバックホール 11ax の空間ストリームを設定します。
1-8	メッシュバックホール 11ax の空間ストリーム値を示します。1 ～ 4 の範囲は 2.4 GHz の範囲を示し、1 ～ 8 の範囲は 5 GHz バックホールの範囲を示します。

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 Bengaluru 17.6.1	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

例

次に、AP メッシュバックホール dot11ax レートを設定する例を示します。

```
Device# ap name cisco-ap mesh backhaul rate dot11ax mcs 6 ss 5
```

ap name name new-ap-name

新しい Cisco AP 名を設定するには、**ap name** *ap name* **name** *new-ap-name* コマンドを使用します。

ap name *ap_name* **name** *new-ap-name*

構文の説明

ap name	AP 名
name	新しい Cisco AP 名を指定します。

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、新しい Cisco AP を設定する例を示します。

```
Device# ap name test name test2
```

ap name no

AP でコマンドを無効にするか、デフォルトに設定するには、**no** コマンドを使用します。

ap name *ap_name* **no**

構文の説明

ap name	AP 名
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。

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、AP でコマンドを無効にするか、デフォルトに設定する例を示します。

```
Device# ap name test no
```

ap name mesh backhaul rate

AP メッシュバックホールレートを設定するには、**ap name** *ap-name* **mesh backhaul rate** コマンドを使用します。

ap name *ap-name* **mesh backhaul rate** { **auto** | **dot11abg** | **dot11ac** | **dot11ax** | **dot11n** }

構文の説明

auto	メッシュバックホールレートを auto に設定します。
dot11abg	メッシュバックホール dot11abg レートを設定します。
dot11ac	メッシュバックホール dot11ac レートを設定します。
dot11ax	メッシュバックホール dot11ax レートを設定します。
dot11n	メッシュバックホール dot11n レートを設定します。

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 Bengaluru 17.6.1	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

例

次に、AP メッシュバックホールレートを auto に設定する例を示します。

```
Device# ap name cisco-ap mesh backhaul rate auto
```

ap name mesh backhaul rate dot11n

メッシュバックホール dot11n レートを設定するには、**ap name** *ap-name* **mesh backhaul rate dot11n** コマンドを使用します。

ap name *ap-name* **mesh backhaul rate dot11n mcs** *0-31*

構文の説明

mcs *0-31*	メッシュバックホール 11n の MCS レートを設定します。
0-31	メッシュバックホールレート dot11n の mcs インデックスを示します。

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 Bengaluru 17.6.1	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

例

次に、AP メッシュバックホール dot11n レートを設定する例を示します。

```
Device# ap name cisco-ap mesh backhaul rate dot11n mcs 20
```

ap name mesh block-child

メッシュ AP のメッシュ ブロック子の状態を設定するには、 **ap name mesh block-child** コマンドを使用します。

ap name *ap-name* **mesh block-child**

構文の説明

ap-name	メッシュ 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ AP のメッシュ ブロック子の状態を設定する例を示します。

```
Device# ap name mymeshap mesh block-child
```

ap name mesh daisy-chaining

メッシュ AP のデイジーチェーン モードを設定するには、**ap name** *ap-name* **mesh daisy-chaining** コマンドを使用します。

ap name *ap-name***mesh daisy-chaining** [{**strict-rap**}]

構文の説明

ap-name	メッシュ AP の名前。
strict-rap	イーサネットインターフェイスのみをメッシュアップリンクとして許可するように設定します。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ AP のデイジーチェーン モードを設定する例を示します。

```
Device# ap name mymeshap mesh daisy-chaining
```

ap name mesh ethernet mode access

メッシュ AP のアクセスとしてイーサネット インターフェイスのモードを設定するには、**ap name** *ap-name* **mesh ethernet** *port-no* **mode access** コマンドを使用します。

ap name *ap-name* **mesh ethernet** *port-no* **mode access** *vlan-id*

構文の説明

ap-name	メッシュ AP の名前。
port-no	AP のポート番号。有効なオプションは1、2、3、および4です。
vlan-id	VLAN ID。有効な範囲は 0 ～ 4095 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、イーサネット インターフェイスのモードをメッシュ AP のアクセスとして設定する例を示します。

```
Device# ap name mymeshap mesh ethernet 0 mode access 10
```

ap name mesh ethernet mode trunk

メッシュ AP のトランクとしてイーサネット インターフェイスのモードを設定するには、**ap name** *ap-name* **mesh ethernet** *port-no* **mode trunk** コマンドを使用します。

ap name *ap-name* **mesh ethernet** *port-no* **mode trunk vlan** {**allowed** | **native**}*vlan-id*

構文の説明

ap-name	メッシュ AP の名前。
port-no	AP のポート番号。有効なオプションは 1、2、3、および 4 です。
allowed	トランク ポートの許可 VLAN を設定します。
native	トランク ポートのネイティブ VLAN を設定します。
vlan-id	VLAN ID。許可 VLAN の有効範囲は 0 ～ 4095 です。ネイティブ VLAN の有効範囲は 1 ～ 4095 です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、イーサネット インターフェイスのモードをメッシュ AP のトランクとして設定し、トランク ポートの許可 VLAN も設定する例を示します。

```
Device# ap name mymeshap mesh ethernet 0 mode trunk vlan allowed 10
```

ap name mesh linktest

メッシュ AP を使用してリンク テストを実行するには、**ap name** *ap-name***mesh linktest** コマンドを使用します。

ap name *ap-name* **mesh linktest** *dest-ap-mac data-rate pkts-per-sec pkt-size test-duration*

構文の説明

ap-name	メッシュ AP の名前。
dest-ap-mac	宛先メッシュ AP の MAC アドレス。
data-rate	データ レート（Mbps）（1、2、5.5、6、9、11、12、24、36、48、53、m0-m15）
pkts-per-sec	1 秒あたりに送信されるパケット数。有効な範囲は 1 ～ 25000 です。
pkt-size	パケット サイズ。有効な範囲は 1 ～ 1500 です。
test-duration	テストの期間。有効な範囲は 10 ～ 300 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ AP のリンク テストを設定する例を示します。

```
Device# ap name mymeshap mesh linktest 00c0.00a0.03fa.0000.0000.0000
 9 100 10 180
```

ap name mesh parent preferred

メッシュ AP で優先される親を設定するには、**ap name mesh parent preferred** コマンドを使用します。

ap name *ap-name* **mesh parent preferred** *mac-address*

構文の説明

ap-name	メッシュ AP の名前。
mac-address	親 AP の無線 MAC アドレス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ AP で優先される親の例を示します。

```
Device # ap name mymeshap mesh parent preferred dc:5f:be:f5:fd:84
```

ap name mesh security psk provisioning delete

メッシュ AP から PSK プロビジョニングキーを削除するには、**ap name mesh security psk provisioning delete** コマンドを使用します。

ap name *ap-name* **mesh security psk provisioning delete**

構文の説明

ap-name	メッシュ 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ AP から PSK プロビジョニング キーを削除する例を示します。

```
Device# ap name mymeshap mesh security psk provisioning delete
```

ap name mesh vlan-trunking native

メッシュ AP のネイティブ VLAN を設定するには、**ap name mesh vlan-trunking native** コマンドを使用します。

ap name *name-of-rap* **vlan-trunking native** *vlan-id*

構文の説明

name-of-rap	ルートアクセスポイントの名前。
vlan-id	VLAN 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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、メッシュ AP のネイティブ VLAN を設定する例を示します。

```
Device # ap name mesh vlan-trunking native 12
```

ap name mode

個別の Cisco Lightweight アクセス ポイントの Cisco device 通信オプションを変更するには、 **ap name mode** 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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deviceを設定する例を示します。

```
デバイス# 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deviceを設定する例を示します。

```
デバイス# 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deviceを設定する例を示します。

```
デバイス# ap name AP02 mode sniffer
```

ap name mode bridge

AP のブリッジ モードを設定するには、**ap name** *ap-name* **mode bridge** コマンドを使用します。

ap name *ap-name* **mode bridge**

構文の説明

ap-name	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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP のブリッジ モードを設定する例を示します。

```
Device# ap name my-ap mode bridge
```

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、**ap name monitor-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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# ap name AP01 monitor-mode wips
```

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、 **ap name monitor-mode dot11b** 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# ap name AP01 monitor-mode dot11b fast-channel 1 6 11
```

ap name management-mode meraki

AP 管理モードを Meraki に変更するには、**ap name management-mode meraki** コマンドを使用します。

ap name management-mode meraki

構文の説明

force	コントローラでの検証をスキップし、AP で Meraki 管理モードの変更を試みます。
noprompt	AP管理モードの変更を試みるためのユーザープロンプトをスキップします。
cisco-ap-name	管理モードを変更する Cisco AP 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが変更されました。

例

次に、AP 管理モードを Meraki に変更する例を示します。

```
Device# ap name Cisco-AP-name management-mode meraki
Device# ap name Cisco-AP-name management-mode meraki force
Device# ap name Cisco-AP-name management-mode meraki noprompt
Device# ap name Cisco-AP-name management-mode meraki force noprompt
```

ap name name

Cisco Lightweight アクセスポイントの名前を変更するには、 **ap name name** 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# ap name AP1 name AP2
```

ap name network-diagnostics

OfficeExtend AP でネットワーク診断をトリガーするには、**ap name network-diagnostics** コマンドを使用します。

ap name *ap-name* **network-diagnostics**

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

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 Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、OfficeExtend AP でネットワーク診断をトリガーする例を示します。

```
Device# ap name ap18 network-diagnostic
```

ap name priority

アクセス ポイントの優先順位を設定するには、**ap name priority** コマンドを使用します。

ap name *ap-name* **priority** *priority-value*

構文の説明

priority-value	AP の優先順位値。有効な範囲は 1 ～ 4 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、アクセス ポイントの優先順位を設定する例を示します。

```
Device# ap name my-ap priority 1
```

ap name remote

AP remote コマンドを開始するには、**ap name** *ap-name* **remote** コマンドを使用します。

ap name *ap-name* **remote** { **command** *command-name* | **disable** | **enable** }

構文の説明

remote command *command-name*	AP remote コマンドを開始します。
disable	AP remote disable コマンドを開始します。
enable	AP remote enable コマンドを開始します。

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 Amsterdam 17.3.1	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

例

次に、AP remote コマンドを開始する例を示します。

```
Device# terminal monitor
Device# ap name ap-name remote enable
Device# ap name ap-name remote command 'show client sum'
.
.
.
Device# ap name ap-name remote disable
```

（注） 出力をリアルタイムで表示するには、**terminal monitor** コマンドを使用します。出力をコントローラログで表示するには、**show logging** コマンドを使用します。

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、 **ap name reset** 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# ap name AP2 reset
```

ap name reset-button

アクセスポイントの Reset ボタンを設定するには、 **ap name reset-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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# ap name AP03 reset-button
```

ap name role

AP の動作のロールを設定するには、**ap name role** コマンドを使用します。

ap name *ap-name* **role** {**mesh-ap** | **root-ap**}

構文の説明

ap-name	AP の名前。
mesh-ap	AP のメッシュ AP ロールを設定します。
root-ap	AP のルート AP ロールを設定します。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP のメッシュ AP として動作のロールを設定する例を示しています。

```
Device# ap name mymeshap role mesh-ap
```

ap name sensor environment

AP のセンサー管理状態を無効にするには、**ap name** *cisco-ap-name* **sensor environment** コマンドを使用します。AP のセンサー管理状態を有効にするには、このコマンドの **no** 形式を使用します。

ap name *cisco-ap-name* **sensor environment** { **air-quality** | **temperature** } **shutdown**

ap name *cisco-ap-name* **no sensor environment** { **air-quality** | **temperature** } **shutdown**

構文の説明

air-quality	電波品質センサーを指定します。
temperature	温湿度センサーを指定します。
shutdown	指定したセンサーをシャットダウンします。

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 Cupertino 17.8.1	このコマンドが導入されました。

例

次に、AP のセンサー管理状態を無効にする例を示します。

```
Device# enable
Device# ap name cisco-ap-name sensor environment temperature shutdown
```

ap name slot

さまざまなスロットパラメータを設定するには、 **ap name slot** 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# 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。

```
デバイス# 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、 **ap name static-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device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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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device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。

```
デバイス# ap name AP2 static-ip ip-address 192.0.2.54 netmask 255.255.255.0 gateway
192.0.2.1
```

ap name shutdown

Cisco Lightweight アクセス ポイントを無効にするには、 **ap name shutdown** 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# ap name AP2 shutdown
```

ap name sniff

アクセス ポイントでスニフィングを有効または無効にするには、 **ap name 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** { **dot116Ghz** | **dot11a** | **dot11b** }
ap name *ap-name* **no sniff** { **dot11a** | **dot11b** | **dot116Ghz** }

構文の説明

ap-name	Cisco Lightweight アクセス ポイントの名前。
dot116Ghz	6 GHz 帯域を指定します。
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。 dot11 6Ghz の場合、範囲は 1 ～ 233 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Cupertino 17.7.1	このコマンドが変更され、6 GHz が追加されました。

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。

```
デバイス# ap name AP2 sniff dot11a 36 192.0.2.54
```

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、 **ap name tftp-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 サーバーの IP アドレスです。
filename	TFTP サーバー上のアクセス 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# ap name Ap01 tftp-downgrade 172.21.12.45 ap3g1-k9w7-tar.124-25d.JA.tar
```

ap name usb-module

アクセスポイント（AP）の USB ポートを有効にするには、**ap name** *ap-name* **usb-module** を使用します。この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* **usb-module**

no ap name *ap-name* **usb-module**

構文の説明

usb-module	AP の USB ポ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

特権 EXEC モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.4.1	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

例

次に、AP の USB ポートを有効にする例を示します。

```
Device# ap name ap-name usb-module
```

ap name vlan-tag

ブリッジ以外の AP の VLAN タグを設定するには、**ap name vlan-tag** コマンドを使用します。

ap name *ap-name* **vlan-tag** *vlan-id*

構文の説明

ap-name	アクセス ポイント名。
vlan-id	VLAN 識別番号。

コマンド デフォルト

VLAN タギングは有効化されていません。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ブリッジ以外の AP の VLAN タギングを設定する例を示します。

```
Device# ap name AP1 vlan-tag 12
```

ap name write tag-config

AP に既存の設定を書き込むには、特権 EXEC モードで **ap name write tag-config** コマンド を使用します

ap name *ap-name***write tag-config**

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

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

このコマンドを使用すると、既存の設定を AP に書き込みできます。

例

次に、既存の設定を AP に書き込む例を示します。

```
Device# ap name AP40CE.2485.D594 write tag-config
```

ap name-regex

一致する AP 名の正規表現に基づいてフィルタを設定するには、**ap name-regex** コマンドを使用します。

ap name-regex *regular-expression*

構文の説明

regular-expression	フィルタ文字列を入力します。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP 名の正規表現の一致に基づいてフィルタを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name filter--name
Device(config-ap-filter)# ap name-regex regular-expression-string
```

ap neighborhood calendar-profile

AP ネイバーフッド カレンダー プロファイルを選択するには、**ap neighborhood calendar-profile** コマンドを使用します。

ap neighborhood calendar-profile *calendar-profile-name*

構文の説明

calendar-profile-name	カレンダープロファイル名。

コマンド デフォルト

なし

コマンド モード

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 Dublin 17.12.1	このコマンドが導入されました。

使用上のガイドライン

AP ネイバーフッド設定でプロファイルを追加する前に、カレンダープロファイルを作成します。

例

次に、AP ネイバーフッド カレンダー プロファイルを選択する例を示します。

```
Device# configure terminal
Device(config)# ap neighborhood calendar-profile ap-calendar-profile
```

ap neighborhood load-balance

RRM ベースの AP ロードバランシングを適用、クリア、または開始するには、**ap neighborhood load-balance** コマンドを使用します。

ap neighborhood load-balance { **apply** | **clear** | **start** }

構文の説明

apply	オンデマンドの RRM ベースの AP ロードバランシングを実行します。
clear	AP ネイバーフッド ロード バランシング アクションおよびリソース割り当て出力をクリアします。
start	AP ネイバーフッド ロード バランシング アクションを開始し、リソースを割り当てます。

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 Dublin 17.12.1	このコマンドが導入されました。

使用上のガイドライン

start キーワードは、データベースから古い反復データ（存在する場合）をクリアし、アルゴリズムの実行を開始します。このコマンドは、カレンダープロファイルの開始タイマーの有効期限切れイベントに似ています。

例

次に、AP ネイバーフッド ロード バランシング アクションを開始する例を示します。

```
Device# ap neighborhood load-balance start
```

ap packet-capture

AP パケット キャプチャ プロセスを開始または停止するには、**ap packet-capture** コマンドを使用します。

ap packet-capture {**start** | **stop**} *client-mac-address* {**auto** | **static** *ap-name*}

構文の説明

client-mac-address	クライアント MAC アドレス
ap-name	AP 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

stop オプションを **ap packet capture** コマンドとともに使用する場合、パケット キャプチャを停止するにはキーワード **all** を使用します。

例

次に、AP パケット キャプチャ プロセスを開始する例を示します。

```
Device# ap packet-capture start 3c08.f672.1ad9 static AP_2029
```

次に、AP パケット キャプチャ プロセスを完全に停止する例を示します。

```
Device# ap packet-capture stop 3c08.f672.1ad9 all
```

ap packet-capture profile

AP パケット キャプチャ プロファイルを設定するには、**ap packet-capture profile** コマンドを使用します。

ap packet-capture profile *profile-name*

構文の説明

profile-name	AP パケット キャプチャ 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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、AP パケット キャプチャ プロファイルを設定する例を示します。

```
Device# ap packet-capture profile test1
```

ap packet-capture start

隣接する一連のアクセス ポイントで指定されたクライアントのパケット キャプチャを有効にするには、**ap packet-capture start** コマンドを使用します。

ap packet-capture start *client-mac-addr* {**auto** | **static** *ap-name*}

構文の説明

client-mac-addr	パケットキャプチャを実行する必要があるクライアントのMACアドレス。
auto	隣接する AP でパケット キャプチャを開始します。
static *ap-name*	パケット キャプチャを実行する必要がある 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、隣接する一連のアクセス ポイントのクライアントのパケット キャプチャを有効にする例を示します。

```
Device# ap packet-capture start 0011.0011.0011 auto
```

ap profile

アクセス ポイント プロファイルを設定するには、**ap profile** コマンドを使用します。

ap profile *profile-name*

構文の説明

profile-name	APプロファイルの名前を入力します。

コマンド デフォルト

デフォルトでは、AP プロファイル名は default-ap-profile 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP プロファイル名を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap profile my-ap-profile
```

ap remote-lan profile-name

リモート LAN プロファイルを設定するには、**ap remote-lan profile-name** コマンドを使用します。

ap remote-lan profile-name *remote-lan-profile-name rlan-id*

構文の説明

remote-lan-profile-name	リモート LAN プロファイル名です。範囲は英数字で 1 ～ 32 文字です。
rlan-id	リモート LAN の識別子です。範囲は 1 ～ 128 です。 （注） 最大 128 の RLAN を作成できます。別の RLAN を作成する場合、既存の RLAN の *rlan-id* を使用することはできません。 RLAN と WLAN の両方のプロファイルに同じ名前を付けることはできません。同様に、RLAN と WLAN のポリシープロファイルに同じ名前を付けることはできません。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

次に、リモート LAN プロファイルを設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# ap remote-lan profile-name rlan_profile_name 3
```

ap remote-lan shutdown

すべての RLAN を有効または無効にするには、 **ap remote-lan shutdown** コマンドを使用します。

ap remote-lan shutdown

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、すべての RLAN を有効または無効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# [no] ap remote-lan shutdown
デバイス(config)# end
```

ap remote-lan-policy policy-name

RLAN ポリシー プロファイルを設定するには、**ap remote-lan-policy policy-name** コマンドを使用します。

ap remote-lan-policy policy-name *profile-name*

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、RLAN ポリシー プロファイルを設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# ap remote-lan-policy policy-name rlan_policy_prof_name
```

ap reset site-tag

特定のサイトに関連付けられているすべての AP を再起動するには、**ap reset site-tag** コマンドを使用します。

ap reset site-tag *site-tag-name*

構文の説明

site-tag-name	サイト タグ名。

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 Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

例

次に、特定のサイト内のすべての AP を再起動する例を示します。

```
Device# ap reset site-tag bgl18
```

ap tag persistency enable

AP タグの永続設定を設定するには、グローバル コンフィギュレーション モードで **ap tag persistency enable** コマンドを使用します。AP タグの永続設定を無効にするには、コマンドの **no** 形式を入力します。

ap tag persistency enable

no ap tag persistency 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

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 Bengaluru 17.6.1	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

例

次に、AP のタグの永続性を有効にする例を示します。

```
Device(config)# ap tag persistency enable
```

ap upgrade method https

HTTPS を介したコントローラからの AP イメージのダウンロードを設定するには、**ap upgrade method https** コマンドを使用します。アップグレード方法のタイプを削除するには、**no ap upgrade method https** コマンドを使用します。

ap upgrade method https

構文の説明

https	APイメージのダウンロードにHTTPSの方法を指定します。

コマンド デフォルト

AP のアップグレード方法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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.11.1	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、AP が効率的なアップグレード方法をサポートしている場合にのみ機能します。

AP が効率的なダウンロード方法をサポートしているかどうかを確認するには、**show ap config general** コマンドを使用します。

例

次に、AP のアップグレード方法を設定する例を示します。

```
Device# configure terminal
Device(config)# ap upgrade method https
```

ap upgrade staggered client-deauth

AP がアップグレードを開始したときに AP に接続されているクライアントの認証を解除するには、**ap upgrade staggered client-deauth** コマンドを使用します。認証の解除を無効にするには、このコマンドの **no** 形式を使用します。

ap upgrade staggered client-deauth

no ap upgrade staggered client-deauth

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

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 Cupertino 17.9.1	このコマンドが導入されました。
Cisco IOS XE Dublin 17.11.1	このコマンドが変更されました。コマンドの **no** 形式が導入されました。

例

次に、AP がアップグレードを開始したときに AP に接続されているクライアントの認証を解除する例を示します。

```
Device(config)# no ap upgrade staggered client-deauth
```

ap upgrade staggered iteration completion

反復の完了を通知するために宛先コントローラに参加する必要があるアクセスポイント（AP）の最小パーセンテージを設定するには、**ap upgrade staggered iteration completion** コマンドを使用します。

ap upgrade staggered iteration completion *min-percent*

構文の説明

min-percent	宛先コントローラに参加する必要がある AP のパーセンテージ。 有効な値の範囲は 0 ～ 100 です。

コマンド デフォルト

最小パーセンテージ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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	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、反復の完了を通知するために宛先コントローラに参加する必要がある AP の最小パーセンテージを設定するために役立ちます。AP が宛先コントローラに参加できない場合、アップグレードは停止されます。各反復の終了時に、欠落している AP の全体的なパーセンテージが、ここで設定されたパーセンテージよりも小さい必要があります。

例

次に、反復の完了を通知するためにネットワークに参加する必要がある AP の最小パーセンテージを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap upgrade staggered iteration completion 50
```

ap upgrade staggered iteration error

AP のアップグレード中の反復後にアクセスポイント（AP）が見つからない場合に実行するアクションを設定するには、**ap upgrade staggered iteration error** コマンドを使用します。

ap upgrade staggered iteration error action stop

構文の説明

stop	AP のアップグレード中の反復後に AP が見つからない場合に実行するアクションを指定します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、反復サイクル後に最小数の AP が宛先コントローラに参加できなかった場合に実行するアクションを設定できます。

たとえば、サイトが 5 回の反復サイクルでアップグレードされていて、宛先コントローラで何らかのエラーが発生したために 5 回目の反復サイクルが失敗した場合、アップグレードを停止するためにこのコマンドが役立ちます。

例

次に、AP のアップグレード中の反復後に AP が参加に失敗した場合に実行するアクションを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap upgrade staggered iteration error action stop
```

ap upgrade staggered iteration timeout

アクセスポイント（AP）のアップグレード中に反復ごとに許可される最長時間を設定するには、**ap upgrade staggered iteration timeout** コマンドを使用します。

ap upgrade staggered iteration timeout *timeout-duration*

構文の説明

timeout-duration	反復ごとに許可される時間（分単位）。 有効な値の範囲は 9 ～ 60 です。

コマンド デフォルト

反復のタイムアウト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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

使用上のガイドライン

指定された期間内にAPアップグレードの反復が完了しない場合、**ap upgrade staggered iteration error** コマンドを使用して設定されたエラーアクションが実行されます。

例

次に、反復ごとに許可される最長時間を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap upgrade staggered iteration timeout 40
```

ap tag-source-priority

AP タグのソース優先順位を設定するには、 **ap tag-source-priority** コマンドを使用します。

ap tag-source-priority *source-priority* **source** { **filter** | **ap** }

構文の説明

source-priority	AP タグのソース優先順位を入力します。有効な範囲は 2 ～ 3 です。
source	優先順位が設定されているソースを指定します。
filter	タグのソースとしての AP フィルタ。
ap	タグのソースとしての AP。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP をタグのソースとして設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap tag-source-priority priority-value source ap
```

ap tag-sources revalidate

アクセス ポイントのタグ ソースを再検証するには、**ap tag-sources revalidate** コマンドを使用します。

ap tag-sources revalidate

構文の説明

tag-sources	タグ送信元。
revalidate	アクセスポイントのタグソースを再検証します。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、アクセス ポイントのタグ ソースを再検証する例を示します。

```
Device# ap tag-sources revalidate
```

ap triradio

すべての Cisco AP でトライ無線を有効または無効にするには、**ap triradio** コマンドを使用します。

ap triradio {**disable** | **enable**}

構文の説明

ap triradio	すべての Cisco AP でトライ無線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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、すべての Cisco AP でトライ無線を有効または無効にする例を示します。

```
Device# ap triradio enable
```

ap vlan-tag

すべての非ブリッジ AP の VLAN タグを設定するには、**ap vlan-tag** コマンドを使用します。

ap vlan-tag *vlan-id*

構文の説明

vlan-id	VLAN 識別番号。

コマンド デフォルト

非ブリッジの AP の VLAN タグは有効になっていません。

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、ブリッジ以外のすべての AP の VLAN タギングを設定する例を示します。

```
Device# ap vlan-tag 1000
```

arp-caching

arp-caching を有効にするには、**arp-caching** コマンドを使用します。

arp-caching

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

config-wireless-flex-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、arp-caching を有効にする例を示します。

```
Device(config-wireless-flex-profile)# arp-caching
```

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

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。

```
デバイス(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。

```
デバイス(config)#wlan test-prediction 2 test-prediction
デバイス(config-wlan)#client vlan 43
デバイス(config-wlan)#no security wpa
デバイス(config-wlan)#load-balance
デバイス(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.
```

association-limit

AP プロファイル コンフィギュレーション モードで AP あたりの最大クライアント関連付け数を設定するには、**association-limit** コマンドを使用します。この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。

association-limit *clients-connections*

構文の説明

client-connections	AP あたりのクライアント接続の最大数を設定します。デフォルト値は 0 です （注） Cisco Catalyst 9136 シリーズ AP の AP あたりの最大クライアント数は、1200 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

AP 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 Cupertino 17.8.1	このコマンドが導入されました。

例

次に、AP プロファイル コンフィギュレーション モードで AP あたりの最大クライアント関連付け数を設定する例を示します。

```
Device# confiure terminal
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# association-limit 300
```

authentication-type

802.11u ネットワーク認証タイプを設定するには、**authentication-type** コマンドを使用します。認証タイプを削除するには、このコマンドの **no** 形式を使用します。

authentication-type {**dns-redirect** | **http-https-redirect** [*redirect-url*] | **online-enrollment** | **terms-and-conditions** [*terms*] }

構文の説明

dns-redirect	認証タイプを DNS リダイレクションに設定します。
http-https-redirect	認証タイプを HTTP/HTTPS リダイレクションに設定します。
redirect-url	HTTP/HTTPS リダイレクション URL。
online-enrollment	認証タイプをオンライン登録に設定します。
terms-and-conditions	認証タイプを利用規約に設定します。
terms	利用規約の URL。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

レイヤ 3 認証などの認証方式を使用する場合は、WLAN 設定（web 認証）で同じ認証を使用していることを確認します。

例

次に、802.11u ネットワーク認証タイプを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# authentication-type dns-redirect
```

autoqos

AutoQos ワイヤレスポリシーを有効にするには、**autoqos** コマンドを使用します。AutoQos 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。

autoqos mode { **enterprise-avc** | **fastlane** | **guest** | **voice** }

構文の説明

enterprise-avc	AutoQos ワイヤレス企業ポリシーを有効にします。
fastlane	AutoQos ワイヤレス fastlane ポリシーを有効にします。
guest	AutoQos ワイヤレスゲストポリシーを有効にします
voice	AutoQos ワイヤレス音声ポリシーを有効にします

コマンド デフォルト

なし

コマンド モード

ワイヤレス 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 Gibraltar 16.10.1	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。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-test
Device(config-wireless-policy)# autoqos mode enterprise-avc
```

avg-packet-size packetsize

ワイヤレス メディアストリームの平均パケット サイズを設定するには、**avg-packet-size** コマンドを使用します。

avg-packet-size *packetsize-value*

構文の説明

packetsize-value	平均パケット サイズ。有効な範囲は 100 ～ 1500 です。

コマンド デフォルト

なし

コマンド モード

media-stream

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス メディアストリームの平均パケット サイズを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group doc-grp 224.0.0.0 224.0.0.223
Device(config-media-stream)# avg-packet-size500
```

avc sd-service

コントローラで Software-Defined Application Visibility and Control（SD-AVC）サービスを有効にするには、**avc sd-service** コマンドを使用します。コントローラで SD-AVC 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。

avc sd-service

no avc sd-service

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

SD-AVC サービスは無効化されています。

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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、コントローラで SD-AVC サービスを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# avc sd-service
```

avoid label exhaustion error

MSMR とファブリック ボーダーが 2 つの異なるノード上にあり、これらのノードのいずれかが catalyst 9300 である場合、BGP ルートでラベル枯渇エラーが発生しないようにするには、グローバル コンフィギュレーション モードで **mpls label mode all-vrfs protocol all-afs per-vrf** コマンドを使用します。

awips

Advanced Wireless Intrusion Prevention System（aWIPS）と呼ばれる、ワイヤレス侵入の脅威を検出および軽減するメカニズムを有効にするには、**awips** コマンドを使用します。aWIPS を無効にするには、このコマンドの **no** 形式を使用します。

awips［ **forensic** ］

構文の説明

forensic	aWIPSのフォレンジックを有効にします。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。
Cisco IOS XE Bengaluru 17.4.1	**forensic** キーワードが追加されました。

例

次に、aWIPS とフォレンジックを有効にする例を示します。

```
Device# configure terminal
Device(config)#ap profile test
Device(config-ap-profile)#awips
Device(config-ap-profile)#awips forensic
```

awips-syslog

Cisco Advanced Wireless Intrusion Prevention System（aWIPS）の syslog しきい値を設定するには、**awips-syslog** コマンドを使用します。aWIPS の syslog しきい値を無効にするには、このコマンドの **no** 形式を使用します。

awips-syslog throttle period *value-btwn-30-600-seconds*

構文の説明

throttle period *value-btwn-30-600-seconds*	aWIPS の syslog しきい値を設定します。 （注） デフォルトのスロットリング間隔は 60 秒です。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

使用上のガイドライン

次に、aWIPS の syslog しきい値を設定する例を示します。

```
Device# configure terminal
Device(config)# awips-syslog throttle period 60
Device(config)# end
```

backhaul（メッシュ）

メッシュ AP プロファイルのメッシュ バックホールを設定するには、**backhaul** コマンドを使用します。

backhaul rate dot11 {**24ghz** | **5ghz**} {**auto** | **dot11abg** *rate* | **dot11n mcs** *mcs-index* }

構文の説明

rate	バックホール転送速度。
dot11	802.11 を指定します。
24ghz	802.11b を指定します。
5ghz	802.11a を指定します。
auto	方式を auto に指定します。
dot11abg	方式を dot11abg に指定します。
dot11n	方式を dot11n に指定します。
mcs	メディア コンバージェンス サーバー。
rate	メディア コンバージェンス サーバー レート。
mcs_index	802.11 のメディア コンバージェンス サーバー レート値。

コマンド デフォルト

バックホール クライアント アクセスは無効になります。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、メッシュ AP プロファイルのメッシュ バックホールの詳細を設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# backhaul rate dot11 24ghz auto
```

background-scanning（メッシュ）

メッシュ APプロファイルのバックグラウンドスキャンを設定するには、**background-scanning** コマンドを使用します。

background-scanning

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

バックグラウンド スキャンは無効になります。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、メッシュ AP プロファイルのバックグラウンド スキャンを設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# background-scanning
```

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。

```
デバイス(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	新規スキャン周期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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(config-rf-profile)#band-select probe-response
```

banner text

バナーのメッセージを設定するには、**banner text** コマンドを使用します。メッセージを削除するには、このコマンドの **no** 形式を使用します。

banner text *text*

no banner text

構文の説明

text	表示するテキストメッセージ。

コマンド デフォルト

なし

コマンド モード

パラメータ 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、バナーのメッセージを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# banner text #Hêllö#
```

battery-state（メッシュ）

AP のバッテリ状態を設定するには、**battery-state** コマンドを使用します。

battery-state

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

バッテリ状態は有効になります。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、AP のバッテリ状態を設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# battery-state
```

boot system flash

ブート システム フラッシュ パラメータを設定するには、**boot system flash** コマンドを使用します。ブート システム フラッシュ 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。

boot system flash ｛ **bootflash:** | **harddisk:** | **usb:** | **cns:** | **crashinfo:** | **flash:** | **null:** | **nvram:** | **system:** | **tar:** | **tmpsys:** | **webui:** ｝*options*

構文の説明

bootflash:	ディレクトリまたはファイル名を有効にします。
harddisk:	ディレクトリまたはファイル名を有効にします。
usb:	ディレクトリまたはファイル名を有効にします。
cns:	ディレクトリを有効にします。この URL プレフィックスはファイル名を受け入れません
crashinfo:	ディレクトリまたはファイル名を有効にします。
flash:	ディレクトリまたはファイル名を有効にします。
null:	ディレクトリを有効にします。この URL プレフィックスはファイル名を受け入れません
nvram:	ディレクトリまたはファイル名を有効にします。
system:	ディレクトリまたはファイル名を有効にします。
tar:	ディレクトリまたはファイル名を有効にします。
tmpsys:	ディレクトリまたはファイル名を有効にします。
webui:	ディレクトリまたはファイル名を有効にします。
options	システムイメージファイル名。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.8.1	このコマンドが導入されました。

使用上のガイドライン

数文字のキーワードと Tab キーを使用して、オートコンプリート機能を使用することができます。たとえば、**boot system flash boot** と入力して Tab キーを押すと、**boot system flash bootflash:**

コマンドが表示されます。オートコンプリート機能は、ローカルファイルシステムに対してのみ機能します。

'?' オプションを使用して、システム内のファイルを表示することができます。たとえば、**boot system flash bootflash:?** を使用すると、このコマンドに関連付けられているすべてのファイルが表示されます。

入力したファイル名がローカルに存在しない場合は、次のエラーが表示されます。

```
Device(config)#boot system flash bootflash:abc.bin
%Error parsing bootflash:/abc.bin (No such file or directory)
```

例

次に、ブート システム フラッシュ パラメータを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# boot system flash
bootflash:C9800-CL-rpboot.BLD_V178_THROTTLE_LATEST_20220111_082010.SSA.pkg
```

bridge-group

メッシュ AP プロファイルのブリッジ グループ パラメータを設定するには、**bridge-group** コマンドを使用します。

bridge-group {**name** *bridge-group-name* | **strict-match** }

構文の説明

name *bridge-group-name*	ブリッジ グループ名を設定します。
strict-match	ブリッジグループの厳密な照合を設定します。

コマンド デフォルト

なし

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ AP プロファイルのブリッジ グループ名を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile mesh mesh-profile
Device(config-wireless-mesh-profile)# bridge-group name mesh-bridge-group
```

bss-transition

WLAN ごとの BSS 移行を設定するには、**bss-transition** コマンドを使用します。

bss-transition ［**disassociation-imminent**］

構文の説明

disassociation-imminent	WLAN ごとの BSS 移行関連付け解除は差し迫っています。

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、WLAN ごとに BSS 移行を設定する例を示します。

```
Device(config-wlan)# bss-transition
```

bssid-stats bssid-stats frequency

BSSID 統計の頻度タイマーを設定するには、**bssid-stats bssid-stats frequency** コマンドを使用します。このタイマ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。

bssid-stats bssid-stats frequency *<timer value>*

[no] bssid-stats bssid-stats frequency

構文の説明

bssid-stats frequency	BSSID統計の頻度タイマーを秒単位で設定します。
<1-180>	頻度の値を 1 ～ 180 秒の範囲で設定します。

コマンド デフォルト

なし

コマンド モード

AP 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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、BSSID 統計の頻度タイマーを設定する例を示します。

```
Device(config-ap-profile)#bssid-stats bssid-stats-frequency 100
```

bssid-neighbor-stats interval

BSSID ネイバー統計を有効にし、BSSID ネイバー統計が AP から送信される間隔（秒単位）を設定するには、**bssid-neighbor-stats interval** 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。

bssid-neighbor-stats interval *bssid-neighbor-stats-interval*

[no] bssid-neighbor-stats interval *bssid-neighbor-stats-interval*

構文の説明

bssid-neighbor-stats	BSSID ネイバー統計を有効または無効にします。
interval	BSSID ネイバー統計が AP から送信される間隔（秒単位）を設定します。
bssid-neighbor-stats-interval	BSSID ネイバー統計が AP から送信される間隔（秒単位）を指定します。値の範囲は 30 ～ 600 秒です。デフォルト値は 180 秒です。

コマンド デフォルト

なし

コマンド モード

AP プロファイル 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 Amsterdam 17.2.1	このコマンドが導入されました。

例

秒単位で設定されている BSSID ネイバー統計の間隔を表示するには、次のようにします。

```
Device(config-ap-profile)#bssid-neighbor-stats interval 90
```

cache timeout active value

アクティブ フロー モニタ タイムアウト値を秒単位で設定するには、 **cache timeout active value** コマンドを使用します。

cache timeout active *value*

構文の説明

value	アクティブタイムアウト値を入力します。有効な範囲は1 ～ 604800 です。

コマンド デフォルト

なし

コマンド モード

config-flow-monitor

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、フロー モニターの非アクティブ タイムアウト値を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# flow monitor flow-monitor-name
Device(config-flow-monitor)# cache timeout active 300
```

cache timeout inactive value

フローモニタの非アクティブ タイムアウト値を秒単位で設定するには、**cache timeout inactive value** コマンドを使用します。

cache timeout inactive *value*

構文の説明

value	非アクティブ タイムアウト値を入力します。有効な範囲は 1 ～ 604800 です。

コマンド デフォルト

なし

コマンド モード

config-flow-monitor

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、フロー モニターの非アクティブ タイムアウト値を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# flow monitor flow-monitor-name
Device(config-flow-monitor)# cache timeout inactive 300
```

call-snoop

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

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

例

次に、WLAN で VoIP を有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless profile policy policy-name
Device(config-wireless-policy)#service-policy input platinum-up
Device(config-wireless-policy)#service-policy output platinum
Device(config-wireless-policy)#call-snoop
Device(config-wireless-policy)#no shutdown
Device(config-wireless-policy)#end
```

calender-profile name

カレンダープロファイルをポリシープロファイルにマッピングするには、**calender-profile name** コマンドを使用します。

calender-profile name *calendar-profile-name*

構文の説明

calendar-profile-name	カレンダープロファイル名を指定します。

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 Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

次に、カレンダープロファイルをポリシープロファイルにマッピングする例を示します。

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# calender-profile name daily_calendar_profile
Device(config-policy-profile-calender)# action deny-client
Device(config-policy-profile-calender)# end
```

captive-bypass-portal

キャプティブ バイパスを設定するには、**captive-bypass-portal** コマンドを使用します。

captive-bypass-portal

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、LWA および CWA で WLAN のキャプティブ バイパスを設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# parameter-map type webauth WLAN1_MAP
デバイス(config)# captive-bypass-portal
デバイス(config)# wlan WLAN1_NAME 4 WLAN1_NAME
デバイス(config-wlan)# security web-auth
デバイス(config-wlan)# security web-auth parameter-map WLAN1_MAP
デバイス(config-wlan)# end
```

capwap-discovery

CAPWAP 検出の応答にコントローラのパブリック IP またはプライベート IP が含まれるかどうかに関する、CAPWAP 検出の応答方式を設定するには、**capwap-discovery** コマンドを使用します。

capwap-discovery{**private** | **public**}

構文の説明

private	CAPWAP 検出の応答にプライベート IP を含めます。
public	CAPWAP 検出の応答にパブリック IP を含めます。

コマンド デフォルト

なし

コマンド モード

管理インターフェイス コンフィギュレーション（config-mgmt-interface）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

例

次に、CAPWAP 検出の応答方式を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless management interface Vlan1
Device(config-mgmt-interface)# capwap-discovery public
```

capwap backup

特定の device に参加しているすべてのアクセス ポイントでセカンダリ バックアップ device を設定するには、**capwap backup** コマンドを使用します。

capwap backup {**primary** *primary-controller-name primary-controller-ip-address* | **secondary** *secondary-controller-name secondary-controller-ip-address*}

構文の説明

primary	プライマリ バックアップ deviceを指定します。
primary-controller-name	プライマリ バックアップ deviceの名前。
primary-controller-ip-address	プライマリ バックアップ deviceの IP アドレス。
secondary	セカンダリ バックアップ deviceを指定します。
secondary-controller-name	セカンダリ バックアップ deviceの名前。
secondary-controller-ip-address	セカンダリ バックアップ deviceの IP アドレス。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

次に、特定のdeviceに参加しているすべてのアクセス ポイントのプライマリ バックアップ deviceを設定する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# capwap backup primary controller1 192.0.2.51
```

次に、特定のdeviceに参加しているすべてのアクセス ポイントのセカンダリ バックアップ deviceを設定する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# capwap backup secondary controller1 192.0.2.52
```

capwap window size

AP CAPWAP 制御パケットの送信キューサイズを設定するには、**capwap window size** コマンドを使用します。AP CAPWAP 制御パケットの送信キューサイズをデフォルトレベル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。

capwap window size *window-size*

構文の説明

window-size	AP CAPWAP 制御パケットの送信キューサイズ。 有効な範囲は 1 ～ 50 です。デフォルト値は 1 です。最大値を 20 に制限することを推奨します。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、AP CAPWAP 制御パケットの送信キューサイズを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# capwap window size 20
```

capwap udplite

Cisco AP で IPv6 CAPWAP UDP Lite を有効にするには、**capwap udplite** コマンドを使用します。

（注） 次のメッセージが表示されます。

This feature is supported only for IPv6 data packets, APs will be rebooted.

capwap udplite

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

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 Amsterdam 17.1.1s	このコマンドが導入されました。

次に、Cisco AP で IPv6 CAPWAP UDP Lite を有効にする例を示します。

```
Device# configure terminal
Device (config)# ap profile default-ap-profile
Device (config-ap-profile)# capwap udplite
Device (config-ap-profile)# end
```

ccn（メッシュ）

メッシュ AP プロファイルのチャネル変更通知を設定するには、**ccn** コマンドを使用します。

ccn

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

チャネル変更通知は無効になります。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、メッシュ AP プロファイルのチャネル変更通知を設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# ccn
```

ccx aironet-iesupport

Aironet IE CCX オプションのサポートを設定するには、次のコマンドを使用します。

ccx aironet-iesupport

構文の説明

ccx	Cisco Client Extension のオプションを設定します。
aironet-iesupport	WLAN での Aironet IE のサポートを設定します。

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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、Aironet IE サポートを設定する例を示します。

```
Device(config-wlan)#ccx aironet-iesupport
```

cdp

AP プロファイルの下の Cisco Lightweight アクセスポイントで Cisco Discovery Protocol（CDP）を有効にするには、 **cdp** 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 profile default-ap-profile

cdp
```
no cdp

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

AP プロファイルモード（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

no cdp コマンドは、device 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、device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、**cdp** 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。device 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。device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。

```
デバイス(config)# ap profile default-ap-profile

デバイス(config-ap-profile)# cdp
```

central authentication

中央集中型認証を有効または無効にするには、**central authentication** コマンドを使用します。

central authentication

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

config-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、中央集中型認証を有効にする例を示します。

```
Device(config-wireless-policy)# central authentication
```

central dhcp

ローカルでスイッチされるクライアントの中央集中型 dhcp を有効にするには、**central dhcp** コマンドを使用します。

central dhcp

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

config-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、ローカルに切り替えられるクライアントの中央集中型dhcpを有効にする例を示します。

```
Device(config-wireless-policy)# central dhcp
```

central switching

中央集中型スイッチを有効または無効にするには、**central switching** コマンドを使用します。

central switching

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	config-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、中央集中型スイッチを有効または無効にする例を示します。

```
Device(config-wireless-policy)# central switching
```

central-webauth

ACL の central-webauth を設定するには、**central-webauth** コマンドを使用します。

central-webauth

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

config-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、ACL の central-webauth を設定する例を示します。

```
Device(config-wireless-policy)# central-webauth
```

chassis redundancy ha-interface

シャーシの高可用性（HA）インターフェイスを設定するには、**chassis redundancy ha-interface** コマンドを使用します。

chassis redundancy ha-interface GigabitEthernet*interface-number* **local-ip** *ip-address netmask* **remote-ip** *remote-chassis-ip-addr*

構文の説明

interface-number	GigabitEthernet インターフェイス番号。有効な範囲は 1 ～ 32 です。
local-ip *ip-address netmask*	ローカル シャーシ HA インターフェイスの IP アドレスを設定します。ネットマスクの場合、次の形式 */nn* または *A.B.C.D* でネットマスクまたはプレフィックス長を入力します。
remote-ip *remote-chassis-ip-addr*	リモート シャーシ IP アドレスを設定します。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、シャーシの HA インターフェイスを設定する例を示します。

```
Device# chassis ha-interface GigabitEthernet 2 local-ip 10.10.10.10 255.255.255.0 remote-ip
 10.10.10.11
```

chassis redundancy ha-interface GigabitEthernet

コントローラの HA インターフェイスを作成するには、**chassis redundancy ha-interface GigabitEthernet** コマンドを使用します。

（注） このコマンドは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにのみ適用されます。

chassis redundancy ha-interface GigabitEthernet *num*

構文の説明

num	GigabitEthernet インターフェイス番号。有効な範囲は 1 ～ 32 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 Gibraltar 16.11.1	このコマンドが導入されました。

次に、コントローラの HA インターフェイスを作成する例を示します。

```
Device# chassis redundancy ha-interface GigabitEthernet 3
```

chassis redundancy keep-alive

ピアキープアライブの再試行回数と、ピアがダウンしていると判断されるまでの時間間隔を設定するには、**chassis redundancy keep-alive** コマンドを使用します。

chassis redundancy keep-alive { **retries** *retries* | **timer** *timer* }

構文の説明

retries	ピアがダウンしていると判断されるまでの、シャーシのピアキープアライブの再試行回数。 有効な値の範囲は 5 ～ 10 です。デフォルトの場合は 5 を入力します。
timer	100 ミリ秒の倍数で表される、シャーシのピアキープアライブの時間間隔。 有効な値の範囲は 1 ～ 10 です。デフォルトの場合は 1 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ピアキープアライブの再試行回数と時間間隔を設定する例を示します。

```
Device# chassis redundancy keep-alive retries 6
Device# chassis redundancy keep-alive timer 6
```

chassis renumber

ローカルシャーシ ID 割り当ての番号を再割り当てするには、**chassis renumber** コマンドを使用します。

chassis *chassis-num* **renumber** *renumber-id*

構文の説明

chassis-num	シャーシ番号。
renumber-id	ローカルシャーシ 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ローカルシャーシ ID 割り当ての番号を再割り当てする例を示します。

```
Device# chassis 1 renumber 1
```

chassis priority

指定したデバイスの優先順位を設定するには、**chassis priority** コマンドを使用します。

chassis *chassis-num* **priority** *priority-id*

構文の説明

chassis-num	シャーシ番号。
priority-id	シャーシの優先順位。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、指定したデバイスの優先順位を設定する例を示します。

```
Device# chassis 1 priority 1
```

chassis transport

シャーシ転送を有効または無効にするには、**chassis transport** コマンドを使用します。

chassis *chassis-num* **transport** {**enable** | **disable**}

構文の説明

chassis-num	シャーシ番号。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、シャーシ転送を有効にする例を示します。

```
Device# chassis 1 transport enable
```

cisco-dna grpc

Cisco DNA で gRPC チャネルを有効にするには、**cisco-dna grpc** コマンドを使用します。この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。

cisco-dna grpc

no cisco-dna grpc

構文の説明

grpc	Cisco DNA で gRPC チャネルを有効にします。

コマンド デフォルト

なし

コマンド モード

AP プロファイル 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 Amsterdam 17.3.1	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

例

次に、Cisco DNA で gRPC チャネルを有効にする例を示します。

```
Device(config-ap-profile)# cisco-dna grpc
```

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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、set（848 ページ）を参照してください。
- **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。

class class-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。

```
デバイス(config)# policy-map policy1
デバイス(config-pmap)# class class1
デバイス(config-pmap-c)# set dscp 10
デバイス(config-pmap-c)# police 1000000 20000 conform-action
デバイス(config-pmap-c)# police 1000000 20000 exceed-action
デバイス(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。

```
デバイス# configure terminal
デバイス(config)# class-map cm-3
デバイス(config-cmap)# match ip dscp 30
```

```
デバイス(config-cmap)# exit

デバイス(config)# class-map cm-4
デバイス(config-cmap)# match ip dscp 40
デバイス(config-cmap)# exit

デバイス(config)# policy-map pm3
デバイス(config-pmap)# class class-default
デバイス(config-pmap-c)# set dscp 10
デバイス(config-pmap-c)# exit

デバイス(config-pmap)# class cm-3
デバイス(config-pmap-c)# set dscp 4
デバイス(config-pmap-c)# exit

デバイス(config-pmap)# class cm-4
デバイス(config-pmap-c)# set precedence 5
デバイス(config-pmap-c)# exit
デバイス(config-pmap)# exit

デバイス# 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
```

classify

不正なデバイスのルールを分類するには、**classify** コマンドを使用します。

classify {**friendly** | **malicious** | **delete**}

構文の説明

friendly	このルールと一致するデバイスを危険なしとして分類します。
malicious	このルールと一致するデバイスを悪意ありとして分類します。
delete	このルールに一致するデバイスは無視されます。

コマンド デフォルト

なし

コマンド モード

config-rule

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、不正なデバイスを危険なしとして分類する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless wps rogue rule my-rogue-rule priority 3
Device(config-rule)# classify friendly
```

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*}][{**match-all***type*}] *class-map-name*
no class-map [{**match-any***type*}][{**match-all***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 Gibraltar 16.10.1	このコマンドが導入されました。
	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** class-map 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。

```
デバイス(config)# access-list 103 permit ip any any dscp 10
デバイス(config)# class-map class1
デバイス(config-cmap)# match access-group 103
デバイス(config-cmap)# exit
```

次に、クラスマップ class1 を削除する例を示します。

```
デバイス(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。

clear ap config

Ciscoアクセスポイントのファイルシステムからファイルを安全に消去するには、**clear ap config** コマンドを使用します。

clear ap config *ap-name*

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

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 Dublin 17.11.1	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、AP コンソールで実行する必要があります。

例

次に、AP でデータワイプをトリガーする例を示します。

```
Device# clear ap config doc-test
```

clear ap meraki stats

Meraki AP 関連のデータをクリアするには、**clear ap meraki stats** コマンドを使用します。

clear ap meraki stats

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 Cupertino 17.9.1	このコマンドが導入されました。

例

次に、Meraki AP 関連のデータをクリアする例を示します。

```
Device# clear ap meraki stats
```

clear ap sort statistics

ソートされた AP の統計をクリアするには、**clear ap sort statistics** コマンドを使用します。

clear ap sort statistics

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 Amsterdam 17.1.1s	このコマンドが導入されました。

次の例では、ソートされた AP の統計をクリアする方法を示します。

```
Device# clear ap sort statistics
```

clear chassis redundancy

高可用性（HA）設定をクリアするには、**clear chassis redundancy** コマンドを使用します。

clear chassis redundancy

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、HA 設定をクリアする例を示します。

```
Device# clear chassis redundancy
```

clear ip nbar protocol-discovery wlan

特定の WLAN の NBAR2 プロトコル検出統計情報をクリアするには、 **clear ip nbar protocol-discovery wlan** コマンドを使用します。

clear ip nbar protocol-discovery wlan *wlan-name*

構文の説明

wlan-name	WLAN 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、特定の WLAN の NBAR プロトコル検出統計情報をクリアする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# clear ip nbar protocol-discovery wlan wlan-name
```

clear mdns-sd statistics

mDNS の統計をクリアするには、**clear mdns-sd statistics** コマンドを使用します。

clear mdns-sd statistics { **debug** | **glan-id** *<1 - 5>* | **rlan-id** *<1 - 128>* **wired** | **wlan-id** *<1 - 4096>* }

構文の説明

debug	mDNS のデバッグの統計をクリアします。
glan-id*<1 - 5>*	GLAN ID をクリアします。値の範囲は 1 ～ 5 です。
rlan-id*<1 - 128>*	RLAN ID をクリアします。値の範囲は 1 ～ 128 です。
wired	mDNS の有線の統計をクリアします。
wlan-id*<1 - 4096>*	WLAN ID をクリアします。値の範囲は 1 ～ 4096 です。

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 Amsterdam 17.3.1	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

例

次に、mDNS の統計をクリアする例を示します。

```
Device# clear mdns-sd statistics
```

clear platform condition all

すべての条件付きデバッグおよびパケットトレースの設定とデータをクリアするには、**clear platform condition all** コマンドを使用します。

clear platform condition all

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、すべての条件付きデバッグおよびパケットトレースの設定とデータをクリアする例を示します。

```
Device# clear platform condition all
```

clear platform hardware chassis active qfp feature wireless trace-buffer ingress

QFP ワイヤレス入力パケットでフィルタリングされたトレースおよびグローバルトレースをクリアするには、**clear platform hardware chassis active qfp feature wireless trace-buffer ingress** コマンドを使用します。

clear platform hardware chassis active qfp feature wireless trace-buffer ingress { **all** | **conditions** | **filtered-trace** | **global-trace** }

構文の説明

all	条件、グローバルトレースバッファ、およびフィルタリングされたトレースバッファをクリアします。
conditions	すべてのフィルタリングされたトレースの条件をクリアします。
filtered-trace	フィルタリングされたトレースバッファをクリアします。
global-trace	グローバルトレースバッファをクリアします。

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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、QFP ワイヤレス入力パケットでフィルタリングされたトレースをクリアする例を示します。

```
Device# clear platform hardware chassis active qfp feature wireless trace-buffer ingress
 all
```

clear platform hardware chassis active qfp feature wireless trace-buffer punt-inject

QFP ワイヤレス パント/インジェクトでフィルタリングされたトレースおよびグローバルトレースをクリアするには、**clear platform hardware chassis active qfp feature wireless trace-buffer punt-inject** コマンドを使用します。

clear platform hardware chassis active qfp feature wireless trace-buffer punt-inject { **all** | **conditions** | **filtered-trace** | **global-trace** }

構文の説明

all	条件、グローバルトレースバッファ、およびフィルタリングされたトレースバッファをクリアします。
conditions	すべてのフィルタリングされたトレースの条件をクリアします。
filtered-trace	フィルタリングされたトレースバッファをクリアします。
global-trace	グローバルトレースバッファをクリアします。

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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、QFP ワイヤレス パント/インジェクト パケットでフィルタリングされたトレースをクリアする例を示します。

```
Device# clear platform hardware chassis active qfp feature wireless punt-inject all
```

clear platform software rif-mgr chassis active R0 clear-lmp-counters

アクティブインスタンスの制御メッセージの統計をクリアするには、**clear platform software rif-mgr chassis active R0 clear-lmp-counters** コマンドを使用します。

clear platform software rif-mgr chassis active R0 clear-lmp-counters

構文の説明

rif-mgr	RIF マネージャに関する情報を表示します。
chassis	シャーシに関する情報を表示します。
active	アクティブインスタンスを指定します。
R0	ルートプロセッサスロット 0 を指定します。
clear-lmp-counters	LMP 統計をクリアします。

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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、アクティブインスタンスの制御メッセージの統計をクリアする例を示します。

```
Device# clear platform software rif-mgr chassis active R0 clear-lmp-counters
```

clear platform software rif-mgr chassis standby R0 clear-lmp-counters

スタンバイインスタンスの制御メッセージの統計をクリアするには、**clear platform software rif-mgr chassis standby R0 clear-lmp-counters** コマンドを使用します。

clear platform software rif-mgr chassis standby R0 clear-lmp-counters

構文の説明

rif-mgr	RIF マネージャに関する情報を表示します。
chassis	シャーシに関する情報を表示します。
standby	スタンバイインスタンスを指定します。
R0	ルートプロセッサスロット 0 を指定します。
clear-lmp-counters	LMP 統計をクリアします。

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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、スタンバイインスタンスの制御メッセージの統計をクリアする例を示します。

```
Device# clear platform software rif-mgr chassis standby R0 clear-lmp-counters
```

clear subscriber policy peer

サブスクライバ ポリシー ピア接続の詳細の表示をクリアするには、特権 EXEC モードで **clear subscriber policy peer** コマンドを使用します。

clear subscriber policy peer {**address** *ip-address* | **handle** *connection-handle-id* | **session** | **all**}

構文の説明

address	IP アドレスで識別される特定のピア接続の表示をクリアします。
ip-address	クリアするピア接続の IP アドレス。
handle	ハンドルで識別される特定のピア接続の表示をクリアします。
connection-handle-id	ピア接続ハンドルのハンドル ID。
session	指定されたピアとのセッションの表示をクリアします。
all	すべてのピア接続の表示をクリアします。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(33)SRC	このコマンドが導入されました。
12.2(33)SB	このコマンドが、Cisco IOS Release 12.2(33)SB に統合されました

使用上のガイドライン

clear subscriber policy peer コマンドは、インテリジェント サービス ゲートウェイ（ISG）デバイスと選択したサービス コントロール エンジン（SCE）デバイス間のピアリング関係を終了します。ただし、SCE は設定された時間が経過した後、ISG デバイスに再接続しようとします。**clear subscriber policy peer** コマンドは、特定の SCE デバイスから選択したセッションの関連付けを削除できます。

例

次に、ルータ プロンプトで **clear subscriber policy peer** コマンドを使用して、サブスクライバ ポリシー ピア接続のすべての詳細の表示をクリアする例を示します。

```
Router# clear subscriber policy peer all
```

関連コマンド

コマンド	説明
show subscriber-policy peer	サブスクライバ ポリシー ピアの詳細を表示します。
subscriber-policy	サブスクライバ ポリシーの転送およびフィルタの決定を定義または変更します。

clear wireless stats mobility

イベントおよびメッセージ レベルの統計情報をクリアするには、**clear wireless stats mobility** コマンドを使用します。

clear wireless stats mobility

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 Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

次に、イベントおよびメッセージ レベルの統計情報をクリアする例を示します。

```
Device# clear wireless stats mobility
```

clear wireless stats mobility peer ip

ピアに関連付けられたコントロールおよびデータ リンク フラップ カウンタをクリアするには、**clear wireless stats mobility peer ip** コマンドを使用します。

clear wireless stats mobility peer ip *ip-address*

構文の説明

ip-address	リモート ピアの IP アドレス

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 Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

次に、ピアに関連付けられたコントロールおよびデータ リンク フラップ カウンタをクリアする例を示します。

```
Device# clear wireless stats mobility peer ip 192.0.2.51
```

clear wireless wps rogue ap

すべての不正 AP または特定の MAC アドレスを持つ不正 AP をクリアするには、**clear wireless wps rogue ap** コマンドを使用します。

clear wireless wps rogue ap ｛ **all** ｜ **mac-address** <*MAC Address*> ｝

構文の説明

all	すべての不正 AP をクリアします。
mac-address <*MAC Address*>	特定の MAC アドレスを持つ不正 AP 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 Amsterdam 16.12.1	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

例

次に、すべての不正 AP または特定の MAC アドレスを持つ不正 AP をクリアする例を示します。

```
Device# clear wireless wps rogue ap all
Device# clear wireless wps rogue ap mac-address 10.10.1
```

clear wireless wps rogue client

すべての不正クライアントまたは特定の MAC アドレスを持つ不正クライアントをクリアするには、**clear wireless wps rogue client** コマンドを使用します。

clear wireless wps rogue client { **all** | **mac-address** <*MAC Address*> }

構文の説明

all	すべての不正クライアントをクリアします。
mac-address <*MAC Address*>	特定の MAC アドレスを持つ不正クライアントをクリアします。

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 Amsterdam 16.12.1	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

例

次に、すべての不正クライアントまたは特定の MAC アドレスを持つ不正クライアントをクリアする例を示します。

```
Device# clear wireless wps rogue client all
Device# clear wireless wps rogue client mac-address 10.10.1
```

clear wireless wps rogue stats

不正な統計をクリアするには、**clear wireless wps rogue stats** コマンドを使用します。

clear wireless wps rogue stats

構文の説明

このコマンドには、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 Amsterdam 16.12.1	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

例

次に、不正な統計をクリアする例を示します。

```
Device# clear wireless wps rogue stats
```

clear wlan sort statistics

ソートされた WLAN の統計をクリアするには、**clear wlan sort statistics** コマンドを使用します。

clear wlan sort statistics

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 Amsterdam 17.1.1s	このコマンドが導入されました。

次の例では、ソートされた WLAN の統計をクリアする方法を示します。

```
Device# clear wlan sort statistics
```

client-access（メッシュ）

メッシュ AP プロファイルのクライアント アクセス AP を使用してバックホールを設定するには、**client-access** コマンドを使用します。

client-access

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

バックホール クライアント アクセスは無効になります。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、メッシュ AP プロファイルのクライアント アクセス AP を使用してバックホールを設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# client-access
```

client association limit

WLAN のクライアント接続 の最大数を設定するには、 **client association limit** 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*}
no client association limit {*association-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 ～ 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。

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 Gibraltar 16.10.1	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。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wlan wlan1
デバイス(config-wlan)# shutdown
デバイス(config-wlan)# client association limit 200
デバイス(config-wlan)# no shutdown
デバイス(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。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wlan wlan1
デバイス(config-wlan)# shutdown
デバイス(config-wlan)# no client association limit
デバイス(config-wlan)# no shutdown
デバイス(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。

```
デバイス# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
デバイス(config)# wlan wlan1
デバイス(config-wlan)# client association limit radio 200
デバイス(config-wlan)# no shutdown
デバイス(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。

```
デバイス# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
デバイス(config)# wlan wlan1
デバイス(config-wlan)# client association limit ap 300
デバイス(config-wlan)# no shutdown
デバイス(config-wlan)# end
```

client-aware-fra

クライアント認識フレキシブル ラジオ アサインメント（FRA）を設定するには、RF プロファイル コンフィギュレーション モードで **client-aware-fra** {**client-count-reset** *client-count* | **client-reset-util** *util-percentage*} コマンドを使用します。

この機能を無効にするには、**client-reset-util** コマンドの no 形式を使用します。

client-aware-fra { **client-count-reset** *client-count* | **client-reset-util** *util-percentage* }

no client-aware-fra client-reset-util *util-percentage*

構文の説明

client-count-reset	6 GHz から 5 GHz に無線を切り替えるためのクライアント数しきい値を設定します。
client-count	6 GHz クライアント数を指定します。値の範囲は 1 ～ 10 クライアントです。
client-reset-util	6 GHz から 5 GHz に無線を切り替えるための使用率しきい値を設定します。
util-percentage	使用率を指定します。値の範囲は 0 ～ 100 パーセントです。

コマンド デフォルト

なし

コマンド モード

RF 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 Cupertino 17.9.1	このコマンドが導入されました。

例

次に、クライアント認識フレキシブルラジオアサインメント（FRA）を設定する例を示します。

```
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(conf-rf-profile)# client-aware-fra client-count-reset 1
Device(conf-rf-profile)# client-aware-fra client-reset-util 5
```

channel foreign

RF プロファイルの DCA 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。

```
デバイス(config-rf-profile)#channel foreign
```

channel chan-width

RF プロファイルの DCA チャネル幅を設定するには、**channel chan-width** コマンドを使用します。

channel chan-width {**160** | **20** | **40** | **80** | **80+80** | **best**}

構文の説明

160	160 MHz。
20	20 MHz。
40	40 MHz。
80	80 MHz。
80+80	80+80 MHz。
best	最適なチャネル幅。

コマンド デフォルト

なし

コマンド モード

RF プロファイルの設定（config-rf-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

例

次に、RF プロファイルの DCA チャネル幅を設定する例を示します。

```
Device(config-rf-profile)# channel chan-width 160
```

channel psc

DCA の優先スキャンチャネル（PSC）バイアスを有効または無効にするには、RF コンフィギュレーション モードで **channel psc** コマンドを使用します。この機能を無効化するには、このコマンドの **no** 形式を使用します。

channel psc

no channel psc

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

RF 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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、DCA の優先スキャンチャネル（PSC）バイアスを有効または無効にする例を示します。

```
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# channel psc
```

client-l2-vnid

ワイヤレス ファブリック プロファイルで client l2-vnid を設定するには、 **client-l2-vnid** コマンドを使用します。

client-l2-vnid *vnid*

構文の説明

vnid	client l2-vnid を設定します。有効な範囲は 0 ～ 16777215 です。

コマンド デフォルト

なし

コマンド モード

config-wireless-fabric

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス ファブリック プロファイルで client l2-vnid 値を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile fabric fabric-profile-name
Device(config-wireless-fabric)# client-l2-vnid 10
```

client-steering

WLAN で 6 GHz クライアントステアリングを設定するには、**client-steering** コマンドを使用します。この機能を無効化するには、このコマンドの **no** 形式を使用します。

client-steering

no client-steering

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

WLAN 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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、WLAN で 6 GHz クライアントステアリングを設定する例を示します。

```
Device # configure terminal
Device (config)# wlan wlan-name 18 ssid-name
Device (config-wlan)# client-steering
```

collect counter

フロー レコードの非キーフィールドとしてフロー内のバイト数またはパケット数を設定するには、フロー レコード コンフィギュレーション モードで **collect counter** コマンドを使用します。フロー（カウンタ）内のバイト数またはパケット数をフロー レコードの非キーフィールドとして使用する設定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。

コマンド デフォルト

フロー内のバイト数またはパケット数は、非キーフィールドとして設定されません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドをデフォルト設定に戻すには、**no collect counter** または **default collect counter** フロー レコード コンフィギュレーション コマンドを使用します。

次に、フローの合計バイト数を非キーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#collect counter bytes long
```

次に、フローからの合計パケット数を非キーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter packets long
```

collect wireless ap mac address（ワイヤレス）

ワイヤレス クライアントが関連付けられているアクセス ポイントの MAC アドレスの収集を有効にするには、フロー レコード コンフィギュレーション モードで **collect wireless ap mac address** コマンドを使用します。アクセス ポイントの MAC アドレスの収集を無効にするには、このコマンドの **no** 形式を使用します。

collect wireless ap mac address
no collect wirelessap mac 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

アクセス ポイントの MAC アドレスの収集は、デフォルトでは有効になっていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

collect コマンドは、フローモニタ レコードの非キー フィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キーフィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キーフィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キーフィールドの値はフロー内の最初のパケットからのみ取得されます。

次に、フロー レコードを設定して、ワイヤレス クライアントが関連付けられているアクセス ポイントの MAC アドレスの収集を有効にする例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# collect wireless ap mac address
```

collect wireless client mac address（ワイヤレス）

アクセス ポイントが関連付けられているワイヤレス クライアントの MAC アドレスの収集を有効にするには、フロー レコード コンフィギュレーション モードで **collect wireless client mac address** コマンドを使用します。アクセス ポイントの MAC アドレスの収集を無効にするには、このコマンドの **no** 形式を使用します。

collect wirelessclient mac address
no collect wireless client mac 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

ワイヤレス クライアントの MAC アドレスの収集は、デフォルトでは有効になっていません。

コマンド モード

フロー レコード 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 XE ジブラルタル 16.10.1	このコマンドが導入されました。

使用上のガイドライン

collect コマンドは、フローモニタ レコードの非キー フィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キーフィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キーフィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キーフィールドの値はフロー内の最初のパケットからのみ取得されます。

次に、フロー レコードを設定して、ワイヤレス クライアントが関連付けられているアクセス ポイントの MAC アドレスの収集を有効にする例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# collect wireless client mac address
```

condition chan-width

不正検出のチャネル幅と帯域を設定するには、**condition chan-width** コマンドを使用します。不正検出からチャネル幅と帯域を削除するには、このコマンドの **no** 形式を使用します。

condition chan-width { **160MHz** | **20MHz** | **40MHz** | **80MHz** } **band** { **2.4GHz** | **5GHz** | **6GHz** }

no condition chan-width

構文の説明

160MHz	チャネル幅を 160 MHz に指定します。
20MHz	チャネル幅を 20 MHz に指定します。
40MHz	チャネル幅を 40 MHz に指定します。
80MHz	チャネル幅を 80 MHz に指定します。
band	無線帯域を指定します。
2.4GHz	無線帯域を 2.4 GHz に指定します。
5GHz	無線帯域を 5 GHz に指定します。
6GHz	無線帯域を 6 GHz に指定します。

コマンド デフォルト

チャネル幅は設定されていません。

コマンド モード

ルール コンフィギュレーション（config-rule）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.12.1	このコマンドが導入されました。

使用上のガイドライン

分類が **Friendly** の場合は、設定された値が最小チャネル幅になります。

分類が **Custom**、**Malicious**、または **Delete** の場合は、設定された値が最大チャネル幅になります。

例

次に、不正検出分類のチャネル幅値と帯域を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless wps rogue rule 1 priority 1
Device(config-rule)#condition chan-width 20MHz band 5gHz
```

connection-capability

ホットスポット 2.0 接続機能を設定するには、**connection-capability** コマンドを使用します。ホットスポット 2.0 接続機能を削除するには、このコマンドの **no** 形式を使用します。

connection-capability *ip-protocol port-number* {**closed** | **open** | **unknown**}

構文の説明

ip-protocol	IP 番号。有効な範囲は 0 ～ 255 です。
port-number	ポート番号。有効な範囲は 0 ～ 65535 です。
closed	接続がクローズドモードであることを示します。
open	接続がオープンモードであることを示します。
unknown	接続ステータスが不明であることを示しています。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

次の表に、定義済みオープン ポートおよびプロトコルを示します。

表 7: オープン ポートおよびプロトコル

IP プロトコル	ポート番号	説明
1	0	ICMP。診断に使用されます。
6	20	FTP
6	22	SSH
6	80	HTTP
6	443	HTTPS および TLS VPN で使用されます。
6	1723	ポイントツーポイント トンネリング プロトコル VPN で使用されます。
6	5060	VoIP
17	500	IKEv2（IPsec VPN）で使用されます。

IP プロトコル	ポート番号	説明
17	5060	VoIP
17	4500	IKEv2（IPsec VPN）で使用できます。
50	0	ESP。IPsec VPN で使用されます。

例

次に、ホットスポット 2.0 接続機能を設定する例を示します。

```
Device(config)#wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# connection-capability 12 655 open
```

consent activation-mode merge

ポリシーの有効化モードを有効にし、802.1X または MAC 認証バイパス（MAB）に適用されるポリシーとマージすることでクライアントがネットワークにアクセスできるようにするには、パラメータ マップ コンフィギュレーション モードで **consent activation-mode merge** 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。

consent activation-mode merge

no consent activation-mode merge

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

パラメータ マップ 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 Dublin 17.11.1	このコマンドが導入されました。

例

次に、ポリシーの有効化モードを有効にし、802.1XまたはMAC認証バイパス（MAB）に適用されるポリシーとマージすることでクライアントがネットワークにアクセスできるようにする例を示します。

```
Device# configure terminal
Device(config)# parameter-map type webauth parameter-map-name
Device(config-params-parameter-map)# consent activation-mode merge
```

console

AP シリアルコンソールポートを有効にするには、AP プロファイル コンフィギュレーションで**console** コマンドを使用します。この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。

console

no console

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

AP 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 Cupertino 17.9.1	このコマンドが導入されました。

例

次に、AP シリアルコンソールポートを有効にする例を示します。

```
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# console
```

controller

SD サービスコントローラ接続パラメータ コンフィギュレーション モードを開始するには、**controller** コマンドを使用します。SD サービス コントローラ 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。

controller

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

SD サービス コンフィギュレーション（config-sd-service）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが導入されました。

例

次に、SD サービスコントローラ接続パラメータ コンフィギュレーション モードを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# avc sd-service
Device(config-sd-service)# controller
```

convergence

メッシュ コンバージェンス方式を設定するには、**convergence** コマンドを使用します。

convergence { **fast** | **noise-tolerant-fast** | **standard** | **very-fast** }

構文の説明

fast	高速コンバージェンス方式を設定します。
noise-tolerant-fast	不安定なRF環境を処理するためのノイズ耐性高速コンバージェンス方式を設定します。
standard	標準コンバージェンス方式を設定します。
very-fast	非常に高速なコンバージェンス方式を設定します。

コマンド デフォルト

標準

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ AP プロファイルの高速コンバージェンス方式を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile mesh mesh-profile
Device(config-wireless-mesh-profile)# convergence fast
```

copy configuration download

SFTP または TFTP サーバーからワークグループブリッジ（WGB）構成ファイルをダウンロードするには、**copy configuration download** コマンドを使用します。

copy configuration download { **sftp:** | **tftp:** } *ip-address* [*directory*] [*file-name*]

構文の説明

sftp:	SFTP サーバーを選択します。
tftp:	TFTP サーバーを選択します。
ip-address	使用する SFTP または TFTP サーバーの IP アドレス。
directory	（任意）SFTP または TFTP サーバーで使用するディレクトリ名。
file-name	（任意）WGB 構成ファイル名。

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 Cupertino 17.8.1	このコマンドが導入されました。

使用上のガイドライン

AP が WGB モードの場合にのみ、AP コンソールでこのコマンドを入力できます。

例

次に、SFTP サーバーから WGB 構成ファイルを選択する例を示します。

```
Device# copy configuration download sftp: 10.10.10.1 C:sample.txt
```

copy configuration upload

ワークグループブリッジ（WGB）構成ファイルを作成し、SFTP または TFTP サーバーにアップロードするには、**copy configuration upload** コマンドを使用します。

copy configuration upload ｛ **sftp:** ｜ **tftp:** ｝ *ip-address* ［ *directory* ］ ［ *file-name* ］

構文の説明

sftp:	SFTP サーバーを選択します。
tftp:	TFTP サーバーを選択します。
ip-address	使用する SFTP または TFTP サーバーの IP アドレス。
directory	（任意）SFTP または TFTP サーバーで使用するディレクトリ名。
file-name	（任意）WGB 構成ファイル名。

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 Cupertino 17.8.1	このコマンドが導入されました。

使用上のガイドライン

AP が WGB モードの場合にのみ、AP コンソールでこのコマンドを入力できます。

例

次に、WGB 構成ファイルを作成し、SFTP サーバーにアップロードする例を示します。

```
Device# copy configuration upload sftp: 10.10.10.1 C:sample.txt
```

core-dump kernel limit

AP で収集されるカーネルコアダンプの数を制限するには、**core-dump kernel limit** コマンドを使用します。この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。

core-dump kernel limit *limit*

no core-dump kernel limit

構文の説明

limit	AP で収集されるカーネルコアダンプの最大数。有効な範囲は 0 ～ 5 です。デフォルト値は 0 です

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.12.1	このコマンドが導入されました。

使用上のガイドライン

core-dump kernel limit コマンドを有効または無効にすると、接続されているすべての AP が再起動します。

例

次に、AP で収集されるカーネルコアダンプの数を制限する例を示します。

```
Device(config)# ap profile default-ap profile
Device(config-ap-profile)# core-dump kernel limit 3
```

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。

```
デバイス(config-rf-profile)#coverage data rssi threshold -85
```

crypto key generate rsa

Rivest、Shamir、Adelman（RSA）キー ペアを生成するには、グローバル設定モードで **crypto key generate rsa** コマンド を使用します。

crypto key generate rsa [{**general-keys** | **usage-keys** | **signature** | **encryption**}] [**label** *key-label*] [**exportable**] [**modulus** *modulus-size*] [**storage** *devicename* **:**] [**redundancy**] [**on** *devicename* **:**]

構文の説明

general-keys	（オプション）デフォルトで汎用キー ペアが生成されることを指定します。
usage-keys	（オプション）2 つの RSA 特定目的キー ペア、1 つの暗号化ペア、および 1 つのシグニチャ ペアが生成されることを指定します。
signature	（オプション）生成される RSA 公開キーがシグニチャ特定目的キーになることを指定します。
encryption	（オプション）生成される RSA 公開キーが暗号化特定目的キーになることを指定します。
label *key-label*	（オプション）エクスポートされているときに RSA キー ペアに使用される名前を指定します。 キー ラベルを指定していない場合、ルータの完全修飾ドメイン名（FQDN）が使用されます。
exportable	（オプション）ルータなどの別のシスコ デバイスに RSA キー ペアをエクスポートできることを指定します。
modulus *modulus-size*	（オプション）キー モジュラスの IP サイズを指定します。 デフォルトでは、認証局（CA）キーのモジュラス サイズは 1024 ビットです。推奨される CA キーのモジュラスは 2048 ビットです。CA キー モジュラスの範囲は 350 ～ 4096 ビットです。 （注） Cisco IOS XE リリース 2.4 および Cisco IOS リリース 15.1(1)T では、秘密キーの動作のために最大キー サイズが 4096 ビットに拡張されました。これらのリリースより前の秘密キーの動作の最大値は 2048 ビットでした。
storage *devicename* **:**	（オプション）キー ストレージの場所を指定します。ストレージ デバイスの名前の後にはコロン（:）を付けます。
redundancy	（オプション）キーをスタンバイ CA に同期させる必要があることを指定します。

on *devicename* **:**	（オプション）指定した装置上でRSAキー ペアが作成されることを指定します。この装置にはユニバーサル シリアル バス（USB）トークン、ローカル ディスク、およびNVRAMなどがあります。装置の名前の後にはコロン（:）を付けます。 USBトークン上で作成されるキーは、2048ビット以下である必要があります。

コマンド デフォルト

RSA キー ペアは存在しません。

コマンド モード

グローバル コンフィギュレーション（config）

Cisco IOS XE Release 17.11.1a 以降では、コマンドモードは特権 EXEC（#）です

コマンド履歴

リリース	変更内容
11.3	このコマンドが導入されました。
12.2(8)T	*key-label* 引数 が追加されました。
12.2(15)T	**exportable** キーワードが追加されました。
12.2(18)SXD	このコマンドが、Cisco IOS リリース 12.2(18)SXD に統合されました。
12.4(4)T	**storage** キーワードおよび *devicename* **:** 引数が追加されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.4(11)T	**storage** キーワードおよび *devicename* **:** 引数が Cisco 7200VXR NPE-G2 プラットフォームに実装されました。 **signature**、**encryption**、**on** キーワードおよび *devicename* **:** 引数が追加されました。
12.4(24)T	IPv6 セキュア ネイバー探索（SeND）のサポートが追加されました。
XE 2.4	秘密キーの動作のために RSA キーの最大サイズが 2048 から 4096 ビットに拡張されました。
15.0(1)M	このコマンドが変更されました。**redundancy** キーワードが導入されました。
15.1(1)T	このコマンドが変更されました。**modulus** キーワード値の範囲が 360 ～ 2048 ビットから 360 ～ 4096 ビットに拡張されました。
15.2(2)SA2	このコマンドが Cisco ME 2600X シリーズ イーサネット アクセス スイッチに実装されました。

リリース	変更内容
Cisco IOS XE リリース 17.11.1a	このコマンドのデフォルトコマンドモードが、グローバル コンフィギュレーション（config）から特権EXEC（#）に変更されました。

使用上のガイドライン

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

シスコ デバイス（ルータなど）の RSA キー ペアを生成するには、このコマンドを使用します。

RSA キーはペアで作成されます。1 つは RSA 公開キー、もう 1 つは RSA 秘密キーです。

このコマンドの発行時に、ルータに RSA キーがすでに設定されている場合は、警告が表示され、既存のキーを新しいキーと置き換えるよう求めるプロンプトが表示されます。

（注） このコマンドを発行する前に、ルータでホスト名および IP ドメイン名が設定されています（**hostname** および **ip domain-name** コマンドを使用）。ホスト名および IP ドメイン名を使用しないと、**crypto key generate rsa** コマンドを完了できません。（名前付きキー ペアのみを生成する場合はこれに当てはまりません。）

（注） RSA キーを使用せずにルータでキー ペアを生成すると、セキュア シェル（SSH）によって追加の RSA キー ペアが生成される場合があります。追加のキー ペアは SSH でのみ使用され、{*router_FQDN*}.server のような名前が付けられます。たとえば、ルータ名が「router1.cisco.com」の場合、キー名は「router1.cisco.com.server」です。

このコマンドはルータの設定には保存されません。ただし、このコマンドによって生成された RSA キーは、次回設定が NVRAM に書き込まれるときに、NVRAM のプライベート設定（ユーザには表示されない、または別のデバイスにバックアップされる）に保存されます。

（注） 設定が NVRAM に保存されていない場合、生成されたキーはルータの次のリロード時に失われます。

RSA キー ペアには用途キーと汎用目的キーの 2 つのタイプがあり、これらは相互に排他的です。RSA キー ペアを生成するとき、用途キーまたは汎用目的キーを選択するためのプロンプトが表示されます。

用途キー

用途キーを生成する場合、RSA キーの 2 つのペアが生成されます。1 つのペアは認証方式として RSA シグニチャを指定する任意のインターネット キー交換（IKE）ポリシーで使用され、その他のペアは認証方式として RSA 暗号化キーを指定するすべての IKE ポリシーで使用されます。

CA は RSA 署名を指定する IKE ポリシーでのみ使用され、RSA 暗号化ナンスを指定する IKE ポリシーでは使用されません。（ただし、複数の IKE ポリシーを指定し、1 つのポリシーで RSA シグニチャを指定し、別のポリシーで RSA 暗号化ナンスを指定することもできます。）

IKE ポリシーで両方のタイプの RSA 認証方式を使用する場合は、用途キーを生成することをお勧めします。用途キーを使用すると、各キーは不必要に暴露されなくなります。（用途キーを使用しない場合、1 つのキーが両方の認証方法に使用されるため、そのキーが暴露される危険性が高くなります。）

汎用キー

汎用キーを生成する場合、生成される RSA キーのペアは 1 つのみです。このペアは、RSA シグニチャまたは RSA 暗号化キーのいずれかを指定する IKE ポリシーで使用されます。そのため、汎用キー ペアは用途キー ペアよりも頻繁に使用される可能性があります。

名前付きキー ペア

key-label 引数を使用して名前付きキー ペアを生成する場合は、**usage-keys** キーワードまたは **general-keys** キーワードも指定する必要があります。名前付きキー ペアを使用して、複数の RSA キー ペアを用意すると、Cisco IOS ソフトウェアがアイデンティティの証明書ごとに異なるキー ペアを維持できるようになります。

係数の長さ

RSA キーのペアを生成する場合に、モジュラスの長さの入力を求められます。モジュラスが長いほど、セキュリティが強化されます。ただし、モジュラスが長いほど、生成には時間がかかり（サンプル時間については、次の表を参照）、使用にも時間がかかります。

表 *8 : RSA* キー生成用のモジュラス長ごとのサンプル時間

ルータ	360 ビット	512 ビット	1024 ビット	2048 ビット（最大）
Cisco 2500	11 秒	20 秒	4 分 38 秒	1 時間以上
Cisco 4700	1 秒未満	1 秒	4 秒	50 秒

Cisco IOS ソフトウェアは 4096 ビットを超えるモジュラスをサポートしていません。通常、512 ビット未満の長さは推奨されません。特定の状況で、モジュラスを短くすると、IKE で適切に機能しない場合があるため、2048 ビット以上のモジュラスを使用することを推奨します。

（注） Cisco IOS Release 12.4(11)T の時点では、最大 4096 ビットまでのピアの公開 RSA キーのモジュラス値が自動的にサポートされます。秘密 RSA キーの最大モジュラス値は 4096 ビットです。したがって、ルータが生成またはインポートできる RSA 秘密キーの最大サイズは、4096 ビットです。ただし、RFC 2409 では、RSA 暗号化の秘密キーのサイズを 2048 ビット以下に制限しています。CA の推奨モジュラスは 2048 ビット、クライアントの推奨モジュラスも 2048 ビットです。

RSA キーが暗号化ハードウェアによって生成される場合は、制限が追加されることがあります。たとえば、RSA キーが Cisco VPN サービス ポート アダプタ（VSPA）によって生成される場合、RSA キー モジュラスは 384 ビット以上にする必要があります。また、64 の倍数にする必要もあります。

RSA キーのストレージ場所の指定

storage *devicename* **:** キーワードおよび引数を使用して **crypto key generate rsa** コマンドを発行すると、指定したデバイスに RSA キーが保存されます。この場所は、**crypto key storage** コマンド設定よりも優先されます。

RSA キー生成用のデバイスの指定

Cisco IOS Release 12.4(11)T 移行のリリースでは、RSA キーが生成されるデバイスを指定できます。サポート対象のデバイスには、NVRAM、ローカル ディスク、および USB トークンが含まれます。ルータで USB トークンを設定し、それが利用可能な場合、USB トークンは、ストレージ デバイスとしてだけでなく、暗号化デバイスとしても使用できます。USB トークンを暗号化装置として使用すると、このトークンでクレデンシャルのキー生成、署名、認証などの RSA 操作を実行できます。秘密キーは決して USB トークンから出ないようになっており、エクスポートできません。公開キーはエクスポート可能です。

RSA キーは、**on** *devicename* **:** キーワードおよび引数を使用して設定済みで利用可能な USB トークンで生成される場合があります。USB トークン上に常駐するキーは、生成された段階でトークンの永続的な保管場所に保存されます。USB トークンで生成できるキーの数は利用可能なスペースによって制限されます。USB トークンでキーを生成しようとしたときに一杯の場合は、次のメッセージが表示されます。

```
% Error in generating keys:no available resources
```

キーの削除操作を行うと、トークンに保存されているキーは、永続的な保管場所からただちに削除されます（トークン上に常駐していないキーは、**copy** またはそれに類するコマンドが発行されると、トークン以外の保管場所で保存や削除が行われます）。

USB トークンの設定詳細については、『Cisco IOS Security Configuration Guide, Release 12.4T』の「Storing PKI Credentials」の章を参照してください。トークン上で RSA クレデンシャルする際の詳細については、『Cisco IOS Security Configuration Guide , Release 12.4T』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章を参照してください。

デバイスでの RSA キー冗長性生成の指定

既存のキーの冗長性がエクスポート可能な場合にのみ指定できます。

例

次の例では、「ms2」というラベルの USB トークンに汎用 1024 ビット RSA キー ペアを生成し、それとともに表示される暗号エンジンのデバッギング メッセージを示します。

```
Router(config)# crypto key generate rsa label ms2 modulus 2048 on usbtoken0:
The name for the keys will be: ms2
% The key modulus size is 2048 bits
% Generating 1024 bit RSA keys, keys will be on-token, non-exportable...
Jan 7 02:41:40.895: crypto_engine: Generate public/private keypair [OK]
Jan 7 02:44:09.623: crypto_engine: Create signature
Jan 7 02:44:10.467: crypto_engine: Verify signature
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_CREATE_PUBKEY(hw)(ipsec)
Jan 7 02:44:10.467: CryptoEngine0: CRYPTO_ISA_RSA_PUB_DECRYPT(hw)(ipsec)
```

これで、「ms2」というラベルが付けられた、トークン上のキーを登録に使用できます。

次に、用途 RSA キーを生成する例を示します。

```
Router(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
 Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
 Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

次に、汎用 RSA キーを生成する例を示します。

（注） 用途と汎用の両方のキーを生成することはできません。生成できるのはいずれか 1 つです。

```
Router(config)# crypto key generate rsa general-keys
The name for the keys will be: myrouter.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
 Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

次に、汎用 RSA キー「exampleCAkeys」を生成する例を示します。

```
crypto key generate rsa general-keys label exampleCAkeys
crypto ca trustpoint exampleCAkeys
 enroll url
http://exampleCAkeys/certsrv/mscep/mscep.dll
 rsakeypair exampleCAkeys 1024 1024
```

次に、「tokenkey1」の RSA キー ストレージの場所として「usbtoken0:」を指定する例を示します。

crypto key generate rsa general-keys label tokenkey1 storage usbtoken0:

次に、**redundancy** キーワードを指定する例を示します。

```
Router(config)# crypto key generate rsa label MYKEYS redundancy
The name for the keys will be: MYKEYS
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable with redundancy...[OK]
```

関連コマンド

コマンド	説明
copy	ファイルをコピー元からコピー先にコピーするには、特権 EXEC モードで copy コマンドを使用します。
crypto key storage	RSA キーペアのデフォルトのストレージ場所を設定します。
debug crypto engine	暗号エンジンに関するデバッグ メッセージを表示します。
hostname	ネットワーク サーバのホスト名を指定または修正します。
ip domain-name	デフォルトのドメイン名を定義して、未修飾のホスト名（ドット付き 10 進表記で記載されていない名前）を完成します。
show crypto key mypubkey rsa	ルータの RSA 公開キーを表示します。
show crypto pki certificates	PKI 証明書、証明書認証局、および任意の登録認局証明書に関する情報を表示します。

crypto pki trustpoint

単一の CA 証明書専用の新しいトラストポイントを作成するには、**crypto pki trustpoint** コマンドを使用します。

crypto pki trustpoint

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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

使用上のガイドライン

次に、単一の CA 証明書専用の新しいトラストポイントを作成する例を示します。

```
Device# configure terminal
Device(config)# crypto pki trustpoint <tp_name>
Device(ca-trustpoint)# enrollment terminal
Device(ca-trustpoint)# exit
Device(config)# crypto pki authenticate <tp_name>
<<< PASTE CA-CERT in PEM format followed by quit >>>
```

crypto pki trust pool import terminal

digicert.com から CA 証明書を貼り付けてルート証明書をインポートするには、**crypto pki trust pool import terminal** コマンドを使用します。

crypto pki trust pool import terminal

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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

使用上のガイドライン

次に、**digicert.com** から CA 証明書を貼り付けてルート証明書をインポートする例を示します。

```
Device# configure terminal
Device(config)# crypto pki trust pool import terminal
Device(config)# end
```

crypto pki trustpool clean

ダウンロードしたCA 証明書バンドルを消去するには、**crypto pki trustpool clean** コマンドを使用します。

crypto pki trustpool clean

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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

使用上のガイドライン

次に、ダウンロードした CA 証明書バンドルを消去する例を示します。

```
Device# configure terminal
Device(config)# crypto pki trustpool clean
Device(config)# end
```

cts inline-tagging

Cisco TrustSec（CTS）インライン タギングを設定するには、**cts inline-tagging** コマンドを使用します。

cts inline-tagging

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

インライン タグは設定されていません。

コマンド モード

ワイヤレス ポリシーの設定（config-wireless-policy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、CTS インライン タグを設定する例を示します。

```
Device(config-wireless-policy)# cts inline-tagging
```

cts role-based enforcement

Cisco TrustSec（CTS）SGACL の適用を設定するには、**cts role-based enforcement** コマンドを使用します。

cts role-based enforcement

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

SGACL は適用されません。

コマンド モード

ワイヤレス ポリシーの設定（config-wireless-policy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、CTS SGACL の適用を設定する例を示します。

```
Device(config-wireless-policy)# cts role-based enforcement
```

cts sgt

Cisco TrustSec（CTS）のデフォルトのセキュリティ グループ タグ（SGT）を設定するには、**cts sgt** コマンドを使用します。

cts sgt *sgt-value*

構文の説明

sgt-value	セキュリティ グループ タグ値。

コマンド デフォルト

SGT タグが設定されていません。

コマンド モード

ワイヤレス ポリシーの設定（config-wireless-policy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、デフォルトの SGT を設定する例を示します。

```
Device(config-wireless-policy)# cts sgt 100
```

custom-page login device

カスタマイズされたログインページを設定するには、**custom-page login device** コマンドを使用します。

custom-page login device *html-filename*

構文の説明

html-filename	ログインページのHTML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

config-params-parameter-map

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、カスタマイズされたログイン ページを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-map-name
Device(config-params-parameter-map)# custom-page login device bootflash:login.html
```

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** | **band-select** | **broadcast-ssid** | **call-snoop** | **ccx** | **channel-scan** | **parameters** | **chd** | **client** | **datalink** | **diag-channel** | **dtim** | **exclusionlist** | **ip** | **ipv6** | **load-balance** | **local-auth** | **mac-filtering** | **media-stream** | **mfp** | **mobility** | **nac** | **passive-client** | **peer-blocking** | **radio** | **roamed-voice-client** | **security** | **service-policy** | **session-timeout** | **shutdown** | **sip-cac** | **static-ip** | **uapsd** | **wgb** | **wmm**}

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 Gibraltar 16.10.1	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。

```
デバイス(config-wlan)# default ccx aironet-iesupport
```

daisychain-stp-redundancy

メッシュプロファイルで冗長ルートアクセスポイント（RAP）のイーサネットデイジーチェーン接続を有効にするには、**daisychain-stp-redundancy** コマンドを使用します。

daisychain-stp-redundancy

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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.4.1	このコマンドが導入されました。

使用上のガイドライン

次に、メッシュプロファイルで冗長 RAP のイーサネット デイジー チェーン接続を有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless profile mesh default-mesh-profile
Device(config-wireless-mesh-profile)# daisychain-stp-redundancy
Device(config-wireless-mesh-profile)# end
```

debug platform qos-acl-tcam

Quality of Service（QoS）およびアクセス コントロール リスト（ACL）のハードウェア メモリ マネージャ ソフトウェアのデバッグを有効にするには、特権EXECモードまたはユーザEXECモードで **debug platform qos-acl-tcam** 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 qos-acl-tcam {**all** | **ctcam** | **errors** | **labels** | **mask** | **rpc** | **tcam**}
no debug platform qos-acl-tcam {**all** | **ctcam** | **errors** | **labels** | **mask** | **rpc** | **tcam**}

構文の説明

all	QoS and ACL Ternary Content Addressable Memory（QATM）マネージャ デバッグ メッセージをすべて表示します。
ctcam	Cisco TCAM（CTCAM）関連イベント デバッグ メッセージを表示します。
errors	QATM エラー関連イベント デバッグ メッセージを表示します。
labels	QATM ラベル関連イベント デバッグ メッセージを表示します。
mask	QATM マスク関連イベント デバッグ メッセージを表示します。
rpc	QATM リモート プロシージャ コール（RPC）関連イベント デバッグ メッセージを表示します。
tcam	QATM ハードウェア メモリ関連イベント 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

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

undebug platform qos-acl-tcam コマンドは **no debug platform qos-acl-tcam** 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。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有効にするには、アクティブスイッチ上で **remote command** *stack-member-number LINE* EXEC コマンドを使用します。

debug platform packet-trace

条件付きデバッグ パケット トレースを有効にするには、特権またはユーザ EXEC モードで **debug platform packet-trace** 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 packet-trace {**copy** | **drop** | **inject** | **packet** | **punt** | **statistics**}
no debug platform packet-trace {**copy** | **drop** | **inject** | **packet** | **punt** | **statistics**}

構文の説明

copy	コピー パケット データを表示します。
drop	トレース ドロップのみを表示します。
inject	トレース挿入のみを表示します。
packet	パケット数を表示します。
punt	トレース パントのみを表示します。
statistics	パケット トレース統計情報を表示します。

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

ユーザ EXEC、特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

undebug platform packet-trace コマンドは **no debug platform packet-trace** コマンドと同じです。

詳細については、『**Cisco ASR 1000 Series Aggregation Services Routers**』マニュアルを参照してください。

https://www.cisco.com/c/en/us/support/docs/content-networking/adaptive-session-redundancy-asr/117858-technote-asr-00.html

debug platform hardware chassis active qfp feature wireless datapath trace-buffer debug-level

グローバルおよびフィルタリングされたロジックのデバッグレベル情報を有効にするには、**debug platform hardware chassis active qfp feature wireless datapath trace-buffer debug-level** コマンドを使用します。この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。

debug platform hardware chassis active qfp feature wireless datapath trace-buffer debug-level { **all** | **error** | **info** | **trace** | **warning** }

no debug platform hardware chassis active qfp feature wireless datapath trace-buffer debug-level { **all** | **error** | **info** | **trace** | **warning** }

構文の説明

debug platform hardware chassis active qfp feature wireless datapath trace-buffer debug-level	QFP ワイヤレスデバッグレベルを有効にします。
all	すべてのデバッグを有効にします。
error	エラーデバッグを有効にします。デバッグレベルでは、エラーがデフォルトです。
info	情報デバッグを有効にします。
trace	トレースデバッグを有効にします。
warning	警告デバッグを有効にします。

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 Bengaluru 17.6.1	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

例

次に、グローバルおよびフィルタリングされたロジックのデバッグレベル情報を有効にする例を示します。

```
Device# debug platform hardware chassis active qfp feature wireless datapath trace-buffer
 debug-level all
```

debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress filtered-trace

入力パスのフィルタリングされたトレースバッファで Quantum Flow Processor を有効にするには、**debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress filtered-trace** コマンドを使用します。この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。

debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress { **filtered-trace** { **capwap** { *ipv4* | *ipv6* | **keepalive** } | **wlclient** { **ipv6-nd** | **ipv6-ra** | **mac-address** *H.H.H* } }

no debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress { **filtered-trace** { **capwap** { *ipv4* | *ipv6* | **keepalive** } | **wlclient** { **ipv6-nd** | **ipv6-ra** | **mac-address** *H.H.H* } }

構文の説明

debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress filtered-trace	QFP ワイヤレス入力パケットのフィルタリングされたトレースを有効にします。
capwap	フィルタリングされたトレースバッファにパケット情報を記録するための CAPWAP の条件を有効にします。
wlclient	フィルタリングされたトレースバッファにパケット情報を記録するためのワイヤレスクライアントの条件を有効にします。
keepalive	すべての CAPWAP トンネルのキープアライブロギングを有効にします。
ipv4	指定した CAPWAP IPv4 アドレスのキープアライブロギングを有効にします。
ipv6	指定した CAPWAP IPv6 アドレスのキープアライブロギングを有効にします。
ipv6-nd	すべてのワイヤレスクライアントの IPv6 ネイバー探索を有効にします。
ipv6-ra	すべてのワイヤレスクライアントの IPv6 ルータアドバタイズメントを有効にします。
mac-address *H.H.H*	指定したクライアント MAC アドレスのパケットロギングを有効にします。

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 Bengaluru 17.6.1	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

例

次に、入力パスのフィルタリングされたトレースバッファで Quantum Flow Processor を有効にする例を示します。

```
Device# debug platform hardware chassis active qfp feature wireless datapath trace-buffer
 ingress filtered-trace capwap ipv4 209.165.200.224/27
```

debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress global-trace

入力パスのグローバルトレースバッファで Quantum Flow Processor を有効にするには、**debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress global-trace** コマンドを使用します。この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。

debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress global-trace

no debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress global-trace

構文の説明

debug platform hardware chassis active qfp feature wireless datapath trace-buffer ingress global-trace	QFP ワイヤレス入力パケットのグローバルトレースを有効にします。

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 Bengaluru 17.6.1	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

例

次に、入力パスのグローバルトレースバッファで Quantum Flow Processor を有効にする例を示します。

```
Device# debug platform hardware chassis active qfp feature wireless datapath trace-buffer
 ingress global-trace
```

debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace

入力パスのフィルタリングされたトレースバッファで Quantum Flow Processor を有効にするには、**debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace** コマンドを使用します。この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。

debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace { **filtered-trace** { **capwap** { *ipv4* | *ipv6* | **keepalive** } | **wlclient** { **ipv6-nd** | **ipv6-ra** | **mac-address** *H.H.H* } }

no debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace { **filtered-trace** { **capwap** { *ipv4* | *ipv6* | **keepalive** } | **wlclient** { **ipv6-nd** | **ipv6-ra** | **mac-address** *H.H.H* } }

構文の説明

debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject filtered-trace	パント/インジェクトパスでフィルタリングされたトレースバッファを有効にします。
capwap	パント/インジェクトパスでフィルタリングされたトレースバッファにパケット情報を記録するための CAPWAP の条件を有効にします。
wlclient	パント/インジェクトパスでフィルタリングされたトレースバッファにパケット情報を記録するためのワイヤレスクライアントの条件を有効にします。
keepalive	すべての CAPWAP トンネルのキープアライブロギングを有効にします。
ipv4	指定した CAPWAP IPv4 アドレスのキープアライブロギングを有効にします。
ipv6	指定した CAPWAP IPv6 アドレスのキープアライブロギングを有効にします。
ipv6-nd	すべてのワイヤレスクライアントの IPv6 ネイバー探索を有効にします。
ipv6-ra	すべてのワイヤレスクライアントの IPv6 ルータアドバタイズメントを有効にします。
mac-address *H.H.H*	指定したクライアント MAC アドレスのパケットロギングを有効にします。

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 Bengaluru 17.6.1	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

例

次に、パント/インジェクトパスのフィルタリングされたトレースバッファで Quantum Flow Processor を有効にする例を示します。

```
Device# debug platform hardware chassis active qfp feature wireless datapath trace-buffer
 punt-inject filtered-trace capwap ipv4 209.165.200.224/27
```

debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject global-trace

パント/インジェクトパスのグローバルトレースバッファで Quantum Flow Processor を有効にするには、**debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject global-trace** コマンドを使用します。この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。

debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject global-trace

no debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject global-trace

構文の説明

debug platform hardware chassis active qfp feature wireless datapath trace-buffer punt-inject global-trace	パント/インジェクトパスのグローバルトレースバッファで Quantum Flow Processor 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 Bengaluru 17.6.1	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

例

次に、パント/インジェクトパスのグローバルトレースバッファで Quantum Flow Processor を有効にする例を示します。

```
Device# debug platform hardware chassis active qfp feature wireless datapath trace-buffer
 punt-inject global-trace
```

debug qos-manager

Quality of Service（QoS）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 qos-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場合は、このコマンドの **no** 形式を使用します。

debug qos-manager {**all** | **event** | **verbose**}
no debug qos-manager {**all** | **event** | **verbose**}

構文の説明

all	すべての QoS マネージャ デバッグ メッセージを表示します。
event	QoS マネージャ関連イベント デバッグ メッセージを表示します。
verbose	QoS マネージャ詳細デバッグ 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

undebug qos-manager コマンドは **no debug qos-manager** コマンドと同じです。

debug wireless bundle client abort

ワイヤレスクライアントのデバッグバンドルの収集をキャンセルするには、**debug wireless bundle client abort** コマンドを使用します。

debug wireless bundle client abort

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 Dublin 17.9.3	このコマンドが導入されました。

使用上のガイドライン

abort コマンドは、**start** コマンドを実行してから 60 秒経たないと実行できません。**stop** コマンドの発行後に **abort** コマンドを使用することはできません。

例

次に、ワイヤレスクライアントのデバッグバンドルの収集をキャンセルする例を示します。

```
Device# debug wireless bundle client abort
```

debug wireless bundle client mac

ワイヤレス クライアント デバッグ ログが必要なクライアント MAC アドレスを追加するには、**debug wireless bundle client mac** コマンドを使用します。MAC アドレスを削除するには、このコマンドの **no** 形式を使用します。

debug wireless bundle client mac *mac-address*

no debug wireless bundle client mac *mac-address*

構文の説明

mac-address	クライアントの 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.9.3	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 32 個のクライアント MAC アドレスを指定できます。

たとえば、**debug wireless bundle client mac***F8XX.F2XX.7DXXaaaa.bbbb.cccc* とします

例

次に、ワイヤレス クライアント デバッグ ログを収集する必要があるクライアント MAC アドレスを追加する例を示します。

```
Device# debug wireless bundle client mac F8XX.F2XX.7DXX
```

debug wireless bundle client start

ワイヤレスクライアントのデバッグバンドルの収集を開始するには、**debug wireless bundle client start** コマンドを使用します。

debug wireless bundle client start { **ap-archive** [**site-tag** *site_tag* **level** { **critical** | **debug** | **error** | **verbose** }] | **epc** | **monitor-time** *monitor-time-seconds* }

debug wireless bundle client start { **epc** | **monitor-time** *monitor-time-seconds* }

構文の説明

ap-archive	サイトタグの AP アーカイブを有効にします。
site-tag *site_tag*	AP アーカイブを有効にするサイトタグ名を指定します。
level	AP アーカイブレベルを指定します。
critical	クリティカルレベルの AP アーカイブを指定します。
debug	デバッグレベルの AP アーカイブを指定します。
error	エラーレベルの AP アーカイブを指定します。
verbose	詳細レベルの AP アーカイブを指定します。
epc	コントロールプレーンでの組み込みパケットキャプチャを有効にします。
monitor-time	モニター時間をトレースする期間を指定します。デフォルトの時間範囲は 30 分です。有効な値の範囲は 1 ～ 2085978494 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 Dublin 17.9.3	このコマンドが導入されました。

例

次に、ワイヤレスクライアントのデバッグバンドルの収集を開始する例を示します。

```
Device# debug wireless bundle client start epc monitor-time 30
```

```
Device# debug wireless bundle client start ap-archive site-tag default-site-tag level debug
```

debug wireless bundle client stop-all collect

設定されているすべてのワイヤレスクライアントのデバッグバンドルの収集を停止するには、**debug wireless bundle client stop-all collect** コマンドを使用します。

debug wireless bundle client stop-all collect { **all** | **mac** *H.H.H* }

構文の説明

all	設定されているすべてのワイヤレスクライアントのデバッグバンドルを収集します。
mac	MAC アドレスが追加されたクライアントデバイスのデバッグバンドルを収集します。最大 5 つの MAC アドレスを入力できます。
H.H.H	クライアントの 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.9.3	このコマンドが導入されました。

例

次に、設定されているすべてのワイヤレスクライアントのデバッグバンドルの収集を停止する例を示します。

```
Device# debug wireless bundle client stop-all collect all
```

description

フロー モニタ、フロー エクスポータ、またはフロー レコードの説明を設定するには、該当するコンフィギュレーション モードで **description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

description *description*
no description *description*

構文の説明

description	フロー モニタ、フロー エクスポータ、またはフロー レコードを説明するテキスト文字列。

コマンド デフォルト

フロー サンプラー、フロー モニタ、フロー エクスポータ、またはフロー レコードのデフォルトの説明は「ユーザ定義」です。

コマンド モード

次のコマンド モードがサポートされています。

フロー エクスポータ コンフィギュレーション

フロー モニタ コンフィギュレーション

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドをデフォルト設定に戻すには、該当するコンフィギュレーション モードで **no description** または **default description** コマンドを使用します。

次に、フロー モニタの説明を設定する例を示します。

```
デバイス(config)# flow monitor FLOW-MONITOR-1
デバイス(config-flow-monitor)# description Monitors traffic to 172.16.0.1 255.255.0.0
```

destination

フロー エクスポータのエクスポート宛先を設定するには、フロー エクスポータ コンフィギュレーション モードで **destination** コマンドを使用します。フローエクスポータのエクスポート宛先を削除するには、このコマンドの **no** 形式を使用します。

destination {*hostnameip-address*}
no destination {*hostnameip-address*}

構文の説明

hostname	NetFlow 情報を送信するデバイスのホスト名。
ip-address	NetFlow 情報を送信するワークステーションの IPv4 アドレス。

コマンド デフォルト

エクスポート宛先は設定されていません。

コマンド モード

フロー エクスポータ 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

各フロー エクスポータには、宛先アドレスまたはホスト名を 1 つのみ指定できます。

デバイスの IP アドレスの代わりに、ホスト名を設定すると、ホスト名は直ちに解決され、IPv4 アドレスが実行コンフィギュレーションに保存されます。ドメイン ネーム システム（DNS）の最初の名前解決に使用されたホスト名と IP アドレスのマッピングが DNS サーバー上で動的に変わる場合は、device でこれが検出されないため、エクスポートされたデータは最初の IP アドレスに送信され続け、データは失われます。

このコマンドをデフォルト設定に戻すには、フローエクスポータ コンフィギュレーション モードで **no destination** または **default destination** コマンドを使用します。

次の例に、宛先システムに キャッシュ エントリをエクスポートするようにネットワーク デバイスを設定する方法を示します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)# destination 10.0.0.4
```

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)# device-role node
```

device-role（IPv6 ND インスペクション）

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 Gibraltar 16.10.1	このコマンドが導入されました。
	キーワード **monitor** および **router** は廃止されました。

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、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。

```
デバイス(config)#  ipv6 nd inspection policy policy1
デバイス(config-nd-inspection)# device-role host
```

device-tracking binding

さまざまな状態のワイヤレスクライアントの IP エントリのタイマー値を設定するには、**device-tracking binding** コマンドを使用します。設定された IP エントリのタイマー値を無効にするには、このコマンドの **no** 形式を使用します。

device-tracking binding { **down-lifetime** | **reachable-lifetime** | **stale-lifetime** } { *seconds* | **infinite** }

no device-tracking binding { **down-lifetime** | **reachable-lifetime** | **stale-lifetime** }

構文の説明

down-lifetime	IP バインディングエントリが削除されるまでの、ダウン状態である最長時間を指定します。
reachable-lifetime	IP バインディングエントリのアクティビティがないときの、到達可能状態である最長時間を指定します。
stale-lifetime	IP バインディングエントリが削除されるまでの、古い状態である最長時間を指定します。
seconds	IP エントリのタイマー値（秒単位）。有効な範囲は 1 ～ 86400 秒です。
infinite	タイマー間隔が期限切れにならないことを示します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドは、Cisco IOS XE Amsterdam 17.3.1 よりも前のリリースで導入されました。

例

次に、さまざまな状態のワイヤレスクライアントのIPエントリのタイマー値を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# device-tracking binding stale-lifetime 3
```

device-tracking binding vlan

IPv4 または IPv6 スタティック エントリを設定するには、**device-tracking binding vlan** コマンドを使用します。

device-tracking binding vlan *vlan-id*{*ipv4-addr ipv6-addr* }**interface gigabitEthernet** *ge-intf-num hardware-or-mac-address*

構文の説明

vlan-id	VLAN ID。有効な範囲は 1 ～ 4096 です。
ipv4-addr	デバイスの IPv4 アドレス。
ipv6-addr	デバイスの IPv6 アドレス。
interface gigabitEthernet	GigabitEthernet IEEE 802.3z。
ge-intf-num	GigabitEthernet インターフェイス番号。有効な範囲は 1 ～ 32 です。
hardware-or-mac-address	48 ビットのハードウェア アドレスまたはデバイスの MAC アドレス。

コマンド デフォルト

なし

コマンド モード

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、IPv4 スタティック エントリを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# device-tracking binding vlan 20 20.20.20.5 interface gigabitEthernet 1
0000.1111.2222
```

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 Gibraltar 16.10.1	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。

```
デバイス(config)# device-tracking policy policy1
デバイス(config-device-tracking)# trusted-port
```

destination-ports

コントローラと通信するための宛先ポートを設定するには、**destination-ports** コマンドを使用します。コントローラと通信するために使用する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。

destination-ports { **application-updates** | **sensor-exporter** } *port-value*

no destination-ports { **application-updates** | **sensor-exporter** }

構文の説明

application-updates	アプリケーションの更新用のTCPポートを設定します。
sensor-exporter	センサーメッセージ用の UDP ポートを設定します。
port-value	ポート値。有効な範囲は 1 ～ 65535 です。

コマンド デフォルト

宛先ポートは設定されていません。

コマンド モード

SD サービス コントローラ コンフィギュレーション（config-sd-service-controller）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが導入されました。

例

次に、コントローラと通信するための宛先ポートを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
VM1(config)# avc sd-service
Device(config-sd-service)# controller
Device(config-sd-service-controller)# destination-ports application-updates 650
```

dhcp-server

Cisco AP プロファイルの DHCP サーバを有効にするには、**dhcp-server** コマンドを使用します。

dhcp-server

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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

次に、Cisco AP プロファイルの DHCP サーバーを有効にする例を示します。

```
Device# configure terminal
Device(config)# ap profile ap-prof1
Device(config-ap-profile)# dhcp-server
```

dhcp-tlv-caching

WLAN で DHCP TLV キャッシングを設定するには、**dhcp-tlv-caching** コマンドを使用します。

dhcp-tlv-caching

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、WLAN で DHCP TLV キャッシングを設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless profile policy rr-xyz-policy-1
デバイス(config-wireless-policy)# dhcp-tlv-caching
デバイス(config-wireless-policy)# radius-profiling
デバイス(config-wireless-policy)# end
```

dns-server（IPv6）

IPv6 用ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）で使用可能なドメイン ネーム システム（DNS）IPv6 サーバを指定するには、IPv6 プール コンフィギュレーション モード用 DHCP で **dns-server** コマンドを使用します。DNS サーバー 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。

dns-server *ipv6-address*
no dns-server *ipv6-address*

構文の説明

ipv6-address	DNS サーバの IPv6 アドレス。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。

コマンド デフォルト

IPv6 用 DHCP プールが初めて作成されるとき、DNS IPv6 サーバは設定されていません。

コマンド モード

IPv6 プール コンフィギュレーションの DHCP

コマンド履歴

リリース	変更内容
12.3(4)T	このコマンドが導入されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
12.2(33)SRE	このコマンドが変更されました。Cisco IOS Release 12.2(33)SRE に統合されました。
12.2(33)XNE	このコマンドが変更されました。Cisco IOS リリース 12.2(33)XNE に統合されました。

使用上のガイドライン

このコマンドを複数回発行すると、複数のドメイン ネーム システム（DNS）サーバのアドレスを設定できます。新しいアドレスは古いアドレスを上書きしません。

例

次に、利用可能な DNS IPv6 サーバーを指定する例を示します。

```
dns-server 2001:0DB8:3000:3000::42
```

関連コマンド

コマンド	説明
domain-name	IPv6 クライアント用 DHCP のドメイン名を設定します。
ipv6 dhcp pool	DHCP for IPv6 設定情報プールを設定し、DHCP for IPv6 プール コンフィギュレーション モードを開始します。

dnscrypt

DNScrypt を有効または無効にするには、**dnscrypt** コマンドを使用します。

dnscrypt

コマンド デフォルト

なし

コマンド モード

config-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、DNScrypt オプションは有効です。

次に、DNScrypt を有効または無効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# parameter-map type umbrella global
デバイス(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166
デバイス(config-profile)# local-domain dns_wl
デバイス(config-profile)# no dnscrypt
デバイス(config-profile)# end
```

domain

802.11u ドメイン名を設定するには、**domain** コマンドを使用します。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。

domain *domain-name*

構文の説明

domain-name	802.11u ドメイン名。最大 32 個のドメイン名を設定できます。*domain-name* は 220 文字を超えないように指定する必要があります。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、802.11u ドメイン名を設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# domain my-domain
```

domain-name（DHCP）

ダイナミック ホスト コンフィギュレーションのドメイン名を指定するには、DHCP プール コンフィギュレーション モードで **domain-name** コマンドを使用します。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。

domain-name *domain*
no domain-name

構文の説明

domain	クライアントのドメイン名文字列を指定します。

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

DHCP プール設定

コマンド履歴

リリース	変更内容
12.0(1)T	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

例

次に、クライアントのドメイン名として cisco.com を指定する例を示します。

```
domain-name cisco.com
```

関連コマンド

コマンド	説明
dns-server	DHCP クライアントで利用可能な DNS IP サーバを指定します。
ip dhcp pool	Cisco IOS DHCP サーバに DHCP アドレス プールを設定し、DHCP プール コンフィギュレーション モードを開始します。

dot11 airtime-fairness

2.4 または 5 GHz 無線の airtime-fairness ポリシーを設定するには、**dot11 airtime-fairness** コマンドを使用します。

dot11 {**24ghz** | **5ghz** } **airtime-fairness** *atf-policy-name*

構文の説明

atf-policy-name	airtime-fairness ポリシーの名前です。

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、2.4 または 5 GHz 無線の airtime-fairness ポリシーを設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless profile policy <profile-name>
デバイス(config-wireless-policy)# dot11 24ghz airtime-fairness <atf-policy-name>
デバイス(config-wireless-policy)# end
```

dot11ax

WLAN で 802.11ax を設定するには、**dot11ax** コマンドを使用します。

dot11ax{ **bss-colorcode** *color-code-range* | **bss-colormode** | **bss-partialcolor** | **downlink-mumimo** | **downlink-ofdma** | **target-waketime** | **twt-broadcast-support** | **uplink-mumimo** | **uplink-ofdma** }

構文の説明

bss-colorcode	WLAN の BSS カラー コード。
color-code-range	BSS カラー コード範囲。有効な範囲は 0 ～ 255 です。
bss-colormode	WLAN の BSS カラー モード。
bss-partialcolor	WLAN の BSS パーシャル カラー モード。
downlink-mumimo	WLAN のダウンリンク MUMIMO。
downlink-ofdma	WLAN のダウンリンク OFDMA。
target-waketime	WLAN のターゲット復帰時間モード。
twt-broadcast-support	WLAN の TWT ブロードキャストのサポート。
uplink-mumimo	WLAN のアップリンク MUMIMO。
uplink-ofdma	WLAN のアップリンク OFDMA。

コマンド デフォルト

なし

コマンド モード

WLAN の設定（config-wlan）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	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 IEEE 802.11ax AP でのみサポートされます。

例

次に、WLAN で OFDMA を設定する例を示します。

```
Device(config-wlan)# dot11ax uplink-ofdma
```

dot11ax bcast-probe-response

802.11axブロードキャストプローブ応答を設定するには、**dot11ax bcast-probe-response** コマンドを使用します。この機能を無効化するには、このコマンドの **no** 形式を使用します。

dot11ax bcast-probe-response

no dot11ax bcast-probe-response

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

RF 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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、802.11ax ブロードキャストプローブ応答を設定する例を示します。

```
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# dot11ax bcast-probe-response
```

dot11ax bcast-probe-response time-interval

802.11ax ブロードキャストプローブ応答の間隔を設定するには、**dot11ax bcast-probe-response time-interval** コマンドを使用します。この機能を無効化するには、このコマンドの **no** 形式を使用します。

dot11ax bcast-probe-response time-interval *5-25*

no dot11ax bcast-probe-response time-interval *5-25*

構文の説明

5-25	ブロードキャストプローブ応答の時間間隔を指定します。

コマンド デフォルト

なし

コマンド モード

RF 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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、802.11ax ブロードキャストプローブ応答の間隔を設定する例を示します。

```
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# dot11ax bcast-probe-response time-interval 25
```

dot11ax fils-discovery

ブロードキャスト用の 802.11ax の Fast Initial Link Setup（FILS）検出フレームを設定するには、**dot11ax fils-discovery** コマンドを使用します。この機能を無効化するには、このコマンドの **no** 形式を使用します。

dot11ax fils-discovery

no dot11ax fils-discovery

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

RF 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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、ブロードキャスト用の 802.11ax の Fast Initial Link Setup（FILS）検出フレームを設定する例を示します。

```
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# dot11ax fils-discovery
```

dot11ax multi-bssid-profile

802.11ax マルチ BSSID プロファイル名を設定するには、**dot11ax multi-bssid-profile** を使用します。この機能を無効化するには、このコマンドの **no** 形式を使用します。

dot11ax multi-bssid-profile *multi-bssid-profilename*

no dot11ax multi-bssid-profile *multi-bssid-profilename*

構文の説明

multi-bssid-profilename	マルチBSSIDプロファイル名を指定します。

コマンド デフォルト

なし

コマンド モード

RF 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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、802.11ax マルチ BSSID プロファイル名を設定する例を示します。

```
Device(config)# ap dot11 6ghz rf-profile rf-profile-name
Device(config-rf-profile)# dot11ax multi-bssid-profile multi-bssid-profilename
```

dot11ax spatial-reuse obss-pd

RF プロファイル コンフィギュレーション モードで 802.11ax OBSS PD の最大を設定するには、**dot11ax spatial-reuse obss-pd** を使用します

dot11ax spatial-reuse obss-pd

no dot11ax spatial-reuse obss-pd

構文の説明

spatial-reuse obss-pd	RF プロファイル コンフィギュレーション モードで 802.11ax OBSS PD ベースの空間再利用を設定します。

コマンド デフォルト

なし

コマンド モード

RF 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 Bengaluru 17.4.1	このコマンドが導入されました。

例

次に、RF プロファイル コンフィギュレーション モードで 802.11ax OBSS PD ベースの空間再利用を設定する例を示します。

```
Device(config-rf-profile)# dot11ax spatial-reuse obss-pd
```

dot11ax spatial-reuse obss-pd non-srg-max

RF プロファイル コンフィギュレーション モードで 802.11ax 非 SRG OBSS PD の最大を設定するには、**dot11ax spatial-reuse obss-pd non-srg-max** *-82 - -62* を使用します

dot11ax spatial-reuse obss-pd non-srg-max *-82 - -62*

no dot11ax spatial-reuse obss-pd non-srg-max *-82 - -62*

構文の説明

spatial-reuse obss-pd non-srg-max	RF プロファイル コンフィギュレーション モードで 802.11ax 非 SRG OBSS PD ベースの空間再利用を設定します。
-82 - -62	非 SRG OBSS PD の最大値を dBm 単位で指定します

コマンド デフォルト

なし

コマンド モード

RF 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 Bengaluru 17.4.1	このコマンドが導入されました。

例

次に、RF プロファイル コンフィギュレーション モードで 802.11ax 非 SRG OBSS PD ベースの空間再利用を設定する例を示します。

```
Device(config-rf-profile)# dot11ax spatial-reuse obss-pd non-srg-max -80
```

dot11ax target-waketime

WLANでのターゲット起動時間モードを設定するには、**dot11ax target-waketime** コマンドを使用します。この機能を無効にするには、このコマンドの **no** コマンドを使用します。

dot11ax target-waketime

[no] dot11ax target-waketime

構文の説明

target-waketime	WLANのターゲット起動時間モードを設定します。

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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、WLAN でのターゲット起動時間を設定する例を示します。

```
Device(config-wlan)# dot11ax target-waketime
```

dot11ax twt-broadcast-support

WLAN の TWT ブロードキャストのサポートを設定するには、**dot11ax twt-broadcast-support** コマンドを使用します。この機能を無効にするには、このコマンドの **no** コマンドを使用します。

dot11ax twt-broadcast-support

[no] dot11ax twt-broadcast-support

構文の説明		
	dot11ax twt-broadcast-support	WLAN の TWT ブロードキャストのサポートを設定します

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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、WLAN でのターゲット起動時間を設定する例を示します。

```
Device(config-wlan)# dot11ax twt-broadcast-support
```

dot11 {24ghz slot0 | 5ghz {slot1 | slot2} radio-profile

802.11a または 802.11b 無線プロファイルを設定するには、**dot11** {**24ghz slot0** | **5ghz** {**slot1** | **slot2**}}**radio-profile** *radio-profile-name* コマンドを使用します。この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。

dot11 { **24ghz slot0** | **5ghz** { **slot1** | **slot2** } } **radio-profile** *radio-profile-name*

no dot11 { **24ghz slot0** | **5ghz** { **slot1** | **slot2** } } **radio-profile** *radio-profile-name*

構文の説明

dot11{**24ghz slot0** | **5ghz** {**slot1** | **slot2**}}	• **dot11**：802.11 パラメータを設定します。 • **24ghz slot0**：スロット 0 の 802.11b ポリシーを設定します。 • **5ghz**：802.11a パラメータを設定します。 • **slot1**：スロット 1 の 802.11a ポリシーを設定します。 • **slot2**：スロット 2 の 802.11a ポリシーを設定します。
radio-profile	802.11a または 802.11a 無線プロファイルを設定します。
radio-profile-name	802.11a または 802.11a 無線プロファイル名を指定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス RF タグ 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 Bengaluru 17.6.1	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

例

次に、802.11a または 802.11b 無線プロファイルを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless tag rf wireless-rf-tagname
Device(config-wireless-rf-tag)# dot11 5ghz slot1 radio-profile wireless-radio-profile
```

dot11 5ghz reporting-interval

802.11a無線でクライアントのAPから送信されるクライアント レポート間隔を設定するには、**dot11 5ghz reporting-interval** コマンドを使用します。

dot11 5ghz reporting-interval *reporting-interval*

構文の説明

reporting-interval	クライアント レポートを送信する必要がある間隔（秒単位）。

コマンド デフォルト

なし

コマンド モード

config-ap-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、クライアント レポート間隔を秒単位で設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap profile profile-name
Device(config-ap-profile)# dot11 5ghz reporting-interval 8
```

dot11 reporting-interval

ボリューム測定間隔を設定するには、**dot11 reporting-interval** コマンドを使用します。

dot11 {**24ghz** | **5ghz** } *reporting-interval*

構文の説明

reporting-interval	クライアントアカウンティング統計情報を送信する間隔。

コマンド デフォルト

デフォルト レベルの間隔は 90 秒に設定されます。

コマンド モード

config-ap-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

CLI では 5 ～ 90 秒の範囲を設定できますが、ボリューム測定には 60 ～ 90 秒の範囲を使用することをお勧めします。

また、この CLI を使用すると、スマート ローミングが有効になる間隔を設定することも使用できます。この範囲は 5 ～ 90 秒です。

ボリューム測定およびスマートローミングには2つの異なる値を設定できますが、値は実行順序に基づいて1つだけが有効になります。そのため、両方に同じレポート間隔を使用することを推奨します。

例

次に、ボリューム測定を設定する例を示します。

```
Device(config-ap-profile)# dot11 24ghz 60
```

dot1x system-auth-control

802.1X SystemAuthControl（ポートベースの認証）をグローバルに有効にするには、グローバル コンフィギュレーション モードで **dot1x system-auth-control** コマンドを使用します。SystemAuthControl を無効にするには、このコマンドの **no** 形式を使用します。

dot1x system-auth-control
no dot1x system-auth-control

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、システム認証は無効になっています。このコマンドを無効にすると、すべてのポートが強制的に許可されているかのように動作します。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.3(2)XA	このコマンドが導入されました。
12.2(14)SX	このコマンドがスーパーバイザ エンジン 720 に実装されました。
12.3(4)T	このコマンドが Cisco IOS Release 12.3(4)T に統合されました。
12.2(17d)SXB	スーパーバイザ エンジン 2 上のこのコマンドのサポートが 12.2(17d)SXB に拡張されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

使用上のガイドライン

IEEE 802.1x 標準では、認証されていないデバイスが一般的にアクセス可能なポートを介して LAN に接続することを制限する、クライアント/サーバベースのアクセス コントロールと認証プロトコルが定義されています。802.1x は、ポートごとに 2 つの個別の仮想アクセス ポイントを作成してネットワーク アクセスを制御します。一方のアクセス ポイントが未制御ポート、もう一方は制御ポートです。単一のポートを通過するすべてのトラフィックは、両方のアクセス ポイントを利用できます。802.1x は、スイッチまたは LAN が提供するサービスを利用できるようにする前に、スイッチのポートに接続されている各ユーザ デバイスを認証し、そのポートを VLAN（仮想 LAN）に割り当てます。802.1x アクセス コントロールによりデバイスが認証されるまでは、Extensible Authentication Protocol（EAP）over LAN（EAPOL）トラフィックだけしか、そのデバイスの接続ポートを通過できません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

このコマンドの **no** 形式は 802.1X 関連の設定をすべて削除します。

802.1X をグローバルに有効にする前に、認証、許可、およびアカウンティング（AAA）を有効にし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。

例

次に、SystemAuthControl を有効にする例を示します。

```
Router(config)# dot1x system-auth-control
```

関連コマンド

コマンド	説明
aaa authentication dot1x	IEEE 802.1X を実行するインターフェイスで使用する 1 つまたは複数の AAA 方式を指定します。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
debug dot1x	802.1X デバッグ情報を表示します。
description	802.1X プロファイルの説明を指定します。
device	個々のデバイスを静的に承認または拒否します。
dot1x initialize	すべての 802.1X 対応インターフェイスで 802.1X ステート マシンを初期化します。
dot1x max-req	ルータまたはイーサネット スイッチ ネットワーク モジュールは EAP 要求/ID フレームをクライアントに送信する最大回数を設定します（応答は受信されていないと仮定）。
dot1x port-control	制御ポートの認証ステートの手動制御を有効にします。
dot1x re-authenticate	手動で指定の 802.1X 対応ポートの再認証を開始します。
dot1x reauthentication	802.1X インターフェイスでクライアント PC の定期認証をグローバルに有効にします。
dot1x timeout	再試行タイムアウトを設定します。
identity profile	アイデンティティ プロファイルを作成し、アイデンティティ プロファイル コンフィギュレーション モードを開始します。
show dot1x	アイデンティティ プロファイルの詳細および統計情報を表示します。
template	コマンドの複製元となる仮想テンプレートを指定します。

dot11-tlv-accounting

クライアント 802.11 のタイプ、長さ、値（TLV）アカウンティングを設定するには、**dot11-tlv-accounting** コマンドを使用します。クライアント 802.11 の TLV 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。

dot11-tlv-accounting

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

クライアント 802.11 の TLV アカウンティングは設定されていません。

コマンド モード

ワイヤレス ポリシー コンフィギュレーション（config-wireless-policy）#

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.10.1	このコマンドが導入されました。

例

次に、クライアント 802.11 の TLV アカウンティングを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# dot11-tlv-accounting
```

dscp

Differentiated Services Code Point（DSCP）マーキングを有効にするには、**dscp** コマンドを使用します。DSCP マーキ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。

dscp *dscp-value*

no dscp

構文の説明

dscp-value	DSCP マーキング値。有効な範囲は 0 ～ 63 です。

コマンド デフォルト

DSCP マーキングは有効になっていません。

コマンド モード

SD サービス コントローラ コンフィギュレーション（config-sd-service-controller）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが導入されました。

例

次に、DSCP マーキングを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# avc sd-service
Device(config-sd-service)# controller
Device(config-sd-service-controller)# dscp 12
```

eap-method

ネットワークアクセス識別子（NAI）レルムの Extensible Authentication Protocol（EAP）方式を設定するには、**eap-method** コマンドを使用します。NAI レルムの EAP 方式を削除するには、このコマンドの **no** 形式を使用します。

eap-method {**eap-aka** | **eap-fast** | **eap-leap** | **eap-peap** | **eap-sim** | **eap-tls** | **eap-ttls**}

構文の説明

eap-aka	EAP 認証とキー共有の方式を有効にします。 EAP-AKA は、UMTS Subscriber Identity Module を使用した認証とセッションキー配布のための EAP メカニズムです。
eap-fast	セキュアトンネリング方式による EAP フレキシブル認証を有効にします。 EAP-FAST は、サプリカントとサーバーの相互認証を可能にするフレキシブル EAP プロトコルです。これは EAP-PEAP に似ていますが、通常はクライアント証明書またはサーバー証明書を使用する必要はありません。
eap-leap	EAP Lightweight Extensible Authentication Protocol 方式を有効にします。 EAP-LEAP は、主に Cisco Aironet WLAN で使用される EAP 認証プロトコルです。動的に生成された Wired Equivalent Privacy（WEP）キーを使用してデータ伝送を暗号化し、相互認証をサポートします。
eap-peap	EAP Protected Extensible Authentication Protocol 方式を有効にします。 EAP-PEAP は、ワイヤレスネットワークとポイントツーポイント接続で使用される EAP 認証プロトコルです。PEAP は、802.1X ポートアクセス制御をサポートする 802.11 WLAN でよりセキュアな認証を提供するために設計されています。
eap-sim	EAP Subscriber Identity Module 方式を有効にします。 EAP-SIM は、Global System for Mobile Communications（GSM）の Subscriber Identity Module（SIM）を使用した、認証とセッションキー配布に使用される EAP 認証プロトコルです。
eap-tls	EAP Transport Layer Security 方式を有効にします。 EAP-TLS は EAP 認証プロトコルであり、Transport Layer Security（TLS）プロトコルを使用する IETF オープン標準です。EAP-TLS は、オリジナルの標準ワイヤレス LAN EAP 認証プロトコルです。
eap-ttls	EAP Tunneled Transport Layer Security 方式を有効にします。 EAP-TTLS はシンプルな WPA2 エンタープライズ Wi-Fi 認証方式であり、長年にわたって標準システムとなっています。ユーザーがネットワークに接続する場合、デバイスはネットワークとの通信を開始し、サーバー証明書を識別することで正しいネットワークであることを確認します。

