コンフィギュレーション コマンド：g ～ z

gas-ap-rate-limit

特定の期間にアクセス ポイント（AP）によってコントローラに送信される Generic Advertisement Service（GAS）または Access Network Query Protocol（ANQP）の要求アクション フレームの数を設定するには、**gas-ap-rate-limit** コマンドを使用します。

gas-ap-rate-limit *number-of-requests request-limit-interval*

構文の説明

number-of-requests	特定の間隔で許可される GAS または ANQP 要求の数。有効な範囲は 1 ～ 100 です。
request-limit-interval	最大数の要求が適用できる間隔。有効な範囲は 100 ～ 1000 ミリ秒です。

コマンド デフォルト

制限は有効になっていません。

コマンド モード

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

コマンド履歴

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

例

次に、特定の期間に AP によってコントローラに送信される GAS または ANQP 要求のアクションフレームの数を設定する例を示します。

```
Device(config)# ap profile hotspot
Device(config-ap-profile)# gas-ap-rate-limit 12 120
```

geolocation ftm initiator burst-duration

AP プロファイルで AP 地理位置情報の詳細タイミング測定（FTM）イニシエータのバースト期間値を設定するには、**geolocation ftm initiator burst-duration**{**128ms** | **16ms** | **1ms** | **250us** | **2ms** | **32ms** | **4ms** | **500us** | **64ms** | **8ms**} コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

geolocation ftm initiator burst-duration { **128ms** | **16ms** | **1ms** | **250us** | **2ms** | **32ms** | **4ms** | **500us** | **64ms** | **8ms** }

no geolocation ftm initiator burst-duration { **128ms** | **16ms** | **1ms** | **250us** | **2ms** | **32ms** | **4ms** | **500us** | **64ms** | **8ms** }

構文の説明

128ms	バースト期間を 128 ミリ秒に設定します。
16ms	バースト期間を 16 ミリ秒に設定します。
1ms	バースト期間を 1 ミリ秒に設定します。
250us	バースト期間を250マイクロ秒に設定します。
2ms	バースト期間を 2 ミリ秒に設定します。
32ms	バースト期間を 32 ミリ秒に設定します。
4ms	バースト期間を 4 ミリ秒に設定します。
500us	バースト期間を500マイクロ秒に設定します。
64ms	バースト期間を 64 ミリ秒に設定します。
8ms	バースト期間を 8 ミリ秒に設定します。

コマンド デフォルト

デフォルト値は 32 ミリ秒です。

コマンド モード

AP プロファイル コンフィギュレーション モード

コマンド履歴

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

例

次に、AP プロファイルで AP 地理位置情報の詳細タイミング測定（FTM）イニシエータのバースト期間値を設定する例を示します。

```
Device# configure terminal
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)#geolocation ftm initiator burst-duration 32
```

geolocation ftm initiator burst-size

AP プロファイルで AP 地理位置情報の詳細タイミング測定（FTM）イニシエータのバーストサイズ値を設定するには、**geolocation ftm initiator burst-size** *burst-size* コマンドを使用します。無効にするには、このコマンドの **no** 形式を使用します

geolocation ftm initiator burst-size *burst-size*

構文の説明

burst-size	バーストサイズを指定します。バーストサイズ値は、4、8、16、32、および64です。

コマンド デフォルト

デフォルト値は 8 です。

コマンド モード

AP プロファイル コンフィギュレーション モード

コマンド履歴

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

例

次に、AP プロファイルで AP 地理位置情報の詳細タイミング測定（FTM）イニシエータのバーストサイズ値を設定する例を示します。

```
Device# configure terminal
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)#geolocation ftm initiator burst-size 8
```

group

施設および施設タイプのグループを設定するには、**group** コマンドを使用します。グループを削除するには、このコマンドの **no** 形式を使用します。

group *venue-group venue-type*

構文の説明

venue-group	施設グループ。オプション：**assembly**、**business**、**educational**、**industrial**、**institutional**、**mercantile**、**outdoor**、**residential**、**storage**、**unspecified**、**utility**、**vehicular**。
venue-type	場所のタイプ。オプションは venue-group によって異なります。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、施設および施設タイプのグループを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# group business bank
```

gtk-randomize

ホール 196 緩和のためにランダム GTK を設定するには、**gtk-randomize** コマンドを使用します。アイコンを削除するには、このコマンドの **no** 形式を使用します。

gtk-randomize

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

WLAN の設定（config-wlan）

コマンド履歴

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

使用上のガイドライン

各モバイル デバイスに使用される GTK は、BSS に関連付けられている他のモバイル デバイスに使用されるすべての GTK とは異なる必要があります。

例

次に、ホール 196 緩和のためにランダム GTK を設定する例を示します。

```
Device(config-wlan)# security wpa wpa2 gtk-randomize
```

gnxi（非セキュアモード）

gNXI は、gNMI および gNOI プロトコルを使用する、ネットワーク管理用のツールのコレクションです。その内容は次のとおりです。

- gNMI：gRPC ネットワーク管理インターフェイス
- gNOI：gRPC ネットワーク操作インターフェイス

gNMI は Google によって開発された gRPC ネットワーク管理インターフェイスです。gNMI はネットワークデバイスの設定をインストール、操作、および削除し、また、運用データの表示も実行するメカニズムです。gRPC ネットワーク操作インターフェイス（gNOI）は、ネットワークデバイス上で操作コマンドを実行するための gRPC ベースのマイクロサービスセットを定義します。

非セキュアモードで gNXI プロセスを設定して開始するには、**gnxi** コマンドを使用します。この機能を無効化するには、このコマンドの **no** 形式を使用します。

gnxi {port *port-number* **| secure-client-auth | seure-init | secure-password-auth | secure-peer-verify-trustpoint | secure-port | secure-server | secure-trustpoint | server}**

no gnxi {port *port-number* **| secure-client-auth | seure-init | secure-password-auth | secure-peer-verify-trustpoint | secure-port | secure-server | secure-trustpoint | server}**

構文の説明

gnxi	gNXI プロセスを開始します
port	gNXI サーバーポートを設定します
port-number	ポート番号を指定します。デフォルトのポート番号は 50052 です。
secure-client-auth	クライアント認証を使用して gNXI を設定します
secure-init	プライマリ自己署名証明書を使用して gNMI セキュアサーバーを有効にします
secure-password-auth	パスワード認証を使用して gNXI を設定します
secure-peer-verify-trustpoint	gNXI サーバーピア検証トラストポイントを設定します
secure-port	gNXI セキュアサーバーポートを設定します
secure-server	gNXI セキュアサーバーを有効にします
secure-trustpoint	gNXI サーバー証明書トラストポイントを設定します
server	gNXI サーバーを有効にします

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、gNIX サーバー（非セキュアモード）を設定する例を示します。

```
Device# configure terminal
Device(config)# gnxi server
Device(config)# end
```

gnxi（セキュアモード）

gNXI は、gNMI および gNOI プロトコルを使用する、ネットワーク管理用のツールのコレクションです。その内容は次のとおりです。

- gNMI：gRPC ネットワーク管理インターフェイス
- gNOI：gRPC ネットワーク操作インターフェイス

gNMI は Google によって開発された gRPC ネットワーク管理インターフェイスです。gNMI はネットワークデバイスの設定をインストール、操作、および削除し、また、運用データの表示も実行するメカニズムです。gRPC ネットワーク操作インターフェイス（gNOI）は、ネットワークデバイス上で操作コマンドを実行するための gRPC ベースのマイクロサービスセットを定義します。

セキュアモードで gNXI プロセスを設定して開始するには、**gnxi** コマンドを使用します。この機能を無効化するには、このコマンドの **no** 形式を使用します。

gnxi {secure-server | secure-trustpoint *trustpoint-name* **| secure-client-auth | secure-port}**

no gnxi {secure-server | secure-trustpoint *trustpoint-name* **| secure-client-auth | secure-port}**

構文の説明

gnxi	gNXI プロセスを開始します
secure-server	gNXI セキュアサーバーを有効にします
secure-trustpoint	gNXI サーバー証明書トラストポイントを設定します
trustpoint-name	トラストポイント名を指定します
secure-client-auth	クライアント認証を使用して gNXI を設定します
secure-port	gNXI セキュアサーバーポートを設定します

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、セキュアモードで gNIX サーバーとセキュアトラストポイントを設定する例を示します。

```
Device# configure terminal
```

```
Device(config)# gnxi secure-trustpoint <trustpoint-name>
Device(config)# end
```

hessid

同種の拡張サービス セットを設定するには、**hessid** コマンドを使用します。サービスセットを削除するには、このコマンドの **no** 形式を使用します。

hessid *HESSID-value*

構文の説明

HESSID-value	HESSID 値。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、同種の拡張サービスセットを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# hessid 00:40:96:b4:82:55
```

high-density clients count

AP無線ごとのクライアント接続の最大数を設定するには、RFプロファイルモードで**high-density clients count** コマンドを使用します。この機能を無効にするには、このコマンドの**no**形式を使用します。

high-density clients count *max-client-conn-per-radio*

[no] high-density clients count *max-client-conn-per-radio*

構文の説明

max-client-conn-per-radio	AP 無線あたりのクライアント接続の最大数を設定します。有効な範囲は、0 ～ 400 です。デフォルト値は 200 クライアント接続です。

コマンド デフォルト

なし

コマンド モード

RF コンフィギュレーション モード

コマンド履歴

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

例

次に、AP 無線あたりのクライアント接続の最大数を設定する例を示します。

```
Device(config)# ap dot11 5ghz rf-profile rfprofile
Device(config-rf-profile)# high-density clients count 30
```

hotspot anqp-server

ホットスポットサーバーをポリシープロファイルに関連付けるには、**hotspot anqp-server** コマンドを使用します。サーバーを削除するには、このコマンドの **no** 形式を使用します。

hotspot anqp-server *server-name*

構文の説明

server-name	Hotspot 2.0 ANQP サーバーの名前。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ポリシーの設定（config-wireless-policy）

コマンド履歴

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

例

次に、Hotspot 2.0 ANQP サーバーを設定する例を示します。

```
Device(config)# wireless profile policy hs-policy
Device(config-wireless-policy)# hotspot anqp-server test
```

hyperlocation

AP グループのハイパーロケーションと関連するパラメータを設定するには、WLAN AP グループ コンフィギュレーション（Device(config-apgroup)#）モードで **hyperlocation** コマンドを使用します。AP グループのハイパーロケーションと関連するパラメータを無効にするには、このコマンドの **no** 形式を使用します。

[no] hyperlocation ［**threshold** ｛**detection** *value-in-dBm* ｜ **reset** *value-btwn-0-99* ｜ **trigger** *value-btwn-1-100*｝］

構文の説明

[no] hyperlocation	AP グループのハイパーロケーションを有効または無効にします。
threshold detection *value-in-dBm*	低い RSSI を持つパケットを除外するためのしきい値を設定します。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。
threshold reset *value-btwn-0-99*	トリガー後のスキャンサイクルの値をリセットします。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。
threshold trigger *value-btwn-1-100*	BAR をクライアントに送信する前のスキャンサイクルの数を設定します。このコマンドの **[no]** 形式を使用すると、しきい値がデフォルト値にリセットされます。 （注） ハイパーロケーションしきい値のリセット値は、必ず、しきい値のトリガー値より小さくします。

コマンド モード

WLAN AP グループ コンフィギュレーション

コマンド履歴

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

- 次に、パケットをフィルタするためのしきい値を低い RSSI に設定する例を示します。

```
Device(config-apgroup)# [no] hyperlocation threshold detection -100
```

- 次に、トリガー後にスキャン サイクルの値をリセットする例を示します。

```
Device(config-apgroup)# [no] hyperlocation threshold reset 8
```

- 次に、BAR をクライアントに送信する前にスキャンサイクルの数を設定する例を示します。

```
Device(config-apgroup)# [no] hyperlocation threshold trigger 10
```

icon

オンラインサインアップ（OSU）プロバイダーのアイコンを設定するには、**icon** コマンドを使用します。アイコンを削除するには、このコマンドの **no** 形式を使用します。

icon *file-name*

構文の説明

file-name	アイコンのファイル名。

コマンド デフォルト

なし

コマンド モード

ANQP OSU プロバイダーの設定（config-anqp-osu-provider）

コマンド履歴

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

使用上のガイドライン

アイコンは、ホットスポット ANQP サーバで設定する必要があります。

例

次に、OSU プロバイダーのアイコンを設定する例を示します。

```
Device(config-wireless-anqp-server)# osu-provider my-osu
Device(config-anqp-osu-provider)# icon test
```

icap subscription client anomaly-detection report-individual enable aggregate

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

icap subscription client anomaly-detection report-individual enable aggregate

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

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

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# icap subscription client anomaly-detection report-individual
 enable aggregate
```

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

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

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

構文の説明

throttle value	クライアントごとのイベントレポートの数。有効な値の範囲は 0 ～ 50 です。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

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

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# icap subscription client anomaly-detection report-individual
 per-client throttle 10
```

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

AP で 5 分ごとにタイプ別の個別レポートを設定するには、**icap subscription client anomaly-detection report-individual per-type throttle** コマンドを使用します。

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

構文の説明

throttle value	クライアントごとのイベントレポートの数。有効な値の範囲は 0 ～ 100 です。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、AP で 5 分ごとにタイプ別の個別レポートを設定する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# icap subscription client anomaly-detection report-individual
 per-type throttle 80
```

icap subscription client exclude telemetry-data wlan

AP で iCAP フィルタリングを有効にするには、**icap subscription client exclude telemetry-data wlan** コマンドを使用します。

icap subscription client exclude telemetry-data wlan *wlan-profile-name*

構文の説明

wlan-profile-name	WLANプロファイルの名前を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.10.1	このコマンドが導入されました。

次に、AP で iCAP フィルタリングを有効にする例を示します。

```
Device# configure terminal
Device(config)# ap profile xyz-ap-profile
Device(config-ap-profile)# description "xyz ap profile"
Device(config-ap-profile)# icap subscription client exclude telemetry-data wlan wlan-name
```

idle-timeout

ワイヤレス プロファイル ポリシーの idle-timeout 値を秒単位で設定するには、 **idle-timeout** コマンドを使用します。

idle-timeout *value*

構文の説明

value	idle-timeout 値を設定します。有効な範囲は 15 ～ 100000 秒です。

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

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

例

次に、ワイヤレス プロファイル ポリシーの idle-timeout を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-profile-name
Device(config-wireless-policy)# idle-timeout 100
```

ids（メッシュ）

屋外メッシュ AP の IDS（不正/シグネチャ検出）レポートを設定するには、**ids** コマンドを使用します。

ids

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

IDS は無効になっています。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

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

例

次に、屋外メッシュ AP の IDS（不正/シグニチャ検出）レポートを設定する例を示します。

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

inactive-timeout

in-active タイマーを有効にするには、**inactive-timeout** コマンドを使用します。

inactive-timeout *timeout-in-seconds*

構文の説明

timeout-in-seconds	非アクティブ フローのタイムアウト値を指定します。値の範囲は1～604800です。

コマンド デフォルト

なし

コマンド モード

ET-Analytics コンフィギュレーション

コマンド履歴

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

次に、ET-Analytics コンフィギュレーション モードで非アクティブタイマーを有効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# et-analytics
デバイス(config-et-analytics)# inactive-timeout 15
デバイス(config-et-analytics)# end
```

inner-auth-eap

内部認証の Extensible Authentication Protocol（EAP）方式を設定するには、**inner-auth-eap** コマンドを使用します。内部認証の EAP 方式を削除するには、このコマンドの **no** 形式を使用します。

inner-auth-eap {**eap-aka** | **eap-fast** | **eap-leap** | **eap-peap** | **eap-sim** | **eap-tls** | **eap-ttls**}

構文の説明

eap-aka	EAP 認証とキー共有の方式を有効にします。 EAP-AKA は、UMTS Subscriber Identity Module を使用した認証とセッションキー配布のための EAP メカニズムです。
eap-fast	セキュアトンネリング方式による EAP フレキシブル認証を有効にします。 EAP-FAST は、サプリカントとサーバーの相互認証を可能にするフレキシブル EAP プロトコルです。これは EAP-PEAP に似ていますが、通常はクライアント証明書またはサーバー証明書を使用する必要はありません。
eap-leap	EAP Lightweight Extensible Authentication Protocol 方式を有効にします。 EAP-LEAP は、主に Cisco Aironet WLAN で使用される EAP 認証プロトコルです。動的に生成された Wired Equivalent Privacy（WEP）キーを使用してデータ伝送を暗号化し、相互認証をサポートします。
eap-peap	EAP Protected Extensible Authentication Protocol 方式を有効にします。 EAP-PEAP は、ワイヤレスネットワークとポイントツーポイント接続で使用される EAP 認証プロトコルです。PEAP は、802.1X ポートアクセス制御をサポートする 802.11 WLAN でよりセキュアな認証を提供するために設計されています。
eap-sim	EAP Subscriber Identity Module 方式を有効にします。 EAP-SIM は、Global System for Mobile Communications（GSM）の Subscriber Identity Module（SIM）を使用した、認証とセッションキー配布に使用される EAP 認証プロトコルです。
eap-tls	EAP Transport Layer Security 方式を有効にします。 EAP-TLS は EAP 認証プロトコルであり、Transport Layer Security（TLS）プロトコルを使用する IETF オープン標準です。EAP-TLS は、オリジナルの標準ワイヤレス LAN EAP 認証プロトコルです。
eap-ttls	EAP Tunneled Transport Layer Security 方式を有効にします。 EAP-TTLS はシンプルな WPA2 エンタープライズ Wi-Fi 認証方式であり、長年にわたって標準システムとなっています。ユーザーがネットワークに接続する場合、デバイスはネットワークとの通信を開始し、サーバー証明書を識別することで正しいネットワークであることを確認します。

コマンド デフォルト

なし

コマンド モード

ANQP NAI EAP 認証コンフィギュレーション（config-anqp-nai-eap-auth）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.1	このコマンドは、Cisco IOS XE Amsterdam 17.3.1 よりも前のリリースで導入されました。

使用上のガイドライン

Cisco IOS XE Amsterdam 17.3.1 より前では、1 つの内部 EAP 認証方式のみが許可されていました。たとえば、**inner-auth-eap eap-aka** です。複数の内部 EAP 認証方式（**inner-auth-eap eap-aka** と **inner-auth-eap eap-fast** など）を使用した場合は、最後の方式のみが使用され、前の方式は破棄されていました。Cisco IOS XE Amsterdam 17.3.1 以降では、複数の内部 EAP 認証方式を設定できます。例については、以下のコードスニペットを参照してください。

```
wireless hotspot anqp-server my_anqp
nai-realm myvenue.cisco.com
eap-method eap-aka
credential certificate
credential usim
inner-auth-eap eap-aka
inner-auth-eap eap-fast
inner-auth-non-eap chap
inner-auth-non-eap pap
tunneled-eap-credential anonymous
tunneled-eap-credential softoken
```

例

次に、内部認証の EAP 方式を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless hotspot anqp-server my_anqp
Device(config-wireless-anqp-server)# nai-realm myvenue.cisco.com
Device(config-anqp-nai-eap)# eap-method eap-aka
Device(config-anqp-nai-eap-auth)#inner-auth-eap eap-aka
```

inner-auth-non-eap

内部認証の Extensible Authentication Protocol（EAP）以外の方式を設定するには、**inner-auth-non-eap** コマンドを使用します。内部認証の EAP 以外の方式を削除するには、このコマンドの **no** 形式を使用します。

inner-auth-non-eap {**chap** | **mschap** | **mschap-v2** | **pap**}

構文の説明

chap	チャレンジハンドシェイク認証プロトコル方式。 CHAP は、リモートクライアントのアイデンティティを検証するために Point-to-Point Protocol（PPP）サーバーで使用される認証スキームです。CHAP は 3 ウェイハンドシェイクを使用して定期的にクライアントのアイデンティティを確認します。
mschap	Microsoft チャレンジハンドシェイク認証プロトコル方式。
mschap-v2	Microsoft チャレンジハンドシェイク認証プロトコルバージョン 2 方式。
pap	パスワード認証プロトコル方式。 PAP は、ユーザーを検証するために PPP で使用されるパスワードベースの認証プロトコルです。

コマンド デフォルト

なし

コマンド モード

ANQP NAI EAP 認証コンフィギュレーション（config-anqp-nai-eap-auth）

コマンド履歴

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

例

次に、内部認証の EAP 以外の方式を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless hotspot anqp-server my_anqp
Device(config-wireless-anqp-server)# nai-realm myvenue.cisco.com
Device(config-anqp-nai-eap)# eap-method eap-aka
Device(config-anqp-nai-eap-auth)#inner-auth-eap pap
```

install abort

進行中の事前ダウンロードまたはローリングアクセスポイント（AP）のアップグレード操作をキャンセルするには、**install abort** コマンドを使用します。

install abort

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、現在の事前ダウンロードまたはインストール操作をキャンセルする例を示します。

```
Device# install abort
```

install add file activate commit

インストール済みSMUパッケージをアクティブ化し、ロードパスの変更をコミットするには、**install add file activate commit** コマンドを使用します。

install add file activate commit

構文の説明

prompt-level	プロンプトレベルを設定します。
none	プロンプトは実行されません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、インストール済みパッケージをアクティブ化し、変更をコミットする例を示します。

```
Device# install add file vwlc_apsp_16.11.1.0_74.bin activate commit
```

install add file flash activate issu commit

issu 技術を使用してインストールされたパッケージをアクティブ化し、ロードパスの変更をコミットするには、**install add file flash activate issu commit** コマンドを使用します。

install add file flash activate issu commit

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、issu 技術を使用してインストールされたパッケージをアクティブ化し、ロードパスの変更をコミットする例を示します。

```
Device# install add file flash activate issu commit
```

install add profile

AP イメージ事前ダウンロード サポートを使用して AP イメージをロールバックするためのプロファイルを選択するには、**install add profile** コマンドを使用します。

install add profile *profile-name* [**activate**]

構文の説明

profile-name	プロファイル名。プロファイル名は最大 15 文字です。
activate	インストール済みパッケージをアクティブ化します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、APイメージをロールバックするためのプロファイルを選択する例を示します。

```
Device# install add profile profile1
```

install activate

インストール済みパッケージをアクティブ化するには、**install activate** コマンドを使用します。

install activate {**auto-abort-timer** | **file** | **profile** | **prompt-level**}

構文の説明

auto-abort-timer	キャンセルタイマーを設定します。時間範囲は 30 ～ 1200 分です。
file	アクティブにするパッケージを指定します。
profile	アクティブにするプロファイルを指定します。
prompt-level	プロンプト レベルを設定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.2s	このコマンドが導入されました。

例

次に、インストール済みパッケージをアクティブ化する例を示します。

```
Device# install activate profile default
install_activate: START Thu Nov 24 20:14:53 UTC 2019

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q] y
Building configuration...
[OK]Modified configuration has been saved
Jan 24 20:15:02.745: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 activate
Jan 24 20:15:02.745 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 activate
install_activate: Activating PACKAGE
```

install activate profile

インストール済みパッケージをアクティブ化するには、**install activate profile** コマンドを使用します。

install activate profile

構文の説明

profile	プロファイルをアクティブにします。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.2s	このコマンドが導入されました。

例

次に、インストール済みパッケージをアクティブ化する例を示します。

```
Device#install activate profile default
install_activate: START Thu Nov 24 20:14:53 UTC 2019

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q] y
Building configuration...
[OK]Modified configuration has been saved
Jan 24 20:15:02.745: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 activate
Jan 24 20:15:02.745 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 activate
install_activate: Activating PACKAGE
```

install activate file

インストール済みパッケージをアクティブ化するには、**install activate file** コマンドを使用します。

install activate file *file-name*

構文の説明

file-name	パッケージ名を指定します。オプションは、bootflash:、flash:、および webui: です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、スタンバイロケーションでインストールパッケージをアクティブ化しているときに自動キャンセルタイマーを使用する例を示します。

```
Device# install activate file vwlc_apsp_16.11.1.0_74.bin
```

install commit

ロードパスの変更をコミットするには、**install commit** コマンドを使用します。

install commit

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、ロードパスの変更をコミットする例を示します。

```
Device# install commit
```

install remove profile default

削除するインストールパッケージを指定するには、**install remove profile default** コマンドを使用します。

install remove profile default

構文の説明

remove	インストールパッケージを削除します。
profile	削除するプロファイルを指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、デフォルトプロファイルを削除する例を示します。

```
Device# install remove profile default
```

install deactivate

非アクティブ化するインストール パッケージを指定するには、**install deactivate file** コマンドを使用します。

install deactivate file *file-name*

構文の説明

file-name	パッケージ名を指定します。オプションは、bootflash:、flash:、および webui: です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、インストールパッケージを非アクティブ化する例を示します。

```
Device# install deactivate file vwlc_apsp_16.11.1.0_74.bin
```

install deactivate

非アクティブ化するインストール パッケージを指定するには、**install deactivate file** コマンドを使用します。

install deactivate file *file-name*

構文の説明

file-name	パッケージ名を指定します。オプションは、bootflash:、flash:、および webui: です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、インストールパッケージを非アクティブ化する例を示します。

```
Device# install deactivate file vwlc_apsp_16.11.1.0_74.bin
```

install prepare

操作をキャンセル、アクティブ化、または非アクティブ化するための SMU パッケージを準備するには、**install prepare** コマンドを使用します。

install prepare {**abort** | **activate file** *file-name* | **deactivate file** *file-name* }

構文の説明

abort	操作のキャンセル用の SMU パッケージを準備します。
activate file	アクティベーション用のSMUパッケージを準備します。
file-name	パッケージ名。
deactivate file	非アクティブ化用の SMU パッケージを準備します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、操作のキャンセル、アクティブ化、または非アクティブ化のためのパッケージを準備する例を示します。

```
Device# install prepare abort
Device# install prepare activate file vwlc_apsp_16.11.1.0_74.bin
Device# install prepare deactivate file vwlc_apsp_16.11.1.0_74.bin
```

install prepare rollback

ロールバック操作用の SMU パッケージを準備するには、**install prepare rollback** コマンドを使用します。

install prepare rollback to {**base** | **committed** | **id** *id* | **label** *label*}

構文の説明

base	ベース イメージへのロールバックを準備します。
committed	最後にコミットされたインストレーション ポイントへのロールバックを準備します。
id	最後にコミットされたインストレーション ポイントへのロールバックを準備します。
id	ロールバック先のインストール ポイントの識別子。
label	特定のインストール ポイント ラベルへのロールバックを準備します。
label	最大 15 文字のラベル名。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、特定の id にロールバックするためのパッケージを準備する例を示します。

```
Device# install prepare rollback to id 2
```

install rollback

特定のインストール ポイントにロールバックするには、**install rollback** コマンドを使用します。

install rollback to {**base** | **committed** | **id** *id* | **label** *label*} [**prompt-level none**]

構文の説明

base	ベース イメージにロールバックします。
prompt-level none	プロンプト レベルをなしに設定します。
committed	最後にコミットされたインストレーション ポイントにロールバックします。
id	特定のインストール ポイント ID にロールバックします。
label	特定のインストール ポイント ラベルにロールバックします。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、ロールバック先のインストール ポイントの ID を指定する例を示します。

```
Device# install rollback to id 1
```

interface vlan

ダイナミック スイッチ仮想インターフェイス（SVI）を作成するか、既存のダイナミック SVI にアクセスし、インターフェイス コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **interface vlan** コマンドを使用します。SVI を削除するには、このコマンドの **no** 形式を使用します。

interface vlan *vlan-id*
no interface vlan *vlan-id*

構文の説明

vlan-id	VLAN 番号。指定できる範囲は 1 ～ 4094 です。

コマンド デフォルト

デフォルトの VLAN インターフェイスは VLAN 1 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

SVI は、特定の VLAN に対して最初に **interface vlan** *vlan-id* コマンドを入力したときに作成されます。*vlan-id* は、IEEE 802.1Q カプセル化トランク上のデータ フレームに対応する VLAN タグ、またはアクセス ポート用に設定された VLAN ID に対応します。

（注） 物理ポートと関連付けられていない場合、SVI を作成してもアクティブにはなりません。

no interface vlan *vlan-id* コマンドを使用して削除した SVI は、**show interfaces** 特権 EXEC コマンドの出力に表示されなくなります。

（注） VLAN 1 インターフェイスを削除することはできません。

削除されたインターフェイスに対して **interface vlan** *vlan-id* コマンドを入力すると、削除された SVI を元に戻すことができます。インターフェイスはバックアップとなりますが、それまでの設定は削除されます。

シャーシまたはシャーシスタック上で設定された SVI の数と、設定された他の機能の数の相互関係によっては、ハードウェア制限により、CPU 使用率に影響が出る可能性があります。**sdm prefer** グローバル コンフィギュレーション コマンドを使用して、システムのハードウェア リソースを、テンプレートおよび機能テーブルに基づいて再度割り当てることができます。

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

次の例では、VLAN ID 23 の新しい SVI を作成し、インターフェイス コンフィギュレーション モードを開始する方法を示します。

```
デバイス(config)# interface vlan 23
デバイス(config-if)#
```

ip access-group

WLAN アクセス コントロール グループ（ACL）を設定するには、**ip access-group** コマンドを使用します。WLAN ACL グループを削除するには、このコマンドの **no** 形式を使用します。

ip access-group [**web**] *acl-name*
no ip access-group [**web**]

構文の説明

web	（任意）IPv4 Web ACL を設定します。
acl-name	セキュリティ タイプ値を webauth として、WLAN に使用する preauth ACL を指定します。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

使用上のガイドライン

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

コマンド履歴

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

次に、WLAN ACL を設定する例を示します。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#wlan wlan1
デバイス(config-wlan)#ip access-group test-acl
```

次に、IPv4 WLAN Web ACL を設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wlan wlan1
デバイス(config-wlan)# ip access-group web test
デバイス(config-wlan)#
```

ip access-list extended

拡張アクセス リストを設定するには、**ip access-list extended** コマンドを使用します。

ip access-list extended {**<100-199>** | **<2000-2699>** *access-list-name*}

構文の説明

<100-199>	拡張 IP アクセス リスト番号。
<2000-2699>	拡張 IP アクセス リスト番号（拡張範囲）。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、拡張アクセス リストを作成する例を示します。

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

ip address

インターフェイスのプライマリまたはセカンダリ IP アドレスを設定するには、インターフェイス コンフィギュレーション モードで **ip address** コマンドを使用します。IP アドレスを削除するか、IP 処理を無効にするには、このコマンドの no 形式を使用します。

ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
no ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

構文の説明

ip-address	IP アドレス。
mask	関連する IP サブネットのマスク。
secondary	（任意）設定されたアドレスをセカンダリ IP アドレスに指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。 （注） セカンダリ アドレスが **vrf** のキーワードでの VRF テーブルの設定に使用される場合には、**vrf** キーワードも指定する必要があります。
vrf	（任意）VRF テーブルの名前*vrf-name* 引数は、入力インターフェイスの VRF 名を指定します。

コマンド デフォルト

IP アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

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

使用上のガイドライン

インターフェイスには、1 つのプライマリ IP アドレスと複数のセカンダリ IP アドレスを設定できます。Cisco IOS ソフトウェアにより生成されるパケットは、必ずプライマリ IP アドレスを使用します。そのため、セグメントのすべてのデバイスとアクセス サーバは、同じプライマリ ネットワーク番号を共有する必要があります。

ホストは、Internet Control Message Protocol（ICMP）マスク要求メッセージを使用して、サブネット マスクを判別できます。デバイスは、ICMP マスク応答メッセージでこの要求に応答できます。

no ip address コマンドを使用して IP アドレスを削除することにより、特定のインターフェイス上の IP 処理を無効にできます。ソフトウェアが、その IP アドレスのいずれかを使用する別のホストを検出すると、コンソールにエラー メッセージを出力します。

オプションの **secondary** キーワードを使用すると、セカンダリ アドレスを無制限に指定できます。システムがセカンダリの送信元アドレスのルーティングの更新以外にデータグラムを生成

しないということを除けば、セカンダリ アドレスはプライマリ アドレスのように処理されます。IP ブロードキャストおよび Address Resolution Protocol（ARP）要求は、IP ルーティング テーブルのインターフェイス ルートのように、正しく処理されます。

セカンダリ IP アドレスは、さまざまな状況で使用できます。次に、一般的な使用状況を示します。

- 特定のネットワーク セグメントに十分なホストアドレスがない場合。たとえば、サブネット化により、論理サブネットあたり最大 254 のホストを使用できますが、1 つの物理サブネットでは、300 のホストアドレスが必要になります。デバイスまたはアクセス サーバでセカンダリ IP アドレスを使用すると、2 つの論理サブネットで 1 つの物理サブネットを使用できます。
- レベル 2 ブリッジを使用して構築された旧式ネットワークがたくさんある場合。セカンダリ アドレスは、慎重に使用することで、サブネット化されたデバイスベース ネットワークへの移行に役立ちます。旧式のブリッジセグメントのデバイスでは、そのセグメントに複数のサブネットがあることを簡単に認識させることができます。
- 1 つのネットワークの 2 つのサブネットは、別の方法で、別のネットワークにより分離できる場合があります。サブネットが使用中の場合、この状況は許可されません。このような場合、最初のネットワークは、セカンダリ アドレスを使用している 2 番目のネットワークの上に拡張されます。つまり、上の階層となります。

（注）

- ネットワーク セグメント上のすべてのデバイスがセカンダリ アドレスを使用した場合、同一のセグメント上にある他のデバイスも、同一のネットワークまたはサブネットからセカンダリ アドレスを使用しなければなりません。ネットワーク セグメント上のセカンダリ アドレスの使用に矛盾があると、ただちにルーティング ループが引き起こされる可能性があります。
- Open Shortest Path First（OSPF）アルゴリズムを使用してルーティングする場合は、インターフェイスのすべてのセカンダリ アドレスがプライマリ アドレスと同じ OSPF エリアにあることを確認してください。
- セカンダリ IP アドレスを設定する場合は、CPU 使用率が高くならないように、**no ip redirects** コマンドを入力して ICMP リダイレクトメッセージの送信を無効にする必要があります。

例

次の例では、192.108.1.27 が プライマリ アドレスで、192.31.7.17 が GigabitEthernet インターフェイス 1/0/1 のセカンダリ アドレスです。

```
Device# enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 192.108.1.27 255.255.255.0
Device(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
```

関連コマンド

コマンド	説明
match ip route-source	送信元 IP アドレスを、VRF で接続されたルートに基づいて設定された必要なルート マップに一致するように指定します。
route-map	1 つのルーティング プロトコルから他のルーティング プロトコルへのルートを再配布するか、またはポリシー ルーティングを有効にするための条件を定義します。
set vrf	ポリシーベース ルーティング VRF の選択のために、ルート マップ内で VPN VRF 選択を有効にします。
show ip arp	SLIP アドレスが固定 ARP テーブル エントリとして表示される ARP キャッシュを表示します。
show ip interface	IP 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。
show route-map	静的ルートマップと動的ルートマップを表示します。

ip arp-limit rate

Address Resolution Protocol（ARP）パケットのレート制限を設定するには、**ip arp-limit rate** コマンドを使用します。

ip arp-limit rate { **burst-interval** *burst-interval* | **none** | **pps** *pps* }

構文の説明

pps	1 秒あたりにクライアントに許可される ARP パケットの最大数。クライアントごとに受信したパケットが設定された制限を超えると、パケットがドロップされます。有効な値の範囲は 15 ～ 1500 で、デフォルト値は 100 秒です。
burst-interval	クライアントを除外するためのバースト間隔（秒単位）。ARP pps が設定された値を超えると、クライアントがブロックリストに登録されます。有効な値の範囲は 3 ～ 255 で、デフォルト値は 5 秒です。
none	ARP レート制限を無効にします。

コマンド デフォルト

デフォルト値が設定されています。

コマンド モード

ワイヤレス ポリシー プロファイル コンフィギュレーション（config-wireless-policy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.5	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Cisco IOS XE Amsterdam 17.3.5 以降、Cisco IOS XE Bengaluru 17.6.3 以降、および Cisco IOS XE Cupertino 17.8.1 以降のリリースでのみ使用できます。

RLAN の場合、デフォルト値が使用されます。このコマンドを使用して値を変更することはできません。

例

次に、ARP パケットのレート制限を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile policy test1
Device(config-wireless-policy)# ip arp-limit rate pps 90
```

ip admission

Web 認証を有効にするには、インターフェイス コンフィギュレーション モードで **ip admission** コマンドを使用します。このコマンドは、フォールバック プロファイル コンフィギュレーション モードでも使用できます。Web 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip admission *rule*
no ip admission *rule*

構文の説明

rule	IP アドミッションルールの名前。

コマンド デフォルト

Web 認証はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

フォールバック プロファイル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

ip admission コマンドはスイッチポートに web 認証ルールを適用します。

次の例では、スイッチポートに Web 認証ルールを適用する方法を示します。

```
デバイス# configure terminal
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip admission rule1
```

次の例では、IEEE 802.1X 対応のスイッチポートで使用するフォールバックプロファイルに Web 認証ルールを適用する方法を示します。

```
デバイス# configure terminal
デバイス(config)# fallback profile profile1
デバイス(config-fallback-profile)# ip admission rule1
```

ip dhcp pool

DHCP サーバで Dynamic Host Configuration Protocol（DHCP）アドレス プールを設定し、DHCP プール コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ip dhcp pool** コマンドを使用します。アドレス プールを削除するには、このコマンドの no 形式を使用します。

ip dhcp pool *name*
no ip dhcp pool *name*

構文の説明

name	プールの名前象徴的な文字列（engineering など）または整数（0 など）を使用できます。

コマンド デフォルト

DHCP アドレス プールは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.0(1)T	このコマンドが導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

このコマンドの実行中、コンフィギュレーション モードが DHCP プール コンフィギュレーション モードに変わります。これは (config-dhcp)# プロンプトで識別されます。このモードでは、管理者は IP サブネット番号やデフォルト ルータ リストなどのプール パラメータを設定できます。

例

次の例では、DHCP アドレス プールとして pool1 を設定しています。

```
ip dhcp pool pool1
```

関連コマンド

コマンド	説明
host	DHCP クライアントに手動でバインドするための IP アドレスおよびネットワーク マスクを指定します。
ip dhcp excluded-address	Cisco IOS DHCP サーバーが DHCP クライアントに割り当ててはいけない IP アドレスを指定します。

コマンド	説明
network (DHCP)	Cisco IOS DHCP サーバの DHCP アドレス プールに、サブネットの番号およびマスクを設定します。

ip dhcp-relay information option server-override

Dynamic Host Configuration Protocol（DHCP）サーバに転送された BOOTREQUEST メッセージの DHCP リレー エージェント情報オプションに、サーバ ID オーバーライドとリンク選択のサブオプションをシステムがグローバルに挿入できるようにするには、グローバル コンフィギュレーション モードで **ip dhcp-relay information option server-override** コマンドを使用します。DHCP リレー エージェント情報オプションへのサーバ ID オーバーライドとリンク選択のサブオプションの挿入を無効にするには、このコマンドの **no** 形式を使用します。

ip dhcp-relay information option server-override
no ip dhcp-relay information option server-override

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

サーバー ID オーバーライドとリンク選択のサブオプションは、DHCP リレー エージェント情報オプションには挿入されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

コマンド履歴

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

使用上のガイドライン

ip dhcp-relay information option server-override コマンドは、DHCP ブロードキャストがクライアントから DHCP サーバにリレー エージェントによって転送された場合、リレー エージェント情報オプションに次のサブオプションを追加します。

- サーバー ID オーバーライド サブオプション
- リンク選択サブオプション

このコマンドが設定されている場合、ゲートウェイ アドレス（giaddr）は DHCP サーバから到達可能なインターフェイスである発信インターフェイスの IP アドレスに設定されます。

ip dhcp relay information option server-id-override コマンドがインターフェイスで設定されている場合、このインターフェイスのグローバル設定のみが上書きされます。

例

次の例では、DHCP リレーによって、DHCP パケットのリレー情報オプションに、サーバー ID のオーバーライドとリンク選択サブオプションが挿入されます。ループバックインターフェイスの IP アドレスが、中継されたメッセージの送信元 IP アドレスになるように設定されます。

```
Device(config)# ip dhcp-relay information option server-override
Device(config)# ip dhcp-relay source-interface loopback 0
Device(config)# interface Loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

関連コマンド

コマンド	説明
ip dhcp relay information option server-id-override	DHCP サーバーに転送される BOOTREQUEST メッセージの DHCP リレー エージェント情報オプションに、サーバー ID オーバーライドとリンク選択のサブオプションをシステムが特定のインターフェイスで挿入できるようにします。

ip dhcp-relay source-interface

中継されたメッセージの送信元 IP アドレスを使用するようにリレー エージェントの送信元インターフェイスをグローバルに設定するには、グローバル コンフィギュレーション モードで **ip dhcp-relay source-interface** コマンドを使用します。送信元インターフェイス設定を削除するには、このコマンドの **no** 形式を使用します。

ip dhcp-relay source-interface *type number*
no ip dhcp-relay source-interface *type number*

構文の説明

type	インターフェイス タイプ。詳細については、疑問符（?）オンライン ヘルプ機能を使用します。
number	インターフェイスまたはサブインターフェイスの番号。ネットワーキング デバイスに対する番号付けシステムの詳細については、疑問符（?）のオンライン ヘルプ機能を使用してください。

コマンド デフォルト

送信元インターフェイスは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。
12.2(33)SRE	このコマンドが、Cisco IOS Release 12.2(33)SRE に統合されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

使用上のガイドライン

ip dhcp-relay source-interface コマンドにより、ネットワーク管理者は中継されたメッセージの安定した、ハードウェアに依存しない IP アドレス（ループバック インターフェイスなど）を指定し、送信元 IP アドレスとしてリレー エージェントを使用することができます。

ip dhcp-relay source-interface グローバル コンフィギュレーション コマンドは設定され、**ip dhcp relay source-interface** コマンドも設定されている場合、**ip dhcp relay source-interface** コマンドはグローバル コンフィギュレーション モードよりも優先されます。ただし、インターフェイス コンフィギュレーションがないインターフェイスにはグローバル コンフィギュレーションが適用されます。

例

次の例では、ループバック インターフェイスの IP アドレスが、中継されたメッセージの送信元 IP アドレスになるように設定されています。

```
Device(config)# ip dhcp-relay source-interface loopback 0
```

```
Device(config)# interface loopback 0
Device(config-if)# ip address 10.2.2.1 255.255.255.0
```

関連コマンド

コマンド	説明
ip dhcp relay source-interface	中継されたメッセージの送信元 IP アドレスとして使用するように、リレー エージェントの送信元インターフェイスを設定します。

ip dhcp compatibility suboption

サーバーオーバーライドおよびリンク選択のサブオプションを RFC またはシスコ固有の値に設定するには、**ip dhcp compatibility suboption** [**server-override** | **link-selection**] コマンドを使用します。

ip dhcp compatibility suboption server-override [cisco | standard]
ip dhcp compatibility suboption link-selection [cisco | standard]

構文の説明

server-override	サーバー オーバーライド サブオプションを RFC またはシスコ固有の値に設定します。
link-selection	link-selection サブオプションを RFC またはシスコ固有の値に設定します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

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

使用上のガイドライン

次に、サーバーオーバーライドにより DHCP オプション 82 を設定する例を示します。

```
Device# configure terminal
Device(config)# ip dhcp compatibility suboption server-override cisco
Device(config)# ip dhcp compatibility suboption link-selection cisco
Device(config)# end
```

ip domain lookup

IP ドメインネームシステム（DNS）ベースのホスト名からアドレスへの変換を有効にするには、グローバル コンフィギュレーション モードで **ip domain lookup** コマンドを使用します。DNS ベースのホスト名からアドレスへの変換を無効にするには、このコマンドの **no** 形式を使用します。

ip domain lookup [**nsap** | **recursive** | **source-interface** *interface-type-number* | **vrf** *vrf-name* { **source-interface** *interface-type-number* }]

構文の説明

nsap	（任意）Connectionless Network Service（CLNS）および Network Service Access Point（NSAP）のアドレスの IP DNS クエリを有効にします。
recursive	（任意）IP DNS 再帰ルックアップを有効にします。
source-interface *interface-type-number*	（任意）DNS リゾルバの送信元インターフェイスを指定します。インターフェイスのタイプと番号を入力します。
vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）テーブルを定義します。vrf-name には、VRF テーブルの名前を入力します。

コマンド デフォルト

IP DNS ベースでのホスト名からアドレスへの変換が有効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Dublin 17.12.1	レイヤ 3 物理インターフェイスでの **ip domain lookup source-interface** *interface-type-number* コマンドの設定に関連する問題が解決されました。 このリリース以降、レイヤ 3 物理インターフェイスで設定されている場合でも、リロードされた場合およびポートモードが変更された場合にこのコマンドが保持されます。

使用上のガイドライン

デバイスでこのコマンドが有効になっている場合、**show tcp brief** コマンドを実行すると、出力の表示が非常に遅くなることがあります。

デバイスで IP と ISO CLNS の両方が有効になっている場合、**ip domain lookup nsap** コマンドでは、ホスト名を指定していれば、完全な CLNS アドレスを指定しなくても CLNS アドレスを検出できます。

このコマンドは、**ping**（ISO CLNS）コマンドおよび CLNS Telnet 接続に役立ちます。

レイヤ 3 物理インターフェイスで **ip domain lookup source-interface** *interface-type-number* コマンドを設定する場合は、ポートモードが変更された場合、またはデバイスがリロードされた場合、このコマンドが実行コンフィギュレーションから自動的に削除されることに注意してください（これが発生した場合は、**show running-configuration** 特権 EXEC コマンドの出力を参照してください）。コマンドが削除されると、指定された送信元インターフェイスを使用する DNS クエリがドロップされます。これは、コマンドを再設定することでのみ回避できます。Cisco IOS XE Dublin 17.12.1 以降では、この問題は解決されています。

例

次に、IP DNS ベースのホスト名からアドレスへの変換を設定する例を示します。

```
Device# configure terminal
Device(config)# ip domain lookup
Device(config)# end
```

次に、DNS ドメインルックアップの送信元インターフェイスを設定する例を示します。

```
Device# configure terminal
Device(config)# ip domain lookup source-interface gigabitethernet1/0/2
Device(config)# end
```

ip domain-name

デバイスでホスト ドメインを設定するには、**ip domain-name** コマンドを使用します。

ip domain-name *domain-name*[**vrf** *vrf-name*]

構文の説明

domain-name	デフォルト ドメイン名。
vrf-name	ドメイン名の解決に使用される VRF を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、デバイスでホスト ドメインを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip domain-name domain-name
```

ip flow-export destination

ETA フロー エクスポートの宛先を設定するには、**ip flow-export destination** コマンドを使用します。

ip flow-export destination *ip_address port_number*

構文の説明

port_number	ポート番号。有効な範囲は 1 ～ 65535 です。

コマンド デフォルト

なし

コマンド モード

ET-Analytics コンフィギュレーション

コマンド履歴

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

次に、ET 分析コンフィギュレーション モードで ETA フロー エクスポートの宛先を設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# et-analytics
デバイス(config-et-analytics)# ip flow-export
destination 120.0.0.1 2055
デバイス(config-et-analytics)# end
```

ip helper-address

インターフェイスで受信したユーザデータグラムプロトコル（UDP）ブロードキャスト（ブーツストラップ プロトコル（BOOTP）を含む）の転送を有効にするには、インターフェイス コンフィギュレーション モードで **ip helper-address** コマンドを使用します。特定のアドレスへのブロードキャスト パケットの転送を無効にするには、このコマンドの **no** 形式を使用します。

ip helper-address[{**vrf** *name* | **global**}] *address* {[**redundancy** *vrg-name*]}
no ip helper-address [{**vrf** *name* | **global**}] *address* {[**redundancy** *vrg-name*]}

構文の説明

vrf *name*	（任意）VPN ルーティング、フォワーディング（VRF）インスタンス、および VRF 名を有効にします。
global	（任意）グローバル ルーティング テーブルを設定します。
address	UDP ブロードキャストの転送時に使用される宛先ブロードキャストまたはホスト アドレス。インターフェイスごとに複数のヘルパー アドレスを使用できます。
redundancy *vrg-name*	（任意）仮想ルータ グループ（VRG）の名前を定義します。

コマンド デフォルト

UDP ブロードキャストは転送されません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。
12.2(4)B	このコマンドが変更されました。**vrf** *name* キーワードと引数のペアおよび **global** キーワードが追加されました。
12.2(15)T	このコマンドが変更されました。**redundancy** *vrg-name* キーワードと引数のペアが追加されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。

使用上のガイドライン

ip forward-protocol コマンドと **ip helper-address** コマンドを使用すると、転送されたブロードキャスト パケットおよびプロトコルを制御できます。

ヘルパー アドレスを必要とする 1 つのコモン アプリケーションは、RFC 1531 で定義されている DHCP です。クライアント セットで BOOTP または DHCP ブロードキャスト転送を有効にするには、クライアントに接続されたルータ インターフェイスでヘルパー アドレスを設定します。ヘルパー アドレスは、BOOTP または DHCP サーバのアドレスを指定する必要があります。複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定します。

UDP または IP パケットで **ip helper-address** コマンドを使用できるようにするには、次の条件を満たす必要があります。

- 受信したフレームの MAC アドレスは、すべてが 1 のブロードキャスト アドレス（ffff.ffff.ffff）である必要があります。
- IP の宛先アドレスは、すべてが 1 のブロードキャスト（255.255.255.255）または受信インターフェイスのサブネット ブロードキャストであるか、あるいは **no ip classless** コマンドも設定されている場合には受信インターフェイスのメジャーネットブロードキャストである必要があります。
- IP の存続可能時間（TTL）値は 2 以上である必要があります。
- IP プロトコルは UDP（17）である必要があります。
- UDP 宛先ポートは、TFTP、ドメイン ネーム システム（DNS）、時間、NetBIOS、ND、BOOTP や DHCP パケット、またはグローバル コンフィギュレーション モードで **ip forward-protocol udp** コマンドによって指定された UDP ポート用である必要があります。

DHCP サーバが VPN または VPN とは異なるグローバル空間に存在する場合は、**vrf** *name* または **global** オプションを使用すると、VRF の名前または DHCP サーバが存在するグローバル空間を指定できます。

ip helper-addressvrf*name address* オプションは、着信インターフェイスの VRF に関係なく、VRF 名に関連付けられているアドレスを使用します。**ip helper-addressvrf***name address* コマンドが設定された後に、VRF が設定から削除されると、この VRF に関連付けられたすべての IP ヘルパー アドレスがインターフェイス コンフィギュレーションから削除されます。

ip helper-address *address* コマンドが、VRF 名が設定されていないインターフェイスですでに設定され、このインターフェイスが **ip helper-address vrf** *name address* コマンドを使用して設定されている場合、以前に設定した **ip helper-address** *address* コマンドはグローバルと見なされます。

（注） ルータはパケットが物理ブロードキャストなのかを判断できないため、**ip helper-address** コマンドは宛先ルータの X.25 インターフェイスでは機能しません。

IP ヘルパー ステートメントが DHCP と連携できるようにするには、ルータで **service dhcp** コマンドを設定する必要があります。このコマンドが設定されていない場合、DHCPパケットは IP ヘルパー ステートメントを介してリレーされません。**service dhcp** コマンドはデフォルトで設定されます。

例

次に、ヘルパー アドレスとして機能するアドレスを定義する例を示します。

```
Router(config)# interface ethernet 1
Router(config-if)# ip helper-address 10.24.43.2
```

次に、ヘルパー アドレスとして機能するアドレスを定義し、host1 という名前の VRF と関連付ける例を示します。

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip helper-address vrf host1 10.25.44.2
```

次に、ヘルパーアドレスとして機能するアドレスを定義し、group1 という名前の VRG と関連付ける例を示します。

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip helper-address 10.25.45.2 redundancy group1
```

関連コマンド

コマンド	説明
ip forward-protocol	ブロードキャスト パケットを転送するとき、ルータによって転送されるプロトコルおよびポートを指定します。
service dhcp	ルータ上の DHCP サーバー機能およびリレー エージェント機能を有効にします。

ip http client secure-ciphersuite

クライアントからリモートサーバーへのセキュアHTTP接続での暗号化に使用する暗号スイートを指定するには、グローバル コンフィギュレーション モードで**ip http client secure-ciphersuite**コマンドを使用します。以前に設定したクライアントの暗号スイートの指定を削除するには、このコマンドの **no** 形式を使用します。

ip http client secure-ciphersuite [**3des-ede-cbc-sha**] [**rc4-128-sha**] [**rc4-128-md5**] [**des-cbc-sha**]
no ip http client secure-ciphersuite

構文の説明

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA：メッセージの暗号化に 3DES と DES-EDE3-CBC、およびメッセージダイジェストにセキュア ハッシュ アルゴリズム（SHA）を使用した Rivest、Shamir、および Adleman（RSA）のキー交換。
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA：メッセージの暗号化に RC4 128 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA キー交換（RSA 公開キー暗号化）。
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5：メッセージの暗号化に RC4 128 ビット暗号化、およびメッセージダイジェストに Message Digest 5（MD5）を使用した RSA キー交換（RSA 公開キー暗号化）。
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA：メッセージの暗号化に DES-CBC、メッセージダイジェストに SHA を使用した RSA キー交換。

コマンド デフォルト

クライアントとサーバーは、使用可能な暗号スイートのリストから、両方がサポートしている最適な暗号スイートをネゴシエートします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

このコマンドを使用すると、クライアントがセキュアHTTPサーバーに接続する際に提供する暗号スイート（暗号化アルゴリズム）のリストを制限できます。たとえば、最も安全な CipherSuite の使用のみを許可したい場合に、このコマンドを使用します。

ある CipherSuite を指定する理由がない場合、またはこれらの CipherSuite の詳細を熟知していない場合はこのコマンドを未設定のままにして、サーバとクライアント間で双方がサポートしている CipherSuite をネゴシエートさせます（これがデフォルトです）。このコマンドの **no** 形式は、使用可能な暗号スイートのリストをデフォルトに戻します（つまり、デバイスでサポートされているすべての暗号スイートをネゴシエーションに使用できます）。

例

次に、SSL_RSA_WITH_3DES_EDE_CBC_SHA 暗号スイートのみを使用するように HTTPS クライアントを設定する例を示します。

```
Router(config)# ip http client secure-ciphersuite 3des-ede-cbc-sha
```

ip http secure-ciphersuite

リモートクライアントとの接続をネゴシエートするときにセキュアHTTPサーバーによって使用される暗号スイートを指定するには、グローバル コンフィギュレーション モードで **ip http secure-ciphersuite** コマンドを使用します。設定をデフォルトセットの暗号スイートに戻すには、このコマンドの **no** 形式を使用します。

ip http secure-ciphersuite [**3des-ede-cbc-sha**] [**rc4-128-sha**] [**rc4-128-md5**] [**des-cbc-sha**]
no ip http secure-ciphersuite

構文の説明

3des-ede-cbc-sha	SSL_RSA_WITH_3DES_EDE_CBC_SHA：メッセージの暗号化に 3DES と DES-EDE3-CBC、およびメッセージダイジェストにセキュア ハッシュ アルゴリズム（SHA）を使用した Rivest、Shamir、および Adleman（RSA）のキー交換。
rc4-128-sha	SSL_RSA_WITH_RC4_128_SHA：メッセージの暗号化に RC4 128 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA キー交換（RSA 公開キー暗号化）。
rc4-128-md5	SSL_RSA_WITH_RC4_128_MD5：メッセージの暗号化に RC4 128 ビット暗号化、およびメッセージダイジェストに Message Digest 5（MD5）を使用した RSA キー交換（RSA 公開キー暗号化）。
des-cbc-sha	SSL_RSA_WITH_DES_CBC_SHA：メッセージの暗号化に DES-CBC、メッセージダイジェストに SHA を使用した RSA キー交換。

コマンド デフォルト

HTTPSサーバーは、接続するクライアントから受信したリストを使用して、最適な暗号スイートをネゴシエートします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

このコマンドは、HTTPS 接続上の暗号化で使用する暗号スイート（暗号化アルゴリズム）のリストを制限するために使用されます。たとえば、最も安全な CipherSuite の使用のみを許可したい場合に、このコマンドを使用します。

ある CipherSuite を指定する理由がない場合、またはこれらの CipherSuite の詳細を熟知していない場合はこのコマンドを未設定のままにして、サーバとクライアント間で双方がサポートしている CipherSuite をネゴシエートさせます（これがデフォルトです）。

サポートされる暗号スイートは、Cisco IOS ソフトウェアイメージによって異なります。たとえば、“IP Sec56”（“k8”）イメージは、Cisco IOS リリース 12.2(15)T の SSL_RSA_WITH_DES_CBC_SHA の暗号スイートのみをサポートしています。

ルータの処理負荷（速度）に関しては、処理速度の速いものから順に並べたリストを示します（セキュリティが強固で複雑な CipherSuite になるほど、わずかながら処理時間が必要になります）。

1. SSL_RSA_WITH_DES_CBC_SHA
2. SSL_RSA_WITH_RC4_128_MD5
3. SSL_RSA_WITH_RC4_128_SHA
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA

これらの暗号スイートに関する追加情報は、セキュアソケットレイヤ（SSL）3.0 プロトコルに関して文書化した情報源からオンラインで入手できます。

例

次に、接続しているセキュア Web クライアントに提供される暗号スイートを制限する例を示します。

```
Router(config)# ip http secure-ciphersuite rc4-128-sha rc4-128-md5
```

ip http secure-server

セキュア HTTP（HTTPS）サーバーを有効にするには、グローバル コンフィギュレーション モードで **ip http secure-server** コマンドを入力します。HTTPS サーバーを無効にするには、このコマンドの **no** 形式を使用します。

ip http secure-server
no ip http secure-server

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

HTTPS サーバーはディセーブルです。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

HTTPS サーバーは、セキュア ソケット レイヤ（SSL）バージョン 3.0 プロトコルを使用します。

注意 HTTPS サーバーをイネーブルにする場合は、同じサービスに対するセキュリティ保護されていない接続を防ぐため、常に標準 HTTP サーバーをディセーブルにする必要があります。グローバル コンフィギュレーション モードで **no ip http server** コマンドを使用して標準 HTTP サーバーを無効にします（この手順は予防手段であり、通常、HTTP サーバーはデフォルトで無効になっています）。

認証に認証局（CA）が使用されている場合は、HTTPS サーバーをイネーブルにする前にルーティング デバイスで CA トラストポイントを宣言する必要があります。

HTTP/TCP ポート 8090 を閉じるには、HTTP と HTTPS の両方のサーバーを無効にする必要があります。**no http server** と **no http secure-server** コマンドをそれぞれ入力します。

例

次の例では、HTTPS サーバーが有効で、（以前に設定された）CA トラストポイント CA-trust-local が指定されています。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#ip http secure-server
デバイス(config)#ip http secure-trustpoint CA-trust-local
デバイス(config)#end

デバイス#show ip http server secure status
HTTP secure server status: Enabled
```

```
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
```

関連コマンド

コマンド	説明
ip http secure-trustpoint	HTTPS サーバーの署名付き証明書を取得するために使用する CA トラストポイントを指定します。
ip http server	シスコの Web ブラウザ ユーザー インターフェイスを含む IP または IPv6 システムで HTTP サーバーを有効にします。
show ip http server secure status	HTTPS サーバーの設定ステータスを表示します。

ip http server

Cisco Web ブラウザのユーザー インターフェイスを含む、IP または IPv6 システム上で HTTP サーバーを有効にするには、グローバル コンフィギュレーション モードで **ip http server** コマンドを入力します。HTTP サーバーを無効にするには、このコマンドの **no** 形式を使用します。

ip http server
no ip http server

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

HTTP サーバーは、デフォルトにより標準のポート 80 を使用します。

HTTP/TCP ポート 8090 はデフォルトにより開いています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

このコマンドは、HTTP サーバーへの IPv4 と IPv6 の両方のアクセスを有効にします。ただし、**ip http access-class** コマンドで設定されたアクセス リストは、IPv4 トラフィックにのみ適用されます。IPv6 トラフィック フィルタリングはサポートされていません。

⚠

注意 標準 HTTP サーバーとセキュア HTTP（HTTPS）サーバーは、同時にシステム上で実行できます。**ip http secure-server** コマンドを使用して HTTPS サーバーを有効にする場合は、**no ip http server** コマンドを使用して標準 HTTP サーバーを無効にし、標準 HTTP 接続を介してセキュアデータにアクセスできないようにします。

HTTP/TCP ポート 8090 を閉じるには、HTTP と HTTPS の両方のサーバーを無効にする必要があります。**no http server** と **no http secure-server** コマンドをそれぞれ入力します。

例

次に、IPv4 と IPV6 の両方のシステムで HTTP サーバーをイネーブルにする例を示します。

HTTP サーバーを有効にした後は、使用する HTML ファイルの場所を指定して基本パスを設定できます。通常、HTTP Web サーバーで使用される HTML ファイルは、システムのフラッシュ メモリに格納されます。リモート URL はこのコマンドを使用して指定できますが、リモート パス名（たとえば、HTML ファイルがリモート TFTP サーバー上にある場合など）の使用は推奨されません。

```
デバイス(config)#ip http server
デバイス(config)#ip http path flash:
```

関連コマンド

コマンド	説明
ip http access-class	HTTP サーバーへのアクセスを制限する際に使用するアクセス リストを指定します。
ip http path	HTTPサーバーが使用するファイルを見つけるために使用する基本パスを指定します。
ip http secure-server	HTTPS サーバーをイネーブルにします。

ip igmp snooping

device で Internet Group Management Protocol（IGMP; インターネットグループ管理プロトコル）スヌーピングをグローバルにイネーブルにするか、または VLAN 単位でイネーブルにするには、device スタックまたはスタンドアロン device で **ip igmp snooping** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping ［**vlan** *vlan-id*］
no ip igmp snooping ［**vlan** *vlan-id*］

構文の説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングをイネーブルにします。範囲は 1 ～ 1001 および 1006 ～ 4094 です。

コマンド デフォルト

device 上で、IGMP スヌーピングはグローバルに有効になっています。

VLAN インターフェイス上で、IGMP スヌーピングはイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

IGMP スヌーピングがグローバルにイネーブルである場合は、すべての既存 VLAN インターフェイスでイネーブルになります。IGMP スヌーピングがグローバルにディセーブルである場合、すべての既存 VLAN インターフェイスで IGMP スヌーピングがディセーブルになります。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

