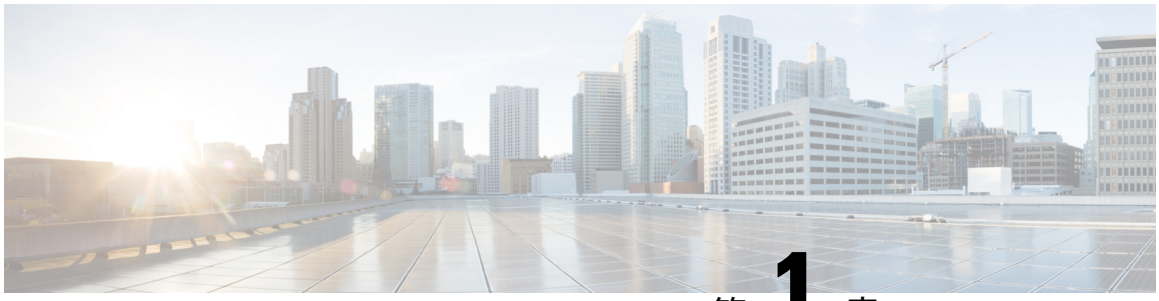
Cisco IOS XE Gibraltar 16.12.x（Catalyst 3650 スイッチ）コマンド リファレンス

初版：2019 年 7 月 31 日

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

目 次



第 1 章

コマンドライン インターフェイスの使用

この章は、次の内容で構成されています。

コマンドライン インターフェイスの使用

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

コマンド モードについて

Cisco IOS ユーザインターフェイスは、いくつかのモードに分かれています。使用可能なコマンドは、現在のモードによって異なります。各コマンドモードで使用できるコマンドのリストを取得するには、システムプロンプトで疑問符（?）を入力します。

スイッチとのセッションを開始するときは、ユーザモード（別名ユーザ EXEC モード）が有効です。ユーザ EXEC モードでは、限られた一部のコマンドしか使用できません。たとえば、現在の設定ステータスを示す **show** コマンドや、カウンタまたはインターフェイスを消去する **clear** コマンドなど、ほとんどのユーザ EXEC コマンドは 1 回限りのコマンドです。スイッチの再起動時には、ユーザ EXEC コマンドは保存されません。

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

コンフィギュレーション モード（グローバル、インターフェイス、およびライン）を使用して、実行コンフィギュレーションを変更できます。コンフィギュレーションを保存するとこれらのコマンドは保存され、スイッチの再起動時に使用されます。各種のコンフィギュレーション モードにアクセスするには、まずグローバル コンフィギュレーション モードを開始する必要があります。グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モードおよびライン コンフィギュレーション モードを開始できます。

次の表に、主要なコマンドモード、各モードへのアクセス方法、各モードで表示されるプロンプト、およびモードの終了方法を示します。表の例では、ホスト名として*Switch*を使用しています。

表 *1*: コマンドモードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	スイッチとのセッションを開始します。	`Switch>`	**logout**または**quit**の入力。	このモードを使用して次の作業を行います。 • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権EXEC	ユーザ EXEC モードで、**enable** コマンドを入力します。	`デバイス#`	終了するには、**disable** と入力します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure** コマンドを入力します。	`デバイス (config)#`	終了して特権 EXEC モードに戻るには、**exit** または **end** を入力するか、**Ctrl+Z** を押します。	このモードを使用して、スイッチ全体に適用されるパラメータを設定します。
VLAN コンフィギュレーション	グローバル コンフィギュレーション モードで、**vlan** *vlan-id* コマンドを入力します。	`デバイス (config-vlan)#`	グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを入力します。 特権 EXEC モードに戻るには、**Ctrl+Z** を押すか、**end** を入力します。	このモードを使用して、VLAN（仮想 LAN）パラメータを設定します。VTP モードがトランスペアレントであるときは、拡張範囲 VLAN（VLAN ID が 1006 以上）を作成してスイッチのスタートアップ コンフィギュレーション ファイルに設定を保存できます。

モード	アクセス方法	プロンプト	終了方法	モードの用途
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、**interface** コマンドを入力し、インターフェイスを指定します。	デバイス(config-if)#	終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権 EXEC モードに戻るには、**Ctrl+Z** を押すか、**end** を入力します。	このモードを使用して、イーサネットポートのパラメータを設定します。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードで回線を指定するには、**line vty** または **line console** コマンドを入力します。	デバイス(config-line)#	終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権 EXEC モードに戻るには、**Ctrl+Z** を押すか、**end** を入力します。	このモードを使用して、端末回線のパラメータを設定します。

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

ヘルプシステムについて

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

表 *2:* ヘルプの概要

コマンド	目的
help	コマンドモードのヘルプ システムの簡単な説明を表示します。
abbreviated-command-entry **?** デバイス# **di?** dir disable disconnect	特定のストリングで始まるコマンドのリストを表示します。

コマンド	目的
abbreviated-command-entry <Tab> デバイス# **sh conf**<tab> デバイス# **show configuration**	特定のコマンド名を補完します。
? Switch> **?**	特定のコマンドモードで使用可能なすべてのコマンドをリストします。
command **?** Switch> **show ?**	コマンドに関連するキーワードを一覧表示します。
command keyword **?** デバイス(config)# **cdp holdtime ?** <10-255> Length of time (in sec) that receiver must keep this packet	キーワードに関連する引数を一覧表示します。

コマンドの省略形

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

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

```
デバイス# show conf
```

コマンドの no 形式および default 形式の概要

ほとんどのコンフィギュレーション コマンドには、**no** 形式もあります。**no** 形式は一般に、特定の機能または動作を無効にする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、インターフェイス コンフィギュレーション コマンド **no shutdown** を使用すると、インターフェイスのシャットダウンが取り消されます。キーワード **no** なしでコマンドを使用すると、無効にされた機能を再度有効にしたり、デフォルトで無効になっている機能を有効にすることができます。

コンフィギュレーション コマンドには、**default** 形式もあります。コマンドの **default** 形式は、コマンド設定をデフォルトに戻します。ほとんどのコマンドはデフォルトで無効に設定されているため、**default** 形式を使用しても **no** 形式と同じ結果になります。ただし、デフォルトで有効に設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもありま

す。このような場合、**default** コマンドはそのコマンドを有効にし、変数をそのデフォルト値に設定します。

CLI のエラーメッセージについて

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

表 *3 : CLI* の代表的なエラーメッセージ

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

コンフィギュレーション ロギングの使用方法

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

（注） CLI または HTTP の変更のみがログとして記録されます。

コマンド履歴の使用

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

コマンド履歴バッファ サイズの変更

デフォルトでは、10のコマンドラインが履歴バッファに保存されます。現在の端末セッションまたは特定回線のすべてのセッションで、この数を変更できます。これらの手順は任意です。

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

```
デバイス# terminal history [size number-of-lines]
```

指定できる範囲は 0 ～ 256 です。

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

```
デバイス(config-line)# history [size number-of-lines]
```

指定できる範囲は 0 ～ 256 です。

コマンドの呼び出し

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

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

表 *4:* コマンドの呼び出し

アクション	結果
Ctrl+P キーまたは↑キーを押します。	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。キーを押すたびに、より古いコマンドが順次表示されます。
Ctrl+N キーまたは↓キーを押します。	Ctrl+P または↑キーでコマンドを呼び出した後で、履歴バッファ内のより新しいコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。

アクション	結果
show history デバイス(config)# **help**	特権 EXEC モードで、直前に入力したいくつかのコマンドを一覧表示します。表示されるコマンドの数は、**terminal history** グローバル コンフィギュレーション コマンドおよび **history** ライン コンフィギュレーション コマンドの設定値によって制御されます。

コマンド履歴機能の無効化

コマンド履歴機能は、自動的に有効になっています。現在の端末セッションまたはコマンドラインで無効にできます。これらの手順は任意です。

現在の端末セッションでこの機能を無効にするには、**terminal no history** 特権 EXEC コマンドを使用します。

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

編集機能の使用方法

ここでは、コマンドラインの操作に役立つ編集機能について説明します。

編集機能の有効化および無効化

拡張編集モードは自動的に有効になりますが、無効にする、再び有効にする、または特定の回線で拡張編集機能を使用できるように設定できます。これらの手順は任意です。

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

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

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

```
デバイス# terminal editing
```

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

```
デバイス(config-line)# editing
```

キーストロークによるコマンドの編集

このテーブルに、コマンドラインの編集に必要なキーストロークを示します。これらのキーストロークは任意です。

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

表 *5:* キーストロークによるコマンドの編集

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

機能	キーストローク	目的
不要なエントリを削除します。	Delete キーまたは Backspace キーを押します。	カーソルの左にある文字を消去します。
	Ctrl+D を押します。	カーソル位置にある文字を削除します。
	Ctrl+K を押します。	カーソル位置からコマンドラインの末尾までのすべての文字を削除します。
	Ctrl+U または Ctrl+X を押します。	カーソル位置からコマンドラインの先頭までのすべての文字を削除します。
	Ctrl+W を押します。	カーソルの左にある単語を削除します。
	Esc+D を押します。	カーソルの位置から単語の末尾までを削除します。
ワードを大文字または小文字にします。または、一連の文字をすべて大文字にします。	Esc+C を押します。	カーソル位置のワードを大文字にします。
	Esc+L を押します。	カーソルの場所にある単語を小文字にします。
	Esc+U を押します。	カーソルの位置から単語の末尾までを大文字にします。
特定のキーストロークを実行可能なコマンド（通常はショートカット）として指定します。	Ctrl+V または Esc+Q キーを押します。	

機能	キーストローク	目的
1行または1画面下へスクロールして、端末画面に収まりきらない表示内容を表示させます。 （注） **show** コマンドの出力など、端末画面に一度に表示できない長い出力では、Moreプロンプトが使用されます。Moreプロンプトが表示された場合は、Returnキーおよび Spaceキーを使用してスクロールできます。	Return キーを押します。	1 行下にスクロールします。
	Space キーを押します。	1 画面分下にスクロールします。
スイッチから画面にメッセージが突然送られた場合に、現在のコマンドラインを再表示します。	Ctrl+L または Ctrl+R を押します。	現在のコマンドラインを再表示します。

画面幅よりも長いコマンドラインの編集

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

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

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

次の例では、**access-list** グローバル コンフィギュレーション コマンドエントリが1行分よりも長くなっています。最初にカーソルが行末に達すると、その行は 10 文字分だけ左へシフトされ、再表示されます。ドル記号（$）は、その行が左へスクロールされたことを表します。カーソルが行末に達するたびに、その行は再び 10 文字分だけ左へシフトされます。

```
デバイス(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
デバイス(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
```

```
デバイス(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
デバイス(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

コマンドの入力が終わった後、Ctrl+A を押して全体の構文をチェックし、その後 Return キーを押してコマンドを実行してください。行末に表示されるドル記号（$）は、その行が右へスクロールされたことを表します。

```
デバイス(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

ソフトウェアでは、端末画面は 80 カラム幅であると想定されています。画面の幅が異なる場合は、**terminal width** 特権 EXEC コマンドを使用して端末の幅を設定します。

ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンドエントリを呼び出して変更できます。

show および more コマンド出力の検索およびフィルタリング

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

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

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

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

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

```
デバイス# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet1/0/1 is up, line protocol is down
GigabitEthernet1/0/2 is up, line protocol is up
```

CLI のアクセス

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

スイッチスタックおよびスタック メンバ インターフェイスは、アクティブスイッチを経由して管理します。スイッチごとにスタックメンバを管理することはできません。1 つまたは複数のスタックメンバのコンソールポートまたはイーサネット管理ポートを経由してactive switchへ接続できます。複数の CLI セッションをactive switchに使用する場合は注意が必要です。1 つのセッションで入力したコマンドは、別のセッションには表示されません。したがって、コマンドを入力したセッションを追跡できない場合があります。

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

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

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

コンソール接続または Telnet による CLI アクセス

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

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

次のいずれかの方法で、スイッチとの接続を確立できます。

- スイッチのコンソール ポートに管理ステーションまたはダイヤルアップ モデムを接続するか、イーサネット管理ポートに PC を接続します。コンソール ポートまたはイーサネット管理ポートへの接続については、スイッチのハードウェア インストレーション ガイドを参照してください。
- リモート管理ステーションから任意の Telnet TCP/IP または暗号化セキュア シェル（SSH）パッケージを使用します。スイッチは Telnet または SSH クライアントとのネットワーク接続が可能でなければなりません。また、スイッチにイネーブル シークレット パスワードを設定しておくことも必要です。

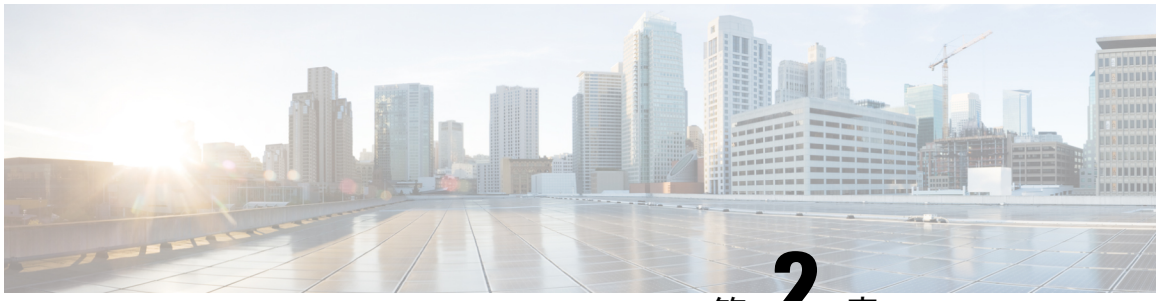
  スイッチは同時に最大 16 の Telnet セッションをサポートします。1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。

  スイッチは最大 5 つの安全な SSH セッションを同時にサポートします。

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

第 I 部

Cisco TrustSec



第 2 章

Cisco TrustSec コマンド

cts authorization list

TrustSec シードデバイスで使用する認証、許可、およびアカウンティング（AAA）サーバのリストを指定するには、Cisco TrustSec シードデバイスでグローバル コンフィギュレーション

モードで**cts authorization list**コマンドを使用します。認証中にリストの使用を停止するには、このコマンドの **no** 形式を使用します。

cts authorization list *server_list*

no cts authorization list *server_list*

構文の説明

server_list	Cisco TrustSec AAA サーバグループ。

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）

サポートされるユーザロール

管理者（Administrator）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、シードデバイスだけです。非シードデバイスは、TrustSec 環境データのコンポーネントとして TrustSec オーセンティケータのピアからの TrustSec AAA サーバリストを取得します。

次の例は、TrustSec シードデバイスの AAA コンフィギュレーションを表示します。

```
Device# cts credentials id Device1 password Cisco123
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
Device(config)# aaa authorization network MLIST group radius
Device(config)# cts authorization list MLIST
Device(config)# aaa accounting dot1x default start-stop group radius
Device(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key
AbCe1234
Device(config)# radius-server vsa send authentication
Device(config)# dot1x system-auth-control
Device(config)# exit
```

関連コマンド

コマンド	説明
show cts server-list	RADIUS サーバ設定を表示します。

cts credentials

ネットワークデバイスの TrustSec ID およびパスワードを指定するには、特権 EXEC モードで **cts credentials** コマンドを使用します。ログイン情報を削除するには、**clear cts credentials** コマンドを使用します。

cts credentials id *cts_id* **password** *cts_pwd*

構文の説明

credentials id *cts_id*	EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのデバイスが使用する Cisco TrustSec デバイス ID を指定します。*cts-id* 変数は、最大 32 文字で大文字と小文字を区別します。
password *cts_pwd*	EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのデバイスが使用するパスワードを指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザロール

管理者（Administrator）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

cts credentials コマンドは、EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのデバイスが使用する Cisco TrustSec デバイス ID およびパスワードを指定します。Cisco TrustSec のログイン情報はスタートアップ コンフィギュレーションではなくキーストアに保存されているため、Cisco TrustSec のログイン情報の状態取得は不揮発性生成（NVGEN）プロセスでは実行されません。デバイスは、Cisco Secure Access Control Server（ACS）から Cisco TrustSec アイデンティティを割り当てられるか、ACS から要求されたときに新しいパスワードを自動生成するようにできます。これらのログイン情報は、キーストアで保存され、実行コンフィギュレーションを保存する必要性がなくなります。Cisco TrustSec デバイス ID を表示するには、**show cts credentials** コマンドを使用します。保存されたパスワードは表示されません。

デバイス ID またはパスワードを変更するには、コマンドを再入力します。キーストアをクリアするには、**clear cts credentials** コマンドを使用します。

（注） Cisco TrustSec デバイス ID が変更された場合、Protected Access Credential（PAC）は古いデバイス ID に関連付けられており、新しいアイデンティティに対しては有効でないため、すべての PAC はキーストアから消去されます。

次に、Cisco TrustSec デバイス ID およびパスワードを設定する例を示します。

```
Device# cts credentials id cts1 password password1
CTS device ID and password have been inserted in the local keystore. Please make sure
that
the same ID and password are configured in the server database.
```

次に、Cisco TrustSec デバイス ID を cts_new、パスワードを password123 に変更する例を示します。

```
Device# cts credentials id cts_new pacssword password123
A different device ID is being configured.
This may disrupt connectivity on your CTS links.
Are you sure you want to change the Device ID? [confirm] y

TS device ID and password have been inserted in the local keystore. Please make sure
that
the same ID and password are configured in the server database.
```

次に、Cisco TrustSec デバイス ID およびパスワードの状態を表示する例を示します。

```
Device# show cts credentials

CTS password is defined in keystore, device-id = cts_new
```

関連コマンド

コマンド	説明
clear cts credentials	Cisco TrustSec デバイス ID とパスワードをクリアします。
show cts credentials	現在の Cisco TrustSec デバイス ID およびパスワードの状態を表示します。
show cts keystore	ハードウェアおよびソフトウェアのキーストアの内容を表示します。

cts refresh

すべてまたは特定の Cisco TrustSec ピアの TrustSec ピア認証ポリシーをリフレッシュするか、認証サーバによりデバイスにダウンロードされた SGACL ポリシーをリフレッシュするには、特権 EXEC モードで **cts refresh** コマンドを使用します。

cts refresh {**peer** [*peer_id*] | **sgt** [{*sgt_number* | **default** | **unknown**}]}

構文の説明

environment-data	環境データをリフレッシュします。
peer *Peer-ID*	（任意）peer-idが指定される場合、指定されたピア接続に関連するポリシーだけがリフレッシュされます。
sgt *sgt_number*	（任意）認証サーバからのSGACLポリシーの即時リフレッシュを実行します。 SGT 番号が指定されている場合、その SGT に関連するポリシーだけがリフレッシュされます。
default	（任意）デフォルトの SGACL ポリシーをリフレッシュします。
unknown	（任意）未知の SGACL ポリシーをリフレッシュします。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザロール

管理者（Administrator）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

すべての TrustSec ピアのピア認証ポリシーをリフレッシュするには、ピア ID を指定しないで **cts policy refresh** を入力します。

ピア認可ポリシーはEAP-FAST NDAC認証の成功の最後にCisco ACSから最初にダウンロードされます。Cisco ACS はピア認証ポリシーを更新するように設定されていますが、**cts policy refresh** コマンドにより、Cisco ACS タイマーが期限切れになる前にポリシーの即時更新を強制できます。このコマンドは、セキュリティ グループ タグ（SGT）を適用でき、セキュリティ グループ アクセス コントロール リスト（SGACL）を強制できる TrustSec デバイスだけに関連します。

次に、すべてのピアの TrustSec ピア認証ポリシーをリフレッシュする例を示します。

```
Device# cts policy refresh
Policy refresh in progress
```

次に、すべてのピアの TrustSec ピア認証ポリシーを表示する出力例を示します。

```
VSS-1# show cts policy peer

CTS Peer Policy
===============
device-id of the peer that this local device is connected to
Peer name: VSS-2T-1
Peer SGT: 1-02
```

```
Trusted Peer: TRUE
Peer Policy Lifetime = 120 secs
Peer Last update time = 12:19:09 UTC Wed Nov 18 2009
Policy expires in 0:00:01:51 (dd:hr:mm:sec)
Policy refreshes in 0:00:01:51 (dd:hr:mm:sec)
Cache data applied = NONE
```

関連コマンド

コマンド	説明
clear cts policy	Cisco TrustSec ポリシーをすべてクリアするか、ピア ID または SGT によりクリアします。
show cts policy peer	すべてまたは特定の TrustSec ピアのピア認可ポリシーが表示されます。

cts rekey

セキュリティ アソシエーション プロトコル（SAP）で使用するペアワイズマスターキーを再生成するには、**cts rekey** 特権 EXEC コマンドを使用します。

cts rekey interface type *slot/port*

構文の説明

interface type *slot/port*	SAP キーを再生成する Cisco TrustSec インターフェイスを指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザロール

管理者（Administrator）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

SAP のペアワイズマスターキー（PMK）のリフレッシュは通常、ネットワークイベントおよび dot1X 認証に関連する設定不可能な内部タイマーの組み合わせによりトリガーされ、自動的に行われます。暗号キーを手動で更新する機能は、多くの場合、ネットワークアドミニストレーションのセキュリティ要件の一部です。手動で PMK のリフレッシュを強制するには、**cts rekey** コマンドを使用します。

TrustSec は、dot1X 認証でスイッチ間のリンク間暗号化を作成する必要のない手動コンフィギュレーション モードをサポートします。この場合、PMK は、**sap pmk** Cisco TrustSec 手動イン

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リンクの両端のデバイスで手動で設定されます。

次に、指定したインターフェイス上で PMK を再生成する例を示します。

```
Device# cts rekey interface gigabitEthernet 2/1
```

関連コマンド

コマンド	説明
sap mode-list (cts manual)	手動モードの Cisco TrustSec SAP を設定します。

cts role-based enforcement

Cisco TrustSec を使用したロールベースのアクセス制御をグローバルおよび特定のレイヤ 3 インターフェイスで有効にするには、グローバル コンフィギュレーション モードおよびインターフェイス コンフィギュレーション モードで **cts role-based enforcement** コマンドをそれぞれ使用します。ロールベースのアクセス制御のインターフェイス レベルでの適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。

cts role-based enforcement
no cts role-based enforcement

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

ロールベースのアクセス制御のインターフェイス レベルでの適用はグローバルに無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

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 Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードで **cts role-based enforcement** コマンドを使用すると、ロールベースのアクセス制御がグローバルに有効になります。ロールベースのアクセス制御がグローバルに有効になると、デバイスのすべてのレイヤ3インターフェイスで自動的に有効になります。特定のレイヤ3インターフェイスでロールベースのアクセス制御を無効にするには、インターフェイス コンフィギュレーション モードでこのコマンドの **no** 形式を使用します。インターフェイス コンフィギュレーション モードで **cts role-based enforcement** コマンドを使用すると、特定のレイヤ3インターフェイスでロールベースのアクセス制御の適用が可能になります。

属性ベースのアクセス制御リストでは、ネットワークデバイスの Cisco TrustSec アクセス制御を整理して管理します。セキュリティグループアクセスコントロールリスト（SGACL）は、セキュリティグループタグ（SGT）の値に基づいてアクセスをフィルタ処理するためのレイヤ 3/4 アクセス制御リストです。通常、フィルタ処理は Cisco TrustSec ドメインの出力ポートで実行されます。ロールベースのアクセス制御リスト（RBACL）と SGACL という用語は同じ意味で使用され、どちらも属性ベースのアクセス制御（ABAC）ポリシーモデルで使用されるトポロジに依存しない ACL を示します。

次に、ギガビットイーサネットインターフェイスでロールベースのアクセス制御を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/3
Device(config-if)# cts role-based enforcement
Device(config-if)# end
```

cts role-based l2-vrf

レイヤ 2 VLAN の Virtual Routing and Forwarding（VRF）インスタンスを選択するには、グローバル コンフィギュレーション モードで **cts role-based l2-vrf** 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。

cts role-based l2-vrf *vrf-name* **vlan-list** {**all** *vlan-ID*} [{**,**}] [{**-**}]
no cts role-based l2-vrf *vrf-name* **vlan-list** {**all** *vlan-ID*} [{**,**}] [{**-**}]

構文の説明

vrf-name	VRF インスタンスの名前。
vlan-list	VRF インスタンスに割り当てられる VLAN のリストを指定します。
all	すべての VLAN を指定します。
vlan-ID	VLAN ID。有効な値は 1 ～ 4094 です。
,	（任意）別の VLAN をカンマで区切って指定します。
-	（任意）VLAN の範囲をハイフンで区切って指定します。

コマンド デフォルト

VRF インスタンスは選択されていません。

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 Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

vlan-list 引数には単一の VLAN ID、カンマで区切られた VLAN ID のリスト、またはハイフンで区切られた VLAN ID の範囲を指定できます。

all キーワードは、ネットワークデバイスによってサポートされている VLAN の全範囲と同等です。**all** キーワードは、不揮発性生成（NVGEN）プロセスで保持されません。

cts role-based l2-vrf コマンドが同じ VRF に複数回実行される場合、入力される連続した各コマンドは、指定された VRF に VLAN ID を追加します。

cts role-based l2-vrf コマンドで設定された VRF 割り当ては、VLAN がレイヤ 2 VLAN として維持されている間はアクティブです。VRF の割り当てがアクティブな間に、学習した IP-SGT バインディングも VRF と IP プロトコルバージョンに関連付けられた転送情報ベース（FIB）テーブルに追加されます。VLANのスイッチ仮想インターフェイス（SVI）がアクティブになると、VRFからVLANへの割り当てが非アクティブになり、VLANで学習されたすべてのバインディングが SVI の VRF に関連付けられた FIB テーブルに移動されます。

SVI インターフェイスを設定するには **interface vlan** コマンドを使用し、VRF インスタンスをインターフェイスに関連付けるには **vrf forwarding** コマンドを使用します。

VRF から VLAN への割り当ては、割り当てが非アクティブになっても保持されます。SVI が削除された、または SVI の IP アドレスの変更された場合に再アクティブ化されます。再アクティブ化された場合、IP-SGT バインディングは、SVI の FIB に関連付けられた FIB テーブルから、**cts role-based l2-vrf** コマンドによって割り当てられた VRF に関連付けられた FIB テーブルに戻されます。

次に、VRFインスタンスに割り当てられるVLANのリストを選択する例を示します。

```
Device(config)# cts role-based l2-vrf vrf1 vlan-list 20
```

次に、SVIインターフェイスを設定し、VRFインスタンスを関連付ける例を示します。

```
Device(config)# interface vlan 101
Device(config-if)# vrf forwarding vrf1
```

関連コマンド

コマンド	説明
interface vlan	VLAN インターフェイスを設定します。
vrf forwarding	VRF インスタンスまたは仮想ネットワークをインターフェイスまたはサブインターフェイスに関連付けます。
show cts role-based permissions	SGACL の権限リストを表示します。

cts role-based monitor

ロールベース（セキュリティグループ）アクセスリストモニタリングを有効にするには、グローバル コンフィギュレーション モードで **cts role-based monitor** コマンドを使用します。ロールベース アクセス リスト モニタリングを削除するには、このコマンドの **no** 形式を使用します。

cts role-based monitor {**all** | **permissions** {**default** [{**ipv4** | **ipv6**}] | **from** {*sgt* | **unknown**} **to** {*sgt* | **unknown**} [{**ipv4** | **ipv6**}]}}
no cts role-based monitor {**all** | **permissions** {**default** [{**ipv4** | **ipv6**}] | **from** {*sgt* | **unknown**} **to** {*sgt* | **unknown**} [{**ipv4** | **ipv6**}]}}

構文の説明

all	すべての宛先タグへのすべての送信元タグの権限をモニタします。
permissions	1 つの送信元タグから 1 つの宛先タグへの権限をモニタします。
default	デフォルトの権限リストをモニタします。
ipv4	（任意）IPv4 プロトコルを指定します。
ipv6	（任意）IPv6 プロトコルを指定します。
from	フィルタリングされるトラフィックの送信元グループ タグを指定します。
sgt	セキュリティグループタグ（SGT）有効値は 2 ～ 65519 です。
unknown	未知の送信元または宛先グループタグ（DST）を指定します。

コマンド デフォルト

ロールベース アクセス コントロール モニタリング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 Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

グローバルモニタモードを有効にするには、**cts role-based monitor all** コマンドを使用します。**cts role-based monitor all** コマンドが設定されている場合、**show cts role-based permissions** コマンドの出力には、設定されているすべてのポリシーのモニタモードが true と表示されます。

次に、送信元タグから宛先タグへの SGACL モニタを設定する例を示します。

```
Device(config)# cts role-based monitor permissions from 10 to 11
```

関連コマンド

コマンド	説明
show cts role-based permissions	SGACLの権限リストを表示します。

cts role-based permissions

1 つの送信元グループから 1 つの宛先グループへの権限を有効にするには、グローバル コンフィギュレーション モードで **cts role-based permissions** コマンドを使用します。権限を削除するには、このコマンドの **no** 形式を使用します。

cts role-based permissions {**default** | **from** {*sgt* | **unknown**}**to** {*sgt* | **unknown**}}{*rbacl-name* | **ipv4** | **ipv6**}
no cts role-based permissions {**default** | **from** {*sgt* | **unknown**}**to** {*sgt* | **unknown**}}{*rbacl-name* | **ipv4** | **ipv6**}

構文の説明

default	デフォルトの権限リストを指定します。セキュリティ グループ アクセス コントロール リスト（SGACL）権限が静的または動的に設定されていないすべてのセル（SGT ペア）は、デフォルトのカテゴリに属します。
from	フィルタリングされるトラフィックの送信元グループ タグを指定します。
sgt	セキュリティグループタグ（SGT）有効値は 2 ～ 65519 です。
unknown	未知の送信元または宛先グループタグを指定します。
rbacl-name	ロールベース アクセス コントロール リスト(RBACL)または SGACL の名前。この設定では最大 16 の SGACL を指定できます。
ipv4	IPv4 プロトコルを指定します。
ipv6	IPv6 プロトコルを指定します。

コマンド デフォルト

1 つの送信元グループから 1 つの宛先グループへの権限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 Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

特定の送信元グループタグ（SGT）、宛先グループタグ（DGT）ペアの SGACL のリストを定義したり、置き換えたり、削除したりするには、**cts role-based permissions** コマンドを使用します。このポリシーは、同じ DGT または SGT に対するダイナミックなポリシーがないかぎり有効です。

cts role-based permissions default コマンドでは、同じ DGT に対するダイナミックなポリシーがないかぎり、デフォルトポリシーの SGACL のリストを定義したり、置き換えたり、削除したりすることができます。

次に、宛先グループの権限を有効にする例を示します。

```
Device(config)# cts role-based permissions from 6 to 6 mon_2
```

関連コマンド

コマンド	説明
show cts role-based permissions	SGACL の権限リストを表示します。

cts role-based sgt-map

ホストまたは VRF のいずれかで送信元 IP アドレスをセキュリティグループタグ（SGT）に手動でマッピングするには、グローバル コンフィギュレーション モードで **cts role-based sgt-map** コマンドを使用します。マッピングを削除するには、このコマンドの **no** 形式を使用します。

cts role-based sgt-map
{*ipv4_netaddress* | *ipv6_netaddress* | *ipv4_netaddress/prefix* | *ipv6_netaddress/prefix*} **sgt** *sgt-number*
cts role-based sgt-map host {*ipv4_hostaddress* | *ipv6_hostaddress*} **sgt** *sgt-number*
cts role-based sgt-map vlan-list [{*vlan_ids* | **all**}] **sgt** *sgt-number*
cts role-based sgt-map vrf *instance_name*
{*ipv4_netaddress* | *ipv6_netaddress* | *ipv4_netaddress/prefix* | *ipv6_netaddress/prefix* | **host** {*ipv4_hostaddress* | *ipv6_hostaddress*}} **sgt** *sgt-number*
no cts role-based sgt-map

構文の説明

ipv4_netaddress | **ipv6_netaddress**	SGT に関連付けるネットワークを指定します。IPv4 アドレスをドット付き 10 進数表記で、IPv6 をコロン 16 進数表記で入力します。
ipv4_netaddress/prefix | **ipv6_netaddress/prefix**	指定したサブネットアドレス（IPv4 または IPv6）のすべてのホストに SGT をマッピングします。IPv4 はドット付き 10 進数 CIDR 表記で、IPv6 はコロン 16 進数表記で指定されます。
host {*ipv4_hostaddress* | *ipv6_hostaddress*}	指定したホスト IP アドレスを SGT とバインドします。IPv4 アドレスをドット付き 10 進数表記で、IPv6 をコロン 16 進数表記で入力します。
vlan-list {*vlan_ids* | **all**}	VLAN ID を指定します。 • （任意）*vlan_ids*：各 VLAN ID はカンマで区切られ、ID の範囲はハイフンで指定されます。 • （任意）**all**：すべての VLAN ID を指定します。

vrf *instance_name*	以前デバイスで作成した VRF インスタンスを指定します。
sgt *sgt-number*	SGT 番号（0 ～ 65,535）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 Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

自動的に SGT を送信元 IP アドレスにマッピングするための、Cisco Identity Services Engine、Cisco Secure ACS、ダイナミックアドレス解決プロトコル（ARP）インスペクション、動的ホスト制御プロトコル（DHCP）スヌーピング、ホストトラッキングがで使用できない場合、**cts role-based sgt-map** コマンドを使用して SGT を次の内容にマッピングできます。

- 単一ホストの IPv4 または IPv6 アドレス
- IPv4 または IPv6 ネットワークまたはサブネットワーク上のすべてのホスト
- VRF
- 単一または複数の VLAN

cts role-based sgt-map コマンドは、指定されたネットワークアドレス範囲内のパケットに、指定された SGT をバインドします。

SXP は指定されたネットワークまたはサブネットワーク内のすべての可能な個別 IP-SGT バインディングの包括的な拡張をエクスポートします。IPv6 バインディングとサブネット バインディングは SXP バージョン 2 以降の SXP リスナー ピアだけにエクスポートされます。拡張には、個別に認識されたホストバインディングや、ネストされたサブネットバインディングに対して SXP から設定または学習されたホストバインディングは含まれません。

cts role-based sgt-map host コマンドは、IP 送信元アドレスが指定ホストアドレスで一致した場合に、この着信パケットに指定 SGT をバインドします。この IP-SGT バインディングは優先順位が最も低く、他の送信元から動的に検出されたその他のバインディング（SXP またはローカルで認証済みホストなど）が存在する場合は無視されます。バインディングは、SGT インポジションおよび SGACL 強制用にデバイス上でローカルに使用されます。このバインディングが指定したホスト IP アドレスに認識される唯一のバインディングである場合、これが SXP ピアにエクスポートされます。

vrf キーワードは、以前に vrf definition グローバル コンフィギュレーション コマンドで定義された仮想ルーティングおよびフォワーディングテーブルを指定します。**cts role-based sgt-map vrf** グローバル コンフィギュレーション コマンドで指定された IP-SGT バインディングは、指定された VRF と、入力された IP アドレスのタイプによって示される IP プロトコルのバージョンに関連付けられた IP-SGT のテーブルに入力されます。

cts role-based sgt-map vlan-list コマンドは、SGT を指定された VLAN または VLAN のセットにバインドします。キーワード **all** は、デバイスでサポートされている VLAN の全範囲と同じで、不揮発性生成（NVGEN）プロセスで保持されません。指定 SGT は指定した VLAN のいずれかで受信した着信パケットにバインドされます。システムでは、DHCP/ARP スヌーピング（別名 IP デバイストラッキング）などの検出方式を使用して、このコマンドによってマッピングされた VLAN のいずれかでアクティブなホストを検出します。また、各 VLAN の SVI に関連付けられたサブネットを指定された SGT にマッピングすることもできます。SXP は、バインディングのタイプに応じて、結果のバインディングをエクスポートします。

例

次に、送信元 IP アドレスを SGT に手動でマッピングする例を示します。

```
Device(config)# cts role-based sgt-map 10.10.1.1 sgt 77
```

次の例では、デバイスでホスト IP アドレス 10.1.2.1 を SGT 3 にバインドし、10.1.2.2 を SGT 4 にバインドしています。これらのバインディングは、SXP によって SGACL 強制のデバイスに転送されます。

```
Device(config)# cts role-based sgt-map host 10.1.2.1 sgt 3
Device(config)# cts role-based sgt-map host 10.1.2.2 sgt 4
```

関連コマンド

コマンド	説明
show cts role-based sgt-map	ロールベースのアクセス制御の情報を表示します。

cts sxp connection peer

Cisco TrustSec セキュリティグループタグ交換プロトコルのピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定し、リスナーまたはスピーカーデバイスのグローバルなホールド時間を指定し、接続が双方向であるかどうかを指定するには、グローバル コンフィギュレーション モードで **cts sxp connection peer** コマンドを使用します。これらのピア接続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。

cts sxp connection peer *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [{[[{**listener** | **speaker**}] [{**hold-time** *minimum-time maximum-time* | **vrf** *vrf-name* }]] | **both** [**vrf** *vrf-name*]}]
cts sxp connection peer *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [{[[{**listener** | **speaker**}] [{**hold-time** *minimum-time maximum-time* | **vrf** *vrf-name* }]] | **both** [**vrf** *vrf-name*]}]

構文の説明

ipv4-address	SXP ピアの IPv4 アドレス。
source	送信元の IPv4 アドレスを指定します。
password	ピア接続に SXP パスワードを使用するように指定します。

default	デフォルトの SXP パスワードを使用するように指定します。
none	パスワードを使用しないように指定します。
mode	ローカルまたはピアのいずれかの SXP 接続モードを指定します。
local	SXP 接続モードでローカルデバイスを参照するように指定します。
peer	SXP 接続モードでピアデバイスを参照するように指定します。
listener	（任意）デバイスを接続のリスナーとして指定します。
speaker	（任意）デバイスを接続のスピーカーとして指定します。
hold-time *minimum-time maximum-time*	（任意）デバイスのホールド時間を秒単位で指定します。最小時間と最大時間の範囲は 0 ～ 65535 です。 *maximum-time* の値は、キーワード **peer speaker** および **local listener** を使用する場合のみ必要です。それ以外の場合は、*minimum-time* の値のみが必要です。 （注） 最小時間と最大時間の両方が必要な場合、*maximum-time* の値を *minimum-time* の値以上にする必要があります。
vrf *vrf-name*	（任意）ピアに対する Virtual Routing and Forwarding（VRF）インスタンス名を指定します。
both	（任意）デバイスを双方向 SXP 接続のスピーカーとリスナーの両方として指定します。

コマンド デフォルト

CTS-SXP ピア IP アドレスは設定されておらず、ピア接続に CTS-SXP ピアパスワードは使用されません。

CTS-SXP 接続パスワードのデフォルトの設定は **none** 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 Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

ピアへの CTS-SXP 接続が **cts sxp connection peer** コマンドを使用して設定された場合、接続モードだけを変更できます。**vrf** キーワードはオプションです。VRF 名が指定されていない、または VRF 名が **default** キーワードで指定されている場合、接続はデフォルトルーティングまたはフォワーディングドメインで設定されます。

hold-time *maximum-period* の値は、キーワード **peer speaker** および **local listener** を使用する場合のみ必要です。それ以外の場合は、**hold-time** *minimum-period* の値のみが必要です。

（注） *maximum-period* 値は、*minimum-period* 値よりも大きいか等しくする必要があります。

双方向 SXP 接続を設定するには、**both** キーワードを使用します。双方向 SXP の設定をサポートすることで、ピアはスピーカーとリスナーのどちらとしても動作し、単一の接続を使用する双方向の SXP バインドを伝播できるようになります。

例

次に、CTS-SXP をイネーブルにし、Device_A（スピーカー）で Device_B（リスナー）への SXP ピア接続を設定する例を示します。

```
Device_A> enable
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

次に、Device_B（リスナー）で Device_A（スピーカー）への CTS-SXP ピア接続を設定する例を示します。

```
Device_B> enable
Device_B# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

SXP 接続のピアと送信元の両方の IP アドレスを設定することもできます。**cts sxp connection** コマンドで送信元 IP アドレスを指定すると、デフォルト値が上書きされます。

```
Device_A(config)# cts sxp connection peer 51.51.51.1 source 51.51.51.2 password none
mode local speaker
```

```
Device_B(config)# cts sxp connection peer 51.51.51.2 source 51.51.51.1 password none
mode local listener
```

次の例は、双方向 CTS-SXP を有効化し、Device_A 上の SXP ピア接続が Device_B に接続するよう設定する方法を示します。

```
Device_A> enable
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local both
```

関連コマンド

コマンド	説明
cts sxp default password	Cisco TrustSec SXP のデフォルトパスワードを設定します。
cts sxp default source-ip	Cisco TrustSec SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで Cisco TrustSec SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングを有効にします。
cts sxp reconciliation	Cisco TrustSec SXP の復帰期間を変更します。
cts sxp retry	Cisco TrustSec SXP の再試行期間タイマーを変更します。
cts sxp speaker hold-time	Cisco TrustSec SGT SXPv4 ネットワークにおけるスピーカーデバイスのグローバルなホールド時間を設定します。
cts sxp listener hold-time	Cisco TrustSec SGT SXPv4 ネットワークにおけるリスナーデバイスのグローバルなホールド時間を設定します。
show cts sxp	Cisco TrustSec SXP のすべての設定のステータスを表示します。

cts sxp default password

Cisco TrustSec セキュリティグループタグ（SGT）交換プロトコル（CTS-SXP）のデフォルトパスワードを指定するには、グローバル コンフィギュレーション モードで **cts sxp default password** コマンドを使用します。CTS-SXP のデフォルトパスワードを削除するには、このコマンドの **no** 形式を使用します。

cts sxp default password {**0** *unencrypted-pwd* | **6** *encrypted-key* | **7** *encrypted-keycleartext-pwd*}
no cts sxp default password {**0** *unencrypted-pwd* | **6** *encrypted-key* | **7** *encrypted-keycleartext-pwd*}

構文の説明

0 *unencrypted-pwd*	暗号化されていない CTS-SXP デフォルトパスワードが続くことを指定します。パスワードの最大長は 32 文字です。
6 *encrypted-key*	タイプ 6 暗号化パスワードを CTS SXP デフォルトパスワードとして使用することを指定します。パスワードの最大長は 32 文字です。
7 *encrypted-key*	タイプ 7 暗号化パスワードを CTS SXP デフォルトパスワードとして使用することを指定します。パスワードの最大長は 32 文字です。
cleartext-pwd	クリアテキストの CTS-SXP デフォルトパスワードを指定します。パスワードの最大長は 32 文字です。

コマンド デフォルト

タイプ **0**（クリアテキスト）

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

cts sxp default password コマンドは、デバイスに設定されているすべての SXP 接続に任意で使用する CTS-SXP デフォルトパスワードを設定します。CTS-SXP パスワードは、クリアテキストまたは**0**、**7**、**6**暗号化タイプキーワードを使用して暗号化したものを使用します。暗号化タイプが 0 の場合は、暗号化されていないクリアテキストパスワードが続きます。

例

次に、CTS-SXP をイネーブルにし、Device_A（スピーカー）で Device_B（リスナー）への SXP ピア接続を設定する例を示します。

```
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

次に、Device_B（リスナー）で Device_A（スピーカー）への CTS-SXP ピア接続を設定する例を示します。

```
Device_B# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

関連コマンド

コマンド	説明
cts sxp connection peer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default source-ip	CTS-SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで CTS-SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングを有効にします。
cts sxp reconciliation	CTS-SXP の復帰期間を変更します。
cts sxp retry	CTS-SXP の再試行期間タイマーを変更します。
show cts sxp	SXP のすべての設定のステータスを表示します。

cts sxp default source-ip

Cisco TrustSec セキュリティグループタグ（SGT）交換プロトコル（CTS-SXP）の送信元 IPv4 アドレスを設定するには、グローバル コンフィギュレーション モードで **cts sxp default source-ip** コマンドを使用します。CTS-SXP のデフォルトの送信元 IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

cts sxp default source-ip *ipv4-address*
no cts sxp default source-ip *ipv4-address*

構文の説明

ip-address	CTS-SXP のデフォルトの送信元 IPv4 アドレス。

コマンド デフォルト

CTS-SXP の送信元 IP アドレ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 Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

cts sxp default source-ip コマンドは、送信元 IP アドレスが指定されていない場合に、CTS-SXP が新規の TCP 接続すべてに使用するデフォルトの送信元 IP アドレスを設定します。既存の TCP 接続は、このコマンドが入力されても影響を受けません。CTS-SXP 接続は 3 つのタイマーによって制御されます。

- 再試行タイマー
- 削除のホールドダウン タイマー
- 復帰タイマー

例

次に、CTS-SXP をイネーブルにし、Device_A（スピーカー）で Device_B（リスナー）への SXP ピア接続を設定する例を示します。