コマンド デフォルト なし

コマンド モード ANQP NAI EAP コンフィギュレーション（config-anqp-nai-eap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、EAP 方式を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless hotspot anqp-server my_anqp
Device(config-wireless-anqp-server)# nai-realm myvenue.cisco.com
Device(config-anqp-nai-eap)# eap-method eap-aka
```

eap profile

EAP プロファイルを設定するには、**eap profile** コマンドを使用します。

eap profile *profile-name*

構文の説明

profile-name	EAPプロファイルの名前。許容最大文字数は63 文字です。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、EAP プロファイル名を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# eap profile eap-profile-name
```

et-analytics

Cisco Elastic ワイヤレス LAN コントローラ（eWLC）で暗号化トラフィック分析（ETA）をグローバルに有効にするには、 **et-analytics** コマンドを使用します。

et-analytics

コマンド デフォルト

なし

コマンド モード

ET-Analytics 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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、ET 分析コンフィギュレーション モードで Cisco Elastic ワイヤレス LAN コントローラ（eWLC）で暗号化トラフィック分析（ETA）をグローバルに有効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# et-analytics
デバイス(config-et-analytics)# end
```

ethernet-vlan-transparent（メッシュ）

メッシュ AP プロファイルのイーサネット ブリッジング VLAN トランスペアレントを設定するには、**ethernet-vlan-transparent** コマンドを使用します。

ethernet-vlan-transparent

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

イーサネット ブリッジング VLAN トランスペアレントは有効になっています。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、メッシュ AP プロファイルのイーサネット ブリッジング VLAN トランスペアレントを設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# ethernet-vlan-transparent
```

ethernet-bridging（メッシュ）

メッシュ AP プロファイルのイーサネット ブリッジングを設定するには、**ethernet-bridging** コマンドを使用します。

ethernet-bridging

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

イーサネット ブリッジングは無効になっています。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、メッシュ AP プロファイルのイーサネット ブリッジングを設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# ethernet-bridging
```

event identity-update

ポリシー マップに一致基準を指定するには、**event identity-update** コマンドを使用します。

event identity-update[{**match-all** | **match-first**}]

構文の説明

match-all	すべてのクラスを評価します。
match-first	最初のクラスを評価します。

コマンド デフォルト

なし

コマンド モード

config-event-control-policymap

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、一致基準をポリシー マップに一致するすべてのクラスとして指定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# policy-map type control subscriber policy-map-name
Device(config-event-control-policymap)# event identity-update match-all
```

exclusionlist

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

ワイヤレス 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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、クライアント除外リストを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# exclusionlist timeout 5
```

exec-character-bits

EXEC コマンドおよびコンフィギュレーション コマンドの文字の文字幅を設定するには、ライン コンフィギュレーション モードで **exec-character-bits** 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。

exec-character-bits { *7* | *8* }

no exec-character-bits

構文の説明

7	7 ビット文字セットを設定します。これはデフォルトです。
8	バナーメッセージやプロンプトなどで国際文字およびグラフィック文字を使用するための、完全な 8 ビット文字セットを設定します。

コマンド デフォルト

7 ビット ASCII 文字セット。

コマンド モード

ライン 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

EXEC 文字幅を 8 に設定すると、バナーやプロンプトなどで特殊なグラフィック文字と国際文字を使用できます。ただし、EXEC 文字幅を 8 ビットに設定すると、障害が発生する可能性があります。たとえば、パリティを送信している端末のユーザーが **help** コマンドを入力すると、「unrecognized command」メッセージが表示されます。これは、システムが 8 ビットすべてを読み取っていて、**help** コマンドに 8 番目のビットは不要なためです。

例

次に、EXEC コマンドおよびコンフィギュレーション コマンドの文字の文字幅を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# line console 0
Device(config-line)# exec-character-bit 8
```

exec time-out

EXEC コマンドインタープリタがユーザー入力を検出するまで待つ時間を設定するには、ライン コンフィギュレーション モードで **exec-timeout** コマンドを使用します。タイムアウト時間を削除するには、このコマンドの **no** 形式を使用します。

exec time-out *minutes* [*seconds*]

exec time-out

構文の説明

minutes	分数を指定する整数です。デフォルトは10分です。
seconds	（任意）追加の時間間隔（秒単位）。

コマンド デフォルト

10 分

コマンド モード

ライン 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

指定した時間内に入力が検出されない場合、EXEC ファシリティは現在の接続を再開します。接続が存在しない場合、EXEC ファシリティは端末をアイドル状態に戻し、着信セッションを切断します。

タイムアウトなしを指定するには、**exec-timeout 0 0** コマンドを入力します。

例

次に、時間間隔を 2 分 30 秒に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# line console 0
Device(config-line)# exec-timeout 12 0
```

exporter default-flow-exporter

レコードのエクスポートに使用するエクスポータを追加するには、**exporter default-flow-exporter** コマンドを使用します。この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。

exporter default-flow-exporter

[no] exporter default-flow-exporter

構文の説明

このコマンドに引数はありません。

コマンド デフォルト

なし

コマンド モード

フロー モニタ 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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、レコードのエクスポートに使用するエクスポータを追加する例を示します。

```
Device(config-flow-monitor)#exporter default-flow-exporter
```

fabric control-plane

ファブリック コントロール プレーンの詳細を設定するには、**fabric control-plane** コマンドを使用します。

fabric control-plane *map-server-name*

構文の説明

map-server-name	サイト タグに関連付けられているファブリック コントロール プレーン名を参照します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

次に、ファブリック コントロール プレーンの詳細を設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless tag site default-site-tag
デバイス(config-site-tag)# fabric control-plane
map-server-name
デバイス(config-site-tag)# end
```

fast-teardown

メッシュアクセスポイント（AP）プロファイルの高速ティアダウンを有効にして、この機能のパラメータを設定するには、**fast-teardown** コマンドを使用します。

（注） メッシュ AP の高速ティアダウンは、Cisco Industrial Wireless（IW）3702 アクセスポイントではサポートされていません。

fast-teardown {enabled | interval *duration* **latency-exceeded-threshold | latency-threshold | uplink-recovery-interval** *duration* **| retries** *retry limit*

構文の説明

enabled	高速ティアダウン機能を有効にします。
interval	（任意）再試行間隔（秒単位）を設定します。有効な値の範囲は1 ～ 10 秒です。
latency-exceeded-threshold	（任意）しきい値の時間未満で少なくとも 1 つの ping が成功する必要がある遅延間隔を指定します。有効な値の範囲は 1 ～ 30 秒です。
latency-threshold	（任意）遅延しきい値を指定します。有効な値の範囲は1 ～ 500 ミリ秒です。
uplink-recovery-interval	（任意）子接続を受け入れるためにルートアクセスポイントのアップリンクが安定している必要がある時間を指定します。有効な値の範囲は 1 ～ 3600 秒です。
retries	（任意）ゲートウェイが到達不能と見なされるまでの最大試行回数を指定します。範囲は 0 ～ 10 です。

コマンド デフォルト

なし

コマンド モード

高速ティアダウン 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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、メッシュ AP プロファイルの高速ティアダウン機能を有効にして、そのパラメータを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless mesh profile mesh-profile-name
```

```
Device(config-wireless-mesh-profile)# fast-teardown
Device(config-wireless-mesh-profile-fast-teardown)# interval 1
```

fallback-radio-shut

無線インターフェイスのシャットダウンを設定するには、**fallback-radio-shut** コマンドを使用します。

fallback-radio-shut

コマンド デフォルト

なし

コマンド モード

config-wireless-flex-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、無線インターフェイスのシャットダウンを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile flex flex-profile-name
Device(config-wireless-flex-profile)# fallback-radio-shut
```

fips authorization-key

FIPS を設定するには、**fips authorization-key** コマンドを使用します。

fips authorization-key *key*

構文の説明

key	キーは32桁の16進数文字である必要があります。

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 Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

（注） アクティブ コントローラとスタンバイ コントローラの両方に同じ FIPS 認証キーが設定されていることを確認します。

次に、FIPS を設定する例を示します。

```
Device# configure terminal
Device(config)# fips authorization-key 12345678901234567890123456789012
Device(config)# end
```

flex

flex 関連のパラメータを設定するには、**flex** コマンドを使用します。

flex {**nat-pat** | **split-mac-acl** *split-mac-acl-name* | **vlan-central-switching** }

構文の説明

nat-pat	NAT-PAT を有効にします。
split-mac-acl	split-mac-acl 名を設定します。
split-mac-acl-name	スプリット MAC ACL の名前。
vlan-central-switching	VLANベースの中央集中型スイッチ。

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、flex 関連の VLAN 中央スイッチングを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy profile-name
Device(config-wireless-policy)# flex vlan-central-switching
```

flow exporter

フロー エクスポータを作成するか、既存の フロー エクスポータを変更して、 フロー エクスポータ 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 **flow exporter** コマンドを使用します。 フロー エクスポ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。

flow exporter *exporter-name*
no flow exporter *exporter-name*

構文の説明

exporter-name	作成または変更するフローエクスポータの名前。

コマンド デフォルト

フロー エクスポータは、コンフィギュレーション内には存在しません。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フローエクスポータでは、フロー モニタ キャッシュ内のデータをリモートシステム（たとえば、分析および保管のためにNetFlowコレクタを実行するサーバ）にエクスポートします。フローエクスポータは、コンフィギュレーションで別のエンティティとして作成されます。フローエクスポータは、フローモニタにデータエクスポート機能を提供するためにフローモニタに割り当てられます。複数のフローエクスポータを作成して、1 つまたは複数のフローモニタに適用すると、いくつかのエクスポート先を指定することができます。1つのフローエクスポータを作成し、いくつかのフローモニタに適用することができます。

例

次に、FLOW-EXPORTER-1 という名前のフロー エクスポータを作成し、 フロー エクスポータ 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。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)#
```

flow monitor

フローモニタを作成するか、または既存のフローモニタを変更して、フロー モニタ 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 **flow monitor** コマンドを使用します。フローモニタを削除するには、このコマンドの **no** 形式を使用します。

flow monitor *monitor-name*
no flow monitor *monitor-name*

構文の説明

monitor-name	作成または変更するフローモニタの名前。

コマンド デフォルト

フロー モニターはコンフィギュレーション内には存在しません。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フローモニターは、ネットワーク トラフィックのモニタリングを実行するためにインターフェイスに適用される コンポーネントです。フローモニタは、フローレコードとキャッシュで構成されます。フローモニタを作成した後に、フローモニタにレコードを追加します。フローモニタのキャッシュは、フローモニタが最初のインターフェイスに適用されると自動的に作成されます。フローデータは、モニタリングプロセス中にネットワークトラフィックから収集されます。このデータ収集は、フローモニタのレコード内のキーフィールドおよび非キーフィールドに基づいて実行され、フローモニタのキャッシュに保存されます。

例

次の例では、FLOW-MONITOR-1 という名前のフローモニタを作成し、フロー モニタ コンフィギュレーション モードを開始します。

```
デバイス(config)# flow monitor FLOW-MONITOR-1
デバイス(config-flow-monitor)#
```

flow record

フロー レコードを作成するか、既存のフロー レコードを変更して、フロー レコード 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 **flow record** コマンドを使用します。 レコードを削除するには、このコマンドの **no** 形式を使用します。

flow record *record-name*
no flow record *record-name*

構文の説明

record-name	作成または変更するフローレコードの名前。

コマンド デフォルト

フロー レコード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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードでは、フロー内のパケットを識別するために で使用するキーとともに、 がフローについて収集する関連フィールドを定義します。キーと関連フィールドを任意の組み合わせで指定して、フロー レコードを定義できます。は、幅広いキー セットをサポートします。フローレコードでは、フロー単位で収集するカウンタのタイプも定義します。64 ビットのパケットまたはバイトカウンタを設定できます。

例

次に、FLOW-RECORD-1 という名前のフロー レコードを作成し、 フロー レコード 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。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)#
```

full-sector-dfs（メッシュ）

メッシュ AP プロファイルのメッシュ フル セクター動的周波数選択（DFS）を設定するには、**full-sector-dfs** コマンドを使用します。

full-sector-dfs

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

フル セクター DFS は有効になっています。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、メッシュ AP プロファイルのメッシュ フル セクター DFS ステータスを設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# full-sector-dfs
```

コンフィギュレーション コマンド：g ～ z

gas-ap-rate-limit

特定の期間にアクセス ポイント（AP）によってコントローラに送信される Generic Advertisement Service（GAS）または Access Network Query Protocol（ANQP）の要求アクション フレームの数を設定するには、**gas-ap-rate-limit** コマンドを使用します。

gas-ap-rate-limit *number-of-requests request-limit-interval*

構文の説明

number-of-requests	特定の間隔で許可される GAS または ANQP 要求の数。有効な範囲は 1 ～ 100 です。
request-limit-interval	最大数の要求が適用できる間隔。有効な範囲は 100 ～ 1000 ミリ秒です。

コマンド デフォルト

制限は有効になっていません。

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、特定の期間に AP によってコントローラに送信される GAS または ANQP 要求のアクションフレームの数を設定する例を示します。

```
Device(config)# ap profile hotspot
Device(config-ap-profile)# gas-ap-rate-limit 12 120
```

geolocation ftm initiator burst-duration

AP プロファイルで AP 地理位置情報の詳細タイミング測定（FTM）イニシエータのバースト期間値を設定するには、**geolocation ftm initiator burst-duration**{**128ms** | **16ms** | **1ms** | **250us** | **2ms** | **32ms** | **4ms** | **500us** | **64ms** | **8ms**} コマンドを使用します。この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。

geolocation ftm initiator burst-duration { **128ms** | **16ms** | **1ms** | **250us** | **2ms** | **32ms** | **4ms** | **500us** | **64ms** | **8ms** }

no geolocation ftm initiator burst-duration { **128ms** | **16ms** | **1ms** | **250us** | **2ms** | **32ms** | **4ms** | **500us** | **64ms** | **8ms** }

構文の説明

128ms	バースト期間を 128 ミリ秒に設定します。
16ms	バースト期間を 16 ミリ秒に設定します。
1ms	バースト期間を 1 ミリ秒に設定します。
250us	バースト期間を250マイクロ秒に設定します。
2ms	バースト期間を 2 ミリ秒に設定します。
32ms	バースト期間を 32 ミリ秒に設定します。
4ms	バースト期間を 4 ミリ秒に設定します。
500us	バースト期間を500マイクロ秒に設定します。
64ms	バースト期間を 64 ミリ秒に設定します。
8ms	バースト期間を 8 ミリ秒に設定します。

コマンド デフォルト

デフォルト値は 32 ミリ秒です。

コマンド モード

AP プロファイル 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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、AP プロファイルで AP 地理位置情報の詳細タイミング測定（FTM）イニシエータのバースト期間値を設定する例を示します。

```
Device# configure terminal
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)#geolocation ftm initiator burst-duration 32
```

geolocation ftm initiator burst-size

AP プロファイルで AP 地理位置情報の詳細タイミング測定（FTM）イニシエータのバーストサイズ値を設定するには、**geolocation ftm initiator burst-size** *burst-size* コマンドを使用します。無効にするには、このコマンドの **no** 形式を使用します

geolocation ftm initiator burst-size *burst-size*

構文の説明

burst-size	バーストサイズを指定します。バーストサイズ値は、4、8、16、32、および64です。

コマンド デフォルト

デフォルト値は 8 です。

コマンド モード

AP プロファイル 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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、AP プロファイルで AP 地理位置情報の詳細タイミング測定（FTM）イニシエータのバーストサイズ値を設定する例を示します。

```
Device# configure terminal
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)#geolocation ftm initiator burst-size 8
```

group

施設および施設タイプのグループを設定するには、**group** コマンドを使用します。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。

group *venue-group venue-type*

構文の説明

venue-group	施設グループ。オプション：**assembly**、**business**、**educational**、**industrial**、**institutional**、**mercantile**、**outdoor**、**residential**、**storage**、**unspecified**、**utility**、**vehicular**。
venue-type	場所のタイプ。オプションは venue-group によって異なります。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、施設および施設タイプのグループを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# group business bank
```

gtk-randomize

ホール 196 緩和のためにランダム GTK を設定するには、**gtk-randomize** コマンドを使用します。アイコンを削除するには、このコマンドの **no** 形式を使用します。

gtk-randomize

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（config-wlan）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

各モバイル デバイスに使用される GTK は、BSS に関連付けられている他のモバイル デバイスに使用されるすべての GTK とは異なる必要があります。

例

次に、ホール 196 緩和のためにランダム GTK を設定する例を示します。

```
Device(config-wlan)# security wpa wpa2 gtk-randomize
```

gnxi（非セキュアモード）

gNXI は、gNMI および gNOI プロトコルを使用する、ネットワーク管理用のツールのコレクションです。その内容は次のとおりです。

- gNMI：gRPC ネットワーク管理インターフェイス
- gNOI：gRPC ネットワーク操作インターフェイス

gNMI は Google によって開発された gRPC ネットワーク管理インターフェイスです。gNMI はネットワークデバイスの設定をインストール、操作、および削除し、また、運用データの表示も実行するメカニズムです。gRPC ネットワーク操作インターフェイス（gNOI）は、ネットワークデバイス上で操作コマンドを実行するための gRPC ベースのマイクロサービスセットを定義します。

非セキュアモードで gNXI プロセスを設定して開始するには、**gnxi** コマンドを使用します。この機能を無効化するには、このコマンドの **no** 形式を使用します。

gnxi {port *port-number* **| secure-client-auth | seure-init | secure-password-auth | secure-peer-verify-trustpoint | secure-port | secure-server | secure-trustpoint | server}**

no gnxi {port *port-number* **| secure-client-auth | seure-init | secure-password-auth | secure-peer-verify-trustpoint | secure-port | secure-server | secure-trustpoint | server}**

構文の説明

gnxi	gNXI プロセスを開始します
port	gNXI サーバーポートを設定します
port-number	ポート番号を指定します。デフォルトのポート番号は 50052 です。
secure-client-auth	クライアント認証を使用して gNXI を設定します
secure-init	プライマリ自己署名証明書を使用して gNMI セキュアサーバーを有効にします
secure-password-auth	パスワード認証を使用して gNXI を設定します
secure-peer-verify-trustpoint	gNXI サーバーピア検証トラストポイントを設定します
secure-port	gNXI セキュアサーバーポートを設定します
secure-server	gNXI セキュアサーバーを有効にします
secure-trustpoint	gNXI サーバー証明書トラストポイントを設定します
server	gNXI サーバーを有効にします

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、gNIX サーバー（非セキュアモード）を設定する例を示します。

```
Device# configure terminal
Device(config)# gnxi server
Device(config)# end
```

gnxi（セキュアモード）

gNXI は、gNMI および gNOI プロトコルを使用する、ネットワーク管理用のツールのコレクションです。その内容は次のとおりです。

- gNMI：gRPC ネットワーク管理インターフェイス
- gNOI：gRPC ネットワーク操作インターフェイス

gNMI は Google によって開発された gRPC ネットワーク管理インターフェイスです。gNMI はネットワークデバイスの設定をインストール、操作、および削除し、また、運用データの表示も実行するメカニズムです。gRPC ネットワーク操作インターフェイス（gNOI）は、ネットワークデバイス上で操作コマンドを実行するための gRPC ベースのマイクロサービスセットを定義します。

セキュアモードで gNXI プロセスを設定して開始するには、**gnxi** コマンドを使用します。この機能を無効化するには、このコマンドの **no** 形式を使用します。

gnxi {secure-server | secure-trustpoint *trustpoint-name* **| secure-client-auth | secure-port}**

no gnxi {secure-server | secure-trustpoint *trustpoint-name* **| secure-client-auth | secure-port}**

構文の説明

gnxi	gNXI プロセスを開始します
secure-server	gNXI セキュアサーバーを有効にします
secure-trustpoint	gNXI サーバー証明書トラストポイントを設定します
trustpoint-name	トラストポイント名を指定します
secure-client-auth	クライアント認証を使用して gNXI を設定します
secure-port	gNXI セキュアサーバーポートを設定します

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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、セキュアモードで gNIX サーバーとセキュアトラストポイントを設定する例を示します。

```
Device# configure terminal
```

```
Device(config)# gnxi secure-trustpoint <trustpoint-name>
Device(config)# end
```

hessid

同種の拡張サービス セットを設定するには、**hessid** コマンドを使用します。サービスセットを削除するには、このコマンドの **no** 形式を使用します。

hessid *HESSID-value*

構文の説明

HESSID-value	HESSID 値。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、同種の拡張サービスセットを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# hessid 00:40:96:b4:82:55
```

high-density clients count

AP無線ごとのクライアント接続の最大数を設定するには、RFプロファイルモードで**high-density clients count** コマンドを使用します。この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。

high-density clients count *max-client-conn-per-radio*

[no] high-density clients count *max-client-conn-per-radio*

構文の説明

max-client-conn-per-radio	AP 無線あたりの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。デフォルト値は 200 クライアント接続です。

コマンド デフォルト

なし

コマンド モード

RF 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 Cupertino 17.8.1	このコマンドが導入されました。

例

次に、AP 無線あたりのクライアント接続の最大数を設定する例を示します。

```
Device(config)# ap dot11 5ghz rf-profile rfprofile
Device(config-rf-profile)# high-density clients count 30
```

hotspot anqp-server

ホットスポットサーバーをポリシープロファイルに関連付けるには、**hotspot anqp-server** コマンドを使用します。サー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。

hotspot anqp-server *server-name*

構文の説明

server-name	Hotspot 2.0 ANQP サーバーの名前。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ポリシーの設定（config-wireless-policy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、Hotspot 2.0 ANQP サーバーを設定する例を示します。

```
Device(config)# wireless profile policy hs-policy
Device(config-wireless-policy)# hotspot anqp-server test
```

hyperlocation

AP グループのハイパーロケーションと関連するパラメータを設定するには、WLAN AP グループ コンフィギュレーション（Device(config-apgroup)#）モードで **hyperlocation** コマンドを使用します。AP グループのハイパーロケーションと関連する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。

[no] hyperlocation ［**threshold** ｛**detection** *value-in-dBm* ｜ **reset** *value-btwn-0-99* ｜ **trigger** *value-btwn-1-100*｝］

構文の説明

[no] hyperlocation	AP グループのハイパーロケーションを有効または無効にします。
threshold detection *value-in-dBm*	低い RSSI を持つパケットを除外するためのしきい値を設定します。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。
threshold reset *value-btwn-0-99*	トリガー後のスキャンサイクルの値をリセットします。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。
threshold trigger *value-btwn-1-100*	BAR をクライアントに送信する前のスキャンサイクルの数を設定します。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。 （注） ハイパーロケーションしきい値のリセット値は、必ず、しきい値のトリガー値より小さくします。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

- 次に、パケットをフィルタするためのしきい値を低い RSSI に設定する例を示します。

```
Device(config-apgroup)# [no] hyperlocation threshold detection -100
```

- 次に、トリガー後にスキャン サイクルの値をリセットする例を示します。

```
Device(config-apgroup)# [no] hyperlocation threshold reset 8
```

- 次に、BAR をクライアントに送信する前にスキャンサイクルの数を設定する例を示します。

```
Device(config-apgroup)# [no] hyperlocation threshold trigger 10
```

icon

オンラインサインアップ（OSU）プロバイダーのアイコンを設定するには、**icon** コマンドを使用します。アイコンを削除するには、このコマンドの **no** 形式を使用します。

icon *file-name*

構文の説明

file-name	アイコンのファイル名。

コマンド デフォルト

なし

コマンド モード

ANQP OSU プロバイダーの設定（config-anqp-osu-provider）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

アイコンは、ホットスポット ANQP サーバで設定する必要があります。

例

次に、OSU プロバイダーのアイコンを設定する例を示します。

```
Device(config-wireless-anqp-server)# osu-provider my-osu
Device(config-anqp-osu-provider)# icon test
```

icap subscription client anomaly-detection report-individual enable aggregate

クライアント サブスクリプションの異常検出を設定し、個々のレポート集約を有効にするには、**icap subscription client anomaly-detection report-individual enable aggregate** コマンドを使用します。

icap subscription client anomaly-detection report-individual enable aggregate

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

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.12.1	このコマンドが導入されました。

例

次に、クライアント サブスクリプションの異常検出を設定し、個々のレポート集約を有効にする例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# icap subscription client anomaly-detection report-individual
 enable aggregate
```

icap subscription client anomaly-detection report-individual per-client throttle

AP で 5 分ごとにクライアント別の個別レポートを設定するには、**icap subscription client anomaly-detection report-individual per-client throttle** コマンドを使用します。

icap subscription client anomaly-detection report-individual per-client throttle *throttle value*

構文の説明

throttle value	クライアントごとのイベントレポートの数。有効な値の範囲は 0 ～ 50 です。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.12.1	このコマンドが導入されました。

例

次に、AP で 5 分ごとにクライアント別の個別レポートを設定する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# icap subscription client anomaly-detection report-individual
 per-client throttle 10
```

icap subscription client anomaly-detection report-individual per-type throttle

AP で 5 分ごとにタイプ別の個別レポートを設定するには、**icap subscription client anomaly-detection report-individual per-type throttle** コマンドを使用します。

icap subscription client anomaly-detection report-individual per-type throttle *throttle value*

構文の説明

throttle value	クライアントごとのイベントレポートの数。有効な値の範囲は 0 ～ 100 です。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.12.1	このコマンドが導入されました。

例

次に、AP で 5 分ごとにタイプ別の個別レポートを設定する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# icap subscription client anomaly-detection report-individual
 per-type throttle 80
```

icap subscription client exclude telemetry-data wlan

AP で iCAP フィルタリングを有効にするには、**icap subscription client exclude telemetry-data wlan** コマンドを使用します。

icap subscription client exclude telemetry-data wlan *wlan-profile-name*

構文の説明

wlan-profile-name	WLANプロ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

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 Dublin 17.10.1	このコマンドが導入されました。

次に、AP で iCAP フィルタリングを有効にする例を示します。

```
Device# configure terminal
Device(config)# ap profile xyz-ap-profile
Device(config-ap-profile)# description "xyz ap profile"
Device(config-ap-profile)# icap subscription client exclude telemetry-data wlan wlan-name
```

idle-timeout

ワイヤレス プロファイル ポリシーの idle-timeout 値を秒単位で設定するには、 **idle-timeout** コマンドを使用します。

idle-timeout *value*

構文の説明

value	idle-timeout 値を設定します。有効な範囲は 15 ～ 100000 秒です。

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス プロファイル ポリシーの idle-timeout を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-profile-name
Device(config-wireless-policy)# idle-timeout 100
```

ids（メッシュ）

屋外メッシュ AP の IDS（不正/シグネチャ検出）レポートを設定するには、**ids** コマンドを使用します。

ids

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

IDS は無効になっています。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、屋外メッシュ AP の IDS（不正/シグニチャ検出）レポートを設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# ids
```

inactive-timeout

in-active タイマーを有効にするには、**inactive-timeout** コマンドを使用します。

inactive-timeout *timeout-in-seconds*

構文の説明

timeout-in-seconds	非アクティブ フローのタイムアウト値を指定します。値の範囲は1～604800です。

コマンド デフォルト

なし

コマンド モード

ET-Analytics 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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、ET-Analytics コンフィギュレーション モードで非アクティブタイマーを有効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# et-analytics
デバイス(config-et-analytics)# inactive-timeout 15
デバイス(config-et-analytics)# end
```

inner-auth-eap

内部認証の Extensible Authentication Protocol（EAP）方式を設定するには、**inner-auth-eap** コマンドを使用します。内部認証の EAP 方式を削除するには、このコマンドの **no** 形式を使用します。

inner-auth-eap {**eap-aka** | **eap-fast** | **eap-leap** | **eap-peap** | **eap-sim** | **eap-tls** | **eap-ttls**}

構文の説明

eap-aka	EAP 認証とキー共有の方式を有効にします。 EAP-AKA は、UMTS Subscriber Identity Module を使用した認証とセッションキー配布のための EAP メカニズムです。
eap-fast	セキュアトンネリング方式による EAP フレキシブル認証を有効にします。 EAP-FAST は、サプリカントとサーバーの相互認証を可能にするフレキシブル EAP プロトコルです。これは EAP-PEAP に似ていますが、通常はクライアント証明書またはサーバー証明書を使用する必要はありません。
eap-leap	EAP Lightweight Extensible Authentication Protocol 方式を有効にします。 EAP-LEAP は、主に Cisco Aironet WLAN で使用される EAP 認証プロトコルです。動的に生成された Wired Equivalent Privacy（WEP）キーを使用してデータ伝送を暗号化し、相互認証をサポートします。
eap-peap	EAP Protected Extensible Authentication Protocol 方式を有効にします。 EAP-PEAP は、ワイヤレスネットワークとポイントツーポイント接続で使用される EAP 認証プロトコルです。PEAP は、802.1X ポートアクセス制御をサポートする 802.11 WLAN でよりセキュアな認証を提供するために設計されています。
eap-sim	EAP Subscriber Identity Module 方式を有効にします。 EAP-SIM は、Global System for Mobile Communications（GSM）の Subscriber Identity Module（SIM）を使用した、認証とセッションキー配布に使用される EAP 認証プロトコルです。
eap-tls	EAP Transport Layer Security 方式を有効にします。 EAP-TLS は EAP 認証プロトコルであり、Transport Layer Security（TLS）プロトコルを使用する IETF オープン標準です。EAP-TLS は、オリジナルの標準ワイヤレス LAN EAP 認証プロトコルです。
eap-ttls	EAP Tunneled Transport Layer Security 方式を有効にします。 EAP-TTLS はシンプルな WPA2 エンタープライズ Wi-Fi 認証方式であり、長年にわたって標準システムとなっています。ユーザーがネットワークに接続する場合、デバイスはネットワークとの通信を開始し、サーバー証明書を識別することで正しいネットワークであることを確認します。

コマンド デフォルト

なし

コマンド モード

ANQP NAI EAP 認証コンフィギュレーション（config-anqp-nai-eap-auth）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドは、Cisco IOS XE Amsterdam 17.3.1 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

Cisco IOS XE Amsterdam 17.3.1 より前では、1 つの内部 EAP 認証方式のみが許可されていました。たとえば、**inner-auth-eap eap-aka** です。複数の内部 EAP 認証方式（**inner-auth-eap eap-aka** と **inner-auth-eap eap-fast** など）を使用した場合は、最後の方式のみが使用され、前の方式は破棄されていました。Cisco IOS XE Amsterdam 17.3.1 以降では、複数の内部 EAP 認証方式を設定できます。例については、以下のコードスニペットを参照してください。

```
wireless hotspot anqp-server my_anqp
nai-realm myvenue.cisco.com
eap-method eap-aka
credential certificate
credential usim
inner-auth-eap eap-aka
inner-auth-eap eap-fast
inner-auth-non-eap chap
inner-auth-non-eap pap
tunneled-eap-credential anonymous
tunneled-eap-credential softoken
```

例

次に、内部認証の EAP 方式を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless hotspot anqp-server my_anqp
Device(config-wireless-anqp-server)# nai-realm myvenue.cisco.com
Device(config-anqp-nai-eap)# eap-method eap-aka
Device(config-anqp-nai-eap-auth)#inner-auth-eap eap-aka
```

inner-auth-non-eap

内部認証の Extensible Authentication Protocol（EAP）以外の方式を設定するには、**inner-auth-non-eap** コマンドを使用します。内部認証の EAP 以外の方式を削除するには、このコマンドの **no** 形式を使用します。

inner-auth-non-eap {**chap** | **mschap** | **mschap-v2** | **pap**}

構文の説明

chap	チャレンジハンドシェイク認証プロトコル方式。 CHAP は、リモートクライアントのアイデンティティを検証するために Point-to-Point Protocol（PPP）サーバーで使用される認証スキームです。CHAP は 3 ウェイハンドシェイクを使用して定期的にクライアントのアイデンティティを確認します。
mschap	Microsoft チャレンジハンドシェイク認証プロトコル方式。
mschap-v2	Microsoft チャレンジハンドシェイク認証プロトコルバージョン 2 方式。
pap	パスワード認証プロトコル方式。 PAP は、ユーザーを検証するために PPP で使用されるパスワードベースの認証プロトコルです。

コマンド デフォルト

なし

コマンド モード

ANQP NAI EAP 認証コンフィギュレーション（config-anqp-nai-eap-auth）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、内部認証の EAP 以外の方式を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless hotspot anqp-server my_anqp
Device(config-wireless-anqp-server)# nai-realm myvenue.cisco.com
Device(config-anqp-nai-eap)# eap-method eap-aka
Device(config-anqp-nai-eap-auth)#inner-auth-eap pap
```

install abort

進行中の事前ダウンロードまたはローリングアクセスポイント（AP）のアップグレード操作をキャンセルするには、**install abort** コマンドを使用します。

install abort

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、現在の事前ダウンロードまたはインストール操作をキャンセルする例を示します。

```
Device# install abort
```

install add file activate commit

インストール済みSMUパッケージをアクティブ化し、ロードパスの変更をコミットするには、**install add file activate commit** コマンドを使用します。

install add file activate commit

構文の説明

prompt-level	プロンプトレベルを設定します。
none	プロンプトは実行されません。

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、インストール済みパッケージをアクティブ化し、変更をコミットする例を示します。

```
Device# install add file vwlc_apsp_16.11.1.0_74.bin activate commit
```

install add file flash activate issu commit

issu 技術を使用してインストールされたパッケージをアクティブ化し、ロードパスの変更をコミットするには、**install add file flash activate issu commit** コマンドを使用します。

install add file flash activate issu commit

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、issu 技術を使用してインストールされたパッケージをアクティブ化し、ロードパスの変更をコミットする例を示します。

```
Device# install add file flash activate issu commit
```

install add profile

AP イメージ事前ダウンロード サポートを使用して AP イメージをロールバックするためのプロファイルを選択するには、**install add profile** コマンドを使用します。

install add profile *profile-name* [**activate**]

構文の説明

profile-name	プロファイル名。プロファイル名は最大 15 文字です。
activate	インストール済みパッケージをアクティブ化します。

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 Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、APイメージをロールバックするためのプロファイルを選択する例を示します。

```
Device# install add profile profile1
```

install activate

インストール済みパッケージをアクティブ化するには、**install activate** コマンドを使用します。

install activate {**auto-abort-timer** | **file** | **profile** | **prompt-level**}

構文の説明

auto-abort-timer	キャンセルタイマーを設定します。時間範囲は 30 ～ 1200 分です。
file	アクティブにするパッケージを指定します。
profile	アクティブにするプロファイルを指定します。
prompt-level	プロンプト レベルを設定します。

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 Gibraltar 16.12.2s	このコマンドが導入されました。

例

次に、インストール済みパッケージをアクティブ化する例を示します。

```
Device# install activate profile default
install_activate: START Thu Nov 24 20:14:53 UTC 2019

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q] y
Building configuration...
[OK]Modified configuration has been saved
Jan 24 20:15:02.745: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 activate
Jan 24 20:15:02.745 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 activate
install_activate: Activating PACKAGE
```

install activate profile

インストール済みパッケージをアクティブ化するには、**install activate profile** コマンドを使用します。

install activate profile

構文の説明	**profile** プロファイルをアクティブにします。
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 Gibraltar 16.12.2s	このコマンドが導入されました。

例

次に、インストール済みパッケージをアクティブ化する例を示します。

```
Device#install activate profile default
install_activate: START Thu Nov 24 20:14:53 UTC 2019

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q] y
Building configuration...
[OK]Modified configuration has been saved
Jan 24 20:15:02.745: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 activate
Jan 24 20:15:02.745 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 activate
install_activate: Activating PACKAGE
```

install activate file

インストール済みパッケージをアクティブ化するには、**install activate file** コマンドを使用します。

install activate file *file-name*

構文の説明

file-name	パッケージ名を指定します。オプションは、bootflash:、flash:、および webui: 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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、スタンバイロケーションでインストールパッケージをアクティブ化しているときに自動キャンセルタイマーを使用する例を示します。

```
Device# install activate file vwlc_apsp_16.11.1.0_74.bin
```

install commit

ロードパスの変更をコミットするには、**install commit** コマンドを使用します。

install commit

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、ロードパスの変更をコミットする例を示します。

```
Device# install commit
```

install remove profile default

削除するインストールパッケージを指定するには、**install remove profile default** コマンドを使用します。

install remove profile default

構文の説明		
	remove	インストールパッケージを削除します。
	profile	削除するプロファイルを指定します。

コマンド デフォルト　なし

コマンド モード　特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、デフォルトプロファイルを削除する例を示します。

```
Device# install remove profile default
```

install deactivate

非アクティブ化するインストール パッケージを指定するには、**install deactivate file** コマンドを使用します。

install deactivate file *file-name*

構文の説明

file-name	パッケージ名を指定します。オプションは、bootflash:、flash:、および webui: 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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、インストールパッケージを非アクティブ化する例を示します。

```
Device# install deactivate file vwlc_apsp_16.11.1.0_74.bin
```

install deactivate

非アクティブ化するインストール パッケージを指定するには、**install deactivate file** コマンドを使用します。

install deactivate file *file-name*

構文の説明

file-name	パッケージ名を指定します。オプションは、bootflash:、flash:、および webui: 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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、インストールパッケージを非アクティブ化する例を示します。

```
Device# install deactivate file vwlc_apsp_16.11.1.0_74.bin
```

install prepare

操作をキャンセル、アクティブ化、または非アクティブ化するための SMU パッケージを準備するには、**install prepare** コマンドを使用します。

install prepare {**abort** | **activate file** *file-name* | **deactivate file** *file-name* }

構文の説明

abort	操作のキャンセル用の SMU パッケージを準備します。
activate file	アクティベーション用のSMUパッケージを準備します。
file-name	パッケージ名。
deactivate file	非アクティブ化用の SMU パッケージを準備します。

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、操作のキャンセル、アクティブ化、または非アクティブ化のためのパッケージを準備する例を示します。

```
Device# install prepare abort
Device# install prepare activate file vwlc_apsp_16.11.1.0_74.bin
Device# install prepare deactivate file vwlc_apsp_16.11.1.0_74.bin
```

install prepare rollback

ロールバック操作用の SMU パッケージを準備するには、**install prepare rollback** コマンドを使用します。

install prepare rollback to {**base** | **committed** | **id** *id* | **label** *label*}

構文の説明

base	ベース イメージへのロールバックを準備します。
committed	最後にコミットされたインストレーション ポイントへのロールバックを準備します。
id	最後にコミットされたインストレーション ポイントへのロールバックを準備します。
id	ロールバック先のインストール ポイントの識別子。
label	特定のインストール ポイント ラベルへのロールバックを準備します。
label	最大 15 文字のラベル名。

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、特定の id にロールバックするためのパッケージを準備する例を示します。

```
Device# install prepare rollback to id 2
```

install rollback

特定のインストール ポイントにロールバックするには、**install rollback** コマンドを使用します。

install rollback to {**base** | **committed** | **id** *id* | **label** *label*} [**prompt-level none**]

構文の説明

base	ベース イメージにロールバックします。
prompt-level none	プロンプト レベルをなしに設定します。
committed	最後にコミットされたインストレーション ポイントにロールバックします。
id	特定のインストール ポイント ID にロールバックします。
label	特定のインストール ポイント ラベルにロールバックします。

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、ロールバック先のインストール ポイントの ID を指定する例を示します。

```
Device# install rollback to id 1
```

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

シャーシまたはシャーシ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。

```
デバイス(config)# interface vlan 23
デバイス(config-if)#
```

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、**ip access-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 Gibraltar 16.10.1	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。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#wlan wlan1
デバイス(config-wlan)#ip access-group test-acl
```

次に、IPv4 WLAN Web ACL を設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wlan wlan1
デバイス(config-wlan)# ip access-group web test
デバイス(config-wlan)#
```

ip access-list extended

拡張アクセス リストを設定するには、**ip access-list extended** コマンドを使用します。

ip access-list extended {**<100-199>** | **<2000-2699>** *access-list-name*}

構文の説明

<100-199>	拡張 IP アクセス リスト番号。
<2000-2699>	拡張 IP アクセス リスト番号（拡張範囲）。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、拡張アクセス リストを作成する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip access-list extended access-list-name
```

ip address

インターフェイスのプライマリまたはセカンダリ IP アドレスを設定するには、インターフェイス コンフィギュレーション モードで **ip address** コマンドを使用します。IP アドレスを削除するか、IP 処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。

ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
no ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

構文の説明

ip-address	IP アドレス。
mask	関連する IP サブネットのマスク。
secondary	（任意）設定されたアドレスをセカンダリ IP アドレスに指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。 （注） セカンダリ アドレスが **vrf** のキーワードでの VRF テーブルの設定に使用される場合には、**vrf** キーワードも指定する必要があります。
vrf	（任意）VRF テーブルの名前*vrf-name* 引数は、入力インターフェイスの VRF 名を指定します。

コマンド デフォルト

IP アドレスはインターフェイスに定義されません。

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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

インターフェイスには、1 つのプライマリ IP アドレスと複数のセカンダリ IP アドレスを設定できます。Cisco IOS ソフトウェアにより生成されるパケットは、必ずプライマリ IP アドレスを使用します。そのため、セグメントのすべてのデバイスとアクセス サーバは、同じプライマリ ネットワーク番号を共有する必要があります。

ホストは、Internet Control Message Protocol（ICMP）マスク要求メッセージを使用して、サブネット マスクを判別できます。デバイスは、ICMP マスク応答メッセージでこの要求に応答できます。

no ip address コマンドを使用して IP アドレスを削除することにより、特定のインターフェイス上の IP 処理を無効にできます。ソフトウェアが、その IP アドレスのいずれかを使用する別のホストを検出すると、コンソールにエラー メッセージを出力します。

オプションの **secondary** キーワードを使用すると、セカンダリ アドレスを無制限に指定できます。システムがセカンダリの送信元アドレスのルーティングの更新以外にデータグラムを生成

しないということを除けば、セカンダリ アドレスはプライマリ アドレスのように処理されます。IP ブロードキャストおよび Address Resolution Protocol（ARP）要求は、IP ルーティング テーブルのインターフェイス ルートのように、正しく処理されます。

セカンダリ IP アドレスは、さまざまな状況で使用できます。次に、一般的な使用状況を示します。

- 特定のネットワーク セグメントに十分なホストアドレスがない場合。たとえば、サブネット化により、論理サブネットあたり最大 254 のホストを使用できますが、1 つの物理サブネットでは、300 のホストアドレスが必要になります。デバイスまたはアクセス サーバでセカンダリ IP アドレスを使用すると、2 つの論理サブネットで 1 つの物理サブネットを使用できます。
- レベル 2 ブリッジを使用して構築された旧式ネットワークがたくさんある場合。セカンダリ アドレスは、慎重に使用することで、サブネット化されたデバイスベース ネットワークへの移行に役立ちます。旧式のブリッジセグメントのデバイスでは、そのセグメントに複数のサブネットがあることを簡単に認識させることができます。
- 1 つのネットワークの 2 つのサブネットは、別の方法で、別のネットワークにより分離できる場合があります。サブネットが使用中の場合、この状況は許可されません。このような場合、最初のネットワークは、セカンダリ アドレスを使用している 2 番目のネットワークの上に拡張されます。つまり、上の階層となります。

（注）

- ネットワーク セグメント上のすべてのデバイスがセカンダリ アドレスを使用した場合、同一のセグメント上にある他のデバイスも、同一のネットワークまたはサブネットからセカンダリ アドレスを使用しなければなりません。ネットワーク セグメント上のセカンダリ アドレスの使用に矛盾があると、ただちにルーティング ループが引き起こされる可能性があります。
- Open Shortest Path First（OSPF）アルゴリズムを使用してルーティングする場合は、インターフェイスのすべてのセカンダリ アドレスがプライマリ アドレスと同じ OSPF エリアにあることを確認してください。
- セカンダリ IP アドレスを設定する場合は、CPU 使用率が高くならないように、**no ip redirects** コマンドを入力して ICMP リダイレクトメッセージの送信を無効にする必要があります。

例

次の例では、192.108.1.27 が プライマリ アドレスで、192.31.7.17 が GigabitEthernet インターフェイス 1/0/1 のセカンダリ アドレスです。

```
Device# enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 192.108.1.27 255.255.255.0
Device(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
```

関連コマンド

コマンド	説明
match ip route-source	送信元 IP アドレスを、VRF で接続されたルートに基づいて設定された必要なルート マップに一致するように指定します。
route-map	1 つのルーティング プロトコルから他のルーティング プロトコルへのルートを再配布するか、またはポリシー ルーティングを有効にするための条件を定義します。
set vrf	ポリシーベース ルーティング VRF の選択のために、ルート マップ内で VPN VRF 選択を有効にします。
show ip arp	SLIP アドレスが固定 ARP テーブル エントリとして表示される ARP キャッシュを表示します。
show ip interface	IP 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。
show route-map	静的ルートマップと動的ルートマップを表示します。

ip arp-limit rate

Address Resolution Protocol（ARP）パケットのレート制限を設定するには、**ip arp-limit rate** コマンドを使用します。

ip arp-limit rate { **burst-interval** *burst-interval* | **none** | **pps** *pps* }

構文の説明

pps	1 秒あたりにクライアントに許可される ARP パケットの最大数。クライアントごとに受信したパケットが設定された制限を超えると、パケットがドロップされます。有効な値の範囲は 15 ～ 1500 で、デフォルト値は 100 秒です。
burst-interval	クライアントを除外するためのバースト間隔（秒単位）。ARP pps が設定された値を超えると、クライアントがブロックリストに登録されます。有効な値の範囲は 3 ～ 255 で、デフォルト値は 5 秒です。
none	ARP レート制限を無効にします。

コマンド デフォルト

デフォルト値が設定されています。

コマンド モード

ワイヤレス ポリシー プロファイル コンフィギュレーション（config-wireless-policy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.5	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、Cisco IOS XE Amsterdam 17.3.5 以降、Cisco IOS XE Bengaluru 17.6.3 以降、および Cisco IOS XE Cupertino 17.8.1 以降のリリースでのみ使用できます。

RLAN の場合、デフォルト値が使用されます。このコマンドを使用して値を変更することはできません。

例

次に、ARP パケットのレート制限を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile policy test1
Device(config-wireless-policy)# ip arp-limit rate pps 90
```

ip admission

Web 認証を有効にするには、インターフェイス コンフィギュレーション モードで **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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

ip admission コマンドはスイッチポートに web 認証ルールを適用します。

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。

```
デバイス# configure terminal
デバイス(config)# interface gigabitethernet1/0/1
デバイス(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。

```
デバイス# configure terminal
デバイス(config)# fallback profile profile1
デバイス(config-fallback-profile)# ip admission rule1
```

ip dhcp pool

DHCP サーバで Dynamic Host Configuration Protocol（DHCP）アドレス プールを設定し、DHCP プール 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 **ip dhcp pool** コマンドを使用します。アドレス プ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。

ip dhcp pool *name*
no ip dhcp pool *name*

構文の説明

name	プールの名前象徴的な文字列（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

DHCP アドレス プール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
12.0(1)T	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

このコマンドの実行中、コンフィギュレーション モードが DHCP プール コンフィギュレーション モードに変わります。これは (config-dhcp)# プロンプトで識別されます。このモードでは、管理者は IP サブネット番号やデフォルト ルータ リストなどのプール パラメータを設定できます。

例

次の例では、DHCP アドレス プールとして pool1 を設定しています。

```
ip dhcp pool pool1
```

関連コマンド

コマンド	説明
host	DHCP クライアントに手動でバインドするための IP アドレスおよびネットワーク マスクを指定します。
ip dhcp excluded-address	Cisco IOS DHCP サーバーが DHCP クライアントに割り当ててはいけない IP アドレスを指定します。

コマンド	説明
network (DHCP)	Cisco IOS DHCP サーバの DHCP アドレス プールに、サブネットの番号およびマスクを設定します。

ip dhcp-relay information option server-override

Dynamic Host Configuration Protocol（DHCP）サーバに転送された BOOTREQUEST メッセージの DHCP リレー エージェント情報オプションに、サーバ ID オーバーライドとリンク選択のサブオプションをシステムがグローバルに挿入できるようにするには、グローバル コンフィギュレーション モードで **ip dhcp-relay information option server-override** コマンドを使用します。DHCP リレー エージェント情報オプションへのサーバ ID オーバーライドとリンク選択のサブオプションの挿入を無効にするには、このコマンドの **no** 形式を使用します。

ip dhcp-relay information option server-override
no ip dhcp-relay information option server-override

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

サーバー ID オーバーライドとリンク選択のサブオプションは、DHCP リレー エージェント情報オプションには挿入されません。

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 Release 2.1	このコマンドが、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

ip dhcp-relay information option server-override コマンドは、DHCP ブロードキャストがクライアントから DHCP サーバにリレー エージェントによって転送された場合、リレー エージェント情報オプションに次のサブオプションを追加します。

- サーバー ID オーバーライド サブオプション
- リンク選択サブオプション

このコマンドが設定されている場合、ゲートウェイ アドレス（giaddr）は DHCP サーバから到達可能なインターフェイスである発信インターフェイスの IP アドレスに設定されます。

ip dhcp relay information option server-id-override コマンドがインターフェイスで設定されている場合、このインターフェイスのグローバル設定のみが上書きされます。

例

次の例では、DHCP リレーによって、DHCP パケットのリレー情報オプションに、サーバー ID のオーバーライドとリンク選択サブオプションが挿入されます。ループバックインターフェイスの IP アドレスが、中継されたメッセージの送信元 IP アドレスになるように設定されます。

```
Device(config)# ip dhcp-relay information option server-override
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface Loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

関連コマンド

コマンド	説明
ip dhcp relay information option server-id-override	DHCP サーバーに転送される BOOTREQUEST メッセージの DHCP リレー エージェント情報オプションに、サーバー ID オーバーライドとリンク選択のサブオプションをシステムが特定のインターフェイスで挿入できるようにします。

ip dhcp-relay source-interface

中継されたメッセージの送信元 IP アドレスを使用するようにリレー エージェントの送信元インターフェイスをグローバルに設定するには、グローバル コンフィギュレーション モードで **ip dhcp-relay source-interface** コマンドを使用します。送信元インターフェイス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。

ip dhcp-relay source-interface *type number*
no ip dhcp-relay source-interface *type number*

構文の説明

type	インターフェイス タイプ。詳細については、疑問符（?）オンライン ヘルプ機能を使用します。
number	インターフェイスまたはサブインターフェイスの番号。ネットワーキング デバイスに対する番号付けシステムの詳細については、疑問符（?）のオンライン ヘルプ機能を使用してください。

コマンド デフォルト

送信元インターフェイ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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

使用上のガイドライン

ip dhcp-relay source-interface コマンドにより、ネットワーク管理者は中継されたメッセージの安定した、ハードウェアに依存しない IP アドレス（ループバック インターフェイスなど）を指定し、送信元 IP アドレスとしてリレー エージェントを使用することができます。

ip dhcp-relay source-interface グローバル コンフィギュレーション コマンドは設定され、**ip dhcp relay source-interface** コマンドも設定されている場合、**ip dhcp relay source-interface** コマンドはグローバル コンフィギュレーション モードよりも優先されます。ただし、インターフェイス コンフィギュレーションがないインターフェイスにはグローバル コンフィギュレーションが適用されます。

例

次の例では、ループバック インターフェイスの IP アドレスが、中継されたメッセージの送信元 IP アドレスになるように設定されています。

```
Device(config)# ip dhcp-relay source-interface loopback 0
```

```
Device(config)# interface loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

関連コマンド

コマンド	説明
ip dhcp relay source-interface	中継されたメッセージの送信元 IP アドレスとして使用するように、リレー エージェントの送信元インターフェイスを設定します。

ip dhcp compatibility suboption

サーバーオーバーライドおよびリンク選択のサブオプションを RFC またはシスコ固有の値に設定するには、**ip dhcp compatibility suboption** [**server-override** | **link-selection**] コマンドを使用します。

ip dhcp compatibility suboption server-override [cisco | standard]
ip dhcp compatibility suboption link-selection [cisco | standard]

構文の説明

server-override	サーバー オーバーライド サブオプションを RFC またはシスコ固有の値に設定します。
link-selection	link-selection サブオプションを RFC またはシスコ固有の値に設定します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.4.1	このコマンドが導入されました。

使用上のガイドライン

次に、サーバーオーバーライドにより DHCP オプション 82 を設定する例を示します。

```
Device# configure terminal
Device(config)# ip dhcp compatibility suboption server-override cisco
Device(config)# ip dhcp compatibility suboption link-selection cisco
Device(config)# end
```

ip domain lookup

IP ドメインネームシステム（DNS）ベースのホスト名からアドレスへの変換を有効にするには、グローバル コンフィギュレーション モードで **ip domain lookup** コマンドを使用します。DNS ベースのホスト名からアドレスへの変換を無効にするには、このコマンドの **no** 形式を使用します。

ip domain lookup [**nsap** | **recursive** | **source-interface** *interface-type-number* | **vrf** *vrf-name* { **source-interface** *interface-type-number* }]

構文の説明

nsap	（任意）Connectionless Network Service（CLNS）および Network Service Access Point（NSAP）のアドレスの IP DNS クエリを有効にします。
recursive	（任意）IP DNS 再帰ルックアップを有効にします。
source-interface *interface-type-number*	（任意）DNS リゾルバの送信元インターフェイスを指定します。インターフェイスのタイプと番号を入力します。
vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）テーブルを定義します。vrf-name には、VRF テーブルの名前を入力します。

コマンド デフォルト

IP DNS ベースでのホスト名からアドレスへの変換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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Dublin 17.12.1	レイヤ 3 物理インターフェイスでの **ip domain lookup source-interface** *interface-type-number* コマンドの設定に関連する問題が解決されました。 このリリース以降、レイヤ 3 物理インターフェイスで設定されている場合でも、リロードされた場合およびポートモードが変更された場合にこのコマンドが保持されます。

使用上のガイドライン

デバイスでこのコマンドが有効になっている場合、**show tcp brief** コマンドを実行すると、出力の表示が非常に遅くなることがあります。

デバイスで IP と ISO CLNS の両方が有効になっている場合、**ip domain lookup nsap** コマンドでは、ホスト名を指定していれば、完全な CLNS アドレスを指定しなくても CLNS アドレスを検出できます。

このコマンドは、**ping**（ISO CLNS）コマンドおよび CLNS Telnet 接続に役立ちます。

レイヤ 3 物理インターフェイスで **ip domain lookup source-interface** *interface-type-number* コマンドを設定する場合は、ポートモードが変更された場合、またはデバイスがリロードされた場合、このコマンドが実行コンフィギュレーションから自動的に削除されることに注意してください（これが発生した場合は、**show running-configuration** 特権 EXEC コマンドの出力を参照してください）。コマンドが削除されると、指定された送信元インターフェイスを使用する DNS クエリがドロップされます。これは、コマンドを再設定することでのみ回避できます。Cisco IOS XE Dublin 17.12.1 以降では、この問題は解決されています。

例

次に、IP DNS ベースのホスト名からアドレスへの変換を設定する例を示します。

```
Device# configure terminal
Device(config)# ip domain lookup
Device(config)# end
```

次に、DNS ドメインルックアップの送信元インターフェイスを設定する例を示します。

```
Device# configure terminal
Device(config)# ip domain lookup source-interface gigabitethernet1/0/2
Device(config)# end
```

ip domain-name

デバイスでホスト ドメインを設定するには、**ip domain-name** コマンドを使用します。

ip domain-name *domain-name*[**vrf** *vrf-name*]

構文の説明

domain-name	デフォルト ドメイン名。
vrf-name	ドメイン名の解決に使用される VRF 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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、デバイスでホスト ドメインを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip domain-name domain-name
```

ip flow-export destination

ETA フロー エクスポートの宛先を設定するには、**ip flow-export destination** コマンドを使用します。

ip flow-export destination *ip_address port_number*

構文の説明

port_number	ポート番号。有効な範囲は 1 ～ 65535 です。

コマンド デフォルト

なし

コマンド モード

ET-Analytics 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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、ET 分析コンフィギュレーション モードで ETA フロー エクスポートの宛先を設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# et-analytics
デバイス(config-et-analytics)# ip flow-export
destination 120.0.0.1 2055
デバイス(config-et-analytics)# end
```

ip helper-address

インターフェイスで受信したユーザデータグラムプロトコル（UDP）ブロードキャスト（ブーツストラップ プロトコル（BOOTP）を含む）の転送を有効にするには、インターフェイス コンフィギュレーション モードで **ip helper-address** コマンドを使用します。特定のアドレスへのブロードキャスト パケットの転送を無効にするには、このコマンドの **no** 形式を使用します。

ip helper-address[{**vrf** *name* | **global**}] *address* {[**redundancy** *vrg-name*]}
no ip helper-address [{**vrf** *name* | **global**}] *address* {[**redundancy** *vrg-name*]}

構文の説明

vrf *name*	（任意）VPN ルーティング、フォワーディング（VRF）インスタンス、および VRF 名を有効にします。
global	（任意）グローバル ルーティング テーブルを設定します。
address	UDP ブロードキャストの転送時に使用される宛先ブロードキャストまたはホスト アドレス。インターフェイスごとに複数のヘルパー アドレスを使用できます。
redundancy *vrg-name*	（任意）仮想ルータ グループ（VRG）の名前を定義します。

コマンド デフォルト

UDP ブロードキャストは転送されません。

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（config-if）

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。
12.2(4)B	このコマンドが変更されました。**vrf** *name* キーワードと引数のペアおよび **global** キーワードが追加されました。
12.2(15)T	このコマンドが変更されました。**redundancy** *vrg-name* キーワードと引数のペアが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

ip forward-protocol コマンドと **ip helper-address** コマンドを使用すると、転送されたブロードキャスト パケットおよびプロトコルを制御できます。

ヘルパー アドレスを必要とする 1 つのコモン アプリケーションは、RFC 1531 で定義されている DHCP です。クライアント セットで BOOTP または DHCP ブロードキャスト転送を有効にするには、クライアントに接続されたルータ インターフェイスでヘルパー アドレスを設定します。ヘルパー アドレスは、BOOTP または DHCP サーバのアドレスを指定する必要があります。複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定します。

UDP または IP パケットで **ip helper-address** コマンドを使用できるようにするには、次の条件を満たす必要があります。

- 受信したフレームの MAC アドレスは、すべてが 1 のブロードキャスト アドレス（ffff.ffff.ffff）である必要があります。
- IP の宛先アドレスは、すべてが 1 のブロードキャスト（255.255.255.255）または受信インターフェイスのサブネット ブロードキャストであるか、あるいは **no ip classless** コマンドも設定されている場合には受信インターフェイスのメジャーネットブロードキャストである必要があります。
- IP の存続可能時間（TTL）値は 2 以上である必要があります。
- IP プロトコルは UDP（17）である必要があります。
- UDP 宛先ポートは、TFTP、ドメイン ネーム システム（DNS）、時間、NetBIOS、ND、BOOTP や DHCP パケット、またはグローバル コンフィギュレーション モードで **ip forward-protocol udp** コマンドによって指定された UDP ポート用である必要があります。

DHCP サーバが VPN または VPN とは異なるグローバル空間に存在する場合は、**vrf** *name* または **global** オプションを使用すると、VRF の名前または DHCP サーバが存在するグローバル空間を指定できます。

ip helper-addressvrf*name address* オプションは、着信インターフェイスの VRF に関係なく、VRF 名に関連付けられているアドレスを使用します。**ip helper-addressvrf***name address* コマンドが設定された後に、VRF が設定から削除されると、この VRF に関連付けられたすべての IP ヘルパー アドレスがインターフェイス コンフィギュレーションから削除されます。

ip helper-address *address* コマンドが、VRF 名が設定されていないインターフェイスですでに設定され、このインターフェイスが **ip helper-address vrf** *name address* コマンドを使用して設定されている場合、以前に設定した **ip helper-address** *address* コマンドはグローバルと見なされます。

（注） ルータはパケットが物理ブロードキャストなのかを判断できないため、**ip helper-address** コマンドは宛先ルータの X.25 インターフェイスでは機能しません。

IP ヘルパー ステートメントが DHCP と連携できるようにするには、ルータで **service dhcp** コマンドを設定する必要があります。このコマンドが設定されていない場合、DHCPパケットは IP ヘルパー ステートメントを介してリレーされません。**service dhcp** コマンドはデフォルトで設定されます。

例

次に、ヘルパー アドレスとして機能するアドレスを定義する例を示します。

```
Router(config)# interface ethernet 1
Router(config-if)# ip helper-address 10.24.43.2
```

次に、ヘルパー アドレスとして機能するアドレスを定義し、host1 という名前の VRF と関連付ける例を示します。

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip helper-address vrf host1 10.25.44.2
```

次に、ヘルパーアドレスとして機能するアドレスを定義し、group1 という名前の VRG と関連付ける例を示します。

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip helper-address 10.25.45.2 redundancy group1
```

関連コマンド

コマンド	説明
ip forward-protocol	ブロードキャスト パケットを転送するとき、ルータによって転送されるプロトコルおよびポートを指定します。
service dhcp	ルータ上の DHCP サーバー機能およびリレー エージェント機能を有効にします。

ip http client secure-ciphersuite

クライアントからリモートサーバーへのセキュアHTTP接続での暗号化に使用する暗号スイ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**ip http client secure-ciphersuite**コマンドを使用します。以前に設定したクライアントの暗号スイートの指定を削除するには、このコマンドの **no** 形式を使用します。

ip http client secure-ciphersuite [**3des-ede-cbc-sha**] [**rc4-128-sha**] [**rc4-128-md5**] [**des-cbc-sha**]
no ip http client secure-ciphersuite

構文の説明

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA：メッセージの暗号化に 3DES と DES-EDE3-CBC、およびメッセージダイジェストにセキュア ハッシュ アルゴリズム（SHA）を使用した Rivest、Shamir、および Adleman（RSA）のキー交換。
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA：メッセージの暗号化に RC4 128 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA キー交換（RSA 公開キー暗号化）。
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5：メッセージの暗号化に RC4 128 ビット暗号化、およびメッセージダイジェストに Message Digest 5（MD5）を使用した RSA キー交換（RSA 公開キー暗号化）。
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA：メッセージの暗号化に DES-CBC、メッセージダイジェストに SHA を使用した RSA キー交換。

コマンド デフォルト

クライアントとサーバーは、使用可能な暗号スイートのリストから、両方がサポートしている最適な暗号スイートをネゴシエートします。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE 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

このコマンドを使用すると、クライアントがセキュアHTTPサーバーに接続する際に提供する暗号スイート（暗号化アルゴリズム）のリストを制限できます。たとえば、最も安全な CipherSuite の使用のみを許可したい場合に、このコマンドを使用します。

ある CipherSuite を指定する理由がない場合、またはこれらの CipherSuite の詳細を熟知していない場合はこのコマンドを未設定のままにして、サーバとクライアント間で双方がサポートしている CipherSuite をネゴシエートさせます（これがデフォルトです）。このコマンドの **no** 形式は、使用可能な暗号スイートのリストをデフォルトに戻します（つまり、デバイスでサポートされているすべての暗号スイートをネゴシエーションに使用できます）。

例

次に、SSL_RSA_WITH_3DES_EDE_CBC_SHA 暗号スイートのみを使用するように HTTPS クライアントを設定する例を示します。

```
Router(config)# ip http client secure-ciphersuite 3des-ede-cbc-sha
```

ip http secure-ciphersuite

リモートクライアントとの接続をネゴシエートするときにセキュアHTTPサーバーによって使用される暗号スイ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 **ip http secure-ciphersuite** コマンドを使用します。設定をデフォルトセットの暗号スイートに戻すには、このコマンドの **no** 形式を使用します。

ip http secure-ciphersuite [**3des-ede-cbc-sha**] [**rc4-128-sha**] [**rc4-128-md5**] [**des-cbc-sha**]
no ip http secure-ciphersuite

構文の説明

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA：メッセージの暗号化に 3DES と DES-EDE3-CBC、およびメッセージダイジェストにセキュア ハッシュ アルゴリズム（SHA）を使用した Rivest、Shamir、および Adleman（RSA）のキー交換。
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA：メッセージの暗号化に RC4 128 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA キー交換（RSA 公開キー暗号化）。
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5：メッセージの暗号化に RC4 128 ビット暗号化、およびメッセージダイジェストに Message Digest 5（MD5）を使用した RSA キー交換（RSA 公開キー暗号化）。
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA：メッセージの暗号化に DES-CBC、メッセージダイジェストに SHA を使用した RSA キー交換。

コマンド デフォルト

HTTPSサーバーは、接続するクライアントから受信したリストを使用して、最適な暗号スイートをネゴシエートします。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE 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

このコマンドは、HTTPS 接続上の暗号化で使用する暗号スイート（暗号化アルゴリズム）のリストを制限するために使用されます。たとえば、最も安全な CipherSuite の使用のみを許可したい場合に、このコマンドを使用します。

ある CipherSuite を指定する理由がない場合、またはこれらの CipherSuite の詳細を熟知していない場合はこのコマンドを未設定のままにして、サーバとクライアント間で双方がサポートしている CipherSuite をネゴシエートさせます（これがデフォルトです）。

サポートされる暗号スイートは、Cisco IOS ソフトウェアイメージによって異なります。たとえば、“IP Sec56”（“k8”）イメージは、Cisco IOS リリース 12.2(15)T の SSL_RSA_WITH_DES_CBC_SHA の暗号スイートのみをサポートしています。

ルータの処理負荷（速度）に関しては、処理速度の速いものから順に並べたリストを示します（セキュリティが強固で複雑な CipherSuite になるほど、わずかながら処理時間が必要になります）。

1. SSL_RSA_WITH_DES_CBC_SHA
2. SSL_RSA_WITH_RC4_128_MD5
3. SSL_RSA_WITH_RC4_128_SHA
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA

これらの暗号スイートに関する追加情報は、セキュアソケットレイヤ（SSL）3.0 プロトコルに関して文書化した情報源からオンラインで入手できます。

例

次に、接続しているセキュア Web クライアントに提供される暗号スイートを制限する例を示します。

```
Router(config)# ip http secure-ciphersuite rc4-128-sha rc4-128-md5
```

ip http secure-server

セキュア HTTP（HTTPS）サーバーを有効にするには、グローバル コンフィギュレーション モードで **ip http secure-server** コマンドを入力します。HTTPS サーバ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。

ip http secure-server
no ip http secure-server

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

HTTPS サーバー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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

HTTPS サーバーは、セキュア ソケット レイヤ（SSL）バージョン 3.0 プロトコルを使用します。

⚠

注意 HTTPS サーバーをイネーブルにする場合は、同じサービスに対するセキュリティ保護されていない接続を防ぐため、常に標準 HTTP サーバーをディセーブルに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 モードで **no ip http server** コマンドを使用して標準 HTTP サーバーを無効にします（この手順は予防手段であり、通常、HTTP サーバーはデフォルトで無効になっています）。

認証に認証局（CA）が使用されている場合は、HTTPS サーバーをイネーブルにする前にルーティング デバイスで CA トラストポイントを宣言する必要があります。

HTTP/TCP ポート 8090 を閉じるには、HTTP と HTTPS の両方のサーバーを無効にする必要があります。**no http server** と **no http secure-server** コマンドをそれぞれ入力します。

例

次の例では、HTTPS サーバーが有効で、（以前に設定された）CA トラストポイント CA-trust-local が指定されています。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#ip http secure-server
デバイス(config)#ip http secure-trustpoint CA-trust-local
デバイス(config)#end

デバイス#show ip http server secure status
HTTP secure server status: Enabled
```

```
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
```

関連コマンド

コマンド	説明
ip http secure-trustpoint	HTTPS サーバーの署名付き証明書を取得するために使用する CA トラストポイントを指定します。
ip http server	シスコの Web ブラウザ ユーザー インターフェイスを含む IP または IPv6 システムで HTTP サーバーを有効にします。
show ip http server secure status	HTTPS サーバーの設定ステータスを表示します。

ip http server

Cisco Web ブラウザのユーザー インターフェイスを含む、IP または IPv6 システム上で HTTP サーバーを有効にするには、グローバル コンフィギュレーション モードで **ip http server** コマンドを入力します。HTTP サーバ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。

ip http server
no ip http server

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

HTTP サーバーは、デフォルトにより標準のポート 80 を使用します。

HTTP/TCP ポート 8090 はデフォルトにより開いています。

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 Gibraltar 16.10.1	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、HTTP サーバーへの IPv4 と IPv6 の両方のアクセスを有効にします。ただし、**ip http access-class** コマンドで設定されたアクセス リストは、IPv4 トラフィックにのみ適用されます。IPv6 トラフィック フィルタリングはサポートされていません。

⚠

注意 標準 HTTP サーバーとセキュア HTTP（HTTPS）サーバーは、同時にシステム上で実行できます。**ip http secure-server** コマンドを使用して HTTPS サーバーを有効にする場合は、**no ip http server** コマンドを使用して標準 HTTP サーバーを無効にし、標準 HTTP 接続を介してセキュアデータにアクセスできないようにします。

HTTP/TCP ポート 8090 を閉じるには、HTTP と HTTPS の両方のサーバーを無効にする必要があります。**no http server** と **no http secure-server** コマンドをそれぞれ入力します。

例

次に、IPv4 と IPV6 の両方のシステムで HTTP サーバーをイネーブルにする例を示します。

HTTP サーバーを有効にした後は、使用する HTML ファイルの場所を指定して基本パスを設定できます。通常、HTTP Web サーバーで使用される HTML ファイルは、システムのフラッシュ メモリに格納されます。リモート URL はこのコマンドを使用して指定できますが、リモート パス名（たとえば、HTML ファイルがリモート TFTP サーバー上にある場合など）の使用は推奨されません。

```
デバイス(config)#ip http server
デバイス(config)#ip http path flash:
```

関連コマンド

コマンド	説明
ip http access-class	HTTP サーバーへのアクセスを制限する際に使用するアクセス リストを指定します。
ip http path	HTTPサーバーが使用するファイルを見つけるために使用する基本パスを指定します。
ip http secure-server	HTTPS サーバーをイネーブルにします。

ip igmp snooping

device で Internet Group Management Protocol（IGMP; インターネットグループ管理プロトコル）スヌーピングをグローバルにイネーブルにするか、または VLAN 単位でイネーブルにするには、device スタックまたはスタンドアロン device で **ip igmp 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。

ip igmp snooping ［**vlan** *vlan-id*］
no ip igmp snooping ［**vlan** *vlan-id*］

構文の説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングをイネーブルにします。範囲は 1 ～ 1001 および 1006 ～ 4094 です。

コマンド デフォルト

device 上で、IGMP スヌーピングはグローバルに有効になっています。

VLAN インターフェイス上で、IGMP スヌーピングはイネーブルです。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

IGMP スヌーピングがグローバルにイネーブルである場合は、すべての既存 VLAN インターフェイスでイネーブルになります。IGMP スヌーピングがグローバルにディセーブルである場合、すべての既存VLANインターフェイスでIGMPスヌーピングがディセーブルになります。

VLAN ID 1002 ～ 1005 は、トークンリングおよびFDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

例

次の例では、IGMP スヌーピングをグローバルにイネーブルにする方法を示します。

```
デバイス(config)# ip igmp snooping
```

次の例では、IGMP スヌーピングを VLAN 1 でイネーブルにする方法を示します。

```
デバイス(config)# ip igmp snooping vlan 1
```

設定を確認するには、特権 EXEC モードで **show ip igmp snooping** コマンドを入力します。

ip mac-binding

デバイスの ip-mac バインディングを設定するには、**ip mac-binding** コマンドを使用します。デバイスの ip-mac バインデ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

[no] ip mac-binding

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

IP MAC バインディングが有効になっています。

コマンド モード

ワイヤレス ポリシーの設定（config-wireless-policy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.4.1	このコマンドが導入されました。

使用上のガイドライン

（背後にある有線クライアントに対して dot11 アソシエーションを実行しない）シスコ以外の WGB デバイスが Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに接続されている場合、WGB の背後にある有線クライアントが IP アドレスを取得しないことがあります。このような場合は、ポリシープロファイルで **no ip mac-binding** および **ipv4 dhcp required** コマンドを実行します。**ipv4 dhcp required** コマンドは、WGB デバイスが DHCP を実行して IP アドレスを取得するようにします。また、クライアント VLAN でパッシブクライアント機能と ARP ブロードキャストも有効にする必要があります。

WGB と有線クライアントがスタティック IP アドレスで設定されている場合、WGB から受信したデータは転送されません。WGB で DHCP を有効にすることを推奨します（有線クライアントでの DHCP の有効化は任意です）。

設定例を次に示します。

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# ipv4 dhcp required
Device(config-wireless-policy)# no ip mac-binding
Device(config-wireless-policy)# passive-client
Device(config-wireless-policy)# exit
Device(config)# vlan configuration 1
Device(config-vlan)# arp broadcast
```

例

次に、ip-mac バインディングを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# [no] ip mac-binding
```

ip multicast vlan

単一の VLAN に IP マルチキャストを設定するには、グローバル コンフィギュレーション モードで **ip multicast vlan** コマンドを使用します。WLAN 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。

ip multicast vlan {*vlan-name vlan-id*}
no ip multicast vlan{*vlan-name vlan-id*}

構文の説明

vlan-name	VLAN 名を指定します。
vlan-id	VLAN ID 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

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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、vlan_id01 をマルチキャスト VLAN として設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless multicast
デバイス(config)# wlan test-wlan 1
デバイス(config-wlan)# ip multicast vlan vlan_id01
```

ip nbar protocol-discovery

NBAR2 エンジンを有効にする際にワイヤレス ポリシーでアプリケーション認識を設定するには、 **ip nbar protocol-discovery** コマンドを使用します。

ip nbar protocol-discovery

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス ポリシーでアプリケーション認識を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy profile-policy-name
Device(config-wireless-policy)# ip nbar protocol-discovery
```

ip nbar protocol-pack

ブートフラッシュからプロトコル パックをロードするには、**ip nbar protocol-pack** コマンドを使用します。

ip nbar protocol-pack bootflash:[{**force**}]

構文の説明

bootflash:	ブートフラッシュからプロトコル パックをロードします。
force	選択したソースからロードプロトコルパックを強制的にロードします。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ブートフラッシュから NBAR2 プロトコル パックをロードする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip nbar protocol-pack bootflash:
```

ip overlap

Flex 展開でクライアント IP アドレスの重複を有効にするには、**ip overlap** コマンドを使用します。

（注） デフォルトでは、この設定は無効になっています。

ip overlap

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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.4.1	このコマンドが導入されました。

使用上のガイドライン

次に、Flex 展開でクライアント IP アドレスの重複を有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless profile flex flex1
Device(config-wireless-flex-profile)# [no] ip overlap
```

ip ssh

ルータでセキュア シェル（SSH）制御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**ip ssh** 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。

ip ssh [{**timeout** *seconds* | **authentication-retries** *integer*}]
no ip ssh [{**timeout** *seconds* | **authentication-retries** *integer*}]

構文の説明

timeout	（任意）ルータが SSH クライアントの応答を待つ時間間隔。 この設定は、SSH ネゴシエーション フェーズに適用されます。EXEC セッションが開始すると、vty に設定された標準のタイムアウトが適用されます。デフォルトで、5 個の vty（0 ～ 4）が定義されているため、5 個のターミナル セッションが可能です。SSH でシェルが実行されると、vty タイムアウトが始動します。vty タイムアウトのデフォルトは 10 分です。
seconds	（任意）タイムアウトが切断されるまでの秒数（最大 120 秒）。デフォルトは 120 秒です。
authentication- retries	（任意）インターフェイスがリセットされるまでの試行回数。
integer	（任意）認証の再試行回数（最大 5 回）。デフォルトは 3 です。

コマンド デフォルト

SSH 制御パラメータはデフォルトのルータ値に設定されます。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.0(5)S	このコマンドが導入されました。
12.1(1)T	このコマンドが Cisco IOS Release 12.1(1) T に統合されました。
12.2(17a)SX	このコマンドは Cisco IOS リリース 12.2(17a)SX に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS リリース 12(33)SRA に統合されました。
Cisco IOS XE リリース 2.4	このコマンドが、Cisco ASR 1000 シリーズ ルータで実装されました。

使用上のガイドライン

ルータで SSH を設定するには、 **crypto key generate rsa** コマンドを使用して SSH サーバーを有効にする必要があります。

例

次に、ルータで SSH コントロール パラメータを設定する例を示します。

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

ip ssh version

ルータ上で実行するセキュア シェル（SSH）のバージョンを指定するには、グローバル コンフィギュレーション モードで **ip ssh version** コマンドを使用します。設定されている SSH のバージョンを無効にして互換モードに戻るには、このコマンドの **no** 形式を使用します。

ip ssh version [{**1** | **2**}]
no ip ssh version [{**1** | **2**}]

構文の説明

1	（任意）ルータは SSH バージョン 1 のみを実行します。
2	（任意）ルータは SSH バージョン 2 のみを実行します。

コマンド デフォルト

このコマンドが設定されていない場合、SSH は互換性モードで動作します。つまり、バージョン 1 とバージョン 2 の両方がサポートされます。

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
12.3(4)T	このコマンドが導入されました。
12.3(2)XE	このコマンドが、Cisco IOS Release 12.3(2)XE に統合されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。
12.3(7)JA	このコマンドが Cisco IOS Release 12.3(7)JA に統合されました。
12.0(32)SY	このコマンドが、Cisco IOS Release 12.0(32)SY に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。
15.2(2)SA2	このコマンドが Cisco ME 2600X シリーズ イーサネット アクセス スイッチに実装されました。

使用上のガイドライン

このコマンドを **2** キーワードとともに使用すると、ルータが誤って脆弱な SSH バージョン 1 接続を確立しないようにすることができます。

例

次の例では、SSH バージョン 1 のサポートのみが設定されていることを示します。

```
Router (config)# ip ssh version 1
```

次の例では、SSH バージョン 2 のみが設定されていることを示します。

```
Router (config)# ip ssh version 2
```

次の例では、SSH バージョン 1 および 2 が設定されていることを示します。

```
Router (config)# no ip ssh version
```

関連コマンド

コマンド	説明
debug ip ssh	SSH のデバッグ メッセージを表示します。
disconnect ssh	ルータ上で SSH 接続を終了します。
ip ssh	ルータで SSH コントロール パラメータを設定します。
ip ssh rsa keypair-name	SSH 接続を使用する際に使用する RSA キー ペアを指定します。
show ip ssh	ルータの SSH 接続を表示します。

ip tftp blocksize

TFTP クライアントのブロックサイズを指定するには、**ip tftp blocksize** コマンドを使用します。

ip tftp blocksize *blocksize-value*

構文の説明

blocksize-value	ブロックサイズ値。有効な範囲は512 ～ 8192 Kbps です。

コマンド デフォルト

TFTP クライアントのブロックサイズが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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

このコマンドを使用すると、デフォルトのブロックサイズを変更し、イメージのダウンロード時間を短縮します。

例

次に、TFTP クライアントのブロックサイズを指定する例を示します。

```
Device(config)# ip tftp blocksize 512
```

ip verify source

インターフェイス上の IP ソース ガードを有効にするには、インターフェイス コンフィギュレーション モードで **ip verify source** コマンドを使用します。IP ソース ガ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。

ip verify source
no ip verify source

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

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。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip verify source
```

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。

ipv4-address-type

802.11u IPv4 アドレスタイプを設定するには、**ipv4-address-type** コマンドを使用します。アドレスタイプを削除するには、このコマンドの **no** 形式を使用します。

ipv4-address-type
{**double-nated-private** | **not-available** | **not-known** | **port-restricted** | **port-restricted-double-nated** | **port-restricted-single-nated** | **public** | **single-nated-private**}

構文の説明

double-nated-private	IPv4アドレスをダブルネットワークアドレス変換（NAT）プライベートとして設定します。
not-available	IPv4 アドレスタイプを使用不可として設定します。
not-known	IPv4 アドレスタイプの可用性を不明として設定します。
port-restricted	IPv4 アドレスタイプをポート制限として設定します。
port-restricted-double-nated	IPv4 アドレスタイプをポート制限およびダブル NAT として設定します。
port-restricted-single-nated	IPv4 アドレスタイプをポート制限およびシングル NAT として設定します。
public	IPv4 アドレスタイプをパブリックとして設定します。
single-nated-private	IPv4アドレスをシングルNATプライベートとして設定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、802.11u IPv4 アドレスタイプを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# ipv4-address-type public
```

ipv4 arp-proxy

プロキシ ARP を有効にするには、**ipv4 arp-proxy** コマンドを使用します。プロキシ ARP を無効にするには、このコマンドの **no** 形式を使用します。

ipv4 arp-proxy

no ipv4 arp-proxy

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

ARP プロキシは有効になっていません。

コマンド モード

ワイヤレス ポリシーの設定（config-wireless-policy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

使用上のガイドライン

プロキシ ARP は、中央スイッチングモードでのみ適用されます。

例

次に、プロキシ ARP を有効にする例を示します。

```
Device(config-wireless-policy)#ipv4 arp-proxy
```

ipv4 dhcp

WLAN の DHCP パラメータを設定するには、**ipv4 dhcp** コマンドを使用します。

ipv4 dhcp {**opt82** | {**ascii** | **rid** | **format** | {**ap_ethmac** | **ap_location** | **apmac** | **apname** | **policy_tag** | **ssid** | **vlan_id** }} | **required** | **server** *dhcp-ip-addr*}

構文の説明

opt82	この WLAN のワイヤレス クライアントに DHCP オプション 82 を設定します
required	DHCP アドレス割り当てが必要かどうかを指定します
server	WLAN の IPv4 DHCP サーバを設定します
ascii	DHCP オプション 82 の ASCII をサポートします
rid	DHCP オプション 82 への Cisco 2 バイト RID の追加をサポートします
format	RemoteID 形式を設定します
ap_ethmac	DHCP AP イーサネット MAC アドレスを有効にします
ap_location	AP ロケーションを有効にします
apmac	AP の MAC アドレスを有効にします
apname	AP 名を有効にします
site_tag (Policy tag)	サイトタグを有効にします
ssid	SSID を有効にします
vlan_id	VLAN ID を有効にします
dhcp-ip-addr	オーバーライド DHCP サーバーの IP アドレスを入力します。

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、DHCP アドレス割り当てを要件として設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy demo-profile-name
Device(config-wireless-policy)# ipv4 dhcp required
```

ipv4 flow monitor

WLAN プロファイル ポリシーの IPv4 トラフィック入力フロー モニタを設定するには、**ipv4 flow monitor input** コマンドを使用します。

ipv4 flow monitor *monitor-name* **input**

構文の説明

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。

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、WLAN プロファイル ポリシーの IPv4 トラフィック入力フロー モニターを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-profile-name
Device(config-wireless-policy)# ipv4 flow monitor flow-monitor-name input
```

ipv6 access-list

IPv6アクセス リストを定義してデバイスをIPv6アクセス リスト コンフィギュレーション モードに設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用します。アクセス 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。

ipv6 access-list *access-list-name* | **match-local-traffic** | **log-update threshold** *threshold-in-msgs* | **role-based** *list-name*
noipv6 access-list *access-list-name* | **client** *permit-control-packets* | **log-update** *threshold* | **role-based** *list-name*

構文の説明

ipv6 *access-list-name*	名前付き IPv6 ACL（最長 64 文字）を作成し、IPv6 ACL コンフィギュレーション モードを開始します。 *access-list-name*：IPv6 アクセス リストの名前。名前は、スペース、疑問符を含むことができず、また、数字で始めることはできません。
match-local-traffic	ローカルで生成されたトラフィックに対する照合を有効にします。
log-update threshold *threshold-in-msgs*	最初のパケットの一致後に、syslog メッセージを生成する方法を決定します。 *threshold-in-msgs*：生成されるパケット数。
role-based *list-name*	ロールベースの IPv6 ACL を作成します。

コマンド デフォルト

IPv6 アクセス リスト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 ジブラルタル 16.10.1	このコマンドが導入されました。

使用上のガイドライン

IPv6 ACL は、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用することで定義され、その許可と拒否の条件は IPv6 アクセス リスト コンフィギュレーション モードで **deny** コマンドおよび **permit** コマンドを使用することで設定されます。**ipv6 access-list** コマンドを設定すると、デバイスはIPv6アクセス リスト コンフィギュレーション モードになり、デバイス プロンプトは Device(config-ipv6-acl)# に変わります。IPv6 アクセス リスト コンフィギュレーション モードから、定義済みの IPv6 ACL に許可および拒否の条件を設定できます。

（注） IPv6 ACL は一意な名前によって定義されます（IPv6 は番号付けされた ACL をサポートしません）。IPv4 ACL と IPv6 ACL は同じ名前を共有できません。

IPv6 は、グローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに変換される **permit any any** ステートメントおよび **deny any any** ステートメントでプロトコル タイプとして自動的に設定されます。

IPv6 ACL にはそれぞれ、最後に一致した条件として、暗黙の **permit icmp any any nd-na** ステートメント、**permit icmp any any nd-ns** ステートメント、および **deny ipv6 any any** ステートメントがあります（前の 2 つの一致条件は、ICMPv6 ネイバー探索を許可します）。1 つの IPv6 ACL には、暗黙の **deny ipv6 any any** ステートメントを有効にするために少なくとも 1 つのエントリが含まれている必要があります。IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを利用するため、デフォルトで、インターフェイス上での IPv6 ネイバー探索パケットの送受信が IPv6 ACL によって暗黙的に許可されます。IPv4 の場合、IPv6 ネイバー探索プロセスに相当するアドレス解決プロトコル（ARP）では、個別のデータ リンク層プロトコルを利用するため、デフォルトで、インターフェイス上での ARP パケットの送受信が IPv4 ACL によって暗黙的に許可されます。

IPv6 ACL を IPv6 インターフェイスに適用するには、*access-list-name* 引数を指定して **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。IPv6 ACL をデバイスとの着信および発信 IPv6 仮想端末接続に適用するには、*access-list-name* 引数を指定して、**ipv6 access-class** ライン コンフィギュレーション コマンドを使用します。

ipv6 traffic-filter コマンドでインターフェイスに適用される IPv6 ACL は、デバイスによって発信されたトラフィックではなく、転送されたトラフィックをフィルタ処理します。

例

次に、list1 という名前の IPv6 ACL を設定し、デバイスを IPv6 アクセス リスト コンフィギュレーション モードにする例を示します。

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

次に、list2 という名前の IPv6 ACL を設定し、その ACL をイーサネット インターフェイス 0 上の発信トラフィックに適用する例を示します。特に、最初の ACL エントリは、ネットワーク FEC0:0:0:2::/64（送信元 IPv6 アドレスの最初の 64 ビットとしてサイトローカルプレフィックス FEC0:0:0:2 を持つパケット）がイーサネットインターフェイス 0 から出て行くことを拒否します。2 番目の ACL エントリは、その他のすべてのトラフィックがイーサネット インターフェイス 0 から出て行くことを許可します。2 番めのエントリは、各 IPv6 ACL の末尾に暗黙的な deny all 条件があるため、必要となります。

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

ipv6-address-type

802.11u IPv6 アドレスタイプを設定するには、**ipv6-address-type** コマンドを使用します。アドレスタイプを削除するには、このコマンドの **no** 形式を使用します。

ipv6-address-type {**available** | **not-available** | **not-known**}

構文の説明

available	IPv6 アドレスタイプを使用可能として設定します。
not-available	IPv6 アドレスタイプを使用不可として設定します。
not-known	IPv6アドレスタイプの可用性を不明として設定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、802.11u IPv6 アドレスタイプを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# ipv4-address-type available
```

ipv6 address

IPv6 汎用プレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスの IPv6 処理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 **ipv6 address** コマンドを使用します。インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address {*ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length*}
no ipv6 address {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}

構文の説明

ipv6-address	使用する IPv6 アドレス。
/ *prefix-length*	IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
prefix-name	インターフェイスに設定するネットワークを表す上位ビットを指定する汎用プレフィックスです。
sub-bits	*prefix-name* 引数で指定された汎用プレフィックスによって提供されるプレフィックスに連結する、アドレスのサブプレフィックス ビットおよびホスト ビットです。 *sub-bits* 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。

コマンド デフォルト

IPv6 アドレスはインターフェイスに定義されません。

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
12.2(2)T	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズ デバイスに統合されました。
15.2(4)S	このコマンドが、Cisco IOS Release 15.2(4)S に統合されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズ アグリゲーション サービス デバイスに実装されました。
Cisco IOS XE リリース 3.2SE	このコマンドが、Cisco IOS XE リリース 3.2SE に統合されました。

使用上のガイドライン

ipv6 address コマンドを使用すると、複数の IPv6 アドレスをさまざまな方法でインターフェイスに設定できます。さまざまなオプションがあります。最も一般的な方法は、プレフィックス長を使用して IPv6 アドレスを指定することです。

アドレスは、集約された IPv6 プレフィックス ビットをサブプレフィックス ビットおよびホスト ビットから分離する汎用プレフィックスのメカニズムを使用して定義することもできます。この場合、アドレスの先頭ビットは、グローバルに設定または（たとえば、Dynamic Host Configuration Protocol-Prefix Delegation（DHCP-PD）を使用して）学習される汎用プレフィックスで定義され、*prefix-name* 引数を使用して適用されます。サブプレフィックス ビットとホスト ビットは、*sub-bits* 引数を使用して定義されます。

引数を指定せずに **no ipv6 address autoconfig** コマンドを使用すると、手動で設定したすべての IPv6 アドレスがインターフェイスから削除されます。

IPv6 リンクローカル アドレスを設定する必要があります。また、**ipv6 address link-local** コマンドを使用して、インターフェイスで IPv6 処理をイネーブルにする必要があります。

例

次に、インターフェイスで IPv6 処理をイネーブルにして、my-prefix という汎用プレフィックスおよび直接指定されたビットに基づいてアドレスを設定する例を示します。

```
Device(config-if) ipv6 address my-prefix 0:0:0:7272::72/64
```

my-prefix という汎用プレフィックスの値が 2001:DB8:2222::/48 である場合、インターフェイスは、グローバル アドレス 2001:DB8:2222:7272::72/64 を使用して設定されます。

関連コマンド

コマンド	説明
ipv6 address anycast	IPv6 エニーキャスト アドレスを設定し、インターフェイスで IPv6 処理をイネーブルにします。
ipv6 address eui-64	IPv6 アドレスを設定して、そのアドレスの下位 64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
ipv6 address link-local	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。

コマンド	説明
ipv6 unnumbered	インターフェイスに明示的なIPv6アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
no ipv6 address autoconfig	インターフェイスからすべての IPv6 アドレスを削除します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 dhcp pool

Dynamic Host Configuration Protocol（DHCP）for IPv6 のサーバ設定情報プールを設定して DHCP for IPv6 プール 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 dhcp pool** コマンドを使用します。DHCP for IPv6 プ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。

ipv6 dhcp pool *poolname*
no ipv6 dhcp pool *poolname*

構文の説明

poolname	ローカルなプレフィックス プールのユーザ定義名。プール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

DHCP for IPv6 プールは設定されません。

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
12.3(4)T	このコマンドが導入されました。
12.2(18)SXE	このコマンドが、Cisco IOS Release 12.2(18)SXE に統合されました。
12.4(24)T	このコマンドが、Cisco IOS Release 12.4(24)T に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
12.2(33)SRE	このコマンドが変更されました。Cisco IOS Release 12.2(33)SRE に統合されました。
12.2(33)XNE	このコマンドが変更されました。Cisco IOS リリース 12.2(33)XNE に統合されました。

使用上のガイドライン

IPv6 用 DHCP サーバ設定情報プールを作成するには、**ipv6 dhcp pool** コマンドを使用します。**ipv6 dhcp pool** 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 用 DHCP プール 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、次のコマンドを使用して、管理者はプレフィックスが委任されるようにプール パラメータを設定し、ドメイン ネーム システム（DNS）サーバを設定できます。

- **address prefix** *IPv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}] はアドレス割り当てにアドレス プレフィックスを設定します。このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。
- **link-address** *IPv6-prefix* はリンクアドレス IPv6 プレフィックスを設定します。着信インターフェイスのアドレスまたはパケット内のリンク アドレスが指定した IPv6 プレフィッ

クスと一致する場合、サーバは設定情報プールを使用します。このアドレスは、16ビット値をコロンで区切った16進数で指定する必要があります。

- **vendor-specific** *vendor-id* はDHCPv6ベンダー固有のコンフィギュレーション モードを有効にします。ベンダーの識別番号を指定します。この番号は、ベンダーのIANAプライベートエンタープライズ番号です。指定できる範囲は1～4294967295です。次のコンフィギュレーション コマンドが利用できます。
  - **suboption** *number* はベンダー固有のサブオプション番号を設定します。指定できる範囲は1 ～ 65535です。IPv6アドレス、ASCIIテキスト、または16進文字列をサブオプション パラメータで定義されている束リに入力できます。

（注） **suboption** キーワードの下に **hex** 値を使用すると、入力できるのは16進数（0 ～ f）のみとなります。無効な **hex** 値を入力しても以前の設定は削除されません。

IPv6用DHCP設定情報プールが作成されたら、**ipv6 dhcp server** コマンドを使用して、プールとインターフェイス上のサーバを関連付けます。情報プールを設定しない場合は、**ipv6 dhcp server interface** コンフィギュレーション コマンドを使用してDHCPv6サーバ関数をインターフェイス上で有効にする必要があります。

DHCPv6プールとインターフェイスを関連付けると、関連付けられているインターフェイス上の要求を処理するのはそのプールだけとなります。プールは、他のインターフェイスについても処理を行います。DHCPv6プールとインターフェイスを関連付けない場合は、すべてのインターフェイスに対する要求を処理できます。

IPv6アドレス プレフィックスを使用しない場合、プールは設定済みのオプションのみを返します。

link-address コマンドでは、必ずしもアドレスを割り当てなくてもリンクアドレスの照合を行うことができます。プール内の複数のリンク アドレス コンフィギュレーション コマンドを使用して、複数のリレーのプールを照合できます。

アドレスプール情報またはリンク情報のいずれかについて最長一致が行われるため、あるプールについてはアドレスを割り当てるように設定して、サブプレフィックスの別のプールについては設定されたオプションだけを返すように設定できます。

例

次に、cisco1というDHCP for IPv6設定情報プールを指定して、ルータをDHCP for IPv6プール コンフィギュレーション モードにする例を示します。

```
Router(config)# ipv6 dhcp pool cisco1
Router(config-dhcpv6)#
```

次に、IPv6コンフィギュレーション プールcisco1にIPv6アドレス プレフィックスを設定する例を示します。

```
Router(config-dhcpv6)# address prefix 2001:1000::0/64
Router(config-dhcpv6)# end
```

次に、3 つのリンクアドレス プレフィックスと IPv6 アドレス プレフィックスを含む engineering という名前のプールを設定する例を示します。

```
Router# configure terminal
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# link-address 2001:1001::0/64
Router(config-dhcpv6)# link-address 2001:1002::0/64
Router(config-dhcpv6)# link-address 2001:2000::0/48
Router(config-dhcpv6)# address prefix 2001:1003::0/64
Router(config-dhcpv6)# end
```

次に、ベンダー固有オプションを含む 350 という名前のプールを設定する例を示します。

```
Router# configure terminal
Router(config)# ipv6 dhcp pool 350
Router(config-dhcpv6)# vendor-specific 9
Router(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Router(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Router(config-dhcpv6-vs)# end
```

関連コマンド

コマンド	説明
ipv6 dhcp server	インターフェイス上で DHCP for IPv6 サービスを有効にします。
show ipv6 dhcp pool	DHCP for IPv6 コンフィギュレーション プール情報を表示します。

ipv6 enable

明示的な IPv6 アドレスが設定されていないインターフェイス上で IPv6 処理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 **ipv6 enable** コマンドを使用します。明示的な IPv6 アドレスでまだ設定されていないインターフェイスで IPv6 処理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。

ipv6 enable
no ipv6 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

IPv6 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（config-if）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズ アグリゲーション サービス デバイスに実装されました。
Cisco IOS XE リリース 3.2SE	このコマンドが、Cisco IOS XE リリース 3.2SE に統合されました。
15.2(2)SA2	このコマンドが Cisco ME 2600X シリーズ イーサネット アクセス スイッチに実装されました。

使用上のガイドライン

ipv6 enable コマンドを実行すると、インターフェイスで IPv6 リンクローカル ユニキャスト アドレスが自動的に設定され、IPv6 処理のインターフェイスもイネーブルになります。明示的な IPv6 アドレスで設定されているインターフェイスで **ipv6 enable** コマンドを実行しても、IPv6 処理はディセーブルになりません。

例

次に、イーサネット インターフェイス 0/0 で IPv6 処理をイネーブルにする例を示します。

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 enable
```

関連コマンド

コマンド	説明
ipv6 address link-local	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ipv6 address eui-64	IPv6 アドレスを設定して、そのアドレスの下位 64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
ipv6 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 flow-export destination

IPv6 ETA フローのエクスポート先を設定するには、**ipv6 flow-export destination** コマンドを使用します。

ipv6 flow-export destination *ipv6_address port_number* [**source-interface** *interface-name*] [**ipfix**]

構文の説明

ip_address	フローの宛先アドレス。
port_number	フローの宛先ポート番号。有効な範囲は 1 ～ 65535 です。
source-interface	（任意）エクスポートされる ETA レコードの送信元インターフェイス名。
interface-number	（任意）エクスポートされる ETA レコードの送信元アドレス。インターフェイスの IP アドレスは、エクスポートされる ETA レコードパケットの送信元 IP アドレスとして使用されます。
ipfix	（任意）エクスポートされる ETA レコードの形式。

コマンド デフォルト

なし

コマンド モード

ET-Analytics 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 Amsterdam 17.1.1s	このコマンドが導入されました。

次に、ETA フローエクスポートの宛先を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# ipv6 flow-export destination 2001:181:181::1 22
source-interface loopback0 ipfix
Device(config-et-analytics)# end
```

ipv6 nd proxy

IPv6 ネイバー探索（ND）または重複アドレス検出（DAD）を有効にするには、**ipv6 nd proxy** コマンドを使用します。ND または DAD プロキシを無効にするには、このコマンドの **no** 形式を使用します。

ipv6 nd proxy {**dad-proxy** | **full-proxy**}

no ipv6 nd proxy {**dad-proxy** | **full-proxy**}

構文の説明

dad-proxy	DAD プロキシを有効にします。
full-proxy	フルプロキシを有効にします。これにより、DAD プロキシと非 DAD ネイバー要請プロキシが有効になります。

コマンド デフォルト

ネイバー探索プロキシは有効になっていません。

コマンド モード

ワイヤレス ポリシーの設定（config-wireless-policy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

使用上のガイドライン

DAD プロキシは、中央スイッチングモードでのみ適用されます。

例

次に、DAD プロキシを有効にする例を示します。

```
Device(config-wireless-policy)#ipv6 nd proxy dad-proxy
```

ipv6 mld snooping

マルチキャスト リスナー検出バージョン 2（MLDv2）プロトコル スヌーピングをグローバルに有効にするには、グローバル コンフィギュレーション モードで **ipv6 mld snooping** コマンドを使用します。MLDv2 スヌーピングをグローバルに無効にするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping
no ipv6 mld snooping

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

このコマンドは有効です。

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
12.2(18)SXE	このコマンドが Supervisor Engine 720 に導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
15.4(2)S	このコマンドが、Cisco ASR 901 シリーズ アグリゲーション サービス ルータに実装されました。

使用上のガイドライン

MLDv2 スヌーピングは、ポリシー フィーチャ カード 3（PFC3）の何らかのバージョンが搭載された Supervisor Engine 720 でサポートされています。

MLDv2 スヌーピングを使用するには、IPv6 マルチキャスト ルーティング用のサブネットでレイヤ 3 インターフェイスを設定するか、またはサブネットで MLDv2 スヌーピング クエリアを有効にします。

例

次に、MLDv2 スヌーピングをグローバルにイネーブルにする例を示します。

```
Router(config)# ipv6 mld snooping
```

関連コマンド

コマンド	説明
show ipv6 mld snooping	MLDv2 スヌーピング情報を表示します。

ipv6 nd managed-config-flag

IPv6 ルータ アドバタイズメントに managed address configuration フラグを設定するには、適切なコンフィギュレーション モードで **ipv6 nd managed-config-flag** コマンドを使用します。IPv6 ルータ アドバタイズメントからこのフラグをクリアするには、このコマンドの **no** 形式を使用します。

ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag

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

managed address configuration フラグは、IPv6 ルータ アドバタイズメントで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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

managed address configuration フラグを IPv6 ルータ アドバタイズメントで設定すると、アドレスの取得にステートフル オートコンフィギュレーションを使用するかどうかを、接続ホストに示すことができます。このフラグが設定されている場合、接続ホストは、アドレスの取得にステートフル オートコンフィギュレーションを使用します。このフラグが設定されていない場合、接続ホストは、アドレスの取得にステートフル オートコンフィギュレーションを使用しません。

ホストは、ステートフルおよびステートレス オートコンフィギュレーションを同時に使用できます。

例

次に、IPv6 ルータ アドバタイズメントに managed address configuration フラグを設定する例を示します。

```
Device(config)# interface
Device(config-if)# ipv6 nd managed-config-flag
```

ipv6 nd other-config-flag

IPv6 ルータ アドバタイズメントに other stateful configuration フラグを設定するには、適切なコンフィギュレーション モードで **ipv6 nd other-config-flag** コマンドを使用します。IPv6 ルータ アドバタイズメントからこのフラグをクリアするには、このコマンドの **no** 形式を使用します。

ipv6 nd other-config-flag

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

other stateful configuration フラグは、IPv6 ルータ アドバタイズメントで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

ダイナミック 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

other stateful configuration フラグを IPv6 ルータ アドバタイズメントで設定すると、アドレス以外のオートコンフィギュレーション情報を取得できるかどうかを、接続ホストに示すことができます。このフラグが設定されている場合、接続ホストは、その他（アドレス以外）の情報の取得にステートフル オートコンフィギュレーションを使用します。

（注） **ipv6 nd managed-config-flag** コマンドを使用して managed address configuration フラグを設定すると、接続ホストは、other stateful configuration フラグの設定に関係なく、ステートフル オートコンフィギュレーションを使用してその他の情報（アドレス以外の情報）を取得できます。

例

次の例（BNG 以外に該当）は、IPv6 ルータ アドバタイズメントに「other stateful configuration」フラグを設定します。

```
Device(config)# interface
Device(config-if)# ipv6 nd other-config-flag
```

ipv6 nd ra throttler attach-policy

フィーチャ RA スロットラの IPv6 ポリシーを設定するには、**ipv6 nd ra-throttler attach-policy** コマンドを使用します。

ipv6 nd ra-throttler attach-policy *policy-name*

構文の説明

ipv6	IPv6 ルート チェーン。
ra-throttler	VLAN で RA スロットラを設定します。
attach-policy	フィーチャ RA スロットラのポリシーを適用します。
policy-name	フィーチャ RA スロットラのポリシー名

コマンド デフォルト

なし

コマンド モード

config-vlan

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、フィーチャ RA スロットラの IPv6 ポリシーを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# vlan configuration vlan-id
Device(config-vlan-config)# ipv6 nd ra-throttler attach-policy
```

ipv6 nd raguard policy

ルータ アドバタイズメント（RA）ガード ポリシー名を定義し、RA ガード 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 **ipv6 nd raguard policy** コマンドを使用します。

ipv6 nd raguardpolicy *policy-name*

構文の説明

policy-name	IPv6 RA ガード ポリシー名。

コマンド デフォルト

RA ガード 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（config）#

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが、Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE リリース 3.2SE	このコマンドが、Cisco IOS XE リリース 3.2SE に統合されました。

使用上のガイドライン

ルータ上でグローバルに RA ガードを設定するには、**ipv6 nd raguard policy** コマンドを使用します。デバイスが NDインスペクション ポリシー コンフィギュレーション モードになったら、次のいずれかのコマンドを使用できます。

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **trusted-port**
- **validate source-mac**

IPv6 RA ガードがグローバルに設定されると、**ipv6 nd raguard attach-policy** コマンドを使用して、特定のインターフェイスで IPv6 RA ガードをイネーブルにできます。

例

次に、RA ガード ポリシー名を policy1 と定義し、デバイスをポリシー コンフィギュレーション モードにする例を示します。

```
Device(config)# ipv6 nd raguard policy policy1
Device(config-ra-guard)#
```

関連コマンド

表 *9*：

コマンド	説明
device-role	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。
drop-unsecure	オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップします。
ipv6 nd raguard attach-policy	指定したインターフェイスに IPv6 RA ガード機能を適用します。
limit address-count	ポートで使用できる IPv6 アドレスの数を制限します。
sec-level minimum	CGA オプションを使用する場合の最小のセキュリティ レベル パラメータ値を指定します。
trusted-port	信頼できるポートにするポートを設定します。
validate source-mac	送信元MACアドレスをリンク層アドレスと照合します。

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、**ipv6 traffic-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 Gibraltar 16.10.1	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。

```
デバイス(config-wlan)# ipv6 traffic-filter TestDocTrafficFilter
```

key

キーチェーンの認証キーを識別するには、キーチェーン コンフィギュレーション モードで **key** コマンドを使用します。キー チェーンからキーを削除するには、このコマンドの **no** 形式を使用します。

key *key-id*
no key *key-id*

構文の説明

key-id	キー チェーンの認証キーの識別番号。キーの範囲は 0 ～ 2147483647 です。キーの ID 番号は連続している必要はありません。

コマンド デフォルト

キー チェーンにキーは存在しません。

コマンド モード

キーチェーン コンフィギュレーション（config-keychain）

使用上のガイドライン

キー チェーンに複数のキーを設定し、**accept-lifetime** および **send-lifetime** キー チェーン キー コマンド設定に基づいてキーが将来無効になるように、ソフトウェアでキーを配列できるようにすると便利です。

各キーには、ローカルに格納される独自のキー識別子があります。キー ID、およびメッセージに関連付けられたインターフェイスの組み合わせにより、使用中の認証アルゴリズムおよび Message Digest 5（MD5）認証キーが一意に識別されます。有効なキーの数にかかわらず、1 つの認証パケットのみが送信されます。ソフトウェアは、最小のキー識別番号の検索を開始し、最初の有効なキーを使用します。

最後のキーが期限切れになった場合、認証は続行されますが、エラー メッセージが生成されます。認証を無効にするには、手動で有効な最後のキーを削除する必要があります。

すべてのキーを削除するには、**no key chain** コマンドを使用してキー チェーンを削除します。

例

次に、キーを指定してキー チェーンでの認証を確認する例を示します。

```
Device(config-keychain)#key 1
```

関連コマンド

コマンド	説明
accept-lifetime	キー チェーンの認証キーが有効として受信される期間を設定します。
key chain	ルーティング プロトコルの認証をイネーブルにするために必要な認証キー チェーンを定義します。
key-string (authentication)	キーの認証文字列を指定します。
show key chain	認証キーの情報を表示します。

key config-key password-encrypt

パスワード暗号化用のプライベート設定キーを設定するには、**key config-key password-encrypt** コマンドを使用します。この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。

key config-key password-encrypt <*config-key*>

構文の説明

config-key	8 文字以上の値を入力します。 （注） 値の先頭を次の特殊文字にすることはできません。 !、#、および;

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 Gibraltar 17.6.1	このコマンドが導入されました。

例

次に、AP 管理用のユーザー名とパスワードを設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# key config-key password-encryption 12345678
Device(config-ap-profile)# password encryption aes
Device(config-ap-profile)# end
```

ldap attribute-map

SLDAP サーバにダイナミック属性マップを設定するには、**ldap attribute-map** コマンドを使用します。

ldap attribute-map *map-name*

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、SLDAP サーバーにダイナミック属性マップを設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# ldap attribute-map map1
デバイス(config-attr-map)# map type department supplicant-group
デバイス(config-attr-map)# exit
```

ldap server

セキュア LDAP を設定するには、**ldap server** コマンドを使用します。

ldap server *name*

構文の説明

name	サーバ名。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、セキュア LDAP を設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# ldap server server1
デバイス(config-ldap-server)# ipv4 9.4.109.20
デバイス(config-ldap-server)# timeout retransmit 20
デバイス(config-ldap-server)# bind authenticate root-dn
CN=ldapipv6user,CN=Users,DC=ca,DC=ssh2,DC=com password Cisco12345
デバイス(config-ldap-server)# base-dn CN=Users,DC=ca,DC=ssh2,DC=com
デバイス(config-ldap-server)# mode secure no- negotiation
デバイス(config-ldap-server)# end
```

license air level

ワイヤレスコントローラでAIRライセンスを設定するには、グローバル コンフィギュレーション モードで**license air level** コマンドを入力します。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。

license air level { **air-network-advantage** [**addon air-dna-advantage**] | **air-network-essentials** [**addon air-dna-essentials**] }

no license air level

構文の説明

air-network-advantage	AIR Network Advantage ライセンスレベルを設定します。
addon air-dna-advantage	（任意）アドオンの AIR DNA Advantage ライセンスレベルを設定します。 このアドオンオプションは AIR Network Advantage ライセンスで使用できます。
air-network-essentials	AIR Network Essentials ライセンスレベルを設定します。
addon air-dna-essentials	（任意）アドオンの AIR DNA Essentials ライセンスレベルを設定します。 このアドオンオプションは AIR Network Essential ライセンスで使用できます。

コマンド デフォルト

すべての Cisco Catalyst 9800 ワイヤレスコントローラのデフォルトライセンスは AIR DNA Advantage です。

EWC-AP の場合：

- Cisco IOS XE Bengaluru 17.4.1 より前では、デフォルトライセンスは AIR DNA Essentials でした。
- Cisco IOS XE Bengaluru 17.4.1 以降のデフォルトライセンスは AIR Network Essentials 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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	このコマンドは、ポリシーを使用したスマートライセンスの導入で、引き続き使用および適用することができます。
Cisco IOS XE Bengaluru 17.4.1	EWC-AP の場合のみ、デフォルトライセンスが AIR DNA Essentials から AIR Network Essentials に変更されました。

使用上のガイドライン

ポリシーを使用したスマートライセンスの環境では、**license air level** コマンドを使用して、製品インスタンスで使用されているライセンスレベルを変更したり、製品インスタンスでアドオンライセンスを追加設定したりすることができます。変更はリロード後に有効になります。

設定できるライセンスは次のとおりです。

- AIR Network Essential
- AIR Network Advantage
- AIR DNA Essential
- AIR DNA Advantage

Cisco DNA ライセンスを更新しない場合は、AIR DNA Essential または AIR DNA Advantage ライセンスレベルを設定し、期限切れになった時点で Network Advantage または Network Essentials のライセンスレベルに移行することができます。

接続しているすべての AP において、コントローラの一意の値プロパティを利用するために、Cisco DNA Center ライセンスが必要です。

例

次に、AIR DNA Essential ライセンスレベルを設定する例を示します。

```
Device# configure terminal
Device(config)# license air level network-essentials addon air-dna-essentials
```

次に、AIR DNA Advantage ライセンスレベルで開始してから AIR DNA Essentials に変更する例を示します。

AIR DNA Advantage としての現在の設定：

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Advantage

Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

AIR DNA Essentials の設定：

```
Device# configure terminal
Device(config)# license air level air-network-essentials addon air-dna-essentials

Device# exit
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Essentials
Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

```
Device# write memory
Device# reload
```

リロード後：

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Essentials
Next reload AIR license Level: AIR DNA Essentials

Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

license smart（グローバル コンフィギュレーション）

製品インスタンスが Cisco Smart Software Manager（CSSM）や Cisco Smart Licensing Utility（CSLU）、または Smart Software Manager オンプレミス（SSM オンプレミス）との通信に使用するトランスポートモードや URL などのライセンス関連の設定を行い、使用状況レポートの間隔を設定し、ライセンス使用状況レポート（RUM レポート）に含めるか、または除外する必要がある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 **license smart** コマンドを入力します。デフォルト値に戻すには、コマンドの **no** 形式を使用します。

license smart { **custom_id** *ID* | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** { **automatic** | **callhome** | **cslu** | **off** | **smart** } | **url** { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] }

no license smart { **custom_id** | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** | **url** { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] }

構文の説明

custom_id *ID*	このオプションは CLI では使用できますがサポートされていません。
enable	このキーワードは CLI には表示されますが、設定しても効果はありません。スマートライセンスは常に有効になっています。

privacy { **all** | **hostname** | **version** }

プライバシーフラグを設定して、指定されたデータプライバシー関連情報の送信を防止します。

フラグが無効になっている場合、対応する情報は、製品インスタンスによって作成されるメッセージまたはオフラインファイルで送信されます。

トポロジに応じて、CSSM、CSLU、SSM オンプレミスなどの1つ以上のコンポーネントに情報が送信されます。

すべてのデータプライバシー設定はデフォルトで無効になっています。すべての通信から除外するオプションを設定する必要があります。

- **all**：すべてのデータプライバシー関連情報がすべての通信から除外されます。

  このコマンドの **no** 形式を使用すると、すべてのデータプライバシー関連情報がメッセージまたはオフラインファイルで送信されます。

  （注） データプライバシーが有効かどうかに関係なく、製品 ID（PID）とシリアル番号がRUMレポートに含まれます。

- **hostname**：ホスト名情報がすべての通信から除外されます。ホスト名のプライバシーが有効になっている場合、製品インスタンスの UDI が該当するユーザーインターフェイス（CSSM、CSLU、およびSSMオンプレミス）に表示されます。

  このコマンドの **no** 形式を使用すると、ホスト名情報がメッセージまたはオフラインファイルで送信されます。ホスト名は、該当するユーザーインターフェイス（CSSM、CSLU、および SSM オンプレミス）に表示されます。

- **version**：製品インスタンスで実行されているCisco IOS-XE ソフトウェアバージョンとスマートエージェントのバージョンがすべての通信から除外されます。

  このコマンドの**no**形式を使用すると、バージョン情報がメッセージまたはオフラインファイルで送信されます。

proxy { **address** *address_hostname* | **port** *port* }	CSLUまたはCSSMとライセンス使用状況を同期するためにプロキシを設定します。つまり、トランスポートモードが **license smart transport smart**（CSSM）または **license smart transport cslu**（CSLU）の場合にのみ、このオプションを使用してプロキシを設定できます。 ただし、トランスポートモードとして **license smart transport cslu** も使用する SSM オンプレミス展開では、ライセンス使用状況の同期にプロキシは設定できません。 次のオプションを設定します。 • **address** *address_hostname*：プロキシアドレスを設定します。 *address_hostname* には、プロキシの IP アドレスまたはホスト名を入力します。 • **port***port*：プロキシポートを設定します。 *port* には、プロキシポート番号を入力します。
reservation	ライセンス予約機能を有効または無効にします。 （注） このオプションは、CLI で使用できますが、ライセンスの予約が適用されないため、ポリシーを使用したスマートライセンシングの環境では適用されません。
server-identity-check	HTTP セキュアサーバの ID チェックを有効または無効にします。

transport { **automatic** | **callhome** | **cslu** | **off** | **smart** }	製品インスタンスが CSSM との通信に使用する転送モードを設定します。次のオプションから選択します。 • **automatic**：転送モード **cslu** を設定します。 （注） **automatic** キーワードは Cisco Catalyst ワイヤレスコントローラではサポートされていません。 • **callhome**：転送モードとして Call Home を有効にします。 • **cslu**：転送モードとして CSLU を有効にします。これがデフォルトの転送モードです。 CSLU と SSM オンプレミスの両方に同じキーワードが適用されますが、URLが異なります。次の行の **cslu***cslu_or_on-prem_url* を参照してください。 • **off**：製品インスタンスからのすべての通信を無効にします。 • **smart**：スマート転送を有効にします。

url { *url* | **cslu** *cslu_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* }

設定された転送モードに使用する URL を設定します。次のオプションから選択します。

- *url*：転送モードとして **callhome** を設定している場合は、このオプションを設定します。CSSM URL を次のように正確に入力します。

  ```
  https://software.cisco.com/#module/SmartLicensing
  ```

  no license smart url *url* コマンドは、デフォルトの URL に戻ります。

- **cslu** *cslu_or_on-prem_url*：トランスポートモードを **cslu** として設定している場合は、必要に応じて CSLU または SSM オンプレミスの URL を使用してこのオプションを設定します。

  - CSLU を使用している場合は、次のように URL を入力します。

    ```
    http://<cslu_ip_or_host>:8182/cslu/v1/pi
    ```

    `<cslu_ip_or_host>` には、CSLU をインストールした Windows ホストのホスト名や IP アドレスを入力します。8182 はポート番号であり、CSLU が使用する唯一のポート番号です。

    no license smart url cslu *cslu_or_on-prem_url* コマンドは `http://cslu-local:8182/cslu/v1/pi` に戻ります。

  - SSM オンプレミスを使用している場合は、次のように URL を入力します。

    ```
    http://<ip>/cslu/v1/pi/<tenant ID>
    ```

    <ip> には、SSM オンプレミスをインストールしたサーバのホスト名または IP アドレスを入力します。<tenantID> はデフォルトのローカルバーチャルアカウント ID にする必要があります。

    ヒント　SSM オンプレミスから URL 全体を取得できます。ソフトウェア設定ガイド（17.3.x 以降）で、「Smart Licensing Using Policy」>「Task Library for Smart Licensing Using Policy」>「Retrieving the Transport URL (SSM On-Prem

UI)」を参照してください。

no license smart url cslu *cslu_or_on-prem_url* コマンドは `http://cslu-local:8182/cslu/v1/pi` に戻ります。

- **default**：設定されている転送モードによって異なります。このオプションでは、**smart** および **cslu** 転送モードのみがサポートされます。

  転送モードが **cslu** に設定されている場合、**license smart url default** を設定すると、CSLU URL は自動的に設定されます（`https://cslu-local:8182/cslu/v1/pi`）。

  転送モードが **smart** に設定されている場合、**license smart url default** を設定すると、スマート URL は自動的に設定されます（`https://smartreceiver.cisco.com/licservice/license`）。

- **smart** *smart_url*：転送タイプとして **smart** を設定している場合は、このオプションを設定します。URL を次のように正確に入力します。

  `https://smartreceiver.cisco.com/licservice/license`

  このオプションを設定すると、システムは **license smart url** *url* で自動的に URL の複製を作成します。重複するエントリは無視できます。これ以上の操作は必要ありません。

  no license smart url smart*smart_url* コマンドは、デフォルトの URL に戻ります。

- **utility** *smart_url*：このオプションは CLI では使用できますがサポートされていません。

usage { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* }	使用状況レポートの設定を構成します。次のオプションを設定できます。 • **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value*：テレメトリ用のデータモデルに含める文字列を定義します。最大4つの文字列（またはタグ）を定義できます。 *tag_value* には、定義する各タグの文字列値を入力します。 • **interval** *interval_in_days*：レポート間隔の日数を設定します。デフォルトでは、RUM レポートは 30 日ごとに送信されます。有効な値の範囲は 1 ～ 3650 です。 この値をゼロに設定すると、適用されるポリシーの指定内容に関係なく、RUM レポートは送信されません。これは、CSLU または CSSM が受信側にある可能性があるトポロジに適用されます。 ゼロより大きい値を設定し、通信タイプが**オフ**に設定されている場合、*interval_in_days* と `Ongoing reporting frequency(days):` のポリシー値の間で、値の小さい方が適用されます。たとえば、*interval_in_days* が 100 に設定され、ポリシーの値が `Ongoing reporting frequency (days):90` の場合、RUM レポートは 90 日ごとに送信されます。 間隔を設定せず、デフォルトが有効な場合、レポート間隔は完全にポリシー値によって決定されます。たとえば、デフォルト値が有効で、不適用ライセンスのみが使用されている場合、ポリシーでレポートが不要と記述されていると、RUM レポートは送信されません。
utility [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }]	このオプションは CLI 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

Cisco IOS XE Amsterdam 17.3.1 以前：スマートライセンスがデフォルトで有効になっています。

Cisco IOS XE Amsterdam 17.3.2a 以降：ポリシーを使用したスマートライセンスがデフォルトで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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	ポリシーを使用したスマートライセンスで、次のキーワードと変数が導入されました。 • **url** キーワードの下に、次のオプションが導入されました。 { **cslu** *cslu_url* | **smart** *smart_url* } • **transport** キーワードの下に、次のオプションが導入されました。 { **cslu** | **off** } さらに、デフォルトの通信タイプが **callhome** から **cslu** に変更されました。 • **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } **license smart** コマンドの次のキーワードと変数は廃止され、CLI では使用できなくなりました：**enable**、**conversion automatic**。
Cisco IOS XE Amsterdam 17.3.3	SSM オンプレミスサポートが導入されました。SSM オンプレミス展開での製品インスタンス開始型通信の場合、既存の [**no**]**license smart url cslu***cslu_or_on-prem_url* コマンドは SSM オンプレミスの URL の設定もサポートします。ただし、SSM オンプレミスで必要な URL 形式は `http://<ip>/cslu/v1/pi/<tenant ID>` です。 設定する必要がある対応するトランスポートモードも、既存のコマンド（**license smart transport cslu**）です。
Cisco IOS XE Cupertino 17.7.1	バージョンプライバシーが無効になっている場合（**no license smart privacy version** グローバル コンフィギュレーション コマンド）、製品インスタンスで実行されている Cisco IOS-XE ソフトウェアバージョンとスマートエージェントのバージョンが RUM レポートに含まれます。 RUM レポートからバージョン情報を除外するには、バージョンプライバシーを有効にする必要があります（**license smart privacy version**）。

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	• すべてのデータプライバシー関連情報を送信する新しいメカニズムが導入されました。この情報は RUM レポートに含まれなくなりました。 データプライバシーが無効になっている場合（**no license smart privacy** {**all** | **hostname** | **version**} グローバル コンフィギュレーション コマンド）、データプライバシー関連情報は、別の同期メッセージまたはオフラインファイルで送信されます。 • ホスト名情報の送信のサポートが導入されました。 ホスト名のプライバシー設定が無効になっている場合（**no license smart privacy hostname** グローバル コンフィギュレーション コマンド）、ホスト名情報が別の同期メッセージまたはオフラインファイルで製品インスタンスから送信されます。実装したトポロジに応じて、ホスト名情報はCSSM、CSLU、またはSSMオンプレミスによって受信されます。ホスト名情報は、対応するユーザーインターフェイスにも表示されます。

使用上のガイドライン

データ プライバシー設定

プライバシー設定を無効にすると、実装したトポロジによって、受信者、および情報が宛先に到達する方法が決まります。

- 情報の受信者は、CSSM、CSLU、および SSM オンプレミスのうち 1 つ以上である可能性があります。プライバシー設定は、コントローラ（Cisco DNA Center）には影響を及ぼしません。

  hostname キーワードの場合、CSSM、CSLU、またはSSMオンプレミスがホスト名情報を受信すると、対応する UI にも表示されます（該当する場合）。その後、プライバシーを有効にすると、対応する UI は製品インスタンスの UDI の表示に戻ります。

- 情報の送信方法。
  - 製品インスタンスが通信を開始するトポロジの場合、製品インスタンスは、CSSM、CSLU、または SSM オンプレミスへのメッセージでこの情報の送信を開始します。

    製品インスタンスは、イベント（製品インスタンスの起動、ホスト名の変更、高可用性セットアップでのスイッチオーバー）の1つが発生するたびに送信されるホスト名を送信します。

  - CSLUまたはSSMオンプレミスが通信を開始するトポロジの場合、対応するコンポーネントが製品インスタンスからのプライバシー情報の取得を開始します。

    ホスト名を CSLU または SSM オンプレミスで設定した頻度で取得し、情報を取得します。

- 製品インスタンスがエアギャップネットワークにあるトポロジの場合、**license smart save usage** 特権 EXEC コマンドの入力時に生成されるオフラインファイルにプライバシー情報が含まれます。

（注） すべてのトポロジにおいて、データプライバシー関連情報はRUMレポートに含まれません。

データプライバシー関連情報は、送信または保存する前に製品インスタンスによって保存されないため、情報が送信される場合、送信時または保存時のデータプライバシー設定と一致することが保証されます。

通信障害とレポート

設定したレポート間隔（**license smart usage interval** *interval_in_days* コマンド）によって、製品インスタンスが RUM レポートを送信する日時が決まります。スケジュールされた間隔が通信障害と一致する場合、製品インスタンスは、スケジュールされた時間が経過した後、最大 4 時間 RUM レポートの送信を試みます。（通信障害が続くために）それでもレポートを送信できない場合、システムは間隔を 15 分にリセットします。通信障害が解消されると、レポート間隔はユーザが最後に設定した値に戻ります。

通信障害の場合に表示される可能性があるシステムメッセージは、%SMART_LIC-3-COMM_FAILED です。このエラーを解決し、レポート間隔の値を復元する方法については、該当するリリース（17.3.x 以降）のソフトウェア設定ガイドで、「System Configuration」>「Smart Licensing Using Policy」>「Troubleshooting Smart Licensing Using Policy」を参照してください。

プロキシサーバーの受け入れ

license smart proxy {**address** *address_hostname* | **port***port*} コマンドを設定するとき、Cisco IOS XE Bengaluru 17.6.1 以降、プロキシサーバーの受け入れ基準が変更されたことに注意してください。プロキシサーバーの応答のステータスコードのみがシステムによって検証され、理由フレーズは検証されません。RFC 形式は、`status-line = HTTP-version SP status-code SP reason-phrase CRLF` で、ステータスコードは 3 桁の数値コードになります。ステータス行の詳細については、RFC 7230 のセクション 3.1.2 を参照してください。

例

- データプライバシーの例 （598 ページ）
- 転送タイプと URL の例 （599 ページ）
- 使用状況レポートのオプションの例 （600 ページ）

データ プライバシーの例

次に、グローバル コンフィギュレーション モードで **license smart privacy** コマンドを使用してデータプライバシー関連情報を設定する例を示します。**show license status** 出力には、設定された情報が表示されます。

（注） **show** コマンドの出力は、特定のオプションが有効か無効かを示すだけです。

ここでは、データプライバシー関連の情報は送信されません。

```
Device# configure terminal
Device(config)# license smart privacy all
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: ENABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

ここでは、製品インスタンスで実行されているソフトウェアバージョンは、Cisco IOS XE Cupertino 17.9.1 です。バージョンプライバシーが無効になっていて、製品インスタンスで実行されている Cisco IOS-XE ソフトウェアバージョンとスマートエージェントのバージョンが RUM レポートに含まれます。

```
Device# configure terminal
Device(config)# license smart privacy hostname
Device(config)# no license smart privacy version
Device(config)# exit

Device# show license all
<output truncated>

Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

<output truncated>
```

ここでは、製品インスタンスで実行されているソフトウェアバージョンは、Cisco IOS XE Cupertino 17.9.1 です。製品インスタンスから開始されるメッセージには、ホスト名

は含まれ、バージョン情報は含まれません。製品インスタンスは CSSM に直接接続されています（トランスポートタイプは **smart** で、対応する URL があります）。

```
Device# configure terminal
Device(config)# license smart privacy version
Device(config)# no license smart privacy hostname
Device(config)# exit

Device# show license all
<output truncated>

Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

<output truncated>
```

転送タイプと URL の例

次に、グローバル コンフィギュレーション モードで **license smart transport** および **license smart url** コマンドを使用して、転送タイプの一部を設定する例を示します。**show license all** 出力には、設定された情報が表示されます。

トランスポート **cslu**：

```
Device# configure terminal
Device(config)# license smart transport cslu
Device(config)# license smart url default
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  Proxy:
    Not Configured
<output truncated>
```

トランスポート **smart**：

```
Device# configure terminal
Device(config)# license smart transport smart
Device(config)# license smart url smart https://smartreceiver.cisco.com/licservice/license
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
```

```
    Not Configured
<output truncated>
```

使用状況レポートのオプションの例

次に、グローバル コンフィギュレーション モードで **license smart usage** コマンドを使用して、使用状況レポートの一部を設定する例を示します。**show running-config** 出力には、設定された情報が表示されます。

customer-tag オプションの設定：

```
Device# configure terminal
Device(config)# license smart usage customer-tags tag1 SA/VA:01
Device(config)# exit
Device# show running-config | include tag1
license smart usage customer-tags tag1 SA/VA:01
```

現在適用されているポリシーよりも絞り込んだレポート間隔の設定：

```
Device# show license status
<output truncated>
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Dec 21 12:02:21 2020 PST
Reporting push interval: 30 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 22 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>

Device# configure terminal
Device(config)# license smart usage interval 20
Device(config)# exit
Device# show license status
<output truncated>

Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Nov 22 12:02:21 2020 PST
Reporting push interval: 20 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 12 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>
```

license smart（特権 EXEC）

承認コードの要求または返却、リソース使用状況測定レポート（RUM レポート）の保存、製品インスタンスへのファイルのインポート、Cisco Smart Software Manager（CSSM）との信頼の確立、CSSM または Cisco Smart License Utility（CSLU）、あるいは Smart Software Manager オンプレミス（SSM オンプレミス）との製品インスタンスの同期、製品インスタンスからのライセンス情報の削除などのライセンス機能を設定するには、対応するキーワードまたは引数を指定して特権 EXEC モードで **license smart** コマンドを入力します。

license smart { **authorization** { **request** { **add** | **replace** | **save** *filepath_filename* } *feature_name* { **all** | **local** } | **return** { **all** | **local** } { **offline** [*filepath_filename*] | **online** } } | **clear eventlog** | **export return** { **all** | **local** } *feature_name* | **factory reset** | **import** *filepath_filename* | **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *filepath_filename* } } | **sync** { **all** | **local** } | **trust idtoken** *id_token_value* { **local** | **all** } [{ **force** }] }

構文の説明

smart	スマートライセンスのオプションを提供します。
authorization	承認コードを要求する、または承認コードを返すオプションを提供します。 認証コードは、輸出規制または輸出規制の適用タイプのライセンスを使用する場合にのみ必要です。
request	承認コードを CSSM、CSLU（CSLU は CSSM から承認コードを取得）、または SSM オンプレミスから要求し、そのコードを製品インスタンスにインストールします。
add	要求されたライセンスを既存の承認コードに追加します。新しい承認コードには、既存の承認コードのすべてのライセンスと要求されたライセンスが含まれます。
replace	既存の承認コードを置き換えます。新しい承認コードには、要求されたライセンスのみが含まれます。現在の承認コードのすべてのライセンスが返されます。 このオプションを入力すると、製品インスタンスは、削除される承認コードに対応するライセンスが使用中であるかどうかを確認します。ライセンスが使用されている場合は、対応する機能を最初に無効にするようにエラーメッセージが表示されます。
save*filepath_filename*	承認コード要求をファイルに保存します。 *filepath_filename* には、ファイルの絶対パス（ファイル名を含む）を指定します。
feature_name	承認コードを要求するライセンスの名前。

all	高可用性セットアップですべての製品インスタンスに対してアクションを実行します。
local	アクティブな製品インスタンスに対してアクションを実行します。これがデフォルトのオプションです。
return	CSSM のライセンスプールに承認コードを返します。
offline *filepath_filename*	製品インスタンスが CSSM に接続されていないことを意味します。承認コードはオフラインで返されます。このオプションでは、戻りコードをファイルに出力する必要があります。 ファイルを保存するパスを指定することもできます。ファイル形式は、.txtなどの読み取り可能な任意の形式にすることができます。 オフラインオプションを選択する場合は、CLI や保存したファイルから戻りコードをコピーして CSSM に入力する、という追加の手順を実行する必要があります。
online	製品インスタンスが接続モードであることを意味します。承認コードは、CSLU や CSSM に直接返されます。
clear eventlog	製品インスタンスからすべてのイベントログファイルをクリアします。
export return	輸出規制ライセンスの承認キーを返します。
factory reset	製品インスタンスから保存されているすべてのライセンス情報をクリアします。
import *filepath_filename*	製品インスタンスにファイルをインポートします。ファイルは、承認コード、信頼コード、またはポリシーのファイルである場合があります。 *filepath_filename* には、場所（ファイル名を含む）を指定します。
save	RUM レポートや信頼コード要求を保存するオプションを提供します。
trust-request *filepath_filename*	アクティブな製品インスタンスの信頼コード要求を指定した場所に保存します。 *filepath_filename* には、ファイルの絶対パス（ファイル名を含む）を指定します。

usage { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* }	RUM レポート（ライセンス使用状況情報）を指定した場所に保存します。次のいずれかのオプションを指定する必要があります。 • **all**：すべての RUM レポートを保存します。 • **days** *days*：過去 n 日間（現在の日を除く）の RUM レポートを保存します。番号を入力します。有効範囲は 0 ～ 4294967295 です。 たとえば、3 と入力すると、過去 3 日間の RUM レポートが保存されます。 • **rum-Id** *rum-ID*：指定した RUM ID を保存します。値の有効な範囲は 0 ～ 18446744073709551615 です。 • **unreported**：すべての未報告の RUM レポートを保存します。 **file** *filepath_filename*：指定した使用状況情報をファイルに保存します。ファイルの絶対パス（ファイル名を含む）を指定します。
sync { **all** | **local** }	CSSM または CSLU、あるいは SSM オンプレミスと同期して、保留中のデータを送受信します。これには、保留中の RUM レポートのアップロード、ACK 応答のダウンロード、および製品インスタンスの保留中の承認コード、信頼コード、ポリシーが含まれます。 次のいずれかのオプションを入力して、製品インスタンスを指定します。 • **all**：高可用性セットアップですべての製品インスタンスに対して同期を実行します。このオプションを選択すると、製品インスタンスは同期要求内にあるすべての UDI のリストも送信します。 • **local**：要求を送信するアクティブな製品インスタンス、つまり自身の UDI に対してのみ同期を実行します。これがデフォルトのオプションです。
trust idtoken *id_token_value*	CSSM との信頼できる接続を確立します。 このオプションを使用するには、最初に CSSM ポータルでトークンを生成する必要があります。*id_token_value* に生成されたトークン値を指定します。
force	信頼コードが製品インスタンスにすでに存在する場合でも、信頼コード要求を送信します。 信頼コードは、製品インスタンスの UDI にノードロックされます。UDI がすでに登録されている場合、CSSM は同じ UDI の新規登録を許可しません。 **force** キーワードを入力すると、この動作が上書きされます。

コマンド デフォルト

Cisco IOS XE Amsterdam 17.3.1 以前：スマートライセンスがデフォルトで有効になっています。

Cisco IOS XE Amsterdam 17.3.2a 以降：ポリシーを使用したスマートライセンスがデフォルトで有効になっています。

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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	ポリシーを使用したスマートライセンスで、次のキーワードと変数が導入されました。 • **authorization** { **request** { **add** | **replace** } *feature_name* { **all** | **local** } | **return** { **all** | **local** } { **offline** [*path*] | **online** } } • **import** *file_path* • **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* } } • **sync** { **all** | **local** } • **trust idtoken** *id_token_value* { **local** | **all** } [**force**] **license smart** コマンドの次のキーワードと変数は廃止され、CLI では使用できなくなりました。 • **register idtoken** *token_id* [**force**] • **renew id** { **ID** | **auth** } • **debug** { **error** | **debug** | **trace** | **all** } • **reservation** { **cancel** [**all** | **local**] | **install** [**file**] *key* | **request** { **all** | **local** | **universal** } | **return** [**all** | **authorization** { *auth_code* | **file** *filename* } | **Local**] *key* } • **mfg reservation** { **request** | **install** | **install file** | **cancel** } • **conversion** { **start** | **stop** }
Cisco IOS XE Amsterdam 17.3.3	SSM オンプレミスのサポートが導入されました。リソース使用状況測定レポート（RUM レポート）の保存、製品インスタンスへのファイルのインポート、製品インスタンスの同期、認証コードの返却、SSM オンプレミス展開での製品インスタンスからのライセンス情報の削除など、ライセンス関連のタスクを実行できます。

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このリリースでは、次の機能拡張が導入されています。 • **save** *filepath_filename* キーワードと変数が **license smart authorization request** 文字列に追加されました。 CLI には表示されますが、Cisco Catalyst ワイヤレスコントローラのいずれにも輸出規制ライセンスまたは適用ライセンスがないため、この新しいキーワードは適用されません。 • 既存の **license smart save usage** コマンドが拡張され、該当するトポロジの信頼コード要求が含まれるようになりました。

使用上のガイドライン

信頼コードの上書き

license smart trust idtoken コマンドを設定する際の **force** オプションのユースケース：1 つのバーチャルアカウントに含まれているすべての製品インスタンスに同じトークンを使用できます。製品インスタンスが 1 つのアカウントから別のアカウントに移動した場合（たとえば、別のバーチャルアカウントの一部である高可用性設定に追加されたため）、既存の信頼コードを上書きすることが必要になる場合があります。

ライセンス情報の削除

licence smart factory reset コマンドを入力すると、承認コード、RUM レポートなど、すべてのライセンス情報（使用中のライセンスを除く）が製品インスタンスから削除されます。そのため、このコマンドは、製品インスタンスを返却する場合（Return Material Authorization（RMA））、または永続的にデコミットする場合にのみ使用することを推奨します。また、製品インスタンスからライセンス情報を削除する前に CSSM に RUM レポートを送信します。これは、CSSM に最新の使用状況情報が含まれていることを確認するためです。

認証コードとライセンス予約：

認証コードとライセンス予約に関連するオプション：

- Cisco Catalyst ワイヤレスコントローラのいずれにも輸出規制ライセンスまたは適用ライセンスがなく、ポリシーを使用したスマートライセンスの環境には予約済みライセンスの概念が適用されないため、次のコマンドは適用されません。
  - { { **license smart authorization request** { **add** | **replace** | **save** *path* } *feature_name* { **all** | **local** } *request_count* } }
  - **license smart export return**
- 返すことも可能な SLR 承認コードの場合は、次のオプションが適用可能になっている必要があります。

  license smart authorization return { **all** | **local** } { **offline** [*path*] | **online** }

例

ライセンス使用状況情報の保存例

次の例は、製品インスタンスのライセンス使用状況情報を保存する方法を示しています。このオプションを使用して、エアギャップネットワークのレポート要件を満たすことができます。この例では、ファイルはまずフラッシュメモリに保存され、次に TFTP の場所にコピーされます。

```
 Device> enable
Device# license smart save usage unreported file flash:RUM-unrep.txt
Device# dir
Directory of bootflash:/

33      -rw-             5994   Nov 2 2020 03:58:04 +05:00  RUM-unrep.txt

Device# copy flash:RUM-unrep.txt tftp://192.168.0.1//auto/tftp-user/user01/
Address or name of remote host [192.168.0.1]?
Destination filename [//auto/tftp-user/user01/RUM-unrep.txt]?
!!
15128 bytes copied in 0.161 secs (93963 bytes/sec)
```

RUM レポートをファイルに保存した後、（インターネットに接続しているワークステーションや Ciscoから）CSSM にアップロードする必要があります。

信頼コードのインストールの例

次の例は、信頼コードがすでに製品インスタンスにインストールされている場合に、信頼コードをインストールする方法を示しています。これには、CSSM への接続が必要です。正常なインストール後の **show license status** 出力例を次に示します。

信頼コードをインストールする前に、トークンを生成し、CSSM から対応するファイルをダウンロードする必要があります。

結果を確認するには、**show license status** コマンド（`Trust Code Installed:`）を使用します。

```
Device> enable
Device# license smart trust idtoken
NGMwMjk5mYtNZaxMS00NzMZmtgWm local force

Device# show license status
<output truncated>
Trust Code Installed:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
    INSTALLED on Nov 02 05:19:05 2020 IST
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
    INSTALLED on Nov 02 05:19:05 2020 IST
<output truncated>
```

SLR 承認コードを返す例

次の例は、SLR 承認コードを削除して返す方法を示しています。ここでは、コードがオフラインで返されます（CSSM への接続なし）。正常に返された後の **show license all** 出力例を次に示します。

```
Device> enable
Device# show license all
<output truncated>
License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Last Confirmation code: ad4382fe
<output truncated>

Device# license smart authorization return local offlline
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS
    Return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h
UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN
    Return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA

Device# show license all
<output truncated>
License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: NOT INSTALLED
      Last return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: NOT INSTALLED
      Last return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA
<output truncated>
```

オフラインオプションを選択する場合は、CLI や保存したファイルから戻りコードをコピーして CSSM に入力する、という追加の手順を実行する必要があります。

license wireless high-performance

Cisco Catalyst C9800-L-K9 ワイヤレスコントローラのスケールとキャパシティをアップグレードするには、**license wireless high-performance** コマンドを使用します。高パフォーマンスライセンスを設定解除するには、このコマンドの **no** 形式を使用します。

license wireless high-performance

no license wireless high-performance

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

高パフォーマンスライセンスは設定されていません

コマンド モード

グローバル（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1s	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2	このコマンドは、このリリースで導入されるポリシーを使用したスマートライセンスで、引き続き使用および適用することができます。

使用上のガイドライン

このコマンドは、スタンバイコントローラと同期されます。ただし、アップグレードされたキャパシティを取得するには、スタンバイコントローラにもパフォーマンスライセンスが必要です。

高パフォーマンスライセンスを設定解除することで、ライセンスを解放してライセンスプールに戻すことができます。ライセンスを解放してライセンスプールに戻すことで、必要に応じて別のコントローラが使用できるようになります。

RMA の場合、お客様が Cisco Technical Assistance Center（TAC）に連絡して、お客様のバーチャルアカウントから製品インスタンスを削除する必要があります。これにより、コントローラが使用するすべてのライセンスがライセンスプールに戻され、新しいハードウェアで使用できるようになります。

license wireless high-performance コマンドを設定する前に、デバイスを再起動してください。

例

コントローラのスケールとキャパシティをアップグレードするには、次のコマンドを使用します。

```
Device# configure terminal
Device(config#) license wireless high-performance
```

link-local-bridging

各ポリシープロファイルのリンクローカルブリッジングを有効にするには、**link-local-bridging** コマンドを使用します。この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。

link-local-bridging

no link-local-bridging

構文の説明

link-local-bridging	各ポリシープロファイルのリンクローカルブリッジングを有効にします。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ポリシー 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 Bengaluru 17.6.1	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

例

次に、各ポリシープロファイルのリンクローカルブリッジングを有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# link-local-bridging
```

load

サイトタグベースのロードバランシングを設定するには、**load** コマンドを使用します。

load *load*

構文の説明

load	サイト用に予約する相対負荷の推定値を指定します。 値の範囲は 0 ～ 1000 です。デフォルト値の 0 は、サイトの負荷に関する推奨事項がないことを意味します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.10.1	このコマンドが導入されました。

次に、サイトタグベースのロードバランシングを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless tag site area1
Device(config-site-tag)# load 200
Device(config-site-tag)# end
```

local-admin-mac deny

ローカルで管理されているアドレスを使用したクライアントの関連付けを拒否するには、**local-admin-mac deny** コマンドを使用します。この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。

local-admin-mac deny

no local-admin-mac deny

構文の説明

local-admin-mac	ローカルで管理されている MAC アドレスを指定します。
deny	ローカルで管理されているアドレスを使用したクライアントの関連付けを拒否します

コマンド デフォルト

なし

コマンド モード

WLAN コンフィギュレーション モード（config-wlan）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、ローカルで管理されているアドレスを使用したクライアントの関連付けを拒否する例を示します。

```
Device# configure terminal
Device(config)# wlan wlan-test 3 ssid-test
Device(config-wlan)# shutdownDevice(config-wlan)# [no] local-admin-mac deny
Device(config-wlan)# no shutdown
```

local-auth ap eap-fast

EAP Fast 方式を使用した Flex ポリシーのローカル認証を設定するには、**local-auth ap eap-fast** コマンドを使用します。

local-auth ap eap-fast *profile-name*

構文の説明

profile-name	eap-fast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

config-wireless-flex-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次の例は、EAP Fast 方式での Flex ポリシーの認証を設定する方法を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile flex profile-name
Device(config-wireless-flex-profile)# local-auth ap eap-fast eap-fast-profile-name
```

local-site

サイトをローカル サイトとして設定するには、 **local-site** コマンドを使用します。

local-site

構文の説明	**local-site** このサイトをローカルサイトとして設定します。
コマンド デフォルト	なし
コマンド モード	config-site-tag

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、現在のサイトをローカル サイトとして設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless tag site tag-name
Device(config-site-tag)# local-site
```

location expiry

ロケーションの有効期間を設定するには、グローバル コンフィギュレーション モードで**location expiry** コマンドを使用します。

location expiry {**calibrating-client** | **client** | **tags** }*timeout-duration*

構文の説明

calibrating-client	調整クライアントのタイムアウト値。
client	クライアントのタイムアウト値。
tags	RFID タグのタイムアウト値。
timeout-duration	タイムアウト時間（秒）。

コマンド デフォルト

タイムアウト値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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、ロケーションの有効期間を設定する例を示します。

```
Device(config)# location expiry tags 50
```

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 **location notify-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 Gibraltar 16.10.1	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。

```
デバイス# configure terminal
デバイス(config)# location notify-threshold client 10
デバイス(config)# end
```

login authentication

ログイン認証パラメータを設定するには、**login authentication** コマンドを使用します。

login authentication *word* **default**

構文の説明

word	名前を記した認証リスト。
default	デフォルトの認証リストを使用します。

コマンド デフォルト

なし

コマンド モード

ライン 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ログイン認証を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# line console 0
Device(config-line)# login authentication NO_LOGIN
```

lsc-only-auth（メッシュ）

ローカルで有効な証明書（LSC）専用の MAP 認証にメッシュ セキュリティを設定するには、**lsc-only-auth** コマンドを使用します。

lsc-only-auth

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

LSC 専用認証はイネーブルになっています。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、LSC 専用 MAP 認証にメッシュ セキュリティを設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# lsc-only-auth
```

mac-filtering

WLAN 上で MAC フィルタリングを有効にするには、 **mac-filtering** コマンドを使用します。

mac-filtering ［*mac-authorization-list* ］

構文の説明

mac-authorization-list	許可リストの名前。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、WLAN で MAC フィルタリングをイネーブルにする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan-name wlan-index SSID-name
Device(config-wlan)# mac-filtering
```

mab request format attribute

WLAN で MAC フィルタリングを設定するときにデリミタを設定するには、グローバル コンフィギュレーション モードで **mab request format attribute** コマンドを使用します。WLAN で MAC フィルタリングを設定するときにデリミ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。

mab request format attribute { **1 groupsize** *size* **separator** *separator* [**lowercase** | **uppercase**] | **2** { **0** | **7** | **LINE** } **LINE** *password* | **32 vlan access-vlan** }

no mab request format attribute { **1 groupsize** *size* **separator** *separator* [**lowercase** | **uppercase**] | **2** { **0** | **7** | **LINE** } **LINE** *password* | **32 vlan access-vlan** }

構文の説明

1	MAB 要求に使用するユーザー名形式を指定します。
groupsize *size*	グループごとの 16 進数の桁数を指定します。 有効な値の範囲は 1 ～ 12 です。
separator *separator*	グループを区切る方法を指定します。 区切り文字は、ハイフン（-）、コロン（:）、およびピリオド（.）です。 groupsize と separator の詳細については、「Overview of the Configurable MAB Username and Password」を参照してください。
lowercase	ユーザー名を小文字で指定します。
uppercase	ユーザー名を大文字で指定します。
2	すべての MAB 要求に使用するグローバル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。
7	非表示のパスワードを指定します。
LINE	暗号化されたパスワードまたは暗号化されていないパスワードを指定します。
password	回線パスワード。
32	NAS-Identifier 属性を指定します。
vlan	VLAN を指定します。
access-vlan	設定されたアクセス 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

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例：

次に、MAC フィルタリングを設定するときにデリミタを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# mab request format attribute 1 groupsize 4 separator -
```

mbo

WLAN で WiFi Alliance Agile Multiband（MBO）を設定するには、**mbo** コマンドを使用します。

mbo

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

MBO は有効になっていません。

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 Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

次に、WLAN で WiFi Alliance Agile Multiband（MBO）を設定する例を示します。

```
Device# configure terminal
Device(config)# wlan wlan-demo 1 ssid-demo
Device(config-wlan)# mbo
Device(config-wlan)# end
```

（注） WLAN での MBO の設定時に WPA2 WLAN を使用する場合は、設定で PMF を有効にする必要があります。

management gateway-failover enable

ゲートウェイモニタリングを有効にするには、**management gateway-failover enable** コマンドを使用します。ゲートウェイ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。

management gateway-failover enable
no management gateway-failover 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

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 Amsterdam 17.1.1s	このコマンドが導入されました。

次に、ゲートウェイモニタリングを有効にする例を示します。

```
Device# configure terminal
Device(config)# management gateway-failover enable
Device(config)# end
```

management gateway-failover interval

ゲートウェイのモニタリング間隔を設定するには、**management gateway-failover interval** コマンドを使用します。

management gateway-failover interval *interval-value*

構文の説明

interval-value	ゲートウェイのモニタリング間隔を示します。有効な範囲は 6 ～ 12 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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.4.1	このコマンドが導入されました。

使用上のガイドライン

次に、ゲートウェイのモニタリング間隔を設定する例を示します。

```
Device# configure terminal
Device(config)# management gateway-failover interval 6
Device(config)# end
```

map-fast-ancestor-find

ワイヤレス メッシュ プロファイルで MAP Fast Ancestor Find モードを設定するには、**map-fast-ancestor-find** コマンドを使用します。

map-fast-ancestor-find

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

ワイヤレス メッシュ プロファイル コンフィギュレーション（config-wireless-mesh-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.11.1	このコマンドが導入されました。

例

次に、メッシュ AP プロファイルに MAP Fast Ancestor Find モードを設定する例を示します。

```
Device # configure terminal
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# map-fast-ancestor-find
```

match activated-service-template

セッションでアクティブ化されているサービス テンプレートに基づいて true と評価される条件を作成するには、コントロール クラスマップ フィルタ コンフィギュレーション モードで **match activated-service-template** コマンドを使用します。セッションでアクティブ化されているサービス テンプレートが指定されたテンプレートと一致しない場合に true と評価する条件を作成するには、コントロール クラスマップ フィルタ コンフィギュレーション モードで **no-match activated-service-template** コマンドを使用します。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。

match activated-service-template *template-name*
no-match activated-service-template *template-name*
no {**match** | **no-match**} **activated-service-template** *template-name*

構文の説明

template-name	**service-template** コマンドによって定義された、設定されているサービス テンプレートの名前。

コマンド デフォルト

コントロール クラスには、サービス テンプレートに基づく条件は含まれていません。

コマンド モード

コントロール クラスマップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

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

使用上のガイドライン

match activated-service-template コマンドは、セッションに適用されているサービス テンプレートに基づいて、コントロール クラスの一致条件を設定します。コントロール クラスには複数の条件を含めることができ、各条件は true または false の評価を行います。コントロール クラスは、コントロール ポリシーのアクションを実行するためには、条件のすべてまたはいずれかが true と評価される必要があるか、あるいはいずれも true と評価されてはならないかを定義します。

このコマンドの **no-match** 形式は、結果が不一致になる値を指定します。指定した一致基準以外のすべての値は、結果が一致になります。たとえば、**no-match activated-service-template SVC_1** コマンドを設定すると、SVC_1 を除くすべてのテンプレート値が一致として受け入れられます。

class コマンドは、コントロール クラスをコントロール ポリシーに関連付けます。

例

次に、VLAN_1 という名前のサービス テンプレートがセッションでアクティブになっている場合に true と評価するコントロール クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match activated-service-template VLAN_1
```

関連コマンド

コマンド	説明
activate (policy-map action)	加入者セッションのコントロールポリシーまたはサービス テンプレートをアクティブ化します。
class	制御ポリシーを制御クラスの 1 つ以上のアクションに関連付けます。
match service-template	イベントのサービス テンプレートに基づいて true と評価される条件を作成します。
service-template	加入者セッションに適用する一連のサービス ポリシー属性が含まれるテンプレートを定義します。

match any

デバイスを通過するすべてのプロトコルで照合を実行するには、**match any** コマンドを使用します。

match any

コマンド デフォルト

なし

コマンド モード

config-cmap

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、デバイスを通過するすべてのパケットを照合する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map cmap-name
Device(config-cmap)# match any
```

match application name

フロー レコードのキー フィールドとしてアプリケーション名を使用するように設定するには、フロー レコード コンフィギュレーション モードで **match application name** コマンドを使用します。アプリケーション名をフロー レコードのキー フィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します。

match application name
no match application name

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

アプリケーション名はキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション（config-flow-record）

コマンド履歴

リリース	変更内容
15.0(1)M	このコマンドが導入されました。
15.2(2)T	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 15.2(2)T に統合されました。
Cisco IOS XE Release 3.5S	このコマンドが Cisco Performance Monitor 用に Cisco IOS XE Release 3.5S に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、このコマンドを発行するコンフィギュレーション モードを開始するために異なるコマンドを使用しますが、モード プロンプトは両方の製品で共通しています。Performance Monitor では、このコマンドを使用する前に、まず **flow record type performance-monitor** コマンドを入力する必要があります。

モード プロンプトは両方の製品で共通しているため、ここでは両方の製品のコマンド モードをフロー レコード コンフィギュレーション モードと呼びます。ただし、Flexible NetFlow の場合、このモードは Flexible NetFlow フロー レコード コンフィギュレーション モードとも呼ばれます。Performance Monitor の場合、このモードは Performance Monitor フロー レコード コンフィギュレーション モードとも呼ばれます。

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを差別化するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

例

次に、アプリケーション名をキー フィールドとして設定する例を示します。

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match application name
```

Cisco IOS リリース 15.2(2)T および XE 3.5S での Cisco Performance Monitor

次に、アプリケーション名をキー フィールドとして設定する例を示します。

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match application name
```

関連コマンド

コマンド	説明
collect application name	Flexible NetFlow のフロー レコードで、アプリケーション名を非キー フィールドとして使用するように設定します。
flow record	フロー レコードを作成し、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。
flow record type performance-monitor	フロー レコードを作成し、Performance Monitor フロー レコード コンフィギュレーション モードを開始します。

match day

日または一般的な日のグループ（週末または平日）を使用して照合を実行するには、 **match day** コマンドを使用します。

match day *day-string*

コマンド デフォルト

なし

コマンド モード

フィルタ コントロール クラスマップ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドが機能するためには、AAA オーバーライドも無効にする必要があります。

例

次に、日を使用して照合を実行する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-all class-map-name
Device(config-filter-control-classmap)# match day day-string
```

match device-type

デバイス タイプを使用して照合を実行するには、 **match device-type** コマンドを使用します。

match device-type*device-type*

コマンド デフォルト なし

コマンド モード フィルタ コントロール クラスマップ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	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 リストに入力するには、デバイス分類子を有効にする必要があります。

例

次に、デバイス タイプを使用して照合を実行する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-allclass-map-name
Device(config-filter-control-classmap)# match device-type device-type
```

match eap-type

拡張認証プロトコル（EAP）を使用して照合を実行するには、**match eap-type** コマンドを使用します。

match eap-type {**fast** | **gtc** | **leap** | **md5** | **mschapv2** | **peap** | **tls**}

構文の説明

fast	セキュア トンネリングを介したフレキシブル認証
gtc	汎用トークン カード
leap	Lightweight Extensible Authentication Protocol。
md5	MD5-tunneled Authentication Protocol。
mschapv2	MSCHAPV2 認証メカニズム。
peap	保護拡張認証プロトコル。
tls	Transport Layer Security。

コマンド デフォルト

なし

コマンド モード

フィルタ コントロール クラスマップ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドが機能するためには、AAA オーバーライドも無効にする必要があります。

例

次に、eap-type PEAP を使用して一致を実行する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-all class-map-name
Device(config-filter-control-classmap)# match eap-type  peap
```

match interface

入力インターフェイスと出力インターフェイスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match interface** コマンドを使用します。入力インターフェイスと出力インターフェイスをフロー レコードのキー フィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します。

match interface {**input** | **output**}
no match interface {**input** | **output**}

構文の説明

input	入力インターフェイスをキー フィールドとして設定します。
output	出力インターフェイスをキー フィールドとして設定します。

コマンド デフォルト

入力インターフェイスと出力インターフェイスは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次に、入力インターフェイスをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match interface input
```

次に、出力インターフェイスをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match interface output
```

match ipv4

フロー レコードのキー フィールドとして 1 つ以上の IPv4 フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv4** コマンドを使用します。フロー レコードのキー フィールドとして 1 つ以上の IPv4 フィールドを使用する設定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。

match ipv4 {**destination address** | **protocol** | **source address** | **tos** | **version**}
no match ipv4 {**destination address** | **protocol** | **source address** | **tos** | **version**}

構文の説明

destination address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv4 destination address （636 ページ）を参照してください。
protocol	キー フィールドとして IPv4 プロトコルを設定します。
source address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv4 source address （638 ページ）を参照してください。
tos	キー フィールドとして IPv4 ToS を設定します。
version	キー フィールドとして IPv4 ヘッダーの IP バージョンを設定します。

コマンド デフォルト

ユーザ定義のフロー レコードのキー フィールドとして 1 つ以上の IPv4 フィールドを使用する設定は、イネーブルになっていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、キー フィールドとして IPv4 プロトコルを設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 protocol
```

match ipv4

フロー レコードのキー フィールドとして 1 つ以上の IPv4 フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv4** コマンドを使用します。フロー レコードのキー フィールドとして 1 つ以上の IPv4 フィールドを使用する設定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。

match ipv4 {**destination address** | **protocol** | **source address** | **tos** | **version**}
no match ipv4 {**destination address** | **protocol** | **source address** | **tos** | **version**}

構文の説明

destination address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv4 destination address （636 ページ）を参照してください。
protocol	キー フィールドとして IPv4 プロトコルを設定します。
source address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv4 source address （638 ページ）を参照してください。
tos	キー フィールドとして IPv4 ToS を設定します。
version	キー フィールドとして IPv4 ヘッダーの IP バージョンを設定します。

コマンド デフォルト

ユーザ定義のフロー レコードのキー フィールドとして 1 つ以上の IPv4 フィールドを使用する設定は、イネーブルになっていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、キー フィールドとして IPv4 プロトコルを設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 protocol
```

match ipv4 destination address

IPv4 宛先アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 destination address** コマンドを使用します。IPv4 宛先アドレスをフロー レコードのキー フィールドとして使用する設定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。

match ipv4 destination address
no match ipv4 destination 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

IPv4 宛先アドレスはキー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv4 destination address** または **default match ipv4 destination address** フロー レコード 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、IPv4 宛先アドレスをフロー レコードのキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 destination address
```

match ipv4 destination address

IPv4 宛先アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 destination address** コマンドを使用します。IPv4 宛先アドレスをフロー レコードのキー フィールドとして使用する設定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。

match ipv4 destination address
no match ipv4 destination 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

IPv4 宛先アドレスはキー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv4 destination address** または **default match ipv4 destination address** フロー レコード 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、IPv4 宛先アドレスをフロー レコードのキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 destination address
```

match ipv4 source address

IPv4 送信元アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 source address** コマンドを使用します。フロー レコードのキー フィールドとして IPv4 送信元アドレスを使用する設定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。

match ipv4 source address
no match ipv4 source 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

IPv4 送信元アドレスがキー フィールドとして設定されません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv4 source address** または **default match ipv4 source address** フロー レコード コンフィギュレーション コマンドを使用します。

次に、キー フィールドとして IPv4 送信元アドレスを設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 source address
```

match ipv4 source address

IPv4 送信元アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 source address** コマンドを使用します。フロー レコードのキー フィールドとして IPv4 送信元アドレスを使用する設定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。

match ipv4 source address
no match ipv4 source 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

IPv4 送信元アドレスがキー フィールドとして設定されません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv4 source address** または **default match ipv4 source address** フロー レコード コンフィギュレーション コマンドを使用します。

次に、キー フィールドとして IPv4 送信元アドレスを設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 source address
```

match ipv4 ttl

フロー レコードのキー フィールドとして IPv4 存続可能時間（TTL）フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 ttl** コマンドを使用します。フロー レコードのキー フィールドとして IPv4 TTL を使用する設定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。

match ipv4 ttl
no match ipv4 ttl

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

IPv4 存続可能時間（TTL）フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match ipv4 ttl** コマンドを使用して定義されます。

次に、キー フィールドとして IPv4 TTL を設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 ttl
```

match ipv4 ttl

フロー レコードのキー フィールドとして IPv4 存続可能時間（TTL）フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 ttl** コマンドを使用します。フロー レコードのキー フィールドとして IPv4 TTL を使用する設定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。

match ipv4 ttl
no match ipv4 ttl

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

IPv4 存続可能時間（TTL）フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match ipv4 ttl** コマンドを使用して定義されます。

次に、キー フィールドとして IPv4 TTL を設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 ttl
```

match ipv6

フロー レコードのキー フィールドとして 1 つ以上の IPv6 フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv6** コマンドを使用します。フロー レコードのキー フィールドとして 1 つ以上の IPv6 フィールドを使用する設定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。

match ipv6 {**destination address** | **protocol** | **source address** | **traffic-class** | **version**}
no match ipv6 {**destination address** | **protocol** | **source address** | **traffic-class** | **version**}

構文の説明

destination address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv6 destination address （644 ページ）を参照してください。
protocol	キー フィールドとして IPv6 プロトコルを設定します。
source address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv6 source address （648 ページ）を参照してください。

コマンド デフォルト

IPv6 の各フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、キー フィールドとして IPv6 プロトコル フィールドを設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 protocol
```

match ipv6

フロー レコードのキー フィールドとして 1 つ以上の IPv6 フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv6** コマンドを使用します。フロー レコードのキー フィールドとして 1 つ以上の IPv6 フィールドを使用する設定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。

match ipv6 {**destination address** | **protocol** | **source address** | **traffic-class** | **version**}
no match ipv6 {**destination address** | **protocol** | **source address** | **traffic-class** | **version**}

構文の説明

destination address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv6 destination address （644 ページ）を参照してください。
protocol	キー フィールドとして IPv6 プロトコルを設定します。
source address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv6 source address （648 ページ）を参照してください。

コマンド デフォルト

IPv6 の各フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、キー フィールドとして IPv6 プロトコル フィールドを設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 protocol
```

match ipv6 destination address

IPv6 宛先アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 destination address** コマンドを使用します。IPv6 宛先アドレスをフロー レコードのキー フィールドとして使用する設定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。

match ipv6 destination address
no match ipv6 destination 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

IPv6 宛先アドレスはキー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv6 destination address** または **default match ipv6 destination address** フロー レコード 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、キー フィールドとして IPv6 宛先アドレスを設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 destination address
```

match ipv6 destination address

IPv6 宛先アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 destination address** コマンドを使用します。IPv6 宛先アドレスをフロー レコードのキー フィールドとして使用する設定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。

match ipv6 destination address
no match ipv6 destination 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

IPv6 宛先アドレスはキー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv6 destination address** または **default match ipv6 destination address** フロー レコード 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、キー フィールドとして IPv6 宛先アドレスを設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 destination address
```

match ipv6 hop-limit

フロー レコードのキー フィールドとしてIPv6ホップ リミットを設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 hop-limit** コマンドを使用します。フロー レコードのキー フィールドとして IPv6 パケットのセクションを使用する設定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。

match ipv6 hop-limit
no match ipv6 hop-limit

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

ユーザ定義のフロー レコードのキー フィールドとして IPv6 ホップ リミットを使用する設定は、デフォルトでイネーブルになっていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

次に、キー フィールドとしてフロー パケットのホップ リミットを設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 hop-limit
```

match ipv6 hop-limit

フロー レコードのキー フィールドとしてIPv6ホップ リミットを設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 hop-limit** コマンドを使用します。フロー レコードのキー フィールドとして IPv6 パケットのセクションを使用する設定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。

match ipv6 hop-limit
no match ipv6 hop-limit

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

ユーザ定義のフロー レコードのキー フィールドとして IPv6 ホップ リミットを使用する設定は、デフォルトでイネーブルになっていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

次に、キー フィールドとしてフロー パケットのホップ リミットを設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 hop-limit
```

match ipv6 source address

IPv6 送信元アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 source address** コマンドを使用します。フロー レコードのキー フィールドとして IPv6 送信元アドレスを使用する設定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。

match ipv6 source address
no match ipv6 source 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

IPv6 送信元アドレスはキー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv6 source address** または **default match ipv6 source address** フロー レコード コンフィギュレーション コマンドを使用します。

次に、IPv6 送信元アドレスをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 source address
```

match ipv6 source address

IPv6 送信元アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 source address** コマンドを使用します。フロー レコードのキー フィールドとして IPv6 送信元アドレスを使用する設定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。

match ipv6 source address
no match ipv6 source 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

IPv6 送信元アドレスはキー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv6 source address** または **default match ipv6 source address** フロー レコード コンフィギュレーション コマンドを使用します。

次に、IPv6 送信元アドレスをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 source address
```

match join-time-of-day

日における時刻を使用して照合を実行するには、 **match join-time-of-day** コマンドを使用します。

match join-time-of-day *start-time end-time*

コマンド デフォルト

なし

コマンド モード

フィルタ コントロール クラスマップ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

照合で参加時刻が考慮されます。たとえば、照合フィルタが午前 11:00 から午後 2:00 に設定されている場合、午前 10:59 に参加するデバイスは、午前 11:00 より後にクレデンシャルを取得しても考慮されません。

このコマンドが機能するためには、AAA オーバーライドも無効にする必要があります。

例

次に、参加時刻を使用して照合を実行する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-all class-map-name
Device(config-filter-control-classmap)# match join-time-of-day start-time end-time
```

match message-type

サービス リストを照合するメッセージ タイプを設定するには、**match message-type** コマンドを使用します。

match message-type {**announcement** | **any** | **query**}

構文の説明

announcement	デバイス のサービス アドバタイズメントまたはアナウンスメントのみを許可します。
any	任意の照合タイプを許可します。
query	ネットワーク内の特定の デバイス に対するクライアントからクエリのみを許可します。

コマンド デフォルト

なし

コマンド モード

サービス 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

異なるシーケンス番号を持つ同じ名前の複数のサービスマップを作成することができ、フィルタの評価順序はシーケンス番号に基づきます。サービス リストは、それぞれが許可または拒否の結果を持つ個々の文を一定の順序で並べたものです。サービス リストの評価は、事前に定義された順序でのリストのスキャンと、一致する各文の基準の評価で構成されています。リストのスキャンは、文の一致が初めて見つかり、その文に関連付けられたアクション permit または deny が実行されると停止します。リスト全体をスキャンした後のデフォルトのアクションは deny です。

（注） **service-list mdns-sd** *service-list-name* **query** コマンドを使用していた場合、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションに対してのみ使用できます。

例

次に、照合されるアナウンスメント メッセージ タイプを設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match message-type announcement
```

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 **match non-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 Gibraltar 16.10.1	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、NRT で非クライアントを設定する例を示します。

```
デバイス(config)# class-map test_1000
デバイス(config-cmap)# match non-client-nrt
```

match protocol

指定されたプロトコルに基づいてクラス マップの一致基準を設定するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **match protocol** コマンドを使用します。プロトコルベースの一致基準をクラス マップから削除するには、このコマンドの **no** 形式を使用します。**match protocol** コマンドの詳細については、『*Cisco IOS Quality of Service Solutions Command Reference*』を参照してください。

match protocol {*protocol-name* | **attribute category** *category-name* | **attribute sub-category** *sub-category-name* | **attribute application-group** *application-group-name*}

構文の説明

protocol-name	一致基準として使用されるプロトコルの名前です（bgp など）。
category-name	一致基準として使用するアプリケーション カテゴリの名前です。
sub-category-name	一致基準として使用するアプリケーションサブカテゴリの名前です。
application-group-name	一致基準とするアプリケーション グループの名前です。アプリケーション名を指定すると、アプリケーション グループの代わりにアプリケーションが一致基準として設定されます。

コマンド デフォルト

一致基準は設定されていません。

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、match protocol でアプリケーション名、カテゴリ、およびサブ カテゴリのフィルタを適用してクラス マップを作成する例を示します。

```
デバイス# configure terminal
デバイス(config)# class-map cat-browsing
デバイス(config-cmap)# match protocol attribute category browsing
デバイス(config-cmap)#end

デバイス# configure terminal
デバイス(config)# class-map cat-fileshare
デバイス(config-cmap)# match protocol attribute category file-sharing
デバイス(config-cmap)#end

デバイス# configure terminal
デバイス(config)# class-map match-any subcat-terminal
デバイス(config-cmap)# match protocol attribute sub-category terminal
デバイス(config-cmap)#end
```

```
デバイス# configure terminal
デバイス(config)# class-map match-any webex-meeting
デバイス(config-cmap)# match protocol webex-meeting
デバイス(config-cmap)#end
```

次に、ポリシー マップを作成し、アップストリーム QoS の既存のクラス マップを定義する例を示します。

```
デバイス# configure terminal
デバイス(config)# policy-map test-avc-up
デバイス(config-pmap)# class cat-browsing
デバイス(config-pmap-c)# police 150000
デバイス(config-pmap-c)# set dscp 12
デバイス(config-pmap-c)#end
```

```
デバイス# configure terminal
デバイス(config)# policy-map test-avc-up
デバイス(config-pmap)# class cat-fileshare
デバイス(config-pmap-c)# police 1000000
デバイス(config-pmap-c)# set dscp 20
デバイス(config-pmap-c)#end
```

```
デバイス# configure terminal
デバイス(config)# policy-map test-avc-up
デバイス(config-pmap)# class subcat-terminal
デバイス(config-pmap-c)# police 120000
デバイス(config-pmap-c)# set dscp 15
デバイス(config-pmap-c)#end
```

```
デバイス# configure terminal
デバイス(config)# policy-map test-avc-up
デバイス(config-pmap)# class webex-meeting
デバイス(config-pmap-c)# police 50000000
デバイス(config-pmap-c)# set dscp 21
デバイス(config-pmap-c)#end
```

次に、ポリシー マップを作成し、ダウンストリーム QoS の既存のクラス マップを定義する例を示します。

```
デバイス# configure terminal
デバイス(config)# policy-map test-avc-down
デバイス(config-pmap)# class cat-browsing
デバイス(config-pmap-c)# police 200000
デバイス(config-pmap-c)# set dscp 10
デバイス(config-pmap-c)#end
```

```
デバイス# configure terminal
デバイス(config)# policy-map test-avc-up
デバイス(config-pmap)# class cat-fileshare
デバイス(config-pmap-c)# police 300000
```

```
デバイス(config-pmap-c)# set wlan user-priority 2
デバイス(config-pmap-c)# set dscp 20
デバイス(config-pmap-c)#end
```

```
デバイス# configure terminal
デバイス(config)# policy-map test-avc-up
デバイス(config-pmap)# class subcat-terminal
デバイス(config-pmap-c)# police 100000
デバイス(config-pmap-c)# set dscp 25
デバイス(config-pmap-c)#end
```

```
デバイス# configure terminal
デバイス(config)# policy-map test-avc-up
デバイス(config-pmap)# class webex-meeting
デバイス(config-pmap-c)# police 60000000
デバイス(config-pmap-c)# set dscp 41
デバイス(config-pmap-c)#end
```

次に、定義された QoS ポリシーを WLAN に適用する例を示します。

```
デバイス# configure terminal
デバイス(config)#wlan  alpha
デバイス(config-wlan)#shut
デバイス(config-wlan)#end
デバイス(config-wlan)#service-policy client input test-avc-up
デバイス(config-wlan)#service-policy client output test-avc-down
デバイス(config-wlan)#no shut
デバイス(config-wlan)#end
```

match service-instance

サービス リストを照合するサービス インスタンスを設定するには、**match service-instance** コマンドを使用します。

match service-instance *line*

構文の説明

line	パケット内のサービスインスタンスを照合するための正規表現。

コマンド デフォルト

なし

コマンド モード

サービス 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

service-list mdns-sd *service-list-name* **query** コマンドを使用していた場合、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションに対してのみ使用できます。

例

次に、照合するサービス インスタンスを設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match service-instance servInst 1
```

match service-type

照合する mDNS サービス タイプ文字列値を設定するには、**match service-type** コマンドを使用します。

match service-type *line*

構文の説明

line	パケット内のサービス タイプを照合するための正規表現。

コマンド デフォルト

なし

コマンド モード

サービス 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

service-list mdns-sd *service-list-name* **query** コマンドを使用していた場合、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションに対してのみ使用できます。

例

次に、照合する mDNS サービス タイプ文字列値を設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match service-type _ipp._tcp
```

match transport

フロー レコードのキー フィールドとして 1 つ以上のトランスポート フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match transport** コマンドを使用します。フロー レコードのキー フィールドとして 1 つ以上のトランスポート フィールドを使用する設定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。

構文の説明

destination-port	キー フィールドとしてトランスポート宛先ポートを設定します。
source-port	キー フィールドとしてトランスポート送信元ポートを設定します。

コマンド デフォルト

トランスポート フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、宛先ポートをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport destination-port
```

次の例では、送信元ポートをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport source-port
```

match transport

フロー レコードのキー フィールドとして 1 つ以上のトランスポート フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match transport** コマンドを使用します。フロー レコードのキー フィールドとして 1 つ以上のトランスポート フィールドを使用する設定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。

構文の説明

destination-port	キー フィールドとしてトランスポート宛先ポートを設定します。
source-port	キー フィールドとしてトランスポート送信元ポートを設定します。

コマンド デフォルト

トランスポート フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、宛先ポートをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport destination-port
```

次の例では、送信元ポートをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport source-port
```

match transport icmp ipv4

ICMP IPv4 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match transport icmp ipv4** コマンドを使用します。ICMP IPv4 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして使用するの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。

match transport icmp ipv4 {**code** | **type**}
no match transport icmp ipv4 {**code** | **type**}

構文の説明

code	ICMP IPv4 コードをキー フィールドとして設定します。
type	ICMP IPv4 タイプをキー フィールドとして設定します。

コマンド デフォルト

ICMP IPv4 のタイプ フィールドとコード フィールドはキー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次に、ICMP IPv4 コード フィールドをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv4 code
```

次に、ICMP IPv4 タイプ フィールドをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv4 type
```

match transport icmp ipv4

ICMP IPv4 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match transport icmp ipv4** コマンドを使用します。ICMP IPv4 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして使用するの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。

match transport icmp ipv4 {**code** | **type**}
no match transport icmp ipv4 {**code** | **type**}

構文の説明

code	ICMP IPv4 コードをキー フィールドとして設定します。
type	ICMP IPv4 タイプをキー フィールドとして設定します。

コマンド デフォルト

ICMP IPv4 のタイプ フィールドとコード フィールドはキー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次に、ICMP IPv4 コード フィールドをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv4 code
```

次に、ICMP IPv4 タイプ フィールドをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv4 type
```

match transport icmp ipv6

ICMP IPv6 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match transport icmp ipv6** コマンドを使用します。ICMP IPv6 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして使用するの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。

match transport icmp ipv6 {**code** | **type**}
no match transport icmp ipv6 {**code** | **type**}

構文の説明

code	IPv6 ICMP コードをキー フィールドとして設定します。
type	IPv6 ICMP タイプをキー フィールドとして設定します。

コマンド デフォルト

ICMP IPv6 タイプ フィールドおよびコード フィールドはキー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、IPv6 ICMP コード フィールドをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv6 code
```

次の例では、IPv6 ICMP タイプ フィールドをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv6 type
```

match transport icmp ipv6

ICMP IPv6 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match transport icmp ipv6** コマンドを使用します。ICMP IPv6 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして使用するの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。

match transport icmp ipv6 {**code** | **type**}
no match transport icmp ipv6 {**code** | **type**}

構文の説明

code	IPv6 ICMP コードをキー フィールドとして設定します。
type	IPv6 ICMP タイプをキー フィールドとして設定します。

コマンド デフォルト

ICMP IPv6 タイプ フィールドおよびコード フィールドはキー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、IPv6 ICMP コード フィールドをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv6 code
```

次の例では、IPv6 ICMP タイプ フィールドをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv6 type
```

match user-role

クラスマップ属性フィルタ条件を設定するには、**match user-role** コマンドを使用します。

match user-role ユーザ ロール

コマンド デフォルト

なし

コマンド モード

config-filter-control-classmap

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、クラス マップ属性フィルタ条件を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-any map-name
Device(config-filter-control-classmap)# match user-role user-role
```

match username

イベントのユーザ名に基づいて true と評価される条件を作成するには、コントロール クラスマップ フィルタ コンフィギュレーション モードで **match username** コマンドを使用します。イベントのユーザ名が指定されたユーザ名と一致しない場合に true と評価される条件を作成するには、コントロール クラスマップ フィルタ コンフィギュレーション モードで **no-match username** コマンドを使用します。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。

match username *username*
no-match username *username*
no {**match** | **no-match**} **username** *username*

構文の説明

username	ユーザー名。

コマンド デフォルト

コントロール クラスには、イベントのユーザ名に基づく条件は含まれていません。

コマンド モード

コントロール クラスマップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

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

使用上のガイドライン

match username コマンドは、ユーザ名に基づいて、コントロール クラスの一致条件を設定します。制御クラスには複数の条件を含めることができ、各条件は true または false の評価を行います。コントロール クラスは、コントロール ポリシーのアクションを実行するためには、条件のすべてまたはいずれかが true と評価される必要があるか、あるいはいずれも true と評価されてはならないかを定義します。

このコマンドの **no-match** 形式は、結果が不一致になる値を指定します。指定した一致基準以外のすべての値は、結果が一致になります。たとえば、**no-match username josmithe** コマンドを設定すると、コントロール クラスは josmithe を除くすべてのユーザ名の値を一致として受け入れます。

class コマンドは、コントロール クラスをコントロール ポリシーに関連付けます。

例

次に、ユーザ名が josmithe である場合に true と評価するコントロール クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match username josmithe
```

関連コマンド

コマンド	説明
class	制御ポリシーを制御クラスの1つ以上のアクションに関連付けます。
policy-map type control subscriber	加入者セッションに対するコントロール ポリシーを定義します

match wireless ssid（ワイヤレス）

ワイヤレス ネットワークの SSID をフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match wireless ssid** コマンドを使用します。ワイヤレス ネットワークの SSID をフロー レコードのキー フィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します

match wireless ssid
no match wireless ssid

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

ワイヤレス ネットワークの SSID はキー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを差別化するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次に、ワイヤレス ネットワークの SSID をキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match wireless ssid
```

match wireless ssid（ワイヤレス）

ワイヤレス ネットワークの SSID をフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match wireless ssid** コマンドを使用します。ワイヤレス ネットワークの SSID をフロー レコードのキー フィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します

match wireless ssid
no match wireless ssid

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

ワイヤレス ネットワークの SSID はキー フィールドとして設定されていません。

コマンド モード

フロー レコード 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 XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを差別化するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次に、ワイヤレス ネットワークの SSID をキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match wireless ssid
```

match（アクセス マップ コンフィギュレーション）

VLANマップを1つまたは複数のアクセスリストとパケットを照合するように設定するには、アクセスマップ コンフィギュレーションモードで**match**コマンドを使用します。一致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*}]...|**mac address** *name* [*name*] [*name*]...}
{**no match ip 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。
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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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、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 アドレスと MAC アドレスの両方を指定できます。

例

次の例では、VLAN アクセス マップ *vmap4* を定義し 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。

```
デバイス(config)# vlan access-map vmap4
デバイス(config-access-map)# match ip address al2
デバイス(config-access-map)# action drop
デバイス(config-access-map)# exit
デバイス(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。

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。

Cisco IOS XE Everest 16.5.x 以前のリリース

match {**access-group**{**name***acl-name acl-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-name acl-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*}

Cisco IOS XE Everest 16.6.x 以降のリリース

match {**access-group**{**name** *acl-name acl-index*} | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **mpls** *experimental-value* | **non-client-nrt** | **precedence** *precedence-value1...value4* | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **vlan** *vlan-id* | **wlan** *wlan-id*}
no match {**access-group**{**name** *acl-name acl-index*} | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **mpls** *experimental-value* | **non-client-nrt** | **precedence** *precedence-value1...value4* | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **vlan** *vlan-id* | **wlan** *wlan-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 ～ 4094 です。
mpls *experimental-value*	マルチ プロトコル ラベル スイッチングの特定の値を指定します。
non-client-nrt	非クライアントの NRT（非リアルタイム）を照合します。
protocol *protocol-name*	プロトコルのタイプを指定します。
wlan *wlan-id*	802.11 特有の値を識別します。

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 Gibraltar 16.10.1	このコマンドが導入

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-map match-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。

- **match access-group name** *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** コマンドを入力すると、**match ip dscp 10** コマンドを入力した場合と同じになります。**match ip precedence critical** コマンドを入力すると、**match ip precedence 5** コマンドを入力した場合と同じになります。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。

```
デバイス(config)# class-map class2
デバイス(config-cmap)# match ip dscp 10 11 12
デバイス(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。

```
デバイス(config)# class-map class3
デバイス(config-cmap)# match ip precedence 5 6 7
デバイス(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。

```
デバイス(config)# class-map class2
デバイス(config-cmap)# match ip precedence 5 6 7
デバイス(config-cmap)# no match ip precedence
デバイス(config-cmap)# match access-group acl1
デバイス(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。

```
デバイス(config)# class-map match-any class4
デバイス(config-cmap)# match cos 4
デバイス(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。

```
デバイス(config)# class-map match-any class4
デバイス(config-cmap)# match cos 4
デバイス(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 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 **match wlan user-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 Gibraltar 16.10.1	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、ユーザ プライオリティ値を設定する例を示します。

```
デバイス(config)# class-map test_1000
デバイス(config-cmap)# match wlan user-priority 7
```

max-bandwidth

ワイヤレス メディアストリームの予想される最大ストリーム帯域幅を Kbps 単位で設定するには、 **max-bandwidth** コマンドを使用します。

max-bandwidth *bandwidth*

構文の説明

bandwidth	予想される最大ストリーム帯域幅（Kbps 単位）。有効な範囲は 1 ～ 35000 Kbps です。

コマンド デフォルト

なし

コマンド モード

media-stream

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス メディアストリームの帯域幅を Kbps 単位で設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group doc-grp 224.0.0.0 224.0.0.223
Device(config-media-stream)# max-bandwidth 3500
```

max-through

スロットル期間ごとにVLANごとのマルチキャストルータアドバタイズメント（RA）を制限するには、IPv6 RA スロットル ポリシー コンフィギュレーション モードで **max-through** コマンドを使用します。コマンド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。

max-through {*mt-value* | **inherit** | **no-limit**}

構文の説明

mt-value	スロットリングが発生する前にVLANで許可されているマルチキャストRAの数。範囲は 0 ～ 256 です。
inherit	ターゲット ポリシー間で設定をマージします。
no-limit	マルチキャスト RA は、VLAN では制限されません。

コマンド デフォルト

RA は VLAN ごとに 10 分間で 10 回

コマンド モード

IPv6 RA スロットル ポリシー コンフィギュレーション（config-nd-ra-throttle）

コマンド履歴

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

使用上のガイドライン

max-through コマンドは、スロットル期間ごとにVLANに渡されるマルチキャストRAの量を制限します。このコマンドは、VLAN でのみ設定できます。

例

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# max-through 25
```

mdns-sd

mDNSサービス検出ゲートウェイを設定するには、**mdns-sd** コマンドを使用します。この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。

mdns-sd { **gateway** | **service-definition** *service-definition-name* | **service-list** *service-list-name* { **IN** | **OUT** } | **service-policy** *service-policy-name* }

no mdns-sd { **gateway** | **service-definition** *service-definition-name* | **service-list** *service-list-name* { **IN** | **OUT** } | **service-policy** *service-policy-name* }

構文の説明

mdns-sd	mDNSサービス検出ゲートウェイを設定します。
gateway	mDNS ゲートウェイを設定します。
service-definition	mDNS サービス定義を設定します。
service-definition-name	mDNS サービス定義名を指定します。
service-list	mDNS サービスリストを設定します。
service-list-name	mDNS サービス定義名を指定します。
IN	インバウンドフィルタリングを指定します。
OUT	アウトバウンド フィルタリングを指定します。
service-policy	mDNS サービスポリシーを設定します。
service-policy-name	mDNS サービスポリシー名を指定します。

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 Amsterdam 17.3.1	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

例

次に、mDNS サービス検出ゲートウェイを設定する例を示します。

```
Device(config)# mdns-sd gateway
```

mdns-sd flex-profile

mDNS サービス検出 Flex プロファイルを設定するには、**mdns-sd flex-profile** コマンドを使用します。このコマン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。

mdns-sd flex-profile *flex-profile-name*

no mdns-sd flex-profile *flex-profile-name*

構文の説明

mdns-sd flex-profile	mDNS サービス検出 Flex プロファイルを設定します。
flex-profile-name	mDNS Flex プロファイル名を指定します。

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 Amsterdam 17.3.1	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

例

次に、mDNS サービス検出 Flex プロファイルを設定する例を示します。

```
Device(config)# mdns-sd flex-profile mdns-flex-profile
```

mdns-sd profile

mDNS Flex プロファイルをワイヤレス Flex プロファイルに適用するには、ワイヤレス Flex プロファイルモードで**mdns-sd profile** コマンドを使用します。このコマン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。

mdns-sd profile *flex-profile-name*

no mdns-sd profile *flex-profile-name*

構文の説明

mdns-sd profile	ワイヤレス Flex プロファイルの mDNS Flex プロファイルを設定します。
flex-profile-name	mDNS Flex プロファイル名を指定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス Flex 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 Amsterdam 17.3.1	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

例

次に、mDNS Flex プロファイルをワイヤレス Flex プロファイルに適用する例を示します。

```
Device(config-wireless-flex-profile)# mdns-sd profile mdns-flex-profile
```

mdns-sd wired-filter

mDNS 有線フィルタを設定するには、**mdns-sd wired-filter** コマンドを使用します。

mdns-sd wired-filter *wired-filter-name*

構文の説明

wired-filter-name	有線フィルタ名です。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.8.1	このコマンドが導入されました。

使用上のガイドライン

次に、mDNS 有線フィルタを設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# mdns-sd wired-filter WIRED_FILTER_APPLE_TV
Device(config-mdns-wired-filter)# match mac a886.ddb2.05e9
Device(config-mdns-wired-filter)# match vlan 100
Device(config-mdns-wired-filter)# exit
```

method

OSU オペレータのプライマリおよびセカンダリでサポートされるオンラインサインアップ（OSU）方式を設定するには、**method** コマンドを使用します。OSU 方式を削除するには、このコマンドの **no** 形式を使用します。

method {**oma-dm** | **soap-xml-sp**}

構文の説明

oma-dm	OMA-DM を、OSU オペレータのプライマリまたはセカンダリの OSU 方式として設定します。
soap-xml-sp	SOAP または XML-SPP を、OSU オペレータのプライマリまたはセカンダリの OSU 方式として設定します。

コマンド デフォルト

なし

コマンド モード

ANQP OSU プロバイダーの設定（config-anqp-osu-provider）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、OSU オペレータのプライマリおよびセカンダリでサポートされる OSU 方式を設定する例を示します。

```
Device(config-wireless-anqp-server)# osu-provider my-osu
Device(config-anqp-osu-provider)# method soap-xml-spp oma-dm
```

method（メッシュ）

メッシュ AP プロファイルの認証および許可方式を設定するには、**method** コマンドを使用します。

method {**authentication** | **authorization** }*method*

構文の説明

authentication	メッシュ AP 認証の AAA 方式。
authorization	メッシュ AP 許可の AAA 方式。
method	名前付き方式リスト。

コマンド デフォルト

認証および許可方式は設定されていません。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、メッシュ AP プロファイルの認証を設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# method authentication auth1
```

method fast

EAP-FAST 方式をサポートするように EAP プロファイルを設定するには、**method fast** コマンドを使用します。

method fast [**profile** *profile-name*]

構文の説明

profile-name	方式プロファイルを指定します。

コマンド デフォルト

なし

コマンド モード

config-eap-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、EAP プロファイルで EAP Fast 方式を有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# eap profile profile-name
Device(config-eap-profile)# method fast
```

mesh backhaul

無線プロファイルコンフィギュレーションモードでメッシュバックホールを有効にするには、**mesh backhaul** コマンドを使用します。この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。

mesh backhaul

no mesh backhaul

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

ワイヤレス無線プロファイル 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 Cupertino 17.7.1	このコマンドが導入されました。

使用上のガイドライン

特定のスロットでメッシュバックホールを無効にできます。メッシュバックホールは、特定のスロットがバックホール候補にならないようにするために無効にされます。

例

次に、無線プロファイルコンフィギュレーションモードでメッシュバックホールを有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless radio profile radio-profile-name
Device(config-wireless-radio-profile)# mesh backhaul
```

mesh designated downlink

無線プロファイル コンフィギュレーション モードで無線スロットを指定メッシュダウンリンクとして有効にするには、**mesh designated downlink** コマンドを使用します。この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。

mesh designated downlink

no mesh designated downlink

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、このコマンドは無効になっています。デフォルトでは、すべての無線スロットでメッシュが有効になっていて、ダウンリンクとして指定されていません。

コマンド モード

ワイヤレス無線プロファイル 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 Cupertino 17.7.1	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、メッシュ AP のスロット 2 に対してのみ有効です。スロット 2 以外のスロットが指定ダウンリンクとして設定された場合、「Designated downlink is supported only on slot 2 of mesh APs. Associate in the RF tag accordingly.」という警告メッセージが表示されます。

例

次に、無線スロットを指定メッシュダウンリンクとして有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless radio profile radio-profile-name
Device(config-wireless-radio-profile)# mesh designated downlink
```

mgmtuser username

AP 管理用のユーザー名とパスワードを設定するには、**mgmtuser username** コマンドを使用します。この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。

mgmtuser username *username* **password {0 | 8}** *password*

構文の説明

username	AP 管理用のユーザー名を入力します。
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	暗号化パスワード（キー）を設定します。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 17.6.1	このコマンドが導入されました。

例

次に、AP 管理用のユーザー名とパスワードを設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# mgmtuser username myusername password 0
Device(config-ap-profile)# end
```

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** コマンドを使用します。モビリティアンカー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*
no mobility anchor *ip-address*

構文の説明

ip-address	ゲストアンカーのIPアドレスを設定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス 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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、ゲスト アンカリングを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# 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。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# mobility anchor
```

monitor capture（アクセスリスト/クラスマップ）

アクセスリストまたはクラスマップをパケットキャプチャのコアフィルタとして指定してモニターキャプチャを設定するには、特権 EXEC モードで **monitor capture** コマンドを使用します。指定したアクセスリストまたはクラスマップをコアフィルタとして使用したモニターキャプチャを無効にするには、このコマンドの **no** 形式を使用します。

monitor capture *capture-name* { **access-list** *access-list-name* | **class-map** *class-map-name* }
no monitor capture *capture-name* { **access-list** *access-list-name* | **class-map** *class-map-name* }

構文の説明

capture-name	キャプチャの名前。
access-list *access-list-name*	指定した名前のアクセスリストを設定します。
class-map *class-map-name*	指定した名前のクラスマップを設定します。

コマンド デフォルト

指定したアクセスリストまたはクラスマップをパケットキャプチャのコアフィルタとして使用したモニター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 リリース 3.7S	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 access-list コマンドを使用してアクセスリストを設定するか、**monitor capture** コマンドを使用する前に **class-map** コマンドを使用してクラスマップを設定します。クラスマップ、アクセスリスト、または明示的なインラインフィルタをコアフィルタとして指定できます。**monitor capture match** コマンドの入力時にすでにフィルタが指定されている場合は、このコマンドによって既存のフィルタが置き換えられます。

例

次に、既存のアクセス制御リストを使用してコアシステムフィルタを定義する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit any
Device(config-std-nacl)# exit
Device(config)# exit
Device# monitor capture mycap access-list acl1
Device# end
```

次に、既存のクラスマップを使用してコアシステムフィルタを定義する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit any
Device(config-std-nacl)# exit
Device(config)# class-map match-all cmap
Device(config-cmap)# match access-group name acl
Device(config-cmap)# exit
Device(config)# exit
Device# monitor capture mycap class-map classmap1
Device# end
```

monitor capture buffer circular file file-size

循環バッファのファイルを設定するには、**monitor capture** *epc-session-name* **buffer circular file** *no-of-files* **file-size** *per-file-size* コマンドを使用します。

または線形。

monitor capture *epc-session-name* **buffer circular file** *no-of-files* **file-size** *per-file-size*

構文の説明

epc-session-name	EPC セッションキャプチャの名前を指定します。
no-of-files	循環バッファで設定するファイルの数を指定します。設定するファイル数の値の範囲は 2 ～ 5 です。
per-file-size	設定する各ファイルのファイルサイズを指定します。ファイルサイズの値の範囲は 1 MB ～ 500 MB 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 Dublin 17.12.1	このコマンドが導入されました。

使用上のガイドライン

循環が設定されている場合、ファイルはリングバッファとして機能します。buffer コマンドには、**circular**、**file**、**size** などのさまざまなオプションを使用できます。継続的なキャプチャには、循環バッファが必要です。

例

次に、循環バッファのファイルを設定する例を示します。

```
Device# monitor capture epc-session1 buffer circular file 4 file-size 20
```

monitor capture continuous-capture

継続的なパケットキャプチャを設定し、バッファが上書きされる前の特定の場所へのファイルの自動エクスポートを有効にするには、**monitor capture** *epc-capture-name* **continuous-capture** {**ftp:** | **http:** | **https:** | **pram:** | **rcp:** | **scp:** | **sftp:** | **tftp:**} を使用します。

monitor capture *epc-capture-name* **continuous-capture** { **ftp:** | **http:** | **https:** | **pram:** | **rcp:** | **scp:** | **sftp:** | **tftp:** }

構文の説明

epc-capture-name	組み込みパケットキャプチャ（EPC）ファイルの名前を指定します。
{ **ftp:** | **http: https:** | **pram:** | **rcp:** | **scp** | **sftp:** | **tftp:**}	EPC ファイルが保存される場所を指定します。ファイル名には、.pcap という拡張子が必要です。 次に、ファイル名と、ファイル名の生成に使用される名称の例を示します。 CONTINUOUS_CAP_20230601130203.pcap CONTINUOUS_CAP_20230601130240.pcap

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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、継続的なキャプチャを設定する例を示します。

```
Device# monitor capture epc-session1 continuous-capture https://www.cisco.com/epc1.pcap
```

monitor capture export

キャプチャされたパケットをファイルに保存するには、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** *filelocation / file-name*

構文の説明

capture-name	キャプチャの名前。
export	.PCAP タイプのファイルにキャプチャバッファ内のすべてのパケットを保存します。
file-location/file-name	宛先ファイルの場所と名前。

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 Gibraltar 16.12.1	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ため、または **monitor capture stop** コマンドが入力されたために停止していることがあります。

例

次に、キャプチャバッファの内容をエクスポートする例を示します。

```
Device> enable
Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap
Device# end
```

monitor capture inner mac

内部フィルタの MAC アドレスを設定するには、**monitor capture** *epc-capture-name* **inner mac** *MAC1 MAC2 MAC3* を使用します

monitor capture *epc-capture-name* **inner mac** *MAC1* *MAC2* *MAC3*

構文の説明

epc-capture-name	組み込みパケットキャプチャ（EPC）ファイルの名前を指定します。
MAC1 [*MAC2...MAC3*]	MAC アドレスを内部 MAC フィルタとして設定します。最大 10 個の MAC アドレスを設定できます。

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 Dublin 17.12.1	このコマンドが導入されました。

使用上のガイドライン

MAC アドレスは、1 つのコマンドで入力することも、複数のコマンドラインを使用して入力することもできます。文字列の制限により、1 つのコマンドラインに入力できる MAC アドレスは 5 つまでです。次のコマンドラインに残りの MAC アドレスを入力できます。

設定された内部 MAC の数が 10 の場合、設定された古い内部 MAC アドレスを削除するまで、新しい MAC アドレスを設定することはできません。

例

次に、内部フィルタの MAC アドレスを設定する例を示します。

```
Device# monitor capture epc-session1 inner mac 1.1.1 2.2.2 3.3.3 4.4.4
```

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ーキャプチャを設定するには、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ーキャプチャを無効にするには、このコマンドの **no** 形式を使用します。

monitor capture *capture-name* { **interface** *type number* | **control-plane** } { **in** | **out** | **both** }
no monitor capture *capture-name* { **interface** *type number* | **control-plane** } { **in** | **out** | **both** }

構文の説明

capture-name	キャプチャの名前。
interface *type number*	指定したタイプと番号のインターフェイスを接続ポイントとして設定します。
control-plane	コントロールプレーンを接続ポイントとして設定します。
in	着信トラフィックの方向を指定します。
out	発信トラフィックの方向を指定します。
both	着信トラフィックと発信トラフィックの両方の方向を指定します。

コマンド デフォルト

モニター パケット キャプチャ フィルタの指定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 Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

複数の接続ポイントを追加するために、必要に応じて何度でも **monitor capture** コマンドを繰り返し実行できます。

例

次に、接続ポイントをインターフェイスに追加する例を示します。

```
Device> enable
Device# monitor capture mycap interface GigabitEthernet 0/0/1 in
Device# end
```

次に、接続ポイントをコントロールプレーンに追加する例を示します。

```
Device> enable
Device# monitor capture mycap control-plane out
Device# end
```

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-name* **limit** ［ **duration** *seconds* ］ ［ **every** *number* ］ ［ **packet-length** *size* ］［ **packets** *number* ］ ［ **pps** *number* ］
no monitor capture *name* **limit** ［ **duration** ］ ［ **every** ］ ［ **packet-length** ］ ［ **packets** ］ ［ **pps** ］

構文の説明

capture-name	パケット 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。
every *number*	（任意）一連のパケットで、*number* 引数で番号順が示されたパケットがキャプチャされます。範囲は 2 ～ 100000 です。
packet-length *bytes*	（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 *bytes* 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 *packets-number*	（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。
pps *pps-number*	（任意）1 秒あたりのキャプチャされるパケット数を指定します。範囲は 1 ～ 1000000 です。

コマンド デフォルト

キャプチャ制限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 Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

期間が指定されていない場合、キャプチャは手動で中断されるまで停止しません。**packet-length** *bytes* のキーワードと引数のペアが指定されていない場合、パケット全体が処理されます。**every** *number* のキーワードと引数のペアが指定されていない場合、一致したすべてのパケットがキャプチャされます。 **packets** *packets-number* のキーワードと引数のペアが指定されていない場合、一致したすべてのパケットがキャプチャされます。**pps** *number* のキーワードと引数のペアが指定されていない場合、着信パケットは 1 秒あたり 100 万パケットのレートでキャプチャされます。

例

次に、キャプチャ制限を指定する例を示します。

```
Device> enable
Device# monitor capture mycap limit duration 10
Device# monitor capture mycap limit packet-length 128
Device# monitor capture mycap limit packets 100
Device# monitor capture mycap limit pps 1000
Device# monitor capture mycap limit duration 10 packet-length 128 packets 100
Device# end
```

monitor capture match

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、コマンドの **no** 形式を使用します。

monitor capture *capture-name* **match** { **any** | { **ipv4** | **ipv6** } { *source-prefix/length* | **any** | **host** } *source-ip-address* { { *destination-prefix/length* | **any** | **host** } *destination-ip-address* } | **protocol** { **tcp** | **udp** } { { *source-prefix/length* | **any** | **host** } { { *destination-prefix/length* | **any** | **host** } | [[{ **eq** | **gt** | **lt** | **neg** }] *port-number*] | **range** *start-port-number end-port-number* | [{ **eq** | **gt** | **lt** | **neg** }] *port-number* | **range** *start-port-number end-port-number* } } | **mac** { *source-mac-address* | { **any** | **host** } *source-mac-address* } *source-mac-address-mask* { *destination-mac-address* | { **any** | **host** } *destination-mac-address* } *destination-mac-address-mask* }

no monitor capture *capture-name* **match**

構文の説明

epc-capture-name	キャプチャの名前。
any	すべてのパケットを指定します。
ipv4	IPv4 パケットを指定します。
ipv6	IPv6 パケットを指定します。
source-prefix/length	IPv4 または IPv6 送信元アドレスのネットワークプレフィックスと長さ。
any	任意の送信元 IPv4 または IPv6 アドレスのネットワークプレフィックスを指定します。
host	送信元ホストを指定します。
source-ip-address	送信元 IPv4 または IPv6 アドレス。
destination-prefix/length	宛先 IPv4 または IPv6 アドレス。
any	IPv4 または IPv6 宛先アドレスのネットワークプレフィックスと長さを指定します。
host	宛先ホストを指定します。
destination-ip-address	宛先 IPv4 または IPv6 アドレス。
protocol	プロトコルを指定します。
tcp	TCP プロトコルを指定します。
udp	UDP プロトコルを指定します。

eq	（任意）IP アドレスに関連付けられたポート番号と同じポート番号を持つパケットのみを一致させることを指定します。
gt	（任意）IP アドレスに関連付けられたポート番号より大きいポート番号を持つパケットのみを一致させることを指定します。
lt	（任意）IP アドレスに関連付けられたポート番号より小さいポート番号を持つパケットのみを一致させることを指定します。
neq	（任意）IP アドレスに関連付けられたポート番号と同じでないポート番号を持つパケットのみを一致させることを指定します。
port-number	（任意）IP アドレスに関連付けられたポート番号。範囲は 0 ～ 65535 です。
range	（任意）ポート番号の範囲を指定します。
start-port-number	（任意）ポート番号の範囲の開始。範囲は 0 ～ 65535 です。
end-port-number	（任意）ポート番号の範囲の終了。範囲は 0 ～ 65535 です。
mac	レイヤ 2 パケットを指定します。
source-mac-address	送信元 MAC アドレス。
any	任意の送信元MACアドレスのネットワークプレフィックスを指定します。
host	MAC 送信元ホストを指定します。
source-mac-address-mask	送信元 MAC アドレスマスク。
destination-mac-address	宛先 MAC アドレス。
any	任意の宛先MACアドレスのネットワークプレフィックスを指定します。
host	MAC 送信元ホストを指定します。
destination-mac-address-mask	宛先 MAC アドレスマスク。

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 Gibraltar 17.12.1	このコマンドが導入されました。

使用上のガイドライン

monitor capture コマンドを使用して、コアフィルタをクラスマップ、アクセスリスト、または明示的なインラインフィルタとして指定します。**monitor capture match** コマンドを入力する前にすでに指定されていたフィルタは、置き換えられます。

例

次に、さまざまな明示的なフィルタを設定する例を示します。

```
Device> enable
Device# monitor capture mycap match any
Device# monitor capture mycap match mac any any
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap match ipv4 protocol udp 198.51.100.0/24 eq 20001 any
Device# end
```

次に、MAC アドレスのフィルタを設定する例を示します。

```
Device> enable
Device# monitor capture match mycap mac 0030.9629.9f84 0000.0000.0000 0030.7524.9f84
0000.0000.0000
Device# end
```

次に、IPv4 トラフィックのフィルタを設定する例を示します。

```
Device> enable
Device# monitor capture match mycap ipv4 198.51.100.0/24 198.51.100.1 203.0.113.0/24
203.0.113.254
Device# end
```

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 *epc-capture-name* **start**

構文の説明

epc-capture-name	キャプチャの名前。

コマンド デフォルト

データパケットはバッファにキャプチャされません。

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 Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

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 start** 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

次に、バッファ内容のキャプチャを開始する例を示します。

```
Device> enable
Device# monitor capture mycap start
Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap
Device# monitor capture mycap limit packets 100 duration 60
Device# monitor capture mycap start
Device# end
```

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 *epc-capture-name* **stop**

構文の説明

epc-capture-name	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 Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

monitor capture start 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開始します。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

次に、バッファ内容のキャプチャを停止する例を示します。

```
Device> enable
Device# monitor capture mycap stop
Device# end
```

mop enabled

インターフェイスが Maintenance Operation Protocol（MOP）をサポートできるようにするには、インターフェイス コンフィギュレーション モードで **mopenabled** コマンドを使用します。インターフェイスで MOP 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。

mop enabled
no mop enabled

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

イーサネット インターフェイスではイネーブル、他のすべてのインターフェイスではディセーブルになっています。

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
10.0	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

例

次に、シリアル インターフェイス 0 で MOP をイネーブルにする例を示します。

```
Router(config)# interface serial 0
Router(config-if)# mop enabled
```

関連コマンド

コマンド	説明
mop retransmit-timer	Cisco IOS ソフトウェアが MOP サーバーにブート要求を再送信するまでに待機する時間の長さを設定します。
mop retries	Cisco IOS ソフトウェアがブート要求を MOP サーバに再送信する回数を設定します。
mop sysid	インターフェイスが定期的な MOP システム識別メッセージを送信できるようにします。

mop sysid

インターフェイスが定期的な Maintenance Operation Protocol（MOP）システム識別メッセージを送信できるようにするには、インターフェイス コンフィギュレーション モードで **mopsysid** コマンドを使用します。インターフェイスで MOP メッセージ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。

mop sysid
no mop sysid

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

有効

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
10.0	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

バックグラウンド システム ID メッセージを送信しなくても、MOP を実行することはできます。このコマンドを使用すると、MOP リモート コンソールを使用できますが、configurator で使用されるメッセージは生成されません。

例

次に、シリアル インターフェイス 0 が MOP システム識別メッセージを送信できるようにする例を示します。

```
Router(config)# interface serial 0
Router(config-if)# mop sysid
```

関連コマンド

コマンド	説明
mop device-code	MOP システム識別メッセージを送信するデバイスのタイプを識別し、プログラム メッセージを要求します。
mop enabled	インターフェイスが MOP をサポートできるようにします。

multicast

メッシュ マルチキャスト モードを設定するには、 **multicast** コマンドを使用します。

multicast { **in-only** | **in-out** | **regular** }

構文の説明

in-only	メッシュ マルチキャスト In モードを設定します。
in-out	メッシュ マルチキャスト In-Out モードを設定します。
regular	メッシュ マルチキャスト Regular モードを設定します。

コマンド デフォルト

in-out

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ AP プロファイルにマルチキャスト In モードを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile mesh mesh-profile
Device(config-wireless-mesh-profile)# multicast in-only
```

multicast vlan

単一の VLAN にマルチキャストを設定するには、 **multicast vlan** コマンドを使用します。マルチキャ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。

multicast vlan *vlan-id*
no multicast vlan *vlan-id*

構文の説明

vlan-id	VLAN ID 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

ワイヤレス 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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、マルチキャストを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-test
Device(config-wireless-policy)# multicast vlan 12
```

multicast filter

マルチキャストフィルタを設定するには、**multicast filter** コマンドを使用します。この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。

multicast filter

構文の説明

multicast filter	マルチキャストフィルタを設定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス 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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、マルチキャストフィルタを設定する例を示します。

```
Device(config-wireless-policy)# multicast filter
```

name

オンラインサインアップ（OSU）オペレータの名前を特定の言語で設定するには、**name** コマンドを使用します。OSU オペレータの名前を削除するには、このコマンドの **no** 形式を使用します。

name *operator-name language-code* [*service-description*]

構文の説明

operator-name	OSU オペレータ名。
language-code	オペレータの 3 文字の言語コード。言語コードには、言語の最初の 3 文字のみを小文字で使用します。たとえば、英語の場合は *eng* を使用します。 言語コードの完全なリストについては、http://www.loc.gov/standards/iso639-2/php/code_list.php を参照してください。
service-description	OSU オペレータのサービスの説明。

コマンド デフォルト

なし

コマンド モード

ANQP OSU プロバイダーの設定（config-anqp-osu-provider）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、OSU オペレータの名前を特定の言語で設定する例を示します。

```
Device(config-wireless-anqp-server)# osu-provider my-osu
Device(config-anqp-osu-provider)# name xxy eng
```

nac

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 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 ［ **ise** | **xwf** ］
no nac

構文の説明

ise	Radius NAC サポート（Identity Service Engine）を設定します
xwf	Express Wi-Fi NAC サポートを設定します。

コマンド デフォルト

NAC は無効です。

コマンド モード

ワイヤレス 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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、RADIUS NAC を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# nac
```

nai-realm

802.11u ネットワーク アクセス識別子（NAI）レルムを設定するには、**nai-realm** コマンドを使用します。レルムを削除するには、このコマンドの **no** 形式を使用します。

nai-realm *nai-realm*

構文の説明

nai-realm	NAI レルム名。 レルム名は 220 文字までです。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、802.11u NAI レルムを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# nai-realm cisco.com
```

nai-realm

課金通知のネットワークアクセス識別子（NAI）レルムを設定するには、**nai-realm** コマンドを使用します。課金通知の NAI レルムを削除するには、このコマンドの **no** 形式を使用します。

nai-realm *realm-name*

構文の説明

realm-name	課金通知の NAI レルム名。

コマンド デフォルト

NAI レルムは設定されていません。

コマンド モード

ワイヤレス ANQP 課金通知コンフィギュレーション（config-anqp-advice-charge）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、課金通知の NAI レルムを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# advice-charge unlimited
Device(config-anqp-advice-charge)# nai-realm cisco
```

nai-realm（OSU プロバイダー）

OSU オペレータのネットワーク アクセス識別子（NAI）レルムを設定するには、**nai-realm** コマンドを使用します。OSU オペレータのレルムを削除するには、このコマンドの **no** 形式を使用します。

nai-realm *nai-realm*

構文の説明

nai-realm	NAI レルム名。 レルム名は220文字までです。

コマンド デフォルト

なし

コマンド モード

ANQP OSU プロバイダーの設定（config-anqp-osu-provider）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、OSU オペレータの NAI レルムを設定する例を示します。

```
Device(config-anqp-osu-provider)# nai-realm cisco.com
```

nas-id

NAS ID のオプションパラメータを設定するには、**nas-id** コマンドを使用します。

nas-id { **option1** | **option2** | **option3** } { **ap-eth-mac** | **ap-ip** | **ap-location** | **ap-mac** | **ap-name** | **ap-policy-tag** | **ap-site-tag** | **custom-string** *custom-string* | **ssid** | **sys-ip** | **sys-mac** | **sys-name** }

構文の説明

ap-eth-mac	AP のイーサネット MAC アドレス。
ap-ip	AP の IP アドレス。
ap-location	AP の場所。
ap-mac	AP の MAC アドレス。
ap-name	AP の名前。
ap-policy-tag	AP のポリシータグ。
ap-site-tag	AP のサイトタグ。
custom-string*custom-string*	option1、option2、および option3 のさまざまな組み合わせを使用した、カスタム文字列。
ssid	SSID。
sys-ip	システムの IP アドレス。
sys-mac	システムの MAC アドレス。
sys-name	システムの名前。

コマンド デフォルト

なし

コマンド モード

config-aaa-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。
Cisco IOS XE Cupertino 17.7.1	次のキーワードと変数が追加されることで、このコマンドが変更されました。 • **custom-string** • *custom-string*

例

次に、NAS-ID のシステム IP アドレスを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy profile-name
Device(config-aaa-policy)# nas-id option2 sys-ip
```

次に、NAS-ID のカスタム文字列を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy profile-name
Device(config-aaa-policy)# nas-id option2 custom-string test
```

nas-id option2

NAS-ID のオプション 2 パラメータを設定するには、**nas-id option2** コマンドを使用します。

nas-id option2 {**sys-ip** | **sys-name** | **sys-mac** }

構文の説明

sys-ip	システム IP アドレス。
sys-name	システム名。
sys-mac	システム MAC アドレス。

コマンド デフォルト

なし

コマンド モード

config-aaa-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、NAS-ID のシステム IP アドレスを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy profile-name
Device(config-aaa-policy)# nas-id option2 sys-ip
```

ndp-mode

RF プロファイルでの AP の NDP モードを設定するには、RF プロファイル コンフィギュレーションで **ndp-mode** コマンドを使用します。

ndp-mode { **auto** | **off-channel** }

構文の説明

ndp-mode	802.11a ネイバー探索の動作モードを設定します。
auto	auto モードを有効にします。
off-channel	RF ASIC 無線で NDP パケットを有効にします。

コマンド モード

RF プロファイル コンフィギュレーション（config-rf-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、802.11a ネイバー探索の動作モードを設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 24ghz rf-profile rf-profile-name
Device(config-rf-profile)# ndp-mode auto
```

network

ネットワーク番号を 10 進表記で設定するには、**network** コマンドを使用します。

network *network-number*[{*network-mask* | **secondary** }]

構文の説明

ipv4-address	ドット付き 10 進表記のネットワーク番号。
network-mask	ネットワーク マスクまたはプレフィックス長。
secondary	セカンダリ サブネットとして設定します。

コマンド デフォルト

なし

コマンド モード

dhcp-config

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ネットワーク番号とマスク アドレスを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip dhcp pool name
Device(dhcp-config)# network 209.165.200.224 255.255.255.0
```

network-type

802.11u ネットワークタイプを設定するには、**network-type** コマンドを使用します。ネットワークタイプを削除するには、このコマンドの **no** 形式を使用します。

network-type { **chargeable-public** | **emergency** | **free-public** | **guest-private** | **personal-device** | **private** | **test** | **wildcard** } **internet-access** { **allowed** | **forbidden** }

構文の説明

chargeable-public	有料のパブリックネットワークとして設定します。
emergency	緊急ネットワークとして設定します。
free-public	無料のパブリックネットワークとして設定します。
guest-private	ゲスト プライベート ネットワークとして設定します。
personal-device	パーソナル デバイス ネットワークとして設定します。
private	プライベートネットワークとして設定します。
test	テストネットワークとして設定します。
wildcard	ワイルドカードネットワークとして設定します。
internet-access	インターネットにアクセスするためのネットワーク機能を設定します。
allowed	インターネットアクセスを有効にします。
disabled	インターネットアクセスを無効にします。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、802.11u ネットワークタイプを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# network-type wildcard internet-access allowed
```

nmsp cloud-services enable

NMSP クラウド サービスを設定するには、 **nmsp cloud-services enable** コマンドを使用します。

nmsp cloud-services enable

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、NMSP クラウド サービスを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services enable
```

nmsp cloud-services http-proxy

NMSP クラウド サーバのプロキシを設定するには、 **nmsp cloud-services http-proxy** コマンドを使用します。

nmsp cloud-services http-proxy *proxy-server port*

構文の説明

proxy-server	NMSP クラウド サービスのプロキシ サーバのホスト名または IP アドレスを入力します。
port	NMSP クラウド サービスのプロキシ サーバのポート番号を入力します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、NMSP クラウド サーバーのプロキシを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services http-proxy host-name port-number
```

nmsp cloud-services server token

NMSP クラウド サービス サーバのパラメータを設定するには、 **nmsp cloud-services server token** コマンドを使用します。

nmsp cloud-services server token *token*

構文の説明

token	NMSP クラウドサービスの認証トークン。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、NMSP クラウド サービス サーバーのパラメータを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services server token authentication-token
```

nmsp cloud-services server url

NMSP クラウド サービス サーバーの URL を設定するには、**nmsp cloud-services server url** コマンドを使用します。

nmsp cloud-services server url *url*

構文の説明

url	NMSP クラウドサービス サーバーの URL。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、NMSP クラウド サービス サーバーの URL を設定する例を示します。

```
Device(config)# nmps cloud-services server url http://www.example.com
```

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**nmsp notification interval** 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 Gibraltar 16.10.1	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。

```
デバイス# configure terminal
デバイス(config)# nmsp notification-interval rfid 25
デバイス(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。

```
デバイス# configure terminal
デバイス(config)# nmsp notification-interval attachment 10
デバイス(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。

```
デバイス# configure terminal
デバイス(config)# nmsp notification-interval location 20
デバイス(config)# end
```

nmsp strong-cipher

新しい暗号化方式を有効にするには、グローバル コンフィギュレーション モードで **nmsp strong-cipher** コマンドを使用します。無効にするには、このコマンドの **no** 形式を使用します。

nmsp strong-cipher
no nmsp strong-cipher

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

新しい暗号化方式は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
15.2(2)E	このコマンドが導入されました。

使用上のガイドライン

nmsp strong-cipher コマンドは、新しい Network Mobility Service Protocol（NMSP）接続に対し、強力な暗号化方式を有効にします。

（注） 既存の NMSP 接続では、デフォルトの暗号化方式が使用されます。

例

次に、NMSP に対して強力な暗号化方式を有効にする例を示します。

```
Device> enable
Device> configure terminal
Device(config)# nmsp strong-cipher
```

関連コマンド

コマンド	説明
show nmsp status	アクティブな NMSP 接続の状態を表示します。

no redun-management fast-switchover

明示的高速スイッチオーバー通知を無効にするには、**no redun-management fast-switchover** コマンドを使用します。

（注） これは、プライマリコントローラで設定します。この設定は、セカンダリコントローラでは必要ありません。

no redun-management fast-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

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 Cupertino 17.9.1	このコマンドが導入されました。

例

次に、明示的高速スイッチオーバー通知を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# no redun-management fast-switchover
```

no redun-management garp-retransmit initial

初期 GARP を無効にするには、**no redun-management garp-retransmit initial** コマンドを使用します。

no redun-management garp-retransmit initial

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、初期 GARP を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# no redun-management garp-retransmit initial
```

no accounting-interim

中間アカウンティングを無効にするには、**no accounting-interim** コマンドを使用します。

no accounting-interim

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、中間アカウンティングを無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy <default-policy-profile>
Device(config-wireless-policy)# no accounting-interim
```

ntp auth-key

AP プロファイルで Network Time Protocol（NTP）サーバー認証キー情報を設定するには、**ntp auth-key** コマンドを使用します。AP プロファイルから NTP サーバー認証キー情報を削除するには、**no ntp auth-key** コマンドを使用します。

ntp auth-key index *key-index* **type** { **md5** | **sha1** } **format** { **ascii** | **hex** } **key** { **0** | **8** } *server-key*

構文の説明

key-index	キーインデックス。有効な範囲は 1 ～ 65535 です。
md5	Message Digest 5（MD5）認証キーが後ろに続くことを指定します。
sha1	セキュア ハッシュ アルゴリズム 1（SHA1）認証キーが後ろに続くことを指定します。
format	キー形式（ASCII または HEX）を定義します。
ascii	ASCII キーが後ろに続くことを指定します。
hex	16 進キーが後ろに続くことを指定します。
key	NTP サーバーキー（非暗号化または暗号化）を定義します。
0	暗号化されていないパスワードが後ろに続くことを指定します。
8	AES 暗号化パスワードが後ろに続くことを指定します。
server-key	NTP サーバーキー。ASCII キーの場合、長さが 21 バイト未満であることを確認してください。HEX キーの場合、長さは 41 未満で、0 ～ 9 の数字と a ～ f の文字のみを使用する必要があります。

コマンド デフォルト

NTP サーバー認証は設定されていません。

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、AP プロファイルで NTP サーバー認証キー情報を設定する例を示します。

```
Device# configure terminal
Device(config)# ap profile test
Device(config-ap-profile)# ntp ip 198.51.100.5
Device(config-ap-profile)# ntp auth-key index 12 type
md5 format ascii key 0 test
```

office-extend

FlexConnect AP の OfficeExtend AP モードを有効にするには、 **office-extend** コマンドを使用します。

office-extend

コマンド デフォルト

なし

コマンド モード

config-wireless-flex-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、FlexConnect AP の OfficeExtend AP モードを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile flex flex-profile-name
Device(config-wireless-flex-profile)# office-extend
```

okc

Opportunistic Key Caching（OKC）がまだ有効になっていない場合、有効にするには、**okc** 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。

okc

[no] okc

構文の説明

okc	Opportunistic Key Caching（OKC）を有効または無効にします。デフォルトでは、OKC は有効になっています。

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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、OKC を有効にする例を示します。

```
Device(config-wlan)# okc
```

open-roaming-oi

オープンローミング要素のエイリアスを設定するには、**open-roaming-oi** コマンドを使用します。オープンローミング要素のエイリアスを削除するには、このコマンドの **no** 形式を使用します。

open-roaming-oi *alias*

構文の説明

alias	ローミング組織識別子のエイリアス。

コマンド デフォルト

ローミング組織識別子のエイリアスは設定されていません。

コマンド モード

ワイヤレス ANQP サーバー コンフィギュレーション（config-wireless-anqp-server）#

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、オープンローミング要素のエイリアスを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless hotspot anqp-server my_server
Device(config-wireless-anqp-server)# open-roaming-oi allow-all
```

operator

Hotspot 2.0 オペレータのフレンドリ名を特定の言語で設定するには、**operator** コマンドを使用します。オペレータ名を削除するには、このコマンドの **no** 形式を使用します。

operator *operator-name language-code*

構文の説明

operator-name	オペレータの名前。
language-code	オペレータの 3 文字の言語コード。言語コードには、言語の最初の 3 文字のみを小文字で使用します。たとえば、英語の場合は *eng* を使用します。 言語コードの完全なリストを確認するには、http://www.loc.gov/standards/iso639-2/php/code_list.php にアクセスしてください。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、オペレータのフレンドリ名を設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# operator XYZ-operator eng
```

operating-class

Hotspot 2.0 の動作クラス ID を設定するには、**operating-class** コマンドを使用します。動作クラスを削除するには、このコマンドの **no** 形式を使用します。

operating-class *class-id*

構文の説明

class-id	動作クラスの ID 番号。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、動作クラス識別子を設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# operating-class 25
```

option

のフロー エクスポータのオプションのデータ パラメータを設定するには、フロー エクスポータ コンフィギュレーション モードで **option** コマンドを使用します。フロー エクスポータのオプションのデータ 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。

option {**exporter-stats** | **interface-table** | **sampler-table**} [{**timeout** *seconds*}]
no option {**exporter-stats** | **interface-table** | **sampler-table**}

構文の説明

exporter-stats	フローエクスポータの統計情報オプションを設定します。
interface-table	フローエクスポータのインターフェイステーブル オプションを設定します。
sampler-table	フロー エクスポータのエクスポート サンプラー テーブル オプションを設定します。
timeout *seconds*	（任意）フローエクスポータのオプションの再送時間を秒単位で設定します。指定できる範囲は 1 ～ 86400 です。デフォルトは 600 です。

コマンド デフォルト

タイムアウトは 600 秒です。他のすべてのオプション データ パラメータは設定されていません。

コマンド モード

フロー エクスポータ 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

option exporter-stats コマンドを実行すると、レコード数、バイト数、送信されたパケット数など、エクスポータの統計情報が定期的に送信されます。このコマンドを使用して、コレクタは受信するエクスポート レコードのパケット損失を見積もります。オプションのタイムアウトでは、レポートが送信される頻度を変更できます。

option interface-table コマンドを実行すると、オプション テーブルが定期的に送信されます。このオプション テーブルを使用して、コレクタはフロー レコードに記録されている SNMP インターフェイス インデックスを各インターフェイス名にマッピングします。オプションのタイムアウトでは、レポートが送信される頻度を変更できます。

option sampler-table コマンドを実行すると、オプション テーブルが定期的に送信されます。このオプションテーブルには、各サンプラーの設定の詳細が含まれており、これを使用して、コレクタは任意のフロー レコードに記録されているサンプラー ID を、フローの統計情報のスケールアップに使用可能な設定にマッピングします。オプションのタイムアウトでは、レポートが送信される頻度を変更できます。

このコマンドをデフォルト設定に戻すには、**no option** または **default option** フロー エクスポータ 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、サンプラー オプション テーブルの定期的な送信をイネーブルにして、コレクタでサンプラー ID をサンプラーのタイプとレートにマッピングする方法を示します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)# option sampler-table
```

次の例では、レコード数、バイト数、送信されたパケット数など、エクスポータの統計情報の定期的な送信をイネーブルする方法を示します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)# option exporter-stats
```

次の例では、オプション テーブルの定期的な送信をイネーブルにし、そのオプション テーブルをコレクタで使用して、フローレコードに記録されている SNMP インターフェイス インデックスをインターフェイス名にマッピングする方法を示します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)# option interface-table
```

osu-provider

Hotspot 2.0 のオンラインサインアップ（OSU）プロバイダーを設定するには、**osu-provider** コマンドを使用します。OSU プロバイダーを削除するには、このコマンドの **no** 形式を使用します。

osu-provider *provider-name*

構文の説明

provider-name	OSU プロバイダーの名前。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、OSU プロバイダーを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# osu-provider yyy
```

osu-ssid

オンラインサインアップ（OSU）に使用するワイヤレスクライアントのサービスセット識別子（SSID）を設定するには、**osu-ssid** コマンドを使用します。SSID を削除するには、このコマンドの **no** 形式を使用します。

osu-ssid *ssid*

構文の説明

ssid	ワイヤレスクライアントの SSID の名前。 SSID の長さは、最大 32 文字です。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、ワイヤレスクライアントが OSU 中に使用する SSID を設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# osu-ssid cisco
```

packet-capture

AP プロファイルでパケット キャプチャを有効にするには、 **packet-capture** コマンドを使用します。

packet-capture *profile-name*

コマンド デフォルト

なし

コマンド モード

config-ap-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP プロファイルでパケット キャプチャを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap profile demo-profile-name
Device(config-ap-profile)# packet capture demo-profile
```

parameter-map type subscriber attribute-to-service

パラメータ マップのタイプと名前を設定するには、 **parameter-map type subscriber attribute-to-service** コマンドを使用します。

parameter-map type subscriber attribute-to-service *parameter-map-name*

構文の説明

attribute-to-service	サービスの属性の名前。
parameter-map-name	パラメータ マップの名前。マップ名は33文字までに制限されています。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、パラメータ マップのタイプと名前を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type subscriber attribute-to-service parameter-map-name
```

pae

製品テレメトリ収集を有効にするには、**pae** コマンドを使用します。製品テレメトリ収集を無効にするには、このコマンドの **no** 形式を使用します。

pae

no pae

コマンド デフォルト

製品テレメトリ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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.10.1	このコマンドが導入されました。

例

次に、製品テレメトリ収集を無効にする例を示します。

```
Device# configure terminal
Device(config)# no pae
```

parameter-map type webauth

特定のパラメータマップまたはすべてのパラメータマップの Web 認証パラメータタイプを設定するには、 **parameter-map type webauth** コマンドを使用します。

parameter-map type webauth { *parameter-map-name* | **global** }

構文の説明

parameter-map-name	パラメータ マップの名前。マップ名は99文字までに制限されています。
global	すべてのパラメータマップに設定を適用します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、*parameter-map1* という名前のパラメータマップの Web 認証パラメータタイプを設定する例を示します。

```
Device# configure terminal
Device(config)# parameter-map type webauth parameter-map1
```

password encryption aes

強力な（AES）パスワード暗号化を有効にするには、**password encryption aes** コマンドを使用します。この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。

password encryption aes
no password encryption aes

構文の説明

password	暗号化パスワード（キー）を設定します。
encryption	システムパスワードを暗号化します。
aes	より強力な（AES）パスワード暗号化を有効にします。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.2s	このコマンドが導入されました。

例

次に、AES パスワード暗号化を有効にする例を示します。

```
Device(config)#password encryption aes
```

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 {**allow-private-group** | **drop** | **forward-upstream**}
no peer-blocking

構文の説明

allow-private-group	プライベートグループを許可するデバイスを指定します。 （注） **allow-private-group** ピアツーピアブロッキングWLAN設定は、Identity PSK（iPSK）WLAN でのみ機能します。
drop	device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。device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。 （注） forward-upstream オプションは、Flex ローカルスイッチングではサポートされていません。このオプションが設定されている場合でも、トラフィックはドロップされます。また、ローカルスイッチングSSIDのピアツーピアブロッキングは、同じAP 上のクライアントに対してのみ使用できます。

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 Gibraltar 16.10.1	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、forward オプション、および private group オプションを有効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wlan wlan1
Device(config-wlan)# peer-blocking  allow-private-group
デバイス(config-wlan)# peer-blocking  drop
デバイス(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、forward オプション、および private group オプションを無効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wlan wlan1
Device(config-wlan)# no peer-blocking  allow-private-group
デバイス(config-wlan)# no peer-blocking  drop
デバイス(config-wlan)# no peer-blocking forward-upstream
```

plan

課金通知のプラン情報を設定するには、**plan** コマンドを使用します。課金通知のプラ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。

plan {*language-code* | *currency-code* | **info** {**bootflash** | **flash**} *file-name*}

構文の説明

filename	bootflash:filename または flash:filename の形式の、ファイル名などのプランの詳細。
language-code	この課金通知の言語コード（ISO 639）の最初の 3 文字（小文字）。たとえば、英語の場合は *eng* です。
currency-code	この課金通知の通貨コード（ISO 4217）の最初の 3 文字。たとえば、ユーロの場合は *EUR* です。

コマンド デフォルト

プラン情報は設定されていません。

コマンド モード

ワイヤレス ANQP 課金通知コンフィギュレーション（config-anqp-advice-charge）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、課金通知のプラン情報を設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# advice-charge unlimited
Device(config-anqp-advice-charge)# plan eng EUR info bootflash:plan-a
```

pmk propagate

（PMK）情報をサイト内の他の AP に伝播するには、**pmk propagate** コマンドを使用します。

pmk propagate

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

config-wireless-flex-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.8.1	このコマンドが導入されました。

例

次に、サイト内の他の AP に PMK 情報を伝播する例を示します。

```
Device# configure terminal
Device(config)# wireless profile flex test-flex-profile
Device(config-wireless-flex-profile)# pmk propogate
```

pmf-deauth

PMF 拒否タイプの認証解除不正 AP 封じ込めを有効にするには、**pmf-deauth** コマンドを使用します。PMF 拒否タイプの認証解除不正 AP 封じ込めを無効にするには、このコマンドの **no** 形式を使用します。

pmf-deauth

no pmf-deauth

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

PMF 拒否コンフィギュレーション（config-pmf-denial）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.12.1	このコマンドが導入されました。

例

次に、PMF 拒否タイプの認証解除不正 AP 封じ込めを有効にする例を示します。

```
Device# configure terminal
Device(config)# ap profile xyz-ap-profile
Device(config-ap-profile)# rogue detection containment pmf-denial
Device(config-pmf-denial)# pmf-deauth
```

no platform sudi cmca3

SUDI99 移行を無効にし、古いリリースに従った証明書マッピングに戻すには、**no platform sudi cmca3** コマンドを使用します。

no platform sudi cmca3

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

SUDI99 がトラストポイントとして設定されています。

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 Cupertino 17.7.1	このコマンドが導入されました。

使用上のガイドライン

高可用性（HA）トポロジの場合は、コマンドを実行する前にHAペアを形成します。その後、設定を保存し、コントローラをリロードして SUDI 証明書を無効にします。

例

次に、SUDI99移行を無効にし、以前のリリースに従った証明書マッピングに戻す例を示します。

```
Device# configure terminal
Device(config)# no platform sudi cmca3
```

policy

メディア ストリームのアドミッション ポリシーを設定するには、**policy** コマンドを使用します。

policy {**admit** | **deny**}

構文の説明

admit	メディア ストリーム グループのトラフィックを許可します。
deny	メディア ストリーム グループのトラフィックを拒否します。

コマンド デフォルト

なし

コマンド モード

media-stream

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メディア ストリーム グループのトラフィックを許可する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group ms-group 224.0.0.0 224.0.0.223
Device(media-stream)# policy admit
```

police

分類したトラフィックにポリサーを定義するには、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 **police** コマンドを使用します。既存のポリ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。

police *rate-bps burst-byte* [**conform-action transmit**]
no police rate-bps *burst-byte* [**conform-action transmit**]

構文の説明

rate-bps	平均トラフィック伝送速度をビット/秒（b/s）で指定します。指定できる範囲は 1000000 ～ 1000000000 です。
burst-byte	通常のバースト サイズ（バイト）を指定します。指定できる範囲は 8000 ～ 1000000 です。
conform-action transmit	（任意）速度が指定できる範囲を下回る場合は、スイッチがパケットを送信するよう指定します。

コマンド デフォルト

ポリサーは定義されません。

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

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。

階層ポリシー マップを設定する場合、セカンダリ インターフェイス レベルのポリシー マップで使用できるのは **police** ポリシーマップ コマンドだけです。

2 つ以上の物理ポートを制御するポート ASIC デバイスは、スイッチ上で 256 個のポリサー（255 個のユーザー設定可能なポリサーと 1 個の内部使用向けに予約されたポリサー）をサポートします。ポートごとにサポートされる設定可能なポリサーの最大数は 63 です。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを予約することはできません。ポートがいずれかのポリサーに割り当てるという保証はありません。

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

この例では、トラフィックの平均レートが 1 Mb/s 未満で、バースト サイズが 20 KB の場合にパケットを送信するポリサーを設定する方法を示します。パケットは変更されません。

```
デバイス(config)# class-map class1
デバイス(config-cmap)# exit
デバイス(config)# policy-map policy1
デバイス(config-pmap)# class class1
デバイス(config-pmap-c)# police 1000000 20000 conform-action transmit
デバイス(config-pmap-c)# exit
```

この例では、トラフィックの平均レートが 1 Mb/s 未満で、バースト サイズが 20 KB の場合にパケットを送信するポリサーを設定する方法を示します。パケットは変更されません。この例では、短縮構文を使用しています。

```
デバイス(config)# class-map class1
デバイス(config-cmap)# exit
デバイス(config)# policy-map policy1
デバイス(config-pmap)# class class1
デバイス(config-pmap-c)# police 1m 20000 conform-action transmit
デバイス(config-pmap-c)# exit
```

次の例では、DSCP 値をポリシング設定 DSCP マップに定義された値でマークダウンしてパケットを送信するポリサーを設定する方法を示します。

```
デバイス(config)# policy-map policy2
デバイス(config-pmap)# class class2
デバイス(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
デバイス(config-pmap-c)# 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。

police cir

認定情報レートのポリシングを設定するには、**police cir** コマンドを使用します。

police cir *<target bit rate>*

構文の説明

police cir	認定情報レートをポリシングします。
8000-10000000000	ターゲットビットレートを 1 秒あたりのビット数で設定します。指定できる範囲は 8000 ～ 10000000000 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

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、認定情報レートを設定する例を示します。

```
Device(config-pmap-c)#police cir 8000
```

policy-tag

ポリシー タグを AP にマッピングするには、**policy-tag** コマンドを使用します。

policy-tag *policy-tag-name*

構文の説明

policy-tag-name	ポリシー タグの名前。

コマンド デフォルト

なし

コマンド モード

config-ap-tag

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを実行すると、AP は、接続解除されたのち再参加します。

例

次に、ポリシー タグを設定する例を示します。

```
Device(config-ap-tag)# policy-tag policytag1
```

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）に適用できるポリシーマップを作成し、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 Gibraltar 16.10.1	このコマンドが導入されまし

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 クラス 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、device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。

（注） すべての MQS QoS の組み合わせが有線ポートでサポートされているわけではありません。これらの制約事項については、QoS コンフィギュレーション ガイドの「Restrictions for QoS on Wired Targets」の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。

```
デバイス(config)# policy-map policy1
デバイス(config-pmap)# class class1
デバイス(config-pmap-c)# set dscp 10
デバイス(config-pmap-c)# police 1000000 20000 conform-action transmit
デバイス(config-pmap-c)# exit
```

次に、階層ポリシーを設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# class-map c1
デバイス(config-cmap)# exit

デバイス(config)# class-map c2
デバイス(config-cmap)# exit

デバイス(config)# policy-map child
デバイス(config-pmap)# class c1
デバイス(config-pmap-c)# priority level 1
デバイス(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop

デバイス(config-pmap-c-police)# exit
デバイス(config-pmap-c)# exit

デバイス(config-pmap)# class c2
デバイス(config-pmap-c)# bandwidth 20000
デバイス(config-pmap-c)# exit

デバイス(config-pmap)# class class-default
デバイス(config-pmap-c)# bandwidth 20000
デバイス(config-pmap-c)# exit
```

```
デバイス(config-pmap)# exit

デバイス(config)# policy-map parent
デバイス(config-pmap)# class class-default
デバイス(config-pmap-c)# shape average 1000000
デバイス(config-pmap-c)# service-policy child
デバイスconfig-pmap-c)# end
```

次に、ポリシー マップを削除する例を示します。

```
デバイス(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。

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）に適用できるポリシーマップを作成し、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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

policy-map 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、device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。

（注） すべての MQS QoS の組み合わせが有線ポートでサポートされているわけではありません。これらの制約事項については、QoS コンフィギュレーション ガイドの「Restrictions for QoS on Wired Targets」の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。

```
デバイス(config)# policy-map policy1
デバイス(config-pmap)# class class1
デバイス(config-pmap-c)# set dscp 10
デバイス(config-pmap-c)# police 1000000 20000 conform-action transmit
デバイス(config-pmap-c)# exit
```

次に、階層ポリシーを設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# class-map c1
デバイス(config-cmap)# exit

デバイス(config)# class-map c2
デバイス(config-cmap)# exit

デバイス(config)# policy-map child
デバイス(config-pmap)# class c1
デバイス(config-pmap-c)# priority level 1
デバイス(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop

デバイス(config-pmap-c-police)# exit
デバイス(config-pmap-c)# exit

デバイス(config-pmap)# class c2
デバイス(config-pmap-c)# bandwidth 20000
デバイス(config-pmap-c)# exit

デバイス(config-pmap)# class class-default
デバイス(config-pmap-c)# bandwidth 20000
デバイス(config-pmap-c)# exit
```

```
デバイス(config-pmap)# exit

デバイス(config)# policy-map parent
デバイス(config-pmap)# class class-default
デバイス(config-pmap-c)# shape average 1000000
デバイス(config-pmap-c)# service-policy child
デバイスconfig-pmap-c)# end
```

次に、ポリシー マップを削除する例を示します。

```
デバイス(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。

port

カスタム アプリケーションを設定する際に使用するポート番号を設定するには、 **port** コマンドを使用します。

port *port-no*

構文の説明

port-no	ポート番号。

コマンド デフォルト

なし

コマンド モード

config-custom

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、カスタム アプリケーションを設定する際に使用するポート番号を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip nbar custom custom-protocol http host host-string
Device(config-custom)# http host hostname
Device(config-custom)# port port-no
```

power-save-client-threshold

省電力用のクライアントしきい値を設定するには、**power-save-client-threshold** *client-threshold* コマンドを使用します。この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。

power-save-client-threshold *client-threshold*

no power-save-client-threshold *client-threshold*

構文の説明

client-threshold	省電力用のクライアントしきい値を指定します。値の範囲は 1 ～ 32 クライアントです。デフォルト値は 1 です。

コマンド デフォルト

デフォルト値は 1 です。

コマンド モード

ワイヤレス電力プロファイルモード

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.12.1	このコマンドが導入されました。

例

次に、省電力用のクライアントしきい値を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile power power-profile1
Device(Config-wireless-power-profile)#power-save-client-threshold 5
```

priority priority-value

メディア ストリームのプライオリティを設定するには、**priority** *priority-value* コマンドを使用します。

priority *priority-value*

構文の説明

priority-value	メディア ストリームのプライオリティ値。有効な範囲は 1 ～ 8 です。1 が最も低いプライオリティで、8 が最も高いプライオリティです。

コマンド デフォルト

なし

コマンド モード

config-media-stream

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メディア ストリームのプライオリティ値を最大（8）に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# priority 8
```

priority-queue

ポート上で出力緊急キュー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 **priority-queue** 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。

priority-queue out
no priority-queue out

構文の説明

out	出力緊急キューをイネーブルにします。

コマンド デフォルト

出力緊急キューは、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 ジブラルタル 16.10.1	このコマンドが導入されました。

使用上のガイドライン

priority-queue out コマンドを設定する場合、シェイプド ラウンド ロビン（SRR）に参加するキューが 1 つ少ないため、SRR の重み比が影響を受けます。これは、**srr-queue bandwidth shape** または **srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンド内の *weight1* が無視される（比率計算に使用されない）ことを意味します。緊急キューはプライオリティ キューであり、他のキューのサービスが提供される前に空になるまでサービスを提供します。

緊急キューがイネーブルにされているとき、または SRR の重みに基づいて出力キューのサービスが提供されるときには、次の注意事項に従ってください。

- 出力緊急キューがイネーブルにされている場合は、キュー 1 に対して SRR のシェーピングおよび共有された重みが無効にされます。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングおよび共有された重みが設定されている場合は、キュー 1 に対して shaped モードは shared モードを無効にし、SRR はこのキューに shaped モードでサービスを提供します。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングされた重みが設定されていない場合は、SRR はキューに対して shared モードでサービスを提供します。

例

次の例では、SRR の重みが設定されている場合、出力緊急キューをイネーブルにする方法を示します。出力緊急キューは、設定された SRR ウェイトを上書きします。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# srr-queue bandwidth shape 25 0 0 0
デバイス(config-if)# srr-queue bandwidth share 30 20 25 25
```

```
デバイス(config-if)# priority-queue out
```

次の例では、SRR のシェーピングおよび共有された重みが設定された後、出力緊急キューをディセーブルにする方法を示します。シェーピング モードは、共有モードを無効にします。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# srr-queue bandwidth shape 25 0 0 0
デバイス(config-if)# srr-queue bandwidth share 30 20 25 25
デバイス(config-if)# no priority-queue out
```

設定を確認するには、**show mls qos interface** *interface-id* **queueing** または **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
show mls qos interface queueing	キューイング方法（SRR、プライオリティ キューイング）、キューに相応する重み、および Class of Service（CoS）から出力キューへのマップを表示します。
srr-queue bandwidth shape	シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにします。
srr-queue bandwidth share	共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。

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。クラスに指定した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

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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、PVC には使用できません。

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。

```
デバイス(config)# class-map cm1
デバイス(config-cmap)#match precedence 2
デバイス(config-cmap)#exit
```

```
デバイス(config)#class-map cm2
デバイス(config-cmap)#match dscp 30
デバイス(config-cmap)#exit

デバイス(config)# policy-map policy1
デバイス(config-pmap)# class cm1
デバイス(config-pmap-c)# priority level 1
デバイス(config-pmap-c)# police 1m
デバイス(config-pmap-c-police)#exit
デバイス(config-pmap-c)#exit
デバイス(config-pmap)#exit

デバイス(config)#policy-map policy1
デバイス(config-pmap)#class cm2
デバイス(config-pmap-c)#priority level 2
デバイス(config-pmap-c)#police 1m
```

profile（プライムフィルタ）

アクセスポイント（AP）フィルタのプライミングプロファイルを適用するには、**profile** コマンドを使用します。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。

profile *profile-name*

no profile *profile-name*

構文の説明

profile-name	APプライミングプロファイル名。

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

AP プライム フィルタ コンフィギュレーション（config-ap-pr-filter）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.2	このコマンドが導入されました。

例

次に、プライミングプロファイルを適用する例を示します。

```
Device# configure terminal
Device(config)# ap filter name test-filter type priming
Device(config-ap-pr-filter)# profile Prime-FX
```

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

アドレスが DHCP または NDP に関連付けられたプレフィックス 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。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)# protocol dhcp
```

primary (ap prime)

アクセスポイント（AP）フォールバック用のプライマリコントローラを設定するには、**primary** コマンドを使用します。AP プライミングに使用されないようにプライマリコントローラを削除するには、このコマンドの **no** 形式を使用します。

primary *controller-name ip-address*

no primary *controller-name ip-address*

構文の説明

controller-name	プライマリ コントローラの名前。
ip-address	コントローラの IPv4 または IPv6 アドレス。

コマンド デフォルト

なし

コマンド モード

AP プライム コンフィギュレーション（config-priming）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.2	このコマンドが導入されました。

例

次に、AP フォールバック用のプライマリコントローラを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile ap priming Prime-FX
Device(config-priming)# primary aaaa 209.165.201.2
```

priming-override

既存のアクセスポイント（AP）のプライミング設定をオーバーライドするには、**priming-override** コマンドを使用します。プライミングの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。

priming-override

no priming-override

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

プライミングのオーバーライドは無効になっています。

コマンド モード

AP プライム コンフィギュレーション（config-priming）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.2	このコマンドが導入されました。

使用上のガイドライン

- プライミングのオーバーライドが無効になっている場合、AP プライミングプロファイルに保存されている情報は AP に送信されません。
- プライミングのオーバーライドが有効になっている場合、N+1 アップグレードが正しく機能しないことがあります。N+1 アップグレードを使用する前に、**no priming-override** コマンドを使用して、プライミングのオーバーライドが無効になっていることを確認してください。

例

次に、既存の AP プライミング設定をオーバーライドする例を示します。

```
Device# configure terminal
Device(config)# wireless profile ap priming Prime-FX
Device(config-priming)# priming-override
```

public-ip

コントローラの NAT パブリック IP アドレスを設定するには、**public-ip** コマンドを使用します。

public-ip { *ipv4-address* | *ipv6-address* }

構文の説明

ipv4-address	IPv4アドレスを設定します。
ipv6-address	IPv6アドレスを設定します。

コマンド デフォルト

なし

コマンド モード

管理インターフェイス コンフィギュレーション（config-mgmt-interface）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

例

次に、コントローラの NAT パブリック IP アドレスを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless management interface Vlan1
Device(config-mgmt-interface)# public-ip 192.168.172.100
```

qbss-load

QoS Enhanced Basic Service Set（QBSS）IE を有効にするには、**qbss-load** 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。

qbss-load

[no] qbss-load

構文の説明

qbss-load	QoS Enhanced Basis Service Set（QBSS）IE 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

ワイヤレス 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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、QBSS ロードを設定する例を示します。

```
Device(config-wireless-policy)#qbss-load
```

qos-map

Quality of Service（QoS）マップを設定するには、**qos-map** コマンドを AP プロファイル コンフィギュレーション モードで使用します。

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。

qos-map { **action-frame** | **dscp-to-up-exception** *dscp-value user-priority* | **dscp-to-up-range** *user-priority dscp-value lower-dscp-range upper-dscp-range* | **trust-dscp-upstream** }

構文の説明

action-frame	QoS マップ設定が変更された場合に、802.11 QoS マップアクションフレームを送信します。
dscp-to-up-exception	DSCPからユーザープライオリティのマッピングの例外を指定します。
dscp-to-up-range	DSCP からユーザープライオリティのマッピングを指定します。 すべてのカスタム マッピングを削除するには、**no dscp-to-up-range** コマンドを使用します。
dscp-value	ユーザープライオリティから DSCP アップストリーム。有効な範囲は 0 ～ 63 です。
user-priority	ユーザー プライオリティ。有効な範囲は 1 ～ 7 です。
lower-dscp-range	DSCP 範囲の下限。有効な範囲は 0 ～ 63 です。
upper-dscp-range	DSCP 範囲の上限。有効な範囲は 0 ～ 63 です。
trust-dscp-upstream	ユーザープライオリティではなくアップストリーム DSCP を信頼するようにアクセスポイント（AP）に指示します。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

IP ネットワークを使用するインターネットワーキングの場合、マッピングは、802.11eユーザープライオリティと IP DSCP の間で作成されます。

マッピングは、個々の UP 値に対する DSCP 範囲として、また、DSCP 値と UP 値の間の 1 対 1 のマッピングを持つ例外のセットとして指定されます。QoS マップが有効になっていて、ユーザ設定が可能なマッピングが追加されていない場合は、デフォルト値が使用されます。

user-priority 値ごとに 1 つずつ、最大 8 つの設定エントリを *user-priority* に設定できます。カスタム値を設定しない場合は、未設定の値（0xFF）が対応する AP とワイヤレスクライアントに送信されます。

dscp-to-up-exception には、最大 21 のエントリを設定できます。

次の表に、対応する AP がワイヤレスクライアントに対し、IP DSCP から 802.11e ユーザープライオリティへの必要なマッピングを提供する QoS マップを示します。

表 *10* : デフォルトの *DSCP* 範囲から *UP* へのマッピング

IP DSCP 範囲	802.11e ユーザー プライオリティ
0 ～ 7	0
8 ～ 15	1
16 ～ 23	2
24 ～ 31	3
32 ～ 39	4
40 ～ 47	5
48 ～ 55	6
56 ～ 63	7

次の表に、DSCP 値とユーザープライオリティ値間の 1 対 1 マッピングを使用した例外のセットを示します。

表 *11* : デフォルトの *DSCP* 範囲から *UP* へのマッピングの例外

IP DSCP	802.11e ユーザー プライオリティ
0	0
2	1
4	1
6	1
10	2
12	2
14	2
18	3
20	3

IP DSCP	802.11e ユーザー プライオリティ
22	3
26	4
34	5
46	6
48	7
56	7

例

次に、QoS マップを設定する例を示します。

```
Device(config)# ap profile hotspot
Device(config-ap-profile)# qos-map dscp-to-up-range 6 52 23 62
```

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。

qos queue-softmax-multiplier *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
	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。

qos video

無線 QoS クラスをビデオ専用に設定するには、**qos video** コマンドを使用します。

qos video

コマンド デフォルト

なし

コマンド モード

config-media-stream

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、無線 QoS クラスをビデオ専用に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# qos video
```

qos wireless-default untrust

信頼できないワイヤレス パケットに対するデフォルトの信頼動作を設定するには、**qos wireless-default untrust** コマンドを使用します。ワイヤレス トラフィックのデフォルトの信頼動作を信頼するように設定するには、このコマンドの **no** 形式を使用します。

qos wireless-default-untrust
no qos wireless-default-untrust

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

device で信頼動作を確認するには、**show running-config** | **sec qos** または **show run** | **include untrust** コマンドを使用します。

コマンド 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 XE ジブラルタル 16.10.1	このコマンドが導入されました。

次に、信頼されているワイヤレス トラフィックのデフォルトの動作を untrusted に変更するコマンドを示します。

```
デバイス(config)# qos wireless-default-untrust
```

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、**bandwidth**、**shape** または **priority** コマンドのいずれか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。

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。

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。

```
デバイス(config)# policy-map policy_queuebuf01
デバイス(config-pmap)# class-map class_queuebuf01
デバイス(config-cmap)# exit
デバイス(config)# policy policy_queuebuf01
デバイス(config-pmap)# class class_queuebuf01
デバイス(config-pmap-c)# bandwidth percent 80
デバイス(config-pmap-c)# queue-buffers ratio 10
デバイス(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。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。クラスに対して定義した最大パケットしきい値に到達した場合、クラスのキューにさらにパケットがキューイングされると、テール ドロップが発生します。

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。

```
デバイス(config)# policy-map policy11
デバイス(config-pmap)# class dscp-1
デバイス(config-pmap-c)# bandwidth percent 20
デバイス(config-pmap-c)# queue-limit dscp 1 percent 20
```

queue-set

キューセットにポートをマッピングするには、インターフェイス コンフィギュレーション モードで **queue-set** 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。

queue-set *qset-id*
no queue-set *qset-id*

構文の説明

qset-id	キューセット ID。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ～ 2 です。

コマンド デフォルト

キューセット ID 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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。

```
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface** [*interface-id*] **buffers** 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
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
mls qos queue-set output threshold	Weighted Tail-Drop（WTD）しきい値を設定し、バッファのアベイラビリティを保証し、キュー セットに対する最大メモリ割り当てを設定します。

radio policy dot11 5ghz slot

特定の 5 GHz スロットでの WLAN 無線ポリシーを設定するには、**radio policy dot11 5ghz slot** コマンドを使用します。

radio policy dot11 5ghz slot *slot_ID*

構文の説明

0	無線スロット 0 を使用した 5 GHz 無線での WLAN を設定します。
1	無線スロット 1 を使用した 5 GHz 無線での WLAN を設定します。
2	無線スロット 2（存在する場合）を使用した 5 GHz 無線での WLAN を設定します。 （注）　指定した 5 GHz 無線スロットでのみ WLAN を設定できます。

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 Bengaluru 17.6.1	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 をブロードキャストする特定の無線とスロットを選択できます。このオプションは、5 GHz 無線でのみ使用できます。

例

次に、特定の WLAN スロットでの無線ポリシーを設定する例を示します。

```
Device# configure terminal
Device(config)#wlan test4
Device(config-wlan)# radio policy dot11 5ghz
Device(config-wlan-radio-5ghz)# slot 1
Device(config-wlan)# end
```

radio spatial-stream

2.4 GHz、5 GHz、6 GHz、およびセカンダリ 5 GHz 無線の空間ストリームを設定するには、**radio spatial-stream** コマンドを使用します。

sequence-number **radio** { **24ghz** | **5ghz** | **6ghz** | **secondary-5ghz** } **spatial-stream** { **1** | **2** | **3** | **4** | **8** }

構文の説明

sequence-number	電力プロファイルの設定は、シーケンス番号順に並べられています。APのディレーティングは、入力されたシーケンス番号に従って行われます。インターフェイス識別子とパラメータ値の同じ組み合わせは、別のシーケンス番号には表示されません。同じパラメータを持つ同じインターフェイスが、異なるパラメータ値で複数回表示されることがあります。
24ghz	2.4 GHz 無線を設定します。
5ghz	5 GHz 無線を設定します。
6ghz	6 GHz 無線を設定します。
secondary-5ghz	セカンダリ 5 GHz 無線を設定します。
{ **1** | **2** |**3** | **4** | **8**}	• **1**：1X1 無線空間ストリームを指定します。 • **2**：2X2 無線空間ストリームを指定します。 • **3**：3X3 無線空間ストリームを指定します。 • **4**：4X4 無線空間ストリームを指定します。 • **8**：8X8 無線空間ストリームを指定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス電力プロファイル 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 Cupertino 17.10.1	このコマンドが導入されました。

例

次に、ワイヤレス電力プロファイル コンフィギュレーション モードで無線空間ストリームを設定する例を示します。

```
Device(config)# wireless profile power power-profile-name
Device(config-wireless-power-profile)# 20 radio radio 5ghz spatial-stream 4
```

radius server

RADIUS サーバを設定するには、グローバル コンフィギュレーション モードで **radius server** コマンドを使用します。

radius server *server-name*

構文の説明

server-name	RADIUS サーバー名。

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 Gibraltar 16.10.1	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、RADIUS サーバーを設定する例を示します。

```
デバイス(config)# radius server ISE
```

radius-server deadtime

一部のサーバーが使用できない場合に RADIUS の応答時間を短縮するには、**radius-server deadtime** コマンドを使用して、使用できないサーバーをただちにスキップします。デッドタイムをデフォルト値の 0 に設定するには、このコマンドの **no** 形式を使用します。

radius-server deadtime *time-in-minutes*

no radius-server deadtime

構文の説明

time-in-minutes	RADIUS サーバーがトランザクション要求によってスキップされる時間を最長 1440 分（24 時間）まで分単位で表したものです。

コマンド デフォルト

デッド タイムは 0 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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

このコマンドを使用して、認証要求に応答しない RADIUS サーバーを "dead" としてマークします。これにより、設定されている次のサーバーを試行する前に要求の待機がタイムアウトにならないようにします。"dead" としてマークされた RADIUS サーバーは、この期間（分単位）、その他の要求でスキップされます。ただし、"dead" としてマークされていないサーバーが他にない場合を除きます。

例

次に、認証要求への応答に失敗した RADIUS サーバーのデッドタイムを設定する例を示します。

```
Device(config)# radius-server deadtime 5
```

radius-server attribute wireless accounting call-station-id

RADIUS アカウンティングメッセージで送信される発信側ステーション識別子を設定するには、**radius-server attribute wireless accounting call-station-id** コマンドを使用します。RADIUS アカウンティングメッセージから発信側ステーション識別子を削除するには、このコマンドの **no** 形式を使用します。

radius-server attribute wireless authentication call-station-id { **ap-ethmac-only** | **ap-ethmac-ssid** | **ap-ethmac-ssid-flexprofilename** | **ap-ethmac-ssid-policytagname** | **ap-ethmac-ssid-sitetagname** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-macaddress** | **ap-macaddress-ssid** | **ap-macaddress-ssid-flexprofilename** | **ap-macaddress-ssid-policytagname** | **ap-macaddress-ssid-sitetagname** | **ap-name** | **ap-name-ssid** | **flex-profile-name** | **ipaddress** | **macaddress** | **policy-tag-name** | **site-tag-name** | **vlan-id** }

構文の説明

ap-ethmac-only	発信側ステーション識別子タイプを、AP の無線 MAC アドレスに設定します。
ap-ethmac-ssid	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスに設定します。
ap-ethmac-ssid-flexprofilename	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスと Flex プロファイル名に設定します。
ap-ethmac-ssid-policytagname	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスとポリシータグ名に設定します。
ap-ethmac-ssid-sitetagname	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスとサイトタグ名に設定します。
ap-group-name	AP グループ名を使用するように発信側ステーション識別子タイプを設定します。
ap-label-address	発信側ステーション識別子タイプを、AP ラベルに印刷されている AP の無線 MAC アドレスに設定します。
ap-label-address-ssid	発信側ステーション識別子タイプを、AP ラベルに印刷されている AP の無線 MAC アドレスおよび SSID に設定します。
ap-location	発信側ステーション識別子タイプを、AP の場所に設定します。
ap-macaddress	発信側ステーション識別子タイプを、AP の無線 MAC アドレスに設定します。
ap-macaddress-ssid	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスに設定します。

ap-macaddress-ssid-flexprofilename	発信側ステーション識別子タイプを、APのSSIDを持つ無線 MAC アドレスと Flex プロファイル名に設定します。
ap-macaddress-ssid-policytagname	発信側ステーション識別子タイプを、APのSSIDを持つ無線 MAC アドレスとポリシータグ名に設定します。
ap-macaddress-ssid-sitetagname	発信側ステーション識別子タイプを、APのSSIDを持つ無線 MAC アドレスとサイトタグ名に設定します。
ap-name	発信側ステーション識別子タイプを、AP名に設定します。
ap-name-ssid	発信側ステーション識別子タイプを、SSIDを持つAP名に設定します。
flex-profile-name	発信側ステーション識別子タイプを、Flexプロファイル名に設定します。
ipaddress	発信側ステーション識別子タイプを、システムの IP アドレスに設定します。
macaddress	発信側ステーション識別子タイプを、システムの MAC アドレスに設定します。
policy-tag-name	発信側ステーション識別子タイプを、ポリシータグ名に設定します。
site-tag-name	発信側ステーション識別子タイプを、サイトタグ名に設定します。
vlan-id	発信側ステーション識別子タイプを、システムの VLAN ID に設定します。

コマンド デフォルト

発信側ステーション識別子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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。
Cisco IOS XE Bengaluru 17.4.1	このコマンドが変更されました。**policy-tag-name**、**flex-profile-name**、**ap-macaddress-ssid-flexprofilename**、**ap-macaddress-ssid-policytagname**、**ap-macaddress-ssid-sitetagname**、**ap-ethmac-ssid-flexprofilename**、**ap-ethmac-ssid-policytagname**、および**ap-ethmac-ssid-sitetagname**キーワードが導入されました。

使用上のガイドライン

例

次に、RADIUS アカウンティングメッセージで送信される発信側ステーション識別子を設定する例を示します。

```
Device(config)# radius-server attribute wireless accounting call-station-id site-tag-name
```

radius-server attribute wireless authentication call-station-id

RADIUS認証メッセージで送信される発信側ステーション識別子を設定するには、**radius-server attribute wireless authentication call-station-id** コマンドを使用します。RADIUS アカウンティングメッセージから発信側ステーション識別子を削除するには、このコマンドの **no** 形式を使用します。

radius-server attribute wireless authentication call-station-id { **ap-ethmac-only** | **ap-ethmac-ssid** | **ap-ethmac-ssid-flexprofilename** | **ap-ethmac-ssid-policytagname** | **ap-ethmac-ssid-sitetagname** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-macaddress** | **ap-macaddress-ssid** | **ap-macaddress-ssid-flexprofilename** | **ap-macaddress-ssid-policytagname** | **ap-macaddress-ssid-sitetagname** | **ap-name** | **ap-name-ssid** | **flex-profile-name** | **ipaddress** | **macaddress** | **policy-tag-name** | **site-tag-name** | **vlan-id** }

構文の説明

ap-ethmac-only	発信側ステーション識別子タイプを、AP の無線 MAC アドレスに設定します。
ap-ethmac-ssid	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスに設定します。
ap-ethmac-ssid-flexprofilename	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスと Flex プロファイル名に設定します。
ap-ethmac-ssid-policytagname	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスとポリシータグ名に設定します。
ap-ethmac-ssid-sitetagname	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスとサイトタグ名に設定します。
ap-group-name	AP グループ名を使用するように発信側ステーション識別子タイプを設定します。
ap-label-address	発信側ステーション識別子タイプを、AP ラベルに印刷されている AP の無線 MAC アドレスに設定します。
ap-label-address-ssid	発信側ステーション識別子タイプを、AP ラベルに印刷されている AP の無線 MAC アドレスおよび SSID に設定します。
ap-location	発信側ステーション識別子タイプを、AP の場所に設定します。
ap-macaddress	発信側ステーション識別子タイプを、AP の無線 MAC アドレスに設定します。
ap-macaddress-ssid	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスに設定します。

ap-macaddress-ssid-flexprofilename	発信側ステーション識別子タイプを、APのSSIDを持つ無線 MAC アドレスと Flex プロファイル名に設定します。
ap-macaddress-ssid-policytagname	発信側ステーション識別子タイプを、APのSSIDを持つ無線 MAC アドレスとポリシータグ名に設定します。
ap-macaddress-ssid-sitetagname	発信側ステーション識別子タイプを、APのSSIDを持つ無線 MAC アドレスとサイトタグ名に設定します。
ap-name	発信側ステーション識別子タイプを、AP名に設定します。
ap-name-ssid	発信側ステーション識別子タイプを、SSIDを持つAP名に設定します。
flex-profile-name	発信側ステーション識別子タイプを、Flexプロファイル名に設定します。
ipaddress	発信側ステーション識別子タイプを、システムの IP アドレスに設定します。
macaddress	発信側ステーション識別子タイプを、システムの MAC アドレスに設定します。
policy-tag-name	発信側ステーション識別子タイプを、ポリシータグ名に設定します。
site-tag-name	発信側ステーション識別子タイプを、サイトタグ名に設定します。
vlan-id	発信側ステーション識別子タイプを、システムの VLAN ID に設定します。

コマンド デフォルト

発信側ステーション識別子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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。
Cisco IOS XE Bengaluru 17.4.1	このコマンドが変更されました。**policy-tag-name**、**flex-profile-name**、**ap-macaddress-ssid-flexprofilename**、**ap-macaddress-ssid-policytagname**、**ap-macaddress-ssid-sitetagname**、**ap-ethmac-ssid-flexprofilename**、**ap-ethmac-ssid-policytagname**、および **ap-ethmac-ssid-sitetagname** キーワードが導入されました。

使用上のガイドライン

例

次に、RADIUS 認証メッセージで送信される発信側ステーション識別子を設定する例を示します。

```
Device(config)# radius-server attribute wireless authentication call-station-id
site-tag-name
```

radius-server attribute wireless location delivery out-of-band include-location-capable

デバイスで設定されたロケーション情報を提供する Location-Capable 属性を有効にするには、**radius-server attribute wireless location delivery out-of-band include-location-capable** コマンドを使用します。Location-Capable 属性を無効にするには、このコマンドの **no** 形式を使用します。

radius-server attribute wireless location delivery out-of-band include-location-capable

no radius-server attribute wireless location delivery out-of-band include-location-capable

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

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 Dublin 17.11.1	このコマンドが導入されました。