例

次の例では、IGMP スヌーピングをグローバルにイネーブルにする方法を示します。

```
デバイス(config)# ip igmp snooping
```

次の例では、IGMP スヌーピングを VLAN 1 でイネーブルにする方法を示します。

```
デバイス(config)# ip igmp snooping vlan 1
```

設定を確認するには、特権 EXEC モードで **show ip igmp snooping** コマンドを入力します。

ip mac-binding

デバイスの ip-mac バインディングを設定するには、**ip mac-binding** コマンドを使用します。デバイスの ip-mac バインディングを無効にするには、このコマンドの **no** 形式を使用します

[no] ip mac-binding

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

IP MAC バインディングが有効になっています。

コマンド モード

ワイヤレス ポリシーの設定（config-wireless-policy）

コマンド履歴

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

使用上のガイドライン

（背後にある有線クライアントに対して dot11 アソシエーションを実行しない）シスコ以外の WGB デバイスが Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに接続されている場合、WGB の背後にある有線クライアントが IP アドレスを取得しないことがあります。このような場合は、ポリシープロファイルで **no ip mac-binding** および **ipv4 dhcp required** コマンドを実行します。**ipv4 dhcp required** コマンドは、WGB デバイスが DHCP を実行して IP アドレスを取得するようにします。また、クライアント VLAN でパッシブクライアント機能と ARP ブロードキャストも有効にする必要があります。

WGB と有線クライアントがスタティック IP アドレスで設定されている場合、WGB から受信したデータは転送されません。WGB で DHCP を有効にすることを推奨します（有線クライアントでの DHCP の有効化は任意です）。

設定例を次に示します。

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# ipv4 dhcp required
Device(config-wireless-policy)# no ip mac-binding
Device(config-wireless-policy)# passive-client
Device(config-wireless-policy)# exit
Device(config)# vlan configuration 1
Device(config-vlan)# arp broadcast
```

例

次に、ip-mac バインディングを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# [no] ip mac-binding
```

ip multicast vlan

単一の VLAN に IP マルチキャストを設定するには、グローバル コンフィギュレーション モードで **ip multicast vlan** コマンドを使用します。WLAN から VLAN を削除するには、このコマンドの **no** 形式を使用します。

ip multicast vlan {*vlan-name vlan-id*}
no ip multicast vlan{*vlan-name vlan-id*}

構文の説明

vlan-name	VLAN 名を指定します。
vlan-id	VLAN ID を指定します。

コマンド デフォルト

ディセーブル

コマンド モード

WLAN の設定

コマンド履歴

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

使用上のガイドライン

なし

次に、vlan_id01 をマルチキャスト VLAN として設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless multicast
デバイス(config)# wlan test-wlan 1
デバイス(config-wlan)# ip multicast vlan vlan_id01
```

ip nbar protocol-discovery

NBAR2 エンジンを有効にする際にワイヤレス ポリシーでアプリケーション認識を設定するには、 **ip nbar protocol-discovery** コマンドを使用します。

ip nbar protocol-discovery

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

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

例

次に、ワイヤレス ポリシーでアプリケーション認識を設定する例を示します。

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

ip nbar protocol-pack

ブートフラッシュからプロトコル パックをロードするには、 **ip nbar protocol-pack** コマンドを使用します。

ip nbar protocol-pack bootflash:[{**force**}]

構文の説明

bootflash:	ブートフラッシュからプロトコル パックをロードします。
force	選択したソースからロードプロトコルパックを強制的にロードします。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、ブートフラッシュから NBAR2 プロトコル パックをロードする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip nbar protocol-pack bootflash:
```

ip overlap

Flex 展開でクライアント IP アドレスの重複を有効にするには、**ip overlap** コマンドを使用します。

（注） デフォルトでは、この設定は無効になっています。

ip overlap

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

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

使用上のガイドライン

次に、Flex 展開でクライアント IP アドレスの重複を有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless profile flex flex1
Device(config-wireless-flex-profile)# [no] ip overlap
```

ip ssh

ルータでセキュア シェル（SSH）制御パラメータを設定するには、グローバル コンフィギュレーション モードで**ip ssh** コマンドを使用します。デフォルト値に戻すには、このコマンドの**no** 形式を使用します。

ip ssh [{**timeout** *seconds* | **authentication-retries** *integer*}]
no ip ssh [{**timeout** *seconds* | **authentication-retries** *integer*}]

構文の説明

timeout	（任意）ルータが SSH クライアントの応答を待つ時間間隔。 この設定は、SSH ネゴシエーション フェーズに適用されます。EXEC セッションが開始すると、vty に設定された標準のタイムアウトが適用されます。デフォルトで、5 個の vty（0 ～ 4）が定義されているため、5 個のターミナル セッションが可能です。SSH でシェルが実行されると、vty タイムアウトが始動します。vty タイムアウトのデフォルトは 10 分です。
seconds	（任意）タイムアウトが切断されるまでの秒数（最大 120 秒）。デフォルトは 120 秒です。
authentication- retries	（任意）インターフェイスがリセットされるまでの試行回数。
integer	（任意）認証の再試行回数（最大 5 回）。デフォルトは 3 です。

コマンド デフォルト

SSH 制御パラメータはデフォルトのルータ値に設定されます。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.0(5)S	このコマンドが導入されました。
12.1(1)T	このコマンドが Cisco IOS Release 12.1(1) T に統合されました。
12.2(17a)SX	このコマンドは Cisco IOS リリース 12.2(17a)SX に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS リリース 12(33)SRA に統合されました。
Cisco IOS XE リリース 2.4	このコマンドが、Cisco ASR 1000 シリーズ ルータで実装されました。

使用上のガイドライン

ルータで SSH を設定するには、 **crypto key generate rsa** コマンドを使用して SSH サーバーを有効にする必要があります。

例

次に、ルータで SSH コントロール パラメータを設定する例を示します。

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

ip ssh version

ルータ上で実行するセキュア シェル（SSH）のバージョンを指定するには、グローバル コンフィギュレーション モードで **ip ssh version** コマンドを使用します。設定されている SSH のバージョンを無効にして互換モードに戻るには、このコマンドの **no** 形式を使用します。

ip ssh version [{**1** | **2**}]
no ip ssh version [{**1** | **2**}]

構文の説明

1	（任意）ルータは SSH バージョン 1 のみを実行します。
2	（任意）ルータは SSH バージョン 2 のみを実行します。

コマンド デフォルト

このコマンドが設定されていない場合、SSH は互換性モードで動作します。つまり、バージョン 1 とバージョン 2 の両方がサポートされます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.3(4)T	このコマンドが導入されました。
12.3(2)XE	このコマンドが、Cisco IOS Release 12.3(2)XE に統合されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。
12.3(7)JA	このコマンドが Cisco IOS Release 12.3(7)JA に統合されました。
12.0(32)SY	このコマンドが、Cisco IOS Release 12.0(32)SY に統合されました。
12.4(20)T	このコマンドが Cisco IOS Release 12.4(20)T に統合されました。
15.2(2)SA2	このコマンドが Cisco ME 2600X シリーズ イーサネット アクセス スイッチに実装されました。

使用上のガイドライン

このコマンドを **2** キーワードとともに使用すると、ルータが誤って脆弱な SSH バージョン 1 接続を確立しないようにすることができます。

例

次の例では、SSH バージョン 1 のサポートのみが設定されていることを示します。

```
Router (config)# ip ssh version 1
```

次の例では、SSH バージョン 2 のみが設定されていることを示します。

```
Router (config)# ip ssh version 2
```

次の例では、SSH バージョン 1 および 2 が設定されていることを示します。

```
Router (config)# no ip ssh version
```

関連コマンド

コマンド	説明
debug ip ssh	SSH のデバッグ メッセージを表示します。
disconnect ssh	ルータ上で SSH 接続を終了します。
ip ssh	ルータで SSH コントロール パラメータを設定します。
ip ssh rsa keypair-name	SSH 接続を使用する際に使用する RSA キー ペアを指定します。
show ip ssh	ルータの SSH 接続を表示します。

ip tftp blocksize

TFTP クライアントのブロックサイズを指定するには、**ip tftp blocksize** コマンドを使用します。

ip tftp blocksize *blocksize-value*

構文の説明

blocksize-value	ブロックサイズ値。有効な範囲は512 ～ 8192 Kbps です。

コマンド デフォルト

TFTP クライアントのブロックサイズが設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

このコマンドを使用すると、デフォルトのブロックサイズを変更し、イメージのダウンロード時間を短縮します。

例

次に、TFTP クライアントのブロックサイズを指定する例を示します。

```
Device(config)# ip tftp blocksize 512
```

ip verify source

インターフェイス上の IP ソース ガードを有効にするには、インターフェイス コンフィギュレーション モードで **ip verify source** コマンドを使用します。IP ソース ガードを無効にするには、このコマンドの **no** 形式を使用します。

ip verify source
no ip verify source

コマンド デフォルト

IP 送信元ガードはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

送信元 IP アドレス フィルタリングによる IP ソース ガードをイネーブルにするには、**ip verify source** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、送信元 IP アドレス フィルタリングによる IP ソース ガードをインターフェイス上でイネーブルにする方法を示します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip verify source
```

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

ipv4-address-type

802.11u IPv4 アドレスタイプを設定するには、**ipv4-address-type** コマンドを使用します。アドレスタイプを削除するには、このコマンドの **no** 形式を使用します。

ipv4-address-type
{**double-nated-private** | **not-available** | **not-known** | **port-restricted** | **port-restricted-double-nated** | **port-restricted-single-nated** | **public** | **single-nated-private**}

構文の説明

double-nated-private	IPv4アドレスをダブルネットワークアドレス変換（NAT）プライベートとして設定します。
not-available	IPv4 アドレスタイプを使用不可として設定します。
not-known	IPv4 アドレスタイプの可用性を不明として設定します。
port-restricted	IPv4 アドレスタイプをポート制限として設定します。
port-restricted-double-nated	IPv4 アドレスタイプをポート制限およびダブル NAT として設定します。
port-restricted-single-nated	IPv4 アドレスタイプをポート制限およびシングル NAT として設定します。
public	IPv4 アドレスタイプをパブリックとして設定します。
single-nated-private	IPv4アドレスをシングルNATプライベートとして設定します。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、802.11u IPv4 アドレスタイプを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# ipv4-address-type public
```

ipv4 arp-proxy

プロキシ ARP を有効にするには、**ipv4 arp-proxy** コマンドを使用します。プロキシ ARP を無効にするには、このコマンドの **no** 形式を使用します。

ipv4 arp-proxy

no ipv4 arp-proxy

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ARP プロキシは有効になっていません。

コマンド モード

ワイヤレス ポリシーの設定（config-wireless-policy）

コマンド履歴

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

使用上のガイドライン

プロキシ ARP は、中央スイッチングモードでのみ適用されます。

例

次に、プロキシ ARP を有効にする例を示します。

```
Device(config-wireless-policy)#ipv4 arp-proxy
```

ipv4 dhcp

WLAN の DHCP パラメータを設定するには、**ipv4 dhcp** コマンドを使用します。

ipv4 dhcp {**opt82** | {**ascii** | **rid** | **format** | {**ap_ethmac** | **ap_location** | **apmac** | **apname** | **policy_tag** | **ssid** | **vlan_id** }} | **required** | **server** *dhcp-ip-addr*}

構文の説明

opt82	この WLAN のワイヤレス クライアントに DHCP オプション 82 を設定します
required	DHCP アドレス割り当てが必要かどうかを指定します
server	WLAN の IPv4 DHCP サーバを設定します
ascii	DHCP オプション 82 の ASCII をサポートします
rid	DHCP オプション 82 への Cisco 2 バイト RID の追加をサポートします
format	RemoteID 形式を設定します
ap_ethmac	DHCP AP イーサネット MAC アドレスを有効にします
ap_location	AP ロケーションを有効にします
apmac	AP の MAC アドレスを有効にします
apname	AP 名を有効にします
site_tag (Policy tag)	サイトタグを有効にします
ssid	SSID を有効にします
vlan_id	VLAN ID を有効にします
dhcp-ip-addr	オーバーライド DHCP サーバーの IP アドレスを入力します。

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

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

例

次に、DHCP アドレス割り当てを要件として設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy demo-profile-name
Device(config-wireless-policy)# ipv4 dhcp required
```

ipv4 flow monitor

WLAN プロファイル ポリシーの IPv4 トラフィック入力フロー モニタを設定するには、**ipv4 flow monitor input** コマンドを使用します。

ipv4 flow monitor *monitor-name* **input**

構文の説明

monitor-name	フロー モニタ名。
input	入力トラフィックのフローモニタを有効にします。

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

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

例

次に、WLAN プロファイル ポリシーの IPv4 トラフィック入力フロー モニターを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-profile-name
Device(config-wireless-policy)# ipv4 flow monitor flow-monitor-name input
```

ipv6 access-list

IPv6アクセス リストを定義してデバイスをIPv6アクセス リスト コンフィギュレーション モードに設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-list *access-list-name* | **match-local-traffic** | **log-update threshold** *threshold-in-msgs* | **role-based** *list-name*
noipv6 access-list *access-list-name* | **client** *permit-control-packets* | **log-update** *threshold* | **role-based** *list-name*

構文の説明

ipv6 *access-list-name*	名前付き IPv6 ACL（最長 64 文字）を作成し、IPv6 ACL コンフィギュレーション モードを開始します。 *access-list-name*：IPv6 アクセス リストの名前。名前は、スペース、疑問符を含むことができず、また、数字で始めることはできません。
match-local-traffic	ローカルで生成されたトラフィックに対する照合を有効にします。
log-update threshold *threshold-in-msgs*	最初のパケットの一致後に、syslog メッセージを生成する方法を決定します。 *threshold-in-msgs*：生成されるパケット数。
role-based *list-name*	ロールベースの IPv6 ACL を作成します。

コマンド デフォルト

IPv6 アクセス リストは定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

IPv6 ACL は、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用することで定義され、その許可と拒否の条件は IPv6 アクセス リスト コンフィギュレーション モードで **deny** コマンドおよび **permit** コマンドを使用することで設定されます。**ipv6 access-list** コマンドを設定すると、デバイスはIPv6アクセス リスト コンフィギュレーション モードになり、デバイス プロンプトは Device(config-ipv6-acl)# に変わります。IPv6 アクセス リスト コンフィギュレーション モードから、定義済みの IPv6 ACL に許可および拒否の条件を設定できます。

（注） IPv6 ACL は一意な名前によって定義されます（IPv6 は番号付けされた ACL をサポートしません）。IPv4 ACL と IPv6 ACL は同じ名前を共有できません。

IPv6 は、グローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに変換される **permit any any** ステートメントおよび **deny any any** ステートメントでプロトコル タイプとして自動的に設定されます。

IPv6 ACL にはそれぞれ、最後に一致した条件として、暗黙の **permit icmp any any nd-na** ステートメント、**permit icmp any any nd-ns** ステートメント、および **deny ipv6 any any** ステートメントがあります（前の 2 つの一致条件は、ICMPv6 ネイバー探索を許可します）。1 つの IPv6 ACL には、暗黙の **deny ipv6 any any** ステートメントを有効にするために少なくとも 1 つのエントリが含まれている必要があります。IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを利用するため、デフォルトで、インターフェイス上での IPv6 ネイバー探索パケットの送受信が IPv6 ACL によって暗黙的に許可されます。IPv4 の場合、IPv6 ネイバー探索プロセスに相当するアドレス解決プロトコル（ARP）では、個別のデータ リンク層プロトコルを利用するため、デフォルトで、インターフェイス上での ARP パケットの送受信が IPv4 ACL によって暗黙的に許可されます。

IPv6 ACL を IPv6 インターフェイスに適用するには、*access-list-name* 引数を指定して **ipv6 traffic-filter** インターフェイス コンフィギュレーション コマンドを使用します。IPv6 ACL をデバイスとの着信および発信 IPv6 仮想端末接続に適用するには、*access-list-name* 引数を指定して、**ipv6 access-class** ライン コンフィギュレーション コマンドを使用します。

ipv6 traffic-filter コマンドでインターフェイスに適用される IPv6 ACL は、デバイスによって発信されたトラフィックではなく、転送されたトラフィックをフィルタ処理します。

例

次に、list1 という名前の IPv6 ACL を設定し、デバイスを IPv6 アクセス リスト コンフィギュレーション モードにする例を示します。

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

次に、list2 という名前の IPv6 ACL を設定し、その ACL をイーサネット インターフェイス 0 上の発信トラフィックに適用する例を示します。特に、最初の ACL エントリは、ネットワーク FEC0:0:0:2::/64（送信元 IPv6 アドレスの最初の 64 ビットとしてサイトローカルプレフィックス FEC0:0:0:2 を持つパケット）がイーサネット インターフェイス 0 から出て行くことを拒否します。2 番目の ACL エントリは、その他のすべてのトラフィックがイーサネット インターフェイス 0 から出て行くことを許可します。2 番めのエントリは、各 IPv6 ACL の末尾に暗黙的な deny all 条件があるため、必要となります。

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

ipv6-address-type

802.11u IPv6 アドレスタイプを設定するには、**ipv6-address-type** コマンドを使用します。アドレスタイプを削除するには、このコマンドの **no** 形式を使用します。

ipv6-address-type {**available** | **not-available** | **not-known**}

構文の説明

available	IPv6 アドレスタイプを使用可能として設定します。
not-available	IPv6 アドレスタイプを使用不可として設定します。
not-known	IPv6アドレスタイプの可用性を不明として設定します。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、802.11u IPv6 アドレスタイプを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# ipv4-address-type available
```

ipv6 address

IPv6 汎用プレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスの IPv6 処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 address** コマンドを使用します。インターフェイスからアドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address {*ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length*}
no ipv6 address {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}

構文の説明

ipv6-address	使用する IPv6 アドレス。
/ *prefix-length*	IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
prefix-name	インターフェイスに設定するネットワークを表す上位ビットを指定する汎用プレフィックスです。
sub-bits	*prefix-name* 引数で指定された汎用プレフィックスによって提供されるプレフィックスに連結する、アドレスのサブプレフィックス ビットおよびホスト ビットです。 *sub-bits* 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。

コマンド デフォルト

IPv6 アドレスはインターフェイスに定義されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが、Cisco ASR 1000 シリーズ デバイスに統合されました。
15.2(4)S	このコマンドが、Cisco IOS Release 15.2(4)S に統合されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズ アグリゲーション サービス デバイスに実装されました。
Cisco IOS XE リリース 3.2SE	このコマンドが、Cisco IOS XE リリース 3.2SE に統合されました。

使用上のガイドライン

ipv6 address コマンドを使用すると、複数の IPv6 アドレスをさまざまな方法でインターフェイスに設定できます。さまざまなオプションがあります。最も一般的な方法は、プレフィックス長を使用して IPv6 アドレスを指定することです。

アドレスは、集約された IPv6 プレフィックス ビットをサブプレフィックス ビットおよびホスト ビットから分離する汎用プレフィックスのメカニズムを使用して定義することもできます。この場合、アドレスの先頭ビットは、グローバルに設定または（たとえば、Dynamic Host Configuration Protocol-Prefix Delegation（DHCP-PD）を使用して）学習される汎用プレフィックスで定義され、*prefix-name* 引数を使用して適用されます。サブプレフィックス ビットとホスト ビットは、*sub-bits* 引数を使用して定義されます。

引数を指定せずに **no ipv6 address autoconfig** コマンドを使用すると、手動で設定したすべての IPv6 アドレスがインターフェイスから削除されます。

IPv6 リンクローカル アドレスを設定する必要があります。また、**ipv6 address link-local** コマンドを使用して、インターフェイスで IPv6 処理をイネーブルにする必要があります。

例

次に、インターフェイスで IPv6 処理をイネーブルにして、my-prefix という汎用プレフィックスおよび直接指定されたビットに基づいてアドレスを設定する例を示します。

```
Device(config-if) ipv6 address my-prefix 0:0:0:7272::72/64
```

my-prefix という汎用プレフィックスの値が 2001:DB8:2222::/48 である場合、インターフェイスは、グローバル アドレス 2001:DB8:2222:7272::72/64 を使用して設定されます。

関連コマンド

コマンド	説明
ipv6 address anycast	IPv6 エニーキャスト アドレスを設定し、インターフェイスで IPv6 処理をイネーブルにします。
ipv6 address eui-64	IPv6 アドレスを設定して、そのアドレスの下位 64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
ipv6 address link-local	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。

コマンド	説明
ipv6 unnumbered	インターフェイスに明示的なIPv6アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
no ipv6 address autoconfig	インターフェイスからすべての IPv6 アドレスを削除します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 dhcp pool

Dynamic Host Configuration Protocol（DHCP）for IPv6 のサーバ設定情報プールを設定して DHCP for IPv6 プール コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 dhcp pool** コマンドを使用します。DHCP for IPv6 プールを削除するには、このコマンドの **no** 形式を使用します。

ipv6 dhcp pool *poolname*
no ipv6 dhcp pool *poolname*

構文の説明

poolname	ローカルなプレフィックス プールのユーザ定義名。プール名には象徴的な文字列（「Engineering」など）または整数（0 など）を使用できます。

コマンド デフォルト

DHCP for IPv6 プールは設定されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.3(4)T	このコマンドが導入されました。
12.2(18)SXE	このコマンドが、Cisco IOS Release 12.2(18)SXE に統合されました。
12.4(24)T	このコマンドが、Cisco IOS Release 12.4(24)T に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
12.2(33)SRE	このコマンドが変更されました。Cisco IOS Release 12.2(33)SRE に統合されました。
12.2(33)XNE	このコマンドが変更されました。Cisco IOS リリース 12.2(33)XNE に統合されました。

使用上のガイドライン

IPv6 用 DHCP サーバ設定情報プールを作成するには、**ipv6 dhcp pool** コマンドを使用します。**ipv6 dhcp pool** コマンドがイネーブルの場合、コンフィギュレーション モードが IPv6 用 DHCP プール コンフィギュレーション モードに変更されます。このモードでは、次のコマンドを使用して、管理者はプレフィックスが委任されるようにプール パラメータを設定し、ドメイン ネーム システム（DNS）サーバを設定できます。

- **address prefix** *IPv6-prefix* [**lifetime** {*valid-lifetime preferred-lifetime* | **infinite**}] はアドレス割り当てにアドレス プレフィックスを設定します。このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。
- **link-address** *IPv6-prefix* はリンクアドレス IPv6 プレフィックスを設定します。着信インターフェイスのアドレスまたはパケット内のリンク アドレスが指定した IPv6 プレフィッ

クスと一致する場合、サーバは設定情報プールを使用します。このアドレスは、16ビット値をコロンで区切った16進数で指定する必要があります。

- **vendor-specific** *vendor-id* はDHCPv6ベンダー固有のコンフィギュレーション モードを有効にします。ベンダーの識別番号を指定します。この番号は、ベンダーのIANAプライベートエンタープライズ番号です。指定できる範囲は1～4294967295です。次のコンフィギュレーション コマンドが利用できます。
  - **suboption** *number* はベンダー固有のサブオプション番号を設定します。指定できる範囲は1 ～ 65535です。IPv6アドレス、ASCIIテキスト、または16進文字列をサブオプション パラメータで定義されている束リに入力できます。

（注） **suboption** キーワードの下に **hex** 値を使用すると、入力できるのは16進数（0 ～ f）のみとなります。無効な **hex** 値を入力しても以前の設定は削除されません。

IPv6用DHCP設定情報プールが作成されたら、**ipv6 dhcp server** コマンドを使用して、プールとインターフェイス上のサーバを関連付けます。情報プールを設定しない場合は、**ipv6 dhcp server interface** コンフィギュレーション コマンドを使用してDHCPv6サーバ関数をインターフェイス上で有効にする必要があります。

DHCPv6プールとインターフェイスを関連付けると、関連付けられているインターフェイス上の要求を処理するのはそのプールだけとなります。プールは、他のインターフェイスについても処理を行います。DHCPv6プールとインターフェイスを関連付けない場合は、すべてのインターフェイスに対する要求を処理できます。

IPv6アドレス プレフィックスを使用しない場合、プールは設定済みのオプションのみを返します。

link-address コマンドでは、必ずしもアドレスを割り当てなくてもリンクアドレスの照合を行うことができます。プール内の複数のリンク アドレス コンフィギュレーション コマンドを使用して、複数のリレーのプールを照合できます。

アドレスプール情報またはリンク情報のいずれかについて最長一致が行われるため、あるプールについてはアドレスを割り当てるように設定して、サブプレフィックスの別のプールについては設定されたオプションだけを返すように設定できます。

例

次に、cisco1というDHCP for IPv6設定情報プールを指定して、ルータをDHCP for IPv6プール コンフィギュレーション モードにする例を示します。

```
Router(config)# ipv6 dhcp pool cisco1
Router(config-dhcpv6)#
```

次に、IPv6コンフィギュレーション プールcisco1にIPv6アドレス プレフィックスを設定する例を示します。

```
Router(config-dhcpv6)# address prefix 2001:1000::0/64
Router(config-dhcpv6)# end
```

次に、3 つのリンクアドレス プレフィックスと IPv6 アドレス プレフィックスを含む engineering という名前のプールを設定する例を示します。

```
Router# configure terminal
Router(config)# ipv6 dhcp pool engineering
Router(config-dhcpv6)# link-address 2001:1001::0/64
Router(config-dhcpv6)# link-address 2001:1002::0/64
Router(config-dhcpv6)# link-address 2001:2000::0/48
Router(config-dhcpv6)# address prefix 2001:1003::0/64
Router(config-dhcpv6)# end
```

次に、ベンダー固有オプションを含む 350 という名前のプールを設定する例を示します。

```
Router# configure terminal
Router(config)# ipv6 dhcp pool 350
Router(config-dhcpv6)# vendor-specific 9
Router(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Router(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Router(config-dhcpv6-vs)# end
```

関連コマンド

コマンド	説明
ipv6 dhcp server	インターフェイス上で DHCP for IPv6 サービスを有効にします。
show ipv6 dhcp pool	DHCP for IPv6 コンフィギュレーション プール情報を表示します。

ipv6 enable

明示的な IPv6 アドレスが設定されていないインターフェイス上で IPv6 処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 enable** コマンドを使用します。明示的な IPv6 アドレスでまだ設定されていないインターフェイスで IPv6 処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 enable
no ipv6 enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IPv6 はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
12.2(2)T	このコマンドが導入されました。
12.0(21)ST	このコマンドが Cisco IOS Release 12.0(21)ST に統合されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
15.2(2)SNG	このコマンドが、Cisco ASR 901 シリーズ アグリゲーション サービス デバイスに実装されました。
Cisco IOS XE リリース 3.2SE	このコマンドが、Cisco IOS XE リリース 3.2SE に統合されました。
15.2(2)SA2	このコマンドが Cisco ME 2600X シリーズ イーサネット アクセス スイッチに実装されました。

使用上のガイドライン

ipv6 enable コマンドを実行すると、インターフェイスで IPv6 リンクローカル ユニキャスト アドレスが自動的に設定され、IPv6 処理のインターフェイスもイネーブルになります。明示的な IPv6 アドレスで設定されているインターフェイスで **ipv6 enable** コマンドを実行しても、IPv6 処理はディセーブルになりません。

例

次に、イーサネット インターフェイス 0/0 で IPv6 処理をイネーブルにする例を示します。

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 enable
```

関連コマンド

コマンド	説明
ipv6 address link-local	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ipv6 address eui-64	IPv6 アドレスを設定して、そのアドレスの下位 64 ビットの EUI-64 インターフェイス ID を使用して、インターフェイスでの IPv6 処理をイネーブルにします。
ipv6 unnumbered	インターフェイスに明示的な IPv6 アドレスを割り当てなくても、インターフェイスで IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 flow-export destination

IPv6 ETA フローのエクスポート先を設定するには、**ipv6 flow-export destination** コマンドを使用します。

ipv6 flow-export destination *ipv6_address port_number* [**source-interface** *interface-name*] [**ipfix**]

構文の説明

ip_address	フローの宛先アドレス。
port_number	フローの宛先ポート番号。有効な範囲は 1 ～ 65535 です。
source-interface	（任意）エクスポートされる ETA レコードの送信元インターフェイス名。
interface-number	（任意）エクスポートされる ETA レコードの送信元アドレス。インターフェイスの IP アドレスは、エクスポートされる ETA レコードパケットの送信元 IP アドレスとして使用されます。
ipfix	（任意）エクスポートされる ETA レコードの形式。

コマンド デフォルト

なし

コマンド モード

ET-Analytics コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1s	このコマンドが導入されました。

次に、ETA フローエクスポートの宛先を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# et-analytics
Device(config-et-analytics)# ipv6 flow-export destination 2001:181:181::1 22
source-interface loopback0 ipfix
Device(config-et-analytics)# end
```

ipv6 nd proxy

IPv6 ネイバー探索（ND）または重複アドレス検出（DAD）を有効にするには、**ipv6 nd proxy** コマンドを使用します。ND または DAD プロキシを無効にするには、このコマンドの **no** 形式を使用します。

ipv6 nd proxy {**dad-proxy** | **full-proxy**}

no ipv6 nd proxy {**dad-proxy** | **full-proxy**}

構文の説明

dad-proxy	DAD プロキシを有効にします。
full-proxy	フルプロキシを有効にします。これにより、DAD プロキシと非 DAD ネイバー要請プロキシが有効になります。

コマンド デフォルト

ネイバー探索プロキシは有効になっていません。

コマンド モード

ワイヤレス ポリシーの設定（config-wireless-policy）

コマンド履歴

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

使用上のガイドライン

DAD プロキシは、中央スイッチングモードでのみ適用されます。

例

次に、DAD プロキシを有効にする例を示します。

```
Device(config-wireless-policy)#ipv6 nd proxy dad-proxy
```

ipv6 mld snooping

マルチキャスト リスナー検出バージョン 2（MLDv2）プロトコル スヌーピングをグローバルに有効にするには、グローバル コンフィギュレーション モードで **ipv6 mld snooping** コマンドを使用します。MLDv2 スヌーピングをグローバルに無効にするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping
no ipv6 mld snooping

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドは有効です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(18)SXE	このコマンドが Supervisor Engine 720 に導入されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
15.4(2)S	このコマンドが、Cisco ASR 901 シリーズ アグリゲーション サービス ルータに実装されました。

使用上のガイドライン

MLDv2 スヌーピングは、ポリシー フィーチャ カード 3（PFC3）の何らかのバージョンが搭載された Supervisor Engine 720 でサポートされています。

MLDv2 スヌーピングを使用するには、IPv6 マルチキャスト ルーティング用のサブネットでレイヤ 3 インターフェイスを設定するか、またはサブネットで MLDv2 スヌーピング クエリアを有効にします。

例

次に、MLDv2 スヌーピングをグローバルにイネーブルにする例を示します。

```
Router(config)# ipv6 mld snooping
```

関連コマンド

コマンド	説明
show ipv6 mld snooping	MLDv2 スヌーピング情報を表示します。

ipv6 nd managed-config-flag

IPv6 ルータ アドバタイズメントに managed address configuration フラグを設定するには、適切なコンフィギュレーション モードで **ipv6 nd managed-config-flag** コマンドを使用します。IPv6 ルータ アドバタイズメントからこのフラグをクリアするには、このコマンドの **no** 形式を使用します。

ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

managed address configuration フラグは、IPv6 ルータ アドバタイズメントで設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

managed address configuration フラグを IPv6 ルータ アドバタイズメントで設定すると、アドレスの取得にステートフル オートコンフィギュレーションを使用するかどうかを、接続ホストに示すことができます。このフラグが設定されている場合、接続ホストは、アドレスの取得にステートフル オートコンフィギュレーションを使用します。このフラグが設定されていない場合、接続ホストは、アドレスの取得にステートフル オートコンフィギュレーションを使用しません。

ホストは、ステートフルおよびステートレス オートコンフィギュレーションを同時に使用できます。

例

次に、IPv6 ルータ アドバタイズメントに managed address configuration フラグを設定する例を示します。

```
Device(config)# interface
Device(config-if)# ipv6 nd managed-config-flag
```

ipv6 nd other-config-flag

IPv6 ルータ アドバタイズメントに other stateful configuration フラグを設定するには、適切なコンフィギュレーション モードで **ipv6 nd other-config-flag** コマンドを使用します。IPv6 ルータ アドバタイズメントからこのフラグをクリアするには、このコマンドの **no** 形式を使用します。

ipv6 nd other-config-flag

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

other stateful configuration フラグは、IPv6 ルータ アドバタイズメントで設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

ダイナミック テンプレート コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

other stateful configuration フラグを IPv6 ルータ アドバタイズメントで設定すると、アドレス以外のオートコンフィギュレーション情報を取得できるかどうかを、接続ホストに示すことができます。このフラグが設定されている場合、接続ホストは、その他（アドレス以外）の情報の取得にステートフル オートコンフィギュレーションを使用します。

（注） **ipv6 nd managed-config-flag** コマンドを使用して managed address configuration フラグを設定すると、接続ホストは、other stateful configuration フラグの設定に関係なく、ステートフル オートコンフィギュレーションを使用してその他の情報（アドレス以外の情報）を取得できます。

例

次の例（BNG 以外に該当）は、IPv6 ルータ アドバタイズメントに「other stateful configuration」フラグを設定します。

```
Device(config)# interface
Device(config-if)# ipv6 nd other-config-flag
```

ipv6 nd ra throttler attach-policy

フィーチャ RA スロットラの IPv6 ポリシーを設定するには、**ipv6 nd ra-throttler attach-policy** コマンドを使用します。

ipv6 nd ra-throttler attach-policy *policy-name*

構文の説明

ipv6	IPv6 ルート チェーン。
ra-throttler	VLAN で RA スロットラを設定します。
attach-policy	フィーチャ RA スロットラのポリシーを適用します。
policy-name	フィーチャ RA スロットラのポリシー名

コマンド デフォルト

なし

コマンド モード

config-vlan

コマンド履歴

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

例

次に、フィーチャ RA スロットラの IPv6 ポリシーを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# vlan configuration vlan-id
Device(config-vlan-config)# ipv6 nd ra-throttler attach-policy
```

ipv6 nd raguard policy

ルータ アドバタイズメント（RA）ガード ポリシー名を定義し、RA ガード ポリシー コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 nd raguard policy** コマンドを使用します。

ipv6 nd raguardpolicy *policy-name*

構文の説明

policy-name	IPv6 RA ガード ポリシー名。

コマンド デフォルト

RA ガード ポリシーは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）#

コマンド履歴

リリース	変更内容
12.2(50)SY	このコマンドが導入されました。
15.2(4)S	このコマンドが、Cisco IOS Release 15.2(4)S に統合されました。
15.0(2)SE	このコマンドが Cisco IOS Release 15.0(2)SE に統合されました。
Cisco IOS XE リリース 3.2SE	このコマンドが、Cisco IOS XE リリース 3.2SE に統合されました。

使用上のガイドライン

ルータ上でグローバルに RA ガードを設定するには、**ipv6 nd raguard policy** コマンドを使用します。デバイスが NDインスペクション ポリシー コンフィギュレーション モードになったら、次のいずれかのコマンドを使用できます。

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **trusted-port**
- **validate source-mac**

IPv6 RA ガードがグローバルに設定されると、**ipv6 nd raguard attach-policy** コマンドを使用して、特定のインターフェイスで IPv6 RA ガードをイネーブルにできます。

例

次に、RA ガード ポリシー名を policy1 と定義し、デバイスをポリシー コンフィギュレーション モードにする例を示します。

```
Device(config)# ipv6 nd raguard policy policy1
Device(config-ra-guard)#
```

関連コマンド

表 *1:*

コマンド	説明
device-role	ポートに接続されているデバイスのロールを指定します。
drop-unsecure	オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップします。
ipv6 nd raguard attach-policy	指定したインターフェイスに IPv6 RA ガード機能を適用します。
limit address-count	ポートで使用できる IPv6 アドレスの数を制限します。
sec-level minimum	CGA オプションを使用する場合の最小のセキュリティ レベル パラメータ値を指定します。
trusted-port	信頼できるポートにするポートを設定します。
validate source-mac	送信元MACアドレスをリンク層アドレスと照合します。

ipv6 traffic-filter

このコマンドは、IPv6 トラフィック フィルタを有効にします。

インターフェイスでの IPv6 トラフィックのフィルタリングを有効にするには、**ipv6 traffic-filter** コマンドを使用します。インターフェイスでの IPv6 トラフィックのフィルタリングを無効にするには、このコマンドの **no** 形式を使用します。

インターフェイス上で IPv6 トラフィックをフィルタ処理するには、スイッチ スタックまたはスタンドアロン スイッチ上で **ipv6 traffic-filter** インターフェイス コンフィギュレーション コマンドを使用します。フィルタリングできるトラフィックのタイプと方向は、スイッチ スタックで稼働するフィーチャ セットによって異なります。インターフェイスでの IPv6 トラフィックのフィルタリングを無効にするには、このコマンドの **no** 形式を使用します。

ipv6 traffic-filter [**web**] *acl-name*
no ipv6 traffic-filter [**web**]

構文の説明

web	（任意）WLAN Web ACL の IPv6 アクセス名を指定します。
acl-name	IPv6 アクセス名を指定します。

コマンド デフォルト

インターフェイス上での IPv6 トラフィックのフィルタリングは設定されません。

コマンド モード

wlan

コマンド履歴

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

使用上のガイドライン

デュアル IPv4/IPv6 テンプレートを設定するには、**sdm prefer dual-ipv4-and-ipv6 {default | vlan}** グローバル コンフィギュレーション コマンドを入力し、スイッチをリロードします。

物理インターフェイス（レイヤ 2 またはレイヤ 3 ポート）、レイヤ 3 ポート チャネル、またはスイッチ仮想インターフェイス（SVI）で **ipv6 traffic-filter** コマンドを使用できます。

ACL をレイヤ 3 インターフェイス（ポート ACL）の発信または着信トラフィックに、またはレイヤ 2 インターフェイス（ルータ ACL）の着信トラフィックに適用できます。

いずれかのポート ACL（IPv4、IPv6、または MAC）がインターフェイスに適用された場合、そのポート ACL を使用してパケットをフィルタ処理し、ポート VLAN の SVI に適用されたルータ ACL は無視されます。**any**

次に、インターフェイスで IPv6 トラフィックをフィルタ処理する例を示します。

```
デバイス(config-wlan)# ipv6 traffic-filter TestDocTrafficFilter
```

key

キーチェーンの認証キーを識別するには、キーチェーン コンフィギュレーション モードで **key** コマンドを使用します。キー チェーンからキーを削除するには、このコマンドの **no** 形式を使用します。

key *key-id*
no key *key-id*

構文の説明

key-id	キー チェーンの認証キーの識別番号。キーの範囲は 0 ～ 2147483647 です。キーの ID 番号は連続している必要はありません。

コマンド デフォルト

キー チェーンにキーは存在しません。

コマンド モード

キーチェーン コンフィギュレーション（config-keychain）

使用上のガイドライン

キー チェーンに複数のキーを設定し、**accept-lifetime** および **send-lifetime** キー チェーン キー コマンド設定に基づいてキーが将来無効になるように、ソフトウェアでキーを配列できるようにすると便利です。

各キーには、ローカルに格納される独自のキー識別子があります。キー ID、およびメッセージに関連付けられたインターフェイスの組み合わせにより、使用中の認証アルゴリズムおよび Message Digest 5（MD5）認証キーが一意に識別されます。有効なキーの数にかかわらず、1 つの認証パケットのみが送信されます。ソフトウェアは、最小のキー識別番号の検索を開始し、最初の有効なキーを使用します。

最後のキーが期限切れになった場合、認証は続行されますが、エラー メッセージが生成されます。認証を無効にするには、手動で有効な最後のキーを削除する必要があります。

すべてのキーを削除するには、**no key chain** コマンドを使用してキー チェーンを削除します。

例

次に、キーを指定してキー チェーンでの認証を確認する例を示します。

```
Device(config-keychain)#key 1
```

関連コマンド

コマンド	説明
accept-lifetime	キー チェーンの認証キーが有効として受信される期間を設定します。
key chain	ルーティング プロトコルの認証をイネーブルにするために必要な認証キー チェーンを定義します。
key-string (authentication)	キーの認証文字列を指定します。
show key chain	認証キーの情報を表示します。

key config-key password-encrypt

パスワード暗号化用のプライベート設定キーを設定するには、**key config-key password-encrypt** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

key config-key password-encrypt <*config-key*>

構文の説明

config-key	8 文字以上の値を入力します。 （注） 値の先頭を次の特殊文字にすることはできません。 !、#、および;

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 17.6.1	このコマンドが導入されました。

例

次に、AP 管理用のユーザー名とパスワードを設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# key config-key password-encryption 12345678
Device(config-ap-profile)# password encryption aes
Device(config-ap-profile)# end
```

ldap attribute-map

SLDAP サーバにダイナミック属性マップを設定するには、**ldap attribute-map** コマンドを使用します。

ldap attribute-map *map-name*

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

次に、SLDAP サーバーにダイナミック属性マップを設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# ldap attribute-map map1
デバイス(config-attr-map)# map type department supplicant-group
デバイス(config-attr-map)# exit
```

ldap server

セキュア LDAP を設定するには、**ldap server** コマンドを使用します。

ldap server *name*

構文の説明

name	サーバ名。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、セキュア LDAP を設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# ldap server server1
デバイス(config-ldap-server)# ipv4 9.4.109.20
デバイス(config-ldap-server)# timeout retransmit 20
デバイス(config-ldap-server)# bind authenticate root-dn
CN=ldapipv6user,CN=Users,DC=ca,DC=ssh2,DC=com password Cisco12345
デバイス(config-ldap-server)# base-dn CN=Users,DC=ca,DC=ssh2,DC=com
デバイス(config-ldap-server)# mode secure no- negotiation
デバイス(config-ldap-server)# end
```

license air level

ワイヤレスコントローラでAIRライセンスを設定するには、グローバル コンフィギュレーション モードで**license air level** コマンドを入力します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

license air level { **air-network-advantage** [**addon air-dna-advantage**] | **air-network-essentials** [**addon air-dna-essentials**] }

no license air level

構文の説明

air-network-advantage	AIR Network Advantage ライセンスレベルを設定します。
addon air-dna-advantage	（任意）アドオンの AIR DNA Advantage ライセンスレベルを設定します。 このアドオンオプションは AIR Network Advantage ライセンスで使用できます。
air-network-essentials	AIR Network Essentials ライセンスレベルを設定します。
addon air-dna-essentials	（任意）アドオンの AIR DNA Essentials ライセンスレベルを設定します。 このアドオンオプションは AIR Network Essential ライセンスで使用できます。

コマンド デフォルト

すべての Cisco Catalyst 9800 ワイヤレスコントローラのデフォルトライセンスは AIR DNA Advantage です。

EWC-AP の場合：

- Cisco IOS XE Bengaluru 17.4.1 より前では、デフォルトライセンスは AIR DNA Essentials でした。
- Cisco IOS XE Bengaluru 17.4.1 以降のデフォルトライセンスは AIR Network Essentials です

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	このコマンドは、ポリシーを使用したスマートライセンスの導入で、引き続き使用および適用することができます。
Cisco IOS XE Bengaluru 17.4.1	EWC-AP の場合のみ、デフォルトライセンスが AIR DNA Essentials から AIR Network Essentials に変更されました。

使用上のガイドライン

ポリシーを使用したスマートライセンスの環境では、**license air level** コマンドを使用して、製品インスタンスで使用されているライセンスレベルを変更したり、製品インスタンスでアドオンライセンスを追加設定したりすることができます。変更はリロード後に有効になります。

設定できるライセンスは次のとおりです。

- AIR Network Essential
- AIR Network Advantage
- AIR DNA Essential
- AIR DNA Advantage

Cisco DNA ライセンスを更新しない場合は、AIR DNA Essential または AIR DNA Advantage ライセンスレベルを設定し、期限切れになった時点で Network Advantage または Network Essentials のライセンスレベルに移行することができます。

接続しているすべての AP において、コントローラの一意の値プロパティを利用するために、Cisco DNA Center ライセンスが必要です。

例

次に、AIR DNA Essential ライセンスレベルを設定する例を示します。

```
Device# configure terminal
Device(config)# license air level network-essentials addon air-dna-essentials
```

次に、AIR DNA Advantage ライセンスレベルで開始してから AIR DNA Essentials に変更する例を示します。

AIR DNA Advantage としての現在の設定：

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Advantage

Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

AIR DNA Essentials の設定：

```
Device# configure terminal
Device(config)# license air level air-network-essentials addon air-dna-essentials

Device# exit
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Essentials
Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

```
Device# write memory
Device# reload
```

リロード後：

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Essentials
Next reload AIR license Level: AIR DNA Essentials

Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

license smart（グローバル コンフィギュレーション）

製品インスタンスが Cisco Smart Software Manager（CSSM）や Cisco Smart Licensing Utility（CSLU）、または Smart Software Manager オンプレミス（SSM オンプレミス）との通信に使用するトランスポートモードや URL などのライセンス関連の設定を行い、使用状況レポートの間隔を設定し、ライセンス使用状況レポート（RUM レポート）に含めるか、または除外する必要がある情報を設定するには、グローバル コンフィギュレーション モードで **license smart** コマンドを入力します。デフォルト値に戻すには、コマンドの **no** 形式を使用します。

license smart { **custom_id** *ID* | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** { **automatic** | **callhome** | **cslu** | **off** | **smart** } | **url** { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] }

no license smart { **custom_id** | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** | **url** { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] }

構文の説明

custom_id *ID*	このオプションは CLI では使用できますがサポートされていません。
enable	このキーワードは CLI には表示されますが、設定しても効果はありません。スマートライセンスは常に有効になっています。

privacy { **all** | **hostname** | **version** }

プライバシーフラグを設定して、指定されたデータプライバシー関連情報の送信を防止します。

フラグが無効になっている場合、対応する情報は、製品インスタンスによって作成されるメッセージまたはオフラインファイルで送信されます。

トポロジに応じて、CSSM、CSLU、SSM オンプレミスなどの1つ以上のコンポーネントに情報が送信されます。

すべてのデータプライバシー設定はデフォルトで無効になっています。すべての通信から除外するオプションを設定する必要があります。

- **all**：すべてのデータプライバシー関連情報がすべての通信から除外されます。

  このコマンドの **no** 形式を使用すると、すべてのデータプライバシー関連情報がメッセージまたはオフラインファイルで送信されます。

  （注） データプライバシーが有効かどうかに関係なく、製品 ID（PID）とシリアル番号がRUMレポートに含まれます。

- **hostname**：ホスト名情報がすべての通信から除外されます。ホスト名のプライバシーが有効になっている場合、製品インスタンスの UDI が該当するユーザーインターフェイス（CSSM、CSLU、およびSSMオンプレミス）に表示されます。

  このコマンドの **no** 形式を使用すると、ホスト名情報がメッセージまたはオフラインファイルで送信されます。ホスト名は、該当するユーザーインターフェイス（CSSM、CSLU、および SSM オンプレミス）に表示されます。

- **version**：製品インスタンスで実行されているCisco IOS-XE ソフトウェアバージョンとスマートエージェントのバージョンがすべての通信から除外されます。

  このコマンドの**no**形式を使用すると、バージョン情報がメッセージまたはオフラインファイルで送信されます。

proxy { **address** *address_hostname* | **port** *port* }	CSLUまたはCSSMとライセンス使用状況を同期するためにプロキシを設定します。つまり、トランスポートモードが **license smart transport smart**（CSSM）または **license smart transport cslu**（CSLU）の場合にのみ、このオプションを使用してプロキシを設定できます。 ただし、トランスポートモードとして **license smart transport cslu** も使用する SSM オンプレミス展開では、ライセンス使用状況の同期にプロキシは設定できません。 次のオプションを設定します。 • **address** *address_hostname*：プロキシアドレスを設定します。 *address_hostname* には、プロキシの IP アドレスまたはホスト名を入力します。 • **port***port*：プロキシポートを設定します。 *port* には、プロキシポート番号を入力します。
reservation	ライセンス予約機能を有効または無効にします。 （注） このオプションは、CLI で使用できますが、ライセンスの予約が適用されないため、ポリシーを使用したスマートライセンシングの環境では適用されません。
server-identity-check	HTTP セキュアサーバの ID チェックを有効または無効にします。

transport { **automatic** | **callhome** | **cslu** | **off** | **smart** }	製品インスタンスが CSSM との通信に使用する転送モードを設定します。次のオプションから選択します。 • **automatic**：転送モード **cslu** を設定します。 （注） **automatic** キーワードは Cisco Catalyst ワイヤレスコントローラではサポートされていません。 • **callhome**：転送モードとして Call Home を有効にします。 • **cslu**：転送モードとして CSLU を有効にします。これがデフォルトの転送モードです。 CSLU と SSM オンプレミスの両方に同じキーワードが適用されますが、URLが異なります。次の行の **cslu***cslu_or_on-prem_url* を参照してください。 • **off**：製品インスタンスからのすべての通信を無効にします。 • **smart**：スマート転送を有効にします。

url { *url* | **cslu** *cslu_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* }

設定された転送モードに使用する URL を設定します。次のオプションから選択します。

- *url*：転送モードとして **callhome** を設定している場合は、このオプションを設定します。CSSM URL を次のように正確に入力します。

  ```
  https://software.cisco.com/#module/SmartLicensing
  ```

  no license smart url *url* コマンドは、デフォルトの URL に戻ります。

- **cslu** *cslu_or_on-prem_url*：トランスポートモードを **cslu** として設定している場合は、必要に応じて CSLU または SSM オンプレミスの URL を使用してこのオプションを設定します。

  - CSLU を使用している場合は、次のように URL を入力します。

    ```
    http://<cslu_ip_or_host>:8182/cslu/v1/pi
    ```

    <cslu_ip_or_host> には、CSLU をインストールした Windows ホストのホスト名や IP アドレスを入力します。8182 はポート番号であり、CSLU が使用する唯一のポート番号です。

    no license smart url cslu *cslu_or_on-prem_url* コマンドは `http://cslu-local:8182/cslu/v1/pi` に戻ります。

  - SSM オンプレミスを使用している場合は、次のように URL を入力します。

    ```
    http://<ip>/cslu/v1/pi/<tenant ID>
    ```

    <ip> には、SSM オンプレミスをインストールしたサーバのホスト名または IP アドレスを入力します。<tenantID> はデフォルトのローカルバーチャルアカウント ID にする必要があります。

    ヒント SSM オンプレミスから URL 全体を取得できます。ソフトウェア設定ガイド（17.3.x 以降）で、「Smart Licensing Using Policy」>「Task Library for Smart Licensing Using Policy」>「Retrieving the Transport URL (SSM On-Prem

UI)」を参照してください。

no license smart url cslu *cslu_or_on-prem_url* コマンドは `http://cslu-local:8182/cslu/v1/pi` に戻ります。

- **default**：設定されている転送モードによって異なります。このオプションでは、**smart** および **cslu** 転送モードのみがサポートされます。

  転送モードが **cslu** に設定されている場合、**license smart url default** を設定すると、CSLU URL は自動的に設定されます（`https://cslu-local:8182/cslu/v1/pi`）。

  転送モードが **smart** に設定されている場合、**license smart url default** を設定すると、スマート URL は自動的に設定されます（`https://smartreceiver.cisco.com/licservice/license`）。

- **smart** *smart_url*：転送タイプとして **smart** を設定している場合は、このオプションを設定します。URL を次のように正確に入力します。

  `https://smartreceiver.cisco.com/licservice/license`

  このオプションを設定すると、システムは **license smart url** *url* で自動的に URL の複製を作成します。重複するエントリは無視できます。これ以上の操作は必要ありません。

  no license smart url smart*smart_url* コマンドは、デフォルトの URL に戻ります。

- **utility** *smart_url*：このオプションは CLI では使用できますがサポートされていません。

usage { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* }	使用状況レポートの設定を構成します。次のオプションを設定できます。 • **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value*：テレメトリ用のデータモデルに含める文字列を定義します。最大4つの文字列（またはタグ）を定義できます。 *tag_value* には、定義する各タグの文字列値を入力します。 • **interval** *interval_in_days*：レポート間隔の日数を設定します。デフォルトでは、RUM レポートは 30 日ごとに送信されます。有効な値の範囲は 1 ～ 3650 です。 この値をゼロに設定すると、適用されるポリシーの指定内容に関係なく、RUM レポートは送信されません。これは、CSLU または CSSM が受信側にある可能性があるトポロジに適用されます。 ゼロより大きい値を設定し、通信タイプが**オフ**に設定されている場合、*interval_in_days* と `Ongoing reporting frequency(days):` のポリシー値の間で、値の小さい方が適用されます。たとえば、*interval_in_days* が 100 に設定され、ポリシーの値が `Ongoing reporting frequency (days):90` の場合、RUM レポートは 90 日ごとに送信されます。 間隔を設定せず、デフォルトが有効な場合、レポート間隔は完全にポリシー値によって決定されます。たとえば、デフォルト値が有効で、不適用ライセンスのみが使用されている場合、ポリシーでレポートが不要と記述されていると、RUM レポートは送信されません。
utility [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }]	このオプションは CLI には表示されますが、サポートされていません。

コマンド デフォルト

Cisco IOS XE Amsterdam 17.3.1 以前：スマートライセンスがデフォルトで有効になっています。

Cisco IOS XE Amsterdam 17.3.2a 以降：ポリシーを使用したスマートライセンスがデフォルトで有効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	ポリシーを使用したスマートライセンスで、次のキーワードと変数が導入されました。 • **url** キーワードの下に、次のオプションが導入されました。 { **cslu** *cslu_url* | **smart** *smart_url* } • **transport** キーワードの下に、次のオプションが導入されました。 { **cslu** | **off** } さらに、デフォルトの通信タイプが **callhome** から **cslu** に変更されました。 • **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } **license smart** コマンドの次のキーワードと変数は廃止され、CLI では使用できなくなりました：**enable**、**conversion automatic**。
Cisco IOS XE Amsterdam 17.3.3	SSM オンプレミスサポートが導入されました。SSM オンプレミス展開での製品インスタンス開始型通信の場合、既存の [**no**]**license smart url cslu***cslu_or_on-prem_url* コマンドは SSM オンプレミスの URL の設定もサポートします。ただし、SSM オンプレミスで必要な URL 形式は `http://<ip>/cslu/v1/pi/<tenant ID>` です。 設定する必要がある対応するトランスポートモードも、既存のコマンド（**license smart transport cslu**）です。
Cisco IOS XE Cupertino 17.7.1	バージョンプライバシーが無効になっている場合（**no license smart privacy version** グローバル コンフィギュレーション コマンド）、製品インスタンスで実行されている Cisco IOS-XE ソフトウェアバージョンとスマートエージェントのバージョンが RUM レポートに含まれます。 RUM レポートからバージョン情報を除外するには、バージョンプライバシーを有効にする必要があります（**license smart privacy version**）。

リリース	変更内容
Cisco IOS XE Cupertino 17.9.1	• すべてのデータプライバシー関連情報を送信する新しいメカニズムが導入されました。この情報は RUM レポートに含まれなくなりました。 データプライバシーが無効になっている場合（**no license smart privacy** {**all** | **hostname** | **version**} グローバル コンフィギュレーション コマンド）、データプライバシー関連情報は、別の同期メッセージまたはオフラインファイルで送信されます。 • ホスト名情報の送信のサポートが導入されました。 ホスト名のプライバシー設定が無効になっている場合（**no license smart privacy hostname** グローバル コンフィギュレーション コマンド）、ホスト名情報が別の同期メッセージまたはオフラインファイルで製品インスタンスから送信されます。実装したトポロジに応じて、ホスト名情報はCSSM、CSLU、またはSSMオンプレミスによって受信されます。ホスト名情報は、対応するユーザーインターフェイスにも表示されます。

使用上のガイドライン

データ プライバシー設定

プライバシー設定を無効にすると、実装したトポロジによって、受信者、および情報が宛先に到達する方法が決まります。

- 情報の受信者は、CSSM、CSLU、および SSM オンプレミスのうち 1 つ以上である可能性があります。プライバシー設定は、コントローラ（Cisco DNA Center）には影響を及ぼしません。

  hostname キーワードの場合、CSSM、CSLU、またはSSMオンプレミスがホスト名情報を受信すると、対応する UI にも表示されます（該当する場合）。その後、プライバシーを有効にすると、対応する UI は製品インスタンスの UDI の表示に戻ります。

- 情報の送信方法。
  - 製品インスタンスが通信を開始するトポロジの場合、製品インスタンスは、CSSM、CSLU、または SSM オンプレミスへのメッセージでこの情報の送信を開始します。

    製品インスタンスは、イベント（製品インスタンスの起動、ホスト名の変更、高可用性セットアップでのスイッチオーバー）の1つが発生するたびに送信されるホスト名を送信します。

  - CSLUまたはSSMオンプレミスが通信を開始するトポロジの場合、対応するコンポーネントが製品インスタンスからのプライバシー情報の取得を開始します。

    ホスト名を CSLU または SSM オンプレミスで設定した頻度で取得し、情報を取得します。

- 製品インスタンスがエアギャップネットワークにあるトポロジの場合、**license smart save usage** 特権 EXEC コマンドの入力時に生成されるオフラインファイルにプライバシー情報が含まれます。

（注） すべてのトポロジにおいて、データプライバシー関連情報はRUMレポートに含まれません。

データプライバシー関連情報は、送信または保存する前に製品インスタンスによって保存されないため、情報が送信される場合、送信時または保存時のデータプライバシー設定と一致することが保証されます。

通信障害とレポート

設定したレポート間隔（**license smart usage interval** *interval_in_days* コマンド）によって、製品インスタンスが RUM レポートを送信する日時が決まります。スケジュールされた間隔が通信障害と一致する場合、製品インスタンスは、スケジュールされた時間が経過した後、最大 4 時間 RUM レポートの送信を試みます。（通信障害が続くために）それでもレポートを送信できない場合、システムは間隔を 15 分にリセットします。通信障害が解消されると、レポート間隔はユーザが最後に設定した値に戻ります。

通信障害の場合に表示される可能性があるシステムメッセージは、%SMART_LIC-3-COMM_FAILED です。このエラーを解決し、レポート間隔の値を復元する方法については、該当するリリース（17.3.x 以降）のソフトウェア設定ガイドで、「System Configuration」>「Smart Licensing Using Policy」>「Troubleshooting Smart Licensing Using Policy」を参照してください。

プロキシサーバーの受け入れ

license smart proxy {**address** *address_hostname* | **port***port*} コマンドを設定するとき、Cisco IOS XE Bengaluru 17.6.1 以降、プロキシサーバーの受け入れ基準が変更されたことに注意してください。プロキシサーバーの応答のステータスコードのみがシステムによって検証され、理由フレーズは検証されません。RFC 形式は、`status-line = HTTP-version SP status-code SP reason-phrase CRLF` で、ステータスコードは 3 桁の数値コードになります。ステータス行の詳細については、RFC 7230 のセクション 3.1.2 を参照してください。

例

- データプライバシーの例 （138 ページ）
- 転送タイプと URL の例 （139 ページ）
- 使用状況レポートのオプションの例 （140 ページ）

データ プライバシーの例

次に、グローバル コンフィギュレーション モードで **license smart privacy** コマンドを使用してデータプライバシー関連情報を設定する例を示します。**show license status** 出力には、設定された情報が表示されます。

（注） **show** コマンドの出力は、特定のオプションが有効か無効かを示すだけです。

ここでは、データプライバシー関連の情報は送信されません。

```
Device# configure terminal
Device(config)# license smart privacy all
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: ENABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

ここでは、製品インスタンスで実行されているソフトウェアバージョンは、Cisco IOS XE Cupertino 17.9.1 です。バージョンプライバシーが無効になっていて、製品インスタンスで実行されている Cisco IOS-XE ソフトウェアバージョンとスマートエージェントのバージョンが RUM レポートに含まれます。

```
Device# configure terminal
Device(config)# license smart privacy hostname
Device(config)# no license smart privacy version
Device(config)# exit

Device# show license all
<output truncated>

Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

<output truncated>
```

ここでは、製品インスタンスで実行されているソフトウェアバージョンは、Cisco IOS XE Cupertino 17.9.1 です。製品インスタンスから開始されるメッセージには、ホスト名

は含まれ、バージョン情報は含まれません。製品インスタンスは CSSM に直接接続されています（トランスポートタイプは **smart** で、対応する URL があります）。

```
Device# configure terminal
Device(config)# license smart privacy version
Device(config)# no license smart privacy hostname
Device(config)# exit

Device# show license all
<output truncated>

Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

<output truncated>
```

転送タイプと URL の例

次に、グローバル コンフィギュレーション モードで **license smart transport** および **license smart url** コマンドを使用して、転送タイプの一部を設定する例を示します。**show license all** 出力には、設定された情報が表示されます。

トランスポート **cslu**：

```
Device# configure terminal
Device(config)# license smart transport cslu
Device(config)# license smart url default
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  Proxy:
    Not Configured
<output truncated>
```

トランスポート **smart**：

```
Device# configure terminal
Device(config)# license smart transport smart
Device(config)# license smart url smart https://smartreceiver.cisco.com/licservice/license
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
```

```
    Not Configured
<output truncated>
```

使用状況レポートのオプションの例

次に、グローバル コンフィギュレーション モードで **license smart usage** コマンドを使用して、使用状況レポートの一部を設定する例を示します。**show running-config** 出力には、設定された情報が表示されます。

customer-tag オプションの設定：

```
Device# configure terminal
Device(config)# license smart usage customer-tags tag1 SA/VA:01
Device(config)# exit
Device# show running-config | include tag1
license smart usage customer-tags tag1 SA/VA:01
```

現在適用されているポリシーよりも絞り込んだレポート間隔の設定：

```
Device# show license status
<output truncated>
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Dec 21 12:02:21 2020 PST
Reporting push interval: 30 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 22 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>

Device# configure terminal
Device(config)# license smart usage interval 20
Device(config)# exit
Device# show license status
<output truncated>

Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Nov 22 12:02:21 2020 PST
Reporting push interval: 20 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 12 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>
```

license smart（特権 EXEC）

承認コードの要求または返却、リソース使用状況測定レポート（RUM レポート）の保存、製品インスタンスへのファイルのインポート、Cisco Smart Software Manager（CSSM）との信頼の確立、CSSM または Cisco Smart License Utility（CSLU）、あるいは Smart Software Manager オンプレミス（SSM オンプレミス）との製品インスタンスの同期、製品インスタンスからのライセンス情報の削除などのライセンス機能を設定するには、対応するキーワードまたは引数を指定して特権 EXEC モードで **license smart** コマンドを入力します。

license smart { **authorization** { **request** { **add** | **replace** | **save** *filepath_filename* } *feature_name* { **all** | **local** } | **return** { **all** | **local** } { **offline** [*filepath_filename*] | **online** } } | **clear eventlog** | **export return** { **all** | **local** } *feature_name* | **factory reset** | **import** *filepath_filename* | **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *filepath_filename* } } | **sync** { **all** | **local** } | **trust idtoken** *id_token_value* { **local** | **all** } [{ **force** }] }