```
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

次に、Device_B（リスナー）で Device_A（スピーカー）への CTS-SXP ピア接続を設定する例を示します。

```
Device_B# configure terminal
Device_B(config)# cts sxp enable
```

```
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

関連コマンド

コマンド	説明
cts sxp connectionpeer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default password	CTS-SXP のデフォルト パスワードを設定します。
cts sxp enable	デバイスで CTS-SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングを有効にします。
cts sxp reconciliation	CTS-SXP の復帰期間を変更します。
cts sxp retry	CTS-SXP の再試行期間タイマーを変更します。
show cts sxp	SXP のすべての設定のステータスを表示します。

cts sxp filter-enable

フィルタリストおよびフィルタグループの作成後にフィルタリングを有効にするには、グローバル コンフィギュレーション モードで **cts sxp filter-enable** コマンドを使用します。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。

cts sxp filter-enable
no cts sxp filter-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 モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、フィルタリングを有効または無効にするためにいつでも使用できます。設定したフィルタリストとフィルタグループは、フィルタリングを有効にした後にのみフィルタリングの実装に使用できます。フィルタアクションでは、フィルタリングを有効にした後に交換されたバインディングのみがフィルタリングされます。フィルタリングを有効にする前に交換されたバインディングに対しては効果はありません。

例

```
Device(config)# cts sxp filter-enable
```

関連コマンド

コマンド	説明
cts sxp filter-list	IP プレフィックス、SGT、またはその両方の組み合わせに基づいて IP-SGT バインディングをフィルタリングするための SXP フィルタリストを作成します。
cts sxp filter-group	一連のピアをグループ化してフィルタリストを適用するためのフィルタグループを作成します。
show cts sxp filter-group	設定されているフィルタグループに関する情報を表示します。
show cts sxp filter-list	設定されているフィルタリストに関する情報を表示します。
debug cts sxp filter events	フィルタリストおよびフィルタグループの作成、削除、更新に関連するイベントをログに記録します。

cts sxp filter-group

一連のピアをグループ化してフィルタリストを適用するためのフィルタグループを作成するには、グローバル コンフィギュレーション モードで **cts sxp filter-group** コマンドを使用します。フィルタ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。

cts sxp filter-group {**listener** | **speaker**} {*filter-group-name* | **global** *filter-list-name*}
no cts sxp filter-group {**listener** | **speaker**} {*filter-group-name* | **global** *filter-list-name*}

構文の説明

listener	一連のリスナーのフィルタグループを作成します。
speaker	一連のスピーカーのフィルタグループを作成します。
global	デバイスのすべてのスピーカーまたはリスナーをグループ化します。
filter-group-name	フィルタグループの名前。
filter-list-name	フィルタ リストの名前。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを発行すると、デバイスがフィルタ グループ コンフィギュレーション モードになります。このモードで、グループ化するデバイスを指定し、フィルタグループにフィルタリストを適用できます。

デバイスまたはピアをグループに追加するためのコマンドの形式は次のとおりです。

peer ipv4 *peer-IP*

1 つのコマンドで 1 つのピアを追加できます。ピアをさらに追加するには、必要な回数だけコマンドを繰り返します。

フィルタリストをグループに適用するためのコマンドの形式は次のとおりです。

filter *filter-list-name*

グローバルリスナーおよびグローバルスピーカーのフィルタグループオプションではピアリストは指定できません。この場合、フィルタはすべての SXP 接続に適用されます。

グローバルなフィルタグループとピアベースのフィルタグループの両方が適用されている場合、グローバルフィルタが優先されます。グローバルリスナーまたはグローバルスピーカーのいずれかのフィルタグループのみが設定されている場合、その方向でのみグローバルフィルタリングが優先されます。もう一方の方向については、ピアベースのフィルタグループが実装されます。

例

次に、**group_1** というリスナーグループを作成し、そのグループにピアとフィルタリストを割り当てる例を示します。

```
Device# configure terminal
Device(config)# cts sxp filter-group listener group_1
Device(config-filter-group)# filter filter_1
Device(config-filter-group)# peer ipv4 10.0.0.1
Device(config-filter-group)# peer ipv4 10.10.10.1
```

次に、**group_2** というグローバルリスナーグループを作成する例を示します。

```
Device# configure terminal
Device(config)# cts sxp filter-group listener global group_2
```

関連コマンド

コマンド	説明
cts sxp filter-list	IP プレフィックス、SGT、またはその両方の組み合わせに基づいて IP-SGT バインディングをフィルタリングするための SXP フィルタリストを作成します。
cts sxp filter-enable	フィルタリングを有効にします。
show cts sxp filter-group	設定されているフィルタグループに関する情報を表示します。
show cts sxp filter-list	設定されているフィルタリストに関する情報を表示します。
debug cts sxp filter events	フィルタリストおよびフィルタグループの作成、削除、更新に関連するイベントをログに記録します。

cts sxp filter-list

IP-SGTバインディングをフィルタリングするための一連のフィルタルールを保持するSXPフィルタ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 **cts sxp filter-list** コマンドを使用します。フィルタ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。

cts sxp filter-list *filter-list-name*
no cts sxp filter-list *filter-list-name*

構文の説明

filter-list-name	フィルタリストの名前。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを発行すると、デバイスがフィルタ リスト コンフィギュレーション モードになります。このモードで、フィルタリストのルールを指定できます。

フィルタルールは、SGT、IP プレフィックス、または SGT と IP プレフィックスの両方の組み合わせに基づいて設定できます。

グループにルールを追加するためのコマンドの形式は次のとおりです。

sequence-number **action(permit/deny) filter-type(ipv4/ipv6/sgt)** *value/values*

たとえば、SGT 値が 20 である SGT-IP バインディングを許可するルールは次のようになります。

```
30 permit sgt 20
```

シーケンス番号はオプションです。シーケンス番号を指定しない場合は、システムによって生成されます。シーケンス番号は、最後に使用/設定されたシーケンス番号から自動的に 10 ずつ増分されます。2 つの既存のルールの間のシーケンス番号を指定することによって新しいルールを挿入できます。

有効なSGT値の範囲は2～65519です。1つのルールに複数のSGT値を指定するには、スペースを使用して値を区切ります。1 つのルールに最大 8 つの SGT 値を指定できます。

SGT と IP プレフィックスを組み合わせたルールでは、ルールの両方の部分にバインディングの一致がある場合、ルールの 2 つ目の部分で指定されたアクションが優先されます。たとえば、次のルールでは、IP プレフィックス 10.0.0.1 の SGT 値が 20 の場合、ルールの最初の部分でバインディングが許可されても、対応するバインディングが拒否されます。

```
Device(config-filter-list)# 10 permit sgt 30 20 deny 10.0.0.1/24
```

同様に、次のルールでは、IP プレフィックス 10.0.0.1 の SGT が 20 で最初のアクションではバインディングが許可されなくても、SGT 値 20 のバインディングが許可されます。

```
Device(config-filter-list)# 10 deny 10.0.0.1/24 permit sgt 30 20
```

例

次に、フィルタリストを作成していくつかのルールを追加する例を示します。

```
Device# configure terminal
Device(config)# cts sxp filter-list filter_1
Device (config-filter-list)# 10 deny ipv4 10.0.0.1/24 permit sgt 100
Device(config-filter-list)# 20 permit sgt 60 61 62 63
```

関連コマンド

コマンド	説明
cts sxp filter-enable	SXP の IP プレフィックスおよび SGT ベースのフィルタリングを有効にします。
cts sxp filter-group	一連のピアをグループ化してフィルタリストを適用するためのフィルタグループを作成します。
show cts sxp filter-group	設定されているフィルタグループに関する情報を表示します。
show cts sxp filter-list	設定されているフィルタリストに関する情報を表示します。
debug cts sxp filter events	フィルタリストおよびフィルタグループの作成、削除、更新に関連するイベントをログに記録します。

cts sxp log binding-changes

IP と Cisco TrustSec セキュリティグループタグ（SGT）交換プロトコル（CTS-SXP）のバインディングの変更のロギングを有効にするには、グローバル コンフィギュレーション モードで **cts sxp log binding-changes** コマンドを使用します。ロギングを無効にするには、このコマンドの **no** 形式を使用します。

cts sxp log binding-changes
no cts sxp log binding-changes

コマンド デフォルト

ロギングは無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

cts sxp log binding-changes コマンドを使用すると、IP と SGT のバインディングの変更のロギングが有効になります。IP アドレスと SGT のバインディングに追加、削除、変更が発生するたびに SXP の syslog（sev 5 syslog）が生成されます。これらの変更は SXP 接続で学習されて伝播されます。

関連コマンド

コマンド	説明
cts sxp connectionpeer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default password	CTS-SXP のデフォルト パスワードを設定します。
cts sxp default source-ip	CTS-SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで CTS-SXP を有効にします。
cts sxp reconciliation	CTS-SXP の復帰期間を変更します。
cts sxp retry	CTS-SXP の再試行期間タイマーを変更します。
show cts sxp	すべての SXP 設定のステータスを表示します。

cts sxp reconciliation period

Cisco TrustSec セキュリティグループタグ（SGT）交換プロトコル（CTS-SXP）の復帰期間を変更するには、グローバル コンフィギュレーション モードで **cts sxp reconciliation period** コマンドを使用します。CTS-SXP の復帰期間をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

cts sxp reconciliation period *seconds*
no cts sxp reconciliation period *seconds*

構文の説明

seconds	CTS-SXP 復帰タイマー（秒）。範囲は 0 ～ 64000 です。デフォルトは 120 です。

コマンド デフォルト

120 秒（2 分）

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

ピアが CTS-SXP 接続を終了すると、内部の削除ホールドダウンタイマーが開始されます。削除ホールドダウンタイマーが終了する前にピアが再接続すると、CTS-SXP 復帰タイマーが開始されます。CTS-SXP 復帰期間タイマーがアクティブな間、CTS-SXP ソフトウェアは前回の接

続で学習した SGT マッピングエントリを保持し、無効なエントリを削除します。SXP 復帰期間を0秒に設定すると、タイマーがディセーブルになり、前回の接続のすべてのエントリが削除されます。

関連コマンド

コマンド	説明
cts sxp connection peer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default password	CTS-SXP のデフォルト パスワードを設定します。
cts sxp default source-ip	CTS-SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで CTS-SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングをオンにします。
cts sxp retry	CTS-SXP の再試行期間タイマーを変更します。
show cts sxp	CTS-SXP のすべての設定のステータスを表示します。

cts sxp retry period

Cisco TrustSec セキュリティグループタグ（SGT）交換プロトコル（CTS-SXP）の再試行期間タイマーを変更するには、グローバル コンフィギュレーション モードで **cts sxp retry period** コマンドを使用します。CTS-SXP の再試行期間タイマーをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

cts sxpretry period *seconds*
no cts sxpretry period *seconds*

構文の説明

seconds	CTS-SXP 再試行タイマー（秒）。範囲は 0 ～ 64000 です。デフォルトは 120 です。

コマンド デフォルト

120 秒（2 分）

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

再試行タイマーは、少なくとも 1 つの CTS-SXP 接続が稼働していない場合にトリガーされます。このタイマーの期限が切れると新しい CTS-SXP 接続が試行されます。ゼロの値は、再試行が発生しなくなります。

関連コマンド

コマンド	説明
cts sxp connectionpeer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default password	CTS-SXP のデフォルト パスワードを設定します。
cts sxp default source-ip	CTS-SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで CTS-SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングを有効にします。
cts sxp reconciliation	CTS-SXP の復帰期間を変更します。
show cts sxp	CTS-SXP のすべての設定のステータスを表示します。

propagate sgt (cts manual)

Cisco TrustSec Security（CTS）インターフェイスでレイヤ 2 のセキュリティグループタグ（SGT）伝達を有効にするには、インターフェイス コンフィギュレーション モードで **propagate sgt** コマンドを使用します。SGT 伝達を無効にするには、このコマンドの **no** 形式を使用します。

propagate sgt

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

SGT 処理の伝達が有効になっています。

コマンド モード

CTS 手動インターフェイス コンフィギュレーション モード（config-if-cts-manual）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

SGT 処理の伝達によって、CTS 対応のインターフェイスは L2 SGT タグに基づいて CTS メタデータ（CMD）を受信および送信できます。ピアデバイスが SGT を受信できず、その結果、SGT タグを L2 ヘッダーに配置できない状況で、インターフェイスの SGT 伝達を無効にするには **no propagate sgt** コマンドを使用します。

例

次に、手動で設定された TrustSec 対応のインターフェイスで SGT 伝達を無効にする例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet 0
```

```
Device(config-if)# cts manual
Device(config-if-cts-manual)# no propagate sgt
```

次に、ギガビット イーサネット インターフェイス 0 で SGT 伝達が無効になっている例を示します。

```
Device#show cts interface brief
Global Dot1x feature is Disabled
Interface GigabitEthernet0:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    NOT APPLICABLE
    SAP Status:              NOT APPLICABLE
    Propagate SGT:           Disabled
    Cache Info:
        Cache applied to link : NONE
```

関連コマンド

コマンド	説明
cts manual	CTS のインターフェイスを有効にします。
show cts interface	インターフェイスごとの Cisco TrustSec ステートおよび統計情報を表示します。

show cts credentials

Cisco TrustSec（CTS）デバイス ID を表示するには、EXEC モードまたは特権 EXEC モードで **show cts credentials** コマンドを使用します。

show cts credentials

構文の説明

このコマンドには、コマンドまたはキーワードはありません。

コマンド モード

特権 EXEC（#）ユーザ EXEC（>）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

例

次に、出力例を示します。

```
Device# show cts credentials

CTS password is defined in keystore, device-id = r4
```

関連コマンド

コマンド	説明
cts credentials	TrustSec ID およびパスワードを指定します。

show cts interface

インターフェイスの Cisco TrustSec（CTS）設定の統計を表示するには、EXEC モードまたは特権 EXEC モードで **show cts interface** コマンドを使用します。

show cts interface [{**GigabitEthernet** *port* | **Vlan** *number* | **brief** | **summary**}]

構文の説明

port	（任意）ギガビットイーサネットインターフェイス番号。このインターフェイスの冗長ステータス出力が返されます。
number	（任意）VLAN インターフェイス番号（1 ～ 4095）。
brief	（任意）すべての CTS インターフェイスの短縮ステータスを表示します。
summary	（任意）インターフェイスごとに、すべての CTS インターフェイスのサマリーを、4 個または 5 個のキー ステータス フィールドを持つ表形式で表示します。

コマンド デフォルト

なし

コマンド モード

EXEC（>） 特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

すべての CTS インターフェイスの冗長ステータスを表示するには、キーワードを使用せずに **show cts interface** コマンドを使用します。

例

次に、キーワードを使用せずに出力を表示する例を示します（すべての CTS インターフェイスの冗長ステータス）。

```
Device# show cts interface

Global Dot1x feature is Disabled
 Interface GigabitEthernet0/1/0:
     CTS is enabled, mode:    MANUAL
     IFC state:               OPEN
     Interface Active for 00:00:18.232
     Authentication Status:   NOT APPLICABLE
         Peer identity:       "unknown"
         Peer's advertised capabilities: ""
     Authorization Status:    NOT APPLICABLE
     SAP Status:              NOT APPLICABLE
```

```
        Configured pairwise ciphers:
            gcm-encrypt
            null

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:

    Propagate SGT:           Enabled
    Cache Info:
        Cache applied to link : NONE

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                0
        sap fail:                   0
        authz success:              0
        authz fail:                 0
        port auth fail:             0
        Ingress:
            control frame bypassed: 0
            sap frame bypassed:     0
            esp packets:            0
            unknown sa:             0
            invalid sa:             0
            inverse binding failed: 0
            auth failed:            0
            replay error:           0
        Egress:
            control frame bypassed: 0
            esp packets:            0
            sgt filtered:           0
            sap frame bypassed:     0
            unknown sa dropped:     0
            unknown sa bypassed:    0
```

次に、**brief** キーワードを使用した出力例を示します。

```
Device# show cts interface brief

Global Dot1x feature is Disabled
 Interface GigabitEthernet0/1/0:
     CTS is enabled, mode:    MANUAL
     IFC state:               OPEN
     Interface Active for 00:00:40.386
     Authentication Status:   NOT APPLICABLE
         Peer identity:       "unknown"
         Peer's advertised capabilities: ""
     Authorization Status:    NOT APPLICABLE
     SAP Status:              NOT APPLICABLE
     Propagate SGT:           Enabled
     Cache Info:
         Cache applied to link : NONE
```

関連コマンド

コマンド	説明
cts manual	CTS のインターフェイスを有効にします。
cts sxp enable	ネットワーク デバイスに SXP を設定します。
propagate sgt	Cisco TrustSec Security（CTS）インターフェイスのレイヤ 2 でのセキュリティ グループ タグ（SGT）の伝達を有効にします。

show cts role-based permissions

ロールベース（セキュリティグループ）アクセスコントロール権限リストを表示するには、特権 EXEC モードで **show cts role-based permissions** コマンドを使用します。

show cts role-based permissions [{**default** [{**details** | **ipv4 [details]** | **ipv6 [details]**}] | **from** {{*sgt* | **unknown** }[{**ipv4** | **ipv6** | **to** {{*sgt* | **unknown**}[{**details** | **ipv4 [details]** | **ipv6 [details]**}]}}}] | **ipv4** | **ipv6** | **platform** | **to** {*sgt* | **unknown**}[{**ipv4** | **ipv6**}]}]

構文の説明

default	（任意）デフォルトの権限リストに関する情報を表示します。
details	（任意）アタッチされたアクセス コントロール リスト（ACL）の詳細を表示します。
ipv4	（任意）IPv4 プロトコルに関する情報を表示します。
ipv6	（任意）IPv6 プロトコルに関する情報を表示します。
from	（任意）送信元グループに関する情報を表示します。
sgt	（任意）セキュリティ グループ タグ。有効値は 2 ～ 65519 です。
to	（任意）宛先グループに関する情報を表示します。
unknown	（任意）不明な送信元グループと宛先グループに関する情報を表示します。
platform	（任意）プラットフォームに関する情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SGACL 権限マトリックスのコンテンツを表示します。送信元セキュリティグループタグ（SGT）は **from** キーワードを使用して、宛先 SGT は **to** キーワードを使用して指定できます。両方のキーワードを指定すると、単一セルの RBACL が表示されます。列全体

は、**to** キーワードを使用した場合にのみ表示されます。行全体は、**from** キーワードを使用した場合に表示されます。権限マトリックス全体は、**from** キーワードと **to** キーワードの両方を省略した場合に表示されます。

コマンド出力は、プライマリ キーの宛先 SGT およびセカンダリ キーの送信元 SGT でソートされます。各セルの SGACL は、設定で定義されているのと同じ順序で、または Cisco Identity Services Engine（ISE）から取得した順序で表示されます。

details キーワードは、 **from** キーワードと **to** キーワードの両方を指定することで、単一のセルが選択された場合に表示されます。**details** キーワードが指定されている場合、単一セルの SGACL のアクセス制御エントリが表示されます。

次に、**show role-based permissions** コマンドの出力例を示します。

```
Device# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
default_sgacl-02
Permit IP-00
IPv4 Role-based permissions from group 305:sgt to group 306:dgt (monitored):
test_reg_tcp_permit-02
RBACL Monitor All for Dynamic Policies : TRUE
RBACL Monitor All for Configured Policies : FALSE
IPv4 Role-based permissions from group 6:SGT_6 to group 6:SGT_6 (configured):
  mon_1
IPv4 Role-based permissions from group 10 to group 11 (configured):
  mon_2
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

関連コマンド

コマンド	説明
cts role-based permissions	送信元グループから宛先グループに対する権限を有効にします。
cts role-based monitor	ロールベースのアクセス リストのモニタリングを有効にします。

show cts server-list

Cisco TrustSec（CTS）シードおよび非シードデバイスで使用可能な RADIUS サーバのリストを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show cts server-list** コマンドを使用します。

show cts server-list

構文の説明

このコマンドには、コマンドまたはキーワードはありません。

コマンド モード

特権 EXEC（#）ユーザ EXEC（>）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Cisco TrustSec RADIUS サーバのアドレスとステータス情報を収集するのに使用できます。

例

次の例は、CTS RADIUS サーバのリストを表示します。

```
Device> show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)
Preferred list, 1 server(s):
 *Server: 10.0.1.6, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Installed list: ACSServerList1-0001, 1 server(s):
 *Server: 101.0.2.61, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

関連コマンド

コマンド	説明
address ipv4 (config-radius-server)	PAC プロビジョニングに使用する RADIUS サーバのアカウンティングおよび認証パラメータを設定します。
pac key	PAC 暗号キーを指定します。

show cts sxp

Cisco TrustSec セキュリティグループタグ（SGT）交換プロトコル（CTS-SXP）接続または送信元 IP と SGT のマッピング情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show cts sxp** コマンドを使用します。

show cts sxp {**connections** [{**brief** | **vrf** *instance-name*}] | **filter-group** [{**detailed** | **global** | **listener** | **speaker** }] | **filter-list** *filter-list-name* | **sgt-map** [{**brief** | **vrf** *instance-name*}]} [{**brief** | **vrf** *instance-name*}]

構文の説明

connections	Cisco TrustSec SXP 接続の情報を表示します。
brief	（任意）SXP 情報の省略形を表示します。
vrf *instance-name*	（任意）指定した Virtual Routing and Forwarding（VRF）インスタンスの SXP 情報を表示します。

filter-group {**detailed** | **global** | **listener** | **speaker** }	（任意）フィルタグループ情報を表示します。
filter-list *filter-list-name*	（任意）フィルタリスト情報を表示します。
sgt-map	（任意）SXP 経由で受信した IP と SGT のマッピングを表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

例

次に、**brief** キーワードを使用して SXP 接続を表示する例を示します。

```
Device# show cts sxp connection brief

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
------------------------------------------------------------------------------
Peer_IP          Source_IP        Conn Status       Duration
------------------------------------------------------------------------------
10.10.10.1          10.10.10.2          On               0:00:02:14 (dd:hr:mm:sec)
10.10.2.1          10.10.2.2          On               0:00:02:14 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

次に、CTS-SXP 接続を表示する例を示します。

```
Device# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
------------------------------------------------
Peer IP          : 10.10.10.1
Source IP        : 10.10.10.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
```

```
----------------------------------------------
Peer IP          : 10.10.2.1
Source IP        : 10.10.2.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

次に、デバイスがスピーカーとリスナーの両方である場合に双方向接続のCTS-SXP接続を表示する例を示します。

```
Device# show cts sxp connections

SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
----------------------------------------------
Peer IP : 2.0.0.2
Source IP : 1.0.0.2
Conn status : On (Speaker) :: On (Listener)
Conn version : 4
Local mode : Both
Connection inst# : 1
TCP conn fd : 1(Speaker) 3(Listener)
TCP conn password: default SXP password
Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46 (dd:hr:mm:sec)
```

次に、SXPスピーカーへの接続が切断されたCTS-SXPリスナーからの出力例を示します。送信元IPとSGTのマッピングは120秒（削除のホールドダウンタイマーのデフォルト値）の間保持されます。

```
Device# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 10.10.10.1
Source IP        : 10.10.10.2
Set up           : Peer
Conn status      : Delete_Hold_Down
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : -1
TCP conn password: not set (using default SXP password)
Delete hold down timer is running
Duration since last state change: 0:00:00:16 (dd:hr:mm:sec)
----------------------------------------------
Peer IP          : 10.10.2.1
```

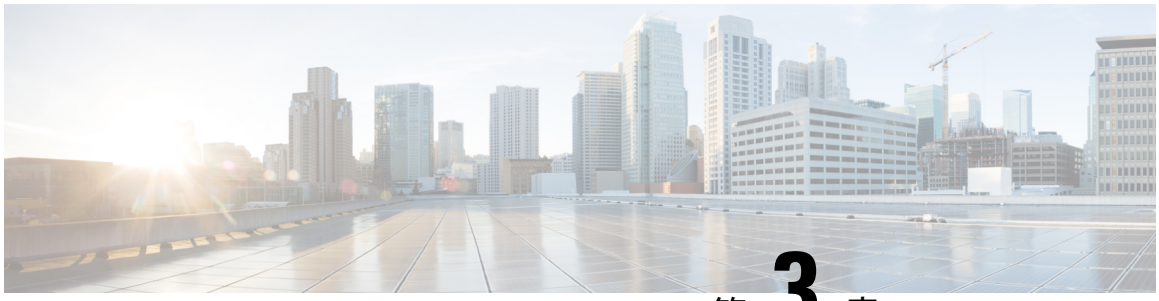
```
Source IP        : 10.10.2.2
Set up           : Peer
Conn status      : On
Connection inst# : 1
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:05:49 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

関連コマンド

コマンド	説明
cts sxp connection peer	Cisco TrustSec SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default password	Cisco TrustSec SXP のデフォルトパスワードを設定します。
cts sxp default source-ip	Cisco TrustSec SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで Cisco TrustSec SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングを有効にします。
cts sxp reconciliation	Cisco TrustSec SXP の復帰期間を変更します。
cts sxp retry	Cisco TrustSec SXP の再試行期間タイマーを変更します。

第 II 部

インターフェイスおよびハードウェア コンポーネント



第 3 章

インターフェイスおよびハードウェア コマンド

• voice vlan（ネットワークポリシー コンフィギュレーション） （186 ページ）

debug ilpower

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

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

構文の説明

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

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

このコマンドは、PoE 対応スイッチだけでサポートされています。

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

debug interface

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

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

構文の説明

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

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

キーワードを指定しない場合は、すべてのデバッグ メッセージが表示されます。

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

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

debug lldp packets

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

debug lldp packets
no debug lldp packets

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

あるスイッチスタック上でデバッグをイネーブルにした場合は、でのみイネーブルになります。スタックメンバのデバッグをイネーブルにする場合は、 **session** *switch-number* EXEC コマンドを使用してからセッションを開始してください。

debug platform poe

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

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

構文の説明

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

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード　特権 EXEC

コマンド履歴

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

使用上のガイドライン　**undebug platform poe** コマンドは **no debug platform poe** コマンドと同じです。

debug platform software fed switch active punt packet-capture start

アクティブスイッチの CPU 使用率が高いときのパケットのデバッグを有効にするには、特権 EXEC モードで **debug platform software fed switch active punt packet-capture start** コマンドを使用します。アクティブスイッチの CPU 使用率が高いときのパケットのデバッグを無効にするには、特権 EXEC モードで **debug platform software fed switch active punt packet-capture stop** コマンドを使用します。

debug platform software fed switch active punt packet-capture start
debug platform software fed switch active punt packet-capture stop

構文の説明

switch active	アクティブスイッチに関する情報を表示します。
punt	パント情報を指定します。
packet-capture	キャプチャされたパケットに関する情報を指定します。
start	アクティブスイッチのデバッグを有効にします。
stop	アクティブスイッチのデバッグを無効にします。

コマンド モード　特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 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　**debug platform software fed switch active punt packet-capture start** コマンドを設定すると、CPU 使用率が高いときにパケットのデバッグが開始されます。バッファサイズが 4K を超えるとパケットキャプチャが停止します。

例

次に、**debug platform software fed switch active punt packet-capture start** コマンドの出力例を示します。

```
Device# debug platform software fed switch active packet-capture start
Punt packet capturing started.
```

次に、**debug platform software fed switch active punt packet-capture stop** コマンドの出力例を示します。

```
Device# debug platform software fed switch active packet-capture stop
Punt packet capturing stopped. Captured 101 packet(s)
```

duplex

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

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

構文の説明

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

コマンド デフォルト

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

100BASE-*x*（-*x* は -BX、-FX、-FX-FE、または -LX）SFP モジュールのデフォルトは **half** です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

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

使用上のガイドライン

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

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

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

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

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

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

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

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

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

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

例

次の例では、インターフェイスを全二重動作に設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# duplex full
```

errdisable detect cause

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

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

構文の説明

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

security-violation shutdown vlan	音声認識 IEEE 802.1X セキュリティをイネーブルにします。
sfp-config-mismatch	SFP 設定の不一致によるエラー検出をイネーブルにします。

コマンド デフォルト

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

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

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

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

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

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

```
デバイス(config)# errdisable detect cause link-flap
```

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

```
デバイス(config)# errdisable detect cause bpduguard shutdown vlan
```

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

```
デバイス(config)# errdisable detect cause security-violation shutdown vlan
```

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

errdisable recovery cause

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

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

構文の説明

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

l2ptguard	レイヤ2プロトコル トンネルによる errdisable ステートから回復するためのタイマーをイネーブルにします。
link-flap	リンクフラップ errdisable ステートから回復するタイマーをイネーブルにします。
loopback	ループバック errdisable ステートから回復するタイマーをイネーブルにします。
mac-limit	MAC 制限 errdisable ステートから回復するタイマーをイネーブルにします。
pagp-flap	ポート集約プロトコル（PAgP）フラップ errdisable ステートから回復するタイマーをイネーブルにします。
port-mode-failure	ポート モードの変更失敗の errdisable ステートから回復するタイマーをイネーブルにします。
pppoe-ia-rate-limit	PPPoE IA レート制限 errdisable ステートから回復するタイマーをイネーブルにします。
psecure-violation	ポートセキュリティ違反ディセーブルステートから回復するタイマーをイネーブルにします。
security-violation	IEEE 802.1X 違反ディセーブルステートから回復するタイマーをイネーブルにします。
sfp-config-mismatch	SFP設定の不一致によるエラー検出をイネーブルにします。
storm-control	ストーム制御エラーから回復するタイマーをイネーブルにします。
udld	単方向リンク検出（UDLD）errdisable ステートから回復するタイマーをイネーブルにします。

コマンド デフォルト

すべての原因に対して回復はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

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

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

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

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

例

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

```
デバイス(config)# errdisable recovery cause bpduguard
```

errdisable recovery interval

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

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

構文の説明

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

コマンド デフォルト

デフォルトの回復間隔は 300 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

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

例

次の例では、タイマーを 500 秒に設定する方法を示します。

```
デバイス(config)# errdisable recovery interval 500
```

interface

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

interface {**Auto-Template** *interface-number* | **GigabitEthernet** *switch-number/slot-number/port-number* | **Group VI** *Group VI interface number* | **Internal Interface** *Internal Interface number* | **Loopback** *interface-number* **Null** *interface-number* **Port-channel** *interface-number* **TenGigabitEthernet** *switch-number/slot-number/port-number* **Tunnel** *interface-number* **Vlan** *interface-number* }

Auto-Template *interface-number*	自動テンプレート インターフェイスを設定できます。範囲は 1 ～ 999 です。
GigabitEthernet *switch-number/slot-number/port-number*	ギガビットイーサネット IEEE 802.3z インターフェイスを設定できます。範囲は 0 ～ 9 です。
Group VI *Group VI interface number*	Group VI インターフェイスを設定できます。範囲は 0 ～ 9 です。
Internal Interface Internal Interface	内部インターフェイスを設定できます。
Loopback *interface-number*	ループバック インターフェイスを設定できます。指定できる範囲は 0 ～ 2147483647 です。
Null *interface-number*	ヌルインターフェイスを設定できます。デフォルト値は 0 です。
Port-channel *interface-number*	ポートチャネル インターフェイスを設定できます。有効な範囲は 1 ～ 128 です。
TenGigabitEthernet *switch-number/slot-number/port-number*	10 ギガビットイーサネットインターフェイスを設定できます。 • *switch-number*：スイッチ ID。有効な範囲は 1 ～ 8 です。 • *slot-number* ：スロット番号。値の範囲は 0 ～ 1 です。 • *port-number*：ポート番号。範囲は 1 ～ 24 および 37 ～ 48 です。 .

Tunnel *interface-number*	トンネルインターフェイスを設定できます。指定できる範囲は 0 ～ 2147483647 です。
Vlan *interface-number*	スイッチ VLAN を設定できます。指定できる範囲は 1 ～ 4094 です。

コマンド デフォルト　なし

コマンド モード　グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン　このコマンドは「no」形式を使用できません。

次に、トンネルインターフェイスを設定する例を示します。

```
デバイス# interface Tunnel 15
```

interface range

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

interface range {**Auto-Template** *interface-number* | **GigabitEthernet** *switch-number/slot-number/port-number* | **Loopback** *interface-number* | **Null** *interface-number* | **Port-channel** *interface-number* | **TenGigabitEthernet** *switch-number/slot-number/port-number* | **Tunnel** *interface-number* | **Vlan** *interface-number* }

Auto-Template *interface-number*	自動テンプレート インターフェイスを設定できます。範囲は 1 ～ 999 です。
GigabitEthernet *switch-number/slot-number/port-number*	ギガビットイーサネット IEEE 802.3z インターフェイスを設定できます。 • *switch-number*：スイッチ ID。有効な範囲は 1 ～ 8 です。 • *slot-number* ：スロット番号。値の範囲は 0 ～ 1 です。 • *port-number* ：ポート番号。有効な範囲は 1 ～ 48 です。

Loopback *interface-number*	ループバック インターフェイスを設定できます。指定できる範囲は 0 ～ 2147483647 です。
Null *interface-number*	ヌルインターフェイスを設定できます。デフォルト値は 0 です。
Port-channel *interface-number*	ポートチャネル インターフェイスを設定できます。有効な範囲は 1 ～ 128 です。
TenGigabitEthernet *switch-number/slot-number/port-number*	10 ギガビットイーサネットインターフェイスを設定できます。 • *switch-number*：スイッチ ID。有効な範囲は 1 ～ 8 です。 • *slot-number*：スロット番号。値の範囲は 0 ～ 1 です。 • *port-number*：ポート番号。有効な範囲は 1 ～ 24 および 37 ～ 48 です。
Tunnel *interface-number*	トンネルインターフェイスを設定できます。指定できる範囲は 0 ～ 2147483647 です。
Vlan *interface-number*	スイッチ VLAN を設定できます。指定できる範囲は 1 ～ 4094 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

次に、インターフェイス範囲を設定する例を示します。

```
デバイス(config)# interface range vlan 1-100
```

ip mtu

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

ip mtu *bytes*
no ip mtu *bytes*

構文の説明

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

コマンド デフォルト

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

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

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

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

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

```
デバイス(config)# interface vlan 200
デバイス(config-if)# ip mtu 1000
```

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

```
デバイス(config)# interface vlan 200
デバイス(config-if)# default ip mtu
```

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

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

<output truncated>
```

ipv6 mtu

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

ipv6 mtu *bytes*
no ipv6 mtu *bytes*

構文の説明

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

コマンド デフォルト

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

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

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

設定を確認するには、**show ipv6 interface** *interface-id* または **show interface** *interface-id* 特権 EXEC コマンドを入力します。

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

```
デバイス(config)# interface gigabitethernet4/0/1
デバイス(config-if)# ipv6 mtu 2000
```

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

```
デバイス(config)# interface gigabitethernet4/0/1
デバイス(config-if)# default ipv6 mtu
```

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

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

<output truncated>
```

lldp（インターフェイス コンフィギュレーション）

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

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

構文の説明

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

コマンド デフォルト

LLDP はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

このコマンドは、802.1 メディア タイプでサポートされています。

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

インターフェイスの LLDP 伝送をディセーブルにする例を示します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# no lldp transmit
```

インターフェイスの LLDP 伝送をイネーブルにする例を示します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# lldp transmit
```

logging event power-inline-status

Power over Ethernet (PoE) イベントのロギングをイネーブルにするには、インターフェイス コンフィギュレーション モードで **logging event power-inline-status** コマンドを使用します。PoE ステータス イベントのロギングを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。

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

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

PoE イベントのロギングはイネーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

このコマンドの **no** 形式を使用しても、PoE エラーイベントはディセーブルになりません。

例

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

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

mdix auto

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

mdix auto
no mdix auto

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

Auto MDIX は、イネーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

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

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

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

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

mode（電源スタックの設定）

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

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

構文の説明

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

コマンド デフォルト

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

コマンド モード

電源スタックの設定

コマンド履歴

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

使用上のガイドライン

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

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

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

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

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

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

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

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

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

```
デバイス(config)# stack-power stack power1
デバイス(config-stackpower)# mode power-shared strict
デバイス(config-stackpower)# exit
```

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

```
デバイス(config)# stack-power stack power2
デバイス(config-stackpower)# mode redundant
デバイス(config-stackpower)# exit
```

network-policy

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

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

構文の説明

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

コマンド デフォルト

ネットワークポリシー プロファイルは適用されません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

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

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

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# network-policy 60
```

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

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

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

構文の説明

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

コマンド デフォルト

ネットワークポリシー プロファイルは定義されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

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

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

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

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

```
デバイス(config)# network-policy profile 60
デバイス(config-network-policy)#
```

power efficient-ethernet auto

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

power efficient-ethernet auto
no power efficient-ethernet auto

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

EEE は、ディセーブルにされています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

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

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

このコマンドにライセンスは必要ありません。

次に、インターフェイスで EEE をイネーブルにする例を示します。

```
デバイス(config-if)# power efficient-ethernet auto
デバイス(config-if)#
```

次に、インターフェイスで EEE をディセーブルにする例を示します。

```
デバイス(config-if)# no power efficient-ethernet auto
デバイス(config-if)#
```

power-priority

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

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

構文の説明

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

コマンド デフォルト

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

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

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

コマンド モード

スイッチのスタック電源設定

コマンド履歴

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

使用上のガイドライン

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

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

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

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

例

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

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

power inline

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

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

構文の説明

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

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

コマンド デフォルト

デフォルトは **auto**（イネーブル）です。

最大ワット数は、30,000 mW です。

デフォルトのポート プライオリティは低です。

コマンド デフォルト

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

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

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

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

max *max-wattage* オプションを使用して、受電デバイスの電力が制限を超えないようにします。この設定によって、受電デバイスが最大ワット数より多い電力を要求する Cisco Discovery

Protocol（CDP）メッセージを送信すると、スイッチはポートへ電力を供給しません。受電装置のIEEEクラスの最大値が最大ワット数を超えると、スイッチは装置に電力を供給しません。電力は、グローバル電力バジェットに送られます。

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

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

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

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

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

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

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

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

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

例

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

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# power inline auto
```

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

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

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

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

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

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# power inline never
```

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

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

power inline police

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

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

構文の説明

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

コマンド デフォルト

受電デバイスのリアルタイムの電力消費のポリシングは、ディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

このコマンドは、LAN Base イメージのみでサポートされています。

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

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

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

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

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

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

カットオフ電力量の値を手動で設定しない場合、deviceは、CDP電力ネゴシエーションまたはデバイスのIEEE分類とLLDP電力ネゴシエーションを使用して自動的に値を決定します。CDPまたはLLDPがイネーブルでない場合は、デフォルト値の30 Wが適用されます。ただし、CDPまたはLLDPがない場合は、15400 ～ 30000 mW の値が CDP 要求または LLDP 要求だけに基づいて割り当てられるため、装置で 15.4 W を超える電力の消費がdevice から許可されません。受電デバイスが CDP または LLDP のネゴシエーションなしに 15.4 W を超える電力を消費する

場合、装置は最大電流 *Imax* の制限に違反し、最大値を超える電流が供給されるという *Icut* 障害が発生する可能性があります。再び電源を入れるまで、ポートは障害状態のままになります。ポートで継続的に 15.4 W を超える電力が給電される場合、このサイクルが繰り返されます。

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

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

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

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

⚠

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

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

例

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

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

power supply

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

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

構文の説明

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

コマンド デフォルト

スイッチの電源がオンになります。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

同じプラットフォームスイッチを含むスイッチスタックでは、**slot** {**A** | **B**} **off** または **on** キーワードの入力前にスタックメンバを指定する必要があります。

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

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

例

次に、スロット A の電源装置をオフに設定する例を示します。

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

次に、スロット A の電源装置をオンに設定する例を示します。

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

次に、show env power コマンドの出力例を示します。

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

show eee

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

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

構文の説明

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

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

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

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

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

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

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

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

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

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

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

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

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

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

表 *6 : show eee status* のフィールドの説明

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

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

show env

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

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

構文の説明

all	ファンと温度環境の状態、および、内部電源を表示します。
fan	スイッチのファンの状態を表示します。
power	アクティブスイッチの内部電源の状態を表示します。

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

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

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

show env temperature コマンドを使用して、スイッチの温度状態を表示することもできます。コマンド出力では、GREEN および YELLOW ステートを *OK* と表示し、RED ステートを *FAULTY*

と表示します。**show env all** コマンドを入力した場合のコマンド出力は、**show env temperature status** コマンド出力と同じです。

例

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

```
デバイス>show env all
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is OK
FAN PS-2 is NOT PRESENT
Switch 1: SYSTEM TEMPERATURE is OK
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
1A  PWR-C2-250WAC       LIT16372A1M  OK              Good     Good     250
1B  Not Present
```

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

次に、**show env power** コマンドの出力例を示します。

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

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

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

```
デバイス# show env power all
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
1A  PWR-C2-250WAC       LIT16372A1M  OK              Good     Good     250
```

```
1B  Not Present


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


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

表 *7 : show env temperature status* コマンド出力のステート

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

show errdisable detect

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

show errdisable detect

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

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

errdisable 検出は次のモードで設定できます。

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

```
デバイス> show errdisable detect
ErrDisable Reason    Detection    Mode
-----------------    ---------    ----
arp-inspection       Enabled      port
bpduguard            Enabled      vlan
channel-misconfig    Enabled      port
community-limit      Enabled      port
dhcp-rate-limit      Enabled      port
dtp-flap             Enabled      port
gbic-invalid         Enabled      port
inline-power         Enabled      port
invalid-policy       Enabled      port
l2ptguard            Enabled      port
link-flap            Enabled      port
loopback             Enabled      port
lsgroup              Enabled      port
pagp-flap            Enabled      port
psecure-violation    Enabled      port/vlan
security-violatio    Enabled      port
sfp-config-mismat    Enabled      port
storm-control        Enabled      port
udld                 Enabled      port
```

show errdisable recovery

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

show errdisable recovery

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

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

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

```
デバイス> show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Enabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Disabled
loopback             Disabled
Timer interval:300 seconds
Interfaces that will be enabled at the next timeout:
Interface    Errdisable reason    Time left(sec)
---------    -----------------    --------------
Gi1/0/2        link-flap             279
```

show interfaces

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

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

構文の説明

interface-id	（任意）インターフェイスの ID です。有効なインターフェイスには、物理ポート（タイプ、スタック構成可能なスイッチのスタックメンバ、モジュール、およびポート番号を含む）やポートチャネルが含まれます。指定できるポート チャネルは 1 ～ 48 です。
vlan *vlan-id*	（任意）VLAN ID です。指定できる範囲は 1 ～ 4094 です。
accounting	（任意）インターフェイスのアカウント情報（アクティブ プロトコル、入出力のパケット、オクテットを含む）を表示します。 （注） ソフトウェアで処理されたパケットだけが表示されます。ハードウェアでスイッチングされるパケットは表示されません。
capabilities	（任意）すべてのインターフェイスまたは指定されたインターフェイスの性能（機能、インターフェイス上で設定可能なオプションを含む）を表示します。このオプションはコマンドラインのヘルプに表示されますが、VLAN ID に使用できません。
module *number*	（任意）スイッチまたは指定されたスタック メンバのすべてのインターフェイスの機能を表示します。 このオプションは、特定のインターフェイス ID を入力したときは利用できません。
description	（任意）特定のインターフェイスに設定された管理ステータスおよび説明を表示します。
etherchannel	（任意）インターフェイス EtherChannel 情報を表示します。
flowcontrol	（任意）インターフェイスのフロー制御情報を表示します。
private-vlan mapping	（任意）VLAN スイッチ仮想インターフェイス（SVI）のプライベート VLAN のマッピング情報を表示します。スイッチが LAN Base フィーチャ セットを実行している場合、このキーワードは使用できません。
pruning	（任意）インターフェイスのトランク VTP プルーニング情報を表示します。

stats	（任意）インターフェイスのパスを切り替えることによる入出力パケットを表示します。
status	（任意）インターフェイスのステータスを表示します。Type フィールドの unsupported のステータスは、他社製の Small Form-Factor Pluggable（SFP）モジュールがモジュール スロットに装着されていることを示しています。
err-disabled	（任意）errdisable ステートのインターフェイスを表示します。
trunk	（任意）インターフェイス トランク情報を表示します。インターフェイスを指定しない場合は、アクティブなトランキング ポートの情報だけが表示されます。

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

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

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

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

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

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

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

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

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

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

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

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

次の例では、プライベート VLAN が設定されている場合の特定のインターフェイスの **show interfaces status** コマンドの出力を示します。ポート 22 をプライベート VLAN ホスト ポートとして設定しています。ポート 22 は、プライマリ VLAN 20 とセカンダリ VLAN 25 に関連付けられます。

```
デバイス# show interfaces gigabitethernet1/0/22 status
Port       Name      Status      Vlan      Duplex      Speed      Type
Gi1/0/22             connected   20,25     a-full      a-100      10/100BaseTX
```

次の例では、ポート 20 がプライベート VLAN 無差別ポートとして設定されています。この出力は、プライマリ VLAN 20 だけを表示します。

```
デバイス# show interfaces gigabitethernet1/0/20 status
Port       Name      Status      Vlan      Duplex      Speed      Type
Gi1/0/20             connected   20        a-full      a-100      10/100BaseTX
```

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

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

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

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


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

Port        Vlans allowed on trunk
Gi1/0/1     none

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

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

show interfaces counters

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

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

構文の説明

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

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

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

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

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

<output truncated>
```

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

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

<output truncated>
```

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

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

<output truncated>
```

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

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

<output truncated>
```

show interfaces switchport

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

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

構文の説明

interface-id	（任意）インターフェイスのIDです。有効なインターフェイスには、物理ポート（タイプ、スタック構成可能なスイッチのスタック メンバ、モジュール、およびポート番号を含む）やポート チャネルが含まれます。指定できるポート チャネルは1 ～ 48です。
module *number*	（任意）スイッチまたは指定されたスタック メンバのすべてのインターフェイスのスイッチポート設定を表示します。 このオプションは、特定のインターフェイス IDを入力したときは利用できません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

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

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

```
デバイス# show interfaces gigabitethernet1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
```

```
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 10 (VLAN0010)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 11-20
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

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

フィールド	説明
Name	ポート名を表示します。
Switchport	ポートの管理ステータスおよび動作ステータスを表示します。この出力の場合、ポートはスイッチポート モードです。
Administrative Mode Operational Mode	管理モードおよび動作モードを表示します。
Administrative Trunking Encapsulation Operational Trunking Encapsulation Negotiation of Trunking	管理上および運用上のカプセル化方式、およびトランキング ネゴシエーションがイネーブルかどうかを表示します。
Access Mode VLAN	ポートを設定する VLAN ID を表示します。
Trunking Native Mode VLAN Trunking VLANs Enabled Trunking VLANs Active	ネイティブ モードのトランクの VLAN ID を一覧表示します。トランク上の許可 VLAN を一覧表示します。トランク上のアクティブ VLAN を一覧表示します。
Pruning VLANs Enabled	プルーニングに適格な VLAN を一覧表示します。
Protected	インターフェイス上で保護ポートがイネーブル（True）であるかまたはディセーブル（False）であるかを表示します。

フィールド	説明
Unknown unicast blocked Unknown multicast blocked	不明なマルチキャストおよび不明なユニキャスト トラフィックがインターフェイス上でブロックされているかどうかを表示します。
Voice VLAN	音声 VLAN がイネーブルである VLAN ID を表示します。
Appliance trust	IP Phone のデータ パケットのサービス クラス（CoS）設定を表示します。

show interfaces transceiver

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

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

構文の説明

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

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

例

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

```
デバイス# show interfaces transceiver

If device is externally calibrated, only calibrated values are printed.
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).