使用上のガイドライン

radius-server attribute wireless location delivery out-of-band include-location-capable コマンドを使用すると、Location-Capable 属性と Location（Location-Information および Location-Data）属性が有効になります。

no radius-server attribute wireless location delivery out-of-band include-location-capable コマンドを使用すると、Location-Capable 属性と Location（Location-Information および Location-Data）属性が無効になります。

Location-Capable 属性を使用せずに Location 属性を有効にするには、**radius-server attribute wireless location delivery out-of-band** コマンドを使用します。

例

次に、Location-Capable 属性を有効にして、デバイスで使用可能なロケーションプロファイル設定の詳細を提供する例を示します。

```
Device# configure terminal
Device(config)# radius-server attribute wireless location delivery out-of-band
include-location-capable
```

range

MAP から RAP ブリッジへの範囲を設定するには、**range** コマンドを使用します。

range *range-in-feet*

構文の説明

range-in-feet	範囲の値をフィート単位で設定します。有効な範囲は 150 ～ 132000 フィートです。

コマンド デフォルト

1200

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ AP プロファイルで MAP から RAP ブリッジへの範囲を設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# range 300
```

reanchor class

選択的リアンカー機能のプロトコルを使用してクラスマップを設定するには、**reanchor class** コマンドを使用します。

reanchor class *class-name*

構文の説明

class-name	AVC リアンカーのクラス名。

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AVC リアンカーのクラス名を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# reanchor class AVC-Reanchor-Class
```

record wireless avc basic

wireless avc basic AVC フロー レコードをフロー モニタに適用するには、**record wireless avc basic** コマンドを使用します。

record wireless avc basic

コマンド デフォルト

なし

コマンド モード

config-flow-monitor

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

このコマンドは、基本的なワイヤレス AVC テンプレートを指定します。AVC を設定する場合は、**record wireless avc basic** コマンドを使用してフロー モニタを作成する必要があります。

例

次に、*wireless avc basic* AVC フロー レコードを *test-flow* という名前のフロー モニターに適用する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# flow monitor test-flow
Device(config-flow-monitor)# record wireless avc basic
```

redundancy revertive

冗長モデルを復元可能に設定するには、**redundancy revertive** コマンドを使用します。

redundancy revertive

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

EoGRE ドメイン 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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次の例では、冗長モードを復元可能に設定する方法を示します。

```
Device(config-eogre-domain)# redundancy revertive
```

redun-management interface Vlan

冗長管理インターフェイス（RMI）を設定するには、**redun-management interface Vlan** コマンドを使用します。

redun-management interface Vlan *vlan-interface-no* **chassis** *chassis-number* **address** *ip-address* **chassis** *chassis-number* **address** *ip-address*

構文の説明

vlan-interface-no	VLAN インターフェイス番号です。有効な範囲は 1 ～ 4094 です。 （注） ここで、*vlan-interface-no* は管理 VLAN と同じ VLAN です。つまり、両方とも同じサブネット上に存在する必要があります。
chassis-number	シャーシ番号です。有効な範囲は 1 ～ 2 です。
ip-address	RMI IP 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 Amsterdam 17.1.1s	このコマンドが導入されました。

次に、冗長管理インターフェイス（RMI）を設定する例を示します。

```
Device# chassis redundancy ha-interface GigabitEthernet 3
Device# configure terminal
Device(config)# redun-management interface Vlan 200 chassis 1 address 9.10.90.147 chassis
 2 address
9.10.90.149
Device(config)# end
```

redun-management garp-retransmit

GARP 再送信が実行されるレートを決定するには、**redun-management garp-retransmit** コマンドを使用します。

redun-management garp-retransmit burst *packet-burst-size* **interval** *time-interval*

構文の説明

packet-burst-size	有効な範囲は 0 ～ 1000 です。値を 0 にすると、再送信が無効になります。
time-interval	時間間隔を秒単位で示します。有効な範囲は 0 ～ 5 秒です。値を 0 にすると、再送信が無効になります。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、GARP 再送信が実行されるレートを決定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# redun-management garp-retransmit burst packet-burst-size interval
time-interval
```

redirect

外部ポータルへのリダイレクトを設定するには、 **redirect** コマンドを使用します。

redirect {**for-login** | **on-failure** | **on-success** }*redirect-url-name*

構文の説明

for-login	ログインするには、この URL にリダイレクトします。
on-failure	ログインが失敗した場合は、このURLにリダイレクトします。
on-success	ログインが成功した場合は、このURLにリダイレクトします。
redirect-url-name	リダイレクト URL 名。

コマンド デフォルト

なし

コマンド モード

config-params-parameter-map

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ログインするための外部IPv4 URL へのリダイレクトを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-name
Device(config-params-parameter-map)# redirect for-login cisco.com
```

redirect portal

外部 IPv4 または IPv6 ポータルを設定するには、 **redirect portal** コマンドを使用します。

redirect portal {**ipv4** | **ipv6** }*ip-addr*

構文の説明

ipv4	IPv4 portal address
ipv6	IPv6 portal address

コマンド デフォルト

なし

コマンド モード

config-params-parameter-map

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、外部 IPv4 ポータルのアドレスを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-name
Device(config-params-parameter-map)# redirect portal ipv4 192.168.1.100
```

remote-span

VLAN をリモート スイッチド ポート アナライザ（RSPAN）VLAN として設定するには、スイッチ スタック上またはスタンドアロン スイッチ上で、VLAN コンフィギュレーション モードで **remote-span** コマンドを使用します。RSPAN 指定を VLAN から削除するには、このコマンドの **no** 形式を使用します。

remote-span
no remote-span

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

RSPAN VLAN は定義されません。

コマンド モード

VLAN コンフィギュレーション（config-VLAN）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

VLAN Trunking Protocol（VTP）がイネーブルで、VLAN ID が 1005 未満の場合は、RSPAN 機能は VTP によって伝達されます。RSPAN VLAN ID が拡張範囲内の場合は、手動で中間スイッチを設定する必要があります（送信元スイッチと宛先スイッチの間の RSPAN VLAN 内に設定）。

RSPAN **remote-span** コマンドを設定する前に、**vlan**（グローバル コンフィギュレーション）コマンドで VLAN を作成してください。

RSPAN VLAN には、次の特性があります。

- MAC アドレス ラーニングは実行されません。
- トランク ポートでは RSPAN VLAN トラフィックだけが流れます。
- スパニングツリー プロトコル（STP）は RSPAN VLAN 内では稼働できますが、RSPAN 宛先ポートでは稼働しません。

既存の VLAN が RSPAN VLAN として設定されている場合は、その VLAN が最初に削除され、RSPAN VLAN として再作成されます。アクセス ポートは、RSPAN 機能がディセーブルになるまでは非アクティブです。

次の例では、RSPAN VLAN として VLAN を設定する方法を示します。

```
デバイス(config)# vlan 901
デバイス(config-vlan)# remote-span
```

次の例では、VLAN から RSPAN 機能を削除する方法を示します。

```
デバイス(config)# vlan 901
デバイス(config-vlan)# no remote-span
```

設定を確認するには、**show vlan remote-span** ユーザー EXEC コマンドを入力します。

remote-lan

RLAN ポリシー プロファイルを RLAN プロファイルにマッピングするには、**remote-lan** コマンドを使用します。

remote-lan *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id*

構文の説明

remote-lan-profile-name	リモート LAN プロファイルの名前。
rlan-policy-profile-name	リモートLANポリシープロファイルの名前。
port-id	ポート ID

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、RLAN ポリシー プロファイルを RLAN プロファイルにマッピングする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless tag policy remote-lan-policy-tag
デバイス(config-policy-tag)# remote-lan rlan_profile_name policy rlan_policy_profile
port-id 2
デバイス(config-policy-tag)# end
```

remote-lan rlan-profile policy rlan-policy ext-module

外部モジュールへのリモート LAN プロファイルおよびポリシーマッピングを設定するには、**remote-lan** *rlan-profile* **policy** *rlan-policy***ext-module** コマンドを使用します。外部モジュールへのリモート LAN プロファイルおよびポリシーマッピ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。

remote-lan *rlan-profile* **policy** *rlan-policy***ext-module**

構文の説明

rlan-profile	外部モジュールの RLAN プロファイルを設定します
rlan-policy	外部モジュールの RLAN ポリシーを設定します

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 Gibraltar 17.3.1	このコマンドが導入されました。

例

次に、ポリシータグの下の外部モジュールへのリモート LAN プロファイルおよびポリシーマッピングを設定する例を示します。

```
Device(config)# wireless tag policy default-policy-tag
Device(config-policy-tag)# remote-lan <rlan-profile> policy <rlan-policy> ext-module
```

request platform software trace archive

シャーシでの最後のリロード以降にシステム上で実行されているすべてのプロセスに関連するすべてのトレースログをアーカイブし、これを指定された場所に保存するには、特権 EXEC モードまたはユーザ EXEC モードで **request platform software trace archive** コマンドを使用します。

request platform software trace archive ［**last** *number-of-days* ［**days** ［**target** *location*］］ | **target** *location*］

構文の説明

last *noofdays*	トレース ファイルをアーカイブする必要がある日数を指定します。
target *location*	アーカイブ ファイルの場所と名前を指定します。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

このアーカイブ ファイルは、tftp コマンドまたは scp コマンドを使用してシステムからコピーできます。

例

次に、過去 5 日以降にシャーシで実行されているプロセスのすべてのトレースログをアーカイブする例を示します。

```
デバイス# request platform software trace archive last 5 days target flash:test_archive
```

resilient

Flex + ブリッジモードの AP で Flex Resilient 機能を有効にするには、**resilient** コマンドを使用します。

resilient

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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.3.1	このコマンドが導入されました。

使用上のガイドライン

次に、Flex + ブリッジモードの AP で Flex Resilient 機能を有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless profile flex new-flex-profile
Device(config-wireless-flex-profile)# arp-caching
Device(config-wireless-flex-profile)# description "new flex profile"
Device(config-wireless-flex-profile)# native-vlan-id 2660
Device(config-wireless-flex-profile)# resilient
Device(config-wireless-flex-profile)# vlan-name VLAN2659
Device(config-wireless-flex-profile)# vlan-id 2659
Device(config-wireless-flex-profile)# end
```

rf tag

AP に RF タグを設定するには、**rf tag** コマンドを使用します。

rf tag *rf-tag-name*

構文の説明

rf-tag-name	RF タグ名。

コマンド デフォルト

なし

コマンド モード

config-ap-tag

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを実行すると、AP は、接続解除されたのち再参加します。

例

次に、RF タグを設定する例を示します。

```
Device(config-ap-tag)# rf-tag rftag1
```

roaming-oi

802.11u ローミング組織識別子を設定するには、**roaming-oi** コマンドを使用します。ローミング組織識別子を削除するには、このコマンドの **no** 形式を使用します。

roaming-oi *OI-value*［**beacon**］

構文の説明

OI-value	ローミング組織識別子の値。
beacon	ローミング組織識別子を BSSID ビーコンの一部としてアドバタイズします。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

最大 255 種類の OI 値を設定できます。

ローミング OI には最大 3 つのビーコンを使用できます。

ビーコンが指定されている場合、ローミング OUI は AP WLAN ビーコンまたはプローブ応答でアドバタイズされます。そうでない場合は、ローミング OUI ANQP クエリの実行中に返されるのみとなります。

例

次に、動作クラス識別子を設定する例を示します。

```
Device(config)#wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# roaming-oi 24 beacon
```

rogue detection containment pmf-denial

PMF 拒否の不正 AP 封じ込めを有効にするには、**rogue detection containment pmf-denial** コマンドを使用します。PMF 拒否の不正 AP 封じ込めを無効にするには、このコマンドの **no** 形式を使用します。

rogue detection containment pmf-denial

no rogue detection containment pmf-denial

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

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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、PMF 拒否の不正 AP 封じ込めを有効にする例を示します。

```
Device# configure terminal
Device(config)# ap profile xyz-ap-profile
Device(config-ap-profile)# rogue detection containment pmf-denial
Device(config-pmf-denial)# pmf-deauth
```

rrc-evaluation

リソース予約コントロール（RRC）再評価アドミッションを設定するには、**rrc-evaluation** コマンドを使用します。

rrc-evaluation {**initial** | **periodic**}

構文の説明

initial	最初のアドミッション評価を設定します。
periodic	定期的なアドミッション評価を設定します。

コマンド デフォルト

なし

コマンド モード

config-media-stream

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次の例は、RRC 再評価アドミッションを最初のアドミッション評価に設定する方法を示しています。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# rrc-evaluation initial
```

sampling

AP センサー環境でデータサンプリング間隔を設定するには、**sampling** コマンドを使用します。データサンプリング間隔をデフォルト時間の 5 秒に設定する場合は、このコマンドの **no** 形式を使用します。

sampling *data-sampling-interval*

no sampling *data-sampling-interval*

構文の説明

data-sampling-interval	データサンプリング間隔を設定します。 有効な範囲は 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

なし

コマンド モード

AP センサー 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 Cupertino 17.8.1	このコマンドが導入されました。

例

次に、AP センサー環境でデータサンプリング間隔を設定する例を示します。

```
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# sensor environment air-quality
Device(config-ap-sensor)# sampling 300
```

scheduler asr

WLAN で高度なスケジューリング要求機能を有効にするには、**scheduler asr** コマンドを使用します。WLAN で高度なスケジューリング要求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。

scheduler asr

no scheduler asr

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

高度なスケジューリング要求機能は有効になっています。

コマンド モード

WLAN コンフィギュレーション（config-wlan）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.4.1	このコマンドが追加されました。

例

次に、WLAN で高度なスケジューリング要求機能を設定する例を示します。

```
Device# configure terminal
Device(config)# wlan test4
Device(config-wlan)# scheduler asr
```

secondary (ap prime)

アクセスポイント（AP）フォールバック用のセカンダリコントローラを設定するには、**secondary** コマンドを使用します。AP プライミングに使用されないようにセカンダリコントローラを削除するには、このコマンドの **no** 形式を使用します。

secondary *controller-name ip-address*

no secondary *controller-name ip-address*

構文の説明

controller-name	セカンダリ コントローラの名前。
ip-address	コントローラの IPv4 または IPv6 アドレス。

コマンド デフォルト

なし

コマンド モード

AP プライム コンフィギュレーション（config-priming）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.2	このコマンドが導入されました。

例

次に、AP フォールバック用のセカンダリコントローラを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile ap priming Prime-FX
Device(config-priming)# secondary bbbb 209.165.201.3
```

secure-webauth-disable

Web 認証用の HTTP セキュアサーバーを無効にするには、グローバル パラメータ マップ モードで **secure-webauth-disable** コマンドを使用します。このコマン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。

secure-webauth-disable

no secure-webauth-disable

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

グローバル パラメータ マップ モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、Web 認証用の HTTP セキュアサーバーを無効にする例を示します。

```
Device(config-params-parameter-map)# secure-weauth-disable
```

security

メッシュ セキュリティを設定するには、 **security** コマンドを使用します。

security { **eap** | **psk** }

構文の説明

eap	メッシュ AP のメッシュ セキュリティ EAP を設定します。
psk	メッシュ AP のメッシュ セキュリティ PSK を設定します

コマンド デフォルト

EAP

コマンド モード

config-wireless-mesh-profile

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ AP で EAP プロトコルを使用してメッシュ セキュリティを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile mesh profile-name
Device(config-wireless-mesh-profile)# security eap
```

security dot1x authentication-list

IEEE 802.1x のセキュリティ認証リストを設定するには、**security dot1x authentication-list** *auth-list-name* コマンドを使用します。

security dot1x authentication-list *auth-list-name*

構文の説明

パラメータ	説明
auth-list-name	認証リスト名。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、IEEE 802.1x のセキュリティ認証リストを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan-name
Device(config-wlan)# security dot1x authentication-list auth-list-realm
```

security dot1x request

EAP 要求関連のパラメータを設定するには、**security dot1x request** コマンドを使用します。EAP 要求関連のパラメータ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。

security dot1x request { **retries** *retry-num* | **timeout** *timeout-value* }

no security dot1x request { **retries** *retry-num* | **timeout** *timeout-value* }

構文の説明

retries *retries*	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を指定します。 有効な値の範囲は 0 ～ 20 です。
timeout *timeout-value*	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を指定します。 有効な値の範囲は 1 ～ 120 です。

コマンド デフォルト

なし

コマンド モード

リモート LAN コンフィギュレーション（config-remote-lan）

コマンド履歴

リリース	変更内容
	このコマンドが導入されました。

次の例では、 **wireless security dot1x** のすべてのコマンドをリストしています。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap remote-lan profile-name rlan_profile_name 3
Device(config-remote-lan)# security dot1x request retries 10
Device(config-remote-lan)# security dot1x request timeout 100
```

security dot1x identity-request

EAP ID 要求関連のパラメータを設定するには、**security dot1x identity-request** コマンドを使用します。EAP ID 要求関連のパラメータ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。

security dot1x identity-request { **retries** *retry-num* | **timeout** *timeout-value* }

no security dot1x identity-request { **retries** *retry-num* | **timeout** *timeout-value* }

構文の説明

retries *retries*	EAP ID 要求について、コントローラが要求を再送信する最大回数を指定します。 有効な値の範囲は 1 ～ 20 です。
timeout *timeout-value*	EAP ID 要求について、コントローラがメッセージを再送信するまでに待機する時間を指定します。 有効な値の範囲は 1 ～ 120 です。

コマンド デフォルト

なし

コマンド モード

リモート LAN コンフィギュレーション（config-remote-lan）

コマンド履歴

リリース	変更内容
	このコマンドが導入されました。

例

次に、EAP ID 要求関連のパラメータを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap remote-lan profile-name rlan_profile_name 3
Device(config-remote-lan)# security dot1x identity-request retries 10
Device(config-remote-lan)# security dot1x identity-request timeout 100
```

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。Fast Transition **over the air** 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 Gibraltar 16.10.1	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

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:

```
デバイス#wlan test
デバイス(config-wlan)# client vlan 0140
デバイス(config-wlan)# no mobility anchor sticky
デバイス(config-wlan)# no security wpa
デバイス(config-wlan)# no security wpa akm dot1x
デバイス(config-wlan)# no security wpa wpa2
デバイス(config-wlan)# no security wpa wpa2 ciphers aes
デバイス(config-wlan)# security ft
デバイス(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。

```
デバイス# wlan test
デバイス(config-wlan)# client vlan 0140
```

```
デバイス(config-wlan)# no security wpa akm dot1x
デバイス(config-wlan)# security wpa akm ft psk
デバイス(config-wlan)# security wpa akm psk set-key ascii 0 test-test
デバイス(config-wlan)# security ft
デバイス(config-wlan)# no shutdown
```

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 サーバー 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 Gibraltar 16.10.1	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。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)# security-level inspect
```

security pmf

WLAN の 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。device 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。値は 100 ミリ秒の倍数で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 Gibraltar 16.10.1	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（device）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。

```
デバイス(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。

```
デバイス(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。

```
デバイス(config-wlan)# security pmf optional
```

次に、saquery パラメータを設定する例を示します。

```
デバイス(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。

```
デバイス(config-wlan)# no security pmf
```

security static-wep-key

WLAN で静的 WEP キーを設定するには、**security static-wep-key** コマンドを使用します。

security static-wep-key {**authentication** {**open** | **sharedkey** } | **encryption** {**104** | **40** }{**ascii** | **hex** | {**0** | **8** }*wep-key* | **wep-index** }}

構文の説明

open	オープン システム認証。
sharedkey	共有キー認証。
0	暗号化されていないパスワードが使用されることを指定します。
8	AES 暗号化パスワードが使用されることを指定します。
wep-key	WEP キー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-wlan

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、共有キーを使用して 802.11 を認証する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan profile-name wlan-id
Device(config-wlan)# security static-wep-key authentication sharedkey
```

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、 **security web-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 Gibraltar 16.10.1	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。

```
デバイス(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** }] }]
no security wpa [{ **akm** { **cckm** | **dot1x** | **ft** | **pmf** | **psk** } | **wpa1** [**ciphers** { **aes** | **tkip** }] | **wpa2** [**ciphers** { **aes** }] }]

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（config-wlan）

コマンド履歴

リリース	変更内容
Cisco IOS XE ジブラルタル 16.10.1	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。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)#security wpa akm cckm
```

security wpa akm ft sae

SAE セキュリティ対応 WLAN で 802.11r Fast Transition を有効にするには、**security wpa akm ft sae** コマンドを使用します。

security wpa akm ft sae

構文の説明

security	WLANのセキュリティポリシーを設定します。
wpa	WLAN の WPA/WPA2 サポートを設定します。
akm	認証キー管理を設定します。
ft	802.11r Fast Transition を設定します。
sae	SAE サポートを設定します。

コマンド デフォルト

なし

コマンド モード

WLAN コンフィギュレーション モード（config-wlan）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、SAE セキュリティ対応 WLAN で 802.11r Fast Transition を有効にする例を示します。

```
Device# configure terminal
Device(config)# wlan wlan-test 3 ssid-test
Device(config-wlan)# security ft
Device(config-wlan)# no security wpa wpa2
Device(config-wlan)# security wpa psk set-key ascii 0 123456789
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# security wpa akm ft sae
Device(config-wlan)# security wpa wpa3
Device(config-wlan)# security pmf mandatory
Device(config-wlan)# no shutdown
```

security wpa akm owe

認証キー管理（AKM）の Opportunistic Wireless Encryption（OWE）を有効にするには、**security wpa akm owe** コマンドを使用します。この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。

security wpa akm owe

no security wpa akm owe

構文の説明

security	WLANのセキュリティポリシーを設定します。
wpa	WLAN の WPA/WPA2 サポートを設定します。
akm	認証キー管理を設定します。
owe	OWE サポートを設定します。

コマンド デフォルト

なし

コマンド モード

WLAN コンフィギュレーション モード（config-wlan）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

次に、認証キー管理（AKM）の Opportunistic Wireless Encryption（OWE）を有効にする例を示します。

```
Device# configure terminal
Device(config)# wlan wlan-test 3 ssid-test
Device(config-wlan)# security wpa akm owe
```

security wpa akm psk

認証キー管理（AKM）の事前共有キー（PSK）を有効にするには、**security wpa akm psk** コマンドを使用します。この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。

security wpa akm psk

no security wpa akm psk

構文の説明

security	WLANのセキュリティポリシーを設定します。
wpa	WLAN の WPA/WPA2 サポートを設定します。
akm	認証キー管理を設定します。
psk	PSK サポートを設定します。

コマンド デフォルト

なし

コマンド モード

WLAN コンフィギュレーション モード（config-wlan）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

次に、認証キー管理（AKM）の事前共有キー（PSK）を有効にする例を示します。

```
Device# configure terminal
Device(config)# wlan wlan-test 3 ssid-test
Device(config-wlan)# security wpa akm psk
```

security wpa akm sae

認証キー管理（AKM）の Secure Agile Exchange（SAE）を有効にするには、**security wpa akm sae pwe** コマンドを使用します。この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。

security wpa akm sae pwe { h2e | hnp | both-h2e-hnp}

no security wpa akm sae pwe { h2e | hnp | both-h2e-hnp}

構文の説明

security	WLAN のセキュリティポリシーを設定します。
wpa	WLAN の WPA/WPA2 サポートを設定します。
akm	認証キー管理を設定します。
sae	SAE サポートを設定します。
pwe	SAE のパスワード要素を設定します。
h2e	Hash To Element のみを設定します（Hunting and Pecking を無効にします）。
hnp	Hunting And Pecking のみを設定します（Hash To Element を無効にします）。
both-h2e-hnp	Hash to Element と Hunting and Pecking の両方のサポートを設定します（デフォルトのオプションです）。

コマンド デフォルト

なし

コマンド モード

WLAN コンフィギュレーション モード（config-wlan）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

次に、認証キー管理（AKM）の Secure Agile Exchange（SAE）を有効にする例を示します。

```
Device# configure terminal
Device(config)# wlan wlan-test 3 ssid-test
Device(config-wlan)# security wpa akm sae
```

security wpa akm sae pwe

認証キー管理（AKM）の Secure Agile Exchange（SAE）PWE サポートを有効にするには、**security wpa akm sae pwe** コマンドを使用します。

security wpa akm sae pwe { h2e | hnp | both-h2e-hnp}

構文の説明

h2e	Hash-to-Element のみ。HnP を無効にします。
hnp	Hunting and Pecking のみ。H2E を無効にします。
Both-h2e-hnp	Hash-to-Element と Hunting and Pecking の両方をサポート（デフォルトのオプションです）。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが変更されました。

使用上のガイドライン

次に、AKM の SAE PWE サポートを有効にする例を示します。

```
Device# configure terminal
Device(config)# wlan WPA3 1 WPA3
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# no security ft over-the-ds
Device(config-wlan)# no security ft
Device(config-wlan)# no security wpa wpa2
Device(config-wlan)# security wpa wpa2 ciphers aes
Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123
Device(config-wlan)# security wpa wpa3
Device(config-wlan)# security wpa akm sae
Device(config-wlan)# security wpa akm sae pwe
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

segment

同じアプリケーションサービスを共有するデバイスのグループを識別するセグメント名を設定するには、**segment** コマンドを使用します。セグメントを削除するには、このコマンドの **no** 形式を使用します。

segment *segment-name*

no segment

構文の説明

segment-name	セグメント名。最大63文字の英数字を指定できます。

コマンド デフォルト

セグメント名は設定されていません。

コマンド モード

SD サービス コンフィギュレーション（config-sd-service）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが導入されました。

例

次に、同じアプリケーションサービスを共有するデバイスのグループを識別するセグメント名を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# avc sd-service
Device(config-sd-service)# segment test-segment
```

sensor environment

APセンサー環境を設定するには、**sensor environment** コマンドを使用します。この機能を無効化するには、このコマンドの **no** 形式を使用します。

sensor environment ｛ **air-quality** ｜ **temperature** ｝

no sensor environment ｛ **air-quality** ｜ **temperature** ｝

構文の説明

air-quality	電波品質センサーを指定します。
temperature	温湿度センサーを指定します。

コマンド デフォルト

なし

コマンド モード

AP プロファイル 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 Cupertino 17.8.1	このコマンドが導入されました。

例

次に、AP センサー環境を設定する例を示します。

```
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# sensor environment air-quality
```

sequence-number ethernet

イーサネットの電源ポリシーを設定するには、ワイヤレス電力プロファイル コンフィギュレーション モードで *sequence-number* **ethernet** コマンドを使用します。この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。

sequence-number **ethernet** { **GigabitEthernet0** | **GigabitEthernet1 speed** { **1000mbps** | **100mbps** | **2500mbps** | **5000mbps** } | **LAN1** | **LAN2** | **LAN3 state disable** }

no *sequence-number* **ethernet** { **GigabitEthernet0** | **GigabitEthernet1 speed** { **1000mbps** | **100mbps** | **2500mbps** | **5000mbps** } | **LAN1** | **LAN2** | **LAN3 state disable** }

構文の説明

sequence-number	電力プロファイルの設定は、シーケンス番号順に並べられています。AP のディレーティングは、入力されたシーケンス番号に従って行われます。インターフェイス識別子とパラメータ値の同じ組み合わせは、別のシーケンス番号には表示されません。同じパラメータを持つ同じインターフェイスが、異なるパラメータ値で複数回表示されることがあります。
GigabitEthernet0	GigabitEthernet0 を設定します。
GigabitEthernet1	GigabitEthernet1 を設定します。
speed	イーサネット速度の制限を設定します。 （注） イーサネット速度設定は、Cisco IOS XE Cupertino 17.8.1 では使用できません。
1000mbps	イーサネット速度の制限を 1000 Mbps に設定します。
100mbps	イーサネット速度の制限を 100 Mbps に設定します。
2500mbps	イーサネット速度の制限を 2500 Mbps に設定します。
5000mbps	イーサネット速度の制限を 5000 Mbps に設定します。
LAN1	LAN1 ポートを設定します。
LAN2	LAN2 ポートを設定します。
LAN3	LAN3 ポートを設定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス電力プロファイル 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 Cupertino 17.8.1	このコマンドが導入されました。

例

次に、ワイヤレス電力プロファイルコンフィギュレーションモードでイーサネットの電源ポリシーを設定する例を示します。

```
Device(config)# wireless profile power power-profile-name
Device(config-wireless-power-profile)# 10 ethernet gigabitethernet1 speed 1000mbps
```

（注） イーサネット速度設定は、Cisco IOS XE Cupertino 17.8.1 では使用できません。

sequence-number radio

無線の電源ポリシーを設定するには、ワイヤレス電力プロファイル コンフィギュレーション モードで *sequence-number* **radio** コマンドを使用します。この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。

sequence-number **radio** { **24ghz** | **5ghz** | **6ghz** | **secondary-5ghz** } **state shutdown**

no *sequence-number* **radio** { **24ghz** | **5ghz** | **6ghz** | **secondary-5ghz** } **state shutdown**

構文の説明

sequence-number	電力プロファイルの設定は、シーケンス番号順に並べられています。APのディレーティングは、入力されたシーケンス番号に従って行われます。インターフェイス識別子とパラメータ値の同じ組み合わせは、別のシーケンス番号には表示されません。同じパラメータを持つ同じインターフェイスが、異なるパラメータ値で複数回表示されることがあります。
24ghz	2.4 GHz 無線を設定します。
5ghz	5 GHz 無線を設定します。
6ghz	6 GHz 無線を設定します。
secondary-5ghz	セカンダリ 5 GHz 無線を設定します。
state shutdown	無線状態をダウンとして指定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス電力プロファイル 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 Cupertino 17.8.1	このコマンドが導入されました。

例

次に、ワイヤレス電力プロファイルコンフィギュレーションモードで無線の電源ポリシーを設定する例を示します。

```
Device(config)# wireless profile power power-profile-name
Device(config-wireless-power-profile)# 20 radio 6ghz state shutdown
```

sequence-number usb 0 state disable

USB の電源ポリシーを設定するには、ワイヤレス電力プロファイル コンフィギュレーション モードで *sequence-number* **usb 0 state disable** コマンドを使用します。この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。

sequence-number **usb 0 state disable**

no *sequence-number* **usb 0 state disable**

構文の説明

sequence-number	電力プロファイルの設定は、シーケンス番号順に並べられています。AP のディレーティングは、入力されたシーケンス番号に従って行われます。インターフェイス識別子とパラメータ値の同じ組み合わせは、別のシーケンス番号には表示されません。同じパラメータを持つ同じインターフェイスが、異なるパラメータ値で複数回表示されることがあります。

コマンド デフォルト

なし

コマンド モード

ワイヤレス電力プロファイル 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 Cupertino 17.8.1	このコマンドが導入されました。

例

次に、ワイヤレス電力プロファイル コンフィギュレーション モードで USB の電源ポリシーを設定する例を示します。

```
Device(config)# wireless profile power power-profile-name
Device(config-wireless-power-profile)# 30 usb 0 state disable
```

server-uri

オンラインサインアップ（OSU）オペレータのサーバー Uniform Resource Identifier（URI）を設定するには、**server-uri** コマンドを使用します。サーバー URI を削除するには、このコマンドの **no** 形式を使用します。

server-uri *server-uri*

構文の説明

server-uri	OSU オペレータのサーバー URI。

コマンド デフォルト

なし

コマンド モード

ANQP OSU プロバイダーの設定（config-anqp-osu-provider）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、OSU オペレータのサーバー URI を設定する例を示します。

```
Device(config-wireless-anqp-server)# osu-provider my-osu
Device(config-anqp-osu-provider)# server-uri yyyy
```

service-policy

Quality of Service（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。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 { **client** | **input** | **output** } *policy-name*

構文の説明

client	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 マップ名。

コマンド デフォルト

なし

コマンド モード

ワイヤレス 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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、入力サービスポリシーを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# service-policy input test1
```

service-policy qos

QoS サービス ポリシーを設定するには、 **service-policy qos** コマンドを使用します。

service-policy qos {**input** | **output**}*policy-name*

構文の説明

input	入力 QoS ポリシー。
output	出力 QoS ポリシー。
policy-name	ポリシー名。

コマンド デフォルト

なし

コマンド モード

config-service-template

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、出力 QoS ポリシーを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# service-template fabric-profile-name
Device(config-service-template)# service-policy qos output policy-name
```

service-template

サービス テンプレートを設定するには、 **service-template** コマンドを使用します。

service-template *service-template-name* {**access-group** *acl_list* | **vlan** *vlan_id* | **absolute-timer** *seconds* | **service-policy qos** {**input** | **output**}}

構文の説明

service-template-name	サービス テンプレートの名前。
acl_list	適用されるアクセス リストの名前。
vlan_id	VLAN ID。VLAN ID 値の範囲は 1 ～ 4094 です。
seconds	サービス テンプレートのセッション タイムアウト値。セッション タイムアウト値の範囲は 1 ～ 65535 秒です。
service-policy qos {**input** | **output**	クライアントの QoS ポリシー。

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 Gibraltar 16.10.1	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、サービス テンプレートを設定する例を示します。

```
デバイス#configure terminal
デバイス(config)#service-template cisco-phone-template
デバイス(config-service-template)#access-group foo-acl
デバイス(config-service-template)#vlan 100
デバイス(config-service-template)#service-policy qos input foo-qos
デバイス(config-service-template)#end
```

service timestamps

デバッグメッセージまたはロギングメッセージにタイムスタンプを使用するようにシステムを設定するには、グローバル コンフィギュレーション コマンドの **service timestamps** コマンドを使用します。この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。

service timestamps debug log{**datetime** | **uptime***localtimemsecshow-timezoneyear*}
no service timestamps debuglog

構文の説明

debug	タイムスタンプ メッセージ タイプとしてデバッグします。
log	タイムスタンプ メッセージ タイプとしてログに記録します。
datetime	**datetime**
uptime	（任意）システムが再起動されてからの時間を使用したタイムスタンプ。
localtime	（任意）ローカルタイムゾーンを基準にしたタイムスタンプ。
msec	（任意）日付とタイムスタンプにミリ秒を含めます。
show-timezone	（任意）タイムスタンプにタイムゾーン名を含めます。
year	（任意）タイムスタンプに年を含めます。

コマンド デフォルト

タイムスタンプは使用されません。

引数またはキーワードを使用せずに **service timestamps** を指定した場合、デフォルトは **service timestamps debug uptime** です。

service timestamps debugdatetime のデフォルトでは、時間は UTC 形式になり、ミリ秒もタイムゾーン名も含まれません。

no service timestamps コマンドは、単独でデバッグメッセージとログメッセージの両方のタイムスタンプを無効にします。

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 Amsterdam 17.1.1s	このコマンドは、Cisco IOS XE Amsterdam 17.1.1s 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

タイムスタンプは、デバッグメッセージまたはロギングメッセージに個別に追加できます。このコマンドの uptime 形式を使用すると、HHHH:MM:SS 形式のタイムスタンプが追加され、システムが再起動されてからの時間が示されます。このコマンドの datetime 形式を使用すると、MMM DD HH:MM:SS 形式のタイムスタンプが追加され、システムクロックによる日付と時刻

が示されます。システムクロックが設定されていない場合、日付と時刻の前にアスタリスク（*）が付き、日付と時刻が正しくない可能性があることが示されます。

例

次に、デバッグメッセージのタイムスタンプを有効にして、再起動してからの時間を表示する例を示します。

```
Device(config)# service timestamps debug uptime
```

次に、ロギングメッセージのタイムスタンプを有効にして、ローカルタイムゾーンを基準にした現在の日付と時刻を、タイムゾーン名を含めて表示する例を示します。

```
Device(config)# service timestamps log datetime localtime show-timezone
```

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。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。

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）。範囲は 300 ～ 86400 です。デフォルト値は 1800 です。 86400 の設定は、最大タイムアウトと同等です。また、値 0 は推奨されません。

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 Gibraltar 16.10.1	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 3600 秒に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless profile policy policy1
Device(config-wireless-policy)#session-timeout 3600
```

set

パケットで DiffServ コード ポイント（DSCP）値または IP precedence 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ユーザー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、precedence 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、precedence 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。

wlan user-priority *wlan-user-priority*	分類されたトラフィックにWLANユーザー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 ユーザー 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2CoSフィールド値をWLANユーザー 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 ユーザー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ユーザー プライオリティとして設定します。 • **wlan**WLAN ユーザー プライオリティ フィールド値をWLANユーザープライオリティとして設定します。 • （任意）**table** *table-map-name*：WLAN ユーザー 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ユーザー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ユーザー 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 Gibraltar 16.10.1	このコマンドが
	cos、**dscp**、**qos** 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* コマンドの場合は、一般に使用されている値のニーモニック名を入力できます。たとえば、**set dscp af11** コマンドを入力すると、**set dscp 10** コマンドを入力した場合と同じになります。**set ip precedence critical** コマンドを入力すると、**set ip precedence 5** コマンドを入力した場合と同じになります。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、**set dscp ?** または **set 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。

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。

```
デバイス(config)# policy-map policy_ftp
デバイス(config-pmap)# class-map ftp_class
デバイス(config-cmap)# exit
デバイス(config)# policy policy_ftp
デバイス(config-pmap)# class ftp_class
デバイス(config-pmap-c)# set dscp 10
デバイス(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。

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** 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）device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	（任意）フィルタの値。
switch *switch*	（任意）device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）device番号を指定します。

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 Gibraltar 16.10.1	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。

```
デバイス# set trace capwap ap ha detail filter mac WORD switch number
```

set trace mobility ha

内のワイヤレス 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** 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）device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*	device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*	device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

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# 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 Quality of Service（QoS）ハイ アベイラビリティを追跡するには、**set trace qos ap ha** 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

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

```
デバイス# set trace QOS ap ha
```

sgt-tag

ファブリック プロファイルに SGT タグを設定するには、**sgt-tag** コマンドを使用します。

sgt-tag *value*

構文の説明

value	SGT タグ値。有効な範囲は 2 ～ 65519 です。

コマンド デフォルト

デフォルトの SGT タグ値は 0 です。

コマンド モード

config-wireless-fabric

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、SGT タグを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile fabric fabric-profile-name
Device(config-wireless-fabric)# sgt tag 8
```

site-tag

サイト タグを AP にマッピングするには、**site-tag** コマンドを使用します。

site-tag *site-tag-name*

構文の説明

site-tag-name	サイト タグの名前。

コマンド デフォルト

なし

コマンド モード

config-ap-tag

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを実行すると、AP は、接続解除されたのち再参加します。

例

次に、サイト タグを設定する例を示します。

```
Device(config-ap-tag)# site-tag sitetag1
```

snmp-server group

新しい Simple Network Management Protocol（SNMP）グループを設定するには、グローバル コンフィギュレーション モードで **snmp-server group** コマンドを使用します。指定した SNMP 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。

snmp-server group *group-name* {**v1** | **v2c** | **v3** } [**access** [**ipv6** *named-access-list*] [{*acl-numberacl-name*}]] [**context** *context-name*] [**notify** *notify-view*] [**read** *read-view*] [**write** *write-view*]
no snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*]

構文の説明

group-name	グループの名前。
v1	グループが SNMPv1 セキュリティ モデルを使用していることを指定します。SNMPv1 は、最も安全性の低い SNMP セキュリティ モデルです。
v2c	グループが SNMPv2c セキュリティ モデルを使用していることを指定します。 SNMPv2c セキュリティ モデルでは、インフォームを送信でき、64 文字の文字列がサポートされています。
v3	グループが SNMPv3 セキュリティ モデルを使用していることを指定します。 SMNPv3 は、サポートされているセキュリティ モデルの中で最も安全です。SMNPv3 では、認証特性を明示的に設定できます。
context	（任意）この SNMP グループとそのビューと関連付ける SNMP コンテキストを指定します。
context-name	（任意）コンテキスト名。
read	（任意）SNMP グループの読み取りビューを指定します。このビューでは、エージェントのコンテンツのみを表示できます。
read-view	（任意）ビューの名前である最大 64 文字の文字列。 デフォルトでは、**read** オプションを使用してこの状態を上書きしない限り、読み取りビューはインターネットオブジェクト識別子（OID）のスペース（1.3.6.1）に属するすべてのオブジェクトであるとみなされます。
write	（任意）SNMP グループの書き込みビューを指定します。このビューでは、データを入力してエージェントのコンテンツを設定できます。
write-view	（任意）ビューの名前である最大 64 文字の文字列。 デフォルトでは、書き込みビュー（つまり、ヌル OID）には何も定義されていません。書き込みアクセスを設定する必要があります。

notify	（任意）SNMP グループの通知ビューを指定します。このビューでは、通知、インフォーム、またはトラップを指定できます。
notify-view	（任意）ビューの名前である最大 64 文字の文字列。 デフォルトでは、**snmp-server host** コマンドが設定されるまで、通知ビュー（つまり、ヌル OID）には何も定義されていません。ビューを **snmp-server group** コマンドで指定した場合、生成されるそのビューのすべての通知は、グループに関連付けられているすべてのユーザに送信されます（そのユーザに対して SNMP サーバホストの設定が存在する場合）。 シスコでは、ソフトウェアに通知ビューを自動生成させることを推奨しています。このドキュメントの「通知ビューの設定」の項を参照してください。
access	（任意）グループに関連付ける標準アクセス コントロール リスト（ACL）を指定します。
ipv6	（任意）IPv6 名前付きアクセス リストを指定します。IPv6 と IPv4 の両方のアクセス リストが示されている場合は、IPv6 名前付きアクセス リストがリストの最初に表示されている必要があります。
named-access-list	（任意）IPv6 アクセス リストの名前。
acl-number	（任意）*acl-number* 引数は、以前に設定された標準アクセス リストを識別する 1 ～ 99 の整数です。
acl-name	（任意）*acl-name* 引数は、以前に設定された標準アクセス リストの名前である最大 64 文字の文字列です。

コマンド デフォルト

SNMP サーバ グループ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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1s	このコマンドは、Cisco IOS XE Amsterdam 17.1.1s 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

コミュニティ ストリングが内部的に設定されている場合、public という名前の 2 つのグループが自動生成されます。1 つは v1 セキュリティ モデル用、もう 1 つは v2c セキュリティ モデル用です。同様に、コミュニティ ストリングを削除すると、public という名前の v1 グループと public という名前の v2c グループが削除されます。

snmp-server group コマンドを設定する際、認証やプライバシーアルゴリズムにはデフォルト値はありません。また、デフォルトのパスワードも存在しません。Message Digest 5（MD5）パスワードの指定については、**snmp-server user** コマンドのドキュメントを参照してください。

通知ビューの設定

notify view オプションは、2 つの目的に使用できます。

- グループに SNMP を使用して設定された通知ビューがあり、その通知ビューを変更する必要がある。
- **snmp-server host** コマンドは、**snmp-server group** コマンドの前に設定されている可能性があります。この場合、**snmp-server host** コマンドを再設定するか、または適切な通知ビューを指定する必要があります。

次の理由から、SNMP グループを設定する際に通知ビューを指定することは推奨されていません。

- **snmp-server host** コマンドによってユーザに対して自動生成された通知ビューを、そのユーザに関連付けられているグループに追加する。
- グループの通知ビューを変更すると、そのグループに対応付けられたすべてのユーザが影響を受けます。

snmp-server group コマンドの一部としてグループの通知ビューを指定する代わりに、指定された順序で次のコマンドを使用します。

1. **snmp-server user** ：SNMP ユーザーを設定します。
2. **snmp-server group** ：通知ビューを追加しないで SNMP グループを設定します。
3. **snmp-server host** ：トラップ操作の受信者を指定して、通知ビューを自動生成します。

SNMP コンテキスト

SNMP コンテキストによって、MIB データにアクセスする安全な方法が VPN ユーザに提供されます。VPN がコンテキストに関連付けられると、VPN 固有の MIB データがそのコンテキストに存在します。VPN をコンテキストに関連付けると、サービス プロバイダーが、複数 VPN でネットワークを管理できます。コンテキストを作成して VPN に関連付けることにより、サービス プロバイダーは、ある VPN のユーザが同じネットワーキング デバイス上で他の VPN のユーザに関する情報にアクセスするのを防ぐことができます。

読み取り、書き込み、または通知 SNMP ビューを SNMP コンテキストに関連付けるには、**context** *context-name* キーワードおよび引数とともにこのコマンドを使用します。

SNMP グループの作成

次の例は、SNMP サーバグループ「public」を作成して、すべてのオブジェクトに対して標準名前付きアクセスリスト「lmnop」のメンバへの読み取り専用アクセスを許可する方法を示しています。

```
Device(config)# snmp-server group public v2c access lmnop
```

SNMP サーバグループの削除

次の例に、設定から SNMP サーバグループ「public」を削除する方法を示します。

```
Device(config)# no snmp-server group public v2c
```

SNMP サバ グループと指定されたビューとの関連付け

次の例に、SNMPv2c グループ「GROUP1」のビューに関連付けられた SNMP コンテキスト「A」を示します。

```
Device(config)# snmp-server context A
Device(config)# snmp mib community commA
Device(config)# snmp mib community-map commA context A target-list commAVpn
Device(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify
viewB
```

snmp-server subagent cache

Simple Network Management Protocol（SNMP）ポーリング中にコントローラで CPU スパイクが発生しないようにするには、**snmp-server subagent cache** コマンドを使用します。サブエージェントキャッシュを無効にするには、このコマンドの **no** 形式を使用します。

snmp-server subagent cache [**timeout** *seconds*]

snmp-server subagent cache [**timeout** *seconds*]

構文の説明

timeout	サブエージェントキャッシュのタイムアウトを指定します。
seconds	サーバーのタイムアウト値（秒単位）。有効な値の範囲は 1 ～ 100 で、デフォルトは 60 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 Dublin 17.11.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、定期的にキャッシュをクリアすることで、コントローラの CPU スパイクを防止します。

例

次に、SNMP ポーリング中にコントローラで CPU スパイクが発生しないようにする例を示します。

```
Device# configure terminal
Device(config)# snmp-server subagent cache
```

software auto-upgrade enable

自動アップグレード機能を有効にするには、**software auto-upgrade enable** コマンドを使用します。

（注） このコマンドの **no** 形式を使用してこの機能を無効にした場合は、特権 EXEC モードで **install autoupgrade** コマンドを使用して、手動で自動アップグレードする必要があります。

software auto-upgrade enable

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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

使用上のガイドライン

次に、自動アップグレード機能を有効にする例を示します。

```
Device# configure terminal
Device(config)# software auto-upgrade enable
Device(config)# end
```

source-interface

コントローラと通信するように送信元インターフェイスを設定するには、**source-interface** コマンドを使用します。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。

source-interface *interface-name interface-number*

no source-interface

構文の説明

interface-name	インターフェイスの名前。
interface-number	インターフェイス番号。

コマンド デフォルト

送信元インターフェイスは設定されていません。

コマンド モード

SD サービス コントローラ コンフィギュレーション（config-sd-service-controller）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが導入されました。

例

次に、コントローラと通信するように送信元インターフェイスを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# avc sd-service
Device(config-sd-service)# controller
Device(config-sd-service-controller)# source-interface vlan 12
```

static-ip-mobility

静的 IP モビリティを設定するには、ワイヤレスポリシー コンフィギュレーション モードで **static-ip-mobility** コマンドを使用します。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。

static-ip-mobility

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

ワイヤレスポリシー 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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、静的 IP モビリティを有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless profile policy test-policy
Device(config-wireless-policy)# static-ip-mobility
```

statistics ap-system-monitoring alarm-enable

AP のリアルタイム統計（CPU とメモリ）のアラームを有効にするには、**statistics ap-system-monitoring alarm-enable** コマンドを使用します。この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。

[no] statistics ap-system-monitoring alarm-enable

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring alarm-enable	AP のリアルタイム統計（CPU とメモリ）のアラームを有効にします。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、AP のリアルタイム統計（CPU とメモリ）のアラームを有効にする例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring alarm-enable
```

statistics ap-system-monitoring alarm-hold-time

アラームをトリガーするまでの保留時間間隔を定義するには、**statistics ap-system-monitoring alarm-hold-time** コマンドを使用します。

statistics ap-system-monitoring alarm-hold-time *0-3600*

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring alarm-hold-time	APのリアルタイム統計（CPUとメモリ）のアラームを有効にします。
0-3600	アラーム保留時間間隔を秒単位で指定します。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、アラームをトリガーするまでの保留時間間隔を定義する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring alarm-hold-time 60
```

statistics ap-system-monitoring alarm-retransmit-time

トラップアラームの再送信間隔を定義するには、**statistics ap-system-monitoring alarm-retransmit-time** を使用します

statistics ap-system-monitoring alarm-retransmit-time *0-65535*

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring alarm-retransmit-time	トラップアラームの再送信間隔を定義します。
0-65535	トラップアラームの再送信間隔（秒単位）を指定します。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、トラップアラームの再送信間隔を定義する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring alarm-retransmit-time 60
```

statistics ap-system-monitoring cpu-threshold

アラームをトリガーする、AP の CPU 使用量のしきい値パーセンテージを定義するには、**statistics ap-system-monitoring cpu-threshold** コマンドを使用します。

statistics ap-system-monitoring cpu-threshold *0-100*

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring cpu-threshold	アラームをトリガーする AP の CPU 使用量のしきい値を定義します。
0-100	アラームをトリガーする AP の CPU 使用量のしきい値のパーセンテージを指定します。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、アラームをトリガーする AP の CPU 使用量のしきい値パーセンテージを定義する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring cpu-threshold 70
```

statistics ap-system-monitoring enable

AP のリアルタイム統計（CPU とメモリ）のモニタリングを有効にするには、**statistics ap-system-monitoring enable** コマンドを使用します。この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。

[no] statistics ap-system-monitoring enable

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring enable	AP のリアルタイム統計（CPU とメモリ）のモニタリングを有効にします。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、AP のリアルタイム統計（CPU とメモリ）のモニタリングを有効にする例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring enable
```

statistics ap-system-monitoring mem-threshold

アラームをトリガーする AP のメモリ使用量のしきい値パーセンテージを定義します。

statistics ap-system-monitoring mem-threshold *0-100*

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring mem-threshold	アラームをトリガーする AP のメモリ使用量のしきい値を定義します。
0-100	アラームをトリガーするAPのメモリ使用量のしきい値のパーセンテージを指定します。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、アラームをトリガーする AP のメモリ使用量のしきい値パーセンテージを定義する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring mem-threshold 60
```

statistics ap-system-monitoring sampling-interval

サンプリング間隔を定義するには、**statistics ap-system-monitoring sampling-interval** を使用します

statistics ap-system-monitoring sampling-interval *2-900*

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring sampling-interval	サンプリング間隔を定義します。
2-900	サンプリング間隔を秒単位で指定します。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、サンプリング間隔を定義する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring sampling-interval 100
```

statistics ap-system-monitoring stats-interval

統計間隔を定義するには、**statistics ap-system-monitoring stats-interval** を使用します。これにより、計算において、最後の統計間隔秒間に受信した統計に、より多くの重みが与えられます

statistics ap-system-monitoring stats-interval *120-900*

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring stats-interval	統計間隔を定義します。これにより、計算において、最後の統計間隔秒間に受信した統計に、より多くの重みが与えられます。
120-900	統計間隔を秒単位で指定します。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、統計間隔を定義する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring stats-interval 120
```

stopbits

コンソール ポートのストップ ビットを設定するには、**stopbits** 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。

stopbits { *1* | *2* }

no stopbits { *1* | *2* }

構文の説明

1	1 ストップ ビットを指定します。
2	2 ストップ ビットを指定します。

コマンド デフォルト

1 ストップ ビット

コマンド モード

ライン 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

コンソール ポートは、コンソール ポート上のセッションからのみ設定できます。

例

次に、コンソールポートのストップビットを設定する例を示します。

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# stopbits 1
```

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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 devices 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** コマンドおよび **switchport mode** コマンドを入力します。

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できません。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。

```
デバイス(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。

```
デバイス(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。device 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*}
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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス(config-if)# switchport access vlan 2
```

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 devices 間、または device 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

（注） **dot1q-tunnel** キーワードは、CLI のインターフェイス ヘルプに表示されますが、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。

```
デバイス(config)# interface gigabitethernet2/0/1
デバイス(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。

```
デバイス(config)# interface gigabitethernet2/0/1
デバイス(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。

```
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# switchport mode trunk
```

tag rf

AP フィルタのポリシー タグを設定するには、**tag rf** コマンドを使用します。

tag rf *rf-tag*

構文の説明

rf-tag	RF タグ名。

コマンド デフォルト

なし

コマンド モード

config-ap-filter

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP フィルタのポリシー タグを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name ap-filter-name
Device(config-ap-filter)# rf tag rf-tag-name
```

tag site

AP フィルタのサイト タグを設定するには、**tag site** *site-tag* コマンドを使用します。

tag site *site-tag*

構文の説明		
	site-tag	サイト タグの名前。

コマンド デフォルト

なし

コマンド モード

config-ap-filter

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP フィルタのサイト タグを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name ap-filter-name
Device(config-ap-filter)# site tag site-tag-name
```

terms-conditions

Access Network Query Protocol（ANQP）サーバーの利用規約パラメータを設定するには、**terms-conditions** コマンドを使用します。利用規約を無効にするには、このコマンドの **no** 形式を使用します。

terms-conditions {**filename** *filename* | **timestamp** *date time* | **urlfilter list** *url-filter-list*}

構文の説明

filename	利用規約ファイルの名前。
date	yyyy-mm-dd形式のタイムスタンプ日付。
time	hh:mm:ss 形式のタイムスタンプ時刻。
url-filter-list	URL フィルタリストの名前。

コマンド デフォルト

利用規約は設定されていません。

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、タイムスタンプを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# terms-conditions timestamp 2020-02-20 20:20:20
```

tertiary (ap prime)

AP フォールバック用のターシャリコントローラを設定するには、**tertiary** コマンドを使用します。AP プライミングに使用されないようにターシャリコントローラを削除するには、このコマンドの **no** 形式を使用します。

tertiary *controller-name ip-address*

no tertiary *controller-name ip-address*

構文の説明

controller-name	ターシャリコントローラの名前。
ip-address	コントローラの IPv4 または IPv6 アドレス。

コマンド デフォルト

なし

コマンド モード

AP プライム コンフィギュレーション（config-priming）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.2	このコマンドが導入されました。

例

次に、AP フォールバック用のターシャリコントローラを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile ap priming Prime-FX
Device(config-priming)# tertiary cccc 209.165.201.4
```

timezone delta

AP のタイムゾーンオフセットを設定するには、**timezone delta** コマンドを使用します。AP のタイムゾーンオフセットを削除するには、**no timezone** コマンドを使用します。

timezone delta hour *offset-hour* **minute** *offset-minute*

構文の説明

hour *offset-hour*	協定世界時（UTC）からのローカル時間の差。有効な範囲は -12 ～ 14 です。
minute *offset-minute*	UTC からのローカル分の差。有効な範囲は 0 ～ 59 です。

コマンド デフォルト

AP のタイムゾーンは設定されていません。

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

使用上のガイドライン

AP タイムゾーンは、AP プロファイルごとにのみ設定できます。AP ごとに AP タイムゾーンを設定することはできません。タイムゾーンを設定するには、現在のコントローラのタイムゾーンまたは時差を適用します。デフォルトでは、タイムゾーンは無効になっています。

例

次に、AP のタイムゾーンオフセットを設定する例を示します。

```
Device# configure terminal
Device(config)# ap profile test
Device(config-ap-profile)# timezone delta hour -12 minute 2
```

timezone use-controller

コントローラのタイムゾーンを使用して AP のタイムゾーンを設定するには、**timezone use-controller** コマンドを使用します。コントローラのタイムゾーンを削除するには、**no timezone** コマンドを使用します。

timezone use-controller

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

AP のタイムゾーンは設定されていません。

コマンド モード

AP プロファイル コンフィギュレーション（config-ap-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

使用上のガイドライン

AP タイムゾーンは、AP プロファイルごとにのみ設定できます。AP ごとにタイムゾーンを設定することはできません。タイムゾーンを設定するには、現在のコントローラのタイムゾーンを適用するか、時差を使用します。デフォルトでは、タイムゾーンは無効になっています。

例

次に、コントローラのタイムゾーンを使用して AP のタイムゾーンを設定する例を示します。

```
Device# configure terminal
Device(config)# ap profile test
Device(config-ap-profile)# timezone use-controller
```

transport application-updates

コントローラと通信するためのトランスポートプロトコルを設定するには、**transport** コマンドを使用します。コントローラと通信するために使用するトランスポートプロトコ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。

transport application-updates { **http** | **https** } **url-prefix** *url-prefix-name*

no transport application-updates

構文の説明

http	HTTP プロトコルを有効にします。
https	HTTPS プロトコルを有効にします。
url-prefix	アプリケーション更新のURLプレフィックスを有効にします。
url-prefix-name	URL プレフィックス名。

コマンド デフォルト

トランスポート通信プロトコルは設定されていません。

コマンド モード

SD サービス コントローラ コンフィギュレーション（config-sd-service-controller）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが導入されました。

使用上のガイドライン

アプリケーション更新のトランスポートプロトコルは、Cisco DNA Center でのみ使用されます。

例

次に、コントローラと通信するためのトランスポートプロトコルを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# avc sd-service
Device(config-sd-service)# controller
Device(config-sd-service-controller)# transport application-updates https url-prefix
cisco
```

transition-disable

移行の無効化を有効にするには、**transition-disable** コマンドを使用します。

transition-disable

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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが導入されました。

使用上のガイドライン

次に、移行の無効化を有効にする例を示します。

```
Device# configure terminal
Device(config)# wlan WPA3 1 WPA3
Device(config-wlan)# transition-disable
Device(config-wlan)# end
```

trapflags ap ap-stats

統計がしきい値を超えたときに送信される AP 関連のトラップの送信を有効または無効にするには、**trapflags ap ap-stats** を使用します。この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。

[no] trapflags ap ap-stats

構文の説明

trapflags	AP 関連のトラップフラグの送信を有効または無効にします。
ap ap-stats	統計がしきい値を超えたときに送信されるトラップを指定します。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、AP 関連のトラップの送信を有効または無効にする例を示します。

```
Device# configure terminal
Device(config)# trapflags ap ap-stats
```

trapflags ap broken-antenna

サポートされているCiscoアクセスポイントでアンテナ障害が発生したときに送信されるSNMPトラップを有効にするには、**trapflags ap broken-antenna** コマンドを使用します。SNMP トラッ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。

trapflags ap broken-antenna

no trapflags ap broken-antenna

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

SNMP トラップは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 Bengaluru 17.4.1	このコマンドが導入されました。

使用上のガイドライン

アンテナは、A、B、C、D、E、F、G、H などの文字でコード化されます。Inter-Access Point Protocol（IAPP）レポートに故障したアンテナの文字が含まれていて、syslog と SNMP トラップにコピーされます。

例

次に、故障したアンテナの SNMP トラップを有効にする例を示します。

```
Device# configure terminal
Device(config)# trapflags ap broken-antenna
```

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 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 **trusted-port** コマンドを使用します。この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。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス(config)# ipv6  nd inspection  policy1
デバイス(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。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)# trusted-port
```

tunnel eogre source

トンネル送信元について特定のトンネル単位の設定が存在しない場合にトンネル送信元インターフェイスを設定するには、**tunnel eogre source** コマンドを使用します。

tunnel eogre source {**gigabitethernet** | **loopback** | **vlan**} *interface-number*

構文の説明

interface-number	インターフェイス番号。

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 Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

トンネル送信元について特定のトンネル単位の設定が存在する場合は、それが使用されます。

例

次に、トンネル送信元インターフェイスを設定する例を示します。

```
Device(config)# tunnel eogre source vlan 21
```

tunnel eogre heartbeat

トンネル キープアライブ ハートビートの ping パラメータを設定するには、**tunnel eogre heartbeat** コマンドを使用します。

tunnel eogre heartbeat {**interval** *interval* | **max-skip-count** *tolerable-heartbeats*}

構文の説明

interval	ハートビート間隔（秒）。
tolerable-heartbeats	許容されるドロップされたハートビート。

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、トンネル キープアライブ ハートビートの ping パラメータを設定する例を示します。

```
Device(config)# tunnel eogre heartbeat 80
```

tunnel mode ethernet

トンネルのカプセル化方式を Ethernet over GRE に設定するには、**tunnel mode ethernet** コマンドを使用します。

tunnel mode ethernet {**gre** {**ipv4** | **ipv6**} [**p2p**] | **manual**}

構文の説明

gre	Ethernet over GRE。
l2tpv3	L2TPv3 カプセル化。
p2p	IPv4 または IPv6 を介したポイントツーポイント カプセル化を提供します。
manual	L2TP パラメータを手動で設定します。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。
Cisco IOS XE Gibraltar 16.11.1	**p2p** キーワードが導入されました。

例

次に、トンネルのカプセル化方式を Ethernet over GRE に設定する例を示します。

```
Device(config-if)# tunnel mode ethernet gre ipv4 p2p
```

tunnel eogre domain

EoGRE 冗長ドメインを設定するには、**tunnel eogre domain** コマンドを使用します。

tunnel eogre domain *domain-name*

構文の説明

domain-name	ドメイン名。

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、EoGRE 冗長ドメインを設定する例を示します。

```
Device(config)# tunnel eogre domain domain1
```

tunnel eogre interface tunnel

EoGRE トンネル インターフェイスの AAA プロキシ キーを設定するには、**tunnel eogre interface tunnel** コマンドを使用します。

tunnel eogre interface tunnel *tunnel-inft-number* **aaa proxy key** {**0** | **8**} *key-string* **auth-port** *auth_port* **acct-port** *acct_port*

構文の説明

tunnel-inft-number	トンネル インターフェイスの番号。
aaa	AAA の設定
proxy	AAA プロキシの設定。
key	AAA プロキシ キーの設定。 0：文字列を暗号化されていないキーとして指定します。 8：文字列を AES 暗号化キーとして指定します。
key-string	キーの文字列。
auth-port *auth_port*	認証ポート番号。
acct-port *acct_port*	アカウンティング用のポート番号。

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 Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.1	このコマンドが変更されました。次のキーワードと変数が追加されました。 **auth-port***auth_port* **acct-port***acct_port*

例

次に、EoGRE トンネル インターフェイスのプロキシ キーを設定する例を示します。

```
Device(config)# tunnel eogre interface tunnel 21 aaa proxy key 0 test
```

次に、AAA ポートを変更する例を示します。

```
Device(config)# tunnel eogre interface Tunnel1 aaa proxy key 0 test
 auth-port 24 acct-port 36
```

tunneled-eap-credential

トンネル化 Extensible Authentication Protocol（EAP）クレデンシャル認証を設定するには、**tunneled-eap-credential** コマンドを使用します。トンネル化 EAP クレデンシャル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。

tunneled-eap-credential {**anonymous** | **certificate** | **hw-token** | **nfc** | **sim** | **softoken** | **username-password** | **usim**}

構文の説明

anonymous	匿名認証。
certificate	証明書を使用する認証。
hw-token	ハードウェアトークンを使用する認証。
nfc	近距離無線通信（NFC）を使用する認証。
sim	SIM カードを使用する認証。
softoken	ソフトトークンを使用する認証。
username-password	ユーザー名とパスワードを使用する認証。
usim	USIM を使用する認証。

コマンド デフォルト

なし

コマンド モード

ANQP NAI EAP 認証（config-anqp-nai-eap-aut）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、トンネル化 EAP クレデンシャル認証を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless hotspot anqp-server my_anqp
Device(config-wireless-anqp-server)# nai-realm myvenue.cisco.com
Device(config-anqp-nai-eap)# eap-method eap-aka
Device(config-anqp-nai-eap-auth)# tunneled-eap-credential anonymous
```

type

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 **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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス: 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:
```

udp-timeout

UDP セッションのタイムアウトを設定するには、**udp-timeout** コマンドを使用します。

udp-timeout *timeout_value*

構文の説明

timeout_value	UDP セッションのタイムアウト値です。 範囲は 1 ～ 30 秒です。 （注） *public-key* および *resolver* パラメータマップ オプションには、デフォルト値が自動的に入力されます。したがって、変更する必要はありません。

コマンド デフォルト

なし

コマンド モード

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、UDP セッションのタイムアウト値を設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# parameter-map type umbrella global
デバイス(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166
デバイス(config-profile)# local-domain dns_wl
デバイス(config-profile)# udp-timeout 2
デバイス(config-profile)# end
```

umbrella-param-map

WLAN の Umbrella OpenDNS 機能を設定するには、**umbrella-param-map** コマンドを使用します。

umbrella-param-map *umbrella-name*

構文の説明

umbrella-name

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、WLAN の Umbrella OpenDNS 機能を設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless profile policy default-policy-profile
デバイス(config-wireless-policy)# umbrella-param-map global
デバイス(config-wireless-policy)# end
```

update-timer

Flex プロファイルの mDNS 更新タイマーを設定するには、**update-timer** コマンドを使用します。このコマン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。

update-timer { **service-cache** *<1-100>* | **statistics** *<1-100>* }

update-timer { **service-cache** *<1-100>* | **statistics** *<1-100>* }

構文の説明

update-timer	Flex プロファイルの mDNS 更新タイマーを設定します。
service-cache *<1-100>*	Flex プロファイルの mDNS 更新のサービスキャッシュタイマーを指定します。デフォルト値は 1 分です。
statistics *<1-100>*	Flex プロファイルの mDNS 更新の統計タイマーを指定します。デフォルト値は 1 分です。

コマンド デフォルト

なし

コマンド モード

mDNS Flex 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 Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、Flex プロファイルの mDNS 更新タイマーを設定する例を示します。

```
Device(config-mdns-flex-prof)# update-timer service-cache 20
```

url

Hotspot 2.0 の施設の URL を設定するには、**url** コマンドを使用します。Hotspot 2.0 の施設の URL を削除するには、このコマンドの **no** 形式を使用します。

url *url*

構文の説明

url	施設名の URL。

コマンド デフォルト

施設の URL は設定されていません。

コマンド モード

ワイヤレス ANQP 施設コンフィギュレーション（config-anqp-venue-name）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、Hotspot 2.0 の施設の URL を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# venue test eng
Device(config-anqp-venue-name)#url www.cisco.com
```

username

SSH を使用して Cisco ISE-3315 にアクセスできるユーザを追加するには、コンフィギュレーション モードで **username** コマンドを使用します。ユーザがすでに存在する場合は、このコマンドを使用してパスワード、特権レベル、または両方を変更します。システムからユーザを削除するには、このコマンドの **no** 形式を使用します。

[no] username *username* **password** {**hash** | **plain**} *password* **role** {**admin** | **user**] [**disabled** [**email** email-address]] [**email** email-address]

既存のユーザに対しては、以下のコマンド オプションを使用します。

username username **password role** {admin | **user**} password

構文の説明

username	1 つの単語のみを入力する必要があります。ハイフン（-）、アンダースコア（_）、およびピリオド（.）を含めることができます。 （注） 初期セットアップでは英数字のみが許可されます。
password	パスワードおよびユーザ ロールを指定するために使用するコマンド。
password	パスワード。40 文字までの英数字で指定します。パスワードは、すべての新規ユーザに指定する必要があります。
hash | plain	パスワードのタイプ。最大 34 文字の英数字。
role admin | user	ユーザの権限レベルを設定します。
[disabled]	ユーザの電子メール アドレスに従って、ユーザをディセーブルにします。
email *email-address*	ユーザのメール アドレス。たとえば、user1@example.com です。
wlan-profile-name	WLAN プロファイルの詳細を表示します。

コマンド デフォルト

設定時の初期ユーザです。

コマンド モード

コンフィギュレーション

使用上のガイドライン

username コマンドでは、username および password キーワードの後に、hash | plain and the admin | user オプションを指定する必要があります。

例 1

```
ncs/admin(config)# username admin password hash ###### role admin
ncs/admin(config)#
```

例 2

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin
ncs/admin(config)#
```

例 3

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin email
admin123@example.com
ncs/admin(config)#
```

venue

802.11u 施設情報を設定するには、**venue** コマンドを使用します。施設を削除するには、このコマンドの **no** 形式を使用します。

venue *venue-name language-code*［*venue-url*］

構文の説明

venue-name	施設の名前。 220 文字を超えないようにする必要があります。
language-code	オペレータの 3 文字の言語コード。言語コードには、言語の最初の 3 文字のみを小文字で使用します。たとえば、英語の場合は *eng* を使用します。 言語コードの完全なリストについては、http://www.loc.gov/standards/iso639-2/php/code_list.php を参照してください。
venue-url	施設の URL。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、802.11u 施設情報を設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# venue test eng cisco.com
```

vnid

サービス テンプレートに VXLAN ネットワーク ID（VNID）を追加するには、 **vnid** コマンドを使用します。

vnid *vnid-name*

構文の説明

vnid-name	VNID の名前。

コマンド デフォルト

VNID は設定されていません。

コマンド モード

サービス テンプレート コンフィギュレーション（config-service-template）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、VNID を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# service-template template
Device(config-service-template)# vnid  vnid-name
```

violation

定期的な再評価でのストリーム違反ポリシーを設定するには、**violation** コマンドを使用します。

violation {**drop** | **fallback**}

構文の説明

パラメータ	説明
drop	ストリームが定期的な再評価でドロップされます。
fallback	ストリームが定期的な再評価でBestEffortクラスに降格されます。

コマンド デフォルト

なし

コマンド モード

config-media-stream

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、定期的な再評価でのストリーム違反ポリシーを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# violation drop
```

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* | **accounting** { **input** | **output** } | **configuration** *vlan-id* | **group** *word* **vlan-list** *vlan-id* | **internal allocation policy** { **ascending** | **descending** } }
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。
accounting	VLAN アカウンティング設定。
configuration	詳細なサービスパラメータの VLAN 機能コンフィギュレーション モード。同じ設定に対して 1 つ以上の VLAN を作成できます。*id* は VLAN 設定 ID を示しています。たとえば、1-10 や 15 などです。
internal	内部VLAN割り当てポリシー。昇順または降順にすることができます。

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、VLAN を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# vlan 12
```

vlan configuration

VLAN 機能を設定するため VLAN コンフィギュレーション モードを開始するには、**vlan configuration** コマンドを使用します。

vlan configuration

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、VLAN ID が 2 の場合に、VLAN 機能を設定するために 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。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# vlan configuration 2
```

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 スイッチ上で、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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス(config)# vlan access-map vac1
デバイス(config-access-map)# match ip address acl1
デバイス(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。

```
デバイス(config)# no vlan access-map vac1
```

vlan encryption osen

アソシエーションおよび認証プロセス中に単一の SSID で Online Subscription with Encryption（OSEN）暗号化を選択するときにクライアントが使用する VLAN を指定するには、**vlan encryption osen** 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-id *vlan-id* **encryption osen**

構文の説明

vlan-id	VLAN 識別番号。

コマンド デフォルト

VLAN ID は設定されていません。

コマンド モード

ワイヤレス ポリシーの設定（config-wireless-policy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、アソシエーションおよび認証プロセス中に単一の SSID で OSEN 暗号化を選択するときにクライアントが使用する VLAN を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy rr-xyz-policy-1
Device(config-wireless-policy)# vlan 10 encryption osen
```

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** {*list* | **all**}
no vlan filter *mapname* **vlan-list** {*list* | **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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス(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。

```
デバイス(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。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス(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。

```
デバイス(config)# no vlan group group1 vlan-list 7
```

vlan-id

FlexConnectプロファイルVLANIDを設定するには、**vlan-id**コマンドを使用します。FlexConnectプロファイル 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-id *vlan-id*

構文の説明

vlan-id	VLAN 識別番号。

コマンド デフォルト

VLAN ID は設定されていません。

コマンド モード

ワイヤレス Flex プロファイル VLAN コンフィギュレーション（config-wireless-flex-profile-vlan）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、Flex プロファイル VLAN ID を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# vlan-name test
Device(config-wireless-flex-profile-vlan)#vlan-id 12
```

vlan-name

FlexConnectプロファイルVLANを設定するには、**vlan-name** コマンドを使用します。FlexConnectプロファイル 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-name

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

VLAN は設定されていません。

コマンド モード

ワイヤレス Flex プロファイル コンフィギュレーション（config-wireless-flex-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、FlexConnect プロファイル VLAN を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# vlan-name test
```

vrf

仮想ルーティングおよび転送（VRF）ラベルを有効にするには、**vrf** コマンドを使用します。VRF ラベルを削除するには、このコマンドの **no** 形式を使用します。

vrf *vrf-name*

no vrf

構文の説明

vrf-name	VRF の名前。

コマンド デフォルト

VRF ラベルは有効になっていません。

コマンド モード

SD サービス コントローラ コンフィギュレーション（config-sd-service-controller）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが導入されました。

例

次に、VRF ラベルを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# avc sd-service
Device(config-sd-service)# controller
Device(config-sd-service-controller)# vrf doc-test
```

wan-metrics

Hotspot 2.0 WAN メトリックを設定するには、**wan-metrics** コマンドを使用します。WAN を削除するには、このコマンドの **no** 形式を使用します。

wan-metrics
{**downlink-load**|**downlink-speed**|**full-capacity-link**|**link-status**{**down**|**not-configured**|**test-state**|**up**}|**load-measurement-duration**|**uplink-load**|**uplink-speed**}

構文の説明

downlink-load	WAN ダウンリンク負荷を設定します。有効な範囲は 0 ～ 255 です。値は線形的にスケーリングされ、255 が 100% を表します。
downlink-speed	WAN のダウンリンク速度（kbps 単位）を設定します。有効な範囲は 0 ～ 4294967295 です。
full-capacity-link	WAN リンクを最大容量で運用します。
link-status	WAN リンクステータスを設定します。 次のオプションがあります。 • **down**：リンク ダウン • **not-configured**：リンクが設定されていません。 • **test-state**：リンクはテスト状態です。 • **up**：リンクがアップしています。
load-measurement-duration	アップリンクまたはダウンリンク負荷の測定期間を設定します。有効な範囲は 0 ～ 65535 です。
uplink-load	WAN アップリンク負荷を設定します。有効な範囲は 0 ～ 255 です。値は線形的にスケーリングされ、255 が 100% を表します。
uplink-speed	WAN のアップリンク速度（kbps 単位）を設定します。有効な範囲は 0 ～ 4294967295 です。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ANQP サーバ コンフィギュレーション（config-wireless-anqp-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、Hotspot 2.0 WAN アップリンク速度を設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# wan-metrics uplink-load 23
```

webauth-http-enable

グローバル パラメータ マップ パラメータ モードで Web 認証用の HTTP サーバーを有効にするには、**webauth-http-enable** を使用します。このコマン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。

webauth-http-enable

no webauth-http-enable

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

グローバル パラメータ マップ モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、Web 認証用の HTTP サーバーを有効にする例を示します。

```
Device(config-params-parameter-map)# webauth-http-enable
```

wgb broadcast-tagging

ワイヤレス ポリシー プロファイルで WGB ブロードキャスト タギングを設定するには、**wgb broadcast-tagging** コマンドを使用します。

wgb broadcast-tagging

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス ポリシー プロファイルで WGB ブロードキャスト タギングをイネーブルにする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy profile-policy-name
Device(config-wireless-policy)# wgb broadcast-tagging
```

wgb vlan

WLAN ポリシー プロファイルで WGB VLAN クライアントのサポートを設定するには、**wgb vlan** コマンドを使用します。

wgb vlan

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、*wlan1-policy-profile* という名前の WLAN ポリシー プロファイルで WGB VLAN クライアントのサポートを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy wlan1-policy-profile
Device(config-wireless-policy)# wgb vlan
```

whitelist acl

ホワイトリスト ACL を設定するには、**whitelist acl** コマンドを使用します。

whitelist acl {*standard_acl_value* | *extended_acl_value* | *acl_name*}

構文の説明

standard_acl_value	標準アクセス リストを指定します。範囲は 1 ～ 199 です。
extended_acl_value	拡張アクセス リストを指定します。範囲は1300 ～ 2699 です。
acl_name	名前付きアクセス リストを指定します。

コマンド デフォルト

なし

コマンド モード

ET-Analytics 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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、ET-Analytics コンフィギュレーション モードで非アクティブタイマーを有効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# et-analytics
デバイス(config-et-analytics)# whitelist acl
eta-whitelist
デバイス((config-et-analytics)# ip access-list
extended eta-whitelist
デバイス(config-ext-nacl)# permit udp any any eq tftp
デバイス(config-ext-nacl)# end
```

wired-vlan-range

mDNS サービス検出を実行する有線 VLAN を設定するには、**wired-vlan-range** コマンドを使用します。このコマン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。

wired-vlan-range *wired-vlan-range-value*

構文の説明

wired-vlan-range	mDNS サービス検出を実行する有線 VLAN を設定します。
wired-vlan-range-value	有線 VLAN の範囲値を指定します。

コマンド デフォルト

なし

コマンド モード

mDNS Flex 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 Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、mDNS サービス検出を実行する有線 VLAN を設定する例を示します。

```
Device(config-mdns-flex-prof)# wired-vlan-range range-value
```

config wlan assisted-roaming

WLAN で経由ローミングを設定するには、**config wlan assisted-roaming** コマンドを使用します。

config wlan assisted-roaming {**neighbor-list** | **dual-list** | **prediction**} {**enable** | **disable**} *wlan_id*

構文の説明

neighbor-list	WLAN の 802.11k ネイバー リストを設定します。
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。
prediction	WLAN の経由ローミング最適化の予測を設定します。
enable	WLAN の設定をイネーブルにします。
disable	WLAN の設定をディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

すべての WLAN で 802.11k ネイバー リストが有効です。

デフォルトでは、ネイバー リスト機能が WLAN に対してイネーブルな場合に、デュアル バンド リストはイネーブルになります。

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イネーブルにすると、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イネーブルになっている場合、ロードバランシングはその WLAN でディセーブルになります。

次に、WLAN の 802.11k ネイバー リストをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan assisted-roaming neighbor-list enable 1
```

wireless aaa policy

ワイヤレス AAA ポリシーを設定するには、**wireless aaa policy** コマンドを使用します。

wireless aaa policy *aaa-policy*

構文の説明

aaa-policy	ワイヤレスAAA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

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、*aaa-policy-test* という名前のワイヤレス AAA ポリシーを設定する例を示します

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy aaa-policy-test
```

wireless aaa policy

新しい AAA ポリシーを設定するには、**wireless aaa policy** コマンドを使用します。

wireless aaa policy *aaa-policy-name*

構文の説明

aaa-policy-name	AAA ポリシー名。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AAA ポリシー名を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy my-aaa-policy
```

wireless autoqos policy-profile

実行可能なコマンドを使用して AutoQoS ワイヤレスポリシーを有効にするには、**autoqos** コマンドを使用します。ワイヤレス AutoQos を無効にするには、**disable** コマンドを使用します。

wireless autoqos policy-profile*policy-profile-name* **default_policy_profile mode** { **clear** | **enterprise-avc** | **fastlane** | **guest** | **voice** }

wireless autoqos disable

構文の説明

autoqos	ワイヤレス AutoQoS を設定します。
mode	ワイヤレス AutoQoS モードを指定します。
enterprise-avc	AutoQos ワイヤレス企業 AVC ポリシーを有効にします。
clear	設定されているワイヤレスポリシーをクリアします。
fastlane	AutoQos fastlane ポリシーを有効にします。これにより、2.4GHz または 5GHz の 802.11 ネットワークが無効化および有効化されます。
guest	AutoQos ワイヤレスゲストポリシーを有効にします。
voice	AutoQos ワイヤレス音声ポリシーを有効にします。これにより、2.4GHz または 5GHz の 802.11 ネットワークが無効化および有効化されます。

コマンド デフォルト

なし

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.2s	このコマンドが導入されました。

例

次に、AutoQoS ワイヤレス企業ポリシーを有効にする例を示します。

```
Device# wireless autoqos policy-profile default-policy-profile mode enterprise-avc
```

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 Gibraltar 16.10.1	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、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。

```
デバイス(config)# wireless broadcast vlan 20
```

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**wireless client** コマンドを使用します。

wireless client {**association limit** *assoc-number* **interval** *interval* | **band-select** {**client-mid-rssi** *rssi* | **client-rssi** *rssi* | **cycle-count** *count* | **cycle-threshold** *threshold* | **expire dual-band** *timeout* | **expire suppression** *timeout*} | **fast-ssid-change** | **max-user-login** *max-user-login* | **notification** {**interval** *time* | **join-failure aaathreshold***percentage* | **roam-failure threshold** *percentage*} | **timers auth-timeout** *seconds* | **user-timeout** *user-timeout*}

構文の説明

association limit *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-mid-rssi *rssi*	バンド選択のクライアント Mid-RSSI のしきい値を設定します。 プローブに応答するためのクライアント RSSI の最小 dBm は、-90 ～ -20 です。
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。 プローブに応答するためのクライアント RSSI の最小 dBm は、-90 ～ -20 です。
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。
expire dual-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。

expire suppression *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。
fast-ssid-change	モバイル端末で高速 SSID の変更を有効にします。
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。
notification	通知を設定します。
interval *time*	インターバルの通知を設定します。 有効な時間は 1 ～ 1440 秒です。
join-failure aaa threshold *percentage*	クライアントの参加の失敗に関する通知を設定します。 アラートをトリガーするしきい値をパーセンテージで設定できます。有効なしきい値のパーセンテージは 1 ～ 100 です。
roam-failure threshold *percentage*	クライアントのローミング障害に関する通知を設定します。 通知のしきい値を設定できます。有効なしきい値のパーセンテージは 1 ～ 100 です。
timers auth-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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.10.1	このコマンドが変更されました。**client-mid-rssi**、**notification**、および **fast-ssid-change** の各キーワードが追加されました。**user-timeout** キーワードが削除されました。

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。

```
デバイス# configure terminal
デバイス(config)# wireless client band-select cycle-count 8
デバイス(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。

```
デバイス# configure terminal
デバイス(config)# wireless client band-select cycle-threshold 700
デバイス(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。

```
デバイス# configure terminal
デバイス(config)# wireless client band-select expire suppression 70
デバイス(config)# end
```

wireless client client-steering client-count

ワイヤレスクライアントでクライアントステアリングの最小クライアント数を設定するには、**wireless client client-steering client-count** コマンドを使用します。この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。

wireless client client-steering client-count *0-200*

no wireless client client-steering client-count

構文の説明

0-200	クライアントステアリングの最小クライアント数を指定します。値の範囲は 0 ～ 200 クライアントです。デフォルト値は 3 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

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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、クライアントステアリングの最小クライアント数を設定する例を示します。

```
Device(config)# wireless client client-steering client-count 25
```

wireless client client-steering min-rssi-24ghz

2.4 GHz でのクライアントステアリングの最小 RSSI しきい値を設定するには、**wireless client client-steering min-rssi-24ghz -70** コマンドを使用します。この機能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。

wireless client client-steering min-rssi-24ghz -70

no wireless client client-steering min-rssi-24ghz -70

構文の説明

-70	2.4 GHz でのクライアントステアリングの最小 RSSI しきい値を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが導入されました。

例

次に、2.4 GHz でのクライアントステアリングの最小 RSSI しきい値を設定する例を示します。

```
Device(config)# wireless client client-steering min-rssi-24ghz -70
```

wireless client client-steering min-rssi-5ghz

5 GHz でのクライアントステアリングの最小 RSSI しきい値を設定するには、**wireless client client-steering min-rssi-5ghz** コマンドを使用します。この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。

wireless client client-steering min-rssi-5ghz -75

no wireless client client-steering min-rssi-5ghz -75

構文の説明

-75	5 GHz でのクライアントステアリングの最小 RSSI しきい値を指定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが導入されました。

例

次に、5 GHz でのクライアントステアリングの最小 RSSI しきい値を設定する例を示します。

```
Device(config)# wireless client client-steering min-rssi-5ghz -75
```

wireless client client-steering util-threshold

クライアントステアリングの最大使用率の差を設定するには、**wireless client client-steering util-threshold** コマンドを使用します。この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。

wireless client client-steering util-threshold *0-100*

no wireless client client-steering util-threshold

構文の説明

0-100	クライアントステアリングの最大使用率の差を指定します。値の範囲は 0 ～ 100 のパーセンテージです。デフォルト値は 20 パーセントです。

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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、クライアントステアリングの最大使用率の差を設定する例を示します。

```
Device(config)# wireless client client-steering util-threshold 20
```

wireless client client-steering window-size

ワイヤレスクライアントでクライアントステアリングの最小ウィンドウサイズを設定するには、**wireless client client-steering window-size** コマンドを使用します。この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。

wireless client client-steering window-size *0-200*

no wireless client client-steering window-size

構文の説明

0-200	クライアント ステアリング ウィンドウの最小サイズを指定します。値の範囲は 0 ～ 200 クライアントです。デフォルト値は 3 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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、クライアントステアリングの最小ウィンドウサイズを設定する例を示します。

```
Device(config)# # wireless client client-steering window-size 25
```

wireless ipv6 client

クライアントの IPv6 を有効にするには、**wireless ipv6 client** コマンドを使用します。クライアントの IPv6 を無効にするには、このコマンドの **no** 形式を使用します。

wireless ipv6 client

no wireless ipv6 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

デフォルトでは、IPv6 は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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

使用上のガイドライン

コントローラでクライアントが入力および出力した、すべてのクライアント IPv6 トラフィックがドロップされます。そのため、ローカルモードのみに制限されます。IPv6 が無効になっている場合、クライアントは IPv6 アドレスを取得しません。この設定は、設定変更が行われた後に関連付けまたは参加するクライアントにのみ影響します。既存のクライアントは影響を受けません。

例

次に、クライアントの IPv6 を有効にする例を示します。

```
Device(config)# wireless ipv6 client
```

wireless client ip-address deauthenticate

ワイヤレスクライアントを IP アドレスに基づいて認証解除するには、**wireless client ip-address deauthenticate** コマンドを使用します。

wireless client ip-address *ip-address* **deauthenticate**

構文の説明

ip-address	クライアント IP アドレス。

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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、IP アドレスに基づいてワイヤレスクライアントを認証解除する例を示します。

```
Device# wireless client ip-address 10.2.2.2 deauthenticate
```

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 **wireless client mac-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-resolve hostname *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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン　**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。

```
デバイス# configure terminal
デバイス(config)# wireless client mac-address 00:1f:ca:cf:b6:60 ccx clear-reports
デバイス(config)# end
```

wireless client syslog-detailed

クライアントイベントの詳細な syslog を有効にするには、**wireless client syslog-detailed** コマンドを使用します。クライアントイベントの詳細な syslog を無効にするには、このコマンドの **no** 形式を使用します。

wireless client syslog-detailed

no wireless client syslog-detailed

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

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 Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、クライアントイベントの詳細な syslog を有効にする例を示します。

```
Device(config)# wireless client syslog-detailed
```

wireless client username deauthenticate

特定のユーザー名を持つワイヤレスクライアントを認証解除するには、**wireless client username deauthenticate** コマンドを使用します。

wireless client username *username* **deauthenticate**

構文の説明

username	クライアントユーザー名。

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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、特定のユーザー名を持つワイヤレスクライアントを認証解除する例を示します。

```
Device# wireless client username Bob deauthenticate
```

wireless config validate

ワイヤレス設定が完全かつ一貫している（すべての機能プロファイルとタグが定義され、すべてのアソシエーションが完全かつ一貫している）かどうかを検証するには、特権EXECモードで **wireless config validate** コマンドを使用します。

wireless config validate

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

Cisco vEWLCでは、ワイヤレス設定はプロファイルのコレクションを使用して作成され、各プロファイルが機能ブロックを定義します。これらの機能ブロックは個別に定義され、無線LANの構築においてインテントベースのワークフローを通じて明確に定義された関連付けを実現するために使用されます。このように、機能ブロックのモジュラ化が柔軟であるため、管理者は、すべてのアソシエーションが一貫していて完全であることを確認する必要があります。

ワイヤレス設定の完全性と一貫性を確保するには、コンフィギュレーション検証ライブラリを使用して、設定の定義をテーブル間で検証します。ワイヤレス設定を検証し、不整合があればbtraceインフラおよび（コンソール ロギングが有効である場合）コンソールで表示されるコンテキスト エラー メッセージを使用して報告するため、このリリースから **wireless config validate** EXEC コマンドが導入されました。このコマンドは、機能的なワイヤレス LAN を実現できるようにするため、不整合（未解決のアソシエーション）を呼び出します。

出力をファイルに転送するには、**show logging | redirect bootflash:** *filename* コマンドを使用します。

次のワイヤレス設定のセットが検証されます。

RF タグ	サイト タグ	ポリシー タグ	ポリシー プロファイル	Flex プロファイル
site-tag	flex-profile	wlan profile	IPv4 ACL 名	VLAN ACL
policy-tag	ap-profile	policy profile	ファブリック名	ACL-policy
rf-tag	—	—	service-policy input および output name	RF ポリシー（5 GHz および 24 GHz）

RF タグ	サイト タグ	ポリシー タグ	ポリシー プロファイル	Flex プロファイル
-—	-—	-—	service-policy input および client output name	-—

例

次に、**wireless config validate** コマンドの出力例を示します

```
Device# wireless config validate

Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0:
wncmgrd: Error in AP: fc99.473e.0a90  Applied site-tag : mysite definitiondoes not exist
Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0:
wncmgrd: Error in AP: fc99.473e.0a90  Applied policy-tag : mypolicy definition does not
 exist
Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0:
wncmgrd: Error in AP: fc99.473e.0a90  Applied rf-tag : myrf definition does not exist
```

wireless country

デバイスの 1 つ以上の国コードを設定するには、 **wireless country** コマンドを使用します。

wireless country *country-code*

構文の説明

country-code	Two-letter country code.

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 Amsterdam 17.3.1	このコマンドが導入されました。

使用上のガイドライン

Cisco は、ネットワーク管理者または資格のある IT 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、デバイスで国コードを IN（インド）に設定する例を示します。

```
Device(config)# wireless country IN
```

wireless exclusionlist mac address

除外リストにクライアントを手動で追加するには、wireless exclusion list コマンドを使用します。手動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_address* **description**

構文の説明

description *value*	エントリの説明を設定します。

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

Cisco IOS XE Gibraltar 16.10.1	変更内容
	このコマンドは本リリースで追加されました。

使用上のガイドライン

クライアントが除外リストに動的に追加された場合、そのクライアントを削除するには、有効モードから **wireless client mac-address xxxx.xxxx.xxxx deauthenticate** コマンドを使用します。

例

次に、除外エントリを管理する例を示します。

```
Device(config)# wireless exclusion list xxxx.xxxx.xxxx
```

wireless fabric control-plane

ワイヤレス ファブリック モードに適用するコントロール プレーン名を設定するには、**wireless fabric control-plane** コマンドを使用します。

wireless fabric control-plane *control-plane-name*

構文の説明

control-plane-name	ワイヤレス ファブリック モードに適用されるコントロール プレーン名。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

コントロール プレーン名を指定しない場合は、自動生成される default-control-plane が使用されます。

例

次に、コントロール プレーン名を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless fabric control-plane test-control-plane
```

wireless fabric

コントローラで SD-Access ワイヤレスをグローバルに有効にするには、 **wireless fabric** コマンドを使用します。

wireless fabric

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、コントローラでSD-Accessワイヤレスをグローバルに有効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless fabric
```

wireless fabric name

ワイヤレス ファブリック名 VXLAN ID（VNID）マップを設定するには、**wireless fabric name** コマンドを使用します。

wireless fabric ［**control-plane** *control-plane-name*］ | ［**name** *vnid-map-name* **l2-vnid** *id* {**control-plane** *control-plane-name* | **l3-vnid** *id* } **ip** {*ipv-addr netmask-addr* | *ipv6-addr netmask-addr*} ［{**control-plane** *control-plane-name*］}］

構文の説明

control-plane *control-plane-name*	コントロール プレーンの詳細を設定します。
name *vnid-map-name*	ワイヤレス ファブリック名を設定します
l2-vnid *id*	レイヤ 2 VNID を設定します。有効な範囲は 0 ～ 16777215 です。
l3-vnid *id*	レイヤ 3 VNID を設定します。有効な範囲は 0 ～ 16777215 です。
ip {*ipv4-addr netmask-addr* | *ipv6-addr netmask-addr*}	IP アドレスとネットマスク アドレスの詳細。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、MAP サーバーを レイヤ 2 およびレイヤ 3 の VNID ごとに設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless fabric name vnid-map l2-vnid 2 l3-vnid 10 ip 209.165.200.224
255.255.255.224
```

wireless hotspot anqp-server

Hotspot 2.0 Access Network Query Protocol（ANQP）サーバーを設定するには、**wireless hotspot anqp-server** コマンドを使用します。Hotspot 2.0 サーバ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。

wireless hotspot anqp-server *server-name*

wireless hotspot anqp-server *server-name* **type open-roaming**

構文の説明

server-name	Hotspot 2.0 ANQP サーバーの名前。
type	ANQP サーバータイプ。
open-roaming	オープンローミングタイプ。

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 Gibraltar 16.12.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.2.1	このコマンドが変更されました。**type** および **open-roaming** のキーワードが導入されました。

例

次に、Hotspot 2.0 ANQP サーバーを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
```

次に、オープンローミングを使用して Hotspot 2.0 ANQP サーバーを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server type open-roaming
```

wireless hotspot gas-rate-limit

1 秒あたりに処理される Generic Advertisement Service（GAS）要求または Access Network Query Protocol（ANQP）要求の最大数を制限するには、**wireless hotspot gas-rate-limit** コマンドを使用します。制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。

wireless hotspot gas-rate-limit *limit*

構文の説明

limit	1 秒あたりに処理される GAS または ANQP 要求の数。有効な範囲は 1 ～ 2500 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 Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、1 秒あたりに処理される GAS または ANQP 要求の最大数を制限する例を示します。

```
Device(config)# wireless hotspot gas-rate-limit 100
```

wireless hotspot icon

Hotspot 2.0 のアイコンを設定するには、**wireless hotspot icon** コマンドを使用します。アイコンを削除するには、このコマンドの **no** 形式を使用します。

wireless hotspot icon {**bootflash:filename** | **flash:filename**} *media-type language-code icon-width icon-height*

構文の説明

media-type	このアイコン ファイルのメディア タイプ。 （注） アイコン ファイルは、次の URL で定義されているタイプと一致している必要があります。 http://www.iana.org/assignments/media-types/index.html
language-code	オペレータの 3 文字の言語コード。言語コードには、言語の最初の 3 文字のみを小文字で使用します。たとえば、英語の場合は *eng* を使用します。 言語コードの完全なリストについては、http://www.loc.gov/standards/iso639-2/php/code_list.php を参照してください。
icon-width	アイコンの幅（ピクセル）。有効な範囲は 0 ～ 65535 です。
icon-height	アイコンの高さ（ピクセル）。有効な範囲は 0 ～ 65535 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 Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、Hotspot 2.0 のアイコンを設定する例を示します。

```
Device(config)# wireless hotspot icon flash:test jpeg en 655 400
```

wireless ipv6 nd ns-forward

ワイヤレスクライアントへのネイバー要請（NS）メッセージの転送を有効にするには、**wireless ipv6 nd ns-forward** コマンドを使用します。この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。

wireless ipv6 nd ns-forward

no wireless ipv6 nd ns-forward

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.2	このコマンドは、Cisco IOS XE Cupertino 17.9.2 以降でサポートされています。

例

次に、ワイヤレスクライアントへのネイバー要請（NS）メッセージの転送を有効にする例を示します。

```
Device(config)# wireless ipv6 nd ns-forward
```

wireless ipv6 ra wired

有線クライアントへのルータ アドバタイズメント メッセージの転送を有効にするには、**wireless ipv6 ra wired** コマンドを使用します。

wireless ipv6 ra wired { **nd** { **na-forward** | **ns-forward** } | **ra-wired** }

構文の説明

nd	ワイヤレス IPv6 ND パラメータを設定します。
na-forward	ワイヤレスクライアントへのネイバーアドバタイズメントの転送を有効にします。
ns-forward	ワイヤレスクライアントへのネイバー要請の転送を有効にします。
ra	ワイヤレス IPv6 ルータアドバタイズメントのパラメータを設定します。
wired	有線クライアントへのルータ アドバタイズメント メッセージの転送を有効にします。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.3	このコマンドが導入されました。

例

次に、有線クライアントへのルータ アドバタイズメント メッセージの転送を有効にする例を示します。

```
Device(config)# wireless ipv6 ra wired
```

警告 **wireless ipv6 ra wired** コマンドは、展開中ではないときに、証明目的でのみ有効にする必要があります。

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 **wireless load-balancing** コマンドを使用します。

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 ポイントでのアグレッシブ 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス# configure terminal
デバイス(config)# wireless load-balancing denial 5
デバイス(config)# end
```

wireless load-balance ap method rf

RF ベースの AP ロードバランシングを設定するには、**wireless load-balance ap method rf** コマンドを使用します。RF ベースの AP 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。

wireless load-balance ap method rf

no wireless load-balance ap method rf

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

RF ベースのロードバランシ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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.12.1	このコマンドが導入されました。

例

次に、RF ベースの AP ロードバランシングを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless load-balance ap method rf
```

wireless macro-micro steering transition-threshold

マイクロ/マクロ遷移のしきい値を設定するには、 **wireless macro-micro steering transition-threshold** コマンドを使用します。

wireless macro-micro steering transition-threshold {**balancing-window** | **client count** *number-clients* }{**macro-to-micro** | **micro-to-macro** *RSSI in dBm*}

構文の説明

balancing-window	ルートプロセッサ スロット 0 の設定のアクティブ インスタンス。
client	ルートプロセッサスロット 0 の設定のスタンバイ インスタンス。
number-clients	有効なクライアント数の範囲は 0 ～ 65535 です。
macro-to-micro	マイクロ/マクロ遷移の RSSI を設定します。
micro-to-macro	マイクロ/マクロ クライアント ロード バランシング ウィンドウを設定します。
RSSI in dBm	RSSI（dBm 単位）。有効な範囲は –128 ～ 0 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、バランシングウィンドウを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless macro-micro steering transition-threshold balancing-window
number-of-clients
```

wireless macro-micro steering probe-suppression

マイクロ/マクロ プローブの抑制を設定するには、**wireless macro-micro steering probe-suppression** コマンドを使用します。

wireless macro-micro steering probe-suppression {**aggressiveness** *number-of-cycles* | | **hysteresis***RSSI in dBm* | **probe-auth** | **probe-only**}

構文の説明

aggressiveness	抑制するプローブ サイクルを設定します。サイクル数の範囲は 0 ～ 255 です。
hysteresis	クライアントが近傍のアクセス ポイントにローミングするためには、そのアクセス ポイントに後どれだけの信号強度が必要であるかを表示します。RSSI デシベル値の範囲は -6 ～ -3 です。
probe-auth	プローブと single auth を抑制するモードを有効にします
probe-only	プローブのみを抑制するモードを有効にします

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドは、Cisco IOS XE Gibraltar 16.12.1 よりも前のリリースで導入されました。

例

次に、バランシングウィンドウを設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless macro-micro steering probe-suppression aggressiveness
number-of-cycles
```

wireless management certificate

ワイヤレス管理証明書の詳細を作成するには、**wireless management certificate** コマンドを使用します。

wireless management certificate ssc {**auth-token** {**0** | **8**} *token* | **trust-hash** *hash-key* }

構文の説明

auth-token	認証トークン。
token	トークン名。
trust-hash	信頼できる SSC ハッシュリスト。
hash-key	SHA1 フィンガープリント。
0	暗号化されていないトークンを指定します。
8	AES 暗号化トークンを指定します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス管理証明書を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless management certificate ssc trust-hash test
```

wireless management interface

ワイヤレス管理インターフェイスを作成するには、**wireless management interface** コマンドを使用します。

wireless management interface {**GigabitEthernet** | **Loopback** | **Vlan** } *interface-number*

構文の説明

interface-number	インターフェイス番号。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス管理インターフェイスを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless management interface vlan vlan1
```

wireless management trustpoint

ワイヤレス管理トラストポイントを作成するには、**wireless management trustpoint** コマンドを使用します。

wireless management trustpoint *trustpoint-name*

構文の説明

trustpoint-name	トラストポイント名。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

アプライアンスはこのコマンドを必要とせずにデフォルトで SUDI 証明書を使用するため、このコマンドはクラウド向け Cisco Catalyst 9800 ワイヤレス コントローラ プラットフォームでのみ使用し、アプライアンスでは使用しません。

例

次に、ワイヤレス管理トラストポイントを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless management trustpoint test
```

wireless max-warning period

ワイヤレス クライアント チェックの周期を設定するには、**wireless max-warning period** コマンドを使用します。ワイヤレス クライアント チェッ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。

wireless max-warning period *interval-in-mins*

no wireless max-warning period

構文の説明

interval-in-mins	ワイヤレス クライアント チェックの周期。有効な値の範囲は、1 ～ 60 分です。

コマンド デフォルト

ワイヤレス クライアント チェックの周期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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、ワイヤレス クライアント チェックの周期を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless max-warning period 20
```

wireless max-warning threshold clients

ワイヤレス クライアント チェックでのワイヤレスクライアントの最大数に対する警告しきい値パーセンテージを設定するには、**wireless max-warning threshold client** コマンドを使用します。ワイヤレス クライアント チェックの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。

wireless max-warning threshold clients *threshold_percentage*

no wireless max-warning threshold clients

構文の説明

threshold_percentage	ワイヤレス クライアント チェックの警告しきい値パーセンテージ。有効な値の範囲は 50 ～ 100 パーセントです。

コマンド デフォルト

しきい値のパーセントは 75 パーセントに設定されています。

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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、ワイヤレス クライアント チェックでのワイヤレスクライアントの最大数に対する警告しきい値パーセンテージを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless max-warning threshold clients 90
```

wireless media-stream

さまざまなパラメータを設定するには、 **wireless media-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。 値は 100 ～ 1500 kbps の範囲で指定できます。
group *default*	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。 値は 1 ～ 35000 kbps の範囲で指定できます。
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 *policy*	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。 次のオプションのいずれかを選択できます。 • admit：メディア ストリーム グループのトラフィックを許可します。 • deny：メディア ストリーム グループのトラフィックを拒否します。
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 *Notes*	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 Gibraltar 16.10.1	このコマンドが変更されました。

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。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#wireless media-stream group GROUP1 231.1.1.1 231.1.1.10
```

wireless media-stream message

セッション アナウンス メッセージを設定するには、**wireless media-stream message** コマンドを使用します。

wireless media-stream message {**Email** | **Notes** | **URL** | **phone**}

構文の説明

Email	セッションアナウンス電子メールを設定します。
Notes	セッション アナウンス メモを設定します。
URL	セッション アナウンス URL を設定します。
phone	セッションアナウンスの電話番号を設定します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

メディア ストリームが（帯域幅制約が原因で）拒否される場合に、ユーザーにメッセージを送信できます。これらのパラメータは、IT サポートの電子メール アドレス、メモ（ストリームが拒否された理由を説明する画面メッセージ）、ユーザがリダイレクトされるURL、拒否されたストリームについてユーザが問い合わせをする電話番号など、送信するメッセージを設定します。

例

次に、セッション アナウンス URL を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream message URL www.example.com
```

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-stream multicast-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

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。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#wireless media-stream multicast-direct
```

wireless mesh alarm association count

メッシュ アラーム アソシエーションの数を設定するには、 **wireless mesh alarm association count** コマンドを使用します。

wireless mesh alarm association count *count*

構文の説明

count	アラーム アソシエーションの数。有効な範囲は 1 ～ 30 です。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、アラーム アソシエーションの数を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy wireless mesh alarm association count 10
```

wireless mesh alarm high-snr

メッシュ アラームの 高 SNR 値を設定するには、 **wireless mesh alarm high-snr** コマンドを使用します。

wireless mesh alarm high-snr *high-snr*

構文の説明

high-snr	高 SNR 値を設定します。有効な範囲は 31 ～ 100 です。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュの高 SNR を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy wireless mesh alarm high-snr 75
```

wireless mesh alarm low-snr

メッシュ アラームの低 SNR 値を設定するには、 **wireless mesh alarm low-snr** コマンドを使用します。

wireless mesh alarm low-snr *low-snr*

構文の説明

low-snr	低 SNR 値を設定します。有効な範囲は 1 ～ 30 です。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュの高 SNR を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy wireless mesh alarm low-snr 5
```

wireless mesh alarm max-children map

メッシュ アラームの最大子 MAP 値を設定するには、 **wireless mesh alarm max-children map** コマンドを使用します。

wireless mesh alarm max-children map *max-children*

構文の説明

max-children	メッシュ アラームの最大子 MAP パラメータを設定します。有効な範囲は 1 ～ 50 です。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ アラームの最大子 MAP 値を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mesh alarm max-children map 35
```

wireless mesh alarm max-children rap

メッシュ アラームの最大子 RAP 値を設定するには、 **wireless mesh alarm max-children rap** コマンドを使用します。

wireless mesh alarm max-children rap *max-children*

構文の説明

max-children	メッシュ アラームの最大子 RAP パラメータを設定します。有効な範囲は 1 ～ 50 です。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ アラームの最大子 RAP 値を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mesh alarm max-children rap 40
```

wireless mesh alarm max-hop

メッシュ アラームの最大ホップ パラメータを設定するには、 **wireless mesh alarm max-hop** コマンドを使用します。

wireless mesh alarm max-hop *max-hop*

構文の説明

max-hop	メッシュ アラームの最大ホップ数を設定します。有効な範囲は1 ～ 16 です。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ アラームの最大ホップ パラメータを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mesh alarm max-hop 15
```

wireless mesh alarm parent-change count

親変更カウントの最大値を設定するには、 **wireless mesh alarm parent-change count** コマンドを使用します。

wireless mesh alarm parent-change count *count*

構文の説明

count	親変更カウントの最大値を設定します。有効な範囲は 1 ～ 30 です。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、アラームの親変更カウント値を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mesh alarm parent-change count 6
```

wireless mesh backhaul bdomain-channels

屋外のメッシュ AP のバックホール無線で拡張 UNII B ドメイン チャネルを設定し、許可するには、 **wireless mesh backhaul bdomain-channels** コマンドを使用します。

wireless mesh backhaul bdomain-channels

構文の説明

bdomain-channels	屋外のメッシュ AP のバックホール無線で拡張 UNII B ドメイン チャネルを許可します。 メッシュ AP のバックホール無線による拡張 UNII B ドメイン チャネルの使用を無効にするには、このコマンドの **[no]** 形式を使用します。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、屋外のメッシュ AP のバックホール無線による拡張 UNII B ドメイン チャネルの使用を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# no wireless mesh backhaul bdomain-channels
```

wireless mesh backhaul rrm

メッシュ バックホールを設定するには、 **wireless mesh backhaul** コマンドを使用します。

wireless mesh backhaul{**bdomain-channels** | **rrm**}

構文の説明

backhaul	メッシュ バックホールを設定します。
bdomain-channels	屋外のメッシュ AP のバックホール無線で拡張 UNII B ドメイン チャネルを許可します。
rrm	メッシュ バックホールの RRM 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

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ バックホールの RRM を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mesh backhaul rrm
```

wireless mesh backhaul rrm auto-dca

無線周波数（RF）特定用途向け集積回路（ASIC）RAP の自動 DCA を設定するには、**wireless mesh backhaul rrm auto-dca** コマンドを使用します。

wireless mesh backhaul rrm auto-dca

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

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 Cupertino 17.9.1	このコマンドが導入されました。

例

次に、RF ASIC 集積回路 RAP の自動 DCA を設定する例を示します。

```
Device# wireless mesh backhaul rrm auto-dca
```

wireless mesh cac

メッシュ CAC モードを設定するには、 **wireless mesh cac** コマンドを使用します。

wireless mesh cac

構文の説明

cac	メッシュ CAC モードを設定します。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ CAC モードを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mesh cac
```

wireless mesh ethernet-bridging allow-bdpu

有線メッシュ アップリンクへの STP BPDU を設定するには、 **wireless mesh ethernet-bridging allow-bdpu** コマンドを使用します。

wireless mesh ethernet-bridging allow-bdpu

構文の説明

ethernet-bridging	イーサネット ブリッジングを設定します。
allow-bdpu	有線メッシュ アップリンクへの STP BPDU 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

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、有線メッシュ アップリンクへの STP BPDU を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mesh ethernet-bridging allow-bdpu
```

wireless mesh security psk provisioning

メッシュ セキュリティ PSK パラメータをプロビジョニングするには、 **wireless mesh security psk provisioning** コマンドを使用します。

wireless mesh security psk provisioning {**default_psk** | **inuse** *psk-index* | **key** *psk-index*{**0** | **8**}*enter-psk-name psk-description*}

構文の説明

provisioning	メッシュ PSK プロビジョニング パラメータを設定します。
default_psk	メッシュ プロビジョニングをデフォルト PSK 設定に設定します。
inuse	PSK inuse インデックスを設定します
psk-index	PSK キー インデックスを入力します。有効な範囲は 1 ～ 5 です。
key	事前共有キーを設定します
psk-index	PSK キー インデックスを入力します。有効な範囲は 1 ～ 5 です。
0	非暗号化パスワードを入力することを選択します。
8	AES 暗号化パスワードを入力することを選択します。
enter-psk-name	設定済みの PSK キーの名前を入力します。
psk-description	このキーの説明を入力します。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュセキュリティでデフォルトPSKキーをプロビジョニングする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mesh security psk provisioning default_psk
```

wireless mesh subset-channel-sync

モビリティ グループのサブセット チャネル同期を設定するには、 **wireless mesh subset-channel-sync** コマンドを使用します。

wireless mesh subset-channel-sync

構文の説明

subset-channel-sync	モビリティ グループのサブセット チャネル同期を設定します

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、モビリティ グループのサブセット チャネル同期を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mesh subset-channel-sync
```

wireless mobility

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 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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、 間の DSCP 値が 20 のモビリティを設定する例を示します。

```
デバイス(config)# wireless mobility dscp 20
```

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。

```
デバイス enable
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(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** *interval*}
no wireless mobility group keepalive {**count** 番号 | **interval** *interval*}

構文の説明

count *number*	モビリティ グループ メンバーに ping 要求を送信する回数。この回数を超えると、メンバー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 *interval*	モビリティ グループ メンバーへの 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。 （注） モビリティ トンネルを介して接続されているコントローラの場合は、両方のコントローラのキープアライブ間隔値が同じであることを確認します。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス(config)# wireless mobility group keepalive count 10
```

wireless mobility group mac-address

モビリティ メッセージで使用される MAC アドレスを設定するには、**wireless mobility group mac-address** コマンドを使用します。

wireless mobility group mac-address *mac-addr*

構文の説明

mac-addr	モビリティ メッセージで使用される MAC 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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、モビリティ メッセージで使用される MAC アドレスを設定する例を示します。

```
Device(config)# wireless mobility group mac-address 00:0d:ed:dd:25:82
```

wireless mobility group member ip

モビリティ グループのメンバ リストのユーザを追加または削除するには、 **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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス(config)# mobility group member ip 10.104.171.101 group TestDocGroup
```

wireless mobility group member mac-address

モビリティ グループ メンバー リストを作成するには、グローバル コンフィギュレーション モードで **wireless mobility group member mac-address** 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 mac-address *peer_mac* **ip** *peer_private_ip* [**public-ip** *peer_public_ip*] **group** *group_name*

構文の説明

peer_mac	ピアコントローラの MAC アドレス。
peer_private_ip	ピアコントローラのプライベート IP アドレス。
peer_public_ip	ピアコントローラのパブリック IP アドレス。
group_name	メンバーコントローラのグループ名。

コマンド デフォルト

モビリティピア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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1s	このコマンドは、Cisco IOS XE Amsterdam 17.1.1s よりも前のリリースで導入されました。 **public-ip** キーワードと *peer_public_ip* 変数は、このリリースからサポートされます。

例

次に、モビリティ グループ メンバー リストを作成する例を示します。

```
Device(config)# wireless mobility group member mac-address 001e.494b.04ff ip 11.0.0.2
public-ip 4.0.0.112 group dom1
```

wireless mobility group multicast-address

非ローカルモビリティグループのマルチキャストIPアドレスを設定するには、**wireless mobility group multicast-address** コマンドを使用します。

wireless mobility group multicast-address *group-name* {**ipv4** | **ipv6**}*ip-addr*

構文の説明

group-name	非ローカル モビリティ グループの名前。
ipv4	IPv4 アドレスを入力するオプション。
ipv6	IPv6 アドレスを入力するオプション。
ip-addr	非ローカルモビリティグループのIPv4またはIPv6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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、非ローカル モビリティ グループのマルチキャスト IPv4 アドレスを設定する例を示します。

```
Device(config)# wireless mobility group multicast-address Mygroup ipv4 224.0.0.5
```

wireless mobility group name

モビリティ ドメイン名を設定するには、**wireless mobility group name** 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 Gibraltar 16.10.1	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。

```
デバイス(config)# mobility group domain lab1
```

wireless mobility multicast ipv4

ローカル モビリティ グループのマルチキャスト IPv4 アドレスを設定するには、**wireless mobility multicast ipv4** コマンドを使用します。

wireless mobility multicast ipv4 *ipv4-addr*

構文の説明

ipv4-addr	ローカル モビリティ グループのマルチキャスト IPv4 アドレスを入力します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ローカル モビリティ グループのマルチキャスト IPv4 アドレスを設定する例を示します。

```
Device(config)# wireless mobility multicast ipv4 224.0.0.4
```

wireless mobility mac-address

モビリティ メッセージで使用される MAC アドレスを設定するには、**wireless mobility mac-address** コマンドを使用します。

wireless mobility mac-address *mac-address*

構文の説明

mac-address	モビリティ メッセージで使用される MAC 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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、モビリティ メッセージで使用される MAC アドレスを設定する例を示します。

```
Device(config)# wireless mobility mac-address 00:0d:bd:5e:9f:00
```

wireless multicast

イーサネット マルチキャスト パラメータを設定するには、**wireless multicast** コマンドを使用します。

wireless multicast {*ipv4-address* | **ipv6** *ipv6-address* | **non-ip** [**vlan** *vlan-id*]}

構文の説明

ipv4-address	マルチキャスト IPv4 アドレス。
ipv6 *ipv6-address*	マルチキャスト IPv6 アドレス。
non-ip	すべての VLAN で非 IP マルチキャストを設定します。トラフィックが通過できるように、ワイヤレス マルチキャストを有効にしておく必要があります。
non-ip vlan *vlan-id*	VLAN ごとに非 IP マルチキャストを設定します。トラフィックが通過できるように、ワイヤレスマルチキャストおよびワイヤレスマルチキャスト非 IP の両方を有効にする必要があります。 VLAN ID の有効な範囲は 1 ～ 4094 です。

コマンド デフォルト

なし

コマンド モード

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ID が 5 の VLAN に非 IP マルチキャストを設定する例を示します。

```
Device(config)# wireless multicast non-ip vlan 5
```

wireless profile airtime-fairness

新しい Cisco ATF ポリシーを作成するには、**wireless profile airtime-fairness** コマンドを使用します。

wireless profile airtime-fairness *atf-policy-name atf-profile-id*

構文の説明

atf-policy-name	ATF プロファイル名を参照します。
atf-profile-id	ATF プロファイル ID を参照します。指定できる範囲は 0 ～ 511 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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、新しい Cisco ATF ポリシーを作成する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless profile airtime-fairness <atf-policy-name> 1
デバイス(config-config-atf)# weight 5
デバイス(config-config-atf)# client-sharing
デバイス(config-config-atf)# end
```

wireless profile ap packet-capture

ワイヤレス AP パケット キャプチャ プロファイルを設定するには、**wireless profile ap packet-capture** コマンドを使用します。

wireless profile ap packet-capture *packet-capture-profile-name*

構文の説明

packet-capture-profile-name	AP パケット キャプチャ 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

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、AP パケット キャプチャ プロファイルを設定する例を示します。

```
Device(config)# wireless profile ap packet-capture test1
```

wireless profile ap priming

アクセスポイント（AP）をプライミングするためのプロファイルを設定するには、**wireless profile ap priming** コマンドを使用します。プライ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。

wireless profile ap priming *profile-name*

no wireless profile ap priming *profile-name*

構文の説明

profile-name	APプライミングプロファイル名。

コマンド デフォルト

AP プライミングプロファイル名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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.2	このコマンドが導入されました。

使用上のガイドライン

- AP フィルタ プライミング プロファイルには、最大 3 つのコントローラを含めることができます。AP プライミングプロファイルは、AP MAC レベルで、または一致する正規表現フィルタを使用して適用することができます。
- AP MAC ベースの AP プライミングの優先順位が最も高くなります。AP MAC ベースの AP プライミングが使用できない場合は、一致する正規表現フィルタの下にあるプライミングプロファイルのうち、有効なプライミング設定を持ち、最も高い優先順位を持つプライミングプロファイルが適用されます。

例

次に、AP をプライミングするためのプロファイルを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile ap priming Prime-FX
```

wireless profile calender-profile name

カレンダー プロファイルを設定するには、**wireless profile calender-profile name** コマンドを使用します。

wireless profile calender-profile name *name*

構文の説明

name	カレンダープロファイルを指定します。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

次に、カレンダー プロファイルを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile calender-profile name daily_calendar_profile
Device(config-calender-profile)# start 09:00:00 end 17:00:00
Device(config-calender-profile)# recurrance daily
Device(config-calender-profile)# end
```

wireless profile fabric

ファブリック プロファイル パラメータを設定するには、 **wireless profile fabric** コマンドを使用します。

wireless profile fabric *fabric-profile-name*

構文の説明

fabric-profile-name	ファブリック プロファイル名。
fabric	ファブリック プロファイル パラメータを設定します。
profile	プロファイル 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

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ファブリック プロファイル パラメータを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile fabric fabric-profile-name
```

wireless profile mesh

アクセスポイント（AP）でメッシュプロファイルを設定するには、**wireless profile mesh** *profile-name* コマンドを使用します。

wireless profile mesh *profile-name*

構文の説明		
	profile-name	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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、AP でメッシュプロファイルを設定する例を示します。

```
Device# configure terminal
(config)#wireless profile mesh test1
```

wireless profile policy

WLAN ポリシー プロファイルを設定するには、**wireless profile policy** コマンドを使用します。

wireless profile policy *policy-profile*

構文の説明

policy-profile	WLAN ポリシープロファイルの名前。

コマンド デフォルト

デフォルトのプロファイル名は default-policy-profile 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、WLAN ポリシー プロファイルを設定する例を示します。

```
Device(config)# wireless profile policy mywlan-profile-policy
```

wireless profile power

ワイヤレス電源ポリシープロファイルを設定するには、**wireless profile power** コマンドを使用します。この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。

wireless profile power *power-profile-name*

構文の説明

power-profile-name	ワイヤレス電源ポリシープロ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

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 Cupertino 17.8.1	このコマンドが導入されました。

例

次に、ワイヤレス電源ポリシープロファイルを設定する例を示します。

```
Device(config)# wireless profile power power-profile-name
```

wireless profile tunnel

トンネル プロファイルを設定するには、**wireless profile tunnel** コマンドを使用します。

wireless profile tunnel

構文の説明

tunnel-profile-name	トンネル プロファイルの名前。
dhcp-opt82 format mac *raw*|*colon-delimited*	オプション 82 の RID および CID フィールドの MAC アドレスの形式を設定します。

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、トンネル プロファイルを設定する例を示します。

```
Device(config)# wireless profile tunnel tun1
```

wireless profile radio

ワイヤレス無線プロファイルを設定するには、**wireless profile radio** コマンドを使用します。この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。

wireless profile radio *radio-profile-name*

no wireless profile radio *radio-profile-name*

構文の説明

wireless profile radio	新しいワイヤレス無線プロファイルを作成します。
radio-profile-name	無線プロファイル名を指定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、ワイヤレス無線プロファイルを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile radio radio-profile-name
```

wireless rfid

スタティック無線周波数 ID（RFID）タグのデータ タイムアウ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 **wireless rfid** コマンドを使用します。

wireless rfid timeout *timeout-value*

構文の説明

timeout	スタティック RFID タグのデータ タイムアウト値を設定します。
timeout-value	RFID タグのデータ タイムアウト値。有効な値の範囲は 60 ～ 7200 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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、スタティック RFID タグのデータ タイムアウト値を設定する例を示します。

```
Device(config)# wireless rfid timeout 70
```

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、 **wireless security dot1x** 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-key interval *sec*	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。
wep key	802.1x WEP 関連パラメータを設定します。
index 0	WEP キーのインデックス値を 0 として指定します。
index 3	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 Gibraltar 16.10.1	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

次の例では、 **wireless security dot1x** のすべてのコマンドをリストしています。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(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 dot1x radius accounting mac-delimiter

called-station-ID または calling-station-ID の MAC デリミタを設定するには、**wireless security dot1x radius accounting username-delimiter** コマンドを使用します。

called-station-ID または calling-station-ID の MAC デリミタを削除するには、このコマンドの **no** 形式を使用します。

wireless security dot1x radius accounting mac-delimiter {**colon** | **hyphen** | **none** | **single-hyphen** }

構文の説明

colon	デリミタをコロンに設定します。
hyphen	デリミタをハイフンに設定します。
none	デリミタを無効にします。
single-hyphen	デリミタをシングル ハイフンに設定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.6.0 E	このコマンドが導入されました。

次に、called-station-ID または calling-station-ID の MAC デリミタをコロンに設定する例を示します。

```
デバイス(config)# wireless security dot1x radius accounting mac-delimiter colon
```

wireless security dot1x radius accounting username-delimiter

デリミタのタイプを設定するには、**wireless security dot1x radius accounting username-delimiter** コマンドを使用します。こ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 security dot1x radius accounting username-delimiter {**colon | hyphen | none | single-hyphen**}

構文の説明

colon	デリミタをコロンに設定します。
hyphen	デリミタをハイフンに設定します。
none	デリミタを無効にします。
single-hyphen	デリミタをシングルハイフンに設定します。

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 モード。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.2 E	このコマンドが導入されました。

次に、デリミタをコロンに設定する例を示します。

```
デバイス(config)# wireless security dot1x radius acounting username-delimiter colon
```

wireless security dot1x radius callStationIdCase

RADIUS メッセージで送信される呼出端末 ID の大文字小文字を設定するには、**wireless security dot1x radius callStationIdCase** コマンドを使用します。

RADIUS メッセージで送信される呼出端末 ID の大文字小文字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 security dot1x radius callStationIdCase {**lower** | **upper**}

構文の説明

lower	すべての呼出端末 ID を小文字で RADIUS に送信します
upper	すべての呼出端末 ID を大文字で RADIUS に送信します

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.6.0 E	このコマンドが導入されました。

次に、RADIUS メッセージで送信される呼出端末 ID を小文字に設定する例を示します。

```
デバイス(config)# wireless security dot1x radius callstationIdCase lower
```

wireless security dot1x radius mac-authentication call-station-id

MAC 認証用の呼出端末 ID タイプを設定するには、**wireless security dot1x radius mac-authentication call-station-id** 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。

wireless security dot1x radius mac-authentication call-station-id ap-ethmac-only | ap-ethmac-ssid | ap-group-name | ap-label-address | ap-label-address-ssid | ap-location | ap-macaddress | ap-macaddress-ssid | ap-name | ap-name-ssid | ipaddress | macaddress | vlan-id

構文の説明

ap-ethmac-only	呼出端末 ID タイプを AP のイーサネット MAC アドレスに設定します。
ap-ethmac-ssid	呼出端末 ID タイプを 'AP のイーサネット MAC アドレス':'SSID' という形式に設定します。
ap-group-name	呼出端末 ID タイプを AP グループ名に設定します。
ap-label-address	呼出端末 ID タイプを AP ラベル上の AP の MAC アドレスに設定します。
ap-label-address-ssid	呼出端末 ID タイプを 'AP ラベル上の MAC アドレス':'SSID' という形式に設定します。
ap-location	呼出端末 ID タイプを AP の場所に設定します。
ap-macaddress	呼出端末 ID タイプを AP の無線 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 無線 MAC アドレス':'SSID' に設定します。
ap-name	呼出端末 ID タイプを AP 名に設定します。
ap-name-ssid	呼出端末 ID タイプを 'AP 名':'SSID' という形式に設定します。
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。
vlan-id	呼出端末 ID タイプを VLAN ID に設定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.2 E	このコマンドが導入されました。

次に、呼出端末 ID タイプを AP の イーサネット MAC アドレスに設定する例を示します。

```
デバイス(config)# wireless security dot1x radius mac-authentication call-station-id
ap-ethmac-only
```

wireless security dot1x radius mac-authentication mac-delimiter

MAC 認証属性を設定するには、**wireless security dot1x radius mac-authentication mac-delimiter** コマンドを使用します。

MAC 認証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。

wireless security dot1x radius mac-authentication mac-delimiter {**colon** | **hyphen** | **none** | **single-hyphen** }

構文の説明

colon	デリミタをコロンに設定します。
hyphen	デリミタをハイフンに設定します。
none	デリミタを無効にします。
single-hyphen	デリミタをシングル ハイフンに設定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.6.0 E	このコマンドが導入されました。

次に、MAC 認証属性をコロンに設定する例を示します。

```
デバイス(config)# Scurity dot1x radius mac-authentication mac-delimiter colon
```

wireless security web-auth retries

特定の WLAN で Web 認証の再試行を有効にするには、 **wireless wireless security web-auth retries** コマンドを使用します。無効にするには、このコマンドの **no** 形式を使用します。

wireless securityweb-authretries*retries*
nowireless securityweb-authretries

構文の説明

wireless security web-auth	特定の WLAN で Web 認証を有効にします。
retries *retries*	Web 認証要求の最大再試行回数を指定します。範囲は 0 ～ 30 です。デフォルト値は 3 です。

コマンド デフォルト

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 Gibraltar 16.10.1	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 WLAN で Web 認証の再試行を有効にする例を示します。

```
デバイス#configure terminal
デバイス# wireless security web-auth retries 10
```

wireless tag policy

ワイヤレス タグ ポリシーを設定するには、**wireless tag policy** コマンドを使用します。

wireless tag policy *policy-tag*

構文の説明

policy-tag	ワイヤレスタグポリシーの名前。

コマンド デフォルト

デフォルトのポリシー タグは、default-policy-tag 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス ポリシー タグを設定する例を示します。

```
Device(config)# wireless tag policy guest-policy
```

wireless tag rf

無線周波数（RF）タグを設定するには、**wireless tag rf** コマンドを使用します。この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。

wireless tag rf *rf-tg-name*

構文の説明

wireless tag rf	RFタグのパラメータを設定します。
rf-tg-name	RF タグ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

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 Bengaluru 17.6.1	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

例

次に、ワイヤレスタグの無線周波数（RF）を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless tag rf rf-tag-name
```

wireless tag site

ワイヤレス サイト タグを設定するには、**wireless tag site** *site-tag* コマンドを使用します。

wireless tag site *site-tag*

構文の説明

site-tag	サイト タグの名前。

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、サイト タグを設定する例を示します。

```
Device(config)# wireless tag site test-site
```

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、**wireless wps ap-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 Gibraltar 16.10.1	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、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。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#wireless wps ap-authentication threshold 65
```

wireless wps ap-authentication threshold

アクセスポイントのネイバー認証のアラームトリガーしきい値を設定するには、 **wireless wps ap-authentication threshold** 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 *value*

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。しきい値の範囲は 1 ～ 255 です。デフォルト値は 1 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 Amsterdam 16.12.1	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

例

次に、アクセスポイントのネイバー認証のアラームトリガーしきい値を設定する例を示します。

```
Device(config)# wireless wps ap-authentication threshold 1
```

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** | **dot1x-timeout** | **ip-theft** | **web-auth**}
no wireless wps client-exclusion {**all** | **dot11-assoc** | **dot11-auth** | **dot1x-auth** | **dot1x-timeout** | **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。
dot1x-timeout	タイムアウト時および応答がない場合の除外を有効にします。
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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#wireless wps client-exclusion dot11-assoc
```

wireless wps mfp

さまざまな管理フレーム保護（MFP）パラメータを設定するには、**wireless wps mfp** コマンドを使用します。

wireless wps mfp **ap-impersonation** | **key-refresh-interval** *interval*

構文の説明

interval	MFP キーの更新間隔を時間単位で指定します。有効な範囲は 1 ～ 24 です。デフォルト値は 24 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 Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

次に、さまざまな管理フレーム保護（MFP）パラメータを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless wps mfp key-refresh-interval 1
```

wireless wps mfp ap-impersonation

AP 偽装検出を設定するには、**wireless wps mfp ap-impersonation** コマンドを使用します。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。

wireless wps mfp ap-impersonation

no wireless wps mfp ap-impersonation

構文の説明

ap-impersonation	AP 偽装検出を設定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 16.12.1	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

例

次に、AP 偽装検出を設定する例を示します。

```
Device(config)# wireless wps mfp ap-impersonation
```

wireless wps rogue

さまざまな不正パラメータを設定するには、 **wireless wps rogue** 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 Gibraltar 16.10.1	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、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。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#wireless wps rouge adhoc alert mac_addr
```

wireless wps rogue network-assurance enable

不正ワイヤレス サービス アシュアランス（WSA）イベントを有効にするには、**wireless wps rogue network-assurance enable** コマンドを使用します。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。

wireless wps rogue network-assurance enable

no wireless wps rogue network-assurance enable

構文の説明

network-assurance enable	不正WSAイベントを有効にします。

コマンド デフォルト

なし

コマンド モード

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 Amsterdam 16.12.1	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

例

次に、不正ワイヤレス サービス アシュアランス イベントを有効にする例を示します。

```
Device(config)# wireless wps rogue network-assurance enable
```

wireless wps rogue ap aaa

有効な AP MAC アドレスを検出するための AAA/ローカルデータベースの使用を設定するには、**wireless wps rogue ap aaa** コマンドを使用します。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。

wireless wps rogue ap aaa

no wireless wps rogue ap aaa

構文の説明

aaa	有効な AP MAC アドレスを検出するための AAA またはローカルデータベースの使用を設定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 16.12.1	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

例

次に、有効な AP MAC アドレスを検出するための AAA/ローカルデータベースの使用を設定する例を示します。

```
Device(config)# wireless wps rogue ap aaa
```

wireless wps rogue ap aaa polling-interval

不正 AP の AAA 検証間隔（秒単位）を設定するには、**wireless wps rogue ap aaa polling-interval** コマンドを使用します。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。

wireless wps rogue ap aaa polling-interval *60 - 86400*

no wireless wps rogue ap aaa polling-interval *60 - 86400*

構文の説明

aaa	有効な AP MAC アドレスを検出するための AAA またはローカルデータベースの使用を設定します。
polling-interval	不正 AP の AAA 検証間隔を設定します。
60 - 86400	AP の AAA 検証間隔（秒単位）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 Gibraltar 16.12.1	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

例

次に、不正 AP の AAA 検証間隔（秒単位）を設定する例を示します。

```
Device(config)# wireless wps rogue ap aaa polling-interval 120
```

wireless wps rogue ap init-timer

不正 AP の初期化タイマーを設定するには、**wireless wps rogue ap init-timer** コマンドを使用します。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。

wireless wps rogue ap init-timer

no wireless wps rogue ap init-timer

構文の説明

init-timer	不正APの初期化タイマーを設定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 16.12.1	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

例

次に、不正 AP の初期化タイマーを設定する例を示します。

```
Device(config)# wireless wps rogue ap init-timer
```

wireless wps rogue ap mac-address rldp initiate

不正 AP で Rogue Location Discovery Protocol を開始および設定するには、**wireless wps rogue ap mac-address rldp initiate** コマンドを使用します。

wireless wps rogue ap mac-address <*MAC Address*> **rldp initiate**

構文の説明

wps	WPS 設定を設定します。
rogue	グローバル不正デバイスを設定します。
ap mac-address <*MAC Address*>	AP の MAC アドレス。
rldp initiate	不正 AP で RLDP を開始します。

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 Amsterdam 16.12.1	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