構文の説明

smart	スマートライセンスのオプションを提供します。
authorization	承認コードを要求する、または承認コードを返すオプションを提供します。 認証コードは、輸出規制または輸出規制の適用タイプのライセンスを使用する場合にのみ必要です。
request	承認コードを CSSM、CSLU（CSLU は CSSM から承認コードを取得）、または SSM オンプレミスから要求し、そのコードを製品インスタンスにインストールします。
add	要求されたライセンスを既存の承認コードに追加します。新しい承認コードには、既存の承認コードのすべてのライセンスと要求されたライセンスが含まれます。
replace	既存の承認コードを置き換えます。新しい承認コードには、要求されたライセンスのみが含まれます。現在の承認コードのすべてのライセンスが返されます。 このオプションを入力すると、製品インスタンスは、削除される承認コードに対応するライセンスが使用中であるかどうかを確認します。ライセンスが使用されている場合は、対応する機能を最初に無効にするようにエラーメッセージが表示されます。
save*filepath_filename*	承認コード要求をファイルに保存します。 *filepath_filename* には、ファイルの絶対パス（ファイル名を含む）を指定します。
feature_name	承認コードを要求するライセンスの名前。

all	高可用性セットアップですべての製品インスタンスに対してアクションを実行します。
local	アクティブな製品インスタンスに対してアクションを実行します。これがデフォルトのオプションです。
return	CSSM のライセンスプールに承認コードを返します。
offline *filepath_filename*	製品インスタンスが CSSM に接続されていないことを意味します。承認コードはオフラインで返されます。このオプションでは、戻りコードをファイルに出力する必要があります。 ファイルを保存するパスを指定することもできます。ファイル形式は、.txtなどの読み取り可能な任意の形式にすることができます。 オフラインオプションを選択する場合は、CLI や保存したファイルから戻りコードをコピーして CSSM に入力する、という追加の手順を実行する必要があります。
online	製品インスタンスが接続モードであることを意味します。承認コードは、CSLU や CSSM に直接返されます。
clear eventlog	製品インスタンスからすべてのイベントログファイルをクリアします。
export return	輸出規制ライセンスの承認キーを返します。
factory reset	製品インスタンスから保存されているすべてのライセンス情報をクリアします。
import *filepath_filename*	製品インスタンスにファイルをインポートします。ファイルは、承認コード、信頼コード、またはポリシーのファイルである場合があります。 *filepath_filename* には、場所（ファイル名を含む）を指定します。
save	RUM レポートや信頼コード要求を保存するオプションを提供します。
trust-request *filepath_filename*	アクティブな製品インスタンスの信頼コード要求を指定した場所に保存します。 *filepath_filename* には、ファイルの絶対パス（ファイル名を含む）を指定します。

usage { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* }	RUM レポート（ライセンス使用状況情報）を指定した場所に保存します。次のいずれかのオプションを指定する必要があります。 • **all**：すべての RUM レポートを保存します。 • **days** *days*：過去 n 日間（現在の日を除く）の RUM レポートを保存します。番号を入力します。有効範囲は 0 ～ 4294967295 です。 たとえば、3 と入力すると、過去 3 日間の RUM レポートが保存されます。 • **rum-Id** *rum-ID*：指定した RUM ID を保存します。値の有効な範囲は 0 ～ 18446744073709551615 です。 • **unreported**：すべての未報告の RUM レポートを保存します。 **file** *filepath_filename*：指定した使用状況情報をファイルに保存します。ファイルの絶対パス（ファイル名を含む）を指定します。
sync { **all** | **local** }	CSSM または CSLU、あるいは SSM オンプレミスと同期して、保留中のデータを送受信します。これには、保留中の RUM レポートのアップロード、ACK 応答のダウンロード、および製品インスタンスの保留中の承認コード、信頼コード、ポリシーが含まれます。 次のいずれかのオプションを入力して、製品インスタンスを指定します。 • **all**：高可用性セットアップですべての製品インスタンスに対して同期を実行します。このオプションを選択すると、製品インスタンスは同期要求内にあるすべての UDI のリストも送信します。 • **local**：要求を送信するアクティブな製品インスタンス、つまり自身の UDI に対してのみ同期を実行します。これがデフォルトのオプションです。
trust idtoken *id_token_value*	CSSM との信頼できる接続を確立します。 このオプションを使用するには、最初に CSSM ポータルでトークンを生成する必要があります。*id_token_value* に生成されたトークン値を指定します。
force	信頼コードが製品インスタンスにすでに存在する場合でも、信頼コード要求を送信します。 信頼コードは、製品インスタンスの UDI にノードロックされます。UDI がすでに登録されている場合、CSSM は同じ UDI の新規登録を許可しません。 **force** キーワードを入力すると、この動作が上書きされます。

コマンド デフォルト

Cisco IOS XE Amsterdam 17.3.1 以前：スマートライセンスがデフォルトで有効になっています。

Cisco IOS XE Amsterdam 17.3.2a 以降：ポリシーを使用したスマートライセンスがデフォルトで有効になっています。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	ポリシーを使用したスマートライセンスで、次のキーワードと変数が導入されました。 • **authorization** { **request** { **add** | **replace** } *feature_name* { **all** | **local** } | **return** { **all** | **local** } { **offline** [*path*] | **online** } } • **import** *file_path* • **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* } } • **sync** { **all** | **local** } • **trust idtoken** *id_token_value* { **local** | **all** } [**force**] **license smart** コマンドの次のキーワードと変数は廃止され、CLI では使用できなくなりました。 • **register idtoken** *token_id* [**force**] • **renew id** { **ID** | **auth** } • **debug** { **error** | **debug** | **trace** | **all** } • **reservation** { **cancel** [**all** | **local**] | **install** [**file**] *key* | **request** { **all** | **local** | **universal** } | **return** [**all** | **authorization** { *auth_code* | **file** *filename* } | **Local**] *key* } • **mfg reservation** { **request** | **install** | **install file** | **cancel** } • **conversion** { **start** | **stop** }
Cisco IOS XE Amsterdam 17.3.3	SSM オンプレミスのサポートが導入されました。リソース使用状況測定レポート（RUM レポート）の保存、製品インスタンスへのファイルのインポート、製品インスタンスの同期、認証コードの返却、SSM オンプレミス展開での製品インスタンスからのライセンス情報の削除など、ライセンス関連のタスクを実行できます。

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	このリリースでは、次の機能拡張が導入されています。 • **save** *filepath_filename* キーワードと変数が **license smart authorization request** 文字列に追加されました。 CLI には表示されますが、Cisco Catalyst ワイヤレスコントローラのいずれにも輸出規制ライセンスまたは適用ライセンスがないため、この新しいキーワードは適用されません。 • 既存の **license smart save usage** コマンドが拡張され、該当するトポロジの信頼コード要求が含まれるようになりました。

使用上のガイドライン

信頼コードの上書き

license smart trust idtoken コマンドを設定する際の **force** オプションのユースケース：1 つのバーチャルアカウントに含まれているすべての製品インスタンスに同じトークンを使用できます。製品インスタンスが 1 つのアカウントから別のアカウントに移動した場合（たとえば、別のバーチャルアカウントの一部である高可用性設定に追加されたため）、既存の信頼コードを上書きすることが必要になる場合があります。

ライセンス情報の削除

licence smart factory reset コマンドを入力すると、承認コード、RUM レポートなど、すべてのライセンス情報（使用中のライセンスを除く）が製品インスタンスから削除されます。そのため、このコマンドは、製品インスタンスを返却する場合（Return Material Authorization（RMA））、または永続的にデコミットする場合にのみ使用することを推奨します。また、製品インスタンスからライセンス情報を削除する前に CSSM に RUM レポートを送信します。これは、CSSM に最新の使用状況情報が含まれていることを確認するためです。

認証コードとライセンス予約：

認証コードとライセンス予約に関連するオプション：

- Cisco Catalyst ワイヤレスコントローラのいずれにも輸出規制ライセンスまたは適用ライセンスがなく、ポリシーを使用したスマートライセンスの環境には予約済みライセンスの概念が適用されないため、次のコマンドは適用されません。
  - { { **license smart authorization request** { **add** | **replace** | **save** *path* } *feature_name* { **all** | **local** } *request_count* } }
  - **license smart export return**
- 返すことも可能な SLR 承認コードの場合は、次のオプションが適用可能になっている必要があります。

  license smart authorization return { **all** | **local** } { **offline** [*path*] | **online** }

例

ライセンス使用状況情報の保存例

次の例は、製品インスタンスのライセンス使用状況情報を保存する方法を示しています。このオプションを使用して、エアギャップネットワークのレポート要件を満たすことができます。この例では、ファイルはまずフラッシュメモリに保存され、次に TFTP の場所にコピーされます。

```
 Device> enable
Device# license smart save usage unreported file flash:RUM-unrep.txt
Device# dir
Directory of bootflash:/

33      -rw-             5994   Nov 2 2020 03:58:04 +05:00  RUM-unrep.txt

Device# copy flash:RUM-unrep.txt tftp://192.168.0.1//auto/tftp-user/user01/
Address or name of remote host [192.168.0.1]?
Destination filename [//auto/tftp-user/user01/RUM-unrep.txt]?
!!
15128 bytes copied in 0.161 secs (93963 bytes/sec)
```

RUM レポートをファイルに保存した後、（インターネットに接続しているワークステーションや Ciscoから）CSSM にアップロードする必要があります。

信頼コードのインストールの例

次の例は、信頼コードがすでに製品インスタンスにインストールされている場合に、信頼コードをインストールする方法を示しています。これには、CSSM への接続が必要です。正常なインストール後の **show license status** 出力例を次に示します。

信頼コードをインストールする前に、トークンを生成し、CSSM から対応するファイルをダウンロードする必要があります。

結果を確認するには、**show license status** コマンド（`Trust Code Installed:`）を使用します。

```
Device> enable
Device# license smart trust idtoken
NGMwMjk5mYtNZaxMS00NzMZmtgWm local force

Device# show license status
<output truncated>
Trust Code Installed:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
    INSTALLED on Nov 02 05:19:05 2020 IST
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
    INSTALLED on Nov 02 05:19:05 2020 IST
<output truncated>
```

SLR 承認コードを返す例

次の例は、SLR 承認コードを削除して返す方法を示しています。ここでは、コードがオフラインで返されます（CSSM への接続なし）。正常に返された後の **show license all** 出力例を次に示します。

```
Device> enable
Device# show license all
<output truncated>
License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Last Confirmation code: ad4382fe
<output truncated>

Device# license smart authorization return local offlline
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS
    Return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h
UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN
    Return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA

Device# show license all
<output truncated>
License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: NOT INSTALLED
      Last return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: NOT INSTALLED
      Last return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA
<output truncated>
```

オフラインオプションを選択する場合は、CLI や保存したファイルから戻りコードをコピーして CSSM に入力する、という追加の手順を実行する必要があります。

license wireless high-performance

Cisco Catalyst C9800-L-K9 ワイヤレスコントローラのスケールとキャパシティをアップグレードするには、**license wireless high-performance** コマンドを使用します。高パフォーマンスライセンスを設定解除するには、このコマンドの **no** 形式を使用します。

license wireless high-performance

no license wireless high-performance

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

高パフォーマンスライセンスは設定されていません

コマンド モード

グローバル（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1s	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2	このコマンドは、このリリースで導入されるポリシーを使用したスマートライセンスで、引き続き使用および適用することができます。

使用上のガイドライン

このコマンドは、スタンバイコントローラと同期されます。ただし、アップグレードされたキャパシティを取得するには、スタンバイコントローラにもパフォーマンスライセンスが必要です。

高パフォーマンスライセンスを設定解除することで、ライセンスを解放してライセンスプールに戻すことができます。ライセンスを解放してライセンスプールに戻すことで、必要に応じて別のコントローラが使用できるようになります。

RMA の場合、お客様が Cisco Technical Assistance Center（TAC）に連絡して、お客様のバーチャルアカウントから製品インスタンスを削除する必要があります。これにより、コントローラが使用するすべてのライセンスがライセンスプールに戻され、新しいハードウェアで使用できるようになります。

license wireless high-performance コマンドを設定する前に、デバイスを再起動してください。

例

コントローラのスケールとキャパシティをアップグレードするには、次のコマンドを使用します。

```
Device# configure terminal
Device(config#) license wireless high-performance
```

link-local-bridging

各ポリシープロファイルのリンクローカルブリッジングを有効にするには、**link-local-bridging** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

link-local-bridging

no link-local-bridging

構文の説明

link-local-bridging	各ポリシープロファイルのリンクローカルブリッジングを有効にします。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ポリシー コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、各ポリシープロファイルのリンクローカルブリッジングを有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# link-local-bridging
```

load

サイトタグベースのロードバランシングを設定するには、**load** コマンドを使用します。

load *load*

構文の説明

load	サイト用に予約する相対負荷の推定値を指定します。 値の範囲は 0 ～ 1000 です。デフォルト値の 0 は、サイトの負荷に関する推奨事項がないことを意味します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.10.1	このコマンドが導入されました。

次に、サイトタグベースのロードバランシングを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless tag site area1
Device(config-site-tag)# load 200
Device(config-site-tag)# end
```

local-admin-mac deny

ローカルで管理されているアドレスを使用したクライアントの関連付けを拒否するには、**local-admin-mac deny** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

local-admin-mac deny

no local-admin-mac deny

構文の説明

local-admin-mac	ローカルで管理されている MAC アドレスを指定します。
deny	ローカルで管理されているアドレスを使用したクライアントの関連付けを拒否します

コマンド デフォルト

なし

コマンド モード

WLAN コンフィギュレーション モード（config-wlan）

コマンド履歴

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

例

次に、ローカルで管理されているアドレスを使用したクライアントの関連付けを拒否する例を示します。

```
Device# configure terminal
Device(config)# wlan wlan-test 3 ssid-test
Device(config-wlan)# shutdownDevice(config-wlan)# [no] local-admin-mac deny
Device(config-wlan)# no shutdown
```

local-auth ap eap-fast

EAP Fast 方式を使用した Flex ポリシーのローカル認証を設定するには、**local-auth ap eap-fast** コマンドを使用します。

local-auth ap eap-fast *profile-name*

構文の説明

profile-name	eap-fastプロファイル名を入力します。

コマンド デフォルト

なし

コマンド モード

config-wireless-flex-profile

コマンド履歴

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

例

次の例は、EAP Fast 方式での Flex ポリシーの認証を設定する方法を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile flex profile-name
Device(config-wireless-flex-profile)# local-auth ap eap-fast eap-fast-profile-name
```

local-site

サイトをローカル サイトとして設定するには、 **local-site** コマンドを使用します。

local-site

構文の説明

local-site	このサイトをローカルサイトとして設定します。

コマンド デフォルト

なし

コマンド モード

config-site-tag

コマンド履歴

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

例

次に、現在のサイトをローカル サイトとして設定する例を示します。

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

location expiry

ロケーションの有効期間を設定するには、グローバル コンフィギュレーション モードで**location expiry** コマンドを使用します。

location expiry {**calibrating-client** | **client** | **tags** }*timeout-duration*

構文の説明

calibrating-client	調整クライアントのタイムアウト値。
client	クライアントのタイムアウト値。
tags	RFID タグのタイムアウト値。
timeout-duration	タイムアウト時間（秒）。

コマンド デフォルト

タイムアウト値は設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、ロケーションの有効期間を設定する例を示します。

```
Device(config)# location expiry tags 50
```

location notify-threshold

RSSI 測定の NMSP 通知しきい値を設定するには、グローバル コンフィギュレーション モードで **location notify-threshold** コマンドを使用します。RSSI 測定の NMSP 通知しきい値を削除するには、このコマンドの **no** 形式を使用します。

location notify-threshold {**client** | **rogue-aps** | **tags** } *db*
no location notify-threshold {**client** | **rogue-aps** | **tags** }

構文の説明

client	クライアントおよび不正クライアントの NMSP 通知しきい値（dB 単位）を指定します。 しきい値パラメータに有効な値の範囲は 0 ～ 10 dB です。デフォルト値は 0 dB です。
rogue-aps	不正アクセス ポイントの NMSP 通知しきい値（dB 単位）を指定します。 しきい値パラメータに有効な値の範囲は 0 ～ 10 dB です。デフォルト値は 0 dB です。
tags	RFID タグの NMSP 通知しきい値（dB 単位）を指定します。 しきい値パラメータに有効な値の範囲は 0 ～ 10 dB です。デフォルト値は 0 dB です。
db	しきい値パラメータに有効な値の範囲は 0 ～ 10 dB です。デフォルト値は 0 dB です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

次に、クライアントの NMSP 通知しきい値を 10 dB に設定する例を示します。クライアント RSSI が差分 10 dB で変更されると同時に、通知 NMSP メッセージが MSE に送信されます。

```
デバイス# configure terminal
デバイス(config)# location notify-threshold client 10
デバイス(config)# end
```

login authentication

ログイン認証パラメータを設定するには、**login authentication** コマンドを使用します。

login authentication *word* **default**

構文の説明

word	名前を記した認証リスト。
default	デフォルトの認証リストを使用します。

コマンド デフォルト

なし

コマンド モード

ライン コンフィギュレーション

コマンド履歴

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

例

次に、ログイン認証を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# line console 0
Device(config-line)# login authentication NO_LOGIN
```

lsc-only-auth（メッシュ）

ローカルで有効な証明書（LSC）専用の MAP 認証にメッシュ セキュリティを設定するには、**lsc-only-auth** コマンドを使用します。

lsc-only-auth

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

LSC 専用認証はイネーブルになっています。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

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

例

次に、LSC 専用 MAP 認証にメッシュ セキュリティを設定する例を示します。

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

mac-filtering

WLAN 上で MAC フィルタリングを有効にするには、 **mac-filtering** コマンドを使用します。

mac-filtering ［*mac-authorization-list* ］

構文の説明

mac-authorization-list	許可リストの名前。

コマンド デフォルト

なし

コマンド モード

config-wlan

コマンド履歴

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

例

次に、WLAN で MAC フィルタリングをイネーブルにする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan-name wlan-index SSID-name
Device(config-wlan)# mac-filtering
```

mab request format attribute

WLAN で MAC フィルタリングを設定するときにデリミタを設定するには、グローバル コンフィギュレーション モードで **mab request format attribute** コマンドを使用します。WLAN で MAC フィルタリングを設定するときにデリミタを無効にするには、このコマンドの **no** 形式を使用します。

mab request format attribute { **1 groupsize** *size* **separator** *separator* [**lowercase** | **uppercase**] | **2** { **0** | **7** | **LINE** } **LINE** *password* | **32 vlan access-vlan** }

no mab request format attribute { **1 groupsize** *size* **separator** *separator* [**lowercase** | **uppercase**] | **2** { **0** | **7** | **LINE** } **LINE** *password* | **32 vlan access-vlan** }

構文の説明

1	MAB 要求に使用するユーザー名形式を指定します。
groupsize *size*	グループごとの 16 進数の桁数を指定します。 有効な値の範囲は 1 ～ 12 です。
separator *separator*	グループを区切る方法を指定します。 区切り文字は、ハイフン（-）、コロン（:）、およびピリオド（.）です。 groupsize と separator の詳細については、「Overview of the Configurable MAB Username and Password」を参照してください。
lowercase	ユーザー名を小文字で指定します。
uppercase	ユーザー名を大文字で指定します。
2	すべての MAB 要求に使用するグローバルパスワードを指定します。
0	暗号化されていないパスワードを指定します。
7	非表示のパスワードを指定します。
LINE	暗号化されたパスワードまたは暗号化されていないパスワードを指定します。
password	回線パスワード。
32	NAS-Identifier 属性を指定します。
vlan	VLAN を指定します。
access-vlan	設定されたアクセス VLAN を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例：

次に、MAC フィルタリングを設定するときにデリミタを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# mab request format attribute 1 groupsize 4 separator -
```

mbo

WLAN で WiFi Alliance Agile Multiband（MBO）を設定するには、**mbo** コマンドを使用します。

mbo

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

MBO は有効になっていません。

コマンド モード

WLAN の設定

コマンド履歴

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

使用上のガイドライン

次に、WLAN で WiFi Alliance Agile Multiband（MBO）を設定する例を示します。

```
Device# configure terminal
Device(config)# wlan wlan-demo 1 ssid-demo
Device(config-wlan)# mbo
Device(config-wlan)# end
```

（注） WLAN での MBO の設定時に WPA2 WLAN を使用する場合は、設定で PMF を有効にする必要があります。

management gateway-failover enable

ゲートウェイモニタリングを有効にするには、**management gateway-failover enable** コマンドを使用します。ゲートウェイモニタリングを無効にするには、このコマンドの **no** 形式を使用します。

management gateway-failover enable
no management gateway-failover enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1s	このコマンドが導入されました。

次に、ゲートウェイモニタリングを有効にする例を示します。

```
Device# configure terminal
Device(config)# management gateway-failover enable
Device(config)# end
```

management gateway-failover interval

ゲートウェイのモニタリング間隔を設定するには、**management gateway-failover interval** コマンドを使用します。

management gateway-failover interval *interval-value*

構文の説明

interval-value	ゲートウェイのモニタリング間隔を示します。有効な範囲は 6 ～ 12 です。デフォルト値は 8 です。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

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

使用上のガイドライン

次に、ゲートウェイのモニタリング間隔を設定する例を示します。

```
Device# configure terminal
Device(config)# management gateway-failover interval 6
Device(config)# end
```

map-fast-ancestor-find

ワイヤレス メッシュ プロファイルで MAP Fast Ancestor Find モードを設定するには、**map-fast-ancestor-find** コマンドを使用します。

map-fast-ancestor-find

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

ワイヤレス メッシュ プロファイル コンフィギュレーション（config-wireless-mesh-profile）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.11.1	このコマンドが導入されました。

例

次に、メッシュ AP プロファイルに MAP Fast Ancestor Find モードを設定する例を示します。

```
Device # configure terminal
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# map-fast-ancestor-find
```

match activated-service-template

セッションでアクティブ化されているサービス テンプレートに基づいて true と評価される条件を作成するには、コントロール クラスマップ フィルタ コンフィギュレーション モードで **match activated-service-template** コマンドを使用します。セッションでアクティブ化されているサービス テンプレートが指定されたテンプレートと一致しない場合に true と評価する条件を作成するには、コントロール クラスマップ フィルタ コンフィギュレーション モードで **no-match activated-service-template** コマンドを使用します。条件を削除するには、このコマンドの **no** 形式を使用します。

match activated-service-template *template-name*
no-match activated-service-template *template-name*
no {**match** | **no-match**} **activated-service-template** *template-name*

構文の説明

template-name	**service-template** コマンドによって定義された、設定されているサービス テンプレートの名前。

コマンド デフォルト

コントロール クラスには、サービス テンプレートに基づく条件は含まれていません。

コマンド モード

コントロール クラスマップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

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

使用上のガイドライン

match activated-service-template コマンドは、セッションに適用されているサービス テンプレートに基づいて、コントロール クラスの一致条件を設定します。コントロール クラスには複数の条件を含めることができ、各条件は true または false の評価を行います。コントロール クラスは、コントロール ポリシーのアクションを実行するためには、条件のすべてまたはいずれかが true と評価される必要があるか、あるいはいずれも true と評価されてはならないかを定義します。

このコマンドの **no-match** 形式は、結果が不一致になる値を指定します。指定した一致基準以外のすべての値は、結果が一致になります。たとえば、**no-match activated-service-template SVC_1** コマンドを設定すると、SVC_1 を除くすべてのテンプレート値が一致として受け入れられます。

class コマンドは、コントロール クラスをコントロール ポリシーに関連付けます。

例

次に、VLAN_1 という名前のサービス テンプレートがセッションでアクティブになっている場合に true と評価するコントロール クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match activated-service-template VLAN_1
```

関連コマンド

コマンド	説明
activate (policy-map action)	加入者セッションのコントロールポリシーまたはサービステンプレートをアクティブ化します。
class	制御ポリシーを制御クラスの 1 つ以上のアクションに関連付けます。
match service-template	イベントのサービステンプレートに基づいて true と評価される条件を作成します。
service-template	加入者セッションに適用する一連のサービスポリシー属性が含まれるテンプレートを定義します。

match any

デバイスを通過するすべてのプロトコルで照合を実行するには、**match any** コマンドを使用します。

match any

コマンド デフォルト

なし

コマンド モード

config-cmap

コマンド履歴

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

例

次に、デバイスを通過するすべてのパケットを照合する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map cmap-name
Device(config-cmap)# match any
```

match application name

フロー レコードのキー フィールドとしてアプリケーション名を使用するように設定するには、フロー レコード コンフィギュレーション モードで **match application name** コマンドを使用します。アプリケーション名をフロー レコードのキー フィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します。

match application name
no match application name

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

アプリケーション名はキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション（config-flow-record）

コマンド履歴

リリース	変更内容
15.0(1)M	このコマンドが導入されました。
15.2(2)T	このコマンドが Cisco Performance Monitor 用に Cisco IOS Release 15.2(2)T に統合されました。
Cisco IOS XE Release 3.5S	このコマンドが Cisco Performance Monitor 用に Cisco IOS XE Release 3.5S に統合されました。

使用上のガイドライン

このコマンドは、Flexible NetFlow と Performance Monitor の両方で使用できます。これらの製品では、このコマンドを発行するコンフィギュレーション モードを開始するために異なるコマンドを使用しますが、モード プロンプトは両方の製品で共通しています。Performance Monitor では、このコマンドを使用する前に、まず **flow record type performance-monitor** コマンドを入力する必要があります。

モード プロンプトは両方の製品で共通しているため、ここでは両方の製品のコマンド モードをフロー レコード コンフィギュレーション モードと呼びます。ただし、Flexible NetFlow の場合、このモードは Flexible NetFlow フロー レコード コンフィギュレーション モードとも呼ばれます。Performance Monitor の場合、このモードは Performance Monitor フロー レコード コンフィギュレーション モードとも呼ばれます。

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを差別化するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

例

次に、アプリケーション名をキー フィールドとして設定する例を示します。

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match application name
```

Cisco IOS リリース 15.2(2)T および XE 3.5S での Cisco Performance Monitor

次に、アプリケーション名をキー フィールドとして設定する例を示します。

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# match application name
```

関連コマンド

コマンド	説明
collect application name	Flexible NetFlow のフロー レコードで、アプリケーション名を非キー フィールドとして使用するように設定します。
flow record	フロー レコードを作成し、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。
flow record type performance-monitor	フロー レコードを作成し、Performance Monitor フロー レコード コンフィギュレーション モードを開始します。

match day

日または一般的な日のグループ（週末または平日）を使用して照合を実行するには、 **match day** コマンドを使用します。

match day *day-string*

コマンド デフォルト

なし

コマンド モード

フィルタ コントロール クラスマップ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

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

使用上のガイドライン

このコマンドが機能するためには、AAA オーバーライドも無効にする必要があります。

例

次に、日を使用して照合を実行する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-all class-map-name
Device(config-filter-control-classmap)# match day day-string
```

match device-type

デバイス タイプを使用して照合を実行するには、 **match device-type** コマンドを使用します。

match device-type*device-type*

コマンド デフォルト なし

コマンド モード フィルタ コントロール クラスマップ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

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

使用上のガイドライン デバイス リストに入力するには、デバイス分類子を有効にする必要があります。

例

次に、デバイス タイプを使用して照合を実行する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-allclass-map-name
Device(config-filter-control-classmap)# match device-type device-type
```

match eap-type

拡張認証プロトコル（EAP）を使用して照合を実行するには、**match eap-type** コマンドを使用します。

match eap-type {**fast** | **gtc** | **leap** | **md5** | **mschapv2** | **peap** | **tls**}

構文の説明

fast	セキュア トンネリングを介したフレキシブル認証
gtc	汎用トークン カード
leap	Lightweight Extensible Authentication Protocol。
md5	MD5-tunneled Authentication Protocol。
mschapv2	MSCHAPV2 認証メカニズム。
peap	保護拡張認証プロトコル。
tls	Transport Layer Security。

コマンド デフォルト

なし

コマンド モード

フィルタ コントロール クラスマップ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

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

使用上のガイドライン

このコマンドが機能するためには、AAA オーバーライドも無効にする必要があります。

例

次に、eap-type PEAP を使用して一致を実行する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-all class-map-name
Device(config-filter-control-classmap)# match eap-type  peap
```

match interface

入力インターフェイスと出力インターフェイスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match interface** コマンドを使用します。入力インターフェイスと出力インターフェイスをフロー レコードのキー フィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します。

match interface {**input** | **output**}
no match interface {**input** | **output**}

構文の説明

input	入力インターフェイスをキー フィールドとして設定します。
output	出力インターフェイスをキー フィールドとして設定します。

コマンド デフォルト

入力インターフェイスと出力インターフェイスは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次に、入力インターフェイスをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match interface input
```

次に、出力インターフェイスをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match interface output
```

match ipv4

フロー レコードのキー フィールドとして 1 つ以上の IPv4 フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv4** コマンドを使用します。フロー レコードのキー フィールドとして 1 つ以上の IPv4 フィールドを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv4 {**destination address** | **protocol** | **source address** | **tos** | **version**}
no match ipv4 {**destination address** | **protocol** | **source address** | **tos** | **version**}

構文の説明

destination address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv4 destination address （176 ページ）を参照してください。
protocol	キー フィールドとして IPv4 プロトコルを設定します。
source address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv4 source address （178 ページ）を参照してください。
tos	キー フィールドとして IPv4 ToS を設定します。
version	キー フィールドとして IPv4 ヘッダーの IP バージョンを設定します。

コマンド デフォルト

ユーザ定義のフロー レコードのキー フィールドとして 1 つ以上の IPv4 フィールドを使用する設定は、イネーブルになっていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、キー フィールドとして IPv4 プロトコルを設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 protocol
```

match ipv4

フロー レコードのキー フィールドとして 1 つ以上の IPv4 フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv4** コマンドを使用します。フロー レコードのキー フィールドとして 1 つ以上の IPv4 フィールドを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv4 {**destination address** | **protocol** | **source address** | **tos** | **version**}
no match ipv4 {**destination address** | **protocol** | **source address** | **tos** | **version**}

構文の説明

destination address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv4 destination address （176 ページ）を参照してください。
protocol	キー フィールドとして IPv4 プロトコルを設定します。
source address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv4 source address （178 ページ）を参照してください。
tos	キー フィールドとして IPv4 ToS を設定します。
version	キー フィールドとして IPv4 ヘッダーの IP バージョンを設定します。

コマンド デフォルト

ユーザ定義のフロー レコードのキー フィールドとして 1 つ以上の IPv4 フィールドを使用する設定は、イネーブルになっていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、キー フィールドとして IPv4 プロトコルを設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 protocol
```

match ipv4 destination address

IPv4 宛先アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 destination address** コマンドを使用します。IPv4 宛先アドレスをフロー レコードのキー フィールドとして使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv4 destination address
no match ipv4 destination address

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IPv4 宛先アドレスはキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv4 destination address** または **default match ipv4 destination address** フロー レコード コンフィギュレーション コマンドを使用します。

次の例では、IPv4 宛先アドレスをフロー レコードのキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 destination address
```

match ipv4 destination address

IPv4 宛先アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 destination address** コマンドを使用します。IPv4 宛先アドレスをフロー レコードのキー フィールドとして使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv4 destination address
no match ipv4 destination address

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IPv4 宛先アドレスはキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv4 destination address** または **default match ipv4 destination address** フロー レコード コンフィギュレーション コマンドを使用します。

次の例では、IPv4 宛先アドレスをフロー レコードのキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 destination address
```

match ipv4 source address

IPv4 送信元アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 source address** コマンドを使用します。フロー レコードのキー フィールドとして IPv4 送信元アドレスを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv4 source address
no match ipv4 source address

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IPv4 送信元アドレスがキー フィールドとして設定されません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv4 source address** または **default match ipv4 source address** フロー レコード コンフィギュレーション コマンドを使用します。

次に、キー フィールドとして IPv4 送信元アドレスを設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 source address
```

match ipv4 source address

IPv4 送信元アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 source address** コマンドを使用します。フロー レコードのキー フィールドとして IPv4 送信元アドレスを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv4 source address
no match ipv4 source address

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IPv4 送信元アドレスがキー フィールドとして設定されません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv4 source address** または **default match ipv4 source address** フロー レコード コンフィギュレーション コマンドを使用します。

次に、キー フィールドとして IPv4 送信元アドレスを設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 source address
```

match ipv4 ttl

フロー レコードのキー フィールドとして IPv4 存続可能時間（TTL）フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 ttl** コマンドを使用します。フロー レコードのキー フィールドとして IPv4 TTL を使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv4 ttl
no match ipv4 ttl

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IPv4 存続可能時間（TTL）フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match ipv4 ttl** コマンドを使用して定義されます。

次に、キー フィールドとして IPv4 TTL を設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 ttl
```

match ipv4 ttl

フロー レコードのキー フィールドとして IPv4 存続可能時間（TTL）フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv4 ttl** コマンドを使用します。フロー レコードのキー フィールドとして IPv4 TTL を使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv4 ttl
no match ipv4 ttl

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IPv4 存続可能時間（TTL）フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match ipv4 ttl** コマンドを使用して定義されます。

次に、キー フィールドとして IPv4 TTL を設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv4 ttl
```

match ipv6

フロー レコードのキー フィールドとして 1 つ以上の IPv6 フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv6** コマンドを使用します。フロー レコードのキー フィールドとして 1 つ以上の IPv6 フィールドを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv6 {**destination address** | **protocol** | **source address** | **traffic-class** | **version**}
no match ipv6 {**destination address** | **protocol** | **source address** | **traffic-class** | **version**}

構文の説明

destination address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv6 destination address （184 ページ）を参照してください。
protocol	キー フィールドとして IPv6 プロトコルを設定します。
source address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv6 source address （188 ページ）を参照してください。

コマンド デフォルト

IPv6 の各フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、キー フィールドとして IPv6 プロトコル フィールドを設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 protocol
```

match ipv6

フロー レコードのキー フィールドとして 1 つ以上の IPv6 フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match ipv6** コマンドを使用します。フロー レコードのキー フィールドとして 1 つ以上の IPv6 フィールドを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv6 {**destination address** | **protocol** | **source address** | **traffic-class** | **version**}
no match ipv6 {**destination address** | **protocol** | **source address** | **traffic-class** | **version**}

構文の説明

destination address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv6 destination address （184 ページ）を参照してください。
protocol	キー フィールドとして IPv6 プロトコルを設定します。
source address	キー フィールドとして IPv4 宛先アドレスを設定します。詳細については、match ipv6 source address （188 ページ）を参照してください。

コマンド デフォルト

IPv6 の各フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、キー フィールドとして IPv6 プロトコル フィールドを設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 protocol
```

match ipv6 destination address

IPv6 宛先アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 destination address** コマンドを使用します。IPv6 宛先アドレスをフロー レコードのキー フィールドとして使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv6 destination address
no match ipv6 destination address

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IPv6 宛先アドレスはキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv6 destination address** または **default match ipv6 destination address** フロー レコード コンフィギュレーション コマンドを使用します。

次の例では、キー フィールドとして IPv6 宛先アドレスを設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 destination address
```

match ipv6 destination address

IPv6 宛先アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 destination address** コマンドを使用します。IPv6 宛先アドレスをフロー レコードのキー フィールドとして使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv6 destination address
no match ipv6 destination address

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IPv6 宛先アドレスはキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv6 destination address** または **default match ipv6 destination address** フロー レコード コンフィギュレーション コマンドを使用します。

次の例では、キー フィールドとして IPv6 宛先アドレスを設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 destination address
```

match ipv6 hop-limit

フロー レコードのキー フィールドとしてIPv6ホップ リミットを設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 hop-limit** コマンドを使用します。フロー レコードのキー フィールドとして IPv6 パケットのセクションを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv6 hop-limit
no match ipv6 hop-limit

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ユーザ定義のフロー レコードのキー フィールドとして IPv6 ホップ リミットを使用する設定は、デフォルトでイネーブルになっていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

次に、キー フィールドとしてフロー パケットのホップ リミットを設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 hop-limit
```

match ipv6 hop-limit

フロー レコードのキー フィールドとしてIPv6ホップ リミットを設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 hop-limit** コマンドを使用します。フロー レコードのキー フィールドとして IPv6 パケットのセクションを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv6 hop-limit
no match ipv6 hop-limit

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ユーザ定義のフロー レコードのキー フィールドとして IPv6 ホップ リミットを使用する設定は、デフォルトでイネーブルになっていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キーフィールドは、**match** コマンドを使用して定義されます。

次に、キー フィールドとしてフロー パケットのホップ リミットを設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 hop-limit
```

match ipv6 source address

IPv6 送信元アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 source address** コマンドを使用します。フロー レコードのキー フィールドとして IPv6 送信元アドレスを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv6 source address
no match ipv6 source address

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IPv6 送信元アドレスはキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv6 source address** または **default match ipv6 source address** フロー レコード コンフィギュレーション コマンドを使用します。

次に、IPv6 送信元アドレスをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 source address
```

match ipv6 source address

IPv6 送信元アドレスをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match ipv6 source address** コマンドを使用します。フロー レコードのキー フィールドとして IPv6 送信元アドレスを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

match ipv6 source address
no match ipv6 source address

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IPv6 送信元アドレスはキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

このコマンドをデフォルト設定に戻すには、**no match ipv6 source address** または **default match ipv6 source address** フロー レコード コンフィギュレーション コマンドを使用します。

次に、IPv6 送信元アドレスをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match ipv6 source address
```

match join-time-of-day

日における時刻を使用して照合を実行するには、 **match join-time-of-day** コマンドを使用します。

match join-time-of-day *start-time end-time*

コマンド デフォルト

なし

コマンド モード

フィルタ コントロール クラスマップ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

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

使用上のガイドライン

照合で参加時刻が考慮されます。たとえば、照合フィルタが午前 11:00 から午後 2:00 に設定されている場合、午前 10:59 に参加するデバイスは、午前 11:00 より後にクレデンシャルを取得しても考慮されません。

このコマンドが機能するためには、AAA オーバーライドも無効にする必要があります。

例

次に、参加時刻を使用して照合を実行する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-all class-map-name
Device(config-filter-control-classmap)# match join-time-of-day start-time end-time
```

match message-type

サービス リストを照合するメッセージ タイプを設定するには、**match message-type** コマンドを使用します。

match message-type {**announcement** | **any** | **query**}

構文の説明

announcement	デバイス のサービス アドバタイズメントまたはアナウンスメントのみを許可します。
any	任意の照合タイプを許可します。
query	ネットワーク内の特定の デバイス に対するクライアントからクエリのみを許可します。

コマンド デフォルト

なし

コマンド モード

サービス リスト コンフィギュレーション。

コマンド履歴

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

使用上のガイドライン

異なるシーケンス番号を持つ同じ名前の複数のサービスマップを作成することができ、フィルタの評価順序はシーケンス番号に基づきます。サービス リストは、それぞれが許可または拒否の結果を持つ個々の文を一定の順序で並べたものです。サービス リストの評価は、事前に定義された順序でのリストのスキャンと、一致する各文の基準の評価で構成されています。リストのスキャンは、文の一致が初めて見つかり、その文に関連付けられたアクション permit または deny が実行されると停止します。リスト全体をスキャンした後のデフォルトのアクションは deny です。

（注） **service-list mdns-sd** *service-list-name* **query** コマンドを使用していた場合、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションに対してのみ使用できます。

例

次に、照合されるアナウンスメント メッセージ タイプを設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match message-type announcement
```

match non-client-nrt

NRT（非リアルタイム）で非クライアントを照合するには、クラスマップ コンフィギュレーション モードで **match non-client-nrt** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

match non-client-nrt
no match non-client-nrt

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

クラスマップ

コマンド履歴

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

使用上のガイドライン

なし

次に、NRT で非クライアントを設定する例を示します。

```
デバイス(config)# class-map test_1000
デバイス(config-cmap)# match non-client-nrt
```

match protocol

指定されたプロトコルに基づいてクラス マップの一致基準を設定するには、クラスマップ コンフィギュレーション モードまたはポリシー インライン コンフィギュレーション モードで **match protocol** コマンドを使用します。プロトコルベースの一致基準をクラス マップから削除するには、このコマンドの **no** 形式を使用します。**match protocol** コマンドの詳細については、『*Cisco IOS Quality of Service Solutions Command Reference*』を参照してください。

match protocol {*protocol-name* | **attribute category** *category-name* | **attribute sub-category** *sub-category-name* | **attribute application-group** *application-group-name*}

構文の説明

protocol-name	一致基準として使用されるプロトコルの名前です（bgp など）。
category-name	一致基準として使用するアプリケーション カテゴリの名前です。
sub-category-name	一致基準として使用するアプリケーションサブカテゴリの名前です。
application-group-name	一致基準とするアプリケーション グループの名前です。アプリケーション名を指定すると、アプリケーション グループの代わりにアプリケーションが一致基準として設定されます。

コマンド デフォルト

一致基準は設定されていません。

コマンド モード

クラスマップ コンフィギュレーション

コマンド履歴

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

次に、match protocol でアプリケーション名、カテゴリ、およびサブ カテゴリのフィルタを適用してクラス マップを作成する例を示します。

```
デバイス# configure terminal
デバイス(config)# class-map cat-browsing
デバイス(config-cmap)# match protocol attribute category browsing
デバイス(config-cmap)#end

デバイス# configure terminal
デバイス(config)# class-map cat-fileshare
デバイス(config-cmap)# match protocol attribute category file-sharing
デバイス(config-cmap)#end

デバイス# configure terminal
デバイス(config)# class-map match-any subcat-terminal
デバイス(config-cmap)# match protocol attribute sub-category terminal
デバイス(config-cmap)#end
```

```
デバイス# configure terminal
デバイス(config)# class-map match-any webex-meeting
デバイス(config-cmap)# match protocol webex-meeting
デバイス(config-cmap)#end
```

次に、ポリシー マップを作成し、アップストリーム QoS の既存のクラス マップを定義する例を示します。

```
デバイス# configure terminal
デバイス(config)# policy-map test-avc-up
デバイス(config-pmap)# class cat-browsing
デバイス(config-pmap-c)# police 150000
デバイス(config-pmap-c)# set dscp 12
デバイス(config-pmap-c)#end

デバイス# configure terminal
デバイス(config)# policy-map test-avc-up
デバイス(config-pmap)# class cat-fileshare
デバイス(config-pmap-c)# police 1000000
デバイス(config-pmap-c)# set dscp 20
デバイス(config-pmap-c)#end

デバイス# configure terminal
デバイス(config)# policy-map test-avc-up
デバイス(config-pmap)# class subcat-terminal
デバイス(config-pmap-c)# police 120000
デバイス(config-pmap-c)# set dscp 15
デバイス(config-pmap-c)#end

デバイス# configure terminal
デバイス(config)# policy-map test-avc-up
デバイス(config-pmap)# class webex-meeting
デバイス(config-pmap-c)# police 50000000
デバイス(config-pmap-c)# set dscp 21
デバイス(config-pmap-c)#end
```

次に、ポリシー マップを作成し、ダウンストリーム QoS の既存のクラス マップを定義する例を示します。

```
デバイス# configure terminal
デバイス(config)# policy-map test-avc-down
デバイス(config-pmap)# class cat-browsing
デバイス(config-pmap-c)# police 200000
デバイス(config-pmap-c)# set dscp 10
デバイス(config-pmap-c)#end

デバイス# configure terminal
デバイス(config)# policy-map test-avc-up
デバイス(config-pmap)# class cat-fileshare
デバイス(config-pmap-c)# police 300000
```

```
デバイス(config-pmap-c)# set wlan user-priority 2
デバイス(config-pmap-c)# set dscp 20
デバイス(config-pmap-c)#end


デバイス# configure terminal
デバイス(config)# policy-map test-avc-up
デバイス(config-pmap)# class subcat-terminal
デバイス(config-pmap-c)# police 100000
デバイス(config-pmap-c)# set dscp 25
デバイス(config-pmap-c)#end

デバイス# configure terminal
デバイス(config)# policy-map test-avc-up
デバイス(config-pmap)# class webex-meeting
デバイス(config-pmap-c)# police 60000000
デバイス(config-pmap-c)# set dscp 41
デバイス(config-pmap-c)#end
```

次に、定義された QoS ポリシーを WLAN に適用する例を示します。

```
デバイス# configure terminal
デバイス(config)#wlan  alpha
デバイス(config-wlan)#shut
デバイス(config-wlan)#end
デバイス(config-wlan)#service-policy client input test-avc-up
デバイス(config-wlan)#service-policy client output test-avc-down
デバイス(config-wlan)#no shut
デバイス(config-wlan)#end
```

match service-instance

サービス リストを照合するサービス インスタンスを設定するには、**match service-instance** コマンドを使用します。

match service-instance *line*

構文の説明

line	パケット内のサービスインスタンスを照合するための正規表現。

コマンド デフォルト

なし

コマンド モード

サービス リスト コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

service-list mdns-sd *service-list-name* **query** コマンドを使用していた場合、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションに対してのみ使用できます。

例

次に、照合するサービス インスタンスを設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match service-instance servInst 1
```

match service-type

照合する mDNS サービス タイプ文字列値を設定するには、**match service-type** コマンドを使用します。

match service-type *line*

構文の説明

line	パケット内のサービス タイプを照合するための正規表現。

コマンド デフォルト

なし

コマンド モード

サービス リスト コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

service-list mdns-sd *service-list-name* **query** コマンドを使用していた場合、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションに対してのみ使用できます。

例

次に、照合する mDNS サービス タイプ文字列値を設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match service-type _ipp._tcp
```

match transport

フロー レコードのキー フィールドとして 1 つ以上のトランスポート フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match transport** コマンドを使用します。フロー レコードのキー フィールドとして 1 つ以上のトランスポート フィールドを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

構文の説明

destination-port	キー フィールドとしてトランスポート宛先ポートを設定します。
source-port	キー フィールドとしてトランスポート送信元ポートを設定します。

コマンド デフォルト

トランスポート フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、宛先ポートをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport destination-port
```

次の例では、送信元ポートをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport source-port
```

match transport

フロー レコードのキー フィールドとして 1 つ以上のトランスポート フィールドを設定するには、フロー レコード コンフィギュレーション モードで **match transport** コマンドを使用します。フロー レコードのキー フィールドとして 1 つ以上のトランスポート フィールドを使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

構文の説明

destination-port	キー フィールドとしてトランスポート宛先ポートを設定します。
source-port	キー フィールドとしてトランスポート送信元ポートを設定します。

コマンド デフォルト

トランスポート フィールドは、キー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、宛先ポートをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport destination-port
```

次の例では、送信元ポートをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport source-port
```

match transport icmp ipv4

ICMP IPv4 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match transport icmp ipv4** コマンドを使用します。ICMP IPv4 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして使用するのをディセーブルにするには、このコマンドの **no** 形式を使用します。

match transport icmp ipv4 {**code** | **type**}
no match transport icmp ipv4 {**code** | **type**}

構文の説明

code	ICMP IPv4 コードをキー フィールドとして設定します。
type	ICMP IPv4 タイプをキー フィールドとして設定します。

コマンド デフォルト

ICMP IPv4 のタイプ フィールドとコード フィールドはキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次に、ICMP IPv4 コード フィールドをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv4 code
```

次に、ICMP IPv4 タイプ フィールドをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv4 type
```

match transport icmp ipv4

ICMP IPv4 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match transport icmp ipv4** コマンドを使用します。ICMP IPv4 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして使用するのをディセーブルにするには、このコマンドの **no** 形式を使用します。

match transport icmp ipv4 {**code** | **type**}
no match transport icmp ipv4 {**code** | **type**}

構文の説明

code	ICMP IPv4 コードをキー フィールドとして設定します。
type	ICMP IPv4 タイプをキー フィールドとして設定します。

コマンド デフォルト

ICMP IPv4 のタイプ フィールドとコード フィールドはキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次に、ICMP IPv4 コード フィールドをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv4 code
```

次に、ICMP IPv4 タイプ フィールドをキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv4 type
```

match transport icmp ipv6

ICMP IPv6 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match transport icmp ipv6** コマンドを使用します。ICMP IPv6 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして使用するのをディセーブルにするには、このコマンドの **no** 形式を使用します。

match transport icmp ipv6 {**code** | **type**}
no match transport icmp ipv6 {**code** | **type**}

構文の説明

code	IPv6 ICMP コードをキー フィールドとして設定します。
type	IPv6 ICMP タイプをキー フィールドとして設定します。

コマンド デフォルト

ICMP IPv6 タイプ フィールドおよびコード フィールドはキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、IPv6 ICMP コード フィールドをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv6 code
```

次の例では、IPv6 ICMP タイプ フィールドをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv6 type
```

match transport icmp ipv6

ICMP IPv6 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match transport icmp ipv6** コマンドを使用します。ICMP IPv6 のタイプ フィールドとコード フィールドをフロー レコードのキー フィールドとして使用するのをディセーブルにするには、このコマンドの **no** 形式を使用します。

match transport icmp ipv6 {**code** | **type**}
no match transport icmp ipv6 {**code** | **type**}

構文の説明

code	IPv6 ICMP コードをキー フィールドとして設定します。
type	IPv6 ICMP タイプをキー フィールドとして設定します。

コマンド デフォルト

ICMP IPv6 タイプ フィールドおよびコード フィールドはキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを区別するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次の例では、IPv6 ICMP コード フィールドをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv6 code
```

次の例では、IPv6 ICMP タイプ フィールドをキー フィールドとして設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match transport icmp ipv6 type
```

match user-role

クラスマップ属性フィルタ条件を設定するには、**match user-role** コマンドを使用します。

match user-role ユーザ ロール

コマンド デフォルト

なし

コマンド モード

config-filter-control-classmap

コマンド履歴

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

例

次に、クラス マップ属性フィルタ条件を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# class-map type control subscriber match-any map-name
Device(config-filter-control-classmap)# match user-role user-role
```

match username

イベントのユーザ名に基づいて true と評価される条件を作成するには、コントロール クラスマップ フィルタ コンフィギュレーション モードで **match username** コマンドを使用します。イベントのユーザ名が指定されたユーザ名と一致しない場合に true と評価される条件を作成するには、コントロール クラスマップ フィルタ コンフィギュレーション モードで **no-match username** コマンドを使用します。条件を削除するには、このコマンドの **no** 形式を使用します。

match username *username*
no-match username *username*
no {**match** | **no-match**} **username** *username*

構文の説明

username	ユーザー名。

コマンド デフォルト

コントロール クラスには、イベントのユーザ名に基づく条件は含まれていません。

コマンド モード

コントロール クラスマップ フィルタ コンフィギュレーション（config-filter-control-classmap）

コマンド履歴

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

使用上のガイドライン

match username コマンドは、ユーザ名に基づいて、コントロール クラスの一致条件を設定します。制御クラスには複数の条件を含めることができ、各条件は true または false の評価を行います。コントロール クラスは、コントロール ポリシーのアクションを実行するためには、条件のすべてまたはいずれかが true と評価される必要があるか、あるいはいずれも true と評価されてはならないかを定義します。

このコマンドの **no-match** 形式は、結果が不一致になる値を指定します。指定した一致基準以外のすべての値は、結果が一致になります。たとえば、**no-match username josmithe** コマンドを設定すると、コントロール クラスは josmithe を除くすべてのユーザ名の値を一致として受け入れます。

class コマンドは、コントロール クラスをコントロール ポリシーに関連付けます。

例

次に、ユーザ名が josmithe である場合に true と評価するコントロール クラスを設定する例を示します。

```
class-map type control subscriber match-all CLASS_1
 match username josmithe
```

関連コマンド

コマンド	説明
class	制御ポリシーを制御クラスの1つ以上のアクションに関連付けます。
policy-map type control subscriber	加入者セッションに対するコントロール ポリシーを定義します

match wireless ssid（ワイヤレス）

ワイヤレス ネットワークの SSID をフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match wireless ssid** コマンドを使用します。ワイヤレス ネットワークの SSID をフロー レコードのキー フィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します

match wireless ssid
no match wireless ssid

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ワイヤレス ネットワークの SSID はキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを差別化するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次に、ワイヤレス ネットワークの SSID をキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match wireless ssid
```

match wireless ssid（ワイヤレス）

ワイヤレス ネットワークの SSID をフロー レコードのキー フィールドとして設定するには、フロー レコード コンフィギュレーション モードで **match wireless ssid** コマンドを使用します。ワイヤレス ネットワークの SSID をフロー レコードのキー フィールドとして使用することを無効にするには、このコマンドの **no** 形式を使用します

match wireless ssid
no match wireless ssid

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ワイヤレス ネットワークの SSID はキー フィールドとして設定されていません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードをフロー モニタで使用するには、1 つ以上のキー フィールドが必要になります。キー フィールドはフローを差別化するものです。各フローのキー フィールドには、一連の一意の値が設定されています。キー フィールドは、**match** コマンドを使用して定義されます。

次に、ワイヤレス ネットワークの SSID をキー フィールドとして設定する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match wireless ssid
```

match（アクセス マップ コンフィギュレーション）

VLANマップを1つまたは複数のアクセスリストとパケットを照合するように設定するには、アクセスマップ コンフィギュレーションモードで**match**コマンドを使用します。一致パラメータを削除するには、このコマンドの **no** 形式を使用します。

{**match ip address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]...|**mac address** *name* [*name*] [*name*]...}
{**no match ip address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]...|**mac address** *name* [*name*] [*name*]...}

構文の説明

ip address	パケットを IP アドレス アクセス リストと照合するようにアクセス マップを設定します。
mac address	パケットを MAC アドレス アクセス リストと照合するようにアクセス マップを設定します。
name	パケットを照合するアクセス リストの名前です。
number	パケットを照合するアクセス リストの番号です。このオプションは、MAC アクセス リストに対しては無効です。

コマンド デフォルト

デフォルトのアクションでは、一致パラメータは VLAN マップに適用されません。

コマンド モード

アクセス マップ コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

vlan access-map グローバル コンフィギュレーション コマンドを使用して、アクセスマップ コンフィギュレーション モードを開始します。

1 つのアクセス リストの名前または番号を入力する必要があります。その他は任意です。パケットは、1つまたは複数のアクセスリストに対して照合できます。いずれかのリストに一致すると、エントリの一致としてカウントされます。

アクセス マップ コンフィギュレーション モードでは、**match** コマンドを使用して、VLAN に適用されるVLANマップの一致条件を定義できます。**action**コマンドを使用すると、パケットが条件に一致したときに実行するアクションを設定できます。

パケットは、同じプロトコル タイプのアクセス リストに対してだけ照合されます。IP パケットは、IP アクセス リストに対して照合され、その他のパケットはすべて MAC アクセス リストに対して照合されます。

同じマップ エントリに、IP アドレスと MAC アドレスの両方を指定できます。

例

次の例では、VLAN アクセス マップ *vmap4* を定義し VLAN 5 と VLAN 6 に適用する方法を示します。このアクセス マップでは、パケットがアクセス リスト *al2* に定義された条件に一致すると、インターフェイスは IP パケットをドロップします。

```
デバイス(config)# vlan access-map vmap4
デバイス(config-access-map)# match ip address al2
デバイス(config-access-map)# action drop
デバイス(config-access-map)# exit
デバイス(config)# vlan filter vmap4 vlan-list 5-6
```

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

match（クラスマップ コンフィギュレーション）

トラフィックを分類するための一致基準を定義するには、クラスマップ コンフィギュレーション モードで **match** コマンドを使用します。一致基準を削除するには、このコマンドの **no** 形式を使用します。

Cisco IOS XE Everest 16.5.x 以前のリリース

match {**access-group**{**name***acl-name acl-index*} | **class-map** *class-map-name* | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **precedence** *precedence-value1...value4* | **qos-group** *qos-group-value* | **vlan** *vlan-id*}
no match {**access-group**{**name***acl-name acl-index*} | **class-map** *class-map-name* | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **precedence** *precedence-value1...value4* | **qos-group** *qos-group-value* | **vlan** *vlan-id*}

Cisco IOS XE Everest 16.6.x 以降のリリース

match {**access-group**{**name** *acl-name acl-index*} | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **mpls** *experimental-value* | **non-client-nrt** | **precedence** *precedence-value1...value4* | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **vlan** *vlan-id* | **wlan** *wlan-id*}
no match {**access-group**{**name** *acl-name acl-index*} | **cos** *cos-value* | **dscp** *dscp-value* | [**ip**] **dscp** *dscp-list* | [**ip**] **precedence** *ip-precedence-list* | **mpls** *experimental-value* | **non-client-nrt** | **precedence** *precedence-value1...value4* | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **vlan** *vlan-id* | **wlan** *wlan-id*}

構文の説明

access-group	アクセス グループを指定します。
name *acl-name*	IP 標準または拡張アクセス コントロール リスト（ACL）または MAC ACL の名前を指定します。
acl-index	IP 標準または拡張アクセス コントロール リスト（ACL）または MAC ACL の番号を指定します。IP 標準 ACL の場合、ACL インデックス範囲は 1 ～ 99 および 1300 ～ 1999 です。IP 拡張 ACL の場合、ACL インデックス範囲は 100 ～ 199 および 2000 ～ 2699 です。
class-map *class-map-name*	トラフィック クラスを分類ポリシーとして使用し、使用するトラフィック クラスの名前を一致基準として指定します。

cos *cos-value*	レイヤ 2 サービス クラス（CoS）/Inter-Switch Link（ISL）マーキングに基づいてパケットを照合します。CoS 値は 0 ～ 7 です。1 つの **match cos** ステートメントに最大 4 つの CoS 値をスペースで区切って指定できます。
dscp *dscp-value*	各 DSCP 値のパラメータを指定します。DiffServ コード ポイント値を指定する 0 ～ 63 の範囲の値を指定できます。
ip dscp *dscp-list*	着信パケットとの照合を行うための、最大 8 つまでの IP DiffServ コード ポイント（DSCP）値の一覧を指定します。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。一般的に使用する値に対してはニーモニック名を入力することもできます。
ip precedence *ip-precedence-list*	着信パケットとの照合を行うための、最大 8 つの IP プレシデンス値の一覧を指定します。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。一般的に使用する値に対してはニーモニック名を入力することもできます。
precedence *precedence-value1...value4*	分類されたトラフィックに IP プレシデンス値を割り当てます。指定できる範囲は 0 ～ 7 です。一般的に使用する値に対してはニーモニック名を入力することもできます。
qos-group *qos-group-value*	特定の QoS グループ値を一致基準として識別します。指定できる範囲は 0 ～ 31 です。
vlan *vlan-id*	特定の VLAN を一致基準として指定します。指定できる範囲は 1 ～ 4094 です。
mpls *experimental-value*	マルチ プロトコル ラベル スイッチングの特定の値を指定します。
non-client-nrt	非クライアントの NRT（非リアルタイム）を照合します。
protocol *protocol-name*	プロトコルのタイプを指定します。
wlan *wlan-id*	802.11 特有の値を識別します。

コマンド デフォルト　一致基準は定義されません。

コマンド モード　クラスマップ コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入

使用上のガイドライン

パケットを分類するために着信パケットのどのフィールドを調べるのかを指定する場合は、**match** コマンドを使用します。IP アクセス グループまたは MAC アクセス グループの Ether Type/Len のマッチングだけがサポートされています。

class-map match-any*class-map-name* グローバル コンフィギュレーション コマンドを入力した場合、次の **match** コマンドを入力できます。

- **match access-group name** *acl-name*

（注） ACL は、名前付き拡張 ACL にする必要があります。

- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

match access-group *acl-index* コマンドはサポートされていません。

物理ポート単位でパケット分類を定義するために、クラス マップごとに 1 つの **match** コマンドのみがサポートされています。この場合、**match-any** キーワードと同じです。

match ip dscp *dscp-list* コマンドまたは **match ip precedence** *ip-precedence-list* コマンドの場合は、よく使用される値のニーモニック名を入力できます。たとえば、**match ip dscp af11** コマンドを入力すると、**match ip dscp 10** コマンドを入力した場合と同じになります。**match ip precedence critical** コマンドを入力すると、**match ip precedence 5** コマンドを入力した場合と同じになります。サポートされているニーモニックの一覧を表示するには、**match ip dscp ?** または **match ip precedence ?** コマンドを入力して、コマンドラインのヘルプ文字列を参照してください。

階層ポリシー マップ内にインターフェイス レベルのクラス マップを設定するときには、**input-interface** *interface-id-list* キーワードを使用します。*interface-id-list* には、最大 6 つのエントリを指定することができます。

例

次の例では、クラス マップ class2 を作成する方法を示します。このマップは、DSCP 値 10、11、および 12 を持つすべての着信トラフィックに一致します。

```
デバイス(config)# class-map class2
デバイス(config-cmap)# match ip dscp 10 11 12
デバイス(config-cmap)# exit
```

次の例では、クラス マップ class3 を作成する方法を示します。このマップは、IP precedence 値 5、6、および 7 を持つすべての着信トラフィックに一致します。

```
デバイス(config)# class-map class3
デバイス(config-cmap)# match ip precedence 5 6 7
デバイス(config-cmap)# exit
```

次の例では、IP precedence 一致基準を削除し、acl1 を使用してトラフィックを分類する方法を示します。

```
デバイス(config)# class-map class2
デバイス(config-cmap)# match ip precedence 5 6 7
デバイス(config-cmap)# no match ip precedence
デバイス(config-cmap)# match access-group acl1
デバイス(config-cmap)# exit
```

次の例では、階層ポリシー マップでインターフェイス レベルのクラス マップが適用する物理ポートのリストの指定方法を示しています。

```
デバイス(config)# class-map match-any class4
デバイス(config-cmap)# match cos 4
デバイス(config-cmap)# exit
```

次の例では、階層ポリシー マップでインターフェイス レベルのクラス マップが適用する物理ポートの範囲の指定方法を示しています。

```
デバイス(config)# class-map match-any class4
デバイス(config-cmap)# match cos 4
デバイス(config-cmap)# exit
```

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

match wlan user-priority

802.11 固有の値を照合するには、クラスマップ コンフィギュレーション モードで **match wlan user-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

match wlan user-priority *wlan-value* ［*wlan-value*］ ［*wlan-value*］ ［*wlan-value*］
no match wlan user-priority *wlan-value* ［*wlan-value*］ ［*wlan-value*］ ［*wlan-value*］