                                          Optical   Optical
           Temperature  Voltage  Current   Tx Power  Rx Power
Port       (Celsius)    (Volts)  (mA)      (dBm)     (dBm)
---------  -----------  -------  --------  --------  --------
Gi5/1/2      42.9       3.28      22.1      -5.4      -8.1
Te5/1/3      32.0       3.28      19.8       2.4      -4.2


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

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

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

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

           Optical          High Alarm  High Warn  Low Warn   Low Alarm
           Transmit Power   Threshold   Threshold  Threshold  Threshold
  Port     (dBm)            (dBm)       (dBm)      (dBm)      (dBm)
  -------  ---------------  ----------  ---------  ---------  ---------
```

```
  Gi1/1/1  1.8                7.9         3.9         0.0         -4.0

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

```
デバイス# show interfaces transceiver supported-list
Transceiver Type           Cisco p/n min version
                               supporting DOM
------------------       -------------------------

   DWDM GBIC                ALL
   DWDM SFP                 ALL
   RX only WDM GBIC         ALL
   DWDM XENPAK              ALL
   DWDM X2                  ALL
   DWDM XFP                 ALL
   CWDM GBIC                NONE
   CWDM X2                  ALL
   CWDM XFP                 ALL
   XENPAK ZR                ALL
   X2 ZR                    ALL
   XFP ZR                   ALL
   Rx_only_WDM_XENPAK       ALL
   XENPAK_ER                10-1888-04
   X2_ER                    ALL
   XFP_ER                   ALL
   XENPAK_LR                10-1838-04
   X2_LR                    ALL
   XFP_LR                   ALL
   XENPAK_LW                ALL
   X2_LW                    ALL
   XFP_LW                   NONE
   XENPAK SR                NONE
   X2 SR                    ALL
   XFP SR                   ALL
   XENPAK LX4               NONE
   X2 LX4                   NONE
   XFP LX4                  NONE
   XENPAK CX4               NONE
   X2 CX4                   NONE
   XFP CX4                  NONE
   SX GBIC                  NONE
   LX GBIC                  NONE
   ZX GBIC                  NONE
   CWDM_SFP                 ALL
   Rx_only_WDM_SFP          NONE
   SX_SFP                   ALL
   LX_SFP                   ALL
   ZX_SFP                   ALL
   EX_SFP                   ALL
   SX SFP                   NONE
   LX SFP                   NONE
   ZX SFP                   NONE
   GIgE BX U SFP            NONE
   GigE BX D SFP            ALL
   X2 LRM                   ALL
   SR_SFPP                  ALL
   LR_SFPP                  ALL
   LRM_SFPP                 ALL
   ER_SFPP                  ALL
```

```
   ZR_SFPP                  ALL
   DWDM_SFPP                ALL
   GIgE BX 40U SFP          ALL
   GigE BX 40D SFP          ALL
   GigE BX 40DA SFP         ALL
   GIgE BX 80U SFP          ALL
   GigE BX 80D SFP          ALL
   GIG BXU_SFPP             ALL
   GIG BXD_SFPP             ALL
   GIG BX40U_SFPP           ALL
   GIG BX40D_SFPP           ALL
   GigE Dual Rate LX SFP    ALL
   CWDM_SFPP                ALL
   CPAK_SR10                ALL
   CPAK_LR4                 ALL
   QSFP_LR                  ALL
   QSFP_SR                  ALL
```

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

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

 DWDM GBIC
Min1             -4.00        -32.00        -4           N/A          4.65
Min2              0.00        -28.00        0            N/A          4.75
Max2              4.00         -9.00        70           N/A          5.25
Max1              7.00         -5.00        74           N/A          5.40
 DWDM SFP
Min1             -4.00        -32.00        -4           N/A          3.00
Min2              0.00        -28.00        0            N/A          3.10
Max2              4.00         -9.00        70           N/A          3.50
Max1              8.00         -5.00        74           N/A          3.60
 RX only WDM GBIC
Min1              N/A         -32.00        -4           N/A          4.65
Min2              N/A         -28.30        0            N/A          4.75
Max2              N/A          -9.00        70           N/A          5.25
Max1              N/A          -5.00        74           N/A          5.40
 DWDM XENPAK
Min1             -5.00        -28.00        -4           N/A          N/A
Min2             -1.00        -24.00        0            N/A          N/A
Max2              3.00         -7.00        70           N/A          N/A
Max1              7.00         -3.00        74           N/A          N/A
 DWDM X2
Min1             -5.00        -28.00        -4           N/A          N/A
Min2             -1.00        -24.00        0            N/A          N/A
Max2              3.00         -7.00        70           N/A          N/A
Max1              7.00         -3.00        74           N/A          N/A
 DWDM XFP
Min1             -5.00        -28.00        -4           N/A          N/A
Min2             -1.00        -24.00        0            N/A          N/A
Max2              3.00         -7.00        70           N/A          N/A
Max1              7.00         -3.00        74           N/A          N/A
 CWDM X2
Min1              N/A           N/A         0            N/A          N/A
Min2              N/A           N/A         0            N/A          N/A
Max2              N/A           N/A         0            N/A          N/A
Max1              N/A           N/A         0            N/A          N/A

<output truncated>
```

関連コマンド

コマンド	説明
transceiver type all	トランシーバタイプ コンフィギュレーション モードを開始します。
monitoring	デジタル オプティカル モニタリングを有効にします。

show memory platform

プラットフォームのメモリ統計情報を表示するには、特権EXECモードで**show memory platform**コマンドを使用します。

show memory platform [{**compressed-swap** | **information** | **page-merging**}]

構文の説明

compressed-swap	（任意）プラットフォーム メモリの圧縮スワップ情報を表示します。
information	（任意）プラットフォームに関する一般的な情報を表示します。
page-merging	（任意）プラットフォーム メモリのページマージング情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

Cisco IOS XE Denali 16.3.1 より前は、コマンド出力に表示される「空きメモリ」は基盤となるLinuxカーネルから得ていました。使用可能な一部のメモリ チャンクは空きメモリと見なされていなかったため、この値は正確ではありませんでした。

Cisco IOS XE Denali 16.3.1では、空きメモリは正確に計算されて、コマンド出力のFree Memoryフィールドに表示されます。

例

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

```
Switch# show memory platform

 Virtual memory   : 12874653696
  Pages resident   : 627041
  Major page faults: 2220
  Minor page faults: 2348631

  Architecture     : mips64
  Memory (kB)
    Physical       : 3976852
    Total          : 3976852
    Used           : 2761276
```

```
    Free           : 1215576
    Active         : 2128196
    Inactive       : 1581856
    Inact-dirty    : 0
    Inact-clean    : 0
    Dirty          : 0
    AnonPages      : 1294984
    Bounce         : 0
    Cached         : 1978168
    Commit Limit   : 1988424
    Committed As   : 3343324
    High Total     : 0
    High Free      : 0
    Low Total      : 3976852
    Low Free       : 1215576
    Mapped         : 516316
    NFS Unstable   : 0
    Page Tables    : 17124
    Slab           : 0
    VMmalloc Chunk : 1069542588
    VMmalloc Total : 1069547512
    VMmalloc Used  : 2588
    Writeback      : 0
    HugePages Total: 0
    HugePages Free : 0
    HugePages Rsvd : 0
    HugePage Size  : 2048

  Swap (kB)
    Total          : 0
    Used           : 0
    Free           : 0
    Cached         : 0

  Buffers (kB)     : 437136

  Load Average
    1-Min          : 1.04
    5-Min          : 1.16
    15-Min         : 0.94
```

次に、**show memory platform information** コマンドの出力例を示します。

```
Device# show memory platform information

 Virtual memory   : 12870438912
  Pages resident   : 626833
  Major page faults: 2222
  Minor page faults: 2362455

  Architecture     : mips64
  Memory (kB)
    Physical       : 3976852
    Total          : 3976852
    Used           : 2761224
    Free           : 1215628
    Active         : 2128060
    Inactive       : 1584444
    Inact-dirty    : 0
    Inact-clean    : 0
    Dirty          : 284
    AnonPages      : 1294656
```

```
  Bounce         : 0
  Cached         : 1979644
  Commit Limit   : 1988424
  Committed As   : 3342184
  High Total     : 0
  High Free      : 0
  Low Total      : 3976852
  Low Free       : 1215628
  Mapped         : 516212
  NFS Unstable   : 0
  Page Tables    : 17096
  Slab           : 0
  VMmalloc Chunk : 1069542588
  VMmalloc Total : 1069547512
  VMmalloc Used  : 2588
  Writeback      : 0
  HugePages Total: 0
  HugePages Free : 0
  HugePages Rsvd : 0
  HugePage Size  : 2048

Swap (kB)
  Total          : 0
  Used           : 0
  Free           : 0
  Cached         : 0

Buffers (kB)     : 438228

Load Average
  1-Min          : 1.54
  5-Min          : 1.27
  15-Min         : 0.99
```

show module

スイッチ番号、モデル番号、シリアル番号、ハードウェア リビジョン番号、ソフトウェア バージョン、MAC アドレスなどのモジュール情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで、このコマンドを使用します。

```
show module [{switch-num }]
```

構文の説明

switch-num	（任意）スイッチの番号。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴	リリース	変更内容
	Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン *switch-num* 引数を指定せずに **show module** コマンドを入力した場合、show module all コマンドを入力した場合と同じ結果になります。

show mgmt-infra trace messages ilpower

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

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

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

コマンド デフォルト なし

コマンド モード 特権 EXEC

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

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

```
デバイス# show mgmt-infra trace messages ilpower
[10/23/12 14:05:10.984 UTC 1 3] Initialized inline power system configuration fo
r slot 1.
[10/23/12 14:05:10.984 UTC 2 3] Initialized inline power system configuration fo
r slot 2.
[10/23/12 14:05:10.984 UTC 3 3] Initialized inline power system configuration fo
r slot 3.
[10/23/12 14:05:10.984 UTC 4 3] Initialized inline power system configuration fo
r slot 4.
[10/23/12 14:05:10.984 UTC 5 3] Initialized inline power system configuration fo
r slot 5.
[10/23/12 14:05:10.984 UTC 6 3] Initialized inline power system configuration fo
r slot 6.
[10/23/12 14:05:10.984 UTC 7 3] Initialized inline power system configuration fo
r slot 7.
[10/23/12 14:05:10.984 UTC 8 3] Initialized inline power system configuration fo
r slot 8.
[10/23/12 14:05:10.984 UTC 9 3] Initialized inline power system configuration fo
r slot 9.
[10/23/12 14:05:10.984 UTC a 3] Inline power subsystem initialized.
[10/23/12 14:05:18.908 UTC b 264] Create new power pool for slot 1
```

```
[10/23/12 14:05:18.909 UTC c 264] Set total inline power to 450 for slot 1
[10/23/12 14:05:20.273 UTC d 3] PoE is not supported on .
[10/23/12 14:05:20.288 UTC e 3] PoE is not supported on .
[10/23/12 14:05:20.299 UTC f 3] PoE is not supported on .
[10/23/12 14:05:20.311 UTC 10 3] PoE is not supported on .
[10/23/12 14:05:20.373 UTC 11 98] Inline power process post for switch 1
[10/23/12 14:05:20.373 UTC 12 98] PoE post passed on switch 1
[10/23/12 14:05:20.379 UTC 13 3] Slot #1: PoE initialization for board id 16387
[10/23/12 14:05:20.379 UTC 14 3] Set total inline power to 450 for slot 1
[10/23/12 14:05:20.379 UTC 15 3] Gi1/0/1 port config Initialized
[10/23/12 14:05:20.379 UTC 16 3] Interface Gi1/0/1 initialization done.
[10/23/12 14:05:20.380 UTC 17 3] Gi1/0/24 port config Initialized
[10/23/12 14:05:20.380 UTC 18 3] Interface Gi1/0/24 initialization done.
[10/23/12 14:05:20.380 UTC 19 3] Slot #1: initialization done.
[10/23/12 14:05:50.440 UTC 1a 3] Slot #1: PoE initialization for board id 16387
[10/23/12 14:05:50.440 UTC 1b 3] Duplicate init event
```

show mgmt-infra trace messages ilpower-ha

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

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

構文の説明

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

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

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

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

show mgmt-infra trace messages platform-mgr-poe

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

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

構文の説明	**switch** *stack-member-number* （任意）トレースバッファ内のメッセージを表示するスタックメンバ番号を指定します。
コマンド デフォルト	なし
コマンド モード	特権 EXEC

コマンド履歴

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

次の例では、**show mgmt-infra trace messages platform-mgr-poe** コマンドの出力の一部を示します。

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

show network-policy profile

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

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

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

detail	（任意）詳細なステータスと統計情報を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

次に、**show network-policy profile** コマンドの出力例を示します。

```
デバイス# show network-policy profile
Network Policy Profile 10
   voice vlan 17 cos 4
  Interface:
   none
Network Policy Profile 30
   voice vlan 30 cos 5
  Interface:
   none
Network Policy Profile 36
   voice vlan 4 cos 3
  Interface:
   Interface_id
```

show platform hardware fed switch forward

デバイス固有のハードウェア情報を表示するには、**show platform hardware fed switch** *switch_number* コマンドを使用します。

このトピックでは、転送特有のオプション、つまり **show platform hardware fed switch** {*switch_num* | **active** | **standby** } **forward summary** コマンドで使用可能なオプションのみについて詳しく説明します。

show platform hardware fed switch *switch_number* **forward summary** の出力には、パケットに対して下された転送決定に関するすべての詳細が表示されます。

show platform hardware fed switch {*switch_num* | **active** | **standby**} **forward summary**

構文の説明

switch {*switch_num* | **active** | **standby** }	情報を表示するスイッチ。次のオプションがあります。 • *switch_num*：スイッチの ID。 • **active**：アクティブなスイッチに関する情報を表示します。 • **standby**：存在する場合、スタンバイスイッチに関する情報を表示します。

forward summary	パケット転送の情報を表示します。 （注） **summary** キーワードは Cisco IOS XE Denali 16.3.1 リリースで追加されました。 **summary** キーワードが Cisco IOS XE Everest 16.6.1 以降のリリースでは廃止されています。

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 3.3SE	このコマンドが導入されました。
Cisco IOS XE Denali 16.3.1	**summary** キーワードのサポートが追加されました。
Cisco IOS XE Everest 16.6.1 以降のリリース	**summary** キーワードのサポートが廃止されました。

使用上のガイドライン

テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。

コマンド出力に表示されるフィールドついて、以下で説明します。

- Station Index（ステーション インデックス）：Station Index は、レイヤ 2 ルックアップの結果で、以下を表示するステーション記述子にポイントします。
  - Destination Index（接続先インデックス）：パケットを送信する出力ポートを決定します。グローバル ポート番号（GPN）は、接続先インデックスとして使用できます。15 から 12 ビットの接続先インデックスのセットは、使用される GPN を示します。たとえば、接続先インデックス 0xF04E は GPN - 78（0x4e）に対応します。
  - Rewrite Index（書き換えインデックス）：パケットで何が実行される必要があるかを決定します。レイヤ 2 スイッチングの場合、通常はブリッジング アクションです。
  - Flexible Lookup Pipeline Stages（FPS）（フレキシブル ルックアップ パイプライン ステージ）：パケットのルーティングまたはブリッジングのために下された転送判断を示します。
  - Replication Bit Map（複製ビット マップ）：パケットを CPU またはスタックに送信する必要があるかどうかを決定します。
    - ローカル データ コピー = 1
    - リモート データ コピー = 0
    - ローカル CPU コピー = 0

- リモート CPU コピー = 0

例

次に、**show platform hardware fed switch** {*switch_num* | **active** | **standby** } **forward summary** コマンドの出力例を示します。

```
デバイス#show platform hardware fed switch 1 forward summary
Time: Fri Sep 16 08:25:00 PDT 2016

Incomming Packet Details:

###[ Ethernet ]###
  dst       = 00:51:0f:f2:0e:11
  src       = 00:1d:01:85:ba:22
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = 6
     plen      = 4
     op        = is-at
     hwsrc     = 00:1d:01:85:ba:22
     psrc      = 10.10.1.33
     hwdst     = 00:51:0f:f2:0e:11
     pdst      = 10.10.1.1

Ingress:
Switch             : 1
Port               : GigabitEthernet1/0/1
Global Port Number : 1
Local Port Number  : 1
Asic Port Number   : 21
ASIC Number        : 0
STP state          :
                     blkLrn31to0: 0xffdfffdf
                     blkFwd31to0: 0xffdfffdf
Vlan               : 1
Station Descriptor : 170
DestIndex          : 0xF009
DestModIndex       : 2
RewriteIndex       : 2
Forwarding Decision: FPS 2A L2 Destination

Replication Bitmap:
Local CPU copy     : 0
Local Data copy    : 1
Remote CPU copy    : 0
Remote Data copy   : 0

Egress:
Switch             : 1
Outgoing Port      : GigabitEthernet1/0/9
Global Port Number : 9
ASIC Number        : 0
Vlan               : 1
```

show platform hardware fed switch forward interface

転送情報をデバッグし、ハードウェアのフォワーディングプレーンのパケットパスをトレースするには、**show platform hardware fed switch** *switch_number* **forward interface** コマンドを使用します。このコマンドは、ユーザ定義のパケットをシミュレートし、ハードウェアのフォワーディングプレーンから転送情報を取得します。このコマンドで指定したパケットパラメータに基づいて、入力ポートでパケットが生成されます。PCAPファイルに格納されているキャプチャされたパケットから完全なパケットを提供することもできます。

このトピックでは、インターフェイス転送特有のオプション、つまり **show platform hardware fed switch** {*switch_num* | **active** | **standby** } **forward interface** コマンドで使用可能なオプションのみについて詳しく説明します。

show platform hardware fed switch {*switch_num* | **active** | **standby**} **forward interface** *interface-type interface-number* **source-mac-address** *destination-mac-address* {*protocol-number* | **arp** | **cos** | **ipv4** | **ipv6** | **mpls**}

show platform hardware fed switch {*switch_num* | **active** | **standby**} **forward interface** *interface-type interface-number* **pcap** *pcap-file-name* **number** *packet-number* **data**

show platform hardware fed switch {*switch_num* | **active** | **standby**} **forward interface** *interface-type interface-number* **vlan** *vlan-id source-mac-address destination-mac-address* {*protocol-number* | **arp** | **cos** | **ipv4** | **ipv6** | **mpls**}

構文の説明

switch {*switch_num* | **active** | **standby** }	パケットのトレースをスケジュールするスイッチ。このスイッチで入力ポートが使用可能である必要があります。次のオプションがあります。 • *switch_num*：入力ポートが存在するスイッチの ID。 • **active**：入力ポートが存在するアクティブスイッチを示します。 • **standby**：入力ポートが存在するスタンバイスイッチを示します。 （注） このキーワードはサポートされていません。
interface *interface-type interface-number*	パケットのトレースをシミュレートする入力インターフェイス。
source-mac-address	シミュレートするパケットの送信元 MAC アドレス。
destination-mac-address	宛先インターフェイスの 16 進形式の MAC アドレス。
protocol-number	いずれかの L3 プロトコルに割り当てられた番号。
arp	Address Resolution Protocol（ARP）のパラメータ。

ipv4	IPv4 パケットのパラメータ。
ipv6	IPv6 パケットのパラメータ。
mpls	マルチプロトコル ラベル スイッチング（MPLS）ラベルのパラメータ。
cos	プライオリティを設定する 0 ～ 7 のサービスクラス（CoS）値。
pcap *pcap-file-name*	内部フラッシュ（flash:）にある PCAP ファイルの名前。 ファイルが flash: にすでに存在していることを確認してください。
number *packet-number*	PCAP ファイル内のパケット番号を指定します。
vlan *vlan-id*	シミュレートされるパケットの dot1q ヘッダーの VLAN ID。指定できる範囲は 1 ～ 4096 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 16.11.1	このコマンドが導入されました。

使用上のガイドライン

テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。

このコマンドでサポートされるパケットタイプは次のとおりです。

- いずれかの L3 プロトコルを使用する非 IP パケット
- ARP パケット
- いずれかの L4 プロトコルを使用する IPv4 パケット
- TCP/UDP/IGMP/ICMP/SCTP ペイロードで構成される IPv4 パケット
- VxLAN パケット
- 最大 3 つのラベルとメタデータで構成される MPLS パケット
- IPv4/IPv6 ペイロードで構成される MPLS パケット
- TCP/UDP/IGMP/ICMP/SCTP ペイロードで構成される IPv6 パケット

スタック環境では、スタックメンバの数やトポロジに関係なく、スタック全体のパケットをトレースできます。**show platform hardware fed switch** *switch-number* **forward interface** *interface-type interface-number* コマンドは、入力スイッチのすべてのスタックメンバのパケット転送情報を統

合します。これを実現するために、*switch_num* 引数と *interface-number* 引数で指定されたスイッチ番号が入力スイッチの番号と一致していることを確認してください。

PCAP ファイルに格納されているキャプチャされたパケットから特定のパケットをトレースするには、**show platform hardware fed switch forward interface** *interface-type interface-number* **pcap** *pcap-file-name number packet-number* **data** コマンドを使用します。

例

次に、**show platform hardware fed switch** {*switch_num* | **active** | **standby** } **forward interface** コマンドの出力例を示します。

```
Device#show platform hardware fed switch active forward interface gigabitEthernet 1/0/35
 0000.0022.0055 0000.0055.0066 ipv4 44.44.0.2 55.55.0.2 udp 1222 3333

Show forward is running in the background. After completion, syslog will be generated.

*Sep 24 05:57:36.614: %SHFWD-6-PACKET_TRACE_DONE: Switch 1 R0/0: fed: Packet Trace
Complete:  Execute (show platform hardware fed switch <> forward last summary|detail)
*Sep 24 05:57:36.614: %SHFWD-6-PACKET_TRACE_FLOW_ID: Switch 1 R0/0: fed: Packet Trace
Flow id is 150323855361
```

関連コマンド

コマンド	説明
monitor capture interface	接続ポイントおよびパケットフロー方向を指定して、モニタキャプチャポイントを設定します。
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します。
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します。
monitor capture export	キャプチャされたパケットをバッファに保存します。 このコマンドは、**show forward** で **pcap** の入力として使用できる flash: 内の PCAP ファイルにモニタキャプチャバッファをエクスポートするために使用します。

show platform hardware fed switch forward last summary

スイッチまたはスタック内のスイッチからのパケットトレースデータの要約を表示するには、**show platform hardware fed switch** *switch_number***forward last summary** コマンドを使用します。

show platform hardware fed switch *switch_number* **forward last summary** コマンドの出力には、**show forward** コマンドの前回の実行後にパケットに対して下された転送決定に関するすべての詳細が表示されます。

show platform hardware fed switch {*switch_number* | **active** | **standby**} **forward last summary**

構文の説明

switch {*switch_number* | **active** | **standby** }	ポートのパケットキャプチャをスケジュールするスイッチ。次のオプションがあります。 • *switch_num*：入力ポートが存在するスイッチの ID。 • **active**：入力ポートが存在するアクティブスイッチを示します。 • **standby**：入力ポートが存在するスタンバイスイッチを示します。 （注） このキーワードはサポートされていません。
forward last summary	パケット転送の情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。

Cisco IOS XE Gibraltar 16.10.1 では、**show platform hardware fed switch forward last summary** コマンドの機能が次のように拡張されています。

- 着信ポートおよびパケットをシミュレートするために、CPUからデバッグパケットが挿入されます。
- ルックアップ、隣接関係、リライト情報、ドロップの決定、発信ポートなどの転送の詳細を提供するために、デバッグパケットを使用してハードウェアデータパスのパケットがトレースされます。
- 発信ポートにパケットを送信しないように、出力で元のパケットがドロップされます。
- すべてのパケットのコピーが CPU に送信され、パケットトレース出力に詳細が表示されます。

例

次に、**show platform hardware fed switch** {*switch_number* | **active** | **standby** } **forward last summary** コマンドの出力例を示します。

```
Device#show platform hardware fed switch active forward last summary
Input Packet Details:
###[ Ethernet ]###
  dst       = 01:00:5e:01:01:02
  src       = 00:00:00:03:00:05
  type      = 0x0
###[ Raw ]###
     load      = '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00'
Ingress:
   Port                       : GigabitEthernet1/0/11
   Global Port Number         : 11
   Local Port Number          : 11
   Asic Port Number           : 10
   Asic Instance              : 1
   Vlan                       : 20
   Mapped Vlan ID             : 6
   STP Instance               : 4
   BlockForward               : 0
   BlockLearn                 : 0
   L3 Interface               : 39
       IPv4 Routing           : enabled
       IPv6 Routing           : enabled
       Vrf Id                 : 0
   Adjacency:
       Station Index          : 3      [SI_DIET_L2]
       Destination Index      : 18
       Rewrite Index          : 2
       Replication Bit Map    : 0x15   ['localData', 'remoteData', 'coreData']
   Decision:
       Destination Index      : 24     [DI_DIET_L2]
       Rewrite Index          : 2      [RI_L2]
       Dest Mod Index         : 9      [DMI_IGMP_CTRL_Q]
       CPU Map Index          : 0      [CMI_NULL]
       Forwarding Mode        : 0      [Bridging]
       Replication Bit Map    :        ['localData', 'remoteData', 'coreData']
       Winner                 :        L2DESTMACVLAN LOOKUP
       Qos Label              : 65
       SGT                    : 0
       DGTID                  : 0
Egress:
   Possible Replication       :
       Port                   : GigabitEthernet1/0/11
       Port                   : GigabitEthernet1/0/22
       Port                   : GigabitEthernet2/0/1
   Output Port Data           :
     Port                     : GigabitEthernet1/0/22
       Global Port Number     : 22
       Local Port Number      : 22
       Asic Port Number       : 21
       Asic Instance          : 0
       Unique RI              : 2
       Rewrite Type           : 1      [L2_BRIDGE]
       Mapped Rewrite Type    : 1      [L2_BRIDGE]
       Vlan                   : 20
```

```
      Mapped Vlan ID        : 6
    Port                    : GigabitEthernet2/0/1
      Global Port Number    : 97
      Local Port Number     : 1
      Asic Port Number      : 0
      Asic Instance         : 1
      Unique RI             : 2
      Rewrite Type          : 1      [L2_BRIDGE]
      Mapped Rewrite Type   : 1      [L2_BRIDGE]
      Vlan                  : 20
      Mapped Vlan ID        : 6

Output Packet Details:
   Port                     : GigabitEthernet1/0/22
###[ Ethernet ]###
  dst       = 01:00:5e:01:01:02
  src       = 00:00:00:03:00:05
  type      = 0x0
###[ Raw ]###
     load      = '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00'
   Port                     : GigabitEthernet2/0/1
###[ Ethernet ]###
  dst       = 01:00:5e:01:01:02
  src       = 00:00:00:03:00:05
  type      = 0x0
###[ Raw ]###
     load      = '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00'
*******************************************************************************
```

show platform resources

プラットフォームのリソース情報を表示するには、特権 EXEC モードで **show platform reources** コマンドを使用します。

show platform resources

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドの出力には、総メモリから正確な空きメモリを引いた値である使用メモリが表示されます。

例

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

```
Switch# show platform resources

**State Acronym: H - Healthy, W - Warning, C - Critical

Resource                Usage                Max             Warning         Critical
        State
------------------------------------------------------------------------------------------

 Control Processor      7.20%                100%            90%             95%
        H
  DRAM                  2701MB(69%)          3883MB          90%             95%
        H
```

show platform software fed switch punt cpuq rates

パントされたパスにおけるドロップを含むパケットのパントレートを表示するには、特権EXECモードで **show platform software fed switch punt cpuq rates** コマンドを使用します。

show platform software fed switch {*switch-number* | **active** | **standby**} **punt cpuq rates**

構文の説明

switch{*switch-number* | **active** | **standby**}	スイッチに関する情報を表示します。次の選択肢があります。 • *switch-number*。 • **active** ：アクティブなスイッチに関する情報を表示します。 • **standby**：存在する場合、スタンバイスイッチに関する情報を表示します。 （注） このキーワードはサポートされていません。
punt	パント情報を指定します。
cpuq	CPU 受信キューに関する情報を指定します。
rates	パケットのパントレートを指定します。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

このコマンドの出力には、10 秒、1 分、5 分の各間隔のレートが 1 秒あたりのパケット数で表示されます。

例

次に、**show platform software fed switch active punt cpuq rates** コマンドの出力例を示します。

```
Device#show platform software fed switch active punt cpuq rates

Punt Rate CPU Q Statistics


Packets per second averaged over 10 seconds, 1 min and 5 mins
================================================================================================
 Q  |          Queue             |  Rx    |  Rx    |  Rx    |  Drop  |  Drop    |  Drop
 no |          Name              |  10s   |  1min  |  5min  |  10s   |  1min    |  5min
================================================================================================
 0  CPU_Q_DOT1X_AUTH                0        0        0        0        0        0

 1  CPU_Q_L2_CONTROL                 0        0        0        0        0        0

 2  CPU_Q_FORUS_TRAFFIC              336      266      320      0        0        0

 3  CPU_Q_ICMP_GEN                   0        0        0        0        0        0

 4  CPU_Q_ROUTING_CONTROL            0        0        0        0        0        0

 5  CPU_Q_FORUS_ADDR_RESOLUTION      0        0        0        0        0        0

 6  CPU_Q_ICMP_REDIRECT              0        0        0        0        0        0

 7  CPU_Q_INTER_FED_TRAFFIC          0        0        0        0        0        0

 8  CPU_Q_L2LVX_CONTROL_PKT          0        0        0        0        0        0

 9  CPU_Q_EWLC_CONTROL               0        0        0        0        0        0

 10 CPU_Q_EWLC_DATA                  0        0        0        0        0        0

 11 CPU_Q_L2LVX_DATA_PKT             0        0        0        0        0        0

 12 CPU_Q_BROADCAST                  0        0        0        0        0        0

 13 CPU_Q_LEARNING_CACHE_OVFL        0        0        0        0        0        0

 14 CPU_Q_SW_FORWARDING              0        0        0        0        0        0

 15 CPU_Q_TOPOLOGY_CONTROL           0        0        0        0        0        0

 16 CPU_Q_PROTO_SNOOPING             0        0        0        0        0        0

 17 CPU_Q_DHCP_SNOOPING              0        0        0        0        0        0

 18 CPU_Q_TRANSIT_TRAFFIC            0        0        0        0        0        0
```

```
19 CPU_Q_RPF_FAILED                0        0        0        0        0        0
20 CPU_Q_MCAST_END_STATION_SERVICE 0        0        0        0        0        0
21 CPU_Q_LOGGING                   0        0        0        0        0        0
22 CPU_Q_PUNT_WEBAUTH              0        0        0        0        0        0
23 CPU_Q_HIGH_RATE_APP             0        0        0        0        0        0
24 CPU_Q_EXCEPTION                 0        0        0        0        0        0
25 CPU_Q_SYSTEM_CRITICAL           0        0        0        0        0        0
26 CPU_Q_NFL_SAMPLED_DATA          0        0        0        0        0        0
27 CPU_Q_LOW_LATENCY               0        0        0        0        0        0
28 CPU_Q_EGR_EXCEPTION             0        0        0        0        0        0
29 CPU_Q_FSS                       0        0        0        0        0        0
30 CPU_Q_MCAST_DATA                0        0        0        0        0        0
31 CPU_Q_GOLD_PKT                  0        0        0        0        0        0

------------------------------------------------------------------------------
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *8 : show platform software fed switch active punt cpuq rates* フィールドの説明

フィールド	説明
Queue Name	キューの名前。
Rx	1 秒あたりのパケットの受信レート（10 秒、1 分、5 分）。
ドロップ	1 秒あたりのパケットのドロップレート（10 秒、1 分、5 分）。

show platform software fed switch punt packet-capture display

CPU 使用率が高いときのパケットキャプチャ情報を表示するには、特権 EXEC モードで **show platform software fed switch active punt packet-capture display** コマンドを使用します。

show platform software fed switch active punt packet-capture display { **detailed** | **hexdump**}

構文の説明

switch{*switch-number* | **active** | **standby**}	スイッチに関する情報を表示します。次の選択肢があります。 • **active** ：アクティブなスイッチに関する情報を表示します。 • **standby**：存在する場合、スタンバイスイッチに関する情報を表示します。 （注） **standby** キーワードはサポートされていません。
punt	パント情報を指定します。
packet-capture display	キャプチャされたパケットに関する情報を指定します。
detailed	キャプチャされたパケットに関する詳細な情報を指定します。
hex-dump	キャプチャされたパケットに関する16進数形式の情報を指定します。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

このコマンドの出力には、CPU使用率が上限しきい値を超えているときのCPUバウンドパケット、インバンドCPUトラフィックレート、および実行中のCPUプロセスに関する定期的なログと永続的なログが表示されます。

例

次に、**show platform software fed switch active punt packet-capture display detailed** コマンドの出力例を示します。

```
Device# show platform software fed switch active punt packet-capture display detailed
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 101 packets. Capture capacity : 4096 packets

------ Packet Number: 1, Timestamp: 2018/09/04 23:22:10.179 ------
 interface : GigabitEthernet2/0/2 [if-id: 0x00000032] (physical)
 ether hdr : dest mac: 0100.0ccc.cccd, src mac: 2c36.f8fc.4884
 ether hdr : ethertype: 0x0032

 Doppler Frame Descriptor :
   0000000044004E04  C00F402D94510000  0000000000000100  0000400401000000
   0000000001000050  000000006D000100  0000000025836200  0000000000000000

 Packet Data Dump (length: 68 bytes) :
```

```
   01000CCCCCCD2C36  F8FC48840032AAAA  0300000C010B0000  00000080012C36F8
   FC48800000000080  012C36F8FC488080  040000140002000F  0071000000020001
   244E733E

------ Packet Number: 2, Timestamp: 2018/09/04 23:22:10.179 ------
 interface : GigabitEthernet2/0/2 [if-id: 0x00000032] (physical)
 ether hdr : dest mac: 0180.c200.0000, src mac: 2c36.f8fc.4884
 ether hdr : ethertype: 0x0026
!
!
!
```

show platform software fed switch punt rates interfaces

すべてのインターフェイスのパントレートの全体的な統計を表示するには、特権EXECモードで **show platform software fed switch punt rates interfaces** コマンドを使用します。

show platform software fed switch {*switch-number* | **active** | **standby**} **punt rates interfaces**[**interface-id**]

構文の説明

switch{*switch-number* | **active** | **standby**}	スイッチに関する情報を表示します。次の選択肢があります。 • *switch-number*。 • **active** ：アクティブなスイッチに関する情報を表示します。 • **standby**：存在する場合、スタンバイスイッチに関する情報を表示します。 （注） このキーワードはサポートされていません。
punt	パント情報を指定します。
rates	パケットのパントレートを指定します。
interfaces[**interface-id**]	（任意）インターフェイスの全体的な統計に加え、インターフェイスの10秒間隔でのキュー単位の設定を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 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 この出力には、10 秒、1 分、5 分の各間隔のパントレートが 1 秒あたりのパケット数で表示されます。

例

次に、すべてのインターフェイスについての **show platform software fed switch active punt rates interfaces** コマンドの出力例を示します。

```
Device#show plataform software fed switch active punt rates interfaces

Punt Rate on Interfaces Statistics

Packets per second averaged over 10 seconds, 1 min and 5 mins

================================================================================================

                               |           |  Rx   |  Rx   |  Rx   | Drop |  Drop  |
Drop
 Interface Name                |  IF_ID    |  10s  |  1min |  5min |  10s  |  1min  |
5min
================================================================================================

 Vlan3                          0x00000034    1000    1000     520       0       0
 0
------------------------------------------------------------------------------------------------
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *9 : show platform software fed switch active punt rates interfaces* のフィールドの説明

フィールド	説明
Interface Name	物理インターフェイスの名前。
IF_ID	物理インターフェイスの ID。
Rx	1 秒あたりのパケットの受信レート（10 秒、1 分、5 分）。
ドロップ	1 秒あたりのパケットのドロップレート（10 秒、1 分、5 分）。

次に、特定のインターフェイスについての **show platform software fed switch active punt rates interfaces** *interface-id* コマンドの出力例を示します。

```
Device#show platform software fed switch active punt rates interfaces 0x31
Punt Rate on Single Interfaces Statistics

Interface : Port-channel1 [if_id: 0x31]

  Received                        Dropped
  --------                        -------
   Total          : 29617          Total          : 0
   10 sec average : 0              10 sec average  : 0
    1 min average : 0               1 min average  : 0
    5 min average : 0               5 min average  : 0
```

```
Per CPUQ punt stats on the interface (rate averaged over 10s interval)
=============================================================================
 Q  |          Queue                 |  Recv   |  Recv  |  Drop  |  Drop  |
 no |          Name                  |  Total  |  Rate  |  Total |  Rate  |
=============================================================================
 0   CPU_Q_DOT1X_AUTH                        0        0        0        0
 1   CPU_Q_L2_CONTROL                    29519        0        0        0
 2   CPU_Q_FORUS_TRAFFIC                     0        0        0        0
 3   CPU_Q_ICMP_GEN                          0        0        0        0
 4   CPU_Q_ROUTING_CONTROL                   0        0        0        0
 5   CPU_Q_FORUS_ADDR_RESOLUTION             0        0        0        0
 6   CPU_Q_ICMP_REDIRECT                     0        0        0        0
 7   CPU_Q_INTER_FED_TRAFFIC                 0        0        0        0
 8   CPU_Q_L2LVX_CONTROL_PKT                 0        0        0        0
 9   CPU_Q_EWLC_CONTROL                      0        0        0        0
 10  CPU_Q_EWLC_DATA                         0        0        0        0
 11  CPU_Q_L2LVX_DATA_PKT                    0        0        0        0
 12  CPU_Q_BROADCAST                         0        0        0        0
 13  CPU_Q_LEARNING_CACHE_OVFL               0        0        0        0
 14  CPU_Q_SW_FORWARDING                     0        0        0        0
 15  CPU_Q_TOPOLOGY_CONTROL                 98        0        0        0
 16  CPU_Q_PROTO_SNOOPING                    0        0        0        0
 17  CPU_Q_DHCP_SNOOPING                     0        0        0        0
 18  CPU_Q_TRANSIT_TRAFFIC                   0        0        0        0
 19  CPU_Q_RPF_FAILED                        0        0        0        0
 20  CPU_Q_MCAST_END_STATION_SERVICE         0        0        0        0
 21  CPU_Q_LOGGING                           0        0        0        0
 22  CPU_Q_PUNT_WEBAUTH                      0        0        0        0
 23  CPU_Q_HIGH_RATE_APP                     0        0        0        0
 24  CPU_Q_EXCEPTION                         0        0        0        0
 25  CPU_Q_SYSTEM_CRITICAL                   0        0        0        0
 26  CPU_Q_NFL_SAMPLED_DATA                  0        0        0        0
 27  CPU_Q_LOW_LATENCY                       0        0        0        0
 28  CPU_Q_EGR_EXCEPTION                     0        0        0        0
 29  CPU_Q_FSS                               0        0        0        0
 30  CPU_Q_MCAST_DATA                        0        0        0        0
 31  CPU_Q_GOLD_PKT                          0        0        0        0

-----------------------------------------------------------------------------
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *10* : *show platform software fed switch punt rates interfaces interface-id* のフィールドの説明

フィールド	説明
Queue Name	キューの名前。
Recv Total	受信されたパケットの合計数。
Recv Rate	1 秒あたりのパケットの受信レート。
Drop Total	破棄されたパケットの総数。
Drop Rate	1秒あたりのパケットのドロップレート。

show platform software ilpower

デバイス上のすべてのPoEポートのインラインパワーの詳細を表示するには、特権EXECモードで **show platform software ilpower** コマンドを使用します。

show platform software ilpower {**details** | **port** {**GigabitEthernet** *interface-number* } | **system** *slot-number* }

構文の説明

details	すべてのインターフェイスのインラインパワーの詳細を表示します。
port	インライン パワー ポートの設定を表示します。
GigabitEthernet *interface-number*	GigabitEthernet インターフェイス番号。値の範囲は 0 ～ 9 です。
system *slot-number*	インライン パワー システムの設定を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが変更されました。キーワード **details** 引数が追加されました。
Cisco IOS XE Denali 16.1.1	このコマンドが追加されました。

例

次に、**show platform software ilpower details** コマンドの出力例を示します。

```
Device# show platform software ilpower details
ILP Port Configuration for interface Gi1/0/1
    Initialization Done:   Yes
    ILP Supported:         Yes
    ILP Enabled:           Yes
    POST:                  Yes
    Detect On:             No
    Powered Device Detected            No
    Powered Device Class Done          No
    Cisco Powered Device:              No
    Power is On:           No
    Power Denied:          No
    Powered Device Type:               Null
    Powerd Device Class:              Null
    Power State:           NULL
    Current State:         NGWC_ILP_DETECTING_S
    Previous State:        NGWC_ILP_SHUT_OFF_S
    Requested Power in milli watts:       0
    Short Circuit Detected:                 0
    Short Circuit Count:            0
```

```
Cisco Powerd Device Detect Count: 0
Spare Pair mode:       0
    IEEE Detect:       Stopped
    IEEE Short:        Stopped
    Link Down:         Stopped
    Voltage sense:            Stopped
Spare Pair Architecture:       1
Signal Pair Power allocation in milli watts: 0
Spare Pair Power On:   0
Powered Device power state:        0
Timer:
    Power Good:        Stopped
    Power Denied:      Stopped
    Cisco Powered Device Detect:   Stopped
```

show platform software memory

指定したスイッチのメモリ情報を表示するには、特権 EXEC モードで **show platform software memory** コマンドを使用します。

show platform software memory [{**chunk** | **database** | **messaging**}] *process slot*