例

次に、不正 AP で Rogue Location Discovery Protocol を開始および設定する例を示します。

```
Device# wireless wps rogue ap mac-address 10.1.1 rldp initiate
```

wireless wps rogue ap notify-min-rssi

不正 AP の最小 RSSI 通知しきい値を設定するには、**wireless wps rogue ap notify-min-rssi** コマンドを使用します。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。

wireless wps rogue ap notify-min-rssi

no wireless wps rogue ap notify-min-rssi

構文の説明

notify-min-rssi	不正 AP の最小 RSSI 通知しきい値を設定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 16.12.1	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

例

次に、不正 AP の最小 RSSI 通知しきい値を設定する例を示します。

```
Device(config)# wireless wps rogue ap notify-min-rssi
```

wireless wps rogue ap notify-rssi-deviation

不正 AP の RSSI 偏差通知しきい値を設定するには、**wireless wps rogue ap notify-rssi-deviation** コマンドを使用します。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。

wireless wps rogue ap notify-rssi-deviation

no wireless wps rogue ap notify-rssi-deviation

構文の説明

notify-rssi-deviation	不正 AP の RSSI 偏差通知しきい値を設定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 16.12.1	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

例

次に、不正 AP の RSSI 偏差通知しきい値を設定する例を示します。

```
Device(config)# wireless wps rogue ap notify-rssi-deviation
```

wireless wps rogue ap rldp alarm-only

Rogue Location Discovery Protocol（RLDP）を設定し、不正が検出された場合にアラームを発生させるには、**wireless wps rogue ap rldp alarm-only** コマンドを使用します。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。

wireless wps rogue ap rldp alarm-only

no wireless wps rogue ap rldp alarm-only

構文の説明

alarm-only	RLDP を設定し、不正が検出された場合にアラームを発生させます。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 16.12.1	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

例

次に、RLDP を設定し、不正が検出された場合にアラームを発生させる例を示します。

```
Device(config)# wireless wps rogue ap rldp alarm-only
```

wireless wps rogue ap rldp alarm-only monitor-ap-only

モニター AP でのみ RLDP を実行するには、**wireless wps rogue ap rldp alarm-only monitor-ap-only** コマンドを使用します。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。

wireless wps rogue ap rldp alarm-only monitor-ap-only

no wireless wps rogue ap rldp alarm-only monitor-ap-only

構文の説明

monitor-ap-only	モニター AP でのみ 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 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 Amsterdam 16.12.1	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

例

次に、モニター AP でのみ RLDP を実行する例を示します。

```
Device(config)# wireless wps rogue ap rldp alarm-only monitor-ap-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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE 3.7.3E	このコマンドの **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。

デバイス**wireless wps rogue ap rldp auto-contain**

wireless wps rogue ap rldp retries

不正 AP での RLDP 再試行回数を設定するには、**wireless wps rogue ap rldp retries** コマンドを使用します。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。

wireless wps rogue ap rldp retries

no wireless wps rogue ap rldp retries

構文の説明

retries	不正 AP での RLDP 再試行回数を設定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 16.12.1	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

例

次に、不正 AP での RLDP 再試行回数を設定する例を示します。

```
Device(config)# wireless wps rogue ap rldp retries
```

wireless wps rogue ap rldp schedule

RLDP スケジューリングを設定するには、**wireless wps rogue ap rldp schedule** コマンドを使用します。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。

wireless wps rogue ap rldp schedule

no wireless wps rogue ap rldp schedule

構文の説明

schedule	RLDP スケジューリングを設定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 16.12.1	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

例

次に、RLDP スケジューリングを設定する例を示します。

```
Device(config)# wireless wps rogue ap rldp schedule
```

wireless wps rogue ap rldp schedule day

RLDP スケジューリングを実行する日を設定するには、**wireless wps rogue ap rldp schedule day** コマンドを使用します。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。

wireless wps rogue ap rldp schedule day { **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** } **start** *[HH:MM:SS]* **end** *[HH:MM:SS]*

no wireless wps rogue ap rldp schedule day { **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** } **start** *[HH:MM:SS]* **end** *[HH:MM:SS]*

構文の説明

day {**friday**	**monday**	**saturday**	**sunday**	**thursday**	**tuesday**	**wednesday**}	RLDP スケジューリングを実行する曜日を設定します。
start *[HH:MM:SS]*	その日の RLDP スケジュールの開始時刻を設定します。
end *[HH:MM:SS]*	その日の RLDP スケジュールの終了時刻を設定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 16.12.1	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

例

次に、RLDP スケジューリングを実行する曜日を設定する例を示します。

```
Device(config)# wireless wps rogue ap rldp schedule day friday start 10:10:10 end 15:15:15
```

wireless wps rogue ap timeout

不正 AP の期限切れ時間（秒単位）を設定するには、**wireless wps rogue ap timeout** コマンドを使用します。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。

wireless wps rogue ap timeout *240-3600*

no wireless wps rogue ap timeout *240-3600*

構文の説明

rogue ap timeout	不正 AP の期限切れ時間（秒単位）を設定します。
240-3600	不正エントリがフラッシュされるまでの秒数を指定します。

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 Gibraltar 16.12.1	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

例

次に、不正 AP の期限切れ時間（秒単位）を設定する例を示します。

```
Device(config)# wireless wps rogue ap timeout 250
```

wireless wps rogue auto-contain

自動封じ込めレベルを設定し、モニター AP モードの自動封じ込めを設定するには、**wireless wps rogue auto-contain** コマンドを使用します。この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。

wireless wps rogue auto-contain { **level** *1 - 4* | **monitor-ap-only** }

no wireless wps rogue auto-contain { **level** *1 - 4* | **monitor-ap-only** }

構文の説明

auto-contain	不正なデバイスの自動封じ込めを設定します。
level	自動封じ込めレベルを設定します。
1 - 4	自動封じ込めレベルを指定します。
monitor-ap-only	モニターAPモードの自動封じ込めを設定します。

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 Gibraltar 16.12.1	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

例

次に、自動封じ込めレベルを設定し、モニター AP モードの自動封じ込めを設定する例を示します。

```
Device(config)# wireless wps rogue auto-contain level 2
Device(config)# wireless wps rogue auto-contain monitor-ap-only
```

wireless wps rogue client aaa

不正クライアントの有効な MAC アドレスを検出するための AAA またはローカルデータベースの使用を設定するには、**wireless wps rogue client aaa** コマンドを使用します。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。

wireless wps rogue client aaa

no wireless wps rogue client aaa

構文の説明

aaa	不正クライアントの有効な MAC アドレスを検出するための AAA またはローカルデータベースの使用を設定します。

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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 16.12.1	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

例

次に、不正クライアントの有効な MAC アドレスを検出するための AAA またはローカルデータベースの使用を設定する例を示します。

```
Device(config)# wireless wps rogue client aaa
```

wireless wps rogue client mse

不正クライアントの有効な MAC アドレスを検出するためのモビリティサービスエンジン（MSE）を設定するには、**wireless wps rogue client mse** コマンドを使用します。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。

wireless wps rogue client mse

no wireless wps rogue client mse

構文の説明

mse	不正クライアントの有効なMACアドレスを検出するためのMSE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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 16.12.1	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

例

次に、不正クライアントの有効な MAC アドレスを検出するためのモビリティサービスエンジン（MSE）を設定する例を示します。

```
Device(config)# wireless wps rogue client mse
```

wireless wps rogue client client-threshold

不正 AP SNMP トラップしきい値ごとに不正クライアントを設定するには、**wireless wps rogue client client-threshold** コマンドを使用します。この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。

wireless wps rogue client client-threshold *0 - 256*

no wireless wps rogue client client-threshold *0 - 256*

構文の説明

rogue client	不正クライアントを設定します。
client-threshold	不正 AP SNMP トラップしきい値ごとに不正なクライアントを設定します。
0 - 256	クライアントしきい値を指定します。

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 Gibraltar 16.12.1	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

例

次に、不正 AP SNMP トラップしきい値ごとに不正クライアントを設定する例を示します。

```
Device(config)# wireless wps rogue ap timeout 250
```

wireless wps rogue client notify-min-rssi

不正クライアントの最小 RSSI 通知しきい値を設定するには、**wireless wps rogue client notify-min-rssi** コマンドを使用します。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。

wireless wps rogue client notify-min-rssi *-128 - -70*

no wireless wps rogue client notify-min-rssi *-128 - -70*

構文の説明

rogue clients	不正クライアントを設定します。
notify-min-rssi	不正なクライアントの最小RSSI通知しきい値を設定します。
-128 - -70	RSSI しきい値をデシベル単位で指定します。

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 Gibraltar 16.12.1	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

例

次に、不正クライアントの最小 RSSI 通知しきい値を設定する例を示します。

```
Device(config)# wireless wps rogue client notify-min-rssi -125
```

wireless wps rogue client notify-rssi-deviation

不正クライアントの RSSI 偏差通知しきい値を設定するには、**wireless wps rogue client notify-rssi-deviation** コマンドを使用します。この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。

wireless wps rogue client notify-rssi-deviation *0 - 10*

no wireless wps rogue client notify-rssi-deviation *0 - 10*

構文の説明

notify-rssi-deviation	不正なクライアントのRSSI偏差通知しきい値を設定します。
0 - 10	RSSI しきい値をデシベル単位で指定します。

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 Gibraltar 16.12.1	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

例

次に、不正クライアントの RSSI 偏差通知しきい値を設定する例を示します。

```
Device(config)# wireless wps rogue client notify-rssi-deviation 6
```

wireless wps rogue detection

さまざまな不正検出パラメータを設定するには、 **wireless wps rogue detection** コマンドを使用します。

wireless wps rogue detection [{**min-rssi** *rssi* | **min-transient-time** *transtime*}]

構文の説明

min-rssi *rssi*	不正に必要な最小RSSI値を設定します。これは、APが不正を検出し、deviceで不正エントリが作成されるために必要な値です。
min-transient-time *transtime*	不正が初めてスキャンされた後、APで不正スキャンを定期的に実行する間隔を入力します。

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 Gibraltar 16.10.1	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、不正検出のための最小RSSI値と、一時的な定期的スキャンの最小間隔を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless wps rogue detection min-rssi 100
デバイス(config)# wireless wps rogue detection min-transient-time 500
デバイス(config)# end
```

wireless wps rogue notify-syslog

不正イベントの syslog 通知を有効にするには、**wireless wps rogue notify-syslog** コマンドを使用します。

wireless wps rogue notify-syslog

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

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、不正イベントの syslog 通知を有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue notify-syslog
```

wireless wps rogue rule

不正分類ルールを設定するには、 **wireless wps rogue rule** コマンドを使用します。

wireless wps rogue rule *rule-name* **priority** *priority* {**classify**{**friendly** | **malicious**} | **condition** {**client-count number** | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**} | **default** | **exit** | **match**{**all** | **any**} | **no** | **shutdown**}

構文の説明

rule *rule-name*	ルール名を指定します。
priority *priority*	特定のルールの優先順位を変更し、それに応じて、リスト内のその他のルールの優先順位を調整します。
classify	ルールの分類を指定します。
friendly	ルールを危険性のないルールとして分類します。
malicious	ルールを悪意のあるルールとして分類します。
condition {**client-count number** | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**}	不正なアクセス ポイントが満たす必要のあるルールに条件を指定します。 設定する条件のタイプ。条件タイプは以下のとおりです。 • client-count：最小数のクライアントが不正なアクセス ポイントにアソシエートされていることが条件となります。有効な範囲は 1 ～ 10 です。 • duration：不正なアクセス ポイントが最短期間で検出されることが条件となります。有効な範囲は 0 ～ 3600 秒です。 • encryption：アドバタイズされた WLAN で暗号化が無効になっている必要があります。 • infrastructure：SSID がコントローラで認識されている必要があります • rssi：不正なアクセス ポイントには、最小の RSSI 値が必要です。範囲は、–95 ～ -50 dBm です。 • ssid：不正なアクセス ポイントには、特定の SSID が必要です。
default	コマンドをデフォルトに設定します。
exit	サブモードを終了します。
match {**all** | **any**}	ルールの一致基準を設定します。検出された不正なアクセス ポイントがルールに一致していると見なされ、そのルールの分類タイプが適用されるためには、ルールで定義されているすべての条件を満たす必要があるか、一部の条件を満たす必要があるかを指定します。
no	コマンドを無効にするか、デフォルト値を設定します。

shutdown	システムをシャットダウンします。

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 Gibraltar 16.10.1	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、不正アクセス ポイントを Friendly として組織および表示できるルールを作成する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless wps rogue rule ap1 priority 1
デバイス(config-rule)# classify friendly
デバイス(config)# end
```

wireless wps rogue scale mode hybrid

不正スケールのハイブリッドモード（優先順位の高い不正 AP 用に予約された未使用のクォータは、スペースが利用可能な場合、優先順位の低い不正 AP によって使用できます）を設定するには、**wireless wps rogue scale mode hybrid** コマンドを使用します。この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。

wireless wps rogue scale mode hybrid

no wireless wps rogue scale mode hybrid

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

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、不正スケールのハイブリッドモードを設定する例を示します。

```
Device(config)# wireless wps rogue scale mode hybrid
```

wireless wps rogue scale priority

不正分類の優先順位を設定するには、**wireless wps rogue scale priority malicious** コマンドを使用します。この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。

wireless wps rogue scale priority malicious { **high** | **highest** | **low** | **medium** } **custom** { **high** | **highest** | **low** | **medium** } **unclassified** { **high** | **highest** | **low** | **medium** } **friendly** { **high** | **highest** | **low** | **medium** }

no wireless wps rogue scale priority malicious { **high** | **highest** | **low** | **medium** } **custom** { **high** | **highest** | **low** | **medium** } **unclassified** { **high** | **highest** | **low** | **medium** } **friendly** { **high** | **highest** | **low** | **medium** }

構文の説明

malicious	悪意のある不正 AP の優先順位を設定します。
{ **high** | **highest** | **low** | **medium** }	不正 AP ストレージの優先順位を、高、最高、中、低として示します。
custom	カスタム分類された不正 AP の優先順位を設定します。
unclassified	未分類の不正 AP の優先順位を設定します。
friendly	危険性のない不正 AP の優先順位を設定します。

コマンド デフォルト

なし

Malicious のデフォルト値は **highest**、Custom のデフォルト値は **high**、Unclassified のデフォルト値は **medium**、Friendly のデフォルト値は **low** 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 Cupertino 17.9.1	このコマンドが導入されました。

例

次に、不正分類の優先順位を設定する例を示します。

```
Device(config)# wireless wps rogue scale priority malicious highest custom high
unclassified medium friendly low
```

wireless wps rogue scale quota

最大スケールの不正 AP の優先順位付けとクォータを設定するには、**wireless wps rogue scale quota** コマンドを使用します。この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。

wireless wps rogue scale quota malicious *percentage-malicious-rogue-AP* **custom** *percentage-custom-rogue-AP* **unclassified** *percentage-unclassified-rogue-AP* **friendly** *percentage-friendly-rogue-AP*

no wireless wps rogue scale quota malicious *percentage-malicious-rogue-AP* **custom** *percentage-custom-rogue-AP* **unclassified** *percentage-unclassified-rogue-AP* **friendly** *percentage-friendly-rogue-AP*

構文の説明

malicious	悪意のある不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージを示します。
percentage-malicious-rogue-AP	悪意のある不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージで値を指定します。値の範囲は 0 ～ 100 です。
custom	カスタム不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージを示します。
percentage-custom-rogue-AP	カスタム不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージで値を指定します。値の範囲は 0 ～ 100 です。
unclassified	未分類の不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージを示します。
percentage-unclassified-rogue-AP	未分類の不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージで値を指定します。値の範囲は 0 ～ 100 です。
friendly	危険性のない不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージを示します。
percentage-friendly-rogue-AP	危険性のない不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージで値を指定します。値の範囲は 0 ～ 100 です。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、最大スケールの不正 AP の優先順位付けとクォータを設定する例を示します。

```
Device(config)# wireless wps rogue scale quota malicious 5 custom 10 unclassified 3
friendly 5
```

wireless wps rogue security-level

ワイヤレス WPS の不正検出セキュリティレベルを設定するには、**wireless wps rogue security-level** コマンドを使用します。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。

wireless wps rogue security-level { **critical** | **custom** | **high** | **low** }

no wireless wps rogue security-level { **critical** | **custom** | **high** | **low** }

構文の説明

rogue security-level	不正検出セキュリティ レベルを設定します。
critical	機密性の高い展開向けの不正検出設定を指定します。
custom	カスタマイズ可能なセキュリティレベルを指定します。
high	中規模な展開向けの不正検出設定を指定します。
low	小規模な展開向けの基本不正検出設定を指定します。

コマンド デフォルト

なし

コマンド モード

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 Gibraltar 16.12.1	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

例

次に、ワイヤレス WPS の不正検出セキュリティレベルを設定する例を示します。

```
Device(config)# wireless wps rogue security-level critical
```

wireless-default radius server

複数の RADIUS サーバーを設定するには、**wireless-default radius server** コマンドを使用します。

wireless-default radius server *IP* **key** *secret*

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

このユーティリティを使用すると、最大 10 の RADIUS サーバーを設定できます。

例

次に、複数の RADIUS サーバーを設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless-default radius server 9.2.58.90 key cisco123
デバイス(config)# end
```

wlan policy

ポリシー プロファイルを WLAN プロファイルにマッピングするには、 **wlan policy** コマンドを使用します。

wlan *wlan-name* **policy** *policy-name*

構文の説明

wlan-name	WLAN プロファイルの名前。
policy	ポリシープロファイルを WLAN プロファイルにマッピングします。
policy-name	ポリシー 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

config-policy-tag

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

wmm

WLAN での WMM を設定するには、**wmm** コマンドを使用します。この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。

wmm {**allowed** | **require**}

[no] wmm

構文の説明

wmm	WMM（WME）を設定します。
allowed	WLAN での WMM の使用を許可します。
require	WLAN 上に WMM クライアントが必要です。

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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、WLAN での WMM を設定する例を示します。

```
Device(config-wlan)#wmm allowed
```

show コマンド

show aaa dead-criteria radius

RADIUS サーバーのデッドサーバー検出情報を確認するには、**show aaa dead-criteria radius** コマンドを使用します。

show aaa dead-criteria radius *ipaddr* **auth-port** *authport* **acct-port** *acctport*

構文の説明

ipaddr	IP アドレス。
authport	認証ポート。
acctport	アカウンティングポート。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

show aaa dead-criteria radius *ipaddr* コマンドは、デフォルトのポートが使用されている場合にのみ出力を表示します。デフォルト以外のポートの場合は、**show aaa dead-criteria radius** *ipaddr* **auth-port** *authport* **acct-port** *acctport* コマンドを使用します。

例

次に、デフォルト以外の認証ポートとアカウンティングポートを使用しているRADIUSサーバーのデッドサーバー検出情報を表示する例を示します。

```
Device# show aaa dead-criteria radius 4.4.4.4 auth-port 4444 acct-port 3333

RADIUS: No server group specified. Using radius
RADIUS Server Dead Criteria:
============================
Server Details:
Address : 4.4.4.4
Auth Port : 4444
Acct Port : 3333
Server Group : radius
Dead Criteria Details:
Configured Retransmits : 3
Configured Timeout : 5
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Dead Detect Time : 10s
Computed Retransmit Tries: 10
Statistics Gathered Since Last Successful Transaction
=====================================================
```

```
Max Computed Outstanding Transactions: 0
Max Computed Dead Detect Time: 0s
Max Computed Retransmits : 0
```

次に、デフォルトポートを使用している RADIUS サーバーのデッドサーバー検出情報を表示する例を示します。

```
Device# show aaa dead-criteria radius 9.3.13.37

RADIUS: No server group specified. Using radius
RADIUS Server Dead Criteria:
============================
Server Details:
Address : 9.3.13.37
Auth Port : 1812
Acct Port : 1813
Server Group : radius
Dead Criteria Details:
Configured Retransmits : 3
Configured Timeout : 30
Estimated Outstanding Access Transactions: 1
Estimated Outstanding Accounting Transactions: 0
Dead Detect Time : 10s
Computed Retransmit Tries: 10
Statistics Gathered Since Last Successful Transaction
=====================================================
Max Computed Outstanding Transactions: 4
Max Computed Dead Detect Time: 48s
Max Computed Retransmits : 30
```

show aaa servers

AAA サーバーの MIB によって解釈された、パブリックおよびプライベートのすべての認証、許可、およびアカウンティング（AAA）RADIUS サーバーとの間で送受信されたパケットのステータスと数を表示するには、**show aaa servers** コマンドを使用します。

show aaa servers [private | public]

構文の説明

private	（任意）AAA サーバーの MIB によっても表示される、プライベート AAA サーバーのみを表示します。
private	（任意）AAA サーバーの MIB によっても表示される、パブリック AAA サーバーのみを表示します。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

show aaa servers コマンドでサポートされるのは、RADIUS サーバーのみです。

例

次のコマンドにより、すべての AAA トランザクションタイプ（認証、許可、およびアカウンティング）で送受信されたパケットに関する情報が表示されます。

```
Device# show aaa servers

RADIUS: id 2, priority 1, host 124.2.2.12, auth-port 1645, acct-port 1612, hostname rsim

     State: current UP, duration 20699s, previous duration 0s
     Dead: total time 0s, count 0
     Platform State from SMD: current UP, duration 20699s, previous duration 0s
     SMD Platform Dead: total time 0s, count 0
     Platform State from WNCD (1) : current UP
     Platform State from WNCD (2) : current UP
     Platform State from WNCD (3) : current UP
     Platform State from WNCD (4) : current UP
     Platform State from WNCD (5) : current UP
     Platform State from WNCD (6) : current UP
     Platform State from WNCD (7) : current UP
     Platform State from WNCD (8) : current UP, duration 964s, previous duration 0s
     Platform Dead: total time 0s, count 0UP
     Quarantined: No
.
.
.
```

```
Elapsed time since counters last cleared: 5h44m
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
Consecutive Response Failures: total 0
        SMD Platform : max 0, current 0 total 0
        WNCD Platform: max 0, current 0 total 0
        IOSD Platform : max 0, current 0 total 0
Consecutive Timeouts: total 0
        SMD Platform : max 0, current 0 total 0
        WNCD Platform: max 0, current 0 total 0
        IOSD Platform : max 0, current 0 total 0
Requests per minute past 24 hours:
        high - 5 hours, 44 minutes ago: 0
        low  - 5 hours, 44 minutes ago: 0
        average: 0
```

show aaa server brief

認証、許可、およびアカウンティング（AAA）サーバーの概要情報を表示するには、**show aaa server brief** コマンドを使用します。

show aaa server brief

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 Dublin 17.11.1	このコマンドが導入されました。

例

次に、AAA サーバーの概要情報を表示する例を示します。

```
Device# show aaa server brief

Access            Access   Access Access   Outstndg Acct.  Acct.  Acct.     Outstndg
Total    Reqs        Total Resp  Uptime  Uptime  Uptime
                  Requests Accept Reject   timeouts Access tx Req Responses timeouts
Acct. tx (Auth+Acct) (Auth+Acct) (IOSD)  (SMD)   (WNCD)
------------------------------------------------------------------------------------------
rsim              0        0      0        0        0      0      0         0
0        0            0           2372790 2372790 964
R1                0        0      0        0        0      0      0         0
0        0            0           2372790 2372790 964
free-radius-aut
hc-server         0        0      0        0        0      0      0         0
0        0            0           2372790 2372790 964
cisco-dnac-auth
z-server          0        0      0        0        0      0      0         0
0        0            0           2372790 2372790 964
r1                0        0      0        0        0      0      0         0
0        0            0           2372790 2372790 964
ise               0        0      0        0        0      0      0         0
0        0            0           2372790 2372790 964
Radius-2          0        0      0        0        0      0      0         0
0        0            0           2274176 2274176 296805
```

show access-list

デバイスに設定されたアクセス制御リスト（ACL）を表示するには、特権EXECモードで**show access-lists** コマンドを使用します。

show access-lists[{*namenumber* | **hardware counters** | **ipc**}]

構文の説明

number	（任意）ACL の番号です。範囲は 1 ～ 2799 です。
name	（任意）ACL の名前です。
hardware counters	（任意）アクセスリストのハードウェアカウンタを表示します。
ipc	（任意）プロセス間通信（IPC）プロトコル アクセス リスト コンフィギュレーションのダウンロード情報を表示します

コマンド デフォルト

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 Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

rate-limit キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません

デバイスは IP 標準および拡張アクセスリストだけをサポートします。したがって、許可される数値は、1 ～ 199 と 1300 ～ 2799 だけです。

このコマンドでは、設定された MAC ACL も表示します。

次に、**show access-lists** コマンドの出力例を示します。

```
Device# show access-lists

Extended IP access list 103
    10 permit ip any any dscp af11
Extended IP access list ssm-range
    10 deny ip any 232.0.0.0 0.255.255.255
    20 permit ip any any
Extended MAC access list mac1
```

次に、**show access-lists hardware counters** コマンドの出力例を示します。

```
Device# show access-lists hardware counters
 L3 ACL INPUT Statistics
     All  Drop:                      frame count: 0
     All  Bridge Only:               frame count: 0
```

```
    All  Forwarding To CPU:         frame count: 294674
    All  Forwarded:                 frame count: 2577677
    All  Drop And Log:              frame count: 0
    All  Bridge Only And Log:       frame count: 0
    All  Forwarded And Log:         frame count: 0
    All  IPv6 Drop:                 frame count: 0
    All  IPv6 Bridge Only:          frame count: 0
    All  IPv6 Forwarding To CPU:    frame count: 0
    All  IPv6 Forwarded:            frame count: 102
    All  IPv6 Drop And Log:         frame count: 0
    All  IPv6 Bridge Only And Log: frame count: 0
    All  IPv6 Forwarded And Log:    frame count: 0

L3 ACL OUTPUT Statistics
    All  Drop:                      frame count: 0
    All  Bridge Only:               frame count: 0
    All  Forwarding To CPU:         frame count: 0
    All  Forwarded:                 frame count: 266050
    All  Drop And Log:              frame count: 0
    All  Bridge Only And Log:       frame count: 0
    All  Forwarded And Log:         frame count: 0
    All  IPv6 Drop:                 frame count: 0
    All  IPv6 Bridge Only:          frame count: 0
    All  IPv6 Forwarding To CPU:    frame count: 0
    All  IPv6 Forwarded:            frame count: 0
    All  IPv6 Drop And Log:         frame count: 0
    All  IPv6 Bridge Only And Log: frame count: 0
    All  IPv6 Forwarded And Log:    frame count: 0
```

show ap name icap subscription ap rf spectrum

対応する AP のスペクトル設定の詳細を表示するには、**show ap name icap subscription ap rf spectrum** コマンドを使用します。

show ap name *ap_name***icap subscription ap rf spectrum**

構文の説明

ap_name	AP 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 Gibraltar 17.2.1	このコマンドが導入されました。

例

次に、AP のスペクトル解析を表示する例を示します。

```
Device# show ap name 4800AP icap subscription ap rf spectrum
Per-AP ICap configuration

AP RF spectrum subscription
  State                     : enabled
  Radio slots               : none
```

show ap airtime-fairness summary

すべての無線の ATF 設定のサマリーを表示するには、**show ap airtime-fairness summary** コマンドを使用します。

show ap airtime-fairness summary

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、すべての無線の ATF 設定のサマリーを表示する例を示します。

```
デバイス# show ap airtime-fairness summary
```

show ap audit-report detail

AP の設定を表示するには、**show ap** *ap-name* **audit-report detail** コマンドを使用します。

show ap *ap-name* **audit-report detail**

構文の説明

ap-name	AP 名。
detail	AP の監査レポートを表示します。

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 Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、AP の監査レポートを表示する例を示します。

```
Device# show ap Cisco-AP audit-report detail
Cisco AP Name   : Cisco-AP
================================================

Radio Audit Report:

Slot   Channel   Bandwidth   Tx Power   Admin State        Operation State   Radio Role
   Radio Operation
-------------------------------------------------------------------------------------------------
0          IN_SYNC   IN_SYNC    IN_SYNC    OUT_OF_SYNC     IN_SYNC              IN_SYNC
      IN_SYNC
1          IN_SYNC   IN_SYNC    IN_SYNC    OUT_OF_SYNC     IN_SYNC              IN_SYNC
      IN_SYNC

WLAN Audit Report:

Slot-id Wlan-id Vlan           State                    SSID        Auth Type     Flags
-------------------------------------------------------------------------------------------------
0           1            IN_SYNC    OUT_OF_SYNC IN_SYNC    IN_SYNC    IN_SYNC
0           2            IN_SYNC    OUT_OF_SYNC IN_SYNC    IN_SYNC    IN_SYNC
1           1            IN_SYNC    OUT_OF_SYNC IN_SYNC    IN_SYNC    IN_SYNC
1           2            IN_SYNC    OUT_OF_SYNC IN_SYNC    IN_SYNC    IN_SYNC
```

show ap audit-report summary

AP の監査レポートの概要を表示するには、**show ap audit-report summary** コマンドを使用します。

show ap audit-report summary

構文の説明

このコマンドには、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 Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、AP の監査レポートの概要を表示する例を示します。

```
Device# show ap audit-report summary
WTP Mac                    Radio                    Wlan                  IPv4 Acl
   IPv6 Acl       Last Report Time
-------------------------------------------------------------------------------
1880.90fd.6b40   OUT_OF_SYNC    OUT_OF_SYNC    IN_SYNC        IN_SYNC        01/01/1970
 05:30:00 IST
```

show ap auth-list

アクセス ポイントの認証リストを表示するには、**show ap auth-list** コマンドを使用します。

show ap auth-list ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）。
active R0	ルートプロセッサ スロット 0 のアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 のスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、アクセス ポイントの認証リストを表示する例を示します。

```
Device# show ap auth-list
```

show ap auth-list ap-cert-policy

AP が AP 証明書ポリシーによって承認されているかどうかを確認するには、**show ap auth-list ap-cert-policy** を使用します

show ap auth-list ap-cert-policy

構文の説明

このコマンドには、引数はありません。

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 Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、AP が AP 証明書ポリシーによって承認されているかどうかを確認する例を示します。

```
Device# show ap auth-list ap-cert-policy
```

show ap 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 auto-rf** コマンドを使用します。

show ap auto-rf dot11 {**24ghz** | **5ghz** | **dual-band**} *cisco_ap*

構文の説明

24ghz	802.11b AP を指定します。
5ghz	802.11a AP を指定します。
dual-band	デュアルバンドを指定します。

コマンド デフォルト

なし

使用上のガイドライン

show ap auto-rf コマンドの出力には、ネイバー AP 名は表示されません。

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。

```
Device# show ap auto-rf dot11 24ghz AP1

######################################################################

Number of Slots                                 : 3
AP Name                                         : APA023.9FD8.EA22
MAC Address                                     : 40ce.24bf.8ca0
Ethernet MAC Address                            : a023.9fd8.ea22
  Slot ID                                       : 0
  Radio Type                                    : 802.11n - 2.4 GHz
  Current TX/RX Band                            : 2.4Ghz band
  Subband Type                                  : All
  Noise Information
    Noise Profile                               : Passed
    Channel   1                                 :  -91 dBm
    Channel   2                                 :  -67 dBm
    Channel   3                                 :  -54 dBm
    Channel   4                                 :  -55 dBm
    Channel   5                                 :  -71 dBm
    Channel   6                                 :  -85 dBm
    Channel   7                                 :  -50 dBm
    Channel   8                                 :  -54 dBm
    Channel   9                                 :  -77 dBm
    Channel  10                                 :  -88 dBm
    Channel  11                                 :  -65 dBm
  Interference Information
    Interference Profile                        : Failed
    Channel   1                                 :  -47 dBm @ 21% busy
    Channel   2                                 :  -45 dBm @  2% busy
    Channel   3                                 : -128 dBm @  0% busy
    Channel   4                                 : -128 dBm @  0% busy
    Channel   5                                 :  -48 dBm @  2% busy
    Channel   6                                 :  -45 dBm @  2% busy
    Channel   7                                 :  -42 dBm @  3% busy
    Channel   8                                 : -128 dBm @  0% busy
    Channel   9                                 : -128 dBm @  0% busy
    Channel  10                                 :  -39 dBm @  3% busy
```

```
    Channel  11                                   :  -46 dBm @  3% busy
    Rogue Histogram (20)
      Channel   1                                 : 36
      Channel   2                                 :  0
      Channel   3                                 :  0
      Channel   4                                 :  1
      Channel   5                                 :  0
      Channel   6                                 : 11
      Channel   7                                 :  0
      Channel   8                                 :  1
      Channel   9                                 :  3
      Channel  10                                 :  0
      Channel  11                                 : 14
  Load Information
    Load Profile                                : Failed
    Receive Utilization                         : 0%
    Transmit Utilization                        : 0%
    Channel Utilization                         : 98%
    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 d0ec.3572.b9a0 slot 0                  :  -23 dBm on ( 11, 20 MHz) (181.22.0.22)

    AP 0c75.bdb3.9000 slot 0                  :  -28 dBm on ( 11, 20 MHz) (181.21.0.21)

    AP a4b2.3980.3740 slot 0                  :  -28 dBm on (  1, 20 MHz) (181.21.0.21)

    AP d0ec.3576.8320 slot 0                   :  -33 dBm on ( 11, 20 MHz) (50.1.1.122)

    AP a0f8.49dc.9780 slot 0                    :  -34 dBm on (  1, 20 MHz) (9.9.57.94)
    AP a0f8.49dc.8260 slot 0                    :  -34 dBm on (  6, 20 MHz) (9.9.57.94)
    AP d0ec.3573.7c80 slot 0                    :  -36 dBm on (  6, 20 MHz)
(192.185.183.44)
    AP 00b0.e192.9d20 slot 0                    :  -36 dBm on ( 11, 20 MHz) (9.9.42.47)
    AP a4b2.397f.41c0 slot 0                  :  -36 dBm on (  1, 20 MHz) (185.10.0.10)

    AP 2c5a.0fd5.b8c0 slot 0                    :  -36 dBm on (  6, 20 MHz) (9.7.97.51)
    AP a488.7351.4740 slot 0                    :  -36 dBm on ( 11, 20 MHz) (9.7.97.51)
    AP 10b3.d5e9.c8e0 slot 0                   :  -36 dBm on (  1, 20 MHz) (50.1.1.122)

    AP 0c75.bdb3.ab00 slot 0                  :  -37 dBm on (  6, 20 MHz) (185.10.0.10)

    AP 68ca.e451.5120 slot 0                   :  -37 dBm on (  1, 20 MHz) (9.4.155.15)
```

```
  AP a0f8.49dc.97a0 slot 0                    :  -37 dBm on ( 11, 20 MHz) (9.9.57.94)
  AP 188b.4501.7940 slot 0                    :  -38 dBm on ( 11, 20 MHz) (9.9.57.94)
  AP 002c.c88a.f8e0 slot 0                    :  -38 dBm on ( 11, 20 MHz) (9.9.50.55)
  AP 7069.5a78.4960 slot 0                    :  -38 dBm on ( 11, 20 MHz) (9.7.97.51)
  AP 3c41.0ea7.0880 slot 0                   :  -39 dBm on ( 11, 20 MHz) (185.10.0.10)

  AP a0f8.49dc.93a0 slot 0                    :  -39 dBm on (  6, 20 MHz) (9.9.57.94)
  AP f4db.e685.7360 slot 0                   :  -39 dBm on (  6, 20 MHz) (50.1.1.122)

  AP 7070.8bb4.4120 slot 0                    :  -40 dBm on ( 11, 20 MHz) (9.9.57.94)
  AP 707d.b93e.39e0 slot 0                    :  -40 dBm on (  1, 20 MHz) (4.4.4.1)
  AP 706d.150c.6860 slot 0                   :  -40 dBm on ( 11, 20 MHz) (50.1.1.122)

Radar Information
Channel Assignment Information via DCA
  Current Channel Average Energy               :  -50 dBm
  Previous Channel Average Energy              :  -50 dBm
  Channel Change Count                         : 9
  Last Channel Change Time                     : 02/14/2021 20:54:57
  Recommended Best Channel                     : 1
RF Parameter Recommendations
  Power Level                                  : 8
  RTS/CTS Threshold                            : 2347
  Fragmentation Threshold                      : 2346
  Antenna Pattern                              : 0
Persistent Interference Devices
Class Type                Channel  DC (%%)  RSSI (dBm)  Last Update Time
------------------------  -------  ------   ---------   ----------------
All third party trademarks are the property of their respective owners.
```

show ap ble cmx detail ip

特定の CMX の BLE 管理機能に関連するグローバル値を、その CMX に関連付けられているすべての AP とともに表示するには、**show ap ble cmx detail ip** コマンドを使用します。

show ap ble cmx detail ip *CMX-IP*

構文の説明

CMX-IP	IPv4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

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

次に、特定の CMX の BLE 管理機能に関連するグローバル値を、その CMX に関連付けられているすべての AP とともに表示する例を示します。

```
Device# show ap ble cmx detail ip 10.1.2.3
BLE administrative status: Up
BLE operational status: Up
Scanning interval: 10

  AP Name                          Interface             Status
  ------------------------------------------------------------------
  AP4001.7AB2.C39A                 Integrated            Open
```

show ap ble cmx summary

BLE 管理機能のために登録されたすべての CMX と、それらの BLE に関するグローバル値のリストを表示するには、**show ap ble cmx summary** コマンドを使用します。

show ap ble cmx 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 Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

次に、BLE 管理機能のために登録されたすべての CMX と、それらの BLE に関するグローバル値のリストを表示する例を示します。

```
Device# show ap ble cmx summary
CMX IP: 10.1.2.3
-----------------------
  BLE administrative status: Up
  BLE operational status: Up
  Scanning interval: 12

CMX IP: 10.1.2.4
-----------------------
  BLE administrative status: Down
  BLE operational status: Down
   Reason: BLE is administratively down
  Scanning interval: 0

CMX IP: 10.1.2.5
------------------
BLE administrative status: Up
BLE operational status: Down
 Reason: CMX is not subscribed to AP Monitor and RSSI services, or NMSP connection is
down
Scanning interval: 10
```

show ap ble summary

結合されている、BLE 管理機能をサポートする AP と、各 AP の BLE の詳細のリストを表示するには、**show ap ble summary** コマンドを使用します。

show ap ble 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 Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Cupertino 17.9.1	コマンドの出力が変更され、スキャンステータスを表示する新しい列が追加されました。

使用上のガイドライン

BLE管理機能が有効になり、APが表示されるのは、CMXがコントローラに登録されていて、CMX で BLE が有効になっている場合のみです。

次に、結合されている、BLE 管理機能をサポートする AP と、各 AP の BLE の詳細のリストを表示する例を示します。

```
Device# show ap ble summary
AP Name                          Interface             Status      CMX IP
-------------------------------------------------------------------------------
AP4001.7AB2.C39A                 Integrated            Open        10.1.2.3
AP4001.7AB2.C39B                 Integrated            Closed      10.1.2.4

Device# show ap ble summary

AP Name   AP Model     AP Ethernet MAC  BLE               BLE           BLE mode
BLE MAC         BLE Profile       BLE Scan
                                        Interface State   Admin State
_____________________________________________________________________________
AP794     C9130AXI-B   04eb.409e.xxxx   Open              Up            Base (Native)
806f.b031.xxxx  Eddystone URL     Enabled/Disabled
AP50      C9130AXI-B   04eb.409e.xxxx   Close             Down          Base (Native)
Unknown         Not Configured    Enabled/Disabled
AP28      C9136I       687d.b45c.xxxx   Close             Down          Base (Native)
Unknown         Not Configured    Enabled/Disabled
```

show ap config

device 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、 **show ap config** コマンドを使用します。

show ap config {**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 Gibraltar 16.10.1	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。

```
デバイス# show ap config global

AP global system logging host                   : 255.255.255.255
```

show ap config general

すべての Cisco AP の全般的な設定情報を表示するには、**show ap config general** コマンドを使用します。

show ap config general

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 Gibraltar 16.11.1	このコマンドが導入されました。

次に、すべての Cisco AP の全般的な設定情報を表示する例を示します。

```
Device# show ap config general

Cisco AP Name   : APA023.9FD8.EA22
================================================

AP image integrity
Time                                    : 07/22/2023 17:10:05
Alterative image loaded                 : Yes
Backup image status
Version                                 : 17.12.0.112
Partition                               : part1
Kernel                                  : Good
Root FS                                 : Good
IOX                                     : Good
Primary image status
Version                                 : 17.13.0.39
Partition                               : part2
Kernel                                  : Good
Root FS                                 : Good
IOX                                     : Good


!Output updated
```

show ap client-trace events all

AP クライアントのトレースイベント情報を表示するには、**show ap client-trace events all** コマンドを使用します。

show ap client-trace events 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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、AP クライアントのトレースイベント情報を表示する例を示します。

```
Device# show ap client-trace events all

[*04/29/2019 11:49:21.964964] [AP58AC.78DC.AAA0] [38:e6:0a:ea:99:d4] <apr1v0> [D:W]
DOT11_AUTHENTICATION : (.)
[*04/29/2019 11:49:21.972209] [AP58AC.78DC.AAA0] [38:e6:0a:ea:99:d4] <apr1v0> [U:W]
DOT11_ASSOC_REQUEST : (.)
[*04/29/2019 11:49:21.972227] [58:ac:78:df:6d:0f] [client] Vendor specific OUI: 00:50:f2
 and Type: 02
[*04/29/2019 11:49:21.975975] [AP58AC.78DC.AAA0] [38:e6:0a:ea:99:d4] <apr1v0> [D:W]
DOT11_ASSOC_RESPONSE : (.)
```

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、 **show ap crash-file** コマンドを使用します。

show ap crash-filechassis *chassis-number <1-2>***active standby**

構文の説明

chassis	シャーシの詳細を表示します。
chassis-number	シャーシ番号（1 または 2 のいずれか）を指定します。
active	アクティブインスタンスを指定します。
standby	スタンバイインスタンスを指定します。

コマンド デフォルト

なし

コマンド モード

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 Gibraltar 16.10.1	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。

```
デバイス# show ap crash-file
```

show ap dot11

802.11a または 802.11b または 6 GHz の設定情報を表示するには、 **show ap dot11** コマンドを使用します。

show ap dot11 { **24ghz** | **5ghz** | **6ghz** } { **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。
6ghz	6 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、6 GHz 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、6 GHz 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、6 GHz または 802.11b のメディアリソース予約コントロールの設定を表示します。
monitor	802.11a、6 GHz 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、6 GHz または 802.11b のネットワーク設定を表示します。
profile	802.11a、6 GHz 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、6 GHz または 802.11b レシーバの設定と統計を表示します。

service-policy	すべての Cisco アクセスポイントの 802.11a、6 GHz または 802.11b 無線に関する Quality of Service（QoS）サービスポリシーを表示します。
summary	802.11a、6 GHz 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概要を表示します。
txpower	802.11a、6 GHz または 802.11b の自動送信電力割り当てを表示します。
ccx global	deviceに結合されたすべての Cisco アクセスポイントに関する 802.11a、6 GHz 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 Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.12.2s	このコマンドが導入されました。
	load-info パラメータが追加されました。
Cisco IOS XE Cupertino 17.7.1	このコマンドは、6 GHz 帯域を含むように変更されました。

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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# show ap dot11 5ghz ccx global
 802.11a Client Beacon Measurements:
     disabled
```

show ap dot11

802.11 帯域パラメータを表示するには、 **show ap dot11** 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-stream rrc	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

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。

```
デバイス#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
```

show ap dot11 24ghz

2.4 GHz RRM パラメータを表示するには、 **show ap dot11 24ghz** 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 Gibraltar 16.10.1	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、802.11b カバレッジの設定と統計情報を表示する例を示します。

```
デバイス#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 24ghz SI config

2.4 GHz 帯域のスペクトル インテリジェンス（SI）設定の詳細を表示するには、**show ap dot11 24ghz SI config** コマンドを使用します。

show ap dot11 24ghz SI config ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）。
active R0	ルートプロセッサ スロット 0 の設定のアクティブ インスタンス。
standby R0	ルートプロセッサスロット 0 の設定のスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、2.4 GHz 帯域の SI 設定の詳細を表示する例を示します。

```
Device# show ap dot11 24ghz SI config chassis 1 R0
```

show ap dot11 24ghz SI device type

2.4 GHz 帯域のさまざまなタイプのスペクトル インテリジェンス（SI）干渉源の詳細を表示するには、**show ap dot11 24ghz SI device type** コマンドを使用します。

show ap dot11 24ghz SI device type {**cont_tx** | **mw_oven** | **si_fhss**} [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

構文の説明

cont_tx	2.4 GHz 帯域の連続トランスミッタ タイプの SI 干渉源。
mw_oven	2.4 GHz 帯域の電子レンジ タイプの SI 干渉源。
si_fhss	2.4 GHz 帯域の周波数ホッピング スペクトラム拡散タイプの SI 干渉源。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の設定のアクティブ インスタンス。
standby R0	ルートプロセッサスロット 0 の設定のスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、2.4 GHz 帯域の電子レンジ タイプの SI 干渉源の詳細を表示する例を示します。

```
Device# show ap dot11 24ghz SI device type mw_oven chassis 1 R0
```

show ap dot11 5ghz

5 GHz RRM パラメータを表示するには、 **show ap dot11 5ghz** 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 Gibraltar 16.10.1	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、802.11a チャネル割り当ての設定と統計情報の例を示します。

```
デバイス#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 24ghz cleanair air-quality

802.11 ネットワークの電波品質の概要情報および最も深刻な電波品質の情報を表示するには、**show ap dot11 cleanair** コマンドを使用します。

show ap dot11 {**24ghz** | **5ghz** | **dual-band**} **cleanair**{**air-quality** | **config** | **device** | **summary**}

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。
dual-band	802.11 デュアルバンド無線を表示します。
cleanair	CleanAir 設定を表示します。
air-quality	2.4GHz 帯域の CleanAir 電波品質（AQ）のデータを表示します。
device	2.4GHz 帯域のデバイスの CleanAir 干渉源を表示します。
config	2.4GHz 帯域の CleanAir 設定を表示します。
summary	すべての 802.11a Cisco AP の CleanAir 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 Gibraltar 16.10.1	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。

```
デバイス# 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。

```
デバイス# 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 24ghz 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、 **show ap dot11 cleanair air-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 Gibraltar 16.10.1	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。

```
デバイス# 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。

```
デバイス# 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、 **show ap dot11 cleanair config** 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 Gibraltar 16.10.1	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。

```
デバイス# 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
	このコマンドが導入されました。

show ap dot11 dual-band summary

デュアルバンド無線を使用するアクセス ポイントの概要を表示するには、**show ap dot11 dual-band summary** コマンドを使用します。

show ap dot11 dual-band 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 Gibraltar 16.12.1	このコマンドが導入されました。

例

次に、タグ名の概要を表示する例を示します。

```
Device# show ap dot11 dual-band summary
```

show ap environment

すべての AP の AP 環境情報を表示するには、**show ap environment** コマンドを使用します。

show ap environment ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP 環境情報を表示する例を示します。

```
Device# show ap environment
```

show ap file-transfer https summary

HTTPS を使用した AP ファイル転送の概要を表示するには、特権 EXEC モードで **show ap file-transfer https summary** コマンドを使用します。

show ap file-transfer https 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 Dublin 17.11.1	このコマンドが導入されました。

例

次に、HTTPS を使用した AP ファイル転送の概要を表示する例を示します。

```
Device# show ap file-transfer https summary

Configured port                 : 8443
Operational port                : 8443
```

show ap filters active

アクティブな AP フィルタの詳細を表示するには、**show ap filters active** コマンドを使用します。

show ap filters active ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）。
active R0	ルートプロセッサ スロット 0 のアクティブな AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 のアクティブな AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、アクティブ インスタンスについてアクティブな AP フィルタの詳細を表示する例を示します。

```
Device# show ap filters active chassis active R0
```

show ap filters active type priming

すべてのアクティブなプライミングフィルタのリストを表示するには、**show ap filters active type priming** コマンドを使用します。

show ap filters active type priming

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 Cupertino 17.9.2	このコマンドが導入されました。

例

次に、すべてのアクティブなプライミングフィルタのリストを表示する例を示します。

```
Device# show ap filters active type priming

Priority   Filter Name                        regex                                Priming
profile
-------------------------------------------------------------------------------------------------------

 0          FLR2                             *AP-FLOOR-2*                        AP-PRIMING-2

 1          FLR1                             *AP-FLOOR-1*                        AP-PRIMING-1
```

show ap filters all

すべての AP フィルタの詳細を表示するには、**show ap filters all** コマンドを使用します。

show ap filters all ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、アクティブ インスタンスについてすべての AP フィルタの詳細を表示する例を示します。

```
Device# show ap filters all chassis active R0
```

show ap filters all type priming

すべてのプライミングフィルタのリストを表示するには、**show ap filters all type priming** コマンドを使用します。

show ap filters all type priming

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 Cupertino 17.9.2	このコマンドが導入されました。

例

次に、すべてのプライミングフィルタのリストを表示する例を示します。

```
Device# show ap filters all type priming

Filter Name                     regex                                Priming profile

-------------------------------------------------------------------------------------------
FLR1                             *AP-FLOOR-1*                        AP-PRIMING-1

FLR2                             *AP-FLOOR-2*                        AP-PRIMING-2
```

show ap fra

AP のフレキシブル ラジオ アサインメント（FRA）サービスの設定を表示するには、**show ap fra** コマンドを使用します。

show ap fra ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）。
active R0	ルートプロセッサ スロット 0 のアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 のスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP の FRA 設定を表示する例を示します。

```
Device# show ap fra
```

show ap fra 5-6ghz

フレキシブル ラジオ アサインメント（FRA）の 5/6 GHz 設定を表示するには、**show ap fra 5-6ghz** コマンドを使用します。

show ap fra 5-6ghz

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 Cupertino 17.9.1	このコマンドが導入されました。

例

次に、フレキシブル ラジオ アサインメント（FRA）の 5/6 GHz 設定を表示する例を示します。

```
Device# show ap fra 5-6ghz
```

show ap geolocation ranging

AP の地理位置情報のレンジング情報を表示するには、**show ap geolocation ranging** {**report** | **request**} コマンドを使用します。

show ap geolocation ranging { **report** | **request** }

構文の説明

report	APの地理位置情報のレンジングレポートを表示します。
request	AP の地理位置情報のレンジング要求を表示します。

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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、AP の地理位置情報のレンジング情報を表示する例を示します。

```
Device# show ap geolocation ranging report
Device# show ap geolocation ranging request
```

show ap gps location

すべての AP の GPS 位置を表示するには、**show ap gps location** コマンドを使用します。

show ap gps location ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、すべての AP の GPS 位置を表示する例を示します。

```
Device# show ap gps location
```

show ap grpc summary

AP から Cisco DNA への GRPC チャネルのステータスの概要を表示するには、**show ap grpc summary** コマンドを使用します。

show ap grpc summary

構文の説明

このコマンドには、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 Amsterdam 17.3.1	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

例

次に、AP から Cisco DNA への GRPC チャネルのステータスの概要を表示する例を示します。

```
Device(config)# show ap grpc summary
```

show ap group hyperlocation

AP グループのハイパーロケーション設定のサマリーまたは詳細情報を表示するには、**show ap group** *ap-group-name* **hyperlocation** コマンドを使用します。

show ap group hyperlocation {**summary** | **detail**}

構文の説明

summary	AP グループの全体的な設定値（AP グループ固有）および動作ステータスとパラメータを表示します。
detail	AP グループの全体的な設定値（AP グループ固有）と AP ごとの設定値の両方および動作ステータスを表示します。リストされている AP は、AP グループに属するもののみです。

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 Denali 16.3.1	このコマンドが導入されました。

次に、AP グループのハイパーロケーション設定のサマリーを表示する例を示します。

```
Device# show ap group my-ap-group hyperlocation summary

Site Name: my-ap-group
Site Description: This is an AP group
Hyperlocation operational status: Up
Reason: N/A
Hyperlocation NTP server: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 11
Hyperlocation reset threshold: 9
```

（注） ハイパーロケーションの動作を可能にするには、次の条件を満たす必要があります。

- ハイパーロケーションが有効な Cisco CMX が 1 つ以上存在する
- ハイパーロケーション管理状態が動作可能である
- AP NTP または IOS NTP のいずれかが設定されている

次に、APグループのハイパーロケーション設定に関する詳細情報を表示する例を示します。

```
Device# show ap group my-ap-group hyperlocation detail

Site Name: my-ap-group
Site Description: This is an AP group
Hyperlocation operational status: Up
Reason: N/A
Hyperlocation NTP server: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 11
Hyperlocation reset threshold: 9

Values for APs in all AP Groups:

AP Name                 Radio MAC        Method    Hyperlocation
-----------------------------------------------------------------
APf07f.0635.2d40        f07f.0676.3b89   WSM       Enabled
APf4cf.e272.4ed0        f4cf.e223.ba31   Local     Enabled
```

show history channel interface dot11Radio all

チャネルの変更またはトリガーの理由と履歴を確認するには、**show history channel interface dot11Radio all** コマンドを使用します。

show history channel interface dot11Radio 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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、チャネルの変更またはトリガーの理由と履歴を確認する例を示します。

```
Device# show history channel interface dot11Radio all

               Timestamp Slot Client count Channel Trigger
Fri May 31 12:57:04 2019    0            0      11 RRM-DCA
Fri May 31 13:10:02 2019    0            0       1 RRM-DCA
Fri May 31 12:57:04 2019    1            0      60  Manual
Fri May 31 13:00:16 2019    1            0     149     DFS
```

show ap hyperlocation

ハイパーロケーション設定に関するサマリーまたは詳細情報を表示するには、**show ap hyperlocation** コマンドを使用します。

show ap hyperlocation {**summary** | **detail**}

構文の説明

summary	全体的な設定値と動作値を表示します。
detail	全体的な設定値と動作値、および各 AP 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。
Cisco IOS XE Denali 16.3.1	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

ハイパーロケーションの動作を可能にするには、次の条件を満たす必要があります。

- ハイパーロケーションが有効な Cisco Connected Mobile Experiences（CMX）が 1 つ以上存在している。
- ハイパーロケーション管理状態が動作可能になっている。
- AP Network Time Protocol（NTP）または IOS NTP のいずれかが設定されている。

例

次に、ハイパーロケーション設定のサマリーを表示する例を示します。

```
Device# show ap hyperlocation summary

Hyperlocation operational status: Up
Hyperlocation NTP server currently used: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8
```

次に、ハイパーロケーション設定に関する詳細情報を表示する例を示します。

```
Device# show ap hyperlocation detail
```

```
Hyperlocation operational status: Up
Hyperlocation NTP server currently used: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8

AP Name                 Radio MAC        Method    Hyperlocation
-----------------------------------------------------------------
AP84b8.0252.b930        84b8.0216.c721   HALO      Enabled
AP84b8.0265.5540        84b8.0243.8796   WSM       Enabled
APf07f.0635.2d40        f07f.0676.3b89   WSM       Enabled
APf4cf.e272.4ed0        f4cf.e223.ba31   HALO      Enabled
```

show ap hyperlocation cmx summary

ハイパーロケーションが有効になっている CMX の情報のサマリーを表示するには、**show ap hyperlocation cmx summary** コマンドを使用します。

show ap hyperlocation cmx summary ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ハイパーロケーションが有効になっている CMX の情報のサマリーを表示する例を示します。

```
Device# show ap hyperlocation cmx summary
```

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、 **show ap image** 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 Gibraltar 16.10.1	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。

```
デバイス# show ap image
```

show ap image file summary

アクセスポイント（AP）のソフトウェアインストールファイルの概要を表示するには、**show ap image file summary** コマンドを使用します。

show ap image file 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 Bengaluru 17.4.1	このコマンドが変更されました。

例

次に、APのソフトウェアインストールファイルのサマリーを表示する例を示します。

```
Device# show ap image file summary
AP Image Active List
============================
Install File Name: base_image.bin
--------------------------------
AP Image Type    Capwap Version Size (KB) Supported AP models
-------------------------------------------------------------------------------------------------------

     ap1g1       17.3.0.30       13300  NA

     ap1g2       17.3.0.30  34324       NA

     ap1g3       17.3.0.30  98549       AP803

    ap1g4       17.3.0.30        34324       AP1852E, AP1852I, AP1832I, AP1830I, AP1810W,
 OEAP1810

     ap1g5       17.3.0.30        23492       AP1815W, AP1815T, OEAP1815, AP1815I,
AP1800I, AP1800S, AP1815M, 1542D, AP1542I, AP1100AC, AP1101AC, AP1840I

     ap1g6       17.3.0.30  93472             AP2900I, C9117AXI

    ap1g6a       17.3.0.30   247377           C9130AXI, C9130AXE, C9140AXI, C9140AXD,
C9140AXT

     ap1g7       17.3.0.30   23988            AP1900I, C9115AXI, AP1900E, C9115AXE,
C9120AXE, C9120AXP, C9120AXI

     ap1g8       17.3.0.30   23473      C9105AXI, C9105AXW, C9110AXI, C9110AXE

     ap3g1       17.3.0.30   23422       NA

     ap3g2       17.3.0.30   23411  AP1702I
```

```
     ap3g3       17.3.0.30   23090  AP3802E, AP3802I, AP3802P, AP4800, AP2802E, AP2802I,
 AP2802H, AP3800, AP1562E, AP1562I, AP1562D, AP1562PS, IW-6300H-DC, IW-6300H-AC,
IW-6300H-DCW, ESW-6300

     c1570       17.3.0.30   13000  AP1572E, 1573E, AP1572I

     c3700      17.3.0.30   14032  AP3702E, AP3701E, AP3701I, AP3702I, AP3701P, AP3702P,
 AP2702E, AP2702I, AP3702, IW3702, AP3701, AP3700C

 virtApImg       17.3.0.30               177056       APVIRTUAL


AP Image Prepare List**
============================
Install File Name: base_image.bin
------------------------------
============================
Install File Name: base_image.bin
------------------------------
AP Image Type    Capwap Version Size (KB) Supported AP models
-------------------------------------------------------------------------------------

     ap1g1       17.3.0.30        13300  NA

     ap1g2       17.3.0.30  34324  NA

     ap1g3       17.3.0.30  98549  AP803

     ap1g4       17.3.0.30        34324  AP1852E, AP1852I, AP1832I, AP1830I, AP1810W,
OEAP1810

     ap1g5       17.3.0.30        23492  AP1815W, AP1815T, OEAP1815, AP1815I, AP1800I,
AP1800S, AP1815M, 1542D, AP1542I, AP1100AC, AP1101AC, AP1840I

     ap1g6       17.3.0.30  93472               AP2900I, C9117AXI

    ap1g6a       17.3.0.30  247377              C9130AXI, C9130AXE, C9140AXI, C9140AXD,
 C9140AXT

     ap1g7       17.3.0.30  23988                AP1900I, C9115AXI, AP1900E, C9115AXE,
C9120AXE, C9120AXP, C9120AXI

     ap1g8       17.3.0.30  23473    C9105AXI, C9105AXW, C9110AXI, C9110AXE

     ap3g1       17.3.0.30  23422     NA

     ap3g2       17.3.0.30  23411     AP1702I

    ap3g3      17.3.0.30  23090    AP3802E, AP3802I, AP3802P, AP4800, AP2802E, AP2802I,
 AP2802H, AP3800, AP1562E, AP1562I, AP1562D, AP1562PS, IW-6300H-DC, IW-6300H-AC,
IW-6300H-DCW, ESW-6300

     c1570       17.3.0.30  13000     AP1572E, 1573E, AP1572I

     c3700       17.3.0.30  14032     AP3702E, AP3701E, AP3701I, AP3702I, AP3701P,
AP3702P, AP2702E, AP2702I, AP3702, IW3702, AP3701, AP3700C

 virtApImg       17.3.0.30              177056     APVIRTUAL

**Difference of Active and Prepare list gives images being predownloaded to Access Points.
```

show ap image site summary

アクセス ポイント（AP）のサイトでフィルタリングされたアップグレードのサマリーを表示するには、**show ap image site summary** コマンドを使用します。

show ap image site 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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、APのサイトでフィルタリングされたアップグレードのサマリーを表示する例を示します。

```
Device# show ap image site summary

Image name: smu1.bin
Site Tag               Prepared              Activated             Committed
------------------------------------------------------------------------------------------------
BGL18                   yes                       ongoing               no
BGL17                   yes                       ongoing               no
```

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[{**chassis** |{*chassis-number* | **active** | **standby**} |**R0**}]

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）。
active R0	ルートプロセッサスロット 0 のアクティブインスタンス。
standby R0	ルートプロセッサスロット 0 のスタンバイインスタンス。

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 Gibraltar 16.10.1	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。

```
デバイス# show Cisco IOS XE Gibraltar 16.12.2s link-encryption
```

show ap lldp neighbors detail

AP がサードパーティ製スイッチに接続されている場合に、コントローラで AP Link Layer Discovery Protocol（LLDP）ネイバー情報の詳細を表示します。

show ap lldp neighbors detail

構文の説明

このコマンドには、引数はありません。

コマンド デフォルト

なし

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 Bengaluru 17.5.1	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

例

次に、AP がサードパーティ製スイッチに接続されている場合に、コントローラで AP Link Layer Discovery Protocol（LLDP）ネイバー情報の詳細を表示する例を示します。

```
Device# show ap lldp neighbors detail
Number of neighbors: 1
AP Name               : 9130-ap1
AP Interface          : GigabitEthernet0
-------------------------------------------------------
Neighbor MAC          : c89c.1db1.1f80
Neighbor Name         : flex-ctlr-switch
System Description    : Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M),
Version 15.2(4)E6, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 05-Apr-18 02:22 by prod_rel_team
Port ID               : Gi1/0/15
Port Description      : 9130-ap2
Chassis Alias         :
Management Addresses  :
  IPv4 address         : None
  IPv6 address         : None
Capabilities          :
  Bridge
  Router
Last updated time     : 12/02/2020 09:15:48
```

show ap lldp neighbors

AP がサードパーティ製スイッチに接続されている場合に、コントローラで AP Link Layer Discovery Protocol（LLDP）ネイバー情報を表示します。

show ap lldp neighbors

構文の説明

このコマンドには、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 Bengaluru 17.5.1	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

例

次に、AP がサードパーティ製スイッチに接続されている場合に、コントローラで AP Link Layer Discovery Protocol（LLDP）ネイバー情報を表示する例を示します。

```
Device# show ap lldp neighbors
Capability Codes:
     (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
     (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other


AP Name   AP Interface      Neighbor Name Neighbor MAC    Port ID    Mgmt. Address
Capabilities  Last updated time
-------------------------------------------------------------------------------------------------
9130-ap1  GigabitEthernet0  switch        cxxc.1dxx.1fxx  Gi1/0/15   None          B R
        12/02/2020 09:15:48

9117-ap1  GigabitEthernet0  switch        cxxc.1dxx.1fxx  Gi1/0/19   None          B R
        12/02/2020 09:15:47
```

show ap name dot11 neighbor summary

802.11 2.4 GHz、5 GHz、または 6 GHz ネットワーク内のアクセスポイント（AP）のネイバーの概要を表示するには、**show ap name** *ap-name* **dot11 {24ghz | 5ghz | 6ghz} neighbor summary** コマンドを使用します。

show ap name dot11 {24ghz | 5ghz | 6ghz} neighbor summary

構文の説明

ap-name	AP 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが導入されました。

例

次に、802.11 2.4 GHz パラメータのネイバーの概要を表示する例を示します。

```
Device# show ap name AP687D.B45C.0554 dot11 24ghz neighbor summary

BSSID             Channel Channel-width Slot  RSSI  Last-Heard           SSID
Neighbor
-------------------------------------------------------------------------------------------
10f9.2077.6140     1      20 Mhz        0    -28   06/23/2021 01:42:51  mdns-psk   TRUE
10f9.2077.614f     1      20 Mhz        0    -28   06/23/2021 01:42:51  mdns-psk   TRUE
00b0.e192.9600    11      20 Mhz        0    -31   06/23/2021 01:42:51  mdns-psk   TRUE
00b0.e192.960f    11      20 Mhz        0    -31   06/23/2021 01:42:51  mdns-psk   TRUE
00ee.ab18.bf0f     6      20 Mhz        0    -38   06/23/2021 01:42:51  mdns-psk   TRUE
f4db.e69f.8860     1      20 Mhz        0    -75   06/23/2021 01:43:06  wlan1      FALSE
68ca.e43f.b902     1      20 Mhz        0    -77   06/23/2021 01:43:06  amaz-open  FALSE
68ca.e43f.b900     1      20 Mhz        0    -78   06/23/2021 01:43:06  amaz-web   FALSE
68ca.e43f.b903     1      20 Mhz        0    -78   06/23/2021 01:43:06  amaz-8021x FALSE
```

次に、802.11 5 GHz パラメータのネイバーの概要を表示する例を示します。

```
Device# show ap name AP1117Q.B22U.0221 dot11 5ghz neighbor summary

BSSID          Channel  Channel-width  Slot RSSI Last-Heard          SSID     Neighbor
-------------------------------------------------------------------------------------

7872.5dee.496f  100      80 Mhz         1    34   6/23/2021 01:43:35 mdns-psk  FALSE
```

次に、802.11 6 GHz パラメータのネイバーの概要を表示する例を示します。

```
Device# show ap name AP1117Q.B22U.0221 dot11 6ghz neighbor summary

BSSID          Channel  Channel-width  Slot  RSSI  Last-Heard          SSID      Neighbor
-------------------------------------------------------------------------------------------

687d.b45e.4c53    1        20 Mhz        3   -37   06/23/2021 01:42:51  wpa3-6ghz  TRUE
687d.b45e.53d3    1        20 Mhz        3   -39   06/23/2021 01:42:51  wpa3-6ghz  TRUE
```

show ap name lldp neighbors detail

AP がサードパーティ製スイッチに接続されている場合に、特定の AP について、コントローラで AP Link Layer Discovery Protocol（LLDP）ネイバー情報の詳細を表示します。

show ap name *ap-name* **lldp neighbors detail**

構文の説明

このコマンドには、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 Bengaluru 17.5.1	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

例

次に、AP がサードパーティ製スイッチに接続されている場合に、特定の AP について、コントローラで AP Link Layer Discovery Protocol（LLDP）ネイバー情報の詳細を表示する例を示します。

```
Device# show ap name 9130-ap1 lldp neighbors detail
AP Name               : 9130-ap1
AP Interface          : GigabitEthernet0
-------------------------------------------------------
Neighbor MAC          : c89c.1db1.1f80
Neighbor Name         : flex-ctlr-switch
System Description    : Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M),
Version 15.2(4)E6, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 05-Apr-18 02:22 by prod_rel_team
Port ID               : Gi1/0/15
Port Description      : 9130-ap2
Chassis Alias         :
Management Addresses  :
  IPv4 address         : None
  IPv6 address         : None
Capabilities          :
  Bridge
  Router
Last updated time     : 12/02/2020 09:15:48
```

show ap name lldp neighbors

AP がサードパーティ製スイッチに接続されている場合に、特定の AP について、コントローラで AP Link Layer Discovery Protocol（LLDP）ネイバー情報を表示します。

show ap name *ap-name* **lldp neighbors**

構文の説明

このコマンドには、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 Bengaluru 17.5.1	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

例

次に、AP がサードパーティ製スイッチに接続されている場合に、特定の AP について、コントローラで AP Link Layer Discovery Protocol（LLDP）ネイバー情報を表示する例を示します。

```
Device# show ap name 9130-ap1 lldp neighbors
AP Name               : 9130-ap1
AP Interface          : GigabitEthernet0
-------------------------------------------------------
Neighbor MAC          : c89c.1db1.1f80
Neighbor Name         : flex-ctlr-switch
System Description    : Cisco IOS Software, C3750E Software (C3750E-UNIVERSALK9-M),
Version 15.2(4)E6, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018     by Cisco Systems, Inc.
Compiled Thu 05-Apr-18 02:22  02:22 by prod_rel_team
Port ID               : Gi1/0/15
Port Description      : 9130-ap2
Chassis Alias         :
Management Addresses  :
  IPv4 address         : None
  IPv6 address         : None
Capabilities          :
  Bridge
  Router
Last updated time     : 12/02/2020 09:15:48
```

show ap name mesh roam history

メッシュ AP のローミング履歴を表示するには、**show ap name** *cisco-ap-name* **mesh roam history** コマンドを使用します。

show ap name *cisco-ap-name* **mesh roam history**

構文の説明

cisco-ap-name	Cisco AP 名を指定します。

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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、メッシュ AP のローミング履歴を表示する例を示します。

```
Device# show ap name cisco-ap-name mesh roam history
```

show ap name ntp status

AP の Network Time Protocol（NTP）ステータスを表示するには、**show ap name ntp status** コマンドを使用します。

show ap name *ap-name* **ntp status**

構文の説明

ap-name	AP 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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、AP の NTP ステータスを表示する例を示します。

```
Device# show ap name AP-G1-230 ntp status

ap-name       enabled v4/v6 IPAddress       Status     Stratum LastSync  SyncOffset
AP-G1-230     Y       v4    198.51.100.5    AuthFail   4       1000      100
```

show ap ntp status

すべての AP の Network Time Protocol（NTP）ステータスを表示するには、**show ap name ntp status** コマンドを使用します。

show ap ntp status

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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、すべての AP の NTP ステータスを表示する例を示します。

```
Device# show ap ntp status

ap-name       enabled    v4/v6 IPAddress       Status   Stratum LastSync SyncOffset
AP-G1-230         Y      v4    198.51.100.5    AuthFail 2       Never
AP-G1-231         Y      v4    198.51.100.10   Synced   3       1000     100
AP-G1-232         Y      v4    198.51.100.15   Synced   16      2000     50
```

show ap master list

AP マスター リストを表示するには、 **show ap master list** コマンドを使用します。

show ap master list[{**chassis** |{*chassis-number* | **active** | **standby**} |**R0**}]

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）。
active R0	ルートプロセッサ スロット 0 のアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 のスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP マスター リストを表示する例を示します。

```
Device# show ap master list
```

show ap mesh cac access

特定の AP とそのメッシュ ツリーのアクセス無線でアクティブなコールの数を表示するには、**show ap mesh cac access** コマンドを使用します。

show ap *ap-name***mesh cac access**

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

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 Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

例

次に、特定の AP とそのメッシュ ツリーのアクセス無線でアクティブなコールの数を表示する例を示します。

```
Device# show ap <ap-name> mesh cac access

Depth   AP Name                           Slot  Radio      BW Used  Call
------  ---------------------------------  ----  ---------  -------  ----
0       AALUKKAL-1562-RAP                  0     802.11b/g  0        0
                                           1     802.11a    0        0
1       AP380E.4DBF.C6B0                   0     802.11b/g  1072     2
                                           1     802.11a    0        0
```

show ap mesh cac bwused voice

特定の AP とそのメッシュツリーの音声帯域幅使用率を表示するには、**show ap mesh cac bwused voice** コマンドを使用します。

show ap *ap-name***mesh cac bwused voice**

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

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 Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

例

次に、特定の AP とそのメッシュ ツリーの音声帯域幅使用率を表示する例を示します。

```
Device# show ap <ap-name> mesh cac bwused voice

Depth   AP Name                          Slot  Radio      BW Used
------  --------------------------------  ----  ---------  -------
1       APA023.9FA9.D920                  0     802.11b/g  1140
                                          1     802.11a    0
2       AP380E.4DBF.C80C                  0     802.11b/g  570
                                          1     802.11a    2144
2       AP380E.4DBF.C816                  0     802.11b/g  0
                                          1     802.11a    0
2       APA023.9FA9.B702                  0     802.11b/g  0
                                          1     802.11a    0
```

show ap mesh cac callpath

特定の AP とそのメッシュ ツリーのアクセスおよびバックホールのアクティブなコールの数を表示するには、**show ap mesh cac callpath** コマンドを使用します。

show ap *ap-name***mesh cac callpath**

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

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 Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

例

次に、特定の AP とそのメッシュ ツリーのアクセスおよびバックホールのアクティブなコールの数を表示する例を示します。

```
Device# show ap <ap-name> mesh cac callpath

Depth   AP Name                          Slot  Radio      Call
------  --------------------------------  ----  ---------  ----
1       APA023.9FA9.D920                  0     802.11b/g  2
                                          1     802.11a    0
2       AP380E.4DBF.C80C                  0     802.11b/g  0
                                          1     802.11a    2
2       AP380E.4DBF.C816                  0     802.11b/g  0
                                          1     802.11a    0
2       APA023.9FA9.B702                  0     802.11b/g  0
                                          1     802.11a    0
```

show ap mesh cac rejected

特定の AP とそのメッシュ ツリーのアクセスおよびバックホールの拒否コールの数を表示するには、**show ap mesh cac rejected** コマンドを使用します。

show ap *ap-name***mesh cac rejected**

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

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 Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

例

次に、特定の AP とそのメッシュ ツリーのアクセスおよびバックホールの拒否コールの数を表示する例を示します。

```
Device# show ap <ap-name> mesh cac rejected
```

show ap monitor-mode summary

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 Gibraltar 16.10.1	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。

```
デバイス# 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 multicast mom（マルチキャスト オーバー マルチキャスト）

AP が、CAPWAP マルチキャストグループを使用して、コントローラにより送信されたマルチキャスト間（mom）トラフィックを受信するかどうかを確認するには、**show ap multicast mom** コマンドを使用します。

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

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.2	このコマンドが導入されました。

次に、AP が、CAPWAP マルチキャストグループを使用して、コントローラにより送信されたマルチキャスト間トラフィックを受信するかどうかを確認する例を示します。

```
Device# show ap multicast mom

AP Name                      MOM-IP     TYPE MOM- STATUS
-------------------------------------------------------
SS-E-1                       IPv4             Up
SS-E-2                       IPv4             Up
9130E-r3-sw2-g1012           IPv4             Up
9115i-r3-sw2-te1-0-38        IPv4             Up
AP9120-r3-sw3-Gi1-0-46       IPv4             Up
ap3800i-r2-sw1-te2-0-2       IPv4             Up
```

show ap name *ap-name* neighbor summary

AP ネイバー情報の概要を表示するには、**show ap name** *ap-name* **neighbor summary** を使用します

show ap name *ap-name* **neighbor summary**

構文の説明

ap-name	ネイバーの概要が表示される AP 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、AP ネイバー情報を表示する例を示します。

```
Device#show ap name APXXXX.6DXX.59XX neighbor summary

BSSID                 Channel   Channel-width Slot       RSSI              Last-Heard
                         SSID                                          Neighbour
-------------------------------------------------------------------------------------------------------
0008.2f1c.8040        1         20 Mhz        0          -39               03/17/2020
 18:25:14                aprusty-un-dot1x                                 FALSE

0008.2f1c.8041        1         20 Mhz        0          -39               03/17/2020
 18:25:14                aprusty-sim-11                                   FALSE

0008.2f1c.8042        1         20 Mhz        0          -39               03/17/2020
 18:25:14                one-ph                                           FALSE

0008.2f1c.8044        1         20 Mhz        0          -38               03/17/2020
 18:25:14                aprusty-test                                     FALSE

0008.3296.f340        11        20 Mhz        0          -51               03/18/2020
 10:39:27                ewlc-ap-dot1x                                    FALSE

0008.3296.f341        11        20 Mhz        0          -49               03/18/2020
 10:39:27                vewlc_small_psk                                  FALSE

002a.1022.d950        1         20 Mhz        0          -57               03/17/2020
 18:25:14                ewlc-ap-dot1x                                    FALSE

002a.105c.bfd0        1         20 Mhz        0          -36               03/17/2020
 18:25:14                ewlc-ap-dot1x                                    FALSE

002a.105c.bfd1        1         20 Mhz        0          -37               03/17/2020
 18:25:14                vewlc_small_psk                                  FALSE
```

```
002c.c864.76d0        11        20 Mhz        0          -61              03/18/2020
 10:37:37                rajwlan                                 FALSE

BSSID                 Channel   Channel-width Slot       RSSI             Last-Heard
                         SSID                                 Neighbour
-------------------------------------------------------------------------------------------------
002c.c8de.59e0        1         20 Mhz        0          -48              03/17/2020
 18:25:14                WQ                                      FALSE

002c.c8de.5d80        11        20 Mhz        0          -54              03/18/2020
 10:39:27                ewlc-ap-dot1x                           FALSE

002c.c8de.5d81        11        20 Mhz        0          -55              03/18/2020
 10:39:27                vewlc_small_psk                         FALSE

002c.c8de.7260        11        20 Mhz        0          -53              03/18/2020
 10:39:27                ewlc-ap-dot1x                           FALSE

002c.c8de.7261        11        20 Mhz        0          -54              03/18/2020
 10:39:27                vewlc_small_psk                         FALSE

005d.7390.e1e0        1         20 Mhz        0          -54              03/17/2020
 18:25:14                rlan                                    FALSE

006b.f114.95a0        1         20 Mhz        0          -60              03/17/2020
 18:25:14                zavc                                    FALSE

006b.f114.b0e0        1         20 Mhz        0          -46              03/17/2020
 18:25:14                ewlc-ap-dot1x                           FALSE

006c.bc61.2340        1         20 Mhz        0          -63              03/17/2020
 18:24:44                dnac-swim                               FALSE

006c.bc72.5ce0        11        20 Mhz        0          -58              03/18/2020
 10:39:17                dnac-swim                               FALSE
```

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** | **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。
5ghz	5 GHz 帯域を表示します。
dual-band	デュアルバンドを表示します。

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 Gibraltar 16.10.1	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。

```
デバイス# 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 ble detail

BLE 管理の詳細を表示するには、**show ap name ble detail** コマンドを使用します。

show ap name *ap-name* **ble detail**

構文の説明

ap-name	AP 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	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

例

次に、BLE 管理の詳細を表示する例を示します。

```
Device(config)# show ap name ap-name ble detail
```

show ap name cablemodem

AP のケーブル モデム情報を表示するには、**show ap name** *ap name* **cablemodem** コマンドを使用します。

show ap name *ap-name* **cablemodem** ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

ap-name	AP の名前。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP のケーブル モデム情報を表示する例を示します。

```
Device# show ap name my-ap cablemodem
```

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 Gibraltar 16.10.1	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。

```
デバイス# 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。

```
デバイス# 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 slot

Cisco AP の設定を表示し、スロットの共通情報も表示するには、**show ap name config slot** コマンドを使用します。

show ap name *Cisco-ap-name* **slot** *0-3*

構文の説明

Cisco-ap-name	Cisco AP の名前を指定します。
0-3	スロット ID 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 Gibraltar 16.10.1	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スロットの共通情報を表示する例を示します。

```
Device# show ap name Cisco-ap-name config slot 3
```

show ap name config ethernet

AP のイーサネット関連の設定情報を表示するには、**show ap name** *ap-name* **config ethernet** コマンドを使用します。

show ap name *ap-name* **config ethernet** ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

ap-name	AP の名前。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP のイーサネット関連の設定情報を表示する例を示します。

```
Device# show ap name my-ap config ethernet
```

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** | **6ghz** } { **ccx** | **cdp** | **profile** | **service-policy output** | **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。
6ghz	6 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-policy output	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。
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。
SI	SI 設定を表示します。
airtime-fairness	24 Ghz または 5 Ghz または 6 GHz の Air Time Fairness の統計を表示します。
call-control	呼制御の情報を表示します。
radio-reset	無線のリセットを表示します。
slot	スロット情報を表示します。
voice	音声情報を表示します。

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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Cupertino 17.7.1	このコマンドは、6 GHz 帯域を含むように変更されました。

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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# show ap name AP01 dot11 24ghz tsm all
```

show ap name environment

AP の AP 環境情報を表示するには、**show ap name** *ap-name* **environment** コマンドを使用します。

show ap name *ap-name* **environment** ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

ap-name	AP の名前。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP の AP 環境情報を表示する例を示します。

```
Device# show ap name my-ap environment
```

show ap name gps location

AP の GPS 位置を表示するには、 **show ap name gps location** コマンドを使用します。

show ap name *ap-name* **gps location** [{*chassis-number* | **active** | **standby**}**R0**

構文の説明

ap-name	アクセス ポイントの名前
gps	Cisco AP の GPS 情報を表示します
location	メッシュ リンクテスト データを表示します
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 のアクティブな AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサスロット 0 の設定のスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP の GPS 位置を表示する例を示します。

```
Device# show ap name mesh-profile-name gps location
```

show ap name grpc detail

AP から Cisco DNA への gRPC チャネルの詳細なステータスを表示するには、**show ap name grpc detail** コマンドを使用します。

show ap name *ap-name* **grpc detail**

構文の説明

ap-name	AP 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	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

例

次に、AP から Cisco DNA への gRPC チャネルの詳細なステータスを表示する例を示します。

```
Device(config)# show ap name APXXXX.BXXX.FXXX grpc detail
```

show ap name hyperlocation

アクセスポイント（AP）のハイパーロケーション設定の概要または詳細情報を表示するには、**show ap name hyperlocation** コマンドを使用します。

show ap name *ap-name* **hyperlocation ble-beacon**

構文の説明

ap-name	アクセス ポイント名。
hyperlocation	APのハイパーロケーション情報を表示します。
ble-beacon	AP の BLE ビーコン設定を表示します。

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 Denali 16.3.1	このコマンドが導入されました。

例

次に、AP の BLE ビーコン設定を表示する例を示します。

```
デバイス# show ap name test-ap hyperlocation ble-beacon

ID  Major  Minor  TX Power(dBm)
------------------------------
0   0      0      0
1   0      0      0
2   0      0      0
3   0      0      0
```

show ap name mesh backhaul

AP のメッシュ バックホール統計情報を表示するには、**show ap name** *ap-name* **mesh backhaul** コマンドを使用します。

show ap name *ap-name* **mesh backhaul** ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP のメッシュ バックホール統計情報を表示する例を示します。

```
Device# show ap name mymeshap mesh backhaul
```

show ap name mesh bhrate

AP のメッシュ バックホール データ レートを表示するには、**show ap name** *ap-name* **mesh bhrate** コマンドを使用します。

show ap name *ap-name* **mesh bhrate** ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

ap-name	AP の名前。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP のメッシュ バックホール データ レートを表示する例を示します。

```
Device# show ap name mymeshap mesh bhrate
```

show ap name mesh linktest

メッシュ リンクテスト データを表示するには、 **show ap name mesh linktest data** コマンドを使用します。

show ap name *ap-name* **mesh linktest data** *dest-mac* [**chassis** {*chassis-number* | **active** | **standby**}**R0**]

構文の説明

ap-name	アクセス ポイントの名前
linktest	メッシュ リンクテストを表示します
data	メッシュ リンクテスト データを表示します
dest-mac	AP の MAC アドレスを入力します。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の設定のアクティブ インスタンス。
standby R0	ルートプロセッサスロット 0 の設定のスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP のメッシュ リンクテスト データを表示する例を示します。

```
Device# show ap name mesh-profile-namemesh linktest data 83-88-15-0C-83-72
```

show ap name mesh neighbor detail

メッシュ AP のネイバーに関する詳細情報を表示するには、**show ap name** *ap-name* **mesh neighbor detail** コマンドを使用します。

show ap name *ap-name* **mesh neighbor detail** ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

ap-name	AP の名前。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ AP のネイバーに関する詳細情報を表示する例を示します。

```
Device# show ap name mymeshap mesh neighbhor detail
```

show ap name mesh neighbor detail

メッシュ AP のネイバーに関する詳細情報を表示するには、**show ap name** *ap-name* **mesh neighbor detail** コマンドを使用します。

show ap name *ap-name* **mesh neighbor detail** ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

ap-name	AP の名前。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ AP のネイバーに関する詳細情報を表示する例を示します。

```
Device# show ap name mymeshap mesh neighbhor detail
```

show ap name mesh path

メッシュ AP のパスに関する情報を表示するには、**show ap name** *ap-name* **mesh path** コマンドを使用します。

show ap name *ap-name* **mesh path** ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ AP のパスに関する情報を表示する例を示します。

```
Device# show ap name mymeshap mesh path
```

show ap name mesh stats

メッシュ統計情報を表示するには、**show ap name** *ap-name* **mesh stats** コマンドを使用します。

show ap name *ap-name*[{**packet error** | **queue** | **security**}]

構文の説明

ap-name	AP の名前。
packet error	メッシュ パケットのエラーの統計。
queue	メッシュ キューの統計。
security	メッシュ セキュリティの統計。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ統計情報を表示する例を示します。

```
Device# show ap name mymeshap mesh stats
```

show ap name tunnel eogre events

AP の Ethernet over GRE（EoGRE）イベントを表示するには、**show ap name tunnel eogre events** コマンドを使用します。

show ap name *ap-name***tunnel eogre events**

構文の説明

ap-name	AP 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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、AP の EoGRE トンネル イベントを表示する例を示します。

```
Device# show ap name ap1 tunnel eogre events

AP 80e8.6fd4.9520  Event history
Timestamp               #Times   Event                RC Context
----------------------- -------- -------------------- --
----------------------------------------
02/18/2019 23:50:26.341 6        IAPP_STATS           0 GW Tunnel2 uptime:0s

02/18/2019 23:49:40.222 2       CLIENT_JOIN         0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:48:43.549 1       CLIENT_LEAVE        0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:47:33.127 1        DOMAIN_STATUS        0 eogre_domain Active GW: Tunnel1

02/18/2019 23:47:33.124 4        AP_TUNNEL_STATUS     0 Tunnel2 Dn

02/18/2019 23:47:33.124 1        MSG_CLIENT_DEL       0 GW Tunnel2 (IP: 9.51.1.12)

02/18/2019 23:47:33.124 2        TUNNEL_ADD           0 GW Tunnel2

02/18/2019 23:47:33.120 3        MSG_CLIENT_DEL_PD    0 GW Tunnel1 (IP: 9.51.1.11)

02/18/2019 23:47:31.763 2        AP_DOMAIN_PUSH       0 Delete:eogre_domain_set, 0 GWs

02/18/2019 23:47:31.753 4        AP_VAP_PUSH          0 profile:'eogre_tunnel',
wlan:pyats_eogre
```

show ap name tunnel eogre domain detailed

AP の Ethernet over GRE（EoGRE）トンネル ドメイン ステータスの詳細情報を表示するには、**show ap name tunnel eogre domain detailed** コマンドを使用します。

show ap name *ap-name* **tunnel eogre domain detailed** *domain-name*

構文の説明

ap-name	AP 名。
domain-name	EoGRE ドメイン名。

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、AP の EoGRE トンネル ドメイン ステータスの詳細情報を表示する例を示します。

```
Device# show ap name ap1 tunnel eogre domain detailed eogre_domain


Domain Name    : eogre_domain
 Primary GW    : Tunnel1
 Secondary GW  : Tunnel2
 Active GW     : Tunnel1
 Redundancy    : Non-Revertive
 AdminState    : Up
```

show ap name tunnel eogre domain summary

AP の Ethernet over GRE（EoGRE）トンネル ドメインのサマリー情報を表示するには、**show ap name tunnel eogre domain summary** コマンドを使用します。

show ap name *ap-name***tunnel eogre domain summary**

構文の説明

ap-name	AP 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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、AP の EoGRE トンネル ドメインのサマリー情報を表示する例を示します。

```
Device# show ap name ap1 tunnel eogre domain summary

AP MAC          Domain                          Active Gateway
-----------------------------------------------------------------------------
80e8.6fd4.9520  eogre_domain
```

show ap name tunnel eogre gateway detailed

AP の Ethernet over GRE（EoGRE）トンネル ゲートウェイ ステータスの詳細情報を表示するには、**show ap name tunnel eogre gateway detailed** コマンドを使用します。

show ap name *ap-name* **tunnel eogre gateway detailed** *gateway-name*

構文の説明

ap-name	AP 名。
gateway-name	EoGRE ゲートウェイ名。

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、AP の EoGRE トンネル ゲートウェイ ステータスの詳細情報を表示する例を示します。

```
Device# show ap name ap1 tunnel eogre gateway detailed Tunnel2

Gateway : Tunnel2
 Mode   : IPv4
 IP     : 9.51.1.12
 State  : Down
 MTU    : 0
 AP MAC : 80e8.6fd4.9520

 Clients
  Total Number of Wireless Clients      : 0
 Traffic
  Total Number of Received Packets      : 0
  Total Number of Received Bytes        : 0
  Total Number of Transmitted Packets   : 0
  Total Number of Transmitted Bytes     : 0
  Total Number of Lost Keepalive        : 151
```

show ap name tunnel eogre gateway summary

AP の Ethernet over GRE（EoGRE）トンネル ゲートウェイのサマリー情報を表示するには、**show ap name tunnel eogre gateway summary** コマンドを使用します。

show ap name *ap-name***tunnel eogre gateway summary**

構文の説明

ap-name	AP 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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、AP の EoGRE トンネル ゲートウェイのサマリー情報を表示する例を示します。

```
Device# show ap name ap1 tunnel eogre gateway summary

AP MAC          Gateway          Type  IP                                        State
Clients
-------------------------------------------------------------------------------------------
80e8.6fd4.9520  Tunnel1          IPv4  9.51.1.11                                 Up     1

80e8.6fd4.9520  Tunnel2          IPv4  9.51.1.12                                 Down   0
```

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 Gibraltar 16.10.1	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。

```
デバイス# 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。

```
デバイス# 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 wlan vlan

各アクセスポイント（AP）の使用できる WLAN-VLAN マッピングを表示するには、**show ap name wlan vlan** コマンドを使用します。

show ap name *ap_name* **wlan vlan**

構文の説明

ap_name	WLAN-VLANマッピングを表示する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 Bengaluru 17.6.1	このコマンドが導入されました。

次に、AP の使用できる wlan vlan マッピングを表示する例を示します。

```
Device# show ap name test wlan vlan

Policy tag mapping
------------------
WLAN Profile Name Name Policy    VLAN   Flex Central Switching  IPv4 ACL    IPv6 ACL
-------------------------------------------------------------------------------------
jey_cwa           pp-local-1     46       Enabled              jey_acl1   Not Configured
swaguest          pp-local-1     46       Enabled              jey_acl1   Not Configured
```

show ap name ble detail

AP に関連付けられている CMX を表示するには、**show ap name ble detail** コマンドを使用します。

show ap name *ap-name* **ble detail**

構文の説明

ap-name	AP 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

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

次の例では、特定の AP の BLE のグローバル値および BLE の詳細を表示する方法を示します。

```
Device# show ap name AP4001.7AB2.C39A ble detail
CMX IP: 9.9.71.100
-----------------------
  BLE administrative status: Up
  BLE operational status: Up
  Scanning interval: 10

  AP Name                          Interface             Status
  ------------------------------------------------------------------
  AP4001.7AB2.C39A                 Integrated            Open
```

show ap management-mode meraki capability summary

Meraki 管理モード対応 AP の情報の概要を表示するには、**show ap management-mode meraki capability summary** を使用します

show ap management-mode meraki capability 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 Cupertino 17.9.1	このコマンドが変更されました。

例

次に、Meraki 管理モード対応 AP の情報の概要を表示する例を示します。

```
Device# show ap management-mode meraki capability summary
```

show ap management-mode meraki change summary

AP 管理モードの Meraki の変更の概要を表示するには、**show ap management-mode meraki change summary** コマンドを使用します。

show ap management-mode meraki change 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 Cupertino 17.9.1	このコマンドが変更されました。

例

次に、AP 管理モードの Meraki の変更の概要を表示する例を示します。

```
Device# show ap management-mode meraki change summary
```

show ap management-mode meraki failure summary

Meraki 管理モードの障害の概要を表示するには、**show ap management-mode meraki failure summary** コマンドを使用します。

show ap management-mode meraki failure 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 Cupertino 17.9.1	このコマンドが変更されました。

例

次に、Meraki 管理モードの障害の概要を表示する例を示します。

```
Device# show ap management-mode meraki failure summary
```

show ap neighborhood

AP ネイバーフッドの情報を表示するには、**show ap neighborhood** コマンドを使用します。

show ap neighborhood *id* **details**

構文の説明

id	ネイバーフッド ID。
details	ネイバーフッド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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、AP ネイバーフッドの情報を表示する例を示します。

```
Device# show ap neighborhood 0 details

NH-ID = Neighborhood ID
AREA-ID = Area ID of neighborhood

Number of APs: 1

NH-ID     AREA-ID          WNCD instance     AP Name              Ethernet MAC
-------------------------------------------------------------------------------
0         0x00000000       0                 APA023.9FD8.EA22     a023.9fd8.ea22
```

show ap neighborhood details

AP ネイバーフッドの詳細を表示するには、**show ap neighborhood details** コマンドを使用します。

show ap neighborhood details

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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、AP ネイバーフッドの詳細を表示する例を示します。

```
Device# show ap neighborhood details

NH-ID = Neighborhood ID
AREA-ID = Area ID of neighborhood

Number of APs: 4

NH-ID   AREA-ID        WNCD instance    AP Name                 Ethernet MAC
-------------------------------------------------------------------------------
0       0x00000000     1                EDU_BR_01_00_28_3702    bc16.6509.bfcc
1       0x00000000     0                ci-glad-mdns-ap         0cd0.f894.567c
1       0x00000000     0                EDU_VW_9120_1_2         c4f7.d54c.f978
2       0x00000000     0                ewlc-hc-tsim-30-1       00b9.3000.02f0
```

show ap neighborhood mac details

MAC アドレスを使用して AP ネイバーフッドの詳細を表示するには、**show ap neighborhood mac details** コマンドを使用します。

show ap neighborhood mac *mac-address* **details**

構文の説明

mac-address	AP の MAC アドレス。
details	AP ネイバーフッドの詳細を指定します。

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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、MAC アドレスを使用して AP ネイバーフッドの詳細を表示する例を示します。

```
Device# show ap neighborhood mac 0aa8.89f0.0001 details

NH-ID = Neighborhood ID
AREA-ID = Area ID of neighborhood

AP Name            Ethernet MAC    Radio MAC       NH-ID  AREA-ID     WNCD instance
-------------------------------------------------------------------------------------
AP6B8B4567-0001    0aa8.89f0.0001  0aa8.8900.0100  0      0x00000000  0
```

show ap neighborhood summary

AP ネイバーフッドの概要を表示するには、**show ap neighborhood summary** コマンドを使用します。

show ap neighborhood 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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、AP ネイバーフッドの概要を表示する例を示します。

```
Device# show ap neighborhood summary

NH-ID = Neighborhood ID
AREA-ID = Area ID of neighborhood

Total number of neighborhood: 5
Total number of algorithm iterations: 1
Ideal AP capacity per WNCD instance: 210

Total number of neighborhood area: 14

NH-ID      AREA-ID         Process Name   Number of APs
-------------------------------------------------
0          0x00000000      WNCD_1         1
1          0x00000000      WNCD_0         2
2          0x00000000      WNCD_0         100
2          0x00000001      WNCD_0         100
2          0x00000002      WNCD_3         100
2          0x00000003      WNCD_4         50
3          0x00000000      WNCD_1         100
3          0x00000001      WNCD_1         100
3          0x00000002      WNCD_4         100
3          0x00000003      WNCD_4         50
4          0x00000000      WNCD_2         100
4          0x00000001      WNCD_2         100
4          0x00000002      WNCD_3         100
4          0x00000003      WNCD_3         50
```

show ap profile

AP プロファイルの HyperLocation の全体的なステータスを表示するには、**show ap profile** コマンドを使用します。

show ap profile *profile-name* {**detailed** | **hyperlocation** {**ble-beacon** | **detail** | **summary**}} [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

構文の説明

profile-name	AP プロファイル名。
detailed	AP 参加プロファイルの詳細パラメータを表示します。
hyperlocation	AP プロファイルの HyperLocation 情報を表示します。
ble-beacon	AP プロファイルの設定済み BLE ビーコンのリストを表示します。
detail	AP プロファイルの HyperLocation の詳細なステータスを表示します。
summary	AP プロファイルの HyperLocation の全体的なステータスを表示します
chassis-number	シャーシ番号（1 または 2 のいずれか）。
active R0	ルートプロセッサ スロット 0 のアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 のスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP プロファイルの HyperLocation の全体的なステータスを表示する例を示します。

```
Device# show ap profile my-ap-profile detailed
```

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。

```
デバイス#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 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。

```
デバイス#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 sensor status

AP センサーの詳細とそのステータスを表示するには、**show ap sensor status** コマンドを使用します。

show ap sensor status

構文の説明

このコマンドには、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 Cupertino 17.8.1	このコマンドが導入されました。

例

次に、AP センサーの詳細とそのステータスを表示する例を示します。

```
Device# show ap sensor status
```

show ap summary

device 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 Gibraltar 16.10.1	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、device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 summary load-info

無線チャネルごとの AP の使用率と、AP ごとのクライアントとスロットの総数を表示するには、**show ap summary load-info** コマンドを使用します。

show ap summary load-info

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 Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、無線チャネルごとの AP の使用率と、AP ごとのクライアントとスロットの総数を表示する例を示します。

```
Device# show ap summary load-info

WTP-Mac         AP-Name          Tot-Slots Tot-Clients  Slot0                  Slot1
                Slot2
                                                        Clients Utilisation(%) Clients
Utilisation(%)  Clients Utilisation(%)
-------------------------------------------------------------------------------------

04eb.409e.a5c0  AP04EB.409E.07EC 3         0            0       99             0
63              0       0
1880.90fd.6b40  paxxxxi-AP       2         0            0       0              0
0               NA      NA
```

show ap summary sort name

名前でソートされたアクセスポイント（AP）の概要を表示するには、**show ap summary sort name** コマンドを使用します。

show ap summary sort name

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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、名前でソートされた AP の概要を表示する例を示します。

```
Device# show ap summary sort name
Number of APs: 05
AP Name         Slots  AP Model          Ethernet MAC    Radio MAC       Location
  Country  IP Address  State
-------------------------------------------------------------------------------------------------
ABC              2    AIR-AP1832I-D-K9   2c0b.e9b6.3618  2c0b.e9b7.3ec0  Real-AP-Testbed
  IN      1.2.22.222  Registered
AP-Farm-1832I-4  2    AIR-AP1832I-D-K9   2c0b.e9b6.3e58  2c0b.e9b7.5fc0  Real-AP-Testbed
  IN      1.2.22.22   Registered
AP-Farm-1832I-5  2    AIR-AP1832I-D-K9   2c0b.e9b6.3f60  2c0b.e9b7.63e0  Real-AP-Testbed
  IN      1.2.22.22   Registered
AP-Farm-1832I-6  2    AIR-AP1832I-D-K9   2c0b.e9b6.3fe8  2c0b.e9b7.6600  Real-AP-Testbed
  IN      1.2.22.22   Registered
AP-Farm-1832I-7  2    AIR-AP1832I-D-K9   2c0b.e9b6.4010  2c0b.e9b7.66a0  Real-AP-Testbed
  IN      1.2.22.222
```

show ap summary sort ascending client-count

クライアント数に基づいて昇順でソートされた AP の概要を表示するには、**show ap summary sort ascending client-count** コマンドを使用します。

show ap summary sort ascending client-count

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 Amsterdam 17.1.1s	このコマンドが導入されました。

次に、クライアント数に基づいて昇順でソートされた AP の概要を表示する例を示します。

```
Device# show ap summary sort ascending client-count
```

```
AP-name                          AP-mac           Client count          Data Usage
     Through-Put     Admin-State
-------------------------------------------------------------------------------------
L2_3802I_1                       7872.5d27.b8c0       1                     622358
         11            Enabled
L2_1815w_1                       707d.b99e.c2e0       2                     5871836
         1422          Enabled
```

show ap summary sort ascending data-usage

データ使用量に基づいて昇順でソートされた AP の概要を表示するには、**show ap summary sort ascending data-usage** コマンドを使用します。

show ap summary sort ascending data-usage

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 Amsterdam 17.1.1s	このコマンドが導入されました。

次に、データ使用量に基づいて昇順でソートされた AP の概要を表示する例を示します。

```
Device# show ap summary sort ascending data-usage
```

```
AP-name                          AP-mac           Client count          Data Usage
     Through-Put     Admin-State
-------------------------------------------------------------------------------------
L2_3802I_1                       7872.5d27.b8c0       1                     622600
          4             Enabled
L2_1815w_1                       707d.b99e.c2e0       2                     6102216
          281           Enabled
```

show ap summary sort ascending throughput

スループットに基づいて昇順でソートされた AP の概要を表示するには、**show ap summary sort ascending throughput** コマンドを使用します。

show ap summary sort ascending throughput

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 Amsterdam 17.1.1s	このコマンドが導入されました。

次に、スループットに基づいて昇順でソートされた AP の概要を表示する例を示します。

```
Device# show ap summary sort ascending throughput
```

```
AP-name                          AP-mac           Client count          Data Usage
     Through-Put     Admin-State
-------------------------------------------------------------------------------------
L2_3802I_1                       7872.5d27.b8c0       1                     6749385
         6             Enabled
L2_1815w_1                       707d.b99e.c2e0       2                     94748042
         35            Enabled
```

show ap summary sort descending client-count

クライアント数に基づいて降順でソートされた AP の概要を表示するには、**show ap summary sort descending client-count** コマンドを使用します。

show ap summary sort descending client-count

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 Amsterdam 17.1.1s	このコマンドが導入されました。

次に、クライアント数に基づいて降順でソートされた AP の概要を表示する例を示します。

```
Device# show ap summary sort descending client-count
```

```
AP-name                          AP-mac           Client count          Data Usage
     Through-Put     Admin-State
-------------------------------------------------------------------------------------
L2_1815w_1                       707d.b99e.c2e0       2                    94753989
         46            Enabled
L2_3802I_1                       7872.5d27.b8c0       1                    6750526
         6             Enabled
```

show ap summary sort descending data-usage

データ使用量に基づいて降順でソートされた AP の概要を表示するには、**show ap summary sort descending data-usage** コマンドを使用します。

show ap summary sort descending data-usage

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 Amsterdam 17.1.1s	このコマンドが導入されました。

次に、データ使用量に基づいて降順でソートされた AP の概要を表示する例を示します。

```
Device# show ap summary sort descending data-usage
```

```
AP-name                          AP-mac           Client count          Data Usage
     Through-Put     Admin-State
-------------------------------------------------------------------------------------
L2_1815w_1                       707d.b99e.c2e0       2                    94756618
         47            Enabled
L2_3802I_1                       7872.5d27.b8c0       0                    6750526
         6             Enabled
```

show ap summary sort descending throughput

スループットに基づいて降順でソートされた AP の概要を表示するには、**show ap summary sort descending throughput** コマンドを使用します。

show ap summary sort descending throughput

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 Amsterdam 17.1.1s	このコマンドが導入されました。

次に、スループットに基づいて降順でソートされた AP の概要を表示する例を示します。

```
Device# show ap summary sort descending throughput
```

```
AP-name                          AP-mac           Client count          Data Usage
     Through-Put     Admin-State
-------------------------------------------------------------------------------------
L2_1815w_1                       707d.b99e.c2e0       2                    94758750
         23            Enabled
L2_3802I_1                       7872.5d27.b8c0       0                    6750526
         6             Enabled
```

show ap support-bundle summary

AP サポートバンドルの概要を表示するには、**show ap support-bundle summary** コマンドを使用します。

show ap support-bundle 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 Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、AP サポートバンドルの概要を表示する例を示します。

```
Device# show ap support-bundle summary
```

show ap tag sources

プライオリティ付きの AP タグソースを表示するには、**show ap tag sources** コマンドを使用します。

show ap tag sources ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、アクティブなインスタンスのプライオリティを持つ AP タグの送信元を表示する例を示します。

```
Device# show ap tag sources chassis active R0
```

show ap tag summary

タグ名の簡潔な概要を表示するには、**show ap tag summary** コマンドを使用します。

show ap tag 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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、タグ名の概要を表示する例を示します。

```
Device# show ap tag summary
```

show ap triradio summary

トライ無線の概要を表示し、スロットが有効になっていて稼働しているかどうかを確認するには、**show ap triradio summary** コマンドを使用します。

show ap triradio 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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、トライ無線の概要を表示し、スロットが有効になっているかどうかを確認する例を示します。

```
Device# show ap triradio summary
```

show ap timezone

AP のタイムゾーン情報を確認するには、**show ap timezone** コマンドを使用します。

show ap timezone

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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、AP のタイムゾーン情報を確認する例を示します。

```
Device# show ap timezone

AP Name   Status     Offsets(h/m)
--------------------------------
AP1       Disabled    0:0
AP2       Enabled     1:0
```

show ap upgrade

AP のアップグレード情報を表示するには、**show ap upgrade** コマンドを使用します。

show ap upgrade [{**name** *ap-upgrade-report-name* | **summary** | **chassis** {*chassis-number* | **active** | **standby**}}]

構文の説明

name *ap-upgrade-report-name*	AP アップグレード レポートの名前を入力します。
summary	AP アップグレード情報の概要を示します。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 のアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 のスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、AP アップグレード情報の概要を表示する例を示します。

```
Device# show ap upgrade summary
```

show ap upgrade method

HTTPS メソッドでのイメージのダウンロードの設定のステータスを確認するには、**show ap upgrade method** コマンドを使用します。

show ap upgrade method

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 Dublin 17.11.1	このコマンドが導入されました。

例

次に、HTTPS イメージのダウンロード設定のステータスを確認する例を示します。

```
Device# show ap upgrade method

AP upgrade method https : Enabled
```

show arp

ARP テーブルを表示するには、**show arp** コマンドを使用します。

show arp

構文の説明

arp	ARP テーブルを表示する

コマンド モード

User EXEC (>)

Privileged EXEC (#)

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

次に、このコマンドの出力例を示します。

```
Device# show arp

Address Age (min)     Hardware Addr
   9.11.8.1         0 84:80:2D:A0:D2:E6
9.11.32.111         0 3C:77:E6:02:33:3F
```

show arp summary

ARP テーブルの概要を表示するには、**show arp summary** コマンドを使用します。

show arp 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ARP テーブルの概要を表示する例を示します。

```
Device# show arp summary
```

show ap tunnel eogre events

Ethernet over GRE（EoGRE）トンネル イベントを表示するには、**show ap tunnel eogre events** コマンドを使用します。

show ap tunnel eogre events

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、EoGRE トンネル イベントを表示する例を示します。

```
Device# show ap tunnel eogre events

AP 80e8.6fd4.9520  Event history
Timestamp               #Times   Event                RC Context
----------------------- -------- -------------------- --
----------------------------------------
02/18/2019 23:50:26.341 6        IAPP_STATS           0 GW Tunnel2 uptime:0s

02/18/2019 23:49:40.222 2       CLIENT_JOIN         0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:48:43.549 1       CLIENT_LEAVE        0 74da.3828.88b0, (eogre_domain/2121)

02/18/2019 23:47:33.127 1         DOMAIN_STATUS        0 eogre_domain Active GW: Tunnel1

02/18/2019 23:47:33.124 4         AP_TUNNEL_STATUS     0 Tunnel2 Dn

02/18/2019 23:47:33.124 1         MSG_CLIENT_DEL       0 GW Tunnel2 (IP: 9.51.1.12)

02/18/2019 23:47:33.124 2         TUNNEL_ADD           0 GW Tunnel2

02/18/2019 23:47:33.120 3         MSG_CLIENT_DEL_PD    0 GW Tunnel1 (IP: 9.51.1.11)

02/18/2019 23:47:31.763 2         AP_DOMAIN_PUSH       0 Delete:eogre_domain_set, 0 GWs

02/18/2019 23:47:31.753 4         AP_VAP_PUSH          0 profile:'eogre_tunnel',
wlan:pyats_eogre
```

show ap tunnel eogre domain detailed

AP の Ethernet over GRE（EoGRE）トンネル ドメイン ステータスの詳細情報を表示するには、**show ap tunnel eogre domain detailed** コマンドを使用します。

show ap tunnel eogre domain detailed *domain-name*

構文の説明

domain-name	EoGRE ドメイン名。

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、EoGRE トンネル ドメイン ステータスの詳細情報を表示する例を示します。

```
Device# show ap tunnel eogre domain detailed Tunnel1


Gateway : Tunnel1
 Mode   : IPv4
 IP     : 9.51.1.11
 State  : Up
 MTU    : 1476
 Up Time: 14 hours 25 minutes 2 seconds
 AP MAC : 80e8.6fd4.9520

 Clients
  Total Number of Wireless Clients      : 1
 Traffic
  Total Number of Received Packets      : 6
  Total Number of Received Bytes        : 2643
  Total Number of Transmitted Packets   : 94
  Total Number of Transmitted Bytes     : 20629
  Total Number of Lost Keepalive        : 3
```

show ap name tunnel eogre domain summary

AP の Ethernet over GRE（EoGRE）トンネル ドメインのサマリー情報を表示するには、**show ap nametunnel eogre domain summary** コマンドを使用します。

show ap name *ap-name***tunnel eogre domain summary**

構文の説明

ap-name	AP 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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、AP の EoGRE トンネル ドメインのサマリー情報を表示する例を示します。

```
Device# show ap name ap1 tunnel eogre domain summary

AP MAC          Domain                          Active Gateway
-----------------------------------------------------------------------------
80e8.6fd4.9520  eogre_domain                    Tunnel1
```

show ap tunnel eogre gateway detailed

AP の Ethernet over GRE（EoGRE）トンネル ゲートウェイ ステータスの詳細情報を表示するには、**show ap name tunnel eogre gateway detailed** コマンドを使用します。

show ap name *ap-name* **tunnel eogre gateway detailed** *gateway-name*

構文の説明

ap-name	AP 名。
gateway-name	EoGRE ドメイン名。

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、AP の EoGRE トンネル ゲートウェイ ステータスの詳細情報を表示する例を示します。

```
Device# show ap name ap1 tunnel eogre gateway detailed Tunnel1

Gateway : Tunnel1
 Mode   : IPv4
 IP     : 9.51.1.11
 State  : Up
 MTU    : 1476
 Up Time: 14 hours 25 minutes 2 seconds
 AP MAC : 80e8.6fd4.9520

 Clients
  Total Number of Wireless Clients      : 1
 Traffic
  Total Number of Received Packets      : 6
  Total Number of Received Bytes        : 2643
  Total Number of Transmitted Packets   : 94
  Total Number of Transmitted Bytes     : 20629
  Total Number of Lost Keepalive        : 3
```

show ap tunnel eogre gateway summary

Ethernet over GRE（EoGRE）トンネル ゲートウェイのサマリー情報を表示するには、**show ap tunnel eogre gateway summary** コマンドを使用します。

show ap tunnel eogre gateway 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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、EoGRE トンネル ゲートウェイのサマリー情報を表示する例を示します。

```
Device# show ap tunnel eogre gateway summary

AP MAC          Gateway          Type  IP                                      State
Clients
-------------------------------------------------------------------------------------------
80e8.6fd4.9520  Tunnel1          IPv4  9.51.1.11                               Up     1

80e8.6fd4.9520  Tunnel2          IPv4  9.51.1.12                               Down   0
```

show ap upgrade site

アップグレードサイト関連の情報を表示するには、**show ap upgrade site** コマンドを使用します。

show ap upgrade site [**summary**]

構文の説明

summary	（任意）個々のサイトのアクセスポイント（AP）アップグレード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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	このコマンドが導入されました。

例

次に、アップグレードサイト関連の情報を表示する例を示します。

```
Device# show ap upgrade site

Site-filtered AP upgrade report data
====================================
Source controller: Controller1
Destination controller: Controller2
Site-filters present: Yes

AP image upgrade site summary
-----------------------------
Operation: N+1 move

Site Tag                                    Status
------------------------------------------------------------
site1                                       In Progress

AP upgrade reports linked to these site-filters
-----------------------------------------------

Start time               Operation type             Report name
-------------------------------------------------------------------------------
01/30/2022 10:34:36 IST  AP image upgrade/move CLI  AP_upgrade_to_Controller2_3002022103435
```

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 Gibraltar 16.10.1	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。

```
デバイス# 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 Gibraltar 16.10.1	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。

```
デバイス# 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 awips wlc-alarm

AWIPS WLC アラームテーブルの内容を表示するには、**show awips wlc-alarm** コマンドを使用します。

show awips wlc-alarm

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 Amsterdam 17.3.1	このコマンドが追加されました。

例

次に、AWIPS WLC アラームテーブルの内容を表示する例を示します。

```
Device# show awips wlc-alarm

Time                  BSSID           Client MAC      Alarm description
------------------------------------------------------------------
04/02/2020 16:03:18  e4aa.5d53.b921  74da.3864.2a94  WPA2 Key Reinstal KRACK
04/02/2020 16:03:19  e4aa.5d53.b921  74da.3864.2a94  WPA2 Key Reinstal KRACK
04/02/2020 16:03:20  e4aa.5d53.b921  74da.3864.2a94  WPA2 Key Reinstal KRACK
04/02/2020 16:03:21  e4aa.5d53.b921  74da.3864.2a94  WPA2 Key Reinstal KRACK
```

show awips syslog throttle

Cisco Advanced Wireless Intrusion Prevention System（aWIPS）の syslog 設定を確認するには、**show awips syslog throttle** コマンドを使用します。

show awips syslog throttle

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 Bengaluru 17.6.1	このコマンドが導入されました。

次に、aWIPS の syslog 設定を確認する例を示します。

```
Device# show awips syslog throttle
Syslog Throttle Interval (seconds)
------------------------------------------------------------
60
```

show capwap client rcb

CAPWAP のステータスとモードを表示するには、アクセスポイントで **show capwap client rcb** コマンドを使用します。

show capwap client rcb

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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

例

次に、アクセスポイントでCAPWAPのステータスとモードを表示する例を示します。

```
AP# show capwap client rcb

OperationState                      : UP
Name                                : AP4001.7A39.2D5A
MwarHwVer                           : 0.0.0.0
Location                            : default location
ApMode                              : Remote Bridge
ApSubMode                           : Not Configured
CAPWAP Path MTU                     : 1485
Software Initiated Reload Reason    : Reload command
CAPWAP Sliding Window
Active Window Size                  : 10
Last Request Send To Application    : 184
Expected Seq Num                    : 185
Received Seq Num                    : 184
Request Packet Count                : 42424
Out Of Range Packets Count          : 0
Window Moved  Packets Count         : 0
In Range Packets Count              : 960
Expected Packets Count              : 41464
```

show chassis

シャーシ情報を表示するには、**show chassis** コマンドを使用します。

show chassis [{*1 2* | **detail** | **mode** | **neighbors** | **ha-status** {**active** | **local** | **standby**}}]

構文の説明

{*1* | *2*}	シャーシ番号を1または2にして、関連するシャーシに関する情報を確認します。
detail	シャーシに関する詳細情報を表示します。
mode	シャーシ モードに関する情報を表示します。
neighbors	シャーシ ネイバーに関する情報を表示します。
ha-status	高可用性（HA）ステータスに関する情報を表示するオプションです。
active	アクティブ状態のシャーシの HA ステータスを表示します。
local	ローカルシャーシの HA ステータスを表示します。
standby	スタンバイ状態のシャーシの HA 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

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、アクティブ シャーシの HA ステータスを表示する例を示します。

```
Device# show chassis ha-status active
```

show chassis rmi

アクティブコントローラにおけるシャーシの冗長管理インターフェイス（RMI）の設定を確認するには、**show chassis rmi** コマンドを使用します。

show chassis rmi

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 Amsterdam 17.1.1	このコマンドが導入されました。

次に、アクティブコントローラにおけるシャーシの冗長管理インターフェイス（RMI）の設定を確認する例を示します。

```
Device# show chassis rmi
Chassis/Stack Mac Address : 000c.2964.1eb6 - Local Mac Address
Mac persistency wait time: Indefinite
H/W Current
Chassis# Role Mac Address Priority Version State IP RMI-IP
---------------------------------------------------------------------------------------------
*1 Active 000c.2964.1eb6 1 V02 Ready 169.254.90.147 9.10.90.147
2 Standby 000c.2975.3aa6 1 V02 Ready 169.254.90.149 9.10.90.149
```

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** *client-ID <0-381>* | **entities***entity-ID <1-7>* | **statisticsbuffer-usage**}

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。
buffer-usage	多数のバッファを使用するクライアントのチェックポイント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 Gibraltar 16.10.1	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 cts environment data

AP での TrustSec 環境データを表示するには、**show cts environment data** コマンドを使用します。

show cts environment data

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 Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、AP での TrustSec 環境データを表示する例を示します。

```
Device# show cts environment

CTS Environment Data
====================
Current state = COMPLETE
Last status   = Successful
Local Device SGT:
SGT tag = 0-07:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
Server: 8.109.0.85, port 1812, A-ID 9818EE1ECA02B7BFE359C28B30EA7E2A
Status = ALIVE
auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
0-07:Unknown
2-00:TrustSec_Devices
3-00:Network_Services
4-00:Employees
5-00:Contractors
6-00:Guests
7-00:Production_Users
8-00:Developers
9-00:Auditors
10-00:Point_of_Sale_Systems
11-02:Production_Servers
12-00:Development_Servers
13-00:Test_Servers
14-00:PCI_Servers
15-00:BYOD
16-06:BGL15
17-00:BGL12
255-00:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 11:50:49 UTC Sun Jan 9 2022
Env-data expires in   0:00:28:54 (dd:hr:mm:sec)
```

```
Env-data refreshes in 0:00:28:54 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

show cts role-based sgt-map all

AP での IP アドレスと SGT の送信元名のバインディングを表示するには、**show cts role-based sgt-map all** コマンドを使用します。

show cts role-based sgt-map all

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 Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、AP での IP アドレスと SGT の送信元名のバインディングを表示する例を示します。

```
Device# show cts role-based stg-map all

Active IPv4-SGT Bindings Information
IP Address                                      SGT       Source
============================================================================
8.73.1.101                                       16      LOCAL
8.73.1.102                                       16      LOCAL
8.73.1.103                                       16      LOCAL
8.73.1.104                                       16      LOCAL
8.73.1.105                                       16      LOCAL
8.73.1.106                                       16      LOCAL
8.73.1.107                                       16      LOCAL
8.73.1.108                                       16      LOCAL
8.73.1.109                                       16      LOCAL
8.73.1.110                                       16      LOCAL
8.73.1.111                                       16      LOCAL
8.73.1.112                                       16      LOCAL
8.73.1.113                                       16      LOCAL
8.73.1.114                                       16      LOCAL
8.73.1.115                                       16      LOCAL
8.73.1.116                                       16      LOCAL
8.73.1.117                                       16      LOCAL
8.73.1.118                                       16      LOCAL
8.73.1.119                                       16      LOCAL
8.73.1.120                                       16      LOCAL
8.73.1.121                                       16      LOCAL
8.73.1.122                                       16      LOCAL
8.73.1.123                                       16      LOCAL
8.73.1.124                                       16      LOCAL
8.73.1.125                                       16      LOCAL
8.73.1.126                                       16      LOCAL
8.73.1.127                                       16      LOCAL
8.73.1.128                                       16      LOCAL
```

```
8.73.1.129                                      16      LOCAL
8.73.1.130                                      16      LOCAL
8.73.1.131                                      16      LOCAL
8.73.1.132                                      16      LOCAL
8.73.1.133                                      16      LOCAL
8.73.1.134                                      16      LOCAL
8.73.1.135                                      16      LOCAL
8.73.1.136                                      16      LOCAL
8.73.1.137                                      16      LOCAL
8.73.1.138                                      16      LOCAL
8.73.1.139                                      16      LOCAL
8.73.1.140                                      16      LOCAL
8.73.1.141                                      16      LOCAL
8.73.1.142                                      16      LOCAL
FD09:8::                                        16      LOCAL
FD09:8:73:0:4051:EB27:B4A2:F6DB                 16      LOCAL
FD09:8:73:0:4C3C:1D75:81E0:DB94                 16      LOCAL
FD09:8:73:0:5136:9045:9D11:E191                 16      LOCAL
FD09:8:73:0:6903:B84E:5BDF:9D54                 16      LOCAL
FD09:8:73:0:A9F8:7825:B07:75A8                  16      LOCAL
FD09:8:73:0:B505:626B:51D7:6DB6                 16      LOCAL
FD09:8:73:0:D0B4:3316:7CE9:8AE8                 16      LOCAL
FD09:8:73:0:ECA8:F5E:CCF5:FFD7                  16      LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 9
Total number of active   bindings = 9
```

show cts role-based counters

AP ですべてのロールベースのカウンタをクリアするには、**show cts role-based counters** コマンドを使用します。

show cts role-based 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 Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、AP ですべてのロールベースのカウンタをクリアする例を示します。

```
Device# show cts role-based counters

From  To   SW-Denied HW-Denied SW-Permitt HW-Permitt  SW-Monitor HW-Monitor
==============================================================================
*     *     0          0          0          178837189  0          0
16    0     0          0          0          39250482   0          0
16    16    0          52835      0          0          0          0
17    16    0          0          0          0          0          0
```

show environment summary

すべての環境モニタリングセンサーの概要を表示するには、**show environment summary** コマンドを使用します。

show environment 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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。
Cisco IOS XE Bengaluru 17.5.1	このコマンドの出力が変更されました。

例

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

例

```
Device# show environment summary


Number of Critical alarms:  0
Number of Major alarms:     0
Number of Minor alarms:     0

 Slot        Sensor          Current State   Reading
Threshold(Minor,Major,Critical,Shutdown)
 ----------  --------------  --------------- ------------
---------------------------------------
 P0          Vin             Normal          231  V AC    na
 P0          Iin             Normal          2    A       na
 P0          Vout            Normal          12   V DC    na
 P0          Iout            Normal          30   A       na
 P0          Temp1           Normal          25   Celsius (na ,na ,na ,na )(Celsius)
 P0          Temp2           Normal          31   Celsius (na ,na ,na ,na )(Celsius)
 P0          Temp3           Normal          37   Celsius (na ,na ,na ,na )(Celsius)
 R0          VDMB1: VX1      Normal          1226 mV      na
 R0          VDMB1: VX2      Normal          6944 mV      na
 R0          VDMB1: VX3      Normal          1226 mV      na
 R0          VDMB1: VX4      Normal          1000 mV      na
 R0          VDMB1: VP1      Normal          1789 mV      na
 R0          VDMB1: VP2      Normal          2555 mV      na
 R0          VDMB1: VP3      Normal          2556 mV      na
 R0          VDMB1: VP4      Normal          1049 mV      na
 R0          VDMB1: VH       Normal          11993mV      na
```

```
R0          VDMB2: VX2      Normal          4975 mV      na
R0          VDMB2: VX3      Normal          853  mV      na
R0          VDMB2: VX4      Normal          907  mV      na
R0          VDMB2: VX5      Normal          1008 mV      na
R0          VDMB2: VP1      Normal          1787 mV      na
R0          VDMB2: VP2      Normal          3323 mV      na
R0          VDMB2: VH       Normal          12003mV      na
R0          VDMB3: VX1      Normal          968  mV      na
R0          VDMB3: VX2      Normal          1002 mV      na
R0          VDMB3: VX5      Normal          5090 mV      na
R0          VDMB3: VP1      Normal          2492 mV      na
R0          VDMB3: VP2      Normal          1196 mV      na
R0          VDMB3: VP3      Normal          1512 mV      na
R0          VDMB3: VP4      Normal          1509 mV      na
R0          VDMB3: VH       Normal          11998mV      na
R0          Temp: DMB IN    Normal          26   Celsius (45 ,55 ,65 ,70 )(Celsius)
R0          Temp: DMB OUT   Normal          40   Celsius (70 ,75 ,80 ,85 )(Celsius)
R0          Temp: Yoda 0    Normal          54   Celsius (95 ,105,110,115)(Celsius)
R0          Temp: Yoda 1    Normal          62   Celsius (95 ,105,110,115)(Celsius)
R0          Temp: CPU Die   Normal          43   Celsius (100,110,120,125)(Celsius)
R0          Temp: FC FANS   Fan Speed 70%   26   Celsius (29 ,39 ,0  )(Celsius)
R0          VDDC1: VX1      Normal          1005 mV      na
R0          VDDC1: VX2      Normal          7084 mV      na
R0          VDDC1: VX3      Normal          950  mV      na
R0          VDDC1: VP1      Normal          1800 mV      na
R0          VDDC1: VP2      Normal          2493 mV      na
R0          VDDC1: VP3      Normal          3325 mV      na
R0          VDDC1: VH       Normal          12019mV      na
R0          VDDC2: VX2      Normal          751  mV      na
R0          VDDC2: VX3      Normal          749  mV      na
R0          VDDC2: VX5      Normal          5076 mV      na
R0          VDDC2: VP1      Normal          1009 mV      na
R0          VDDC2: VP2      Normal          1008 mV      na
R0          VDDC2: VP3      Normal          1197 mV      na
R0          VDDC2: VP4      Normal          1514 mV      na
R0          VDDC2: VH       Normal          12003mV      na
R0          Temp: DDC IN    Normal          25   Celsius (55 ,65 ,75 ,80 )(Celsius)
R0          Temp: DDC OUT   Normal          35   Celsius (75 ,85 ,95 ,100)(Celsius)
P0          Stby Vin        Normal          230  V AC    na
P0          Stby Iin        Normal          2    A       na
P0          Stby Vout       Normal          12   V DC    na
P0          Stby Iout       Normal          32   A       na
P0          Stby Temp1      Normal          24   Celsius (na ,na ,na ,na )(Celsius)
P0          Stby Temp2      Normal          29   Celsius (na ,na ,na ,na )(Celsius)
P0          Stby Temp3      Normal          35   Celsius (na ,na ,na ,na )(Celsius)
R0          Stby VDMB1: VX1 Normal          1225 mV      na
R0          Stby VDMB1: VX2 Normal          6979 mV      na
R0          Stby VDMB1: VX3 Normal          1226 mV      na
R0          Stby VDMB1: VX4 Normal          999  mV      na
R0          Stby VDMB1: VP1 Normal          1791 mV      na
R0          Stby VDMB1: VP2 Normal          2560 mV      na
R0          Stby VDMB1: VP3 Normal          2558 mV      na
R0          Stby VDMB1: VP4 Normal          1050 mV      na
R0          Stby VDMB1: VH  Normal          11977mV      na
R0          Stby VDMB2: VX2 Normal          5005 mV      na
R0          Stby VDMB2: VX3 Normal          854  mV      na
R0          Stby VDMB2: VX4 Normal          878  mV      na
R0          Stby VDMB2: VX5 Normal          1008 mV      na
R0          Stby VDMB2: VP1 Normal          1789 mV      na
R0          Stby VDMB2: VP2 Normal          3312 mV      na
R0          Stby VDMB2: VH  Normal          11977mV      na
R0          Stby VDMB3: VX1 Normal          972  mV      na
R0          Stby VDMB3: VX2 Normal          1001 mV      na
R0          Stby VDMB3: VX5 Normal          5060 mV      na
```

```
R0          Stby VDMB3: VP1 Normal          2497 mV      na
R0          Stby VDMB3: VP2 Normal          1199 mV      na
R0          Stby VDMB3: VP3 Normal          1510 mV      na
R0          Stby VDMB3: VP4 Normal          1511 mV      na
R0          Stby VDMB3: VH  Normal          11982mV      na
R0          Stby Temp: DMB INormal          22   Celsius (45 ,55 ,65 ,70 )(Celsius)
R0          Stby Temp: DMB ONormal          32   Celsius (70 ,75 ,80 ,85 )(Celsius)
R0          Stby Temp: Yoda Normal          43   Celsius (95 ,105,110,115)(Celsius)
R0          Stby Temp: Yoda Normal          45   Celsius (95 ,105,110,115)(Celsius)
R0          Stby Temp: CPU DNormal          33   Celsius (100,110,120,125)(Celsius)
R0          Stby Temp: FC FAFan Speed 70%   22   Celsius (29 ,39 ,0  )(Celsius)
R0          Stby VDDC1: VX1 Normal          1005 mV      na
R0          Stby VDDC1: VX2 Normal          7070 mV      na
R0          Stby VDDC1: VX3 Normal          949  mV      na
R0          Stby VDDC1: VP1 Normal          1814 mV      na
R0          Stby VDDC1: VP2 Normal          2501 mV      na
R0          Stby VDDC1: VP3 Normal          3331 mV      na
R0          Stby VDDC1: VH  Normal          11993mV      na
R0          Stby VDDC2: VX2 Normal          752  mV      na
R0          Stby VDDC2: VX3 Normal          750  mV      na
R0          Stby VDDC2: VX5 Normal          5052 mV      na
R0          Stby VDDC2: VP1 Normal          1009 mV      na
R0          Stby VDDC2: VP2 Normal          994  mV      na
R0          Stby VDDC2: VP3 Normal          1195 mV      na
R0          Stby VDDC2: VP4 Normal          1514 mV      na
R0          Stby VDDC2: VH  Normal          11993mV      na
R0          Stby Temp: DDC INormal          22   Celsius (55 ,65 ,75 ,80 )(Celsius)
R0          Stby Temp: DDC ONormal          28   Celsius (75 ,85 ,95 ,100)(Celsius)
```

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 Gibraltar 16.10.1	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 fips authorization-key

インストール済みの認証キーを表示するには、**show fips authorization-key** コマンドを使用します。

show fips authorization-key

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 Gibraltar 16.12.1	このコマンドが導入されました。

次に、インストール済みの認証キーを表示する例を示します。

```
Device# show fips authorization-key
FIPS: Stored key (16) : 12345678901234567890123456789012
```

show fips status

デバイスの FIPS のステータスを表示するには、**show fips status** コマンドを使用します。

show fips status

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 Gibraltar 16.12.1	このコマンドが導入されました。

次に、デバイスの FIPS のステータスを表示する例を示します。

```
Device# show fips status
Chassis is running in fips mode
```

show flash wipeout-log

アクセスポイントのファイル数、削除されたバイト数、空き領域、および PID を表示するには、 **show flash wipeout-log** コマンドを使用します。

show flash wipeout-log

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 Dublin 17.11.1	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、AP コンソールで実行する必要があります。

例

次に、アクセスポイントのファイル数、削除されたバイト数、空き領域、および PID を表示する例を示します。

```
Device# show flash wipeout-log
```

show flexconnect office-extend diagnostics

すべての FlexConnect OfficeExtend AP のネットワーク診断の結果を表示するには、**show flexconnect office-extend diagnostics** コマンドを使用します。

show flexconnect office-extend diagnostics

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 Bengaluru 17.5.1	このコマンドが導入されました。

使用上のガイドライン

遅延の詳細（現在、最小、または最大）を定期的に取得するには、次の例に示すように、apプロファイルで link-latency を有効にします。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# link-latency
```

上記の設定が行われていない場合は、次の出力のみが表示されます。

```
Summary of OfficeExtend AP Link Latency

CAPWAP Latency Heartbeat

Current: current latency (ms)
Min: minimum latency (ms)
Max: maximum latency (ms)

Link Test

Upload: DTLS Upload (Mbps)
Latency: DTLS Link Latency (ms)
Jitter: DTLS Link Jitter (ms)

AP Name Last Latency Heartbeat from AP Current Max Min Last Link Test Run Upload Latency
 Jitter
-----------------------------------------------------------------------------------------
ap-18   Disabled                        -       -   -  12/04/20 11:08:58   16     3
   0
```

例

次に、OfficeExtend AP のネットワーク診断情報を表示する例を示します。

```
Device# show flexconnect office-extend diagnostics

Summary of OfficeExtend AP Link Latency

CAPWAP Latency Heartbeat

Current: current latency (ms)
```

```
Min: minimum latency (ms)
Max: maximum latency (ms)

Link Test

Upload: DTLS Upload (Mbps)
Latency: DTLS Link Latency (ms)
Jitter: DTLS Link Jitter (ms)

AP Name Last Latency Heartbeat from AP Current Max Min Last Link Test Run Upload Latency
 Jitter
-------------------------------------------------------------------------------------------------
ap-18    1 minute 1 second             0        0   0  12/04/20 09:19:48  8       2
   0
```

show flow exporter

フロー エクスポー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 **show flow exporter** コマンドを使用します。

show flow exporter [{**export-ids netflow-v9** | [**name**] *exporter-name* [{**statistics** | **templates**}] | **statistics** | **templates**}]

構文の説明

export-ids netflow-v9	（任意）エクスポート可能なNetFlowバージョン9エクスポートフィールドとその ID を表示します。
name	（任意）フローエクスポータの名前を指定します。
exporter-name	（任意）以前に設定されたフローエクスポータの名前。
statistics	（任意）すべてのフローエクスポータまたは指定されたフローエクスポータの統計情報を表示します。
templates	（任意）すべてのフローエクスポータまたは指定されたフローエクスポータのテンプレート情報を表示します。