構文の説明

wlan-value	802.11 固有の値。ユーザ プライオリティ 802.11 TID user priority（0-7）を入力します。（任意）ユーザ プライオリティ値を 3 つまで、空白文字区切りで入力します。

コマンド デフォルト

なし

コマンド モード

クラス マップ コンフィギュレーション（config-cmap）

コマンド履歴

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

使用上のガイドライン

なし

次に、ユーザ プライオリティ値を設定する例を示します。

```
デバイス(config)# class-map test_1000
デバイス(config-cmap)# match wlan user-priority 7
```

max-bandwidth

ワイヤレス メディアストリームの予想される最大ストリーム帯域幅を Kbps 単位で設定するには、 **max-bandwidth** コマンドを使用します。

max-bandwidth *bandwidth*

構文の説明

bandwidth	予想される最大ストリーム帯域幅（Kbps 単位）。有効な範囲は 1 ～ 35000 Kbps です。

コマンド デフォルト

なし

コマンド モード

media-stream

コマンド履歴

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

例

次に、ワイヤレス メディアストリームの帯域幅を Kbps 単位で設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group doc-grp 224.0.0.0 224.0.0.223
Device(config-media-stream)# max-bandwidth 3500
```

max-through

スロットル期間ごとにVLANごとのマルチキャストルータアドバタイズメント（RA）を制限するには、IPv6 RA スロットル ポリシー コンフィギュレーション モードで **max-through** コマンドを使用します。コマンドをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

max-through {*mt-value* | **inherit** | **no-limit**}

構文の説明

mt-value	スロットリングが発生する前にVLANで許可されているマルチキャストRAの数。範囲は 0 ～ 256 です。
inherit	ターゲット ポリシー間で設定をマージします。
no-limit	マルチキャスト RA は、VLAN では制限されません。

コマンド デフォルト

RA は VLAN ごとに 10 分間で 10 回

コマンド モード

IPv6 RA スロットル ポリシー コンフィギュレーション（config-nd-ra-throttle）

コマンド履歴

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

使用上のガイドライン

max-through コマンドは、スロットル期間ごとにVLANに渡されるマルチキャストRAの量を制限します。このコマンドは、VLAN でのみ設定できます。

例

```
Device(config)# ipv6 nd ra-throttle policy policy1
Device(config-nd-ra-throttle)# max-through 25
```

mdns-sd

mDNSサービス検出ゲートウェイを設定するには、**mdns-sd** コマンドを使用します。この設定を無効にするには、このコマンドの **no** 形式を使用します。

mdns-sd { **gateway** | **service-definition** *service-definition-name* | **service-list** *service-list-name* { **IN** | **OUT** } | **service-policy** *service-policy-name* }

no mdns-sd { **gateway** | **service-definition** *service-definition-name* | **service-list** *service-list-name* { **IN** | **OUT** } | **service-policy** *service-policy-name* }

構文の説明

mdns-sd	mDNSサービス検出ゲートウェイを設定します。
gateway	mDNS ゲートウェイを設定します。
service-definition	mDNS サービス定義を設定します。
service-definition-name	mDNS サービス定義名を指定します。
service-list	mDNS サービスリストを設定します。
service-list-name	mDNS サービス定義名を指定します。
IN	インバウンドフィルタリングを指定します。
OUT	アウトバウンド フィルタリングを指定します。
service-policy	mDNS サービスポリシーを設定します。
service-policy-name	mDNS サービスポリシー名を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし

例

次に、mDNS サービス検出ゲートウェイを設定する例を示します。

```
Device(config)# mdns-sd gateway
```

mdns-sd flex-profile

mDNS サービス検出 Flex プロファイルを設定するには、**mdns-sd flex-profile** コマンドを使用します。このコマンドを無効にするには、このコマンドの **no** 形式を使用します。

mdns-sd flex-profile *flex-profile-name*

no mdns-sd flex-profile *flex-profile-name*

構文の説明

mdns-sd flex-profile	mDNS サービス検出 Flex プロファイルを設定します。
flex-profile-name	mDNS Flex プロファイル名を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし

例

次に、mDNS サービス検出 Flex プロファイルを設定する例を示します。

```
Device(config)# mdns-sd flex-profile mdns-flex-profile
```

mdns-sd profile

mDNS Flex プロファイルをワイヤレス Flex プロファイルに適用するには、ワイヤレス Flex プロファイルモードで**mdns-sd profile** コマンドを使用します。このコマンドを無効にするには、このコマンドの **no** 形式を使用します。

mdns-sd profile *flex-profile-name*

no mdns-sd profile *flex-profile-name*

構文の説明

mdns-sd profile	ワイヤレス Flex プロファイルの mDNS Flex プロファイルを設定します。
flex-profile-name	mDNS Flex プロファイル名を指定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス Flex プロファイル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし

例

次に、mDNS Flex プロファイルをワイヤレス Flex プロファイルに適用する例を示します。

```
Device(config-wireless-flex-profile)# mdns-sd profile mdns-flex-profile
```

mdns-sd wired-filter

mDNS 有線フィルタを設定するには、**mdns-sd wired-filter** コマンドを使用します。

mdns-sd wired-filter *wired-filter-name*

構文の説明

wired-filter-name	有線フィルタ名です。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

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

使用上のガイドライン

次に、mDNS 有線フィルタを設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# mdns-sd wired-filter WIRED_FILTER_APPLE_TV
Device(config-mdns-wired-filter)# match mac a886.ddb2.05e9
Device(config-mdns-wired-filter)# match vlan 100
Device(config-mdns-wired-filter)# exit
```

method

OSU オペレータのプライマリおよびセカンダリでサポートされるオンラインサインアップ（OSU）方式を設定するには、**method** コマンドを使用します。OSU 方式を削除するには、このコマンドの **no** 形式を使用します。

method {**oma-dm** | **soap-xml-sp**}

構文の説明

oma-dm	OMA-DM を、OSU オペレータのプライマリまたはセカンダリの OSU 方式として設定します。
soap-xml-sp	SOAP または XML-SPP を、OSU オペレータのプライマリまたはセカンダリの OSU 方式として設定します。

コマンド デフォルト

なし

コマンド モード

ANQP OSU プロバイダーの設定（config-anqp-osu-provider）

コマンド履歴

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

例

次に、OSU オペレータのプライマリおよびセカンダリでサポートされる OSU 方式を設定する例を示します。

```
Device(config-wireless-anqp-server)# osu-provider my-osu
Device(config-anqp-osu-provider)# method soap-xml-spp oma-dm
```

method（メッシュ）

メッシュ AP プロファイルの認証および許可方式を設定するには、**method** コマンドを使用します。

method {**authentication** | **authorization** }*method*

構文の説明

authentication	メッシュ AP 認証の AAA 方式。
authorization	メッシュ AP 許可の AAA 方式。
method	名前付き方式リスト。

コマンド デフォルト

認証および許可方式は設定されていません。

コマンド モード

config-wireless-mesh-profile

コマンド履歴

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

例

次に、メッシュ AP プロファイルの認証を設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# method authentication auth1
```

method fast

EAP-FAST 方式をサポートするように EAP プロファイルを設定するには、**method fast** コマンドを使用します。

method fast [**profile** *profile-name*]

構文の説明

profile-name	方式プロファイルを指定します。

コマンド デフォルト

なし

コマンド モード

config-eap-profile

コマンド履歴

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

例

次に、EAP プロファイルで EAP Fast 方式を有効にする例を示します。

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

mesh backhaul

無線プロファイルコンフィギュレーションモードでメッシュバックホールを有効にするには、**mesh backhaul** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

mesh backhaul

no mesh backhaul

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

ワイヤレス無線プロファイル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

特定のスロットでメッシュバックホールを無効にできます。メッシュバックホールは、特定のスロットがバックホール候補にならないようにするために無効にされます。

例

次に、無線プロファイルコンフィギュレーションモードでメッシュバックホールを有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless radio profile radio-profile-name
Device(config-wireless-radio-profile)# mesh backhaul
```

mesh designated downlink

無線プロファイル コンフィギュレーション モードで無線スロットを指定メッシュダウンリンクとして有効にするには、**mesh designated downlink** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

mesh designated downlink

no mesh designated downlink

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

デフォルトでは、このコマンドは無効になっています。デフォルトでは、すべての無線スロットでメッシュが有効になっていて、ダウンリンクとして指定されていません。

コマンド モード

ワイヤレス無線プロファイル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

このコマンドは、メッシュ AP のスロット 2 に対してのみ有効です。スロット 2 以外のスロットが指定ダウンリンクとして設定された場合、「Designated downlink is supported only on slot 2 of mesh APs. Associate in the RF tag accordingly.」という警告メッセージが表示されます。

例

次に、無線スロットを指定メッシュダウンリンクとして有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless radio profile radio-profile-name
Device(config-wireless-radio-profile)# mesh designated downlink
```

mgmtuser username

AP 管理用のユーザー名とパスワードを設定するには、**mgmtuser username** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

mgmtuser username *username* **password {0 | 8}** *password*

構文の説明

username	AP 管理用のユーザー名を入力します。
0	暗号化されていないパスワードを指定します。
8	AES 暗号化パスワードを指定します。
password	暗号化パスワード（キー）を設定します。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 17.6.1	このコマンドが導入されました。

例

次に、AP 管理用のユーザー名とパスワードを設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# mgmtuser username myusername password 0
Device(config-ap-profile)# end
```

mobility anchor

モビリティ スティッキ アンカリングを設定するには、 **mobility anchor** コマンドを使用します。モビリティアンカーリングを無効にするには、このコマンドの **no** 形式を使用します。

ゲスト アンカリングを設定するには、**mobility anchor** *ip-address* コマンドを使用します。ゲスト アンカーを削除するには、このコマンドの **no** 形式を使用します。

デバイスを自動アンカーとして設定するには、**mobility anchor** コマンドを使用します。

mobility anchor *ip-address*
no mobility anchor *ip-address*

構文の説明

ip-address	ゲストアンカーのIPアドレスを設定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ポリシー コンフィギュレーション

コマンド履歴

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

次に、ゲスト アンカリングを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# mobility anchor 209.165.200.224
```

次に、デバイスを自動アンカーとして設定する例を示します。

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

monitor capture（アクセスリスト/クラスマップ）

アクセスリストまたはクラスマップをパケットキャプチャのコアフィルタとして指定してモニターキャプチャを設定するには、特権 EXEC モードで **monitor capture** コマンドを使用します。指定したアクセスリストまたはクラスマップをコアフィルタとして使用したモニターキャプチャを無効にするには、このコマンドの **no** 形式を使用します。

monitor capture *capture-name* { **access-list** *access-list-name* | **class-map** *class-map-name* }
no monitor capture *capture-name* { **access-list** *access-list-name* | **class-map** *class-map-name* }

構文の説明

capture-name	キャプチャの名前。
access-list *access-list-name*	指定した名前のアクセスリストを設定します。
class-map *class-map-name*	指定した名前のクラスマップを設定します。

コマンド デフォルト

指定したアクセスリストまたはクラスマップをパケットキャプチャのコアフィルタとして使用したモニターキャプチャは設定されていません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 3.7S	このコマンドが導入されました。

使用上のガイドライン

ip access-list コマンドを使用してアクセスリストを設定するか、**monitor capture** コマンドを使用する前に **class-map** コマンドを使用してクラスマップを設定します。クラスマップ、アクセスリスト、または明示的なインラインフィルタをコアフィルタとして指定できます。**monitor capture match** コマンドの入力時にすでにフィルタが指定されている場合は、このコマンドによって既存のフィルタが置き換えられます。

例

次に、既存のアクセス制御リストを使用してコアシステムフィルタを定義する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit any
Device(config-std-nacl)# exit
Device(config)# exit
Device# monitor capture mycap access-list acl1
Device# end
```

次に、既存のクラスマップを使用してコアシステムフィルタを定義する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit any
Device(config-std-nacl)# exit
Device(config)# class-map match-all cmap
Device(config-cmap)# match access-group name acl
Device(config-cmap)# exit
Device(config)# exit
Device# monitor capture mycap class-map classmap1
Device# end
```

monitor capture buffer circular file file-size

循環バッファのファイルを設定するには、**monitor capture** *epc-session-name* **buffer circular file** *no-of-files* **file-size** *per-file-size* コマンドを使用します。

または線形。

monitor capture *epc-session-name* **buffer circular file** *no-of-files* **file-size** *per-file-size*

構文の説明

epc-session-name	EPC セッションキャプチャの名前を指定します。
no-of-files	循環バッファで設定するファイルの数を指定します。設定するファイル数の値の範囲は 2 ～ 5 です。
per-file-size	設定する各ファイルのファイルサイズを指定します。ファイルサイズの値の範囲は 1 MB ～ 500 MB です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

循環が設定されている場合、ファイルはリングバッファとして機能します。buffer コマンドには、**circular**、**file**、**size** などのさまざまなオプションを使用できます。継続的なキャプチャには、循環バッファが必要です。

例

次に、循環バッファのファイルを設定する例を示します。

```
Device# monitor capture epc-session1 buffer circular file 4 file-size 20
```

monitor capture continuous-capture

継続的なパケットキャプチャを設定し、バッファが上書きされる前の特定の場所へのファイルの自動エクスポートを有効にするには、**monitor capture** *epc-capture-name* **continuous-capture** {**ftp:** | **http:** | **https:** | **pram:** | **rcp:** | **scp:** | **sftp:** | **tftp:**} を使用します。

monitor capture *epc-capture-name* **continuous-capture** { **ftp:** | **http:** | **https:** | **pram:** | **rcp:** | **scp:** | **sftp:** | **tftp:** }

構文の説明

epc-capture-name	組み込みパケットキャプチャ（EPC）ファイルの名前を指定します。
{ **ftp:** | **http: https:** | **pram:** | **rcp:** | **scp** | **sftp:** | **tftp:**}	EPC ファイルが保存される場所を指定します。ファイル名には、.pcap という拡張子が必要です。 次に、ファイル名と、ファイル名の生成に使用される名称の例を示します。 CONTINUOUS_CAP_20230601130203.pcap CONTINUOUS_CAP_20230601130240.pcap

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、継続的なキャプチャを設定する例を示します。

```
Device# monitor capture epc-session1 continuous-capture https://www.cisco.com/epc1.pcap
```

monitor capture export

キャプチャされたパケットをファイルに保存するには、特権 EXEC モードで **monitor capture export** コマンドを使用します。

monitor capture *capture-name* **export** *filelocation* / *file-name*

構文の説明

capture-name	キャプチャの名前。
export	.PCAP タイプのファイルにキャプチャバッファ内のすべてのパケットを保存します。
file-location/file-name	宛先ファイルの場所と名前。

コマンド デフォルト

キャプチャされたパケットは保存されません。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

ストレージの宛先がキャプチャバッファである場合にのみ **monitor capture export** コマンドを使用します。ファイルはリモートにもローカルにも保存できます。キャプチャ中またはパケットキャプチャ停止後にこのコマンドを使用します。パケットキャプチャは、1 つ以上の終了条件が満たされたため、または **monitor capture stop** コマンドが入力されたために停止していることがあります。

例

次に、キャプチャバッファの内容をエクスポートする例を示します。

```
Device> enable
Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap
Device# end
```

monitor capture inner mac

内部フィルタの MAC アドレスを設定するには、**monitor capture** *epc-capture-name* **inner mac** *MAC1 MAC2 MAC3* を使用します

monitor capture *epc-capture-name* **inner mac** *MAC1* *MAC2* *MAC3*

構文の説明

epc-capture-name	組み込みパケットキャプチャ（EPC）ファイルの名前を指定します。
MAC1 [*MAC2...MAC3*]	MAC アドレスを内部 MAC フィルタとして設定します。最大 10 個の MAC アドレスを設定できます。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

MAC アドレスは、1 つのコマンドで入力することも、複数のコマンドラインを使用して入力することもできます。文字列の制限により、1 つのコマンドラインに入力できる MAC アドレスは 5 つまでです。次のコマンドラインに残りの MAC アドレスを入力できます。

設定された内部 MAC の数が 10 の場合、設定された古い内部 MAC アドレスを削除するまで、新しい MAC アドレスを設定することはできません。

例

次に、内部フィルタの MAC アドレスを設定する例を示します。

```
Device# monitor capture epc-session1 inner mac 1.1.1 2.2.2 3.3.3 4.4.4
```

monitor capture (interface/control plane)

接続ポイントおよびパケットフロー方向を指定してモニターキャプチャを設定するには、特権 EXEC モードで **monitor capture** コマンドを使用します。指定した接続ポイントおよびパケットフロー方向でモニターキャプチャを無効にするには、このコマンドの **no** 形式を使用します。

monitor capture *capture-name* { **interface** *type number* | **control-plane** } { **in** | **out** | **both** }
no monitor capture *capture-name* { **interface** *type number* | **control-plane** } { **in** | **out** | **both** }

構文の説明

capture-name	キャプチャの名前。
interface *type number*	指定したタイプと番号のインターフェイスを接続ポイントとして設定します。
control-plane	コントロールプレーンを接続ポイントとして設定します。
in	着信トラフィックの方向を指定します。
out	発信トラフィックの方向を指定します。
both	着信トラフィックと発信トラフィックの両方の方向を指定します。

コマンド デフォルト

モニター パケット キャプチャ フィルタの指定は設定されていません。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

複数の接続ポイントを追加するために、必要に応じて何度でも **monitor capture** コマンドを繰り返し実行できます。

例

次に、接続ポイントをインターフェイスに追加する例を示します。

```
Device> enable
Device# monitor capture mycap interface GigabitEthernet 0/0/1 in
Device# end
```

次に、接続ポイントをコントロールプレーンに追加する例を示します。

```
Device> enable
Device# monitor capture mycap control-plane out
Device# end
```

monitor capture limit

キャプチャ制限を設定するには、特権 EXEC モードで **monitor capture limit** コマンドを使用します。キャプチャ制限を削除するには、このコマンドの **no** 形式を使用します。

monitor capture *capture-name* **limit** ［ **duration** *seconds* ］ ［ **every** *number* ］ ［ **packet-length** *size* ］［ **packets** *number* ］ ［ **pps** *number* ］
no monitor capture *name* **limit** ［ **duration** ］ ［ **every** ］ ［ **packet-length** ］ ［ **packets** ］ ［ **pps** ］

構文の説明

capture-name	パケット キャプチャの名前。
duration *seconds*	（任意）キャプチャ期間（秒）を指定します。範囲は 1 ～ 1000000 です。
every *number*	（任意）一連のパケットで、*number* 引数で番号順が示されたパケットがキャプチャされます。範囲は 2 ～ 100000 です。
packet-length *bytes*	（任意）パケット長（バイト）を指定します。実際のパケットが特定の長さより長い場合、数が *bytes* 引数によって示される最初のセットのバイトのみが保存されます。
packets *packets-number*	（任意）キャプチャに対して処理されるパケット数を指定します。
pps *pps-number*	（任意）1 秒あたりのキャプチャされるパケット数を指定します。範囲は 1 ～ 1000000 です。

コマンド デフォルト

キャプチャ制限は設定されていません。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

期間が指定されていない場合、キャプチャは手動で中断されるまで停止しません。**packet-length** *bytes* のキーワードと引数のペアが指定されていない場合、パケット全体が処理されます。**every** *number* のキーワードと引数のペアが指定されていない場合、一致したすべてのパケットがキャプチャされます。 **packets** *packets-number* のキーワードと引数のペアが指定されていない場合、一致したすべてのパケットがキャプチャされます。**pps** *number* のキーワードと引数のペアが指定されていない場合、着信パケットは 1 秒あたり 100 万パケットのレートでキャプチャされます。

例

次に、キャプチャ制限を指定する例を示します。

```
Device> enable
Device# monitor capture mycap limit duration 10
Device# monitor capture mycap limit packet-length 128
Device# monitor capture mycap limit packets 100
Device# monitor capture mycap limit pps 1000
Device# monitor capture mycap limit duration 10 packet-length 128 packets 100
Device# end
```

monitor capture match

明示的にインラインコアフィルタを定義するには、特権 EXEC モードで **monitor capture match** コマンドを使用します。このフィルタを削除するには、コマンドの **no** 形式を使用します。

monitor capture *capture-name* **match** { **any** | { **ipv4** | **ipv6** } { *source-prefix/length* | **any** | **host** } *source-ip-address* { { *destination-prefix/length* | **any** | **host** } *destination-ip-address* } | **protocol** { **tcp** | **udp** } { { *source-prefix/length* | **any** | **host** } { { *destination-prefix/length* | **any** | **host** } | [[{ **eq** | **gt** | **lt** | **neg** }] *port-number*] | **range** *start-port-number end-port-number* | [{ **eq** | **gt** | **lt** | **neg** }] *port-number* | **range** *start-port-number end-port-number* } } | **mac** { *source-mac-address* | { **any** | **host** } *source-mac-address* } *source-mac-address-mask* { *destination-mac-address* | { **any** | **host** } *destination-mac-address* } *destination-mac-address-mask* }

no monitor capture *capture-name* **match**

構文の説明

epc-capture-name	キャプチャの名前。
any	すべてのパケットを指定します。
ipv4	IPv4 パケットを指定します。
ipv6	IPv6 パケットを指定します。
source-prefix/length	IPv4 または IPv6 送信元アドレスのネットワークプレフィックスと長さ。
any	任意の送信元 IPv4 または IPv6 アドレスのネットワークプレフィックスを指定します。
host	送信元ホストを指定します。
source-ip-address	送信元 IPv4 または IPv6 アドレス。
destination-prefix/length	宛先 IPv4 または IPv6 アドレス。
any	IPv4 または IPv6 宛先アドレスのネットワークプレフィックスと長さを指定します。
host	宛先ホストを指定します。
destination-ip-address	宛先 IPv4 または IPv6 アドレス。
protocol	プロトコルを指定します。
tcp	TCP プロトコルを指定します。
udp	UDP プロトコルを指定します。

eq	（任意）IP アドレスに関連付けられたポート番号と同じポート番号を持つパケットのみを一致させることを指定します。
gt	（任意）IP アドレスに関連付けられたポート番号より大きいポート番号を持つパケットのみを一致させることを指定します。
lt	（任意）IP アドレスに関連付けられたポート番号より小さいポート番号を持つパケットのみを一致させることを指定します。
neq	（任意）IP アドレスに関連付けられたポート番号と同じでないポート番号を持つパケットのみを一致させることを指定します。
port-number	（任意）IP アドレスに関連付けられたポート番号。範囲は 0 ～ 65535 です。
range	（任意）ポート番号の範囲を指定します。
start-port-number	（任意）ポート番号の範囲の開始。範囲は 0 ～ 65535 です。
end-port-number	（任意）ポート番号の範囲の終了。範囲は 0 ～ 65535 です。
mac	レイヤ 2 パケットを指定します。
source-mac-address	送信元 MAC アドレス。
any	任意の送信元MACアドレスのネットワークプレフィックスを指定します。
host	MAC 送信元ホストを指定します。
source-mac-address-mask	送信元 MAC アドレスマスク。
destination-mac-address	宛先 MAC アドレス。
any	任意の宛先MACアドレスのネットワークプレフィックスを指定します。
host	MAC 送信元ホストを指定します。
destination-mac-address-mask	宛先 MAC アドレスマスク。

コマンド モード　特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

monitor capture コマンドを使用して、コアフィルタをクラスマップ、アクセスリスト、または明示的なインラインフィルタとして指定します。**monitor capture match** コマンドを入力する前にすでに指定されていたフィルタは、置き換えられます。

例

次に、さまざまな明示的なフィルタを設定する例を示します。

```
Device> enable
Device# monitor capture mycap match any
Device# monitor capture mycap match mac any any
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap match ipv4 protocol udp 198.51.100.0/24 eq 20001 any
Device# end
```

次に、MAC アドレスのフィルタを設定する例を示します。

```
Device> enable
Device# monitor capture match mycap mac 0030.9629.9f84 0000.0000.0000 0030.7524.9f84
0000.0000.0000
Device# end
```

次に、IPv4 トラフィックのフィルタを設定する例を示します。

```
Device> enable
Device# monitor capture match mycap ipv4 198.51.100.0/24 198.51.100.1 203.0.113.0/24
203.0.113.254
Device# end
```

monitor capture start

トラフィック トレース ポイントでパケットデータのバッファへのキャプチャを開始するには、特権 EXEC モードで **monitor capture start** コマンドを使用します。

monitor capture *epc-capture-name* **start**

構文の説明

epc-capture-name	キャプチャの名前。

コマンド デフォルト

データパケットはバッファにキャプチャされません。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

キャプチャポイントが定義された後にパケットデータキャプチャを有効にするには、**monitor capture start** コマンドを使用します。パケットデータのキャプチャを停止するには、**monitor capture stop** コマンドを使用します。

CPU およびメモリなどのシステム リソースがキャプチャの開始前に使用可能であることを確認します。

例

次に、バッファ内容のキャプチャを開始する例を示します。

```
Device> enable
Device# monitor capture mycap start
Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap
Device# monitor capture mycap limit packets 100 duration 60
Device# monitor capture mycap start
Device# end
```

monitor capture stop

トラフィック トレース ポイントでパケットデータのキャプチャを停止するには、特権 EXEC モードで **monitor capture stop** コマンドを使用します。

monitor capture *epc-capture-name* **stop**

構文の説明

epc-capture-name	キャプチャの名前。

コマンド デフォルト

パケット データ キャプチャが進行中です。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

monitor capture start コマンドを使用して、**monitor capture start** コマンドによって開始したパケットデータのキャプチャを開始します。線形および循環の 2 つのタイプのキャプチャ バッファを設定できます。線形バッファがいっぱいになった場合、データ キャプチャは自動的に停止します。循環バッファがいっぱいになると、データ キャプチャは最初から開始し、データは上書きされます。

例

次に、バッファ内容のキャプチャを停止する例を示します。

```
Device> enable
Device# monitor capture mycap stop
Device# end
```

mop enabled

インターフェイスが Maintenance Operation Protocol（MOP）をサポートできるようにするには、インターフェイス コンフィギュレーション モードで **mopenabled** コマンドを使用します。インターフェイスで MOP をディセーブルにするには、このコマンドの **no** 形式を使用します。

mop enabled
no mop enabled

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

イーサネット インターフェイスではイネーブル、他のすべてのインターフェイスではディセーブルになっています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

例

次に、シリアル インターフェイス 0 で MOP をイネーブルにする例を示します。

```
Router(config)# interface serial 0
Router(config-if)# mop enabled
```

関連コマンド

コマンド	説明
mop retransmit-timer	Cisco IOS ソフトウェアが MOP サーバーにブート要求を再送信するまでに待機する時間の長さを設定します。
mop retries	Cisco IOS ソフトウェアがブート要求を MOP サーバに再送信する回数を設定します。
mop sysid	インターフェイスが定期的な MOP システム識別メッセージを送信できるようにします。

mop sysid

インターフェイスが定期的な Maintenance Operation Protocol（MOP）システム識別メッセージを送信できるようにするには、インターフェイス コンフィギュレーション モードで **mopsysid** コマンドを使用します。インターフェイスで MOP メッセージのサポートを無効にするには、このコマンドの **no** 形式を使用します。

mop sysid
no mop sysid

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

有効

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

バックグラウンド システム ID メッセージを送信しなくても、MOP を実行することはできます。このコマンドを使用すると、MOP リモート コンソールを使用できますが、configurator で使用されるメッセージは生成されません。

例

次に、シリアル インターフェイス 0 が MOP システム識別メッセージを送信できるようにする例を示します。

```
Router(config)# interface serial 0
Router(config-if)# mop sysid
```

関連コマンド

コマンド	説明
mop device-code	MOP システム識別メッセージを送信するデバイスのタイプを識別し、プログラム メッセージを要求します。
mop enabled	インターフェイスが MOP をサポートできるようにします。

multicast

メッシュ マルチキャスト モードを設定するには、 **multicast** コマンドを使用します。

multicast { **in-only** | **in-out** | **regular** }

構文の説明

in-only	メッシュ マルチキャスト In モードを設定します。
in-out	メッシュ マルチキャスト In-Out モードを設定します。
regular	メッシュ マルチキャスト Regular モードを設定します。

コマンド デフォルト

in-out

コマンド モード

config-wireless-mesh-profile

コマンド履歴

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

例

次に、メッシュ AP プロファイルにマルチキャスト In モードを設定する例を示します。

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

multicast vlan

単一の VLAN にマルチキャストを設定するには、 **multicast vlan** コマンドを使用します。マルチキャストを削除するには、このコマンドの **no** 形式を使用します。

multicast vlan *vlan-id*
no multicast vlan *vlan-id*

構文の説明

vlan-id	VLAN ID を指定します。

コマンド デフォルト

ディセーブル

コマンド モード

ワイヤレス ポリシー コンフィギュレーション

コマンド履歴

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

次に、マルチキャストを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy policy-test
Device(config-wireless-policy)# multicast vlan 12
```

multicast filter

マルチキャストフィルタを設定するには、**multicast filter** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

multicast filter

構文の説明

multicast filter	マルチキャストフィルタを設定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ポリシー コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、マルチキャストフィルタを設定する例を示します。

```
Device(config-wireless-policy)# multicast filter
```

name

オンラインサインアップ（OSU）オペレータの名前を特定の言語で設定するには、**name** コマンドを使用します。OSU オペレータの名前を削除するには、このコマンドの **no** 形式を使用します。

name *operator-name language-code* [*service-description*]

構文の説明

operator-name	OSU オペレータ名。
language-code	オペレータの 3 文字の言語コード。言語コードには、言語の最初の 3 文字のみを小文字で使用します。たとえば、英語の場合は *eng* を使用します。 言語コードの完全なリストについては、http://www.loc.gov/standards/iso639-2/php/code_list.php を参照してください。
service-description	OSU オペレータのサービスの説明。

コマンド デフォルト

なし

コマンド モード

ANQP OSU プロバイダーの設定（config-anqp-osu-provider）

コマンド履歴

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

例

次に、OSU オペレータの名前を特定の言語で設定する例を示します。

```
Device(config-wireless-anqp-server)# osu-provider my-osu
Device(config-anqp-osu-provider)# name xxy eng
```

nac

RADIUS ネットワーク アドミッション コントロール（NAC）サポートを有効にするには、**nac** コマンドを使用します。NAC サポートを無効にするには、このコマンドの **no** 形式を使用します。

nac ［ **ise** | **xwf** ］
no nac

構文の説明

ise	Radius NAC サポート（Identity Service Engine）を設定します
xwf	Express Wi-Fi NAC サポートを設定します。

コマンド デフォルト

NAC は無効です。

コマンド モード

ワイヤレス ポリシー コンフィギュレーション

コマンド履歴

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

次に、RADIUS NAC を設定する例を示します。

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

nai-realm

802.11u ネットワーク アクセス識別子（NAI）レルムを設定するには、**nai-realm** コマンドを使用します。レルムを削除するには、このコマンドの **no** 形式を使用します。

nai-realm *nai-realm*

構文の説明

nai-realm	NAI レルム名。 レルム名は 220 文字までです。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、802.11u NAI レルムを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# nai-realm cisco.com
```

nai-realm

課金通知のネットワークアクセス識別子（NAI）レルムを設定するには、**nai-realm** コマンドを使用します。課金通知の NAI レルムを削除するには、このコマンドの **no** 形式を使用します。

nai-realm *realm-name*

構文の説明

realm-name	課金通知の NAI レルム名。

コマンド デフォルト

NAI レルムは設定されていません。

コマンド モード

ワイヤレス ANQP 課金通知コンフィギュレーション（config-anqp-advice-charge）

コマンド履歴

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

例

次に、課金通知の NAI レルムを設定する例を示します。

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

nai-realm（OSU プロバイダー）

OSU オペレータのネットワーク アクセス識別子（NAI）レルムを設定するには、**nai-realm** コマンドを使用します。OSU オペレータのレルムを削除するには、このコマンドの **no** 形式を使用します。

nai-realm *nai-realm*

構文の説明

nai-realm	NAI レルム名。 レルム名は220文字までです。

コマンド デフォルト

なし

コマンド モード

ANQP OSU プロバイダーの設定（config-anqp-osu-provider）

コマンド履歴

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

例

次に、OSU オペレータの NAI レルムを設定する例を示します。

```
Device(config-anqp-osu-provider)# nai-realm cisco.com
```

nas-id

NAS ID のオプションパラメータを設定するには、**nas-id** コマンドを使用します。

nas-id { **option1** | **option2** | **option3** } { **ap-eth-mac** | **ap-ip** | **ap-location** | **ap-mac** | **ap-name** | **ap-policy-tag** | **ap-site-tag** | **custom-string** *custom-string* | **ssid** | **sys-ip** | **sys-mac** | **sys-name** }

構文の説明

ap-eth-mac	AP のイーサネット MAC アドレス。
ap-ip	AP の IP アドレス。
ap-location	AP の場所。
ap-mac	AP の MAC アドレス。
ap-name	AP の名前。
ap-policy-tag	AP のポリシータグ。
ap-site-tag	AP のサイトタグ。
custom-string*custom-string*	option1、option2、および option3 のさまざまな組み合わせを使用した、カスタム文字列。
ssid	SSID。
sys-ip	システムの IP アドレス。
sys-mac	システムの MAC アドレス。
sys-name	システムの名前。

コマンド デフォルト

なし

コマンド モード

config-aaa-policy

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。
Cisco IOS XE Cupertino 17.7.1	次のキーワードと変数が追加されることで、このコマンドが変更されました。 • **custom-string** • *custom-string*

例

次に、NAS-ID のシステム IP アドレスを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy profile-name
Device(config-aaa-policy)# nas-id option2 sys-ip
```

次に、NAS-ID のカスタム文字列を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy profile-name
Device(config-aaa-policy)# nas-id option2 custom-string test
```

nas-id option2

NAS-ID のオプション 2 パラメータを設定するには、**nas-id option2** コマンドを使用します。

nas-id option2 {**sys-ip** | **sys-name** | **sys-mac** }

構文の説明

sys-ip	システム IP アドレス。
sys-name	システム名。
sys-mac	システム MAC アドレス。

コマンド デフォルト

なし

コマンド モード

config-aaa-policy

コマンド履歴

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

例

次に、NAS-ID のシステム IP アドレスを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless aaa policy profile-name
Device(config-aaa-policy)# nas-id option2 sys-ip
```

ndp-mode

RF プロファイルでの AP の NDP モードを設定するには、RF プロファイル コンフィギュレーションで **ndp-mode** コマンドを使用します。

ndp-mode { **auto** | **off-channel** }

構文の説明

ndp-mode	802.11a ネイバー探索の動作モードを設定します。
auto	auto モードを有効にします。
off-channel	RF ASIC 無線で NDP パケットを有効にします。

コマンド モード

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

コマンド履歴

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

例

次に、802.11a ネイバー探索の動作モードを設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 24ghz rf-profile rf-profile-name
Device(config-rf-profile)# ndp-mode auto
```

network

ネットワーク番号を 10 進表記で設定するには、**network** コマンドを使用します。

network *network-number*[{*network-mask* | **secondary** }]

構文の説明

ipv4-address	ドット付き 10 進表記のネットワーク番号。
network-mask	ネットワーク マスクまたはプレフィックス長。
secondary	セカンダリ サブネットとして設定します。

コマンド デフォルト

なし

コマンド モード

dhcp-config

コマンド履歴

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

例

次に、ネットワーク番号とマスク アドレスを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip dhcp pool name
Device(dhcp-config)# network 209.165.200.224 255.255.255.0
```

network-type

802.11u ネットワークタイプを設定するには、**network-type** コマンドを使用します。ネットワークタイプを削除するには、このコマンドの **no** 形式を使用します。

network-type { **chargeable-public** | **emergency** | **free-public** | **guest-private** | **personal-device** | **private** | **test** | **wildcard** } **internet-access** { **allowed** | **forbidden** }

構文の説明

chargeable-public	有料のパブリックネットワークとして設定します。
emergency	緊急ネットワークとして設定します。
free-public	無料のパブリックネットワークとして設定します。
guest-private	ゲスト プライベート ネットワークとして設定します。
personal-device	パーソナル デバイス ネットワークとして設定します。
private	プライベートネットワークとして設定します。
test	テストネットワークとして設定します。
wildcard	ワイルドカードネットワークとして設定します。
internet-access	インターネットにアクセスするためのネットワーク機能を設定します。
allowed	インターネットアクセスを有効にします。
disabled	インターネットアクセスを無効にします。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、802.11u ネットワークタイプを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# network-type wildcard internet-access allowed
```

nmsp cloud-services enable

NMSP クラウド サービスを設定するには、 **nmsp cloud-services enable** コマンドを使用します。

nmsp cloud-services enable

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、NMSP クラウド サービスを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services enable
```

nmsp cloud-services http-proxy

NMSP クラウド サーバのプロキシを設定するには、 **nmsp cloud-services http-proxy** コマンドを使用します。

nmsp cloud-services http-proxy *proxy-server port*

構文の説明

proxy-server	NMSP クラウド サービスのプロキシ サーバのホスト名または IP アドレスを入力します。
port	NMSP クラウド サービスのプロキシ サーバのポート番号を入力します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、NMSP クラウド サーバーのプロキシを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services http-proxy host-name port-number
```

nmsp cloud-services server token

NMSP クラウド サービス サーバのパラメータを設定するには、 **nmsp cloud-services server token** コマンドを使用します。

nmsp cloud-services server token *token*

構文の説明

token	NMSP クラウドサービスの認証トークン。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

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

例

次に、NMSP クラウド サービス サーバーのパラメータを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# nmsp cloud-services server token authentication-token
```

nmsp cloud-services server url

NMSP クラウド サービス サーバーの URL を設定するには、**nmsp cloud-services server url** コマンドを使用します。

nmsp cloud-services server url *url*

構文の説明

url	NMSP クラウドサービス サーバーの URL。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、NMSP クラウド サービス サーバーの URL を設定する例を示します。

```
Device(config)# nmps cloud-services server url http://www.example.com
```

nmsp notification interval

コントローラの Network Mobility Services Protocol（NMSP）通知間隔値をネットワークの遅延に対応するように変更するには、グローバル コンフィギュレーション モードで**nmsp notification interval** コマンドを使用します。

nmsp notification interval { **attachment** | **location** | **rssi** {**clients** | **rfid** | **rogues** {**ap** | **client** } } }

構文の説明

attachment	アタッチメント情報の集約に使用する時間を指定します。
location	ロケーション情報の集約に使用する時間を指定します。
rssi	RSSI 情報の集約に使用する時間を指定します。
clients	クライアントの時間間隔を指定します。
rfid	RFID タグの時間間隔を指定します。
rogues	不正 AP および不正クライアントの時間間隔を指定します。
ap	不正 AP の集約に使用する時間を指定します。
client	不正なクライアントの集約に使用する時間を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

次に、アクティブな RFID タグの NMSP 通知間隔を 25 秒に設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# nmsp notification-interval rfid 25
デバイス(config)# end
```

次に、デバイス アタッチメント（ネットワークへの接続またはネットワークからの切断）の NMSP 通知間隔を 10 秒に変更する例を示します。

```
デバイス# configure terminal
デバイス(config)# nmsp notification-interval attachment 10
デバイス(config)# end
```

次に、ロケーション パラメータ（ロケーション変更）の NMSP 通知間隔を 20 秒に設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# nmsp notification-interval location 20
デバイス(config)# end
```

nmsp strong-cipher

新しい暗号化方式を有効にするには、グローバル コンフィギュレーション モードで **nmsp strong-cipher** コマンドを使用します。無効にするには、このコマンドの **no** 形式を使用します。

nmsp strong-cipher
no nmsp strong-cipher

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

新しい暗号化方式は有効になっていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
15.2(2)E	このコマンドが導入されました。

使用上のガイドライン

nmsp strong-cipher コマンドは、新しい Network Mobility Service Protocol（NMSP）接続に対し、強力な暗号化方式を有効にします。

（注） 既存の NMSP 接続では、デフォルトの暗号化方式が使用されます。

例

次に、NMSP に対して強力な暗号化方式を有効にする例を示します。

```
Device> enable
Device> configure terminal
Device(config)# nmsp strong-cipher
```

関連コマンド

コマンド	説明
show nmsp status	アクティブな NMSP 接続の状態を表示します。

no redun-management fast-switchover

明示的高速スイッチオーバー通知を無効にするには、**no redun-management fast-switchover** コマンドを使用します。

（注） これは、プライマリコントローラで設定します。この設定は、セカンダリコントローラでは必要ありません。

no redun-management fast-switchover

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、明示的高速スイッチオーバー通知を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# no redun-management fast-switchover
```

no redun-management garp-retransmit initial

初期 GARP を無効にするには、**no redun-management garp-retransmit initial** コマンドを使用します。

no redun-management garp-retransmit initial

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、初期 GARP を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# no redun-management garp-retransmit initial
```

no accounting-interim

中間アカウンティングを無効にするには、**no accounting-interim** コマンドを使用します。

no accounting-interim

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、中間アカウンティングを無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy <default-policy-profile>
Device(config-wireless-policy)# no accounting-interim
```

ntp auth-key

AP プロファイルで Network Time Protocol（NTP）サーバー認証キー情報を設定するには、**ntp auth-key** コマンドを使用します。AP プロファイルから NTP サーバー認証キー情報を削除するには、**no ntp auth-key** コマンドを使用します。

ntp auth-key index *key-index* **type** { **md5** | **sha1** } **format** { **ascii** | **hex** } **key** { **0** | **8** } *server-key*

構文の説明

key-index	キーインデックス。有効な範囲は 1 ～ 65535 です。
md5	Message Digest 5（MD5）認証キーが後ろに続くことを指定します。
sha1	セキュア ハッシュ アルゴリズム 1（SHA1）認証キーが後ろに続くことを指定します。
format	キー形式（ASCII または HEX）を定義します。
ascii	ASCII キーが後ろに続くことを指定します。
hex	16 進キーが後ろに続くことを指定します。
key	NTP サーバーキー（非暗号化または暗号化）を定義します。
0	暗号化されていないパスワードが後ろに続くことを指定します。
8	AES 暗号化パスワードが後ろに続くことを指定します。
server-key	NTP サーバーキー。ASCII キーの場合、長さが 21 バイト未満であることを確認してください。HEX キーの場合、長さは 41 未満で、0 ～ 9 の数字と a ～ f の文字のみを使用する必要があります。

コマンド デフォルト

NTP サーバー認証は設定されていません。

コマンド モード

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

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、AP プロファイルで NTP サーバー認証キー情報を設定する例を示します。

```
Device# configure terminal
Device(config)# ap profile test
Device(config-ap-profile)# ntp ip 198.51.100.5
Device(config-ap-profile)# ntp auth-key index 12 type
md5 format ascii key 0 test
```

office-extend

FlexConnect AP の OfficeExtend AP モードを有効にするには、 **office-extend** コマンドを使用します。

office-extend

コマンド デフォルト

なし

コマンド モード

config-wireless-flex-profile

コマンド履歴

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

例

次に、FlexConnect AP の OfficeExtend AP モードを有効にする例を示します。

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

okc

Opportunistic Key Caching（OKC）がまだ有効になっていない場合、有効にするには、**okc** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

okc

[no] okc

構文の説明

okc	Opportunistic Key Caching（OKC）を有効または無効にします。デフォルトでは、OKC は有効になっています。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、OKC を有効にする例を示します。

```
Device(config-wlan)# okc
```

open-roaming-oi

オープンローミング要素のエイリアスを設定するには、**open-roaming-oi** コマンドを使用します。オープンローミング要素のエイリアスを削除するには、このコマンドの **no** 形式を使用します。

open-roaming-oi *alias*

構文の説明

alias	ローミング組織識別子のエイリアス。

コマンド デフォルト

ローミング組織識別子のエイリアスは設定されていません。

コマンド モード

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

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、オープンローミング要素のエイリアスを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless hotspot anqp-server my_server
Device(config-wireless-anqp-server)# open-roaming-oi allow-all
```

operator

Hotspot 2.0 オペレータのフレンドリ名を特定の言語で設定するには、**operator** コマンドを使用します。オペレータ名を削除するには、このコマンドの **no** 形式を使用します。

operator *operator-name language-code*

構文の説明

operator-name	オペレータの名前。
language-code	オペレータの 3 文字の言語コード。言語コードには、言語の最初の 3 文字のみを小文字で使用します。たとえば、英語の場合は *eng* を使用します。 言語コードの完全なリストを確認するには、http://www.loc.gov/standards/iso639-2/php/code_list.php にアクセスしてください。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、オペレータのフレンドリ名を設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# operator XYZ-operator eng
```

operating-class

Hotspot 2.0 の動作クラス ID を設定するには、**operating-class** コマンドを使用します。動作クラスを削除するには、このコマンドの **no** 形式を使用します。

operating-class *class-id*

構文の説明

class-id	動作クラスの ID 番号。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、動作クラス識別子を設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# operating-class 25
```

option

のフロー エクスポータのオプションのデータ パラメータを設定するには、フロー エクスポータ コンフィギュレーション モードで **option** コマンドを使用します。フロー エクスポータのオプションのデータ パラメータを削除するには、このコマンドの **no** 形式を使用します。

option {**exporter-stats** | **interface-table** | **sampler-table**} [{**timeout** *seconds*}]
no option {**exporter-stats** | **interface-table** | **sampler-table**}

構文の説明

exporter-stats	フローエクスポータの統計情報オプションを設定します。
interface-table	フローエクスポータのインターフェイステーブル オプションを設定します。
sampler-table	フロー エクスポータのエクスポート サンプラー テーブル オプションを設定します。
timeout *seconds*	（任意）フローエクスポータのオプションの再送時間を秒単位で設定します。指定できる範囲は 1 ～ 86400 です。デフォルトは 600 です。

コマンド デフォルト

タイムアウトは 600 秒です。他のすべてのオプション データ パラメータは設定されていません。

コマンド モード

フロー エクスポータ コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

option exporter-stats コマンドを実行すると、レコード数、バイト数、送信されたパケット数など、エクスポータの統計情報が定期的に送信されます。このコマンドを使用して、コレクタは受信するエクスポート レコードのパケット損失を見積もります。オプションのタイムアウトでは、レポートが送信される頻度を変更できます。

option interface-table コマンドを実行すると、オプション テーブルが定期的に送信されます。このオプション テーブルを使用して、コレクタはフロー レコードに記録されている SNMP インターフェイス インデックスを各インターフェイス名にマッピングします。オプションのタイムアウトでは、レポートが送信される頻度を変更できます。

option sampler-table コマンドを実行すると、オプション テーブルが定期的に送信されます。このオプションテーブルには、各サンプラーの設定の詳細が含まれており、これを使用して、コレクタは任意のフロー レコードに記録されているサンプラー ID を、フローの統計情報のスケールアップに使用可能な設定にマッピングします。オプションのタイムアウトでは、レポートが送信される頻度を変更できます。

このコマンドをデフォルト設定に戻すには、**no option** または **default option** フロー エクスポータ コンフィギュレーション コマンドを使用します。

次の例では、サンプラー オプション テーブルの定期的な送信をイネーブルにして、コレクタでサンプラー ID をサンプラーのタイプとレートにマッピングする方法を示します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)# option sampler-table
```

次の例では、レコード数、バイト数、送信されたパケット数など、エクスポータの統計情報の定期的な送信をイネーブルする方法を示します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)# option exporter-stats
```

次の例では、オプション テーブルの定期的な送信をイネーブルにし、そのオプション テーブルをコレクタで使用して、フローレコードに記録されている SNMP インターフェイス インデックスをインターフェイス名にマッピングする方法を示します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)# option interface-table
```

osu-provider

Hotspot 2.0 のオンラインサインアップ（OSU）プロバイダーを設定するには、**osu-provider** コマンドを使用します。OSU プロバイダーを削除するには、このコマンドの **no** 形式を使用します。

osu-provider *provider-name*

構文の説明

provider-name	OSU プロバイダーの名前。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、OSU プロバイダーを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# osu-provider yyy
```

osu-ssid

オンラインサインアップ（OSU）に使用するワイヤレスクライアントのサービスセット識別子（SSID）を設定するには、**osu-ssid** コマンドを使用します。SSID を削除するには、このコマンドの **no** 形式を使用します。

osu-ssid *ssid*

構文の説明

ssid	ワイヤレスクライアントの SSID の名前。 SSID の長さは、最大 32 文字です。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、ワイヤレスクライアントが OSU 中に使用する SSID を設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# osu-ssid cisco
```

packet-capture

AP プロファイルでパケット キャプチャを有効にするには、 **packet-capture** コマンドを使用します。

packet-capture *profile-name*

コマンド デフォルト

なし

コマンド モード

config-ap-profile

コマンド履歴

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

例

次に、AP プロファイルでパケット キャプチャを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap profile demo-profile-name
Device(config-ap-profile)# packet capture demo-profile
```

parameter-map type subscriber attribute-to-service

パラメータ マップのタイプと名前を設定するには、 **parameter-map type subscriber attribute-to-service** コマンドを使用します。

parameter-map type subscriber attribute-to-service *parameter-map-name*

構文の説明

attribute-to-service	サービスの属性の名前。
parameter-map-name	パラメータ マップの名前。マップ名は33文字までに制限されています。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、パラメータ マップのタイプと名前を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type subscriber attribute-to-service parameter-map-name
```

pae

製品テレメトリ収集を有効にするには、**pae** コマンドを使用します。製品テレメトリ収集を無効にするには、このコマンドの **no** 形式を使用します。

pae

no pae

コマンド デフォルト

製品テレメトリが有効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.10.1	このコマンドが導入されました。

例

次に、製品テレメトリ収集を無効にする例を示します。

```
Device# configure terminal
Device(config)# no pae
```

parameter-map type webauth

特定のパラメータマップまたはすべてのパラメータマップの Web 認証パラメータタイプを設定するには、 **parameter-map type webauth** コマンドを使用します。

parameter-map type webauth { *parameter-map-name* | **global** }

構文の説明

parameter-map-name	パラメータ マップの名前。マップ名は99文字までに制限されています。
global	すべてのパラメータマップに設定を適用します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、*parameter-map1* という名前のパラメータマップの Web 認証パラメータタイプを設定する例を示します。

```
Device# configure terminal
Device(config)# parameter-map type webauth parameter-map1
```

password encryption aes

強力な（AES）パスワード暗号化を有効にするには、**password encryption aes** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

password encryption aes
no password encryption aes

構文の説明

password	暗号化パスワード（キー）を設定します。
encryption	システムパスワードを暗号化します。
aes	より強力な（AES）パスワード暗号化を有効にします。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.2s	このコマンドが導入されました。

例

次に、AES パスワード暗号化を有効にする例を示します。

```
Device(config)#password encryption aes
```

peer-blocking

WLANにピアツーピア ブロッキング機能を設定するには、**peer-blocking** コマンドを使用します。ピアツーピア ブロッキング機能を無効にするには、このコマンドの **no** 形式を使用します。

peer-blocking {**allow-private-group** | **drop** | **forward-upstream**}
no peer-blocking

構文の説明

allow-private-group	プライベートグループを許可するデバイスを指定します。 （注） **allow-private-group** ピアツーピアブロッキングWLAN設定は、Identity PSK（iPSK）WLAN でのみ機能します。
drop	deviceでパケットを破棄するように指定します。
forward-upstream	パケットがアップストリームVLANに転送されるように指定します。deviceの次に上の階層のデバイスが、パケットに関して実行するアクションを決定します。 （注） forward-upstream オプションは、Flex ローカルスイッチングではサポートされていません。このオプションが設定されている場合でも、トラフィックはドロップされます。また、ローカルスイッチングSSIDのピアツーピアブロッキングは、同じAP 上のクライアントに対してのみ使用できます。

コマンド デフォルト

ピア ブロッキングは無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

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

使用上のガイドライン

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

次に、ピアツーピアブロッキングの drop オプション、forward オプション、および private group オプションを有効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wlan wlan1
Device(config-wlan)# peer-blocking  allow-private-group
デバイス(config-wlan)# peer-blocking  drop
デバイス(config-wlan)# peer-blocking forward-upstream
```

次に、ピアツーピアブロッキングの drop オプション、forward オプション、および private group オプションを無効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wlan wlan1
Device(config-wlan)# no peer-blocking  allow-private-group
デバイス(config-wlan)# no peer-blocking  drop
デバイス(config-wlan)# no peer-blocking forward-upstream
```

plan

課金通知のプラン情報を設定するには、**plan** コマンドを使用します。課金通知のプラン情報を削除するには、このコマンドの **no** 形式を使用します。

plan {*language-code* | *currency-code* | **info** {**bootflash** | **flash**} *file-name*}

構文の説明

filename	bootflash:filename または flash:filename の形式の、ファイル名などのプランの詳細。
language-code	この課金通知の言語コード（ISO 639）の最初の 3 文字（小文字）。たとえば、英語の場合は *eng* です。
currency-code	この課金通知の通貨コード（ISO 4217）の最初の 3 文字。たとえば、ユーロの場合は *EUR* です。

コマンド デフォルト

プラン情報は設定されていません。

コマンド モード

ワイヤレス ANQP 課金通知コンフィギュレーション（config-anqp-advice-charge）

コマンド履歴

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

例

次に、課金通知のプラン情報を設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# advice-charge unlimited
Device(config-anqp-advice-charge)# plan eng EUR info bootflash:plan-a
```

pmk propagate

（PMK）情報をサイト内の他の AP に伝播するには、**pmk propagate** コマンドを使用します。

pmk propagate

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

config-wireless-flex-profile

コマンド履歴

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

例

次に、サイト内の他の AP に PMK 情報を伝播する例を示します。

```
Device# configure terminal
Device(config)# wireless profile flex test-flex-profile
Device(config-wireless-flex-profile)# pmk propogate
```

pmf-deauth

PMF 拒否タイプの認証解除不正 AP 封じ込めを有効にするには、**pmf-deauth** コマンドを使用します。PMF 拒否タイプの認証解除不正 AP 封じ込めを無効にするには、このコマンドの **no** 形式を使用します。

pmf-deauth

no pmf-deauth

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

PMF 拒否コンフィギュレーション（config-pmf-denial）

コマンド履歴

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

例

次に、PMF 拒否タイプの認証解除不正 AP 封じ込めを有効にする例を示します。

```
Device# configure terminal
Device(config)# ap profile xyz-ap-profile
Device(config-ap-profile)# rogue detection containment pmf-denial
Device(config-pmf-denial)# pmf-deauth
```

no platform sudi cmca3

SUDI99 移行を無効にし、古いリリースに従った証明書マッピングに戻すには、**no platform sudi cmca3** コマンドを使用します。

no platform sudi cmca3

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

SUDI99 がトラストポイントとして設定されています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

高可用性（HA）トポロジの場合は、コマンドを実行する前にHAペアを形成します。その後、設定を保存し、コントローラをリロードして SUDI 証明書を無効にします。

例

次に、SUDI99移行を無効にし、以前のリリースに従った証明書マッピングに戻す例を示します。

```
Device# configure terminal
Device(config)# no platform sudi cmca3
```

policy

メディア ストリームのアドミッション ポリシーを設定するには、**policy** コマンドを使用します。

policy {**admit** | **deny**}

構文の説明

admit	メディア ストリーム グループのトラフィックを許可します。
deny	メディア ストリーム グループのトラフィックを拒否します。

コマンド デフォルト

なし

コマンド モード

media-stream

コマンド履歴

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

例

次に、メディア ストリーム グループのトラフィックを許可する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group ms-group 224.0.0.0 224.0.0.223
Device(media-stream)# policy admit
```

police

分類したトラフィックにポリサーを定義するには、ポリシーマップ クラス コンフィギュレーション モードで **police** コマンドを使用します。既存のポリサーを削除するには、このコマンドの **no** 形式を使用します。

police *rate-bps burst-byte* [**conform-action transmit**]
no police rate-bps *burst-byte* [**conform-action transmit**]

構文の説明

rate-bps	平均トラフィック伝送速度をビット/秒（b/s）で指定します。指定できる範囲は 1000000 ～ 1000000000 です。
burst-byte	通常のバースト サイズ（バイト）を指定します。指定できる範囲は 8000 ～ 1000000 です。
conform-action transmit	（任意）速度が指定できる範囲を下回る場合は、スイッチがパケットを送信するよう指定します。

コマンド デフォルト

ポリサーは定義されません。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

ポリサーは、最大許容伝送速度、最大バースト伝送サイズ、およびいずれかの最大値を超過した場合の対処法を定義します。

階層ポリシー マップを設定する場合、セカンダリ インターフェイス レベルのポリシー マップで使用できるのは **police** ポリシーマップ コマンドだけです。

2 つ以上の物理ポートを制御するポート ASIC デバイスは、スイッチ上で 256 個のポリサー（255 個のユーザー設定可能なポリサーと 1 個の内部使用向けに予約されたポリサー）をサポートします。ポートごとにサポートされる設定可能なポリサーの最大数は 63 です。ポリサーはソフトウェアによってオンデマンドで割り振られ、ハードウェアおよび ASIC の限界によって制約されます。ポートごとにポリサーを予約することはできません。ポートがいずれかのポリサーに割り当てるという保証はありません。

ポリシーマップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

例

この例では、トラフィックの平均レートが 1 Mb/s 未満で、バースト サイズが 20 KB の場合にパケットを送信するポリサーを設定する方法を示します。パケットは変更されません。

```
デバイス(config)# class-map class1
デバイス(config-cmap)# exit
デバイス(config)# policy-map policy1
デバイス(config-pmap)# class class1
デバイス(config-pmap-c)# police 1000000 20000 conform-action transmit
デバイス(config-pmap-c)# exit
```

この例では、トラフィックの平均レートが 1 Mb/s 未満で、バースト サイズが 20 KB の場合にパケットを送信するポリサーを設定する方法を示します。パケットは変更されません。この例では、短縮構文を使用しています。

```
デバイス(config)# class-map class1
デバイス(config-cmap)# exit
デバイス(config)# policy-map policy1
デバイス(config-pmap)# class class1
デバイス(config-pmap-c)# police 1m 20000 conform-action transmit
デバイス(config-pmap-c)# exit
```

次の例では、DSCP 値をポリシング設定 DSCP マップに定義された値でマークダウンしてパケットを送信するポリサーを設定する方法を示します。

```
デバイス(config)# policy-map policy2
デバイス(config-pmap)# class class2
デバイス(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
デバイス(config-pmap-c)# exit
```

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

police cir

認定情報レートのポリシングを設定するには、**police cir** コマンドを使用します。

police cir *<target bit rate>*

構文の説明

police cir	認定情報レートをポリシングします。
8000-10000000000	ターゲットビットレートを 1 秒あたりのビット数で設定します。指定できる範囲は 8000 ～ 10000000000 です。

コマンド デフォルト

なし

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、認定情報レートを設定する例を示します。

```
Device(config-pmap-c)#police cir 8000
```

policy-tag

ポリシー タグを AP にマッピングするには、**policy-tag** コマンドを使用します。

policy-tag *policy-tag-name*

構文の説明

policy-tag-name	ポリシー タグの名前。

コマンド デフォルト

なし

コマンド モード

config-ap-tag

コマンド履歴

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

使用上のガイドライン

このコマンドを実行すると、AP は、接続解除されたのち再参加します。

例

次に、ポリシー タグを設定する例を示します。

```
Device(config-ap-tag)# policy-tag policytag1
```

policy-map

複数の物理ポートまたはスイッチ仮想インターフェイス（SVI）に適用できるポリシーマップを作成し、ポリシーマップ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **policy-map** コマンドを使用します。既存のポリシー マップを削除し、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

policy-map *policy-map-name*
no policy-map *policy-map-name*

構文の説明

policy-map-name	ポリシーマップ名です。

コマンド デフォルト

ポリシー マップは定義されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

policy-map コマンドを入力すると、ポリシー マップ クラス コンフィギュレーション モードに入り、次のコンフィギュレーション コマンドが使用可能になります。

- **class**：指定したクラス マップの分類一致基準を定義します。
- **description**：ポリシー マップを説明します（最大 200 文字）。
- **exit**：ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
- **no**：定義済みポリシー マップを削除します。
- **sequence-interval**：シーケンス番号機能をイネーブルにします。

グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

一致基準がクラス マップに定義されているクラスのポリシーを設定する前に、**policy-map** コマンドを使用して作成、追加または変更するポリシーマップの名前を指定します。**policy-map** コマンドを入力した場合も、ポリシーマップ コンフィギュレーション モードがイネーブルになり、このモードでポリシーマップのクラスポリシーを設定または変更することができます。

クラス ポリシーをポリシー マップ内で設定できるのは、クラスに一致基準が定義されている場合だけです。クラスの一致基準を設定するには、**class-map** グローバル コンフィギュレーション コマンドおよび **match** クラスマップ コンフィギュレーション コマンドを使用します。物理ポート単位でパケット分類を定義します。

入力ポートごとに 1 つのポリシー マップのみがサポートされます。同じポリシー マップを複数の物理ポート に適用できます。

物理ポートに非階層ポリシーマップを適用できます。非階層ポリシーマップは、deviceのポート ベース ポリシー マップと同じです。

階層ポリシーマップには親子ポリシーの形式で2つのレベルがあります。親ポリシーは変更できませんが、子ポリシー（port-child ポリシー）は、QoS 設定に合わせて変更できます。

VLAN ベースの QoS では、サービス ポリシーが SVI インターフェイスに適用されます。

（注） すべての MQS QoS の組み合わせが有線ポートでサポートされているわけではありません。これらの制約事項については、QoS コンフィギュレーション ガイドの「Restrictions for QoS on Wired Targets」の章を参照してください。

例

次の例では、policy1 という名前のポリシー マップを作成する方法を示します。入力ポートに適用した場合、class1 で定義されたすべての着信トラフィックの照合を行い、IP DSCP を 10 に設定し、平均伝送速度 1 Mb/s、バースト 20 KB のトラフィックをポリシングします。プロファイル未満のトラフィックが送信されます。

```
デバイス(config)# policy-map policy1
デバイス(config-pmap)# class class1
デバイス(config-pmap-c)# set dscp 10
デバイス(config-pmap-c)# police 1000000 20000 conform-action transmit
デバイス(config-pmap-c)# exit
```

次に、階層ポリシーを設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# class-map c1
デバイス(config-cmap)# exit

デバイス(config)# class-map c2
デバイス(config-cmap)# exit

デバイス(config)# policy-map child
デバイス(config-pmap)# class c1
デバイス(config-pmap-c)# priority level 1
デバイス(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop

デバイス(config-pmap-c-police)# exit
デバイス(config-pmap-c)# exit

デバイス(config-pmap)# class c2
デバイス(config-pmap-c)# bandwidth 20000
デバイス(config-pmap-c)# exit

デバイス(config-pmap)# class class-default
デバイス(config-pmap-c)# bandwidth 20000
デバイス(config-pmap-c)# exit
```

```
デバイス(config-pmap)# exit

デバイス(config)# policy-map parent
デバイス(config-pmap)# class class-default
デバイス(config-pmap-c)# shape average 1000000
デバイス(config-pmap-c)# service-policy child
デバイスconfig-pmap-c)# end
```