構文の説明

構文の説明

chunk	（任意）指定したプロセスのチャンクメモリ情報を表示します。
database	（任意）指定したプロセスのデータベースメモリ情報を表示します。
messaging	（任意）指定したプロセスのメッセージングメモリ情報を表示します。 表示される情報は、内部デバッグのみを目的としています。

process

設定されているレベル。次のオプションがあります。

- **bt-logger**：Binary-Tracing Logger プロセス。
- **btrace-manager**：Btrace Manager プロセス。
- **chassis-manager**：Chassis Manager プロセス。
- **cli-agent**：CLI Agent プロセス。
- **cmm**：CMM プロセス。
- **dbm**：Database Manager プロセス。
- **dmiauthd**：DMI Authentication Daemon プロセス。
- **emd**：Environmental Monitoring プロセス。
- **fed**：Forwarding Engine Driver プロセス。
- **forwarding-manager**：Forwarding Manager プロセス。
- **geo**：Geo Manager プロセス。
- **gnmi**：GNMI プロセス。
- **host-manager**：Host Manager プロセス。
- **interface-manager**：Interface Manager プロセス。
- **iomd**：Input/Output Module daemon（IOMd）プロセス。
- **ios**：IOS プロセス。
- **iox-manager**：IOx Manager プロセス。
- **license-manager**：License Manager プロセス。
- **logger**：Logging Manager プロセス。
- **mdt-pubd**：Model Defined Telemetry Publisher プロセス。
- **ndbman**：Netconf DataBase Manager プロセス。
- **nesd**：Network Element Synchronizer Daemon プロセス。
- **nginx**：Nginx Webserver プロセス。
- **nif_mgr**：NIF Manager プロセス。
- **platform-mgr**：Platform Manager プロセス。
- **pluggable-services**：Pluggable Services プロセス。
- **replication-mgr**：Replication Manager プロセス。
- **shell-manager**：Shell Manager プロセス。

- **sif**：Stack Interface（SIF）Manager プロセス。
- **smd**：Session Manager プロセス。
- **stack-mgr**：Stack Manager プロセス。
- **syncfd**：SyncmDaemon プロセス。
- **table-manager**：Table Manager サーバ。
- **thread-test**：Multithread Manager プロセス。
- **virt-manager**：Virtualization Manager プロセス。

slot	レベルが設定されているプロセスを実行中のハードウェアスロット。次のオプションがあります。 • *number*：レベルが設定されているハードウェアモジュールの SIP スロット番号。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。 • *SIP-slot / SPA-bay*：SIP スイッチ スロットの数とその SIP の共有ポートアダプタ（SPA）ベイの数。たとえば、スイッチスロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。 • **F0**：Embedded Service Processor スロット 0。 • **FP active**：アクティブな Embedded Service Processor。 • **R0**：スロット 0 のルート プロセッサ。 • **RP active**：アクティブなルート プロセッサ。 • **switch** <*number*> ：指定された番号を持つスイッチ。 • **switch active**：アクティブなスイッチ。 • **switch standby**：スタンバイスイッチ。 • *number*：レベルが設定されているハードウェアモジュールの SIP スロット番号。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。 • *SIP-slot / SPA-bay*：SIP スイッチ スロットの数とその SIP の共有ポートアダプタ（SPA）ベイの数。たとえば、スイッチスロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。 • **F0**：スロット 0 の Embedded Service Processor。 • **FP active**：アクティブな Embedded Service Processor。 • **R0**：スロット 0 のルート プロセッサ。 • **RP active**：アクティブなルート プロセッサ。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

コマンド履歴

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

次に、Cisco Catalyst 3000 シリーズ ESP スロット 0 の Forwarding Manager プロセスについての簡略化した形式（briefキーワード）のメモリ情報を表示する出力例を示します。

```
Device# show platform software memory forwarding-manager switch 1 fp active brief

  module                  allocated     requested     allocs        frees
  ------------------------------------------------------------------------------
  Summary                 5702540       5619788       121888        116716
  AOM object              1920374       1920310       4             0
  AOM links array         880379        880315        4             0
  smc_message             819575        819511        4             0
  AOM update state        640380        640316        4             0
  dpidb-config            208776        203544        351           24
  fman-infra-avl          178016        153680        1521          0
  AOM batch               152373        152309        4             0
  AOM asynchronous conte  128388        128324        4             0
  AOM basic data          124824        124760        5             1
  eventutil               118939        118299        50            10
  AOM tree node           96465         96385         5             0
  AOM tree root           72377         72313         4             0
  acl                     36090         31914         504           243
  fman-infra-ipc          35326         24366         115097        114412
  AOM uplink update node  32386         32322         4             0
  unknown                 30528         23808         424           4
  uipeer                  27232         27152         5             0
  fman-infra-qos          26872         24712         164           29
  cce-class               19427         15411         251           0
  l2 control protocol     15472         12896         325           164
  fman-infra-cce          15272         13576         106           0
  smc_channel             15223         15159         4             0
  unknown                 14208         8736          447           105
  chunk                   12513         12033         33            3
  cce-bind                8496          7552          82            23
  MATM mac entry          8040          5928          544           412
  adj                     7064          6312          157           110
  route-pfx               6116          5412          157           113
  Filter_rules            4912          4896          1             0
  fman-infra-dpidb        4130          2338          112           0
  SMC Buffer              3794          3202          43            6
  urpf-list               3028          2100          85            27
  lookup                  2480          2160          30            10
  MATM mac table          2432          1600          148           96
  cdllib                  1688          1672          1             0
  route-tbl               1600          1264          21            0
  FNF Flowdef             1492          1460          3             1
  acl-ref                 1120          1024          8             2
  cgm-lib                 1120          880           410           395
  pbr_if_cfg              1088          976           205           198
  FNF Monitor             1048          1032          1             0
  pbr_routemap            960           864           18            12
!
!
!
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *11 : show platform software memory brief* のフィールドの説明

フィールド	説明
module	サブモジュールの名前。
allocated	割り当て済みのメモリ（バイト数）。
要求済み	アプリケーションによって要求されたバイト数。
allocs	個別の割り当てイベントの試行回数。
frees	解放イベントの数。

show platform software process list

プラットフォームで実行中のプロセスのリストを表示するには、特権 EXEC モードで **show platform software process list** コマンドを使用します。

show platform software process list switch {*switch-number* | **active** | **standby**} {**0** | **F0** | **R0**} [{**name** *process-name* | **process-id** *process-ID* | **sort memory** | **summary**}]

構文の説明

switch *switch-number*	スイッチに関する情報を表示します。 *switch-number* 引数の有効な値は 0 ～ 9 です。
active	スイッチのアクティブ インスタンスに関する情報を表示します。
standby	スイッチのスタンバイ インスタンスに関する情報を表示します。
0	共有ポート アダプタ（SPA）インターフェイス プロセッサ スロット 0 に関する情報を表示します。
F0	Embedded Service Processor（ESP）スロット 0 に関する情報を表示します。
R0	ルート プロセッサ（RP）スロット 0 に関する情報を表示します。
name *process-name*	（任意）指定されたプロセスに関する情報を表示します。プロセス名を入力します。
process-id *process-ID*	（任意）指定されたプロセス ID に関する情報を表示します。プロセス ID を入力します。
sort	（任意）プロセスに従いソートされた情報を表示します。

memory	（任意）メモリに従いソートされた情報を表示します。
summary	（任意）ホスト デバイスのプロセス メモリのサマリーを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが追加されました。

使用上のガイドライン

Cisco IOS XE Denali 16.3.1 より前は、コマンド出力に表示される「空きメモリ」は基盤となる Linux カーネルから得ていました。使用可能な一部のメモリ チャンクは空きメモリと見なされていなかったため、この値は正確ではありませんでした。

Cisco IOS XE Denali 16.3.1 では、空きメモリは正確に計算されて、コマンド出力の Free Memory フィールドに表示されます。

例

次に、**show platform software process list switch active R0** コマンドの出力例を示します。

```
Switch# show platform software process list switch active R0 summary

Total number of processes: 278
  Running          : 2
  Sleeping         : 276
  Disk sleeping    : 0
  Zombies          : 0
  Stopped          : 0
  Paging           : 0

  Up time          : 8318
  Idle time        : 0
  User time        : 216809
  Kernel time      : 78931

  Virtual memory   : 12933324800
  Pages resident   : 634061
  Major page faults: 2228
  Minor page faults: 3491744

  Architecture     : mips64
  Memory (kB)
    Physical       : 3976852
    Total          : 3976852
    Used           : 2766952
    Free           : 1209900
    Active         : 2141344
    Inactive       : 1589672
    Inact-dirty    : 0
    Inact-clean    : 0
    Dirty          : 4
    AnonPages      : 1306800
    Bounce         : 0
    Cached         : 1984688
    Commit Limit   : 1988424
    Committed As   : 3358528
    High Total     : 0
```

```
  High Free      : 0
  Low Total      : 3976852
  Low Free       : 1209900
  Mapped         : 520528
  NFS Unstable   : 0
  Page Tables    : 17328
  Slab           : 0
  VMmalloc Chunk : 1069542588
  VMmalloc Total : 1069547512
  VMmalloc Used  : 2588
  Writeback      : 0
  HugePages Total: 0
  HugePages Free : 0
  HugePages Rsvd : 0
  HugePage Size  : 2048

Swap (kB)
  Total          : 0
  Used           : 0
  Free           : 0
  Cached         : 0

Buffers (kB)     : 439528

Load Average
  1-Min          : 1.13
  5-Min          : 1.18
  15-Min         : 0.92
```

次に、**show platform software process list switch active R0** コマンドの出力例を示します。

```
Device# show platform software process list switch active R0
Name                         Pid    PPid  Group Id  Status    Priority  Size
-------------------------------------------------------------------------------
systemd                        1       0         1  S               20  7892
kthreadd                       2       0         0  S               20  0
ksoftirqd/0                    3       2         0  S               20  0
kworker/0:0H                   5       2         0  S                0  0
rcu_sched                      7       2         0  S               20  0
rcu_bh                         8       2         0  S               20  0
migration/0                    9       2         0  S       4294967196  0
migration/1                   10       2         0  S       4294967196  0
ksoftirqd/1                   11       2         0  S               20  0
kworker/1:0H                  13       2         0  S                0  0
migration/2                   14       2         0  S       4294967196  0
ksoftirqd/2                   15       2         0  S               20  0
kworker/2:0H                  17       2         0  S                0  0
systemd-journal              221       1       221  S               20  4460
kworker/1:3                  246       2         0  S               20  0
systemd-udevd                253       1       253  S               20  5648
kvm-irqfd-clean              617       2         0  S                0  0
scsi_eh_6                    620       2         0  S               20  0
scsi_tmf_6                   621       2         0  S                0  0
usb-storage                  622       2         0  S               20  0
scsi_eh_7                    625       2         0  S               20  0
scsi_tmf_7                   626       2         0  S                0  0
usb-storage                  627       2         0  S               20  0
kworker/7:1                  630       2         0  S               20  0
bioset                       631       2         0  S                0  0
kworker/3:1H                 648       2         0  S                0  0
```

```
kworker/0:1H             667       2         0  S                0  0
kworker/1:1H             668       2         0  S                0  0
bioset                   669       2         0  S                0  0
kworker/6:2              698       2         0  S               20  0
kworker/2:2              699       2         0  S               20  0
kworker/2:1H             703       2         0  S                0  0
kworker/7:1H             748       2         0  S                0  0
kworker/5:1H             749       2         0  S                0  0
kworker/6:1H             754       2         0  S                0  0
kworker/7:2              779       2         0  S               20  0
auditd                   838       1       838  S               16  2564
.
.
.
```

次の表で、この出力で表示される重要なフィールドについて説明します。

表 *12 : show platform software process list* のフィールドの説明

フィールド	説明
Name	プロセスに関連付けられているコマンド名が表示されます。同じプロセスのスレッドでも、スレッドごとにコマンドの値が異なる場合があります。
Pid	プロセスを識別して追跡するためにオペレーティングシステムで使用されるプロセスIDが表示されます。
PPID	親プロセスのプロセス ID が表示されます。
Group Id	グループ ID が表示されます。
Status（ステータス）	人間が判読可能な形式でプロセスのステータスが表示されます。
プライオリティ	無効にされたスケジューリングの優先順位が表示されます。
サイズ	Cisco IOS XE Gibraltar 16.10.1 よりも前： 仮想メモリのサイズが表示されます。 Cisco IOS XE Gibraltar 16.10.1 以降： RAM でそのプロセスに割り当てられているメモリ量を示す常駐セットサイズ（RSS）が表示されます。

show platform software process memory

各システムプロセスで使用されているメモリの量を表示するには、特権 EXEC モードで **show platform software process memory** コマンドを使用します。

show platform process memory
switch {*switch-number* | **active** | **standby**} {**0** | **F0** | **FP** | **R0**} {**all** [**sorted** | **virtual** [**sorted**]] | **name** *process-name* {**maps** | **smaps** [**summary**] } | **process-id** *process-id* {**maps** | **smaps** [**summary**] } }

構文の説明

switch *switch-number*	スイッチに関する情報を表示します。スイッチ番号を入力します。
active	デバイスのアクティブインスタンスを指定します。
standby	デバイスのスタンバイインスタンスを指定します。
0	共有ポートアダプタ（SPA）インターフェイス プロセッサ スロット 0 を指定します。
F0	Embedded Service Processor（ESP）スロット 0 を指定します。
FP	Embedded Service Processor（ESP）を指定します。
R0	ルート プロセッサ（RP）スロット 0 を指定します。
all	すべてのプロセスを一覧表示します。
sorted	（任意）常駐セットサイズ（RSS）に基づいて出力をソートします。
virtual	（任意）仮想メモリを指定します。
name*process-name*	プロセス名を指定します。
maps	プロセスのメモリマップを指定します。
smaps summary	プロセスの smaps の要約を指定します。
process-id*process-id*	プロセス ID を指定します。

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。

コマンド モード

特権 EXEC（#）

次に例を示します。

次に、**show platform software process memory active R0 all** コマンドの出力例を示します。

```
Device# show platform software process memory switch active R0 all

   Pid       RSS       PSS      Heap    Shared   Private              Name
-------------------------------------------------------------------------
     1      4876      3229      1064      1808      3068           systemd
   118      3184      1327       132      2352       832   systemd-journal
   159      3008      1191       396      1996      1012     systemd-udevd
   407      3192      1262       132      2196       996       dbus-daemon
  3406      4772      3064       264      1940      2832          virtlogd
  3411      5712      3474      2964      2344      3368       droputil.sh
  3416      2588       358       132      2336       252       libvirtd.sh
  3420      5708      3484      2976      2308      3400      reflector.sh
  3424      1804       263       132      1632       172            xinetd
  3425       964       118       132       872        92             sleep
  3434      3060       844       528      2304       756            oom.sh
  3442      2068       606       132      1604       464          rpcbind
  3485      2380       845       132      1636       744        rpc.statd
  3486      1632       338       132      1348       284   boothelper_evt.
  3493      1136       156       132      1004       132     inotifywait
  3504      2048       753       132      1372       676       rpc.mountd
  3584      2868       620        36      2384       484            rotee
  3649      1032       116       132       944        88            sleep
  3705      2784       613        36      2296       488            rotee
  3718      2856       610        36      2376       480            rotee
  3759      1292       184       132      1136       156     inotifywait
  3787      4256      2040      1640      2300      1956         iptbl.sh
  3894      2948       637        36      2460       488            rotee
  4017      1380       175       132      1236       144     inotifywait
  4866      1820       287       132      1624       196            xinetd
  5887      1692       257       132      1508       184            xinetd
  5891      7248      4984      4584      2348      4900   rollback_timer.
  5893      1764       257       132      1588       176            xinetd
  6031      2804       601        36      2332       472            rotee
  6037      1228       163       132      1092       136     inotifywait
  6077      4736      3389      2992      1368      3368          psvp.sh
  6115      1620       476        36      1152       468            rotee
  6122       624       149       132       480       144     inotifywait
  6127      5440      4077      3680      1384      4056           pvp.sh
  6165      1736       592        36      1152       584            rotee
  6245       624       149       132       480       144     inotifywait
  6353      2592      1260       924      1352      1240          pman.sh
  6470      1632       488        36      1152       480            rotee
  6499      2588      1262       924      1348      1240          pman.sh
  6666      1640       496        36      1152       488            rotee
  6718      2584      1258       800      1348      1236          pman.sh
  6736      8360      7020      6640      1360      7000   auto_upgrade_cl
  6909      1636       492        36      1152       484            rotee
  6955      2588      1262       928      1348      1240          pman.sh
  7029      2196       679        40      1552       644   auto_upgrade_se
  7149      1636       492        36      1152       484            rotee
  7224     13200      4595        48      9368      3832       bt_logger
  7295      2588      1262       800      1348      1240          pman.sh
.
.
.
```

次の表で、この出力で表示される重要なフィールドについて説明します。

表 *13 : show platform software process memory* のフィールドの説明

フィールド	説明
PID	プロセスを識別して追跡するためにオペレーティングシステムで使用されるプロセスIDが表示されます。
RSS	RAMでそのプロセスに割り当てられているメモリ量を示す常駐セットサイズ（キロバイト（KB））が表示されます。
PSS	プロセスの比例セットサイズが表示されます。これは、メモリ内のページの数であり、各ページはそれを共有するプロセスの数で除算されます。
Heap	ユーザが割り当てたすべてのメモリの場所が表示されます。
Shared	共有クリーン＋共有ダーティ
プライベート	プライベートクリーン+プライベートダーティ
Name	プロセスに関連付けられているコマンド名が表示されます。同じプロセスのスレッドでも、スレッドごとにコマンドの値が異なる場合があります。

show platform software process slot switch

プラットフォーム ソフトウェア プロセスのスイッチ情報を表示するには、特権 EXEC モードで **show platform software process slot switch** コマンドを使用します。

show platform software process slot switch {*switch-number* | **active** | **standby**} {**0** | **F0** | **R0**} **monitor** [{**cycles** *no-of-times* [{**interval** *delay*[{**lines** *number*}]}]}]

構文の説明

switch-number	スイッチ番号。
active	アクティブ インスタンスを指定します。
standby	スタンバイ インスタンスを指定します。
0	共有ポート アダプタ（SPA）インターフェイスプロセッサ スロット0を指定します。

F0	Embedded Service Processor（ESP）スロット 0 を指定します。
R0	ルートプロセッサ（RP）スロット 0 を指定します。
monitor	実行中のプロセスをモニタします。
cycles *no-of-tmes*	（任意）monitor コマンドを実行する回数を設定します。有効な値は、1 ～ 4294967295 です。デフォルトは 5 です。
interval *delay*	（任意）それぞれの遅延を設定します。有効値は 0 ～ 300 です。デフォルトは 3 です。
lines *number*	（任意）表示される出力の行数を設定します。有効値は 0 ～ 512 です。デフォルトは 0 です。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

show platform software process slot switch コマンドと **show processes cpu platform monitor location** コマンドの出力に、Linux **top** コマンドの出力が表示されます。これらのコマンドの出力には、**top** コマンドで表示される「空きメモリ」と「使用メモリ」が表示されます。これらのコマンドによって「空きメモリ」と「使用メモリ」に表示される値は、その他のプラットフォーム メモリ関連 CLI の出力で表示される値とは一致しません。

例

次に、**show platform software process slot switch active R0 monitor** コマンドの出力例を示します。

```
Switch# show platform software process slot switch active R0 monitor

top - 00:01:52 up 1 day, 11:20,  0 users,  load average: 0.50, 0.68, 0.83
Tasks: 311 total,   2 running, 309 sleeping,   0 stopped,   0 zombie
Cpu(s):  7.4%us,  3.3%sy,  0.0%ni, 89.2%id,  0.0%wa,  0.0%hi,  0.1%si,  0.0%st
Mem:   3976844k total,  3955036k used,    21808k free,   419312k buffers
Swap:        0k total,        0k used,        0k free,  1946764k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 5693 root      20   0  3448 1368  912 R    7  0.0   0:00.07 top
17546 root      20   0 2044m 244m  79m S    7  6.3 186:49.08 fed main event
18662 root      20   0 1806m 678m 263m S    5 17.5 215:32.38 linux_iosd-imag
30276 root      20   0  171m  42m  33m S    5  1.1 125:06.77 repm
17835 root      20   0  935m  74m  63m S    4  1.9  82:28.31 sif_mgr
18534 root      20   0  182m 150m  10m S    2  3.9   8:12.08 smand
```

```
  1 root      20   0  8440 4740 2184 S    0  0.1   0:09.52 systemd
  2 root      20   0     0    0    0 S    0  0.0   0:00.00 kthreadd
  3 root      20   0     0    0    0 S    0  0.0   0:02.86 ksoftirqd/0
  5 root       0 -20     0    0    0 S    0  0.0   0:00.00 kworker/0:0H
  7 root      RT   0     0    0    0 S    0  0.0   0:01.44 migration/0
  8 root      20   0     0    0    0 S    0  0.0   0:00.00 rcu_bh
  9 root      20   0     0    0    0 S    0  0.0   0:23.08 rcu_sched
 10 root      20   0     0    0    0 S    0  0.0   0:58.04 rcuc/0
 11 root      20   0     0    0    0 S    0  0.0  21:35.60 rcuc/1
 12 root      RT   0     0    0    0 S    0  0.0   0:01.33 migration/1
```

関連コマンド

コマンド	説明
show processes cpu platform monitor location	IOS XE プロセスの CPU 使用率に関する情報を表示します。

show platform software status control-processor

プラットフォーム ソフトウェアの制御プロセッサのステータスを表示するには、特権 EXEC モードで **show platform software status control-processor** コマンドを使用します。

show platform software status control-processor [{**brief**}]

構文の説明

brief	（任意）プラットフォームの制御プロセッサのステータスのサマリーを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

Cisco IOS XE Denali 16.3.1 より前は、コマンド出力に表示される「空きメモリ」は基盤となる Linux カーネルから得ていました。使用可能な一部のメモリ チャンクは空きメモリと見なされていなかったため、この値は正確ではありませんでした。

Cisco IOS XE Denali 16.3.1 では、空きメモリは正確に計算されて、コマンド出力の Free Memory フィールドに表示されます。

例

次に、**show platform memory software status control-processor** コマンドの出力例を示します。

```
Switch# show platform software status control-processor

2-RP0: online, statistics updated 7 seconds ago
Load Average: healthy
  1-Min: 1.00, status: healthy, under 5.00
  5-Min: 1.21, status: healthy, under 5.00
```

```
  15-Min: 0.90, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 2766284 (70%), status: healthy
  Free: 1210568 (30%)
  Committed: 3358008 (84%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  4.40, System:  1.70, Nice:  0.00, Idle: 93.80
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  3.80, System:  1.20, Nice:  0.00, Idle: 94.90
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  7.00, System:  1.10, Nice:  0.00, Idle: 91.89
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  4.49, System:  0.69, Nice:  0.00, Idle: 94.80
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00

3-RP0: unknown, statistics updated 2 seconds ago
Load Average: healthy
  1-Min: 0.24, status: healthy, under 5.00
  5-Min: 0.27, status: healthy, under 5.00
  15-Min: 0.32, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 2706768 (68%), status: healthy
  Free: 1270084 (32%)
  Committed: 3299332 (83%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  4.50, System:  1.20, Nice:  0.00, Idle: 94.20
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  5.20, System:  0.50, Nice:  0.00, Idle: 94.29
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  3.60, System:  0.70, Nice:  0.00, Idle: 95.69
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  3.00, System:  0.60, Nice:  0.00, Idle: 96.39
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00

4-RP0: unknown, statistics updated 2 seconds ago
Load Average: healthy
  1-Min: 0.21, status: healthy, under 5.00
  5-Min: 0.24, status: healthy, under 5.00
  15-Min: 0.24, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 1452404 (37%), status: healthy
  Free: 2524448 (63%)
  Committed: 1675120 (42%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  2.30, System:  0.40, Nice:  0.00, Idle: 97.30
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  4.19, System:  0.69, Nice:  0.00, Idle: 95.10
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  4.79, System:  0.79, Nice:  0.00, Idle: 94.40
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
```

```
CPU3: CPU Utilization (percentage of time spent)
  User:  2.10, System:  0.40, Nice:  0.00, Idle: 97.50
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00

9-RP0: unknown, statistics updated 4 seconds ago
Load Average: healthy
  1-Min: 0.20, status: healthy, under 5.00
  5-Min: 0.35, status: healthy, under 5.00
  15-Min: 0.35, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 1451328 (36%), status: healthy
  Free: 2525524 (64%)
  Committed: 1675932 (42%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  1.90, System:  0.50, Nice:  0.00, Idle: 97.60
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  4.39, System:  0.19, Nice:  0.00, Idle: 95.40
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  5.70, System:  1.00, Nice:  0.00, Idle: 93.30
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  1.30, System:  0.60, Nice:  0.00, Idle: 98.00
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
```

次に、**show platform memory software status control-processor brief** コマンドの出力例を示します。

```
Switch# show platform software status control-processor brief

Load Average
 Slot  Status  1-Min  5-Min 15-Min
2-RP0 Healthy   1.10   1.21   0.91
3-RP0 Healthy   0.23   0.27   0.31
4-RP0 Healthy   0.11   0.21   0.22
9-RP0 Healthy   0.10   0.30   0.34

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
2-RP0 Healthy  3976852  2766956 (70%)  1209896 (30%)   3358352 (84%)
3-RP0 Healthy  3976852  2706824 (68%)  1270028 (32%)   3299276 (83%)
4-RP0 Healthy  3976852  1451888 (37%)  2524964 (63%)   1675076 (42%)
9-RP0 Healthy  3976852  1451580 (37%)  2525272 (63%)   1675952 (42%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
2-RP0    0   4.10   2.00   0.00  93.80   0.00   0.10   0.00
         1   4.60   1.00   0.00  94.30   0.00   0.10   0.00
         2   6.50   1.10   0.00  92.40   0.00   0.00   0.00
         3   5.59   1.19   0.00  93.20   0.00   0.00   0.00
3-RP0    0   2.80   1.20   0.00  95.90   0.00   0.10   0.00
         1   4.49   1.29   0.00  94.20   0.00   0.00   0.00
         2   5.30   1.60   0.00  93.10   0.00   0.00   0.00
         3   5.80   1.20   0.00  93.00   0.00   0.00   0.00
4-RP0    0   1.30   0.80   0.00  97.89   0.00   0.00   0.00
         1   1.30   0.20   0.00  98.50   0.00   0.00   0.00
         2   5.60   0.80   0.00  93.59   0.00   0.00   0.00
         3   5.09   0.19   0.00  94.70   0.00   0.00   0.00
9-RP0    0   3.99   0.69   0.00  95.30   0.00   0.00   0.00
```

```
1   2.60   0.70   0.00  96.70   0.00   0.00   0.00
2   4.49   0.89   0.00  94.60   0.00   0.00   0.00
3   2.60   0.20   0.00  97.20   0.00   0.00   0.00
```

show platform software thread list

プラットフォームのスレッドのリストを表示するには、特権 EXEC モードで **show platform software thread list** コマンドを使用します。

show platform software thread list switch {*switch-number* | **active** | **standby**} {**0** | **F0** | **FP active** | **R0**} **pname** {**cdman** | **vidman** | **all**} **tname** {**main** | **pktio** | **rt** | **all**}

構文の説明

switch *switch-number*	スイッチに関する情報を表示します。スイッチ番号を入力します。
active	デバイスのアクティブインスタンスを指定します。
standby	デバイスのスタンバイインスタンスを指定します。
0	共有ポートアダプタ（SPA）インターフェイス プロセッサ スロット 0 を指定します。
F0	Embedded Service Processor（ESP）スロット 0 を指定します。
FP active	Embedded Service Processor（ESP）のアクティブインスタンスを指定します。
R0	ルート プロセッサ（RP）スロット 0 を指定します。
pname	プロセス名を指定します。指定できる値は **cdman**、**vidman**、および **all** です。
tname	スレッド名を指定します。指定できる値は **main**、**pktio**、**rt**、および **all** です。

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。

コマンド モード

特権 EXEC（#）

次に例を示します。

次に、**show platform software thread list switch active R0 pname cdman tname all** コマンドの出力例を示します。

```
Device# show platform software thread list switch active R0 pname cdman tname all

Name           Tid    PPid  Group Id  Core    Vcswch   Nvcswch  Status    Priority
  TIME+  Size
-------------------------------------------------------------------------------------------------
cdman         8407    7295      8407     1         0         0  S               20
  12309  36976
```

次の表で、この出力で表示される重要なフィールドについて説明します。

表 *14 : show platform software thread list* のフィールドの説明

フィールド	説明
Name	プロセスに関連付けられているコマンド名が表示されます。同じプロセスのスレッドでも、スレッドごとにコマンドの値が異なる場合があります。
Tid	プロセス ID が表示されます。
PPid	親プロセスのプロセス ID が表示されます。
Group Id	グループ ID が表示されます。
コア	プロセッサ情報が表示されます。
Vcswch	自発的なコンテキストスイッチの回数が表示されます。
Nvcswch	非自発的なコンテキストスイッチの回数が表示されます。
Status（ステータス）	人間が判読可能な形式でプロセスのステータスが表示されます。
プライオリティ	無効にされたスケジューリングの優先順位が表示されます。
TIME+	プロセスが開始されてからの経過時間が表示されます。
サイズ	RAM でそのプロセスに割り当てられているメモリ量を示す常駐セットサイズ（キロバイト（KB））が表示されます。

show processes cpu platform

IOS XE プロセスの CPU 使用率に関する情報を表示するには、特権 EXEC モードで **show processes cpu platform** コマンドを使用します。

show processes cpu platform [[**sorted** [**1min** | **5min** | **5sec**]] **location switch** {*switch-number* | **active** | **standby** } { **F0** | **FP active** | **R0** | **RP active** }]

構文の説明

sorted	（任意）プラットフォームの CPU 使用率に基づいてソートした出力を表示します。
1min	（任意）1 分間隔でソートします。
5min	（任意）5 分間隔でソートします。
5sec	（任意）5 秒間隔でソートします。
location	Field Replaceable Unit（FRU）の場所を指定します。
switch *switch-number*	スイッチに関する情報を表示します。スイッチ番号を入力します。
active	デバイスのアクティブインスタンスを指定します。
standby	デバイスのスタンバイインスタンスを指定します。
F0	Embedded Service Processor（ESP）スロット 0 を指定します。
FP active	Embedded Service Processor（ESP）のアクティブインスタンスを指定します。
R0	ルート プロセッサ（RP）スロット 0 を指定します。
RP active	ルートプロセッサ（RP）のアクティブインスタンスを指定します。

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。

コマンド モード

特権 EXEC（#）

次に例を示します。

次に、**show processes cpu platform** コマンドの出力例を示します。

```
Device# show processes cpu platform

CPU utilization for five seconds:  1%, one minute:  3%, five minutes:  2%
Core 0: CPU utilization for five seconds:  2%, one minute:  2%, five minutes:  2%
```

```
Core 1: CPU utilization for five seconds:  2%, one minute:  1%, five minutes:  1%
Core 2: CPU utilization for five seconds:  3%, one minute:  1%, five minutes:  1%
Core 3: CPU utilization for five seconds:  2%, one minute:  5%, five minutes:  2%
   Pid    PPid    5Sec    1Min    5Min  Status        Size  Name
------------------------------------------------------------------------------
     1       0      0%      0%      0%  S             4876  systemd
     2       0      0%      0%      0%  S                0  kthreadd
     3       2      0%      0%      0%  S                0  ksoftirqd/0
     5       2      0%      0%      0%  S                0  kworker/0:0H
     7       2      0%      0%      0%  S                0  rcu_sched
     8       2      0%      0%      0%  S                0  rcu_bh
     9       2      0%      0%      0%  S                0  migration/0
    10       2      0%      0%      0%  S                0  watchdog/0
    11       2      0%      0%      0%  S                0  watchdog/1
    12       2      0%      0%      0%  S                0  migration/1
    13       2      0%      0%      0%  S                0  ksoftirqd/1
    15       2      0%      0%      0%  S                0  kworker/1:0H
    16       2      0%      0%      0%  S                0  watchdog/2
    17       2      0%      0%      0%  S                0  migration/2
    18       2      0%      0%      0%  S                0  ksoftirqd/2
    20       2      0%      0%      0%  S                0  kworker/2:0H
    21       2      0%      0%      0%  S                0  watchdog/3
    22       2      0%      0%      0%  S                0  migration/3
    23       2      0%      0%      0%  S                0  ksoftirqd/3
    24       2      0%      0%      0%  S                0  kworker/3:0
    25       2      0%      0%      0%  S                0  kworker/3:0H
    26       2      0%      0%      0%  S                0  kdevtmpfs
    27       2      0%      0%      0%  S                0  netns
    28       2      0%      0%      0%  S                0  perf
    29       2      0%      0%      0%  S                0  khungtaskd
    30       2      0%      0%      0%  S                0  writeback
    31       2      7%      8%      8%  S                0  ksmd
    32       2      0%      0%      0%  S                0  khugepaged
    33       2      0%      0%      0%  S                0  crypto
    34       2      0%      0%      0%  S                0  bioset
    35       2      0%      0%      0%  S                0  kblockd
    36       2      0%      0%      0%  S                0  ata_sff
    37       2      0%      0%      0%  S                0  rpciod
    63       2      0%      0%      0%  S                0  kswapd0
    64       2      0%      0%      0%  S                0  vmstat
    65       2      0%      0%      0%  S                0  fsnotify_mark
.
.
.
```

次に、 **show processes cpu platform sorted 5min location switch 5 R0**

```
Device# show processes cpu platform sorted 5min location switch 5 R0

CPU utilization for five seconds:  0%, one minute:  0%, five minutes:  0%
Core 0: CPU utilization for five seconds:  1%, one minute:  1%, five minutes:  1%
Core 1: CPU utilization for five seconds:  1%, one minute:  1%, five minutes:  1%
Core 2: CPU utilization for five seconds:  1%, one minute:  1%, five minutes:  1%
Core 3: CPU utilization for five seconds:  2%, one minute:  2%, five minutes:  1%
Core 4: CPU utilization for five seconds:  0%, one minute:  0%, five minutes:  0%
Core 5: CPU utilization for five seconds:  0%, one minute:  0%, five minutes:  0%
Core 6: CPU utilization for five seconds:  0%, one minute:  0%, five minutes:  0%
Core 7: CPU utilization for five seconds:  0%, one minute:  0%, five minutes:  0%
   Pid    PPid    5Sec    1Min    5Min  Status        Size  Name
------------------------------------------------------------------------------
 16358   15516      4%      4%      4%  S           221376  fed main event
 14062   12756      1%      1%      1%  S            52140  sif_mgr
 32105    8618      0%      0%      0%  S              260  inotifywait
 31396   31393      0%      0%      0%  S            36516  python2.7
 31393   31271      0%      0%      0%  S             2744  rdope.sh
```

```
 31319       1      0%      0%      0%  S             2648  rotee
 31271       1      0%      0%      0%  S             3852  pman.sh
 29671       2      0%      0%      0%  S                0  kworker/u16:0
 29341   29329      0%      0%      0%  S             1780  sntp
 29329       1      0%      0%      0%  S             2788  stack_sntp.sh
.
.
.
```

次に、**show processes cpu platform location switch 7 R0** コマンドの出力例を示します。

```
Device# show processes cpu platform location switch 7 R0

CPU utilization for five seconds:  3%, one minute:  3%, five minutes:  3%
Core 0: CPU utilization for five seconds:  1%, one minute:  5%, five minutes:  5%
Core 1: CPU utilization for five seconds:  1%, one minute: 11%, five minutes:  5%
Core 2: CPU utilization for five seconds: 22%, one minute:  7%, five minutes:  6%
Core 3: CPU utilization for five seconds:  5%, one minute:  6%, five minutes:  6%
Core 4: CPU utilization for five seconds:  0%, one minute:  0%, five minutes:  0%
Core 5: CPU utilization for five seconds:  0%, one minute:  0%, five minutes:  0%
Core 6: CPU utilization for five seconds:  0%, one minute:  0%, five minutes:  0%
Core 7: CPU utilization for five seconds:  0%, one minute:  0%, five minutes:  6%
   Pid    PPid    5Sec    1Min    5Min  Status        Size  Name
------------------------------------------------------------------------------
     1       0      0%      0%      0%  S             8044  systemd
     2       0      0%      0%      0%  S                0  kthreadd
.
.
.
```

show processes cpu platform history

システムのCPU使用率の履歴に関する情報を表示するには、**show processes cpu platform history** コマンドを使用します。

show processes cpu platform history [**1min** | **5min** | **5sec** | **60min**] **location switch** { *switch-number* | **active** | **standby** } { **0** | **F0** | **FP active** | **R0** }

1min	（任意）1 分間隔の CPU 使用率の履歴を表示します。
5min	（任意）5 分間隔の CPU 使用率の履歴を表示します。
5sec	（任意）5 秒間隔の CPU 使用率の履歴を表示します。
60min	（任意）60 分間隔の CPU 使用率の履歴を表示します。
location	Field Replaceable Unit（FRU）の場所を指定します。
switch *switch-number*	スイッチに関する情報を表示します。スイッチ番号を入力します。

active	デバイスのアクティブインスタンスを指定します。
standby	デバイスのスタンバイインスタンスを指定します。
0	共有ポートアダプタ（SPA）インターフェイス プロセッサ スロット 0 を指定します。
F0	Embedded Service Processor（ESP）スロット 0 を指定します。
FP active	Embedded Service Processor（ESP）のアクティブインスタンスを指定します。
R0	ルート プロセッサ（RP）スロット 0 を指定します。

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。

コマンド モード

特権 EXEC（#）

次に例を示します。

次に、**show processes cpu platform** コマンドの出力例を示します。

```
Device# show processes cpu platform

CPU utilization for five seconds:  1%, one minute:  3%, five minutes:  2%
Core 0: CPU utilization for five seconds:  2%, one minute:  2%, five minutes:  2%
Core 1: CPU utilization for five seconds:  2%, one minute:  1%, five minutes:  1%
Core 2: CPU utilization for five seconds:  3%, one minute:  1%, five minutes:  1%
Core 3: CPU utilization for five seconds:  2%, one minute:  5%, five minutes:  2%
   Pid    PPid    5Sec    1Min    5Min  Status        Size  Name
--------------------------------------------------------------------------------
     1       0      0%      0%      0%  S             4876  systemd
     2       0      0%      0%      0%  S                0  kthreadd
     3       2      0%      0%      0%  S                0  ksoftirqd/0
     5       2      0%      0%      0%  S                0  kworker/0:0H
     7       2      0%      0%      0%  S                0  rcu_sched
     8       2      0%      0%      0%  S                0  rcu_bh
     9       2      0%      0%      0%  S                0  migration/0
    10       2      0%      0%      0%  S                0  watchdog/0
    11       2      0%      0%      0%  S                0  watchdog/1
    12       2      0%      0%      0%  S                0  migration/1
    13       2      0%      0%      0%  S                0  ksoftirqd/1
    15       2      0%      0%      0%  S                0  kworker/1:0H
    16       2      0%      0%      0%  S                0  watchdog/2
    17       2      0%      0%      0%  S                0  migration/2
    18       2      0%      0%      0%  S                0  ksoftirqd/2
    20       2      0%      0%      0%  S                0  kworker/2:0H
    21       2      0%      0%      0%  S                0  watchdog/3
    22       2      0%      0%      0%  S                0  migration/3
```

```
    23       2       0%      0%      0%  S                0  ksoftirqd/3
    24       2       0%      0%      0%  S                0  kworker/3:0
    25       2       0%      0%      0%  S                0  kworker/3:0H
    26       2       0%      0%      0%  S                0  kdevtmpfs
    27       2       0%      0%      0%  S                0  netns
    28       2       0%      0%      0%  S                0  perf
    29       2       0%      0%      0%  S                0  khungtaskd
    30       2       0%      0%      0%  S                0  writeback
    31       2       7%      8%      8%  S                0  ksmd
    32       2       0%      0%      0%  S                0  khugepaged
    33       2       0%      0%      0%  S                0  crypto
    34       2       0%      0%      0%  S                0  bioset
    35       2       0%      0%      0%  S                0  kblockd
    36       2       0%      0%      0%  S                0  ata_sff
    37       2       0%      0%      0%  S                0  rpciod
    63       2       0%      0%      0%  S                0  kswapd0
    64       2       0%      0%      0%  S                0  vmstat
    65       2       0%      0%      0%  S                0  fsnotify_mark
.
.
.
```

次に、**show processes cpu platform history 5sec** コマンドの出力例を示します。

```
Device# show processes cpu platform history 5sec

5 seconds ago, CPU utilization: 0%
10 seconds ago, CPU utilization: 0%
15 seconds ago, CPU utilization: 0%
20 seconds ago, CPU utilization: 0%
25 seconds ago, CPU utilization: 0%
30 seconds ago, CPU utilization: 0%
35 seconds ago, CPU utilization: 0%
40 seconds ago, CPU utilization: 0%
45 seconds ago, CPU utilization: 0%
50 seconds ago, CPU utilization: 0%
55 seconds ago, CPU utilization: 0%
60 seconds ago, CPU utilization: 0%
65 seconds ago, CPU utilization: 0%
70 seconds ago, CPU utilization: 0%
75 seconds ago, CPU utilization: 0%
80 seconds ago, CPU utilization: 0%
85 seconds ago, CPU utilization: 0%
90 seconds ago, CPU utilization: 0%
95 seconds ago, CPU utilization: 0%
100 seconds ago, CPU utilization: 0%
105 seconds ago, CPU utilization: 0%
110 seconds ago, CPU utilization: 0%
115 seconds ago, CPU utilization: 0%
120 seconds ago, CPU utilization: 0%
125 seconds ago, CPU utilization: 0%
130 seconds ago, CPU utilization: 0%
135 seconds ago, CPU utilization: 0%
140 seconds ago, CPU utilization: 0%
145 seconds ago, CPU utilization: 1%
150 seconds ago, CPU utilization: 0%
155 seconds ago, CPU utilization: 0%
160 seconds ago, CPU utilization: 0%
165 seconds ago, CPU utilization: 0%
170 seconds ago, CPU utilization: 0%
175 seconds ago, CPU utilization: 0%
180 seconds ago, CPU utilization: 0%
185 seconds ago, CPU utilization: 0%
190 seconds ago, CPU utilization: 0%
195 seconds ago, CPU utilization: 0%
```

```
200 seconds ago, CPU utilization: 0%
205 seconds ago, CPU utilization: 0%
210 seconds ago, CPU utilization: 0%
215 seconds ago, CPU utilization: 0%
220 seconds ago, CPU utilization: 0%
225 seconds ago, CPU utilization: 0%
230 seconds ago, CPU utilization: 0%
235 seconds ago, CPU utilization: 0%
240 seconds ago, CPU utilization: 0%
245 seconds ago, CPU utilization: 0%
250 seconds ago, CPU utilization: 0%
.
.
.
```

show processes cpu platform monitor

IOS XE プロセスの CPU 使用率に関する情報を表示するには、特権 EXEC モードで **show processes cpu platform monitor** コマンドを使用します。

show processes cpu platform monitor location switch {*switch-number* | **active** | **standby**} {**0** | **F0** | **R0**}

構文の説明

location	Field Replaceable Unit（FRU）の場所に関する情報を表示します。
switch	スイッチを指定します。
switch-number	スイッチ番号。
active	アクティブ インスタンスを指定します。
standby	スタンバイ インスタンスを指定します。
0	共有ポート アダプタ（SPA）インターフェイス プロセッサ スロット 0 を指定します。
F0	Embedded Service Processor（ESP）スロット 0 を指定します。
R0	ルート プロセッサ（RP）スロット 0 を指定します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

show platform software process slot switch コマンドと **show processes cpu platform monitor location** コマンドの出力に、Linux **top** コマンドの出力が表示されます。これらのコマンドの出力には、**top** コマンドで表示される「空きメモリ」と「使用メモリ」が表示されます。これら

のコマンドによって「空きメモリ」と「使用メモリ」に表示される値は、その他のプラットフォーム メモリ関連 CLI の出力で表示される値とは一致しません。

例

次に、**show processes cpu monitor location switch active R0** コマンドの出力例を示します。