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、device で設定されているすべてのフロー エクスポータのステータスと統計情報を表示する例を示します。

```
デバイス# show flow exporter
Flow Exporter FLOW-EXPORTER-1:
  Description:              Exports to the datacenter
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 192.168.0.1
    Source IP address:      192.168.0.2
    Transport Protocol:     UDP
    Destination Port:       9995
    Source Port:            55864
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
```

次の表で、この出力に表示される重要なフィールドについて説明します。

表 *12 : show flow exporter* のフィールドの説明

フィールド	説明
Flow Exporter	設定したフロー エクスポータの名前。
Description	エクスポータに設定した説明、またはユーザ定義のデフォルトの説明。
Transport Configuration	このエクスポータのトランスポート設定フィールド。
Destination IP address	宛先ホストの IP アドレス。
Source IP address	エクスポートされたパケットで使用される送信元 IP アドレス。
Transport Protocol	エクスポートされたパケットで使用されるトランスポート層プロトコル。
Destination Port	エクスポートされたパケットが送信される宛先 UDP ポート。
Source Port	エクスポートされたパケットが送信される送信元 UDP ポート。
DSCP	Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値。
TTL	存続可能時間値。
Output Features	**output-features** コマンドが使用されたかどうかを指定します。このコマンドが使用されると、Flexible NetFlow エクスポート パケット上で出力機能が実行されます。

次に、device で設定されているすべてのフロー エクスポータのステータスと統計情報を表示する例を示します。

```
デバイス# show flow exporter name FLOW-EXPORTER-1 statistics
Flow Exporter FLOW-EXPORTER-1:
  Packet send statistics (last cleared 2w6d ago):
    Successfully sent:         0                     (0 bytes)
```

show flow interface

インターフェイスの 設定およびステータスを表示するには、特権 EXEC モードで **show flow interface** コマンドを使用します。

show flow interface [*type number*]

構文の説明

type	（任意） アカウンティング設定情報を表示するインターフェイスのタイプ。
number	（任意） アカウンティング設定情報を表示するインターフェイスの番号。

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、イーサネット インターフェイス 0/0 と 0/1 の アカウンティング設定を表示する例を示します。

```
デバイス# show flow interface gigabitethernet1/0/1

Interface Ethernet1/0
        monitor:          FLOW-MONITOR-1
        direction:        Output
        traffic(ip):      on
デバイス# show flow interface gigabitethernet1/0/2
Interface Ethernet0/0
        monitor:          FLOW-MONITOR-1
        direction:        Input
        traffic(ip):      sampler SAMPLER-2#
```

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 *13 : show flow interface* のフィールドの説明

フィールド	説明
Interface	情報が適用されるインターフェイス。
monitor	インターフェイス上に設定されているフローモニタの名前。
direction:	フローモニタによってモニタされているトラフィックの方向。 次の値が可能です。 • Input：インターフェイスが受信しているトラフィック。 • Output：インターフェイスが送信しているトラフィック。

フィールド	説明
traffic(ip)	フロー モニタが通常モードとサンプラー モードのどちらであるかを示します。 次の値が可能です。 • on：通常モード。 • sampler：サンプラー モード（サンプラーの名前も表示されます）。

show flow monitor

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**show flow monitor**コマンドを使用します。

構文の説明

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。
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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

show flowmonitor *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 が使用するキー フィールドです。**show flow monitor** *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、 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。

```
デバイス# 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 *14 : show flow monitor monitor-name* フィールドの説明

フィールド	説明
Flow Monitor	設定したフロー モニタの名前。
Description	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。
Flow Record	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。
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。
Status	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。
Size	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。

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。

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。

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。

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。

show flow record

フロー レコード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 **show flow record** コマンドを使用します。

show flow record [{[**name**] *record-name*}]

構文の説明

name	（任意）フロー レコードの名前を指定します。
record-name	（任意）前に設定されたユーザ定義のフロー レコードの名前。

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、FLOW-RECORD-1 のステータスおよび統計情報を表示する例を示します。

```
デバイス# show flow record FLOW-RECORD-1
flow record FLOW-RECORD-1:
  Description:        User defined
  No. of users:       0
  Total field space:  24 bytes
  Fields:
    match ipv6 destination address
    match transport source-port
    collect interface input
```

show flow record wireless avc basic

wireless avc basic のフローレコードに関する情報を表示するには、**show flow record wireless avc basic** コマンドを使用します。

show flow record wireless avc basic

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、wireless avc basic のフローレコードに関する情報を表示する例を示します。

```
Device# show flow record wireless avc basic

flow record wireless avc basic:
  Description:        Basic Wireless AVC template
  No. of users:       1
  Total field space:  78 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match flow direction
    match application name
    match wireless ssid
    collect counter bytes long
    collect counter packets long
    collect wireless ap mac address
    collect wireless client mac address
```

show flow record wireless avc ipv6 basic

wireless avc ipv6 basic のフローレコードに関する情報を表示するには、**show flow record wireless avc ipv6 basic** コマンドを使用します。

show flow record wireless avc ipv6 basic

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、wireless avc ipv6 basic のフローレコードに関する情報を表示する例を示します。

```
Device# show flow record wireless avc ipv6 basic

flow record wireless avc ipv6 basic:
  Description:        Ipv6 Wireless AVC flow template
  No. of users:       1
  Total field space:  102 bytes
  Fields:
    match ipv6 protocol
    match ipv6 source address
    match ipv6 destination address
    match transport source-port
    match transport destination-port
    match flow direction
    match wireless ssid
    collect counter bytes long
    collect counter packets long
    collect application name
    collect wireless ap mac address
    collect wireless client mac address
```

show gnxi state

gnxi の詳細を確認するには、**show gnxi state** コマンドを使用します。

show gnxi state

構文の説明

detail	gnxi の詳細な状態を表示します。
stats	gnxi の動作統計を表示します。

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 Bengaluru 17.6.1	このコマンドが導入されました。

次に、gnxi の詳細を確認する例を示します。

```
Device# show gnxi state detail
Settings
========
Server: Enabled
Server port: 50052
Secure server: Disabled
Secure server port: 5000
Secure client authentication: Enabled
Secure trustpoint: test
Secure client trustpoint:
Secure password authentication: Disabled

GNMI
====
Admin state: Enabled
Oper status: Up
State: Provisioned

gRPC Server
-----------
Admin state: Enabled
Oper status: Up

Configuration service
---------------------
Admin state: Enabled
Oper status: Up

Telemetry service
-----------------
Admin state: Enabled
Oper status: Up

GNOI
```

```
====

Cert Management service
-----------------
Admin state: Enabled
Oper status: Up

OS Image service
----------------
Admin state: Disabled
Oper status: Up
Supported: Not supported on this platform
```

show history channel interface dot11Radio all

チャネルの変更またはトリガーの理由と履歴を確認するには、**show history channel interface dot11Radio all** コマンドを使用します。

show history channel interface dot11Radio 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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、チャネルの変更またはトリガーの理由と履歴を確認する例を示します。

```
Device# show history channel interface dot11Radio all

               Timestamp Slot Client count Channel Trigger
Fri May 31 12:57:04 2019    0            0      11 RRM-DCA
Fri May 31 13:10:02 2019    0            0       1 RRM-DCA
Fri May 31 12:57:04 2019    1            0      60  Manual
Fri May 31 13:00:16 2019    1            0     149     DFS
```

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** | **private-vlan mapping** | **pruning** | **stats** | **status** [{**err-disabled**}] | **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、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 メンバのすべてのインターフェイスの機能を表示します。 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。
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。

private-vlan mapping	（任意）VLAN スイッチ仮想インターフェイス（SVI）のプライベート VLAN のマッピング情報を表示します。スイッチが LAN Base フィーチャ セットを実行している場合、このキーワードは使用できません。
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。
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**、**rate-limit**、および **shape** 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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、スタックのシャーシ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 シャーシがない場合、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。

```
デバイス# 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、**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。

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

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。

```
デバイス# 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。

```
デバイス# 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、プライベートVLANが設定されている場合の特定のインターフェイスの**show interfaces status**コマンドの出力を示します。ポート22をプライベートVLANホストポートとして設定しています。ポート22は、プライマリVLAN 20とセカンダリVLAN 25に関連付けられます。

```
デバイス# show interfaces gigabitethernet1/0/22 status
Port       Name      Status      Vlan      Duplex      Speed      Type
Gi1/0/22             connected   20,25     a-full      a-100      10/100BaseTX
```

次の例では、ポート20がプライベートVLAN無差別ポートとして設定されています。この出力は、プライマリVLAN 20だけを表示します。

```
デバイス# show interfaces gigabitethernet1/0/20 status
Port       Name      Status      Vlan      Duplex      Speed      Type
Gi1/0/20             connected   20        a-full      a-100      10/100BaseTX
```

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

```
デバイス# 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。

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


デバイス# 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
```

show interfaces dot11Radio asr-info

WLAN上の高度なスケジューリング要求クライアントの高度なスケジューリング要求機能およびアップリンク遅延の統計とともに、高度なスケジューリング要求の統計を表示するには、**show interfaces dot11Radio asr-info** コマンドを使用します。

show interfaces dot11Radio asr-info *radio-interface-number* { **all** | *mac-address* }

構文の説明

radio-interface-number	802.11 無線のインターフェイス番号。
all	WLAN 上のすべての高度なスケジューリング要求クライアントの高度なスケジューリング要求機能およびアップリンク遅延の統計とともに、高度なスケジューリング要求の統計を表示します。
mac-address	AP の MAC アドレス。

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 Bengaluru 17.4.1	このコマンドが追加されました。

例

次に、WLAN 上のすべての高度なスケジューリング要求クライアントの高度なスケジューリング要求機能およびアップリンク遅延の統計とともに、高度なスケジューリング要求の統計を表示する例を示します。

```
Device# show interfaces dot11Radio 1 asr-info all

[*10/12/2020 18:45:21.0149]
[*10/12/2020 18:45:21.0150]  Client-MAC:[26:52:CF:C8:D0:1C] AID:[3] ASR-Capability:[0x1]
[*10/12/2020 18:45:21.0150]  BE- LAT[0-20]:[267] LAT[20-40]:[57] LAT[40-100]:[32]
LAT[>100]:[26]
[*10/12/2020 18:45:21.0150]  BK- LAT[0-20]:[0] LAT[20-40]:[0] LAT[40-100]:[0] LAT[>100]:[0]
[*10/12/2020 18:45:21.0150]  VI- LAT[0-20]:[0] LAT[20-40]:[0] LAT[40-100]:[0] LAT[>100]:[0]
[*10/12/2020 18:45:21.0150]  VO- LAT[0-20]:[2222] LAT[20-40]:[409] LAT[40-100]:[224]
LAT[>100]:[163]
[*10/12/2020 18:45:21.0150]
[*10/12/2020 18:45:21.0206] HTT_PEER_DETAILS_TLV:
[*10/12/2020 18:45:21.0206] peer_type = 0
[*10/12/2020 18:45:21.0206] sw_peer_id = 98
[*10/12/2020 18:45:21.0206] vdev_id = 25
[*10/12/2020 18:45:21.0206] pdev_id = 0
[*10/12/2020 18:45:21.0206] ast_idx = 1187
[*10/12/2020 18:45:21.0206] mac_addr = 26:52:cf:c8:d0:1c
[*10/12/2020 18:45:21.0206] peer_flags = 0x200006f9
[*10/12/2020 18:45:21.0206] qpeer_flags = 0x8
[*10/12/2020 18:45:21.0206]
[*10/12/2020 18:45:21.0206] HTT_STATS_PEER_ASR_STATS_TLV
[*10/12/2020 18:45:21.0206] asr_bmap: 0x8
[*10/12/2020 18:45:21.0206] asr_muedca_update_cnt: 1
```

```
[*10/12/2020 18:45:21.0206] asr_muedca_reset_cnt: 1
[*10/12/2020 18:45:21.0206] asr_ul_mu_bsr_trigger: 2376
[*10/12/2020 18:45:21.0206] asr_min_trig_intv- BE:0         BK:0 VI:0 VO:19
[*10/12/2020 18:45:21.0206] asr_max_trig_intv- BE:0         BK:0 VI:0 VO:20
[*10/12/2020 18:45:21.0207] asr_min_alloc_rate- BE:0         BK:0 VI:0 VO:12
[*10/12/2020 18:45:21.0207] asr_ul_su_data_ppdu_cnt- BE:0         BK:0 VI:0 VO:2149
[*10/12/2020 18:45:21.0207] asr_ul_su_data_ppdu_bytes- BE:0         BK:0 VI:0 VO:757546
[*10/12/2020 18:45:21.0207] asr_ul_mu_trig_ppdu_cnt- BE:0         BK:0 VI:0 VO:5002
[*10/12/2020 18:45:21.0207] asr_ul_mu_trig_ppdu_bytes- BE:0         BK:0 VI:0 VO:2400960
[*10/12/2020 18:45:21.0207] asr_ul_mu_data_ppdu_cnt- BE:0         BK:0 VI:0 VO:2134
[*10/12/2020 18:45:21.0207] asr_ul_mu_data_ppdu_bytes- BE:0         BK:0 VI:0 VO:736578
[*10/12/2020 18:45:21.0207] asr_ul_mu_data_padding_bytes- BE:0         BK:0 VI:0 VO:2953488
```

show interfaces wired

有線インターフェイスの詳細を表示するには、**show interfaces wired** コマンドを使用します。

show interfaces wired *wired-interface-number*

構文の説明

wired-interface-number	有線インターフェイス番号。

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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、有線インターフェイスの詳細を表示する例を示します。

```
Device# show interfaces wired 0

wired0    Link encap:Ethernet  HWaddr C8:8B:5E:BA:D0 eMac Status: UP
          inet addr:20.200.51.14  Bcast:20.255.255.255  Mask:255.255.255.255
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:2400  Metric:1
          full Duplex, 1000 Mb/s

Wired0 Port Statistics:
ID         :               2             TYPE       :               0
RX PKTS    :           35109/431         TX PKTS    :            1307/11
RX OCTETS  :         2899435/34925       TX OCTETS  :          377424/1575
RX ERR     :             287/0           TX ERR     :               0/0
```

show ip

IP 情報を表示するには、**show ip** コマンドを使用します。

構文の説明

access-lists	IP アクセス リストを表示する
interface	IP インターフェイスのステータスおよび設定を表示する
brief	IP ステータスおよび設定の概要を表示する
route	IP ルーティング テーブルを表示する
tunnel	IP トンネル情報を表示する
eogre	EoGRE トンネル情報を表示する
domain	EoGRE トンネル ドメイン情報を表示する
forwarding-table	EoGRE トンネルのカプセル化およびカプセル化解除の情報を表示する
gateway	EoGRE トンネルのゲートウェイ情報を表示する
fabric	IP ファブリック トンネルの情報を表示する
summary	すべてのトンネルの情報を表示する

コマンド モード

User EXEC (>)

Privileged EXEC (#)

コマンド履歴

リリース	変更内容
8.1.111.0	このコマンドが導入されました。

次に、IP アクセス リストについての情報を表示する例を示します。

```
cisco-wave2-ap# show ip access-lists
```

show ip igmp snooping igmpv2-tracking

グループおよびIPアドレス エントリを表示するには、特権 EXEC モードで **show ip igmp snooping igmpv2-tracking** コマンドを使用します。

（注） このコマンドでは、有線結合ではなく、ワイヤレス マルチキャスト IGMP 結合に関するグループおよびIPアドレス エントリのみ表示されます。また、このコマンドでは、ワイヤレス マルチキャストが有効になっている場合のみ出力が表示されます。

show ip igmp snooping igmpv2-tracking

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 Gibraltar 16.10.1	このコマンドが導入されました。

show ip igmp snooping querier

device で設定されている IGMP クエリアの設定と操作情報を表示するには、ユーザ EXEC モードで **show ip igmp snooping querier** コマンドを使用します。

show ip igmp snooping querier ［**vlan** *vlan-id*］ ［**detail** ］

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。範囲は 1 ～ 1001 と 1006 ～ 4094 です。
detail	（任意）IGMP クエリア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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

IGMP クエリ メッセージを送信する検出デバイス（クエリアとも呼ばれます）の IGMP バージョンと IP アドレスを表示するには、**show ip igmp snooping querier** コマンドを使用します。サブネットは複数のマルチキャストルータを保有できますが、IGMP クエリアは 1 つしか保有できません。IGMPv2 を実行しているサブネットでは、マルチキャスト ルータの 1 つがクエリアとして設定されます。クエリアには、レイヤ 3 device を指定できます。

show ip igmp snooping querier コマンド出力では、クエリアが検出された VLAN およびインターフェイスも表示されます。クエリアが device の場合、出力の Port フィールドには「Router」と表示されます。クエリアがルータの場合、出力の Port フィールドにはクエリアを学習したポート番号が表示されます。

show ip igmp snooping querier detail ユーザ EXEC コマンドは、**show ip igmp snooping querier** コマンドに似ています。ただし、**show ip igmp snooping querier** コマンドでは、device クエリアによって最後に検出されたデバイスの IP アドレスのみが表示されます。

show ip igmp snooping querier detail コマンドでは、device クエリアによって最後に検出されたデバイスの IP アドレスのほか、次の追加情報が表示されます。

- VLAN で選択されている IGMP クエリア
- VLAN で設定された device クエリア（存在する場合）に関連する設定情報と動作情報

式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。

例

次に、**show ip igmp snooping querier** コマンドの出力例を示します。

```
デバイス> show ip igmp snooping querier
Vlan      IP Address     IGMP Version        Port
---------------------------------------------------
1         172.20.50.11   v3                  Gi1/0/1
2         172.20.40.20   v2                  Router
```

次に、**show ip igmp snooping querier detail** コマンドの出力例を示します。

```
デバイス> show ip igmp snooping querier detail

Vlan      IP Address     IGMP Version   Port
-----------------------------------------------------------
1         10.0.0.10      v2             Fa8/0/1
Global IGMP device querier status

-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 0.0.0.0
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
Vlan 1:   IGMP device querier status
-----------------------------------------------------------
elected querier is 10.0.0.10         on port Fa8/0/1
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 10.1.1.65
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
operational state              : Non-Querier
operational version            : 2
tcn query pending count        : 0
```

show ip igmp snooping wireless mcast-spi-count

device に送信されるマルチキャスト グループ ID（MGID）ごとのマルチキャスト ステートフル パケット インスペクション（SPI）の数の統計を表示するには、特権 EXEC モードで **show ip igmp snooping wireless mcast-spi-count** コマンドを使用します。

show ip igmp snooping wireless mcast-spi-count

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 Gibraltar 16.10.1	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

例

次に、**show ip igmp snooping wireless mcast-spi-count** コマンドの出力例を示します。

```
デバイス# show ip igmp snooping wireless mcast-spi-count

Stats for Mcast Client Add/Delete SPI Messages Sent to WCM

MGID    ADD MSGs        Del MSGs
--------------------------------
4160    1323            667
```

show ip igmp snooping wireless mgid

マルチキャスト グループ ID（MGID）マッピングを表示するには、特権 EXEC モードで **show ip igmp snooping wireless mgid** コマンドを使用します。

show ip igmp snooping wireless mgid

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 Gibraltar 16.10.1	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

例

次に、**show ip igmp snooping wireless mgid** コマンドの出力例を示します。

```
デバイス# show ip igmp snooping wireless mgid

Total number of L2-MGIDs    = 0

Total number of MCAST MGIDs = 0

 Wireless multicast is Enabled in the system
 Vlan     bcast   nonip-mcast   mcast    mgid    Stdby Flags
 1     Disabled   Disabled   Enabled    Disabled  0:0:1:0
 25    Disabled   Disabled   Enabled    Disabled  0:0:1:0
 34    Disabled   Disabled   Enabled    Disabled  0:0:1:0
 200   Disabled   Disabled   Enabled    Disabled  0:0:1:0
 1002  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1003  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1004  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1005  Enabled    Enabled    Enabled    Disabled  0:0:1:0

Index  MGID                  (S, G, V)
-----------------------------------------------------------
```

show ip nbar protocol-discovery wlan

WLAN の NBAR プロトコル検出統計情報を表示するには、**show ip nbar protocol-discovery wlan** コマンドを使用します。

show ip nbar protocol-discovery wlan *wlan-name*

構文の説明

wlan-name	WLAN 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、*mywlan* という名前の WLAN の NBAR プロトコル検出統計情報を表示する例を示します。

```
Device# show ip nbar protocol-discovery wlan mywlan
```

show ipv6 access-list

現在のすべての IPv6 アクセス リストの内容を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 access-list** コマンドを使用します。

show ipv6 access-list [*access-list-name*]

構文の説明

access-list-name	（任意）アクセスリストの名前

コマンド デフォルト

すべての IPv6 アクセス リストが表示されます。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

show ipv6 access-list コマンドは、IPv6 専用である点を除き、**show ip access-list** コマンドと同様の出力を提供します。

例

次の **show ipv6 access-list** コマンドの出力には、inbound、tcptraffic、および outbound という IPv6 アクセス リストが表示されます。

```
Device# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
   permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
         left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
       (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

次に、IPSec で使用する IPv6 アクセス リスト情報を表示する例を示します。

```
Device#  show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
     permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
     permit 89 FE80::/10 any (85 matches) sequence 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 *15 : show ipv6 access-list* フィールドの説明

フィールド	説明
ipv6 access list inbound	IPv6 アクセス リスト名（例：inbound）。
permit	指定されたプロトコル タイプと一致するパケットを許可します。
tcp	伝送制御プロトコル。パケットが一致しなければならない高いレベル（レイヤ 4）のプロトコル タイプ。
any	::/0 と同じです。
eq	TCP または UDP パケットの送信元または宛先ポートを比較する equal オペランド。
bgp	ボーダー ゲートウェイ プロトコル。パケットが一致しなければならない低いレベル（レイヤ 3）のプロトコル タイプ。
reflect	再帰 IPv6 アクセス リストを示します。
tcptraffic (8 matches)	再帰 IPv6 アクセス リストの名前と、そのアクセス リストの一致数。**clear ipv6 access-list** 特権 EXEC コマンドは IPv6 アクセス リストの一致カウンタをリセットします。
sequence 10	着信パケットが比較されるアクセス リストの行のシーケンス。アクセス リストの行は、最初のプライオリティ（最低の数、たとえば 10）から最後のプライオリティ（最高の数、たとえば 80）の順に並んでいます。
host 2001:0DB8:1::1	パケットの送信元アドレスが一致していなければならない送信元 IPv6 ホスト アドレス。
host 2001:0DB8:1::2	パケットの宛先アドレスが一致していなければならない宛先 IPv6 ホストアドレス。
11000	発信接続用の一時送信元ポート番号。
timeout 300	tcptraffic という一時 IPv6 再帰アクセス リストが指定したセッションでタイム アウトするまでのアイドル時間の総間隔（秒単位）。
(time left 243)	tcptraffic という一時 IPv6 再帰アクセス リストが指定したセッションで削除されるまでの残りのアイドル時間（秒単位）。指定したセッションに一致する追加の受信トラフィックがこの値を 300 秒にリセットします。
evaluate udptraffic	udptraffic という IPv6 再帰アクセス リストが outbound という IPv6 アクセス リスト内に入れ子になっていることを示します。

show ipv6 hop-by-hop status

IPv6 ホップバイホップヘッダー処理に関する情報を表示するには、**show ipv6 hop-by-hop status** コマンドを使用します。

show ipv6 hop-by-hop 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

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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、IPv6 ホップバイホップヘッダー処理に関する情報を表示する例を示します。

```
Device# show ipv6 hop-by-hop status
```

show ipv6 mld snooping

スイッチまたは VLAN の IP Version 6（IPv6）マルチキャスト リスナー検出（MLD）スヌーピング設定を表示するには、**show ipv6 mld snooping** コマンドを EXEC モードで使用します。

show ipv6 mld snooping [**vlan** *vlan-id*]

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

スイッチまたは特定の VLAN の MLD スヌーピングの設定を表示するのにこのコマンドを使用します。

1002 ～ 1005 の VLAN 番号は、トークンリング VLAN および FDDI VLAN のために予約されているため、MLD スヌーピングには使用できません。

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** 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。

例

次に、show ipv6 mld snooping vlan コマンドの出力例を示します。ここでは、特定の VLAN のスヌーピング特性を表示します。

```
Device# show ipv6 mld snooping vlan 100
Global MLD Snooping configuration:
-------------------------------------------
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
Vlan 100:
--------
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
```

```
Last listener query count : 2
Last listener query interval : 1000
```

次に、**show ipv6 mld snooping** コマンドの出力例を示します。ここでは、スイッチ上の VLAN すべてのスヌーピング特性を表示します。

```
Device# show ipv6 mld snooping
Global MLD Snooping configuration:
-------------------------------------------
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000

Vlan 1:
--------
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 1
Last listener query count : 2
Last listener query interval : 1000

<output truncated>

Vlan 951:
--------
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
```

show ipv6 mld snooping querier vlan

VLAN 内の IPv6 MLD クエリア情報を表示するには、**show ipv6 mld snooping querier vlan** コマンドを使用します。

show ipv6 mld snooping querier vlan *vlan-id*

構文の説明

vlan-id	VLAN ID。有効な範囲は 1 ～ 1001 または 1006 ～ 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ID が 3 である VLAN の IPv6 MLD クエリア情報を表示する例を示します。

```
Device# show ipv6 mld snooping querier vlan 3
```

show ipv6 mld snooping wireless mgid

IPv6 MLD ワイヤレス関連スヌーピング イベントのマルチキャスト グループ識別子（MGID）マッピング情報を表示するには、**show ipv6 mld snooping wireless mgid** コマンドを使用します。

show ipv6 mld snooping wireless mgid

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、IPv6 MLD ワイヤレス関連スヌーピング イベントのマルチキャスト グループ識別子（MGID）マッピング情報を表示する例を示します。

```
Device# show ipv6 mld snooping wireless mgid
```

show ipv6 nd ra specific-route

IPv6 ネイバー探索ルータ アドバタイズメント メッセージに関する情報を表示するには、**show ipv6 nd ra specific-route** コマンドを使用します。

show ipv6 nd ra specific-route *interface*

構文の説明

interface	インターフェイス情報

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 Bengaluru 17.6.1	このコマンドが導入されました。

使用上のガイドライン

インターフェイスを指定しない場合は、すべてのインターフェイスで設定されているルートが表示されます。

例

次に、IPv6 ネイバー探索ルータ アドバタイズメント メッセージに関する情報を表示する例を示します。

```
Device# show ipv6 nd ra specific-route
```

show ldap attributes

デフォルトの LDAP 属性マッピングに関する情報を表示するには、**show ldap attributes** コマンドを使用します。

show ldap attributes

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、デフォルトの LDAP 属性マッピングに関する情報を表示する例を示します。

```
デバイス# show ldap attributes
LDAP Attribute                    Format     AAA Attribute
==============                    ======     =============
airespaceBwDataBurstContract      Ulong      bsn-data-bandwidth-burst-contr
userPassword                      String     password
airespaceBwRealBurstContract      Ulong      bsn-realtime-bandwidth-burst-c
employeeType                      String     employee-type
airespaceServiceType              Ulong      service-type
airespaceACLName                  String     bsn-acl-name
priv-lvl                          Ulong      priv-lvl
memberOf                          String DN  supplicant-group
cn                                String     username
airespaceDSCP                     Ulong      bsn-dscp
policyTag                         String     tag-name
airespaceQOSLevel                 Ulong      bsn-qos-level
airespace8021PType                Ulong      bsn-8021p-type
airespaceBwRealAveContract        Ulong      bsn-realtime-bandwidth-average
airespaceVlanInterfaceName        String     bsn-vlan-interface-name
airespaceVapId                    Ulong      bsn-wlan-id
airespaceBwDataAveContract        Ulong      bsn-data-bandwidth-average-con
sAMAccountName                    String     sam-account-name
meetingContactInfo                String     contact-info
telephoneNumber                   String     telephone-number
Map: att_map_1
department                        String DN  element-req-qos
```

show ldap server

LDAP サーバー情報を表示するには、**show ldap server** コマンドを使用します。

show ldap server { *server-name* | **all** }

構文の説明

server-name	サーバ名を指定します。
all	すべてのサーバーの情報。

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、LDAP サーバーの情報を表示する例を示します。

```
Device# show ldap server all
```

show license air entities

Cisco Catalyst ワイヤレスコントローラに接続されているアクティブな AP、新しい AP、および削除された AP に関する情報を表示するには、特権 EXEC モードで **show license air entities** コマンドを入力します。

show license air entities { **added** | **bulk** | **deleted** | **no-change** | **summary** }

構文の説明

`added`	新しくレポートされた AP のリストを表示します。新しく追加された AP は、製品インスタンスにより生成された最後の RUM レポートにリストされていなかった AP です。
bulk	製品インスタンスの現在アクティブなすべての AP のリストを表示します
deleted	削除された AP のリストを表示します。削除 AP は、製品インスタンスにより生成された最後の RUM レポートでアクティブな AP としてリストされていた、現在は切断されている AP です。
no-change	最後のレポート以降、ステータスに変化がない AP のリストを表示します。
summary	RUM レポート生成の詳細と、アクティブな AP、新しい AP、および削除された AP に関する情報を表示し、いつまでに製品インスタンスに確認応答（ACK）をインストールする必要があるかを示します。

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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンスに関する情報が表示されるようになりました。
Cisco IOS XE Cupertino 17.7.1	**show license air entities summary** コマンドの出力が拡張され、Cisco Catalyst 9800-CL ワイヤレスコントローラでのみ、新しいフィールドの `License Ack expected within` が表示されるようになりました

使用上のガイドライン

スマートライセンス：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます。

ポリシーを使用したスマートライセンス：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.2 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

例

show license air entities summary コマンドについてディスプレイに表示されるフィールドについては、表 16 : show license air entities summary のフィールドの説明 （1293 ページ）を参照してください。

出力例については、次を参照してください

- Cisco Catalyst 9800-CL ワイヤレスコントローラでの show license air entities summary （1294 ページ）
- Cisco Catalyst 9800-L ワイヤレスコントローラでの show license air entities summary （1294 ページ）

表 *16 : show license air entities summary* のフィールドの説明

フィールド	説明
Last license report time	最後の RUM レポートが生成された時間（ローカルタイムゾーン）。
Upcoming license report time	次の RUM レポートが生成される時間（ローカルタイムゾーン）。
No. of APs active at last report	最後に生成された RUM レポートでアクティブな AP としてリストされていた AP の総数。
No. of APs newly added with last report	最後に生成された RUM レポート内の新しい AP の数。 たとえば、ここに表示される数値が 2 の場合は、前々回の RUM レポートにこれらの 2 つの AP がリストされていなかったため、製品インスタンスにより生成された最後の RUM レポートにこれらの AP が新しく追加されたことを意味します。
No. of APs deleted with last report	最後に生成された RUM レポートの時点で削除された AP の合計数。 たとえば、ここに表示される数値が 2 の場合は、前々回の RUM レポートに含まれていた 2 つの AP が、最後に生成された RUM レポートで削除されたことを意味します。
License Ack expected within	（注） このフィールドは、Cisco IOS XE Cupertino 17.7.1 以降のリリースを実行している Cisco Catalyst 9800-CL ワイヤレスコントローラでのみ表示されます。 このフィールドが表示されている場合は、RUM レポートを完了し、製品インスタンスで ACK が少なくとも 1 回利用できるようにする必要があることを意味します。

Cisco Catalyst 9800-CL ワイヤレスコントローラでの show license air entities summary

次に、Cisco Catalyst 9800-CL ワイヤレスコントローラで ACK がいつ必要になるかを特定する例を示します

Cisco IOS XE Cupertino 17.7.1 以降、Cisco Catalyst 9800-CL ワイヤレスコントローラを使用している場合は、RUM レポートを完了し、製品インスタンスで ACK が少なくとも 1 回利用できるようにする必要があります。これは、正しい最新の使用状況情報が CSSM に反映されるようにするためです。

17.7.1 より前は、レポートと ACK のインストールは、Cisco Catalyst 9800-CL ワイヤレスコントローラでは必須ではありませんでした。

次に、Cisco Catalyst 9800-CL ワイヤレスコントローラの出力例を示します。この例では、179 日以内に ACK を製品インスタンスで使用可能にする必要があります。この期限に間に合わない場合、現在アクティブな AP は切断されませんが、ACK の期限が過ぎた後は新しい AP の参加は許可されません。また、最初の ACK がインストールされるまでシステムメッセージが毎日表示されます。

```
Device# show license air entities summary
Upcoming license report time.....................: 21:05:16.092 UTC Mon Oct 25 2021
No. of APs active at last report.................: 57
No. of APs newly added with last report..........: 57
No. of APs deleted with last report..............: 0
License Ack expected within.....................: 179 days
```

この要件の詳細については、設定ガイドを参照してください。『Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide』のバージョン Cisco IOS XE Cupertino 17.7.1 以降で、「System Configuration」→「Smart Licensing Using Policy」→「RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller」を参照してください。

Cisco Catalyst 9800-L ワイヤレスコントローラでの show license air entities summary

次に、Cisco Catalyst 9800-L ワイヤレスコントローラの出力例を示します。このデバイスの出力には [License Ack expected within] フィールドが表示されないことに注意してください。すべての Cisco Catalyst ワイヤレスコントローラ（Cisco Catalyst 9800-CL ワイヤレスコントローラを除く）のレポート要件は、ポリシーを使用したスマートライセンス環境の標準ガイドラインに従っていて、ポリシー（**show license status**）またはシステムメッセージで示された場合にレポートが必要です。

```
Device# show license air entities summary
Upcoming license report time.....................: 15:13:27.403 IST Tue Oct 26 2021
No. of APs active at last report.................: 1
No. of APs newly added with last report..........: 1
No. of APs deleted with last report..............: 0
```

show license all

すべてのライセンス情報を表示するには、特権 EXEC モードで **show license all** コマンドを入力します。このコマンドは、ステータス、承認、UDI、および使用状況の情報をすべて組み合わせて表示します。

show license all

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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンスに関する情報が表示されるようになりました。 コマンド出力にスマートアカウントとバーチャルアカウントの情報が表示されなくなりました。
Cisco IOS XE Cupertino 17.7.1	コマンドの出力が強化され、次の情報が表示されるようになりました。 • RUM レポートの統計情報（[Usage Report Summary] セクション）。 • [Account Information] セクションにあるスマートアカウントとバーチャルアカウントの情報。

使用上のガイドライン

スマートライセンス：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます。

[Smart Licensing Using Policy]：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2 以降のリリースの場合、コマンド出力には Smart Licensing Using Policy に関連するフィールドが表示されます。

このコマンドは、他の **show license** コマンドの出力を連結して、さまざまな種類のライセンス情報をまとめて表示できるようにします。フィールドの説明については、以下に示すリンクから対応するコマンドを参照してください。

show license all コマンドの [Smart Licensing Status] セクションと [Account Information] セクションは、show license status （1318 ページ） コマンドの出力に対応しています。

show license all コマンドの [License Usage] セクションは、show license usage （1349 ページ） コマンドの出力に対応しています。

show license all コマンドの [Product Information] セクションは、show license udi （1347 ページ） コマンドの出力に対応しています。

show license all コマンドの [Agent Version] セクションには、スマートエージェントのバージョンが表示され、このコマンドでのみ使用できます。

show license all コマンドの [License Authorizations] セクションは、show license authorization （1301 ページ） コマンドの出力に対応しています

show license all コマンドの [Usage Report Summary] セクションは、show license tech （1332 ページ） コマンドの出力に対応しています。

例

出力例については、次を参照してください。

例：show license all（Cisco Catalyst 9800-CL ワイヤレスコントローラ、17.7.1） （1296 ページ）

例：show license all（Cisco Catalyst 9800-CL ワイヤレスコントローラ） （1298 ページ）

例：show license all（Cisco Catalyst 9800-CL ワイヤレスコントローラ、17.7.1）

次に、ソフトウェアバージョンが Cisco IOS XE cupertino 17.7.1 である製品インスタンスの **show license all** コマンドの出力例を示します。このリリースでは、[Usage Report Summary] と [Usage Report Summary] の 2 つの新しいセクションが追加されています。

```
Device# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
```

```
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage
=============

No licenses in use

Product Information
===================
UDI: PID:C9800-CL-K9,SN:9KGIXIDOXFE

HA UDI List:
    Active:PID:C9800-CL-K9,SN:9KGIXIDOXFE
    Standby:PID:C9800-CL-K9,SN:9UBKZU955E4

Agent Version
=============
Smart Agent for Licensing: 5.3.14_rel/47

License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:9KGIXIDOXFE
      Status: NOT INSTALLED
  Standby: PID:C9800-CL-K9,SN:9UBKZU955E4
      Status: NOT INSTALLED
```

```
Purchased Licenses:
  No Purchase Information Available

Usage Report Summary:
=====================
Total: 0,  Purged: 0
Total Acknowledged Received: 0,  Waiting for Ack: 0
Available to Report: 0  Collecting Data: 0
```

例：show license all（Cisco Catalyst 9800-CL ワイヤレスコントローラ）

次に、Cisco Catalyst 9800-CL ワイヤレスコントローラの **show license all** コマンドの出力例を示します。同様の出力が、サポートされているすべての Cisco Catalyst ワイヤレスコントローラで表示されます。

```
Device# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED
License Reservation is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Transport Off

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
```

```
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: Nov 01 20:31:46 2020 IST
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage
=============

air-network-advantage (DNA_NWStack):
  Description: air-network-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

air-dna-advantage (AIR-DNA-A):
  Description: air-dna-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

Product Information
===================
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS

HA UDI List:
    Active:PID:C9800-CL-K9,SN:93BBAH93MGS
    Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN

Agent Version
=============
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
```

```
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Last Confirmation code: ad4382fe

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled with DNA-A
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10

Purchased Licenses:
  No Purchase Information Available
```

show license authorization

ライセンス（輸出規制および適用）の承認関連情報を表示するには、特権 EXEC モードで **show license authorization** コマンドを入力します。

show license authorization

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 Amsterdam 17.3.2a	このコマンドが導入されました。

使用上のガイドライン

輸出規制ライセンスまたは適用ライセンスのみ、使用前に承認が必要です。

Cisco Catalyst ワイヤレスコントローラには、輸出制御ライセンスまたは適用ライセンスはありませんが、このコマンドを使用して、移行された SLR 承認コードを表示できます。

例

ディスプレイに表示されるフィールドについては、表 17 : show license authorization のフィールドの説明 （1302 ページ） を参照してください。

出力例については、show license authorization の移行された承認コードの表示 （1305 ページ） を参照してください。

表 *17 : show license authorization* のフィールドの説明

フィールド		説明
Overall Status	設定内にあるすべての製品インスタンスの UDI 情報のヘッダー、インストールされている承認のタイプ、および設定エラー（存在する場合）。 高可用性設定では、設定内にあるすべての UDI がリストされます。	
	Active: ステータス：	アクティブ製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 承認コードがインストールされていることを示すステータスであり、確認コードがある場合は、これも表示されます。
	Standby: ステータス：	スタンバイ製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 承認コードがインストールされていることを示すステータスであり、確認コードがある場合は、これも表示されます。
	Member: ステータス：	メンバー製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 承認コードがインストールされていることを示すステータスであり、確認コードがある場合は、これも表示されます。
	ERROR:	高可用性設定の設定エラーまたは不一致（存在する場合）。

フィールド		説明
承認	詳細なライセンス承認情報のヘッダー。すべてのライセンス、その適用タイプ、および有効期間が表示されます。承認またはモードがアクティブにインストールされているものと一致しない場合、製品インスタンスごとにエラーが表示されます。 このセクションは、製品インスタンスが承認コードを必要とするライセンスを使用している場合にのみ表示されます。	
	():	ライセンス名およびライセンス名の短縮形。
	Description	ライセンスの説明。
	Total available count:	使用可能なライセンスの合計数。 これには、高可用性設定のすべての製品インスタンスに関して、期限切れのサブスクリプション ライセンスを含む、すべての期間のライセンス（永久ライセンスおよびサブスクリプション）が含まれます。
	Enforcement type	ライセンスの適用タイプ。これは、次のいずれかです。 • 適用 • 非適用 • 輸出規制
	Term information:	

フィールド		説明
		ライセンス期間情報を提供するヘッダー。このヘッダーには、次のフィールドが含まれることがあります。 • Active：アクティブ製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 • Authorization type：インストールされている承認コードのタイプとインストール日。タイプは、SLAC、UNIVERSAL、SPECIFIED、PAK、RTU です。 • Start Date：ライセンスが特定の期間または時間の場合に、有効期間の開始日を表示します。 • Start Date：ライセンスが特定の期間または時間の場合に、有効期間の終了日を表示します。 • Term Count：ライセンス数。 • Subscription ID：ライセンスが特定の期間または時間の場合に、ID を表示します。 • License type：ライセンス継続期間。これは、SUBSCRIPTION または PERPETUAL です。 • Standby：スタンバイ製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 • Member：メンバー製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 ライセンスの有効期間の詳細については、次を参照してください： <link tbd>.

フィールド		説明
Purchased Licenses	ライセンス購入情報のヘッダー。	
	Active:	アクティブ製品インスタンスとその UDI。
	Count:	ライセンス数。
	Description:	ライセンスの説明。
	License type:	ライセンス継続期間。これは、SUBSCRIPTION または PERPETUAL です。
	Standby:	スタンバイ製品インスタンスの UDI。
	Member:	メンバー製品インスタンスの UDI。

show license authorization の移行された承認コードの表示

次に、Cisco Catalyst 9800-CL ワイヤレスコントローラの **show license authorization** コマンドの出力例を示します。`Last Confirmation code:` が、移行後に使用できる SLR 承認コードを示しています。同様の出力が、サポートされているすべての Cisco Catalyst ワイヤレスコントローラで表示されます。

```
Device# show license authorization
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Last Confirmation code: ad4382fe

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
  AP Perpetual Networkstack Advantage (DNA_NWStack):
```

```
    Description: AP Perpetual Network Stack entitled with DNA-A
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10

Purchased Licenses:
  No Purchase Information Available
```

show license data translation

ライセンスデータ転換情報を表示するには、特権 EXEC モードで **show license data** コマンドを入力します。

show license data conversion

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（Device#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	このコマンドは、ポリシーを使用したスマートライセンスの導入で、引き続き使用することができます。

使用上のガイドライン

このコマンドはCLIに表示されますが、Cisco Catalyst ワイヤレスコントローラには適用されません。

show license eventlog

ポリシーを使用したスマートライセンスに関連するイベントログを表示するには、特権 EXEC モードで **show license eventlog** コマンドを入力します。

show license eventlog ［ *days* ］

構文の説明

days	イベントログを表示する日数を入力します。0 ～ 2147483647 の範囲の値を指定できます。

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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	ポリシーを使用したスマートライセンスの導入により、次のイベントが追加されました。 • ポリシーのインストールと削除 • 承認コードの要求、インストール、および削除。 • 信頼コードのインストールと削除。 • ライセンス使用状況に関する承認ソース情報の追加。

使用上のガイドライン

ポリシーを使用したスマートライセンス：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

スマートライセンス：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます。

show license history message

製品インスタンスとCSSMまたはCSLU（該当する場合）の間の通信履歴を表示するには、特権 EXEC モードで **show license history message** コマンドを入力します。このコマンドの出力は、テクニカルサポートチームがトラブルシューティングに使用します。

show license history message

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 モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.2a	このコマンドが導入されました。

使用上のガイドライン

解決できないエラーメッセージが表示された場合は、コンソールまたはシステムログに表示されるメッセージともに、シスコのテクニカルサポート担当者に **show license tech support**、**show license history message**、および **show platform software sl-infra** 特権 EXEC コマンドの出力例を提供してください。

show license reservation

ライセンス予約情報を表示するには、特権 EXEC モードで **show license reservation** コマンドを入力します。

show license reservation

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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	このコマンドは、ポリシーを使用したスマートライセンスの導入で、引き続き使用することができます。

使用上のガイドライン

コマンドはCLIで引き続き使用可能であり、対応する出力が表示されますが、ポリシーを使用したスマートライセンシングの導入により、予約の概念は適用されなくなりました。代わりに、特権 EXEC モードで **show license all** コマンドを使用して、移行された SLR ライセンスを表示します（SLR 承認コードはポリシーを使用してスマートライセンスに移行されます）。

show license rum

製品インスタンスのリソース使用率測定レポート（RUM レポート）に関する情報を表示したり、レポート ID、レポートの現在の処理状態、エラー情報（ある場合）、および表示された詳細または概要情報を保存するには、特権 EXEC モードで **show license rum** コマンドを入力します。

show license rum { **feature** { *license_name* | **all** } | **id** { *rum_id* | **all** } } [**detail**] [**save** *path*]

構文の説明

feature { *license_name*	**all** }	ライセンス名に基づいて RUM レポート情報を表示します。 特定のライセンス名を指定してそのライセンスのすべての RUM レポートを表示するか、**all** キーワードを使用して製品インスタンスで使用可能なすべての RUM レポートを表示します。
id { *rum_id*	**all** }	RUM レポート ID に基づいて RUM レポート情報を表示します。 単一のレポートの情報を表示するレポート ID を指定するか、製品インスタンスで使用可能なすべての RUM レポートを表示するには、**all** キーワードを使用します。
detail	詳細な RUM レポート情報を表示します。 これを使用して、ライセンス名ごとの詳細情報と RUM レポート ID ごとの詳細情報を表示できます。
save *path*	表示される情報を保存します。これは簡易バージョンまたは詳細バージョンで、入力した先行キーワードによって異なります。 200 の RUM レポートに関する情報を表示できます。製品インスタンスに 200 を超える RUM レポートがある場合は、テキスト（.txt）ファイルに保存することで、すべての RUM レポートに関する情報を表示できます。 （注） このオプションでは、RUM レポートに関する情報が保存され、レポート用ではありません。使用状況情報を含む XML ファイルである RUM レポートは保存されません。

コマンド モード

特権 EXEC（Device#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが導入されました。

使用上のガイドライン

RUM レポートは、ポリシーで指定されたレポート要件を満たすために、製品インスタンスが生成するライセンス使用状況レポートです。確認応答（ACK）は CSSM からの応答であり、RUM レポートのステータスに関する情報を提供します。レポートの ACK が製品インスタンスで使用可能になると、対応する RUM レポートが不要になり、削除できることが示されます。**show license rum** コマンドを使用すると、次のことができます。

- ID またはライセンス名でフィルタリングされた、製品インスタンスで使用可能な RUM レポートに関する情報を表示します。
- 概要を表示するか、情報の詳細ビューを表示します。
- RUM レポートをそのライフサイクル全体（最初に生成されてから CSSM から確認されるまで）を追跡します。レポートの現在の処理状態と条件を表示することで、レポートワークフローに問題があるかどうか、また問題が発生した場合にはそれを確認できます。
- 表示された情報を保存します。CLI には、最大 200 のレポートに関する情報が表示されます。製品インスタンスに 200 を超えるレポートがあり、それらすべてに関する情報を表示する場合は、表示された情報を .txt ファイルに保存し、表示する目的の場所にエクスポートします。

RUM レポート情報の統計ビュー（製品インスタンスのレポートの総数、対応する ACK を含むレポートの数、ACK を待機しているレポートの数など）を表示するには、**show license all** および **show license tech** 特権 EXEC コマンドについては、[Usage Report Summary] セクションを参照してください。

show license tech コマンドは、RUM レポートに問題がある場合に、シスコ テクニカル サポート チームがトラブルシューティングに使用できる RUM レポート関連情報も提供します。

例

ディスプレイに表示されるフィールドについては、「#unique_1035 unique_1035_Connect_42_table_ytd_q4m_hrb」と「#unique_1035 unique_1035_Connect_42_table_gtn_q4m_hrb」参照してください。

show license rum コマンドの出力例については、次を参照してください。

- #unique_1035 unique_1035_Connect_42_example_ugm_lsd_4rb
- #unique_1035 unique_1035_Connect_42_example_stg_msd_4rb

表 *18 : show license rum*（簡易ビュー）のフィールド説明

フィールド名	説明
Report Id	RUM レポートを識別する数値フィールドです。製品インスタンスは、生成するすべての RUM レポートに ID を自動的に割り当てます。ID の長さは最大 20 文字です。
状態	このフィールドには、RUM レポートの現在の処理状態が表示され、次のいずれかになります。 • OPEN：新しい測定値がこのレポートに追加されることを意味します。 • CLOSED：このレポートに追加できる新しい測定値がなく、CSSM への通信の準備ができていることを意味します。 • PENDING：送信中にレポートを閲覧した場合に表示される移行ステータスです。 • UNACK：レポートが送信され、CSSM からの確認を待っていることを意味します。 • ACK：レポートが CSSM によって処理または確認され、削除の対象となります。

フィールド名	説明
フラグ	RUM レポートの状態を示し、文字の形式で表示されます。各文字は特定の条件を表し、次のいずれかの値になります。 • N：正常。これは、エラーが検出されておらず、レポートが通常の動作を行っていることを意味します。 • P：消去。これは、システムリソースの制限によりレポートが削除されたことを意味し、ディスク領域の不足またはメモリ不足を示している可能性があります。このフラグが表示された場合は、詳細ビューの [State Change Reason] フィールドを参照してください。 • E：エラー。これは、RUM レポートでエラーが検出されたことを意味します。このフラグが表示される場合、詳細情報については詳細ビューを参照してください。考えられるワークフローの問題には、次のものが含まれますが、これらに限定されません。 • RUM レポートが CSSM によってドロップされました。これが問題の場合、[State] フィールドに値 ACK が表示されますが、[State Change Reason] は ACKED に変更されません。 • RUM レポートデータがありません。これが問題の場合は、[Storage State] フィールドに値 MISSING が表示されます。 • 追跡情報がありません。この場合、[State] フィールドには値 UNACK が表示され、[Transaction ID] フィールドには情報がありません。 （注） RUM レポートで時折発生するエラーは、ユーザーによる操作を必要とせず、問題を示すものではありません。シスコ テクニカル サポート チームに連絡する必要があるのは、多数のレポート（10 を超える）にエラーがある場合だけです。
機能名	RUM レポートが適用されるライセンスの名前です。

表 *19 : show license rum*（詳細ビュー）のフィールド説明

フィールド名	説明
Report Id	RUM レポートを識別する数値フィールドです。製品インスタンスは、生成するすべての RUM レポートに ID を自動的に割り当てます。ID の長さは最大 20 文字です。

フィールド名	説明
Metric Name：	記録されるデータのタイプを示します。 RUM レポートの場合、唯一の可能な値は ENTITLEMENT で、ライセンスの使用状況の測定値を参照します。
Feature Name：	RUM レポートが適用されるライセンスの名前です。
メトリック値	記録されるデータの一意の識別子です。 これは、**show license tech** コマンドの出力の「Entitlement Tag」と同じで、追跡対象のライセンスに関する情報が表示されます。
UDI	製品インスタンスの製品 ID（PID）とシリアル番号で構成されます。
Previous Report Id：	製品インスタンスがライセンスに対して生成した以前の RUM レポート ID です。
Next Report Id：	製品インスタンスがライセンス用に生成する次の RUM レポートに使用する ID です。
State:	RUM レポートの現在の処理状態を表示します。ここに表示される値は、簡易ビューに表示される値と常に同じです。 可能な値のリストについては、上記の「#unique_1035 unique_1035_Connect_42_table_ytd_q4m_hrb」を参照してください。
State Change Reason：	RUM レポートの状態が変更された理由を表示します。すべての状態変更が理由を示すわけではありません。 • NONE：これは、RUM レポートが通常のライフサイクル（たとえば、OPEN→CLOSED→ACK）を通過していることを意味します。この状態変更の理由には、通常、簡易ビューでNフラグ（通常という意味）が表示され、ユーザーによる操作は必要ありません。 • ACKED：RUM レポートは CSSM によって正常に処理されました。 • REMOVED：RUM レポートを受信し、CSSM に削除するように要求されました。 • RELOAD：ある種のデバイスのリロードが原因で、RUM レポートの状態が変更されました。
Start Time：	RUM レポートの測定開始および測定終了を示すタイムスタンプです。 開始時刻と終了時刻を合わせて、測定の対象となる期間を指定します。
End Time：	

フィールド名	説明
Storage State：	RUM レポートの現在のストレージ状態を表示します。次のいずれかの値になります。 • EXIST：RUM レポートのデータがストレージにあることを意味します。 • DELETED：データが意図的に削除されたことを意味します。このストレージ状態の詳細については、**show license tech** コマンドの出力の「`Storage State Change Reason`」を参照してください。 • PURGED：システムリソースの制限によりデータが削除されたことを意味します。このストレージ状態の詳細については、**show license tech** コマンドの出力の「`Storage State Change Reason`」を参照してください。 • MISSING：データがストレージから欠落していることを意味します。レポートが欠落していると識別された場合、リカバリプロセスはありません。
Transaction ID： Transaction Message：	RUM レポートの追跡情報が含まれます。この情報は、ポーリング情報または ACK インポート情報のいずれかである可能性があります。 製品インスタンスが ACK のインポート時にエラーメッセージを受信した場合、トランザクションメッセージにはエラーメッセージが含まれます。 これらのフィールドの情報は、RUM レポートの問題をトラブルシューティングする際に、シスコ テクニカル サポート チームによって使用されます。

例：**show license rum feature**：簡易ビューと詳細ビュー

次に、Cisco Catalyst 9500 シリーズ スイッチでの **show license rum feature***license-name* および **show license rum feature***license-name***detail** コマンドの出力例を示します。他のすべての Catalyst スイッチでも同様の出力が表示されます。

出力は、Cisco DNA Advantage ライセンスのすべての RUM レポートと、その詳細ビューが表示されるようにフィルタ処理されます。

```
Device# show license rum feature air-dna-advantage

Smart Licensing Usage Report:

====================================

Report Id,          State,    Flag, Feature Name

1638055644          CLOSED    N     air-dna-advantage

1638055646          OPEN      N     air-dna-advantage
```

```
Device# show license rum feature air-dna-advantage detail
Smart Licensing Usage Report Detail:
====================================
Report Id: 1638055644
  Metric Name: ENTITLEMENT
  Feature Name: air-dna-advantage
 Metric Value: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790

  UDI: PID:C9800-CL-K9,SN:93SZ7RXN93Y
  Previous Report Id: 0,    Next Report Id: 1638055646
  State: CLOSED,      State Change Reason: RELOAD
  Start Time: Nov 28 12:02:09 2021 UTC,      End Time: Nov 30 22:02:13 2021 UTC
  Storage State: EXIST
  Transaction ID: 0
  Transaction Message: <none>

Report Id: 1638055646
  Metric Name: ENTITLEMENT
  Feature Name: air-dna-advantage
 Metric Value: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790

  UDI: PID:C9800-CL-K9,SN:93SZ7RXN93Y
  Previous Report Id: 1638055644,    Next Report Id: 0
  State: OPEN,      State Change Reason: None
  Start Time: Nov 30 23:12:56 2021 UTC,      End Time: Dec 01 02:12:56 2021 UTC
  Storage State: EXIST
  Transaction ID: 0
  Transaction Message: <none>
```

例：RUM レポートビューの保存

次に、表示された情報を保存する例を示します。

feature キーワードと **all** キーワードを使用すると、出力がフィルタ処理され、製品インスタンスで使用されているすべてのライセンスにおける全 RUM レポートが表示されます。その後、TFTP ロケーションに転送され、そこから開いて情報を表示することができます。

```
Device# show license rum feature all save bootflash:all-rum-stats.txt
Device# copy tftp://10.8.0.6/bootflash:all-rum-stats.txt
```

show license status

データプライバシー、ポリシー、転送、使用状況レポート、信頼コードなどのライセンス設定に関する情報を表示するには、特権EXECモードで**show license status**コマンドを入力します。

show license 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 モード

特権 EXEC（Device#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンスに適用可能な新しいフィールドが反映されました。これには、`Trust code installed:`、`Policy in use`、`Policy name:` 、ポリシーと同様のレポート要件（`Attributes:` ）および使用状況レポートに関連するフィールドが含まれます。 コマンド出力にスマートアカウントとバーチャルアカウントの情報が表示されなくなりました。
Cisco IOS XE Cupertino 17.7.1	コマンド出力が更新され、スマートアカウントと仮想アカウントの情報が表示されるようになりました。

使用上のガイドライン

スマートライセンス：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます。

ポリシーを使用したスマートライセンス：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

出力のアカウント情報

Cisco IOS XE Cupertino 17.7.1 以降、すべての ACK には、CSSM で報告されたスマートアカウントとバーチャルアカウントが含まれています。ACK を受信すると、製品インスタンスにはこの情報の最新バージョンのみが安全に保存されます。これは、ACKのタイムスタンプによって決定されます。したがって、このコマンドの出力の `[Account Information]` セクションに表示されるスマートアカウントとバーチャルアカウントの情報は、常に製品インスタンスで使用可能な最新の ACK に基づいています。

製品インスタンスが1つのスマートアカウントとバーチャルアカウントから別のアカウントに移動された場合、移動後の次のACKにはこの更新された情報が含まれます。このACKが製品インスタンスで使用可能になると、このコマンドの出力が更新されます。

ACK は、直接的に（製品インスタンスが CSSM に接続されている場合）または間接的に（製品インスタンスが CSLU、Cisco DNA Center、または SSM On-Prem を介して CSSM に接続されている場合）、あるいは手動で ACK をインポートすることによって（製品インスタンスがエアーギャップネットワークにある場合）受信することができます。

例

ディスプレイに表示されるフィールドについては、表 20 : ポリシーを使用したスマートライセンスの show license status のフィールドの説明 （1319 ページ）を参照してください。

出力例については、次を参照してください。

- アカウント情報での show license status（ポリシーを使用したスマートライセンス） （1325 ページ）
- シスコのデフォルトポリシーでの show license status（ポリシーを使用したスマートライセンス） （1326 ページ）
- カスタムポリシーでの show license status（ポリシーを使用したスマートライセンス） （1327 ページ）

表 *20 :* ポリシーを使用したスマートライセンスの *show license status* のフィールドの説明

フィールド		説明
ユーティリティ	製品インスタンスで設定されているユーティリティ設定のヘッダー。	
	ステータス：	Status
	ユーティリティレポート：	最後の試行結果：
	顧客情報：	次のフィールドが表示されます。 • ID: • Name: • Street • City: • State: • Country: • Postal Code:

フィールド		説明
ポリシーを使用したスマートライセンス	製品インスタンスのポリシー設定のヘッダー。	
	ステータス：	ポリシーを使用したスマートライセンスが有効になっているかどうかを示します。 ポリシーを使用したスマートライセンスは、Cisco IOS XE Amsterdam 17.3.2 以降でサポートされ、サポートされているソフトウェアイメージでは常に有効になっています。
アカウント情報：	製品インスタンスが属するアカウント情報のヘッダー（CSSM 内）。 このセクションは、製品インスタンスのソフトウェアバージョンが Cisco IOS XE Cupertino 17.7.1 以降のリリースの場合にのみ表示されます。	
	スマートアカウント:	製品インスタンスが属するスマートアカウント。この情報は、常に製品インスタンスで使用可能な最新のACKに基づいています。
	バーチャルアカウント:	製品インスタンスが属するバーチャルアカウント。この情報は、常に製品インスタンスで使用可能な最新のACK に基づいています。
データプライバシー：	製品インスタンスで設定されているプライバシー設定のヘッダー。	
	送信ホスト名：	ホスト名が使用状況レポートで送信されるかどうかを示す *yes* または *no* の値。
	Callhome ホスト名のプライバシー：	Call Home 機能がレポートの転送モードとして設定されているかどうかを示します。設定されている場合、次のいずれかの値が表示されます。 • ENABLED • DISABLED
	スマートライセンスホスト名のプライバシー：	次のいずれかの値が表示されます。 • ENABLED • DISABLED
	バージョンプライバシー：	次のいずれかの値が表示されます。 • ENABLED • DISABLED

フィールド		説明
トランスポート：	製品インスタンスで設定されているトランスポート設定のヘッダー。	
	Type:	使用中の転送モード。 特定の転送モードでは、追加のフィールドが表示されます。たとえば、通信タイプが CSLU に設定されている場合、CSLU アドレスも表示されます。

フィールド		説明
ポリシー：	製品インスタンスに適用されるポリシー情報のヘッダー。	
	使用中のポリシー：	適用されるポリシー これは、Cisco default、Product default、Permanent License Reservation、Specific License Reservation、PAK license、Installed on <date>、Controller のいずれかです。
	ポリシー名：	ポリシーの名前
	レポートの ACK が必要：	この製品インスタンスのレポートに CSSM 確認応答（ACK）が必要かどうかを指定する *yes* または *no* の値。デフォルトポリシーは常に「yes」に設定されます。
	Unenforced/Non-Export Perpetual 属性	永久ライセンスのポリシー値を表示します。 • 最初のレポート要件（日）：最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • レポート頻度（日）：次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • 変化レポート（日）：ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます
	Unenforced/Non-Export Subscription 属性	サブスクリプション ライセンスのポリシー値を表示します。 • 最初のレポート要件（日）：最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • レポート頻度（日）：次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • 変化レポート（日）：ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます
	Enforced (Perpetual/Subscription) ライセンス属性	

フィールド		説明
		適用されたライセンスのポリシー値を表示します。 • 最初のレポート要件（日）：最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • レポート頻度（日）：次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • 変化レポート（日）：ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます
	Export (Perpetual/Subscription) ライセンス属性	輸出規制ライセンスのポリシー値を表示します。 • 最初のレポート要件（日）：最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • レポート頻度（日）：次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。 • 変化レポート（日）：ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます
その他	カスタム ID のヘッダー。	
	カスタム ID：	ID

フィールド		説明
使用状況レポート：	使用状況レポート（RUM レポート）情報のヘッダー。	
	最後に受信した ACK：	最後に受信したACKの日時（ローカルタイムゾーン）。
	次の ACK 期限：	次の ACK の日時。ACK が不要であることがポリシーで示されている場合、このフィールドには none と表示されます。 （注） ACK が必要で、この期限までに受信されない場合、syslog が表示されます。
	レポート間隔：	日単位のレポート間隔 ここに表示される値は、**license smart usage interval***interval_in_days* とポリシー値の設定によって異なります。詳細については、license smart（グローバルコンフィギュレーション） （587 ページ） で対応する構文の説明を参照してください。
	次の ACK プッシュチェック：	製品インスタンスが ACK の次のポーリング要求を送信する日時。日時はローカルタイムゾーンで表示されます。 これは、CSSM または CSLU への製品インスタンスによって開始された通信にのみ適用されます。レポート間隔がゼロの場合、または ACK ポーリングが保留されていない場合、このフィールドには none と表示されます。
	次のレポートプッシュ：	製品インスタンスが次の RUM レポートを送信する日時。日時はローカルタイムゾーンで表示されます。レポート間隔がゼロの場合、または保留中の RUM レポートがない場合、このフィールドには none と表示されます。
	最後のレポートプッシュ：	製品インスタンスが最後の RUM レポートを送信した日時。日時はローカルタイムゾーンで表示されます。
	最後のレポートファイル書き込み：	製品インスタンスが最後にオフライン RUM レポートを保存した日時。日時はローカルタイムゾーンで表示されます。
	最後のレポートプル：	データモデルを使用して使用状況レポート情報が取得された日時。日時はローカルタイムゾーンで表示されます。

フィールド		説明
インストール済みの信頼コード：	信頼コード関連情報のヘッダー。 信頼コードがインストールされている場合は、日時が表示されます。日時はローカルタイムゾーンで表示されます。 信頼コードがインストールされていない場合、このフィールドには none と表示されます。	
	Active:	アクティブ製品インスタンス。 高可用性セットアップでは、セットアップ内のすべての製品インスタンスの UDI と、対応する信頼コードのインストール日時が表示されます。
	Standby:	スタンバイ製品インスタンス。
	Member:	メンバー製品インスタンス。

アカウント情報での show license status（ポリシーを使用したスマートライセンス）

次に、ソフトウェアバージョンが Cisco IOS XE cupertino 17.7.1 である製品インスタンスの **show license status** コマンドの出力例を示します。

```
Device# show license status
Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
```

```
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>
```

シスコのデフォルトポリシーでの show license status（ポリシーを使用したスマートライセンス）

次に、**show license status** コマンドの出力例を示します。ここで適用されているポリシーは、デフォルトです。

```
Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
```

```
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>
```

カスタムポリシーでの show license status（ポリシーを使用したスマートライセンス）

次に、**show license status** コマンドの出力例を示します。カスタムポリシーを適用します。

```
Device# show license status
Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Policy:
  Policy in use: Installed On Nov 02 05:09:31 2020 IST
  Policy name: SLE Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 60 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
```

```
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
    INSTALLED on Nov 02 05:09:31 2020 IST
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
    INSTALLED on Nov 02 05:09:31 2020 IST
```

show license summary

使用されているライセンス、カウント、およびステータスに関する情報を含む、ライセンス使用状況の概要を表示するには、特権 EXEC モードで **show license summary** コマンドを入力します。

show license 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 モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンシングの有効なライセンスステータスが反映されました。有効なライセンスステータスには、`IN USE`、`NOT IN USE`、`NOT AUTHORIZED` などがあります。 コマンド出力が更新され、登録および承認情報が削除されました。 コマンド出力にスマートアカウントとバーチャルアカウントの情報が表示されなくなりました。
Cisco IOS XE Cupertino 17.7.1	コマンド出力が更新され、スマートアカウントと仮想アカウントの情報が表示されるようになりました。

使用上のガイドライン

スマートライセンス：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます。

ポリシーを使用したスマートライセンス：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

Cisco Catalyst ワイヤレスコントローラのライセンスは、いずれも輸出規制または適用されていないため、`NOT AUTHORIZED` になることはありません（これらのライセンスのみ、使用する前に許可が必要です）。

出力のアカウント情報

Cisco IOS XE Cupertino 17.7.1 以降、すべての ACK には、CSSM で報告されたスマートアカウントとバーチャルアカウントが含まれています。ACK を受信すると、製品インスタンスにはこの情報の最新バージョンのみが安全に保存されます。これは、ACK のタイムスタンプによって決定されます。したがって、このコマンドの出力の `[Account Information]` セクションに表

示されるスマートアカウントとバーチャルアカウントの情報は、常に製品インスタンスで使用可能な最新の ACK に基づいています。

製品インスタンスが 1 つのスマートアカウントとバーチャルアカウントから別のアカウントに移動された場合、移動後の次の ACK にはこの更新された情報が含まれます。この ACK が製品インスタンスで使用可能になると、このコマンドの出力が更新されます。

ACK は、直接的に（製品インスタンスが CSSM に接続されている場合）または間接的に（製品インスタンスが CSLU、Cisco DNA Center、または SSM On-Prem を介して CSSM に接続されている場合）、あるいは手動で ACK をインポートすることによって（製品インスタンスがエアーギャップネットワークにある場合）受信することができます。

例

ディスプレイに表示されるフィールドについては、表 21 : show license summary のフィールドの説明 （1330 ページ） を参照してください。

show license summary：使用中（ポリシーを使用したスマートライセンス） （1331 ページ）

show license summary：使用中でない（ポリシーを使用したスマートライセンス） （1331 ページ）

表 *21 : show license summary* のフィールドの説明

フィールド	説明
アカウント情報： Smart Account: Virtual Account:	製品インスタンスが属するスマートアカウントとバーチャルアカウント。この情報は、常に製品インスタンスで使用可能な最新の ACK に基づいています。 このフィールドは、製品インスタンスのソフトウェアバージョンが Cisco IOS XE Cupertino 17.7.1 以降のリリースの場合にのみ表示されます。
License	使用中のライセンスの名前
Entitlement Tag	ライセンスの短縮名
Count	ライセンス数
Status	ライセンスのステータスは次のいずれかになります。 • In-Use：有効なライセンスかつ使用中。 • Not In-Use • Not Authorized：ライセンスを使用する前に SLAC のインストールが必要であることを意味します。

show license summary：使用中（ポリシーを使用したスマートライセンス）

次に、ソフトウェアバージョンが Cisco IOS XE cupertino 17.7.1 である製品インスタンスの **show license summary** コマンドの出力例を示します。

```
Devide# show license summary

Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  air-network-essentials  (DNA_NWSTACK_E)                   1 IN USE
  air-dna-essentials      (AIR-DNA-E)                       1 IN USE
```

show license summary：使用中でない（ポリシーを使用したスマートライセンス）

次に、AP がコントローラに接続されていない場合の **show license summary** コマンドの出力例を示します。現在の使用数（カウント）はゼロであり、[Status] フィールドにはライセンスが [NOT IN USE] であると表示されます。

```
Device# show license summary

Device#show license summary
License Reservation is ENABLED

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  Aironet DNA Advantag... (AIR-DNA-A)                       0 NOT IN USE
  AP Perpetual Network... (DNA_NWStack)                     0 NOT IN USE
```

show license tech

テクニカルサポートチームが問題を解決するために役立つライセンス情報を表示するには、特権 EXEC モードで **show license tech** コマンドを入力します。このコマンドの出力には、他のいくつかの **show license** コマンドの出力などが含まれます。

show license tech { **message** | **rum** { **feature** { *license_name* | **all** } | **id** { *rum_id* | **all** } } [**detail**] [**save** *path*] | **support** }

構文の説明

message	信頼の確立、使用状況レポート、結果のポーリング、承認コードの要求と返却、および信頼の同期に関するメッセージを表示します。 これは、**show license history message** コマンドの出力に表示される情報と同じです。
rum { **feature** { *license_name* | **all** } | **id** { *rum_id* | **all** } } [**detail**] [**save** *path*]	製品インスタンスのリソース使用率測定レポート（RUM レポート）に関する情報を表示します。これには、レポート ID、レポートの現在の処理状態、エラー情報（ある場合）、および表示された RUM レポート情報を保存するオプションが含まれます。 （注） このオプションでは、RUM レポートに関する情報が保存され、レポート用ではありません。使用状況情報を含む XML ファイルである RUM レポートは保存されません。
support	テクニカルサポートチームが問題をデバッグするのに役立つライセンス情報を表示します。

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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンスに適用可能な新しいフィールドが反映されました。

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	**rum** キーワードおよびこのキーワードの下に追加のオプションが追加されました。 { **feature** { *license_name* | **all** } | **id** { *rum_id* | **all** } } **show license tech support** コマンドの出力が強化され、次の情報が表示されるようになりました。 • [License Usage] と [Usage Report Summary] セクションに記載されている RUM レポート情報。 • [Account Information:] セクションにあるスマートアカウントとバーチャルアカウント情報。 **data conversion**、**eventlog**、および **reservation** キーワードがこのコマンドから削除されました。これらは引き続き、個別の show コマンド、つまり、**show license data**、**show license eventlog**、および **show license reservation** として使用できます。

使用上のガイドライン

[Smart Licensing]：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます（スマートライセンスが有効になっているかどうか、関連するすべてのライセンス証明書、コンプライアンスステータスなど）。

[Smart Licensing Using Policy]：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2 以降のリリースの場合、コマンド出力には Smart Licensing Using Policy に関連するフィールドが表示されます。次のガイドラインに留意してください。

- サポート担当者によるトラブルシューティング

  解決できないエラーメッセージが表示された場合は、コンソールまたはシステムログに表示されるメッセージともに、シスコのテクニカルサポート担当者に **show license tech support**、**show license history message**、および **show platform software sl-infra all** 特権 EXEC コマンドの出力例を提供してください。

- 出力の RUM レポート情報

  - **show license tech support** コマンドの出力には、RUM レポートに関する次のセクションが表示されます。

    表 22 : show license tech support：ヘッダー「ライセンスの使用状況」のフィールドの説明 （1334 ページ）

```
<output truncated>
License Usage
=============
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 800
```

```
      Current Report: 1638055645       Previous: 0
 <output truncated>
```

表 23 : show license tech support：ヘッダー「使用状況レポートの概要」のフィールドの説明 （1335 ページ）

```
<output truncated>
Usage Report Summary:
=====================
Total: 4,  Purged: 0(0)
Total Acknowledged Received: 0,  Waiting for Ack: 0(4)
Available to Report: 4  Collecting Data: 2
Maximum Display: 4  In Storage: 4,  MIA: 0(0)
Report Module Status: Ready

<output truncated>
```

- **detail** キーワードと一緒に使用した **show license tech rum** コマンドの出力には、RUM レポートに関する次のフィールドが表示されます：表 24 : show license tech rum：ヘッダー「スマートライセンシングの使用状況レポート詳細」のフィールドの説明 （1336 ページ）。

  show license tech rum キーワードで使用できるオプションは、**show license rum** 特権 EXEC コマンドで使用できるオプションと同じです。簡易ビューに表示される出力例も同じです。ただし、**detail** キーワードを使用する場合（たとえば、**show license tech rum feature** *license_name* **detail** を入力する場合）、詳細ビューが表示され、**show license rum** と比較していくつかの追加フィールドがあります。

```
<output truncated>
Smart Licensing Usage Report Detail:
====================================
Report Id: 1638055644
  Metric Name: ENTITLEMENT
  Feature Name: air-dna-advantage
  Metric Value:
regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790
  UDI: PID:C9800-CL-K9,SN:93SZ7RXN93Y
  Previous Report Id: 0,    Next Report Id: 1638055646
  Version: 2.0
  State: CLOSED,      State Change Reason: RELOAD
  Start Time: Nov 28 12:02:09 2021 UTC,      End Time: Nov 30 22:02:13 2021 UTC

  Storage State: EXIST,  Storage State Change Reason: None
  Transaction ID: 0
  Transaction Message: <none>
  Report Size: 54880(54987)
<output truncated>
```

表 *22 : show license tech support*：ヘッダー「ライセンスの使用状況」のフィールドの説明

フィールド名	説明
Interval:	これは固定の測定時間で、常に 15 分です。
Current Value:	現在のライセンス数に関する情報。
Current Report:	ライセンスの現在 OPEN レポートの ID。

フィールド名	説明
Previous:	ライセンスの最後の OPEN レポートの ID。このレポートのステータスは現在 CLOSED です。

表 *23 : show license tech support* : ヘッダー「使用状況レポートの概要」のフィールドの説明

フィールド名	説明
Total:	製品インスタンスが生成したレポートの合計数。 （注） この合計は、製品インスタンスで現在使用可能であり、追跡されているレポートの合計数を示すものではありません。このためには、[Total Acknowledged Received:] フィールドと [Available to Report] フィールドを合計する必要があります。
Purged:	システムリソースの制限により削除されたレポートの数。この数には、製品インスタンスにトラッキング情報がない RUM レポートが含まれます。
Total Acknowledged Received:	この製品インスタンスで確認された RUM レポートの数。
Waiting for Ack:	ACK を待機している RUM レポートの数。これは、UNACK 状態のレポートの総数です。この場合、製品インスタンスにはトラッキング情報があります。
Available to Report:	CSSM に送信可能な RUM レポートの数。これは、OPEN または CLOSED 状態のレポートの総数です。この場合、製品インスタンスにはトラッキング情報があります。
Collecting Data:	製品インスタンスが現在測定値を収集しているレポートの数。
Maximum Display:	**show** コマンドの出力に表示できるレポートの数。
In Storage:	ディスクに現在保存されているレポートの数。
MIA:	欠落しているレポートの数。

表 *24 : show license tech rum* : ヘッダー「スマートライセンシングの使用状況レポート詳細」のフィールドの説明

フィールド名	説明
Version:	送信中のレポートの形式を表示します。 Cisco IOS XE Cupertino 17.7.1 以降、RUM レポートは処理時間を短縮する新しい形式で保存されます。このフィールドは、製品インスタンスが古い形式を使用しているか、新しい形式を使用しているかを示します。
Storage State:	特定のレポートが現在ストレージにあるかどうかを示します。 RUM レポートの現在のストレージ状態の表示に加えて、EXIST、DELETED、PURGED、MISSING の各値が表示されます。ラベルの横に「(1)」が表示されている場合（`Storage State (1)`）、RUM レポートは古い（17.7.1 より前の）形式であり、それに応じて処理されます。RUM レポートが新しい形式の場合、フィールドは [Storage State] として表示され、追加情報はありません。
Storage State Change Reason:	ストレージの状態が変化した理由を表示します。すべての状態変更が理由を示すわけではありません。 • NONE：これは、ストレージの状態変更の理由が記録されなかったことを意味します。 • PROCESSED：これは、CISCO がデータを処理した後に RUM レポートが削除されたことを意味します。 • LIMIT_STORAGE：これは、製品インスタンスがストレージ制限に達したため、RUM レポートが削除されたことを意味します。 • LIMIT_TIME：これは、レポートが永続的な時間制限に達したため、RUM レポートが削除されたことを意味します。
Transaction ID: Transaction Message:	トランザクション ID に相関 ID が表示され、エラーステータスが表示される場合、製品インスタンスのこのセクションにエラーコードフィールドが表示されます。エラーがない場合、データはここに表示されません。
Report Size	このフィールドには 2 つの数字が表示されます。最初の数値は、通信の raw レポートのサイズ（バイト単位）です。2 番目の数値は、レポートの保存に使用されるディスク容量（バイト単位）です。2 番目の数値は、レポートが新しい形式で保存されている場合にのみ表示されます。

Cisco Catalyst 9800-CL ワイヤレスコントローラでの show license tech support

次に、ソフトウェアバージョン Cisco IOS XE Cupertino 17.7.1 を実行している Cisco Catalyst 98000-CL ワイヤレスコントローラでの **show license tech support** コマンドの出力例を示します。

```
Device# show license tech support
Smart Licensing Tech Support info

Smart Licensing Status
======================

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: <none>
  Virtual Account: <none>

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Address: <empty>
    Port: <empty>
    Username: <empty>
    Password: <empty>
  Server Identity Check: True
  VRF: <empty>

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
```

```
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting) State(1) InPolicy(0)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

License Usage
=============
Handle: 1
  License: air-network-advantage
  Entitlement Tag:
regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
  Description: air-network-advantage
  Count: 0
  Version: 1.0
  Status: NOT IN USE(1)
  Status time: Oct 05 22:24:24 2021 UTC
  Request Time: None
  Export status: NOT RESTRICTED
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 0
      Current Report: 0       Previous: 0
  Soft Enforced: True

Handle: 2
  License: air-dna-advantage
  Entitlement Tag:
regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790
  Description: air-dna-advantage
  Count: 0
  Version: 1.0
  Status: NOT IN USE(1)
  Status time: Oct 05 22:24:24 2021 UTC
  Request Time: None
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 0
      Current Report: 0       Previous: 0
  Soft Enforced: True

Product Information
===================
UDI: PID:C9800-CL-K9,SN:9KGIXIDOXFE
```

```
HA UDI List:
    Active:PID:C9800-CL-K9,SN:9KGIXIDOXFE
    Standby:PID:C9800-CL-K9,SN:9UBKZU955E4

Agent Version
=============
Smart Agent for Licensing: 5.3.14_rel/47

Upcoming Scheduled Jobs
=======================
Current time: Oct 06 00:38:46 2021 UTC
Daily: Oct 06 21:24:22 2021 UTC (20 hours, 45 minutes, 36 seconds remaining)
Authorization Renewal: Expired Not Rescheduled
Init Flag Check: Expired Not Rescheduled
Reservation configuration mismatch between nodes in HA mode: Expired Not Rescheduled
Start Utility Measurements: Oct 06 00:39:25 2021 UTC (39 seconds remaining)
Send Utility RUM reports: Oct 06 22:24:54 2021 UTC (21 hours, 46 minutes, 8 seconds
remaining)
Save unreported RUM Reports: Oct 06 01:24:35 2021 UTC (45 minutes, 49 seconds remaining)
Data Synchronization: Expired Not Rescheduled
External Event: Expired Not Rescheduled
Operational Model: Expired Not Rescheduled

Communication Statistics:
=========================
Communication Level Allowed: INDIRECT
Overall State: Insufficient trust for direct communication
Trust Establishment:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Acknowledgement:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Usage Reporting:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Result Polling:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Request:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Confirmation:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
```

```
Authorization Return:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Sync:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Hello Message:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>

License Certificates
====================
Production Cert: False
Not registered. No certificates installed

HA Info
==========
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: False

Reservation Info
================
License reservation: DISABLED

Overall status:
  Active: PID:C9800-CL-K9,SN:9KGIXIDOXFE
      Reservation status: NOT INSTALLED
      Request code: <none>
      Last return code: <none>
      Last Confirmation code: <none>
      Reservation authorization code: <none>
  Standby: PID:C9800-CL-K9,SN:9UBKZU955E4
      Reservation status: NOT INSTALLED
      Request code: <none>
      Last return code: <none>
      Last Confirmation code: <none>
      Reservation authorization code: <none>

Specified license reservations:

Purchased Licenses:
  No Purchase Information Available

Usage Report Summary:
=====================
Total: 0,  Purged: 0(0)
Total Acknowledged Received: 0,  Waiting for Ack: 0(0)
Available to Report: 0  Collecting Data: 0
Maximum Display: 0  In Storage: 0,  MIA: 0(0)
Report Module Status: Ready
```

```
Other Info
==========
Software ID: regid.2018-05.com.cisco.WLC_9500C,1.0_85665885-b865-4e32-8184-5510412fcb54
Agent State: authorized
TS enable: True
Transport: Smart
  Default URL: https://smartreceiver.cisco.com/licservice/license
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char)  : 1
sizeof(int)   : 4
sizeof(long)  : 4
sizeof(char *): 8
sizeof(time_t): 4
sizeof(size_t): 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: False
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN
Check Point Interface: True
Config Management Interface: False
License Map Interface: True
HA Interface: True
Trusted Store Interface: True
Platform Data Interface: True
Crypto Version 2 Interface: False
SAPluginMgmtInterfaceMutex: True
SAPluginMgmtIPDomainName: True
SmartTransportVRFSupport: True
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartTransportServerIdCheck: True
SmartTransportProxySupport: True
SmartAgentPolicyDisplayFormat: 0
SmartAgentReportOnUpgrade: False
SmartAgentIndividualRUMEncrypt: 2
SmartAgentMaxRumMemory: 2
SmartAgentConcurrentThreadMax: 10
SmartAgentPolicyControllerModel: False
SmartAgentPolicyModel: True
SmartAgentFederalLicense: True
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
```

```
conversionAutomatic: True
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
HighAvailabilityOverrideEvent: UnknownPlatformEvent
platformIndependentOverrideEvent: UnknownPlatformEvent
platformOverrideEvent: UnknownPlatformEvent
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 3 KB
P:C9800-CL-K9,S:9KGIXIDOXFE: No Trust Data
P:C9800-CL-K9,S:9UBKZU955E4: No Trust Data
Overall Trust: No ID
Clock sync-ed with NTP: True

Platform Provided Mapping Table
===============================
  C9800-CL-K9: Total licenses found: 5
Enforced Licenses:
  P:C9800-CL-K9,S:9KGIXIDOXFE:
    No PD enforced licenses
  P:C9800-CL-K9,S:9UBKZU955E4:
    No PD enforced licenses
```

例（ポリシーを使用したスマートライセンス）

次に、**show license tech support** コマンドの出力例を示します。

```
Device# show license tech support

Smart Licensing Tech Support info

Smart Licensing Status
======================

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Nov 02 03:16:01 2020 IST

License Authorization:
  Status: AUTHORIZED - RESERVED on Nov 02 03:16:01 2020 IST

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED
```

```
Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 89 days, 23 hours, 42 minutes, 47 seconds

License Usage
=============
Handle: 1
  License: AP Perpetual Networkstack Advantage
  Entitlement tag:
regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
  Description: AP Perpetual Network Stack entitled with DNA-A
  Count: 1
  Version: 1.0
  Status: AUTHORIZED(3)
  Status time: Nov 02 03:16:01 2020 IST
  Request Time: Nov 02 02:55:34 2020 IST
  Export status: NOT RESTRICTED
  Soft Enforced: True

Handle: 2
  License: Aironet DNA Advantage Term Licenses
  Entitlement tag:
regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790
  Description: DNA Advantage for Wireless
  Count: 1
  Version: 1.0
  Status: AUTHORIZED(3)
  Status time: Nov 02 03:16:01 2020 IST
  Request Time: Nov 02 02:55:34 2020 IST
  Export status: NOT RESTRICTED
  Soft Enforced: True

Product Information
===================
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS

HA UDI List:
    Active:PID:C9800-CL-K9,SN:93BBAH93MGS
    Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN

Agent Version
=============
Smart Agent for Licensing: 4.8.7_rel/52

Upcoming Scheduled Jobs
=======================
Current time: Nov 02 03:17:23 2020 IST
Daily: Nov 03 02:47:04 2020 IST (23 hours, 29 minutes, 41 seconds remaining)
Certificate Renewal: Not Available
Certificate Expiration Check: Not Available
Authorization Renewal: Not Available
Authorization Expiration Check: Not Available
Init Flag Check: Not Available
```

```
Evaluation Expiration Check: Not Available
Ack Expiration Check: Not Available
Evaluation Expiration Warning: Not Available
IdCert Expiration Warning: Not Available
Reservation request in progress warning: Not Available
Reservation configuration mismatch between nodes in HA mode: Nov 09 03:16:30 2020 IST
(6 days, 23 hours, 59 minutes, 7 seconds remaining)
Endpoint Report Request: Not Available

License Certificates
====================
Production Cert: True
Not registered. No certificates installed

HA Info
==========
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: False

Reservation Info
================
License reservation: ENABLED

Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
       Reservation status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
       Export-Controlled Functionality: ALLOWED
       Request code: <none>
       Last return code: <none>
       Last Confirmation code: 102fc949
       Reservation authorization code:
<encoded data>
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>Aironet DNA Advantage Term
Licenses</displayName><tagDescription>DNA Advantage for
<encoded data>
 UTC</startDate><endDate>2020-Dec-15
UTC</endDate><licenseType>TERM</licenseType><displayName>Aironet DNA Advantage Term
Licenses</displayName><tagDescription>DNA Advantage for
<encoded data>
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>AP Perpetual Networkstack
Advantage</displayName><tagDescription>AP Perpetual Network Stack entitled with
<encoded data>
 UTC</startDate><endDate>2020-Dec-15
UTC</endDate><licenseType>TERM</licenseType><displayName>AP Perpetual Networkstack
Advantage</displayName><tagDescription>AP Perpetual Network Stack entitled with
<encoded data>

  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
       Reservation status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
       Export-Controlled Functionality: ALLOWED
       Request code: <none>
       Last return code: <none>
       Last Confirmation code: ad4382fe
       Reservation authorization code:
<encoded data>
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>AP Perpetual Networkstack
```

```
Advantage</displayName><tagDescription>AP Perpetual Network Stack entitled with
DNA-A</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2017-08.com.cisco.AIR-DNA-A,1.0_[illegible]</tag><count>10</count><startDate>2020-Oct-14
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>Aironet DNA Advantage Term
Licenses</displayName><tagDescription>DNA Advantage for
Wireless</tagDescription><subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode><signature>[illegible]</signature><udi>P:C9800-CL-K9,S:9XECPSUU4XN</udi></specificPLR>

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
          Subscription ID: <none>
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
          Subscription ID: <none>
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
          Subscription ID: <none>
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled with DNA-A
    Total reserved count: 20
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
          Subscription ID: <none>
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
          Subscription ID: <none>
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
          Subscription ID: <none>

Other Info
==========
Software ID: regid.2018-05.com.cisco.WLC_9500C,1.0_85665885-b865-4e32-8184-5510412fcb54
Agent State: authorized
TS enable: True
Transport: Smart
  Default URL: https://smartreceiver.cisco.com/licservice/license
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char)  : 1
```

```
sizeof(int)   : 4
sizeof(long)  : 4
sizeof(char *): 8
sizeof(time_t): 4
sizeof(size_t): 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: False
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartAgentFederalLicense: True
SmartAgent_Crypto_Exit_CB: 0x55B353357A20
SmartAgent_Crypto_Start_CB: 0x55B353357A10
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: True
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
platformOverrideEvent: UnknownPlatformEvent
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 21 KB

Platform Provided Mapping Table
================================
<empty>
```

show license udi

製品インスタンスの Unique Device Identifier（UDI）情報を表示するには、特権 EXEC モードで **show license udi** コマンドを入力します。高可用性セットアップでは、接続されたすべての製品インスタンスの UDI 情報が出力に表示されます。

show license udi

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 Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	このコマンドは、ポリシーを使用したスマートライセンスの導入で、引き続き使用することができます。

使用上のガイドライン

ポリシーを使用したスマートライセンス：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

スマートライセンス：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます。

例

スタンドアロン製品インスタンスでの show license udi （1347 ページ）

アクティブおよびスタンバイでの show license udi （1347 ページ）

スタンドアロン製品インスタンスでの show license udi

次に、スタンドアロン製品インスタンスでの **show license udi** コマンドの出力例を示します。

```
Device# show license udi

UDI: PID:C9800-L-F-K9,SN:FCW2323W016
```

アクティブおよびスタンバイでの show license udi

次に、アクティブ製品インスタンスとスタンバイ製品インスタンスが存在する高可用性セットアップでの **show license udi** コマンドの出力例を示します。両方の UDI 情報が表示されます。

```
Device# show license udi

UDI: PID:C9800-CL-K9,SN:93BBAH93MGS
```

```
HA UDI List:
    Active:PID:C9800-CL-K9,SN:93BBAH93MGS
    Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN
```

show license usage

ステータス、使用中のライセンス数、適用タイプなどのライセンス使用状況の情報を表示するには、特権 EXEC モードで **show license usage** コマンドを入力します。

show license usage

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
このコマンドは、Cisco IOS XE Amsterdam 17.3.2 よりも前のリリースで導入されました。	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンスに適用可能な新しいフィールドが反映されました。これには、`Status`、`Enforcement type` フィールドが含まれます。 コマンド出力が更新され、予約関連情報、承認ステータス情報、および輸出ステータス情報が削除されました。

使用上のガイドライン

ポリシーを使用したスマートライセンス：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

スマートライセンス：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます。

例

ディスプレイに表示されるフィールドについては、表 25 : show license usage のフィールドの説明 （1350 ページ） を参照してください。

show license usage with unenforced licenses（ポリシーを使用したスマートライセンス） （1351 ページ）

show license usage with unenforced SLR licenses（ポリシーを使用したスマートライセンス） （1351 ページ）

表 *25 : show license usage* のフィールドの説明

フィールド	説明
License Authorization: Status:	全体的な承認ステータスを表示します。
():	CSSM におけるようなライセンスの名前。 このライセンスが承認コードを必要とする場合、ライセンスの 取得されます。
Description	CSSM におけるようなライセンスの説明。
Count	ライセンス数。ライセンスが使用中でない場合、カウントはゼ ます。
Version	バージョン。
Status	ライセンスのステータスは次のいずれかになります。 • In-Use：有効なライセンスかつ使用中。 • Not In-Use • Not Authorized：ライセンスを使用する前に SLAC のインス ることを意味します。詳細については、次を参照してくだ
Export Status:	このライセンスが輸出規制されているかどうかを示します。そ テータスのいずれかが表示されます。 • RESTRICTED - ALLOWED • RESTRICTED - NOT ALLOWED • NOT RESTRICTED
Feature name	このライセンスを使用する機能の名前。
Feature Description:	このライセンスを使用する機能の説明。
ユーティリティのサブスクリプションID：	ID 対応する設定オプションがサポートされていないため、該当し

フィールド	説明
Enforcement type	ライセンスの適用タイプのステータス。これは、次のいず • ENFORCED • NOT ENFORCED • EXPORT RESTRICTED - ALLOWED • EXPORT RESTRICTED - NOT ALLOWED 適用タイプの詳細については、次を参照してください。 <l

show license usage with unenforced licenses（ポリシーを使用したスマートライセンス）

次に、**show license usage** コマンドの出力例を示します。ここでは、不適用ライセンスを使用中です。

```
Device# show license usage

License Authorization:
  Status: Not Applicable

air-network-essentials (DNA_NWSTACK_E):
  Description: air-network-essentials
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-network-essentials
  Feature Description: air-network-essentials
  Enforcement type: NOT ENFORCED
  License type: Perpetual

air-dna-essentials (AIR-DNA-E):
  Description: air-dna-essentials
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-essentials
  Feature Description: air-dna-essentials
  Enforcement type: NOT ENFORCED
  License type: Perpetual
```

show license usage with unenforced SLR licenses（ポリシーを使用したスマートライセンス）

次に、**show license usage** コマンドの出力例を示します。ここでは、移行された SLR ライセンスが使用されています。

```
Device# show license usage

air-network-advantage (DNA_NWStack):
  Description: air-network-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
```

```
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

air-dna-advantage (AIR-DNA-A):
  Description: air-dna-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20
```

show platform software rif-mgr chassis active R0 resource-status

アクティブインスタンスの冗長ポートインターフェイス（RIF）リソースのステータスを確認するには、**show platform software rif-mgr chassis active R0 resource-status** コマンドを使用します。

show platform software rif-mgr chassis active R0 resource-status

構文の説明

rif-mgr	RIFマネージャに関する情報を表示します。
chassis	シャーシに関する情報を表示します。
active	アクティブインスタンスを指定します。
R0	ルートプロセッサスロット0を指定します。
resource-status	リソース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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

使用上のガイドライン

RIF リソースのステータスには、RP ステータス、RMI ステータス、現在のシャーシの状態、およびピアシャーシの状態が表示されます。

例

次に、アクティブインスタンスの RIF リソースのステータスを確認する例を示します。

```
Device# show platform software rif-mgr chassis active R0 resource-status
RIF Resource Status

    RP Status             : Up
    RMI Status            : Up
    Current Chassis State : Active
    Peer Chassis State    : Standby
```

show platform software rif-mgr chassis standby R0 resource-status

スタンバイインスタンスの冗長ポートインターフェイス（RIF）リソースのステータスを確認するには、**show platform software rif-mgr chassis standby R0 resource-status** コマンドを使用します。

show platform software rif-mgr chassis standby R0 resource-status

構文の説明

rif-mgr	RIF マネージャに関する情報を表示します。
chassis	シャーシに関する情報を表示します。
standby	スタンバイインスタンスを指定します。
R0	ルートプロセッサスロット 0 を指定します。
resource-status	リソース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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

使用上のガイドライン

RIF リソースのステータスには、RP ステータス、RMI ステータス、現在のシャーシの状態、およびピアシャーシの状態が表示されます。

例

次に、スタンバイインスタンスの RIF リソースのステータスを確認する例を示します。

```
Device# show platform software rif-mgr chassis standby R0 resource-status
RIF Resource Status

    RP Status             : Up
    RMI Status            : Up
    Current Chassis State : Standby
    Peer Chassis State    : Active
```

show platform software rif-mgr chassis active R0 rmi-connection-details

RMI リンクの再確立カウントと、アクティブインスタンスで RMI リンクがアップまたはダウンになってからの時間を確認するには、**show platform software rif-mgr chassis active R0 rmi-connection-details** コマンドを使用します。

show platform software rif-mgr chassis active R0 rmi-connection-details

構文の説明

rif-mgr	RIF マネージャに関する情報を表示します。
chassis	シャーシに関する情報を表示します。
active	アクティブインスタンスを指定します。
R0	ルートプロセッサスロット 0 を指定します。
rmi-connection-details	RMI 接続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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、RMI リンクの再確立カウントと、アクティブインスタンスでアップになってからの時間を確認する例を示します。

```
Device# show platform software rif-mgr chassis active R0 rmi-connection-details
RMI Connection Details
    RMI Link re-establish count : 2
    RMI Link Uptime             : 21 hours 8 minutes 43 seconds
    RMI Link Upsince            : 08/05/2021 13:46:01
```

次に、RMI リンクの再確立カウントと、アクティブインスタンスでダウンになってからの時間を確認する例を示します。

```
Device# show platform software rif-mgr chassis active R0 rmi-connection-details
RMI Connection Details
    RMI Link re-establish count : 1
    RMI Link Downtime           : 28 seconds
    RMI Link Downsince          : 07/16/2021 03:19:11
```

show platform software rif-mgr chassis standby R0 rmi-connection-details

RMI リンクの再確立カウントと、スタンバイインスタンスで RMI リンクがアップまたはダウンになってからの時間を確認するには、**show platform software rif-mgr chassis standby R0 rmi-connection-details** コマンドを使用します。

show platform software rif-mgr chassis standby R0 rmi-connection-details

構文の説明

rif-mgr	RIF マネージャに関する情報を表示します。
chassis	シャーシに関する情報を表示します。
standby	スタンバイインスタンスを指定します。
R0	ルートプロセッサスロット 0 を指定します。
rmi-connection-details	RMI 接続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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、RMI リンクの再確立カウントと、スタンバイインスタンスでアップになってからの時間を確認する例を示します。

```
Device# show platform software rif-mgr chassis standby R0 rmi-connection-details
RMI Connection Details
    RMI Link re-establish count : 1
    RMI Link Uptime             : 1 hour 39 minute 9 seconds
    RMI Link Upsince            : 07/16/2021 01:31:41
```

次に、RMI リンクの再確立カウントと、スタンバイインスタンスでダウンになってからの時間を確認する例を示します。

```
Device# show platform software rif-mgr chassis standby R0 rmi-connection-details
RMI Connection Details
    RMI Link re-establish count : 1
    RMI Link Downtime           : 22 seconds
    RMI Link Downsince          : 07/16/2021 03:19:17
```

show platform software rif-mgr chassis active R0 rp-connection-details

RP リンクの再確立カウントと、アクティブインスタンスでRP リンクがアップまたはダウンになってからの時間を確認するには、**show platform software rif-mgr chassis active R0 rp-connection-details** コマンドを使用します。

show platform software rif-mgr chassis active R0 rp-connection-details

構文の説明

rif-mgr	RIF マネージャに関する情報を表示します。
chassis	シャーシに関する情報を表示します。
active	アクティブインスタンスを指定します。
R0	ルートプロセッサスロット 0 を指定します。
rp-connection-details	RP 接続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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、RP リンクの再確立カウントと、アクティブインスタンスで数日間アップになってからの時間を確認する例を示します。

```
Device# show platform software rif-mgr chassis active R0 rp-connection-details
RP Connection Details
    RP Connection Uptime  : 12 days 17 hours 1 minute 39 seconds
    RP Connection Upsince : 07/03/2021 07:06:20
```

次に、RP リンクの再確立カウントと、アクティブインスタンスでダウンになってからの時間を確認する例を示します。

```
Device# show platform software rif-mgr chassis active R0 rp-connection-details
RP Connection Details
    RP Connection Downtime     : 4 seconds
    RP Connection Downsince    : 07/16/2021 03:33:04
```

show platform software rif-mgr chassis standby R0 rp-connection-details

RP リンクの再確立カウントと、スタンバイインスタンスで RP リンクがアップまたはダウンになってからの時間を確認するには、**show platform software rif-mgr chassis standby R0 rp-connection-details** コマンドを使用します。

show platform software rif-mgr chassis standby R0 rp-connection-details

構文の説明

rif-mgr	RIF マネージャに関する情報を表示します。
chassis	シャーシに関する情報を表示します。
standby	スタンバイインスタンスを指定します。
R0	ルートプロセッサスロット 0 を指定します。
rp-connection-details	RP 接続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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、RP リンクの再確立カウントと、スタンバイインスタンスでアップになってからの時間を確認する例を示します。

```
Device# show platform software rif-mgr chassis standby R0 rp-connection-details
RP Connection Details
    RP Connection Uptime  : 12 days 17 hours 2 minutes 1 second
    RP Connection Upsince : 07/03/2021 07:05:58
```

次に、RP リンクの再確立カウントと、スタンバイインスタンスでダウンになってからの時間を確認する例を示します。

```
Device# show platform software rif-mgr chassis standby R0 rp-connection-details
RP Connection Details
    RP Connection Downtime    : 22 seconds
    RP Connection Downsince   : 07/16/2021 03:19:17
```

show platform software rif-mgr chassis active R0 rif-stk-internal-stats

アクティブインスタンスの RIF およびスタックマネージャの内部統計を確認するには、**show platform software rif-mgr chassis active R0 rif-stk-internal-stats** コマンドを使用します。

show platform software rif-mgr chassis active R0 rif-stk-internal-stats

構文の説明

rif-mgr	RIF マネージャに関する情報を表示します。
chassis	シャーシに関する情報を表示します。
active	アクティブインスタンスを指定します。
R0	ルートプロセッサスロット 0 を指定します。
rif-stk-internal-stats	RIF およびスタックマネージャの内部統計を表示します。

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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、アクティブインスタンスの RIF およびスタックマネージャの内部統計を確認する例を示します。

```
Device# show platform software rif-mgr chassis active R0 rif-stk-internal-stats
RIF Stack Manager internal stats

    Stack-mgr reported RP down            : False
    DAD link status reported to Stack-Mgr : True
```

show platform software rif-mgr chassis standby R0 rif-stk-internal-stats

スタンバイインスタンスの RIF およびスタックマネージャの内部統計を確認するには、**show platform software rif-mgr chassis standby R0 rif-stk-internal-stats** コマンドを使用します。

show platform software rif-mgr chassis standby R0 rif-stk-internal-stats

構文の説明

rif-mgr	RIF マネージャに関する情報を表示します。
chassis	シャーシに関する情報を表示します。
standby	スタンバイインスタンスを指定します。
R0	ルートプロセッサスロット 0 を指定します。
rif-stk-internal-stats	RIFおよびスタックマネージャの内部統計を表示します。

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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、スタンバイインスタンスのRIFおよびスタックマネージャの内部統計を確認する例を示します。

```
Device# show platform software rif-mgr chassis standby R0 rif-stk-internal-stats
RIF Stack Manager internal stats

    Stack-mgr reported RP down            : False
    DAD link status reported to Stack-Mgr : True
```

show platform software rif-mgr chassis active R0 lmp-statistics

アクティブインスタンスでタイプごとに送受信されたパケット数を確認するには、**show platform software rif-mgr chassis active R0 lmp-statistics** コマンドを使用します。

show platform software rif-mgr chassis active R0 lmp-statistics

構文の説明

rif-mgr	RIFマネージャに関する情報を表示します。
chassis	シャーシに関する情報を表示します。
active	アクティブインスタンスを指定します。
R0	ルートプロセッサスロット0を指定します。
lmp-statistics	LMP 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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、アクティブインスタンスでタイプごとに送受信されたパケット数を確認する例を示します。

```
Device# show platform software rif-mgr chassis active R0 lmp-statistics
LMP Statistics

Info Type Sent                    : 6
Solicit Info Type Sent            : 0
Unsolicit Info Type Sent          : 6
Reload Type Sent                  : 0
Recovery Type Sent                : 1
Gateway Info Type Sent            : 0
Enquiry Type Sent                 : 0
Solicit Enquiry Type Sent         : 0
Unsolicit Enquiry Type Sent       : 0

Info Type Received                : 5
Solicit Info Type Received        : 2
Unsolicit Info Type Received      : 3
Reload Type Received              : 0
Recovery Type Received            : 0
Gateway Info Type Received        : 4
Enquiry Type Received             : 0
Solicit Enquiry Type Received     : 0
Unsolicit Enquiry Type Received   : 0
```

show platform software rif-mgr chassis standby R0 lmp-statistics

スタンバイインスタンスでタイプごとに送受信されたパケット数を確認するには、**show platform software rif-mgr chassis standby R0 lmp-statistics** コマンドを使用します。

show platform software rif-mgr chassis standby R0 lmp-statistics

構文の説明

rif-mgr	RIF マネージャに関する情報を表示します。
chassis	シャーシに関する情報を表示します。
standby	スタンバイインスタンスを指定します。
R0	ルートプロセッサスロット 0 を指定します。
lmp-statistics	LMP 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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、スタンバイインスタンスでタイプごとに送受信されたパケット数を確認する例を示します。

```
Device# show platform software rif-mgr chassis standby R0 lmp-statistics
LMP Statistics

Info Type Sent                  : 6
Solicit Info Type Sent          : 0
Unsolicit Info Type Sent        : 6
Reload Type Sent                : 0
Recovery Type Sent              : 0
Gateway Info Type Sent          : 4
Enquiry Type Sent               : 0
Solicit Enquiry Type Sent       : 0
Unsolicit Enquiry Type Sent     : 0

Info Type Received              : 5
Solicit Info Type Received      : 3
Unsolicit Info Type Received    : 2
Reload Type Received            : 0
Recovery Type Received          : 1
Gateway Info Type Received      : 0
Enquiry Type Received           : 0
```

```
Solicit Enquiry Type Received    : 0
Unsolicit Enquiry Type Received  : 0
```

show platform software sl-infra

トラブルシューティング情報を表示し、デバッグに関する情報を表示するには、特権 EXEC モードで **show platform software sl-infra** コマンドを入力します。このコマンドの出力は、テクニカルサポートチームがトラブルシューティングとデバッグに使用します。

show platform software sl-infra { **all** | **current** | **debug** | **stored** }

構文の説明

all	現在の情報、デバッグ情報、および保存されている情報を表示します。
current	現在のライセンス関連情報を表示します。
debug	デバッグを有効にします。
stored	製品インスタンスに保存されている情報を表示します。

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 Amsterdam 17.3.2a	このコマンドが導入されました。

使用上のガイドライン

解決できないエラーメッセージが表示された場合は、コンソールまたはシステムログに表示されるメッセージともに、シスコのテクニカルサポート担当者に **show license tech support**、**show license history message**、および **show platform software sl-infra all** 特権 EXEC コマンドの出力例を提供してください。

show platform software tls client summary

TLS クライアントの概要の詳細を表示するには、**show platform software tls client summary** コマンドを使用します。

show platform software tls client 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 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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、TLS クライアント概要の詳細を表示する例を示します。

```
Device # show platform software tls client summary

Name     ID     Gateway   Port   Auth     Trustpoint   DPD Time Rekey Time  Retry Time
-------------------------------------------------------------------------------------
fqdn     0               8443   PSK       N/A           60       300         20
```

show platform software client detail

TLS クライアントセッションの詳細、セッションの統計、トンネルの統計、および DNS カウンタの概要を表示するには、**show platform software client detail** コマンドを使用します。

show platform software client detail

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 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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、TLS クライアント概要の詳細を表示する例を示します。

```
Device # show platform software client detail

TLS Client           : Session Detail
Session Name         : fqdn
FQDN resolved IP     : 10.194.234.149
ID                   : 0
Created              : 04/20/21 00:36:42
Updated              : 04/22/21 05:56:03
State                : Up (Rekey)
Up Time              : 04/21/21 20:30:21 ( 9 hours 25 minutes 45 seconds )
Down Time            : 04/21/21 20:30:01
Rekey Time           : 04/22/21 05:55:51 ( 15 seconds )

TLS Session Statistics

Up Notifications     : 3
Down Notifications   : 2
Rekey Notifications  : 636
DP State Updates     : 0
DPD Cleanups         : 0

Packets From     Packets To  Packet Errors To     Bytes From           Bytes To
-------------------------------------------------------------------------------
  BinOS              80           0                                      0
  IOSd                0           0                    0                 0

  TLS Client          0           0                    0                 0


TLS Tunnel Statistics
Type            Tx Packets      Rx Packets
-------------------------------------------
  Total             0               80
  CSTP Ctrl      3836             3836
  CSTP Data        80                0

Type            Requests         Responses
```

```
-------------------------------------------
CSTP Cfg          639                 639
CSTP DPD         3197                3197

Invalid CSTP Rx          : 0
Injected Packet Success  : 0
Injected Packet Failed   : 0
Consumed Packets         : 0

TLS Tunnel DNS Counters
DNS Resolve Request Success Count    : 641
DNS Resolve Request Failure Count    :  0
DNS Resolve Success Count            : 639
DNS Resolve Failure Count            :  2
```

show platform software tls statistics

TLS クライアントグローバル統計の詳細を表示するには、**show platform software tls statistics** コマンドを使用します。

show platform software tls statistics

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 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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、TLS クライアント概要の詳細を表示する例を示します。

```
Device # show platform software tls statistics

TLS Client - Global Statistics
Session Statistics
Up/Down           : 5/2
Rekeys            : 636
DP Updates        :   0
DPD Cleanups      :   0

Packets From    Packets To   Packet Errors To     Bytes From   Bytes To
-------------------------------------------------------------------------
BinOS              85             0                   0             0
IOSd 0             0              0                   0             0
TLS Client  0      0                                  0             0

Tunnel Statistics
SSL Handshake Init/Done     : 641/641
TCP Connection Req/Done     : 641/641

Tunnel Packets
Rx/Tx                       : 85/0
Injected / Failed           : 0/0
Consumed                    :  0

CSTP Packets
Control Rx/Tx               : 3839 / 3839
Data Rx/Tx                  : 0 / 85
Config Req/Resp             : 641 / 641
DPD Req/Resp                : 3198 / 3198
Invalid Rx                  : 0

FQDN Counters
Req/Resp/Success            : 0/0/0

NAT Counters
Transalte In/Out            : 0/0
Ignore    In/Out            : 0/0
```

```
Failed                      : 0
Invalid                     : 0
No Entry                    : 0
Unsupported                 : 0

Internal Counters
Type           Allocated            Freed
------------------------------------------------
EV              1299                 1295
Tunnel           5                    4
Conn            643                  642
Sess             3                    2

Config Message Related Counters
Type               Success              Failed
------------------------------------------------
Create                3                    0
Delete                2                    0
```

show platform software tls session summary

tls クライアントセッションの概要を表示するには、**show platform software tls session summary** コマンドを使用します。

show platform software tls session 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 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 Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、TLS クライアント概要の詳細を表示する例を示します。

```
Device # show platform software tls session summary

TLS Client - Session Summary
Name     ID      Created            State    Since               Elapsed
-------------------------------------------------------------------------------------------
fqdn     0       04/20/21 00:36:42    Up     04/21/21 20:30:21   9 hours 26 minutes 44
seconds
```

show product-analytics kpi report

特定の製品分析エンジンレポートの詳細を表示するには、**show product-analytics kpi report** コマンドを使用します。

show product-analytics kpi report

構文の説明

report-id	レポート識別子。

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 Dublin 17.10.1	このコマンドが導入されました。

例

次に、特定の製品分析エンジンレポートの詳細を表示する例を示します。

```
Device# show product-analytics kpi report <report-id>

Product Analytics Engine KPIs

 Report ID     : 1662422400
 Computed at   : 09/06/2022 00:00:00
 KPI Name      : ap_mode
.
.
.
 Report ID     : 1662422400
 Computed at   : 09/06/2022 00:00:00
 KPI Name      : clients_distinct_wireless_lua
 KPI Value     : 0
```

show product-analytics kpi summary

製品分析エンジンレポートの概要を表示するには、**show product-analytics kpi summary** コマンドを使用します。

show product-analytics kpi 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 Dublin 17.10.1	このコマンドが導入されました。

例

次に、製品分析エンジンレポートの概要を表示する例を示します。

```
Device# show product-analytics kpi summary

Product Analytics Engine KPIs

Time                          Report ID                     KPI Name
----------------------------- ----------------------------- ----------------------------

09/06/2022 00:00:00            1662422400                      ap_mode

09/06/2022 00:00:00            1662422400                      ap_type

09/06/2022 00:00:00            1662422400                      fra_usage

.
.
.
09/15/2022 00:00:00           1663200000                    clients_concurrent_wireless

09/15/2022 00:00:00            1663200000
clients_distinct_wireless_lua
```

show product-analytics report detail

製品分析エンジンレポートの詳細を表示するには、**show product-analytics report detail** コマンドを使用します。

show product-analytics report detail

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 Dublin 17.10.1	このコマンドが導入されました。

例

次に、製品分析エンジンレポートの詳細を表示する例を示します。

```
Device# show product-analytics report detail

Product Analytics Engine Reports

Report ID          : 1662422400
Policy Version     : 17.10.1
Engine Version     : 17.10.1
File version       : 1
Period start       :
Period End         :
Timezone           : 0

Event History
Timestamp               #Times   Event               RC Context
----------------------- -------- ------------------- --
----------------------------------------
09/14/2022 22:15:01.814 1        REPORT_SEND          5 DRAGONFLY

.
.
.


Report ID          : 1663200000
Policy Version     : 17.10.1
Engine Version     : 17.10.1
File version       : 1
Period start       :
Period End         :
Timezone           : 0

Event History
Timestamp               #Times   Event               RC Context
----------------------- -------- ------------------- --
----------------------------------------
```

```
09/15/2022 00:00:00.836 1        KPI_ADD             0 clients_distinct_wireless_lua
09/15/2022 00:00:00.824 1        KPI_ADD             0 client_auth_protocol_lua
09/15/2022 00:00:00.793 1        KPI_ADD             0 clients_concurrent_wireless
09/15/2022 00:00:00.793 1        KPI_ADD             0 network_ssid_count
09/15/2022 00:00:00.793 1        KPI_ADD             0 ap_type
09/15/2022 00:00:00.792 1        KPI_ADD             0 fra_enabled
09/15/2022 00:00:00.792 1        KPI_ADD             0 ap_software_version
09/15/2022 00:00:00.792 1        KPI_ADD             0 ap_mode
09/15/2022 00:00:00.792 1        KPI_ADD             0 fra_usage
09/15/2022 00:00:00.791 1        NEW_REPORT          0
```

show product-analytics stats

製品分析エンジンの統計とイベント履歴を表示するには、**show product-analytics stats** コマンドを使用します。

show product-analytics stats

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 Dublin 17.10.1	このコマンドが導入されました。

例

次に、製品分析エンジンの統計とイベント履歴を表示する例を示します。

```
Device# show product-analytics stats

Product Analytics Engine Statistics

Policy-Version
 File version                          : 1
Data-Store
 #Writes                               : 941442
 Total write time (us)                 : 754856891
 Average write time (us)               : 801
 #Single Writes                        : 1890439
 Total Single write time (us)          : 41098825
 Average Single write time (us)        : 21
 #Queries                              : 737
 Total query time (us)                 : 4534566
 Average query time (us)               : 6152
 #Query errors                         :

Data-Source
 #Periodic reads                       : 2195456
 Total periodic-read time (us)         : 7414384002
 Average periodic-read time (us)       : 3377
 #Periodic read batches                : 3136361
 Total periodic-read-batch time (us)   : 1826634998
 Average periodic-read-batch time (us) : 582
 #On-change reads                      : 604

KPI
 #SQL computatious                     : 66
 Total SQL KPI compute time (us)       : 202907
 Average SQL KPI compute time (us)     : 3074
 #LUA computatious                     : 66
 Total LUA KPI compute time (us)       : 3211022
 Average LUA KPI compute time (us)     : 48651
```

```
Event History
Timestamp               #Times   Event               RC Context
----------------------- -------- ------------------- --
----------------------------------------
09/15/2022 02:18:24.428 40323979 DSRC_PERIOD_RD       0
/services;serviceName=ewlc_oper/radio_oper_data
09/15/2022 01:18:07.561 941442   DST_STORE_END        0

09/15/2022 01:18:07.561 941442   DST_STORE_BEGIN      0

09/15/2022 01:18:07.560 941442   DSRC_NORMALIZE       0 rrmRadSlot

09/15/2022 00:00:03.583 604      DSRC_ONCHG_RD        0
/services;serviceName=ewlc/wlan_config
```

show lisp site detail

マップ サーバの詳細な Locator ID Separation Protocol（LISP）サイト情報を表示するには、**show lisp site detail** コマンドを使用します。

show lisp site detail [{**eid-table** {**default** | **vlan** *vlan-id* | **vrf** *vrf-name* } | **instance-id** *id-number* | **internal** {**eid-table** {**default** | **vlan** *vlan-id* | **vrf** *vrf-name* } | **instance-id** *id-number*}}]

構文の説明

eid-table	EIDテーブルを入力するオプション。
default	デフォルト VRF の情報を示します。
vlan *vlan-id*	VLAN 情報を入力します。
vrf *vrf-name*	VRF 名を入力します。
instance-id *id-number*	EID インスタンス ID を入力します。
internal	サイトの内部情報の詳細を示します。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、マップ サーバー の詳細な Locator ID Separation Protocol（LISP）サイト情報を表示する例を示します。

```
Device# show lisp site detail
```

show logging profile wireless end timestamp

フィルタリングのためにログ フィルタリングの終了位置のタイムスタンプを指定するには、**show logging profile wireless end timestamp** コマンドを使用します。

show logging profile wireless end timestamp *time-stamp*

構文の説明

time-stamp	フィルタリングを終了する時間。たとえば、2017/02/10 14:41:50.849 のようになります。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

トレース出力を取得するには、**show logging profile wireless internal** コマンドを使用して internal キーワードが有効になっていることを確認します。

例

次に、フィルタリングのためにログ フィルタリングの終了位置のタイムスタンプを指定する例を示します。

```
Device# show logging profile wireless end timestamp 2017/02/10 14:41:50.849
```

show logging profile wireless filter

ログのフィルタを指定するには、**show logging profile wireless filter** コマンドを使用します。

show logging profile wireless filter {**ipv4** | **mac** | **string** | **uuid**}

構文の説明

ipv4	特定の IP アドレス アプリケーション コンテキストを含むログを選択します。
mac	特定の MAC アプリケーション コンテキストを含むログを選択します。
string	特定の文字列アプリケーション コンテキストを含むログを選択します。
uuid	特定の汎用一意識別子（UUID）アプリケーション コンテキストを含むログを選択します。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

トレース出力を取得するには、**show logging profile wireless internal** コマンドを使用して **internal** キーワードが有効になっていることを確認します。

internal キーワードを指定しない場合は、顧客の選定したログのみが表示されます。

例

次に、ログのフィルタを指定する例を示します。

```
Device# show logging profile wireless filter ipv4 10.10.11.1
```

show logging profile wireless fru

Field Replaceable Unit（FRU）固有のコマンドを指定するには、**show logging profile wireless fru** コマンドを使用します。

show logging profile wireless fru {0 {reverse | to-file}| chassis} {**0** {**reverse** | **to-file**} | **chassis**}

構文の説明

0	SPA-Inter-Processor スロット 0。
reverse	時系列の逆順でログを表示します。
to-file	ディスクに保存されているファイルをデコードし、出力をファイルに書き込みます。
chassis	シャーシ名。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

トレース出力を取得するには、**show logging profile wireless internal** コマンドを使用して **internal** キーワードが有効になっていることを確認します。

internal キーワードを指定しない場合は、顧客の選定したログのみが表示されます。

例

次に、FRU 固有のコマンドを指定する例を示します。

```
Device# show logging profile wireless fru 0
```

show logging profile wireless internal

すべてのログを選択するには、**show logging profile wireless internal** コマンドを使用します。

show logging profile wireless internal

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

トレース出力を取得するには、**show logging profile wireless internal** コマンドを使用して **internal** キーワードが有効になっていることを確認します。

internal キーワードを指定しない場合は、顧客の選定したログのみが表示されます。

例

次に、すべてのログを表示する例を示します。

```
Device# show logging profile wireless internal
```

show logging profile wireless level

特定のレベルを超えるログを選択するには、**show logging profile wireless level** コマンドを使用します。

show logging profile wireless level {**debug** | **emergency** | **error** | **info** | **noise** | **notice** | **verbose** | **warning** }

構文の説明

debug	デバッグ メッセージを選択します。
emergency	緊急事態が考えられるメッセージを選択します。
error	エラー メッセージを選択します。
info	情報メッセージを選択します。
noise	考えられる最大のメッセージを選択します。
notice	通知メッセージを選択します。
verbose	詳細デバッグ メッセージを選択します。
warning	警告メッセージを選択します。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

トレース出力を取得するには、**show logging profile wireless internal** コマンドを使用して **internal** キーワードが有効になっていることを確認します。

internal キーワードを指定しない場合は、顧客の選定したログのみが表示されます。

例

次に、特定のレベルを超えるログを選択する例を示します。

```
Device# show logging profile wireless level info
```

show logging profile wireless module

特定のモジュールのログを選択するには、**show logging profile wireless module** コマンドを使用します。

show logging profile wireless module *module-name*

構文の説明

module-name	モジュール名のカンマまたはスペースで区切られたリスト。たとえば、dbal、tdllib、または「dbal tdllib」などです。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

トレース出力を取得するには、**show logging profile wireless internal** コマンドを使用して **internal** キーワードが有効になっていることを確認します。

internal キーワードを指定しない場合は、顧客の選定したログのみが表示されます。

例

次に、特定のモジュールのログを選択する例を示します。

```
Device# show logging profile wireless module dbal
```

show logging profile wireless reverse

ログを時系列の逆の順序で表示するには、**show logging profile wireless reverse** コマンドを使用します。

show logging profile wireless reverse

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

トレース出力を取得するには、**show logging profile wireless internal** コマンドを使用して **internal** キーワードが有効になっていることを確認します。

internal キーワードを指定しない場合は、顧客の選定したログのみが表示されます。

例

次に、時系列の逆順でログを表示する例を示します。

```
Device# show logging profile wireless reverse
```

show logging profile wireless start

ログ フィルタリングの開始場所を指定するには、**show logging profile wireless start** コマンドを使用します。

show logging profile wireless start {**marker** *marker* | **timestamp** *time-stamp*}

構文の説明

marker	フィルタリングを開始するマーカー。これは、以前に設定したマーカーと一致している必要があります。
timestamp	フィルタリングのタイムスタンプ。たとえば、「2017/02/10 14:41:50.849」というようになります。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

トレース出力を取得するには、**show logging profile wireless internal** コマンドを使用して **internal** キーワードが有効になっていることを確認します。

internal キーワードを指定しない場合は、顧客の選定したログのみが表示されます。

例

次に、ログ フィルタリングの開始場所を指定する例を示します。

```
Device# show logging profile wireless start timestamp 2017/02/10 14:41:50.849
```

show logging profile wireless switch

ログを検索するようにスイッチを指定するには、**show logging profile wireless switch** コマンドを使用します。

show logging profile wireless switch {*switch-num* | **active** | **standby**}

構文の説明

chassis-num	シャーシ番号。
active	アクティブインスタンスを選択します。
standby	スタンバイインスタンスを選択します。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

トレース出力を取得するには、**show logging profile wireless internal** コマンドを使用して **internal** キーワードが有効になっていることを確認します。

internal キーワードを指定しない場合は、顧客の選定したログのみが表示されます。

例

次に、ログを検索するシャーシ番号を指定する例を示します。

```
Device# show logging profile wireless switch active
```

show logging profile wireless to-file

ディスクに保存されているファイルをデコードし、出力をファイルに書き込むには、**show logging profile wireless to-file** コマンドを使用します。

show logging profile wireless to-file *output-file-name*

構文の説明

output-file-name	出力ファイル名。この名前のファイルがフラッシュ メモリに作成されます。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

トレース出力を取得するには、**show logging profile wireless internal** コマンドを使用して **internal** キーワードが有効になっていることを確認します。

internal キーワードを指定しない場合は、顧客の選定したログのみが表示されます。

例

次に、ディスクに保存されているファイルをデコードし、出力をファイルに書き込む例を示します。

```
Device# show logging profile wireless to-file testfile
```

show mdns-sd cache

mDNS キャッシュの詳細を表示するには、**show mdns-sd cache** コマンドを使用します。

show mdns-sd cache { **ap-mac** *mac-address (H.H.H)* | **client-mac** *client-mac-address (H.H.H)* | **detail** | **glan-id** *<1 - 5>* | **location-group** *<0 - 4096>* | **mdns-ap** *mdns-ap mac address (H.H.H)* | **rlan-id** *<1 - 128>* | **statistics** | **type** { **A-AAAA** | **PTR** | **SRV** | **TXT** } | **udn** { *<1 - 4294967295>* | **shared** } | **wired** | **wlan-id** *<0 - 4096>* }

構文の説明

ap-mac *mac-address (H.H.H)*	AP イーサネット MAC アドレスを指定します。
client-mac *client-mac-address (H.H.H)*	クライアントの MAC アドレスを指定します。
detail	キャッシュを詳細に指定します。
location-group *<0 - 4096>*	ロケーショングループを指定します。値の範囲は 0 ～ 4096 です。
mdns-ap *mdns-ap mac address (H.H.H)*	特定の mDNS AP から学習したキャッシュを指定します。
rlan-id *<1 - 128>*	リモート LAN ID を指定します。値の範囲は 1 ～ 128 です。
statistics	mDNS キャッシュの統計を指定します。
type	mDNS レコードタイプを指定します。レコードタイプは、A-AAAA、PTR、SRV、および TXT です。
udn *<1 - 4294967295>*	UDN ID を指定します。値の範囲は 1 ～ 4294967295 です。
shared	UDN 共有サービスを指定します。
wired	有線クライアントからの mDNS サービスを指定します。
wlan-id *<0 - 4096>*	WLAN ID を指定します。値の範囲は 1 ～ 4096 です。

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 Amsterdam 17.3.1	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

例

次に、mDNS キャッシュの詳細を表示する例を示します。

```
Device# show mdns-sd cache
```

show mdns-sd cache detail

マルチキャスト DNS（mDNS）キャッシュの詳細を表示するには、**show mdns-sd cache detail** コマンドを使用します。

show mdns-sd cache detail

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 Amsterdam 17.1.1s	このコマンドが導入されました。

例

次に、**show mdns-sd cache detail** コマンドの出力例を示します。

```
Device# show mdns-sd cache detail

Name: _printer._tcp.local
  Type: PTR
  TTL: 4500
  VLAN: 21
  Client MAC: ace2.d3bc.047e
  Remaining-Time: 4383
  mDNS Service Policy: default-mdns-service-policy
  Rdata: HP OfficeJet Pro 8720 [BC047E] (2)._printer._tcp.local
```

show mdns-sd cache upn shared

マルチキャスト DNS（mDNS）キャッシュのユーザー パーソナル ネットワーク共有サービスの詳細を表示するには、**show mdns-sd cache upn shared** コマンドを使用します。

show mdns-sd cache upn shared

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 Amsterdam 17.1.1s	このコマンドが導入されました。

例

次に、mDNS キャッシュの UPN 共有サービスの詳細を表示する **show mdns-sd cache upn shared** コマンドの出力例を示します。

```
Device# show mdns-sd cache upn shared

------------------------------------------------------------------ PTR Records
------------------------------------------------------------------
RECORD-NAME                                        TTL      TYPE      ID    CLIENT-MAC
  RR-RECORD-DATA
-------------------------------------------------------------------------------------------------------------------
9.1.1.7.5.D.E.F.F.F.6.C.7.E.2.1.0.0.0.0.0.0.0.0.0  4500     WLAN      2     10e7.c6d5.7119
  HP10E7C6D57119-2860.local
_services._dns-sd._udp.local                       4500     WLAN      2     10e7.c6d5.7119
  _ipps._tcp.local
_universal._sub._ipps._tcp.local                   4500     WLAN      2     10e7.c6d5.7119
  HP DeskJet 5000 series [D57119] (3127)._ipps._tcp.
_print._sub._ipps._tcp.local                       4500     WLAN      2     10e7.c6d5.7119
  HP DeskJet 5000 series [D57119] (3127)._ipps._tcp.
_ePCL._sub._ipps._tcp.local                        4500     WLAN      2     10e7.c6d5.7119
  HP DeskJet 5000 series [D57119] (3127)._ipps._tcp.
_ipps._tcp.local                                   4500     WLAN      2     10e7.c6d5.7119
  HP DeskJet 5000 series [D57119] (3127)._ipps._tcp.
_services._dns-sd._udp.local                       4500     WLAN      2     10e7.c6d5.7119
  _ipp._tcp.local
_universal._sub._ipp._tcp.local                    4500     WLAN      2     10e7.c6d5.7119
  HP DeskJet 5000 series [D57119] (3127)._ipp._tcp.l
_print._sub._ipp._tcp.local                        4500     WLAN      2     10e7.c6d5.7119
  HP DeskJet 5000 series [D57119] (3127)._ipp._tcp.l
_ePCL._sub._ipp._tcp.local                         4500     WLAN      2     10e7.c6d5.7119
  HP DeskJet 5000 series [D57119] (3127)._ipp._tcp.l
.
.
.
------------------------------------------------------------------ SRV Records
------------------------------------------------------------------
```

```
RECORD-NAME                                        TTL      TYPE      ID    CLIENT-MAC
  RR-RECORD-DATA
-------------------------------------------------------------------------------------------
HP DeskJet 5000 series [D57119] (3127)._ipp._  4500     WLAN      2     10e7.c6d5.7119
  0 0 631 HP10E7C6D57119-2860.local
HP DeskJet 5000 series [D57119] (3127)._http.  4500     WLAN      2     10e7.c6d5.7119
  0 0 80 HP10E7C6D57119-2860.local
HP DeskJet 5000 series [D57119] (3127)._ipps.  4500     WLAN      2     10e7.c6d5.7119
  0 0 631 HP10E7C6D57119-2860.local
HP DeskJet 5000 series [D57119] (3127)._uscan  4500     WLAN      2     10e7.c6d5.7119
  0 0 8080 HP10E7C6D57119-2860.local
HP DeskJet 5000 series [D57119] (3127)._prive  4500     WLAN      2     10e7.c6d5.7119
  0 0 80 HP10E7C6D57119-2860.local
HP DeskJet 5000 series [D57119] (3127)._uscan  4500     WLAN      2     10e7.c6d5.7119
  0 0 443 HP10E7C6D57119-2860.local
HP DeskJet 5000 series [D57119] (3127)._scann  4500     WLAN      2     10e7.c6d5.7119
  0 0 8080 HP10E7C6D57119-2860.local
HP DeskJet 5000 series [D57119] (3127)._pdl-d  4500     WLAN      2     10e7.c6d5.7119
  0 0 9100 HP10E7C6D57119-2860.local

------------------------------------------------------------- A/AAAA Records
-------------------------------------------------------------------
RECORD-NAME                                        TTL      TYPE      ID    CLIENT-MAC
  RR-RECORD-DATA
-------------------------------------------------------------------------------------------
HP10E7C6D57119-2860.local                          4500     WLAN      2     10e7.c6d5.7119
  8.16.16.99

------------------------------------------------------------- TXT Records
-------------------------------------------------------------------
RECORD-NAME                                        TTL      TYPE      ID    CLIENT-MAC
  RR-RECORD-DATA
-------------------------------------------------------------------------------------------
HP DeskJet 5000 series [D57119] (3127)._ipp._  4500     WLAN      2     10e7.c6d5.7119
  [502]'txtvers=1''adminurl=http://HP10E7C6D57119-28
HP DeskJet 5000 series [D57119] (3127)._http.  4500     WLAN      2     10e7.c6d5.7119
  [1]''
HP DeskJet 5000 series [D57119] (3127)._ipps.  4500     WLAN      2     10e7.c6d5.7119
  [502]'txtvers=1''adminurl=http://HP10E7C6D57119-28
HP DeskJet 5000 series [D57119] (3127)._uscan  4500     WLAN      2     10e7.c6d5.7119
  [280]'txtvers=1''adminurl=http://HP10E7C6D57119-28
HP DeskJet 5000 series [D57119] (3127)._prive  4500     WLAN      2     10e7.c6d5.7119
  [124]'txtvers=1''ty=HP DeskJet 5000 series [D57119
HP DeskJet 5000 series [D57119] (3127)._uscan  4500     WLAN      2     10e7.c6d5.7119
  [280]'txtvers=1''adminurl=http://HP10E7C6D57119-28
HP DeskJet 5000 series [D57119] (3127)._scann  4500     WLAN      2     10e7.c6d5.7119
  [177]'txtvers=1''adminurl=http://HP10E7C6D57119-28
HP DeskJet 5000 series [D57119] (3127)._pdl-d  4500     WLAN      2     10e7.c6d5.7119
  [211]'txtvers=1''rp=''priority=40''UUID=9fe36149-9
```

show mdns-sd cache upn detail

マルチキャスト DNS（mDNS）キャッシュのユーザー パーソナル ネットワーク識別子の詳細を表示するには、**show mdns-sd cache upn detail** コマンドを使用します。

show mdns-sd cache upn*upn-id* **detail**

構文の説明

upn-id	ユーザーパーソナルネットワーク識別子。

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 Amsterdam 17.1.1s	このコマンドが導入されました。