次に、ポリシー マップを削除する例を示します。

```
デバイス(config)# no policy-map policymap2
```

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

policy-map

複数の物理ポートまたはスイッチ仮想インターフェイス（SVI）に適用できるポリシーマップを作成し、ポリシーマップ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **policy-map** コマンドを使用します。既存のポリシー マップを削除し、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

policy-map *policy-map-name*
no policy-map *policy-map-name*

構文の説明

policy-map-name	ポリシーマップ名です。

コマンド デフォルト

ポリシー マップは定義されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

policy-map コマンドを入力すると、ポリシー マップ クラス コンフィギュレーション モードに入り、次のコンフィギュレーション コマンドが使用可能になります。

- **class**：指定したクラス マップの分類一致基準を定義します。
- **description**：ポリシー マップを説明します（最大 200 文字）。
- **exit**：ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
- **no**：定義済みポリシー マップを削除します。
- **sequence-interval**：シーケンス番号機能をイネーブルにします。

グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

一致基準がクラス マップに定義されているクラスのポリシーを設定する前に、**policy-map** コマンドを使用して作成、追加または変更するポリシーマップの名前を指定します。**policy-map** コマンドを入力した場合も、ポリシーマップ コンフィギュレーション モードがイネーブルになり、このモードでポリシーマップのクラスポリシーを設定または変更することができます。

クラス ポリシーをポリシー マップ内で設定できるのは、クラスに一致基準が定義されている場合だけです。クラスの一致基準を設定するには、**class-map** グローバル コンフィギュレーション コマンドおよび **match** クラスマップ コンフィギュレーション コマンドを使用します。物理ポート単位でパケット分類を定義します。

入力ポートごとに 1 つのポリシー マップのみがサポートされます。同じポリシー マップを複数の物理ポート に適用できます。

物理ポートに非階層ポリシーマップを適用できます。非階層ポリシーマップは、deviceのポート ベース ポリシー マップと同じです。

階層ポリシーマップには親子ポリシーの形式で2つのレベルがあります。親ポリシーは変更できませんが、子ポリシー（port-child ポリシー）は、QoS 設定に合わせて変更できます。

VLAN ベースの QoS では、サービス ポリシーが SVI インターフェイスに適用されます。

（注） すべての MQS QoS の組み合わせが有線ポートでサポートされているわけではありません。これらの制約事項については、QoS コンフィギュレーション ガイドの「Restrictions for QoS on Wired Targets」の章を参照してください。

例

次の例では、policy1 という名前のポリシー マップを作成する方法を示します。入力ポートに適用した場合、class1 で定義されたすべての着信トラフィックの照合を行い、IP DSCP を 10 に設定し、平均伝送速度 1 Mb/s、バースト 20 KB のトラフィックをポリシングします。プロファイル未満のトラフィックが送信されます。

```
デバイス(config)# policy-map policy1
デバイス(config-pmap)# class class1
デバイス(config-pmap-c)# set dscp 10
デバイス(config-pmap-c)# police 1000000 20000 conform-action transmit
デバイス(config-pmap-c)# exit
```

次に、階層ポリシーを設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# class-map c1
デバイス(config-cmap)# exit

デバイス(config)# class-map c2
デバイス(config-cmap)# exit

デバイス(config)# policy-map child
デバイス(config-pmap)# class c1
デバイス(config-pmap-c)# priority level 1
デバイス(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop

デバイス(config-pmap-c-police)# exit
デバイス(config-pmap-c)# exit

デバイス(config-pmap)# class c2
デバイス(config-pmap-c)# bandwidth 20000
デバイス(config-pmap-c)# exit

デバイス(config-pmap)# class class-default
デバイス(config-pmap-c)# bandwidth 20000
デバイス(config-pmap-c)# exit
```

```
デバイス(config-pmap)# exit

デバイス(config)# policy-map parent
デバイス(config-pmap)# class class-default
デバイス(config-pmap-c)# shape average 1000000
デバイス(config-pmap-c)# service-policy child
デバイスconfig-pmap-c)# end
```

次に、ポリシー マップを削除する例を示します。

```
デバイス(config)# no policy-map policymap2
```

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

port

カスタム アプリケーションを設定する際に使用するポート番号を設定するには、 **port** コマンドを使用します。

port *port-no*

構文の説明

port-no	ポート番号。

コマンド デフォルト

なし

コマンド モード

config-custom

コマンド履歴

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

例

次に、カスタム アプリケーションを設定する際に使用するポート番号を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip nbar custom custom-protocol http host host-string
Device(config-custom)# http host hostname
Device(config-custom)# port port-no
```

power-save-client-threshold

省電力用のクライアントしきい値を設定するには、**power-save-client-threshold** *client-threshold* コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

power-save-client-threshold *client-threshold*

no power-save-client-threshold *client-threshold*

構文の説明

client-threshold	省電力用のクライアントしきい値を指定します。値の範囲は 1 ～ 32 クライアントです。デフォルト値は 1 です。

コマンド デフォルト

デフォルト値は 1 です。

コマンド モード

ワイヤレス電力プロファイルモード

コマンド履歴

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

例

次に、省電力用のクライアントしきい値を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile power power-profile1
Device(Config-wireless-power-profile)#power-save-client-threshold 5
```

priority priority-value

メディア ストリームのプライオリティを設定するには、**priority** *priority-value* コマンドを使用します。

priority *priority-value*

構文の説明

priority-value	メディア ストリームのプライオリティ値。有効な範囲は 1 ～ 8 です。1 が最も低いプライオリティで、8 が最も高いプライオリティです。

コマンド デフォルト

なし

コマンド モード

config-media-stream

コマンド履歴

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

例

次に、メディア ストリームのプライオリティ値を最大（8）に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# priority 8
```

priority-queue

ポート上で出力緊急キューをイネーブルにするには、インターフェイス コンフィギュレーション モードで **priority-queue** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

priority-queue out
no priority-queue out

構文の説明

out	出力緊急キューをイネーブルにします。

コマンド デフォルト

出力緊急キューは、ディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

priority-queue out コマンドを設定する場合、シェイプド ラウンド ロビン（SRR）に参加するキューが 1 つ少ないため、SRR の重み比が影響を受けます。これは、**srr-queue bandwidth shape** または **srr-queue bandwidth shape** インターフェイス コンフィギュレーション コマンド内の *weight1* が無視される（比率計算に使用されない）ことを意味します。緊急キューはプライオリティ キューであり、他のキューのサービスが提供される前に空になるまでサービスを提供します。

緊急キューがイネーブルにされているとき、または SRR の重みに基づいて出力キューのサービスが提供されるときには、次の注意事項に従ってください。

- 出力緊急キューがイネーブルにされている場合は、キュー 1 に対して SRR のシェーピングおよび共有された重みが無効にされます。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングおよび共有された重みが設定されている場合は、キュー 1 に対して shaped モードは shared モードを無効にし、SRR はこのキューに shaped モードでサービスを提供します。
- 出力緊急キューがディセーブルにされており、SRR のシェーピングされた重みが設定されていない場合は、SRR はキューに対して shared モードでサービスを提供します。

例

次の例では、SRR の重みが設定されている場合、出力緊急キューをイネーブルにする方法を示します。出力緊急キューは、設定された SRR ウェイトを上書きします。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# srr-queue bandwidth shape 25 0 0 0
デバイス(config-if)# srr-queue bandwidth share 30 20 25 25
```

```
デバイス(config-if)# priority-queue out
```

次の例では、SRR のシェーピングおよび共有された重みが設定された後、出力緊急キューをディセーブルにする方法を示します。シェーピング モードは、共有モードを無効にします。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# srr-queue bandwidth shape 25 0 0 0
デバイス(config-if)# srr-queue bandwidth share 30 20 25 25
デバイス(config-if)# no priority-queue out
```

設定を確認するには、**show mls qos interface** *interface-id* **queueing** または **show running-config** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show mls qos interface queueing	キューイング方法（SRR、プライオリティ キューイング）、キューに相応する重み、および Class of Service（CoS）から出力キューへのマップを表示します。
srr-queue bandwidth shape	シェーピングされた重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅シェーピングをイネーブルにします。
srr-queue bandwidth share	共有する重みを割り当て、ポートにマッピングされた 4 つの出力キュー上で帯域幅の共有をイネーブルにします。

priority

ポリシーマップに属するトラフィックのクラスにプライオリティを割り当てるには、ポリシーマップ クラス コンフィギュレーション モードで **priority** コマンドを使用します。クラスに指定したプライオリティを削除するには、このコマンドの **no** 形式を使用します。

priority ［*Kbps* ［*burst -in-bytes*］ | **level** *level-value* ［*Kbps* ［*burst -in-bytes*］］ | **percent** *percentage* ［*Kb/s* ［*burst -in-bytes*］］］
no priority ［*Kb/s* ［*burst -in-bytes*］ | **level** *level value* ［*Kb/s* ［*burst -in-bytes*］］ | **percent** *percentage* ［*Kb/s* ［*burst -in-bytes*］］］

構文の説明

コマンド デフォルト

プライオリティは設定されません。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

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

使用上のガイドライン

priority コマンドを使用すると、（User Datagram Ports（UDP）ポートだけではなく）さまざまな基準に基づいてクラスと設定し、プライオリティを割り当てることができます。これは、シリアル インターフェイスと相手先固定接続（PVC）で使用できます。類似の **ip rtp priority** コマンドを使用すると、UDP ポート番号にだけ基づいてプライオリティ フローを決定することができ、PVC には使用できません。

同じポリシーマップ内では、bandwidth コマンドおよびpriority コマンドは、同じクラスに使用できません。ただし、これらのコマンドは、同じポリシーマップ内では一緒に使用できます。

ポリシーマップで、1つまたは複数のクラスにプライオリティ ステータスを指定できます。単一ポリシー マップ内の複数のクラスがプライオリティ クラスとして設定されると、これらのクラスからのすべてのトラフィックが、同じ単一のプライオリティ キューにキューイングされます。

クラス ポリシー設定が含まれているポリシー マップがインターフェイスに付加されて、そのインターフェイスのサービス ポリシーが決定される場合、使用可能な帯域幅が評価されます。インターフェイスの帯域幅が不十分なことが原因で、特定のインターフェイスにポリシーマップがアタッチできない場合、そのポリシーは、正常にアタッチされていたすべてのインターフェイスから削除されます。

例

次に、ポリシー マップ policy1 のクラスのプライオリティを設定する例を示します。

```
デバイス(config)# class-map cm1
デバイス(config-cmap)#match precedence 2
デバイス(config-cmap)#exit
```

```
デバイス(config)#class-map cm2
デバイス(config-cmap)#match dscp 30
デバイス(config-cmap)#exit

デバイス(config)# policy-map policy1
デバイス(config-pmap)# class cm1
デバイス(config-pmap-c)# priority level 1
デバイス(config-pmap-c)# police 1m
デバイス(config-pmap-c-police)#exit
デバイス(config-pmap-c)#exit
デバイス(config-pmap)#exit

デバイス(config)#policy-map policy1
デバイス(config-pmap)#class cm2
デバイス(config-pmap-c)#priority level 2
デバイス(config-pmap-c)#police 1m
```

profile（プライムフィルタ）

アクセスポイント（AP）フィルタのプライミングプロファイルを適用するには、**profile** コマンドを使用します。プロファイルを無効にするには、このコマンドの **no** 形式を使用します。

profile *profile-name*

no profile *profile-name*

構文の説明

profile-name	APプライミングプロファイル名。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

AP プライム フィルタ コンフィギュレーション（config-ap-pr-filter）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.2	このコマンドが導入されました。

例

次に、プライミングプロファイルを適用する例を示します。

```
Device# configure terminal
Device(config)# ap filter name test-filter type priming
Device(config-ap-pr-filter)# profile Prime-FX
```

protocol（IPv6 スヌーピング）

アドレスを Dynamic Host Configuration Protocol（DHCP）または Neighbor Discovery Protocol（NDP）で収集する必要があることを指定するか、プロトコルを IPv6 プレフィックス リストに対応させるには、**protocol** コマンドを使用します。DHCP または NDP によるアドレス収集をディセーブルにするには、このコマンドの **no** 形式を使用します。

protocol {**dhcp** | **ndp**}
no protocol {**dhcp** | **ndp**}

構文の説明

dhcp	アドレスをダイナミック ホスト コンフィギュレーション プロトコル（DHCP）パケットで収集する必要があることを指定します。
ndp	アドレスをネイバー探索プロトコル（NDP）パケットで収集する必要があることを指定します。

コマンド デフォルト

スヌーピングとリカバリは DHCP および NDP の両方を使用して試行します。

コマンド モード

IPv6 スヌーピング コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

アドレスが DHCP または NDP に関連付けられたプレフィックス リストと一致しない場合は、制御パケットがドロップされ、バインディング テーブル エントリのリカバリはそのプロトコルに対しては試行されません。

- **no protocol** {**dhcp** | **ndp**} コマンドを使用すると、プロトコルはスヌーピングまたはグリーニングに使用されません。
- **no protocol dhcp** コマンドを使用すると、DHCP は依然としてバインディング テーブルのリカバリに使用できます。
- データ収集は DHCP および NDP でリカバリできますが、宛先ガードは DHCP によってのみリカバリできます。

次に、IPv6 スヌーピングポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、アドレスの収集に DHCP を使用するようにポートを設定する例を示します。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)# protocol dhcp
```

primary (ap prime)

アクセスポイント（AP）フォールバック用のプライマリコントローラを設定するには、**primary** コマンドを使用します。AP プライミングに使用されないようにプライマリコントローラを削除するには、このコマンドの **no** 形式を使用します。

primary *controller-name ip-address*

no primary *controller-name ip-address*

構文の説明

controller-name	プライマリ コントローラの名前。
ip-address	コントローラの IPv4 または IPv6 アドレス。

コマンド デフォルト

なし

コマンド モード

AP プライム コンフィギュレーション（config-priming）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.2	このコマンドが導入されました。

例

次に、AP フォールバック用のプライマリコントローラを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile ap priming Prime-FX
Device(config-priming)# primary aaaa 209.165.201.2
```

priming-override

既存のアクセスポイント（AP）のプライミング設定をオーバーライドするには、**priming-override** コマンドを使用します。プライミングのオーバーライドを無効にするには、このコマンドの **no** 形式を使用します。

priming-override

no priming-override

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

プライミングのオーバーライドは無効になっています。

コマンド モード

AP プライム コンフィギュレーション（config-priming）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.2	このコマンドが導入されました。

使用上のガイドライン

- プライミングのオーバーライドが無効になっている場合、AP プライミングプロファイルに保存されている情報は AP に送信されません。
- プライミングのオーバーライドが有効になっている場合、N+1 アップグレードが正しく機能しないことがあります。N+1 アップグレードを使用する前に、**no priming-override** コマンドを使用して、プライミングのオーバーライドが無効になっていることを確認してください。

例

次に、既存の AP プライミング設定をオーバーライドする例を示します。

```
Device# configure terminal
Device(config)# wireless profile ap priming Prime-FX
Device(config-priming)# priming-override
```

public-ip

コントローラの NAT パブリック IP アドレスを設定するには、**public-ip** コマンドを使用します。

public-ip { *ipv4-address* | *ipv6-address* }

構文の説明

ipv4-address	IPv4アドレスを設定します。
ipv6-address	IPv6アドレスを設定します。

コマンド デフォルト

なし

コマンド モード

管理インターフェイス コンフィギュレーション（config-mgmt-interface）

コマンド履歴

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

使用上のガイドライン

例

次に、コントローラの NAT パブリック IP アドレスを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless management interface Vlan1
Device(config-mgmt-interface)# public-ip 192.168.172.100
```

qbss-load

QoS Enhanced Basic Service Set（QBSS）IE を有効にするには、**qbss-load** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

qbss-load

[no] qbss-load

構文の説明

qbss-load	QoS Enhanced Basis Service Set（QBSS）IE を有効にします。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ポリシー コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、QBSS ロードを設定する例を示します。

```
Device(config-wireless-policy)#qbss-load
```

qos-map

Quality of Service（QoS）マップを設定するには、**qos-map** コマンドを AP プロファイル コンフィギュレーション モードで使用します。

設定を無効にするには、このコマンドの **no** 形式を使用します。

qos-map { **action-frame** | **dscp-to-up-exception** *dscp-value user-priority* | **dscp-to-up-range** *user-priority dscp-value lower-dscp-range upper-dscp-range* | **trust-dscp-upstream** }

構文の説明

action-frame	QoS マップ設定が変更された場合に、802.11 QoS マップアクションフレームを送信します。
dscp-to-up-exception	DSCPからユーザープライオリティのマッピングの例外を指定します。
dscp-to-up-range	DSCP からユーザープライオリティのマッピングを指定します。 すべてのカスタム マッピングを削除するには、**no dscp-to-up-range** コマンドを使用します。
dscp-value	ユーザープライオリティから DSCP アップストリーム。有効な範囲は 0 ～ 63 です。
user-priority	ユーザー プライオリティ。有効な範囲は 1 ～ 7 です。
lower-dscp-range	DSCP 範囲の下限。有効な範囲は 0 ～ 63 です。
upper-dscp-range	DSCP 範囲の上限。有効な範囲は 0 ～ 63 です。
trust-dscp-upstream	ユーザープライオリティではなくアップストリーム DSCP を信頼するようにアクセスポイント（AP）に指示します。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

使用上のガイドライン

IP ネットワークを使用するインターネットワーキングの場合、マッピングは、802.11eユーザープライオリティと IP DSCP の間で作成されます。

マッピングは、個々の UP 値に対する DSCP 範囲として、また、DSCP 値と UP 値の間の 1 対 1 のマッピングを持つ例外のセットとして指定されます。QoS マップが有効になっていて、ユーザ設定が可能なマッピングが追加されていない場合は、デフォルト値が使用されます。

user-priority 値ごとに 1 つずつ、最大 8 つの設定エントリを *user-priority* に設定できます。カスタム値を設定しない場合は、未設定の値（0xFF）が対応する AP とワイヤレスクライアントに送信されます。

dscp-to-up-exception には、最大 21 のエントリを設定できます。

次の表に、対応する AP がワイヤレスクライアントに対し、IP DSCP から 802.11e ユーザープライオリティへの必要なマッピングを提供する QoS マップを示します。

表 *2：*デフォルトの *DSCP* 範囲から *UP* へのマッピング

IP DSCP 範囲	802.11e ユーザー プライオリティ
0 ～ 7	0
8 ～ 15	1
16 ～ 23	2
24 ～ 31	3
32 ～ 39	4
40 ～ 47	5
48 ～ 55	6
56 ～ 63	7

次の表に、DSCP 値とユーザープライオリティ値間の 1 対 1 マッピングを使用した例外のセットを示します。

表 *3：*デフォルトの *DSCP* 範囲から *UP* へのマッピングの例外

IP DSCP	802.11e ユーザー プライオリティ
0	0
2	1
4	1
6	1
10	2
12	2
14	2
18	3
20	3

IP DSCP	802.11e ユーザー プライオリティ
22	3
26	4
34	5
46	6
48	7
56	7

例

次に、QoS マップを設定する例を示します。

```
Device(config)# ap profile hotspot
Device(config-ap-profile)# qos-map dscp-to-up-range 6 52 23 62
```

qos queue-softmax-multiplier

softmax バッファの値を増やすには、グローバル コンフィギュレーション モードで **qos queue-softmax-multiplier** コマンドを使用します。

qos queue-softmax-multiplier *range-of-multiplier*
no qos queue-softmax-multiplier *range-of-multiplier*

構文の説明

range-of-multiplier	値は、100 ～ 1200 の範囲で指定できます。デフォルト値は 100 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
	このコマンドが導入されました。

使用上のガイドライン

（注） このコマンドは、ポリシーマップが対応付けられているポートでのみ有効です。1200 で設定されている場合、非プライオリティ キューおよび非プライマリ プライオリティ キュー（!=level 1）の softmax は、それぞれのデフォルト値に 12 を乗じた値になります。このコマンドは、プライオリティ キュー レベル 1 には適用されません。

qos video

無線 QoS クラスをビデオ専用に設定するには、**qos video** コマンドを使用します。

qos video

コマンド デフォルト

なし

コマンド モード

config-media-stream

コマンド履歴

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

例

次に、無線 QoS クラスをビデオ専用に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# qos video
```

qos wireless-default untrust

信頼できないワイヤレス パケットに対するデフォルトの信頼動作を設定するには、**qos wireless-default untrust** コマンドを使用します。ワイヤレス トラフィックのデフォルトの信頼動作を信頼するように設定するには、このコマンドの **no** 形式を使用します。

qos wireless-default-untrust
no qos wireless-default-untrust

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

device で信頼動作を確認するには、**show running-config | sec qos** または **show run | include untrust** コマンドを使用します。

コマンド モード

コンフィギュレーション

コマンド履歴

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

次に、信頼されているワイヤレス トラフィックのデフォルトの動作を untrusted に変更するコマンドを示します。

```
デバイス(config)# qos wireless-default-untrust
```

queue-buffers ratio

クラスのキュー バッファを設定するには、ポリシーマップ クラス コンフィギュレーション モードで **queue-buffers ratio** コマンドを使用します。比率制限を削除するには、このコマンドの **no** 形式を使用します。

queue-buffers ratio *ratio limit*
no queue-buffers ratio *ratio limit*

構文の説明

ratio limit	（任意）クラスのキュー バッファを設定します。キュー バッファの比率制限（0 ～ 100）を入力します。

コマンド デフォルト

クラスのキュー バッファは定義されていません。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

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

使用上のガイドライン

このコマンドを使用する前に、**bandwidth**、**shape** または **priority** コマンドのいずれかを使用する必要があります。これらのコマンドの詳細については、Cisco.com で入手可能な *Cisco IOS Quality of Service* ソリューションのコマンド リファレンスを参照してください。

を使用すると、キューにバッファを割り当てることができます。バッファが割り当てられていない場合、すべてのキューの間で均等に分割されます。queue-buffer ratio を使用して、特定の比率で分割できます。デフォルトでは、ダイナミックしきい値およびスケーリング（DTS）がすべてのキューでアクティブであるため、バッファはソフト バッファです。

例

次にキュー バッファの比率を 10% に設定する例を示します。

```
デバイス(config)# policy-map policy_queuebuf01
デバイス(config-pmap)# class-map class_queuebuf01
デバイス(config-cmap)# exit
デバイス(config)# policy policy_queuebuf01
デバイス(config-pmap)# class class_queuebuf01
デバイス(config-pmap-c)# bandwidth percent 80
デバイス(config-pmap-c)# queue-buffers ratio 10
デバイス(config-pmap)# end
```

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

queue-limit

キューが保持できる、ポリシーマップ内に設定されたクラスポリシーのパケットの最大数を指定または変更するには、**queue-limit** ポリシーマップ クラス コンフィギュレーション コマンドを使用します。クラスからキュー パケット制限を削除するには、このコマンドの **no** 形式を使用します。

queue-limit *queue-limit-size*[{**packets**}] {**cos** *cos-value* | **dscp** *dscp-value*} **percent** *percentage-of-packets*
no queue-limit *queue-limit-size* [{**packets**}] {**cos** *cos-value* | **dscp** *dscp-value*} **percent** *percentage-of-packets*

構文の説明

queue-limit-size	キューの最大サイズ。最大値は、オプションの指定される測定単位用キーワード（bytes、ms、または packets）の単位によって異なります。
cos *cos-value*	各 cos 値のパラメータを指定します。CoS 値の範囲は 0 ～ 7 です。
dscp *dscp-value*	各 DSCP 値のパラメータを指定します。 キュー制限のタイプに合わせて DiffServ コードポイント値を指定します。範囲は 0 ～63 です。
percent *percentage-of-packets*	このクラスのキューが蓄積できるパケットの最大割合を指定します。範囲は 1 ～ 100 です。

コマンド デフォルト

なし

コマンド モード

ポリシー マップ クラス コンフィギュレーション（policy-map-c）

コマンド履歴

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

使用上のガイドライン

packets 測定単位は、コマンドラインのヘルプ文字列には表示されますが、サポートされていません。**percent** 測定単位を使用してください。

（注） このコマンドは、出力方向の有線ポートでのみサポートされています。

Weighted Fair Queueing（WFQ）により、クラス マップが定義される各クラスのキューが作成されます。クラスの一致条件を満たすパケットは、送信されるまで、このクラス専用のキューに蓄積されます。この処理は、均等化キューイング プロセスによってキューが処理される場合

に発生します。クラスに対して定義した最大パケットしきい値に到達した場合、クラスのキューにさらにパケットがキューイングされると、テール ドロップが発生します。

重み付けテール ドロップ（WTD）を設定するためにキュー制限を使用します。WTDを使用すると、キューごとに複数のしきい値を設定できます。各サービス クラスが異なるしきい値でドロップされて QoS 差別化が実現されます。

トラフィックの異なるサブクラス、つまり、DSCP と CoS に最大キューしきい値を設定し、各サブクラスに最大キューしきい値を設定できます。

例

次の例では、dscp-1 というクラスのポリシーを含めるために port-queue というポリシーマップを設定しています。このクラスのポリシーは、確保されているキューの最大パケット制限が 20% になるように設定されています。

```
デバイス(config)# policy-map policy11
デバイス(config-pmap)# class dscp-1
デバイス(config-pmap-c)# bandwidth percent 20
デバイス(config-pmap-c)# queue-limit dscp 1 percent 20
```

queue-set

キューセットにポートをマッピングするには、インターフェイス コンフィギュレーション モードで **queue-set** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

queue-set *qset-id*
no queue-set *qset-id*

構文の説明

qset-id	キューセット ID。各ポートはキューセットに属し、ポート単位で出力キュー 4 つの特性すべてを定義します。指定できる範囲は 1 ～ 2 です。

コマンド デフォルト

キューセット ID は 1 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

例

次の例では、ポートをキューセット 2 にマッピングする方法を示します。

```
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# queue-set 2
```

設定を確認するには、**show mls qos interface** [*interface-id*] **buffers** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
mls qos queue-set output buffers	バッファをキューセットに割り当てます。
mls qos queue-set output threshold	Weighted Tail-Drop（WTD）しきい値を設定し、バッファのアベイラビリティを保証し、キュー セットに対する最大メモリ割り当てを設定します。

radio policy dot11 5ghz slot

特定の 5 GHz スロットでの WLAN 無線ポリシーを設定するには、**radio policy dot11 5ghz slot** コマンドを使用します。

radio policy dot11 5ghz slot *slot_ID*

構文の説明

0	無線スロット 0 を使用した 5 GHz 無線での WLAN を設定します。
1	無線スロット 1 を使用した 5 GHz 無線での WLAN を設定します。
2	無線スロット 2（存在する場合）を使用した 5 GHz 無線での WLAN を設定します。 （注）　指定した 5 GHz 無線スロットでのみ WLAN を設定できます。

コマンド デフォルト

無線ポリシーは、すべての帯域で有効になっています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

使用上のガイドライン

WLAN をブロードキャストする特定の無線とスロットを選択できます。このオプションは、5 GHz 無線でのみ使用できます。

例

次に、特定の WLAN スロットでの無線ポリシーを設定する例を示します。

```
Device# configure terminal
Device(config)#wlan test4
Device(config-wlan)# radio policy dot11 5ghz
Device(config-wlan-radio-5ghz)# slot 1
Device(config-wlan)# end
```

radio spatial-stream

2.4 GHz、5 GHz、6 GHz、およびセカンダリ 5 GHz 無線の空間ストリームを設定するには、**radio spatial-stream** コマンドを使用します。

sequence-number **radio** { **24ghz** | **5ghz** | **6ghz** | **secondary-5ghz** } **spatial-stream** { **1** | **2** | **3** | **4** | **8** }

構文の説明

sequence-number	電力プロファイルの設定は、シーケンス番号順に並べられています。APのディレーティングは、入力されたシーケンス番号に従って行われます。インターフェイス識別子とパラメータ値の同じ組み合わせは、別のシーケンス番号には表示されません。同じパラメータを持つ同じインターフェイスが、異なるパラメータ値で複数回表示されることがあります。
24ghz	2.4 GHz 無線を設定します。
5ghz	5 GHz 無線を設定します。
6ghz	6 GHz 無線を設定します。
secondary-5ghz	セカンダリ 5 GHz 無線を設定します。
{ **1** | **2** |**3** | **4** | **8**}	• **1**：1X1 無線空間ストリームを指定します。 • **2**：2X2 無線空間ストリームを指定します。 • **3**：3X3 無線空間ストリームを指定します。 • **4**：4X4 無線空間ストリームを指定します。 • **8**：8X8 無線空間ストリームを指定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス電力プロファイル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.10.1	このコマンドが導入されました。

例

次に、ワイヤレス電力プロファイル コンフィギュレーション モードで無線空間ストリームを設定する例を示します。

```
Device(config)# wireless profile power power-profile-name
Device(config-wireless-power-profile)# 20 radio radio 5ghz spatial-stream 4
```

radius server

RADIUS サーバを設定するには、グローバル コンフィギュレーション モードで **radius server** コマンドを使用します。

radius server *server-name*

構文の説明

server-name	RADIUS サーバー名。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし

次に、RADIUS サーバーを設定する例を示します。

```
デバイス(config)# radius server ISE
```

radius-server deadtime

一部のサーバーが使用できない場合に RADIUS の応答時間を短縮するには、**radius-server deadtime** コマンドを使用して、使用できないサーバーをただちにスキップします。デッドタイムをデフォルト値の 0 に設定するには、このコマンドの **no** 形式を使用します。

radius-server deadtime *time-in-minutes*

no radius-server deadtime

構文の説明

time-in-minutes	RADIUS サーバーがトランザクション要求によってスキップされる時間を最長 1440 分（24 時間）まで分単位で表したものです。

コマンド デフォルト

デッド タイムは 0 に設定されます。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

このコマンドを使用して、認証要求に応答しない RADIUS サーバーを "dead" としてマークします。これにより、設定されている次のサーバーを試行する前に要求の待機がタイムアウトにならないようにします。"dead" としてマークされた RADIUS サーバーは、この期間（分単位）、その他の要求でスキップされます。ただし、"dead" としてマークされていないサーバーが他にない場合を除きます。

例

次に、認証要求への応答に失敗した RADIUS サーバーのデッドタイムを設定する例を示します。

```
Device(config)# radius-server deadtime 5
```

radius-server attribute wireless accounting call-station-id

RADIUS アカウンティングメッセージで送信される発信側ステーション識別子を設定するには、**radius-server attribute wireless accounting call-station-id** コマンドを使用します。RADIUS アカウンティングメッセージから発信側ステーション識別子を削除するには、このコマンドの **no** 形式を使用します。

radius-server attribute wireless authentication call-station-id { **ap-ethmac-only** | **ap-ethmac-ssid** | **ap-ethmac-ssid-flexprofilename** | **ap-ethmac-ssid-policytagname** | **ap-ethmac-ssid-sitetagname** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-macaddress** | **ap-macaddress-ssid** | **ap-macaddress-ssid-flexprofilename** | **ap-macaddress-ssid-policytagname** | **ap-macaddress-ssid-sitetagname** | **ap-name** | **ap-name-ssid** | **flex-profile-name** | **ipaddress** | **macaddress** | **policy-tag-name** | **site-tag-name** | **vlan-id** }

構文の説明

ap-ethmac-only	発信側ステーション識別子タイプを、AP の無線 MAC アドレスに設定します。
ap-ethmac-ssid	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスに設定します。
ap-ethmac-ssid-flexprofilename	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスと Flex プロファイル名に設定します。
ap-ethmac-ssid-policytagname	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスとポリシータグ名に設定します。
ap-ethmac-ssid-sitetagname	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスとサイトタグ名に設定します。
ap-group-name	AP グループ名を使用するように発信側ステーション識別子タイプを設定します。
ap-label-address	発信側ステーション識別子タイプを、AP ラベルに印刷されている AP の無線 MAC アドレスに設定します。
ap-label-address-ssid	発信側ステーション識別子タイプを、AP ラベルに印刷されている AP の無線 MAC アドレスおよび SSID に設定します。
ap-location	発信側ステーション識別子タイプを、AP の場所に設定します。
ap-macaddress	発信側ステーション識別子タイプを、AP の無線 MAC アドレスに設定します。
ap-macaddress-ssid	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスに設定します。

ap-macaddress-ssid-flexprofilename	発信側ステーション識別子タイプを、APのSSIDを持つ無線 MAC アドレスと Flex プロファイル名に設定します。
ap-macaddress-ssid-policytagname	発信側ステーション識別子タイプを、APのSSIDを持つ無線 MAC アドレスとポリシータグ名に設定します。
ap-macaddress-ssid-sitetagname	発信側ステーション識別子タイプを、APのSSIDを持つ無線 MAC アドレスとサイトタグ名に設定します。
ap-name	発信側ステーション識別子タイプを、AP名に設定します。
ap-name-ssid	発信側ステーション識別子タイプを、SSIDを持つAP名に設定します。
flex-profile-name	発信側ステーション識別子タイプを、Flexプロファイル名に設定します。
ipaddress	発信側ステーション識別子タイプを、システムの IP アドレスに設定します。
macaddress	発信側ステーション識別子タイプを、システムの MAC アドレスに設定します。
policy-tag-name	発信側ステーション識別子タイプを、ポリシータグ名に設定します。
site-tag-name	発信側ステーション識別子タイプを、サイトタグ名に設定します。
vlan-id	発信側ステーション識別子タイプを、システムの VLAN ID に設定します。

コマンド デフォルト

発信側ステーション識別子は設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。
Cisco IOS XE Bengaluru 17.4.1	このコマンドが変更されました。**policy-tag-name**、**flex-profile-name**、**ap-macaddress-ssid-flexprofilename**、**ap-macaddress-ssid-policytagname**、**ap-macaddress-ssid-sitetagname**、**ap-ethmac-ssid-flexprofilename**、**ap-ethmac-ssid-policytagname**、および**ap-ethmac-ssid-sitetagname**キーワードが導入されました。

使用上のガイドライン

例

次に、RADIUS アカウンティングメッセージで送信される発信側ステーション識別子を設定する例を示します。

```
Device(config)# radius-server attribute wireless accounting call-station-id site-tag-name
```

radius-server attribute wireless authentication call-station-id

RADIUS認証メッセージで送信される発信側ステーション識別子を設定するには、**radius-server attribute wireless authentication call-station-id** コマンドを使用します。RADIUS アカウンティングメッセージから発信側ステーション識別子を削除するには、このコマンドの **no** 形式を使用します。

radius-server attribute wireless authentication call-station-id { **ap-ethmac-only** | **ap-ethmac-ssid** | **ap-ethmac-ssid-flexprofilename** | **ap-ethmac-ssid-policytagname** | **ap-ethmac-ssid-sitetagname** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-macaddress** | **ap-macaddress-ssid** | **ap-macaddress-ssid-flexprofilename** | **ap-macaddress-ssid-policytagname** | **ap-macaddress-ssid-sitetagname** | **ap-name** | **ap-name-ssid** | **flex-profile-name** | **ipaddress** | **macaddress** | **policy-tag-name** | **site-tag-name** | **vlan-id** }

構文の説明

ap-ethmac-only	発信側ステーション識別子タイプを、AP の無線 MAC アドレスに設定します。
ap-ethmac-ssid	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスに設定します。
ap-ethmac-ssid-flexprofilename	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスと Flex プロファイル名に設定します。
ap-ethmac-ssid-policytagname	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスとポリシータグ名に設定します。
ap-ethmac-ssid-sitetagname	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスとサイトタグ名に設定します。
ap-group-name	AP グループ名を使用するように発信側ステーション識別子タイプを設定します。
ap-label-address	発信側ステーション識別子タイプを、AP ラベルに印刷されている AP の無線 MAC アドレスに設定します。
ap-label-address-ssid	発信側ステーション識別子タイプを、AP ラベルに印刷されている AP の無線 MAC アドレスおよび SSID に設定します。
ap-location	発信側ステーション識別子タイプを、AP の場所に設定します。
ap-macaddress	発信側ステーション識別子タイプを、AP の無線 MAC アドレスに設定します。
ap-macaddress-ssid	発信側ステーション識別子タイプを、AP の SSID を持つ無線 MAC アドレスに設定します。

ap-macaddress-ssid-flexprofilename	発信側ステーション識別子タイプを、APのSSIDを持つ無線 MAC アドレスと Flex プロファイル名に設定します。
ap-macaddress-ssid-policytagname	発信側ステーション識別子タイプを、APのSSIDを持つ無線 MAC アドレスとポリシータグ名に設定します。
ap-macaddress-ssid-sitetagname	発信側ステーション識別子タイプを、APのSSIDを持つ無線 MAC アドレスとサイトタグ名に設定します。
ap-name	発信側ステーション識別子タイプを、AP名に設定します。
ap-name-ssid	発信側ステーション識別子タイプを、SSIDを持つAP名に設定します。
flex-profile-name	発信側ステーション識別子タイプを、Flexプロファイル名に設定します。
ipaddress	発信側ステーション識別子タイプを、システムの IP アドレスに設定します。
macaddress	発信側ステーション識別子タイプを、システムの MAC アドレスに設定します。
policy-tag-name	発信側ステーション識別子タイプを、ポリシータグ名に設定します。
site-tag-name	発信側ステーション識別子タイプを、サイトタグ名に設定します。
vlan-id	発信側ステーション識別子タイプを、システムの VLAN ID に設定します。

コマンド デフォルト

発信側ステーション識別子は設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。
Cisco IOS XE Bengaluru 17.4.1	このコマンドが変更されました。**policy-tag-name**、**flex-profile-name**、**ap-macaddress-ssid-flexprofilename**、**ap-macaddress-ssid-policytagname**、**ap-macaddress-ssid-sitetagname**、**ap-ethmac-ssid-flexprofilename**、**ap-ethmac-ssid-policytagname**、および **ap-ethmac-ssid-sitetagname** キーワードが導入されました。

使用上のガイドライン

例

次に、RADIUS 認証メッセージで送信される発信側ステーション識別子を設定する例を示します。

```
Device(config)# radius-server attribute wireless authentication call-station-id
site-tag-name
```

radius-server attribute wireless location delivery out-of-band include-location-capable

デバイスで設定されたロケーション情報を提供する Location-Capable 属性を有効にするには、**radius-server attribute wireless location delivery out-of-band include-location-capable** コマンドを使用します。Location-Capable 属性を無効にするには、このコマンドの **no** 形式を使用します。

radius-server attribute wireless location delivery out-of-band include-location-capable

no radius-server attribute wireless location delivery out-of-band include-location-capable

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.11.1	このコマンドが導入されました。

使用上のガイドライン

radius-server attribute wireless location delivery out-of-band include-location-capable コマンドを使用すると、Location-Capable 属性と Location（Location-Information および Location-Data）属性が有効になります。

no radius-server attribute wireless location delivery out-of-band include-location-capable コマンドを使用すると、Location-Capable 属性と Location（Location-Information および Location-Data）属性が無効になります。

Location-Capable 属性を使用せずに Location 属性を有効にするには、**radius-server attribute wireless location delivery out-of-band** コマンドを使用します。

例

次に、Location-Capable 属性を有効にして、デバイスで使用可能なロケーションプロファイル設定の詳細を提供する例を示します。

```
Device# configure terminal
Device(config)# radius-server attribute wireless location delivery out-of-band
include-location-capable
```

range

MAP から RAP ブリッジへの範囲を設定するには、**range** コマンドを使用します。

range *range-in-feet*

構文の説明

range-in-feet	範囲の値をフィート単位で設定します。有効な範囲は 150 ～ 132000 フィートです。

コマンド デフォルト

1200

コマンド モード

config-wireless-mesh-profile

コマンド履歴

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

例

次に、メッシュ AP プロファイルで MAP から RAP ブリッジへの範囲を設定する例を示します。

```
Device # configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device (config)# wireless profile mesh mesh-profile
Device (config-wireless-mesh-profile)# range 300
```

reanchor class

選択的リアンカー機能のプロトコルを使用してクラスマップを設定するには、**reanchor class** コマンドを使用します。

reanchor class *class-name*

構文の説明

class-name	AVC リアンカーのクラス名。

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

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

例

次に、AVC リアンカーのクラス名を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# reanchor class AVC-Reanchor-Class
```

record wireless avc basic

wireless avc basic AVC フロー レコードをフロー モニタに適用するには、**record wireless avc basic** コマンドを使用します。

record wireless avc basic

コマンド デフォルト

なし

コマンド モード

config-flow-monitor

コマンド履歴

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

使用上のガイドライン

このコマンドは、基本的なワイヤレス AVC テンプレートを指定します。AVC を設定する場合は、**record wireless avc basic** コマンドを使用してフロー モニタを作成する必要があります。

例

次に、*wireless avc basic* AVC フロー レコードを *test-flow* という名前のフロー モニターに適用する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# flow monitor test-flow
Device(config-flow-monitor)# record wireless avc basic
```

redundancy revertive

冗長モデルを復元可能に設定するには、**redundancy revertive** コマンドを使用します。

redundancy revertive

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

EoGRE ドメイン コンフィギュレーション

コマンド履歴

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

例

次の例では、冗長モードを復元可能に設定する方法を示します。

```
Device(config-eogre-domain)# redundancy revertive
```

redun-management interface Vlan

冗長管理インターフェイス（RMI）を設定するには、**redun-management interface Vlan** コマンドを使用します。

redun-management interface Vlan *vlan-interface-no* **chassis** *chassis-number* **address** *ip-address* **chassis** *chassis-number* **address** *ip-address*

構文の説明

vlan-interface-no	VLAN インターフェイス番号です。有効な範囲は 1 ～ 4094 です。 （注） ここで、*vlan-interface-no* は管理 VLAN と同じ VLAN です。つまり、両方とも同じサブネット上に存在する必要があります。
chassis-number	シャーシ番号です。有効な範囲は 1 ～ 2 です。
ip-address	RMI IP です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1s	このコマンドが導入されました。

次に、冗長管理インターフェイス（RMI）を設定する例を示します。

```
Device# chassis redundancy ha-interface GigabitEthernet 3
Device# configure terminal
Device(config)# redun-management interface Vlan 200 chassis 1 address 9.10.90.147 chassis
 2 address
9.10.90.149
Device(config)# end
```

redun-management garp-retransmit

GARP 再送信が実行されるレートを決定するには、**redun-management garp-retransmit** コマンドを使用します。

redun-management garp-retransmit burst *packet-burst-size* **interval** *time-interval*

構文の説明

packet-burst-size	有効な範囲は 0 ～ 1000 です。値を 0 にすると、再送信が無効になります。
time-interval	時間間隔を秒単位で示します。有効な範囲は 0 ～ 5 秒です。値を 0 にすると、再送信が無効になります。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、GARP 再送信が実行されるレートを決定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# redun-management garp-retransmit burst packet-burst-size interval
time-interval
```

redirect

外部ポータルへのリダイレクトを設定するには、 **redirect** コマンドを使用します。

redirect {**for-login** | **on-failure** | **on-success** }*redirect-url-name*

構文の説明

for-login	ログインするには、この URL にリダイレクトします。
on-failure	ログインが失敗した場合は、このURLにリダイレクトします。
on-success	ログインが成功した場合は、このURLにリダイレクトします。
redirect-url-name	リダイレクト URL 名。

コマンド デフォルト

なし

コマンド モード

config-params-parameter-map

コマンド履歴

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

例

次に、ログインするための外部IPv4 URL へのリダイレクトを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-name
Device(config-params-parameter-map)# redirect for-login cisco.com
```

redirect portal

外部 IPv4 または IPv6 ポータルを設定するには、 **redirect portal** コマンドを使用します。

redirect portal {**ipv4** | **ipv6** }*ip-addr*

構文の説明

ipv4	IPv4 portal address
ipv6	IPv6 portal address

コマンド デフォルト

なし

コマンド モード

config-params-parameter-map

コマンド履歴

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

例

次に、外部 IPv4 ポータルのアドレスを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parameter-map type webauth parameter-name
Device(config-params-parameter-map)# redirect portal ipv4 192.168.1.100
```

remote-span

VLAN をリモート スイッチド ポート アナライザ（RSPAN）VLAN として設定するには、スイッチ スタック上またはスタンドアロン スイッチ上で、VLAN コンフィギュレーション モードで **remote-span** コマンドを使用します。RSPAN 指定を VLAN から削除するには、このコマンドの **no** 形式を使用します。

remote-span
no remote-span

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

RSPAN VLAN は定義されません。

コマンド モード

VLAN コンフィギュレーション（config-VLAN）

コマンド履歴

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

使用上のガイドライン

VLAN Trunking Protocol（VTP）がイネーブルで、VLAN ID が 1005 未満の場合は、RSPAN 機能は VTP によって伝達されます。RSPAN VLAN ID が拡張範囲内の場合は、手動で中間スイッチを設定する必要があります（送信元スイッチと宛先スイッチの間の RSPAN VLAN 内に設定）。

RSPAN **remote-span** コマンドを設定する前に、**vlan**（グローバル コンフィギュレーション）コマンドで VLAN を作成してください。

RSPAN VLAN には、次の特性があります。

- MAC アドレス ラーニングは実行されません。
- トランク ポートでは RSPAN VLAN トラフィックだけが流れます。
- スパニングツリー プロトコル（STP）は RSPAN VLAN 内では稼働できますが、RSPAN 宛先ポートでは稼働しません。

既存の VLAN が RSPAN VLAN として設定されている場合は、その VLAN が最初に削除され、RSPAN VLAN として再作成されます。アクセス ポートは、RSPAN 機能がディセーブルになるまでは非アクティブです。

次の例では、RSPAN VLAN として VLAN を設定する方法を示します。

```
デバイス(config)# vlan 901
デバイス(config-vlan)# remote-span
```

次の例では、VLAN から RSPAN 機能を削除する方法を示します。

```
デバイス(config)# vlan 901
デバイス(config-vlan)# no remote-span
```

設定を確認するには、**show vlan remote-span** ユーザー EXEC コマンドを入力します。

remote-lan

RLAN ポリシー プロファイルを RLAN プロファイルにマッピングするには、**remote-lan** コマンドを使用します。

remote-lan *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id*

構文の説明

remote-lan-profile-name	リモート LAN プロファイルの名前。
rlan-policy-profile-name	リモート LAN ポリシープロファイルの名前。
port-id	ポート ID

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、RLAN ポリシー プロファイルを RLAN プロファイルにマッピングする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless tag policy remote-lan-policy-tag
デバイス(config-policy-tag)# remote-lan rlan_profile_name policy rlan_policy_profile
port-id 2
デバイス(config-policy-tag)# end
```

remote-lan rlan-profile policy rlan-policy ext-module

外部モジュールへのリモート LAN プロファイルおよびポリシーマッピングを設定するには、**remote-lan** *rlan-profile* **policy** *rlan-policy***ext-module** コマンドを使用します。外部モジュールへのリモート LAN プロファイルおよびポリシーマッピングを無効にするには、このコマンドの **no** 形式を使用します。

remote-lan *rlan-profile* **policy** *rlan-policy***ext-module**

構文の説明

rlan-profile	外部モジュールの RLAN プロファイルを設定します
rlan-policy	外部モジュールの RLAN ポリシーを設定します

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

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

例

次に、ポリシータグの下の外部モジュールへのリモート LAN プロファイルおよびポリシーマッピングを設定する例を示します。

```
Device(config)# wireless tag policy default-policy-tag
Device(config-policy-tag)# remote-lan <rlan-profile> policy <rlan-policy> ext-module
```

request platform software trace archive

シャーシでの最後のリロード以降にシステム上で実行されているすべてのプロセスに関連するすべてのトレースログをアーカイブし、これを指定された場所に保存するには、特権 EXEC モードまたはユーザ EXEC モードで **request platform software trace archive** コマンドを使用します。

request platform software trace archive ［**last** *number-of-days* ［**days** ［**target** *location*］］ | **target** *location*］

構文の説明

last *noofdays*	トレース ファイルをアーカイブする必要がある日数を指定します。
target *location*	アーカイブ ファイルの場所と名前を指定します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

このアーカイブ ファイルは、tftp コマンドまたは scp コマンドを使用してシステムからコピーできます。

例

次に、過去 5 日以降にシャーシで実行されているプロセスのすべてのトレースログをアーカイブする例を示します。

```
デバイス# request platform software trace archive last 5 days target flash:test_archive
```

resilient

Flex + ブリッジモードの AP で Flex Resilient 機能を有効にするには、**resilient** コマンドを使用します。

resilient

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

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

使用上のガイドライン

次に、Flex + ブリッジモードの AP で Flex Resilient 機能を有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless profile flex new-flex-profile
Device(config-wireless-flex-profile)# arp-caching
Device(config-wireless-flex-profile)# description "new flex profile"
Device(config-wireless-flex-profile)# native-vlan-id 2660
Device(config-wireless-flex-profile)# resilient
Device(config-wireless-flex-profile)# vlan-name VLAN2659
Device(config-wireless-flex-profile)# vlan-id 2659
Device(config-wireless-flex-profile)# end
```

rf tag

AP に RF タグを設定するには、**rf tag** コマンドを使用します。

rf tag *rf-tag-name*

構文の説明

rf-tag-name	RF タグ名。

コマンド デフォルト

なし

コマンド モード

config-ap-tag

コマンド履歴

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

使用上のガイドライン

このコマンドを実行すると、AP は、接続解除されたのち再参加します。

例

次に、RF タグを設定する例を示します。

```
Device(config-ap-tag)# rf-tag rftag1
```

roaming-oi

802.11u ローミング組織識別子を設定するには、**roaming-oi** コマンドを使用します。ローミング組織識別子を削除するには、このコマンドの **no** 形式を使用します。

roaming-oi *OI-value*［**beacon**］

構文の説明

OI-value	ローミング組織識別子の値。
beacon	ローミング組織識別子を BSSID ビーコンの一部としてアドバタイズします。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

使用上のガイドライン

最大 255 種類の OI 値を設定できます。

ローミング OI には最大 3 つのビーコンを使用できます。

ビーコンが指定されている場合、ローミング OUI は AP WLAN ビーコンまたはプローブ応答でアドバタイズされます。そうでない場合は、ローミング OUI ANQP クエリの実行中に返されるのみとなります。

例

次に、動作クラス識別子を設定する例を示します。

```
Device(config)#wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# roaming-oi 24 beacon
```

rogue detection containment pmf-denial

PMF 拒否の不正 AP 封じ込めを有効にするには、**rogue detection containment pmf-denial** コマンドを使用します。PMF 拒否の不正 AP 封じ込めを無効にするには、このコマンドの **no** 形式を使用します。

rogue detection containment pmf-denial

no rogue detection containment pmf-denial

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、PMF 拒否の不正 AP 封じ込めを有効にする例を示します。

```
Device# configure terminal
Device(config)# ap profile xyz-ap-profile
Device(config-ap-profile)# rogue detection containment pmf-denial
Device(config-pmf-denial)# pmf-deauth
```

rrc-evaluation

リソース予約コントロール（RRC）再評価アドミッションを設定するには、**rrc-evaluation** コマンドを使用します。

rrc-evaluation {**initial** | **periodic**}

構文の説明

initial	最初のアドミッション評価を設定します。
periodic	定期的なアドミッション評価を設定します。

コマンド デフォルト

なし

コマンド モード

config-media-stream

コマンド履歴

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

例

次の例は、RRC 再評価アドミッションを最初のアドミッション評価に設定する方法を示しています。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# rrc-evaluation initial
```

sampling

AP センサー環境でデータサンプリング間隔を設定するには、**sampling** コマンドを使用します。データサンプリング間隔をデフォルト時間の 5 秒に設定する場合は、このコマンドの **no** 形式を使用します。

sampling *data-sampling-interval*

no sampling *data-sampling-interval*

構文の説明

data-sampling-interval	データサンプリング間隔を設定します。 有効な範囲は 5 ～ 3600 秒です。デフォルト値は 5 秒です。

コマンド デフォルト

なし

コマンド モード

AP センサー コンフィギュレーション モード

コマンド履歴

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

例

次に、AP センサー環境でデータサンプリング間隔を設定する例を示します。

```
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# sensor environment air-quality
Device(config-ap-sensor)# sampling 300
```

scheduler asr

WLANで高度なスケジューリング要求機能を有効にするには、**scheduler asr**コマンドを使用します。WLANで高度なスケジューリング要求機能を無効にするには、このコマンドの**no**形式を使用します。

scheduler asr

no scheduler asr

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

高度なスケジューリング要求機能は有効になっています。

コマンド モード

WLAN コンフィギュレーション（config-wlan）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.4.1	このコマンドが追加されました。

例

次に、WLANで高度なスケジューリング要求機能を設定する例を示します。

```
Device# configure terminal
Device(config)# wlan test4
Device(config-wlan)# scheduler asr
```

secondary (ap prime)

アクセスポイント（AP）フォールバック用のセカンダリコントローラを設定するには、**secondary** コマンドを使用します。AP プライミングに使用されないようにセカンダリコントローラを削除するには、このコマンドの **no** 形式を使用します。

secondary *controller-name ip-address*

no secondary *controller-name ip-address*

構文の説明

controller-name	セカンダリ コントローラの名前。
ip-address	コントローラの IPv4 または IPv6 アドレス。

コマンド デフォルト

なし

コマンド モード

AP プライム コンフィギュレーション（config-priming）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.2	このコマンドが導入されました。

例

次に、AP フォールバック用のセカンダリコントローラを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile ap priming Prime-FX
Device(config-priming)# secondary bbbb 209.165.201.3
```

secure-webauth-disable

Web 認証用の HTTP セキュアサーバーを無効にするには、グローバル パラメータ マップ モードで **secure-webauth-disable** コマンドを使用します。このコマンドを無効にするには、このコマンドの **no** 形式を使用します。

secure-webauth-disable

no secure-webauth-disable

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル パラメータ マップ モード

コマンド履歴

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

例

次に、Web 認証用の HTTP セキュアサーバーを無効にする例を示します。

```
Device(config-params-parameter-map)# secure-weauth-disable
```

security

メッシュ セキュリティを設定するには、 **security** コマンドを使用します。

security { **eap** | **psk** }

構文の説明

eap	メッシュ AP のメッシュ セキュリティ EAP を設定します。
psk	メッシュ AP のメッシュ セキュリティ PSK を設定します

コマンド デフォルト

EAP

コマンド モード

config-wireless-mesh-profile

コマンド履歴

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

例

次に、メッシュ AP で EAP プロトコルを使用してメッシュ セキュリティを設定する例を示します。

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

security dot1x authentication-list

IEEE 802.1x のセキュリティ認証リストを設定するには、**security dot1x authentication-list** *auth-list-name* コマンドを使用します。

security dot1x authentication-list *auth-list-name*

構文の説明

パラメータ	説明
auth-list-name	認証リスト名。

コマンド デフォルト

なし

コマンド モード

config-wlan

コマンド履歴

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

例

次に、IEEE 802.1x のセキュリティ認証リストを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan-name
Device(config-wlan)# security dot1x authentication-list auth-list-realm
```

security dot1x request

EAP 要求関連のパラメータを設定するには、**security dot1x request** コマンドを使用します。EAP 要求関連のパラメータをリセットするには、このコマンドの **no** 形式を使用します。

security dot1x request { **retries** *retry-num* | **timeout** *timeout-value* }

no security dot1x request { **retries** *retry-num* | **timeout** *timeout-value* }

構文の説明

retries *retries*	EAP メッセージについて、コントローラが無線クライアントにメッセージを再送信する最大回数を指定します。 有効な値の範囲は 0 ～ 20 です。
timeout *timeout-value*	EAP メッセージについて、コントローラが無線クライアントにメッセージを再送信するまでに待機する時間を指定します。 有効な値の範囲は 1 ～ 120 です。

コマンド デフォルト

なし

コマンド モード

リモート LAN コンフィギュレーション（config-remote-lan）

コマンド履歴

リリース	変更内容
	このコマンドが導入されました。

次の例では、 **wireless security dot1x** のすべてのコマンドをリストしています。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap remote-lan profile-name rlan_profile_name 3
Device(config-remote-lan)# security dot1x request retries 10
Device(config-remote-lan)# security dot1x request timeout 100
```

security dot1x identity-request

EAP ID 要求関連のパラメータを設定するには、**security dot1x identity-request** コマンドを使用します。EAP ID 要求関連のパラメータをリセットするには、このコマンドの **no** 形式を使用します。

security dot1x identity-request { **retries** *retry-num* | **timeout** *timeout-value* }

no security dot1x identity-request { **retries** *retry-num* | **timeout** *timeout-value* }

構文の説明

retries *retries*	EAP ID 要求について、コントローラが要求を再送信する最大回数を指定します。 有効な値の範囲は 1 ～ 20 です。
timeout *timeout-value*	EAP ID 要求について、コントローラがメッセージを再送信するまでに待機する時間を指定します。 有効な値の範囲は 1 ～ 120 です。

コマンド デフォルト

なし

コマンド モード

リモート LAN コンフィギュレーション（config-remote-lan）

コマンド履歴

リリース	変更内容
	このコマンドが導入されました。

例

次に、EAP ID 要求関連のパラメータを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap remote-lan profile-name rlan_profile_name 3
Device(config-remote-lan)# security dot1x identity-request retries 10
Device(config-remote-lan)# security dot1x identity-request timeout 100
```

security ft

802.11r Fast Transition パラメータを設定するには、**security ft** コマンドを使用します。Fast Transition **over the air** を設定するには、**no security ft over-the-ds** コマンドを使用します。

security ft [{**over-the-ds** | **reassociation-timeout** *timeout-jn-seconds*}]
no security ft [{**over-the-ds** | **reassociation-timeout**}]

構文の説明

over-the-ds	（任意）802.11r Fast Transition が分散システムを介して発生するように指定します。このパラメータを指定したコマンドの no 形式は、無線を介したセキュリティ Fast Transition を設定します。
reassociation-timeout	（任意）再アソシエーションのタイムアウト間隔を設定します。
timeout-in-seconds	（任意）再アソシエーションのタイムアウト間隔を秒単位で指定します。有効な範囲は 1 ～ 100 です。デフォルト値は 20 です。

コマンド デフォルト

機能はディセーブルです。

コマンド モード

WLAN の設定

コマンド履歴

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

使用上のガイドライン

なし

WLAN セキュリティを有効にする必要があります。

例

次に、オープンな WLAN のセキュリティ FT を設定する例を示します:

```
デバイス#wlan test
デバイス(config-wlan)# client vlan 0140
デバイス(config-wlan)# no mobility anchor sticky
デバイス(config-wlan)# no security wpa
デバイス(config-wlan)# no security wpa akm dot1x
デバイス(config-wlan)# no security wpa wpa2
デバイス(config-wlan)# no security wpa wpa2 ciphers aes
デバイス(config-wlan)# security ft
デバイス(config-wlan)# shutdown
```

次に、WPA 対応の WLAN のセキュリティ FT を表示する例を示します。

```
デバイス# wlan test
デバイス(config-wlan)# client vlan 0140
```

```
デバイス(config-wlan)# no security wpa akm dot1x
デバイス(config-wlan)# security wpa akm ft psk
デバイス(config-wlan)# security wpa akm psk set-key ascii 0 test-test
デバイス(config-wlan)# security ft
デバイス(config-wlan)# no shutdown
```

security level（IPv6 スヌーピング）

適用されるセキュリティのレベルを指定するには、IPv6 スヌーピング ポリシー コンフィギュレーション モードで **security-level** コマンドを使用します。

security level {**glean** | **guard** | **inspect**}

構文の説明

glean	アドレスをメッセージから抽出し、検証を行わずにそれらをバインディング テーブルにインストールします。
guard	収集と検査の両方を実行します。さらに、信頼できるポートで受信されていない場合、または別のポリシーによって許可されていない場合、RA メッセージおよび DHCP サーバー メッセージは拒否されます。
inspect	メッセージの一貫性と準拠度を検証します。特に、アドレス所有権が強制されます。無効なメッセージはドロップされます。

コマンド デフォルト

デフォルトのセキュリティ レベルは guard です。

コマンド モード

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

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

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、デバイスを IPv6 スヌーピング コンフィギュレーション モードにし、セキュリティ レベルを inspect として設定する例を示します。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)# security-level inspect
```

security pmf

WLAN の 802.11w 管理フレーム保護（PMF）を設定するには、**security pmf** コマンドを使用します。管理フレーム保護を無効にするには、このコマンドの **no** 形式を使用します。

security pmf {**association-comeback** *association-comeback-time-seconds* | **mandatory** | **optional** | **saquery-retry-time** *saquery-retry-time-milliseconds*}
no security pmf [{**association-comeback** *association-comeback-time-seconds* | **mandatory** | **optional** | **saquery-retry-time** *saquery-retry-time-milliseconds*}]

構文の説明

association-comeback	802.11w アソシエーション復帰時間を設定します。
association-comeback-time-seconds	アソシエーション復帰間隔（秒単位）。アソシエーションがステータス コード 30 によって拒否された後に、アソシエートされているクライアントがアソシエーションを再試行するまでに待機する必要がある時間間隔。ステータス コード 30 のメッセージは、「Association request rejected temporarily; Try again later」です。 有効範囲は 1 ～ 20 秒です。
mandatory	クライアントが WLAN の 802.1w PMF 保護をネゴシエートする必要があることを指定します。
optional	WLAN がクライアントでの 802.11w サポートを必要としていないことを指定します。802.11w 機能のないクライアントも、参加可能です。
saquery-retry-time	SA クエリの応答を受け取るまでの時間。device が応答を受け取らなかった場合、別の SA クエリーが試行されます。
saquery-retry-time-milliseconds	SA クエリの再試行時間は、ミリ秒単位で指定します。指定できる範囲は 100 ～ 500 ミリ秒です。値は 100 ミリ秒の倍数で指定する必要があります。

コマンド デフォルト

PMF は無効になっています。

コマンド モード

WLAN の設定

コマンド履歴

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

使用上のガイドライン

この機能を使用するには、WPA（Wi-Fi Protected Access）と AKM（認証キー管理）が設定されている必要があります。セキュリティ パラメータの設定の詳細については、「関連コマンド」の項を参照してください。

802.11w では、ブロードキャストまたはマルチキャストの堅牢な管理フレームを保護するために使用される Integrity Group Temporal Key（IGTK）が導入されています。IGTK は、ソース STA からの MAC 管理プロトコル データ ユニット（MMPDU）を保護するために使用するオーセンティケータ ステーション（device）によって割り当てられる、ランダムな値です。802.11w IGTK キーは、4 ウェイ ハンドシェイクを使用して取得され、レイヤ 2 で WPA2 セキュリティが設定されている WLAN でのみ使用されます。

次に、アソシエーション復帰時間値を 15 秒で有効にする例を示します。

