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 *1 : 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 *2 : 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 *3 : 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 *4: 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 *5:* 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 *6 : 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
```

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。