例

次に、mDNS キャッシュの UPN 識別子の詳細を表示する **show mdns-sd cache upn detail** コマンドの出力例を示します。

```
Device# show mdns-sd cache upn 777 detail

Name: _services._dns-sd._udp.local
  Type: PTR
  TTL: 4500
  WLAN: 2
  WLAN Name: mdns-psk
  VLAN: 16
  Client MAC: f4f9.51e2.a6a6
  AP Ethernet MAC: 002a.1087.d68a
  Remaining-Time: 4486
  Site-Tag: default-site-tag
  mDNS Service Policy: madhu-mDNS-Policy
  Overriding mDNS Service Policy: NO
  UPN-ID: 7777
  UPN-Status: Enabled
  Rdata: _airplay._tcp.local
```

show mdns-sd flexconnect summary

mDNS FlexConnect サイトの概要を表示するには、**show mdns-sd flexconnect summary** コマンドを使用します。

show mdns-sd flexconnect 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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	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

例

次に、mDNS FlexConnect サイトの概要を表示する例を示します。

```
Device# show mdns-sd flexconnect summary
```

show mdns-sd statistics

mDNS の統計を表示するには、**show mdns-sd statistics** コマンドを使用します。

show mdns-sd statistics { **debug** | **flexconnect** | **rlan-id** *<1 - 128>* **wired** | **wlan-id** *<1 - 4096>* }

構文の説明

debug	mDNS のデバッグの統計を指定します。
flexconnect	mDNS の FlexConnect の統計を指定します。
rlan-id*<1 - 128>*	リモート LAN（RLAN）ID を指定します。値の範囲は 1 ～ 128 です。
wired	mDNS の有線の統計を指定します。
wlan-id*<1 - 4096>*	WLAN ID を指定します。値の範囲は 1 ～ 4096 です。

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 Amsterdam 17.3.1	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

例

次に、mDNS の統計を表示する例を示します。

```
Device# show mdns-sd statistics
```

show mdns-sd summary

mDNS サービス検出設定の概要を表示するには、**show mdns-sd summary** コマンドを使用します。

show mdns-sd 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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	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

例

次に、mDNS サービス検出設定の概要を表示する例を示します。

```
Device# show mdns-sd summary
```

show mdns-sd sp-sdg statistics

サービスピア SDG 通信の統計を確認するには、**show mdns-sd sp-sdg statistics** コマンドを使用します。

show mdns-sd sp-sdg statistics

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 Bengaluru 17.5.1	このコマンドが導入されました。

次に、サービスピア SDG 通信の統計を確認する例を示します。

```
Device# show mdns-sd sp-sdg statistics
                          One min, 5 mins, 1 hour
Average Input rate (pps) :    0,       0,    0
Average Output rate (pps) :   0,       0,    0
Messages sent:
Query : 0
ANY query : 0
Advertisements : 0
Advertisement Withdraw : 0
Interface down : 0
Vlan down : 0
Service-peer ID change : 0
Service-peer cache clear : 0
Resync response : 0
Keep-Alive : 1
Messages received:
Query response : 0
ANY Query response : 0
Cache-sync : 0
Get service-instance : 0
Keep-Alive response : 1
```

show mobility

レイヤ3モビリティおよびワイヤレス ネットワークに関する情報を表示するには、特権EXECモードで **showmobility** コマンドを使用します。

show mobility {**ap** [*ip-address*] | **mn** [**ip** *ip-address*] | **mac** *mac-address* | **network** *network-id* | **status**}

構文の説明

ap	アクセス ポイントに関する情報を表示します。
ip-address	（任意）IP アドレス。
mn	モバイル ノードに関する情報を表示します。
ip *ip-address*	（任意）IP データベース スレッドに関する情報を表示します。
mac *mac-address*	MAC データベース スレッドに関する情報を表示します。
network *network-id*	特定のワイヤレス ネットワーク ID に関する情報を表示します。
status	ステータス情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(18)SXD	このコマンドが Supervisor Engine 720 に導入されました。
12.2(18)SXD3	このコマンドの出力は、TCP adjust-mss ステータスを含むように変更されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

使用上のガイドライン

このコマンドは、WLSM が搭載された Cisco 7600 シリーズ ルータでのみサポートされます。

例

次に、アクセス ポイントに関する情報を表示する例を示します。

```
Router# show mobility
 ap
AP IP Address   AP Mac Address Wireless Network-ID
--------------- -------------- -------------------
10.1.1.2 000d.29a2.a852 101 102 109 103
```

次に、特定のネットワーク ID のアクセス ポイントに関する情報を表示する例を示します。

```
Router# show mobility
 ap 172.16.1.2 detail
```

```
IP Address : 172.16.1.2
MAC Address : 000d.29a2.a852
Participating Wireless Tunnels: 101, 102, 109, 103
Registered Mobile Nodes on AP {172.16.1.2, 000d.29a2.a852} :
MN Mac Address MN IP Address AP IP Address Wireless Network-ID
-------------- --------------- --------------- -------------------
000a.8afa.85c9 10.1.3.11 172.16.1.2 103
000d.bdb7.83f7 10.1.2.11 172.16.1.2 102
000d.bdb7.83fb 10.1.1.11 172.16.1.2 101
Router# show mobility
 network-id 101
Wireless Network ID : 101
Wireless Tunnel Source IP Address : 10.1.1.1
Wireless Network Properties : Trusted
Wireless Network State : Up
Registered Access Point on Wireless Network 101:
AP IP Address AP Mac Address Wireless Network-ID
--------------- -------------- -------------------
176.16.1.2 000d.29a2.a852 101 102 109 103
Registered Mobile Nodes on Wireless Network 101:
MN Mac Address MN IP Address AP IP Address Wireless Network-ID
-------------- --------------- --------------- -------------------
000d.bdb7.83fb 10.1.1.11 176.16.1.2 101
Router# show mobility
 status
WLAN Module is located in Slot: 4 (HSRP State: Active) LCP
Communication status      : up
MAC address used for Proxy ARP: 0030.a349.d800
Number of Wireless Tunnels    : 1
Number of Access Points       : 2
Number of Mobile Nodes        : 0
Wireless Tunnel Bindings:
Src IP Address   Wireless Network-ID  Flags
---------------  -------------------  -------
10.1.1.1          101                  B
Flags: T=Trusted, B=IP Broadcast enabled, A=TCP Adjust-mss enabled
```

関連コマンド

コマンド	説明
mobility	ワイヤレス mGRE トンネルを設定します。

show monitor capture

モニターキャプチャバッファまたはキャプチャポイントの内容を表示するには、特権 EXEC モードで **show monitor capture** コマンドを使用します。

show monitor capture [*epc-capture-name* [**parameter** | **buffer** [{ **brief** | **detailed** | **dump** }]]]

構文の説明

epc-capture-name	組み込みパケットキャプチャの名前を指定します。
buffer	指定されたキャプチャバッファの内容を表示します。
dump	（任意）キャプチャされたパケットの 16 進数ダンプおよびメタデータを表示します。
brief	（任意）キャプチャされたパケットの情報の簡単な出力を提供します。
detail	（任意）キャプチャされたパケットの情報の詳細な出力を提供します。
parameter	キャプチャを指定するために使用された EXEC コマンドを再構成し、表示します。
detailed	キャプチャされたパケットの情報の詳細な出力を提供します。

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 Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

show monitor capture コマンドは、キャプチャバッファが実行状態でないときに入力できます。

detail キーワードを入力すると、パケットはレイヤ 4 プロトコルレベルに復号されて表示されます。**dump** キーワードを入力すると、非 IP パケットが 16 進数ダンプ形式で表示されます。ACL を表示フィルタとして設定して、ACL によって許可されたパケットのみを表示することができます。

次に、キャプチャバッファのすべてのパケットを表示する例を示します。出力は見ればすぐわかります。

```
Device# show monitor capture mycap buffer

buffer size (KB) : 2048000
buffer used (KB) : 128
packets in buf : 17
packets dropped : 0
packets per sec : 3
```

次に、キャプチャの指定に使用されたコマンドのリストを表示する例を示します。

```
Device# show monitor capture cap1 parameter

  monitor capture cap1 interface GigabitEthernet 1/0/1 both
  monitor capture cap1 match any
  monitor capture cap1 buffer size 10
  monitor capture cap1 limit pps 1000
```

次に、キャプチャされたパケットの情報から簡単な出力を表示する例を示します。出力は見ればすぐわかります。

```
Device# show monitor capture cap1 buffer brief

------------------------------------------------------------------
#   size   timestamp     source             destination   protocol
------------------------------------------------------------------
   0   62    0.000000   10.0.0.1         ->  203.0.113.254  UDP
   1   46    0.267992   10.0.1.2         ->  203.0.113.204  IGMP
   2   76    0.428979   172.16.255.3     ->  172.16.255.3   UDP
   3   62    1.613982   10.0.29.1        ->  172.16.200.2   UDP
   4   74    1.659970   10.0.1.3         ->  10.0.0.10      EIGRP
   5   90    2.016006   10.29.0.4        ->  203.0.113.224  UDP
   6   74    2.088008   10.1.9.2         ->  203.0.113.10   EIGRP
   7   76    2.114008   172.17.254.1     ->  172.16.255.1   UDP
   8   74    2.245990   10.29.0.3        ->  203.0.113.10   EIGRP
   9   46    2.262987   10.0.0.0         ->  203.0.113.1    IGMP
  10   77    2.362988   10.1.9.2         ->  203.0.113.10   EIGRP
  11   62    2.631971   10.29.0.2        ->  203.0.113.2    UDP
  12   74    2.934009   10.29.0.5        ->  203.0.113.10   EIGRP
  13   74    3.331984   10.29.0.6        ->  203.0.113.10   EIGRP
  14   46    3.499974   10.0.0.0         ->  203.0.113.1    IGMP
  15   46    4.304992   10.0.0.0         ->  203.0.113.1    IGMP
  16   76    5.157005   172.16.255.3     ->  172.17.255.3   UDP
```

次に、キャプチャバッファのすべてのパケットを表示する例を示します。出力は見ればすぐわかります。

```
Device# show monitor capture cap1 buffer detailed

 ------------------------------------------------------------------
#   size   timestamp     source             destination   protocol
------------------------------------------------------------------
   0   62    0.000000   10.29.0.2         ->  172.16.255.3   UDP
  0000:  01005E00 00020000 0C07AC1D 080045C0   ..^...........E.
  0010:  00300000 00000111 CFDC091D 0002E000   .0..............
  0020:  000207C1 07C1001C 802A0000 10030AFA   .........*......
  0030:  1D006369 73636F00 0000091D 0001       ..example.......

   1   46    0.267992   10.0.0.0          ->  172.16.255.1   IGMP
  0000:  01005E00 0002001B 2BF69280 080046C0   ..^.....+.....F.
  0010:  00200000 00000102 44170000 0000E000   . ......D.......
  0020:  00019404 00001700 E8FF0000 0000       ..............

   2   76    0.428979   172.16.255.3     ->  172.17.255.3    UDP
  0000:  00000C07 AC1DB414 89031124 080045C0   ...........$..E.
  0010:  003E0000 0000FF11 64C5AC10 FF03AC11   .>......d.......
  0020:  FF030286 0286002A 84A40001 001EAC10   .......*........
  0030:  FF030000 01000014 00000000 04000004   ................

   3   62    1.613982   10.26.11.3        ->  172.16.255.1    UDP
```

```
 0000:  01005E00 0002001B 2BF68680 080045C0   ..^.....+.....E.
 0010:  00300000 00000111 CFDB091D 0003E000   .0..............
 0020:  000207C1 07C1001C 88B50000 08030A6E   ...............n
 0030:  1D006369 73636F00 0000091D 0001       ..example.......

  4   74    1.659970   10.29.3.2         ->  172.16.255.2   EIGRP
 0000:  01005E00 000A001B 2BF69280 080045C0   ..^.....+.....E.
 0010:  003C0000 00000258 CE81091D 0002E000   .<.....X........
 0020:  000A0205 F3000000 00000000 00000000   ................
 0030:  00000000 00D10001 000C0100 01000000   ................

  5   90    2.016006   10.22.1.4         ->  203.0.113.1     UDP
 0000:  FFFFFFFF FFFF001C 0F2EDC00 080045C0   ..............E.
 0010:  004C0000 00000111 AFC1091D 0004FFFF   .L..............
 0020:  FFFF007B 007B0038 5B14E500 06E80000   ...{.{.8[.......
 0030:  00000021 BE23494E 49540000 00000000   ...!.#INIT......
```

次に、キャプチャされたパケットの 16 進数ダンプを表示する例を示します。

```
Device# show monitor capture cap1 buffer dump
0
 0000:  01005E00 00020000 0C07AC1D 080045C0   ..^...........E.
 0010:  00300000 00000111 CFDC091D 0002E000   .0..............
 0020:  000207C1 07C1001C 802A0000 10030AFA   .........*......
 0030:  1D006369 73636F00 0000091D 0001       ..example.......

1
 0000:  01005E00 0002001B 2BF69280 080046C0   ..^.....+.....F.
 0010:  00200000 00000102 44170000 0000E000   . ......D.......
 0020:  00019404 00001700 E8FF0000 0000       ..............

2
 0000:  01005E00 0002001B 2BF68680 080045C0   ..^.....+.....E.
 0010:  00300000 00000111 CFDB091D 0003E000   .0..............
 0020:  000207C1 07C1001C 88B50000 08030A6E   ...............n
 0030:  1D006369 73636F00 0000091D 0001       ..example.......

3
 0000:  01005E00 000A001C 0F2EDC00 080045C0   ..^...........E.
 0010:  003C0000 00000258 CE7F091D 0004E000   .<.....X........
 0020:  000A0205 F3000000 00000000 00000000   ................
 0030:  00000000 00D10001 000C0100 01000000   ................
 0040:  000F0004 00080501 0300                ..........
```

show nmsp

Network Mobility Services Protocol（NMSP）構成の設定を表示するには、**show nmsp** 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

attachment suppress interfaces	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。
notification interval	NMSP 通知間隔を表示します。
statistics connection	すべての接続別カウンタを表示します。
statistics summary	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。
subscription detail *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。
subscription summary	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 Gibraltar 16.10.1	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。

```
デバイス#  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 nmsp cloud-services statistics

NMSP クラウドサービスの統計情報を表示するには、**show nmsp cloud-services statistics** コマンドを使用します。

show nmsp cloud-services statistics ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）。
active R0	ルートプロセッサ スロット 0 のアクティブな NMSP クラウド サービスのアクティブなインスタンス。
standby R0	ルートプロセッサ スロット 0 のアクティブな NMSP クラウド サービスのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、NMSP クラウドサービスの統計情報を表示する例を示します。

```
Device# show nmsp cloud-services statistics
```

show nmsp cloud-services summary

NMSP クラウドサービスに関する情報の要約を表示するには、**show nmsp cloud-services summary** コマンドを使用します。

show nmsp cloud-services summary ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）。
active R0	ルートプロセッサ スロット 0 の NMSP クラウド サービスのアクティブなインスタンス。
standby R0	ルートプロセッサ スロット 0 のアクティブな NMSP クラウド サービスのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、NMSP クラウドサービスのサマリー情報を表示する例を示します。

```
Device# show nmsp cloud-services summary
```

show nmsp subscription group detail all

すべての CMX 接続のモビリティサービスグループのサブスクリプションの詳細を表示するには、**show nmsp subscription group detail all** コマンドを使用します。

show nmsp subscription group detail 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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、すべての CMX 接続のモビリティサービスグループのサブスクリプションの詳細を表示する例を示します。

```
Device# show nmsp subscription group detail all
```

show nmsp subscription group detail ap-list

CMX 接続によってグループに登録された AP MAC リストを表示するには、**show nmsp subscription group detail ap-list** コマンドを使用します。

show nmsp subscription group detail ap-list *group-name cmx-IP-addrress*

構文の説明

group-name	CMX AP グループ名。
cmx-IP-addrress	CMX の IP アドレス。

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、CMX 接続によってグループに登録された AP MAC リストを確認する例を示します。

```
Device# show nmsp subscription group detail ap-list Group1 127.0.0.1

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group AP MACs:
: 00:00:00:00:70:02  00:00:00:00:66:02  00:99:00:00:00:02  00:00:00:bb:00:02
  00:00:00:00:55:02  00:00:00:00:50:02  00:33:00:00:00:02  00:d0:00:00:00:02
  00:10:00:10:00:02  00:00:00:06:00:02  00:00:00:02:00:02  00:00:00:00:40:02
  00:00:00:99:00:02  00:00:00:00:a0:02  00:00:77:00:00:02  00:22:00:00:00:02
  00:00:00:00:00:92  00:00:00:00:00:82  00:00:00:00:03:02  aa:00:00:00:00:02
  00:00:00:50:00:42  00:00:0d:00:00:02  00:00:00:00:00:32  00:00:00:cc:00:02
  00:00:00:88:00:02  20:00:00:00:00:02  10:00:00:00:00:02  01:00:00:00:00:02
  00:00:00:00:00:02  00:00:00:00:00:01  00:00:00:00:00:00
```

show nmsp subscription group detail services

CMX 接続によってグループに登録されたサービスを表示するには、**show nmsp subscription group detail services** コマンドを使用します。

show nmsp subscription group detail services *group-name cmx-IP-addrress*

構文の説明

group-name	CMX AP グループ名。
cmx-IP-addrress	CMX の IP アドレス。

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、CMX 接続によってグループに登録されたサービスを確認する例を示します。

```
Device# show nmsp subscription group detail services Group1 127.0.0.1

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group filtered services:
Service            Subservice
----------------------------
RSSI               Mobile Station,
Spectrum
Info
Statistics
```

show nmsp subscription group summary

すべての CMX 接続のモビリティ サービス グループのサブスクリプションの概要を表示するには、**show nmsp subscription group summary** コマンドを使用します。

show nmsp subscription group 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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、すべての CMX 接続のモビリティ サービス グループのサブスクリプションの概要を確認する例を示します。

```
Device# show nmsp subscription group summary

CMX IP address: 127.0.0.1
  Groups subscribed by this CMX server:
  Group name: Group1
```

show ntp associations

Network Time Protocol（NTP）アソシエーションのステータスを表示するには、特権 EXEC モードで **show ntp associations** コマンドを使用します。

show ntp associations

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、NTP アソシエーションを表示する例を示します。:

```
Device# show ntp associations
  address         ref clock       st   when   poll reach  delay  offset   disp
*~10.1.1.99       72.163.32.44     2    918   1024   377  0.177   7.618  1.102
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
--
```

show parameter-map type webauth name

パラメータマップの webauth パラメータを確認するには、 **show parameter-map type webauth name** コマンドを使用します。

show parameter-map type webauth name *parameter-map name*

構文の説明

parameter-map name	パラメータマップの名前。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、パラメータマップの webauth パラメータを確認する例を示します。

```
Device# configure terminal
Device(config)# show parameter-map type webauth name parameter-map-name
```

show platform conditions

条件付きデバッグに関する情報を表示するには、**show platform conditions** コマンドを使用します。

show platform conditions

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、条件付きデバッグに関する情報を表示する例を示します。

```
Device# show platform conditions
```

show platform hardware

ハードウェア プラットフォームの Quantum flow processor データパスの統計情報を表示するには、 **show platform hardware chassis active qfp feature wireless wlclient datapath cpp-if-handle statistics** コマンドを使用します。

show hardware chassis active qfp feature wireless wlclient datapath cpp-if-handle *client-cpp-value* **statistics**{**clear** | **start** | **stop**}

構文の説明

active	アクティブ インスタンス。
qfp	Quantum Flow Processor。
wlclient	QFP ワイヤレス クライアント。
cpp-if-handle	クライアント cpp インターフェイスのハンドル。
client-cpp-value	クライアント cpp if ハンドル値。指定できる範囲は 1 ～ 4294967295 です。
statistics	クライアントの統計情報を示します。
clear	クライアントの統計情報を表示およびクリアします。
start	クライアントの統計情報の収集を開始します。
stop	クライアントの統計情報の収集を停止します。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、クライアントの統計情報の収集を開始する例を示します。

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
cpp-if-handle cpp-if-handle value statistics start
```

show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf

DSA がイネーブルになっているインターフェイスを表示するには、**show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf** コマンドを使用します。

show platform hardware chassis active qfp feature dns-snoop-agent client enabled-intf

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、DSA がイネーブルになっているインターフェイスを表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature dns-snoop-agent client
enabled-intf
Interface name: GigabitEthernet0/0/0, handle: 5
```

show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list

パターン リストの OpenDNS 文字列または FQDN フィルタを表示するには、**show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list** コマンドを使用します。

show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list {**fqdn-filter** *fqdn_filter_ID* | **odns_string**}

構文の説明

fqdn-filter	パターン リストの FQDN フィルタを表示します。
fqdn_filter_ID	FQDN フィルタ ID を参照します。有効範囲は 1 ～ 16 です。
odns_string	パターン リストの OpenDNS 文字列を表示します。

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、パターン リストの FQDN フィルタを表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature dns-snoop-agent client
hw-pattern-list fqdn-filter 1
Filter Name: urllist_flex_preauth

Name: url1.dns.com
Feature mask: 16, Dirty: 0, Ref count: 0, Match count: 0
```

show platform hardware chassis active qfp feature dns-snoop-agent client info

DSA クライアントの詳細を表示するには、**show platform hardware chassis active qfp feature dns-snoop-agent client info** コマンドを使用します。

show platform hardware chassis active qfp feature dns-snoop-agent client info

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、DSA クライアントの詳細を表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature dns-snoop-agent client info
Number of patterns added/deleted/total: 2/0/2
Number of re_table rebuilt : : 0
Number of str_table rebuilt: : 2
Registered clients: 0x001ffff0
Number of transaction started/ended: 2/2
Memory pool size/limit: 512/81920
Pending Deletion Pattern List:
```

show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list

パターン リストの OpenDNS 文字列または FQDN フィルタを表示するには、**show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list** コマンドを使用します。

show platform hardware chassis active qfp feature dns-snoop-agent client pattern-list {**fqdn-filter** *fqdn_filter_ID* | **odns_string**}

構文の説明

fqdn-filter	パターン リストの FQDN フィルタを表示します。
fqdn_filter_ID	FQDN フィルタ ID を参照します。有効範囲は 1 ～ 16 です。
odns_string	パターン リストの OpenDNS 文字列を表示します。

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、パターン リストの FQDN フィルタを表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature dns-snoop-agent client
pattern-list fqdn-filter 1
Filter Name: urllist_flex_preauth
Pattern List in CPP client: 1

Name: url1.dns.com
feature_mask: 0x00000010, hw_ptr: 0xdf86d510
```

show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache

DSA IP キャッシュ テーブルの詳細を表示するには、**show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache** コマンドを使用します。

show platform hardware chassis active qfp feature dns-snoop-agent datapath ip-cache {**address** [**ipv4** *ipv4_address* | **ipv6** *ipv6_address*] | **all** | **pattern** *regex_pattern*}

構文の説明

address [**ipv4** *ipv4_address* | **ipv6** *ipv6_address*]	DSA アドレス エントリの詳細を表示します
all	すべての DSA IP キャッシュ アドレスの詳細を表示します
pattern *regex_pattern*	DSA IP キャッシュ パターン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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、DSA アドレス エントリの詳細を表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature dns-snoop-agent datapath
ip-cache address ipv4 104.122.2.194
IP address: 104.122.2.194, client(s): 32, regex: www.adobe.com, expire in 0 seconds
```

次に、すべての DSA IP キャッシュ アドレスの詳細を表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature dns-snoop-agent datapath
ip-cache all
IP Address        Client(s) Expire     Match         RegexId      Dirty
-------------------------------------------------------------------------
172.217.13.228      2       132     .*google.com    0x4d7f9e20     0x0
```

次に、DSA IP キャッシュ パターンの詳細を表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature dns-snoop-agent datapath
ip-cache pattern .*google*
1 IP Addresses matching pattern .*google*
IP Address                    Client(s)  Expire   Match       RegexId    Dirty
-------------------------------------------------------------------------------
2607:f8b0:4004:800:0:0:0:2004   32         13    .*google*   0x31156220   0x0
```

show platform hardware chassis active qfp feature dns-snoop-agent datapath memory

DSA データパス メモリの詳細を表示するには、**show platform hardware chassis active qfp feature dns-snoop-agent datapath memory** コマンドを使用します。

show platform hardware chassis active qfp feature dns-snoop-agent datapath memory

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、DSA データパス メモリの詳細を表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature dns-snoop-agent datapath memory
Table-Name   Address      Size
----------------------------------------
IP Cache DB   0xda5bb420   512
IP Hash       0xda41f400   1024
String Table  0xdec6ac10
String Table  0xda41f010

==DSA Chunk info==
Chunk-Pool   Allocated     Total_Free   Init-Num     Low_Wat
------------------------------------------------------------
ip cache chunk   0             512          512          512

==DSA Runtime Info==
------------------------------------------------------------
dsa init state 0x7   dsa client mask 0x100010
```

show platform hardware chassis active qfp feature dns-snoop-agent datapath regexp-table

DSA 正規表現テーブルを表示するには、**show platform hardware chassis active qfp feature dns-snoop-agent datapath regexp-table** コマンドを使用します。

show platform hardware chassis active qfp feature dns-snoop-agent datapath regexp-table

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、DSA 正規表現テーブルを表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature dns-snoop-agent datapath
regexp-table
String Table 0xdec6ac10     WLS_FQDN_GRP_1
String Table 0xda41f010     ODNS String
```

show platform hardware chassis active qfp feature dns-snoop-agent datapath stats

DSA 統計情報を表示するには、**show platform hardware chassis active qfp feature dns-snoop-agent datapath stats** コマンドを使用します。

show platform hardware chassis active qfp feature dns-snoop-agent datapath stats

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、DSA 統計情報を表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature dns-snoop-agent datapath stats
DNS Snoop Agent Stats:
  parser unknown pkt: 0
  parser not needed: 0
  parser fmt error: 0
  parser pa error: 0
  parser non resp: 0
  parser multiple name: 0
  parser dns name err: 0
  parser matched ip: 0
  parser redirect: 0
  parser whitelist redirect: 0
  parser blacklist redirect: 0
  parser invalid redirect ip: 0
  parser skip: 0
  regex locked: 0
  regex not matched: 0
  pkt drop whitelist no redirect ip: 0
  pkt drop blacklist no redirect ip: 0
  entries in use: 0
  ip cache allocation fail: 0
  ip addr add: 0
  ip addr update: 0
  ip addr delete: 0
  ip addr cache hit: 0
  ip addr cache miss: 0
  ip addr bad param: 0
  ip addr delete not found: 0
  ip cache not initialized: 0
```

show platform hardware chassis active qfp feature et-analytics datapath runtime

データパスの ETA グローバル状態を表示するには、**show platform hardware chassis active qfp feature et-analytics datapath runtime** コマンドを使用します。

show platform hardware chassis active qfp feature et-analytics datapath runtime

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

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 Gibraltar 16.11.1	このコマンドが導入されました。

次に、ETA グローバルおよびインターフェイスの詳細を表示する例を示します。

```
Device# show platform hardware chassis active qfp feature et-analytics datapath runtime
ET-Analytics run-time information:
   Feature state: initialized (0x00000004)
   Inactive timeout : 15 secs (default 15 secs)
   WhiteList information :
      flag: False
      cgacl w0 : n/a
      cgacl w1 : n/a
   Flow CFG information :
      instance ID : 0x0
      feature ID : 0x1
      feature object ID : 0x1
      chunk ID : 0xC
```

show platform hardware chassis active qfp feature et-analytics datapath memory

ETA メモリの詳細を表示するには、**show platform hardware chassis active qfp feature et-analytics datapath memory** コマンドを使用します。

show platform hardware chassis active qfp feature et-analytics datapath memory

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、ETA メモリの詳細を表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature et-analytics datapath memory
ET-Analytics memory information:
   Size of FO : 3200 bytes
   No. of FO allocs : 0
   No. of FO frees : 0
```

show platform hardware chassis active qfp feature et-analytics datapath stats export

データパスの ETA フロー エクスポートを表示するには、**show platform hardware chassis active qfp feature et-analytics datapath stats export** コマンドを使用します。

show platform hardware chassis active qfp feature et-analytics datapath stats export

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、データパスの ETA フロー エクスポートを表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature et-analytics datapath stats
export
ET-Analytics 192.168.5.2:2055 vrf 0 Stats:
   Export statistics:
      Total records exported : 5179231
      Total packets exported : 3124873
      Total bytes exported : 3783900196
      Total dropped records : 0
      Total dropped packets : 0
      Total dropped bytes : 0
      Total IDP records exported :
            initiator->responder : 1285146
            responder->initiator : 979284
      Total SPLT records exported:
            initiator->responder : 1285146
            responder->initiator : 979284
      Total SALT records exported:
            initiator->responder : 0
            responder->initiator : 0
      Total BD records exported :
            initiator->responder : 0
            responder->initiator : 0
      Total TLS records exported :
            initiator->responder : 309937
            responder->initiator : 329469
```

show platform hardware chassis active qfp feature et-analytics datapath stats flow

ETA フローの統計情報を表示するには、**show platform hardware chassis active qfp feature et-analytics datapath stats flow** コマンドを使用します。

show platform hardware chassis active qfp feature et-analytics datapath stats flow

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、ETA フローの統計情報を表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature et-analytics datapath stats
flow
ET-Analytics Stats:
   Flow statistics:
      feature object allocs : 0
      feature object frees : 0
      flow create requests : 0
      flow create matching : 0
      flow create successful: 0
      flow create failed, CFT handle: 0
      flow create failed, getting FO: 0
      flow create failed, malloc FO : 0
      flow create failed, attach FO : 0
      flow create failed, match flow: 0
      flow create, aging already set: 0
      flow ageout requests : 0
      flow ageout failed, freeing FO: 0
      flow ipv4 ageout requests : 0
      flow ipv6 ageout requests : 0
      flow whitelist traffic match : 0
```

show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree

ETA 保留ワイヤレス クライアント ツリー内のクライアントを表示するには、**show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree** コマンドを使用します。

show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、ETA 保留ワイヤレス クライアント ツリー内のクライアントを表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature wireless et-analytics
eta-pending-client-tree
CPP IF_H    DPIDX        MAC Address    VLAN   AS  MS  WLAN        POA
------------------------------------------------------------------------------
0X2A      0XA0000001    2c33.7a5b.827b  160    RN  LC ewlc_ssid 0x90000003
0X2B      0XA0000002    2c33.7a5b.80fb  160    RN  LC ewlc_ssid 0x90000003
```

show platform hardware chassis active qfp feature wireless et-analytics statistics

ETA 保留ワイヤレス クライアント ツリーの統計情報を表示するには、**show platform hardware chassis active qfp feature wireless et-analytics statistics** コマンドを使用します。

show platform hardware chassis active qfp feature wireless et-analytics statistics

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、ETA保留ワイヤレスクライアントツリーの統計情報を表示する例を示します。

```
デバイス# show platform hardware chassis active qfp feature wireless et-analytics statistics
Wireless ETA cpp-client plumbing statistics
Number of ETA pending clients : 2
Counter                                                      Value
-----------------------------------------------------------------
Enable ETA on wireless client called                           0
Delete ETA on wireless client called                           0
ETA global cfg init cb TVI FIA enable error                    0
ETA global cfg init cb output SB read error                    0
ETA global cfg init cb output SB write error                   0
ETA global cfg init cb input SB read error                     0
ETA global cfg init cb input SB write error                    0
ETA global cfg init cb TVI FIA enable success                  0
ETA global cfg uninit cb ingress feat disable                  0
ETA global cfg uninit cb ingress cfg delete                    0
ETA global cfg uninit cb egress feat disable                   0
ETA global cfg uninit cb egress cfg delete er                  0
ETA pending list insert entry called                           4
ETA pending list insert invalid arg error                      0
ETA pending list insert entry exists error                     0
ETA pending list insert no memory error                        0
ETA pending list insert entry failed                           0
ETA pending list insert entry success                          4
ETA pending list delete entry called                           2
ETA pending list delete invalid arg error                      0
ETA pending list delete entry missing                          0
ETA pending list delete entry remove error                     0
ETA pending list delete entry success                          2
```

show platform hardware slot R0 ha_port interface stats

HA ポートインターフェイスの設定ステータスを表示するには、**show platform hardware slot R0 ha_port interface stats** コマンドを使用します。

show platform hardware slot R0 ha_port interface stats

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 Bengaluru 17.5.1	このコマンドが導入されました。

例

次に、HA ポートインターフェイスの設定ステータスを表示する例を示します。

```
Device# show platform hardware slot R0 ha_port interface stats
HA Port
ha_port   Link encap:Ethernet  HWaddr 70:18:a7:c8:80:70
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Memory:e0900000-e0920000


Settings for ha_port:
        Supported ports:            [ TP ]
        Supported link modes:       10baseT/Half 10baseT/Full
                                    100baseT/Half 100baseT/Full
                                    1000baseT/Full
        Supported pause frame use:   Symmetric
        Supports auto-negotiation:   Yes
        Supported FEC modes:         Not reported
        Advertised link modes:       10baseT/Half 10baseT/Full
                                     100baseT/Half 100baseT/Full
                                     1000baseT/Full
        Advertised pause frame use:  Symmetric
        Advertised auto-negotiation: Yes
        Advertised FEC modes:        Not reported
        Speed:                       Unknown!
        Duplex:                      Unknown! (255)
        Port:                        Twisted Pair
        PHYAD:                       1
        Transceiver:                 internal
        Auto-negotiation:            on
        MDI-X:                       off (auto)
        Supports Wake-on:            pumbg
        Wake-on:                     g
        Current message level:       0x00000007 (7)
                                     drv probe link
```

```
        Link detected:               no

NIC statistics:
     rx_packets:             0
     tx_packets:             0
     rx_bytes:               0
     tx_bytes:               0
     rx_broadcast:           0
     tx_broadcast:           0
     rx_multicast:           0
     tx_multicast:           0
     multicast:              0
     collisions:             0
     rx_crc_errors:          0
     rx_no_buffer_count:     0
     rx_missed_errors:       0
     tx_aborted_errors:      0
     tx_carrier_errors:      0
     tx_window_errors:       0
     tx_abort_late_coll:     0
     tx_deferred_ok:         0
     tx_single_coll_ok:      0
     tx_multi_coll_ok:       0
     tx_timeout_count:       0
     rx_long_length_errors:  0
     rx_short_length_errors: 0
     rx_align_errors:        0
     tx_tcp_seg_good:        0
     tx_tcp_seg_failed:      0
     rx_flow_control_xon:    0
     rx_flow_control_xoff:   0
     tx_flow_control_xon:    0
     tx_flow_control_xoff:   0
     rx_long_byte_count:     0
     tx_dma_out_of_sync:     0
     tx_smbus:               0
     rx_smbus:               0
     dropped_smbus:          0
     os2bmc_rx_by_bmc:       0
     os2bmc_tx_by_bmc:       0
     os2bmc_tx_by_host:      0
     os2bmc_rx_by_host:      0
     tx_hwtstamp_timeouts:   0
     rx_hwtstamp_cleared:    0
     rx_errors:              0
     tx_errors:              0
     tx_dropped:             0
     rx_length_errors:       0
     rx_over_errors:         0
     rx_frame_errors:        0
     rx_fifo_errors:         0
     tx_fifo_errors:         0
     tx_heartbeat_errors:    0
     tx_queue_0_packets:     0
     tx_queue_0_bytes:       0
     tx_queue_0_restart:     0
     tx_queue_1_packets:     0
     tx_queue_1_bytes:       0
     tx_queue_1_restart:     0
     rx_queue_0_packets:     0
     rx_queue_0_bytes:       0
     rx_queue_0_drops:       0
     rx_queue_0_csum_err:    0
     rx_queue_0_alloc_failed:0
```

```
rx_queue_1_packets:     0
rx_queue_1_bytes:       0
rx_queue_1_drops:       0
rx_queue_1_csum_err:    0
rx_queue_1_alloc_failed:0
```

show platform integrity

起動段階のチェックサムレコードを表示するには、**show platform integrity** コマンドを使用します。

show platform integrity [sign [nonce *nonce* **]]**

構文の説明

sign	（任意）。署名を表示します。
nonce	（任意）。ナンス値を入力します。

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 Bengaluru 17.4.1	このコマンドが導入されました。

次に、起動段階のチェックサムレコードを表示する例を示します。

```
Device# show platform integrity sign nonce 123
Platform: C9800-L-F-K9
Boot 0 Version: R04.1173930452019-06-11
Boot 0 Hash: A6C92C44976FC77DD42234444FFD87798FB9036A2762FAA4999A190A0258B18C
Boot Loader Version: 16.12(1r)
Boot Loader Hash:
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
OS Version: 2020-03-19_20.26
OS Hashes:
C9800-L-universalk9_wlc.2020-03-19_20.26.SSA.bin:
53E2DF1A1A082E36EA4CAB817C1794EC9D69AC0E90BCCBFECF9BCD0BCA9385AA9E9372ABF7431E4A08FC5E5B9670131C09D158E5B8A7B457501FE77AB9F1C26D
C9800-L-mono-universalk9_wlc.2020-03-19_20.26.SSA.pkg:
1D3279D53B0311CE42C669824DF86FB5596CD7CA45CA8D7FDC3D10657B8C9A48F4B0508D7BCFFD645CB6571AC1E674A57A82414E3D6E1666BE64E6132F707671
PCR0: EE14A2D5099DA343B3941C54A429C4AC1D3EE8E9B609F1AC00049768A470734E
PCR8: 78794D0F5667F8FA4E425E3CA2AF3CD99B90B219FD90222D622B3D563416BBAA
```

show platform software audit

Security Enhanced Linux（SELinux）監査ログを表示するには、特権 EXEC モードで **show platform software audit** コマンドを使用します。

show platform software audit {**all** | **summary** | **0** | **1** | **2** | **F0** | **R0** | **FP active** | **RP active**}

構文の説明

all	すべてのスロットからの監査ログを表示します。
summary	すべてのスロットからの監査ログの要約カウントを表示します。
0	SM-Inter-Processor スロット 0 の監査ログを表示します。
1	SM-Inter-Processor スロット 1 の監査ログを表示します。
2	SM-Inter-Processor スロット 2 の監査ログを表示します。
F0	Embedded-Service-Processor スロット 0 の監査ログを表示します。
R0	Route-Processor スロット 0 の監査ログを表示します。
FP active	アクティブな Embedded-Service-Processor スロットの監査ログを表示します。
RP active	アクティブな Route-Processor スロットの監査ログを表示します。

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 Gibraltar 16.11.1	このコマンドは、Cisco ISR 4000 シリーズ ルータ、Cisco CSR 1000V シリーズ ルータ、およびタイム センシティブ ネットワーキング（TSN）を実行している Cisco 1000 ISR シリーズ ルータに導入されました。
Cisco IOS XE Gibraltar 16.12.1	このコマンドは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに実装されました。

使用上のガイドライン

show platform software audit コマンドは、アクセス違反イベントを含むシステム ログを表示します。

Cisco IOS XE Gibraltar 16.11.1 では、許可モードでの操作は、IOS XE プラットフォームの特定のコンポーネント（プロセスまたはアプリケーション）を制限する目的で利用できます。許可モードでは、アクセス違反イベントが検出され、システム ログが生成されますが、イベントまたは操作自体はブロックされません。このソリューションは、主にアクセス違反検出モードで動作します。

次に、**show software platform software audit summary** コマンドの出力例を示します。

```
Device# show platform software audit summary
====================================
AUDIT LOG ON ACTIVE
------------------------------------
AVC Denial count: 7
```

次に、**show software platform software audit all** コマンドの出力例を示します。このコマンドは、audit.log ファイルの情報を表示します。

```
Device# show platform software audit all
====================================
AUDIT LOG ON ACTIVE
------------------------------------
========== START ============
type=DAEMON_START msg=audit(1553837190.262:3031): op=start ver=2.6.6 format=raw
kernel=4.4.172 auid=4294967295 pid=446 subj=system_u:system_r:auditd_t:s0 res=success
type=NETFILTER_CFG msg=audit(1553837185.956:2): table=nat family=2 entries=0
type=MAC_STATUS msg=audit(1553837186.523:3): enforcing=1 old_enforcing=0 auid=4294967295
 ses=4294967295
type=SYSCALL msg=audit(1553837186.523:3): arch=c000003e syscall=1 success=yes exit=1
a0=3 a1=7ffcf1c22070 a2=1 a3=0 items=0 ppid=203 pid=205 auid=4294967295 uid=0 gid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="load_policy"
 exe="/usr/sbin/load_policy" subj=kernel key=(null)
type=PROCTITLE msg=audit(1553837186.523:3):
proctitle=2F7573722F7362696E2F6C6F61645F706F6C696379002D69
type=MAC_POLICY_LOAD msg=audit(1553837186.528:4): policy loaded auid=4294967295
ses=4294967295
type=SYSCALL msg=audit(1553837186.528:4): arch=c000003e syscall=1 success=yes exit=1693637
 a0=4 a1=7f792d1d6000 a2=19d7c5 a3=f items=0 ppid=203 pid=205 auid=4294967295 uid=0 gid=0
 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="load_policy"
 exe="/usr/sbin/load_policy" subj=system_u:system_r:kernel_t:s0 key=(null)
…
```

このコマンドの出力を使用して、audit.log の内容をファイルにコピーしてから、リモートホストに転送することができます。

```
Device# show platform software audit all | redirect bootflash:audi_123.log

Device#dir bootflash:audi_123.log
Directory of bootflash:/audi_123.log
   27  -rw-            35305  Mar 29 2019 22:16:36 +00:00  audi_123.log

3249049600 bytes total (538112000 bytes free)
```

show platform software arp broadcast

アクセスポイント（AP）で Address Resolution Protocol（ARP）ブロードキャストステータスを表示するには、**show platform software arp broadcast** コマンドを使用します。

show platform software arp broadcast

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 Cupertino 17.8.1	このコマンドが導入されました。

例

次に、AP で ARP ブロードキャストを表示する例を示します。

```
Device# show platform software arp broadcast

Arp broadcast is enabled on vlans:
20,50
```

show platform software system all

現在の仮想マシンのステータスをチェックし、リソース不足によるパフォーマンスの問題（またはホスティング環境に関するその他の問題）を検出するには、特権EXECモードで**set platform software system all** コマンドを使用します。

show platform software system 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 モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、現在の仮想マシンとそのリソースのステータスをチェックする例を示します。

```
Device# show platform software system all

Processor Details
=================
Number of Processors : 6
Processor : 1 - 6
vendor_id : GenuineIntel
cpu MHz  : 2593.750
cache size : 35840 KB
Crypto Supported : Yes
model name : Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz

Memory Details
==============
Physical Memory : 16363904KB

VNIC Details
============
Name   Mac Address  Status Platform MTU
GigabitEthernet1 000c.2964.7126  UP 1500
GigabitEthernet2 000c.2964.7130  UP 1500

Hypervisor Details
====================
Hypervisor: VMWARE
Manufacturer: VMware, Inc.
Product Name: VMware Virtual Platform
Serial Number: VMware-56 4d e5 0a a7 dd 27 2b-0e 2f 36 6e 0f 64 71 26
UUID: 564DE50A-A7DD-272B-0E2F-366E0F647126
image_variant :

Boot Details
====================
Boot mode: BIOS
Bootloader version: 1.1
```

show platform software trace filter-binary

特定のモジュールの最新のトレース情報を表示するには、特権 EXEC モードまたはユーザー EXEC モードで **show platform software trace filter-binary** コマンドを使用します。

show platform software trace filter-binary*modules* ［**context** *mac-address*］

構文の説明

context*mac-address*	フィルタ処理に使用されるコンテキストを表します。また、モジュール名とトレース レベルに基づいてフィルタ処理できます。コンテキスト キーワードは、タグが付いているトレースに基づき MAC アドレスまたは他の引数を受け入れます。

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 Gibraltar 16.10.1	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、モジュールに関連するすべてのプロセス全体で `/tmp/.../` に存在するすべてのログを照合してソートします。指定されたモジュールに関連するすべてのプロセスのトレース ログがコンソールに出力されます。このコマンドでは、同じコンテンツの `collated_log_{system time}` という名前のファイルも `/crashinfo/tracelogs` ディレクトリに生成されます。

例

次に、ワイヤレス モジュールのトレース情報を表示する例を示します。

```
デバイス# show platform software trace filter-binary wireless
```

show platform software trace filter-binary

特定のモジュールの最新のトレース情報を表示するには、特権EXECモードまたはユーザEXECモードで **show platform software trace filter-binary** コマンドを使用します。

show platform software trace filter-binary*modules* ［**context** *mac-address*］

構文の説明

context*mac-address*	フィルタ処理に使用されるコンテキストを表します。また、モジュール名とトレース レベルに基づいてフィルタ処理できます。コンテキスト キーワードは、タグが付いているトレースに基づき MAC アドレスまたは他の引数を受け入れます。

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
	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、モジュールに関連するすべてのプロセス全体で /tmp/.../ に存在するすべてのログを照合してソートします。指定されたモジュールに関連するすべてのプロセスのトレース ログがコンソールに出力されます。このコマンドでは、同じコンテンツの collated_log_{system time} という名前のファイルも /crashinfo/tracelogs ディレクトリに生成されます。

例

次に、ワイヤレス モジュールのトレース情報を表示する例を示します。

```
Device# show platform software trace filter-binary wireless
```

show platform software trace level

特定のプロセスですべてのモジュールのトレース レベルを表示するには、特権 EXEC モードまたはユーザ EXEC モードで **show platform software trace level** コマンドを使用します。

show platform software trace level wireless ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明		
	process	トレース レベルが設定されているプロセス。次のオプションがあります。 • **chassis-manager**：Chassis Manager プロセス。 • **cli-agent**：CLI Agent プロセス。 • **cmm**：CMM プロセス。 • **dbm**：Database Manager プロセス。 • **emd**：Environmental Monitoring プロセス。 • **fed**：Forwarding Engine Driver プロセス。 • **forwarding-manager**：Forwarding Manager プロセス。 • **geo**：Geo Manager プロセス。 • **host-manager**：Host Manager プロセス。 • **interface-manager**：Interface Manager プロセス。 • **iomd**：Input/Output Module daemon（IOMd）プロセス。 • **ios**：IOS プロセス。 • **license-manager**：License Manager プロセス。 • **logger**：Logging Manager プロセス。 • **platform-mgr**：Platform Manager プロセス。 • **pluggable-services**：Pluggable Services プロセス。 • **replication-mgr**：Replication Manager プロセス。 • **shell-manager**：Shell Manager プロセス。 • **sif**：Stack Interface（SIF）Manager プロセス。 • **smd**：Session Manager プロセス。 • **stack-mgr**：Stack Manager プロセス。 • **table-manager**：Table Manager サーバ。 • **thread-test**：Multithread Manager プロセス。 • **virt-manager**：Virtualization Manager プロセス。 • **wireless**：ワイヤレス コントローラ モジュール プロセス。

slot	トレース レベルが設定されているプロセスを実行中のハードウェア スロット。次のオプションがあります。 • *number*：トレース レベルが設定されているハードウェア モジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。 • *SIP-slot / SPA-bay*：SIP スイッチ スロットの数とその SIP の共有ポート アダプタ（SPA）ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。 • **F0**：スロット 0 の Embedded Service Processor。 • **F1**：スロット 1 の Embedded Service Processor。 • **FP active**：アクティブな Embedded Service Processor。 • **R0**：スロット 0 のルート プロセッサ。 • **RP active**：アクティブなルート プロセッサ。 • **switch** <*number*> ：指定された番号を持つスイッチ。 • **switch active**：アクティブなスイッチ。 • **switch standby**：スタンバイスイッチ。 • *number*：トレース レベルが設定されているハードウェア モジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。 • *SIP-slot / SPA-bay*：SIP スイッチ スロットの数とその SIP の共有ポート アダプタ（SPA）ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。 • **F0**：スロット 0 の Embedded Service Processor。 • **FP active**：アクティブな Embedded Service Processor。 • **R0**：スロット 0 のルート プロセッサ。 • **RP active**：アクティブなルート プロセッサ。

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）。
active R0	ルートプロセッサ スロット 0 の AP フィルタのアクティブ インスタンス。

standby R0	ルートプロセッサ スロット 0 の AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、トレース レベルを表示する例を示します。

```
Device# show platform software trace level dbm switch active R0
Module Name                      Trace Level
-------------------------------------------------
binos                            Notice
binos/brand                      Notice
bipc                             Notice
btrace                           Notice
bump_ptr_alloc                   Notice
cdllib                           Notice
chasfs                           Notice
dbal                             Informational
dbm                              Debug
evlib                            Notice
evutil                           Notice
file_alloc                       Notice
green-be                         Notice
ios-avl                          Notice
klib                             Debug
services                         Notice
sw_wdog                          Notice
syshw                            Notice
tdl_cdlcore_message              Notice
tdl_dbal_root_message            Notice
tdl_dbal_root_type               Notice
```

show platform software trace message

プロセスのトレース メッセージを表示するには、特権 EXEC モードまたはユーザ EXEC モードで **set platform software trace** コマンドを使用します。

show platform software trace message *process slot*

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、Stack Manager プロセスおよび Forwarding Engine Driver プロセスのトレース メッセージを表示する例を示します。

```
Device# show platform software trace message stack-mgr switch active R0
10/30 09:42:48.767 [btrace] [8974]: (note): Successfully registered module [97] [uiutil]
10/30 09:42:48.762 [btrace] [8974]: (note): Successfully registered module [98]
[tdl_cdlcore_message]
10/29 13:28:19.023 [stack_mgr] [8974]: (note): Examining peer state
10/29 13:28:19.023 [stack_mgr] [8974]: (note): no switch eligible for standby election
presently
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Posting event
stack_fsm_event_wait_standby_elect_timer_expired, curstate stack_fsm_state_active_ready
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Timer HDL - STACK_WAIT_STANDBY_ELECT_TIMER
 expired
10/29 13:26:46.584 [btrace] [8974]: (note): Successfully registered module [99]
[tdl_ui_message]
10/29 13:26:46.582 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:36.582 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect
10/29 13:26:36.582 [evutil] [8974]: (ERR): Asynchronous connect failed for [uipeer uplink
 to slot 1] (fd == -1)
10/29 13:26:36.581 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:26.581 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect

Device# show platform software trace message fed switch active
11/02 10:55:01.832 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered
module [86] [uiutil]
11/02 10:55:01.848 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Single message size is
greater than 1024
11/02 10:55:01.822 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered
module [87] [tdl_cdlcore_message]
11/01 09:54:41.474 [btrace]: [12312]:  UUID: 0, ra: 0 (note): Successfully registered
module [88] [tdl_ngwc_gold_message]
11/01 09:54:11.228 [btrace]: [12312]:  UUID: 0, ra: 0 (note): Successfully registered
module [89] [tdl_doppler_iosd_matm_type]
11/01 09:53:37.454 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered
module [90] [tdl_ui_message]
11/01 09:53:37.382 [bipc]: [11310]:  UUID: 0, ra: 0 (note): Pending connection to server
 10.129.1.0
```

```
11/01 09:53:34.227 [xcvr]: [18846]:  UUID: 0, ra: 0 (ERR): FRU hardware authentication
Fail, result = 1.
11/01 09:53:33.775 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR): SMART COOKIE: SCC I2C
receive failed: rc=10
11/01 09:53:33.775 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR):
SMART COOKIE receive failed, try again
11/01 09:53:33.585 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR):
```

show platform software trace message license-manager chassis active R0

アクティブ ルート プロセッサのライセンスマネージャ プロセスのトレース メッセージを表示するには、特権 EXEC モードで **show platform software trace message license-manager chassis active R0** コマンドを使用します。

```
show platform software trace message license-managerchassis {chassis-number | active | standby}R0reverse
```

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、Forwarding Engine Driver プロセスのトレース メッセージを表示する例を示します。

```
Device# show platform software trace message license-manager chassis active R0
.......
2018/06/25 07:16:53.121 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 Decode of the file /tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy completed
in 35 msecs
/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy: DECODE(50:50:0:7)
2018/06/25 07:16:53.088 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 Decode of file [/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy] returned [0]
2018/06/25 06:53:20.421 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 Decode of the file /tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy completed
in 34 msecs
2018/06/25 06:53:20.389 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 Decode of file [/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy] returned [0]
2018/06/20 07:55:10.540 {lman_R0-0}{1}: [trccfg] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 Processing all-modules
2018/06/20 07:55:10.540 {lman_R0-0}{1}: [trccfg] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 Empty trace conf file
2018/06/20 07:54:46.453 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Constructing domain iosd_lmrp for RP/0/0 to RP/0/0
2018/06/20 07:54:46.453 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Received registration msg from [IOS]
2018/06/20 07:54:46.449 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Received a connection from client for path /tmp/rp/lipc/license_mgr_socket
2018/06/20 07:54:45.557 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:44.556 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:43.556 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:42.555 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
```

```
The ipc information for IOS is invalid
2018/06/20 07:54:41.554 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:40.553 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:39.553 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:38.552 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:37.551 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:36.550 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:35.550 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:34.549 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:33.548 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:32.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:31.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:30.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:30.537 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Pending connection to server 10.0.1.0
2018/06/20 07:54:29.546 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:28.545 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:27.545 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:26.544 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:25.543 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:24.542 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:23.542 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:22.541 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:21.540 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:20.633 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Peer attach: from location R0:0 is successful
2018/06/20 07:54:20.633 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Not setting domain for cmand
2018/06/20 07:54:20.625 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Received a connection from client for path /tmp/rp/lipc/lman_lic_serv_socket
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 epoch file read /tmp/tdlresolve/epoch_dir//2018_06_20_07_54_2413.epoch
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 Detect newly epoch file generated: new epoch:
/tmp/tdlresolve/epoch_dir//2018_06_20_07_54_2413.epoch
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 Flag tdlh stale epoch for all tdl handles
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Chasfs Watch on rp/0/0/rtu_licensing for platform to create RTU properties
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
The chassis product id: 'ISR4461/K9'
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
The chassis serial number: 'FDO2213A0GL'
```

```
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [bcrdu] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 CRDU
/tmp/sw/mount/isr4400v2-mono-universalk9.BLD_V169_THROTTLE_LATEST_20180618_044856_V16_9_0_163.SSA.pkg/usr/binos/bin/lman
 proc path is /tmp/patch/CRDU/BPROC_LM_RP/
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [bcrdu] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 CRDU
/tmp/sw/mount/isr4400v2-mono-universalk9.BLD_V169_THROTTLE_LATEST_20180618_044856_V16_9_0_163.SSA.pkg/usr/binos/bin/lman
 procstr is BPROC_LM_RP
2018/06/20 07:54:20.533 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
No licensing objects present in chasfs to delete
2018/06/20 07:54:20.533 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Deleting any existing licensing chasfs objects under [rp/0/0/licensing]
2018/06/20 07:54:20.532 {lman_R0-0}{1}: [syshw] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
syshw build device: could not add register 7 dev:
/sys/bus/platform/devices/cpld/reg_rp_sku_register (No such file or directory) due to
No such file or directory
2018/06/20 07:54:20.532 {lman_R0-0}{1}: [syshw] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
syshw build device: could not add register 5 dev:
/sys/bus/platform/devices/cpld/phys_slot_number (No such file or directory) due to No
such file or directory

Total messages : 49
```

show platform software trace message license-manager

ルータ プロセッサのライセンスマネージャ プロセスのトレース メッセージを表示するには、特権 EXEC モードで **show platform software trace message license-manager** コマンドを使用します。

show platform software trace message license-manager [**chassis** {*chassis-number* | **active** | **standby** } **R0**]

構文の説明

active R0	ルートプロセッサ スロット 0 のアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 のスタンバイ インスタンス。

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 Gibraltar 16.12.2s	このコマンドが導入されました。

例

次に、Forwarding Engine Driver プロセスのトレース メッセージを表示する例を示します。

```
Device# show platform software trace message license-manager chassis active R0
.......
2018/06/25 06:53:20.421 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 Decode of the file /tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy completed
in 34 msecs
/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy: DECODE(48:48:0:7)
2018/06/25 06:53:20.389 {lman_R0-0}{1}: [btrace] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 Decode of file [/tmp/rp/trace/lman_R0-0.21231_0.20180620075420.bin.copy] returned [0]
2018/06/20 07:55:10.540 {lman_R0-0}{1}: [trccfg] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 Processing all-modules
2018/06/20 07:55:10.540 {lman_R0-0}{1}: [trccfg] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 Empty trace conf file
2018/06/20 07:54:46.453 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Constructing domain iosd_lmrp for RP/0/0 to RP/0/0
2018/06/20 07:54:46.453 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Received registration msg from [IOS]
2018/06/20 07:54:46.449 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Received a connection from client for path /tmp/rp/lipc/license_mgr_socket
2018/06/20 07:54:45.557 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:44.556 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:43.556 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:42.555 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:41.554 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:40.553 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
```

```
The ipc information for IOS is invalid
2018/06/20 07:54:39.553 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:38.552 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:37.551 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:36.550 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:35.550 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:34.549 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:33.548 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:32.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:31.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:30.547 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:30.537 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Pending connection to server 10.0.1.0
2018/06/20 07:54:29.546 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:28.545 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:27.545 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:26.544 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:25.543 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:24.542 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:23.542 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:22.541 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:21.540 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
The ipc information for IOS is invalid
2018/06/20 07:54:20.633 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Peer attach: from location R0:0 is successful
2018/06/20 07:54:20.633 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Not setting domain for cmand
2018/06/20 07:54:20.625 {lman_R0-0}{1}: [bipc] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Received a connection from client for path /tmp/rp/lipc/lman_lic_serv_socket
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 epoch file read /tmp/tdlresolve/epoch_dir//2018_06_20_07_54_2413.epoch
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 Detect newly epoch file generated: new epoch:
/tmp/tdlresolve/epoch_dir//2018_06_20_07_54_2413.epoch
2018/06/20 07:54:20.624 {lman_R0-0}{1}: [tdllib] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 Flag tdlh stale epoch for all tdl handles
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Chasfs Watch on rp/0/0/rtu_licensing for platform to create RTU properties
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
The chassis product id: 'ISR4461/K9'
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
The chassis serial number: 'FDO2213A0GL'
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [bcrdu] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 CRDU
/tmp/sw/mount/isr4400v2-mono-universalk9.BLD_V169_THROTTLE_LATEST_20180618_044856_V16_9_0_163.SSA.pkg/usr/binos/bin/lman
 proc path is /tmp/patch/CRDU/BPROC_LM_RP/
```

```
2018/06/20 07:54:20.536 {lman_R0-0}{1}: [bcrdu] [21231]: UUID: 0, ra: 0, TID: 0 (note):
 CRDU
/tmp/sw/mount/isr4400v2-mono-universalk9.BLD_V169_THROTTLE_LATEST_20180618_044856_V16_9_0_163.SSA.pkg/usr/binos/bin/lman
 procstr is BPROC_LM_RP
2018/06/20 07:54:20.533 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
No licensing objects present in chasfs to delete
2018/06/20 07:54:20.533 {lman_R0-0}{1}: [lman] [21231]: UUID: 0, ra: 0, TID: 0 (note):
Deleting any existing licensing chasfs objects under [rp/0/0/licensing]
2018/06/20 07:54:20.532 {lman_R0-0}{1}: [syshw] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
syshw build device: could not add register 7 dev:
/sys/bus/platform/devices/cpld/reg_rp_sku_register (No such file or directory) due to
No such file or directory
2018/06/20 07:54:20.532 {lman_R0-0}{1}: [syshw] [21231]: UUID: 0, ra: 0, TID: 0 (ERR):
syshw build device: could not add register 5 dev:
/sys/bus/platform/devices/cpld/phys_slot_number (No such file or directory) due to No
such file or directory
```

show platform software utd chassis active F0 et-analytics global

ETA グローバルおよびインターフェイスの詳細を表示するには、 **show platform software utd chassis active F0 et-analytics global** コマンドを使用します。

show platform software utd chassis active F0 et-analytics global

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、ETA グローバルおよびインターフェイスの詳細を表示する例を示します。

```
デバイス# show platform software utd chassis active F0 et-analytics global
ET Analytics Global Configuration
ID: 1
All Interfaces: Off
IP address and port and vrf: 192.168.5.2:2055:0
```

show platform software et-analytics global

ETA グローバル設定を表示するには、**show platform software et-analytics global** コマンドを使用します。

（注） **show platform software et-analytics global** コマンドでは、ETA が有効になっているワイヤレス クライアント インターフェイスは表示されません。

show platform software et-analytics global

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、ETA グローバルおよびインターフェイスの詳細を表示する例を示します。

```
デバイス# show platform software et-analytics global
ET-Analytics Global state
=========================
All Interfaces : Off
IP Flow-record Destination: 192.168.5.2 : 2055
Inactive timer: 15
```

show platform sudi certificate

特定の SUDI のチェックサムレコードを表示するには、**show platform sudi certificate** コマンドを使用します。

show platform sudi certificate [sign [nonce *nonce* **]]**

構文の説明

sign	（任意）。署名を表示します。
nonce	（任意）。ナンス値を入力します。

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 Bengaluru 17.4.1	このコマンドが導入されました。

次に、特定の SUDI のチェックサムレコードを表示する例を示します。

```
Device# show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUl4F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1aO6g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQMqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
```

```
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcCl0lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KND15618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIEAwQD7zANBgkqhkiG9w0BAQsFADAnMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMB4XDTE4MDkyMzIyMzIwNloXDTI5
MDUxNDIwMjU0MVowaTEnMCUGA1UEBRMeUElEOkM5NjAwLVNVUC0xIFNOOkNBVDIy
MzZMMFE5MQ4wDAYDVQQKEwVDaXNjbzEYMBYGA1UECxMPQUNULTIgTGl0ZSBTVURJ
MRQwEgYDVQQDEwtDOTYwMC1TVVAtMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBANsh0jcvgh1pdOjP9KnffDnDc/zEHDzbCTWPJi2FZcsaSE5jvq6CUqc4
MYpNAZU2Jym7NSD8iQbMXwbnCtoL64QtxQeFhRYmc4d5o933M7GwpEH0I7HUSbO/
Fxyp7JBmGPPgAkY7rKsYENiNK2hiR7Q2O7X2BidOKknEuofWdJMNyMaZgLYLOHbJ
5oXaORxhUy3VRaxNl6qI7kYxuugg2LcAbZ539sRXe8JtHyK8llURNSGMiQ0S17pS
idGmrJJ0pEHA0EUVTZqEny3z+NW9uxLVSzu6+hEJYlqfI+YEf0DbVZly1cy5r/jF
yNdGuGKvd5agvgCly8aYMZa3P+D5S8sCAwEAAaNvMG0wDgYDVR0PAQH/BAQDAgXg
MAwGA1UdEwEB/wQCMAAwTQYDVR0RBEYwRKBCBgkrBgEEAQkVAgOgNRMzQ2hpcElE
PVUxUk5TVEl3TVRjd05qSTFBQUFwZndBQUFBQUFBQUFBQUFBQUFBQUhtSlU9MA0G
CSqGSIb3DQEBCwUAA4IBAQCrpHo/CUyk5Hs/asIcYW0ep8KocSkbNh8qamyd4oWD
e/MGJW9Bs5f09IEbILWPdytCCS2lSyJbxz2HvVDzdxQdxjDwUNiWuu3dWMXN/i67
yuCGM+lA1AAG5dT6lNgWYHh+YzsZm9eoq1+4NM+JuMXWsnzAK8rSy+dSpBxqFsBq
E0OlPsaK7y2h8gs+XrV9x+D48OZQkTRXpxhJfiWvs+EbdgsAM/vBxTAoTJPVmXWN
Cmcj9X52Xl3i4MdOUXocZLO2kh6JSgOYGkFeZifJ0iDvMfAf0cJ6+cEF6bSxAqBL
veel+8LmeiE/2O9h6qGHPPDacCaXA2oJCDHveAt8iPTG
-----END CERTIFICATE-----

Signature version: 1
Signature:
[redacted]
```

show platform sudi pki

ハードウェアユニットが正しくプログラムされているかどうかを検証するには、**show platform sudi pki** コマンドを使用します。

show platform sudi pki

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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、ハードウェアユニットが正しくプログラムされているかどうかを確認する例を示します。

```
Device# show platform sudi pki

CMCA3 cert status : Enabled / Disabled

SUDI Issuer                          Validity status
------------------------------------------------------------------------
Cisco Manufacturing CA III           Valid / Not-valid
Cisco Manufacturing CA SHA2          Valid / Not-valid
Cisco Manufacturing CA               Valid / Not-valid
```

show parameter-map type umbrella global

Umbrella グローバル パラメータ マップの詳細を表示するには、**show parameter-map type umbrella global** コマンドを使用します。

show parameter-map type umbrella global

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、Umbrella グローバル パラメータ マップの詳細を表示する例を示します。

```
デバイス# show parameter-map type umbrella global
parameter-map type umbrella global
   token   57CC80106C087FB1B2A7BAB4F2F4373C00247166
   local-domain dns_wl
   dnscrypt
   udp-timeout 2
   resolver ipv4 208.67.220.220
   resolver ipv4 208.67.222.222
   resolver ipv6 2620:119:53::53
   resolver ipv6 2620:119:35::35
```

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 interface {**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。
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 Gibraltar 16.10.1	このコマ

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。

- 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。

```
デバイス# 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
```

show processes cpu

IOS タスクの詳細な CPU 使用率の統計を表示するには、**show processes cpu** コマンドを使用します。

show processes cpu ［**autoprofile** | **extended** | **history** ［**table**］| **sorted** ［**1min** | **5min** | **5sec**］］

構文の説明

autoprofile	（任意）IOS（d）の「自動 CPUHOG プロファイリング」情報を表示します。
extended	（任意）IOS（d）プロセスの最後の 5 秒間の拡張 CPU 使用率レポートを表示します。
history	（任意）グラフ形式で CPU 履歴を表示します。
table	（任意）表形式で CPU 履歴を表示します。
sorted	（任意）Cisco IOS イメージの場合のみ。パーセンテージでソートされた CPU 使用率を表示します。
history	（任意）CPU 使用率の履歴をソートします。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。
1min	（任意）1 分間の使用率に基づいて CPU 使用率をソートします。
5min	（任意）5 分間の使用率に基づいて CPU 使用率をソートします。
5sec	（任意）5 秒間の使用率に基づいて CPU 使用率をソートします。

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 Amsterdam 17.3.1	このコマンドが Cisco IOS XE Amsterdam 17.3.1 に統合されました。

使用上のガイドライン

history キーワードを使用すると、Cisco IOS イメージに対して次の 3 つのグラフが表示されます。

- 過去 60 秒間の CPU 使用率
- 過去 60 分間の CPU 使用率
- 過去 72 時間の CPU 使用率

最大使用率は毎秒測定され、記録されます。平均使用量は1秒より長い期間で計算されます。長期間にわたって CPU 使用率が一貫して高い場合は、問題があることを示しています。

スタンバイコンソールを有効にするには、次の設定が行われていることを確認します。

```
redundancy
main-cpu
secondary console enable
```

例

次に、キーワードを指定しない **show processes cpu** コマンドの出力例を示します。

```
Device# show processes cpu

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
  10     1576556      281188       5606  0.15%  0.05%  0.05%   0 Check heaps
 232      845057    54261160         15  0.07%  0.05%  0.06%   0 IPAM Manager
 595         177         300        590  0.07%  0.02%  0.01%   2 Virtual Exec
 138     1685973   108085955         15  0.07%  0.08%  0.08%   0 L2 LISP Punt Pro
 193       19644      348767         56  0.07%  0.00%  0.00%   0 DTP Protocol
   5           0           1          0  0.00%  0.00%  0.00%   0 CTS SGACL db cor
   4          24          15       1600  0.00%  0.00%  0.00%   0 RF Slave Main Th
   6           0           1          0  0.00%  0.00%  0.00%   0 Retransmission o
   7           0           1          0  0.00%  0.00%  0.00%   0 IPC ISSU Dispatc
   2      117631      348801        337  0.00%  0.00%  0.00%   0 Load Meter
   8           0           1          0  0.00%  0.00%  0.00%   0 EDDRI_MAIN
.
.
.
```

show rate-limit client

AP でのクライアントのレート制限を設定するには、**show rate-limit client** コマンドを使用します。

show rate-limit client

構文の説明

このコマンドには、引数はありません。

コマンド モード

Privileged EXEC (#)

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

次に、AP でのクライアントのレート制限を設定する例を示します。

```
Device# show rate-limit client
Config:
mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in
nrt_burst_out nrt_burst_in
00:1C:F1:09:85:E7 0 8001 8002 8003 8004 8005 8006 8007 8008
Statistics:
name up down
Unshaped 0 0
Client RT pass 0 0
Client NRT pass 0 0
Client RT drops 0 0
Client NRT drops 0 0
Per client rate limit:
mac vap rate_out rate_in policy
```

show remote-lan all

すべての RLAN の詳細な出力を表示するには、**show remote-lan all** コマンドを使用します。

show remote-lan all

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、すべての RLAN の詳細な出力を表示する例を示します。

```
デバイス# show remote-lan all
Remote-LAN Profile Name      : rlan_test_1
================================================
Identifier                          : 1
Status                              : Enabled
Mac-filtering                       : Not Configured
Number of Active Clients            : 1
Security_8021X                      : Disabled
8021.x Authentication list name     : Not Configured
Local Auth eap Profile Name         : Not Configured
Web Auth Security                   : Disabled
Webauth Authentication list name    : Not Configured
Web Auth Parameter Map              : Not Configured
Client association limit            : 0
Ipv4 Web Pre Auth Acl               : Not Configured
Ipv6 Web Pre Auth Acl               : Not Configured

Remote-LAN Profile Name      : rlan_test_2
================================================
Identifier                          : 2
Status                              : Enabled
Mac-filtering                       : Not Configured
Number of Active Clients            : 1
Security_8021X                      : Disabled
8021.x Authentication list name     : Not Configured
Local Auth eap Profile Name         : Not Configured
Web Auth Security                   : Disabled
Webauth Authentication list name    : Not Configured
Web Auth Parameter Map              : Not Configured
Client association limit            : 0
Ipv4 Web Pre Auth Acl               : Not Configured
Ipv6 Web Pre Auth Acl               : Not Configured
```

show remote-lan id

ID 別に RLAN 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*

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、ID 別に RLAN 設定を表示する例を示します。

```
デバイス# show remote-lan id <id>
Remote-LAN Profile Name      : rlan_test_1
================================================
Identifier                                    : 1
Status                                        : Enabled
Mac-filtering                                 : Not Configured
Number of Active Clients                   : 1
Security_8021X                                : Disabled
8021.x Authentication list name         : Not Configured
Local Auth eap Profile Name             : Not Configured
Web Auth Security                              : Disabled
Webauth Authentication list name      : Not Configured
Web Auth Parameter Map                   : Not Configured
Client association limit                       : 0
Ipv4 Web Pre Auth Acl                       : Not Configured
Ipv6 Web Pre Auth Acl                        : Not Configured
```

show remote-lan name

プロファイル名別に RLAN 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 *profile-name*

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 Gibraltar 16.10.1	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 RLAN 設定を表示する例を示します。

```
デバイス# show remote-lan name <profile-name>
Remote-LAN Profile Name      : rlan_test_1
================================================
Identifier                          : 1
Status                              : Enabled
Mac-filtering                       : Not Configured
Number of Active Clients            : 1
Security_8021X                      : Disabled
8021.x Authentication list name     : Not Configured
Local Auth eap Profile Name         : Not Configured
Web Auth Security                   : Disabled
Webauth Authentication list name    : Not Configured
Web Auth Parameter Map              : Not Configured
Client association limit            : 0
Ipv4 Web Pre Auth Acl               : Not Configured
Ipv6 Web Pre Auth Acl               : Not Configured
```

show remote-lan policy detail

プロファイル名別に RLAN ポリシー プロファイルの詳細を表示するには、**show remote-lan policy detail** コマンドを使用します。

show remote-lan policy detail *rlan_profile_name*

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 Gibraltar 16.10.1	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RLANポリシープロファイルの詳細を表示する例を示します。

```
デバイス# show remote-lan policy detail <rlan_profile_name>
Profile Name                    : rlan_named_pp1
Status                                : Enabled
Description                           :
REMOTE-LAN ACL
  IPv4 ACL name                       : Not Configured
  IPv6 ACL name                 : Not Configured
AAA Policy Params
  AAA Override                  : Disabled
  AAA Policy name               : default-aaa-policy
RLAN Switching policy
  Central Switching             : Enabled
  Central Dhcp                  : Enabled
VLAN                            : 20
Pre Authentication              : Disabled
Session Time out                : 1800
Violation Mode                  : REPLACE
Host Mode                       : SINGLE_HOST_MODE
Host mode VLANs
  Voice Vlan Id                 : Not Configured
  Data Vlan Id                  : Not Configured
Exclusionlist Params
  Exclusionlist                 : Enabled
  Exclusion Timeout             : 60
Flow Monitor IPv4
  Flow Monitor Ingress Name     : Not Configured
  Flow Monitor Egress Name      : Not Configured
  Flow Moniter Ingress status   : Disabled
  Flow Moniter egress status    : Disabled
Flow Monitor IPv6
  Flow Monitor Ingress Name     : Not Configured
  Flow Monitor Egress Name      : Not Configured
  Flow Moniter Ingress status   : Disabled
  Flow Moniter egress status    : Disabled
Split Tunnel Parameters
  Status                        : Disabled
  ACL name                      : Not Configured
  Override Status               : Disabled
```

```
  Gateway Address              : Not Configured
  Netmask Address              : Not Configured
DHCP
  DHCP Required                : Disabled
  DHCP Server                  : Not Configured
Accounting List                : Not Configured
```

show remote-lan policy summary

すべてのRLANのポリシープロファイルの概要を表示するには、**show remote-lan policy summary** コマンドを使用します。

show remote-lan policy summary

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、すべての RLAN のポリシー プロファイルの概要を表示する例を示します。

```
デバイス# show remote-lan policy summary
Number of Policy Profiles: 1

Profile Name                    Description                              Status

-------------------------------------------------------------------------------------------
rlan_named_pp1                Testing RLAN policy profile              Enabled
```

show remote-lan summary

すべての RLAN の概要を表示するには、**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、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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、すべての RLAN の概要を表示する例を示します。

```
デバイス# show remote-lan summary
Number of RLANs: 1

RLAN    Profile Name                     Status
-----------------------------------------------------------------
1       rlan_test_1                      Enabled
```

show sdavc ap download status

Software-Defined Application Visibility and Control（SD-AVC）のアクセスポイントごと（AP ごと）のダウンロードステータスを表示するには、**show sdavc ap download status** コマンドを使用します。

show sdavc ap download status

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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、SD-AVC の AP ごとのダウンロードステータスを表示する例を示します。

```
Device# show sdavc ap download status

AP  MAC         Latest filename    Status
------------------------------------------------------------
00d7.8f58.2f80      xyz            SUCCESS
00d7.8f58.2d82      abc            FAILED
```

show sdavc status ap

アクセスポイント（AP）の Software-Defined Application Visibility and Control（SD-AVC）ステータスを表示するには、**show sdavc status ap** コマンドを使用します。

show sdavc status ap *ap-name*

構文の説明

ap-name	AP名またはMACアドレス。

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 Cupertino 17.7.1	このコマンドが導入されました。

例

次に、AP の SD-AVC ステータスを表示する例を示します。

```
Device# show sdavc status ap 00d7.8f58.2f80

AP MAC                Status
-------------------------------------
00d7.8f58.2f80        ENABLED
```

show ssh

SSH 接続ステータスを表示するには、 **show ssh** コマンドを使用します。

show ssh {*connection-number* | {**vty** *connection-number* }}

構文の説明

connection-number	SSH接続番号。有効な範囲は0～530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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、SSH 接続ステータスを表示する例を示します。

```
Device# show ssh connection-number
```

show split-tunnel client access-list

ワイヤレスクライアントごとにスプリット トンネリング ドメイン ネーム システム（DNS）アクセス制御リスト（ACL）を確認するには、**show split-tunnel client access-list** コマンドを使用します。

show split-tunnel client *mac-address* **access-list**

構文の説明

mac-address	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

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 Cupertino 17.1.1	このコマンドが導入されました。

例

次に、ワイヤレスクライアントのスプリットトンネリング DNS ACL を確認する例を示します。

```
Device# show split-tunnel client 00:11:22:33:44:55 access-list

Split tunnel ACLs for Client: 00:11:22:33:44:55

IP ACL: SplitTunnelACL

Tunnel packets Tunnel bytes NAT packets NAT bytes
             1          242           3       768

URL ACL: SplitTunnelACL

Tunnel packets Tunnel bytes NAT packets NAT bytes
             3          778           0         0

Resolved IPs for Client: 00:11:22:33:44:55 for Split tunnel

HIT-COUNT       URL             ACTION  IP-LIST

1               base1.com       deny.   209.165.200.224
                                        209.165.200.225

2               base2.com       deny.   209.165.200.226

3               base3.com       deny.   209.165.200.227
```

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 Gibraltar 16.10.1	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。

```
デバイス# 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 tech-support wireless ap

Cisco Technical Assistance Center（TAC）によって頻繁に要求されるシスコ AP の変数に関する特定の情報を表示するには、特権 EXEC モードで **show tech-support wireless ap** コマンドを使用します。

show tech-support wireless ap

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

show tech-support wireless ap コマンドの一部として、次のコマンドの出力が表示されます。

- show ap session termination statistics
- show ap status
- show ap tag summary
- show platform software bssid chassis active F0 statistics
- show platform software bssid chassis active R0 statistics
- show platform software capwap chassis active F0 statistics
- show platform software capwap chassis active R0 statistics
- show platform software dtls chassis active F0 statistics
- show platform software dtls chassis active R0 statistics
- show platform software radio chassis active F0 statistics
- show platform software radio chassis active R0 statistics

例

次に、**show tech-support wireless ap** コマンドの出力例を示します

```
Device# show tech-support wireless ap

------------------- show platform software dtls chassis active R0 statistics
-------------------
```

```
DTLS Counters     (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0

Switch 1:
OM Create               0/0
OM Delete               0/0
Ack Nack Notify         0/0


------------------ show platform software radio chassis active R0 statistics
------------------



Switch 1:
NACK Notify             0/0
  Create Failure        0
  Delete Failure        0


------------------ show platform software bssid chassis active R0 statistics
------------------



Switch 1:
NACK Notify             0/0
  Create Failure        0
  Delete Failure        0


------------------ show platform software capwap chassis active R0 statistics
------------------


Capwap Counters   (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
Modify                  0/0

Switch 1:
OM Create               0/0
OM Delete               0/0
ACK-NACK Notify         0/0
  Tunnel State          0/0
  Tunnel Create         0/0
  Tunnel Modify         0/0
  Tunnel Delete         0/0


------------------ show platform software dtls chassis active F0 statistics
------------------


DTLS Counters     (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
HW Create               0/0
HW Modify               0/0
HW Delete               0/0
```

```
Create Ack              0/0
Modify Ack              0/0
Delete Ack              0/0
Ack Ack Notify          0/0
Ack Nack Notify         0/0
Nack Notify             0/0
HA Seq GET              665/0
HA Seq SET              0/0
HA Seq Crypto GET       0/0
HA Seq Crypto SET       0/0
HA Seq Crypto Callback  0/0

HA Seq last Responsed   0
HA Seq Pending          0
HA Seq Outstanding cb   0


------------------ show platform software radio chassis active F0 statistics
------------------


Radio Counters    (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
HW Create               0/0
HW Modify               0/0
HW Delete               0/0
Create Ack              0/0
Modify Ack              0/0
Delete Ack              0/0
Nack Notify             0/0


------------------ show platform software bssid chassis active F0 statistics
------------------


Bssid Counters    (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
HW Create               0/0
HW Modify               0/0
HW Delete               0/0
Create Ack              0/0
Modify Ack              0/0
Delete Ack              0/0
Nack Notify             0/0


------------------ show platform software capwap chassis active F0 statistics
------------------


Capwap Counters   (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
HW Create               0/0
HW Modify               0/0
HW Delete               0/0
Create Ack              0/0
Modify Ack              0/0
```

```
Delete Ack              0/0
Ack Ack Notify          0/0
Ack Nack Notify         0/0
Nack Notify             0/0


------------------ show ap auto-rf dot11 24ghz ------------------


------------------ show ap auto-rf dot11 5ghz ------------------


------------------ show ap capwap retransmit ------------------


------------------ show ap config dot11 dual-band summary ------------------


------------------ show ap config general ------------------



------------------ show ap dot11 24ghz channel ------------------


Leader Automatic Channel Assignment
  Channel Assignment Mode                     : AUTO
  Channel Update Interval                     : 600 seconds
  Anchor time (Hour of the day)               : 0
  Channel Update Contribution
    Noise                                     : Enable
    Interference                              : Enable
    Load                                      : Disable
    Device Aware                              : Disable
  CleanAir Event-driven RRM option            : Disabled
  Channel Assignment Leader                   : ewlc-doc (9.12.32.10)
  Last Run                                    : 25 seconds ago

  DCA Sensitivity Level                       : MEDIUM : 10 dB
  DCA Minimum Energy Limit                    : -95 dBm
  Channel Energy Levels
    Minimum                                   : unknown
    Average                                   : unknown
    Maximum                                   : -128 dBm
  Channel Dwell Times
    Minimum                                   : unknown
    Average                                   : unknown


------------------ show ap dot11 24ghz group ------------------


Radio RF Grouping

  802.11b Group Mode               : AUTO
  802.11b Group Update Interval    : 600 seconds
  802.11b Group Leader             : ewlc-doc (9.12.32.10)
  802.11b Last Run                 : 26 seconds ago
```

```
RF Group Members

Controller name                   Controller IP
-------------------------------------------------
ewlc-doc                          9.12.32.10



------------------ show ap dot11 24ghz load-info ------------------


------------------ show ap dot11 24ghz monitor ------------------


Default 802.11b AP monitoring
  802.11b Monitor Mode                 : Enabled
  802.11b Monitor Channels             : Country channels
  802.11b RRM Neighbor Discover Type   : Transparent
  802.11b AP Coverage Interval         : 180 seconds
  802.11b AP Load Interval             : 60 seconds
  802.11b AP Noise Interval            : 180 seconds
  802.11b AP Signal Strength Interval  : 60 seconds
  802.11b NDP RSSI Normalization       : Enabled


------------------ show ap dot11 24ghz network ------------------



802.11b Network                           : Enabled
11gSupport                                : Enabled
11nSupport                                : Enabled
802.11b/g Operational Rates
  802.11b 1M                              : Mandatory
  802.11b 2M                              : Mandatory
  802.11b 5.5M                            : Mandatory
  802.11b 11M                             : Mandatory
  802.11g 6M                              : Supported
  802.11g 9M                              : Supported
  802.11g 12M                             : Supported
  802.11g 18M                             : Supported
  802.11g 24M                             : Supported
  802.11g 36M                             : Supported
  802.11g 48M                             : Supported
  802.11g 54M                             : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported


------------------ show ap dot11 24ghz profile ------------------



Default 802.11b AP performance profiles
  802.11b Global Interference threshold    : 10 %
  802.11b Global noise threshold           : -70 dBm
  802.11b Global RF utilization threshold  : 80 %
  802.11b Global throughput threshold      : 1000000 bps
```

```
  802.11b Global clients threshold         : 12 clients


------------------ show ap dot11 24ghz summary ------------------


------------------ show ap dot11 24ghz 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
Update Contribution
    Noise                               : Enable
    Interference                        : Enable
    Load                                : Disable
    Device Aware                        : Disable
Transmit Power Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                                : 27 seconds ago


------------------ show ap dot11 5ghz channel ------------------


Leader Automatic Channel Assignment
  Channel Assignment Mode                     : AUTO
  Channel Update Interval                     : 600 seconds
  Anchor time (Hour of the day)               : 0
  Channel Update Contribution
    Noise                                     : Enable
    Interference                              : Enable
    Load                                      : Disable
    Device Aware                              : Disable
  CleanAir Event-driven RRM option            : Disabled
  Channel Assignment Leader                   : ewlc-doc (9.12.32.10)
  Last Run                                    : 27 seconds ago

  DCA Sensitivity Level                       : MEDIUM : 15 dB
  DCA 802.11n/ac Channel Width                : 20 MHz
  DCA Minimum Energy Limit                    : -95 dBm
  Channel Energy Levels
    Minimum                                   : unknown
    Average                                   : unknown
    Maximum                                   : -128 dBm
  Channel Dwell Times
    Minimum                                   : unknown


------------------ show ap dot11 5ghz group ------------------


Radio RF Grouping

  802.11a Group Mode               : AUTO
  802.11a Group Update Interval    : 600 seconds
  802.11a Group Leader             : ewlc-doc (9.12.32.10)
  802.11a Last Run                 : 28 seconds ago
```

```
RF Group Members

Controller name                   Controller IP
-------------------------------------------------
ewlc-doc                          9.12.32.10



------------------ show ap dot11 5ghz load-info ------------------


------------------ show ap dot11 5ghz monitor ------------------


Default 802.11a AP monitoring
  802.11a Monitor Mode                 : Enabled
  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
  802.11a NDP RSSI Normalization       : Enabled


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


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

------------------ show ap dot11 5ghz summary ------------------


------------------ 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
Update Contribution
    Noise                               : Enable
    Interference                        : Enable
    Load                                : Disable
    Device Aware                        : Disable
Transmit Power Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                                : 28 seconds ago


------------------ show ap image ------------------



------------------ show wireless stats ap join summary ------------------

Number of APs: 0

Base MAC        Ethernet MAC    AP Name                           IP Address       Status
      Last Failure Type     Last Disconnect Reason
-----------------------------------------------------------------------------------------


------------------ show ap rf-profile summary ------------------


Number of RF-profiles: 6

RF Profile Name                  Band     Description                              State
------------------------------------------------------------------------------------------
Low_Client_Density_rf_5gh        5 GHz    pre configured Low Client Density rf Up
High_Client_Density_rf_5gh       5 GHz    pre configured High Client Density r Up
Low_Client_Density_rf_24gh       2.4 GHz  pre configured Low Client Density rf Up
High_Client_Density_rf_24gh      2.4 GHz  pre configured High Client Density r Up
Typical_Client_Density_rf_5gh    5 GHz    pre configured Typical Density rfpro Up
Typical_Client_Density_rf_24gh   2.4 GHz  pre configured Typical Client Densit Up


------------------ show ap slots ------------------


------------------ show ap summary ------------------
```

```
Number of APs: 0


------------------ show ap uptime ------------------

Number of APs: 0


------------------ show ap tag summary ------------------

Number of APs: 0


------------------ show ap status ------------------


------------------ show ap cdp neighbors ------------------

Number of neighbors: 0


------------------ show ap ap-join-profile summary ------------------


Number of AP Profiles: 1
AP Profile Name                  Description
------------------------------------------------------------------------
default-ap-profile               default ap profile

------------------ show ap link-encryption ------------------


------------------ show wireless stats ap session termination ------------------


------------------ show wireless loadbalance ap affinity wncd 0 ------------------


------------------ show wireless loadbalance ap affinity wncd 1 ------------------


------------------ show wireless loadbalance ap affinity wncd 2 ------------------


------------------ show wireless loadbalance ap affinity wncd 3 ------------------


------------------ show wireless loadbalance ap affinity wncd 4 ------------------
```

```
------------------ show wireless loadbalance ap affinity wncd 5 ------------------

------------------ show wireless loadbalance ap affinity wncd 6 ------------------

------------------ show wireless loadbalance ap affinity wncd 7 ------------------
```

show tech-support wireless client

すべてのクライアントまたは特定のクライアントに関連するデータを印刷するには、特権EXECモードで **show tech-support wireless client** コマンドを使用します。

show tech-support wireless client

構文の説明

mac-address	クライアント MAC アドレス

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

show tech-support wireless client コマンドの一部として、次のコマンドの出力が表示されます。

- show platform software wireless-client chassis active F0 statistics
- show platform software wireless-client chassis active R0 statistics
- show wireless client calls active
- show wireless client calls rejected
- show wireless client client-statistics summary
- show wireless client device summary
- show wireless client mac <mac-addr> details
- show wireless client probing
- show wireless client sleeping-client
- show wireless client statistic
- show wireless client steering
- show wireless client summary
- show wireless exclusionlist
- show wireless pmk-cache

（注） **show tech-support wireless client** コマンドを実行しても、**show wireless client summary detail** コマンドの出力は表示されません。

例

次に、**show tech-support wireless client** コマンドの出力例を示します

```
Device# show tech-support wireless client

------------------ show wireless stats client summary ------------------

Number of Local Clients : 0


MAC Address    AP Name                          WLAN UpTime(secs) Rx Pkts Tx Pkts RSSI
SNR  Data Retries
-----------------------------------------------------------------------------------------




------------------ show wireless client summary ------------------

Number of Local Clients: 0


Number of Excluded Clients: 0



------------------ show wireless client device summary ------------------



------------------ show wireless client steering ------------------


Client Steering Configuration Information
  Macro to micro transition threshold                  : -55 dBm
  Micro to Macro transition threshold                  : -65 dBm
  Micro-Macro transition minimum client count          : 3
  Micro-Macro transition client balancing window       : 3
  Probe suppression mode                               : Disabled
  Probe suppression validity window                    : 100 s
  Probe suppression aggregate window                   : 200 ms
  Probe suppression transition aggressiveness          : 3
  Probe suppression hysteresis                         : -6 dBm

WLAN Configuration Information



------------------ show wireless client calls active ------------------



------------------ show wireless client calls rejected ------------------



------------------ show wireless client sleeping-client ------------------

Total number of sleeping-client entries: 0
```

```
------------------ show wireless client probing ------------------


------------------ show wireless client ap dot11 24ghz ------------------




------------------ show wireless client ap dot11 5ghz ------------------




------------------ show wireless pmk-cache ------------------

Number of PMK caches in total : 0

Type      Station             Entry Lifetime  VLAN Override         IP Override
 Audit-Session-Id
-----------------------------------------------------------------------------------------------


------------------ show wireless exclusionlist ------------------


------------------ show wireless country  configured ------------------


Configured Country.........................   US - United States

Configured Country Codes
        US  - United States                 802.11a Indoor/ 802.11b Indoor/ 802.11g
Indoor


------------------ show wireless tag rf summary ------------------


Number of RF Tags: 1

RF tag name                     Description
------------------------------------------------------------------------
default-rf-tag                  default RF tag


------------------ show platform software wireless-client chassis active R0 statistics
------------------


Client Counters   (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
Modify                  0/0

Switch 1:
OM Create               0/0
```

```
OM Delete               0/0
NACK Notify             0/0
  Create Failure        0
  Modify Failure        0
  Delete Failure        0


------------------ show platform software wireless-client chassis active F0 statistics
------------------


Client Counters   (Success/Failure)
-----------------------------------
Create                  0/0
Delete                  0/0
HW Create               0/0
HW Modify               0/0
HW Delete               0/0
Create Ack              0/0
Modify Ack              0/0
Delete Ack              0/0
NACK Notify             0/0


------------------ show platform hardware chassis active qfp feature wireless wlclient
cpp-client summary ------------------


------------------ show platform hardware chassis active qfp feature wireless wlclient
datapath summary ------------------

Vlan   pal_if_hdl   mac            Input Uidb Output Uidb
------ ------------ -------------- ---------- -----------
```

show tech-support wireless datapath

CPP データパスに関連するデータを印刷するには、特権 EXEC モードで **show tech-support wireless datapath** コマンドを使用します。

show tech-support wireless datapath

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 Gibraltar 16.10.1	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、Cisco vEWLC、Cisco 9540 WLC、Cisco 9880 WLC などの CPP データパス アーキテクチャを備えたプラットフォームでのみ使用できます。

show tech-support wireless datapath コマンドの一部として、次のコマンドの出力が表示されます。

- show platform hardware chassis active qfp feature wireless bssid summary
- show platform hardware chassis active qfp feature wireless capwap cpp-client statistics
- show platform hardware chassis active qfp feature wireless capwap cpp-client summary
- show platform hardware chassis active qfp feature wireless capwap datapath statistics drop
- show platform hardware chassis active qfp feature wireless capwap datapath statistics fragmentation
- show platform hardware chassis active qfp feature wireless capwap datapath statistics reassembly
- show platform hardware chassis active qfp feature wireless capwap datapath summary
- show platform hardware chassis active qfp feature wireless dtls cpp-client statistics
- show platform hardware chassis active qfp feature wireless dtls cpp-client summary
- show platform hardware chassis active qfp feature wireless dtls datapath statistics
- show platform hardware chassis active qfp feature wireless dtls datapath summary
- show platform hardware chassis active qfp feature wireless et-analytics eta-pending-client-tree
- show platform hardware chassis active qfp feature wireless et-analytics statistics
- show platform hardware chassis active qfp feature wireless fqdn-filter summary
- show platform hardware chassis active qfp feature wireless halo statistics
- show platform hardware chassis active qfp feature wireless ipsg cpp-client statistics

- show platform hardware chassis active qfp feature wireless ipsg cpp-client table ipv4 all
- show platform hardware chassis active qfp feature wireless ipsg cpp-client table ipv6 all
- show platform hardware chassis active qfp feature wireless ipsg datapath statistics global
- show platform hardware chassis active qfp feature wireless ipsg datapath table ipv4 all
- show platform hardware chassis active qfp feature wireless ipsg datapath table ipv6 all
- show platform hardware chassis active qfp feature wireless mgmt-intf cpp-client summary
- show platform hardware chassis active qfp feature wireless mgmt-intf datapath summary
- show platform hardware chassis active qfp feature wireless punt statistics
- show platform hardware chassis active qfp feature wireless wlan summary
- show platform hardware chassis active qfp feature wireless wlclient cpp-client statistics
- show platform hardware chassis active qfp feature wireless wlclient cpp-client summary
- show platform hardware chassis active qfp feature wireless wlclient datapath statistic drop
- show platform hardware chassis active qfp feature wireless wlclient datapath summary
- show platform hardware chassis active qfp feature wireless wlclient datapath table dataglean all
- show platform hardware chassis active qfp infrastructure punt statistics type per-cause
- show platform hardware chassis active qfp statistics drop
- show platform software bssid chassis active F0
- show platform software bssid chassis active F0 statistics
- show platform software capwap chassis active F0
- show platform software capwap chassis active F0 statistics
- show platform software dtls chassis active F0
- show platform software dtls chassis active F0 statistics
- show platform software wireless-client chassis active F0
- show platform software wireless-client chassis active F0 statistics
- show platform software wlan chassis active F0

スタンバイ ノードが存在する場合は、次のデータパス コマンドも表示されます。

- show platform hardware chassis standby qfp feature wireless bssid summary
- show platform hardware chassis standby qfp feature wireless capwap cpp-client statistics
- show platform hardware chassis standby qfp feature wireless capwap cpp-client summary
- show platform hardware chassis standby qfp feature wireless capwap datapath statistics drop
- show platform hardware chassis standby qfp feature wireless capwap datapath statistics fragmentation
- show platform hardware chassis standby qfp feature wireless capwap datapath statistics reassembly

- show platform hardware chassis standby qfp feature wireless capwap datapath summary
- show platform hardware chassis standby qfp feature wireless dtls cpp-client statistics
- show platform hardware chassis standby qfp feature wireless dtls cpp-client summary
- show platform hardware chassis standby qfp feature wireless dtls datapath statistics
- show platform hardware chassis standby qfp feature wireless dtls datapath summary
- show platform hardware chassis standby qfp feature wireless halo statistics
- show platform hardware chassis standby qfp feature wireless ipsg cpp-client statistics
- show platform hardware chassis standby qfp feature wireless ipsg cpp-client table ipv4 all
- show platform hardware chassis standby qfp feature wireless ipsg cpp-client table ipv6 all
- show platform hardware chassis standby qfp feature wireless ipsg datapath statistics global
- show platform hardware chassis standby qfp feature wireless ipsg datapath table ipv4 all
- show platform hardware chassis standby qfp feature wireless ipsg datapath table ipv6 all
- show platform hardware chassis standby qfp feature wireless mgmt-intf cpp-client summary
- show platform hardware chassis standby qfp feature wireless mgmt-intf datapath summary
- show platform hardware chassis standby qfp feature wireless punt statistics
- show platform hardware chassis standby qfp feature wireless wlan summary
- show platform hardware chassis standby qfp feature wireless wlclient cpp-client statistics
- show platform hardware chassis standby qfp feature wireless wlclient cpp-client summary
- show platform hardware chassis standby qfp feature wireless wlclient datapath statistic drop
- show platform hardware chassis standby qfp feature wireless wlclient datapath summary
- show platform hardware chassis standby qfp feature wireless wlclient datapath table dataglean all
- show platform hardware chassis standby qfp statistics drop
- show platform software bssid chassis standby F0
- show platform software bssid chassis standby F0 statistics
- show platform software capwap chassis standby F0
- show platform software capwap chassis standby F0 statistics
- show platform software dtls chassis standby F0
- show platform software dtls chassis standby F0 statistics
- show platform software wireless-client chassis standby F0
- show platform software wireless-client chassis standby F0 statistics
- show platform software wlan chassis standby F0

例

次に、**show tech-support wireless datapath** コマンドの出力例を示します

```
Device# show tech-support wireless datapath


------------------ show platform hardware chassis active qfp statistics drop
------------------

-------------------------------------------------------------------------
Global Drop Stats                                Packets              Octets
-------------------------------------------------------------------------
Disabled                                           22230             2045194
InvL2Hdr                                         4765368           744492240
Ipv4NoAdj                                              6                 736
Ipv4NoRoute                                           18                2358
Ipv6mcNoRoute                                          3                 270
SWPortDrop                                         14432             2886027
SWPortSrcFilter                                    53265            53992718
SWPortStpState                                     42041             3269790
SWPortVlanNotCfg                                 5515542           674079804
SwitchL2m                                             78               10062
SwitchL2mIGMP                                      18866             1283348
SwitchL2mUnconfigWireless                             78               11622
WlsCapwapNoTunnel                                      3                 627


------------------ show platform hardware chassis active qfp feature wireless punt
statistics ------------------


CPP Wireless Punt stats:

                                App Tag     Packet Count
                                -------     ------------
         CAPWAP_PKT_TYPE_DOT11_PROBE_REQ               0
              CAPWAP_PKT_TYPE_DOT11_MGMT              56
              CAPWAP_PKT_TYPE_DOT11_IAPP           22177
              CAPWAP_PKT_TYPE_DOT11_RFID               0
               CAPWAP_PKT_TYPE_DOT11_RRM               0
             CAPWAP_PKT_TYPE_DOT11_DOT1X               0
       CAPWAP_PKT_TYPE_CAPWAP_KEEPALIVE               0
     CAPWAP_PKT_TYPE_MOBILITY_KEEPALIVE               0
           CAPWAP_PKT_TYPE_CAPWAP_CNTRL          303661
            CAPWAP_PKT_TYPE_CAPWAP_DATA               0
         CAPWAP_PKT_TYPE_MOBILITY_CNTRL               0
                        WLS_SMD_WEBAUTH               0
                     SISF_PKT_TYPE_ARP             303
                    SISF_PKT_TYPE_DHCP             282
                   SISF_PKT_TYPE_DHCP6               0
                 SISF_PKT_TYPE_IPV6_ND               0
               SISF_PKT_TYPE_DATA_GLEAN               0
            SISF_PKT_TYPE_DATA_GLEAN_V6               0
               SISF_PKT_TYPE_DHCP_RELAY               0
       CAPWAP_PKT_TYPE_CAPWAP_RESERVED               0


------------------ show platform hardware chassis active qfp infrastructure punt statistics
 type per-cause ------------------

Global Per Cause Statistics
```

```
Number of punt causes =   136

Per Punt Cause Statistics
                                                                    Packets              Packets
Counter ID  Punt Cause Name                                       Received             Transmitted

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

000         Reserved                                              0                    0
001         MPLS ICMP Can't Fragment                              0                    0
002         IPv4 Options                                          0                    0
003         Layer2 control and legacy                             0                    0
004         PPP Control                                           0                    0
005         CLNS IS-IS Control                                    0                    0
006         HDLC keepalives                                       0                    0
007         ARP request or response                               2687                 2687
008         Reverse ARP request or repsonse                       0                    0
009         Frame-relay LMI Control                               0                    0
010         Incomplete adjacency                                  0                    0
011         For-us data                                           0                    0
012         Mcast Directly Connected Source                       0                    0
013         Mcast IPv4 Options data packet                        0                    0
014         Skip egress processing                                0                    0
015         MPLS TTL expired                                      0                    0
016         MPLS Reserved label (ie: 0-15)                        0                    0
017         IPv6 Bad hop limit                                    0                    0
018         IPV6 Hop-by-hop Options                               0                    0
019         Mcast Internal Copy                                   0                    0
020         Generic QFP generated packet                          0                    0
021         RP<->QFP keepalive                                    46691                46691
022         QFP Fwall generated packet                            0                    0
023         Mcast IGMP Unroutable                                 0                    0
024         Glean adjacency                                       2557                 2556
025         Mcast PIM signaling                                   0                    0
026         QFP ICMP generated packet                             0                    0
027         Subscriber session control                            0                    0
```

028	Subscriber data switching back	0	0
029	RP handled ICMP	0	0
030	RP injected For-us data	0	0
031	Punt adjacency	0	0
032	SBC RTP DTMF	0	0
033	Pseudowire VCCV control channel	0	0
034	Generic QFP generated packet (keep GPM)	0	0
035	Ethernet slow protocol (ie: LACP, OAM)	0	0
036	Ethernet OAM Loopback	0	0
037	UNUSED	0	0
038	SPA IPC packet	0	0
039	Punt and replicate	0	0
040	PPPoE control	0	0
041	PPPoE session	0	0
042	L2TP control	0	0
043	IP Subscriber control (ie: FSOL, keepali	0	0
044	L2TP session	0	0
045	BFD control	0	0
046	MVPN non-RPF signaling packet	0	0
047	MVPN PIM signalling packet	0	0
048	Mcast punt to RP	0	0
049	SBC generated packet	0	0
050	IPv6 packet	0	0
051	DMVPN NHRP redirect	0	0
052	PFR monitored prefix logging	0	0
053	PFR top talkers logging	0	0
054	PFR top talkers application logging	0	0
055	For-us control	0	0
056	RP injected for-us control	0	0
057	QFP VTCP generated packet	0	0
058	Layer2 bridge domain data packet	0	0
059	QFP Stile generated packet	0	0

060	IP subnet or broadcast packet	167	167
061	Ethernet CFM packet	0	0
062	Ethernet CFM notify packet	0	0
063	LISP LSB NOTIFICATION	0	0
064	Service Engine packet	0	0
065	L2BD Control packet from FIA	0	0
066	L2BD Control Message from CPP	0	0
067	MFR_LIP_CONTROL	0	0
068	Media Monitoring record punted from CPP	0	0
069	OTV Control packet	0	0
070	OTV ARP packet	0	0
071	REP control	0	0
072	IP MTU EXCEPTION	0	0
073	STP BPDU's	186832	186832
074	ACL log	0	0
075	EPC	0	0
076	Lisp Dynamic eid	0	0
077	L2 Control packet	122389	122389
078	WAAS CPP to CPP punt	0	0
079	dhcp snoop	0	0
080	Metric Mediation Agent record punted fro	0	0
081	IPv6 DMVPN NHRP redirect	0	0
082	Ethernet CFM packet from core	0	0
083	Ethernet CFM punt fwd packet	0	0
084	PTP punt fwd packet	0	0
085	ISDN D-Channel raw packet	0	0
086	Service controller SCG punt pkt	0	0
087	IPv6 FHS SG dropped packet	0	0
088	IPv6 FHS Data glean packet	0	0
089	SBC DSP pkts	0	0
090	Raw Socket Data packet	0	0
091	SSLVPN session control	0	0

092	ICMP unreachables for ACL denied packets	0	0
093	CENT Smart Probe packet	0	0
094	AppNav vPATH pktless API generated pkt	0	0
095	Autonomic Network Channel Discovery pack	0	0
096	Layer2 control protocols	0	0
097	Packets to LFTS	22177	22177
098	VLAN Auto Sense FSOL	0	0
099	ZTP Discovery packet	0	0
100	cable arp filter	0	0
101	Cable L3 mobility	0	0
102	Source Verify inconclusive	0	0
103	cable modem pre reg	0	0
104	mpls receive adj	0	0
105	MKA EAPoL packet	0	0
106	ICMP Unreachable	0	0
107	Cable DHCP	0	0
108	Snooping packet	0	0
109	snoop packets	0	0
110	msg Indicating ppp intf assigned ip addr	0	0
111	msg indicating there is another common h	0	0
112	QoS CAC Flow Report	0	0
113	Active identity	0	0
114	BGP Overlay Tunnel packet	0	0
115	Lisp gsmr enabled	0	0
116	Async TS	0	0
117	Metric Mediation Agent Packet	0	0
118	Cable DHCPV6 Solicit	0	0
119	Cable DHCPV6 Request	0	0
120	SBC RTP FWD DTMF	0	0
121	Path Manager	0	0
122	L2 LISP VXLAN	0	0
123	dialer-list	0	0

```
124         Dialer update time                          0                   0
125         Cable RPHY CTRL                             0                   0
126         OpenFlow SDN                                0                   0
127         Path Manager TTL expired                    0                   0
128         L3 PTP message                              0                   0
129         wls 802.11 Packets to LFTS                  56                  56
130         wls CAPWAP Packets to LFTS                  303661              303661
131         wls MOBILITY Packets to LFTS                0                   0
132         wls SISF Packets to LFTS                    585                 585
133         cable DHCPv6 subscriber-side                0                   0
134         cable DHCPv4 subscriber-side                0                   0
135         cable DHCPv4 sub-side disc/req              0                   0


Number of inject causes = 49

Per Inject Cause Statistics
                                                         Packets             Packets
Counter ID  Inject Cause Name                            Received            Transmitted

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

000         RESERVED                                    0                   0
001         L2 control/legacy                           3115                3115
002         QFP destination lookup                      0                   0
003         QFP IPv4/v6 nexthop lookup                  0                   0
004         QFP generated packet                        0                   0
005         QFP <->RP keepalive                         46691               0
006         QFP Fwall generated packet                  0                   0
007         QFP adjacency-id lookup                     0                   0
008         Mcast specific inject packet                0                   0
009         QFP ICMP generated packet                   0                   0
010         QFP/RP->QFP Subscriber data packet          0                   0
011         SBC DTMF                                    0                   0
012         ARP request or response                     3637                3637
013         Ethernet OAM loopback packet                0                   0
```

014	UNUSED	0	0
015	PPPoE discovery packet	0	0
016	PPPoE session packet	0	0
017	QFP inject for pp_index lookup	0	0
018	QFP inject replicate	0	0
019	QFP inject PIT lookup	0	0
020	SBC generated packets	0	0
021	QFP VTCP generated packet	0	0
022	QFP Stile generated packet	0	0
023	Service Engine generated packet	0	0
024	Layer2 frame to EFP	0	0
025	Layer2 frame to BD	0	0
026	QfP Asym Routing redirected pkt	0	0
027	Compressed packet from WAAS	0	0
028	Media (e.g. voice) associated with a ses	0	0
029	service controller scg packet	0	0
030	Packet for 14 port Serial IM	0	0
031	Subscriber generated TCP reset packet	0	0
032	Layer2 frame to INPUT EFP	0	0
033	SSLVPN inject control	0	0
034	injected packet from UTD SP	0	0
035	injected packet from DPSS SN	0	0
036	injected packet by AppNav vPath	0	0
037	Uncompressed packet from WAAS	0	0
038	Autonomic Network Channel Discovery pack	0	0
039	Cable Bundle Flood Inject	0	0
040	Cable L2 unicast inject	0	0
041	downstream jib packet	0	0
042	switch port layer 2 control packet	6254	6253
043	Applications Injecting Pkts using LFTS	303874	303269
044	Enhanced ping and traceroute	0	0
045	Applications Injecting packets with SGT	0	0

```
  046         CoPP packets from EPC_WS                  0                    0

  047         Async TS                                  0                    0

  048         Layer2 frame to VLAN                      0                    0


------------------ show platform hardware chassis active qfp feature wireless mgmt-intf
 cpp-client summary ------------------

Wireless Management Interface Info
 CPP IF_H   VLAN   MAC Address
--------------------------------
   0XF       78   001e.1405.2bff


------------------ show platform hardware chassis active qfp feature wireless mgmt-intf
 datapath summary ------------------

Wireless Management Interface Info
IF_H       VLAN   MAC Address
--------------------------------------
0xF        78     001e.1405.2bff


------------------ show platform software wlan chassis active F0 ------------------

WLAN Interface ID  WLAN ID     WLAN Name                                AOM ID  Status

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

0xf0400001         1           att                                        275  Done

0xf0400002         2           verizon                                    292  Done



------------------ show platform hardware chassis active qfp feature wireless wlan summary
 ------------------

CPP Wlan Database Summary
Total number of wlan interfaces : 2
         if_name             cpp_if_hdl    pal_if_hdl     in_uidb       out_uidb
           ssid
-----------------------------------------------------------------------------------------------

   WLAN-IF-0x00f0400001         0X74       0XF0400001     0X1768E       0X1768C
           att
   WLAN-IF-0x00f0400002         0X78       0XF0400002     0X1768A       0X17688
         verizon


------------------ show platform software bssid chassis active F0 statistics
------------------


Bssid Counters    (Success/Failure)
-----------------------------------
Create                 0/0
Delete                 0/0
HW Create              0/0
```

```
HW Modify              0/0
HW Delete              0/0
Create Ack             0/0
Modify Ack             0/0
Delete Ack             0/0
Nack Notify            0/0


------------------ show platform software bssid chassis active F0 ------------------


------------------ show platform hardware chassis active qfp feature wireless bssid
summary ------------------


------------------ show platform software capwap chassis active F0 statistics
------------------


Capwap Counters   (Success/Failure)
-----------------------------------
Create                  424/0
Delete                  420/0
HW Create               424/0
HW Modify               0/0
HW Delete               420/0
Create Ack              424/0
Modify Ack              0/0
Delete Ack              420/0
Ack Ack Notify          0/0
Ack Nack Notify         0/0
Nack Notify             0/0


------------------ show platform software capwap chassis active F0 ------------------

 Tunnel ID  AP MAC          Type            IP                Port      AOM ID  Status

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

0x90000042  00a8.2200.0200  Data            78.1.50.1        52345        3271  Done

0xa0000002  0000.0000.0000  Mobility Data   78.1.1.23        16667        1426  Done

0xa0000003  0000.0000.0000  Mobility Data   78.1.1.24        16667        1427  Done

0xa0000004  0000.0000.0000  Mobility Data   78.1.1.25        16667        1428  Done


------------------ show platform hardware chassis active qfp feature wireless capwap
cpp-client statistics ------------------


CAPWAP cpp-client plumbing statistics
Number Msg in = ack + nak + ack fail + nak fail + errors

Counter                                          Value
-----------------------------------------------------------------
Create from fp                                   424
```

```
Modify from fp                                  0
Delete from fp                                  420
Create ack to fp                                424
Create ack fail to fp                           0
Create nack to fp                               0
Create nack fail to fp                          0
Modify ack to fp                                0
Modify ack fail to fp                           0
Modify nack to fp                               0
Modify nack fail to fp                          0
Delete ack to fp                                420
Delete ack fail to fp                           0
Delete nack to fp                               0
Delete nak fail to fp                           0


------------------ show platform hardware chassis active qfp feature wireless capwap
cpp-client summary ------------------

 cpp_if_hdl    pal_if_hdl       AP MAC           Src IP            Dst IP       Dst Port
  Tun Type
-------------------------------------------------------------------------------------------

   0X108       0X90000042   00a8.2200.0200      78.1.1.7         78.1.50.1       52345
     DATA
   0X10B       0XA0000002   0000.0000.0000      78.1.1.7         78.1.1.23       16667
   MOBILITY
   0X10C       0XA0000003   0000.0000.0000      78.1.1.7         78.1.1.24       16667
   MOBILITY
   0X10D       0XA0000004   0000.0000.0000      78.1.1.7         78.1.1.25       16667
   MOBILITY


------------------ show platform hardware chassis active qfp feature wireless capwap
datapath summary ------------------

Vrf Src Port Dst IP          Dsp Port Input Uidb Output Uidb Instance Id
--- -------- ------          -------- ---------- ----------- -----------
0   16667    78.1.1.25       16667    95733      95731       0
0   5247     78.1.50.1       52345    95738      95736       3
0   16667    78.1.1.24       16667    95734      95732       0
0   16667    78.1.1.23       16667    95735      95733       0


------------------ show platform hardware chassis active qfp feature wireless capwap
datapath statistics drop ------------------


Drop Cause                                                                    Packets
         Octets
==============================================================================
====================
Wls Capwap unsupported link type Error                                           0
              0
Wls Capwap invalid tunnel Error                                                  0
              0
Wls Capwap input config missing Error                                            0
              0
Wls Capwap invalid TPID Error                                                    0
              0
Wls Capwap ingress parsing Error                                                 0
              0
```

```
Wls Capwap invalid FC subtype Error                                          0
              0
Wls Capwap SNAP Invalid HLEN Error                                           0
              0
Wls Client V6 Max Address Error                                              0
              0


------------------ show platform hardware chassis active qfp feature wireless capwap
datapath statistics fragmentation ------------------


CPP Wireless Fragmentation stats:

                             Description         Packet Count          Octet Count

                             -----------         ------------          -----------
 Capwap Packets to be Fragmented (RX)                       0                    0
 Capwap Fragments to be Recycled                            0                    0
 Capwap Fragments Recycled (TX)                             0                    0
 Error: Original Packet Too Big                             0                    0
 Error: CAPWAP MTU Not Valid                                0                    0
 Error: Recycle Queue Full                                  0                    0
 Error: Recycle Queue Not Valid                             0                    0
 Error: GPM Memory Init Failure                             0                    0
 Error: Multipass Requeue Failure                           0                    0


------------------ show platform hardware chassis active qfp feature wireless capwap
datapath statistics reassembly ------------------


CPP Wireless Reassembly Memory stats:

                             Description            Count
                             -----------            -----
                          Free info chunk            32768
                     Allocated info chunks           32768
                       Free fragment chunks         131072
                  Allocated fragment chunks         131072


CPP Wireless Reassembly Packet stats: (outstanding pkt_cnt 0)

                             Description     Packet Count      Octet Count
                             -----------     ------------      -----------
     Capwap Reassembled Packets                          0                0
     Capwap Fragments Received                           0                0
     Capwap Fragments Consumed (Saved)                   0                0
     Capwap Fragments Dropped                            0                0
     Capwap Reassembly Timeouts                          0                0
     Error - Early-drop fragments                        0                0
     Error - Invalid packet size                         0                0
     Error - Fragment size too big                       0                0
     Error - Too many fragments                          0                0
     Error - Overlap offset fragments                    0                0
     Error - Duplicated fragments                        0                0
     Error - Allocate info chunk memory                  0                0
     Error - Allocate frag chunk memory                  0                0
     Error - Hash bucket threshold                       0                0
     Error - Cannot save and gather pkts                 0                0
     Error - Get recycle reass_info NULL                 0                0
     Error - BQS memory alloc NULL                       0                0
     Error - BQS memory free NULL                        0                0
```

```
     DEBUG - # of lock sync aquired                    2               2
     DEBUG - # of lock released                        2               2
     DEBUG - CPP_CW_BQS_MX_ALLOC #                     0               0
     DEBUG - CPP_CW_BQS_MX_FREE  #                     0               0
     DEBUG - CPP_REASS_INFO_ALLOC #                    0               0
     DEBUG - CPP_REASS_INFO_FREE  #                    0               0
     DEBUG - CPP_REASS_FRAG_ALLOC #                    0               0
     DEBUG - CPP_REASS_FRAG_FREE  #                    0               0


------------------ show platform software dtls chassis active F0 statistics
------------------


DTLS Counters     (Success/Failure)
-----------------------------------
Create                  847/0
Delete                  424/0
HW Create               425/0
HW Modify               422/0
HW Delete               424/0
Create Ack              425/0
Modify Ack              422/0
Delete Ack              424/0
Ack Ack Notify          1271/0
Ack Nack Notify         0/0
Nack Notify             0/0
HA Seq GET              782/0
HA Seq SET              0/0
HA Seq Crypto GET       1542/0
HA Seq Crypto SET       0/0
HA Seq Crypto Callback  1542/0

HA Seq last Responsed   0
HA Seq Pending          0
HA Seq Outstanding cb   0
Total DTLS CTX count    1


------------------ show platform software dtls chassis active F0 ------------------


Forwarding Manager DTLS Session Summary

Session ID          Type        Peer IP          Port   AOM ID      Status

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

0x0300000000000001  AP Control  78.1.50.1        52345  3270        Done



------------------ show platform hardware chassis active qfp feature wireless dtls
cpp-client statistics ------------------


DTLS cpp-client plumbing statistics
Number Msg in = ack + nak + ack fail + nak fail + errors

Counter                                          Value
-----------------------------------------------------------------
Create from fp                                   425
Modify from fp                                   422
```

```
Delete from fp                                  424
Create ack to fp                                425
Create ack fail to fp                           0
Create nack to fp                               0
Create nack fail to fp                          0
Modify ack to fp                                422
Modify ack fail to fp                           0
Modify nack to fp                               0
Modify nack fail to fp                          0
Delete ack to fp                                424
Delete ack fail to fp                           0
Delete nack to fp                               0
Delete nak fail to fp                           0


------------------ show platform hardware chassis active qfp feature wireless dtls
cpp-client summary ------------------

    Session ID          CDH Handle      Session Type     Parent if-h        Instance id

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

0x0300000000000001  0x00000000D902D9E0   AP Control           0                 3



------------------ show platform hardware chassis active qfp feature wireless dtls
datapath summary ------------------


Src IP          Dst IP          Src Port Dst Port   Crypto HDL         Instance Id
------          ------          -------- -------    -----------        ----------
78.1.1.7        78.1.50.1       5246     52345      0xd902d9e0           3

------------------ show platform hardware chassis active qfp feature wireless dtls
datapath statistics ------------------


CPP Wireless DTLS Feature Stats

                            Description     Packet Count      Octet Count
                            -----------     ------------      -----------
   DTLS Packets To Encrypt                        286494          8860778
   DTLS Packets Encrypted                         286494         35681366
   DTLS Packets To Decrypt                        286734         41001830
   DTLS Packets Decrypted                         286734         33401602
   Skip Encryption - Handshake                         0                0
   Skip Encryption - Not AppData                       0                0
   Skip Encryption - No Hash Entry                     0                0
   Skip Encryption - No Crypto Handle                  0                0
   Skip Encryption - No DTLS header                  563            76419
   Skip Encryption - Requested by RP               16234          5042852
   Skip Decryption - Handshake                         0                0
   Skip Decryption - Not AppData                    2949           996248
   Skip Decryption - No Hash Entry                   447            56474
   Skip Decryption - No Crypto Handle              13024          3626640
   Skip Decryption - No DTLS header                  507           116600
   Skip Decryption - Multiple Records                  0                0
   Error - Encrypt Invalid Length                      0                0
   Error - Encrypt Header Restore                      0                0
   Error - DataEncrypt No Crypto Handle                0                0
   Error - DataEncrypt Header Restore                  0                0
   Error - Decrypt Invalid Length                      0                0
   Error - Decrypt Header Restore                      0                0
```

```
   Error - DataDecrypt Zero Epoch                      0               0
   Error - DataDecrypt No Hash Entry                   0               0
   Error - DataDecrypt No Crypto Handle                0               0
   Error - DataDecrypt Header Restore                  0               0


------------------ show platform software wireless-client chassis active F0 statistics
------------------


Client Counters   (Success/Failure)
-----------------------------------
Create                  112/0
Delete                  55/0
HW Create               56/0
HW Modify               56/0
HW Delete               55/0
Create Ack              56/0
Modify Ack              56/0
Delete Ack              55/0
NACK Notify             0/0


------------------ show platform software wireless-client chassis active F0
------------------


        ID  MAC Address     WLAN  Client State           AOM ID  Status
-------------------------------------------------------------------------------
0xa0000001  0028.b122.0001     1  Run                      3272  Done


------------------ show platform hardware chassis active qfp feature wireless wlclient
cpp-client statistics ------------------


Wlclient cpp-client plumbing statistics
Number Msg in = ack + nak + ack fail + nak fail + errors

Counter                                          Value
-----------------------------------------------------------------
Create from fp                                   56
Modify from fp                                   56
Delete from fp                                   55
Create ack to fp                                 56
Create ack fail to fp                            0
Create nack to fp                                0
Create nack fail to fp                           0
Modify ack to fp                                 56
Modify ack fail to fp                            0
Modify nack to fp                                0
Modify nack fail to fp                           0
Delete ack to fp                                 55
Delete ack fail to fp                            0
Delete nack to fp                                0
Delete nak fail to fp                            0


------------------ show platform hardware chassis active qfp feature wireless wlclient
cpp-client summary ------------------

Auth State Abbreviations:
  UK - UNKNOWN IP - LEARN IP
```

```
  L3 - L3 AUTH RN - RUN
  IV - INVALID
Mobility State Abbreviations:
  UK - UNKNOWN IN - INIT
  LC - LOCAL   AN - ANCHOR
  FR - FOREIGN MT - MTE
  IV - INVALID
 CPP IF_H     DPIDX      MAC Address    VLAN  AS  MS                WLAN
     POA
------------------------------------------------------------------------------------------------

  0X102     0XA0000001  0028.b122.0001  177   RN  LC                 att
  0x90000042


------------------ show platform hardware chassis active qfp feature wireless wlclient
datapath summary ------------------


Vlan   pal_if_hdl   mac            Input Uidb Output Uidb
------ ------------ -------------- ---------- -----------
177    0xa0000001   0028.b122.0001 95744      95742


------------------ show platform hardware chassis active qfp feature wireless wlclient
datapath statistic drop ------------------


Drop Cause                                                                  Packets
         Octets
============================================================ ====================
====================
Wls Client V6 Max Address Error                                                   0
                0
Wls Client IPGlean Counter Index Error                                            0
                0
Wls Client IPGlean Counter Unchanged Error                                        0
                0
Wls Client IPGlean alloc no memory Error                                          0
                0
Wls Client invalid punt packet error                                              0
                0
Wls Client input subblock missing error                                           0
                0
Wls Client input config missing                                                   0
                0
Wls Client global mac address fetch error                                         0
                0
Wls Client header add error                                                       0
                0
Wls Client IP entry theft error                                                   0
                0
Wls Client IPSG input subblock missing error                                      0
                0
Wls Client DOT1Q Hdr add anchor error                                             0
                0
Wls Client DOT1Q Hdr add anchor avc error                                         0
                0
Wls Client Guest Foreign Multicast error                                          0
                0


------------------ show platform hardware chassis active qfp feature wireless wlclient
```

```
datapath table dataglean all ------------------


CPP Wireless IPv6 Data Gleaning Table:

IP Address                                VLAN    uIDB   Interface
----------------------------------------  ----  ------  -------------


------------------ show platform hardware chassis active qfp feature wireless ipsg
cpp-client statistics ------------------

CPP Wireless IPSG CPP-client Statistics
Counter                         Value
-------------------------------------------------
Total IPv4 Address Count        1
Total IPv6 Address Count        0
IPv4 Entry Add Success          56
IPv4 Entry Add Fail             0
IPv4 Entry Delete Success       55
IPv4 Entry Delete Fail          0
IPv6 Entry Add Success          0
IPv6 Entry Add Fail             0
IPv6 Entry Delete Success       0
IPv6 Entry Delete Fail          0
IP Entry Override               0
IP Entry Add Req Skip           0
Data Glean Memory Req Recv      0
Data Glean Memory Req Fail      0
Data Glean Memory Reg Send      0
Data Glean Memory Ret Recv      0
Data Glean Memory Ret Send      0
Data Glean Entry Send           0
IPSG Subblock Allocate          0
IPSG Subblock Allocate Fail     0
IPSG Subblock Free              0
IPSG Subblock Free Fail         0
IPSG FIA Enable                 0
IPSG FIA Enable Fail            0
IPSG FIA Disable                0
IPSG FIA Disable Fail           0
IPSG Feature Enable             0
IPSG Feature Enable Fail        0
IPSG Feature Disable            0
IPSG Feature Disable Fail       0


------------------ show platform hardware chassis active qfp feature wireless ipsg
cpp-client table ipv4 all ------------------

CPP Wireless IPSG Table Summary
Total number of address entries: 1
IP Address                                VLAN  uIDB
-------------------------------------------------
177.1.0.7                                 177   95744


------------------ show platform hardware chassis active qfp feature wireless ipsg
cpp-client table ipv6 all ------------------

CPP Wireless IPSG Table Summary
Total number of address entries: 0
```

```
------------------ show platform hardware chassis active qfp feature wireless ipsg
datapath statistics global ------------------


  Wireless IPSG Global Statistics
  ---------------------------------
    IPv6 Dataglean entry add          :  0
    IPv6 Dataglean entry remove       :  0
    IPv6 Dataglean allocation fail    :  0
    IPv6 Dataglean pool req send      :  0
    IPv6 Dataglean pool req send fail :  0
    IPv6 Dataglean pool req resp      :  0
    IPv6 Dataglean pool ret send      :  0
    IPv6 Dataglean pool ret send fail :  0
    IPv6 Dataglean punt packet        :  0
    IPv6 Dataglean drop packet        :  0


------------------ show platform hardware chassis active qfp feature wireless ipsg
datapath table ipv4 all ------------------


CPP Wireless IPSG IPv4 Table:

IP Address                                VLAN    uIDB   Interface
----------------------------------------  ----  ------  -------------
177.1.0.7                                  177   95744  WLCLIENT-IF-0x00a0000001


------------------ show platform hardware chassis active qfp feature wireless ipsg
datapath table ipv6 all ------------------


CPP Wireless IPSG IPv6 Table:

IP Address                                VLAN    uIDB   Interface
----------------------------------------  ----  ------  -------------


------------------ show platform hardware chassis active qfp feature wireless halo
statistics ------------------


Wireless HALO Statistics
                         Rx Packet Count               0
                         Rx Packet Bytes               0


------------------ show platform hardware chassis active qfp feature wireless fqdn-filter
 summary ------------------


CPP Wireless FQDN Filter Info:
ID   Type     DSA_hdl    Redirect_IPv4    Virtual_IPv4
---- -------- ---------- ---------------- ----------------


------------------ show platform hardware chassis active qfp feature wireless et-analytics
 statistics ------------------


Wireless ETA cpp-client plumbing statistics
Number of ETA pending clients : 0
```

```
Counter                                          Value
-------------------------------------------------------------------
Enable ETA on wireless client called             0
Delete ETA on wireless client called             0
ETA global cfg init cb TVI FIA enable error      0
ETA global cfg init cb output SB read error      0
ETA global cfg init cb output SB write error     0
ETA global cfg init cb input SB read error       0
ETA global cfg init cb input SB write error      0
ETA global cfg init cb TVI FIA enable success    0
ETA global cfg uninit cb ingress feat disable    0
ETA global cfg uninit cb ingress cfg delete e    0
ETA global cfg uninit cb egress feat disable     0
ETA global cfg uninit cb egress cfg delete er    0
ETA pending list insert entry called             0
ETA pending list insert invalid arg error        0
ETA pending list insert entry exists error       0
ETA pending list insert no memory error          0
ETA pending list insert entry failed             0
ETA pending list insert entry success            0
ETA pending list delete entry called             0
ETA pending list delete invalid arg error        0
ETA pending list delete entry missing            0
ETA pending list delete entry remove error       0
ETA pending list delete entry success            0


------------------ show platform hardware chassis active qfp feature wireless et-analytics
 eta-pending-client-tree ------------------
```

show tech-support wireless fabric

グローバル ファブリック パラメータを表示するには、特権 EXEC モードで **show tech-support wireless fabric** コマンドを使用します。

show tech-support wireless fabric

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

show tech-support wireless fabric コマンドの一部として、次のコマンドの出力が表示されます。

- show wireless fabric summary
- show wireless profile fabric summary
- show fabric wlan summary
- show fabric ap summary
- show wireless fabric client summary
- show wireless fabric media-stream client summary
- show wireless stats fabric memory
- show wireless stats fabric control-plane all

例

次に、**show tech-support wireless fabric** コマンドの出力例を示します

show tech-support wireless mobility

モビリティに関連するデータを印刷するには、特権 EXEC モードで **show tech-support wireless mobility** コマンドを使用します。

show tech-support wireless mobility

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

show tech-support wireless mobility コマンドの一部として、次のコマンドの出力が表示されます。

- show platform hardware chassis active qfp feature wireless capwap cpp-client summary
- show platform hardware chassis active qfp feature wireless capwap datapath summary
- show platform hardware chassis active qfp feature wireless dtls cpp-client summary
- show platform hardware chassis active qfp feature wireless dtls datapath statistics
- show platform hardware chassis active qfp feature wireless dtls datapath summary
- show platform software capwap chassis active f0
- show platform software capwap chassis active r0
- show platform software dtls chassis active f0
- show platform software dtls chassis active r0
- show platform software ipc queue-based mobilityd chassis active R0 connection
- show platform software memory messaging mobilityd chassis active R0
- show platform software memory mobilityd chassis active R0 brief
- show wireless mobility ap-list
- show wireless mobility summary
- show wireless stats mobility
- show wireless stats mobility messages

スタンバイ ノードが存在する場合は、次のモビリティ コマンドの出力も表示されます。

- show platform hardware chassis standby qfp feature wireless capwap cpp-client summary
- show platform hardware chassis standby qfp feature wireless capwap datapath summary
- show platform hardware chassis standby qfp feature wireless dtls cpp-client summary
- show platform hardware chassis standby qfp feature wireless dtls datapath statistics
- show platform hardware chassis standby qfp feature wireless dtls datapath summary
- show platform software capwap chassis standby f0
- show platform software capwap chassis standby r0
- show platform software dtls chassis standby f0
- show platform software dtls chassis standby r0
- show platform software ipc queue-based mobilityd chassis standby R0 connection
- show platform software memory messaging mobilityd chassis standby R0
- show platform software memory mobilityd chassis standby R0 brief
- show wireless stats mobility messages chassis standby r0

例

次に、**show tech-support wireless mobility** コマンドの出力例を示します

```
Device# show tech-support wireless mobility

------------------ show wireless stats mobility ------------------


Mobility event statistics:
     Joined as
         Local                          : 0
         Foreign                        : 0
         Export foreign                 : 0
         Export anchor                  : 0
     Delete
         Local                          : 0
         Remote                         : 0
     Role changes
         Local to anchor                : 0
         Anchor to local                : 0
     Roam stats
         L2 roam count                  : 0
         L3 roam count                  : 0
         Flex client roam count         : 0
         Inter-WNCd roam count          : 0
         Intra-WNCd roam count          : 0
     Anchor Request
         Sent                           : 0
           Grant received               : 0
           Deny received                : 0
         Received                       : 0
           Grant sent                   : 0
           Deny  sent                   : 0
     Handoff Status Received
```

```
            Success                       : 0
            Group mismatch                : 0
            Client unknown                : 0
            Client blacklisted            : 0
            SSID mismatch                 : 0
            Denied                        : 0
        Handoff Status Sent
            Success                       : 0
            Group mismatch                : 0
            Client unknown                : 0
            Client blacklisted            : 0
            SSID mismatch                 : 0
            Denied                        : 0
        Export Anchor
            Request Sent                  : 0
            Response Received             :
                Ok                        : 0
                Deny - generic            : 0
                Client blacklisted        : 0
                Client limit reached      : 0
                Profile mismatch          : 0
                Deny - unknown reason     : 0
            Request Received              : 0
            Response Sent                 :
                Ok                        : 0
                Deny - generic            : 0
                Client blacklisted        : 0
                Client limit reached      : 0
                Profile mismatch          : 0
MM mobility event statistics:
        Event data allocs                 : 0
        Event data frees                  : 0
        FSM set allocs                    : 0
        FSM set frees                     : 0
        Timer allocs                      : 0
        Timer frees                       : 0
        Timer starts                      : 0
        Timer stops                       : 0
        Invalid events                    : 0
        Internal errors                   : 0