```
デバイス(config-wlan)# security pmf association-comeback 15
```

次に、WLAN のクライアントに必須の 802.11w MPF 保護を設定する例を示します。

```
デバイス(config-wlan)# security pmf mandatory
```

次に、WLAN のクライアントにオプションの 802.11w MPF 保護を設定する例を示します。

```
デバイス(config-wlan)# security pmf optional
```

次に、saquery パラメータを設定する例を示します。

```
デバイス(config-wlan)# security pmf saquery-retry-time 100
```

次に、PMF 機能を無効にする例を示します。

```
デバイス(config-wlan)# no security pmf
```

security static-wep-key

WLAN で静的 WEP キーを設定するには、**security static-wep-key** コマンドを使用します。

security static-wep-key {**authentication** {**open** | **sharedkey** } | **encryption** {**104** | **40** }{**ascii** | **hex** | {**0** | **8** }*wep-key* | **wep-index** }}

構文の説明

open	オープン システム認証。
sharedkey	共有キー認証。
0	暗号化されていないパスワードが使用されることを指定します。
8	AES 暗号化パスワードが使用されることを指定します。
wep-key	WEP キーの名前を入力します。

コマンド デフォルト

なし

コマンド モード

config-wlan

コマンド履歴

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

例

次に、共有キーを使用して 802.11 を認証する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan profile-name wlan-id
Device(config-wlan)# security static-wep-key authentication sharedkey
```

security web-auth

WLAN で使用する Web 認証のステータスを変更するには、 **security web-auth** コマンドを使用します。WLAN で Web 認証を無効にするには、このコマンドの **no** 形式を使用します。

security web-auth [{**authentication-list** *authentication-list-name* | **on-macfilter-failure** | **parameter-map** *parameter-map-name*}]
no security web-auth [{**authentication-list** [**authentication-list-name**] | **on-macfilter-failure** | **parameter-map** [**parameter-name**]}]

構文の説明

authentication-list *authentication-list-name*	IEEE 802.1x の認証リストを設定します。
on-macfilter-failure	MAC の失敗時の Web 認証を有効にします。
parameter-map *parameter-map-name*	パラメータ マップを設定します。

コマンド デフォルト

Web 認証はディセーブルです。

コマンド モード

WLAN の設定

コマンド履歴

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

例

次に、WLAN に認証リストによる Web 認証を設定する例を示します。

```
デバイス(config-wlan)# security web-auth authentication-list test
```

security wpa akm

Cisco Centralized Key Management（CCKM）を使用して認証キー管理を設定するには、**security wpa akm** コマンドを使用します。Cisco Centralized Key Management の認証キー管理を無効にするには、このコマンドの **no** 形式を使用します。

security wpa [{ **akm** { **cckm** | **dot1x** | **ft** | **pmf** | **psk** } | **wpa1** [**ciphers** { **aes** | **tkip** }] | **wpa2** [**ciphers** { **aes** }] }]
no security wpa [{ **akm** { **cckm** | **dot1x** | **ft** | **pmf** | **psk** } | **wpa1** [**ciphers** { **aes** | **tkip** }] | **wpa2** [**ciphers** { **aes** }] }]

構文の説明

akm	認証キー管理（AKM）パラメータを設定します。
aes	AES（Advanced Encryption Standard）暗号化サポートを設定します。
cckm	Cisco Centralized Key Management のサポートを設定します。
ciphers	WPA 暗号方式を設定します。
dot1x	802.1x のサポートを設定します。
ft	802.11r を使用して Fast Transition を設定します。
pmf	802.11w 管理フレーム保護を設定します。
psk	802.11r Fast Transition の事前共有キー（PSK）のサポートを設定します。
tkip	Temporal Key Integrity Protocol（TKIP）暗号化のサポートを設定します。
wpa2	Wi-Fi Protected Access 2（WPA2）のサポートを設定します。

コマンド デフォルト

デフォルトでは Wi-Fi Protected Access2、802.1x は有効になっています。WPA2、PSK、CCKM、FT dot1x、FT PSK、PMF dot1x、PMF PSK、FT のサポートは無効になっています。FT の再アソシエーションのタイムアウトは 20 秒、PMF SA クエリ時間は 200 に設定されています。

コマンド モード

WLAN の設定（config-wlan）

コマンド履歴

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

例

次に、WLAN に CCKM を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)#security wpa akm cckm
```

security wpa akm ft sae

SAE セキュリティ対応 WLAN で 802.11r Fast Transition を有効にするには、**security wpa akm ft sae** コマンドを使用します。

security wpa akm ft sae

構文の説明

security	WLANのセキュリティポリシーを設定します。
wpa	WLAN の WPA/WPA2 サポートを設定します。
akm	認証キー管理を設定します。
ft	802.11r Fast Transition を設定します。
sae	SAE サポートを設定します。

コマンド デフォルト

なし

コマンド モード

WLAN コンフィギュレーション モード（config-wlan）

コマンド履歴

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

例

次に、SAE セキュリティ対応 WLAN で 802.11r Fast Transition を有効にする例を示します。

```
Device# configure terminal
Device(config)# wlan wlan-test 3 ssid-test
Device(config-wlan)# security ft
Device(config-wlan)# no security wpa wpa2
Device(config-wlan)# security wpa psk set-key ascii 0 123456789
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# security wpa akm ft sae
Device(config-wlan)# security wpa wpa3
Device(config-wlan)# security pmf mandatory
Device(config-wlan)# no shutdown
```

security wpa akm owe

認証キー管理（AKM）の Opportunistic Wireless Encryption（OWE）を有効にするには、**security wpa akm owe** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

security wpa akm owe

no security wpa akm owe

構文の説明

security	WLANのセキュリティポリシーを設定します。
wpa	WLAN の WPA/WPA2 サポートを設定します。
akm	認証キー管理を設定します。
owe	OWE サポートを設定します。

コマンド デフォルト

なし

コマンド モード

WLAN コンフィギュレーション モード（config-wlan）

コマンド履歴

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

次に、認証キー管理（AKM）の Opportunistic Wireless Encryption（OWE）を有効にする例を示します。

```
Device# configure terminal
Device(config)# wlan wlan-test 3 ssid-test
Device(config-wlan)# security wpa akm owe
```

security wpa akm psk

認証キー管理（AKM）の事前共有キー（PSK）を有効にするには、**security wpa akm psk** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

security wpa akm psk

no security wpa akm psk

構文の説明

security	WLANのセキュリティポリシーを設定します。
wpa	WLAN の WPA/WPA2 サポートを設定します。
akm	認証キー管理を設定します。
psk	PSK サポートを設定します。

コマンド デフォルト

なし

コマンド モード

WLAN コンフィギュレーション モード（config-wlan）

コマンド履歴

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

次に、認証キー管理（AKM）の事前共有キー（PSK）を有効にする例を示します。

```
Device# configure terminal
Device(config)# wlan wlan-test 3 ssid-test
Device(config-wlan)# security wpa akm psk
```

security wpa akm sae

認証キー管理（AKM）の Secure Agile Exchange（SAE）を有効にするには、**security wpa akm sae pwe** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

security wpa akm sae pwe { h2e | hnp | both-h2e-hnp}

no security wpa akm sae pwe { h2e | hnp | both-h2e-hnp}

構文の説明

security	WLAN のセキュリティポリシーを設定します。
wpa	WLAN の WPA/WPA2 サポートを設定します。
akm	認証キー管理を設定します。
sae	SAE サポートを設定します。
pwe	SAE のパスワード要素を設定します。
h2e	Hash To Element のみを設定します（Hunting and Pecking を無効にします）。
hnp	Hunting And Pecking のみを設定します（Hash To Element を無効にします）。
both-h2e-hnp	Hash to Element と Hunting and Pecking の両方のサポートを設定します（デフォルトのオプションです）。

コマンド デフォルト

なし

コマンド モード

WLAN コンフィギュレーション モード（config-wlan）

コマンド履歴

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

次に、認証キー管理（AKM）の Secure Agile Exchange（SAE）を有効にする例を示します。

```
Device# configure terminal
Device(config)# wlan wlan-test 3 ssid-test
Device(config-wlan)# security wpa akm sae
```

security wpa akm sae pwe

認証キー管理（AKM）の Secure Agile Exchange（SAE）PWE サポートを有効にするには、**security wpa akm sae pwe** コマンドを使用します。

security wpa akm sae pwe { h2e | hnp | both-h2e-hnp}

構文の説明

h2e	Hash-to-Element のみ。HnP を無効にします。
hnp	Hunting and Pecking のみ。H2E を無効にします。
Both-h2e-hnp	Hash-to-Element と Hunting and Pecking の両方をサポート（デフォルトのオプションです）。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

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

使用上のガイドライン

次に、AKM の SAE PWE サポートを有効にする例を示します。

```
Device# configure terminal
Device(config)# wlan WPA3 1 WPA3
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# no security ft over-the-ds
Device(config-wlan)# no security ft
Device(config-wlan)# no security wpa wpa2
Device(config-wlan)# security wpa wpa2 ciphers aes
Device(config-wlan)# security wpa psk set-key ascii 0 Cisco123
Device(config-wlan)# security wpa wpa3
Device(config-wlan)# security wpa akm sae
Device(config-wlan)# security wpa akm sae pwe
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

segment

同じアプリケーションサービスを共有するデバイスのグループを識別するセグメント名を設定するには、**segment** コマンドを使用します。セグメントを削除するには、このコマンドの **no** 形式を使用します。

segment *segment-name*

no segment

構文の説明

segment-name	セグメント名。最大63文字の英数字を指定できます。

コマンド デフォルト

セグメント名は設定されていません。

コマンド モード

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

コマンド履歴

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

例

次に、同じアプリケーションサービスを共有するデバイスのグループを識別するセグメント名を設定する例を示します。

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

sensor environment

APセンサー環境を設定するには、**sensor environment**コマンドを使用します。この機能を無効化するには、このコマンドの **no** 形式を使用します。

sensor environment ｛ **air-quality** ｜ **temperature** ｝

no sensor environment ｛ **air-quality** ｜ **temperature** ｝

構文の説明

air-quality	電波品質センサーを指定します。
temperature	温湿度センサーを指定します。

コマンド デフォルト

なし

コマンド モード

AP プロファイル コンフィギュレーション モード

コマンド履歴

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

例

次に、AP センサー環境を設定する例を示します。

```
Device(config)# ap profile ap-profile-name
Device(config-ap-profile)# sensor environment air-quality
```

sequence-number ethernet

イーサネットの電源ポリシーを設定するには、ワイヤレス電力プロファイル コンフィギュレーション モードで *sequence-number* **ethernet** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

sequence-number **ethernet** { **GigabitEthernet0** | **GigabitEthernet1 speed** { **1000mbps** | **100mbps** | **2500mbps** | **5000mbps** } | **LAN1** | **LAN2** | **LAN3 state disable** }

no *sequence-number* **ethernet** { **GigabitEthernet0** | **GigabitEthernet1 speed** { **1000mbps** | **100mbps** | **2500mbps** | **5000mbps** } | **LAN1** | **LAN2** | **LAN3 state disable** }

構文の説明

sequence-number	電力プロファイルの設定は、シーケンス番号順に並べられています。AP のディレーティングは、入力されたシーケンス番号に従って行われます。インターフェイス識別子とパラメータ値の同じ組み合わせは、別のシーケンス番号には表示されません。同じパラメータを持つ同じインターフェイスが、異なるパラメータ値で複数回表示されることがあります。
GigabitEthernet0	GigabitEthernet0 を設定します。
GigabitEthernet1	GigabitEthernet1 を設定します。
speed	イーサネット速度の制限を設定します。 （注） イーサネット速度設定は、Cisco IOS XE Cupertino 17.8.1 では使用できません。
1000mbps	イーサネット速度の制限を 1000 Mbps に設定します。
100mbps	イーサネット速度の制限を 100 Mbps に設定します。
2500mbps	イーサネット速度の制限を 2500 Mbps に設定します。
5000mbps	イーサネット速度の制限を 5000 Mbps に設定します。
LAN1	LAN1 ポートを設定します。
LAN2	LAN2 ポートを設定します。
LAN3	LAN3 ポートを設定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス電力プロファイル コンフィギュレーション モード

コマンド履歴

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

例

次に、ワイヤレス電力プロファイルコンフィギュレーションモードでイーサネットの電源ポリシーを設定する例を示します。

```
Device(config)# wireless profile power power-profile-name
Device(config-wireless-power-profile)# 10 ethernet gigabitethernet1 speed 1000mbps
```

（注） イーサネット速度設定は、Cisco IOS XE Cupertino 17.8.1 では使用できません。

sequence-number radio

無線の電源ポリシーを設定するには、ワイヤレス電力プロファイル コンフィギュレーション モードで *sequence-number* **radio** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

sequence-number **radio** { **24ghz** | **5ghz** | **6ghz** | **secondary-5ghz** } **state shutdown**

no *sequence-number* **radio** { **24ghz** | **5ghz** | **6ghz** | **secondary-5ghz** } **state shutdown**

構文の説明

sequence-number	電力プロファイルの設定は、シーケンス番号順に並べられています。APのディレーティングは、入力されたシーケンス番号に従って行われます。インターフェイス識別子とパラメータ値の同じ組み合わせは、別のシーケンス番号には表示されません。同じパラメータを持つ同じインターフェイスが、異なるパラメータ値で複数回表示されることがあります。
24ghz	2.4 GHz 無線を設定します。
5ghz	5 GHz 無線を設定します。
6ghz	6 GHz 無線を設定します。
secondary-5ghz	セカンダリ 5 GHz 無線を設定します。
state shutdown	無線状態をダウンとして指定します。

コマンド デフォルト

なし

コマンド モード

ワイヤレス電力プロファイル コンフィギュレーション

コマンド履歴

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

例

次に、ワイヤレス電力プロファイル コンフィギュレーション モードで無線の電源ポリシーを設定する例を示します。

```
Device(config)# wireless profile power power-profile-name
Device(config-wireless-power-profile)# 20 radio 6ghz state shutdown
```

sequence-number usb 0 state disable

USB の電源ポリシーを設定するには、ワイヤレス電力プロファイル コンフィギュレーション モードで *sequence-number* **usb 0 state disable** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

sequence-number **usb 0 state disable**

no *sequence-number* **usb 0 state disable**

構文の説明

sequence-number	電力プロファイルの設定は、シーケンス番号順に並べられています。AP のディレーティングは、入力されたシーケンス番号に従って行われます。インターフェイス識別子とパラメータ値の同じ組み合わせは、別のシーケンス番号には表示されません。同じパラメータを持つ同じインターフェイスが、異なるパラメータ値で複数回表示されることがあります。

コマンド デフォルト

なし

コマンド モード

ワイヤレス電力プロファイル コンフィギュレーション モード

コマンド履歴

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

例

次に、ワイヤレス電力プロファイル コンフィギュレーション モードで USB の電源ポリシーを設定する例を示します。

```
Device(config)# wireless profile power power-profile-name
Device(config-wireless-power-profile)# 30 usb 0 state disable
```

server-uri

オンラインサインアップ（OSU）オペレータのサーバー Uniform Resource Identifier（URI）を設定するには、**server-uri** コマンドを使用します。サーバー URI を削除するには、このコマンドの **no** 形式を使用します。

server-uri *server-uri*

構文の説明

server-uri	OSU オペレータのサーバー URI。

コマンド デフォルト

なし

コマンド モード

ANQP OSU プロバイダーの設定（config-anqp-osu-provider）

コマンド履歴

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

例

次に、OSU オペレータのサーバー URI を設定する例を示します。

```
Device(config-wireless-anqp-server)# osu-provider my-osu
Device(config-anqp-osu-provider)# server-uri yyyy
```

service-policy

Quality of Service（QoS）サービスポリシーを設定するには、**service-policy** コマンドを使用します。QoS ポリシーを無効にするには、このコマンドの **no** 形式を使用します。

service-policy { **client** | **input** | **output** } *policy-name*
no { **client** | **input** | **output** } *policy-name*

構文の説明

client	WLAN 上のすべてのクライアントにポリシーマップを割り当てます。
input	入力ポリシー マップを割り当てます。
output	出力ポリシー マップを割り当てます。
policy-name	ポリシー マップ名。

コマンド デフォルト

なし

コマンド モード

ワイヤレス ポリシー コンフィギュレーション

コマンド履歴

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

例

次に、入力サービスポリシーを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# service-policy input test1
```

service-policy qos

QoS サービス ポリシーを設定するには、 **service-policy qos** コマンドを使用します。

service-policy qos {**input** | **output**}*policy-name*

構文の説明

input	入力 QoS ポリシー。
output	出力 QoS ポリシー。
policy-name	ポリシー名。

コマンド デフォルト

なし

コマンド モード

config-service-template

コマンド履歴

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

例

次に、出力 QoS ポリシーを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# service-template fabric-profile-name
Device(config-service-template)# service-policy qos output policy-name
```

service-template

サービス テンプレートを設定するには、 **service-template** コマンドを使用します。

service-template *service-template-name* {**access-group** *acl_list* | **vlan** *vlan_id* | **absolute-timer** *seconds* | **service-policy qos** {**input** | **output**}}

構文の説明

service-template-name	サービス テンプレートの名前。
acl_list	適用されるアクセス リストの名前。
vlan_id	VLAN ID。VLAN ID 値の範囲は 1 ～ 4094 です。
seconds	サービス テンプレートのセッション タイムアウト値。セッション タイムアウト値の範囲は 1 ～ 65535 秒です。
service-policy qos {**input** | **output**	クライアントの QoS ポリシー。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし

次に、サービス テンプレートを設定する例を示します。

```
デバイス#configure terminal
デバイス(config)#service-template cisco-phone-template
デバイス(config-service-template)#access-group foo-acl
デバイス(config-service-template)#vlan 100
デバイス(config-service-template)#service-policy qos input foo-qos
デバイス(config-service-template)#end
```

service timestamps

デバッグメッセージまたはロギングメッセージにタイムスタンプを使用するようにシステムを設定するには、グローバル コンフィギュレーション コマンドの **service timestamps** コマンドを使用します。このサービスを無効にするには、このコマンドの **no** 形式を使用します。

service timestamps debug log{**datetime** | **uptime***localtimemsecshow-timezoneyear*}
no service timestamps debuglog

構文の説明

debug	タイムスタンプ メッセージ タイプとしてデバッグします。
log	タイムスタンプ メッセージ タイプとしてログに記録します。
datetime	**datetime**
uptime	（任意）システムが再起動されてからの時間を使用したタイムスタンプ。
localtime	（任意）ローカルタイムゾーンを基準にしたタイムスタンプ。
msec	（任意）日付とタイムスタンプにミリ秒を含めます。
show-timezone	（任意）タイムスタンプにタイムゾーン名を含めます。
year	（任意）タイムスタンプに年を含めます。

コマンド デフォルト

タイムスタンプは使用されません。

引数またはキーワードを使用せずに **service timestamps** を指定した場合、デフォルトは **service timestamps debug uptime** です。

service timestamps debugdatetime のデフォルトでは、時間は UTC 形式になり、ミリ秒もタイムゾーン名も含まれません。

no service timestamps コマンドは、単独でデバッグメッセージとログメッセージの両方のタイムスタンプを無効にします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1s	このコマンドは、Cisco IOS XE Amsterdam 17.1.1s よりも前のリリースで導入されました。

使用上のガイドライン

タイムスタンプは、デバッグメッセージまたはロギングメッセージに個別に追加できます。このコマンドの uptime 形式を使用すると、HHHH:MM:SS 形式のタイムスタンプが追加され、システムが再起動されてからの時間が示されます。このコマンドの datetime 形式を使用すると、MMM DD HH:MM:SS 形式のタイムスタンプが追加され、システムクロックによる日付と時刻

が示されます。システムクロックが設定されていない場合、日付と時刻の前にアスタリスク（*）が付き、日付と時刻が正しくない可能性があることが示されます。

例

次に、デバッグメッセージのタイムスタンプを有効にして、再起動してからの時間を表示する例を示します。

```
Device(config)# service timestamps debug uptime
```

次に、ロギングメッセージのタイムスタンプを有効にして、ローカルタイムゾーンを基準にした現在の日付と時刻を、タイムゾーン名を含めて表示する例を示します。

```
Device(config)# service timestamps log datetime localtime show-timezone
```

session-timeout

WLAN に関連付けられたクライアントのセッション タイムアウトを設定するには、**session-timeout** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

session-timeout seconds
no session-timeout

構文の説明

seconds	タイムアウトまたはセッション時間（秒）。範囲は 300 ～ 86400 です。デフォルト値は 1800 です。 86400 の設定は、最大タイムアウトと同等です。また、値 0 は推奨されません。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

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

次に、セッション タイムアウトを 3600 秒に設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless profile policy policy1
Device(config-wireless-policy)#session-timeout 3600
```

set

パケットで DiffServ コード ポイント（DSCP）値または IP precedence 値を設定して IP トラフィックを分類するには、ポリシーマップ クラス コンフィギュレーション モードで **set** コマンドを使用します。トラフィックの分類を削除するには、このコマンドの **no** 形式を使用します。

set
cos | **dscp** | **precedence** | **ip** | **qos-group** | **wlan**
set cos
{*cos-value*} | {**cos** | **dscp** | **precedence** | **qos-group** | **wlan**} [{**table** *table-map-name*}]
set dscp
{*dscp-value*} | {**cos** | **dscp** | **precedence** | **qos-group** | **wlan**} [{**table** *table-map-name*}]
set ip {**dscp** | **precedence**}
set precedence {*precedence-value* } | {**cos** | **dscp** | **precedence** | **qos-group**} [{**table** *table-map-name*}]
set qos-group
{*qos-group-value* | **dscp** [{**table** *table-map-name*}] | **precedence** [{**table** *table-map-name*}]}
set wlan user-priority
user-priority-value | **costable** *table-map-name* | **dscptable** *table-map-name* | **qos-grouptable** *table-map-name* | **wlantable** *table-map-name*

構文の説明		
	cos	発信パケットのレイヤ 2 サービス クラス（CoS）値またはユーザ プライオリティを設定します。次の値を指定できます。 • *cos-value*：0 ～ 7 の CoS 値。一般的に使用する値に対してはニーモニック名を入力することもできます。 • パケットに CoS 値を設定するためのパケット マーキング カテゴリを指定します。パケット マーキング値をマッピングおよび変換するためのテーブル マップも設定している場合は、これによって「map from」パケットマーキング カテゴリが確立されます。パケットマーキングカテゴリのキーワードは次のとおりです。 • **cos**：CoS 値またはユーザ プライオリティからの値を設定します。 • **dscp**：DiffServ コード ポイント（DSCP）からの値を設定します。 • **precedence**：パケット優先順位からの値を設定します。 • **qos-group**：QoS グループからの値を設定します。 • **wlan**：WLAN ユーザー プライオリティ値を設定します。 • （任意）**table** *table-map-name*：CoS 値の設定に使用される指定されたテーブル マップに設定されている値を示します。CoS 値の指定に使用されるテーブル マップの名前を入力します。テーブルマップ名には、最大 64 の英数字を使用できます。 パケットマーキング カテゴリを指定したが、テーブルマップを指定していない場合、デフォルトアクションは、パケットマーキング カテゴリに関連付けられた値を CoS 値としてコピーすることです。たとえば、**set cos precedence** コマンドを入力する場合、precedence（パケットマーキングカテゴリ）値がコピーされ、CoS 値として使用されます。

dscp	IP（v4）およびIPv6パケットのDiffServコードポイント（DSCP）を指定します。次の値を指定できます。 • *cos-value*：DSCP値を設定する番号。範囲は0～63です。一般的に使用する値に対してはニーモニック名を入力することもできます。 • パケットにDSCP値を設定するためのパケットマーキング カテゴリを指定します。パケットマーキング値をマッピングおよび変換するためのテーブルマップも設定している場合は、これによって「map from」パケットマーキング カテゴリが確立されます。パケットマーキングカテゴリのキーワードは次のとおりです。 • **cos**：CoS値またはユーザプライオリティからの値を設定します。 • **dscp**：DiffServコードポイント（DSCP）からの値を設定します。 • **precedence**：パケット優先順位からの値を設定します。 • **qos-group**：QoSグループからの値を設定します。 • **wlan**：WLANから値を設定します。 • （任意）**table** *table-map-name*：DSCP値の設定に使用される指定されたテーブル マップに設定されている値を示します。DSCP値の指定に使用されるテーブル マップの名前を入力します。テーブルマップ名には、最大64の英数字を使用できます。 パケットマーキング カテゴリを指定したが、テーブルマップを指定していない場合、デフォルトアクションは、パケットマーキング カテゴリに関連付けられた値をDSCP値としてコピーすることです。たとえば、**set dscp cos** コマンドを入力する場合、CoS値（パケットマーキング カテゴリ）がコピーされ、DSCP値として使用されます。

ip	分類されたトラフィックに IP 値を設定します。次の値を指定できます。 • **dscp**：0 ～ 63 の IP DSCP 値またはパケット マーキング カテゴリを指定します。 • **precedence**：IP ヘッダーの precedence ビット値を指定します（有効な値は 0 ～ 7）。または、パケットマーキング カテゴリを指定します。
precedence	パケット ヘッダーに precedence 値を設定します。次の値を指定できます。 • *precedence-value*：パケット ヘッダーに precedence ビットを設定します。有効な値は 0 ~7 です。一般的に使用する値に対してはニーモニック名を入力することもできます。 • パケットの優先順位値を設定するためのパケットマーキング カテゴリを指定します。 • **cos**：CoS またはユーザ プライオリティからの値を設定します。 • **dscp**：DiffServ コード ポイント（DSCP）からの値を設定します。 • **precedence**：パケット優先順位からの値を設定します。 • **qos-group**：QoS グループからの値を設定します。 • （任意）**table** *table-map-name*：優先順位値の設定に使用される指定されたテーブル マップに設定されている値を示します。優先順位値の指定に使用されるテーブル マップの名前を入力します。テーブルマップ名には、最大 64 の英数字を使用できます。 パケットマーキング カテゴリを指定したが、テーブルマップを指定していない場合、デフォルト アクションは、パケットマーキング カテゴリに関連付けられた値を優先順位値としてコピーすることです。たとえば、**set precedence cos** コマンドを入力する場合、CoS 値（パケットマーキング カテゴリ）がコピーされ、precedence 値として使用されます。

qos-group	後でパケットを分類するために使用できる QoS グループ ID を割り当てます。 • *qos-group-value*：分類されたトラフィックに QoS 値を設定します。指定できる範囲は 0 ～ 31 です。一般的に使用する値に対してはニーモニック名を入力することもできます。 • **dscp**：パケットの元の DSCP フィールド値を QoS グループ値として設定します。 • **precedence**：パケットの元の precedence フィールド値を QoS グループ値として設定します。 • （任意）**table** *table-map-name*：DSCP 値または優先順位値の設定に使用される指定されたテーブル マップに設定されている値を示します。値の指定に使用されるテーブル マップの名前を入力します。テーブル マップ名には、最大 64 の英数字を使用できます。 パケットマーキング カテゴリ（**dscp** または **precedence**）を指定したが、テーブル マップを指定していない場合、デフォルト アクションは、パケットマーキング カテゴリに関連付けられた値を QoS グループ値としてコピーすることです。たとえば、**set qos-group precedence** コマンドを入力する場合、precedence 値（パケットマーキング カテゴリ）がコピーされ、QoS グループ値として使用されます。

wlan user-priority *wlan-user-priority*	分類されたトラフィックにWLANユーザープライオリティを割り当てます。次の値を指定できます。 • *wlan-user-priority*：分類されたトラフィックにWLAN ユーザー プライオリティを設定します。指定できる範囲は 0 ～ 7 です。 • **cos**：レイヤ2CoSフィールド値をWLANユーザー プライオリティとして設定します。 • **dscp**：DSCP フィールド値を WLAN ユーザープライオリティとして設定します。 • **precedence**：precedenceフィールド値をWLANユーザー プライオリティとして設定します。 • **wlan**WLAN ユーザー プライオリティ フィールド値をWLANユーザープライオリティとして設定します。 • （任意）**table** *table-map-name*：WLAN ユーザー プライオリティ値の設定に使用される指定されたテーブル マップに設定されている値を示します。値の指定に使用されるテーブル マップの名前を入力します。テーブル マップ名には、最大 64 の英数字を使用できます。 パケットマーキング カテゴリを指定したが、テーブルマップを指定していない場合、デフォルトアクションは、パケットマーキング カテゴリに関連付けられた値をWLANユーザープライオリティとしてコピーすることです。たとえば、**set wlan user-priority cos** コマンドを入力する場合、CoS 値（パケットマーキング カテゴリ）がコピーされ、WLANユーザー プライオリティとして使用されます。

コマンド デフォルト

トラフィックの分類は定義されていません。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが
	cos、**dscp**、**qos** た。

使用上のガイドライン

set dscp *dscp-value* コマンド、**set cos** *cos-value* コマンド、および **set ip precedence** *precedence-value* コマンドの場合は、一般に使用されている値のニーモニック名を入力できます。たとえば、**set dscp af11** コマンドを入力すると、**set dscp 10** コマンドを入力した場合と同じになります。**set ip precedence critical** コマンドを入力すると、**set ip precedence 5** コマンドを入力した場合と同じになります。サポートされているニーモニックの一覧を表示するには、**set dscp ?** または **set ip precedence ?** コマンドを入力して、コマンドラインのヘルプ文字列を参照してください。

set dscp cos コマンドを設定する場合は、CoS 値が 3 ビット フィールドで、DSCP 値は 6 ビット フィールドであり、CoS フィールドの 3 ビットのみが使用される点に注意してください。

set dscp qos-group コマンドを設定する場合は、次の点に注意してください。

- DSCP 値の有効な範囲は 0 ～ 63 の数字です。QoS グループの有効値の範囲は 0 ～ 99 です。
- QoS グループの値が両方の値の範囲内の場合（たとえば、44）、パケットマーキング値がコピーされ、パケットがマーク付けされます。
- QoS グループの値が DSCP の範囲を超える場合（たとえば、77）、パケットマーキング値はコピーされず、パケットはマーク付けされません。アクションは実行されません。

ポリシー マップ コンフィギュレーション モードでサービス ポリシーを作成し、インターフェイスまたは ATM 仮想回線（VC）にサービス ポリシーを付加するまで、**set qos-group** コマンドは適用できません。

ポリシーマップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

例

次の例では、ポリサーが設定されていないすべての FTP トラフィックに DSCP 値 10 を割り当てる方法を示します。

```
デバイス(config)# policy-map policy_ftp
デバイス(config-pmap)# class-map ftp_class
デバイス(config-cmap)# exit
デバイス(config)# policy policy_ftp
デバイス(config-pmap)# class ftp_class
デバイス(config-pmap-c)# set dscp 10
デバイス(config-pmap)# exit
```

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

set trace capwap ap ha

ワイヤレス アクセス ポイントの制御およびプロビジョニングのハイ アベイラビリティを追跡するには、**set trace capwap ap ha** コマンドを使用します。

set trace capwap ap ha [{**detail** | **event** | **dump** | {**filter** [{**none** [**switch** *switch*] | *filter_name* [*filter_value* [**switch** *switch*]]}] | **filtered***switch***level** {**default***trace_level*} [**switch** *switch*]}}]

構文の説明

detail	（任意）ワイヤレス CAPWAP HA の詳細を指定します。
event	（任意）ワイヤレス CAPWAP HA イベントを指定します。
dump	（任意）ワイヤレス CAPWAP HA の出力を指定します。
filter *mac*	MAC アドレスを指定します。
switch switch number	スイッチ番号を指定します。
none	（任意）フィルタ オプションを指定しません。
switch *switch*	（任意）device番号を指定します。
filter name	適用されたフラグ フィルタ名を追跡します。
filter_value	（任意）フィルタの値。
switch *switch*	（任意）device番号を指定します。
filtered	フィルタ処理されたトレース メッセージを指定します。
switch	スイッチ番号を指定します。
level	トレース レベルを指定します。
default	解除されたトレース レベル値を指定します。
trace_level	トレース レベルを指定します。
switch *switch*	（任意）device番号を指定します。

コマンド デフォルト

なし

コマンド履歴

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

次に、ワイヤレス CAPWAP HA を表示する例を示します。

```
デバイス# set trace capwap ap ha detail filter mac WORD switch number
```

set trace mobility ha

内のワイヤレス モビリティ ハイ アベイラビリティをデバッグするには、**set trace mobility ha** コマンドを使用します。

set trace mobility ha [{**event** | **detail** | **dump**}] {**filter**[**mac** *WORD switch switch number*] [{**none** [**switch** *switch*] | *filter_name* [*filter_value* [**switch** *switch*]]}] | **level** {**default***trace_level*} [**switch** *switch*]{**filtered***switch*}}

構文の説明

event	（任意）ワイヤレス モビリティ ハイ アベイラビリティのイベントを指定します。
detail	（任意）ワイヤレス モビリティ ハイ アベイラビリティの詳細を指定します。
dump	（任意）ワイヤレス モビリティ ハイ アベイラビリティの出力を指定します。
filter	トレース適用フラグ フィルタを指定します。
mac	MACアドレスを指定します。
WORD switch	スイッチを指定します。
switch number	スイッチ番号を指定します。値の範囲は 1 ～ 4 です。
none	トレース適用フラグ フィルタを指定しません。
switch *switch*	（任意）device番号を指定します。
filter_name	適用されたフラグ フィルタ名を追跡します。
filter_value	適用されたフラグ フィルタの値を追跡します。
switch *switch*	device番号を指定します。
level	トレース レベル値を指定します。

default	解除されたトレース レベル値を指定します。
trace_level	トレース レベル値を指定します。
switch *switch*	device番号を指定します。
filtered	フィルタ処理されたトレースメッセージを指定します。
switch	スイッチを指定します。

コマンド デフォルト

なし

コマンド履歴

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

次に、ワイヤレスモビリティハイアベイラビリティの詳細を表示する例を示します。

```
デバイス# set trace mobility ha detail filter mac WORD
[08/27/13 10:38:35.349 UTC 1 8135] Invalid src ip: 169.254.1.1
[08/27/13 10:38:35.349 UTC 2 8135] Invalid sysIp: Skip plumbing MC-MA
tunnels.
[08/27/13 10:38:54.393 UTC 3 8135] Mobility version mismatch, v10
received, or m
sglen mismatch msglen=74 recvBytes=0, dropping
```

set trace qos ap ha

ワイヤレス Quality of Service（QoS）ハイ アベイラビリティを追跡するには、**set trace qos ap ha** コマンドを使用します。

set trace QOS ap ha [{**event** | **error**}] {**filter** [{**MACnone** [**switch** *switch*] | *filter_name* [*filter_value* [**switch** *switch*]]}] | **level** {**default***trace_level*} [**switch** *switch*]}

構文の説明

event	（任意）トレース QoS ワイヤレス AP イベントを指定します。
event *mac*	AP の MAC アドレスを指定します。
event *none*	MAC アドレス値を指定しません。
error	（任意）トレース QoS ワイヤレス AP エラーを指定します。
error *mac*	AP の MAC アドレスを指定します。
error *none*	値を指定しません。
filter	トレース適用フラグ フィルタを指定します。
filter *mac*	AP の MAC アドレスを指定します。
filter *none*	値を指定しません。
switch *switch*	スイッチ番号を指定します。
filter_name	（任意）スイッチ フィルタの名前を指定します。
filter_value	（任意）スイッチ フィルタの値を指定します。値は 1 です。
switch *switch*	（任意）スイッチ番号を指定します。値は 1 です。
level	トレース レベルを指定します。
default	トレース QoS ワイヤレス AP デフォルトを指定します。
trace_level	トレース レベルです。
switch *switch*	（任意）スイッチ番号を指定します。値は 1 です。

コマンド デフォルト

なし

コマンド履歴

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

次に、ワイヤレス QoS ハイ アベイラビリティを追跡する例を示します。

デバイス# **set trace QOS ap ha**

sgt-tag

ファブリック プロファイルに SGT タグを設定するには、**sgt-tag** コマンドを使用します。

sgt-tag *value*

構文の説明

value	SGT タグ値。有効な範囲は 2 ～ 65519 です。

コマンド デフォルト

デフォルトの SGT タグ値は 0 です。

コマンド モード

config-wireless-fabric

コマンド履歴

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

例

次に、SGT タグを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile fabric fabric-profile-name
Device(config-wireless-fabric)# sgt tag 8
```

site-tag

サイト タグを AP にマッピングするには、**site-tag** コマンドを使用します。

site-tag *site-tag-name*

構文の説明

site-tag-name	サイト タグの名前。

コマンド デフォルト

なし

コマンド モード

config-ap-tag

コマンド履歴

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

使用上のガイドライン

このコマンドを実行すると、AP は、接続解除されたのち再参加します。

例

次に、サイト タグを設定する例を示します。

```
Device(config-ap-tag)# site-tag sitetag1
```

snmp-server group

新しい Simple Network Management Protocol（SNMP）グループを設定するには、グローバル コンフィギュレーション モードで **snmp-server group** コマンドを使用します。指定した SNMP グループを削除するには、このコマンドの **no** 形式を使用します。

snmp-server group *group-name* {**v1** | **v2c** | **v3** } [**access** [**ipv6** *named-access-list*] [{*acl-numberacl-name*}]] [**context** *context-name*] [**notify** *notify-view*] [**read** *read-view*] [**write** *write-view*]
no snmp-server group *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*]

構文の説明

group-name	グループの名前。
v1	グループが SNMPv1 セキュリティ モデルを使用していることを指定します。SNMPv1 は、最も安全性の低い SNMP セキュリティ モデルです。
v2c	グループが SNMPv2c セキュリティ モデルを使用していることを指定します。 SNMPv2c セキュリティ モデルでは、インフォームを送信でき、64 文字の文字列がサポートされています。
v3	グループが SNMPv3 セキュリティ モデルを使用していることを指定します。 SMNPv3 は、サポートされているセキュリティ モデルの中で最も安全です。SMNPv3 では、認証特性を明示的に設定できます。
context	（任意）この SNMP グループとそのビューと関連付ける SNMP コンテキストを指定します。
context-name	（任意）コンテキスト名。
read	（任意）SNMP グループの読み取りビューを指定します。このビューでは、エージェントのコンテンツのみを表示できます。
read-view	（任意）ビューの名前である最大 64 文字の文字列。 デフォルトでは、**read** オプションを使用してこの状態を上書きしない限り、読み取りビューはインターネットオブジェクト識別子（OID）のスペース（1.3.6.1）に属するすべてのオブジェクトであるとみなされます。
write	（任意）SNMP グループの書き込みビューを指定します。このビューでは、データを入力してエージェントのコンテンツを設定できます。
write-view	（任意）ビューの名前である最大 64 文字の文字列。 デフォルトでは、書き込みビュー（つまり、ヌル OID）には何も定義されていません。書き込みアクセスを設定する必要があります。

notify	（任意）SNMP グループの通知ビューを指定します。このビューでは、通知、インフォーム、またはトラップを指定できます。
notify-view	（任意）ビューの名前である最大 64 文字の文字列。 デフォルトでは、**snmp-server host** コマンドが設定されるまで、通知ビュー（つまり、ヌル OID）には何も定義されていません。ビューを **snmp-server group** コマンドで指定した場合、生成されるそのビューのすべての通知は、グループに関連付けられているすべてのユーザに送信されます（そのユーザに対して SNMP サーバホストの設定が存在する場合）。 シスコでは、ソフトウェアに通知ビューを自動生成させることを推奨しています。このドキュメントの「通知ビューの設定」の項を参照してください。
access	（任意）グループに関連付ける標準アクセス コントロール リスト（ACL）を指定します。
ipv6	（任意）IPv6 名前付きアクセス リストを指定します。IPv6 と IPv4 の両方のアクセス リストが示されている場合は、IPv6 名前付きアクセス リストがリストの最初に表示されている必要があります。
named-access-list	（任意）IPv6 アクセス リストの名前。
acl-number	（任意）*acl-number* 引数は、以前に設定された標準アクセス リストを識別する 1 ～ 99 の整数です。
acl-name	（任意）*acl-name* 引数は、以前に設定された標準アクセス リストの名前である最大 64 文字の文字列です。

コマンド デフォルト

SNMP サーバ グループは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1s	このコマンドは、Cisco IOS XE Amsterdam 17.1.1s よりも前のリリースで導入されました。

使用上のガイドライン

コミュニティ ストリングが内部的に設定されている場合、public という名前の 2 つのグループが自動生成されます。1 つは v1 セキュリティ モデル用、もう 1 つは v2c セキュリティ モデル用です。同様に、コミュニティ ストリングを削除すると、public という名前の v1 グループと public という名前の v2c グループが削除されます。

snmp-server group コマンドを設定する際、認証やプライバシーアルゴリズムにはデフォルト値はありません。また、デフォルトのパスワードも存在しません。Message Digest 5（MD5）パスワードの指定については、**snmp-server user** コマンドのドキュメントを参照してください。

通知ビューの設定

notify view オプションは、2 つの目的に使用できます。

- グループにSNMPを使用して設定された通知ビューがあり、その通知ビューを変更する必要がある。
- **snmp-server host** コマンドは、**snmp-server group** コマンドの前に設定されている可能性があります。この場合、**snmp-server host** コマンドを再設定するか、または適切な通知ビューを指定する必要があります。

次の理由から、SNMP グループを設定する際に通知ビューを指定することは推奨されていません。

- **snmp-server host** コマンドによってユーザに対して自動生成された通知ビューを、そのユーザに関連付けられているグループに追加する。
- グループの通知ビューを変更すると、そのグループに対応付けられたすべてのユーザが影響を受けます。

snmp-server group コマンドの一部としてグループの通知ビューを指定する代わりに、指定された順序で次のコマンドを使用します。

1. **snmp-server user** ：SNMP ユーザーを設定します。
2. **snmp-server group** ：通知ビューを追加しないで SNMP グループを設定します。
3. **snmp-server host** ：トラップ操作の受信者を指定して、通知ビューを自動生成します。

SNMP コンテキスト

SNMP コンテキストによって、MIB データにアクセスする安全な方法が VPN ユーザに提供されます。VPN がコンテキストに関連付けられると、VPN 固有の MIB データがそのコンテキストに存在します。VPN をコンテキストに関連付けると、サービス プロバイダーが、複数 VPN でネットワークを管理できます。コンテキストを作成してVPNに関連付けることにより、サービス プロバイダーは、ある VPN のユーザが同じネットワーキング デバイス上で他の VPN のユーザに関する情報にアクセスするのを防ぐことができます。

読み取り、書き込み、または通知 SNMP ビューを SNMP コンテキストに関連付けるには、**context** *context-name* キーワードおよび引数とともにこのコマンドを使用します。

SNMP グループの作成

次の例は、SNMPサーバグループ「public」を作成して、すべてのオブジェクトに対して標準名前付きアクセスリスト「lmnop」のメンバへの読み取り専用アクセスを許可する方法を示しています。

```
Device(config)# snmp-server group public v2c access lmnop
```

SNMP サーバグループの削除

次の例に、設定から SNMP サーバグループ「public」を削除する方法を示します。

```
Device(config)# no snmp-server group public v2c
```

SNMP サバ グループと指定されたビューとの関連付け

次の例に、SNMPv2c グループ「GROUP1」のビューに関連付けられた SNMP コンテキスト「A」を示します。

```
Device(config)# snmp-server context A
Device(config)# snmp mib community commA
Device(config)# snmp mib community-map commA context A target-list commAVpn
Device(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify
viewB
```

snmp-server subagent cache

Simple Network Management Protocol（SNMP）ポーリング中にコントローラで CPU スパイクが発生しないようにするには、**snmp-server subagent cache** コマンドを使用します。サブエージェントキャッシュを無効にするには、このコマンドの **no** 形式を使用します。

snmp-server subagent cache [**timeout** *seconds*]

snmp-server subagent cache [**timeout** *seconds*]

構文の説明

timeout	サブエージェントキャッシュのタイムアウトを指定します。
seconds	サーバーのタイムアウト値（秒単位）。有効な値の範囲は 1 ～ 100 で、デフォルトは 60 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Dublin 17.11.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、定期的にキャッシュをクリアすることで、コントローラの CPU スパイクを防止します。

例

次に、SNMP ポーリング中にコントローラで CPU スパイクが発生しないようにする例を示します。

```
Device# configure terminal
Device(config)# snmp-server subagent cache
```

software auto-upgrade enable

自動アップグレード機能を有効にするには、**software auto-upgrade enable** コマンドを使用します。

（注） このコマンドの **no** 形式を使用してこの機能を無効にした場合は、特権 EXEC モードで **install autoupgrade** コマンドを使用して、手動で自動アップグレードする必要があります。

software auto-upgrade enable

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

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

使用上のガイドライン

次に、自動アップグレード機能を有効にする例を示します。

```
Device# configure terminal
Device(config)# software auto-upgrade enable
Device(config)# end
```

source-interface

コントローラと通信するように送信元インターフェイスを設定するには、**source-interface** コマンドを使用します。送信元インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

source-interface *interface-name interface-number*

no source-interface

構文の説明

interface-name	インターフェイスの名前。
interface-number	インターフェイス番号。

コマンド デフォルト

送信元インターフェイスは設定されていません。

コマンド モード

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

コマンド履歴

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

例

次に、コントローラと通信するように送信元インターフェイスを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# avc sd-service
Device(config-sd-service)# controller
Device(config-sd-service-controller)# source-interface vlan 12
```

static-ip-mobility

静的 IP モビリティを設定するには、ワイヤレスポリシー コンフィギュレーション モードで **static-ip-mobility** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

static-ip-mobility

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ワイヤレスポリシー コンフィギュレーション モード

コマンド履歴

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

例

次に、静的 IP モビリティを有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless profile policy test-policy
Device(config-wireless-policy)# static-ip-mobility
```

statistics ap-system-monitoring alarm-enable

AP のリアルタイム統計（CPU とメモリ）のアラームを有効にするには、**statistics ap-system-monitoring alarm-enable** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

[no] statistics ap-system-monitoring alarm-enable

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring alarm-enable	AP のリアルタイム統計（CPU とメモリ）のアラームを有効にします。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、AP のリアルタイム統計（CPU とメモリ）のアラームを有効にする例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring alarm-enable
```

statistics ap-system-monitoring alarm-hold-time

アラームをトリガーするまでの保留時間間隔を定義するには、**statistics ap-system-monitoring alarm-hold-time** コマンドを使用します。

statistics ap-system-monitoring alarm-hold-time *0-3600*

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring alarm-hold-time	APのリアルタイム統計（CPUとメモリ）のアラームを有効にします。
0-3600	アラーム保留時間間隔を秒単位で指定します。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、アラームをトリガーするまでの保留時間間隔を定義する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring alarm-hold-time 60
```

statistics ap-system-monitoring alarm-retransmit-time

トラップアラームの再送信間隔を定義するには、**statistics ap-system-monitoring alarm-retransmit-time** を使用します

statistics ap-system-monitoring alarm-retransmit-time *0-65535*

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring alarm-retransmit-time	トラップアラームの再送信間隔を定義します。
0-65535	トラップアラームの再送信間隔（秒単位）を指定します。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、トラップアラームの再送信間隔を定義する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring alarm-retransmit-time 60
```

statistics ap-system-monitoring cpu-threshold

アラームをトリガーする、AP の CPU 使用量のしきい値パーセンテージを定義するには、**statistics ap-system-monitoring cpu-threshold** コマンドを使用します。

statistics ap-system-monitoring cpu-threshold *0-100*

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring cpu-threshold	アラームをトリガーする AP の CPU 使用量のしきい値を定義します。
0-100	アラームをトリガーする AP の CPU 使用量のしきい値のパーセンテージを指定します。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、アラームをトリガーする AP の CPU 使用量のしきい値パーセンテージを定義する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring cpu-threshold 70
```

statistics ap-system-monitoring enable

AP のリアルタイム統計（CPU とメモリ）のモニタリングを有効にするには、**statistics ap-system-monitoring enable** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

[no] statistics ap-system-monitoring enable

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring enable	AP のリアルタイム統計（CPU とメモリ）のモニタリングを有効にします。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、AP のリアルタイム統計（CPU とメモリ）のモニタリングを有効にする例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring enable
```

statistics ap-system-monitoring mem-threshold

アラームをトリガーする AP のメモリ使用量のしきい値パーセンテージを定義します。

statistics ap-system-monitoring mem-threshold *0-100*

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring mem-threshold	アラームをトリガーする AP のメモリ使用量のしきい値を定義します。
0-100	アラームをトリガーするAPのメモリ使用量のしきい値のパーセンテージを指定します。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、アラームをトリガーする AP のメモリ使用量のしきい値パーセンテージを定義する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring mem-threshold 60
```

statistics ap-system-monitoring sampling-interval

サンプリング間隔を定義するには、**statistics ap-system-monitoring sampling-interval** を使用します

statistics ap-system-monitoring sampling-interval *2-900*

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring sampling-interval	サンプリング間隔を定義します。
2-900	サンプリング間隔を秒単位で指定します。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、サンプリング間隔を定義する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring sampling-interval 100
```

statistics ap-system-monitoring stats-interval

統計間隔を定義するには、**statistics ap-system-monitoring stats-interval** を使用します。これにより、計算において、最後の統計間隔秒間に受信した統計に、より多くの重みが与えられます

statistics ap-system-monitoring stats-interval *120-900*

構文の説明

statistics	AP 統計を設定します。
ap-system-monitoring stats-interval	統計間隔を定義します。これにより、計算において、最後の統計間隔秒間に受信した統計に、より多くの重みが与えられます。
120-900	統計間隔を秒単位で指定します。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、統計間隔を定義する例を示します。

```
Device(config)# ap profile default-ap-profile
Device(config-ap-profile)# statistics ap-system-monitoring stats-interval 120
```

stopbits

コンソール ポートのストップ ビットを設定するには、**stopbits** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

stopbits { *1* | *2* }

no stopbits { *1* | *2* }

構文の説明

1	1 ストップ ビットを指定します。
2	2 ストップ ビットを指定します。

コマンド デフォルト

1 ストップ ビット

コマンド モード

ライン コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

コンソール ポートは、コンソール ポート上のセッションからのみ設定できます。

例

次に、コンソールポートのストップビットを設定する例を示します。

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# stopbits 1
```

switchport

レイヤ 3 モードになっているインターフェイスをレイヤ 2 設定用のレイヤ 2 モードに配置するには、インターフェイス コンフィギュレーション モードで **switchport** コマンドを使用します。インターフェイスをレイヤ 3 モードに配置するには、このコマンドの **no** 形式を使用します。

switchport
no switchport

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、すべてのインターフェイスがレイヤ 2 モードです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

インターフェイスをルーテッドインターフェイスの状態に設定して、レイヤ 2 の設定をすべて削除するには、**no switchport** コマンド（パラメータの指定なし）を使用します。このコマンドは、ルーテッド ポートに IP アドレスを割り当てる前に使用する必要があります。

（注） このコマンドは、LAN Base 機能セットを実行している devices ではサポートされません。

no switchport コマンドを入力するとポートがシャットダウンされて、その後再び有効になります。その際に、ポートの接続先のデバイスでメッセージが生成されることがあります。

レイヤ 2 モードからレイヤ 3 モード（またはその逆）にインターフェイスを変更すると、影響を受けたインターフェイスに関連する以前の設定情報が失われる可能性があり、インターフェイスがデフォルト設定に戻ります。

（注） インターフェイスがレイヤ 3 インターフェイスとして設定されている場合、最初に **switchport** コマンドを入力して、そのインターフェイスをレイヤ 2 ポートとして設定する必要があります。その後、**switchport access vlan** コマンドおよび **switchport mode** コマンドを入力します。

switchport コマンドは、シスコ ルーテッド ポートをサポートしないプラットフォームでは使用できません。このようなプラットフォーム上のすべての物理ポートは、レイヤ 2 のスイッチド インターフェイスとして想定されます。

インターフェイスのポート ステータスを確認するには、**show running-config** 特権 EXEC コマンドを入力します。

例

次の例では、インターフェイスをレイヤ 2 ポートとして運用することを中止し、シスコのルーテッド ポートにする方法を示します。

```
デバイス(config-if)# no switchport
```

次の例では、ポートのインターフェイスをシスコのルーテッドポートとして運用することを中止し、レイヤ 2 のスイッチドインターフェイスに変更する方法を示します。

```
デバイス(config-if)# switchport
```

switchport access vlan

ポートをスタティック アクセス ポートとして設定するには、インターフェイス コンフィギュレーション モードで **switchport access vlan** コマンドを使用します。device のアクセス モードをデフォルトの VLAN モードにリセットするには、このコマンドの **no** 形式を使用します。

switchport access vlan {*vlan-id*}
no switchport access vlan

構文の説明

vlan-id	アクセス モード VLAN のVLAN ID。範囲は 1 ~ 4094。

コマンド デフォルト

デフォルトのアクセス VLAN およびトランク インターフェイス ネイティブ VLAN は、プラットフォームまたはインターフェイス ハードウェアに対応したデフォルト VLAN です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

switchport access vlan コマンドを有効にするには、事前にポートをアクセス モードにする必要があります。

スイッチポートのモードが **access vlan** *vlan-id* に設定されている場合、ポートは指定された VLAN のメンバとして動作します。アクセス ポートを割り当てることができるのは、1 つの VLAN だけです。

no switchport access コマンドを使用すると、アクセス モード VLAN がデバイスに適したデフォルト VLAN にリセットされます。

例

次の例では、アクセス モードで動作するスイッチド ポート インターフェイスが、デフォルト VLAN ではなく VLAN 2 で動作するように変更します。

```
デバイス(config-if)# switchport access vlan 2
```

switchport mode

ポートの VLAN メンバーシップモードを設定するには、インターフェイス コンフィギュレーション モードで **switchport mode** コマンドを使用します。モードをデバイスに適したデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

switchport mode {**access** | **dynamic** | {**auto** | **desirable**} | **trunk**}
noswitchport mode {**access** | **dynamic** | {**auto** | **desirable**} | **trunk**}

構文の説明

access	ポートをアクセス モードに設定します（**switchport access vlan** インターフェイス コンフィギュレーション コマンドの設定に応じて、スタティック アクセスまたはダイナミック アクセスのいずれか）。ポートは無条件にアクセスするように設定され、非カプセル化（タグなし）フレームを送受信する単一の非トランク VLAN インターフェイスとして動作します。アクセス ポートを割り当てることができるのは、1 つの VLAN だけです。
dynamic auto	ポート トランキング モードのダイナミック パラメータを auto に設定して、インターフェイスがリンクをトランク リンクに変換するように指定します。これがデフォルトのスイッチポート モードになります。
dynamic desirable	ポート トランキング モードのダイナミック パラメータを desirable に設定して、インターフェイスがリンクをトランク リンクにアクティブに変換するように指定します。
trunk	ポートを無条件にトランクに設定します。ポートはトランキング VLAN レイヤ 2 インターフェイスです。ポートは、送信元の VLAN を識別するカプセル化（タグ付き）フレームを送受信します。トランクは、2 つの devices 間、または device とルータ間のポイントツーポイント リンクです。

コマンド デフォルト

デフォルト モードは **dynamic auto** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

（注） **dot1q-tunnel** キーワードは、CLI のインターフェイス ヘルプに表示されますが、サポートされていません。

access または **trunk** キーワードによる設定が有効となるのは、**switchport mode** コマンドを使用して適切なモードでポートを設定した場合のみです。スタティック アクセスおよびトランクの設定は保存されますが、同時にアクティブにできるのはいずれかの設定だけです。

access モードを開始すると、インターフェイスは永続的な非トランキング モードになり、隣接インターフェイスがリンクから非トランク リンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

trunk モードを開始すると、インターフェイスは永続的なトランキング モードになり、接続先のインターフェイスがリンクからトランク リンクへの変換に合意しない場合でも、この変換を行うようにネゴシエートします。

dynamic auto モードを開始すると、隣接インターフェイスが **trunk** または **desirable** モードに設定された場合に、インターフェイスはリンクをトランク リンクに変換します。

dynamic desirable モードを開始すると、隣接インターフェイスが **trunk**、**desirable**、または **auto** モードに設定された場合に、インターフェイスはトランク インターフェイスになります。

トランキングを自動ネゴシエーションするには、インターフェイスが同じ VLAN トランキング プロトコル（VTP）ドメインに存在する必要があります。トランク ネゴシエーションは、ポイントツーポイント プロトコルである Dynamic Trunking Protocol（DTP）によって管理されます。ただし、一部のインターネットワーキング デバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。この問題を避けるには、DTP をサポートしないデバイスに接続されたインターフェイスが DTP フレームを転送しないように設定し、DTP をオフにします。

- これらのリンク上でトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスへのトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

アクセス ポートとトランク ポートは、互いに排他的な関係にあります。

IEEE 802.1X 機能は、次の方法でスイッチポート モードに作用します。

- トランク ポートで IEEE 802.1X をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1X 対応ポートのモードをトランクに変更しようとしても、ポート モードは変更されません。
- ポート設定で IEEE 802.1X を **dynamic auto** または **dynamic desirable** にイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1X 対応ポートのモードを **dynamic auto** または **dynamic desirable** に変更しようとしても、ポート モードは変更されません。
- ダイナミック アクセス（VLAN Query Protocol（VQP））ポートで IEEE 802.1X をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1X はイネーブルになりません。IEEE 802.1X 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。

設定を確認するには、**show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力して、*Administrative Mode* 行と *Operational Mode* 行の情報を調べます。

例

次の例では、ポートをアクセス モードに設定する方法を示します。

```
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# switchport mode access
```

次の例では、ポートを dynamic desirable モードに設定する方法を示します。

```
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# switchport mode dynamic desirable
```

次の例では、ポートをトランク モードに設定する方法を示します。

```
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# switchport mode trunk
```

tag rf

AP フィルタのポリシー タグを設定するには、**tag rf** コマンドを使用します。

tag rf *rf-tag*

構文の説明

rf-tag	RF タグ名。

コマンド デフォルト

なし

コマンド モード

config-ap-filter

コマンド履歴

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

例

次に、AP フィルタのポリシー タグを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name ap-filter-name
Device(config-ap-filter)# rf tag rf-tag-name
```

tag site

AP フィルタのサイト タグを設定するには、**tag site** *site-tag* コマンドを使用します。

tag site *site-tag*

構文の説明

site-tag	サイト タグの名前。

コマンド デフォルト

なし

コマンド モード

config-ap-filter

コマンド履歴

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

例

次に、AP フィルタのサイト タグを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap filter name ap-filter-name
Device(config-ap-filter)# site tag site-tag-name
```

terms-conditions

Access Network Query Protocol（ANQP）サーバーの利用規約パラメータを設定するには、**terms-conditions** コマンドを使用します。利用規約を無効にするには、このコマンドの **no** 形式を使用します。

terms-conditions {**filename** *filename* | **timestamp** *date time* | **urlfilter list** *url-filter-list*}

構文の説明

filename	利用規約ファイルの名前。
date	yyyy-mm-dd形式のタイムスタンプ日付。
time	hh:mm:ss 形式のタイムスタンプ時刻。
url-filter-list	URL フィルタリストの名前。

コマンド デフォルト

利用規約は設定されていません。

コマンド モード

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

コマンド履歴

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

例

次に、タイムスタンプを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# terms-conditions timestamp 2020-02-20 20:20:20
```

tertiary (ap prime)

AP フォールバック用のターシャリコントローラを設定するには、**tertiary** コマンドを使用します。AP プライミングに使用されないようにターシャリコントローラを削除するには、このコマンドの **no** 形式を使用します。

tertiary *controller-name ip-address*

no tertiary *controller-name ip-address*

構文の説明

controller-name	ターシャリコントローラの名前。
ip-address	コントローラの IPv4 または IPv6 アドレス。

コマンド デフォルト

なし

コマンド モード

AP プライム コンフィギュレーション（config-priming）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.2	このコマンドが導入されました。

例

次に、AP フォールバック用のターシャリコントローラを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile ap priming Prime-FX
Device(config-priming)# tertiary cccc 209.165.201.4
```

timezone delta

AP のタイムゾーンオフセットを設定するには、**timezone delta** コマンドを使用します。AP のタイムゾーンオフセットを削除するには、**no timezone** コマンドを使用します。

timezone delta hour *offset-hour* **minute** *offset-minute*

構文の説明

hour *offset-hour*	協定世界時（UTC）からのローカル時間の差。有効な範囲は -12 ～ 14 です。
minute *offset-minute*	UTC からのローカル分の差。有効な範囲は 0 ～ 59 です。

コマンド デフォルト

AP のタイムゾーンは設定されていません。

コマンド モード

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

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

使用上のガイドライン

AP タイムゾーンは、AP プロファイルごとにのみ設定できます。AP ごとに AP タイムゾーンを設定することはできません。タイムゾーンを設定するには、現在のコントローラのタイムゾーンまたは時差を適用します。デフォルトでは、タイムゾーンは無効になっています。

例

次に、AP のタイムゾーンオフセットを設定する例を示します。

```
Device# configure terminal
Device(config)# ap profile test
Device(config-ap-profile)# timezone delta hour -12 minute 2
```

timezone use-controller

コントローラのタイムゾーンを使用して AP のタイムゾーンを設定するには、**timezone use-controller** コマンドを使用します。コントローラのタイムゾーンを削除するには、**no timezone** コマンドを使用します。

timezone use-controller

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

AP のタイムゾーンは設定されていません。

コマンド モード

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

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

使用上のガイドライン

AP タイムゾーンは、AP プロファイルごとにのみ設定できます。AP ごとにタイムゾーンを設定することはできません。タイムゾーンを設定するには、現在のコントローラのタイムゾーンを適用するか、時差を使用します。デフォルトでは、タイムゾーンは無効になっています。