```
Switch# show processes cpu platform monitor location switch active R0

top - 00:04:21 up 1 day, 11:22,  0 users,  load average: 0.42, 0.60, 0.78
Tasks: 312 total,   4 running, 308 sleeping,   0 stopped,   0 zombie
Cpu(s):  7.4%us,  3.3%sy,  0.0%ni, 89.2%id,  0.0%wa,  0.0%hi,  0.1%si,  0.0%st
Mem:   3976844k total,  3956928k used,    19916k free,   419312k buffers
Swap:        0k total,        0k used,        0k free,  1947036k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 6294 root      20   0  3448 1368  912 R    9  0.0   0:00.07 top
17546 root      20   0 2044m 244m  79m S    7  6.3 187:02.07 fed main event
30276 root      20   0  171m  42m  33m S    7  1.1 125:15.54 repm
   16 root      20   0     0    0    0 S    5  0.0  22:07.92 rcuc/2
   21 root      20   0     0    0    0 R    5  0.0  22:13.24 rcuc/3
18662 root      20   0 1806m 678m 263m R    5 17.5 215:47.59 linux_iosd-imag
   11 root      20   0     0    0    0 S    4  0.0  21:37.41 rcuc/1
10333 root      20   0  6420 3916 1492 S    4  0.1   4:47.03 btrace_rotate.s
   10 root      20   0     0    0    0 S    2  0.0   0:58.13 rcuc/0
 6304 root      20   0   776   12    0 R    2  0.0   0:00.01 ls
17835 root      20   0  935m  74m  63m S    2  1.9  82:34.07 sif_mgr
    1 root      20   0  8440 4740 2184 S    0  0.1   0:09.52 systemd
    2 root      20   0     0    0    0 S    0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S    0  0.0   0:02.86 ksoftirqd/0
    5 root       0 -20     0    0    0 S    0  0.0   0:00.00 kworker/0:0H
    7 root      RT   0     0    0    0 S    0  0.0   0:01.44 migration/0
```

関連コマンド

コマンド	説明
show platform software process slot switch	プラットフォーム ソフトウェア プロセスのスイッチ情報を表示します。

show processes memory platform

各 Cisco IOS XE プロセスのメモリ使用率を表示するには、特権 EXEC モードで **show processes memory platform** コマンドを使用します。

show processes memory platform [[**detailed** { **name** *process-name* | **process-id** *process-ID* } [**location** | **maps** [**location**] | **smaps** [**location**]] | **location** | **sorted** [**location**]] **switch** { *switch-number* | **active** | **standby** } { **0** | **F0** | **R0** } | **accounting**]

構文の説明

accounting	（任意）各 Cisco IOS XE プロセスの上位のメモリアロケータを表示します。
detailed	（任意）指定された Cisco IOS XE プロセスの詳細なメモリ情報を表示します。

name *process-name*	（任意）Cisco IOS XE プロセス名を表示します。プロセス名を入力します。
process-id *process-ID*	（任意）Cisco IOS XE プロセス ID を表示します。プロセス ID を入力します。
location	（任意）Field Replaceable Unit（FRU）の場所に関する情報を表示します。
maps	（任意）プロセスのメモリ マップを表示します。
smaps	（任意）プロセスの静的メモリマップを表示します。
sorted	（任意）Cisco IOS XE プロセスによって使用されている常駐セットサイズ（RSS）メモリに基づいてソートされた出力を表示します。
switch *switch-number*	デバイスに関する情報を表示します。
active	デバイスのアクティブインスタンスに関する情報を表示します。
standby	デバイスのスタンバイインスタンスに関する情報を表示します。
0	共有ポートアダプタ（SPA）インターフェイス プロセッサ スロット 0 に関する情報を表示します。
F0	Embedded Service Processor（ESP）スロット 0 に関する情報を表示します。
R0	ルートプロセッサ（RP）スロット 0 に関する情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
	このコマンドが導入されました。

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが変更されました。キーワード **accounting** が追加されました。 出力から **Total** 列が削除されました。

例

次に、**show processes memory platform** コマンドの出力例を示します。

```
device# show processes memory platform

System memory: 3976852K total, 2761580K used, 1215272K free,
Lowest: 1215272K
   Pid    Text      Data   Stack   Dynamic       RSS                  Name
--------------------------------------------------------------------------------
     1    1246      4400     132      1308      4400               systemd
    96     233      2796     132       132      2796       systemd-journal
   105     284      1796     132       176      1796         systemd-udevd
   707      52      2660     132       172      2660            in.telnetd
   744     968      3264     132      1700      3264             brelay.sh
   835      52      2660     132       172      2660            in.telnetd
   863     968      3264     132      1700      3264             brelay.sh
   928     968      3996     132      2312      3996          reflector.sh
   933     968      3976     132      2312      3976           droputil.sh
   934     968      2140     132       528      2140                oom.sh
   936     173       936     132       132       936               xinetd
   945     968      1472     132       132      1472           libvirtd.sh
   947     592     43164     132      3096     43164                 repm
   954      45       932     132       132       932              rpcbind
   986     482      3476     132       132      3476              libvirtd
   988      66       940     132       132       940             rpc.statd
   993     968       928     132       132       928       boothelper_evt.
  1017      21       640     132       132       640            inotifywait
  1089     102      1200     132       132      1200             rpc.mountd
  1328       9      2940     132       148      2940                 rotee
  1353      39       532     132       132       532                 sleep
!
!
!
```

次に、**show processes memory platform accounting** コマンドの出力例を示します。

```
device# show processes memory platform accounting
Hourly Stats

  process                 callsite_ID(bytes)  max_diff_bytes   callsite_ID(calls)
max_diff_calls   tracekey                                    timestamp(UTC)

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

  smand_rp_0              3624155137          172389           3624155138          50
            1#a3e0e4361082c702e5bf1afbd90e6313        2018-09-04 14:23
  linux_iosd-imag_rp_0    3626295305          49188            3624155138          12
            1#545420bd869d25eb5ab826182ee5d9ce        2018-09-04 12:03
  btman_rp_0              3624737792          17080            2953915394          64
            1#d6888bd9564a3c4fcf049c31ba07a036        2018-09-04 22:29
```

```
  fman_fp_image_fp_0      3624059905          16960            4027402242          298
            1#921ba4d9df5b0a6e946a3b270bd6592d       2018-09-04 22:55
  fed_main_event_fp_0     3626295305          16396            4027402242          32
            1#27083f7bf3985d892505806cae2bfb0d       2018-09-04 12:03
  dbm_rp_0                3626295305          16396            4027402242          3
            1#2b878f802bd7703c5298d37e7a4e8ac3       2018-09-04 12:02
  tamd_proc_rp_0          3895208962          12632            3624667171          7
            1#5b0ed8f88ef5f873abcaf8a744037a44       2018-09-04 18:47
  btman_fp_0              3624233985          12288            3624737792          9
            1#d6888bd9564a3c4fcf049c31ba07a036       2018-09-04 15:23
  sif_mgr_rp_0            3624059907          8216             4027402242          4
            1#de2a951a8a7bae83ca2c04c56810eb72       2018-09-04 14:21
  python2.7_fp_0          2954560513          8000             2954560513          1
                                                               2018-09-04 12:16
  nginx_rp_0              3357041665          4608             4027402242          4
            1#32e56bb09e0509c5fa5ac32093631206       2018-09-04 16:18
  rotee_FRU_SLOT_NUM      3624667169          4097             3624667169          1
            1#ff68e5150a698cd59fa259828614995b       2018-09-04 10:43
  hman_rp_0               3893617664          1488             3893617664          1
            1#1c4aadada30083c5d6f66dc8ca8cd4cb       2018-09-04 10:42
  tams_proc_rp_0          3895096320          1024             3895096320          1
            1#a36a3afa9884c8dc4d40af1e80cacd26       2018-09-04 10:42
  stack_mgr_rp_0          4027402242          904              4027402242          4
            1#ca902eab11a18ab056b16554f49871e8       2018-09-04 14:21
  sessmgrd_rp_0           3491618816          848              3624155138          8
            1#720239fc8bddcabc059768c55a1640ed       2018-09-04 14:32
  psd_rp_0                4027402242          696              4027402242          4
            1#98cf04e0ddd78c2400b3ca3b5f298594       2018-09-04 14:21
  lman_rp_0               4027402242          592              4027402242          4
            1#dc8ed9e428d36477a617d56c51d5caf2       2018-09-04 14:21
  bt_logger_rp_0          4027402242          592              4027402242          4
            1#ba882be1ed783e72575e97cc0908e0e8       2018-09-04 14:21
  repm_rp_0               4027402242          592              4027402242          4
            1#ae461a05430efa767427f2ab40aba372       2018-09-04 14:21
  fman_rp_rp_0            4027402242          592              4027402242          3
            1#09def9cc1390911be9e3a7a9c89f4cf7       2018-09-04 12:16
  epc_ws_liaison_fp_0     4027402242          592              4027402242          4
            1#41451626dcce9d1478b22e2ebbbdcf54       2018-09-04 14:21
  cli_agent_rp_0          4027402242          592              4027402242          4
            1#92d3882919daf3a9e210807c61de0552       2018-09-04 14:21
  cmm_rp_0                4027402242          592              4027402242          4
            1#15ed1d79e96874b1e0621c42c3de6166       2018-09-04 14:21
  tms_rp_0                4027402242          352              4027402242          4
            1#5c6efe2e21f15aa16318576d3ec9153c       2018-09-04 12:03
  plogd_rp_0              4027402242          48               4027402242          1
            1#2d7f2ef57206f4fa763d7f2f5400bf1b       2018-09-04 10:43
  cmand_rp_0              3624155137          17               3624155137          1
            1#f1f41f61c44d73014023db5d8a46ecf5       2018-09-04 10:42
!
!
!
```

次に、**show processes memory platform sorted** コマンドの出力例を示します。

```
device# show processes memory platform sorted
System memory: 3976852K total, 2762884K used, 1213968K free,
Lowest: 1213968K

   Pid      Text      Data    Stack   Dynamic       RSS                Name
--------------------------------------------------------------------------------
  7885    149848     684864    136        80    684864     linux_iosd-imag
```

```
  9655      3787     264964    136     18004    264964                wcm
  17261     324      248588    132    103908    248588       fed main event
  4268      391      102084    136      5596    102084            cli_agent
  4856      357       93388    132      3680     93388                dbm
17067     1087       77912    136      1796     77912         platform_mgr
!
!
!
```

次に、 **show processes memory platform sorted location switch active R0** コマンドの出力例を示します。

```
device# show processes memory platform sorted location switch active R0
System memory: 3976852K total, 2762884K used, 1213968K free,
Lowest: 1213968K

   Pid      Text      Data   Stack   Dynamic       RSS                Name
--------------------------------------------------------------------------------
  7885    149848     684864    136        80    684864     linux_iosd-imag
  9655      3787     264964    136     18004    264964                wcm
  17261     324      248588    132    103908    248588       fed main event
  4268      391      102084    136      5596    102084            cli_agent
  4856      357       93388    132      3680     93388                dbm
17067     1087       77912    136      1796     77912         platform_mgr
!
!
!
```

show processes platform

プラットフォームで実行中の IOS-XE プロセスに関する情報を表示するには、特権 EXEC モードで **show processes platform** コマンドを使用します。

show processes platform [**detailed name** *process-name*] [**location switch** {*switch-number* | **active** | **standby**} {**0** | **F0** | **FP active** | **R0**}]

detailed	（任意）指定した IOS-XE プロセスの詳細な情報を表示します。
name*process-name*	（任意）プロセス名を指定します。
location	（任意）Field Replaceable Unit（FRU）の場所を指定します。
switch *switch-number*	（任意）スイッチに関する情報を表示します。
active	（任意）デバイスのアクティブインスタンスを指定します。
standby	（任意）デバイスのスタンバイインスタンスを指定します。
0	共有ポートアダプタ（SPA）インターフェイス プロセッサ スロット 0 を指定します。

F0	Embedded Service Processor（ESP）スロット 0 を指定します。
FP active	Embedded Service Processor（ESP）のアクティブインスタンスを指定します。
R0	ルート プロセッサ（RP）スロット 0 を指定します。

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。

コマンド モード

特権 EXEC（#）

次に例を示します。

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

```
Device# show processes platform

CPU utilization for five seconds: 1%, one minute: 2%, five minutes: 1%
   Pid    PPid  Status        Size  Name
------------------------------------------------------------
     1       0  S             4876  systemd
     2       0  S                0  kthreadd
     3       2  S                0  ksoftirqd/0
     5       2  S                0  kworker/0:0H
     7       2  S                0  rcu_sched
     8       2  S                0  rcu_bh
     9       2  S                0  migration/0
    10       2  S                0  watchdog/0
    11       2  S                0  watchdog/1
    12       2  S                0  migration/1
    13       2  S                0  ksoftirqd/1
    15       2  S                0  kworker/1:0H
    16       2  S                0  watchdog/2
    17       2  S                0  migration/2
    18       2  S                0  ksoftirqd/2
    20       2  S                0  kworker/2:0H
    21       2  S                0  watchdog/3
    22       2  S                0  migration/3
    23       2  S                0  ksoftirqd/3
    24       2  S                0  kworker/3:0
    25       2  S                0  kworker/3:0H
    26       2  S                0  kdevtmpfs
    27       2  S                0  netns
    28       2  S                0  perf
    29       2  S                0  khungtaskd
    30       2  S                0  writeback
    31       2  S                0  ksmd
    32       2  S                0  khugepaged
    33       2  S                0  crypto
    34       2  S                0  bioset
    35       2  S                0  kblockd
    36       2  S                0  ata_sff
    37       2  S                0  rpciod
    63       2  S                0  kswapd0
    64       2  S                0  vmstat
    65       2  S                0  fsnotify_mark
```

```
 66       2  S                0  nfsiod
 74       2  S                0  bioset
 75       2  S                0  bioset
 76       2  S                0  bioset
 77       2  S                0  bioset
 78       2  S                0  bioset
 79       2  S                0  bioset
 80       2  S                0  bioset
 81       2  S                0  bioset
 82       2  S                0  bioset
 83       2  S                0  bioset
 84       2  S                0  bioset
 85       2  S                0  bioset
 86       2  S                0  bioset
 87       2  S                0  bioset
 88       2  S                0  bioset
 89       2  S                0  bioset
 90       2  S                0  bioset
 91       2  S                0  bioset
 92       2  S                0  bioset
 93       2  S                0  bioset
 94       2  S                0  bioset
 95       2  S                0  bioset
 96       2  S                0  bioset
 97       2  S                0  bioset
100       2  S                0  ipv6_addrconf
102       2  S                0  deferwq
```

次の表で、この出力で表示される重要なフィールドについて説明します。

表 *15 : show processes platform* のフィールドの説明

フィールド	説明
Pid	プロセス ID が表示されます。
PPid	親プロセスのプロセス ID が表示されます。
Status（ステータス）	人間が判読可能な形式でプロセスのステータスが表示されます。
サイズ	RAM でそのプロセスに割り当てられているメモリ量を示す常駐セットサイズ（キロバイト（KB））が表示されます。
Name	プロセスに関連付けられているコマンド名が表示されます。同じプロセスのスレッドでも、スレッドごとにコマンドの値が異なる場合があります。

show power inline

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

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

構文の説明

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

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

例

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

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

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

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

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

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

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

表 *16 : show power inline* のフィールドの説明

フィールド	説明
Available	PoE スイッチ上の設定電力[1]の合計で、ワット数（W）です。
Used	PoE ポートに割り当てられている設定電力の合計で、ワット数です。
Remaining	システムで割り当てられていない設定電力の合計（ワット数）です。（Available - Used = Remaining）

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

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

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

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

```
Gi1/0/2   auto   off         log         n/a         5.4    0.0
Gi1/0/3   auto   off         errdisable  n/a         5.4    0.0
Gi1/0/4   off    off         none        n/a         n/a    0.0
Gi1/0/5   off    off         log         n/a         5.4    0.0
Gi1/0/6   off    off         errdisable  n/a         5.4    0.0
Gi1/0/7   auto   off         none        n/a         n/a    0.0
Gi1/0/8   auto   off         log         n/a         5.4    0.0
Gi1/0/9   auto   on          none        n/a         n/a    5.1
Gi1/0/10  auto   on          log         ok          5.4    4.2
Gi1/0/11  auto   on          log         log         5.4    5.9
Gi1/0/12  auto   on          errdisable  ok          5.4    4.2
Gi1/0/13  auto   errdisable  errdisable  n/a         5.4    0.0
<output truncated>
```

上の例では、次のようになっています。

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

- Gi1/0/11 ポートはアップしていて、受電デバイスが接続されています。ポリシングはイネーブルであり、ポリシング アクションとして syslog メッセージを生成するよう設定されています。
- Gi1/0/12 ポートはアップしていて、受電デバイスが接続されています。ポリシングはイネーブルであり、ポリシング アクションとしてポートをシャットダウンするよう設定されています。リアルタイム電力消費がカットオフ値より少ないため、ポリシング アクションは作動しません。
- Gi1/0/13 ポートはアップしていて、受電デバイスが接続されています。ポリシングはイネーブルであり、ポリシング アクションとしてポートをシャットダウンするよう設定されています。

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

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

表 *17 : show power inline police* のフィールドの説明

フィールド	説明
Available	スイッチ上の設定電力[2]
Used	PoE ポートに割り当てられている設定電力の合計で、ワット数です。
Remaining	システムで割り当てられていない設定電力の合計（ワット数）です。（Available - Used = Remaining）
Admin State	管理モード：auto、off、static
Oper State	動作モード： • errdisable：ポリシングはイネーブルです。 • faulty：受電デバイスでの装置検出が障害の状態です。 • off：PoE が適用されていません。 • on：受電デバイスが検出され、電力が適用されています。 • power-deny：受電デバイスが検出されていますが、PoE が使用できない状態か、リアルタイム電力消費が最大電力割り当てを超えています。 （注） 動作モードは、指定した PoE ポート、指定したスタック メンバ、またはスイッチのすべての PoE ポートの現在の PoE ステートです。

フィールド	説明
Admin Police	リアルタイム電力消費ポリシング機能のステータス： • errdisable：ポリシングがイネーブルで、リアルタイム電力消費が最大電力割り当てを超えるとスイッチはポートをシャットダウンします。 • log：ポリシングはイネーブルで、リアルタイム電力消費が最大電力割り当てを超えるとスイッチが Syslog メッセージを生成します。 • none：ポリシングはディセーブルです。
Oper Police	ポリシング ステータス： • errdisable：リアルタイム電力消費が最大電力割り当てを超えています。スイッチが PoE ポートをシャットダウンします。 • log：リアルタイム電力消費が最大電力割り当てを超えています。スイッチが Syslog メッセージを生成します。 • n/a：装置検出がディセーブルで、電力が PoE ポートに適用されていないか、ポリシング アクションが設定されていません。 • ok：リアルタイム電力消費が最大電力割り当てより少ない状態です。
Cutoff Power	ポートに割り当てられている最大電力です。リアルタイム電力消費がこの値を上回ると、スイッチは設定されたポリシング アクションを実行します。
Oper Power	受電デバイスのリアルタイム電力消費です。

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

次の例では、スタンドアロンスイッチに対する **show power inline priority** コマンドの出力を示します。

```
デバイス> show power inline priority
Interface  Admin  Oper       Priority
           State  State
---------- ------ ---------- --------

Gi1/0/1    auto   off        low
Gi1/0/2    auto   off        low
Gi1/0/3    auto   off        low
Gi1/0/4    auto   off        low
Gi1/0/5    auto   off        low
Gi1/0/6    auto   off        low
Gi1/0/7    auto   off        low
Gi1/0/8    auto   off        low
Gi1/0/9    auto   off        low
```

show stack-power

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

{**show stack-power** [{**budgeting** | **detail** | **load-shedding** | **neighbors**}] [**order** *power-stack-name*] | [{**stack-name** [*stack-id*] | **switch** [*switch-id*]}]}

構文の説明

budgeting	（任意）スタック電源のバジェット テーブルを表示します。
detail	（任意）スタック電源のスタックの詳細を表示します。
load-shedding	（任意）スタック電源の負荷制限テーブルを表示します。
neighbors	（任意）スタック電源のネイバー テーブルを表示します。
order *power-stack-name*	（任意）電源スタックの負荷制限優先順位を表示します。 （注） このキーワードは、**load-shedding** キーワードの後にのみ使用できます。
stack-name	（任意）すべての電源スタックまたは指定された電源スタックのバジェット テーブル、詳細、またはネイバーを表示します。 （注） このキーワードは、**load-shedding** キーワードの後には使用できません。
stack-id	（任意）電源スタックの電源スタック ID。スタック ID は、31 文字以下である必要があります。
switch	（任意）すべてのスイッチ、または指定されたスイッチのバジェット テーブル、詳細、負荷制限、またはネイバーを表示します。
switch-id	（任意）スイッチのスイッチ ID。スイッチ番号は 1～9 です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	すべてのオプションのサポートは、このコマンドに対して有効になっています。
Cisco IOS XE Denali 16.1.1	このコマンドが再度導入されました。

使用上のガイドライン

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

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

例

次に、**show stack-power** コマンドの出力例を示します。

```
デバイス# show stack-power
Power Stack           Stack   Stack    Total   Rsvd    Alloc   Unused  Num  Num
Name                  Mode    Topolgy  Pwr(W)  Pwr(W)  Pwr(W)  Pwr(W)  SW   PS
--------------------  ------  -------  ------  ------  ------  ------  ---  ---
Powerstack-1          SP-PS   Stndaln  350     150     200     0       1    1
```

次に、**show stack-power budgeting** コマンドの出力例を示します。

```
デバイス# show stack-power budgeting
Power Stack           Stack   Stack    Total   Rsvd    Alloc   Unused  Num  Num
Name                  Mode    Topolgy  Pwr(W)  Pwr(W)  Pwr(W)  Pwr(W)  SW   PS
--------------------  ------  -------  ------  ------  ------  ------  ---  ---
Powerstack-1          SP-PS   Stndaln  350     150     200     0       1    1

    Power Stack           PS-A   PS-B   Power     Alloc     Avail   Consumd Pwr
SW  Name                  (W)    (W)    Budgt(W)  Power(W)  Pwr(W)  Sys/PoE(W)
--  --------------------  -----  -----  --------  --------  ------  -----------
1   Powerstack-1          350    0      200       200       0       60   /0
--  --------------------  -----  -----  --------  --------  ------  -----------
Totals:                                          200       0       60   /0
```

show system mtu

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

show system mtu

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

例

次に、**show system mtu** コマンドの出力例を示します。

```
デバイス# show system mtu
Global Ethernet MTU is 1500 bytes.
```

show tech-support

システム情報を表示する **show** コマンドを自動的に実行するには、特権 EXEC モードで **show tech-support** コマンドを使用します。

show tech-support
[cef | cft | eigrp | evc | fnf | | ipc | ipmulticast | ipsec | mfib | nat | nbar | onep | ospf | page | password | rsvp | subscriber | vrrp | wccp

構文の説明

cef	（任意）CEF 関連情報を表示します。
cft	（任意）CFT 関連情報を表示します。
eigrp	（任意）EIGRP 関連情報を表示します。
evc	（任意）EVC 関連情報を表示します。
fnf	（任意）Flexible NetFlow 関連情報を表示します。
ipc	（任意）IPC 関連情報を表示します。
ipmulticast	（任意）IP 関連情報を表示します。
ipsec	（任意）IPSEC 関連情報を表示します。
mfib	（任意）MFIB 関連情報を表示します。
nat	（任意）NAT 関連情報を表示します。
onep	（任意）ONEP 関連情報を表示します。
ospf	（任意）OSPF 関連情報を表示します。
page	（任意）コマンド出力を 1 ページずつ表示します。Return キーを押して、出力の次の行を表示するか、スペースバーを使用して、次の情報ページを表示します。使用しない場合、出力がスクロールします（つまり、改ページで停止しません）。 コマンド出力を停止するには、**Ctrl+C** キーを押します。

password	（任意）パスワードおよびその他のセキュリティ情報を出力に残します。使用しない場合、出力中のパスワードおよびそのほかのセキュリティ関連情報は、ラベル「<removed>」と置き換えられます。
subscriber	（任意）サブスクライバ関連情報を表示します。
vrrp	（任意）VRRP 関連情報を表示します。
wccp	（任意）WCCP 関連情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが拡張され、**show logging onboard uptime** コマンドの出力が表示されるようになりました。
Cisco IOS XE Denali 16.3.2	このコマンドは、出力修飾子の次のコマンドの出力を表示できるよう強化されました。 • **show power inline** • **show platform software ilpower details** • **show power inline police** • **show stack-power budgeting**
Cisco IOS XE Denali 16.1.1	このコマンドが以下に実装されました。 Cisco Catalyst 3650 シリーズスイッチ

使用上のガイドライン

show tech-support コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします（たとえば、**show tech-support** > *filename*）。ファイルに出力をリダイレクトすると、出力を Cisco Technical Assistance Center（TAC）の担当者に送信することも容易になります。

リダイレクトには、次のいずれかの方法を使用できます。

- > *filename*：出力をファイルにリダイレクトします。
- >> *filename*：出力をファイルにアペンドモードでリダイレクトします。

show tech-support diagnostic

テクニカルサポートに使用する診断情報を表示するには、特権EXECモードで**show tech-support diagnostic** コマンドを使用します。

show tech-support diagnostic

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします（たとえば、**show tech-support diagnostic** > **flash:***filename*）。

（注） スタック構成をサポートしているデバイスの場合、このコマンドはアップしているすべてのスイッチで実行されます。スタック構成をサポートしていないデバイスの場合、このコマンドはアクティブスイッチでのみ実行されます。

このコマンドの出力には次のコマンドの出力が表示されます。

- **show clock**
- **show version**
- **show running-config**
- **show inventory**
- **show diagnostic bootup level**
- **show diagnostic status**
- **show diagnostic content switch all**
- **show diagnostic result switch all detail**
- **show diagnostic schedule switch all**
- **show diagnostic post**
- **show diagnostic description switch [switch number] test all**
- **show logging onboard switch [switch number] clilog detail**
- **show logging onboard switch [switch number] counter detail**

- **show logging onboard switch [switch number] environment detail**
- **show logging onboard switch [switch number] message detail**
- **show logging onboard switch [switch number] poe detail**
- **show logging onboard switch [switch number] status**
- **show logging onboard switch [switch number] temperature detail**
- **show logging onboard switch [switch number] uptime detail**
- **show logging onboard switch [switch number] voltage detail**

例

次に、**show tech-support diagnostic** コマンドの出力例を示します。

```
Device# show tech-support diagnostic

.
.
.
------------------ show diagnostic status ------------------

<BU> - Bootup Diagnostics, <HM> - Health Monitoring Diagnostics,

<OD> - OnDemand Diagnostics, <SCH> - Scheduled Diagnostics

====== ================================= ================================ ======
Card   Description                       Current Running Test             Run by
------ --------------------------------- -------------------------------- ------
1      C3650                             N/A                              N/A


2      MODEL UNSET                       N/A                              N/A


3      MODEL UNSET                       N/A                              N/A


4      MODEL UNSET                       N/A                              N/A


5      MODEL UNSET                       N/A                              N/A


6      MODEL UNSET                       N/A                              N/A


7      MODEL UNSET                       N/A                              N/A
```

```
====== ================================= ============================== ======

------------------ show diagnostic content switch all ------------------

switch 1:


  Diagnostics test suite attributes:
    M/C/* - Minimal bootup level test / Complete bootup level test / NA
      B/* - Basic ondemand test / NA
    P/V/* - Per port test / Per device test / NA
    D/N/* - Disruptive test / Non-disruptive test / NA
      S/* - Only applicable to standby unit / NA
      X/* - Not a health monitoring test / NA
      F/* - Fixed monitoring interval test / NA
      E/* - Always enabled monitoring test / NA
      A/I - Monitoring is active / Monitoring is inactive

                                                          Test Interval   Thre-
  ID   Test Name                           Attributes     day hh:mm:ss.ms shold
  ==== ================================== ============   =============== =====
    1) DiagGoldPktTest -----------------> *BPN*X**I       not configured  n/a
    2) DiagThermalTest -----------------> *B*N****A       000 00:01:30.00 5
    3) DiagFanTest ---------------------> *B*N****A       000 00:01:30.00 5
    4) DiagPhyLoopbackTest -------------> *BPD*X**I       not configured  n/a
    5) DiagScratchRegisterTest ---------> *B*N****A       000 00:01:30.00 5
    6) TestUnusedPortLoopback ----------> *BPN****I       not configured  n/a
    7) TestPortTxMonitoring ------------> *BPN****A       000 00:01:30.00 1
    8) DiagPoETest ---------------------> ***D*X**I       not configured  n/a
    9) DiagStackCableTest --------------> ***D*X**I       not configured  n/a
   10) DiagMemoryTest ------------------> *B*D*X**I       not configured  n/a


switch 2:
```

```
  Diagnostics test suite attributes:
    M/C/* - Minimal bootup level test / Complete bootup level test / NA
      B/* - Basic ondemand test / NA
    P/V/* - Per port test / Per device test / NA
    D/N/* - Disruptive test / Non-disruptive test / NA
      S/* - Only applicable to standby unit / NA
      X/* - Not a health monitoring test / NA
      F/* - Fixed monitoring interval test / NA
      E/* - Always enabled monitoring test / NA
      A/I - Monitoring is active / Monitoring is inactive

                                                          Test Interval   Thre-
  ID   Test Name                           Attributes     day hh:mm:ss.ms shold
  ==== ================================== ============   =============== =====
    1) DiagGoldPktTest -----------------> *BPN*X**I       not configured  n/a
    2) DiagThermalTest -----------------> *B*N****A       000 00:01:30.00 5
    3) DiagFanTest ---------------------> *B*N****A       000 00:01:30.00 5
    4) DiagPhyLoopbackTest -------------> *BPD*X**I       not configured  n/a
    5) DiagScratchRegisterTest ---------> *B*N****A       000 00:01:30.00 5
    6) TestUnusedPortLoopback ----------> *BPN****I       not configured  n/a
    7) TestPortTxMonitoring ------------> *BPN****A       000 00:01:30.00 1
    8) DiagPoETest ---------------------> ***D*X**I       not configured  n/a
    9) DiagStackCableTest --------------> ***D*X**I       not configured  n/a
   10) DiagMemoryTest ------------------> *B*D*X**I       not configured  n/a
.
.
.
------------------ show logging onboard switch 4 clilog detail ------------------


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

CLI LOGGING SUMMARY INFORMATION

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

COUNT COMMAND
```

```
------------------------------------------------------------------------------

No summary data to display

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

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

CLI LOGGING CONTINUOUS INFORMATION

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

MM/DD/YYYY HH:MM:SS COMMAND

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


No continuous data

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



------------------ show logging onboard switch 5 clilog detail ------------------


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

CLI LOGGING SUMMARY INFORMATION

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

COUNT COMMAND

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

No summary data to display

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

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

CLI LOGGING CONTINUOUS INFORMATION

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

MM/DD/YYYY HH:MM:SS COMMAND

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


No continuous data

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

.
```

.
.

speed

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

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

構文の説明

10	ポートが 10 Mbps で稼働することを指定します。
100	ポートが 100 Mbps で稼働することを指定します。
1000	ポートが 1000 Mbps で稼働することを指定します。このオプションは、10/100/1000 Mb/s ポートでだけ有効になって表示されます。
2500	ポートが 2500 Mbps で稼働することを指定します。このオプションは、マルチギガビット対応のイーサネット ポートでのみ有効であり、表示されます。
5000	ポートが 5000 Mbps で稼働することを指定します。このオプションは、マルチギガビット対応のイーサネット ポートでのみ有効であり、表示されます。
auto	稼働時のポートの速度を、リンクのもう一方の終端のポートを基準にして自動的に検出します。**auto** キーワードと一緒に **10**、**100**、**1000**、**1000**、**2500**、または **5000** キーワードを使用した場合、ポートは指定の速度でのみ自動ネゴシエートします。
nonegotiate	自動ネゴシエーションをディセーブルにし、ポートは 1000 Mbps で稼働します。

コマンド デフォルト

デフォルトは **auto** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

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

使用上のガイドライン

10 ギガビット イーサネット ポートでは速度を設定できません。

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

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

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

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

⚠

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

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

設定を確認するには、**show interfaces** 特権 EXEC コマンドを使用します。

例

次に、ポートの速度を 100 Mbps に設定する例を示します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# speed 100
```

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

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# speed auto 10
```

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

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

stack-power

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

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

構文の説明

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

コマンド デフォルト

デフォルトはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

- **default**：コマンドをデフォルト設定に戻します。
- **exit**：ARP アクセスリスト コンフィギュレーション モードを終了します。
- **mode**：電源スタックの電源モードを設定します。**mode** コマンドを参照してください。
- **no**：コマンドを無効にするか、またはデフォルト設定に戻します。

StackPower に関係のないスイッチ番号を指定して **stack-power switch** *switch-number* コマンドを入力すると、エラーメッセージが表示されます。

StackPower に関係するスイッチ番号を指定して **stack-power switch** *switch-number* コマンドを入力すると、スイッチスタック電源コンフィギュレーション モードが開始され、次のコマンドが使用可能になります。

- **default**：コマンドをデフォルト設定に戻します。
- **exit**：スイッチ スタック電源コンフィギュレーション モードを終了します。
- **no**：コマンドを無効にするか、またはデフォルト設定に戻します。
- **power-priority**：スイッチとスイッチ ポートの電源プライオリティを設定します。**power-priority** コマンドを参照してください。
- **stack-id** *name*：スイッチが属する電源スタックの名前を入力します。電源スタック ID を入力しない場合、スイッチはスタック パラメータを継承しません。名前は最大で 31 文字にできます。
- **standalone**：スイッチをスタンドアロン電源モードで動作させます。このモードに設定すると、両方の電源ポートがシャットダウンします。

例

次の例では、電源スタックに接続されたスイッチ 2 が電源プールから削除され、両方の電源ポートがシャットダウンされます。

```
デバイス(config)# stack-power switch 2
デバイス(config-switch-stackpower)# standalone
デバイス(config-switch-stackpower)# exit
```

switchport block

不明なマルチキャストまたはユニキャストパケットが転送されないようにするには、インターフェイス コンフィギュレーション モードで **switchport block** コマンドを使用します。不明なマルチキャストまたはユニキャストパケットの転送を許可するには、このコマンドの **no** 形式を使用します。

switchport block {**multicast** | **unicast**}
no switchport block {**multicast** | **unicast**}

構文の説明

multicast	不明のマルチキャスト トラフィックがブロックされるように指定します。 （注） 純粋なレイヤ 2 マルチキャスト トラフィックだけがブロックされます。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。
unicast	不明のユニキャスト トラフィックがブロックされるように指定します。

コマンド デフォルト

不明なマルチキャストおよびユニキャスト トラフィックはブロックされていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

デフォルトでは、不明な MAC アドレスを持つすべてのトラフィックがすべてのポートに送信されます。保護ポートまたは非保護ポート上の不明なマルチキャストまたはユニキャスト トラフィックをブロックすることができます。不明なマルチキャストまたはユニキャスト トラフィックが保護ポートでブロックされない場合、セキュリティに問題のある場合があります。

マルチキャスト トラフィックでは、ポート ブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。

不明なマルチキャストまたはユニキャスト トラフィックのブロックは、保護ポート上で自動的にイネーブルにはなりません。明示的に設定する必要があります。

パケットのブロックに関する情報は、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

次の例では、インターフェイス上で不明なユニキャスト トラフィックをブロックする方法を示します。

```
デバイス(config-if)# switchport block unicast
```

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

system mtu

構文の説明

bytes

コマンド デフォルト

すべてのポートのデフォルトの MTU サイズは 1500 バイトです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

スイッチはインターフェイス単位では MTU をサポートしていません。

特定のインターフェイス タイプで許容範囲外の値を入力した場合、その値は受け入れられません。

test mcu read-register

Power over Ethernet（PoE）コントローラのデバッグを有効にするには、特権 EXEC モードで **test mcu read-register** コマンドを使用します。

test mcu read-register {**det-cls-offset** | **manufacture-id** | **port-mode**}

構文の説明

det-cls-offset	読み取り検出分類登録の概要を表示します。
manufacture-id	PoE コントローラの製造 ID を表示します。
port-mode	ポート モードの詳細を表示します。

コマンド モード

特権 EXEC

コマンド履歴

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

例

次に、**test mcu read-register det-cls-offset** コマンドの出力例を示します。

```
Device# test mcu read-register det-cls-offset 1
 DETECTION ENABLE BIT SUMMARY

Controller    port1          port2          port3          port4       register
                                                                      (hexadecimal)
----------   -------        -------        -------        -------    ------------
1               1              0              1              0           5
2               1              0              1              0           5
3               1              0              1              0           5
4               1              0              1              0           5
5               1              0              1              0           5
6               1              0              1              0           5
7               1              0              1              0           5
8               1              0              1              0           5
9               1              0              1              0           5
10              1              0              1              0           5
11              0              0              1              0           4
12              1              0              0              0           1

 CLASSIFICATION ENABLE BIT SUMMARY
```

```
Controller    port1          port2          port3          port4       register
                                                                      (hexadecimal)
----------   -------        -------        -------        -------    ------------
1               1              0              1              0           5
2               1              0              1              0           5
3               1              0              1              0           5
4               1              0              1              0           5
5               1              0              1              0           5
6               1              0              1              0           5
7               1              0              1              0           5
8               1              0              1              0           5
9               1              0              1              0           5
10              1              0              1              0           5
11              0              0              1              0           4
12              1              0              0              0           1
```

次に、**test mcu read-register manufacture-id** コマンドの出力例を示します。

```
MANUFACTURE ID : DEVICE_BCM_PALPATINE reg_val = 0x1B
```

次に、**test mcu read-register port-mode** コマンドの出力例を示します。

```
 PORT MODE SUMMERY
Controller    port1          port2          port3          port4       register
                                                                      (hexadecimal)
----------   -------        -------        -------        -------    ------------
1              01             00             01             00          22
2              01             00             01             00          22
3              01             00             01             00          22
4              01             00             01             00          22
5              01             00             01             00          22
6              01             00             01             00          22
7              01             00             01             00          22
8              01             00             01             00          22
9              01             00             01             00          22
10             01             00             01             00          22
11             00             00             01             00          20
12             01             00             00             00           2
```

voice-signalingvlan（ネットワークポリシーコンフィギュレーション）

音声シグナリング アプリケーション タイプのネットワークポリシー プロファイルを作成するには、ネットワークポリシー コンフィギュレーション モードで **voice-signaling vlan** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

voice-signaling vlan {*vlan-id* [{**cos** *cos-value* | **dscp** *dscp-value*}] | **dot1p** [{**cos** *l2-priority* | **dscp** *dscp*}] | **none** | **untagged**}

構文の説明

vlan-id	（任意）音声トラフィック用の VLAN。指定できる範囲は 1 ～ 4094 です。
cos *cos-value*	（任意）設定された VLAN に対するレイヤ 2 プライオリティ Class of Service（CoS）を指定します。指定できる範囲は 0 ～ 7 です。デフォルト値は 5 です。
dscp *dscp-value*	（任意）設定された VLAN に対する Diffserv コード ポイント（DSCP）値を指定します。指定できる範囲は 0 ～ 63 です。デフォルト値は 46 です。
dot1p	（任意）IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話を設定します。
none	（任意）音声 VLAN に関して Cisco IP Phone に指示しません。電話は電話のキー パッドから入力された設定を使用します。
untagged	（任意）タグなしの音声トラフィックを送信するように電話を設定します。これが電話のデフォルトになります。

コマンド デフォルト

音声シグナリング アプリケーション タイプのネットワークポリシー プロファイルは定義されていません。

デフォルトの CoS 値は、5 です。

デフォルトの DSCP 値は、46 です。

デフォルトのタギング モードは、untagged です。

コマンド モード

ネットワークポリシー プロファイル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

voice-signaling アプリケーション タイプは、音声メディアと異なる音声シグナリング用のポリシーを必要とするネットワーク トポロジ用です。すべての同じネットワーク ポリシーが voice policy TLV にアドバタイズされたポリシーとして適用される場合、このアプリケーション タイプはアドバタイズしないでください。

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

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

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

次の例では、プライオリティ 2 の CoS を持つ VLAN 200 用の音声シグナリングを設定する方法を示します。

```
デバイス(config)# network-policy profile 1
デバイス(config-network-policy)# voice-signaling vlan 200 cos 2
```

次の例では、DSCP 値 45 を持つ VLAN 400 用の音声シグナリングを設定する方法を示します。

```
デバイス(config)# network-policy profile 1
デバイス(config-network-policy)# voice-signaling vlan 400 dscp 45
```

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声シグナリングを設定する方法を示します。

```
デバイス(config-network-policy)# voice-signaling vlan dot1p cos 4
```

voicevlan（ネットワークポリシーコンフィギュレーション）

音声アプリケーションタイプのネットワークポリシー プロファイルを作成するには、ネットワークポリシー コンフィギュレーション モードで **voice vlan** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

voice vlan {*vlan-id* [{**cos** *cos-value* | **dscp** *dscp-value*}] | **dot1p** [{**cos** *l2-priority* | **dscp** *dscp*}] | **none** | **untagged**}

構文の説明

vlan-id	（任意）音声トラフィック用の VLAN。指定できる範囲は 1 ～ 4094 です。

cos *cos-value*	（任意）設定された VLAN に対するレイヤ 2 プライオリティ Class of Service（CoS）を指定します。指定できる範囲は 0 ～ 7 です。デフォルト値は 5 です。
dscp *dscp-value*	（任意）設定された VLAN に対する Diffserv コード ポイント（DSCP）値を指定します。指定できる範囲は 0 ～ 63 です。デフォルト値は 46 です。
dot1p	（任意）IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話を設定します。
none	（任意）音声 VLAN に関して Cisco IP Phone に指示しません。電話は電話のキー パッドから入力された設定を使用します。
untagged	（任意）タグなしの音声トラフィックを送信するように電話を設定します。これが電話のデフォルトになります。

コマンド デフォルト

音声アプリケーション タイプのネットワークポリシー プロファイルは定義されていません。

デフォルトの CoS 値は、5 です。

デフォルトの DSCP 値は、46 です。

デフォルトのタギング モードは、untagged です。

コマンド モード

ネットワークポリシー プロファイル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

voice アプリケーション タイプは IP Phone 専用であり、対話形式の音声サービスをサポートするデバイスに似ています。通常、これらのデバイスは、展開を容易に行えるようにし、データ アプリケーションから隔離してセキュリティを強化するために、別個の VLAN に配置されます。

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

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

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

次の例では、プライオリティ 4 の CoS を持つ VLAN 100 用の音声アプリケーション タイプを設定する方法を示します。

```
デバイス(config)# network-policy profile 1
デバイス(config-network-policy)# voice vlan 100 cos 4
```

次の例では、DSCP 値 34 を持つ VLAN 100 用の音声アプリケーション タイプを設定する方法を示します。

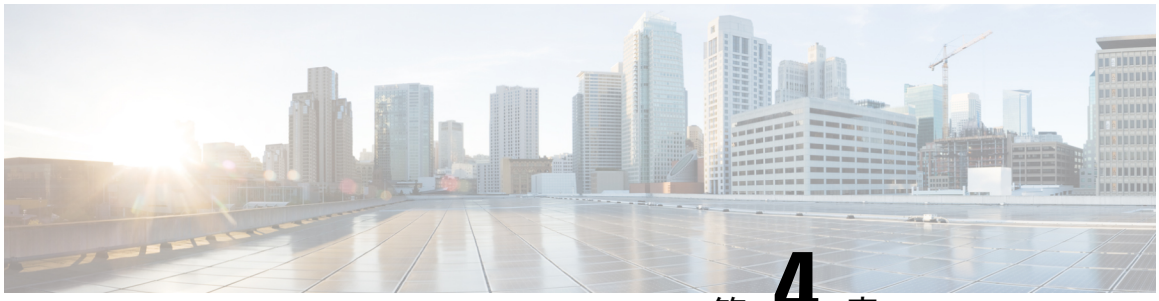
```
デバイス(config)# network-policy profile 1
デバイス(config-network-policy)# voice vlan 100 dscp 34
```

次の例では、プライオリティ タギングを持つネイティブ VLAN 用の音声アプリケーション タイプを設定する方法を示します。

```
デバイス(config-network-policy)# voice vlan dot1p cos 4
```

第 III 部

IP アドレッシングサービス



第 4 章

IP コマンド

clear ip nhrp

Next Hop Resolution Protocol（NHRP）キャッシュ内のすべてのダイナミックエントリをクリアするには、ユーザ EXEC モードまたは特権 EXEC モードで **clear ip nhrp** コマンドを使用します。

clear ip nhrp[{**vrf** {*vrf-name* | **global**}}] [{*dest-ip-address* [{*dest-mask*}] | **tunnel** *number* | **counters** [{**interface tunnel** *number*}] | **stats** [{**tunnel** *number*[{**vrf** {*vrf-name* | **global**}}]}]}]

構文の説明

vrf	（任意）指定された Virtual Routing and Forwarding（VRF）インスタンスの NHRP キャッシュからエントリを削除します。
vrf-name	（任意）コマンドが適用された VRF アドレス ファミリの名前。
global	（任意）グローバル VRF インスタンスを指定します。
dest-ip-address	（任意）宛先 IP アドレス。この引数を指定すると、指定された宛先 IP アドレスの NHRP マッピングエントリがクリアされます。
dest-mask	（任意）宛先ネットワークマスク。
counters	（任意）NHRP カウンタをクリアします。
interface	（任意）すべてのインターフェイスの NHRP マッピングエントリをクリアします。
tunnel *number*	（任意）NHRP キャッシュから指定されたインターフェイスを削除します。
stats	（任意）すべてのインターフェイスの IPv4 統計情報をすべてクリアします。

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 Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

clear ip nhrp コマンドでは、スタティックに設定された IP と NBMA のいずれのアドレスマッピングも NHRP キャッシュからクリアしません。

例

次に、インターフェイスの NHRP キャッシュ内のダイナミックエントリすべてをクリアする例を示します。