MMIF mobility event statistics:
        Event data allocs                 : 0
        Event data frees                  : 0
        Invalid events                    : 0
        Unkown events                     : 0
        Event schedule errors             : 0
        Internal errors                   : 0


------------------ show wireless stats mobility messages ------------------


MM datagram message statistics:
  Message Type              Built  Tx    Rx    Processed  Tx Error  Rx Error  Forwarded
  Retry  Drops  Allocs  Frees

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

  Mobile Announce            0      0     0     0          0         0         0
   0      0      0       0
```

```
Mobile Announce Nak         0       0       0       0           0           0           0
 0       0       0        0
Static IP Mobile Annc       0       0       0       0           0           0           0
 0       0       0        0
Static IP Mobile Annc Rsp   0       0       0       0           0           0           0
 0       0       0        0
Handoff                     0       0       0       0           0           0           0
 0       0       0        0
Handoff End                 0       0       0       0           0           0           0
 0       0       0        0
Handoff End Ack             0       0       0       0           0           0           0
 0       0       0        0
Anchor Req                  0       0       0       0           0           0           0
 0       0       0        0
Anchor Grant                0       0       0       0           0           0           0
 0       0       0        0
Anchor Xfer                 0       0       0       0           0           0           0
 0       0       0        0
Anchor Xfer Ack             0       0       0       0           0           0           0
 0       0       0        0
Export Anchor Req           0       0       0       0           0           0           0
 0       0       0        0
Export Anchor Rsp           0       0       0       0           0           0           0
 0       0       0        0
AAA Handoff                 0       0       0       0           0           0           0
 0       0       0        0
AAA Handoff Ack             0       0       0       0           0           0           0
 0       0       0        0
IPv4 Addr Update            0       0       0       0           0           0           0
 0       0       0        0
IPv4 Addr Update Ack        0       0       0       0           0           0           0
 0       0       0        0
IPv6 ND Packet              0       0       0       0           0           0           0
 0       0       0        0
IPv6 Addr Update            0       0       0       0           0           0           0
 0       0       0        0
IPv6 Addr Update Ack        0       0       0       0           0           0           0
 0       0       0        0
Client Add                  0       0       0       0           0           0           0
 0       0       0        0
Client Delete               0       0       0       0           0           0           0
 0       0       0        0
Keepalive Ctrl Req          0       0       0       0           0           0           0
 0       0       0        0
Keepalive Ctrl Resp         0       0       0       0           0           0           0
 0       0       0        0
AP List Update              0       0       0       0           0           0           0
 0       0       0        0
Client Device Profile Info  0       0       0       0           0           0           0
 0       0       0        0
PMK Update                  0       0       0       0           0           0           0
 0       0       0        0
PMK Delete                  0       0       0       0           0           0           0
 0       0       0        0
PMK 11r Nonce Update        0       0       0       0           0           0           0
 0       0       0        0
Device cache Update         0       0       0       0           0           0           0
 0       0       0        0
HA SSO Announce             0       0       0       0           0           0           0
 0       0       0        0
HA SSO Announce Resp        0       0       0       0           0           0           0
 0       0       0        0

MM IPC message statistics:
```

```
Message Type              Built  Tx    Rx    Processed  Tx Error  Rx Error  Forwarded
Drops  Allocs  Frees

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

Mobile Announce           0      0     0     0          0         0         0
 0      0       0
Mobile Announce Nak       0      0     0     0          0         0         0
 0      0       0
Static IP Mobile Annc     0      0     0     0          0         0         0
 0      0       0
Static IP Mobile Annc Rsp 0      0     0     0          0         0         0
 0      0       0
Handoff                   0      0     0     0          0         0         0
 0      0       0
Handoff End               0      0     0     0          0         0         0
 0      0       0
Handoff End Ack           0      0     0     0          0         0         0
 0      0       0
Anchor Req                0      0     0     0          0         0         0
 0      0       0
Anchor Grant              0      0     0     0          0         0         0
 0      0       0
Anchor Xfer               0      0     0     0          0         0         0
 0      0       0
Anchor Xfer Ack           0      0     0     0          0         0         0
 0      0       0
Export Anchor Req         0      0     0     0          0         0         0
 0      0       0
Export Anchor Rsp         0      0     0     0          0         0         0
 0      0       0
AAA Handoff               0      0     0     0          0         0         0
 0      0       0
AAA Handoff Ack           0      0     0     0          0         0         0
 0      0       0
IPv4 Addr Update          0      0     0     0          0         0         0
 0      0       0
IPv4 Addr Update Ack      0      0     0     0          0         0         0
 0      0       0
IPv6 ND Packet            0      0     0     0          0         0         0
 0      0       0
IPv6 Addr Update          0      0     0     0          0         0         0
 0      0       0
IPv6 Addr Update Ack      0      0     0     0          0         0         0
 0      0       0
Client Add                0      0     0     0          0         0         0
 0      0       0
Client Delete             0      0     0     0          0         0         0
 0      0       0
Keepalive Ctrl Req        0      0     0     0          0         0         0
 0      0       0
Keepalive Ctrl Resp       0      0     0     0          0         0         0
 0      0       0
AP List Update            0      0     0     0          0         0         0
 0      0       0
Client Device Profile Info 0     0     0     0          0         0         0
 0      0       0
PMK Update                0      0     0     0          0         0         0
 0      0       0
PMK Delete                0      0     0     0          0         0         0
 0      0       0
PMK 11r Nonce Update      0      0     0     0          0         0         0
 0      0       0
Device cache Update       0      0     0     0          0         0         0
```

```
   0       0       0
  HA SSO Announce             0       0      0      0          0          0          0
   0       0       0
  HA SSO Announce Resp        0       0      0      0          0          0          0
   0       0       0

MMIF IPC message statistics:
  Message Type                Built  Tx     Rx     Processed  Tx Error  Rx Error  Drops
Allocs  Frees

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

  Mobile Announce             0       0      0      0          0          0          0       0
       0
  Mobile Announce Nak         0       0      0      0          0          0          0       0
       0
  Static IP Mobile Annc       0       0      0      0          0          0          0       0
       0
  Static IP Mobile Annc Rsp   0       0      0      0          0          0          0       0
       0
  Handoff                     0       0      0      0          0          0          0       0
       0
  Handoff End                 0       0      0      0          0          0          0       0
       0
  Handoff End Ack             0       0      0      0          0          0          0       0
       0
  Anchor Req                  0       0      0      0          0          0          0       0
       0
  Anchor Grant                0       0      0      0          0          0          0       0
       0
  Anchor Xfer                 0       0      0      0          0          0          0       0
       0
  Anchor Xfer Ack             0       0      0      0          0          0          0       0
       0
  Export Anchor Req           0       0      0      0          0          0          0       0
       0
  Export Anchor Rsp           0       0      0      0          0          0          0       0
       0
  AAA Handoff                 0       0      0      0          0          0          0       0
       0
  AAA Handoff Ack             0       0      0      0          0          0          0       0
       0
  IPv4 Addr Update            0       0      0      0          0          0          0       0
       0
  IPv4 Addr Update Ack        0       0      0      0          0          0          0       0
       0
  IPv6 ND Packet              0       0      0      0          0          0          0       0
       0
  IPv6 Addr Update            0       0      0      0          0          0          0       0
       0
  IPv6 Addr Update Ack        0       0      0      0          0          0          0       0
       0
  Client Add                  0       0      0      0          0          0          0       0
       0
  Client Delete               0       0      0      0          0          0          0       0
       0
  Keepalive Ctrl Req          0       0      0      0          0          0          0       0
       0
  Keepalive Ctrl Resp         0       0      0      0          0          0          0       0
       0
  AP List Update              0       0      0      0          0          0          0       0
       0
  Client Device Profile Info  0       0      0      0          0          0          0       0
       0
```

```
  PMK Update                0      0      0      0          0          0          0       0
       0
  PMK Delete                0      0      0      0          0          0          0       0
       0
  PMK 11r Nonce Update      0      0      0      0          0          0          0       0
       0
  Device cache Update       0      0      0      0          0          0          0       0
       0
  HA SSO Announce           0      0      0      0          0          0          0       0
       0
  HA SSO Announce Resp      0      0      0      0          0          0          0       0
       0


------------------ show wireless mobility summary ------------------


Mobility Summary

Wireless Management VLAN: 32
Wireless Management IP Address: 9.12.32.10
Mobility Control Message DSCP Value: 48
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: default
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: 001e.f6c1.f6ff

Controllers configured in the Mobility Domain:

 IP               Public Ip         Group Name                        Multicast IPv4
Multicast IPv6                                  Status                        PMTU
-------------------------------------------------------------------------------------------------------------------
9.12.32.10        N/A               default                           0.0.0.0
::                                              N/A                           N/A


------------------ show wireless mobility ap-list ------------------


------------------ show platform software capwap chassis active r0 ------------------


------------------ show platform software capwap chassis active f0 ------------------


------------------ show platform software dtls chassis active r0 ------------------


------------------ show platform software dtls chassis active f0 ------------------


------------------ show platform hardware chassis active qfp feature wireless capwap
cpp-client summary ------------------


------------------ show platform hardware chassis active qfp feature wireless dtls
cpp-client summary ------------------
```

```
------------------ show platform hardware chassis active qfp feature wireless capwap
datapath summary ------------------


Vrf Src Port Dst IP          Dsp Port Input Uidb Output Uidb Instance Id
--- -------- ------          -------- ---------- ----------- -----------


------------------ show platform hardware chassis active qfp feature wireless dtls
datapath statistics ------------------


CPP Wireless DTLS Feature Stats

                            Description     Packet Count      Octet Count
                            -----------     ------------      -----------
   DTLS Packets To Encrypt                              0                0
   DTLS Packets Encrypted                               0                0
   DTLS Packets To Decrypt                              0                0
   DTLS Packets Decrypted                               0                0
   Skip Encryption - Handshake                          0                0
   Skip Encryption - Not AppData                        0                0
   Skip Encryption - No Hash Entry                      0                0
   Skip Encryption - No Crypto Handle                   0                0
   Skip Encryption - No DTLS header                     0                0
   Skip Encryption - Requested by RP                    0                0
   Skip Decryption - Handshake                          0                0
   Skip Decryption - Not AppData                        0                0
   Skip Decryption - No Hash Entry                      0                0
   Skip Decryption - No Crypto Handle                   0                0
   Skip Decryption - No DTLS header                     0                0
   Skip Decryption - Multiple Records                   0                0
   Error - Encrypt Invalid Length                       0                0
   Error - Encrypt Header Restore                       0                0
   Error - DataEncrypt No Crypto Handle                 0                0
   Error - DataEncrypt Header Restore                   0                0
   Error - Decrypt Invalid Length                       0                0
   Error - Decrypt Header Restore                       0                0
   Error - DataDecrypt Zero Epoch                       0                0
   Error - DataDecrypt No Hash Entry                    0                0
   Error - DataDecrypt No Crypto Handle                 0                0
   Error - DataDecrypt Header Restore                   0                0


------------------ show platform hardware chassis active qfp feature wireless dtls
datapath summary ------------------


Src IP          Dst IP          Src Port Dst Port   Crypto HDL         Instance Id
------          ------          -------- -------    ----------         -----------

------------------ show platform software ipc queue-based mobilityd chassis active R0
connection ------------------

Name: -mobilityd_to_wncd-b0
  Number     : 0
  Mode       : writer
  Created on : 03/22/18 05:35:06
  Queue Size : 524288 bytes, 0 bytes currently used
  Enqueued   : 12 msgs, 432 bytes, 0 err, 0 back-pressures,
               360 bytes max queue utilization,
```

```
               0 times reached above 90%, 0 times reached above 75%

Name: -mobilityd_to_wncd-b1
  Number     : 1
  Mode       : writer
  Created on : 03/22/18 05:35:06
  Queue Size : 524288 bytes, 0 bytes currently used
  Enqueued   : 12 msgs, 432 bytes, 0 err, 0 back-pressures,
               360 bytes max queue utilization,
               0 times reached above 90%, 0 times reached above 75%

Name: -mobilityd_to_wncd-b2
  Number     : 2
  Mode       : writer
  Created on : 03/22/18 05:35:06
  Queue Size : 524288 bytes, 0 bytes currently used
  Enqueued   : 12 msgs, 432 bytes, 0 err, 0 back-pressures,
               360 bytes max queue utilization,
               0 times reached above 90%, 0 times reached above 75%

Name: -mobilityd_to_fman_rp-b0
  Number     : 3
  Mode       : writer
  Created on : 03/22/18 05:35:06
  Queue Size : 524288 bytes, 0 bytes currently used
  Enqueued   : 0 msgs, 0 bytes, 0 err, 0 back-pressures,
               0 bytes max queue utilization,
               0 times reached above 90%, 0 times reached above 75%

Name: -mobilityd_to_iosd_rp-b0
  Number     : 4
  Mode       : writer
  Created on : 03/22/18 05:35:06
  Queue Size : 524288 bytes, 0 bytes currently used
  Enqueued   : 204647 msgs, 15757819 bytes, 0 err, 0 back-pressures,
               81 bytes max queue utilization,
               0 times reached above 90%, 0 times reached above 75%

Name: -mobilityd_to_wncmgrd-b0
  Number     : 5
  Mode       : writer
  Created on : 03/22/18 05:35:06
  Queue Size : 524288 bytes, 0 bytes currently used
  Enqueued   : 12 msgs, 432 bytes, 0 err, 0 back-pressures,
               360 bytes max queue utilization,
               0 times reached above 90%, 0 times reached above 75%

Name: -odm_clnt2svr_data-mobilityd-000-1
  Number     : 6
  Mode       : writer
  Created on : 03/22/18 05:35:06
  Queue Size : 2097152 bytes, 0 bytes currently used
  Enqueued   : 33 msgs, 12535 bytes, 0 err, 0 back-pressures,
               3769 bytes max queue utilization,
               0 times reached above 90%, 0 times reached above 75%

Name: -odm_svr2clnt_data-mobilityd-000-1
  Number     : 7
  Mode       : reader
  Created on : 03/22/18 05:35:06
  Queue Size : 2097152 bytes, 0 bytes currently used
  Dequeued   : 0 msgs, 0 bytes, 0 err

Name: -fman_rp_to_mobilityd-b0
```

```
  Number     : 8
  Mode       : reader
  Created on : 03/22/18 05:35:08
  Queue Size : 524288 bytes, 0 bytes currently used
  Dequeued   : 0 msgs, 0 bytes, 0 err

Name: -wncd_to_mobilityd-b0
  Number     : 9
  Mode       : reader
  Created on : 03/22/18 05:35:13
  Queue Size : 524288 bytes, 0 bytes currently used
  Dequeued   : 39 msgs, 1404 bytes, 0 err

Name: -wncd_to_mobilityd-b1
  Number     : 10
  Mode       : reader
  Created on : 03/22/18 05:35:13
  Queue Size : 524288 bytes, 0 bytes currently used
  Dequeued   : 39 msgs, 1404 bytes, 0 err

Name: -wncd_to_mobilityd-b2
  Number     : 11
  Mode       : reader
  Created on : 03/22/18 05:35:14
  Queue Size : 524288 bytes, 0 bytes currently used
  Dequeued   : 39 msgs, 1404 bytes, 0 err

Name: -wncmgrd_to_mobilityd-b0
  Number     : 12
  Mode       : reader
  Created on : 03/22/18 05:35:14
  Queue Size : 524288 bytes, 0 bytes currently used
  Dequeued   : 18 msgs, 648 bytes, 0 err

Name: -iosd_rp_to_mobilityd-b0
  Number     : 13
  Mode       : reader
  Created on : 03/22/18 05:35:30
  Queue Size : 1048576 bytes, 0 bytes currently used
  Dequeued   : 204647 msgs, 18827524 bytes, 0 err

Name: -odm_clnt2svr_data-ifid-005-1
  Number     : 14
  Mode       : writer
  Created on : 03/22/18 05:35:37
  Queue Size : 2097152 bytes, 0 bytes currently used
  Enqueued   : 0 msgs, 0 bytes, 0 err, 0 back-pressures,
               0 bytes max queue utilization,
               0 times reached above 90%, 0 times reached above 75%

Name: -odm_svr2clnt_data-ifid-005-1
  Number     : 15
  Mode       : reader
  Created on : 03/22/18 05:35:37
  Queue Size : 2097152 bytes, 0 bytes currently used
  Dequeued   : 0 msgs, 0 bytes, 0 err



------------------ show platform software memory messaging mobilityd chassis active R0
------------------

[tdl_toc] type toc_table_info/47da701cd9c36de7e888ca6d8dd80390/0 created:3 destroyed:3
diff:0
```

```
[tdl_sr] type repl_table_name/29184a6d15c1ba11acb2d0bd22eb6e36/0 created:33 destroyed:33
 diff:0
[tdl_sr] type repl_database_name/e9118a691a20b4b8f1118bc37a894603/0 created:33 destroyed:33
 diff:0
[tdl_sr] type repl_pkey_tdl/83de2d20ec3ca19b8ae9a89147480a25/1 created:33 destroyed:33
diff:0
[tdl_sr] type repl_blob_tdl/016a67083ea407334130436c855ae237/0 created:33 destroyed:33
diff:0
[tdl_sr] type repl_luid/b9c9d9f4876af528cb82273df98479d6/0 created:33 destroyed:33 diff:0
[tdl_sr] type repl_objinfo/6c8800fedf8d71512f9b6c9754db3a70/0 created:33 destroyed:33
diff:0
[tdl_sr] message repl_trec_update/15fe2a39409473179c9e7111851b2196/0 created:33
destroyed:33 diff:0
[pki_ssl] type buff/941d8a519d6f23d27067617119f1bb38/0 created:613944 destroyed:613944
diff:0
[pki_ssl] type get_certid_params/0d7bcce690f74649c2e33bbf341e2229/0 created:204648
destroyed:204648 diff:0
[pki_ssl] type get_certid_callback_params/708b7fb964ace7971d90a452c830488c/0 created:204648
 destroyed:204648 diff:0
[pki_ssl] message get_certid/ee3bfe6b93901440346417a4ad67fa63/0 created:204648
destroyed:204648 diff:0
[pki_ssl] message get_certid_callback/372218059d7a753ba73f7b06f18532e9/0 created:204648
 destroyed:204648 diff:0
[svc_defs] type svc_loc/929237802cf26e862f8e8716169e31ef/0 created:40952 destroyed:40951
 diff:1
[ui_shr] type ui_client/bec7457db0c33cae9eeebbf80073b771/0 created:3 destroyed:2 diff:1
[ui] type ui_info/4b8b42a883fabbb98ec8b919f60e4ad6/0 created:40949 destroyed:40949 diff:0
[ui] type ui_req/69f1e2a5943e050f0aa12df8639ba442/0 created:3 destroyed:2 diff:1
[ui] type event_statistics/7f346ee47165c035a72e139b84afb2a0/0 created:40948 destroyed:40948
 diff:0
[ui] type hostinfo_data/54d5a8b0cd4d29d575b2fc0d91695b5e/0 created:3 destroyed:3 diff:0
[ui] message ui_info_msg/bec533dd713e0222cb8fe5df868031f0/0 created:1 destroyed:1 diff:0
[ui] message ui_req_msg/ac9905cc4488c976847affab56d8b50c/0 created:3 destroyed:2 diff:1
[ui] message process_event_statistics/65d07aa3a04ad950cddd46444df6bc02/0 created:40948
destroyed:40948 diff:0
[ui] message hostinfo_notify/2e9d975712b85b41bc489a6adbc4a46c/0 created:3 destroyed:3
diff:0
[uipeer_comm_ui] type mqipc_enqueue_stats/8f41e408c97a799a5e431d2279acd8de/0 created:8
destroyed:8 diff:0
[uipeer_comm_ui] type mqipc_dequeue_stats/aafe5d0a37ba9652d68550efa26eb0b6/0 created:8
destroyed:8 diff:0
[uipeer_comm_ui] type mqipc_connection_properties/35bd274fd85f7359066f898f25c853ee/0
created:16 destroyed:16 diff:0
[uipeer_comm_ui] message mqipc_connection/a1b22c74b279335b895531ce708c804b/0 created:16
 destroyed:16 diff:0
[mem_stats_ui] type tdl_variant_stat/bd85e4b89fb10501e68c1a3cedb9f321/0 created:1
destroyed:0 diff:1
[mem_stats_ui] message tdl_mem_stats/60ffd9d51213767d041b543869df15d2/0 created:1
destroyed:0 diff:1
[cdlcore] type cdl_params/a3e74327d37abf27f799f2b5155f4923/0 created:2 destroyed:1 diff:1
[cdlcore] message cdl_message/35205e535c7ab2cdcb3c265ac788f973/0 created:2 destroyed:1
diff:1
[odm_defs] type odm_context/73aeecb77a1ccb6e44f690745cdafe0d/1 created:23 destroyed:23
diff:0
[odm_defs] type odm_register_info/48a7d590e9df0cc9d150801315c50307/1 created:4 destroyed:4
 diff:0
[odm_defs] type odm_table_register_info/4f355a34615affd49af9f90b679d8ce5/1 created:17
destroyed:17 diff:0
[odm_defs] type odm_register_result/53ba304bc0a71a7d2a044518c21f662a/0 created:2
destroyed:2 diff:0
[odm_defs] message odm_register/2c98272b43d973fa08bbf5acdf3106b0/0 created:2 destroyed:2
 diff:0
[odm_defs] message odm_table_register/46694ec1005c3b084337748eeb3768cd/0 created:17
destroyed:17 diff:0
```

```
[odm_defs] message odm_register_done/1f6c8f81fcbb8a3052428bab7588e8b5/0 created:2
destroyed:2 diff:0
[odm_defs] message odm_register_ack/03b8040ed4f7b03517b410c32568ecaa/0 created:2
destroyed:2 diff:0


------------------ show platform software memory mobilityd chassis active R0 brief
------------------

  module                  allocated     requested     allocs        frees
  ---------------------------------------------------------------------------
  Summary                 620441        617113        233           25
  unknown                 198515        198435        5             0
  chunk                   139689        139209        30            0
  eventutil               118939        118299        48            8
  process                 67642         67594         3             0
  odm-db-ctx              29950         28430         100           5
  uipeer                  22672         22592         11            6
  odm-ipc-ctx             20272         19984         18            0
  unknown                 18024         18008         1             0
  odm-client-ctx          1872          1824          3             0
  cdllib                  1688          1672          3             2
  trccfg                  512           496           5             4
  bidb                    472           456           1             0
  unknown                 96            48            3             0
  bcrdu_avl               72            56            1             0
  orchestrator_main       26            10            1             0
```

show tech-support wireless radio

無線に関連するデータを印刷するには、特権 EXEC モードで **show tech-support wireless radio** コマンドを使用します。

show tech-support wireless radio

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

show tech-support wireless radio コマンドの一部として、次のコマンドの出力が表示されます。

- show ap auto-rf dot11 24ghz
- show ap auto-rf dot11 5ghz
- show ap config dot11 dual-band summary
- show ap config general
- show ap dot11 24ghz channel
- show ap dot11 24ghz coverage
- show ap dot11 24ghz group
- show ap dot11 24ghz high-density
- show ap dot11 24ghz load-info
- show ap dot11 24ghz monitor
- show ap dot11 24ghz network
- show ap dot11 24ghz summary
- show ap dot11 24ghz txpower
- show ap dot11 5ghz channel
- show ap dot11 5ghz coverage
- show ap dot11 5ghz group
- show ap dot11 5ghz high-density
- show ap dot11 5ghz load-info

- show ap dot11 5ghz monitor
- show ap dot11 5ghz network
- show ap dot11 5ghz summary
- show ap dot11 5ghz txpower
- show ap fra
- show ap rf-profile name Rf1 detail
- show ap rf-profile summary
- show ap summary
- show wireless band-select

例

次に、**show tech-support wireless radio** コマンドの出力例を示します

```
Device# show tech-support wireless radio

------------------ show ap summary ------------------

Number of APs: 0


------------------ show ap dot11 24ghz summary ------------------


------------------ show ap dot11 5ghz summary ------------------


------------------ show ap config dot11 dual-band summary ------------------


------------------ show ap dot11 24ghz channel ------------------


Leader Automatic Channel Assignment
  Channel Assignment Mode                   : AUTO
  Channel Update Interval                   : 600 seconds
  Anchor time (Hour of the day)             : 0
  Channel Update Contribution
    Noise                                   : Enable
    Interference                            : Enable
    Load                                    : Disable
    Device Aware                            : Disable
  CleanAir Event-driven RRM option          : Disabled
  Channel Assignment Leader                 : ewlc-doc (9.12.32.10)
  Last Run                                  : 550 seconds ago

  DCA Sensitivity Level                     : MEDIUM : 10 dB
  DCA Minimum Energy Limit                  : -95 dBm
  Channel Energy Levels
```

```
    Minimum                                 : unknown
    Average                                 : unknown
    Maximum                                 : -128 dBm
  Channel Dwell Times
    Minimum                                 : unknown
    Average                                 : unknown
    Maximum                                 : unknown
  802.11b 2.4 GHz Auto-RF Channel List
    Allowed Channel List                    : 1,6,11
    Unused Channel List                     : 2,3,4,5,7,8,9,10


------------------ show ap dot11 5ghz channel ------------------


Leader Automatic Channel Assignment
  Channel Assignment Mode                   : AUTO
  Channel Update Interval                   : 600 seconds
  Anchor time (Hour of the day)             : 0
  Channel Update Contribution
    Noise                                   : Enable
    Interference                            : Enable
    Load                                    : Disable
    Device Aware                            : Disable
  CleanAir Event-driven RRM option          : Disabled
  Channel Assignment Leader                 : ewlc-doc (9.12.32.10)
  Last Run                                  : 552 seconds ago

  DCA Sensitivity Level                     : MEDIUM : 15 dB
  DCA 802.11n/ac Channel Width              : 20 MHz
  DCA Minimum Energy Limit                  : -95 dBm
  Channel Energy Levels
    Minimum                                 : unknown
    Average                                 : unknown
    Maximum                                 : -128 dBm
  Channel Dwell Times
    Minimum                                 : unknown
    Average                                 : unknown
    Maximum                                 : unknown
  802.11a 5 GHz Auto-RF Channel List
    Allowed Channel List                    :
36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,144,149,153,157,161
    Unused Channel List                     : 165


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


------------------ show ap dot11 24ghz group ------------------


Radio RF Grouping

  802.11b Group Mode               : AUTO
  802.11b Group Update Interval    : 600 seconds
  802.11b Group Leader             : ewlc-doc (9.12.32.10)
  802.11b Last Run                 : 553 seconds ago


RF Group Members

Controller name                   Controller IP
-------------------------------------------------
ewlc-doc                          9.12.32.10




------------------ show ap dot11 5ghz group ------------------


Radio RF Grouping

  802.11a Group Mode               : AUTO
  802.11a Group Update Interval    : 600 seconds
  802.11a Group Leader             : ewlc-doc (9.12.32.10)
  802.11a Last Run                 : 553 seconds ago


RF Group Members

Controller name                   Controller IP
-------------------------------------------------
ewlc-doc                          9.12.32.10




------------------ show ap dot11 24ghz high-density ------------------


------------------ show ap dot11 5ghz high-density ------------------


------------------ show ap dot11 5ghz load-info ------------------


------------------ show ap dot11 24ghz load-info ------------------
```

```
------------------ show ap dot11 24ghz profile ------------------


Default 802.11b AP performance profiles
  802.11b Global Interference threshold    : 10 %
  802.11b Global noise threshold           : -70 dBm
  802.11b Global RF utilization threshold  : 80 %
  802.11b Global throughput threshold      : 1000000 bps
  802.11b Global clients threshold         : 12 clients


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


------------------ show ap dot11 24ghz monitor ------------------


Default 802.11b AP monitoring
  802.11b Monitor Mode                 : Enabled
  802.11b Monitor Channels             : Country channels
  802.11b RRM Neighbor Discover Type   : Transparent
  802.11b AP Coverage Interval         : 180 seconds
  802.11b AP Load Interval             : 60 seconds
  802.11b AP Noise Interval            : 180 seconds
  802.11b AP Signal Strength Interval  : 60 seconds
  802.11b NDP RSSI Normalization       : Enabled


------------------ show ap dot11 5ghz monitor ------------------


Default 802.11a AP monitoring
  802.11a Monitor Mode                 : Enabled
  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
  802.11a NDP RSSI Normalization       : Enabled


------------------ show ap dot11 24ghz network ------------------



802.11b Network                          : Enabled
11gSupport                               : Enabled
11nSupport                               : Enabled
802.11b/g Operational Rates
  802.11b 1M                             : Mandatory
```

```
  802.11b 2M                                : Mandatory
  802.11b 5.5M                              : Mandatory
  802.11b 11M                               : Mandatory
  802.11g 6M                                : Supported
  802.11g 9M                                : Supported
  802.11g 12M                               : Supported
  802.11g 18M                               : Supported
  802.11g 24M                               : Supported
  802.11g 36M                               : Supported
  802.11g 48M                               : Supported
  802.11g 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
  MCS 24 : Supported
  MCS 25 : Supported
  MCS 26 : Supported
  MCS 27 : Supported
  MCS 28 : Supported
  MCS 29 : Supported
  MCS 30 : Supported
  MCS 31 : 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
    Aggregation scheduler                   : Enabled
    Realtime timeout                        : 10
  A-MSDU Tx:
    Priority 0                              : Enable
    Priority 1                              : Enable
    Priority 2                              : Enable
    Priority 3                              : Enable
    Priority 4                              : Enable
    Priority 5                              : Enable
    Priority 6                              : Disable
```

```
    Priority 7                              : Disable
  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                             : 1
Default Tx Power Level                      : 1
DTPC Status                                 : Enabled
Call Admission Limit                        :
G711 CU Quantum                             :
ED Threshold                                : -50
Fragmentation Threshold                     : 2346
RSSI Low Check                             : Disabled
RSSI Threshold                              : -127 dbm
PBCC Mandatory                              : unknown
Pico-Cell-V2 Status                         : unknown
RTS Threshold                               : 2347
Short Preamble Mandatory                    : Enabled
Short Retry Limit                           : 7
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
Maximum Number of Clients per AP Radio      : 200


------------------ 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
  MCS 24 : Supported
  MCS 25 : Supported
  MCS 26 : Supported
  MCS 27 : Supported
  MCS 28 : Supported
  MCS 29 : Supported
  MCS 30 : Supported
  MCS 31 : 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
    Aggregation scheduler               : Enabled
    Realtime timeout                    : 10
  A-MSDU Tx:
    Priority 0                          : Enable
    Priority 1                          : Enable
    Priority 2                          : Enable
    Priority 3                          : Enable
    Priority 4                          : Enable
    Priority 5                          : Enable
    Priority 6                          : Disable
    Priority 7                          : Disable
  Guard Interval                        : Any
  Rifs Rx                               : Enabled
802.11ac                                : Enabled
  Frame burst                           : Automatic
802.11ac MCS Settings:
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
```

```
RSSI Low Check                           : Disabled
RSSI Threshold                            : -127 dbm
Pico-Cell-V2 Status                       : unknown
TI Threshold                              :
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
Maximum Number of Clients per AP Radio    : 200


------------------ show ap dot11 24ghz 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
Update Contribution
    Noise                               : Enable
    Interference                        : Enable
    Load                                : Disable
    Device Aware                        : Disable
Transmit Power Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                                : 558 seconds ago


------------------ 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
Update Contribution
    Noise                               : Enable
    Interference                        : Enable
    Load                                : Disable
    Device Aware                        : Disable
Transmit Power Assignment Leader        : ewlc-doc (9.12.32.10)
Last Run                                : 558 seconds ago
```

```
------------------ show ap auto-rf dot11 5ghz ------------------


------------------ show ap auto-rf dot11 24ghz ------------------


------------------ show ap config general ------------------



------------------ show ap dot11 5ghz optimized-roaming ------------------

802.11a OptimizedRoaming

  Mode                                : Disabled
  Reporting Interval                  : 90 seconds
  Rate Threshold                      : Disabled
  Hysteresis                          : 6 db


------------------ show ap rf-profile summary ------------------



Number of RF-profiles: 6

RF Profile Name                  Band     Description                              State
------------------------------------------------------------------------------------------
Low_Client_Density_rf_5gh        5 GHz    pre configured Low Client Density rf Up
High_Client_Density_rf_5gh       5 GHz    pre configured High Client Density r Up
Low_Client_Density_rf_24gh       2.4 GHz  pre configured Low Client Density rf Up
High_Client_Density_rf_24gh      2.4 GHz  pre configured High Client Density r Up
Typical_Client_Density_rf_5gh    5 GHz    pre configured Typical Density rfpro Up
Typical_Client_Density_rf_24gh   2.4 GHz  pre configured Typical Client Densit Up


------------------ show ap fra ------------------

FRA State                                          : Disabled
FRA Sensitivity                                    : medium (95%)
FRA Interval                                       : 1 Hour(s)
  Last Run                                         : 2299 seconds ago
  Last Run time                                    : 0 seconds

AP Name              MAC Address       Slot ID  Current-Band      COF %      Suggested
Mode
------------------------------------------------------------------------------------------

COF : Coverage Overlap Factor


------------------ 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
Client Mid RSSI (dBm)        : -80
```

```
------------------ show wireless  country  configure ------------------


Configured Country.........................   US - United States

Configured Country Codes
        US  - United States                  802.11a Indoor/ 802.11b Indoor/ 802.11g
Indoor


------------------ show wireless tag rf summary ------------------


Number of RF Tags: 1

RF tag name                      Description
------------------------------------------------------------------------------
default-rf-tag                   default RF tag


------------------ show ap tag summary ------------------


Number of APs: 0


------------------ show ap status ------------------


------------------ show ap uptime ------------------


Number of APs: 0
```

show tunnel eogre global-configuration

Ethernet over GRE（EoGRE）のグローバル設定を表示するには、**show tunnel eogre global-configuration** コマンドを使用します。

show tunnel eogre global-configuration

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、EoGRE のグローバル設定を表示する例を示します。

```
Device# show tunnel eogre global-configuration

Heartbeat interval       : 60
Max Heartbeat skip count : 3
Source Interface         : (none)
```

show tunnel eogre domain detailed

Ethernet over GRE（EoGRE）トンネル ドメインの詳細情報を表示するには、**show tunnel eogre domain detailed** コマンドを使用します。

show tunnel eogre domain detailed *domain-name*

構文の説明

domain-name	EoGRE ドメイン名。

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、EoGRE トンネル ドメインの詳細情報を表示する例を示します。

```
Device# show tunnel eogre domain detailed eogre_domain

Domain Name    : eogre_domain
 Primary GW    : Tunnel1
 Secondary GW  : Tunnel2
 Active GW     : Tunnel1
 Redundancy    : Non-Revertive
```

show tunnel eogre domain summary

Ethernet over GRE（EoGRE）トンネル ドメインのサマリー情報を表示するには、**show tunnel eogre domain summary** コマンドを使用します。

show tunnel eogre domain 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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、EoGRE トンネル ドメインのサマリー情報を表示する例を示します。

```
Device# show tunnel eogre domain summary

Domain Name          Primary GW   Secondary GW      Active GW      Redundancy
-------------------------------------------------------------------------------
domain1              Tunnel1      Tunnel2           Tunnel1        Non-Revertive
eogre_domain         Tunnel1      Tunnel2           Tunnel1        Non-Revertive
```

show tunnel eogre gateway summary

Ethernet over GRE（EoGRE）トンネル ゲートウェイのサマリー情報を表示するには、**show tunnel eogre gateway summary** コマンドを使用します。

show tunnel eogre gateway 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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、EoGRE トンネル ゲートウェイのサマリー情報を表示する例を示します。

```
Device# show tunnel eogre gateway summary

Name               Type  Address                                  AdminState  State
Clients
-------------------------------------------------------------------------------------------
Tunnel1            IPv4  9.51.1.11                                Up          Up      0

Tunnel2            IPv4  9.51.1.12                                Up          Down    0

Tunnel10           IPv6  fd09:9:8:21::90                          Down        Down    0

Tunnel11           IPv4  9.51.1.11                                Up          Up      0

Tunnel12           IPv6  fd09:9:8:21::90                          Up          Down    0

Tunnel100          IPv4  9.51.1.100                               Up          Down    0
```

show tunnel eogre gateway detailed

Ethernet over GRE（EoGRE）トンネル ドメインの詳細情報を表示するには、**show tunnel eogre gateway detailed** コマンドを使用します。

show tunnel eogre gateway detailed *gateway-name*

構文の説明

gateway-name	EoGRE ゲートウェイ名。

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、EoGRE トンネル ゲートウェイの詳細情報を表示する例を示します。

```
Device# show tunnel eogre domain detailed Tunnel1

Gateway : Tunnel1
 Mode   : IPv4
 IP     : 9.51.1.11
 Source : Vlan51 / 9.51.1.1
 State  : Up
 SLA ID : 56
 MTU    : 1480
 Up Time: 4 minutes 45 seconds

 Clients
  Total Number of Wireless Clients      : 0
 Traffic
  Total Number of Received Packets      : 0
  Total Number of Received Bytes        : 0
  Total Number of Transmitted Packets   : 0
  Total Number of Transmitted Bytes     : 0
 Keepalives
  Total Number of Lost Keepalives       : 0
  Total Number of Received Keepalives   : 5
  Total Number of Transmitted Keepalives: 5
  Windows                               : 1
  Transmitted Keepalives in last window : 2
  Received Keepalives in last window    : 2
```

show tunnel eogre manager stats global

グローバル トンネル マネージャの統計情報を表示するには、**show tunnel eogre manager stats global** コマンドを使用します。

show tunnel eogre manager stats global

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次の例では、グローバル トンネルマネージャの統計情報を表示する方法を示します。

```
Device# show tunnel eogre manager stats global

Tunnel Global Statistics
Last Updated                     : 02/18/2019 23:50:35
EoGRE Objects
  Gateways                       : 6
  Domains                        : 2

EoGRE Flex Objects
  AP Gateways                    : 2
  AP Domains                     : 1
  AP Gateways HA inconsistencies : 0
  AP Domains HA inconsistencies  : 0

Config events
  IOS Tunnel updates             : 806
  IOS Domain updates             : 88
  Global updates                 : 48
  Tunnel Profile updates         : 120
  Tunnel Rule updates            : 16
  AAA proxy key updates          : 0

AP events
  Flex AP Join                   : 1
  Flex AP Leave                  : 0
  Local AP Join                  : 0
  Local AP leave                 : 0
  Tunnel status (rx)             : 4
  Domain status (rx)             : 1
  IAPP stats msg (rx)            : 3
  Client count (rx)              : 6
  VAP Payload msg (tx)           : 4
  Domain config (tx)             : 1
  Global config (tx)             : 1
```

```
  Client delete (tx)              : 1
  Client delete per domain (tx)   : 3
  DHCP option 82 (tx)             : 4

Client events
  Add-mobile                      : 2
  Run-State                       : 3
  Delete                          : 1
  Cleanup                         : 0
  Join                            : 2
  Plumb                           : 0
  Join Errors                     : 0
  HandOff                         : 0
  MsPayload                       : 2
  FT Recover                      : 0
  Zombie GW counter increase      : 0
  Zombie GW counter decrease      : 0
  Tunnel Profile reset            : 88
  Client deauth                   : 0
  HA reconciliation               : 0

Client Join Events
  Generic Error                   : 0
  MSPayload Fail                  : 0
  Invalid VLAN                    : 0
  Invalid Domain                  : 0
  No GWs in Domain                : 0
  Domain Shut                     : 0
  Invalid GWs                     : 0
  GWs Down                        : 0
  Rule Match Error                : 0
  AAA-override                    : 0
  Flex No Active GW               : 0
  Open Auth join attempt          : 2
  Dot1x join attempt              : 2
  Mobility join attempt           : 0
  Tunnel Profile not valid        : 2
  Tunnel Profile valid            : 2
  No rule match                   : 0
  Rule match                      : 2
  AAA proxy                       : 0
  AAA proxy accounting            : 0
  AAA eogre attributes            : 0
  Has aaa override                : 0
  Error in handoff payload        : 0
  Handoff AAA override            : 0
  Handoff no AAA override         : 0
  Handoff payload received        : 0
  Handoff payload sent            : 0

SNMP Traps
  Client                          : 0
  Tunnel                          : 2
  Domain                          : 0

IPC
  IOSd TX messages                : 0

Zombie Client
  Entries                         : 0
```

show tunnel eogre manager stats instance

特定の WNCd インスタンスのトンネルマネージャ統計情報を表示するには **show tunnel eogre manager stats instance** 、コマンドを使用します。

show tunnel eogre manager stats instance *instance-number*

構文の説明

instance-number	WNCd インスタンス番号。

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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、特定のWNCdインスタンスのトンネルマネージャの統計情報を表示する例を示します。

```
Device# show tunnel eogre manager stats instance 0

Tunnel Manager statistics for process instance : 0
Last Updated                     : 02/18/2019 23:50:35
EoGRE Objects
  Gateways                       : 6
  Domains                        : 2

EoGRE Flex Objects
  AP Gateways                    : 2
  AP Domains                     : 1
  AP Gateways HA inconsistencies : 0
  AP Domains HA inconsistencies  : 0

Config events
  IOS Tunnel updates             : 102
  IOS Domain updates             : 11
  Global updates                 : 6
  Tunnel Profile updates         : 15
  Tunnel Rule updates            : 2
  AAA proxy key updates          : 0

AP events
  Flex AP Join                   : 1
  Flex AP Leave                  : 0
  Local AP Join                  : 0
  Local AP leave                 : 0
  Tunnel status (rx)             : 4
  Domain status (rx)             : 1
  IAPP stats msg (rx)            : 3
```

```
  Client count (rx)              : 6
  VAP Payload msg (tx)           : 4
  Domain config (tx)             : 1
  Global config (tx)             : 1
  Client delete (tx)             : 1
  Client delete per domain (tx)  : 3
  DHCP option 82 (tx)            : 4

Client events
  Add-mobile                     : 2
  Run-State                      : 3
  Delete                         : 1
  Cleanup                        : 0
  Join                           : 2
  Plumb                          : 0
  Join Errors                    : 0
  HandOff                        : 0
  MsPayload                      : 2
  FT Recover                     : 0
  Zombie GW counter increase     : 0
  Zombie GW counter decrease     : 0
  Tunnel Profile reset           : 11
  Client deauth                  : 0
  HA reconciliation              : 0

Client Join Events
  Generic Error                  : 0
  MSPayload Fail                 : 0
  Invalid VLAN                   : 0
  Invalid Domain                 : 0
  No GWs in Domain               : 0
  Domain Shut                    : 0
  Invalid GWs                    : 0
  GWs Down                       : 0
  Rule Match Error               : 0
  AAA-override                   : 0
  Flex No Active GW              : 0
  Open Auth join attempt         : 2
  Dot1x join attempt             : 2
  Mobility join attempt          : 0
  Tunnel Profile not valid       : 2
  Tunnel Profile valid           : 2
  No rule match                  : 0
  Rule match                     : 2
  AAA proxy                      : 0
  AAA proxy accounting           : 0
  AAA eogre attributes           : 0
  Has aaa override               : 0
  Error in handoff payload       : 0
  Handoff AAA override           : 0
  Handoff no AAA override        : 0
  Handoff payload received       : 0
  Handoff payload sent           : 0

SNMP Traps
  Client                         : 0
  Tunnel                         : 2
  Domain                         : 0

IPC
  IOSd TX messages               : 0

Zombie Client
  Entries                        : 0
```

show umbrella config

Umbrella 設定の詳細を表示するには、**show umbrella config** コマンドを使用します。

show umbrella config

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、Umbrella 設定の詳細を表示する例を示します。

```
デバイス# show umbrella config
Umbrella Configuration
=======================
   Token: 57CC80106C087FB1B2A7BAB4F2F4373C00247166
   OrganizationID: 1892929
   Local Domain Regex parameter-map name: dns_wl
   DNSCrypt: Enabled
   Public-key:
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
   UDP Timeout: 2 seconds
   Resolver address:
       1. 208.67.220.220
       2. 208.67.222.222
       3. 2620:119:53::53
       4. 2620:119:35::35
```

show umbrella deviceid

デバイス登録の詳細を表示するには、**show umbrella deviceid** コマンドを使用します。

show umbrella deviceid

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、デバイス登録の詳細を表示する例を示します。

```
デバイス# show umbrella deviceid
Device registration details
Profile Name             Tag             Status            Device-id
GigabitEthernet0/0/0    guest          200 SUCCESS     010a470b042a072d
```

show umbrella deviceid detailed

Umbrella デバイス ID の詳細な説明を表示するには、**show umbrella deviceid detailed** コマンドを使用します。

show umbrella deviceid *detailed*

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、Umbrella デバイス ID の詳細な説明を表示する例を示します。

```
デバイス# show umbrella deviceid detailed
Device registration details
 1.GigabitEthernet0/0/0
      Tag               : guest
      Device-id         : 010a470b042a072d
      Description       : Device Id recieved successfully
```

show umbrella dnscrypt

Umbrella DNScrypt の詳細を表示するには、**show umbrella dnscrypt** コマンドを使用します。

show umbrella dnscrypt

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、Umbrella DNScrypt の詳細を表示する例を示します。

```
デバイス# show umbrella dnscrypt
DNSCrypt: Enabled
   Public-key:
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
   Certificate Update Status:
        Last Successfull Attempt: 17:45:57 IST Nov 9 2017
   Certificate Details:
       Certificate Magic     : DNSC
       Major Version         : 0x0001
       Minor Version         : 0x0000
       Query Magic           : 0x713156774457306E
       Serial Number         : 1490391488
       Start  Time           : 1490391488 (03:08:08 IST Mar 25 2017)
       End Time              : 1521927488 (03:08:08 IST Mar 25 2018)
       Server Public Key     :
E7F8:4477:BF89:1434:1ECE:23F0:D6A6:6EB9:4F45:3167:D71F:80BB:4E80:A04F:F180:F778
       Client Secret Key Hash:
F1A5:1993:F729:5416:53B7:94E3:6509:8182:A708:0561:8050:6CE0:DFA1:5C94:6EE4:0010
       Client Public key     :
BC6D:3758:48B6:120B:D2F5:F25B:2979:564D:F52C:5EFA:B0BD:76FE:3CD6:828B:44D2:FF3A
       NM key Hash           :
1FF7:2E1E:EFB9:7987:9CB4:3EF8:A25B:4DAD:10FC:7DF7:6985:6E8E:6E4D:D56A:1C70:B9EB
```

show vlan

設定されたすべての VLAN またはスイッチ上の 1 つの 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** | **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。
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。 （注） Controller-PI が各インターフェイスの VLAN ルックアップを行うときに、VLAN CLI パーサーでトレースバックが発生します。
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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

次に、**show vlan** 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。

```
デバイス> 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 *26 : 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。
Name	VLAN の名前（設定されている場合）。
Status	VLAN のステータス（active または suspend）。
Ports	VLAN に属するポート。
Type	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。
Parent	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。

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

```
デバイス> show vlan summary
Number of existing VLANs              : 45
 Number of existing VTP VLANs         : 45
 Number of existing extended VLANS    : 0
```

次に、**show vlan id** コマンドの出力例を示します。

```
デバイス# 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
```

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、**show vlan access-map** コマンドの出力例を示します。

```
デバイス# 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
```

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 Gibraltar 16.10.1	このコマンドが導入されました。

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

```
デバイス# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

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。

show vrrp events

Virtual Router Redundancy Protocol（VRRP）イベントを表示するには、**show vrrp events** コマンドを使用します。

show vrrp events

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 Amsterdam 17.2.1	このコマンドが導入されました。

使用上のガイドライン

VRRP コマンドは、ME モードでのみ表示されます。他の AP モードでは非表示になります。

例

次に、VRRP イベントを表示する例を示します。

```
Device# show vrrp events

VRRP Events:
Dec 7 2019 01:17:23: Current state : backup, My Eth : A4:53:0E:7B:CD:84, event : VRRP
Element is started. Start
sending KeepAlive Pkts to check if Ether link is up
Dec 7 2019 01:17:28: Current state : backup, My Eth : A4:53:0E:7B:CD:84, event : Detected
 Link is up. Now
waiting for 30 seconds to participate in VRRP election
Dec 7 2019 01:18:01: Current state : master, My Eth : A4:53:0E:7B:CD:84, event : Current
 master
(00:00:00:00:00:00) went down (lost 3 advertisement). Moving to master state. And starting
 election
Dec 7 2019 01:18:05: Current state : master, My Eth : A4:53:0E:7B:CD:84, event : Launched
 controller process on
this ap
```

show vrrp statistics

Virtual Router Redundancy Protocol（VRRP）の統計を表示するには、特権 EXEC モードで **show vrrp statistics** コマンドを使用します。

show vrrp statistics

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 Amsterdam 17.2.1	このコマンドが導入されました。

使用上のガイドライン

VRRP コマンドは、ME モードでのみ表示されます。他の AP モードでは非表示になります。

例

次に、VRRP の統計を表示する例を示します。

```
Device# show vrrp statistics

VRRP Statistics :
VRRP Statistics :
Invalid VRRP packets recvd:0
Number of incoming VRRP Pkts:0
Number of VRRP Pkts transmitted:148054
Number of VRRP Pkts recvd from Master:0
Number of VRRP Pkts recvd in Init state:0
Number of VRRP Pkts with STOP Priority:0
```

show vrrp status

Virtual Router Redundancy Protocol（VRRP）ステータスを表示するには、**show vrrp status** コマンドを使用します。

show vrrp status

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 Amsterdam 17.2.1	このコマンドが導入されました。

使用上のガイドライン

VRRP コマンドは、ME モードでのみ表示されます。他の AP モードでは非表示になります。

例

次に、VRRP ステータスを表示する例を示します。

```
Device# show vrrp status

 VRRP Status : MASTER
Preferred AP : 00:00:00:00:00:00
My Eth : A4:53:0E:7B:CD:84
AP Type : VANCOUVER
VRRP Instance : vrid state priority vrrp_ip_vlans adver_ival
1 master 1 0.0.0.0:0 3.000000
```

show wireless stats ap history

AP の履歴統計を確認するには、**show wireless stats ap history** コマンドを使用します。

show wireless stats ap history

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 Cupertino 17.7.1	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履歴の統計を確認する例を示します。

```
Device# show wireless stats ap history
AP Name             Radio MAC       Event      Time               Recent      Disconnect
 Reason          Disconnect
                                                                    Disconnect  Reason
                  Count
                                                                    Time
-------------------------------------------------------------------------------------------
APA023.9FD8.EA22   40ce.24bf.8ca0  Joined     06/26/21 10:11:52  NA           NA
                  NA
APA023.9FD8.EA22   40ce.24bf.8ca0  Disjoined  06/26/21 10:05:18  NA          Heart beat
 timer expiry    1
APA023.9FD8.EA22   40ce.24bf.8ca0  Joined     06/22/21 17:00:39  NA           NA
                  NA
APA023.9FD8.EA22   40ce.24bf.8ca0  Disjoined  06/22/21 16:54:54  NA          Heart beat
 timer expiry    1
APA023.9FD8.EA22   40ce.24bf.8ca0  Joined     06/21/21 23:01:17  NA           NA
                  NA
APA023.9FD8.EA22   40ce.24bf.8ca0  Disjoined  06/21/21 22:56:21  NA           Image
Download Success     1
```

show wireless stats ap join summary

アクセスポイントの参加の概要の統計を確認するには、**show wireless stats ap join summary** コマンドを使用します。

show wireless stats ap join 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 Cupertino 17.7.1	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参加の概要の統計を確認する例を示します。

```
Device# show wireless stats ap join summary
Number of APs: 001

Base MAC        Ethernet MAC    AP Name           IP Address  Status  Last
Last
                                                                      Failure Phase
Disconnect Reason
-----------------------------------------------------------------------------------------------------
002a.1075.47c0  002a.104d.c9fc  AP002a.104d.c9fc  8.9.10.222  Joined   Run
High CPU usage
003a.1475.57c0  002a.104d.c9fc  AP003a.144d.59fc  7.8.09.111  Joined   Run
High Memory usage
```

show wireless stats ap join summary sort

ソートされたワイヤレス統計のアクセスポイント（AP）の参加の概要を表示するには、**show wireless stats ap join summary sort** コマンドを使用します。

show wireless stats ap join summary sort

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 Cupertino 17.7.1	このコマンドが導入されました。

使用上のガイドライン

ワイヤレス AP の統計は、AP 名の昇順または降順でソートできます。

- 昇順：下から 10 個の AP を表示します。
- 降順：上から AP を表示します。
- 名前：名前でソートされた AP リストを表示します。

例

次に、ソートされたワイヤレス統計の AP の参加の概要を表示する例を示します。

```
Device# show wireless stats ap join summary sort
Number of APs: 8

Base MAC        Ethernet MAC      AP Name                             IP Address   Status
  Last Failure Phase Last Disconnect Reason
-----------------------------------------------------------------------------------------
7872.5dee.4960  7872.5ded.cb74   4800-abcdefghijklmnopqrstuvwxyz1   1.11.22.11  Joined
 Image-Download     Image Download Success
10f9.2077.6140  10f9.2076.2c58   9105-abcdefghijklmnopqrstuvwxyz1   1.11.22.11  Joined
 Image-Download     Image Download Success
00ee.ab18.bf00  7069.5a74.9670   9115-abcdefghijklmnopqrstuvwxyz1   1.11.22.11  Joined
 Image-Download     Image Download Success
1416.9d82.ef40  2c57.4152.5e60   9130-abcdefghijklmnopqrstuvwxyz1   1.11.22.11  Joined
 Image-Download     Image Download Success
00d7.8f4e.7040  002a.1087.d68a   AP2800                              1.11.22.11  Joined
 Config             DTLS close alert from peer
687d.b45e.3ed0  687d.b45c.0554   AP687D.B45C.0554                    1.11.22.11  Joined
 Image-Download     Image Download Success
687d.b45e.4c50  687d.b45c.0674   AP687D.B45C.0674                    1.11.22.11  Joined
 Config             DTLS close alert from peer
687d.b45e.53d0  687d.b45c.0714   AP687D.B45C.0714                    1.11.22.11  Joined
 Config             DTLS close alert from peer
```

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 Gibraltar 16.10.1	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。

```
デバイス# 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 certification config

ワイヤレス認定設定の概要を表示するには、**show wireless certification config** コマンドを使用します。

show wireless cerification config

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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、ワイヤレス認定設定の概要を表示する例を示します。

```
Device# show wireless certification config
Wireless Certification Configurations

WLANCC                                    : Not Configured
FIPS                                      : Not Configured

AP DTLS Version                           : DTLS v1.0 - v1.2
AP DTLS Cipher Suite List:

                          Ciphersuite (Implicit list)
--------------------------------------------------------------------------------
                          AES128-SHA
                          DHE-RSA-AES128-SHA
                          DHE-RSA-AES256-SHA
                          DHE-RSA-AES256-SHA256
                          ECDHE-RSA-AES128-GCM-SHA256
                          ECDHE-ECDSA-AES128-GCM-SHA256
                          ECDHE-ECDSA-AES256-GCM-SHA384
The output can vary depending on the various security modes and AP DTLS configurations.
```

show wireless client

分類されたデバイスの概要を表示するには、**show wireless client** コマンドを使用します。

show wireless client device {**cache** | **count** | **summary** } | **{steering**}[{**chassis**{*chassis-number* | **active** | **standby** }}]**R0**

構文の説明

device	分類されたデバイスを表示します。
steering	ワイヤレス クライアントのステアリング情報
cache	キャッシュされた分類済みデバイスの概要を表示します。
count	ワイヤレス デバイスの数を表示します。
summary	アクティブな分類済みデバイスの概要を表示します。
chassis-number	シャーシ番号。有効な範囲は 1 ～ 2 です。
active	アクティブ インスタンス。
standby	スタンバイ インスタンス。
R0	ルートプロセッサ スロット 0。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、分類済みデバイスの概要を表示する例を示します。

```
Device# show wireless client device summary
```

show wireless client mac-address

mac アドレスを使用してクライアントの詳細情報を表示するには、 **show wireless client mac-addressdetail** コマンドを使用します。

show wireless client mac-address *mac-address* **detail** ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

mac-address	Client MAC address.
chassis-number	シャーシ番号。有効な範囲は 1 ～ 2 です。
active	アクティブ インスタンス。
standby	スタンバイ インスタンス。
R0	ルートプロセッサ スロット 0。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

show wireless client mac-address detail の出力の Client Scan Reports セクションは、次の Apple デバイスに対してのみ入力されます。

- iPhone 7 以降の iOS 11.0 以降を実行している iPhone
- iPad Pro（第 1 世代、12.9 インチ、2015 年）以降の iOS 11.0 以降を実行している iPad

他のクライアントデバイスでは、802.11k がサポートされている場合や、Wi-Fi Agile Multiband（MBO）認定されている場合でも、Client Scan Reports セクションへの入力は現在サポートされていません。

show wireless client mac-address <*mac address*> **detail** で表示されるクライアントの ACL は、AAA オーバーライドが有効になっている MAB+Web 認証 WLAN を使用した FlexConnect ローカル認証のケースでクライアントに適用されている ACL です。これは、コントローラの Express Wi-Fi by Facebook ポリシーにのみ適用されます。Facebook ポリシーの詳細については、「Express Wi-Fi by Facebook」を参照してください。

Cisco IOS XE Amsterdam 17.3.1 以降、コントローラはクライアントセッションを 10 秒間保持します。この機能は RUN 状態のクライアントに適用され、ローカルおよびフレックスモードの中央認証でサポートされます。

アイドル状態では、10 sec はアイドル状態のタイムアウトを表し、09 sec は 10 sec のうちの残り時間を表します。次に例を示します。

```
Idle state timeout : 10 sec (Remaining time: 09 sec)
```

例

次に、MAC アドレスを使用して詳細なクライアント情報を表示する例を示します。

```
Device# show wireless client mac-address 98-XX-7B-XX-EF-XX detail
```

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-control call-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 Gibraltar 16.10.1	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。

```
デバイス# 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 **show wireless client mac-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 Gibraltar 16.10.1	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。

```
デバイス# 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 mac-address mobility history

サブドメイン内のアクティブなクライアントのローミング履歴を表示するには、**show wireless client mac-address** *mac-address* **mobility history** コマンドを使用します。

show wireless client mac-address *mac-address* **mobility history**[{**chassis** {*chassis-number* | **active** | **standby**} **R0**] | **events** [**chassis** {*chassis-number* | **active** | **standby**} **R0**]}]

構文の説明

mac-address	クライアントの MAC アドレス。
chassis-number	シャーシ番号（1 または 2 のいずれか）。
active R0	ルートプロセッサ スロット 0 のクライアントのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 のクライアントのスタンバイ インスタンス。
events	クライアントの FSM イベント履歴を表示します。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、サブドメイン内のアクティブなクライアントのローミング履歴を表示する例を示します。

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 mobility history
```

show wireless client mac-address stats latency

クライアントの MAC アドレスを使用してワイヤレスクライアントの統計を表示するには、**show wireless client mac-address** *mac-address* **stats latency** コマンドを使用します。

show wireless client mac-address *mac-address* **stats latency** ［ **chassis** { *chassis-number* | **active** | **standby** } **R0** ］

構文の説明

mac-address	Client MAC address.
stats	ワイヤレスクライアントの MAC アドレスの統計を指定します。
latency	ワイヤレスクライアントの MAC アドレスの遅延統計を指定します。
chassis	遅延統計のシャーシを指定します。
chassis-number	シャーシ番号（1 または 2 のいずれか）。
active	アクティブインスタンスを指定します。
standby	スタンバイインスタンスを指定します。
R0	スロット 0 のルートプロセッサを指定します。

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 Dublin 17.11.1	このコマンドが導入されました。

例

次に、MACアドレスを使用してワイヤレスクライアントの統計を表示する例を示します。

```
Device# show wireless client mac-address aaaa.bbbb.cccc stats latency
```

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

次に、**show wireless client summary** コマンドの出力例を示します。

除外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。

```
Device# show wireless client summary

Number of Clients: 1

MAC Address       AP Name                 Type ID  State  Protocol  Method  Role
------------------------------------------------------------------------------
6c40.0899.0466    9115i-r4-sw2-te1-0-37   WLAN 7   Run    11ac      None    Local
```

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 Gibraltar 16.10.1	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。

```
デバイス# show wireless client timers
 Authentication Response Timeout (seconds)      : 10
```

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。
supported tx-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 Gibraltar 16.10.1	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。

```
デバイス# 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。

```
デバイス# 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。

```
デバイス# 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 Gibraltar 16.10.1	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
- 高速 SSID 変更

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

```
デバイス# show wireless detail
User Timeout               : 300
RF network                 : default
Fast SSID                  : Disabled
```

show wireless dhcp relay statistics

AP でワイヤレス DHCP リレーを設定するには、**show wireless dhcp relay statistic** コマンドを使用します。

show wireless dhcp relay statistic

構文の説明

A.B.C.D	ターゲット IPv4 アドレスを示します。

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 Gibraltar 17.3.1	このコマンドが導入されました。

例

次に、AP でワイヤレス DHCP リレーを設定する例を示します。

```
Device# show wireless dhcp relay statistics ip-address 10.1.1.1
```

show wireless dot11h

802.11h 設定の詳細を表示するには、**show wireless dot11h** コマンドを使用します。

show wireless dot11h [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

構文の説明

chassis-number	シャーシ番号。有効な範囲は1～2です。
active	アクティブ インスタンス。
standby	スタンバイ インスタンス。
R0	ルートプロセッサ スロット 0。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、802.11h 設定の詳細を表示する例を示します。

```
Device# show wireless dot11h
```

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 Gibraltar 16.10.1	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。

```
デバイス# 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 exclusionlist

無線の除外リストを表示するには、**show wireless exclusionlist** コマンドを使用します。

show wireless exclusionlist [{**client mac-address** *client-mac-addr* **detail** }] ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

client-mac-addr	Client MAC address.
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の設定のアクティブ インスタンス。
standby R0	ルートプロセッサスロット 0 の設定のスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。
Cisco IOS XE Cupertino 17.9.1	コマンドの出力が変更され、ARP アクティビティ情報が含まれるようになりました。

例

次に、ワイヤレスの除外リストを表示する例を示します。

```
Device# show wireless exclusionlist

Excluded Clients

MAC Address       Description          Exclusion Reason               Time Remaining
---------------------------------------------------------------------------------------
10da.4320.cce9                         Client Policy  failure          59
```

次に、Cisco IOS XE Cupertino 17.9.x 以降、Client Policy failure から Excess ARP activity に変更されたクライアントの除外理由の例を示します。

```
Device# show wireless exclusionlist


MAC Address       Description         Exclusion Reason               Time Remaining
-------------------------------------------------------------------------------------
6c96.cff2.889a                        Excess ARP activity             53
```

show wireless exclusionlist client mac-address detail

アクティブなクライアントの詳細情報を表示するには、**show wireless exclusionlist client mac-address detail** コマンドを使用します。

show wireless exclusionlist client mac-address *client-mac-addr* **detail**

構文の説明

client-mac-addr	クライアント MAC アドレス

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。
Cisco IOS XE Cupertino 17.9.1	コマンドの出力が変更され、ARP アクティビティ情報が含まれるようになりました。

例

次に、アクティブなクライアントの詳細情報を表示する例を示します。

```
Device# show wireless exclusionlist client mac-address 12da.4820.cce9 detail

Client State : Excluded
Client MAC Address : 12da.4820.cce9
Client IPv4 Address: 20.20.20.6
Client IPv6 Address: N/A
Client Username: N/A
Exclusion Reason :  Client Policy  failure
Authentication Method : None
Protocol: 802.11ac
AP MAC Address : 58ac.780e.08f0
AP Name: charlie2
AP slot : 1
Wireless LAN Id : 2
Wireless LAN Name: mhe-ewlc
VLAN Id : 20
```

次に、アクティブなクライアントの詳細情報を表示する例を示します。ここでは、Cisco IOS XE Cupertino 17.9.x 以降、Client Policy failure から Excess ARP activity に変更された ARP レート制限の除外が表示されています。

```
Device# show wireless exclusionlist client mac-address 6c96.cff2.889a detail

Client State : Excluded
Client MAC Address : 6c96.cff2.889a
Client IPv4 Address: N/A
```

```
Client IPv6 Address: N/A
Client Username: N/A
Exclusion Reason : Excess ARP activity
Authentication Method : None
Protocol: 802.11ac
AP MAC Address : 4001.7aca.5680
AP Name: AP40CE.2485.D5E8
AP slot : 1
Wireless LAN Id : N/A
VLAN Id : 63
```

show wireless fabric summary

ファブリック ステータスを表示するには、**show wireless fabric summary** コマンドを使用します。

show wireless fabric summary

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、ファブリック ステータスを表示する例を示します。

```
デバイス# show wireless fabric summary
Fabric Status      : Enabled


Control-plane:
Name                              IP-address        Key
Status
-------------------------------------------------------------------------------------------
test-map                          10.12.13.14       test1                             Down


Fabric VNID Mapping:
  Name               L2-VNID        L3-VNID        IP Address             Subnet
 Control plane name
-------------------------------------------------------------------------------------------

  test1               12             10             10.6.8.9            255.255.255.236
    test2
```

show wireless fabric client summary

ファブリックが有効になっているワイヤレス クライアントの概要を表示するには、**show wireless fabric client summary** コマンドを使用します。

show wirelessvfabricvclientv 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ファブリックが有効になっているワイヤレス クライアントの概要を表示する例を示します。

```
Device# show wireless fabric client summary
```

show wireless fabric vnid mapping

すべての VNID マッピングの詳細を表示するには、**show wireless fabric vnid mapping** コマンドを使用します。

show wireless fabric vnid mapping

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、VNID マッピングの詳細を表示する例を示します。

```
デバイス# show wireless fabric vnid mapping
Fabric VNID Mapping:
  Name               L2-VNID        L3-VNID        IP Address              Subnet
Control plane name
------------------------------------------------------------------------------------------------------

  test1               12             10             10.6.8.9            255.255.255.236
    test2
```

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 **show wireless flow-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 Gibraltar 16.10.1	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。

```
デバイス# 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 Gibraltar 16.10.1	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。

```
デバイス# 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 Gibraltar 16.10.1	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 mesh ap fabric summary

メッシュ AP ファブリックの概要を表示するには、**show wireless mesh ap fabric summary** コマンドを使用します。

show wireless mesh ap fabric 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 Dublin 17.12.1	このコマンドが導入されました。

例

次に、メッシュ AP ファブリックの概要を表示する例を示します。

```
Device# show wireless mesh ap fabric summary
```

show wireless media-stream client detail

ストリーム名別にメディア ストリーム クライアント情報を表示するには、 **show wireless media-stream client detail** コマンドを使用します。

show wireless media-stream client detail

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ストリーム名別にメディア ストリーム クライアント情報を表示する例を示します。

```
Device# show wireless media-stream client detail
```

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

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。

```
デバイス#show wireless media-stream group detail GRP1
```

```
デバイス#show wireless media-stream group detail GRP1
Media Stream Name : GRP1
Start IP Address : 234.1.1.1
End IP Address : 234.1.1.5
RRC Parameters:
Avg Packet Size(Bytes) : 1200
Expected Bandwidth(Kbps) : 1000
Policy : Admitted
RRC re-evaluation : Initial
QoS : video
Status : Multicast-direct
```

次に、**show wireless media-stream group summary** コマンドの出力例を示します。

```
デバイス#show wireless media-stream group summary
Number of Groups:: 1
Stream Name          Start IP                                End IP
Status
------------------------------------------------------------------------------------------------
GRP1                 234.1.1.1                               234.1.1.5
 Enabled
```

show wireless media-stream message details

ワイヤレス マルチキャストダイレクト セッション アナウンス メッセージの詳細を表示するには、 **show wireless media-stream message details** コマンドを使用します。

show wireless media-stream message details

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス マルチキャストダイレクト セッション アナウンス メッセージの詳細を表示する例を示します。

```
Device# show wireless media-stream message details
```

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。

```
デバイス#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
```

show wireless media-stream multicast-direct state

ワイヤレス マルチキャストダイレクト設定の状態を表示するには、**show wireless media-stream multicast-direct state** コマンドを使用します。

show wireless media-stream multicast-direct state

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス マルチキャストダイレクト設定の状態を表示する例を示します。

```
Device# show wireless media-stream multicast-direct state
```

show wireless mesh ap

メッシュ AP 関連情報を表示するには、 **show wireless mesh ap** コマンドを使用します。

show wireless mesh ap { **summary** | **tree** | **backhaul** } [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

構文の説明

summary	接続されているすべてのメッシュ AP の概要を表示します。
tree	メッシュ AP ツリーを表示します。
backhaul	メッシュ AP バックホール情報を表示します。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 の設定のアクティブ インスタンス。
standby R0	ルートプロセッサスロット 0 の設定のスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、接続されているすべてのメッシュ AP の概要を表示する例を示します。

```
Device# show wireless mesh ap summary
```

show wireless mesh ap summary

接続されているすべてのメッシュ AP の概要を表示するには、 **show wireless mesh ap summary** コマンドを使用します。

show wireless mesh ap summary ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

summary	接続されているすべてのメッシュ AP の概要を表示します。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 のアクティブな AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 のアクティブな AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、接続されているすべてのメッシュ AP の概要を表示する例を示します。

```
Device# wireless mesh ap summary
```

show wireless mesh ap tree

メッシュ AP ツリーを表示するには、**show wireless mesh ap tree** コマンドを使用します。

show wireless mesh ap tree

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、ワイヤレス メッシュ AP ツリーを表示する例を示します。

```
Device # show wireless mesh ap tree
```

show wireless mesh ap tree

メッシュ AP ツリーを表示するには、**show wireless mesh ap tree** コマンドを使用します。

show wireless mesh ap tree

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、ワイヤレス メッシュ AP ツリーを表示する例を示します。

```
Device # show wireless mesh ap tree
```

show wireless mesh cac summary

メッシュ ネットワーク内の AP の音声コールの合計数と帯域幅使用率を表示するには、**show wireless mesh cac summary** コマンドを使用します。

show wireless mesh cac 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 Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

例

次に、メッシュ ネットワーク内の AP の音声コールの合計数と帯域幅使用率を表示する例を示します。

```
Device# show wireless mesh cac summary


AP Name                           Slot  Radio      BW Used  Call
--------------------------------  ----  ---------  -------  ----
APA023.9FA9.B702                  0     802.11b/g  0        0
                                  1     802.11a    0        0
APA023.9FA9.D920                  0     802.11b/g  1140     2
                                  1     802.11a    0        0
AP380E.4DBF.C6A6                  0     802.11b/g  0        0
                                  1     802.11a    0        0
AP380E.4DBF.C80C                  0     802.11b/g  570      0
                                  1     802.11a    2144     2
AP380E.4DBF.C816                  0     802.11b/g  0        0
                                  1     802.11a    0        0
```

show wireless mesh config

メッシュ設定を表示するには、 **show wireless mesh config** コマンドを使用します。

show wireless mesh config ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

config	メッシュ設定を表示します。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 のアクティブな AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 のアクティブな AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、メッシュ設定を表示する例を示します。

```
Device# wireless mesh config
```

show wireless mesh rrm dca status

無線ごとに実行された最後の DCA のステータスを表示するには、**show wireless mesh rrm dca status** コマンドを使用します。

show wireless mesh rrm dca status

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 Cupertino 17.9.1	このコマンドが導入されました。

例

次に、無線ごとに実行された最後の DCA のステータスを表示する例を示します。

```
Device# show wireless mesh rrm dca status
```

show wireless mesh neighbor

接続されているすべてのメッシュ AP のネイバーを表示するには、**show wireless mesh neighbor** コマンドを使用します。

show wireless mesh neighbor ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

neighbor	接続されているすべてのメッシュ AP のネイバーを表示します。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 のアクティブな AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 のアクティブな AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 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

[State] フィールドの定義は次のとおりです。

- **UPDATED**：隣接関係は到達可能です。通信は対称的であり、その AP とフレームを交換できます。
- **NEIGH**：隣接関係は親に対応しています。ローカル基準：到達可能性、厳密な BGN 設定、有効なコスト、潜在的なループなど。
- **CHILD**：隣接関係は実際には子メッシュ AP です（対象の AP に関連付けられています）。
- **PARENT**：隣接関係は実際には親メッシュ AP です。
- **DEFAULT**：隣接関係 BGN が、バックホールで設定されたものと異なります。
- **BLOCK**：認証の失敗、capwap のティアダウンなどにより、隣接関係が現在ブロックリストに登録されています。

例

次に、接続されているすべてのメッシュ AP のネイバーを表示する例を示します。

```
Device# show wireless mesh neighbor

AP Name/Radio             Channel   Rate      Link-snr   Flags   State
-----------------------------------------------------------------------------------------------


AP Name : Mesh-AP01

54:9f:c6:fa:5c:71         149       auto      0          40
b0:c5:3c:e5:d9:71         149       auto      22         49      UPDATED NEIGH
e8:eb:34:d5:88:d1         149       auto      0          40
e8:eb:34:d5:8d:d1         149       auto      18         49      UPDATED CHILD
e8:eb:34:d5:94:d1         149       auto      37         4b      UPDATED NEIGH PARENT
e8:eb:34:d5:d3:11         149       auto      31         49      UPDATED NEIGH
e8:eb:34:d5:d8:91         149       auto      0          41      UPDATED
e8:eb:34:d5:da:31         149       auto      18         49      UPDATED NEIGH
e8:eb:34:d5:da:51         149       auto      0          1040    DEFAULT
e8:eb:34:d5:dc:d1         149       auto      9          49      UPDATED NEIGH
e8:eb:34:d5:ef:51         149       auto      0          40
e8:eb:34:d5:f6:51         149       auto      9          49      UPDATED NEIGH
e8:eb:34:d5:fd:51         149       auto      21         49      UPDATED NEIGH
ec:ce:13:9a:89:91         149       auto      19         49      UPDATED NEIGH
ec:ce:13:d7:6f:91         149       auto      18         49      UPDATED NEIGH
ec:ce:13:d7:75:71         149       auto      19         49      UPDATED NEIGH
ec:ce:13:d7:87:91         149       auto      0          41      UPDATED
ec:ce:13:d7:8e:51         149       auto      6          49      UPDATED NEIGH
```

show wireless profile ap priming summary

プライミング AP の概要を表示するには、**show wireless profile ap priming summary** コマンドを使用します。

show wireless profile ap priming summary

構文の説明

このコマンドには、キーワードも引数もありません。

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 Cupertino 17.9.1	このコマンドが導入されました。

例

次に、プライミング AP の概要を表示する例を示します。

```
Device# show wireless profile ap priming summary
```

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 { **agent** *mobility-agent-ip* **client summary** | **ap-list ip-address** *ip-address* | **controller client summary** | **dtls connections** | **statistics summary** }

構文の説明

agent *mobility-agent-ip* **client summary**	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-list ip-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。
controller client summary	サブドメインのアクティブ クライアントを表示します。
dtls connections	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 Gibraltar 16.10.1	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。

```
デバイス (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
```

show wireless mobility peer ip

IP アドレスを使用してモビリティ ピアの詳細を表示するには、 **show wireless mobility peer ip** コマンドを使用します。

show wireless mobility peer ip *ip-address*

構文の説明

ip-address	モビリティ ピアの IPv4 IP アドレス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、IP アドレスを使用してワイヤレス モビリティ ピアの詳細を表示する例を示します。

```
Device# show wireless mobility peer ip 209.165.200.224
```

show wireless multicast group summary

ワイヤレス マルチキャスト グループの概要を表示するには、 **show wireless multicast group summary** コマンドを使用します。

show wireless multicast group 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス マルチキャスト グループの概要を表示する例を示します。

```
Device# show wireless multicast group summary
```

show wireless mobility summary

ワイヤレス モビリティ マネージャ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 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス モビリティ マネージャの概要を表示する例を示します。

```
Device# show wireless mobility summary
```

show wireless multicast

ワイヤレス マルチキャスト情報を表示するには、特権 EXEC モードで **show wireless multicast** コマンドを使用します。

show wireless multicast [**source** *source-ip* **group** *group-ip* **vlan** *vlan-id* | **group** *group-ip* **vlan** *vlan-id*]

構文の説明

source *source-ip*	（任意）マルチキャスト トラフィックの送信元 IPv4 および IPv6 アドレスを指定します。
group *group-ip*	（任意）マルチキャスト トラフィックの宛先グループおよびグループ IP を指定します。
vlan *vlan-id*	特定の VLAN ID を持つ VLAN 上のクライアント情報を表示します。

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 Gibraltar 16.10.1	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、ワイヤレス マルチキャスト情報を表示する例を示します。

```
Device# show wireless multicast

Multicast                                 : Enabled
AP Capwap Multicast                       : Unicast
Wireless Broadcast                        : Disabled
Wireless Multicast non-ip-mcast           : Disabled

Vlan        Non-ip-mcast     Broadcast        MGID
------------------------------------------------------
1           Enabled          Enabled          Enabled
2           Enabled          Enabled          Disabled
94          Enabled          Enabled          Disabled

Device# show wireless multicast
Multicast                                 : Disabled
AP Capwap Multicast                       : Unicast
Wireless Broadcast                        : Disabled
Wireless Multicast non-ip-mcast           : Disabled
Wireless Multicast link-local             : Enabled
```

show wireless multicast group

ワイヤレス マルチキャストの非 IP VLAN またはグループの情報を表示するには、特権 EXEC モードで **show wireless multicast group** コマンドを使用します。

show wireless multicast group {**summary** | *group-ip* **vlan** *vlan-id*}

構文の説明

summary	ワイヤレス マルチキャストの非 IP グループのサマリーを表示します。
group-ip	グループ IP アドレスを指定します。
vlan *vlan-id*	マルチキャスト トラフィックの宛先グループ IPv4 および IPv6 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

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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。

例

次に、ワイヤレス マルチキャストの非 IP グループのサマリーを表示する例を示します。

```
デバイス# show wireless multicast group summary
```

show wireless mesh ethernet daisy-chain summary

イーサネット デイジー チェーンの概要を確認するには、**show wireless mesh ethernet daisy-chain summary** コマンドを使用します。

show wireless mesh ethernet daisy-chain 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 Bengaluru 17.4.1	このコマンドが導入されました。

次に、イーサネット デイジー チェーンの概要を確認する例を示します。

```
Device# show wireless mesh ethernet daisy-chain summary

AP Name BVI MAC         BGN   Backhaul   Ethernet      STP Red
-----------------------------------------------------------------------------------------------------
RAP4    683b.78bf.15f0  IOT  Ethernet0   Up Up Dn Dn   Enabled
RAP3    683b.78bf.1634  IOT  Ethernet0   Up Up Dn Dn   Enabled
RAP1    6c8b.d383.b4d4  IOT  Ethernet0   Up Up Dn Dn   Enabled
RAP2    6c8b.d383.b4e8  IOT  Ethernet0   Up Up Up Dn   Enabled
```

show wireless mesh ethernet daisy-chain bgn

イーサネット デイジー チェーンのブリッジグループ名（BGN）の詳細を確認するには、**show wireless mesh ethernet daisy-chain bgn** コマンドを使用します。

show wireless mesh ethernet daisy-chain bgn *bridge-group-name*

構文の説明

bridge-group-name	ブリッジ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 Bengaluru 17.4.1	このコマンドが導入されました。

次に、イーサネットデイジーチェーンのブリッジグループ名（BGN）の詳細を確認する例を示します。

```
Device# show wireless mesh ethernet daisy-chain bgn <IOT>

AP Name   BVI MAC       BGN  Backhaul    Ethernet      STP Red
-----------------------------------------------------------------------------------------------------
RAP4    683b.78bf.15f0  IOT  Ethernet0   Up Up Dn Dn   Enabled
RAP3    683b.78bf.1634  IOT  Ethernet0   Up Up Dn Dn   Enabled
RAP1    6c8b.d383.b4d4  IOT  Ethernet0   Up Up Dn Dn   Enabled
RAP2    6c8b.d383.b4e8  IOT  Ethernet0   Up Up Up Dn   Enabled
```

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 **show wireless performance** コマンドを使用します。

show wireless performance {**ap** | **client**} **summary**

構文の説明

ap summary	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 Gibraltar 16.10.1	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。

```
デバイス# 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。

```
デバイス# 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 Gibraltar 16.10.1	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。

```
デバイス# 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 **show wireless probe** 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 Gibraltar 16.10.1	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。

```
デバイス# 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 profile ap priming all

プライミングプロファイルの詳細を表示するには、**show wireless profile ap priming all** コマンドを使用します。

show wireless profile ap priming all

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 Cupertino 17.9.2	このコマンドが導入されました。

例

次に、プライミングプロファイルの詳細を表示する例を示します。

```
Device# show wireless profile ap priming all

Profile Name  Primary Controller Name  Primary Controller IP  Secondary Controller Name
  Secondary Controller IP  Tertiary Controller Name  Tertiary Controller IP  Override
------------------------------------------------------------------------------------------
AP-PRIMING-1  BGL18-wlc                209.165.201.1          BGL17-wlc
  209.165.201.2                                      0.0.0.0                 Disabled
AP-PRIMING-2  BGL18-wlc                209.165.201.2          BGL17-wlc
  209.165.201.2            BGL12-wlc                 209.165.201.3           Disabled
```

show wireless profile ap priming all

プライミングプロファイルの詳細を表示するには、**show wireless profile ap priming all** コマンドを使用します。

show wireless profile ap priming all

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 Cupertino 17.9.2	このコマンドが導入されました。

例

次に、プライミングプロファイルの詳細を表示する例を示します。

```
Device# show wireless profile ap priming all

Profile Name  Primary Controller Name  Primary Controller IP  Secondary Controller Name
  Secondary Controller IP  Tertiary Controller Name  Tertiary Controller IP  Override
------------------------------------------------------------------------------------------
AP-PRIMING-1  BGL18-wlc                209.165.201.1          BGL17-wlc
  209.165.201.2                                       0.0.0.0                Disabled
AP-PRIMING-2  BGL18-wlc                209.165.201.2          BGL17-wlc
  209.165.201.2            BGL12-wlc                 209.165.201.3          Disabled
```

show wireless profile airtime-fairness mapping

ワイヤレス プロファイルとの ATF ポリシー マッピングを表示するには、**show wireless profile airtime-fairness mapping** コマンドを使用します。

show wireless profile airtime-fairness mapping

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、ワイヤレス プロファイルとの ATF ポリシー マッピングを表示する例を示します。

```
デバイス# show wireless profile airtime-fairness mapping
Policy Profile                  Band      ATF Policy                      Weight
 Client Sharing    Availability
-------------------------------------------------------------------------------------
WGB                             2.4GHz                                     -
 -                 No
WGB                             5GHz                                       -
 -                 No
Policy1                         2.4GHz                                     -
 -                 No
Policy1                         5GHz                                       -
 -                 No
Test WBG                        2.4GHz                                     -
 -                 No
Test WBG                        5GHz                                       -
 -                 No
profile-name                    2.4GHz    atf-policy-name                  5
 Enabled           Yes
```

show wireless profile airtime-fairness summary

電波時間正常性プロファイルの要約を表示するには、**show wireless profile airtime-fairness summary** コマンドを使用します。

show wireless profile airtime-fairness summary

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、電波時間正常性プロファイルの要約を表示する例を示します。

```
デバイス# show wireless profile airtime-fairness summary
Policy Id      Policy Name                     Weight      Client Sharing
------------------------------------------------------------------------
1              atf-policy-name                  5           Enabled
```

show wireless profile ap packet-capture

AP パケット キャプチャ情報を表示するには、**show wireless profile ap packet-capture** コマンドを使用します。

show wireless profile ap packet-capture {**detailed** *profile-name* | **summary**}

構文の説明

profile-name	APパケットキャプチャ プロファイル。

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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

例

次に、AP パケット キャプチャ情報を表示する例を示します。

```
Device# show wireless profile ap packet-capture summary
Number of AP packet capture profiles: 3

Profile Name               Buffer   Duration(M Packet Len FTP IP
-------------------------------------------------------------------------
test                        1200        20         0      9.1.0.101
test1                       2048        10         0      0.0.0.0
tets1                       1024        10         0      0.0.0.0
```

例

次に、AP プロファイルの詳細な AP パケット キャプチャ情報を表示する例を示します。

```
Device# show wireless profile ap packet-capture detailed test1

Profile Name : test1
Description  :
-----------------------------------------------------
Buffer Size       : 2048 KB
Capture Duration  : 10 Minutes
Truncate Length   : packet length
FTP Server IP     : 0.0.0.0
FTP path          :
FTP Username      :

Packet Classifiers
  802.11 Control  : Enabled
  802.11 Mgmt     : Enabled
  802.11 Data     : Disabled
```

```
Dot1x           : Disabled
ARP             : Disabled
IAPP            : Disabled
IP              : Disabled
TCP             : Disabled
TCP port        : all
UDP             : Disabled
UDP port        : all
Broadcast       : Disabled
Multicast       : Disabled
```

show wireless profile calendar-profile detailed

特定のプロファイル名のカレンダープロファイルの詳細を表示するには、**show wireless profile calendar-profile detailed** コマンドを使用します。

show wireless profile calendar-profile detailed *profile-name*

構文の説明

profile-name	カレンダープロファイル名を指定します。

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 Gibraltar 16.12.1	このコマンドが導入されました。

次に、特定のプロファイル名のカレンダープロファイルの詳細を表示する例を示します。

```
Device# show wireless profile calendar-profile detailed daily_calendar_profile
Calendar profiles : daily_calendar_profile
------------------------------------------------------------------------
Recurrence : DAILY
Start Time : 09:00:00
End Time : 17:00:00
```

show wireless profile calendar-profile summary

カレンダープロファイルの要約を表示するには、**show wireless profile calendar-profile summary** コマンドを使用します。

show wireless profile calendar-profile 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 Gibraltar 16.12.1	このコマンドが導入されました。

次に、カレンダー プロファイルの概要の例を示します。

```
Device# show wireless profile calendar-profile summary
Number of Calendar Profiles: 3
Profile-Name
---------------------------------
monthly_25_profile
weekly_mon_profile
daily_calendar_profile
```

show wireless profile fabric detailed

特定のファブリック プロファイル名の詳細を表示するには、**show wireless profile fabric detailed** コマンドを使用します。

show wireless profile fabric detailed *fabric_profile_name*

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、特定のファブリック プロファイル名の詳細を表示する例を示します。

```
デバイス# show wireless profile fabric detailed test1
Profile-name      : test-fabric
VNID              : 12
SGT               : 5
```

show wireless profile flex

ワイヤレス プロファイルの flex パラメータを表示するには、**show wireless profile flex** コマンドを使用します。

show wireless profile flex { **detailed** *flex-profile-name* **chassis** {*chassis-number* | **active** | **standby** }**R0** } | **summary chassis** {*chassis-number* | **active** | **standby**}**R0**}

構文の説明

detailed	flex プロファイルの詳細パラメータを表示します
summary	flex プロファイルの概要を表示します。
chassis-number	シャーシ番号。有効な範囲は 1 ～ 2 です。
active	アクティブ インスタンス。
standby	スタンバイ インスタンス。
R0	ルートプロセッサ スロット 0。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス プロファイルの flex パラメータの概要を表示する例を示します。

```
Device# show wireless profile flex summary
```

show wireless profile policy all

すべてのポリシープロファイルの詳細な出力を表示するには、**show wireless profile policy all** コマンドを使用します。

show wireless profile policy 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 Gibraltar 16.12.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.5	コマンドの出力が変更され、ARP アクティビティ情報が含まれるようになりました。

例

次に、すべてのポリシープロファイルの詳細な出力を表示する例を示します。

```
Device# show wireless profile policy all

Policy Profile Name                : policy_name
Description                        :
Status                             : ENABLED
.
.
.
!the section of the output that shows whether ARP is enabled or disabled in the policy
profile.
ARP Activity Limit
  Exclusion                        : ENABLED
  PPS                              : 100
  Burst Interval                   : 5
```

show wireless profile policy detailed

ワイヤレス ポリシー プロファイルの詳細を表示するには、**show wireless profile policy detailed** コマンドを使用します。

show wireless profile policy detailed *policy-profile-name*

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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、ワイヤレス ポリシー プロファイルの詳細を表示する例を示します。

```
Device#show wireless profile policy detailed policy-profile-name
```

show wireless profile mesh detailed

メッシュプロファイルを確認するには、**show wireless profile mesh detailed** コマンドを使用します。

show wireless profile mesh detailed *profile-name*

構文の説明

profile-name	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 Bengaluru 17.4.1	このコマンドが導入されました。

次に、メッシュプロファイルを確認する例を示します。

```
Device# show wireless profile mesh detailed default-mesh-profile

Mesh Profile Name : default-mesh-profile
-------------------------------------------------
Description : default mesh profile
Bridge Group Name : IOT
Strict match BGN : ENABLED
Amsdu : ENABLED
Background Scan : ENABLED
Channel Change Notification : ENABLED
Backhaul client access : ENABLED
Ethernet Bridging : ENABLED
Ethernet Vlan Transparent : DISABLED
Daisy Chain STP Redundancy : ENABLED
Full Sector DFS : ENABLED
IDS : ENABLED
Multicast Mode : In-Out
Range in feet : 12000
Security Mode : EAP
Convergence Method : Standard
LSC only Authentication : DISABLED
Battery State : ENABLED
Authorization Method : eap_methods
Authentication Method : eap_methods
Backhaul tx rate(802.11bg) : auto
Backhaul tx rate(802.11a) : auto
```

show wireless profile radio summary

ワイヤレス無線プロファイルの概要を表示するには、**show wireless profile radio summary** コマンドを使用します。

show wireless profile radio 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 モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	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

例

次に、ワイヤレス無線プロファイルの概要を表示する例を示します。

```
Device# show wireless profile radio summary
```

show wireless profile tunnel summary

ワイヤレス トンネルプロファイルの概要を表示するには、**show wireless profile tunnel summary** コマンドを使用します。

show wireless profile tunnel 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 Gibraltar 16.11.1	このコマンドが導入されました。

例

次に、ワイヤレス トンネル プロファイルの概要を表示する例を示します。

```
Device# show wireless profile tunnel summary

Profile Name                    AAA-Override AAA-Proxy DHCP Opt82 Enabled
------------------------------- ------------ --------- ---------- --------
eogre_tunnel                              No        No        Yes      Yes
eogre_tunnel_set                          No        No        Yes       No
eogre_tunnel_snmp                         No        No         No       No
```

show wireless redundancy statistics

ハイアベイラビリティの統計情報を表示するには、 **show wireless redundancy statistics** コマンドを使用します。

show wireless redundancy statistics{**ap-group** | **wncdallchassis**{*chassis-num* | **active** | **standby**}**R0**}
{**ap-recovery** | {*instance-id* | **all** | **chassis**{*chassis-num* | **active** | **standby**}**R0**}}
{**client-group** | **wncdallchassis**{*chassis-num* | **active** | **standby**}**R0**}
{**client-recovery** | {**mobilityd** | **sisf**}**chassis**{*chassis-num* | **active** | **standby**}**R0**}
{**wncd** | {*instance-id* | **all** | **chassis**{*chassis-num* | **active** | **standby**}**R0**}}

構文の説明

chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサスロット 0 の設定のアクティブインスタンス。
standby R0	ルートプロセッサスロット 0 の設定のスタンバイインスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、WNCD のすべての統計情報を表示する例を示します。

show wireless rfid

RFID タグ情報を表示するには、特権 EXEC モードで **show wireless rfid** コマンドを使用します。

show wireless rfid {**client** | **detail** *rfid-mac-address* | **stats** | **summary**}

構文の説明

client	クライアントである RFID タグの概要を表示します。
detail	特定の RFID タグに関する情報を表示します。
stats	RFID 統計情報を表示します。
summary	既知のすべての RFID タグの概要情報を表示します。
rfid-mac-address	RFID MAC アドレス。

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、RFID 情報を表示する例を示します。

```
Device# show wireless rfid summary

Total RFID entries: : 16
Total Unique RFID entries : 16
RFID ID VENDOR Closet AP RSSI Time Since Last Heard
0012.b80a.c791 Cisco 7069.5a63.0520 -31 1 minute 40 seconds ago
0012.b80a.c953 Cisco 7069.5a63.0460 -33 2 minutes 15 seconds ago
0012.b80b.806c Cisco 7069.5a63.0260 -45 22 seconds ago
0012.b80d.e9f9 Cisco 7069.5a63.0460 -38 2 minutes 37 seconds ago
0012.b80d.ea03 Cisco 7069.5a63.0520 -43 2 minutes 38 seconds ago
0012.b80d.ea6b Cisco 7069.5a63.0460 -39 2 minutes 35 seconds ago
0012.b80d.ebe8 Cisco 7069.5a63.0520 -43 1 minute 31 seconds ago
0012.b80d.ebeb Cisco 7069.5a63.0520 -43 2 minutes 37 seconds ago
0012.b80d.ec48 Cisco 7069.5a63.0460 -42 2 minutes 16 seconds ago
0012.b80d.ec55 Cisco 7069.5a63.0520 -41 1 second ago
```

show wireless stats ap name

ワイヤレス AP の BSSID の統計を表示するには、**show wireless stats ap name** *ap-name* **dot11 24ghz slot 0** *wlan-name 1-4096* **statistics** を使用します

show wireless stats ap name *ap-name* **dot11 24ghz slot 0** *wlan-name 1-4096* **statistics**

構文の説明

ap-name	AP の名前を指定します。
wlan-name	WLAN の名前を指定します。
wlan-id	WLAN ID を指定します。値の範囲は 1 ～ 4096 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 Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、ワイヤレス AP の BSSID の統計を表示する例を示します。

```
Device#show wireless stats ap name ap-name dot11 24ghz slot 0 wlan-name 1-4096 statistics
BSSID                   : 7069.5a38.112e
WLAN ID                 : 18
Client Count            : 1
TX Statistics
------------------------------------------------------------------------------
Mgmt          Retries      Data Bytes      Data Retries       Subframe Retries
------------------------------------------------------------------------------
12            18           16081           18                 0
RX Statistics
------------------------------------------------------------------------------
Mgmt          Data Bytes
------------------------------------------------------------------------------
74            17693
Data Distribution
------------------------------------------------------------------------------
Bytes                        RX                          TX
------------------------------------------------------------------------------
0-64                         55                          93
65-128                       66                          40
129-256                      21                          5
257-512                      10                          3
513-1024                     1                           9
1025-2048                    0                           1
2049-4096                    0                           0
4097-8192                    0                           0
8193-16384                   0                           0
16385-32768                  0                           0
```

```
32769-65536                0                          0
65537-131072               0                          0
131073-262144              0                          0
262145-524288              0                          0
524289-1048576             0                          0
WMM Statistics
-------------------------------------------------------------------------------
                           RX                         TX
-------------------------------------------------------------------------------
Voice                      0                          43
Video                      0                          0
Best Effort                154                        39
Background                 0                          0
MCS
-------------------------------------------------------------------------------
MCS                        RX                         TX
-------------------------------------------------------------------------------
mcs0                       39                          0
mcs1                       2                           0
mcs2                       5                           0
mcs3                       7                           0
mcs4                       25                          0
mcs5                       59                          0
mcs6                       290                         0
mcs7                       1148                        3
mcs8                       2288                        0
mcs9                       4440                        2
```

show wireless stats ap image-download

AP イメージのダウンロードの統計を確認するには、特権 EXEC モードで **show wireless stats ap image-download** コマンドを使用します。

show wireless stats ap image-download ［ **chassis** { *chassis_number* | **active** | **standby** } **R0** ］

構文の説明

chassis	AP イメージのダウンロード用のシャーシを指定します。
chassis_number	シャーシ番号（1 または 2 のいずれか）。
active	アクティブインスタンスを指定します。
standby	スタンバイインスタンスを指定します。
R0	スロット 0 のルートプロセッサを指定します。

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 Dublin 17.11.1	このコマンドが導入されました。

例

次に、AP イメージのダウンロードの統計を確認する例を示します。

```
Device# show wireless stats ap image-download

AP image download info for last attempt
AP Name  Count  ImageSize   StartTime         EndTime           Diff(secs)  Predownload
 Aborted  Method
-------------------------------------------------------------------------------------------------------
JK3800   1      59228160    09/06/21 15:20:53  09/06/21 15:21:36  43          No
 No       HTTPS
mysore1  4      40509440    08/30/21 22:51:08  08/30/21 22:51:51  44          No
 No       HTTPS
```

show wireless stats client delete reasons

クライアントの削除理由の合計を確認するには、**show wireless stats client delete reasons** コマンドを使用します。

show wireless stats client delete reasons

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 Amsterdam 17.1.1	このコマンドが導入されました。

次に、クライアントの削除理由の合計を確認する例を示します。

```
Device# show wireless stats client delete reasons

Total client delete reasons
---------------------------
Controller deletes
---------------------------
---------------------------
No Operation                                                    : 0
Unknown                                                         : 0
Session Manager                                                 : 0
Connection timeout                                              : 0
Datapath plumb                                                  : 0
WPA key exchange timeout                                        : 0
802.11w MAX SA queries reached                                  : 0
Client deleted during HA recovery                               : 0
Inter instance roam failure                                     : 0
Inter instance roam success                                     : 0
Inter controller roam success                                   : 0
Due to mobility failure                                         : 0
NAS error                                                       : 0
Policy Manager internal error                                   : 0
80211v smart roam failed                                        : 0
DOT11v association failed                                       : 0
DOT11r pre-authentication failure                               : 0
SAE authentication failure                                      : 0
DOT11 failure                                                   : 0
DOT11 SAE invalid message                                       : 0
DOT11 denied data rates                                         : 0
802.11v Client RSSI lower than the association RSSI threshold   : 0
invalid QoS parameter                                           : 0
DOT11 IE validation failed                                      : 0
DOT11 group cipher in IE validation failed                      : 0
DOT11 invalid pairwise cipher                                   : 0
DOT11 invalid AKM                                               : 0
DOT11 unsupported RSN version                                   : 0
```

```
DOT11 invalid RSNIE capabilities                                : 0
DOT11 received invalid PMKID in the received RSN IE             : 0
DOT11 received invalid PMK length                               : 0
DOT11 invalid MDIE                                              : 0
DOT11 invalid FT IE                                             : 0
DOT11 AID allocation conflicts                                  : 0
AVC client re-anchored at the foreign controller                : 0
Client EAP ID timeout                                           : 0
Client DOT1x timeout                                            : 0
Malformed EAP key frame                                         : 0
EAP key install bit is not expected                             : 0
EAP key error bit is not expected                               : 0
EAP key ACK bit is not expected                                 : 0
Invalid key type                                                : 0
EAP key secure bit is not expected                              : 0
key description version mismatch                                : 0
wrong replay counter                                            : 0
EAP key MIC bit expected                                        : 0
MIC validation failed                                           : 0
MAC theft                                                       : 0
IP theft                                                        : 0
Policy bind failure                                             : 0
Web authentication failure                                      : 0
802.1X authentication credential failure                        : 0
802.1X authentication timeout                                   : 0
802.11 authentication failure                                   : 0
802.11 association failure                                      : 0
Manually excluded                                               : 0
DB error                                                        : 0
Anchor creation failure                                         : 0
Anchor invalid Mobility BSSID                                   : 0
Anchor no memory                                                : 0
Call admission controller at anchor node                        : 0
Supplicant restart                                              : 0
Port admin disabled                                             : 0
Reauthentication failure                                        : 0
Client connection lost                                          : 0
Error while PTK computation                                     : 0
MAC and IP theft                                                : 0
QoS policy failure                                              : 0
QoS policy send to AP failure                                   : 0
QoS policy bind on AP failure                                   : 0
QoS policy unbind on AP failure                                 : 0
Static IP anchor discovery failure                              : 0
VLAN failure                                                    : 0
ACL failure                                                     : 0
Redirect ACL failure                                            : 0
Accounting failure                                              : 0
Security group tag failure                                      : 0
FQDN filter definition does not exist                           : 0
Wrong filter type, expected postauth FQDN filter                : 0
Wrong filter type, expected preauth FQDN filter                 : 0
Invalid group id for FQDN filter valid range  1..16             : 0
Policy parameter mismatch                                       : 0
Reauth failure                                                  : 0
Wrong PSK                                                       : 0
Policy failure                                                  : 0
AAA server unavailable                                          : 0
AAA server not ready                                            : 0
No dot1x method configuration                                   : 0
Association connection timeout                                  : 0
MAC-AUTH connection timeout                                     : 0
L2-AUTH connection timeout                                      : 0
L3-AUTH connection timeout                                      : 0
```

```
Mobility connection timeout                                : 0
static IP connection timeout                               : 0
SM session creation timeout                                : 0
IP-LEARN connection timeout                                : 0
NACK IFID exists                                           : 0
Guest-LAN invalid MBSSID                                   : 0
Guest-LAN no memory                                        : 0
Guest-LAN ceate request failed                             : 0
EoGRE Reset                                                : 0
EoGRE Generic Join Failure                                 : 0
EoGRE HA-Reconciliation                                    : 0
Wired idle timeout                                         : 0
IP Update timeout                                          : 0
SAE Commit received in Associated State                    : 0
NACK IFID mismatch                                         : 0
EoGRE Invalid VLAN                                         : 0
EoGRE Empty Domain                                         : 0
EoGRE Invalid Domain                                       : 0
EoGRE Domain Shut                                          : 0
EoGRE Invalid Gateway                                      : 0
EoGRE All Gateways down                                    : 0
EoGRE Flex - no active gateway                             : 0
EoGRE Rule Matching error                                  : 0
EoGRE AAA Override error                                   : 0
EoGRE client onboarding error                              : 0
EoGRE Mobility Handoff error                               : 0
L3 VLAN Override connection timeout                        : 0
Delete received from AP                                    : 0
QoS failure                                                : 0
WPA group key update timeout                               : 0
DOT11 unsupported client capabilities                      : 0
DOT11 association denied unspecified                       : 0
DOT11 AP have insufficient bandwidth                       : 0
DOT11 invalid QoS parameter                                : 0
Client not allowed by assisted roaming                     : 0
Wired client deleted due to WGB delete                     : 0
Client Abort                                               : 0
Mobility peer delete                                       : 0
No IP                                                      : 0
BSSID down                                                 : 0
DOT11 QoS policy                                           : 0
Roam across policy profile deny                            : 0
4WAY handshake failure - M1 issue                          : 0
4WAY handshake failure - M3 issue                          : 0
Exclusion policy template fail                             : 0
DOT11 Cipher Suite Rejected                                : 0
WLAN-ID mismatch in access accept failures                 : 0
EasyPSK AAA unknown error                                  : 0
EasyPSK unspecified error                                  : 0
EasyPSK PSK mismatch error                                 : 0
EasyPSK radius busy error                                  : 0
EasyPSK limit reached error                                : 0
EasyPSK bad 802.1X frame error                             : 0
EasyPSK missing parameter error                            : 0
Supplicant name failure                                    : 0
User name failure                                          : 0
Service set ID failure                                     : 0
Anchor VLAN ID failure                                     : 0
PSK failure                                                : 0
PSK mode failure                                           : 0
Interim interval failure                                   : 0
Link-local bridging VLAN failure                           : 0
Link-local bridging VLAN failure                           : 0
Maximum client limit reached on AP                         : 0
```

```
Maximum client limit reached on AP per wlan                    : 0
Maximum client limit reached on AP radio per wlan              : 0
Maximum client limit reached on AP radio                       : 0
L3 Access Roam across policy profile deny                      : 0
L3 Access Inter controller roam deny                           : 0
----------------------------
Informational Delete Reason
----------------------------
Mobility WLAN down                                             : 0
AP upgrade                                                     : 0
L3 authentication failure                                      : 0
AP down/disjoin                                                : 0
MAC authentication failure                                     : 0
Due to SSID change                                             : 0
Due to VLAN change                                             : 0
Admin deauthentication                                         : 0
Session timeout                                                : 0
Idle timeout                                                   : 0
Supplicant request                                             : 0
Mobility tunnel down                                           : 0
DOT11v timer timeout                                           : 0
DOT11 max STA                                                  : 0
IAPP disassociation for wired client                           : 0
Wired WGB change                                               : 0
Wired VLAN change                                              : 0
WGB Wired client joins as a direct wireless client             : 0
Incorrect credentials                                          : 0
Wired client cleanup due to WGB roaming                        : 0
Radio Down                                                     : 0
Mobility failure on fast roam                                  : 0
Due to IP Zone change                                          : 0
Access denied due to Locally Administered MAC Address          : 0
----------------------------
----------------------------
Client initiate delete
----------------------------
Deauthentication or disassociation request                     : 0
Client DHCP                                                    : 0
Client EAP timeout                                             : 0
Client 8021x failure                                           : 0
Client device idle                                             : 0
Client captive portal security failure                         : 0
Client decryption failure                                      : 0
Client interface disabled                                      : 0
Client user triggered disassociation                           : 0
Client miscellaneous reason                                    : 0
Unknown                                                        : 0
Client peer triggered                                          : 0
Client beacon loss                                             : 0
STA triggered PMK timeout                                   : 0
Excess ARP activity                                         : 0
Excess NDP activity                                         : 0
Unspecified QOS failure                                        : 0
Dpath encode failed                                            : 0
VRF-VLAN mismatch failures                                  : 0
----------------------------
AP Deletes
----------------------------
When client is sending disassociation                       : 0
Idle timeout                                                : 0
Client ACL mismatch                                         : 0
AP authentication stop                                      : 0
Association expired at AP                                   : 0
4-way handshake failed                                      : 0
```

```
DHCP timeout                                                : 0
Reassociation timeout                                       : 0
SA query timeout                                            : 0
Intra AP roam                                               : 0
Channel switch at AP                                        : 0
Bad AID                                                     : 0
AP requests for client deletion                             : 0
Interface reset                                             : 0
All on slot                                                 : 0
Link to client has changed and uplink can be reaper         : 0
Slot disable                                                : 0
MIC failure                                                 : 0
VLAN delete                                                 : 0
Channel change                                              : 0
Stop reassociation                                          : 0
Packet maximum retry                                        : 0
Transmission deauthentication                               : 0
Sensor station timeout                                      : 0
Age timeout                                                 : 0
Transmission threshold fail                                 : 0
Uplink receive timeout                                      : 0
Sensor scan next radio                                      : 0
Sensor scan other BSSID                                     : 0
Authentication timeout and web-auth timeout                 : 0
Sending deauthentication packet to client                   : 0
AP IP learn timeout                                         : 0
Flex group change                                           : 0
EAPOL log off                                               : 0
EAP request timeout                                         : 0
4way handshake failure                                      : 0
MIC validation                                              : 0
Wrong replay counter                                        : 0
AP tunnel down                                              : 0
Inter roam                                                  : 0
Unknown client                                              : 0
Reauthentication timeout                                    : 0
Continuous idle timeout                                     : 0
RLDP cleanup                                                : 0
Intra-switch roam                                           : 0
PEM cleanup                                                 : 0
RLAN Central switch                                         : 0
RLAN data path add failure                                  : 0
RLAN Delete                                                 : 0
RLAN Inactive timeout                                       : 0
RLAN MAB failure                                            : 0
CLSM No memory counter                                      : 0
CLSM BSSID mismatch                                         : 0
CLSM No ACL found                                           : 0
CLSM no parent WGB found                                    : 0
CLSM Key plumb faiure                                       : 0
CLSM Mesh key plumb failure                                 : 0
CLSM data path add fail                                     : 0
CLSM Authentication response reject                         : 0
CLSM Authentication response send failure                   : 0
CLSM Association response send failure                      : 0
CLSM association response failure with status               : 0
CLSM Webauth timer expired                                  : 0
CLSM Dot1x timer expired                                    : 0
CLSM deauthentication and disassociation send failure       : 0
Driver event Class3 received                                : 0
Driver event PsPoll when not authenticated                  : 0
Driver event ioctl error                                    : 0
Flex FT failure                                             : 0
CLSM driver add failure                                     : 0
```

```
Driver client not found                                          : 0
Driver management packet allocation failure                      : 0
Driver invalid cipher                                            : 0
Driver invalid association identifier                            : 0
Driver invalid key                                               : 0
Driver firmware set key failure                                  : 0
Driver found invalid HT VHT rates                                : 0
Driver found invalid legacy rates                                : 0
Driver found no overlapping legacy rates                         : 0
Driver found maximum VHT streams                                 : 0
Driver found association identifer in use                        : 0
Driver found too many association requests                       : 0
Driver found cipher attach failure                               : 0
Driver found algorithm mismatch                                  : 0
Driver found invalid key length                                  : 0
Driver found invalid key index                                   : 0
Driver rejected association due to authentication failure        : 0
Driver found client addition to internal records failure         : 0
Driver found client association entry failure                    : 0
Driver found client additions to firmware failure                : 0
Driver related internal failure                                  : 0
AP limiting maximum client per AP                                : 0
AP limiting maximum client per AP radio per wlan                 : 0
AP limiting maximum client per AP radio                          : 0
-------------------
PC Analytics stats:
---------------------------------------
Report Type            Processed Reports
---------------------------------------
 PC_STA_INFO          : 0
 PC_NEIGH_INFO        : 0
 PC_LOW_RSSI          : 0
 PC_TEMP_DISCONN      : 0
 PC_AP_FAILURE        : 0
 PC_UNKNOWN_AP        : 0
--------------------------------------
Report Type            Dropped Reports
--------------------------------------
 PC_STA_INFO          : 0
 PC_NEIGH_INFO        : 0
 PC_LOW_RSSI          : 0
 PC_TEMP_DISCONN      : 0
 PC_AP_FAILURE        : 0
 PC_UNKNOWN_AP        : 0
```

show wireless statistics mobility

ワイヤレス モビリティ マネージャの統計情報を表示するには、 **show wireless stats mobility** コマンドを使用します。

show wireless stats mobility {**dtls** | **messages**} ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

dtls	モビリティ dtls メッセージの統計情報を表示します。
messages	モビリティ メッセージの統計情報を表示します。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active	ルートプロセッサ スロット 0 の設定のアクティブ インスタンス。
standby	ルートプロセッサスロット 0 の設定のスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス モビリティ マネージャの統計情報を表示する例を示します。

```
Device# show wireless stats mobility
```

show wireless stats mesh packet error

接続されているすべてのメッシュ AP のパケット統計情報を表示するには、 **show wireless stats mesh packet error** コマンドを使用します。

show wireless stats mesh packet error ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

構文の説明

packet	パケット統計情報を表示します。
error	接続されているすべてのメッシュ AP のパケット統計情報を表示します。
active R0	ルートプロセッサ スロット 0 のアクティブな AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 のアクティブな AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、接続されているすべてのメッシュ AP のパケット エラー統計情報を表示する例を示します。

```
Device# show wireless stats mesh packet error
```

show wireless stats pmk-propagation

シスコ ワイヤレス コントローラでの PMK 伝達の統計を表示するには、特権 EXEC モードで **show wireless stats pmk-propagation** コマンドを使用します。

show wireless stats pmk-propagation

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 Cupertino 17.8.1	このコマンドが導入されました。

例

次に、シスコ ワイヤレス コントローラでの PMK 伝達の統計を表示する例を示します。

```
Device# show wireless stats pmk-propagation

Site-Tag       Bulk Sync Success     Bulk Sync Failure     Incremental Sync Failure
-------------------------------------------------------------------------------------
flex-site-tag       97                       0                    0
```

show wireless stats mesh security and queue

接続されているすべてのメッシュ AP のメッシュ キューとセキュリティの統計情報を表示するには、 **show wireless stats mesh** コマンドを使用します。

show wireless stats mesh {**security** | **queue**} [**chassis** {*chassis-number* | **active** | **standby**} **R0**]

構文の説明

queue	接続されているすべてのメッシュ AP のキュー統計情報を表示します。
security	接続されているすべてのメッシュ AP のセキュリティ統計情報を表示します。
chassis-number	シャーシ番号（1 または 2 のいずれか）を入力します。
active R0	ルートプロセッサ スロット 0 のアクティブな AP フィルタのアクティブ インスタンス。
standby R0	ルートプロセッサ スロット 0 のアクティブな AP フィルタのスタンバイ インスタンス。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、接続されているすべてのメッシュ AP のセキュリティ統計情報を表示する例を示します。

```
Device# show wireless stats mesh security
```

show wireless stats client detail

クライアントに関する統計を確認するには、**show wireless stats client detail** コマンドを使用します。

show wireless stats client detail

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 Amsterdam 17.1.1	このコマンドが導入されました。

次に、クライアントに関する統計を確認する例を示します。

```
Device# show wireless stats client detail
[…]
Total L3 VLAN Override vlan change received : 1
Total L3 VLAN Override disassociations sent : 1
Total L3 VLAN Override re-associations received : 1
Total L3 VLAN Override successful VLAN change : 1
[…]
L3 VLAN Override connection timeout : 0
```

show wireless stats redundancy config database

高可用性冗長設定の統計を表示するには、**show wireless stats redundancy config database** コマンドを使用します。

show wireless stats redundancy config database { **mobility** | **nmspd** | **rrm** | **wncd** | **wncmgrd** } *instance-id* **chassis** { *chassis-num* | **active** | **standby** } **R0**

構文の説明

mobility	Mobilityd 設定データベースの統計を指定します。
nmspd	NMSPD 設定データベースの統計を指定します。
rrm	RRM 設定データベースの統計を指定します。
wncd	WNCD 設定データベースの統計を指定します。
wncmgrd	WNCD 設定データベースの統計を指定します。
instance-id	インスタンス ID です。有効値の範囲は 0 ～ 7 です。
chassis	シャーシを指定します。
chassis-num	シャーシ番号。
active	アクティブ インスタンスを指定します。
standby	スタンバイ インスタンスを指定します。
R0	ルートプロセッサスロットを指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このコマンドが導入されました。

例

次に、高可用性冗長設定の統計を表示する例を示します。

```
Device# show wireless stats redundancy config database wncd 0 chassis 1 R0

Wncd Configuration Sync Statistics
 Index   Number of Locks    Duration(sec)   Threshold-count   Max-Duration(nsec)
------------------------------------------------------------------------------
    1        535                127               1           1112156700
```

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 Gibraltar 16.10.1	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。

```
デバイス# 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 tag rf

ワイヤレス RF タグの詳細を表示するには、**show wireless tag rf** コマンドを使用します。

show wireless tag rf { **summary** | **detailed***rf-tag-name*

構文の説明

summary	すべてのRFタグの概要を表示します。
detailed	RF タグの詳細を表示します。
rf-tag-name	RF タグ名。

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 Gibraltar 16.10.1	このコマンドが導入されました。

例

次に、**show wireless tag rf summary** コマンドの出力例を示します。

```
Device# show  wireless tag rf summary

Number of RF Tags: 1

RF tag name                     Description
------------------------------------------------------------------------
default-rf-tag                  default RF tag
```

show wireless urlfilter details

指定されたワイヤレス URL フィルタの詳細を表示するには、**show wireless urlfilter details** コマンドを使用します。

show wireless urlfilter details *list-name*

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、指定されたワイヤレス URL フィルタの詳細を表示する例を示します。

```
デバイス# show wireless urlfilter details urllist_flex_preauth
List Name..................... : urllist_flex_preauth
Filter ID..................... : : 1
Filter Type................... : PRE-AUTH
Action........................ : PERMIT
Redirect server ipv4...... : 8.8.8.8
Redirect server ipv6...... : 2001:0300:0008:0000:0000:0000:0000:0081
Configured List of URLs
   URL........................ : url1.dns.com
```

show wireless urlfilter summary

すべてのワイヤレス URL フィルタの概要を表示するには、**show wireless urlfilter summary** コマンドを使用します。

show wireless urlfilter summary

構文の説明

このコマンドには、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

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 Gibraltar 16.10.1	このコマンドが導入されました。

次に、すべてのワイヤレス URL フィルタの概要を表示する例を示します。

```
デバイス# show wireless urlfilter summary
Black-list    - DENY
White-list    - PERMIT
Filter-Type   - Specific to Local Mode

URL-List                          ID  Filter-Type  Action   Redirect-ipv4  Redirect-ipv6
-------------------------------------------------------------------------------------------------------
urllist_flex_preauth              1    PRE-AUTH     PERMIT    8.8.8.8
2001:0300:0008:0000:0000:0000:0000:0081
```

show wireless vlan details

VLAN の詳細を表示するには、**show wireless vlan details** コマンドを使用します。

show wireless vlan details ［**chassis** {*chassis-number* | **active** | **standby**} **R0**］

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、VLAN の詳細を表示する例を示します。

```
Device# show wireless vlan details chassis active r0
```

show wireless wgb mac-address

MAC アドレスを使用してワイヤレス ワークグループ ブリッジ（WGB）のすべてのクライアントを表示するには、 **show wireless wgb mac-address** コマンドを使用します。

show wireless wgb mac-address *mac-address* **detail**

構文の説明

mac-address	WGB の MAC アドレス。
detail	ワイヤレス WGB のクライアントを表示します。

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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、ワイヤレス WGB のクライアントを表示する例を示します。

```
Device# show wireless wgb mac-address 98-C7-7B-09-EF-ED detail
```

show wireless wgb summary

アクティブなワークグループ ブリッジ（WGB）を表示するには、 **show wireless wgb summary** コマンドを使用します。

show wireless wgb 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 Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、アクティブなワークグループ ブリッジ（WGB）を表示する例を示します。

```
Device# show wireless wgb summary
```

show wireless wps mfp ap summary

アクセスポイントが管理フレーム保護（MFP）の検証と保護をサポートしているかどうかを確認するには、**show wireless wps mfp ap summary** コマンドを使用します。

show wireless wps mfp ap 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 Gibraltar 16.12.1	このコマンドが導入されました。

次に、MFP 検証と保護をサポートするアクセス ポイントの例を示します。

```
Device# show wireless wps mfp ap summary
AP Name                          Radio MAC              Validation           Protection
-------------------------------------------------------------------------------------------
AP002A.1087.CBF4                   00a2.eefd.bdc0          Enabled               Enabled

AP58AC.78DE.9946                   00a2.eeb8.4ae0          Enabled               Enabled

APb4de.3196.caac                   4c77.6d83.6b90          Enabled               Enabled
```

show wireless wps mfp statistics

管理フレーム保護（MFP）の統計情報を表示するには、**show wireless wps mfp statistics** コマンドを使用します。

show wireless wps mfp statistics

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 Gibraltar 16.12.1	このコマンドが導入されました。

次に、管理フレーム保護（MFP）の統計情報の例を示します。

```
Device# show wireless wps mfp statistics
BSSID          Radio DetectorAP                      LastSourceAddr Error
Count     FrameTypes

aabb.ccdd.eeff a     AP3800                          aabb.ccdd.eeff Invalid MIC     10
        Beacon, Probe Response
                                                                    Invalid MIC     20
        Beacon, Probe Response
```

show wireless wps mfp summary

管理フレーム保護（MFP）の詳細情報を表示するには、**show wireless wps mfp summary** コマンドを使用します。

show wireless wps mfp 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 Gibraltar 16.12.1	このコマンドが導入されました。

次に、管理フレーム保護（MFP）の詳細情報の例を示します。

```
Device# show wireless wps mfp summary
Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

show wireless wps rogue

不正 AP とクライアント情報を表示するには、 **show wireless wps rogue** コマンドを使用します。

アドホック不正（IBSS）情報を表示する
show wireless wps rogue {**adhoc** | {**detailed***mac-addr*} | **summary**}

不正 AP 情報を表示する
show wireless wps rogueap{**clients***mac-addr* | **customsummary** | **detailed***mac-addr* | **friendlysummary** | **listmac-address***mac-addr* | **malicious summary** | **summary** | **unclassifiedsummary** | **rldp**{**summary** | **in-progress** | **detailed***rogue-ap-mac-addr*}}

不正の自動抑制情報を表示する
show wireless wps rogueauto-contain

不正クライアント情報を表示する
show wireless wps rogueclient{**summary** | **detailed***mac-addr*}

不正無視リストを表示する
show wireless wps rogueignore-list

分類ルール情報を表示する
show wireless wps roguerule{**detailed***rule-name* | **summary**}

不正機能に関する統計情報を表示する
show wireless wps roguestats[{**internal**}]

構文の説明

mac-address	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

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。

例

次に、不正機能の統計情報を表示する例を示します。

```
Device# show wireless wps rogue stats
```

show wireless wps rogue ap summary

deviceによって検出されたすべての不正なアクセス ポイントを一覧表示するには、**show wireless wps rogue ap summary** コマンドを使用します。

show wireless wps rogue ap 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
	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、device によって検出されたすべての不正なアクセス ポイントのリストを表示する例を示します。

```
デバイス# show wireless wps rogue ap summary
Rogue Location Discovery Protocol            : Disabled
Rogue on wire Auto-Contain                   : Disabled
Rogue using our SSID Auto-Contain            : Disabled
Valid client on rogue AP Auto-Contain        : Disabled
Rogue AP timeout                             : 1200
Rogue Detection Report Interval              : 10
Rogue AP minimum RSSI                        : -128
Rogue AP minimum transient time              : 0

Number of rogue APs detected : 624

MAC Address         Classification     # APs    # Clients   Last Heard
-----------------------------------------------------------------------------------------
0018.e78d.250a      Unclassified       1        0           Thu Jul 25 05:04:01 2013
0019.0705.d5bc      Unclassified       1        0           Thu Jul 25 05:16:26 2013
0019.0705.d5bd      Unclassified       1        0           Thu Jul 25 05:10:28 2013
0019.0705.d5bf      Unclassified       1        0           Thu Jul 25 05:16:26 2013
```

show wireless wps rogue client detailed

特定の不正なクライアントの詳細情報を表示するには、 **show wireless wps rogue client detailed** *client-mac* コマンドを入力します。

show wireless wps rogue client detailed *client-mac*

構文の説明

client-mac	不正なクライアントのMACアドレス。

コマンド デフォルト

なし。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	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、特定の不正なクライアントの詳細情報を表示する例を示します。

```
デバイス# show wireless wps rogue client detail  0024.d7f1.2558
Rogue BSSID                          : 64d8.146f.379f
Rogue Radio Type                     : 802.11n - 5GHz
State                                : Alert
First Time Rogue was Reported        : Wed Aug  7 12:51:43 2013
Last Time Rogue was Reported         : Wed Aug  7 12:51:43 2013
Reported by
  AP 2
    MAC Address                      : 3cce.7309.0370
    Name                             : AP3502-talwar-ccie
    Radio Type                       : 802.11a
    RSSI                             : -42 dBm
    SNR                              : 47 dB
    Channel                          : 52
    Last reported by this AP         : Wed Aug  7 12:51:43 2013
```

show wireless wps rogue ap detailed

不正アクセスポイントの詳細情報を表示するには、**show wireless wps rogue ap detailed** *mac-address* コマンドを使用します。

show wireless wps rogue ap detailed *0008.30a7.7797*

構文の説明

mac-address 不正アクセスポイントの MAC アドレスの検索。

（注） 不正アクセスポイントが 2.4GHz で dot11n を使用している場合、コマンド出力には **radio type** が **dot11g , dot11n - 2.4 GHz** として表示されます。

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 Fuji 16.7.x	このコマンドが導入されました。

例

次に、不正アクセスポイントに関する詳細情報を表示する例を示します。

```
デバイス# wireless wps rogue ap detailed 0008.30a7.7797
Rogue Event history

Rogue BSSID                              : 0008.30a7.7797
Is Rogue on Wired Network                : No
Classification                           : Unclassified
Manually Contained                       : Yes
State                                    : Contained Pending
Containment Level                        : 1
Number of Containing APs                 : 0
First Time Rogue was Reported            : 03/08/2017 17:41:55
Last Time Rogue was Reported             : 03/08/2017 21:48:34

Number of clients                        : 0

Reported By
  AP Name : JEWLC-AA
    MAC Address                          : 00d7.8f4e.7240
    Detecting slot ID                    : 0
    Radio Type                           : dot11g , dot11n - 2.4 GHz
    SSID                                 : psk
    Channel                              : 5
    Channel Width                        : 20 MHz
    RSSI                                 : -128 dBm
    SNR                                  : 0 dB
    Encryption                           : Enabled
```

```
ShortPreamble                     : Disabled
WPA Support                       : Not Friendly
Last reported by this AP          : 03/08/2017 21:48:34
```

show wireless wps rogue client summary

WPS 不正クライアントの概要を表示するには、**show wireless wps rogue client summary** コマンドを使用します。

show wireless wps rogue client 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 Gibraltar 16.10.1	このコマンドが導入されました。

使用上のガイドライン

例

次に、**show wireless wps rogue client summary** コマンドの出力を示します。

```
デバイス# show wireless wps rogue client summary
Validate rogue clients against AAA  : Disabled
Validate rogue clients against MSE  : Enabled
Number of rogue clients detected : 0
```

show wireless wps summary

WPS の詳細情報を表示するには、**show wireless wps summary** コマンドを使用します。

show wireless wps 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 Gibraltar 16.12.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.5	コマンドの出力が変更され、ARP アクティビティ情報が含まれるようになりました。

次に、管理フレーム保護（MFP）が有効または無効になっている場合の例を示します。

```
Device# show wireless wps summary

Client Exclusion Policy
  Excessive 802.11-association failures   : unknown
  Excessive 802.11-authentication failures: unknown
  Excessive 802.1x-authentication         : unknown
  IP-theft                                : unknown
  Excessive Web authentication failure    : unknown
  Failed Qos Policy                       : unknown

Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

次に、ARP パケットのレート制限が有効になっているかどうかの例を示します。

```
Device# show wireless wps summary

Client Exclusion Policy
  Excessive 802.11-association failures   : Enabled
  Excessive 802.1x-authentication         : Enabled
  Mac and IP-theft                        : Enabled
  Excessive Web authentication failure    : Enabled
  Failed Qos Policy                       : Enabled
  Excessive ARP Activity                  : Enabled (per policy setting)
```

show wlan name client stats

WLAN クライアントの統計を表示するには、**show wlan name client stats** コマンドを使用します。

show wlan name *wlan-name* **client stats**

構文の説明

wlan-name	WLAN 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 Amsterdam 17.1.1s	このコマンドが導入されました。

次に、WLAN クライアントの統計を表示する例を示します。

```
Device# show wlan name wlan1 client stats

Wlan Profile Name: wlan1, Wlan Id: 3
Current client state statistics:
------------------------------------------------------------------------------
  Authenticating         : 0
  Mobility               : 0
  IP Learn               : 0
  Webauth Pending        : 0
  Run                    : 0

Locally Administered MAC Clients  : 0
L3 Access Clients                 : 0

.
.
.
```

show wlan summary sort ascending client-count

クライアント数に基づいて昇順でソートされた WLAN の概要を表示するには、**show wlan summary sort ascending client-count** コマンドを使用します。

show wlan summary sort ascending client-count

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 Amsterdam 17.1.1s	このコマンドが導入されました。

次に、クライアント数に基づいて昇順でソートされたWLANの概要を表示する例を示します。

```
Device# show wlan summary sort ascending client-count
-------------------------------------------------------------------------------------------
Wlan-name                       ID            Client count           Data Usage
-------------------------------------------------------------------------------------------
rlan_test_1                     1               1                      6277
WLAN_CA_WPA2_AES_DOT1X          70              1                      167781
```

show wlan summary sort descending client-count

クライアント数に基づいて降順でソートされた WLAN の概要を表示するには、**show wlan summary sort descending client-count** コマンドを使用します。

show wlan summary sort descending client-count

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 Amsterdam 17.1.1s	このコマンドが導入されました。

次に、クライアント数に基づいて降順でソートされたWLANの概要を表示する例を示します。

```
Device# show wlan summary sort descending client-count
-------------------------------------------------------------------------------------------
Wlan-name                       ID            Client count           Data Usage
-------------------------------------------------------------------------------------------
rlan_test_1                     1               1                      6277
WLAN_CA_WPA2_AES_DOT1X          70              1                      167781
```

show wlan summary sort ascending data-usage

データ使用量に基づいて昇順でソートされたwlanの概要を表示するには、**show wlan summary sort ascending data-usage** コマンドを使用します。

show wlan summary sort ascending data-usage

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 Gibraltar 17.1.1	このコマンドが導入されました。

次に、データ使用量に基づいて昇順でソートされたwlanの概要を表示する例を示します。

```
Device# show wlan summary sort ascending data-usage
-------------------------------------------------------------------------------------------
Wlan-name                       ID            Client count           Data Usage
-------------------------------------------------------------------------------------------
rlan_test_1                     1               1                      6277
WLAN_CA_WPA2_AES_DOT1X          70              1                      167781
```

show wlan summary sort descending data-usage

データ使用量に基づいて降順でソートされたWLANの概要を表示するには、**show wlan summary sort descending data-usage** コマンドを使用します。

show wlan summary sort descending data-usage

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 Amsterdam 17.1.1s	このコマンドが導入されました。

次に、データ使用量に基づいて降順でソートされたWLANの概要を表示する例を示します。

```
Device# show wlan summary sort descending data-usage
-------------------------------------------------------------------------------------------
Wlan-name                       ID            Client count           Data Usage
-------------------------------------------------------------------------------------------
WLAN_CA_WPA2_AES_DOT1X          70              1                      167781
rlan_test_1                     1               1                      6277
```

show wps summary

Wireless Protection System（WPS）の要約情報を表示するには、**show wps summary** コマンドを使用します。

show wps 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

次に、WPS の要約情報を表示する例を示します。

```
(Cisco Controller) > show wps summary
Auto-Immune
  Auto-Immune.................................... Disabled
Client Exclusion Policy
  Excessive 802.11-association failures.......... Enabled
  Excessive 802.11-authentication failures....... Enabled
  Excessive 802.1x-authentication................ Enabled
  IP-theft....................................... Enabled
  Excessive Web authentication failure........... Enabled
Trusted AP Policy
  Management Frame Protection.................... Disabled
  Mis-configured AP Action....................... Alarm Only
    Enforced encryption policy................... none
    Enforced preamble policy..................... none
    Enforced radio type policy................... none
    Validate SSID................................ Disabled
  Alert if Trusted AP is missing................. Disabled
  Trusted AP timeout............................. 120
Untrusted AP Policy
  Rogue Location Discovery Protocol.............. Disabled
    RLDP Action.................................. Alarm Only
  Rogue APs
    Rogues AP advertising my SSID................ Alarm Only
    Detect and report Ad-Hoc Networks............ Enabled
  Rogue Clients
    Validate rogue clients against AAA........... Enabled
    Detect trusted clients on rogue APs.......... Alarm Only
  Rogue AP timeout............................... 1300
Signature Policy
  Signature Processing........................... Enabled
...
```

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

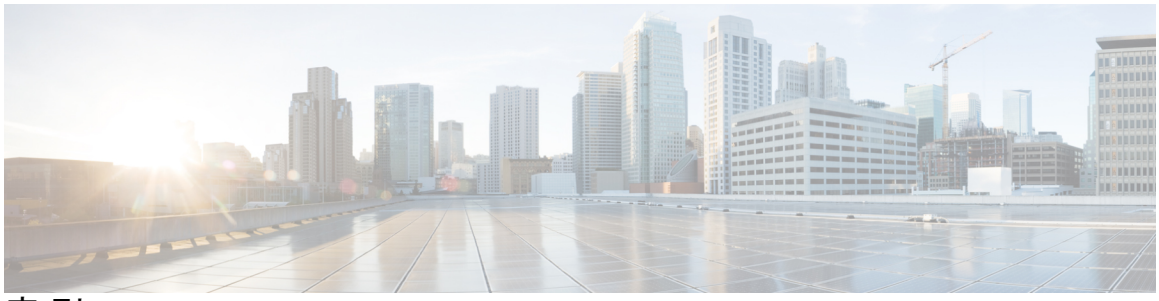
コマンド履歴

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。

```
デバイス(config-rf-profile)#shutdown
```



索 引

記号

A

B

C

D

E

F

I

L

M

N

O

P

Q

R

S

T

U

V

W

こ

せ

ほ

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