例

次に、コントローラのタイムゾーンを使用して AP のタイムゾーンを設定する例を示します。

```
Device# configure terminal
Device(config)# ap profile test
Device(config-ap-profile)# timezone use-controller
```

transport application-updates

コントローラと通信するためのトランスポートプロトコルを設定するには、**transport** コマンドを使用します。コントローラと通信するために使用するトランスポートプロトコルを無効にするには、このコマンドの **no** 形式を使用します。

transport application-updates { **http** | **https** } **url-prefix** *url-prefix-name*

no transport application-updates

構文の説明

http	HTTP プロトコルを有効にします。
https	HTTPS プロトコルを有効にします。
url-prefix	アプリケーション更新のURLプレフィックスを有効にします。
url-prefix-name	URL プレフィックス名。

コマンド デフォルト

トランスポート通信プロトコルは設定されていません。

コマンド モード

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

コマンド履歴

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

使用上のガイドライン

アプリケーション更新のトランスポートプロトコルは、Cisco DNA Center でのみ使用されます。

例

次に、コントローラと通信するためのトランスポートプロトコルを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# avc sd-service
Device(config-sd-service)# controller
Device(config-sd-service-controller)# transport application-updates https url-prefix
cisco
```

transition-disable

移行の無効化を有効にするには、**transition-disable** コマンドを使用します。

transition-disable

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

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

使用上のガイドライン

次に、移行の無効化を有効にする例を示します。

```
Device# configure terminal
Device(config)# wlan WPA3 1 WPA3
Device(config-wlan)# transition-disable
Device(config-wlan)# end
```

trapflags ap ap-stats

統計がしきい値を超えたときに送信される AP 関連のトラップの送信を有効または無効にするには、**trapflags ap ap-stats** を使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

[no] trapflags ap ap-stats

構文の説明

trapflags	AP 関連のトラップフラグの送信を有効または無効にします。
ap ap-stats	統計がしきい値を超えたときに送信されるトラップを指定します。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、AP 関連のトラップの送信を有効または無効にする例を示します。

```
Device# configure terminal
Device(config)# trapflags ap ap-stats
```

trapflags ap broken-antenna

サポートされているCiscoアクセスポイントでアンテナ障害が発生したときに送信されるSNMPトラップを有効にするには、**trapflags ap broken-antenna** コマンドを使用します。SNMP トラップを無効にするには、このコマンドの **no** 形式を使用します。

trapflags ap broken-antenna

no trapflags ap broken-antenna

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

SNMP トラップは有効になっていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

アンテナは、A、B、C、D、E、F、G、H などの文字でコード化されます。Inter-Access Point Protocol（IAPP）レポートに故障したアンテナの文字が含まれていて、syslog と SNMP トラップにコピーされます。

例

次に、故障したアンテナの SNMP トラップを有効にする例を示します。

```
Device# configure terminal
Device(config)# trapflags ap broken-antenna
```

trusted-port

あるポートを信頼できるポートとして設定するには、IPv6 スヌーピング ポリシー モードまたは ND インスペクション ポリシー コンフィギュレーション モードで **trusted-port** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

trusted-port
no trusted-port

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

どのポートも信頼されていません。

コマンド モード

ND インスペクション ポリシーの設定

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

trusted-port コマンドをイネーブルにすると、メッセージがこのポリシーを持つポートで受信された場合、限定的に実行されるか、まったく実行されません。ただし、アドレス スプーフィングから保護するために、メッセージは伝送するバインディング情報の使用によってバインディングテーブルを維持できるように分析されます。これらのポートで検出されたバインディングは、信頼できるものとして設定されていないポートから受信したバインディングよりも信頼性が高いものと見なされます。

次に、NDP ポリシー名を policy1 と定義し、スイッチを NDP インスペクション ポリシー コンフィギュレーション モードにし、ポートを信頼するように設定する例を示します。

```
デバイス(config)# ipv6  nd inspection  policy1
デバイス(config-nd-inspection)# trusted-port
```

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、ポートを信頼するように設定する例を示します。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)# trusted-port
```

tunnel eogre source

トンネル送信元について特定のトンネル単位の設定が存在しない場合にトンネル送信元インターフェイスを設定するには、**tunnel eogre source** コマンドを使用します。

tunnel eogre source {**gigabitethernet** | **loopback** | **vlan**} *interface-number*

構文の説明

interface-number	インターフェイス番号。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

トンネル送信元について特定のトンネル単位の設定が存在する場合は、それが使用されます。

例

次に、トンネル送信元インターフェイスを設定する例を示します。

```
Device(config)# tunnel eogre source vlan 21
```

tunnel eogre heartbeat

トンネル キープアライブ ハートビートの ping パラメータを設定するには、**tunnel eogre heartbeat** コマンドを使用します。

tunnel eogre heartbeat {**interval** *interval* | **max-skip-count** *tolerable-heartbeats*}

構文の説明

interval	ハートビート間隔（秒）。
tolerable-heartbeats	許容されるドロップされたハートビート。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

例

次に、トンネル キープアライブ ハートビートの ping パラメータを設定する例を示します。

```
Device(config)# tunnel eogre heartbeat 80
```

tunnel mode ethernet

トンネルのカプセル化方式を Ethernet over GRE に設定するには、**tunnel mode ethernet** コマンドを使用します。

tunnel mode ethernet {**gre** {**ipv4** | **ipv6**} [**p2p**] | **manual**}

構文の説明

gre	Ethernet over GRE。
l2tpv3	L2TPv3 カプセル化。
p2p	IPv4 または IPv6 を介したポイントツーポイント カプセル化を提供します。
manual	L2TP パラメータを手動で設定します。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドは、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースで導入されました。
Cisco IOS XE Gibraltar 16.11.1	**p2p** キーワードが導入されました。

例

次に、トンネルのカプセル化方式を Ethernet over GRE に設定する例を示します。

```
Device(config-if)# tunnel mode ethernet gre ipv4 p2p
```

tunnel eogre domain

EoGRE 冗長ドメインを設定するには、**tunnel eogre domain** コマンドを使用します。

tunnel eogre domain *domain-name*

構文の説明

domain-name	ドメイン名。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

例

次に、EoGRE 冗長ドメインを設定する例を示します。

```
Device(config)# tunnel eogre domain domain1
```

tunnel eogre interface tunnel

EoGRE トンネル インターフェイスの AAA プロキシ キーを設定するには、**tunnel eogre interface tunnel** コマンドを使用します。

tunnel eogre interface tunnel *tunnel-inft-number* **aaa proxy key** {**0** | **8**} *key-string* **auth-port** *auth_port* **acct-port** *acct_port*

構文の説明

tunnel-inft-number	トンネル インターフェイスの番号。
aaa	AAA の設定
proxy	AAA プロキシの設定。
key	AAA プロキシ キーの設定。 0：文字列を暗号化されていないキーとして指定します。 8：文字列を AES 暗号化キーとして指定します。
key-string	キーの文字列。
auth-port *auth_port*	認証ポート番号。
acct-port *acct_port*	アカウンティング用のポート番号。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.1	このコマンドが変更されました。次のキーワードと変数が追加されました。 **auth-port***auth_port* **acct-port***acct_port*

例

次に、EoGRE トンネル インターフェイスのプロキシ キーを設定する例を示します。

```
Device(config)# tunnel eogre interface tunnel 21 aaa proxy key 0 test
```

次に、AAA ポートを変更する例を示します。

```
Device(config)# tunnel eogre interface Tunnel1 aaa proxy key 0 test
 auth-port 24 acct-port 36
```

tunneled-eap-credential

トンネル化 Extensible Authentication Protocol（EAP）クレデンシャル認証を設定するには、**tunneled-eap-credential** コマンドを使用します。トンネル化 EAP クレデンシャル認証を削除するには、このコマンドの **no** 形式を使用します。

tunneled-eap-credential {**anonymous** | **certificate** | **hw-token** | **nfc** | **sim** | **softoken** | **username-password** | **usim**}

構文の説明

anonymous	匿名認証。
certificate	証明書を使用する認証。
hw-token	ハードウェアトークンを使用する認証。
nfc	近距離無線通信（NFC）を使用する認証。
sim	SIM カードを使用する認証。
softoken	ソフトトークンを使用する認証。
username-password	ユーザー名とパスワードを使用する認証。
usim	USIM を使用する認証。

コマンド デフォルト

なし

コマンド モード

ANQP NAI EAP 認証（config-anqp-nai-eap-aut）

コマンド履歴

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

例

次に、トンネル化 EAP クレデンシャル認証を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless hotspot anqp-server my_anqp
Device(config-wireless-anqp-server)# nai-realm myvenue.cisco.com
Device(config-anqp-nai-eap)# eap-method eap-aka
Device(config-anqp-nai-eap-auth)# tunneled-eap-credential anonymous
```

type

1 つ以上のファイルの内容を表示するには、ブートローダモードで **type** コマンドを使用します。

type *filesystem:/file-url...*

構文の説明

filesystem:	ファイルシステムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。USB メモリスティックには **usbflash0:** を使用します。
/file-url...	表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

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

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

ファイルのリストを指定すると、各ファイルの内容が順次表示されます。

例

次に、ファイルの内容を表示する例を示します。

```
デバイス: type flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

udp-timeout

UDP セッションのタイムアウトを設定するには、**udp-timeout** コマンドを使用します。

udp-timeout *timeout_value*

構文の説明

timeout_value	UDP セッションのタイムアウト値です。 範囲は 1 ～ 30 秒です。 （注） *public-key* および *resolver* パラメータマップ オプションには、デフォルト値が自動的に入力されます。したがって、変更する必要はありません。

コマンド デフォルト

なし

コマンド モード

プロファイル コンフィギュレーション

コマンド履歴

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

例

次に、UDP セッションのタイムアウト値を設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# parameter-map type umbrella global
デバイス(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166
デバイス(config-profile)# local-domain dns_wl
デバイス(config-profile)# udp-timeout 2
デバイス(config-profile)# end
```

umbrella-param-map

WLAN の Umbrella OpenDNS 機能を設定するには、**umbrella-param-map** コマンドを使用します。

umbrella-param-map *umbrella-name*

構文の説明

umbrella-name

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

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

例

次に、WLAN の Umbrella OpenDNS 機能を設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless profile policy default-policy-profile
デバイス(config-wireless-policy)# umbrella-param-map global
デバイス(config-wireless-policy)# end
```

update-timer

Flex プロファイルの mDNS 更新タイマーを設定するには、**update-timer** コマンドを使用します。このコマンドを無効にするには、このコマンドの **no** 形式を使用します。

update-timer { **service-cache** *<1-100>* | **statistics** *<1-100>* }

update-timer { **service-cache** *<1-100>* | **statistics** *<1-100>* }

構文の説明

update-timer	Flex プロファイルの mDNS 更新タイマーを設定します。
service-cache *<1-100>*	Flex プロファイルの mDNS 更新のサービスキャッシュタイマーを指定します。デフォルト値は 1 分です。
statistics *<1-100>*	Flex プロファイルの mDNS 更新の統計タイマーを指定します。デフォルト値は 1 分です。

コマンド デフォルト

なし

コマンド モード

mDNS Flex プロファイル コンフィギュレーション

コマンド履歴

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

例

次に、Flex プロファイルの mDNS 更新タイマーを設定する例を示します。

```
Device(config-mdns-flex-prof)# update-timer service-cache 20
```

url

Hotspot 2.0 の施設の URL を設定するには、**url** コマンドを使用します。Hotspot 2.0 の施設の URL を削除するには、このコマンドの **no** 形式を使用します。

url *url*

構文の説明

url	施設名の URL。

コマンド デフォルト

施設の URL は設定されていません。

コマンド モード

ワイヤレス ANQP 施設コンフィギュレーション（config-anqp-venue-name）

コマンド履歴

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

例

次に、Hotspot 2.0 の施設の URL を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# venue test eng
Device(config-anqp-venue-name)#url www.cisco.com
```

username

SSH を使用して Cisco ISE-3315 にアクセスできるユーザを追加するには、コンフィギュレーション モードで **username** コマンドを使用します。ユーザがすでに存在する場合は、このコマンドを使用してパスワード、特権レベル、または両方を変更します。システムからユーザを削除するには、このコマンドの **no** 形式を使用します。

[no] username *username* **password** {**hash** | **plain**} *password* **role** {**admin** | **user**] [**disabled** [**email** email-address]] [**email** email-address]

既存のユーザに対しては、以下のコマンド オプションを使用します。

username username **password role** {admin | **user**} password

構文の説明

username	1 つの単語のみを入力する必要があります。ハイフン（-）、アンダースコア（_）、およびピリオド（.）を含めることができます。 （注）　初期セットアップでは英数字のみが許可されます。
password	パスワードおよびユーザ ロールを指定するために使用するコマンド。
password	パスワード。40 文字までの英数字で指定します。パスワードは、すべての新規ユーザに指定する必要があります。
hash | plain	パスワードのタイプ。最大 34 文字の英数字。
role admin | user	ユーザの権限レベルを設定します。
[disabled]	ユーザの電子メール アドレスに従って、ユーザをディセーブルにします。
email *email-address*	ユーザのメール アドレス。たとえば、user1@example.com です。
wlan-profile-name	WLAN プロファイルの詳細を表示します。

コマンド デフォルト

設定時の初期ユーザです。

コマンド モード

コンフィギュレーション

使用上のガイドライン

username コマンドでは、username および password キーワードの後に、hash | plain and the admin | user オプションを指定する必要があります。

例 1

```
ncs/admin(config)# username admin password hash ###### role admin
ncs/admin(config)#
```

例 2

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin
ncs/admin(config)#
```

例 3

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin email
admin123@example.com
ncs/admin(config)#
```

venue

802.11u 施設情報を設定するには、**venue** コマンドを使用します。施設を削除するには、このコマンドの **no** 形式を使用します。

venue *venue-name language-code*［*venue-url*］

構文の説明

venue-name	施設の名前。 220 文字を超えないようにする必要があります。
language-code	オペレータの 3 文字の言語コード。言語コードには、言語の最初の 3 文字のみを小文字で使用します。たとえば、英語の場合は *eng* を使用します。 言語コードの完全なリストについては、http://www.loc.gov/standards/iso639-2/php/code_list.php を参照してください。
venue-url	施設の URL。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、802.11u 施設情報を設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# venue test eng cisco.com
```

vnid

サービス テンプレートに VXLAN ネットワーク ID（VNID）を追加するには、**vnid** コマンドを使用します。

vnid *vnid-name*

構文の説明

vnid-name	VNID の名前。

コマンド デフォルト

VNID は設定されていません。

コマンド モード

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

コマンド履歴

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

例

次に、VNID を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# service-template template
Device(config-service-template)# vnid  vnid-name
```

violation

定期的な再評価でのストリーム違反ポリシーを設定するには、**violation** コマンドを使用します。

violation {**drop** | **fallback**}

構文の説明

パラメータ	説明
drop	ストリームが定期的な再評価でドロップされます。
fallback	ストリームが定期的な再評価でBestEffortクラスに降格されます。

コマンド デフォルト

なし

コマンド モード

config-media-stream

コマンド履歴

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

例

次に、定期的な再評価でのストリーム違反ポリシーを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream group my-media-group 224.0.0.0 224.0.0.223
Device(config-media-stream)# violation drop
```

vlan

VLAN を追加して、VLAN コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **vlan** コマンドを使用します。VLAN を削除するには、このコマンドの **no** 形式を使用します。

vlan { *vlan-id* | **accounting** { **input** | **output** } | **configuration** *vlan-id* | **group** *word* **vlan-list** *vlan-id* | **internal allocation policy** { **ascending** | **descending** } }
no vlan *vlan-id*

構文の説明

vlan-id	追加および設定する VLAN の ID。指定できる範囲は 1 ～ 4094 です。1 つの VLAN ID、それぞれをカンマで区切った一連の VLAN ID、またはハイフンを間に挿入した VLAN ID の範囲を入力できます。
group *word* **vlan-list**	VLAN グループの作成をイネーブルにします。VLAN グループ名は最大 32 文字であり、文字で始める必要があります。
accounting	VLAN アカウンティング設定。
configuration	詳細なサービスパラメータの VLAN 機能コンフィギュレーション モード。同じ設定に対して 1 つ以上の VLAN を作成できます。*id* は VLAN 設定 ID を示しています。たとえば、1-10 や 15 などです。
internal	内部 VLAN 割り当てポリシー。昇順または降順にすることができます。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

次に、VLAN を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# vlan 12
```

vlan configuration

VLAN 機能を設定するため VLAN コンフィギュレーション モードを開始するには、**vlan configuration** コマンドを使用します。

vlan configuration

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、VLAN ID が 2 の場合に、VLAN 機能を設定するために VLAN コンフィギュレーション モードを開始する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# vlan configuration 2
```

vlan access-map

VLAN パケット フィルタリング用の VLAN マップ エントリを作成または修正し、VLAN アクセスマップ コンフィギュレーション モードに変更するには、スイッチ スタックまたはスタンドアロン スイッチ上で、グローバル コンフィギュレーション モードで **vlan access-map** コマンドを使用します。VLAN マップ エントリを削除するには、このコマンドの **no** 形式を使用します。

vlan access-map *name* [*number*]
no vlan access-map *name* [*number*]

（注） このコマンドは、LAN ベース フィーチャ セットを実行しているスイッチではサポートされません。

構文の説明

name	VLAN マップ名
number	（任意）作成または変更するマップ エントリのシーケンス番号（0 ～ 65535）。VLAN マップを作成する際にシーケンス番号を指定しない場合、番号は自動的に割り当てられ、10から開始して10ずつ増加します。この番号は、VLANアクセスマップ エントリに挿入するか、またはVLAN アクセス マップ エントリから削除する順番です。

コマンド デフォルト

VLAN に適用する VLAN マップ エントリまたは VLAN マップはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

グローバル コンフィギュレーション モードでは、このコマンドは VLAN マップを作成または修正します。このエントリは、モードを VLAN アクセス マップ コンフィギュレーションに変更します。**match** アクセス マップ コンフィギュレーション コマンドを使用して、照合する IP または非 IP トラフィックのアクセス リストを指定できます。また、**action** コマンドを使用して、この照合によりパケットを転送またはドロップするかどうかを設定します。

VLAN アクセス マップ コンフィギュレーション モードでは、次のコマンドが利用できます。

- **action**：実行するアクションを設定します（転送またはドロップ）。
- **default**：コマンドをデフォルト値に設定します。
- **exit**：VLAN アクセス マップ コンフィギュレーション モードを終了します。

- **match**：照合する値を設定します（IP アドレスまたは MAC アドレス）。
- **no**：コマンドを無効にするか、デフォルト値を設定します。

エントリ番号（シーケンス番号）を指定しない場合、マップの最後に追加されます。

VLAN ごとに VLAN マップは 1 つだけ設定できます。VLAN マップは、VLAN でパケットを受信すると適用されます。

シーケンス番号を指定して **no vlan access-map** *name* [*number*] コマンドを使用すると、エントリを個別に削除できます。

VLAN マップを 1 つまたは複数の VLAN に適用するには、**vlan filter** インターフェイス コンフィギュレーション コマンドを使用します。

VLANマップエントリの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

次の例では、vac1 という名の VLAN マップを作成し、一致条件とアクションをその VLAN マップに適用する方法を示します。他のエントリがマップに存在しない場合、これはエントリ 10 になります。

```
デバイス(config)# vlan access-map vac1
デバイス(config-access-map)# match ip address acl1
デバイス(config-access-map)# action forward
```

次の例では、VLAN マップ vac1 を削除する方法を示します。

```
デバイス(config)# no vlan access-map vac1
```

vlan encryption osen

アソシエーションおよび認証プロセス中に単一の SSID で Online Subscription with Encryption（OSEN）暗号化を選択するときにクライアントが使用する VLAN を指定するには、**vlan encryption osen** コマンドを使用します。VLAN ID を削除するには、このコマンドの **no** 形式を使用します。

vlan-id *vlan-id* **encryption osen**

構文の説明

vlan-id	VLAN 識別番号。

コマンド デフォルト

VLAN ID は設定されていません。

コマンド モード

ワイヤレス ポリシーの設定（config-wireless-policy）

コマンド履歴

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

例

次に、アソシエーションおよび認証プロセス中に単一の SSID で OSEN 暗号化を選択するときにクライアントが使用する VLAN を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile policy rr-xyz-policy-1
Device(config-wireless-policy)# vlan 10 encryption osen
```

vlan filter

1 つ以上の VLAN に VLAN マップを適用するには、スイッチ スタックまたはスタンドアロン スイッチ上で、グローバル コンフィギュレーション モードで **vlan filter** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

vlan filter *mapname* **vlan-list** {*list* | **all**}
no vlan filter *mapname* **vlan-list** {*list* | **all**}

（注） このコマンドは、LAN ベース フィーチャ セットを実行しているスイッチではサポートされません。

構文の説明

mapname	VLAN マップ エントリ名
vlan-list	マップを適用する VLAN を指定します。
リスト	tt、uu-vv、xx、および yy-zz 形式での 1 つまたは複数の VLAN リスト。カンマとダッシュの前後のスペースは任意です。指定できる範囲は 1 ～ 4094 です。
all	マップをすべての VLAN に追加します。

コマンド デフォルト

VLAN フィルタはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

パケットを誤って過剰にドロップし、設定プロセスの途中で接続が無効になることがないように、VLAN アクセス マップを完全に定義してから VLAN に適用することを推奨します。

VLANマップエントリの詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

次の例では、VLAN マップ エントリ map1 を VLAN 20 および 30 に適用します。

```
デバイス(config)# vlan filter map1 vlan-list 20, 30
```

次の例では、VLAN マップ エントリ map1 を VLAN 20 から削除する方法を示します。

```
デバイス(config)# no vlan filter map1 vlan-list 20
```

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

vlan group

VLANグループを作成または変更するには、グローバルコンフィギュレーションモードで**vlan group**コマンドを使用します。VLANグループからVLANリストを削除するには、このコマンドの**no**形式を使用します。

vlan group *group-name* **vlan-list** *vlan-list*
no vlan group *group-name* **vlan-list** *vlan-list*

構文の説明

group-name	VLANグループの名前。名前は最大32文字で、文字から始める必要があります。
vlan-list *vlan-list*	VLANグループに追加される1つ以上のVLANを指定します。*vlan-list*引数には単一のVLAN ID、VLAN IDのリスト、またはVLAN IDの範囲を指定できます。複数のエントリはハイフン（-）またはカンマ（,）で区切ります。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

指定されたVLANグループが存在しない場合、**vlan group**コマンドはグループを作成し、指定されたVLANリストをそのグループにマッピングします。指定されたVLANグループが存在する場合は、指定されたVLANリストがそのグループにマッピングされます。

vlan groupコマンドの**no**形式を使用すると、指定されたVLANリストがVLANグループから削除されます。VLANグループから最後のVLANを削除すると、そのVLANグループは削除されます。

最大100のVLANグループを設定でき、1つのVLANグループに最大4094のVLANをマッピングできます。

次に、VLAN 7 ～ 9と11をVLANグループにマッピングする例を示します。

```
デバイス(config)# vlan group group1 vlan-list 7-9,11
```

次の例では、VLANグループからVLAN 7を削除する方法を示します。

```
デバイス(config)# no vlan group group1 vlan-list 7
```

vlan-id

FlexConnectプロファイルVLANIDを設定するには、**vlan-id**コマンドを使用します。FlexConnectプロファイル VLAN ID を削除するには、このコマンドの **no** 形式を使用します。

vlan-id *vlan-id*

構文の説明

vlan-id	VLAN 識別番号。

コマンド デフォルト

VLAN ID は設定されていません。

コマンド モード

ワイヤレス Flex プロファイル VLAN コンフィギュレーション（config-wireless-flex-profile-vlan）

コマンド履歴

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

例

次に、Flex プロファイル VLAN ID を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# vlan-name test
Device(config-wireless-flex-profile-vlan)#vlan-id 12
```

vlan-name

FlexConnectプロファイルVLANを設定するには、**vlan-name** コマンドを使用します。FlexConnectプロファイル VLAN を削除するには、このコマンドの **no** 形式を使用します。

vlan-name

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

VLAN は設定されていません。

コマンド モード

ワイヤレス Flex プロファイル コンフィギュレーション（config-wireless-flex-profile）

コマンド履歴

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

例

次に、FlexConnect プロファイル VLAN を設定する例を示します。

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

vrf

仮想ルーティングおよび転送（VRF）ラベルを有効にするには、**vrf** コマンドを使用します。VRF ラベルを削除するには、このコマンドの **no** 形式を使用します。

vrf *vrf-name*

no vrf

構文の説明

vrf-name	VRF の名前。

コマンド デフォルト

VRF ラベルは有効になっていません。

コマンド モード

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

コマンド履歴

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

例

次に、VRF ラベルを有効にする例を示します。

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

wan-metrics

Hotspot 2.0 WAN メトリックを設定するには、**wan-metrics** コマンドを使用します。WAN を削除するには、このコマンドの **no** 形式を使用します。

wan-metrics
{**downlink-load**|**downlink-speed**|**full-capacity-link**|**link-status**{**down**|**not-configured**|**test-state**|**up**}|**load-measurement-duration**|**uplink-load**|**uplink-speed**}

構文の説明

downlink-load	WAN ダウンリンク負荷を設定します。有効な範囲は 0 ～ 255 です。値は線形的にスケーリングされ、255 が 100% を表します。
downlink-speed	WAN のダウンリンク速度（kbps 単位）を設定します。有効な範囲は 0 ～ 4294967295 です。
full-capacity-link	WAN リンクを最大容量で運用します。
link-status	WAN リンクステータスを設定します。 次のオプションがあります。 • **down**：リンク ダウン • **not-configured**：リンクが設定されていません。 • **test-state**：リンクはテスト状態です。 • **up**：リンクがアップしています。
load-measurement-duration	アップリンクまたはダウンリンク負荷の測定期間を設定します。有効な範囲は 0 ～ 65535 です。
uplink-load	WAN アップリンク負荷を設定します。有効な範囲は 0 ～ 255 です。値は線形的にスケーリングされ、255 が 100% を表します。
uplink-speed	WAN のアップリンク速度（kbps 単位）を設定します。有効な範囲は 0 ～ 4294967295 です。

コマンド デフォルト

なし

コマンド モード

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

コマンド履歴

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

例

次に、Hotspot 2.0 WAN アップリンク速度を設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server
Device(config-wireless-anqp-server)# wan-metrics uplink-load 23
```

webauth-http-enable

グローバル パラメータ マップ パラメータ モードで Web 認証用の HTTP サーバーを有効にするには、**webauth-http-enable** を使用します。このコマンドを無効にするには、このコマンドの **no** 形式を使用します。

webauth-http-enable

no webauth-http-enable

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル パラメータ マップ モード

コマンド履歴

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

例

次に、Web 認証用の HTTP サーバーを有効にする例を示します。

```
Device(config-params-parameter-map)# webauth-http-enable
```

wgb broadcast-tagging

ワイヤレス ポリシー プロファイルで WGB ブロードキャスト タギングを設定するには、**wgb broadcast-tagging** コマンドを使用します。

wgb broadcast-tagging

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

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

例

次に、ワイヤレス ポリシー プロファイルで WGB ブロードキャスト タギングをイネーブルにする例を示します。

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

wgb vlan

WLAN ポリシー プロファイルで WGB VLAN クライアントのサポートを設定するには、**wgb vlan** コマンドを使用します。

wgb vlan

コマンド デフォルト

なし

コマンド モード

config-wireless-policy

コマンド履歴

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

例

次に、*wlan1-policy-profile* という名前の WLAN ポリシー プロファイルで WGB VLAN クライアントのサポートを有効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy wlan1-policy-profile
Device(config-wireless-policy)# wgb vlan
```

whitelist acl

ホワイトリスト ACL を設定するには、**whitelist acl** コマンドを使用します。

whitelist acl {*standard_acl_value* | *extended_acl_value* | *acl_name*}

構文の説明

standard_acl_value	標準アクセス リストを指定します。範囲は 1 ～ 199 です。
extended_acl_value	拡張アクセス リストを指定します。範囲は1300 ～ 2699 です。
acl_name	名前付きアクセス リストを指定します。

コマンド デフォルト

なし

コマンド モード

ET-Analytics コンフィギュレーション

コマンド履歴

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

次に、ET-Analytics コンフィギュレーション モードで非アクティブタイマーを有効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# et-analytics
デバイス(config-et-analytics)# whitelist acl
eta-whitelist
デバイス((config-et-analytics)# ip access-list
extended eta-whitelist
デバイス(config-ext-nacl)# permit udp any any eq tftp
デバイス(config-ext-nacl)# end
```

wired-vlan-range

mDNS サービス検出を実行する有線 VLAN を設定するには、**wired-vlan-range** コマンドを使用します。このコマンドを無効にするには、このコマンドの **no** 形式を使用します。

wired-vlan-range *wired-vlan-range-value*

構文の説明

wired-vlan-range	mDNS サービス検出を実行する有線 VLAN を設定します。
wired-vlan-range-value	有線 VLAN の範囲値を指定します。

コマンド デフォルト

なし

コマンド モード

mDNS Flex プロファイル コンフィギュレーション

コマンド履歴

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

例

次に、mDNS サービス検出を実行する有線 VLAN を設定する例を示します。

```
Device(config-mdns-flex-prof)# wired-vlan-range range-value
```

config wlan assisted-roaming

WLAN で経由ローミングを設定するには、**config wlan assisted-roaming** コマンドを使用します。

config wlan assisted-roaming {**neighbor-list** | **dual-list** | **prediction**} {**enable** | **disable**} *wlan_id*

構文の説明

neighbor-list	WLAN の 802.11k ネイバー リストを設定します。
dual-list	WLAN のデュアル バンド 802.11k ネイバー リストを設定します。デフォルトは、クライアントが現在関連付けられている帯域です。
prediction	WLAN の経由ローミング最適化の予測を設定します。
enable	WLAN の設定をイネーブルにします。
disable	WLAN の設定をディセーブルにします。
wlan_id	1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

すべての WLAN で 802.11k ネイバー リストが有効です。

デフォルトでは、ネイバー リスト機能が WLAN に対してイネーブルな場合に、デュアル バンド リストはイネーブルになります。

使用上のガイドライン

経由ローミングの予測のリストをイネーブルにすると、警告が表示されます。また、WLAN でロードバランシングがすでにイネーブルになっている場合、ロードバランシングはその WLAN でディセーブルになります。

次に、WLAN の 802.11k ネイバー リストをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan assisted-roaming neighbor-list enable 1
```

wireless aaa policy

ワイヤレス AAA ポリシーを設定するには、**wireless aaa policy** コマンドを使用します。

wireless aaa policy *aaa-policy*

構文の説明

aaa-policy	ワイヤレスAAAポリシーの名前。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、*aaa-policy-test* という名前のワイヤレス AAA ポリシーを設定する例を示します

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

wireless aaa policy

新しい AAA ポリシーを設定するには、**wireless aaa policy** コマンドを使用します。

wireless aaa policy *aaa-policy-name*

構文の説明

aaa-policy-name	AAA ポリシー名。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、AAA ポリシー名を設定する例を示します。

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

wireless autoqos policy-profile

実行可能なコマンドを使用して AutoQoS ワイヤレスポリシーを有効にするには、**autoqos** コマンドを使用します。ワイヤレス AutoQos を無効にするには、**disable** コマンドを使用します。

wireless autoqos policy-profile*policy-profile-name* **default_policy_profile mode** { **clear** | **enterprise-avc** | **fastlane** | **guest** | **voice** }

wireless autoqos disable

構文の説明

autoqos	ワイヤレス AutoQoS を設定します。
mode	ワイヤレス AutoQoS モードを指定します。
enterprise-avc	AutoQos ワイヤレス企業 AVC ポリシーを有効にします。
clear	設定されているワイヤレスポリシーをクリアします。
fastlane	AutoQos fastlane ポリシーを有効にします。これにより、2.4GHz または 5GHz の 802.11 ネットワークが無効化および有効化されます。
guest	AutoQos ワイヤレスゲストポリシーを有効にします。
voice	AutoQos ワイヤレス音声ポリシーを有効にします。これにより、2.4GHz または 5GHz の 802.11 ネットワークが無効化および有効化されます。

コマンド デフォルト

なし

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.2s	このコマンドが導入されました。

例

次に、AutoQoS ワイヤレス企業ポリシーを有効にする例を示します。

```
Device# wireless autoqos policy-profile default-policy-profile mode enterprise-avc
```

wireless broadcast vlan

VLAN 上でブロードキャストのサポートをイネーブルにするには、グローバル コンフィギュレーション モードで **wireless broadcast vlan** コマンドを使用します。イーサネット ブロードキャストのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

wireless broadcast vlan ［*vlan-id*］
no wireless broadcast vlan ［*vlan-id*］

構文の説明

vlan-id	（任意） VLAN ID を指定して、その VLAN に対するブロードキャスト サポートをイネーブルにします。値の範囲は 1 ～ 4095 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

このコマンドは、グローバル コンフィギュレーション モードのみで使用してください。

次の例では、VLAN 20 でブロードキャスティングをイネーブルにする方法を示します。

```
デバイス(config)# wireless broadcast vlan 20
```

wireless client

クライアントパラメータを設定するには、グローバルコンフィギュレーションモードで**wireless client** コマンドを使用します。

wireless client {**association limit** *assoc-number* **interval** *interval* | **band-select** {**client-mid-rssi** *rssi* | **client-rssi** *rssi* | **cycle-count** *count* | **cycle-threshold** *threshold* | **expire dual-band** *timeout* | **expire suppression** *timeout*} | **fast-ssid-change** | **max-user-login** *max-user-login* | **notification** {**interval** *time* | **join-failure aaathreshold***percentage* | **roam-failure threshold** *percentage*} | **timers auth-timeout** *seconds* | **user-timeout** *user-timeout*}

構文の説明

association limit *assoc-number* **interval** *interval*	所定の間隔での 1 つのアクセス ポイント スロットあたりの関連付け要求制限を有効にし、関連付け要求制限間隔を設定します。 所定の間隔での 1 つのアクセス ポイント スロットあたりの関連付け要求の数は、1 ~ 100 の範囲で設定できます。 クライアント関連付け要求制限間隔は、100 ~ 10000 ミリ秒の範囲で設定できます。
band-select	クライアントのバンド選択オプションを設定します。
client-mid-rssi *rssi*	バンド選択のクライアント Mid-RSSI のしきい値を設定します。 プローブに応答するためのクライアント RSSI の最小 dBm は、-90 ～ -20 です。
client-rssi *rssi*	バンド選択のクライアント受信信号強度インジケータ（RSSI）しきい値を設定します。 プローブに応答するためのクライアント RSSI の最小 dBm は、-90 ～ -20 です。
cycle-count *count*	バンド選択プローブ周期カウントを設定します。 周期カウントは、1 ～ 10 の範囲で設定できます。
cycle-threshold *threshold*	新規スキャン周期の時間しきい値を設定します。 周期しきい値は、1 ～ 1000 ミリ秒の範囲で設定できます。
expire dual-band *timeout*	特定のクライアントを 5 GHz 帯域にプッシュする試行を停止するまでのタイムアウトを設定します。 タイムアウトは 10 ～ 300 秒の範囲で設定できます。デフォルト値は 60 秒です。

expire suppression *timeout*	既知のデュアルバンド クライアントが失効してプルーニングされるまでの時間を設定します。 抑止時間は 10 ～ 200 秒の範囲で設定できます。デフォルトのタイムアウト値は 20 秒です。
fast-ssid-change	モバイル端末で高速 SSID の変更を有効にします。
max-user-login *max-user-login*	ユーザのログイン セッションの最大数を設定します。
notification	通知を設定します。
interval *time*	インターバルの通知を設定します。 有効な時間は 1 ～ 1440 秒です。
join-failure aaa threshold *percentage*	クライアントの参加の失敗に関する通知を設定します。 アラートをトリガーするしきい値をパーセンテージで設定できます。有効なしきい値のパーセンテージは 1 ～ 100 です。
roam-failure threshold *percentage*	クライアントのローミング障害に関する通知を設定します。 通知のしきい値を設定できます。有効なしきい値のパーセンテージは 1 ～ 100 です。
timers auth-timeout *seconds*	クライアント タイマーを設定します。
user-timeout *user-timeout*	アイドル クライアント タイムアウトを設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.10.1	このコマンドが変更されました。**client-mid-rssi**、**notification**、および **fast-ssid-change** の各キーワードが追加されました。**user-timeout** キーワードが削除されました。

次に、帯域幅選択のプローブ サイクルカウントを 8 に設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless client band-select cycle-count 8
デバイス(config)# end
```

次に、しきい値が 700 ミリ秒の新しいスキャン サイクルの時間のしきい値を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless client band-select cycle-threshold 700
デバイス(config)# end
```

次に、70 秒後にデュアルバンド データベースのデュアルバンド クライアントを抑止する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless client band-select expire suppression 70
デバイス(config)# end
```

wireless client client-steering client-count

ワイヤレスクライアントでクライアントステアリングの最小クライアント数を設定するには、**wireless client client-steering client-count** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

wireless client client-steering client-count *0-200*

no wireless client client-steering client-count

構文の説明

0-200	クライアントステアリングの最小クライアント数を指定します。値の範囲は 0 ～ 200 クライアントです。デフォルト値は 3 クライアントです。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

例

次に、クライアントステアリングの最小クライアント数を設定する例を示します。

```
Device(config)# wireless client client-steering client-count 25
```

wireless client client-steering min-rssi-24ghz

2.4 GHz でのクライアントステアリングの最小 RSSI しきい値を設定するには、**wireless client client-steering min-rssi-24ghz -70** コマンドを使用します。この機能をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

wireless client client-steering min-rssi-24ghz -70

no wireless client client-steering min-rssi-24ghz -70

構文の説明

-70	2.4 GHz でのクライアントステアリングの最小 RSSI しきい値を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

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

例

次に、2.4 GHz でのクライアントステアリングの最小 RSSI しきい値を設定する例を示します。

```
Device(config)# wireless client client-steering min-rssi-24ghz -70
```

wireless client client-steering min-rssi-5ghz

5 GHz でのクライアントステアリングの最小 RSSI しきい値を設定するには、**wireless client client-steering min-rssi-5ghz** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

wireless client client-steering min-rssi-5ghz -75

no wireless client client-steering min-rssi-5ghz -75

構文の説明

-75	5 GHz でのクライアントステアリングの最小 RSSI しきい値を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

例

次に、5 GHz でのクライアントステアリングの最小 RSSI しきい値を設定する例を示します。

```
Device(config)# wireless client client-steering min-rssi-5ghz -75
```

wireless client client-steering util-threshold

クライアントステアリングの最大使用率の差を設定するには、**wireless client client-steering util-threshold** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

wireless client client-steering util-threshold *0-100*

no wireless client client-steering util-threshold

構文の説明

0-100	クライアントステアリングの最大使用率の差を指定します。値の範囲は 0 ～ 100 のパーセンテージです。デフォルト値は 20 パーセントです。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

例

次に、クライアントステアリングの最大使用率の差を設定する例を示します。

```
Device(config)# wireless client client-steering util-threshold 20
```

wireless client client-steering window-size

ワイヤレスクライアントでクライアントステアリングの最小ウィンドウサイズを設定するには、**wireless client client-steering window-size** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

wireless client client-steering window-size *0-200*

no wireless client client-steering window-size

構文の説明

0-200	クライアント ステアリング ウィンドウの最小サイズを指定します。値の範囲は 0 ～ 200 クライアントです。デフォルト値は 3 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

例

次に、クライアントステアリングの最小ウィンドウサイズを設定する例を示します。

```
Device(config)# # wireless client client-steering window-size 25
```

wireless ipv6 client

クライアントの IPv6 を有効にするには、**wireless ipv6 client** コマンドを使用します。クライアントの IPv6 を無効にするには、このコマンドの **no** 形式を使用します。

wireless ipv6 client

no wireless ipv6 client

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

デフォルトでは、IPv6 は有効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

コントローラでクライアントが入力および出力した、すべてのクライアント IPv6 トラフィックがドロップされます。そのため、ローカルモードのみに制限されます。IPv6 が無効になっている場合、クライアントは IPv6 アドレスを取得しません。この設定は、設定変更が行われた後に関連付けまたは参加するクライアントにのみ影響します。既存のクライアントは影響を受けません。

例

次に、クライアントの IPv6 を有効にする例を示します。

```
Device(config)# wireless ipv6 client
```

wireless client ip-address deauthenticate

ワイヤレスクライアントを IP アドレスに基づいて認証解除するには、**wireless client ip-address deauthenticate** コマンドを使用します。

wireless client ip-address *ip-address* **deauthenticate**

構文の説明

ip-address	クライアント IP アドレス。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、IP アドレスに基づいてワイヤレスクライアントを認証解除する例を示します。

```
Device# wireless client ip-address 10.2.2.2 deauthenticate
```

wireless client mac-address

ワイヤレス クライアントの設定を構成するには、グローバル コンフィギュレーション モードで **wireless client mac-address** コマンドを使用します。

wireless client mac-address *mac-addr* **ccx** {**clear-reports** | **clear-results** | **default-gw-ping** | **dhcp-test** | **dns-ping** | **dns-resolve hostname** *host-name* | **get-client-capability** | **get-manufacturer-info** | **get-operating-parameters** | **get-profiles** | **log-request** {**roam** | **rsna** | **syslog**} | **send-message** *message-id* | **stats-request** *measurement-duration* {**dot11** | **security**} | **test-abort** | **test-association** *ssid bssid dot11 channel* | **test-dot1x** [*profile-id*] *bssid dot11 channel* | **test-profile** {**any***profile-id*}}

構文の説明

mac-addr	クライアントの MAC アドレス。
ccx	Cisco Client Extension（CCX）。
clear-reports	クライアント レポートの情報をクリアします。
clear-results	コントローラのテスト結果をクリアします。
default-gw-ping	デフォルト ゲートウェイ pingテストの実行要求をクライアントに送信します。
dhcp-test	DHCP テストの実行要求をクライアントに送信します。
dns-ping	ドメイン ネーム システム（DNS）サーバ IP アドレス ping テストの実行要求をクライアントに送信します。
dns-resolve hostname *host-name*	指定されたホスト名に対するドメイン ネーム システム（DNS）解決テストの実行要求をクライアントに送信します。
get-client-capability	クライアントにその機能情報を送信するよう指示する要求を送信します。
get-manufacturer-info	製造元の情報を送信するよう指示する要求をクライアントに送信します。
get-operating-parameters	クライアントに現在の動作パラメータを送信するよう指示する要求を送信します。
get-profiles	クライアントにプロファイルを送信するよう指示する要求を送信します。
log-request	指定されたクライアント デバイスに対する CCX ログ要求を設定します。
roam	（任意）クライアント CCX ローミング ログを指定する要求を指定します。

rsna	（任意）クライアント CCX RSNA ログを指定する要求を指定します。
syslog	（任意）クライアント CCX システム ログを指定する要求を指定します。

send-message *message-id*

メッセージをクライアントに送ります。

次のいずれかを含むメッセージ タイプ。

- 1：SSID が無効です。
- 2：ネットワーク設定が無効です。
- 3：WLAN の信頼性に不一致があります。
- 4：ユーザの資格情報が間違っています。
- 5：サポートにお問い合わせください。
- 6：問題は解決されました。
- 7：問題は解決されていません。
- 8：もう一度後で作業を行ってください。
- 9：示された問題を修正してください。
- 10：ネットワークにより、トラブルシューティングが拒否されました。
- 11：クライアント レポートを取得中です。
- 12：クライアント ログを取得中です。
- 13：取得が完了しました。
- 14：アソシエーション テストを開始します。
- 15：DHCP テストを開始します。
- 16：ネットワーク接続テストを開始します。
- 17：DNS ping テストを開始します。
- 18：名前解決テストを開始します。
- 19：802.1X 認証テストを開始します。
- 20：クライアントを特定のプロファイルにリダイレクトしています。
- 21：テストが完了しました。
- 22：テストに合格しました。
- 23：テストに失敗しました。
- 24：通常の操作を再開するには、診断チャネル操作をキャンセルするか、WLAN プロファイルを選択してください。
- 25：クライアントにより、ログの取得が拒否されました。

- 26：クライアントにより、クライアント レポートの取得が拒否されました。
- 27：クライアントにより、テスト要求が拒否されました。
- 28：無効なネットワーク（IP）設定です。
- 29：ネットワークで機能停止または問題が発生しています。
- 30：予定された保守期間です。
- 31：WLAN セキュリティ方式が正しくありません。
- 32：WLAN 暗号化方式が正しくありません。
- 33：WLAN 認証方式が正しくありません。

stats-request *measurement-duration*	統計情報の要求を送信します。
dot11	（任意）dot11 カウンタを指定します。
security	（任意）セキュリティ カウンタを指定します。
test-abort	現在のテストを中止するよう指示する要求をクライアントに送信します。
test-association *ssid bssid dot11 channel*	関連付けテストの実行要求をクライアントに送信します。
test-dot1x	802.1x テストの実行要求をクライアントに送信します。
profile-id	（任意）テストのプロファイル名。
bssid	Basic SSID。
dot11	802.11a、802.11b、または 802.11g ネットワークを指定します。
channel	チャネル番号。
test-profile	プロファイル リダイレクト テストの実行要求をクライアントに送信します。
any	プロファイル リダイレクト テストの実行要求をクライアントに送信します。
profile-id	テスト プロファイル名。 （注） プロファイル ID には、必ずクライアント レポートが有効なクライアント プロファイルのプロファイル ID を指定します。

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン **default-gw-ping** テストでは、クライアントは診断チャネルを使用する必要はありません。

次に、クライアントの MAC アドレス 00:1f:ca:cf:b6:60 のレポート情報をクリアする例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless client mac-address 00:1f:ca:cf:b6:60 ccx clear-reports
デバイス(config)# end
```

wireless client syslog-detailed

クライアントイベントの詳細な syslog を有効にするには、**wireless client syslog-detailed** コマンドを使用します。クライアントイベントの詳細な syslog を無効にするには、このコマンドの **no** 形式を使用します。

wireless client syslog-detailed

no wireless client syslog-detailed

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション (#)

コマンド履歴

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

例

次に、クライアントイベントの詳細な syslog を有効にする例を示します。

```
Device(config)# wireless client syslog-detailed
```

wireless client username deauthenticate

特定のユーザー名を持つワイヤレスクライアントを認証解除するには、**wireless client username deauthenticate** コマンドを使用します。

wireless client username *username* **deauthenticate**

構文の説明

username	クライアントユーザー名。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、特定のユーザー名を持つワイヤレスクライアントを認証解除する例を示します。

```
Device# wireless client username Bob deauthenticate
```

wireless config validate

ワイヤレス設定が完全かつ一貫している（すべての機能プロファイルとタグが定義され、すべてのアソシエーションが完全かつ一貫している）かどうかを検証するには、特権EXECモードで **wireless config validate** コマンドを使用します。

wireless config validate

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

Cisco vEWLCでは、ワイヤレス設定はプロファイルのコレクションを使用して作成され、各プロファイルが機能ブロックを定義します。これらの機能ブロックは個別に定義され、無線LANの構築においてインテントベースのワークフローを通じて明確に定義された関連付けを実現するために使用されます。このように、機能ブロックのモジュラ化が柔軟であるため、管理者は、すべてのアソシエーションが一貫していて完全であることを確認する必要があります。

ワイヤレス設定の完全性と一貫性を確保するには、コンフィギュレーション検証ライブラリを使用して、設定の定義をテーブル間で検証します。ワイヤレス設定を検証し、不整合があればbtraceインフラおよび（コンソール ロギングが有効である場合）コンソールで表示されるコンテキスト エラー メッセージを使用して報告するため、このリリースから **wireless config validate** EXEC コマンドが導入されました。このコマンドは、機能的なワイヤレス LAN を実現できるようにするため、不整合（未解決のアソシエーション）を呼び出します。

出力をファイルに転送するには、**show logging | redirect bootflash:** *filename* コマンドを使用します。

次のワイヤレス設定のセットが検証されます。

RF タグ	サイト タグ	ポリシー タグ	ポリシー プロファイル	Flex プロファイル
site-tag	flex-profile	wlan profile	IPv4 ACL 名	VLAN ACL
policy-tag	ap-profile	policy profile	ファブリック名	ACL-policy
rf-tag	—	—	service-policy input および output name	RF ポリシー（5 GHz および 24 GHz）

RF タグ	サイト タグ	ポリシー タグ	ポリシー プロファイル	Flex プロファイル
-—	-—	-—	service-policy input および client output name	-—

例

次に、**wireless config validate** コマンドの出力例を示します

```
Device# wireless config validate

Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0:
wncmgrd: Error in AP: fc99.473e.0a90  Applied site-tag : mysite definitiondoes not exist
Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0:
wncmgrd: Error in AP: fc99.473e.0a90  Applied policy-tag : mypolicy definition does not
 exist
Oct 10 18:21:59.576 IST: %CONFIG_VALIDATOR_MESSAGE-5-EWLC_GEN_ERR: Chassis 1 R0/0:
wncmgrd: Error in AP: fc99.473e.0a90  Applied rf-tag : myrf definition does not exist
```

wireless country

デバイスの 1 つ以上の国コードを設定するには、 **wireless country** コマンドを使用します。

wireless country *country-code*

構文の説明

country-code	Two-letter country code.

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

Cisco は、ネットワーク管理者または資格のある IT プロフェッショナルがインストールしてください。その際、正しい国コードを選択する必要があります。インストール後は、法的な規制基準を遵守するためおよび、適切なユニット機能を保証するために、ユニットへのアクセスはパスワードで保護する必要があります。最新の国コードおよび規制区域については、関連する製品マニュアルを参照してください。

次に、デバイスで国コードを IN（インド）に設定する例を示します。

```
Device(config)# wireless country IN
```

wireless exclusionlist mac address

除外リストにクライアントを手動で追加するには、wireless exclusion list コマンドを使用します。手動エントリを削除するには、このコマンドの no 形式を使用します。

wireless exclusionlist *mac_address* **description**

構文の説明

description *value*	エントリの説明を設定します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

Cisco IOS XE Gibraltar 16.10.1	変更内容
	このコマンドは本リリースで追加されました。

使用上のガイドライン

クライアントが除外リストに動的に追加された場合、そのクライアントを削除するには、有効モードから **wireless client mac-address xxxx.xxxx.xxxx deauthenticate** コマンドを使用します。

例

次に、除外エントリを管理する例を示します。

```
Device(config)# wireless exclusion list xxxx.xxxx.xxxx
```

wireless fabric control-plane

ワイヤレス ファブリック モードに適用するコントロール プレーン名を設定するには、**wireless fabric control-plane** コマンドを使用します。

wireless fabric control-plane *control-plane-name*

構文の説明

control-plane-name	ワイヤレス ファブリック モードに適用されるコントロール プレーン名。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

コントロール プレーン名を指定しない場合は、自動生成される default-control-plane が使用されます。

例

次に、コントロール プレーン名を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless fabric control-plane test-control-plane
```

wireless fabric

コントローラで SD-Access ワイヤレスをグローバルに有効にするには、 **wireless fabric** コマンドを使用します。

wireless fabric

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

次に、コントローラでSD-Accessワイヤレスをグローバルに有効にする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless fabric
```

wireless fabric name

ワイヤレス ファブリック名 VXLAN ID（VNID）マップを設定するには、**wireless fabric name** コマンドを使用します。

wireless fabric ［**control-plane** *control-plane-name*］ | ［**name** *vnid-map-name* **l2-vnid** *id* {**control-plane** *control-plane-name* | **l3-vnid** *id* } **ip** {*ipv-addr netmask-addr* | *ipv6-addr netmask-addr*} ［{**control-plane** *control-plane-name*］}］

構文の説明

control-plane *control-plane-name*	コントロール プレーンの詳細を設定します。
name *vnid-map-name*	ワイヤレス ファブリック名を設定します
l2-vnid *id*	レイヤ 2 VNID を設定します。有効な範囲は 0 ～ 16777215 です。
l3-vnid *id*	レイヤ 3 VNID を設定します。有効な範囲は 0 ～ 16777215 です。
ip {*ipv4-addr netmask-addr* | *ipv6-addr netmask-addr*}	IP アドレスとネットマスク アドレスの詳細。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、MAP サーバーを レイヤ 2 およびレイヤ 3 の VNID ごとに設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless fabric name vnid-map l2-vnid 2 l3-vnid 10 ip 209.165.200.224
255.255.255.224
```

wireless hotspot anqp-server

Hotspot 2.0 Access Network Query Protocol（ANQP）サーバーを設定するには、**wireless hotspot anqp-server** コマンドを使用します。Hotspot 2.0 サーバーを無効にするには、このコマンドの **no** 形式を使用します。

wireless hotspot anqp-server *server-name*

wireless hotspot anqp-server *server-name* **type open-roaming**

構文の説明

server-name	Hotspot 2.0 ANQP サーバーの名前。
type	ANQP サーバータイプ。
open-roaming	オープンローミングタイプ。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.2.1	このコマンドが変更されました。**type** および **open-roaming** のキーワードが導入されました。

例

次に、Hotspot 2.0 ANQP サーバーを設定する例を示します。

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

次に、オープンローミングを使用して Hotspot 2.0 ANQP サーバーを設定する例を示します。

```
Device(config)# wireless hotspot anqp-server my-server type open-roaming
```

wireless hotspot gas-rate-limit

1 秒あたりに処理される Generic Advertisement Service（GAS）要求または Access Network Query Protocol（ANQP）要求の最大数を制限するには、**wireless hotspot gas-rate-limit** コマンドを使用します。制限を無効にするには、このコマンドの **no** 形式を使用します。

wireless hotspot gas-rate-limit *limit*

構文の説明

limit	1 秒あたりに処理される GAS または ANQP 要求の数。有効な範囲は 1 ～ 2500 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、1 秒あたりに処理される GAS または ANQP 要求の最大数を制限する例を示します。

```
Device(config)# wireless hotspot gas-rate-limit 100
```

wireless hotspot icon

Hotspot 2.0 の アイコンを設定するには、**wireless hotspot icon** コマンドを使用します。アイコンを削除するには、このコマンドの **no** 形式を使用します。

wireless hotspot icon {**bootflash:filename** | **flash:filename**} *media-type language-code icon-width icon-height*

構文の説明

media-type	このアイコン ファイルのメディア タイプ。 （注） アイコン ファイルは、次の URL で定義されているタイプと一致している必要があります。 http://www.iana.org/assignments/media-types/index.html
language-code	オペレータの 3 文字の言語コード。言語コードには、言語の最初の 3 文字のみを小文字で使用します。たとえば、英語の場合は *eng* を使用します。 言語コードの完全なリストについては、http://www.loc.gov/standards/iso639-2/php/code_list.php を参照してください。
icon-width	アイコンの幅（ピクセル）。有効な範囲は 0 ～ 65535 です。
icon-height	アイコンの高さ（ピクセル）。有効な範囲は 0 ～ 65535 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、Hotspot 2.0 のアイコンを設定する例を示します。

```
Device(config)# wireless hotspot icon flash:test jpeg en 655 400
```

wireless ipv6 nd ns-forward

ワイヤレスクライアントへのネイバー要請（NS）メッセージの転送を有効にするには、**wireless ipv6 nd ns-forward** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

wireless ipv6 nd ns-forward

no wireless ipv6 nd ns-forward

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.2	このコマンドは、Cisco IOS XE Cupertino 17.9.2 以降でサポートされています。

例

次に、ワイヤレスクライアントへのネイバー要請（NS）メッセージの転送を有効にする例を示します。

```
Device(config)# wireless ipv6 nd ns-forward
```

wireless ipv6 ra wired

有線クライアントへのルータ アドバタイズメント メッセージの転送を有効にするには、**wireless ipv6 ra wired** コマンドを使用します。

wireless ipv6 ra wired { **nd** { **na-forward** | **ns-forward** } | **ra-wired** }

構文の説明

nd	ワイヤレス IPv6 ND パラメータを設定します。
na-forward	ワイヤレスクライアントへのネイバーアドバタイズメントの転送を有効にします。
ns-forward	ワイヤレスクライアントへのネイバー要請の転送を有効にします。
ra	ワイヤレス IPv6 ルータアドバタイズメントのパラメータを設定します。
wired	有線クライアントへのルータ アドバタイズメント メッセージの転送を有効にします。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.3	このコマンドが導入されました。

例

次に、有線クライアントへのルータ アドバタイズメント メッセージの転送を有効にする例を示します。

```
Device(config)# wireless ipv6 ra wired
```

警告 **wireless ipv6 ra wired** コマンドは、展開中ではないときに、証明目的でのみ有効にする必要があります。

wireless load-balancing

コントローラでアグレッシブ ロード バランシングを設定するには、グローバル コンフィギュレーション モードで **wireless load-balancing** コマンドを使用します。

wireless load-balancing {**denial** *denial-count* | **window** *client-count*}

構文の説明

denial *denial-count*	ロードバランシング時に拒否されるアソシエーションの数を指定します。 ロード バランシング時の関連付け拒否の最大数は、1 ~ 10 の範囲で指定できます。デフォルト値は 3 です。
window *client-count*	アグレッシブ ロード バランシング クライアント ウィンドウと、特定のアクセス ポイントでのアグレッシブ ロードバランシングをトリガーするのに必要なクライアント数を指定します。 クライアント数を指定するアグレッシブ ロードバランシング クライアント ウィンドウは、0~20 の範囲で指定できます。デフォルト値は 5 です。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

負荷分散が有効になっている WLAN は、音声およびビデオなどの時間依存型アプリケーションをサポートしません。これは、ローミングでの遅延が存在するためです。

コントローラとともに Cisco 7921 および 7920 Wireless IP Phone を使用する場合、各コントローラの音声 WLAN でアグレッシブなロードバランシングが無効化されていることを確認します。無効化されていない場合、電話による初期ローミングが失敗し、オーディオパスが中断されることがあります。

次に、ロード バランシング中の関連付け拒否を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless load-balancing denial 5
デバイス(config)# end
```

wireless load-balance ap method rf

RF ベースの AP ロードバランシングを設定するには、**wireless load-balance ap method rf** コマンドを使用します。RF ベースの AP ロードバランシングを無効にするには、このコマンドの **no** 形式を使用します。

wireless load-balance ap method rf

no wireless load-balance ap method rf

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

RF ベースのロードバランシングは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、RF ベースの AP ロードバランシングを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless load-balance ap method rf
```

wireless macro-micro steering transition-threshold

マイクロ/マクロ遷移のしきい値を設定するには、 **wireless macro-micro steering transition-threshold** コマンドを使用します。

wireless macro-micro steering transition-threshold {**balancing-window** | **client count** *number-clients* }{**macro-to-micro** | **micro-to-macro** *RSSI in dBm*}

構文の説明

balancing-window	ルートプロセッサ スロット 0 の設定のアクティブ インスタンス。
client	ルートプロセッサスロット 0 の設定のスタンバイ インスタンス。
number-clients	有効なクライアント数の範囲は 0 ～ 65535 です。
macro-to-micro	マイクロ/マクロ遷移の RSSI を設定します。
micro-to-macro	マイクロ/マクロ クライアント ロード バランシング ウィンドウを設定します。
RSSI in dBm	RSSI（dBm 単位）。有効な範囲は –128 ～ 0 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、バランシングウィンドウを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless macro-micro steering transition-threshold balancing-window
number-of-clients
```

wireless macro-micro steering probe-suppression

マイクロ/マクロ プローブの抑制を設定するには、**wireless macro-micro steering probe-suppression** コマンドを使用します。

wireless macro-micro steering probe-suppression {**aggressiveness** *number-of-cycles* | | **hysteresis***RSSI in dBm* | **probe-auth** | **probe-only**}

構文の説明

aggressiveness	抑制するプローブ サイクルを設定します。サイクル数の範囲は 0 ～ 255 です。
hysteresis	クライアントが近傍のアクセス ポイントにローミングするためには、そのアクセス ポイントに後どれだけの信号強度が必要であるかを表示します。RSSI デシベル値の範囲は -6 ～ -3 です。
probe-auth	プローブと single auth を抑制するモードを有効にします
probe-only	プローブのみを抑制するモードを有効にします

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドは、Cisco IOS XE Gibraltar 16.12.1 よりも前のリリースで導入されました。

例

次に、バランシングウィンドウを設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless macro-micro steering probe-suppression aggressiveness
number-of-cycles
```

wireless management certificate

ワイヤレス管理証明書の詳細を作成するには、**wireless management certificate** コマンドを使用します。

wireless management certificate ssc {**auth-token** {**0** | **8**} *token* | **trust-hash** *hash-key* }

構文の説明

auth-token	認証トークン。
token	トークン名。
trust-hash	信頼できる SSC ハッシュリスト。
hash-key	SHA1 フィンガープリント。
0	暗号化されていないトークンを指定します。
8	AES 暗号化トークンを指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、ワイヤレス管理証明書を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless management certificate ssc trust-hash test
```

wireless management interface

ワイヤレス管理インターフェイスを作成するには、**wireless management interface** コマンドを使用します。

wireless management interface {**GigabitEthernet** | **Loopback** | **Vlan** } *interface-number*

構文の説明

interface-number	インターフェイス番号。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、ワイヤレス管理インターフェイスを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless management interface vlan vlan1
```

wireless management trustpoint

ワイヤレス管理トラストポイントを作成するには、**wireless management trustpoint** コマンドを使用します。

wireless management trustpoint *trustpoint-name*

構文の説明

trustpoint-name	トラストポイント名。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

アプライアンスはこのコマンドを必要とせずにデフォルトで SUDI 証明書を使用するため、このコマンドはクラウド向け Cisco Catalyst 9800 ワイヤレス コントローラ プラットフォームでのみ使用し、アプライアンスでは使用しません。

例

次に、ワイヤレス管理トラストポイントを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless management trustpoint test
```

wireless max-warning period

ワイヤレス クライアント チェックの周期を設定するには、**wireless max-warning period** コマンドを使用します。ワイヤレス クライアント チェックを無効にするには、このコマンドの **no** 形式を使用します。

wireless max-warning period *interval-in-mins*

no wireless max-warning period

構文の説明

interval-in-mins	ワイヤレス クライアント チェックの周期。有効な値の範囲は、1 ～ 60 分です。

コマンド デフォルト

ワイヤレス クライアント チェックの周期は設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、ワイヤレス クライアント チェックの周期を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless max-warning period 20
```

wireless max-warning threshold clients

ワイヤレス クライアント チェックでのワイヤレスクライアントの最大数に対する警告しきい値パーセンテージを設定するには、**wireless max-warning threshold client** コマンドを使用します。ワイヤレス クライアント チェックのデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

wireless max-warning threshold clients *threshold_percentage*

no wireless max-warning threshold clients

構文の説明

threshold_percentage	ワイヤレス クライアント チェックの警告しきい値パーセンテージ。有効な値の範囲は 50 ～ 100 パーセントです。

コマンド デフォルト

しきい値のパーセントは 75 パーセントに設定されています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、ワイヤレス クライアント チェックでのワイヤレスクライアントの最大数に対する警告しきい値パーセンテージを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless max-warning threshold clients 90
```

wireless media-stream

さまざまなパラメータを設定するには、 **wireless media-stream** コマンドを使用します。

wireless media-stream group *groupName* [*startipAddr endipAddr*]

wireless media-stream group{ `avg-packet-size default exit max-bandwidth no policy qos`}

wireless media-stream {**multicast-direct** | **message** [{**phone** *phone* | **URL** *URL* | **Notes** 注 | **Email** *Email*}]}