```
Switch# clear ip nhrp
```

関連コマンド

コマンド	説明
show ip nhrp	NHRP マッピング情報を表示します。

debug nhrp

Next Hop Resolution Protocol（NHRP）のデバッグを有効にするには、特権 EXEC モードで **debug nhrp** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug nhrp [{**attribute** | **cache** | **condition** {**interface tunnel** *number* | **peer** {**nbma** {*ipv4-nbma-address nbma-name ipv6-nbma-address*} } | **umatched** | **vrf** *vrf-name* } | **detail** | **error** | **extension** | **group** | **packet** | **rate**}]
no debug nhrp [{**attribute** | **cache** | **condition** {**interface tunnel** *number* | **peer** {**nbma** {*ipv4-nbma-address nbma-name ipv6-nbma-address*} } **unmatched** | **vrf** *vrf-name* } | **detail** | **error** | **extension** | **group** | **packet** | **rate** }]

構文の説明

attribute	（任意）NHRP 属性デバッグ操作を有効にします。
cache	（任意）NHRP キャッシュ デバッグ操作を有効にします。
condition	（任意）NHRP 条件デバッグ操作を有効にします。
interface tunnel *number*	（任意）トンネルインターフェイスのデバッグ操作を有効にします。
nbma	（任意）ノンブロードキャスト マルチプル アクセス（NBMA）ネットワークのデバッグ操作を有効にします。
ipv4-nbma-address	（任意）NBMA ネットワークの IPv4 アドレスに基づくデバッグ操作を有効にします。
nbma-name	（任意）NBMA ネットワーク名。

IPv6-address	（任意）NBMA ネットワークの IPv6 アドレスに基づくデバッグ操作を有効にします。 （注） *IPv6-address* 引数は、Cisco IOS XE Denali 16.3.1 ではサポートされていません。
vrf *vrf-name*	（任意）Virtual Routing and Forwarding インスタンスのデバッグ操作を有効にします。
detail	（任意）NHRP デバッグの詳細なログを表示します。
error	（任意）NHRP エラー デバッグ操作を有効にします。
extension	（任意）NHRP 拡張処理デバッグ操作を有効にします。
group	（任意）NHRP グループ デバッグ操作を有効にします。
packet	（任意）NHRP アクティビティ デバッグを有効にします。
rate	（任意）NHRP レート制限を有効にします。
routing	（任意）NHRP ルーティング デバッグ操作を有効にします。

コマンド デフォルト

NHRP デバッグは有効になっていません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

（注） Cisco IOS XE Denali 16.3.1 では、このコマンドは IPv4 だけをサポートしています。*IPv6-nbma-address* 引数は、スイッチでは使用可能ですが、設定しても機能しません。

NHRP 属性ログを表示するには、**debug nhrp detail** コマンドを使用します。

Virtual-Access *number* キーワードと引数のペアは、デバイスで仮想アクセスインターフェイスが使用可能な場合にのみ表示されます。

例

次に、**debug nhrp** コマンドの出力例と、IPv4 に関する NHRP デバッグ出力を表示する例を示します。

```
Switch# debug nhrp

Aug  9 13:13:41.486: NHRP: Attempting to send packet via DEST 10.1.1.99
```

```
Aug  9 13:13:41.486: NHRP: Encapsulation succeeded.  Tunnel IP addr 10.11.11.99
Aug  9 13:13:41.486: NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 105
Aug  9 13:13:41.486:       src: 10.1.1.11, dst: 10.1.1.99
Aug  9 13:13:41.486: NHRP: 105 bytes out Tunnel0
Aug  9 13:13:41.486: NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size:
125
Aug  9 13:13:41.486: NHRP: netid_in = 0, to_us = 1
```

関連コマンド

コマンド	説明
show ip nhrp	NHRPマッピング情報を表示します。

fhrp delay

First Hop Redundancy Protocol（FHRP）クライアントの初期化の遅延時間を指定するには、インターフェイス コンフィギュレーション モードで **fhrp delay** コマンドを使用します。指定した時間を削除するには、このコマンドの **no** 形式を使用します。

fhrp delay {[**minimum**] [**reload**] *seconds*}
no fhrp delay {[**minimum**] [**reload**] *seconds*}

構文の説明

minimum	（任意）インターフェイスが使用可能になった後の遅延時間を設定します。
reload	（任意）デバイスのリロード後の遅延時間を設定します。
seconds	秒単位の遅延時間。範囲は 0 ～ 3600 です。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション（config-if）

例

次に、FHRP クライアントの初期化の遅延期間を指定する例を示します。

```
Device(config-if)# fhrp delay minimum 90
```

関連コマンド

コマンド	説明
show fhrp	ファーストホップ冗長性プロトコル（FHRP）の情報を表示します。

fhrp version vrrp v3

Virtual Router Redundancy Protocol バージョン 3（VRRPv3）と Virtual Router Redundancy Service（VRRS）をデバイスで有効にするには、グローバル コンフィギュレーション モードで **fhrp**

version vrrp v3 コマンドを使用します。VRRPv3 と VRRS の設定機能をデバイスで無効にするには、このコマンドの **no** 形式を使用します。

fhrp version vrrp v3
no fhrp version vrrp v3

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

VRRPv3 と VRRS 設定はデバイスで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）

使用上のガイドライン

VRRPv3 が使用中の場合、VRRP バージョン 2（VRRPv2）は使用できません。

例

次の例では、トラッキング プロセスは、VRRPv3 グループを使用して IPv6 オブジェクトの状態を追跡するように設定されています。ギガビットイーサネットインターフェイス 0/0/0 の VRRP は、VRRPv3 グループで IPv6 オブジェクトに何らかの変更が生じた場合には通知されるように、トラッキング プロセスに登録します。シリアル インターフェイス VRRPv3 の IPv6 オブジェクト ステートがダウンになると、VRRP グループのプライオリティは 20 だけ引き下げられます。

```
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# vrrp 1 address-family ipv6
Device(config-if-vrrp)# track 1 decrement 20
```

関連コマンド

コマンド	説明
track (VRRP)	VRRPv3 グループを使用したオブジェクトの追跡を有効にします。

glbp authentication

Gateway Load Balancing Protocol（GLBP）の認証文字列を設定するには、インターフェイス コンフィギュレーション モードで **glbp authentication** コマンドを使用します。認証を無効にするには、このコマンドの **no** 形式を使用します。

glbp *group-number***authentication** {**text** *string* | **md5** {**key-string** [{**0** | **7**}] *key* | **key-chain** *name-of-chain*}}
no glbp *group-number* **authentication** {**text** *string* | **md5** {**key-string** [{**0** | **7**}] *key* | **key-chain** *name-of-chain*}}

構文の説明

group-number	0 ～ 1023 の範囲の GLBP グループ番号。
text *string*	認証ストリングを指定します。コマンドとテキストを合わせた文字数が 255 文字を超えないようにします。

md5	Message Digest 5（MD5）認証。
key-string *key*	MD5 認証の秘密キーを指定します。キー ストリングは、100 文字の長さを超えることはできません。少なくとも 16 文字使用することを推奨します。
0	（任意）非暗号化キー。プレフィックスが指定されていない場合、キーは暗号化されません。
7	（任意）暗号化キー。
key-chain *name-of-chain*	認証キーのグループを指定します。

コマンド デフォルト

GLBP メッセージの認証は発生しません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

使用上のガイドライン

同じGLBPグループのメンバーとして設定されているすべてのデバイスで同じ認証方式を設定し、確実に相互運用できるようにする必要があります。デバイスは、誤った認証情報を含むすべての GLBP メッセージを無視します。

パスワード暗号化が **service password-encryption** コマンドで設定されると、ソフトウェアは、キー文字列を暗号化されたテキストとして設定に保存します。

例

次に、グループ 10 の GLBP デバイスの相互運用を許可するために必要な認証文字列として stringxyz を設定する例を示します。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 authentication text stringxyz
```

次に、GLBPがキーチェーン「AuthenticateGLBP」を照会して、指定されたキーチェーンの現在アクティブなキーとキー ID を取得する例を示します。

```
Device(config)# key chain AuthenticateGLBP
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string ThisIsASecretKey
Device(config-keychain-key)# exit
Device(config-keychain)# exit
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
```

関連コマンド

Command	Description
glbp ip	GLBP をイネーブルにします。

glbp forwarder preempt

現在のアクティブ バーチャル フォワーダ（AVF）がその低い重み付けしきい値を下回った場合に、デバイスが Gateway Load Balancing Protocol（GLBP）グループの AVF として引き継がれるように設定するには、インターフェイス コンフィギュレーション モードで **glbp forwarder preempt** 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。

glbp *group* **forwarder preempt** [**delay minimum** *seconds*]
no glbp *group* **forwarder preempt** [**delay minimum**]

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
delay minimum *seconds*	（任意）デバイスが AVF のロールを引き継ぐ前に遅延する最小秒数を指定します。範囲は 0 ～ 3600 秒です。デフォルトの遅延時間は 30 秒です。

コマンド デフォルト

フォワーダ強制排除は、30 秒のデフォルト遅延でイネーブルになります。

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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 16.2.1	このコマンドが導入されました。

例

次に、現在の AVF がその低い重み付けしきい値を下回った場合に、デバイスが現在の AVF をプリエンプション処理するように設定する例を示します。デバイスが現在の AVF をプリエンプション処理した場合、デバイスは AVF の役割を引き継ぐ前に 60 秒間待ちます。

```
Device(config-if)# glbp 10 forwarder preempt delay minimum 60
```

関連コマンド

コマンド	説明
glbp ip	GLBP をイネーブルにします。

glbp ip

Gateway Load Balancing Protocol（GLBP）を有効化するには、インターフェイス コンフィギュレーション モードで **glbp ip** コマンドを使用します。GLBP を無効にするには、このコマンドの **no** 形式を使用します。

glbp *group* **ip** [*ip-address* [**secondary**]]
no glbp *group* **ip** [*ip-address* [**secondary**]]

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
ip-address	（任意）GLBP グループの仮想 IP アドレス。この IP アドレスはインターフェイス IP アドレスと同じサブネット内になければなりません。
secondary	（任意）IP アドレスがセカンダリ GLBP 仮想アドレスであることを示します。

コマンド デフォルト

GLBP はデフォルトでは無効になっています。

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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 16.2.1	このコマンドが導入されました。

使用上のガイドライン

glbp ip コマンドを実行すると、設定されたインターフェイスで GLBP が有効になります。指定されている IP アドレスがある場合、そのアドレスが GLBP グループの指定仮想 IP アドレスとして使用されます。指定されている IP アドレスがない場合、指定アドレスは、同じ GLBP グループに属するよう設定された別のデバイスから取得されます。GLBP がアクティブ仮想ゲートウェイ（AVG）を選択する場合、ケーブル上の少なくとも 1 つのデバイスが指定アドレスで設定されている必要があります。デバイスは、GLBP ゲートウェイまたはフォワーダの権限を引き受ける前に、GLBP グループの仮想 IP アドレスで設定されているか、そのアドレスを取得している必要があります。AVG の指定アドレスを設定すると、常に使用されている指定アドレスが上書きされます。

glbp ip コマンドがインターフェイスで有効になっている場合、プロキシの Address Resolution Protocol（ARP）要求の処理方法が変更されます（プロキシ ARP が無効になっていない場合）。ARP 要求はホストにより送信され、IP アドレスが MAC アドレスにマッピングされます。GLBP ゲートウェイは、ARP 要求を代行受信し、接続先ノードの代わりに ARP に応答します。GLBP グループのフォワーダがアクティブである場合、プロキシ ARP 要求への応答には、グループ内の最初のアクティブ フォワーダの MAC アドレスが使用されます。アクティブなフォワーダがない場合、プロキシ ARP 要求は停止されます。

例

次の例では、GigabitEthernet インターフェイス 1/0/1 上の グループ 10 の GLBP を有効にします。GLBP グループで使用される仮想 IP アドレスは、10.21.8.10 に設定されます。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 ip 10.21.8.10
```

関連コマンド

Command	Description
show glbp	GLBPの情報を表示します。

glbp load-balancing

Gateway Load Balancing Protocol（GLBP）のアクティブ仮想ゲートウェイ（AVG）で使用されるロードバランシング方式を指定するには、インターフェイス コンフィギュレーション モードで **glbp load-balancing** コマンドを使用します。ロードバランシングを無効にするには、このコマンドの **no** 形式を使用します。

glbp *group* **load-balancing** [{**host-dependent** | **round-robin** | **weighted**}]
no glbp *group* **load-balancing**

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
host-dependent	（任意）ホストの MAC アドレスに基づくロード バランシング方式（GLBP グループ メンバーの数を一定に保ったまま、特定のホストに常に同じフォワーダが使用される）を指定します。
round-robin	（任意）各仮想フォワーダが仮想 IP アドレスのアドレス解決応答に含まれるようなロード バランシング方式を指定します。この方式がデフォルトです。
weighted	（任意）ゲートウェイによってアドバタイズされる重み値に基づくロード バランシング方式を指定します。

コマンド デフォルト

ラウンドロビン方式がデフォルトです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 16.2.1	このコマンドが導入されました。

使用上のガイドライン

各ホストが常に同じデバイスを使用する必要がある場合は、ホスト依存方式の GLBP ロード バランシングを使用します。GLBP グループ内のデバイスの転送能力が異なるために不均等な ロード バランシングを必要とする場合は、重み値方式の GLBP ロード バランシングを使用します。

例

次に、GLBP グループ 10 の AVG に設定されたホスト依存的な GLBP ロード バランシングの例を示します。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 ip 10.21.8.10
Device(config-if)# glbp 10 load-balancing host-dependent
```

関連コマンド

コマンド	説明
show glbp	GLBP の情報を表示します。

glbp name

Gateway Load Balancing Protocol（GLBP）グループに名前を割り当てて IP 冗長性を有効にするには、インターフェイス コンフィギュレーション モードで**glbp name** コマンドを使用します。グループの IP 冗長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。

glbp *group-number* **name** *group-name*
no glbp *group-number* **name** *group-name*

構文の説明

group-number	GLBP グループ番号。指定できる値の範囲は 0 ～ 1023 です。
group-name	文字列で指定された GLBP グループ名。文字数は最大で 255 です。

コマンド デフォルト

グループの IP 冗長性は無効になっています。

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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが導入されました。

使用上のガイドライン

冗長クライアントと GLBP グループを接続できるように、GLBP 冗長クライアントに同じ GLBP グループ名を設定する必要があります。

例

次に、GLBP グループ 10 に abccomp 名を割り当てる例を示します。

```
Device(config-if)# glbp 10 name abccomp
```

関連コマンド

コマンド	説明
glbp authentication	GLBP に認証ストリングを設定します。
glbp forwarder preempt	デバイスの優先順位が現在の AVF より高い場合、デバイスが GLBP グループの AVF として引き継がれるように設定します。
glbp ip	GLBP を有効にします。
glbp load-balancing	GLBP のアクティブ仮想ゲートウェイ（AVG）によって使用されるロード バランシング方式を指定します。
glbp preempt	ゲートウェイの優先順位が現在の AVG より高い場合、ゲートウェイが GLBP グループの AVG として引き継がれるように設定します。
glbp priority	GLBP グループ内のゲートウェイのプライオリティ レベルを設定します。
glbp timers	GLBP ゲートウェイによって送信される hello パケット間の時間、および仮想ゲートウェイと仮想フォワーダの情報が有効と見なされる時間を設定します。
glbp timers redirect	GLBP グループの AVG がセカンダリ AVF にクライアントをリダイレクトし続ける時間を設定します。
glbp weighting	GLBP ゲートウェイの最初の重み値を指定します。
glbp weighting track	GLBP の重み値の変更がトラッキングされるオブジェクトの可用性に基づいているトラッキング オブジェクトを指定します。
show glbp	GLBP の情報を表示します。
track	GLBP 重み付けの変更がインターフェイスの状態に基づいている場合、インターフェイスをトラッキングするように設定します。

glbp preempt

現在のアクティブ仮想ゲートウェイ（AVG）よりも優先順位の高いゲートウェイがある場合、そのゲートウェイが Gateway Load Balancing Protocol（GLBP）グループの AVG を引き継ぐように設定するには、インターフェイス コンフィギュレーション モードで **glbp preempt** 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。

glbp *group* **preempt** [**delay minimum** *seconds*]
no glbp *group* **preempt** [**delay minimum**]

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。

delay minimum *seconds*	（任意）デバイスが AVG の役割を引き継ぐ前に遅延する最小秒数を指定します。範囲は 0 ～ 3600 秒です。デフォルトの遅延時間は 30 秒です。

コマンド デフォルト

現在の AVG よりも優先順位の高い GLBP ゲートウェイが、AVG の役割を引き継ぐことはできません。デフォルトの遅延時間は 30 秒です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが導入されました。

例

次に、デバイスの優先順位が 254 で、現在の AVG よりも優先順位が高い場合に、そのデバイスが現在の AVG をプリエンプション処理するように設定する例を示します。デバイスが現在の AVG をプリエンプション処理する場合、デバイスは、AVG の役割を引き継ぐ前に 60 秒間待ちます。

```
Device(config-if)# glbp 10 preempt delay minimum 60
Device(config-if)# glbp 10 priority 254
```

関連コマンド

コマンド	説明
glbp ip	GLBP をイネーブルにします。
glbp priority	GLBP グループ内のデバイスの優先度レベルを設定します。

glbp priority

Gateway Load Balancing Protocol（GLBP）グループ内のゲートウェイの優先度レベルを設定するには、インターフェイス コンフィギュレーション モードで **glbp priority** コマンドを使用します。ゲートウェイの優先度レ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。

glbp *group* **priority** *level*
no glbp *group* **priority** *level*

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
level	GLBP グループ内のゲートウェイのプライオリティ。範囲は 1 ～ 255 です。デフォルトは 100 です。

コマンド デフォルト

GLBP 仮想ゲートウェイのプリエンプション スキームは無効になっています。

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（config-if）

使用上のガイドライン

アクティブ仮想ゲートウェイ（AVG）になる仮想ゲートウェイを制御するには、このコマンドを使用します。異なる複数の仮想ゲートウェイの優先順位を比較した後、優先順位の数値が高いゲートウェイが AVG として選択されます。2 つの仮想ゲートウェイの優先順位が等しい場合、優先順位の高い IP アドレスが選択されます。

例

次に、仮想ゲートウェイを 254 の優先順位に設定する例を示します。

```
Device(config-if)# glbp 10 priority 254
```

関連コマンド

コマンド	説明
glbp ip	GLBP をイネーブルにします。
glbp preempt	現在の AVG よりも優先順位の高いデバイスがある場合、そのデバイスが GLBP グループの AVG を引き継ぐように設定します。

glbp timers

Gateway Load Balancing Protocol（GLBP）ゲートウェイにより送信される hello パケットの時間間隔、および仮想ゲートウェイと仮想フォワーダ情報が有効と見なされる時間を設定するには、インターフェイス コンフィギュレーション モードで **glbp timers** コマンドを使用します。タイマーをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

glbp *group* **timers** {*hellotime*{*holdtime* | **msec** *holdtime*} | **msec** { *holdtime* | **msec** *holdtime*} | **redirect** *time-interval-to-redirect* | *timeout*}
no glbp *group* **timers** {*hellotime*{*holdtime* | **msec** *holdtime*} | **msec** { *holdtime* | **msec** *holdtime*} | **redirect** *time-interval-to-redirect* | *timeout*}

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
msec	（任意）下記の（*hellotime* または *holdtime*）引数値をミリ秒で表すように指定します。
hellotime	hello 間隔デフォルトは 3 秒（3000 ミリ秒）です。
holdtime	hello パケットに含まれる仮想ゲートウェイおよび仮想フォワーダの情報が無効と見なされるまでの時間。デフォルトは 10 秒（10,000 ミリ秒）です。
redirect	Gateway Load Balancing Protocol（GLBP）グループのアクティブ仮想ゲートウェイ（AVG）が継続してクライアントをセカンダリ アクティブ仮想フォワーダ（AVF）にリダイレクトする時間間隔を指定します。

time-interval-to-redirect	リダイレクト タイマーの間隔は、0 ～ 3600 秒の範囲内です。デフォルトは 600 秒（10 分）です。 （注） *time-interval-to-redirect* 引数のゼロ（0）値は、指定できる値の範囲から除外することはできません。Cisco IOS ソフトウェアの事前設定でゼロ（0）値を使用しているため、アップグレードに悪影響を及ぼすことになります。ただし、ゼロ（0）値に設定することは推奨しません。*time-interval-to-redirect* にこの値を使用すると、リダイレクトタイマーが期限切れになりません。リダイレクトタイマーが期限切れにならず、デバイスに障害が発生すると、新しいホストがバックアップへリダイレクトされずに、障害が発生したデバイスに引き続き割り当てられます。
timeout	セカンダリ仮想フォワーダが使用できなくなるまでの 600 秒から 64,800 秒の範囲の時間間隔。デフォルトは 14,400 秒（4 時間）です。

コマンド デフォルト

GLBP タイマーはデフォルト値に設定されています。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが導入されました。

使用上のガイドライン

タイマー値が設定されていないデバイスは、アクティブ仮想ゲートウェイ（AVG）からタイマー値を取得できます。AVG 上に設定されているタイマーは、他のすべてのタイマー設定を常に上書きします。GLBP グループ内のすべてのデバイスが同じタイマー値を使用するようにしてください。GLBP ゲートウェイが hello メッセージを送信した場合、その情報は 1 ホールドタイムの間有効と見なされます。通常、保留時間は hello タイムの値の 3 倍より大きくします（*holdtime* > 3 * *hellotime*）。保留時間の値の範囲によって、hello タイムより大きい保留時間が強制されます。

例

次に、GigabitEthernet インターフェイス 1/0/1 の GLBP グループ 10 の hello パケットの間隔を 5 秒に設定し、仮想ゲートウェイとバーチャル フォワーダの情報が無効と見なされる時間を 18 秒に設定する例を示します。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 ip
Device(config-if)# glbp 10 timers 5 18
```

関連コマンド

コマンド	説明
glbp ip	GLBP を有効にします。

コマンド	説明
show glbp	GLBPの情報を表示します。

glbp weighting

Gateway Load Balancing Protocol（GLBP）ゲートウェイの初期重み値を指定するには、インターフェイス コンフィギュレーション モードで **glbp weighting** 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。

glbp *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]
no glbp *group* **weighting**

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
maximum	1 ～ 254 の範囲の最大重み値。デフォルト値は 100 です。
lower *lower*	（任意）1 から指定された最大重み値までの範囲で重み値の下限を指定します。デフォルト値は 1 です。
upper *upper*	（任意）重み値の下限から最大重み値までの範囲で重み値の上限を指定します。デフォルト値は指定された最大重み値です。

コマンド デフォルト

デフォルトのゲートウェイ重み値は 100 で、デフォルトの下限重み値は 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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが導入されました。

使用上のガイドライン

仮想ゲートウェイの重み値は、ゲートウェイの転送能力の指標です。デバイス上の追跡対象インターフェイスに障害が発生し、そのデバイスの重み値が最大値から下限しきい値を下回るまで減ると、デバイスは仮想フォワーダとしての役割を放棄します。デバイスの重み値が上限しきい値を上回るまで増えると、デバイスは仮想フォワーダのアクティブな役割を再開できます。

トラッキング対象となるインターフェイスのパラメータを設定するには、**glbp weighting track** および **track** コマンドを使用します。デバイスのインターフェイスがダウンすると、デバイスの重み値が指定された値まで減少する場合があります。

例

次に、GLBP グループ 10 のゲートウェイの重み値を、重み値の下限を 95 に、重み値の上限を105 に、最大値を 110 に設定する例を示します。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
```

関連コマンド

Command	Description
glbp weighting track	GLBP ゲートウェイの重み付けに影響する、追跡対象のオブジェクトを指定します。
track	追跡対象インターフェイスを設定します。

glbp weighting track

トラッキング対象オブジェクトの可用性に基づいて Gateway Load Balancing Protocol（GLBP）の重み値が増減するようにトラッキング対象オブジェクトを指定するには、インターフェイス コンフィギュレーション モードで **glbp weighting track** コマンドを使用します。トラッキングを削除するには、このコマンドの **no** 形式を使用します。

glbp *group* **weighting track** *object-number* [**decrement** *value*]
no glbp *group* **weighting track** *object-number* [**decrement** *value*]

構文の説明

group	0 ～ 1023 の範囲の GLBP グループ番号。
object-number	トラッキング対象オブジェクトを表すオブジェクト番号。有効な範囲は 1 ～ 1000 です。トラッキング対象オブジェクトを設定するには、**track** コマンドを使用します。
decrement *value*	（任意）インターフェイスがダウン（または復旧）したときにデバイスの GLBP の重み値を減らす（または増やす）量を指定します。値の範囲は 1 ～ 254 です。デフォルト値は 10 です。

コマンド デフォルト

GLBP の重み値の変更時に、オブジェクトはトラッキングされません。

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 Release 2.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、GLBP ゲートウェイの重み値とゲートウェイ インターフェイスの可用性を関連付けます。これは、GLBP に設定されてないインターフェイスをトラッキングする場合に便利です。

トラッキング対象のインターフェイスがダウンすると、GLBP ゲートウェイの重み値は 10 減少します。インターフェイスがトラッキングされない場合、インターフェイスの状態の変化は GLBP ゲートウェイの重み値に影響しません。GLBP グループごとに、トラッキング対象インターフェイスの個別のリストを設定できます。

オプションの *value* 引数は、トラッキング対象のインターフェイスがダウンした場合に GLBP ゲートウェイの重み値をどれだけデクリメントするかを指定します。トラッキング対象インターフェイスが稼働状態に戻ると、重み値は同じ分だけ増加します。

複数の追跡対象インターフェイスがダウンすると、それぞれに設定されている重みの減分値が累計されます。

各インターフェイスをトラッキング対象に設定するには、**track** コマンドを使用します。

最大 1000 のオブジェクトを追跡できます。トラッキング対象オブジェクトは 1000 個設定できますが、各トラッキング対象オブジェクトは CPU リソースを使用します。デバイスで使用可能な CPU リソースの合計は、トラフィック負荷などの変数や、他のプロトコルがどのように設定され実行されているかに応じて異なります。1000 個の追跡対象オブジェクトが使用できるかどうかは、使用可能な CPU によって異なります。特定のサイト トラフィック条件下でサービスが機能することを保証するには、サイト上でテストを実施する必要があります。

例

この例では、GigabitEthernet インターフェイス 1/0/1 で、番号の 1 と 2 で表される 2 つのインターフェイスがトラッキングされることを示します。インターフェイス 1 がダウンすると、GLBP ゲートウェイ重み付けがデフォルト値の 10 だけ減算されます。インターフェイス 2 がダウンすると、GLBP ゲートウェイ重み付けが 5 だけ減算されます。

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting track 1
Device(config-if)# glbp 10 weighting track 2 decrement 5
```

関連コマンド

Command	Description
glbp weighting	GLBP ゲートウェイの初期重み値を指定します。
track	追跡対象インターフェイスを設定します。

ip address dhcp

DHCP からインターフェイスの IP アドレスを取得するには、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 dhcp** コマンドを使用します。取得されたいずれかの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。

ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]
no ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

構文の説明

client-id	（任意）クライアント ID を指定します。デフォルトでは、クライアント識別子は ASCII 値です。**client-id** *interface-type number* オプションは、クライアント識別子を、指定されたインターフェイスの 16 進数 MAC アドレスに設定します。
interface-type	（任意）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	（任意）インターフェイスまたはサブインターフェイスの番号です。ネットワーキング デバイスに対する番号付け構文の詳細については、疑問符（?）のオンライン ヘルプ機能を使用してください。
hostname	（任意）ホスト名を指定します。
hostname	（任意）ホスト名を DHCP オプション 12 フィールドに配置します。この名前は、グローバル コンフィギュレーション モードで入力されたホスト名と同じにする必要はありません。

コマンド デフォルト

ホスト名は、デバイスのグローバル コンフィギュレーション ホスト名です。クライアント識別子は ASCII 値です。

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）

使用上のガイドライン

ip address dhcp コマンドを使用すると、インターフェイスは DHCP プロトコルを使用して IP アドレスを動的に学習できます。これはインターネット サービス プロバイダー（ISP）に動的に接続するイーサネット インターフェイスで特に役立ちます。このインターフェイスにダイナミック アドレスを割り当てると、同インターフェイスを使用して、Cisco IOS ネットワーク アドレス変換（NAT ）のポート アドレス変換（PAT）で、デバイスに接続済みの個別に処理されたネットワークにインターネット アクセスを提供できます。

また **ip address dhcp** コマンドは、ATM ポイントツーポイント インターフェイスと連動し、どのカプセル化方式でも受け入れます。ただし、ATM マルチポイント インターフェイスの場合、**protocol ip inarp** インターフェイス コンフィギュレーション コマンドで Inverse ARP を指定し、aa15snap カプセル化タイプのみを使用する必要があります。

一部の ISP の場合、DHCPDISCOVER メッセージに、特定のホスト名と、インターフェイスの MAC アドレスであるクライアント識別子を含める必要があります。**ip address dhcp client-id** *interface-type number* **hostname** *hostname* コマンドは、*interface-type* が、このコマンドが設定されたイーサネット インターフェイスであり、*interface-type number* が ISP によって提供されたホスト名である場合に最も一般的に使用されます。

クライアント識別子（DHCP オプション 61）には、16 進数または ASCII 値を使用できます。デフォルトでは、クライアント識別子は ASCII 値です。**client-id** *interface-type number* オプションは、デフォルトの値を上書きし、指定されたインターフェイスの 16 進数 MAC アドレスの使用を強制します。

DHCP サーバから IP アドレスを取得するようシスコ デバイスが設定されている場合、デバイスは、ネットワークの DHCP サーバにデバイスに関する情報を提供する DHCPDISCOVER メッセージを送信します。

ip address dhcp コマンドを使用する場合、オプションキーワードの有無にかかわらず、DHCP オプション 12 フィールド（ホスト名オプション）が DISCOVER メッセージに含められます。デフォルトでは、オプション 12 で指定されたホスト名は、デバイスのグローバル コンフィギュレーション ホスト名になります。ただし、**ip address dhcp hostname** *hostname* コマンドを使用して、デバイスのグローバル コンフィギュレーション ホスト名ではない別の名前を DHCP オプション 12 フィールドに入力することもできます。

no ip address dhcp コマンドは、取得済みの IP アドレスを削除して、DHCPRELEASE メッセージを送信します。

DHCP サーバで必要なものを判別するため、さまざまな設定を試行しなければならない場合があります。下の表に、使用可能なコンフィギュレーション方式と、各方式の DISCOVER メッセージに含まれる情報を示します。

表 *18* : コンフィギュレーション方式と生成される *DISCOVER* メッセージの内容

コンフィギュレーション方式	DISCOVER メッセージの内容
ip address dhcp	DISCOVER メッセージのクライアント ID フィールドには「cisco-*mac-address* -Eth1」が含まれます。*mac-address* は、イーサネット 1 インターフェイスの MAC アドレスで、オプション 12 フィールドのデバイスのデフォルト ホスト名を含んでいます。
ip address dhcp hostname *hostname*	DISCOVER メッセージのクライアント ID フィールドには「cisco-*mac-address* -Eth1」が含まれます。*mac-address* は、イーサネット 1 インターフェイスの MAC アドレスで、オプション 12 フィールドの *hostname* を含んでいます。
ip address dhcp client-id ethernet 1	DISCOVER メッセージは、クライアント ID フィールドにイーサネット 1 インターフェイスの MAC アドレスを含んでおり、オプション 12 フィールドにデバイスのデフォルト ホスト名を含んでいます。
ip address dhcp client-id ethernet 1 hostname *hostname*	DISCOVER メッセージは、クライアント ID フィールドにイーサネット 1 インターフェイスの MAC アドレスを含んでおり、オプション 12 フィールドに *hostname* を含んでいます。

例

次の例では、**ip address dhcp** コマンドがイーサネット インターフェイス 1 に入力されます。次の例のように設定されたデバイスによって送信された DISCOVER メッセージには、クライアント ID フィールドの「cisco- *mac-address* -Eth1」と、オプション 12 フィールドの値 abc が含まれます。

```
hostname abc
```

```
!
interface GigabitEthernet 1/0/1
 ip address dhcp
```

次の例のように設定されたデバイスによって送信されたDISCOVERメッセージには、クライアントIDフィールドの「cisco- mac-address -Eth1」と、オプション12フィールドの値defが含まれます。

```
hostname abc
!
interface GigabitEthernet 1/0/1
 ip address dhcp hostname def
```

次の例のように設定されたデバイスによって送信されたDISCOVERメッセージには、クライアントIDフィールドのイーサネットインターフェイス1のMACアドレスと、オプション12フィールドの値abcが含まれます。

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1
```

次の例のように設定されたデバイスによって送信されたDISCOVERメッセージには、クライアントIDフィールドのイーサネットインターフェイス1のMACアドレスと、オプション12フィールドの値defが含まれます。

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1 hostname def
```

関連コマンド

コマンド	説明
ip dhcp pool	Cisco IOS DHCP サーバに DHCP アドレス プールを設定し、DHCP プール コンフィギュレーション モードを開始します。

ip address pool (DHCP)

Dynamic Host Configuration Protocol（DHCP）に IP Control Protocol （IPCP）ネゴシエーションからサブネットが入力されるときに、インターフェイスの IP アドレスが自動設定されるようにするには、インターフェイス コンフィギュレーション モードで **ip address pool** コマンドを使用します。インターフェイスの IP アドレスの自動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。

ip address pool *name*
no ip address pool

構文の説明

name	DHCP プールの名前。インターフェイスの IP アドレスは、*name* で指定された DHCP プールから自動設定されます。

コマンド デフォルト

IP アドレスのプーリングは無効になっています。

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

使用上のガイドライン

デバイスのDHCPプールによって処理する必要のある LAN に接続されている DHCP クライアントが存在する場合、このコマンドを使用して LAN インターフェイスの IP アドレスを自動設定します。DHCP プールは、IPCP サブネット ネゴシエーションによってサブネットを動的に取得します。

例

次の例では、GigabitEthernet インターフェイス 1/0/1 の IP アドレスが abc という名前のアドレス プールから自動設定されるように指定します。

```
ip dhcp pool abc
  import all
  origin ipcp
!
interface GigabitEthernet 1/0/1
  ip address pool abc
```

関連コマンド

コマンド	説明
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。

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 Release 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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。

インターフェイスで IP を透過的にブリッジする前に、次の手順を実行する必要があります。

- IP ルーティングを無効にします（**no ip routing** コマンドを指定します）。
- インターフェイスをブリッジ グループに追加して、**bridge-group** コマンドを参照してください。

インターフェイスで IP のルーティングと透過的なブリッジングを同時に実行するには、**bridge crb** コマンドを参照してください。

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。

```
interface GigabitEthernet 1/0/1
 ip address 192.108.1.27 255.255.255.0
 ip address 192.31.7.17 255.255.255.0 secondary
```

関連コマンド

Command	Description
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。

Command	Description
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 http server

Cisco Web ブラウザのユーザ 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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、HTTP サーバへの 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 サーバとセキュア HTTP（HTTPS）サーバは、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 サーバをイネーブルにする例を示します。

HTTP サーバを有効にした後は、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 サーバをイネーブルにします。

ip http secure-server

セキュア HTTP（HTTPS）サーバを有効にするには、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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

HTTPS サーバは、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 インターフェイスを含む IP または IPv6 システムで HTTP サーバを有効にします。
show ip http server secure status	HTTPS サーバの設定ステータスを表示します。

ip nhrp map

ノンブロードキャスト マルチアクセス（NBMA）ネットワークに接続された IP 宛先の IP と NBMA 間のアドレスマッピングをスタティックに設定するには、インターフェイス コンフィギュレーション モードで **ip nhrp map** コマンドを使用します。Next Hop Resolution Protocol（NHRP）キャッシュからスタティックエントリを削除するには、このコマンドの **no** 形式を使用します。

ip nhrp map *ip-address* {*ip-nbma-address* | *destination-mask* [{*ip-nbma-address ipv6-nbma-address*}] *ipv6-nbma-address*}
no ip nhrp map *ip-address* {*ip-nbma-address* | *destination-mask* [{*ip-nbma-address ipv6-nbma-address*}] *ipv6-nbma-address*}

構文の説明

ip-address	NBMA ネットワーク経由で到達可能な宛先の IP アドレス。このアドレスは、NBMA アドレスにマッピングされます。
ip-nbma-address	NBMA ネットワーク経由で直接到達可能な NBMA アドレス。アドレス形式はメディアによって異なります。たとえば、ATM にはネットワーク サービス アクセス ポイント（NSAP）アドレスがあり、イーサネットには MAC アドレスがあり、Switched Multimegabit Data Service（SMDS; スイッチドマルチメガビット データ サービス）には E.164 アドレスがあります。このアドレスは、IP アドレスにマッピングされます。
destination-mask	宛先アドレス マスク。
ipv6-nbma-address	IPv6 NBMA アドレス。 （注） この引数は、Cisco IOS XE Denali 16.3.1 ではサポートされていません。

コマンド デフォルト

スタティック IP-to-NBMA キャッシュは存在しません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

Cisco IOS XE Denali 16.3.1 では、NHRP はハブ/スポーク間通信のみをサポートし、スポーク間通信はサポートされていません。

（注） Cisco IOS XE Denali 16.3.1 では、このコマンドは IPv4 だけをサポートしています。*ipv6-nbma-address* 引数は、スイッチでは使用可能ですが、設定しても機能しません。

ネクストホップ サーバに到達するには、少なくとも 1 つのスタティック マッピングを設定します。統計的に複数の IP-to-NBMA アドレス マッピングを設定するには、このコマンドを複数回設定します。

ルーティング プロトコル、Open Shortest Path First（OSPF）または Enhanced Interior Gateway Routing Protocol（EIGRP）を使用している場合は、トラフィックを許可するトンネルで、**ip ospf network point-to-multipoint** コマンド（OSPF がハブ/スポーク通信に使用されている場合）および **ip split-horizon eigrp** コマンド（EIGRP が使用されている場合）を設定します。

例

次に、マルチポイント トンネル ネットワーク内のこのステーションが 2 つのネクスト ホップ サーバ 10.0.0.1 と 10.0.1.3 によってサービス提供されるようにスタティックに設定する例を示します。10.0.0.1 の NBMA アドレスは 192.0.2.1 としてスタティックに設定され、10.0.1.3 の NBMA アドレスは 198.51.100.1 です。

```
Switch(config)# interface tunnel 0
Switch(config-if)# ip nhrp nhs 10.0.0.1
Switch(config-if)# ip nhrp nhs 10.0.1.3
Switch(config-if)# ip nhrp map 10.0.0.1 192.0.2.1
Switch(config-if)# ip nhrp map 10.0.1.3 198.51.100.1
```

関連コマンド

Command	Description
clear ip nhrp	NHRP キャッシュからすべてのダイナミック エントリを削除します。
debug nhrp	NHRP デバッグをイネーブルにします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ip split-horizon eigrp	EIGRP スプリット ホライズンを有効にします。
ip ospf network point-to-multipoint	OSPF ネットワーク タイプをポイントツーマルチポイントに設定します。

ip nhrp map multicast

トンネルネットワーク経由で送信されるブロードキャストまたはマルチキャストパケットの宛先として使用されるノンブロードキャスト マルチアクセス（NBMA）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 nhrp map multicast** コマンドを使用します。宛先を削除するには、このコマンドの **no** 形式を使用します。

ip nhrp map multicast {*ip-nbma-address ipv6-nbma-address* | **dynamic**}
no ip nhrp map multicast {*ip-nbma-address ipv6-nbma-address* | **dynamic**}

構文の説明

ip-nbma-address	NBMA ネットワーク経由で直接到達可能な NBMA アドレス。アドレス形式は、使用しているメディアによって異なります。
ipv6-nbma-address	IPv6 NBMA アドレス。 （注） この引数は、Cisco IOS XE Denali 16.3.1 ではサポートされていません。
dynamic	ハブのクライアント登録から宛先をダイナミックに学習します。

コマンド デフォルト

NBMA アドレスは、ブロードキャストまたはマルチキャスト パケットの宛先として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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

（注） Cisco IOS XE Denali 16.3.1 では、このコマンドは IPv4 だけをサポートしています。*ipv6-nbma-address* 引数は、スイッチでは使用可能ですが、設定しても機能しません。

このコマンドは、トンネルインターフェイスだけに適用されます。このコマンドは、基盤となるネットワークが IP マルチキャストをサポートしていない場合に、トンネル ネットワーク経由でブロードキャストをサポートするために役立ちます。基盤となるネットワークが IP マルチキャストをサポートしている場合は、**tunnel destination** コマンドを使用して、トンネルブロードキャストまたはマルチキャストを伝送するためのマルチキャスト宛先を設定する必要があります。

複数の NBMA アドレスが設定されている場合、システムはアドレスごとにブロードキャストパケットを複製します。

例

次に、パケットが 10.255.255.255 に送信される場合に、宛先 10.0.0.1 と 10.0.0.2 に対してパケットが複製される例を示します。

```
Switch(config)# interface tunnel 0
Switch(config-if)# ip address 10.0.0.3 255.0.0.0
Switch(config-if)# ip nhrp map multicast 10.0.0.1
Switch(config-if)# ip nhrp map multicast 10.0.0.2
```

関連コマンド

コマンド	説明
debug nhrp	NHRP デバッグをイネーブルにします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
tunnel destination	トンネル インターフェイスの宛先を指定します。

ip nhrp network-id

インターフェイスの Next Hop Resolution Protocol（NHRP）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 nhrp network-id** コマンドを使用します。インターフェイスで NHRP 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 nhrp network-id *number*
no ip nhrp network-id [{*number*}]

構文の説明

number	ノンブロードキャスト マルチアクセス（NBMA）ネットワークからのグローバルに一意な 32 ビット ネットワーク識別子。範囲は 1 ～ 4294967295 です。

コマンド デフォルト

NHRP はインターフェイスで無効になっています。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

一般に、論理 NBMA ネットワーク内のすべての NHRP ステーションは、同じネットワーク ID を使用して設定する必要があります。

例

次に、インターフェイスで NHRP を有効にする例を示します。

```
Switch(config-if)# ip nhrp network-id 1
```

関連コマンド

コマンド	説明
clear ip nhrp	NHRP キャッシュからすべてのダイナミック エントリを削除します。
debug nhrp	NHRP デバッグをイネーブルにします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

ip nhrp nhs

1 つ以上の Next Hop Resolution Protocol（NHRP）サーバのアドレスを指定するには、インターフェイス コンフィギュレーション モードで **ip nhrp nhs** コマンドを使用します。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。

ip nhrp nhs {*nhs-address* [**nbma** {*nbma-address FQDN-string*}] [**multicast**] [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value* | **dynamic nbma** {*nbma-address FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] | **fallback** *seconds*}
no ip nhrp nhs {*nhs-address* [**nbma** {*nbma-address FQDN-string*}] [**multicast**] [**priority** *value*] [**cluster** *value*] | **cluster** *value* **max-connections** *value* | **dynamic nbma** {*nbma-address FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] | **fallback** *seconds*}

構文の説明

nhs-address	指定されているネクストホップ サーバのアドレス。
nbma	（任意）ノンブロードキャスト マルチアクセス（NBMA）アドレスまたは FQDN を指定します。
nbma-address	NBMA アドレス。
FQDN-string	ネクスト ホップ サーバ（NHS）の完全修飾ドメイン名（FQDN）文字列。
multicast	（任意）ブロードキャストおよびマルチキャストに NBMA マッピングを使用することを指定します。
priority *value*	（任意）ハブに優先順位を割り当てて、トンネルを確立するためにスポークがハブを選択する順序を制御します。指定できる範囲は 0 ～ 255 で、0 は最高の優先順位、255 は最低の優先順位です。
cluster *value*	（任意）NHS グループを指定します。範囲は 0 ～ 10 です。
max-connections *value*	アクティブにする必要がある各 NHS グループの NHS 要素の数を指定します。有効な範囲は 0 ～ 255 です。
dynamic	NHS プロトコル アドレスをダイナミックに学習するようにスポークを設定します。
fallback *seconds*	リカバリ時により優先順位の高い NHS にフォール バックする前にスポークが待機する必要のある期間を秒単位で指定します。

コマンド デフォルト

ネクストホップ サーバは明示的に設定されていないため、通常のネットワーク層のルーティング決定が NHRP トラフィックの転送に使用されます。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

ネクストホップサーバのアドレスとそれがサービスを提供するネットワークを指定するには、**ip nhrp nhs** コマンドを使用します。通常、NHRP は、ネットワーク層転送テーブルを使用して、NHRP パケットの転送方法を決定します。ネクストホップ サーバが設定されている場合

は、これらのネクストホップ アドレスの方が、通常 NHRP トラフィック向けに使用されている転送パスより優先されます。

設定されたネクスト ホップサーバに対して、同じ *nhs-address* 引数と異なる IP ネットワークアドレスを使用して **ip nhrp nhs** コマンドを繰り返すことで、複数のネットワークを指定できます。

例

次に、NBMA と FQDN を使用してハブをスポークに登録する例を示します。

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs 192.0.2.1 nbma examplehub.example1.com
```