構文の説明

group *groupName*	グループのマルチキャスト ダイレクト ステータスを設定します。
startipAddr	グループの開始 IP アドレスを設定します。
endipAddr	グループの終了 IP アドレスを設定します。
group *avg-packet-size*	平均パケット サイズを設定します。 値は 100 ～ 1500 kbps の範囲で指定できます。
group *default*	コマンドをデフォルト値に設定します。
group *exit*	サブモードを終了します。
group *max-bandwidth*	予想されるストリームの最大帯域幅を Kbps 単位で設定します。 値は 1 ～ 35000 kbps の範囲で指定できます。
group *no*	コマンドを無効にするか、そのデフォルトに設定します。
group *policy*	メディア ストリームのアドミッション ポリシーを設定します。 次のオプションのいずれかを選択できます。 • admit：メディア ストリーム グループのトラフィックを許可します。 • deny：メディア ストリーム グループのトラフィックを拒否します。
group *qos*	エア QoS クラスを <'video'> ONLY に設定します。
multicast-direct	マルチキャスト ダイレクト ステータスを設定します。
message	セッション アナウンス メッセージを設定します。
phone *phone*	セッション アナウンスの電話番号を設定します。
URL *URL*	セッション アナウンス URL を設定します。

Notes *Notes*	セッション アナウンス メモを設定します。
Email *Email*	セッション アナウンス電子メールを設定します。

コマンド デフォルト

ディセーブル

コマンド モード

config

コマンド履歴

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

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。

例

次に、予想されるマルチキャスト宛先アドレス、ストリームの帯域幅の使用量およびストリームの優先順位のパラメータなど、各メディア ストリームとそのパラメータを設定する例を示します。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#wireless media-stream group GROUP1 231.1.1.1 231.1.1.10
```

wireless media-stream message

セッション アナウンス メッセージを設定するには、**wireless media-stream message** コマンドを使用します。

wireless media-stream message {**Email** | **Notes** | **URL** | **phone**}

構文の説明

Email	セッションアナウンス電子メールを設定します。
Notes	セッション アナウンス メモを設定します。
URL	セッション アナウンス URL を設定します。
phone	セッションアナウンスの電話番号を設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

メディア ストリームが（帯域幅制約が原因で）拒否される場合に、ユーザーにメッセージを送信できます。これらのパラメータは、IT サポートの電子メール アドレス、メモ（ストリームが拒否された理由を説明する画面メッセージ）、ユーザがリダイレクトされるURL、拒否されたストリームについてユーザが問い合わせをする電話番号など、送信するメッセージを設定します。

例

次に、セッション アナウンス URL を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless media-stream message URL www.example.com
```

wireless media-stream multicast-direct

マルチキャストダイレクトのステータスを設定するには、 **media-stream multicast-direct** コマンドを使用します。マルチキャストダイレクトのステータスを削除するには、このコマンドの no 形式を使用します。

no wireless media-stream multicast-direct

コマンド デフォルト

なし

コマンド モード

config

使用上のガイドライン

メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御（CAC）が実行されている必要があります。WLAN Quality of Service（QoS）を gold または platinum のいずれかに設定する必要があります。

例

次に、ワイヤレス LAN メディア ストリームのマルチキャストダイレクトを設定する例を示します。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#wireless media-stream multicast-direct
```

wireless mesh alarm association count

メッシュ アラーム アソシエーションの数を設定するには、 **wireless mesh alarm association count** コマンドを使用します。

wireless mesh alarm association count *count*

構文の説明

count	アラーム アソシエーションの数。有効な範囲は 1 ～ 30 です。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

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

例

次に、アラーム アソシエーションの数を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy wireless mesh alarm association count 10
```

wireless mesh alarm high-snr

メッシュ アラームの 高 SNR 値を設定するには、 **wireless mesh alarm high-snr** コマンドを使用します。

wireless mesh alarm high-snr *high-snr*

構文の説明

high-snr	高 SNR 値を設定します。有効な範囲は 31 ～ 100 です。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

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

例

次に、メッシュの高 SNR を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy wireless mesh alarm high-snr 75
```

wireless mesh alarm low-snr

メッシュ アラームの低 SNR 値を設定するには、 **wireless mesh alarm low-snr** コマンドを使用します。

wireless mesh alarm low-snr *low-snr*

構文の説明

low-snr	低 SNR 値を設定します。有効な範囲は 1 ～ 30 です。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

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

例

次に、メッシュの高 SNR を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless profile policy wireless mesh alarm low-snr 5
```

wireless mesh alarm max-children map

メッシュ アラームの最大子 MAP 値を設定するには、 **wireless mesh alarm max-children map** コマンドを使用します。

wireless mesh alarm max-children map *max-children*

構文の説明

max-children	メッシュ アラームの最大子 MAP パラメータを設定します。有効な範囲は 1 ～ 50 です。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

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

例

次に、メッシュ アラームの最大子 MAP 値を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mesh alarm max-children map 35
```

wireless mesh alarm max-children rap

メッシュ アラームの最大子 RAP 値を設定するには、 **wireless mesh alarm max-children rap** コマンドを使用します。

wireless mesh alarm max-children rap *max-children*

構文の説明

max-children	メッシュ アラームの最大子 RAP パラメータを設定します。有効な範囲は 1 ～ 50 です。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

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

例

次に、メッシュ アラームの最大子 RAP 値を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mesh alarm max-children rap 40
```

wireless mesh alarm max-hop

メッシュ アラームの最大ホップ パラメータを設定するには、 **wireless mesh alarm max-hop** コマンドを使用します。

wireless mesh alarm max-hop *max-hop*

構文の説明

max-hop	メッシュ アラームの最大ホップ数を設定します。有効な範囲は1 ～ 16 です。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

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

例

次に、メッシュ アラームの最大ホップ パラメータを設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mesh alarm max-hop 15
```

wireless mesh alarm parent-change count

親変更カウントの最大値を設定するには、 **wireless mesh alarm parent-change count** コマンドを使用します。

wireless mesh alarm parent-change count *count*

構文の説明

count	親変更カウントの最大値を設定します。有効な範囲は 1 ～ 30 です。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

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

例

次に、アラームの親変更カウント値を設定する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mesh alarm parent-change count 6
```

wireless mesh backhaul bdomain-channels

屋外のメッシュ AP のバックホール無線で拡張 UNII B ドメイン チャネルを設定し、許可するには、 **wireless mesh backhaul bdomain-channels** コマンドを使用します。

wireless mesh backhaul bdomain-channels

構文の説明

bdomain-channels	屋外のメッシュ AP のバックホール無線で拡張 UNII B ドメイン チャネルを許可します。 メッシュ AP のバックホール無線による拡張 UNII B ドメイン チャネルの使用を無効にするには、このコマンドの **[no]** 形式を使用します。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

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

例

次に、屋外のメッシュ AP のバックホール無線による拡張 UNII B ドメイン チャネルの使用を無効にする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# no wireless mesh backhaul bdomain-channels
```

wireless mesh backhaul rrm

メッシュ バックホールを設定するには、 **wireless mesh backhaul** コマンドを使用します。

wireless mesh backhaul{**bdomain-channels** | **rrm**}

構文の説明

backhaul	メッシュ バックホールを設定します。
bdomain-channels	屋外のメッシュ AP のバックホール無線で拡張 UNII B ドメイン チャネルを許可します。
rrm	メッシュ バックホールの RRM を設定します。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

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

例

次に、メッシュ バックホールの RRM を設定する例を示します。

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

wireless mesh backhaul rrm auto-dca

無線周波数（RF）特定用途向け集積回路（ASIC）RAP の自動 DCA を設定するには、**wireless mesh backhaul rrm auto-dca** コマンドを使用します。

wireless mesh backhaul rrm auto-dca

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

例

次に、RF ASIC 集積回路 RAP の自動 DCA を設定する例を示します。

```
Device# wireless mesh backhaul rrm auto-dca
```

wireless mesh cac

メッシュ CAC モードを設定するには、 **wireless mesh cac** コマンドを使用します。

wireless mesh cac

構文の説明

cac	メッシュ CAC モードを設定します。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

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

例

次に、メッシュ CAC モードを設定する例を示します。

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

wireless mesh ethernet-bridging allow-bdpu

有線メッシュ アップリンクへの STP BPDU を設定するには、 **wireless mesh ethernet-bridging allow-bdpu** コマンドを使用します。

wireless mesh ethernet-bridging allow-bdpu

構文の説明

ethernet-bridging	イーサネット ブリッジングを設定します。
allow-bdpu	有線メッシュ アップリンクへの STP BPDU を設定します。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

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

例

次に、有線メッシュ アップリンクへの STP BPDU を設定する例を示します。

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

wireless mesh security psk provisioning

メッシュ セキュリティ PSK パラメータをプロビジョニングするには、 **wireless mesh security psk provisioning** コマンドを使用します。

wireless mesh security psk provisioning {**default_psk** | **inuse** *psk-index* | **key** *psk-index*{**0** | **8**}*enter-psk-name psk-description*}

構文の説明

provisioning	メッシュ PSK プロビジョニング パラメータを設定します。
default_psk	メッシュ プロビジョニングをデフォルト PSK 設定に設定します。
inuse	PSK inuse インデックスを設定します
psk-index	PSK キー インデックスを入力します。有効な範囲は 1 ～ 5 です。
key	事前共有キーを設定します
psk-index	PSK キー インデックスを入力します。有効な範囲は 1 ～ 5 です。
0	非暗号化パスワードを入力することを選択します。
8	AES 暗号化パスワードを入力することを選択します。
enter-psk-name	設定済みの PSK キーの名前を入力します。
psk-description	このキーの説明を入力します。

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

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

例

次に、メッシュセキュリティでデフォルトPSKキーをプロビジョニングする例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mesh security psk provisioning default_psk
```

wireless mesh subset-channel-sync

モビリティ グループのサブセット チャネル同期を設定するには、 **wireless mesh subset-channel-sync** コマンドを使用します。

wireless mesh subset-channel-sync

構文の説明

subset-channel-sync	モビリティ グループのサブセット チャネル同期を設定します

コマンド デフォルト

なし

コマンド モード

config

コマンド履歴

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

例

次に、モビリティ グループのサブセット チャネル同期を設定する例を示します。

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

wireless mobility

間のモビリティ マネージャを設定するには、 **wireless mobility** コマンドを使用します。

wireless mobility {**dscp** *value*}

構文の説明

dscp *value*	モビリティの 間の DSCP 値を設定します。

コマンド デフォルト

デフォルトの DSCP 値は、48 です。

コマンド モード

グローバル設定

コマンド履歴

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

次に、 間の DSCP 値が 20 のモビリティを設定する例を示します。

```
デバイス(config)# wireless mobility dscp 20
```

wireless mobility controller peer-group

モビリティ ピア グループを設定するには **wireless mobility controller peer-group** コマンドを使用し、設定を削除するにはこのコマンドの **no** 形式を使用します。

wireless mobility controller peer-group *peer-group* **member IP** *ip-address***mode centralized**

構文の説明

peer group	ピア グループの名前。
member IP	ピア グループ メンバーを追加します。
ip-address	追加するピア グループ メンバーの IP アドレス。
mode centralized	集約的に管理されるピア グループ メンバーの管理モードを設定します。

コマンド デフォルト

集約型モードはオフです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.0 E	このコマンドが導入されました。

```
デバイス enable
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless mobility controller peer-group peer1 member ip 10.0.0.1 mode
centralized
```

wireless mobility group keepalive

モビリティ グループ パラメータを設定し、その ping パラメータをキープアライブにするには、**wireless mobility group keepalive** コマンドを使用します。モビリティ グループ パラメータを削除するには、このコマンドの **no** 形式を使用します。

wireless mobility group keepalive {**count** *number* | **interval** *interval*}
no wireless mobility group keepalive {**count** 番号 | **interval** *interval*}

構文の説明

count *number*	モビリティ グループ メンバーに ping 要求を送信する回数。この回数を超えると、メンバーにはアクセスできないと見なされます。有効な範囲は 3 ～ 20 です。デフォルトは 3 です。
interval *interval*	モビリティ グループ メンバーへの ping 要求の送信間隔。範囲は 1 ～ 30 秒です。デフォルト値は 10 秒です。 （注） モビリティ トンネルを介して接続されているコントローラの場合は、両方のコントローラのキープアライブ間隔値が同じであることを確認します。

コマンド デフォルト

カウントは 3秒、間隔は 10 秒です。

コマンド モード

グローバル コンフィギュレーション。

コマンド履歴

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

使用上のガイドライン

interval のデフォルト値は 10 秒、*retries* のデフォルト値は 3 秒に設定されます。

次に、モビリティ グループ メンバに送信する各 ping 要求の間隔を 10 秒に指定する例を示します。

```
デバイス(config)# wireless mobility group keepalive count 10
```

wireless mobility group mac-address

モビリティ メッセージで使用される MAC アドレスを設定するには、**wireless mobility group mac-address** コマンドを使用します。

wireless mobility group mac-address *mac-addr*

構文の説明

mac-addr	モビリティ メッセージで使用される MAC アドレス。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、モビリティ メッセージで使用される MAC アドレスを設定する例を示します。

```
Device(config)# wireless mobility group mac-address 00:0d:ed:dd:25:82
```

wireless mobility group member ip

モビリティ グループのメンバ リストのユーザを追加または削除するには、 **wireless mobility group member ip** コマンドを使用します。モビリティ グループからメンバを削除するには、このコマンドの **no** 形式を使用します。

wireless mobility group member ip *ip-address* [**public-ip** *public-ip-address*] [**group** *group-name*]
no wireless mobility group member ip *ip-address*

構文の説明

ip-address	メンバー コントローラの IP アドレス。
public-ip *public-ip-address*	（任意）メンバー コントローラのパブリック IP アドレス。 （注） このコマンドは、メンバーが NAT に関与する場合にのみ使用されます。サポートされているのは、スタティック IP NAT のみです。
group *group-name*	（任意）メンバー コントローラのグループ名。 （注） このコマンドは、メンバーがローカル モビリティ コントローラと同じグループに追加されない場合にのみ使用されます。

コマンド デフォルト

なし。

コマンド モード

グローバル コンフィギュレーション。

コマンド履歴

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

使用上のガイドライン

モビリティ グループは、特定の導入に複数のモビリティ コントローラ（MC）がある場合に使用されます。モビリティ グループに任意の名前を割り当てることもできますし、デフォルト グループの名前を割り当てることもできます。モビリティ グループ メンバーは、グループ内でローミングするグループのすべてのメンバーに対して設定する必要があります。

次に、モビリティ グループにメンバーを追加する例を示します。

```
デバイス(config)# mobility group member ip 10.104.171.101 group TestDocGroup
```

wireless mobility group member mac-address

モビリティ グループ メンバー リストを作成するには、グローバル コンフィギュレーション モードで **wireless mobility group member mac-address** コマンドを使用します。モビリティグループからメンバーを削除するには、このコマンドの **no** 形式を使用します。

wireless mobility group member mac-address *peer_mac* **ip** *peer_private_ip* [**public-ip** *peer_public_ip*] **group** *group_name*

構文の説明

peer_mac	ピアコントローラの MAC アドレス。
peer_private_ip	ピアコントローラのプライベート IP アドレス。
peer_public_ip	ピアコントローラのパブリック IP アドレス。
group_name	メンバーコントローラのグループ名。

コマンド デフォルト

モビリティピアは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1s	このコマンドは、Cisco IOS XE Amsterdam 17.1.1s よりも前のリリースで導入されました。 **public-ip** キーワードと *peer_public_ip* 変数は、このリリースからサポートされます。

例

次に、モビリティ グループ メンバー リストを作成する例を示します。

```
Device(config)# wireless mobility group member mac-address 001e.494b.04ff ip 11.0.0.2
public-ip 4.0.0.112 group dom1
```

wireless mobility group multicast-address

非ローカルモビリティグループのマルチキャストIPアドレスを設定するには、**wireless mobility group multicast-address** コマンドを使用します。

wireless mobility group multicast-address *group-name* {**ipv4** | **ipv6**}*ip-addr*

構文の説明

group-name	非ローカル モビリティ グループの名前。
ipv4	IPv4 アドレスを入力するオプション。
ipv6	IPv6 アドレスを入力するオプション。
ip-addr	非ローカルモビリティグループのIPv4またはIPv6アドレス。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、非ローカル モビリティ グループのマルチキャスト IPv4 アドレスを設定する例を示します。

```
Device(config)# wireless mobility group multicast-address Mygroup ipv4 224.0.0.5
```

wireless mobility group name

モビリティ ドメイン名を設定するには、**wireless mobility group name** コマンドを使用します。モビリティ ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

（注） ネットワーク アドレス変換（NAT）が有効になっているネットワークのモビリティ グループを設定する際に、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。そうしないと、モビリティ グループ内のコントローラ間でモビリティが失敗します。

wireless mobility group name *domain-name*
no wireless mobility group name

構文の説明

domain-name	次のコマンドを入力して、新しいモビリティ グループを作成します。ドメイン名は最大 31 文字で、大文字と小文字を区別します。

コマンド デフォルト

これがデフォルトです。

コマンド モード

グローバル コンフィギュレーション。

コマンド履歴

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

次に、モビリティ ドメイン名 lab1 を設定する例を示します。

```
デバイス(config)# mobility group domain lab1
```

wireless mobility multicast ipv4

ローカル モビリティ グループのマルチキャスト IPv4 アドレスを設定するには、**wireless mobility multicast ipv4** コマンドを使用します。

wireless mobility multicast ipv4 *ipv4-addr*

構文の説明

ipv4-addr	ローカル モビリティ グループのマルチキャスト IPv4 アドレスを入力します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、ローカル モビリティ グループのマルチキャスト IPv4 アドレスを設定する例を示します。

```
Device(config)# wireless mobility multicast ipv4 224.0.0.4
```

wireless mobility mac-address

モビリティ メッセージで使用される MAC アドレスを設定するには、**wireless mobility mac-address** コマンドを使用します。

wireless mobility mac-address *mac-address*

構文の説明

mac-address	モビリティ メッセージで使用される MAC アドレス。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、モビリティ メッセージで使用される MAC アドレスを設定する例を示します。

```
Device(config)# wireless mobility mac-address 00:0d:bd:5e:9f:00
```

wireless multicast

イーサネット マルチキャスト パラメータを設定するには、**wireless multicast** コマンドを使用します。

wireless multicast {*ipv4-address* | **ipv6** *ipv6-address* | **non-ip** [**vlan** *vlan-id*]}

構文の説明

ipv4-address	マルチキャスト IPv4 アドレス。
ipv6 *ipv6-address*	マルチキャスト IPv6 アドレス。
non-ip	すべての VLAN で非 IP マルチキャストを設定します。トラフィックが通過できるように、ワイヤレス マルチキャストを有効にしておく必要があります。
non-ip vlan *vlan-id*	VLAN ごとに非 IP マルチキャストを設定します。トラフィックが通過できるように、ワイヤレスマルチキャストおよびワイヤレスマルチキャスト非 IP の両方を有効にする必要があります。 VLAN ID の有効な範囲は 1 ～ 4094 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、ID が 5 の VLAN に非 IP マルチキャストを設定する例を示します。

```
Device(config)# wireless multicast non-ip vlan 5
```

wireless profile airtime-fairness

新しい Cisco ATF ポリシーを作成するには、**wireless profile airtime-fairness** コマンドを使用します。

wireless profile airtime-fairness *atf-policy-name atf-profile-id*

構文の説明

atf-policy-name	ATF プロファイル名を参照します。
atf-profile-id	ATF プロファイル ID を参照します。指定できる範囲は 0 ～ 511 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

次に、新しい Cisco ATF ポリシーを作成する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless profile airtime-fairness <atf-policy-name> 1
デバイス(config-config-atf)# weight 5
デバイス(config-config-atf)# client-sharing
デバイス(config-config-atf)# end
```

wireless profile ap packet-capture

ワイヤレス AP パケット キャプチャ プロファイルを設定するには、**wireless profile ap packet-capture** コマンドを使用します。

wireless profile ap packet-capture *packet-capture-profile-name*

構文の説明

packet-capture-profile-name	AP パケット キャプチャ プロファイル名。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、AP パケット キャプチャ プロファイルを設定する例を示します。

```
Device(config)# wireless profile ap packet-capture test1
```

wireless profile ap priming

アクセスポイント（AP）をプライミングするためのプロファイルを設定するには、**wireless profile ap priming** コマンドを使用します。プライミングを無効にするには、このコマンドの **no** 形式を使用します。

wireless profile ap priming *profile-name*

no wireless profile ap priming *profile-name*

構文の説明

profile-name	APプライミングプロファイル名。

コマンド デフォルト

AP プライミングプロファイル名は設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Cupertino 17.9.2	このコマンドが導入されました。

使用上のガイドライン

- AP フィルタ プライミング プロファイルには、最大 3 つのコントローラを含めることができます。AP プライミングプロファイルは、AP MAC レベルで、または一致する正規表現フィルタを使用して適用することができます。
- AP MAC ベースの AP プライミングの優先順位が最も高くなります。AP MAC ベースの AP プライミングが使用できない場合は、一致する正規表現フィルタの下にあるプライミングプロファイルのうち、有効なプライミング設定を持ち、最も高い優先順位を持つプライミングプロファイルが適用されます。

例

次に、AP をプライミングするためのプロファイルを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile ap priming Prime-FX
```

wireless profile calender-profile name

カレンダー プロファイルを設定するには、**wireless profile calender-profile name** コマンドを使用します。

wireless profile calender-profile name *name*

構文の説明

name	カレンダープロファイルを指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

次に、カレンダー プロファイルを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless profile calender-profile name daily_calendar_profile
Device(config-calender-profile)# start 09:00:00 end 17:00:00
Device(config-calender-profile)# recurrance daily
Device(config-calender-profile)# end
```

wireless profile fabric

ファブリック プロファイル パラメータを設定するには、 **wireless profile fabric** コマンドを使用します。

wireless profile fabric *fabric-profile-name*

構文の説明

fabric-profile-name	ファブリック プロファイル名。
fabric	ファブリック プロファイル パラメータを設定します。
profile	プロファイル パラメータを設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、ファブリック プロファイル パラメータを設定する例を示します。

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

wireless profile mesh

アクセスポイント（AP）でメッシュプロファイルを設定するには、**wireless profile mesh** *profile-name* コマンドを使用します。

wireless profile mesh *profile-name*

構文の説明

profile-name	プロファイルの名前

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、AP でメッシュプロファイルを設定する例を示します。

```
Device# configure terminal
(config)#wireless profile mesh test1
```

wireless profile policy

WLAN ポリシー プロファイルを設定するには、**wireless profile policy** コマンドを使用します。

wireless profile policy *policy-profile*

構文の説明

policy-profile	WLAN ポリシープロファイルの名前。

コマンド デフォルト

デフォルトのプロファイル名は default-policy-profile です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、WLAN ポリシー プロファイルを設定する例を示します。

```
Device(config)# wireless profile policy mywlan-profile-policy
```

wireless profile power

ワイヤレス電源ポリシープロファイルを設定するには、**wireless profile power** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

wireless profile power *power-profile-name*

構文の説明

power-profile-name	ワイヤレス電源ポリシープロファイルの名前を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

例

次に、ワイヤレス電源ポリシープロファイルを設定する例を示します。

```
Device(config)# wireless profile power power-profile-name
```

wireless profile tunnel

トンネル プロファイルを設定するには、**wireless profile tunnel** コマンドを使用します。

wireless profile tunnel

構文の説明

tunnel-profile-name	トンネル プロファイルの名前。
dhcp-opt82 format mac *raw*|*colon-delimited*	オプション 82 の RID および CID フィールドの MAC アドレスの形式を設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

例

次に、トンネル プロファイルを設定する例を示します。

```
Device(config)# wireless profile tunnel tun1
```

wireless profile radio

ワイヤレス無線プロファイルを設定するには、**wireless profile radio** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

wireless profile radio *radio-profile-name*

no wireless profile radio *radio-profile-name*

構文の説明

wireless profile radio	新しいワイヤレス無線プロファイルを作成します。
radio-profile-name	無線プロファイル名を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

例

次に、ワイヤレス無線プロファイルを設定する例を示します。

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

wireless rfid

スタティック無線周波数 ID（RFID）タグのデータ タイムアウト値を設定するには、グローバル コンフィギュレーション モードで **wireless rfid** コマンドを使用します。

wireless rfid timeout *timeout-value*

構文の説明

timeout	スタティック RFID タグのデータ タイムアウト値を設定します。
timeout-value	RFID タグのデータ タイムアウト値。有効な値の範囲は 60 ～ 7200 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、スタティック RFID タグのデータ タイムアウト値を設定する例を示します。

```
Device(config)# wireless rfid timeout 70
```

wireless security dot1x

IEEE 802.1x のグローバル コンフィギュレーションを設定するには、 **wireless security dot1x** コマンドを使用します。

wireless security dot1x [{**eapol-key** {**retries** *retries* | **timeout** *milliseconds*} | **group-key interval** 秒 | **identity-request** {**retries** *retries* | **timeout** *seconds*} | **radius** [**call-station-id**] {**ap-macaddress** | **ap-macaddress-ssid** | **ipaddress** | **macaddress**} | **request** {**retries** *retries* | **timeout** *seconds*} | **wep key** {**index 0** | **index 3**}}]

構文の説明

eapol-key	eapol-key 関連パラメータを設定します。
retries *retries*	（任意）コントローラが無線クライアントに EAPOL（WPA）キー メッセージを再送信する最大回数（0～4）を指定します。 デフォルト値は 2 です。
timeout *milliseconds*	（任意）EAP または WPA/WPA-2 PSK を使用してコントローラが無線クライアントに EAPOL（WPA）キー メッセージを再送信するまでに待機する時間（200 ～ 5000 ミリ秒）を指定します。 デフォルト値は 1000 ミリ秒です。
group-key interval *sec*	EAP ブロードキャスト キーを更新する間隔を秒で設定します（120～86400 秒）。
identity-request	EAP ID 要求の関連パラメータを設定します。
retries *retries*	（任意）コントローラが EAP ID を要求する最大試行回数（0～4）を指定します。 デフォルト値は 2 です。
timeout *seconds*	（任意）コントローラが無線クライアントに EAP ID 要求メッセージを再送信するまでに待機する時間（1 ～ 120 秒）を指定します。 デフォルト値は 30 秒です。
radius	RADIUS メッセージを設定します。
call-station-id	（任意）RADIUS メッセージで送信されるコール ステーション ID を設定します。
ap-macaddress	呼出端末 ID タイプを AP の MAC アドレスに設定します。
ap-macaddress-ssid	呼出端末 ID タイプを 'AP の MAC アドレス':'SSID' に設定します。
ipaddress	呼出端末 ID タイプをシステムの IP アドレスに設定します。
macaddress	呼出端末 ID タイプをシステムの MAC アドレスに設定します。

request	EAP 要求の関連パラメータを設定します。
retries *retries*	（任意）ID 要求または EAPOL（WPA）キー メッセージ以外の EAP メッセージについて、コントローラが無線クライアントにメッセージを再送信する最大回数（0 ～ 20）を指定します。 デフォルト値は 2 です。
timeout *seconds*	（任意）ID 要求または EAPOL（WPA）キー メッセージ以外の EAP メッセージについて、コントローラが無線クライアントにメッセージを再送信するまでに待機する時間（1 ～ 120 秒）を指定します。 デフォルト値は 30 秒です。
wep key	802.1x WEP 関連パラメータを設定します。
index 0	WEP キーのインデックス値を 0 として指定します。
index 3	WEP キーのインデックス値を 3 として指定します。

コマンド デフォルト

eapol-key-timeout のデフォルト値：1 秒。

eapol-key-retries のデフォルト値：2 回。

コマンド モード

config

コマンド履歴

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

使用上のガイドライン

なし

次の例では、 **wireless security dot1x** のすべてのコマンドをリストしています。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#wireless security dot1x ?
  eapol-key         Configure eapol-key related parameters
  group-key         Configures EAP-broadcast key renew interval time in seconds
  identity-request  Configure EAP ID request related parameters
  radius            Configure radius messages
  request           Configure EAP request related parameters
  wep               Configure 802.1x WEP related paramters
  <cr>
```

wireless security dot1x radius accounting mac-delimiter

called-station-ID または calling-station-ID の MAC デリミタを設定するには、**wireless security dot1x radius accounting username-delimiter** コマンドを使用します。

called-station-ID または calling-station-ID の MAC デリミタを削除するには、このコマンドの **no** 形式を使用します。

wireless security dot1x radius accounting mac-delimiter {**colon** | **hyphen** | **none** | **single-hyphen** }

構文の説明

colon	デリミタをコロンに設定します。
hyphen	デリミタをハイフンに設定します。
none	デリミタを無効にします。
single-hyphen	デリミタをシングル ハイフンに設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.6.0 E	このコマンドが導入されました。

次に、called-station-ID または calling-station-ID の MAC デリミタをコロンに設定する例を示します。

```
デバイス(config)# wireless security dot1x radius accounting mac-delimiter colon
```

wireless security dot1x radius accounting username-delimiter

デリミタのタイプを設定するには、**wireless security dot1x radius accounting username-delimiter** コマンドを使用します。この設定を削除するには、このコマンドの **no** 形式を使用します。

wireless security dot1x radius accounting username-delimiter {**colon | hyphen | none | single-hyphen**}

構文の説明

colon	デリミタをコロンに設定します。
hyphen	デリミタをハイフンに設定します。
none	デリミタを無効にします。
single-hyphen	デリミタをシングルハイフンに設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード。

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.2 E	このコマンドが導入されました。

次に、デリミタをコロンに設定する例を示します。

```
デバイス(config)# wireless security dot1x radius acounting username-delimiter colon
```

wireless security dot1x radius callStationIdCase

RADIUS メッセージで送信される呼出端末 ID の大文字小文字を設定するには、**wireless security dot1x radius callStationIdCase** コマンドを使用します。

RADIUS メッセージで送信される呼出端末 ID の大文字小文字の設定を削除するには、このコマンドの **no** 形式を使用します。

wireless security dot1x radius callStationIdCase {**lower** | **upper**}

構文の説明

lower	すべての呼出端末 ID を小文字で RADIUS に送信します
upper	すべての呼出端末 ID を大文字で RADIUS に送信します

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.6.0 E	このコマンドが導入されました。

次に、RADIUS メッセージで送信される呼出端末 ID を小文字に設定する例を示します。

```
デバイス(config)# wireless security dot1x radius callstationIdCase lower
```

wireless security dot1x radius mac-authentication call-station-id

MAC 認証用の呼出端末 ID タイプを設定するには、**wireless security dot1x radius mac-authentication call-station-id** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

wireless security dot1x radius mac-authentication call-station-id ap-ethmac-only | ap-ethmac-ssid | ap-group-name | ap-label-address | ap-label-address-ssid | ap-location | ap-macaddress | ap-macaddress-ssid | ap-name | ap-name-ssid | ipaddress | macaddress | vlan-id

構文の説明

ap-ethmac-only	呼出端末 ID タイプを AP のイーサネット MAC アドレスに設定します。
ap-ethmac-ssid	呼出端末 ID タイプを 'AP のイーサネット MAC アドレス':'SSID' という形式に設定します。
ap-group-name	呼出端末 ID タイプを AP グループ名に設定します。
ap-label-address	呼出端末 ID タイプを AP ラベル上の AP の MAC アドレスに設定します。
ap-label-address-ssid	呼出端末 ID タイプを 'AP ラベル上の MAC アドレス':'SSID' という形式に設定します。
ap-location	呼出端末 ID タイプを AP の場所に設定します。
ap-macaddress	呼出端末 ID タイプを AP の無線 MAC アドレスに設定します。
ap-macaddress-ssid	呼出端末 ID タイプを 'AP の 無線 MAC アドレス':'SSID' に設定します。
ap-name	呼出端末 ID タイプを AP 名に設定します。
ap-name-ssid	呼出端末 ID タイプを 'AP 名':'SSID' という形式に設定します。
ipaddress	呼出端末 ID タイプをシステムの IP アドレスに設定します。
macaddress	呼出端末 ID タイプをシステムの MAC アドレスに設定します。
vlan-id	呼出端末 ID タイプを VLAN ID に設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.2 E	このコマンドが導入されました。

次に、呼出端末 ID タイプを AP のイーサネット MAC アドレスに設定する例を示します。

```
デバイス(config)# wireless security dot1x radius mac-authentication call-station-id
ap-ethmac-only
```

wireless security dot1x radius mac-authentication mac-delimiter

MAC 認証属性を設定するには、**wireless security dot1x radius mac-authentication mac-delimiter** コマンドを使用します。

MAC 認証属性を削除するには、このコマンドの **no** 形式を使用します。

wireless security dot1x radius mac-authentication mac-delimiter {**colon** | **hyphen** | **none** | **single-hyphen** }

構文の説明

colon	デリミタをコロンに設定します。
hyphen	デリミタをハイフンに設定します。
none	デリミタを無効にします。
single-hyphen	デリミタをシングル ハイフンに設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.6.0 E	このコマンドが導入されました。

次に、MAC 認証属性をコロンに設定する例を示します。

```
デバイス(config)# Scurity dot1x radius mac-authentication mac-delimiter colon
```

wireless security web-auth retries

特定の WLAN で Web 認証の再試行を有効にするには、 **wireless wireless security web-auth retries** コマンドを使用します。無効にするには、このコマンドの **no** 形式を使用します。

wireless securityweb-authretries*retries*
nowireless securityweb-authretries

構文の説明

wireless security web-auth	特定の WLAN で Web 認証を有効にします。
retries *retries*	Web 認証要求の最大再試行回数を指定します。範囲は 0 ～ 30 です。デフォルト値は 3 です。

コマンド デフォルト

コマンド モード

config

コマンド履歴

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

使用上のガイドライン

なし

次に、特定の WLAN で Web 認証の再試行を有効にする例を示します。

```
デバイス#configure terminal
デバイス# wireless security web-auth retries 10
```

wireless tag policy

ワイヤレス タグ ポリシーを設定するには、**wireless tag policy** コマンドを使用します。

wireless tag policy *policy-tag*

構文の説明

policy-tag	ワイヤレスタグポリシーの名前。

コマンド デフォルト

デフォルトのポリシー タグは、default-policy-tag です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、ワイヤレス ポリシー タグを設定する例を示します。

```
Device(config)# wireless tag policy guest-policy
```

wireless tag rf

無線周波数（RF）タグを設定するには、**wireless tag rf** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

wireless tag rf *rf-tg-name*

構文の説明

wireless tag rf	RFタグのパラメータを設定します。
rf-tg-name	RF タグの名前を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、ワイヤレスタグの無線周波数（RF）を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless tag rf rf-tag-name
```

wireless tag site

ワイヤレス サイト タグを設定するには、**wireless tag site** *site-tag* コマンドを使用します。

wireless tag site *site-tag*

構文の説明

site-tag	サイト タグの名前。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、サイト タグを設定する例を示します。

```
Device(config)# wireless tag site test-site
```

wireless wps ap-authentication

アクセス ポイントのネイバー認証を設定するには、**wireless wps ap-authentication** コマンドを使用します。アクセス ポイントのネイバー認証を削除するには、このコマンドの no 形式を使用します。

wireless wps ap-authentication [**threshold** *value*]
no wireless wps ap-authentication [**threshold**]

構文の説明

threshold *value*	（任意）無線 LAN の WMM 対応クライアントであることを指定します。しきい値（1 ～ 255）。

コマンド デフォルト

なし。

コマンド モード

config

コマンド履歴

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

使用上のガイドライン

なし

次に、WMM 対応クライアントのしきい値を設定する例を示します。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#wireless wps ap-authentication threshold 65
```

wireless wps ap-authentication threshold

アクセスポイントのネイバー認証のアラームトリガーしきい値を設定するには、 **wireless wps ap-authentication threshold** コマンドを使用します。アクセス ポイントのネイバー認証を削除するには、このコマンドの no 形式を使用します。

wireless wps ap-authentication threshold *value*

no wireless wps ap-authentication threshold *value*

構文の説明

threshold *value*	（任意）無線 LAN の WMM 対応クライアントであることを指定します。しきい値の範囲は 1 ～ 255 です。デフォルト値は 1 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

なし

例

次に、アクセスポイントのネイバー認証のアラームトリガーしきい値を設定する例を示します。

```
Device(config)# wireless wps ap-authentication threshold 1
```

wireless wps client-exclusion

クライアント除外ポリシーを設定するには、 **wireless wps client-exclusion** コマンドを使用します。クライアント除外ポリシーを削除するには、このコマンドの **no** 形式を使用します。

wireless wps client-exclusion {**all** | **dot11-assoc** | **dot11-auth** | **dot1x-auth** | **dot1x-timeout** | **ip-theft** | **web-auth**}
no wireless wps client-exclusion {**all** | **dot11-assoc** | **dot11-auth** | **dot1x-auth** | **dot1x-timeout** | **ip-theft** | **web-auth**}

構文の説明

dot11-assoc	コントローラが 802.11 アソシエーションに連続 5 回失敗すると、6 回目の試行を除外することを指定します。
dot11-auth	コントローラが 802.11 認証に連続 5 回失敗すると、6 回目の試行を除外することを指定します。
dot1x-auth	コントローラが 802.11X 認証に連続 5 回失敗すると、6 回目の試行を除外することを指定します。
dot1x-timeout	タイムアウト時および応答がない場合の除外を有効にします。
ip-theft	IP アドレスがすでに別のデバイスに割り当てられている場合は、コントローラがクライアントを除外することを指定します。 詳細については、「使用上のガイドライン」セクションを参照してください。
web-auth	コントローラが Web 認証に連続 3 回失敗すると、4 回目の試行を除外することを指定します。
all	コントローラが上記のすべての理由でクライアントを除外することを指定します。

コマンド デフォルト

イネーブル

コマンド モード

config

コマンド履歴

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

使用上のガイドライン

IP 窃盗シナリオに、古い Cisco IOS XE リリースと Cisco IOS XE Denali 16.x リリースの相違点があります。

古い Cisco IOS XE リリース	Cisco IOS XE Denali 16.x リリース
優先順位に従って、有線クライアントはワイヤレス クライアントよりも優先され、DHCP IP はスタティック IP よりも優先されます。クライアントのセキュリティ タイプはチェックされません。すべてのクライアント タイプのセキュリティが同じ優先順位で処理されます。 既存のバインドが優先順位の高いソースに由来する場合、新しいバインドは無視され、IP 窃盗の信号が送信されます。既存のバインドが新しいバインドと同じ優先順位のソースに由来する場合、新しいバインドは無視され、IP 窃盗の信号が送信されます。その結果、2 つのホストが同じ IP を使用してトラフィックを送信した場合、バインドは切り替わらないことになります。最初のバインドのみがソフトウェアに格納されます。新しいバインドが優先順位のより高いソースに由来する場合、既存のバインドは置き換えられます。その結果、既存のバインドの IP 窃盗通知と、新しいバインドの通知が送信されます。	有線とワイヤレスの間に基本的な相違はありません。重視されるのは、エントリの信頼性（優先度）、エントリの伝達経路となった機能（ARP、DHCP、ND など）、およびポートに付与されているポリシーです。優先度が等しい場合、古いエントリが到達可能であれば、IP テイクオーバーは拒否されます。IP テイクオーバーは、更新が信頼できるポートから発信され、新しいエントリが DHCP サーバから IP アドレスを取得した場合に発生します。そうでない場合には、明示的に許可する必要があります。古いエントリが新しいより信頼できるエントリに置き換えられた場合、IP 窃盗は報告されません。

次に、802.11 アソシエーションに連続 5 回失敗した場合にクライアントを無効にする例を示します。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#wireless wps client-exclusion dot11-assoc
```

wireless wps mfp

さまざまな管理フレーム保護（MFP）パラメータを設定するには、**wireless wps mfp** コマンドを使用します。

wireless wps mfp **ap-impersonation** | **key-refresh-interval** *interval*

構文の説明

interval	MFP キーの更新間隔を時間単位で指定します。有効な範囲は 1 ～ 24 です。デフォルト値は 24 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

次に、さまざまな管理フレーム保護（MFP）パラメータを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless wps mfp key-refresh-interval 1
```

wireless wps mfp ap-impersonation

AP 偽装検出を設定するには、**wireless wps mfp ap-impersonation** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps mfp ap-impersonation

no wireless wps mfp ap-impersonation

構文の説明

ap-impersonation	AP 偽装検出を設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

なし

例

次に、AP 偽装検出を設定する例を示します。

```
Device(config)# wireless wps mfp ap-impersonation
```

wireless wps rogue

さまざまな不正パラメータを設定するには、 **wireless wps rogue** コマンドを使用します。

wireless wps rogue {**adhoc** | **client**} [{**alert** *mac-addr* | **contain** *mac-addr no-of-aps*}]

構文の説明

adhoc	Independent Basic Service Set（IBSS またはアドホック）の不正なアクセス ポイントのステータスを設定します。
client	不正なクライアントを設定します。
alert *mac-addr*	アドホックの不正を検出すると SNMP トラップを生成し、システム管理者に即座にアラートを発信して、アドホックの不正アクセス ポイントの MAC アドレスに対し必要な措置を促します。
contain *mac-addr no-of-aps*	加害デバイスを阻止し、その信号が正規クライアントを阻害しないようにします。 アドホックの不正なアクセス ポイントをアクティブに阻止するために割り当てられた、シスコのアクセス ポイントの最大数（1 ～ 4）。

コマンド デフォルト

なし。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし

次に、システム管理者に即座にアラートを生成し、アドホックの不正アクセス ポイントの MAC アドレスに対し必要な措置を促す例を示します。

```
デバイス#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)#wireless wps rouge adhoc alert mac_addr
```

wireless wps rogue network-assurance enable

不正ワイヤレス サービス アシュアランス（WSA）イベントを有効にするには、**wireless wps rogue network-assurance enable** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue network-assurance enable

no wireless wps rogue network-assurance enable

構文の説明

network-assurance enable	不正WSAイベントを有効にします。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

なし

例

次に、不正ワイヤレス サービス アシュアランス イベントを有効にする例を示します。

```
Device(config)# wireless wps rogue network-assurance enable
```

wireless wps rogue ap aaa

有効な AP MAC アドレスを検出するための AAA/ローカルデータベースの使用を設定するには、**wireless wps rogue ap aaa** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue ap aaa

no wireless wps rogue ap aaa

構文の説明

aaa	有効な AP MAC アドレスを検出するための AAA またはローカルデータベースの使用を設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

なし

例

次に、有効な AP MAC アドレスを検出するための AAA/ローカルデータベースの使用を設定する例を示します。

```
Device(config)# wireless wps rogue ap aaa
```

wireless wps rogue ap aaa polling-interval

不正 AP の AAA 検証間隔（秒単位）を設定するには、**wireless wps rogue ap aaa polling-interval** コマンドを使用します。設定を無効にするには、このコマンドの no 形式を使用します。

wireless wps rogue ap aaa polling-interval *60 - 86400*

no wireless wps rogue ap aaa polling-interval *60 - 86400*

構文の説明

aaa	有効な AP MAC アドレスを検出するための AAA またはローカルデータベースの使用を設定します。
polling-interval	不正 AP の AAA 検証間隔を設定します。
60 - 86400	AP の AAA 検証間隔（秒単位）を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし

例

次に、不正 AP の AAA 検証間隔（秒単位）を設定する例を示します。

```
Device(config)# wireless wps rogue ap aaa polling-interval 120
```

wireless wps rogue ap init-timer

不正 AP の初期化タイマーを設定するには、**wireless wps rogue ap init-timer** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue ap init-timer

no wireless wps rogue ap init-timer

構文の説明

init-timer	不正APの初期化タイマーを設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

なし

例

次に、不正 AP の初期化タイマーを設定する例を示します。

```
Device(config)# wireless wps rogue ap init-timer
```

wireless wps rogue ap mac-address rldp initiate

不正 AP で Rogue Location Discovery Protocol を開始および設定するには、**wireless wps rogue ap mac-address rldp initiate** コマンドを使用します。

wireless wps rogue ap mac-address <*MAC Address*> **rldp initiate**

構文の説明

wps	WPS 設定を設定します。
rogue	グローバル不正デバイスを設定します。
ap mac-address <*MAC Address*>	AP の MAC アドレス。
rldp initiate	不正 AP で RLDP を開始します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

なし

例

次に、不正 AP で Rogue Location Discovery Protocol を開始および設定する例を示します。

```
Device# wireless wps rogue ap mac-address 10.1.1 rldp initiate
```

wireless wps rogue ap notify-min-rssi

不正 AP の最小 RSSI 通知しきい値を設定するには、**wireless wps rogue ap notify-min-rssi** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue ap notify-min-rssi

no wireless wps rogue ap notify-min-rssi

構文の説明

notify-min-rssi	不正 AP の最小 RSSI 通知しきい値を設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

なし

例

次に、不正 AP の最小 RSSI 通知しきい値を設定する例を示します。

```
Device(config)# wireless wps rogue ap notify-min-rssi
```

wireless wps rogue ap notify-rssi-deviation

不正 AP の RSSI 偏差通知しきい値を設定するには、**wireless wps rogue ap notify-rssi-deviation** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue ap notify-rssi-deviation

no wireless wps rogue ap notify-rssi-deviation

構文の説明

notify-rssi-deviation	不正 AP の RSSI 偏差通知しきい値を設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

なし

例

次に、不正 AP の RSSI 偏差通知しきい値を設定する例を示します。

```
Device(config)# wireless wps rogue ap notify-rssi-deviation
```

wireless wps rogue ap rldp alarm-only

Rogue Location Discovery Protocol（RLDP）を設定し、不正が検出された場合にアラームを発生させるには、**wireless wps rogue ap rldp alarm-only** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue ap rldp alarm-only

no wireless wps rogue ap rldp alarm-only

構文の説明

alarm-only	RLDP を設定し、不正が検出された場合にアラームを発生させます。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

なし

例

次に、RLDP を設定し、不正が検出された場合にアラームを発生させる例を示します。

```
Device(config)# wireless wps rogue ap rldp alarm-only
```

wireless wps rogue ap rldp alarm-only monitor-ap-only

モニター AP でのみ RLDP を実行するには、**wireless wps rogue ap rldp alarm-only monitor-ap-only** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue ap rldp alarm-only monitor-ap-only

no wireless wps rogue ap rldp alarm-only monitor-ap-only

構文の説明

monitor-ap-only	モニター AP でのみ RLDP を実行します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

なし

例

次に、モニター AP でのみ RLDP を実行する例を示します。

```
Device(config)# wireless wps rogue ap rldp alarm-only monitor-ap-only
```

wireless wps rogue ap rldp auto-contain

不正が検出された場合の RLDP、アラーム、自動阻止を設定するには **wirelesswps rogueaprldp auto-contain** コマンドを使用します。アラームを無効にするには、このコマンドの **no** 形式を使用します。

[no] wireless wps rogue ap rldp auto-contain monitor-ap-only

構文の説明

monitor-ap-only	モニタ AP のみで RLDP を実行します。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。
Cisco IOS XE 3.7.3E	このコマンドの **no** 形式が導入されました。

例

次に、検出された不正に対するアラームを設定する例を示します。

デバイス**wireless wps rogue ap rldp auto-contain**

wireless wps rogue ap rldp retries

不正 AP での RLDP 再試行回数を設定するには、**wireless wps rogue ap rldp retries** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue ap rldp retries

no wireless wps rogue ap rldp retries

構文の説明

retries	不正 AP での RLDP 再試行回数を設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

なし

例

次に、不正 AP での RLDP 再試行回数を設定する例を示します。

```
Device(config)# wireless wps rogue ap rldp retries
```

wireless wps rogue ap rldp schedule

RLDP スケジューリングを設定するには、**wireless wps rogue ap rldp schedule** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue ap rldp schedule

no wireless wps rogue ap rldp schedule

構文の説明

schedule	RLDP スケジューリングを設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

なし

例

次に、RLDP スケジューリングを設定する例を示します。

```
Device(config)# wireless wps rogue ap rldp schedule
```

wireless wps rogue ap rldp schedule day

RLDP スケジューリングを実行する日を設定するには、**wireless wps rogue ap rldp schedule day** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue ap rldp schedule day { **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** } **start** *[HH:MM:SS]* **end** *[HH:MM:SS]*

no wireless wps rogue ap rldp schedule day { **friday** | **monday** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday** } **start** *[HH:MM:SS]* **end** *[HH:MM:SS]*

構文の説明

day {**friday**	**monday**	**saturday**	**sunday**	**thursday**	**tuesday**	**wednesday**}	RLDP スケジューリングを実行する曜日を設定します。
start *[HH:MM:SS]*	その日の RLDP スケジュールの開始時刻を設定します。
end *[HH:MM:SS]*	その日の RLDP スケジュールの終了時刻を設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

なし

例

次に、RLDP スケジューリングを実行する曜日を設定する例を示します。

```
Device(config)# wireless wps rogue ap rldp schedule day friday start 10:10:10 end 15:15:15
```

wireless wps rogue ap timeout

不正 AP の期限切れ時間（秒単位）を設定するには、**wireless wps rogue ap timeout** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue ap timeout *240-3600*

no wireless wps rogue ap timeout *240-3600*

構文の説明

rogue ap timeout	不正 AP の期限切れ時間（秒単位）を設定します。
240-3600	不正エントリがフラッシュされるまでの秒数を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし

例

次に、不正 AP の期限切れ時間（秒単位）を設定する例を示します。

```
Device(config)# wireless wps rogue ap timeout 250
```

wireless wps rogue auto-contain

自動封じ込めレベルを設定し、モニター AP モードの自動封じ込めを設定するには、**wireless wps rogue auto-contain** コマンドを使用します。この設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue auto-contain ｛ **level** *1 - 4* ｜ **monitor-ap-only** ｝

no wireless wps rogue auto-contain ｛ **level** *1 - 4* ｜ **monitor-ap-only** ｝

構文の説明

auto-contain	不正なデバイスの自動封じ込めを設定します。
level	自動封じ込めレベルを設定します。
1 - 4	自動封じ込めレベルを指定します。
monitor-ap-only	モニターAPモードの自動封じ込めを設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし

例

次に、自動封じ込めレベルを設定し、モニター AP モードの自動封じ込めを設定する例を示します。

```
Device(config)# wireless wps rogue auto-contain level 2
Device(config)# wireless wps rogue auto-contain monitor-ap-only
```

wireless wps rogue client aaa

不正クライアントの有効な MAC アドレスを検出するための AAA またはローカルデータベースの使用を設定するには、**wireless wps rogue client aaa** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue client aaa

no wireless wps rogue client aaa

構文の説明

aaa	不正クライアントの有効な MAC アドレスを検出するための AAA またはローカルデータベースの使用を設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

なし

例

次に、不正クライアントの有効な MAC アドレスを検出するための AAA またはローカルデータベースの使用を設定する例を示します。

```
Device(config)# wireless wps rogue client aaa
```

wireless wps rogue client mse

不正クライアントの有効な MAC アドレスを検出するためのモビリティサービスエンジン（MSE）を設定するには、**wireless wps rogue client mse** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue client mse

no wireless wps rogue client mse

構文の説明

mse	不正クライアントの有効なMACアドレスを検出するためのMSEを設定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

なし

例

次に、不正クライアントの有効な MAC アドレスを検出するためのモビリティサービスエンジン（MSE）を設定する例を示します。

```
Device(config)# wireless wps rogue client mse
```

wireless wps rogue client client-threshold

不正 AP SNMP トラップしきい値ごとに不正クライアントを設定するには、**wireless wps rogue client client-threshold** コマンドを使用します。この設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue client client-threshold *0 - 256*

no wireless wps rogue client client-threshold *0 - 256*

構文の説明

rogue client	不正クライアントを設定します。
client-threshold	不正 AP SNMP トラップしきい値ごとに不正なクライアントを設定します。
0 - 256	クライアントしきい値を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし

例

次に、不正 AP SNMP トラップしきい値ごとに不正クライアントを設定する例を示します。

```
Device(config)# wireless wps rogue ap timeout 250
```

wireless wps rogue client notify-min-rssi

不正クライアントの最小 RSSI 通知しきい値を設定するには、**wireless wps rogue client notify-min-rssi** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue client notify-min-rssi *-128 - -70*

no wireless wps rogue client notify-min-rssi *-128 - -70*

構文の説明

rogue clients	不正クライアントを設定します。
notify-min-rssi	不正なクライアントの最小RSSI通知しきい値を設定します。
-128 - -70	RSSI しきい値をデシベル単位で指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし

例

次に、不正クライアントの最小 RSSI 通知しきい値を設定する例を示します。

```
Device(config)# wireless wps rogue client notify-min-rssi -125
```

wireless wps rogue client notify-rssi-deviation

不正クライアントの RSSI 偏差通知しきい値を設定するには、**wireless wps rogue client notify-rssi-deviation** コマンドを使用します。この設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue client notify-rssi-deviation *0 - 10*

no wireless wps rogue client notify-rssi-deviation *0 - 10*

構文の説明

notify-rssi-deviation	不正なクライアントのRSSI偏差通知しきい値を設定します。
0 - 10	RSSI しきい値をデシベル単位で指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし

例

次に、不正クライアントの RSSI 偏差通知しきい値を設定する例を示します。

```
Device(config)# wireless wps rogue client notify-rssi-deviation 6
```

wireless wps rogue detection

さまざまな不正検出パラメータを設定するには、 **wireless wps rogue detection** コマンドを使用します。

wireless wps rogue detection [{**min-rssi** *rssi* | **min-transient-time** *transtime*}]

構文の説明

min-rssi *rssi*	不正に必要な最小RSSI値を設定します。これは、APが不正を検出し、deviceで不正エントリが作成されるために必要な値です。
min-transient-time *transtime*	不正が初めてスキャンされた後、APで不正スキャンを定期的に実行する間隔を入力します。

コマンド デフォルト

なし。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし。

次に、不正検出のための最小RSSI値と、一時的な定期的スキャンの最小間隔を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless wps rogue detection min-rssi 100
デバイス(config)# wireless wps rogue detection min-transient-time 500
デバイス(config)# end
```

wireless wps rogue notify-syslog

不正イベントの syslog 通知を有効にするには、**wireless wps rogue notify-syslog** コマンドを使用します。

wireless wps rogue notify-syslog

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

例

次に、不正イベントの syslog 通知を有効にする例を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue notify-syslog
```

wireless wps rogue rule

不正分類ルールを設定するには、 **wireless wps rogue rule** コマンドを使用します。

wireless wps rogue rule *rule-name* **priority** *priority* {**classify**{**friendly** | **malicious**} | **condition** {**client-count number** | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**} | **default** | **exit** | **match**{**all** | **any**} | **no** | **shutdown**}

構文の説明

rule *rule-name*	ルール名を指定します。
priority *priority*	特定のルールの優先順位を変更し、それに応じて、リスト内のその他のルールの優先順位を調整します。
classify	ルールの分類を指定します。
friendly	ルールを危険性のないルールとして分類します。
malicious	ルールを悪意のあるルールとして分類します。
condition {**client-count number** | **duration** | **encryption** | **infrastructure** | **rssi** | **ssid**}	不正なアクセス ポイントが満たす必要のあるルールに条件を指定します。 設定する条件のタイプ。条件タイプは以下のとおりです。 • client-count：最小数のクライアントが不正なアクセス ポイントにアソシエートされていることが条件となります。有効な範囲は 1 ～ 10 です。 • duration：不正なアクセス ポイントが最短期間で検出されることが条件となります。有効な範囲は 0 ～ 3600 秒です。 • encryption：アドバタイズされた WLAN で暗号化が無効になっている必要があります。 • infrastructure：SSID がコントローラで認識されている必要があります • rssi：不正なアクセス ポイントには、最小の RSSI 値が必要です。範囲は、–95 ～ -50 dBm です。 • ssid：不正なアクセス ポイントには、特定の SSID が必要です。
default	コマンドをデフォルトに設定します。
exit	サブモードを終了します。
match {**all** | **any**}	ルールの一致基準を設定します。検出された不正なアクセス ポイントがルールに一致していると見なされ、そのルールの分類タイプが適用されるためには、ルールで定義されているすべての条件を満たす必要があるか、一部の条件を満たす必要があるかを指定します。
no	コマンドを無効にするか、デフォルト値を設定します。

shutdown	システムをシャットダウンします。

コマンド デフォルト

なし。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし。

次に、不正アクセス ポイントを Friendly として組織および表示できるルールを作成する例を示します。

```
デバイス# configure terminal
デバイス(config)# wireless wps rogue rule ap1 priority 1
デバイス(config-rule)# classify friendly
デバイス(config)# end
```

wireless wps rogue scale mode hybrid

不正スケールのハイブリッドモード（優先順位の高い不正 AP 用に予約された未使用のクォータは、スペースが利用可能な場合、優先順位の低い不正 AP によって使用できます）を設定するには、**wireless wps rogue scale mode hybrid** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue scale mode hybrid

no wireless wps rogue scale mode hybrid

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

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

例

次に、不正スケールのハイブリッドモードを設定する例を示します。

```
Device(config)# wireless wps rogue scale mode hybrid
```

wireless wps rogue scale priority

不正分類の優先順位を設定するには、**wireless wps rogue scale priority malicious** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue scale priority malicious { **high** | **highest** | **low** | **medium** } **custom** { **high** | **highest** | **low** | **medium** } **unclassified** { **high** | **highest** | **low** | **medium** } **friendly** { **high** | **highest** | **low** | **medium** }

no wireless wps rogue scale priority malicious { **high** | **highest** | **low** | **medium** } **custom** { **high** | **highest** | **low** | **medium** } **unclassified** { **high** | **highest** | **low** | **medium** } **friendly** { **high** | **highest** | **low** | **medium** }

構文の説明

malicious	悪意のある不正 AP の優先順位を設定します。
{ **high** | **highest** | **low** | **medium** }	不正 AP ストレージの優先順位を、高、最高、中、低として示します。
custom	カスタム分類された不正 AP の優先順位を設定します。
unclassified	未分類の不正 AP の優先順位を設定します。
friendly	危険性のない不正 AP の優先順位を設定します。

コマンド デフォルト

なし

Malicious のデフォルト値は **highest**、Custom のデフォルト値は **high**、Unclassified のデフォルト値は **medium**、Friendly のデフォルト値は **low** です。

コマンド モード

グローバル設定

コマンド履歴

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

例

次に、不正分類の優先順位を設定する例を示します。

```
Device(config)# wireless wps rogue scale priority malicious highest custom high
unclassified medium friendly low
```

wireless wps rogue scale quota

最大スケールの不正 AP の優先順位付けとクォータを設定するには、**wireless wps rogue scale quota** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue scale quota malicious *percentage-malicious-rogue-AP* **custom** *percentage-custom-rogue-AP* **unclassified** *percentage-unclassified-rogue-AP* **friendly** *percentage-friendly-rogue-AP*

no wireless wps rogue scale quota malicious *percentage-malicious-rogue-AP* **custom** *percentage-custom-rogue-AP* **unclassified** *percentage-unclassified-rogue-AP* **friendly** *percentage-friendly-rogue-AP*

構文の説明

malicious	悪意のある不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージを示します。
percentage-malicious-rogue-AP	悪意のある不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージで値を指定します。値の範囲は 0 ～ 100 です。
custom	カスタム不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージを示します。
percentage-custom-rogue-AP	カスタム不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージで値を指定します。値の範囲は 0 ～ 100 です。
unclassified	未分類の不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージを示します。
percentage-unclassified-rogue-AP	未分類の不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージで値を指定します。値の範囲は 0 ～ 100 です。
friendly	危険性のない不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージを示します。
percentage-friendly-rogue-AP	危険性のない不正 AP 用に予約されている不正 AP スケールの合計のパーセンテージで値を指定します。値の範囲は 0 ～ 100 です。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

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

例

次に、最大スケールの不正 AP の優先順位付けとクォータを設定する例を示します。

```
Device(config)# wireless wps rogue scale quota malicious 5 custom 10 unclassified 3
friendly 5
```

wireless wps rogue security-level

ワイヤレス WPS の不正検出セキュリティレベルを設定するには、**wireless wps rogue security-level** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

wireless wps rogue security-level { **critical** | **custom** | **high** | **low** }

no wireless wps rogue security-level { **critical** | **custom** | **high** | **low** }

構文の説明

rogue security-level	不正検出セキュリティ レベルを設定します。
critical	機密性の高い展開向けの不正検出設定を指定します。
custom	カスタマイズ可能なセキュリティレベルを指定します。
high	中規模な展開向けの不正検出設定を指定します。
low	小規模な展開向けの基本不正検出設定を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし

例

次に、ワイヤレス WPS の不正検出セキュリティレベルを設定する例を示します。

```
Device(config)# wireless wps rogue security-level critical
```

wireless-default radius server

複数の RADIUS サーバーを設定するには、**wireless-default radius server** コマンドを使用します。

wireless-default radius server *IP* **key** *secret*

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

このユーティリティを使用すると、最大 10 の RADIUS サーバーを設定できます。

例

次に、複数の RADIUS サーバーを設定する例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wireless-default radius server 9.2.58.90 key cisco123
デバイス(config)# end
```

wlan policy

ポリシー プロファイルを WLAN プロファイルにマッピングするには、 **wlan policy** コマンドを使用します。

wlan *wlan-name* **policy** *policy-name*

構文の説明

wlan-name	WLAN プロファイルの名前。
policy	ポリシープロファイルを WLAN プロファイルにマッピングします。
policy-name	ポリシー プロファイルの名前。

コマンド デフォルト

なし

コマンド モード

config-policy-tag

コマンド履歴

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

wmm

WLAN での WMM を設定するには、**wmm** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

wmm {**allowed** | **require**}

[no] wmm

構文の説明

wmm	WMM（WME）を設定します。
allowed	WLAN での WMM の使用を許可します。
require	WLAN 上に WMM クライアントが必要です。

コマンド デフォルト

なし

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。

例

次に、WLAN での WMM を設定する例を示します。

```
Device(config-wlan)#wmm allowed
```

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。