次に、目的の **max-connections** 値を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs cluster 5 max-connections 100
```

次に、NHS フォールバック時間を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs fallback 25
```

次に、NHS 優先順位とグループ値を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs 192.0.2.1 priority 1 cluster 2
```

関連コマンド

コマンド	説明
ip nhrp map	NBMA ネットワークに接続された IP 宛先の IP-to-NBMA アドレス マッピングをスタティックに設定します。
show ip nhrp	NHRP マッピング情報を表示します。

ipv6 address-validate

IPv6 アドレス検証をイネーブルにするには、グローバル コンフィギュレーション モードで **ipv6 address-validate** を使用します。IPv6 アドレス検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。

ipv6 address-validate
no ipv6 address-validate

コマンド デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

ipv6 address-validate コマンドは、割り当てられた IPv6 アドレスのインターフェイス識別子が RFC5453 で規定されている予約済み IPv6 インターフェイス識別子の範囲に含まれていないかどうかを検証するために使用します。割り当てられた IPv6 アドレスのインターフェイス識別子が予約済みの範囲に含まれている場合は、新しい IPv6 アドレスが割り当てられます。

検証されるのは、自動設定されたアドレスと DHCPv6 によって設定されたアドレスのみです。

（注） **no ipv6-address validate** コマンドを使用すると、IPv6 アドレス検証がディセーブルになり、予約済み IPv6 インターフェイス識別子の範囲に含まれるインターフェイス識別子を使用した IPv6 アドレスの割り当てが可能になります。このコマンドを使用することは推奨しません。

例

次に、IPv6 アドレス検証が no ipv6-address validate コマンドを使用してディセーブルにされた場合に再度イネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 address-validate
```

ipv6 nd cache expire

IPv6 ネイバー探索のキャッシュエントリの有効期限が切れるまでの時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd cache expire** 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。

ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]
no ipv6 nd cache expire *expire-time-in-seconds* [**refresh**]

構文の説明

構文の説明

expire-time-in-seconds	時間の範囲は 1 ～ 65,536 秒です。デフォルトは 14,400 秒、つまり 4 時間です。
refresh	（任意）ネイバー探索キャッシュエントリを自動的に更新します。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

コマンド履歴

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

使用上のガイドライン

デフォルトでは、14,400 秒間、つまり 4 時間にわたって STALE 状態が続いた場合は、ネイバー探索キャッシュエントリの有効期限が切れて削除されます。**ipv6 nd cache expire** コマンドを使用すると、有効期限を変更したり、エントリが削除される前に期限切れのエントリの自動更新をトリガーすることができます。

refresh キーワードを使用すると、ネイバー探索キャッシュエントリが自動更新されます。エントリは DELAY 状態に移行し、ネイバー到達不能検出プロセスが実行され、5 秒後にエントリは DELAY 状態から PROBE 状態に遷移します。エントリが PROBE 状態に到達すると、ネイバー送信要求が送信され、設定に従って再送信されます。

例

次に、ネイバー探索キャッシュエントリが 7,200 秒（2 時間）で期限が切れるように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd cache expire 7200
```

関連コマンド

コマンド	説明
ipv6 nd na glean	非送信要求ネイバー アドバタイズメントからエントリを収集するネイバー探索を設定します。
ipv6 nd nud retry	ネイバー到達不能検出でネイバー送信要求を再送信する回数を設定します。
show ipv6 interface	IPv6 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。

ipv6 nd na glean

非送信要求ネイバーアドバタイズメントからエントリを収集するようにネイバー探索を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd na glean** 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。

ipv6 nd na glean
no ipv6 nd na glean

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

重複アドレス検出（DAD）が正常に完了すると、IPv6 ノードからマルチキャスト非送信要求ネイバー アドバタイズメント パケットが発行されることがあります。デフォルトでは、これらの非送信要求ネイバー アドバタイズメント パケットは他の IPv6 ノードから無視されます。**ipv6 nd na glean** コマンドは、非送信要求ネイバー アドバタイズメント パケットの受信時にルータでネイバー アドバタイズメント エントリを作成するように設定します（これらのエントリがまだ存在せず、ネイバーアドバタイズメントにリンク層アドレスオプションがある場合）。このコマンドを使用すると、データトラフィックをネイバーと交換する前に、デバイスのネイバーアドバタイズメントキャッシュにネイバーのエントリを読み込むことができます。

例

次に、非送信要求ネイバーアドバタイズメントからエントリを収集するようにネイバー探索を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd na glean
```

関連コマンド

コマンド	説明
ipv6 nd cache expire	IPv6 ネイバー探索キャッシュエントリの期限が切れるまでの時間を設定します。
ipv6 nd nud retry	ネイバー到達不能検出でネイバー送信要求を再送信する回数を設定します。
show ipv6 interface	IPv6 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。

ipv6 nd nud retry

ネイバー到達不能検出プロセスでネイバー送信要求を再送信する回数を設定するには、インターフェイスコンフィギュレーションモードで **ipv6 nd nud retry** 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。

ipv6 nd nud retry *base interval max-attempts* {*final-wait-time*}
no ipv6 nd nud retry *base interval max-attempts* {*final-wait-time*}

構文の説明

base	ネイバー到達不能検出プロセスのベース値。
間隔	再試行の時間間隔（ミリ秒）。 有効な範囲は 1000 ～ 32000 です。

max-attempts	再試行の最大回数（ベース値に依存）。 有効な範囲は 1 ～ 128 です。
final-wait-time	最後のプローブの待機時間（ミリ秒）。 有効な範囲は 1000 ～ 32000 です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

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

使用上のガイドライン

ネイバーのネイバー検出エントリを再度解決するためにデバイスでネイバー到達不能検出を実行する際、ネイバー送信要求パケットが 1 秒間隔で 3 回送信されます。スパニングツリーイベント、トラフィックの多いイベント、エンドホストのリロードなどの特定の状況においては、ネイバー送信要求が 1 秒間隔で 3 回送信されても十分でない場合があります。このような状況でネイバーキャッシュを維持するには、**ipv6 nd nud retry** コマンドを使用してネイバー送信要求の再送信の指数タイマーを設定します。

再試行の最大回数は、*max-attempts* 引数を使用して設定されます。再送信間隔は、次の式で計算されます。

tm^n

各値は次のとおりです。

- t = 時間間隔
- m = ベース（1、2、または 3）
- n = 現在のネイバー送信要求番号（最初のネイバー送信要求が 0）

したがって、**ipv6 nd nud retry 3 1000 5** コマンドは、1、3、9、27、81 秒の間隔で再送信します。最終待機時間が設定されていない場合、エントリは 243 秒後に削除されます。

ipv6 nd nud retry コマンドはネイバー到達不能検出プロセスの再送信レートにのみ影響し、最初の解決には影響しません。最初の解決では、デフォルトに基づいてネイバー送信要求パケットが 1 秒間隔で 3 回送信されます。

例

次に、1 秒の固定間隔で 3 回再送信するように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 1 1000 3
```

次に、再送信間隔を 1、2、4、8 に設定する例を示します。

```
Device> enable
Device# configure terminal
```

```
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 2 1000 4
```

次に、再送信間隔を 1、3、9、27、81 に設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 3 1000 5
```

関連コマンド

コマンド	説明
ipv6 nd cache expire	IPv6 ネイバー探索（ND）キャッシュエントリの期限が切れるまでの時間を設定します。
ipv6 nd na glean	非送信要求ネイバー アドバタイズメントからエントリを収集するネイバー探索を設定します。
show ipv6 interface	IPv6 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。

key chain

ルーティングプロトコルの認証を有効にするために必要な認証キーチェーンを定義して、キーチェーン 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 **key chain** コマンドを使用します。キーチェーンを削除するには、このコマンドの **no** 形式を使用します。

key chain *name-of-chain*
no key chain *name-of-chain*

構文の説明

name-of-chain	キー チェーンの名前。キー チェーンには、少なくとも 1 つのキーを含める必要がありますが、最大 2147483647 個のキーを含めることができます。

コマンド デフォルト

キー チェーンは存在しません。

コマンド モード

グローバル コンフィギュレーション（config）

使用上のガイドライン

認証を有効にするには、キーでキー チェーンを設定する必要があります。

複数のキー チェーンの識別が可能ですが、ルーティング プロトコルごとのインターフェイスごとに 1 つのキー チェーンを使用することを推奨します。**key chain** コマンドを指定すると、キー チェーン コンフィギュレーション モードが開始されます。

例

次に、キー チェーンを指定する例を示します。

```
Device(config-keychain-key)# key-string chestnut
```

関連コマンド

Command	Description
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	キー チェーンの認証キーを識別します。
key-string (authentication)	キーの認証文字列を指定します。
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。
show key chain	認証キーの情報を表示します。

key-string（認証）

キーの認証文字列を指定するには、キーチェーン キー コンフィギュレーション モードで **key-string**（認証）コマンドを使用します。認証文字列を削除するには、このコマンドの **no** 形式を使用します。

key-string key-string *text*
no key-string *text*

構文の説明

text	認証されるルーティング プロトコルを使用してパケットで送信および受信される必要のある認証文字列。文字列には、大文字小文字の英数字 1 ～ 80 文字を含めることができます。

コマンド デフォルト

キーの認証文字列は存在しません。

コマンド モード

キー チェーン キー コンフィギュレーション（config-keychain-key）

例

次に、キーの認証文字列を指定する例を示します。

```
Device(config-keychain-key)# key-string key1
```

関連コマンド

Command	Description
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	キー チェーンの認証キーを識別します。
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。

Command	Description
send-lifetime	キー チェーンの認証キーが有効に送信される期間を設定します。
show key chain	認証キーの情報を表示します。

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

Command	Description
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。

Command	Description
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。

show glbp

Gateway Load Balancing Protocol（GLBP）情報を表示するには、特権 EXEC モードで **show glbp** コマンドを使用します。

capability [*interface-type interface-number*]
interface-type interface-number [*group-number*] [*state*] [**brief**]

構文の説明

capability	（任意）GLBP 機能インターフェイスを表示します。
interface-type interface-number	（任意）出力を表示するインターフェイスのタイプおよび番号
group-number	（任意）0 ～ 1023 の範囲の GLBP グループ番号
state	（任意）次のいずれかの GLBP デバイスの状態：**active**、**disabled**、**init**、**listen**、**standby**
brief	（任意）1行の出力で各仮想ゲートウェイまたは仮想フォワーダの要約を示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが導入されました。

使用上のガイドライン

デバイスの GLBP グループに関する情報を表示するには、**show glbp** コマンドを使用します。**brief** キーワードは、各仮想ゲートウェイまたは仮想フォワーダに関する情報を 1 行で表示します。**capability** キーワードは、すべての GLBP 対応インターフェイスを表示します。

例

次に、GLBP グループ 10 を表示する **show glbp** コマンドからの出力例を示します。

```
Device# show glbp GigabitEthernet 1/0/1 10
GigabitEthernet1/0/1 - Group 10
  State is Active
    1 state change, last state change 00:04:52
```

```
Virtual IP address is 10.21.8.10
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.608 secs
Redirect time 600 sec, forwarder time-out 14400 sec
Preemption disabled
Active is local
Standby is unknown
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
Group members:
  ac7e.8a35.6364 (10.21.8.32) local
There is 1 forwarder (1 active)
Forwarder 1
  State is Active
    1 state change, last state change 00:04:41
  MAC address is 0007.b400.0a01 (default)
  Owner ID is ac7e.8a35.6364
  Redirection enabled
  Preemption enabled, min delay 30 sec
  Active is local, weighting 100
```

下の表で、この出力で表示される重要なフィールドについて説明します。

表 *19 : show glbp* フィールドの説明

フィールド	説明
GigabitEthernet 1/0/1 Group	インターフェイス タイプおよびインターフェイスの GLBP グループ番号。
State is	仮想ゲートウェイまたは仮想フォワーダのステート。仮想ゲートウェイの場合、ステートは次のいずれかになります。 • Active：ゲートウェイはアクティブ仮想ゲートウェイ（AVG）で、仮想 IP アドレスの Address Resolution Protocol（ARP）要求に応答します。 • Disabled：仮想 IP アドレスはまだ設定されていない、または学習されていませんが、別の GLBP 設定が存在します。 • Initial：仮想 IP アドレスは設定されている、または学習されていますが、仮想ゲートウェイの設定が完全ではありません。インターフェイスはアップ状態で、ルート IP に設定されている必要があります。インターフェイス IP アドレスが設定されている必要があります。 • Listen：仮想ゲートウェイは hello パケットを受信し、アクティブまたはスタンバイ仮想ゲートウェイが使用できなくなった場合に Speak ステートに変更できます。 • Speak：仮想ゲートウェイはアクティブまたはスタンバイ仮想ゲートウェイになろうとしています。 • Standby：ゲートウェイは次に AVG になる位置にいます。

フィールド	説明
Virtual IP address is	GLBP グループの仮想 IP アドレス。すべてのセカンダリ仮想 IP アドレスは、1 行ごとに表示されます。仮想 IP アドレスの 1 つが別のデバイスに設定されたアドレスと重複している場合、「duplicate」としてマークされます。重複アドレスは、デバイスが ARP キャッシュ エントリの保護に失敗したことを示します。
Hello time, hold time	Hello timeとは、hello パケット間の時間のことです（秒またはミリ秒単位）。Hold timeとは、他のデバイスがアクティブ ルータのダウンを宣言するまでの時間です（秒またはミリ秒単位）。GLBP グループのすべてのデバイスは、現在の AVG の hello 時間値と保留時間値を使用します。ローカルに設定された値が異なる場合、設定された値が hello 時間値と保留時間値の後ろのカッコ内に表示されます。
Next hello sent in	GLBP が次の hello パケットを送信するまでの時間（秒またはミリ秒単位）。
プリエンプション	GLBP ゲートウェイのプリエンプションがイネーブルであるかどうか。有効な場合、最小遅延は、優先順位の低いアクティブデバイスをプリエンプトするまで、優先順位の高いの非アクティブデバイスが待つ時間です（秒単位）。 このフィールドも、GLBP フォワーダのプリエンプションを示すフォワーダ セクションの下に表示されます。
Active is	仮想ゲートウェイのアクティブ状態。値は「local」、「unknown」、または IP アドレスです。アドレス（およびアドレスの有効期限）は、現在の AVG のアドレスです。 このフィールドも、現在の AVF のアドレスを示すフォワーダ セクションの下に表示されます。
Standby is	仮想ゲートウェイのスタンバイ状態。値は「local」、「unknown」、または IP アドレスです。アドレス（およびアドレスの有効期限）は、スタンバイ ゲートウェイのアドレスです（ゲートウェイは次に AVG になります）。
重み付け	下限しきい値と上限しきい値のある初期重み値。
Track object	追跡対象オブジェクトのリストとそれらに対応する状態。
IP redundancy name is	GLBP グループの名前。

関連コマンド

Command	Description
glbp ip	GLBP をイネーブルにします。

Command	Description
glbp timers	hello メッセージの間隔と、他のデバイスによってアクティブ GLBP デバイスのダウンが宣言されるまでの時間を設定します。
glbp weighting track	GLBP ゲートウェイの重み付けに影響する、追跡対象のオブジェクトを指定します。

show ip nhrp nhs

Next Hop Resolution Protocol（NHRP）ネクストホップサーバ（NHS）情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip nhrp nhs** コマンドを使用します。

show ip nhrp nhs [{*interface*}] [**detail**] [{**redundancy** [{**cluster** *number* | **preempted** | **running** | **waiting**}]}]

構文の説明

interface	（任意）インターフェイスに現在設定されている NHS 情報を表示します。タイプ、番号範囲、説明については、下の表を参照してください。
detail	（任意）詳細な NHS 情報を表示します。
redundancy	（任意）NHS 冗長スタックに関する情報を表示します。
cluster *number*	（任意）冗長クラスタ情報を表示します。
preempted	（任意）アクティブになれず、プリエンプション処理された NHS に関する情報を表示します。
running	（任意）現在「Responding」または「Expecting replies」状態になっている NHS を表示します。
waiting	（任意）スケジュール処理待ち状態の NHS を表示します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

次の表に、任意指定の *interface* 引数の有効なタイプ、番号の範囲、および説明を示します。

（注） 有効なタイプは、プラットフォームとプラットフォーム上のインターフェイスによって異なります。

表 *20*：有効なタイプ、番号の範囲、およびインターフェイスの説明

有効なタイプ	番号の範囲	インターフェイスの説明
ANI	0 ～ 1000	自律型ネットワーク仮想インターフェイス
Auto-Template	1 ～ 999	自動テンプレート インターフェイス
GMPLS	0 ～ 1000	マルチプロトコル ラベル スイッチング（MPLS）インターフェイス
GigabitEthernet	0 ～ 9	GigabitEthernet IEEE 802.3z
InternalInterface	0 ～ 9	内部インターフェイス
LISP	0 ～ 65520	Locator/ID Separation Protocol（LISP）仮想インターフェイス
loopback	0 ～ 2,147,483,647	ループバック インターフェイス
Null	0 ～ 0	ヌル インターフェイス
PROTECTION_GROUP	0 ～ 0	保護グループ コントローラ
Port-channel	1 ～ 128	ポート チャネル インターフェイス
TenGigabitEthernet	0 ～ 9	TenGigabitEthernet インターフェイス
Tunnel	0 ～ 2,147,483,647	トンネル インターフェイス
Tunnel-tp	0 ～ 65535	MPLS トランスポート プロファイル インターフェイス
Vlan	1 ～ 4094	VLAN インターフェイス

例

次に、**show ip nhrp nhs detail** コマンドの出力例を示します。

```
Switch# show ip nhrp nhs detail

Legend:
  E=Expecting replies
  R=Responding
Tunnel1:
   10.1.1.1           E  req-sent 128  req-failed 1  repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 1, Ret 64  NHS 10.1.1.1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *21 : show ip nhrp nhs* のフィールドの説明

フィールド	説明
Tunnel1	ターゲット ネットワークに到達するために経由するインターフェイス。

関連コマンド

コマンド	説明
ip nhrp map	NBMA ネットワークに接続された IP 宛先の IP-to-NBMA アドレス マッピングをスタティックに設定します。
show ip nhrp	NHRP マッピング情報を表示します。

show key chain

キーチェーンを表示するには、**show key chain** コマンドを使用します。

show key chain ［*name-of-chain*］

構文の説明

name-of-chain	（任意）キーチェーン コマンドで命名された表示対象のキー チェーン名。

コマンド デフォルト

パラメータを指定せずにコマンドを使用すると、すべてのキー チェーンのリストを表示します。

コマンド モード

特権 EXEC（#）

例

次に、**show key chain** コマンドの出力例を示します。

```
show key chain
Device# show key chain

Key-chain AuthenticationGLBP:
    key 1 -- text "Thisisasecretkey"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
Key-chain glbp2:
    key 100 -- text "abc123"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
```

関連コマンド

コマンド	説明
key-string	キーの認証文字列を指定します。
send-lifetime	キーチェーンの認証キーが有効に送信される期間を設定します。

show track

トラッキングプロセスが追跡したオブジェクトに関する情報を表示するには、特権EXECモードで **show track** コマンドを使用します。

show track [{*object-number* **[brief]** | **application [brief]** | **interface [brief]** | **ip[route [brief]** | **[sla [brief]]** | **ipv6 [route [brief]]** | **list [route [brief]]** | **resolution [ip** | **ipv6]** | **stub-object [brief]** | **summary** | **timers**}]

構文の説明

object-number	（任意）トラッキング対象オブジェクトを表すオブジェクト番号。範囲は1～1000 です。
brief	（任意）先行する引数やキーワードに関連する 1 行の情報を表示します。
application	（任意）トラッキング対象のアプリケーション オブジェクトを表示します。
interface	（任意）トラッキング対象のインターフェイス オブジェクトを表示します。
ip route	（任意）トラッキング対象の IP ルート オブジェクトを表示します。
ip sla	（任意）トラッキング対象の IP SLA オブジェクトを表示します。
ipv6 route	（任意）トラッキング対象の IPv6 ルート オブジェクトを表示します。
list	（任意）ブール オブジェクトを表示します。
resolution	（任意）トラッキング対象パラメータの解像度を表示します。
summary	（任意）指定されたオブジェクトの概要を表示します。
timers	（任意）ポーリング間隔タイマーを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 16.2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
	このコマンドが導入されました。

使用上のガイドライン

トラッキングプロセスによってトラッキングされているオブジェクトに関する情報を表示するには、このコマンドを使用します。引数やキーワードを指定しない場合は、すべてのオブジェクトの情報が表示されます。

最大 1000 のオブジェクトを追跡できます。トラッキング対象オブジェクトは 1000 個設定できますが、各トラッキング対象オブジェクトは CPU リソースを使用します。デバイスで使用可能な CPU リソースの合計は、トラフィック負荷などの変数や、他のプロトコルがどのように設定され実行されているかに応じて異なります。1000 個の追跡対象オブジェクトが使用できる

かどうかは、使用可能な CPU によって異なります。特定のサイト トラフィック条件下でサービスが機能することを保証するには、サイト上でテストを実施する必要があります。

例

次に、インターフェイスでIPルーティングの状態をトラッキングした場合の例を示します。

```
Device# show track 1

Track 1
 Interface GigabitEthernet 1/0/1 ip routing
 IP routing is Down (no IP addr)
  1 change, last change 00:01:08
```

次の表で、この出力で表示される重要なフィールドについて説明します。

表 *22 : show track* フィールドの説明

フィールド	説明
Track	トラッキング対象オブジェクトの数。
Interface GigabitEthernet 1/0/1 IP routing	インターフェイス タイプ、インターフェイス番号、およびトラッキング対象オブジェクト。
IP routing is	Up または Down で表示されるオブジェクトの状態の値。オブジェクトがダウンしている場合は、理由が示されます。
1 change、last change	トラッキング対象オブジェクトの状態が変更された回数と、最後の変更からの経過時間（*hh:mm:ss* で表示）。

関連コマンド

Command	Description
show track resolution	追跡対象パラメータの解像度を表示します。
track interface	インターフェイスをトラッキングされるように設定し、トラッキング コンフィギュレーション モードを開始します。
track ip route	IP ルートの状態を追跡し、トラッキング コンフィギュレーション モードを開始します。

track

Gateway Load Balancing Protocol（GLBP）の重み付けがインターフェイスの状態に基づいて変更されている場合にトラッキング対象インターフェイスを設定するには、グローバル コンフィギュレーション モードで **track** コマンドを使用します。トラッキングを削除するには、このコマンドの **no** 形式を使用します。

track *object-number* **interface** *type number* {**line-protocol** | **ip routing** | **ipv6 routing**}
no track *object-number* **interface** *type number* {**line-protocol** | **ip routing** | **ipv6 routing**}

構文の説明

object-number	トラッキングされるインターフェイスを表すオブジェクト番号。値の範囲は 1 ～ 1000 です。
interface *type number*	トラッキングするインターフェイス タイプおよび番号。
line-protocol	インターフェイスがアップ状態かどうかをトラッキングします。
ip routing	インターフェイスがアップの状態であることをGLBPに報告する前に、IP ルーティングが有効かどうか、インターフェイスに IP アドレスが設定されているか、インターフェイスがアップの状態かどうかをトラッキングします。
ipv6 routing	インターフェイスがアップの状態であることをGLBPに報告する前に、IPv6 ルーティングが有効かどうか、インターフェイスに IP アドレスが設定されているか、インターフェイスがアップの状態かどうかをトラッキングします。

コマンド デフォルト

インターフェイスの状態はトラッキングされません。

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
	このコマンドが導入されました。

使用上のガイドライン

トラッキング対象インターフェイスのパラメータを設定するには、**track** コマンドと併せて **glbp weighting** および **glbp weighting track** コマンドを使用します。GLBP デバイスのトラッキング対象インターフェイスがダウンすると、そのデバイスの重み値は減らされます。重み値が指定された最小値を下回った場合、デバイスは、アクティブGLBP仮想フォワーダとしての機能を失います。

最大 1000 のオブジェクトを追跡できます。トラッキング対象オブジェクトは 1000 個設定できますが、各トラッキング対象オブジェクトは CPU リソースを使用します。デバイスで使用可能な CPU リソースの合計は、トラフィック負荷などの変数や、他のプロトコルがどのように設定され実行されているかに応じて異なります。1000 個の追跡対象オブジェクトが使用できるかどうかは、使用可能な CPU によって異なります。特定のサイト トラフィック条件下でサービスが機能することを保証するには、サイト上でテストを実施する必要があります。

例

次に、TenGigabitEthernet インターフェイス 0/0/1 が、GigabitEthernet インターフェイス 1/0/1 および 1/0/3 がアップの状態にあるかどうかをトラッキングする例を示します。GigabitEthernet インターフェイスのいずれかがダウンすると、GLBP の重み値は、デフォルト値である 10 まで減らされます。両方の GigabitEthernet インターフェイスがダ

ウンすると、GLBPの重み値は下限しきい値未満に下がり、デバイスはアクティブフォワーダではなくなります。アクティブフォワーダとしての役割を再開するには、デバイスは、両方のトラッキング対象インターフェイスをアップの状態に戻し、重み値を上限しきい値を超える値に上げる必要があります。

```
Device(config)# track 1 interface GigabitEthernet 1/0/1 line-protocol
Device(config-track)# exit
Device(config)# track 2 interface GigabitEthernet 1/0/3 line-protocol
Device(config-track)# exit
Device(config)# interface TenGigabitEthernet 0/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
Device(config-if)# glbp 10 weighting track 1
Device(config-if)# glbp 10 weighting track 2
```

関連コマンド

コマンド	説明
glbp weighting	GLBP ゲートウェイの初期重み値を指定します。
glbp weighting track	GLBP ゲートウェイの重み付けに影響する、追跡対象のオブジェクトを指定します。

vrrp

Virtual Router Redundancy Protocol バージョン 3（VRRPv3）グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始するには、**vrrp** を使用します。VRRPv3 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。

vrrp *group-id* **address-family** {**ipv4** | **ipv6**}
no vrrp *group-id* **address-family** {**ipv4** | **ipv6**}

構文の説明

group-id	仮想ルータ グループ番号。範囲は 1 ～ 255 です。
address-family	このVRRPグループのアドレス ファミリを指定します。
ipv4	（任意）IPv4 アドレスを指定します。
ipv6	（任意）IPv6 アドレスを指定します。

コマンド デフォルト

なし

コマンド モード

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
	このコマンドが導入されました。

使用上のガイドライン

例

次の例は、VRRPv3 グループの作成方法と VRRP コンフィギュレーション モードの開始方法を示しています。

```
Device(config-if)# vrrp 3 address-family ipv4
```

関連コマンド

コマンド	説明
timers advertise	アドバタイズメント タイマーを設定します（ミリ秒単位）。

vrrp description

Virtual Router Redundancy Protocol（VRRP）に説明を割り当てるには、インターフェイス コンフィギュレーション モードで **vrrp description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

description *text*
no description

構文の説明

text	グループの目的または用途を説明するテキスト（最大 80 文字）。

コマンド デフォルト

VRRP グループの説明はありません。

コマンド モード

VRRP 設定（config-if-vrrp）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 16.2.1	このコマンドが導入されました。

例

次の例では、VRRP を有効にしています。VRRP グループ 1 は、「Building A – Marketing and Administration（ビルディング A：マーケティングおよび管理）」と説明されます。

```
Device(config-if-vrrp)# description Building A - Marketing and Administration
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。

vrrp preempt

デバイスに現在のマスター仮想ルータより高い優先順位が与えられている場合、そのデバイスが Virtual Router Redundancy Protocol（VRRP）グループのマスター仮想ルータの機能を引き継ぐように設定するには、VRRP コンフィギュレーション モードで **preempt** 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。

preempt [**delay minimum** *seconds*]
no preempt

構文の説明

delay minimum *seconds*	（任意）マスターの所有権を要求するアドバタイズメントを発行するまでに、デバイスが待機する秒数。デフォルト遅延値は 0 秒です。

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

VRRP 設定（config-if-vrrp）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、このコマンドで設定されるデバイスは、現在のマスター仮想ルータよりも高い優先順位を持つ場合、マスター仮想ルータとしての機能を引き継ぎます。VRRP デバイスが、マスター所有権を要求するアドバタイズメントを発行するまで、指定された秒数待機するように遅延時間を設定できます。

（注） このコマンドの設定にかかわらず、IP アドレスの所有者であるデバイスがプリエンプション処理します。

例

次に、デバイスの 200 の優先順位が現在のマスター仮想ルータの優先順位よりも高い場合に、デバイスが現在のマスター仮想ルータをプリエンプション処理するように設定する例を示します。デバイスは、現在のマスター仮想ルータをプリエンプション処理する場合、マスター仮想ルータであることを要求するアドバタイズメントを発行するまでに 15 秒待機します。

```
Device(config-if-vrrp)#preempt delay minimum 15
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。
priority	VRRP グループ内のデバイスの優先度レベルを設定します。

vrrp priority

Virtual Router Redundancy Protocol（VRRP）内のデバイスの優先度レベルを設定するには、インターフェイス コンフィギュレーション モードで **priority** コマンドを使用します。デバイスの優先度レ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。

priority *level*
no priority *level*

構文の説明

level	VRRP グループ内のデバイスの優先順位。有効な範囲は 1 ～ 254 です。デフォルトは 100 です。

コマンド デフォルト

優先度レベルはデフォルト値の 100 に設定されています。

コマンド モード

VRRP 設定（config-if-vrrp）

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、どのデバイスをマスター仮想ルータにするかを制御できます。

例

次に、デバイスを 254 の優先順位に設定する例を示します。

```
Device(config-if-vrrp)# priority 254
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。
vrrp preempt	デバイスに現在のマスター仮想ルータより高い優先順位が与えられている場合、そのデバイスが VRRP グループのマスター仮想ルータの機能を引き継ぐように設定します。

vrrp timers advertise

Virtual Router Redundancy Protocol（VRRP）グループ内のマスター仮想ルータによる連続したアドバタイズメント間の間隔を設定するには、VRRP コンフィギュレーション モードで **timers advertise** 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。

timers advertise [**msec**] *interval*
no timers advertise [**msec**] *interval*

構文の説明

group	仮想ルータ グループ番号。グループ番号の範囲は 1 ～ 255 です。
msec	（任意）アドバタイズメント時間の単位を秒からミリ秒に変更します。このキーワードを付加しないと、アドバタイズメント間隔は秒単位になります。
interval	マスター仮想ルータによる連続したアドバタイズメント間の時間間隔。**msec** キーワードを指定しなかった場合、間隔は秒単位になります。デフォルト値は1秒です。有効範囲は 1 ～ 255 秒です。**msec** キーワードを指定した場合、有効な範囲は 50 ～ 999 ミリ秒です。

コマンド デフォルト

デフォルトの間隔である 1 秒に設定されています。

コマンド モード

VRRP 設定（config-if-vrrp）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 16.2.1	このコマンドが導入されました。

使用上のガイドライン

マスター仮想ルータから送信されるアドバタイズメントは、現在のマスター仮想ルータの状態と優先順位を伝えます。

vrrp timers advertise コマンドは、連続するアドバタイズメントパケットの間の時間間隔と、マスタールータがダウンしていると他のルータが宣言するまでの時間を設定します。タイマー値が設定されていないルータまたはアクセス サーバは、マスター ルータからタイマー値を取得できます。マスタールータで設定されたタイマーは、他のすべてのタイマー設定を常に上書きします。VRRP グループ内のすべてのルータが同じタイマー値を使用する必要があります。同じタイマー値が設定されていないと、VRRP グループ内のデバイスが相互通信せず、正しく設定されていないデバイスのステートがマスターに変わります。

例

次に、マスター仮想ルータがアドバタイズメントを 4 秒ごとに送信するように設定する例を示します。

```
Device(config-if-vrrp)# timers advertise 4
```

関連コマンド

コマンド	説明
vrrp	VRRPv3 グループを作成し、VRRPv3 グループ コンフィギュレーション モードを開始します。
timers learn	VRRP グループのバックアップ仮想ルータとして動作するときに、マスター仮想ルータが使用していたアドバタイズ間隔を学習するようにデバイスを設定します。

vrrs leader

リーダーの名前を Virtual Router Redundancy Service（VRRS）に登録されるように指定するには、**vrrs leader** コマンドを使用します。指定された VRRS リー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。

vrrs leader *vrrs-leader-name*
no vrrs leader *vrrs-leader-name*

構文の説明

vrrs-leader-name	リードする VRRS タグの名前。

コマンド デフォルト

登録済みの VRRS 名はデフォルトで使用不可になっています。

コマンド モード

VRRP 設定（config-if-vrrp）

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、VRRS に登録されるリーダーの名前を指定する例を示します。

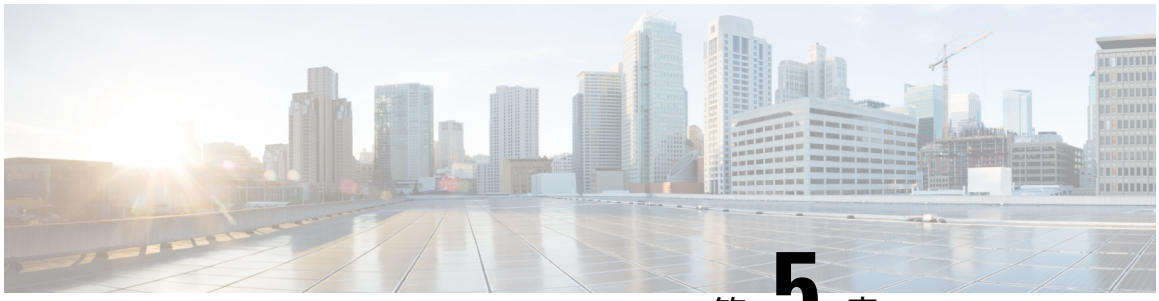
```
Device(config-if-vrrp)# vrrs leader leader-1
```

関連コマンド

コマンド	説明
vrrp	VRRP グループを作成し、VRRP コンフィギュレーション モードを開始します。

第 IV 部

IP マルチキャスト ルーティング



第 5 章

IP マルチキャスト ルーティング

cache-memory-max

キャッシュに使用するシステムメモリの割合を設定するには、**cache-memory-max** コマンドを使用します。キャッシュに使用するシステムメモリの割合を削除するには、このコマンドの **no** 形式を使用します。

cache-memory-max キャッシュ設定-割合
no cache-memory-max *cache-config-percentage*

構文の説明

cache-config-percentage	キャッシュに使用するシステム メモリの割合。

コマンド デフォルト

デフォルトでは、システム メモリは 10 パーセントに設定されています。

コマンド モード

mDNS コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

ネットワークで学習されるサービスの数が大きくなる可能性があるため、使用できるキャッシュ メモリの容量には上限があります。

（注） デフォルト値は、次のコマンドを使用してオーバーライドできます。

新しいレコードを追加しようとする場合、キャッシュがいっぱいになると、キャッシュ内の期限切れに近いレコードが削除され、新しいレコードのためのスペースが確保されます。

例

次に、キャッシュに使用するシステムメモリの割合を20%に設定する例を示します。

```
デバイス(config-mdns)# cache-memory-max 20
```

clear ip mfib counters

すべてのアクティブIPV4マルチキャスト転送情報ベース（MFIB）トラフィックカウンタをクリアするには、特権 EXEC モードで **clear ip mfib counters** コマンドを使用します。

clear ip mfib ［**global** ｜ **vrf** ***］ **counters** ［*group-address*］［*hostname* ｜ *source-address*］

構文の説明

global	（任意）IP MFIB キャッシュをグローバルデフォルト設定にリセットします。
vrf *	（任意）すべての VPN ルーティングおよび転送インスタンスの IP MFIB キャッシュをクリアします。
group-address	（任意）アクティブ MFIB トラフィックカウンタを指定されたグループアドレスに制限します。
hostname	（任意）アクティブ MFIB トラフィックカウンタを指定されたホスト名に制限します。
source-address	（任意）アクティブ MFIB トラフィックカウンタを指定された送信元アドレスに制限します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

例

次に、すべてのマルチキャストテーブルのアクティブ MFIB トラフィックカウンタをすべてリセットする例を示します。

```
デバイス# clear ip mfib counters
```

次に、IP MFIB キャッシュカウンタをグローバルデフォルト設定にリセットする例を示します。

```
デバイス# clear ip mfib global counters
```

次に、すべての VPN ルーティングおよび転送インスタンスの IP MFIB キャッシュをクリアする例を示します。

```
デバイス# clear ip mfib vrf * counters
```

clear ip mroute

IP マルチキャスト ルーティング テーブルのエントリを削除するには、特権 EXEC モードで **clear ip mroute** コマンドを使用します。

clear ip mroute [**vrf** *vrf-name*] {***** | *ip-address* | *group-address*} [*hostname* | *source-address*]

構文の説明

vrf *vrf-name*	（任意）マルチキャスト VPN ルーティング/転送（VRF）インスタンスに割り当てられている名前を指定します。
*	すべてのマルチキャストルートを指定します。
ip-address	IP アドレスのマルチキャストルート。
group-address	グループ アドレスのマルチキャストルート。
hostname	（任意）ホスト名のマルチキャストルート。
source-address	（任意）送信元アドレスのマルチキャストルート。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

group-address 変数は、次のいずれかを指定します。

- DNS ホストテーブルまたは **ip host** コマンドで定義されるマルチキャストグループ名

• 4 分割ドット表記によるマルチキャストグループの IP アドレス

group の名前またはアドレスを指定する場合、source 引数を入力して、グループに送信するマルチキャスト送信元の名前またはアドレスも指定できます。送信元は、グループのメンバである必要はありません。

例

次に、IP マルチキャスト ルーティング テーブルからすべてのエントリを削除する例を示します。

```
デバイス# clear ip mroute *
```

次に、マルチキャストグループ 224.2.205.42 に送信する 228.3.0.0 サブネット上のすべての送信元を IP マルチキャスト ルーティング テーブルから削除する例を示します。この例では、ネットワーク 228.3 上の個別の送信元ではなく、すべての送信元が削除されます。

```
デバイス# clear ip mroute 224.2.205.42 228.3.0.0
```

ip igmp explicit-tracking

Internet Group Management Protocol Version 3（IGMPv3）のホスト、グループ、およびチャネルの明示的なトラッキングを有効にするには、インターフェイス コンフィギュレーション モードで **ip igmp explicit-tracking** 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。

ip igmp explicit-tracking
no ip igmp explicit-tracking

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IGMPv3 のホスト、グループ、およびチャネルの明示的なトラッキングは無効になっています。

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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、レイヤ 3 インターフェイスでの明示的なトラッキングが有効になります。

マルチキャストデバイスが特定のマルチアクセスネットワークに含まれるマルチキャストホストのメンバーシップの明示的なトラッキングを行えるようにするには、**ip igmp explicit-tracking** コマンドを使用します。これにより、マルチキャストデバイスは、特定のグループまたはチャ

ネルに参加している各ホストを個別にトラッキングし、ホストがマルチキャスト グループまたはチャネルを離れるときの離脱レイテンシを最小限に抑えることができるようになります。

（注） **ip igmp explicit-tracking** コマンドを設定する前に、IGMP を有効にする必要があります（IGMP は、 **ip pim** コマンドを使用してインターフェイスで PIM を有効にすると有効になります）。さらに、インターフェイスで IGMPv3 を設定する必要があります。IGMPv3 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 igmp version 3** コマンドを使用します。

（注） 明示的なトラッキングが有効になっていると、ルータがインターフェイス上のすべてのホストのメンバシップ状態を保存する必要があるため、デバイスは、明示的なトラッキングが無効の場合よりも多くのメモリを使用します。

ホストの IGMP メンバーシップをモニタするには、**show ip igmp membership** コマンドを使用します。

例

次に、明示的なトラッキングを有効にする例を示します。この例は、SSM、IGMPv3、および明示的なトラッキングを使用して IP マルチキャストを有効にする基本を示しています。

```
Device(config)# ip multicast-routing
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# ip address 10.1.0.1 255.255.255.0
Device(config-if)# ip pim sparse-dense-mode
Device(config-if)# ip igmp version 3
Device(config-if)# ip igmp explicit-tracking
Device(config-if)# end
```

関連コマンド

コマンド	説明
ip igmp version	デバイスが使用する IGMP のバージョンを設定します。
ip pim	インターフェイスで PIM を有効にします。
show ip igmp membership	マルチキャスト グループおよびチャネルの IGMP メンバーシップ情報を表示します。

ip igmp filter

Internet Group Management Protocol（IGMP）プロファイルをインターフェイスに適用することで、レイヤ 2 インターフェイスのすべてのホストが 1 つ以上の IP マルチキャストグループに参加できるかどうかを制御するには、device スタックまたはスタンドアロン device で **ip igmp**

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。インターフェイスから指定されたプロファイルを削除するには、このコマンドの **no** 形式を使用します。

ip igmp filter *profile number*
no ip igmp filter

構文の説明

profile number	適用する IGMP プロファイル番号。範囲は 1 ～ 4294967295 です。

コマンド デフォルト

IGMP フィルタは適用されていません。

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（config-if）

コマンド履歴

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

使用上のガイドライン

IGMP フィルタはレイヤ 2 の物理インターフェイスだけに適用できます。ルーテッドポート、Switch Virtual Interface（SVI）、または EtherChannel グループに属するポートに対して IGMP フィルタを適用することはできません。

IGMP プロファイルは 1 つまたは複数のdevice ポートインターフェイスに適用できますが、1 つのポートに対して 1 つのプロファイルだけ適用できます。

例

設定を確認するには、特権 EXEC モードで **show running-config** コマンドを使用してインターフェイスを指定します。

ip igmp max-groups

レイヤ 2 インターフェイスが参加可能な Internet Group Management Protocol（IGMP）グループの最大数を設定するか、最大数のエントリが転送テーブルにあるときの IGMP スロットリング アクションを設定するには、device スタックまたはスタンドアロン device で **ip igmp max-groups** インターフェイス コンフィギュレーション コマンドを使用します。最大数をデフォルト値（無制限）に戻すか、デフォルトのスロットリング アクション（レポートをドロップ）に戻すには、このコマンドの **no** 形式を使用します。

ip igmp max-groups {*max number* | **action** { **deny** | **replace**}}
no ip igmp max-groups {*max number* | **action**}

構文の説明

max number	インターフェイスが参加できる IGMP グループの最大数。範囲は 0 ～ 4294967294 です。デフォルト設定は無制限です。

action deny	最大数のエントリが IGMP スヌーピング転送テーブルにある場合は、次の IGMP 参加レポートをドロップします。これがデフォルトのアクションになります。
action replace	最大数のエントリが IGMP スヌーピング転送テーブルにある場合に、IGMP レポートを受信した既存のグループを新しいグループで置き換えます。

コマンド デフォルト

デフォルトの最大グループ数は制限なしです。

インターフェイス上に IGMP グループエントリの最大数があることをdeviceが学習した後の、デフォルトのスロットリングアクションでは、インターフェイスが受信する次の IGMP レポートをドロップし、インターフェイスに IGMP グループのエントリを追加しません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

このコマンドは、レイヤ 2 物理インターフェイスおよび論理 EtherChannel インターフェイスでだけ使用できます。ルーテッドポート、Switch Virtual Interface（SVI）、または EtherChannel グループに属するポートに対して IGMP 最大グループ数を設定することはできません。

IGMP スロットリングアクションを設定する場合には、次の注意事項に従ってください。

- スロットリングアクションを deny として設定して最大グループ制限を設定する場合、以前転送テーブルにあったエントリは、削除されませんが期限切れになります。これらのエントリの期限が切れた後で、エントリの最大数が転送テーブルにある場合は、インターフェイス上で受信された次の IGMP レポートを device がドロップします。
- スロットリングアクションを replace として設定して最大グループ制限を設定する場合、以前転送テーブルにあったエントリは削除されます。最大数のエントリが転送テーブルにある場合、deviceはランダムに選択したマルチキャストエントリを受信した IGMP レポートで置き換えます。
- グループの最大数に関する制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups {deny | replace}** コマンドを入力しても効果はありません。

例

次に、ポートが加入できる IGMP グループ数を 25 に制限する例を示します。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# ip igmp max-groups 25
```

次に、最大数のエントリが転送テーブルにあるときに、IGMP レポートを受信した既存のグループを新しいグループと置き換えるようにdeviceを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)# ip igmp max-groups action replace
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを使用してインターフェイスを指定します。

ip igmp profile

Internet Group Management Protocol（IGMP）プロファイルを作成し、IGMP プロファイル コンフィギュレーション モードを開始するには、device スタックまたはスタンドアロン device で **ip igmp profile** グローバル コンフィギュレーション コマンドを使用します。このモードで、スイッチポートからの IGMP メンバーシップレポートをフィルタリングするための IGMP プロファイルの設定を指定できます。IGMP プロファイルを削除するには、このコマンドの **no** 形式を使用します。

ip igmp profile *profile number*
no ip igmp profile *profile number*

構文の説明

profile number	設定する IGMP プロファイル番号。範囲は 1 ～ 4294967295 です。

コマンド デフォルト

IGMP プロファイルは定義されていません。設定された場合、デフォルトの IGMP プロファイルとの一致機能は、一致するアドレスを拒否する設定になります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。

- **deny**：一致するアドレスを拒否するように指定します（デフォルト設定の状態）。
- **exit**：IGMP プロファイル コンフィギュレーション モードを終了します。
- **no**：コマンドを無効にする、またはデフォルトにリセットします。
- **permit**：一致するアドレスを許可するように指定します。
- **range**：プロファイルの IP アドレスの範囲を指定します。1 つの IP アドレス、またはアドレスの最初と最後で範囲を指定することもできます。

  範囲を入力する場合、低い方の IP マルチキャストアドレスを入力してからスペースを入力し、次に高い方の IP マルチキャストアドレスを入力します。

IGMP のプロファイルを、1 つまたは複数のレイヤ 2 インターフェイスに適用できますが、各インターフェイスに適用できるプロファイルは 1 つだけです。

例

次の例では、指定された範囲の IP マルチキャストアドレスを許可する IGMP プロファイル 40 の設定方法を示します。

```
デバイス(config)# ip igmp profile 40
デバイス(config-igmp-profile)# permit
デバイス(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

設定を確認するには、特権 EXEC モードで **show ip igmp profile** コマンドを使用します。

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 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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 igmp snooping vlan explicit-tracking

Internet Group Management Protocol（IGMP）のホスト、グループ、およびチャネルの明示的なトラッキングを有効にするには、グローバル コンフィギュレーション モードで**ip igmp snooping vlan explicit-tracking** コマンドを使用します。IGMP の明示的なトラッキングを無効にするには、このコマンドの **no** 形式を使用します。

ip igmp snooping vlan *vlan-ID* **explicit-tracking**
no ip igmp snooping vlan *vlan-ID* **explicit-tracking**

構文の説明

vlan-ID	VLAN ID。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。

コマンド デフォルト

IGMP のホスト、グループ、およびチャネルの明示的なトラッキングは無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

マルチキャストデバイスが特定のマルチアクセスネットワークに含まれるマルチキャストホストのメンバーシップの明示的なトラッキングを行えるようにするには、**ip igmp snooping vlan explicit-tracking** コマンドを使用します。これにより、マルチキャスト デバイスは、特定のグループまたはチャネルに参加している各ホストを個別にトラッキングし、ホストがマルチキャスト グループまたはチャネルを離れるときの離脱レイテンシを最小限に抑えることができるようになります。

（注） 明示的なトラッキングが有効になっていると、デバイスは、インターフェイス上のすべてのホストのメンバシップ状態を保存する必要があるため、明示的なトラッキングが無効の場合よりも多くのメモリを使用します。

例

次に、明示的なトラッキングを有効にする例を示します。

```
Device# configure terminal
Device(config)# ip multicast-routing
Device(config)# ip igmp snooping vlan 1 explicit-tracking
Device(config)# exit
```

関連コマンド

コマンド	説明
ip multicast-routing	IPマルチキャストルーティングを有効にします。

ip igmp snooping last-member-query-count

Internet Group Management Protocol（IGMP）スヌーピングが IGMP 脱退メッセージの受信に対してクエリーメッセージを送信する回数を設定するには、グローバル コンフィギュレーション モードで **ip igmp snooping last-member-query-count** コマンドを使用します。*count* をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

ip igmp snooping ［**vlan** *vlan-id*］ **last-member-query-count** *count*
no ip igmp snooping ［**vlan** *vlan-id*］ **last-member-query-count** *count*

構文の説明

vlan *vlan-id*	（任意）特定の VLAN ID のカウント値を指定します。範囲は 1 ～ 1001 です。先頭の 0 は入力しないでください。
count	クエリーメッセージの送信インターバルを、ミリ秒単位で設定します。範囲は 1 ～ 7 です。デフォルトは 2 です。

コマンド デフォルト

クエリーが 2 ミリ秒ごとに送信されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

マルチキャストホストがグループから脱退すると、ホストはIGMP脱退メッセージを送信します。このホストがグループを脱退する最終ホストかどうかを確認するために、脱退メッセージが確認されると、**last-member-query-interval** タイムアウト期間が過ぎるまで IGMP クエリー

メッセージが送信されます。タイムアウト期限が切れる前に last-member クエリーへの応答が受信されないと、グループレコードは削除されます。

タイムアウト期間を設定するには、**ip igmp snooping last-member-query-interval** コマンドを使用します。

IGMP スヌーピング即時脱退処理とクエリーカウントの両方を設定した場合は、即時脱退処理が優先されます。

（注） カウントを 1 に設定しないでください。単一パケットの損失（device からホストへのクエリーパケット、またはホストから device へのレポートパケット）により、受信者がまだいてもトラフィックの転送が停止される場合があります。トラフィックは、次の一般クエリーが device から送信された後も転送され続けますが、受信者がクエリーを受信しない間隔は 1 分間（デフォルトのクエリー間隔で）となる可能性があります。

Cisco IOS ソフトウェアの脱退遅延は、device が last-member-query-interval（LMQI）内で複数の脱退を処理しているときに、1 つの LMQI 値まで増やすことができます。このシナリオでは、平均脱退遅延は (カウント数 + 0.5) * LMQI によって決まります。その結果、デフォルトの脱退遅延は 2.0 ～ 3.0 秒の範囲となり、IGMP 脱退処理の負荷が高い状態では平均 2.5 秒となります。100 ミリ秒でカウントが 1 という LMQI の最小値の負荷条件下では、脱退遅延は 100 ～ 200ミリ秒となり、平均は 150 ミリ秒です。これは、高レートの IGMP 脱退メッセージから受ける影響を抑えるために行われます。

例

次に、最後のメンバクエリーの数を 5 に設定する例を示します。

```
デバイス(config)# ip igmp snooping last-member-query-count 5
```

ip igmp snooping querier

レイヤ 2 ネットワークで Internet Group Management Protocol（IGMP）クエリア機能をグローバルにイネーブルにするには、**ip igmp snooping querier** 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。キーワードとともにコマンドを入力すると、VLANインターフェイスの IGMP クエリア機能をイネーブルにし、設定できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** *ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** {**count** *count* | **interval** *interval*} | **timer expiry** *expiry-time* | **version** *version*]
no ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** | **max-response-time** | **query-interval** | **tcn query** {**count** | **interval**} | **timer expiry** | **version**]

構文の説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングおよび IGMP クエリア機能をイネーブルにします。範囲は 1 ～ 1001 および 1006 ～ 4094 です。
address *ip-address*	（任意）送信元 IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。
max-response-time *response-time*	（任意）IGMP クエリアレポートを待機する最長時間を設定します。範囲は 1 ～ 25 秒です。
query-interval *interval-count*	（任意）IGMP クエリアの間隔を設定します。範囲は 1 ～ 18000 秒です。
tcn query	（任意）トポロジ変更通知（TCN）に関連するパラメータを設定します。
count *count*	TCN 時間間隔に実行される TCN クエリの数を設定します。範囲は 1 ～ 10 です。
interval 間隔	TCN クエリの時間間隔を設定します。範囲は 1 ～ 255 です。
timer expiry *expiry-time*	（任意）IGMP クエリアが期限切れになる時間を設定します。範囲は 60 ～ 300 秒です。
version *version*	（任意）クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。

コマンド デフォルト

IGMP スヌーピングクエリア機能は、device でグローバルにディセーブルに設定されています。

IGMP スヌーピングクエリアは、イネーブルの場合でも、マルチキャストルータからの IGMP トラフィックが検出されると、自らをディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

クエリアとも呼ばれる IGMP クエリメッセージを送信するデバイスの IGMP バージョンおよび IP アドレスを検出するために IGMP スヌーピングをイネーブルにするには、このコマンドを使用します。

デフォルトでは、IGMP スヌーピングクエリアは、IGMP バージョン 2（IGMPv2）を使用するデバイスを検出するよう設定されていますが、IGMP バージョン 1（IGMPv1）を使用しているクライアントは検出しません。デバイスが IGMPv2 を使用している場合、**max-response-time**

値を手動で設定できます。デバイスが IGMPv1 を使用している場合は、max-response-time を設定できません（値を設定できず、0 に設定されています）。

IGMPv1 を実行している RFC に準拠していないデバイスは、**max-response-time** 値としてゼロ以外の値を持つ IGMP 一般クエリメッセージを拒否することがあります。デバイスで IGMP 一般クエリメッセージを受け入れる場合、IGMP スヌーピングクエリアが IGMPv1 を実行するように設定します。

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 スヌーピングクエリア機能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 querier
```

次の例では、IGMP スヌーピングクエリアの最大応答時間を 25 秒に設定する方法を示します。

```
デバイス(config)# ip igmp snooping querier max-response-time 25
```

次の例では、IGMP スヌーピングクエリアの時間間隔を 60 秒に設定する方法を示します。

```
デバイス(config)# ip igmp snooping querier query-interval 60
```

次の例では、IGMP スヌーピングクエリアの TCN クエリカウントを 25 に設定する方法を示します。

```
デバイス(config)# ip igmp snooping querier tcn count 25
```

次の例では、IGMP スヌーピングクエリアのタイムアウト値を 60 秒に設定する方法を示します。

```
デバイス(config)# ip igmp snooping querier timer expiry 60
```

次に、IGMP スヌーピングクエリア機能をバージョン 2 に設定する例を示します。

```
デバイス(config)# ip igmp snooping querier version 2
```

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

ip igmp snooping report-suppression

Internet Group Management Protocol（IGMP）レポート抑制を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 report-suppression** 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。IGMP レポート抑制をディセーブルにして、すべての IGMP レポートをマルチキャストルータに転送するには、このコマンドの **no** 形式を使用します。

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

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

IGMP レポート抑制はイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

IGMP レポート抑制は、マルチキャストクエリに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリに IGMPv3 レポートが含まれている場合はサポートされません。

device は IGMP レポート抑制を使用して、マルチキャストルータクエリごとに 1 つの IGMP レポートのみをマルチキャストデバイスに転送します。IGMP レポート抑制がイネーブル（デフォルト）である場合、device は最初の IGMP レポートをグループのすべてのホストからすべてのマルチキャストルータに送信します。deviceは、グループの残りの IGMP レポートをマルチキャストルータに送信しません。この機能により、マルチキャストデバイスにレポートが重複して送信されることを防ぎます。

マルチキャストルータクエリに IGMPv1 および IGMPv2 レポートに対する要求のみが含まれている場合、device は最初の IGMPv1 レポートまたは IGMPv2 レポートのみを、グループのすべてのホストからすべてのマルチキャストルータに転送します。マルチキャストルータクエリに IGMPv3 レポートに対する要求も含まれる場合、deviceはグループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャストデバイスに転送します。

no ip igmp snooping report-suppression コマンドを入力して IGMP レポート抑制をディセーブルにした場合、すべての IGMP レポートがすべてのマルチキャストルータに転送されます。

例

次の例では、レポート抑制をディセーブルにする方法を示します。

```
デバイス(config)# no ip igmp snooping report-suppression
```

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 igmp snooping vlan mrouter

マルチキャストルータポートの追加を行うには、deviceスタックまたはスタンドアロンdeviceで **ip igmp snooping mrouter** 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。

コマンド デフォルト

デフォルトでは、マルチキャストルータポートはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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。

設定は、NVRAM に保存されます。

例

次の例では、ポートをマルチキャストルータポートとして設定する方法を示します。

```
デバイス(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/0/2
```

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

ip igmp snooping vlan static

Internet Group Management Protocol（IGMP）スヌーピングをイネーブルにし、マルチキャストグループのメンバとしてレイヤ 2 ポートをスタティックに追加するには、device スタックまたはスタンドアロン device で **ip igmp snooping vlan static** 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。静的マルチキャストグループのメンバとして指定されたポートを削除するには、このコマンドの **no** 形式を使用します。

ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*
no ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

構文の説明

vlan-id	指定した 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。
ip-address	指定のグループ IP アドレスを持ったマルチキャストグループのメンバとして、レイヤ 2 ポートを追加します。

interface *interface-id*	メンバポートのインターフェイスを指定します。 *interface-id* には次のオプションがあります。 • *fastethernet interface number*：ファストイーサネット IEEE 802.3 インターフェイス。 • *gigabitethernet interface number*：ギガビットイーサネット IEEE 802.3z インターフェイス。 • *tengigabitethernet interface number*：10 ギガビットイーサネット IEEE 802.3z インターフェイス。 • *port-channel interface number*：チャネルインターフェイス。範囲は 0 ～ 128 です。

コマンド デフォルト

デフォルトでは、マルチキャストグループのメンバとしてスタティックに設定されたポートはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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。

設定は、NVRAM に保存されます。

例

次の例では、インターフェイス上のホストをスタティックに設定する方法を示します。

```
デバイス(config)# ip igmp snooping vlan 1 static 224.2.4.12 interface
gigabitEthernet1/0/1

Configuring port gigabitethernet1/0/1 on group 224.2.4.12
```

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 igmp version

デバイスで Internet Group Management Protocol（IGMP）のバージョンを設定するには、インターフェイス コンフィギュレーション モードで **ip igmp version** 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 igmp version {**1** | **2** | **3**}
no ip igmp version

構文の説明

1	IGMP バージョン 1。
2	IGMP バージョン 2。これはデフォルトです。
3	IGMP バージョン 3。

コマンド デフォルト

Version 2

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 Everest 16.6.1	このコマンドは、Cisco IOS XE Everest 16.6.1 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

サブネット上のすべてのデバイスが、同じバージョンの IGMP をサポートする必要があります。ホストは任意の IGMP バージョン（1、2、または 3）を搭載でき、デバイスはホストの存在を正しく検出して適切にホストを照会できます。

例

次に、デバイスで IGMP バージョン 3 を設定する例を示します。

```
Device(config-if)# ip igmp version 3
```

関連コマンド

Command	Description
show ip igmp groups	ルータに直接接続され、IGMP を通じて学習されたマルチキャスト グループを表示します。
show ip igmp interface	インターフェイスのマルチキャスト関連情報を表示します。

ip multicast auto-enable

IP マルチキャストの認証、許可、およびアカウンティング（AAA）の有効化をサポートするには、 **ip multicast auto-enable** コマンドを使用します。このコマンドによって、RADIUS サーバから、AAA 属性を使用しているダイヤルアップ インターフェイスでのマルチキャストルーティングをダイナミックに有効化できます。AAA の IP マルチキャストを無効にするには、このコマンドの **no** 形式を使用します。

ip multicast auto-enable
no ip multicast auto-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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

なし

例

次の例は、IP マルチキャスト上の AAA をイネーブルにする方法を示します。

```
デバイス(config)# ip multicast auto-enable
```

ip pim accept-register

Protocol Independent Multicast（PIM）登録メッセージをフィルタ処理するように候補ランデブーポイント（RP）スイッチを設定するには、グローバル コンフィギュレーション モードで **ip pim accept-register** 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。

ip pim ［**vrf** *vrf-name* ］ **accept-register** {**list** *access-list*}
no ip pim ［**vrf** *vrf-name* ］ **accept-register**

構文の説明

vrf *vrf-name*	（任意）*vrf-name* 引数に指定されたマルチキャスト バーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（MVRF）インスタンスに関連付けられている (S, G) トラフィック用の候補 RP で PIM 登録フィルタを設定します。
list *access-list*	許可または拒否する PIM 登録メッセージ内の (S, G) トラフィックを定義する数値または名前として、*access-list* 引数を指定します。指定できる範囲は 100 ～ 199 で、拡張された範囲は 2000 ～ 2699 です。IP 名前付きアクセス リストも使用できます。

コマンド デフォルト

PIM 登録フィルタは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

不正な送信元が RP に登録されないようにするには、このコマンドを使用します。不正な送信元がRPに登録メッセージを送信すると、RPはただちに登録停止メッセージを送り返します。

ip pim accept-register コマンドに提供されるアクセスリストは IP 送信元アドレスと IP 宛先アドレスのみをフィルタ処理します。その他のフィールドのフィルタリング（たとえば、IPプロトコルまたはUDPポート番号）は無効になっています。これらは、共有ツリーの下方のRPからマルチキャスト グループ メンバに不要なトラフィックを転送する場合があります。より複雑なフィルタリングが必要な場合は、代わりに、**ip multicast boundary** コマンドを使用します。

例

次に、SSM グループ範囲（232.0.0.0/8）に送信している送信元アドレス 172.16.10.1 を除き、任意のグループ範囲に送信している送信元アドレスの登録パケットを許可する例を示します。これらは拒否されます。候補 RP は最初のホップ ルータまたはスイッチから PIM 登録を受信するため、これらのステートメントはすべての候補 RP に設定する必要があります。

```
デバイス(config)# ip pim accept-register list ssm-range
デバイス(config)# ip access-list extended ssm-range
デバイス(config-ext-nacl)# deny ip any 232.0.0.0 0.255.255.255
デバイス(config-ext-nacl)# permit ip any any
```

ip pim bsr-candidate

候補 BSR になるように デバイス を設定するには、グローバル コンフィギュレーション モードで **ip pim bsr-candidate** コマンドを使用します。候補 BSR としてのスイッチを削除するには、このコマンドの **no** 形式を使用します。

ip pim ［**vrf** *vrf-name*］ **bsr-candidate** *interface-id* ［*hash-mask-length*］［*priority*］
no ip pim ［**vrf** *vrf-name* ］ **bsr-candidate**

構文の説明

vrf *vrf-name*	（任意） *vrf-name* 引数に指定されたマルチキャスト バーチャル プライベート ネットワーク（MVPN）ルーティングおよび転送（MVRF）インスタンスの候補 BSR になるように デバイス を設定します。
interface-id	BSR アドレスを候補にするための、そのアドレスの派生元である デバイス のインターフェイスの ID。このインターフェイスは、**ip pim** コマンドを使用して、Protocol Independent Multicast（PIM）に対して有効にする必要があります。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。

hash-mask-length	（任意）PIMv2 ハッシュ機能がコールされる前にグループ アドレスと論理積をとるマスク長（最大 32 ビット）。同じシード ハッシュを持つグループはすべて、同じランデブーポイント（RP）に対応します。たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。ハッシュ マスク長により、1 つの RP を複数のグループで使用できるようになります。デフォルトのハッシュ マスク長は 0 です。
priority	（任意）BSR（C-BSR）候補のプライオリティ。有効な範囲は 0 ～ 255 です。デフォルトのプライオリティは 0 です。最高のプライオリティ値を持つ C-BSR が優先されます。

コマンド デフォルト

デバイス はそれ自体を候補 BSR として通知するように設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

このコマンドに指定したインターフェイスは、**ip pim** コマンドを使用して、Protocol Independent Multicast（PIM）に対して有効にする必要があります。

このコマンドは、指定されたインターフェイスのアドレスを BSR アドレスとして示す BSR メッセージをすべての PIM ネイバーに送信するように デバイス を設定します。

このコマンドは、PIM ドメイン内のすべての部分に良好に接続できるバックボーン デバイス で設定する必要があります。

BSR メカニズムは RFC 2362 で指定されています。候補 RP（C-RP）は、ユニキャスト C-RP アドバタイズメント パケットを BSR にスイッチングします。その後、BSR は、これらのアドバタイズメントを BSR メッセージに集約します。BSR メッセージは、TTL 1 で、ALL-PIM-ROUTERS グループのアドレス 224.0.0.13 に定期的にマルチキャストされます。これらのメッセージのマルチキャストは、ホップバイホップ RPF フラッディングによって処理されます。事前の IP マルチキャスト ルーティング設定は必要がありません（AutoRP とは異なる）。また、BSR は、特定のグループ範囲について指定された RP を事前に選択しません（AutoRPとは異なる）。代わりに、BSR メッセージを受信する各スイッチが BSR メッセージ内の情報に基づいてグループ範囲の RP を選択します。

シスコ デバイス は BSR メッセージを常に受け入れ、処理します。この機能を無効にするコマンドはありません。

シスコ デバイス は、次の手順で、どの C-RP がグループで使用されているかを判別します。

- BSR C-RP で通知されるグループ プレフィックスに対して最長一致ルックアップを実行します。
- 最長一致ルックアップによって BSR が学習した C-RP が複数見つかった場合は、優先順位が最低の C-RP（**ip pim rp-candidate** コマンドで設定される）が優先されます。

- 複数の BSR が学習した C-RP で優先順位が同じ場合は、グループの RP を選択するために、BSR ハッシュ関数が使用されます。
- 複数の BSR が学習した C-RP が BSR ハッシュ関数から派生された同じハッシュ値を返す場合は、最高の IP アドレスの BSR C-RP が優先されます。

例

次に、ハッシュ マスク長 0 および優先順位 192 を使用して、ギガビット イーサネット インターフェイス 1/0/0 の デバイス の IP アドレスが BSR C-RP になるように設定する例を示します。

```
デバイス(config)# ip pim bsr-candidate GigabitEthernet1/0/1 0 192
```

ip pim rp-candidate

自身を Protocol Independent Multicast（PIM）バージョン 2（PIMv2）候補ランデブーポイント（C-RP）として BSR にアドバタイズするように デバイス を設定するには、グローバル コンフィギュレーション モードで **ip pim rp-candidate** コマンドを使用します。C-RP としての デバイス を削除するには、このコマンドの **no** 形式を使用します。

ip pim ［**vrf** *vrf-name*］ **rp-candidate** *interface-id* ［**group-list** *access-list-number*］
no ip pim ［**vrf** *vrf-name*］ **rp-candidate** *interface-id* ［**group-list** *access-list-number*］

構文の説明

vrf *vrf-name*	（任意） *vrf-name* 引数に指定されたマルチキャスト バーチャル プライベート ネットワーク（MVPN）ルーティングおよび転送（MVRF）インスタンスの PIMv2 C-RP として自身を BSR にアドバタイズするようにスイッチを設定します。
interface-id	対応する IP アドレスが候補 RP アドレスとしてアドバタイズされるインターフェイスの ID。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。
group-list *access-list-number*	（任意）RPアドレスに関連してアドバタイズされるグループ プレフィックスを定義する標準 IP アクセス リスト番号を指定します。

コマンド デフォルト

デバイス は PIMv2 C-RP として自身を BSR に通知するように設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

自身を候補 RP として BSR アドバタイズするために PIMv2 メッセージを送信するように デバイス を設定するには、このコマンドを使用します。

このコマンドは、PIM ドメイン内のすべての部分に良好に接続できるバックボーン デバイス で設定する必要があります。

interface-id によって指定されたインターフェイスに関連付けられている IP アドレスは C-RP アドレスとしてアドバタイズされます。

このコマンドに指定したインターフェイスは、**ip pim** コマンドを使用して、Protocol Independent Multicast（PIM）に対して有効にする必要があります。

オプションの **group-list** キーワードと *access-list-number* 引数が設定されている場合は、RP アドレスとのアソシエーション時に、標準 IP アクセスリストによって定義されたグループプレフィックスもアドバタイズされます。

例

次に、自身を C-RP として PIM ドメイン内の BSR にアドバタイズするようにスイッチを設定する例を示します。標準アクセス リスト番号 4 により、ギガビット イーサネット インターフェイス 1/0/1 で識別されるアドレスを持つ RP に対応するグループ プレフィックスが指定されます。

```
デバイス(config)# ip pim rp-candidate GigabitEthernet1/0/1 group-list 4
```

ip pim send-rp-announce

Auto-RP を使用して、デバイス がランデブーポイント（RP）として動作する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 **ip pim send-rp-announce** コマンドを使用します。デバイス の RP としての設定を解除するには、このコマンドの **no** 形式を使用します。

ip pim ［**vrf** *vrf-name*］ **send-rp-announce** *interface-id* **scope** *ttl-value* ［**group-list** *access-list-number*］［**interval** *seconds*］
no ip pim ［**vrf** *vrf-name*］ **send-rp-announce** *interface-id*

構文の説明

vrf *vrf-name*	（任意）デバイス がランデブーポイント（RP）として動作するグループを設定するには、*vrf-name* 引数に Auto-RP を使用します。
interface-id	RP アドレスを識別するインターフェイスのインターフェイス ID を入力します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。
scope *ttl-value*	Auto-RP アナウンスメントの数を制限するホップでの存続可能時間（TTL）を指定します。RP アナウンス メッセージがネットワーク内のすべてのマッピング エージェントに確実に到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。範囲は 1 ～ 255 です。

group-list *access-list-number*	（任意）RPアドレスに関連してアドバタイズされるグループプレフィックスを定義する標準IPアクセスリスト番号を指定します。IP標準アクセス リスト番号を入力します。指定できる範囲は 1 ～ 99 です。アクセスリストが設定されていない場合は、すべてのグループにRPが使用されます。
interval *seconds*	（任意）RP アナウンスメント間の間隔を秒単位で指定します。RP アナウンスメントの合計保留時間は、間隔値の 3 倍に自動設定されます。デフォルト インターバルは 60 秒です。範囲は 1 ～ 16383 です。

コマンド デフォルト

Auto-RP はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

RP にする デバイス で次のコマンドを入力します。Auto-RP を使用してグループ/RP マッピングを配信すると、ルータはこのコマンドにより既知のグループ CISCO-RP-ANNOUNCE（224.0.1.39）にAuto-RPアナウンスメントメッセージを送信します。このメッセージは、ルータがアクセス リストで規定される範囲内のグループに対する候補 RP であることを通知します。

例

次に、最大31ホップのすべてのProtocol Independent Multicast（PIM）対応インターフェイスにRPアナウンスメントを送信するように デバイス を設定する例を示します。スイッチを RP として識別するために使用される IP アドレスは、120 秒間隔でギガビット イーサネット インターフェイス 1/0/1 に関連付けられる IP アドレスです。

```
デバイス(config)# ip pim send-rp-announce GigabitEthernet1/0/1 scope 31 group-list 5
interval 120
```

ip pim spt-threshold

最短パスツリー（spt）に移行する上限値となるしきい値を指定するには、グローバルコンフィギュレーション モードで **ip pim spt-threshold** コマンドを使用します。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。

ip pim {*kbps* | **infinity**} [**group-list** *access-list*]
no ip pim {*kbps* | **infinity**} [**group-list** *access-list*]

構文の説明

kbps	最短パス ツリー（spt）に移行する上限値となるしきい値を指定します。有効な範囲は 0 ～ 4294967 ですが、0 が唯一有効なエントリです。0 エントリは、常に送信元ツリーに切り替わります。
infinity	指定されたグループのすべての送信元が共有ツリーを使用し、送信元ツリーに切り替わらないように指定します。
group-list *access-list*	（任意）アクセス リスト番号を指定するか、または作成した特定のアクセス リストを名前で指定します。値 0 を指定する場合、または **group-list** *access-list* オプションを使用しない場合、しきい値はすべてのグループに適用されます。

コマンド デフォルト

PIM 最短パス ツリー（spt）に切り替わります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

例

次に、アクセス リスト 16 のすべての送信元が共有ツリーを使用するように指定する例を示します。

```
デバイス(config)# ip pim spt-threshold infinity group-list 16
```

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン 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 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 3.3SE	このコマンドが導入されました。

使用上のガイドライン **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 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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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
```

mrinfo

ピアとして動作している隣接するマルチキャストルータまたはマルチレイヤスイッチをクエリするには、ユーザ EXEC モードまたは特権 EXEC モードで **mrinfo** コマンドを使用します。

mrinfo [**vrf** *route-name*] [*hostname* | *address*] [*interface-id*]

構文の説明

vrf *route-name*	（任意）VPN ルーティングおよび転送インスタンスを指定します。

hostname | *address*	（任意）クエリするマルチキャスト ルータまたはマルチレイヤ スイッチのドメイン ネーム システム（DNS）名または IP アドレス。省略すると、スイッチは自身をクエリします。
interface-id	（任意）インターフェイス ID。

コマンド デフォルト

このコマンドはディセーブルです。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

mrinfo コマンドは、マルチキャストルータまたはスイッチのピアとして動作している隣接するマルチキャストルータまたはスイッチを判別するためのマルチキャストバックボーン（MBONE）のオリジナルのツールです。シスコルータは、Cisco IOS リリース 10.2 から **mrinfo** 要求をサポートしています。

mrinfo コマンドを使用して、マルチキャストルータまたはマルチレイヤスイッチをクエリすることができます。出力フォーマットは、マルチキャスト ルーテッド バージョンのディスタンス ベクター マルチキャスト ルーティング プロトコル（DVMRP）と同じです（mrouted ソフトウェアは、DVMRP を実装する UNIX ソフトウェアです）。

例

次に、**mrinfo** コマンドの出力例を示します。

```
デバイス# mrinfo
 vrf 192.0.1.0
192.31.7.37 (barrnet-gw.cisco.com) [version cisco 11.1] [flags: PMSA]:
  192.31.7.37 -> 192.31.7.34 (sj-wall-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.47 (dirtylab-gw-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.44 (dirtylab-gw-1.cisco.com) [1/0/pim]
```

（注） フラグの意味は次のとおりです。

- P：プルーニング対応
- M：mtrace 対応
- S：シンプル ネットワーク管理プロトコルに対応
- A：Auto RP に対応

redistribute mdns-sd

サブネット全体にサービスやサービスアナウンスメントを再配布するには、**redistribute mdns-sd** コマンドを使用します。サブネット全体へのサービスやサービスアナウンスメントの再配布を無効にするには、このコマンドの **no** 形式を使用します。

redistribute mdns-sd
no redistribute mdns-sd

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

サブネット全体へのサービスやサービス アナウンスメントの再配布は無効になっています。

コマンド モード

mDNS コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

インターフェイスにサービスアナウンスメントを再配布するには、**redistribute mdns-sd** コマンドを使用します。このコマンドは、1 つのインターフェイスで受信した非要請アナウンスメントを他のすべてのインターフェイスに送信します。発信アナウンスメントはインターフェイスに定義された出力サービス ポリシーに従って、または、インターフェイスごとのサービス ポリシーがない場合はグローバル出力サービス ポリシーに基づいてフィルタ処理されます。

再配布オプションがない場合は、サービス プロバイダーに対してローカルでないレイヤ 3 ドメインでクエリすることで、サービスを検出できます。

例

次に、サブネット全体にサービスやサービス アナウンスメントを再配布する例を示します。

```
デバイス(config-mdns)# redistribute mdns-sd
```

（注） 再配布がグローバルに有効になっている場合は、グローバル コンフィギュレーションがインターフェイス コンフィギュレーションよりも優先順位が高くなります。

service-list mdns-sd

deviceで mDNS サービス検出サービスリストモードを開始するには、**service-list mdns-sd** コマンドを使用します。mDNS サービス検出サービスリストモードを終了するには、このコマンドの **no** 形式を使用します。

service-list mdns-sd *service-list-name* {**permit** | **deny**} *sequence-number* [**query**]
no service-list mdns-sd *service-list-name* {**permit** | **deny**} *sequence-number* [**query**]

構文の説明

service-list-name	サービス リストの名前。
permit *sequence number*	シーケンス番号に対するサービス リストのフィルタの適用を許可します。
deny *sequence number*	シーケンス番号に対するサービス リストのフィルタの適用を拒否します。
query	サービス リスト名のクエリを関連付けます。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

サービス フィルタは、アクセス リストとルートマップに関してモデル化されています。

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。

このコマンドは mDNS サービス検出サービスリスト モードを開始するために使用できます。

このモードでは、次の操作を実行できます。

- サービス リストを作成し、シーケンス番号に適用された **permit** または **deny** オプションに従って、サービス リストにフィルタを適用します。

例

次に、サービス リストを作成し、シーケンス番号に適用された **permit** または **deny** オプションに従って、サービス リストにフィルタを適用する例を示します。

```
デバイス(config)# service-list mdns-sd sl1 permit 3
```

service-policy-query

サービスリストクエリの周期を設定するには、**service-policy-query** 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。

service-policy-query ［*service-list-query-name service-list-query-periodicity*］
no service-policy-query

構文の説明

service-list-query-name service-list-query-periodicity	（任意）サービスリストクエリの周期。

コマンド デフォルト

ディセーブル

コマンド モード

mDNS コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

非要請アナウンスメントを送信しないデバイスがあるため、そのようなデバイスにサービスを強制的に学習させ、それらをキャッシュ内で最新に維持するために、このコマンドには、アクティブ クエリ リストに一覧されているサービスが確実にクエリされるようにするアクティブ クエリ機能が含まれています。

例

次に、サービス リストのクエリの周期を設定する例を示します。

```
デバイス(config-mdns)# service-policy-query sl-query1 100
```

service-routing mdns-sd

デバイスの mDNS ゲートウェイ機能を有効にし、マルチキャスト DNS コンフィギュレーション モードを開始するには、**service-routing mdns-sd** コマンドを使用します。デフォルト設定を復元し、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。

service-routing mdns-sd
no service-routing mdns-sd

このコマンドには引数またはキーワードはありません。

コマンド デフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン mDNS ゲートウェイ機能は、インターフェイス単位ではなく、グローバルでのみ有効または無効にすることができます。サービス フィルタ ポリシーと再配布は、グローバルでも、インターフェイス単位でも設定できます。インターフェイス固有の設定は、グローバルな設定より優先されます。

例

次に、デバイスの mDNS ゲートウェイ機能を有効にして、マルチキャスト DNS コンフィギュレーション モードを開始する例を示します。

```
デバイス(config)# service-routing mdns-sd
```

service-policy

サービスリストの着信または発信サービス検出情報にフィルタを適用するには、**service-policy** コマンドを使用します。フィルタを削除するには、このコマンドの **no** 形式を使用します。

service-policy *service-policy-name* {**IN** | **OUT**}
no service-policy *service-policy-name* {**IN** | **OUT**}

構文の説明

IN	着信サービス検出情報にフィルタを適用します。
OUT	発信サービス検出情報にフィルタを適用します。

コマンド デフォルト ディセーブル

コマンド モード mDNS コンフィギュレーション

コマンド履歴

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

例

次の例に、サービス リストの着信サービス検出情報にフィルタを適用する方法を示します。

```
デバイス(config-mdns)#  service-policy serv-pol1 IN
```

show ip igmp filter

Internet Group Management Protocol（IGMP）フィルタ情報を表示するには、特権 EXEC モードで **show ip igmp filter** コマンドを使用します。

show ip igmp ［**vrf** *vrf-name* ］ **filter**

構文の説明

vrf *vrf-name*	（任意）マルチキャスト VPN ルーティングおよび転送（VRF）インスタンスをサポートします。

コマンド デフォルト

IGMP フィルタは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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

show ip igmp filter コマンドは、deviceに定義されているすべてのフィルタに関する情報を表示します。

例

次に、**show ip igmp filter** コマンドの出力例を示します。

```
デバイス# show ip igmp filter

IGMP filter enabled
```

show ip igmp profile

設定済みのすべての Internet Group Management Protocol（IGMP）プロファイルまたは指定された IGMP プロファイルを表示するには、特権 EXEC モードで **show ip igmp profile** コマンドを使用します。

show ip igmp ［**vrf** *vrf-name*］ **profile** ［*profile number*］

構文の説明

vrf *vrf-name*	（任意）マルチキャスト VPN ルーティングおよび転送（VRF）インスタンスをサポートします。
profile number	（任意）表示する IGMP プロファイル番号。指定できる範囲は 1 ～ 4294967295 です。プロファイル番号が入力されていない場合、すべての IGMP プロファイルが表示されます。

コマンド デフォルト

IGMP プロファイルはデフォルトでは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

なし

例

次に、device のプロファイル番号 40 に対する **show ip igmp profile** コマンドの出力例を示します。

```
デバイス# show ip igmp profile 40
IGMP Profile 40
    permit
    range 233.1.1.1 233.255.255.255
```

次に、device に設定されているすべてのプロファイルに対する **show ip igmp profile** コマンドの出力例を示します。

```
デバイス# show ip igmp profile

IGMP Profile 3
    range 230.9.9.0 230.9.9.0
IGMP Profile 4
    permit
    range 229.9.9.0 229.255.255.255
```

show ip igmp membership

マルチキャストグループおよびチャネルの Internet Group Management Protocol（IGMP）メンバーシップ情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip igmp membership** コマンドを使用します。

show ip igmp membership [{*group-address group-name*}] [**tracked**] [**all**]

構文の説明

group-address	（任意）IGMP メンバーシップ情報を表示するマルチキャスト グループの IP アドレス。

group-name	（任意）IGMP メンバーシップ情報を表示するマルチキャスト グループの、ドメイン ネーム システム（DNS）ホスト テーブルで定義されている名前。
tracked	（任意）明示的なトラッキング機能が有効になっているマルチキャスト グループを表示します。
all	（任意）明示的なトラッキング機能が有効になっているマルチキャスト グループと有効になっていないマルチキャスト グループの詳細情報を表示します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

マルチキャスト グループおよびチャネルの IGMP メンバーシップ情報を表示するには、このコマンドを使用します。このコマンドを使用すると、マルチキャスト グループおよびチャネルのメンバーシップと明示的なトラッキングに関する詳細情報が表示されます。

例

次に、**show ip igmp membership tracked** コマンドの出力例を示します。

```
Device> show ip igmp membership tracked

Flags:A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, D - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP, the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (*,G))
Reporter:
       <ip-address> - last reporter if group is not explicitly tracked
       <n>/<m>      - <n> reporter in include mode,<m> reporter in exclude
 Channel/Group                  Reporter        Uptime   Exp.  Flags  Interface
 *,203.0.113.10                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.10        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.11                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.11        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.14                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.14        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.15                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.15        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.12                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.12        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.13                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.13        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.19                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.19        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.18                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.18        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.17                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.17        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.16                  1/0             00:20:46 stop  3AT    Gi1/0/24
```

```
192.168.0.2,203.0.113.16        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
*,203.0.113.40                  0/1             00:20:48 02:16 3LAT   Gi1/0/24
*,209.165.201.1                 10.34.34.1      00:20:48 02:16 3LT    Gi1/0/24
```

次の表で、この出力で表示される重要なフィールドについて説明します。

表 *23 : show ip igmp membership* のフィールドの説明

フィールド	説明
Channel/Group	(S, G) チャネルまたはマルチキャスト グループ フィルタリング エントリ。
Reporter	(S, G) チャネルまたはマルチキャスト グループ エントリを持つメンバーシップをレポートしているホストに関する情報を表示します。
Uptime	Uptime タイマーは、エントリが認識されている時間の長さ（時、分、および秒単位）です。
Exp.	Exp. タイマーは、エントリが期限切れになるまでの時間（分および秒単位）です。

フィールド	説明
Flags	エントリに関する情報を提供します。 • A：集約。(S, G) チャネルまたはマルチキャスト グループの集約情報が表示されていることを示します。 • T：トラッキング。マルチキャスト グループに明示的なトラッキング機能が設定されていることを示します。 • L：ローカル。ルータ自体がこのマルチキャスト グループまたはチャネルのトラフィックの受信に関与していることを示します。アプリケーションがこのトラフィックを受信するために、パケットがルータのプロセス レベルに送信されます。マルチキャストグループに関して **ip igmp join-group** コマンドが設定されている場合は、L フラグが設定されます。 • S：静的。インターフェイスでマルチキャスト グループまたはチャネルが転送されることを示します。インターフェイスで **ip igmp static-group** コマンドが設定されている場合は、S フラグが設定されます。 • V：仮想。マルチキャスト グループまたはチャネルのトラフィックを要求しているルータで Hoot & Holler などのサービスが実行されていることを示します。これらのサービスは、ファスト スイッチング パスで IP マルチキャスト トラフィックを処理できます。L フラグは、これらのアプリケーションによって設定されません。 • R：v3 によるレポート。このエントリに関して IGMP バージョン 3（IGMPv3）レポートが受信されたことを示します。 • I：v3lite。このエントリに関して IGMP バージョン 3 lite (IGMP v3lite）レポートが受信されたことを示します。 • D：URD。このエントリに関して URL Rendezvous Directory（URD）レポートが受信されたことを示します。 • M：SSM (S, G) チャネル。マルチキャスト グループのアドレスが Source Specific Multicast（SSM）の範囲内にあることを示します。 • 1、2、3：IGMP のバージョン。マルチキャスト グループが実行している IGMP のバージョン。
Interface	インターフェイスのタイプと番号。

関連コマンド

コマンド	説明
ip igmp explicit-tracking	IGMP バージョン 3 のホスト、グループ、およびチャンネルの明示的なトラッキングが有効になります。
ip igmp version	ルータが使用する IGMP のバージョンを設定します。

コマンド	説明
show ip igmp groups	ルータに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャスト グループを表示します。

show ip igmp snooping

deviceまたは VLAN の Internet Group Management Protocol（IGMP）スヌーピング構成を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip igmp snooping** コマンドを使用します。

show ip igmp snooping ［**groups** | **mrouter** | **querier**］ ［**vlan** *vlan-id*］［**detail**］

構文の説明

groups	（任意）IGMP スヌーピング マルチキャスト テーブルを表示します。
mrouter	（任意）IGMP スヌーピング マルチキャスト ルータ ポートを表示します。
querier	（任意）IGMP クエリアの設定情報と動作情報を表示します。
vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。
detail	（任意）動作状態の情報を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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。

文字列では、大文字と小文字が区別されます。たとえば、「|**exclude output**」と入力した場合、「output」を含む行は表示されませんが、「Output」を含む行は表示されます。

例

次に、**show ip igmp snooping vlan 1** コマンドの出力例を示します。ここでは、特定の VLAN のスヌーピング特性を表示します。

```
デバイス# show ip igmp snooping vlan 1
```

```
Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
```

次に、**show ip igmp snooping** コマンドの出力例を示します。ここでは、device 上のすべての VLAN のスヌーピング特性を表示します。

```
デバイス# show ip igmp snooping

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
Vlan 2:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
-
.
.
.
```

show ip igmp snooping groups

device またはマルチキャスト情報の Internet Group Management Protocol（IGMP）スヌーピング マルチキャスト テーブルを表示するには、特権 EXEC モードで **show ip igmp snooping groups** コマンドを使用します。

show ip igmp snooping groups ［**vlan** *vlan-id* ］［［**count**］ ｜ *ip_address*］

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。指定されたマルチキャスト VLAN のマルチキャスト テーブル、または特定のマルチキャスト情報を表示するには、このオプションを使用します。
count	（任意）実エントリの代わりに、指定のコマンド オプションのエントリ総数を表示します。
ip_address	（任意）指定グループ IP アドレスのマルチキャスト グループの特性を表示します。

コマンド モード

特権 EXEC

ユーザ EXEC

コマンド履歴

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

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、「|**exclude output**」と入力した場合、「output」を含む行は表示されませんが、「Output」を含む行は表示されます。

例

次に、キーワードを指定しない **show ip igmp snooping groups** コマンドの出力例を示します。device のマルチキャスト テーブルが表示されます。

```
デバイス# show ip igmp snooping groups

Vlan      Group           Type        Version     Port List
------------------------------------------------------------
1         224.1.4.4       igmp                    Gi1/0/11
1         224.1.4.5       igmp                    Gi1/0/11
2         224.0.1.40      igmp        v2          Gi1/0/15
104       224.1.4.2       igmp        v2          Gi2/0/1, Gi2/0/2
104       224.1.4.3       igmp        v2          Gi2/0/1, Gi2/0/2
```

次に、**show ip igmp snooping groups count** コマンドの出力例を示します。device 上のマルチキャスト グループの総数が表示されます。

```
デバイス# show ip igmp snooping groups count

Total number of multicast groups: 2
```

次に、**show ip igmp snooping groups vlan vlan-id ip-address** コマンドの出力例を示します。指定された IP アドレスのグループのエントリを表示します。

```
デバイス# show ip igmp snooping groups vlan 104 224.1.4.2

Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi2/0/1, Gi1/0/15
```

show ip igmp snooping membership

Internet Group Management Protocol Version 3（IGMPv3）ホストメンバーシップを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip igmp snooping membership** コマンドを使用します。

show ip igmp snooping membership [{**interface** *typenumber*}] [{**reporter** *reporter-ip-address*}] [{**source** *source-ip-address* **group** *group-ip-address*}] [{**vlan** *vlan-ID*}]

構文の説明

interface *type number*	（任意）指定されたインターフェイスのエントリを表示します。
reporter *reporter-ip-address*	（任意）マルチキャスト レポータ IP アドレスと一致するエントリを表示します。
source *source-ip-address*	（任意）マルチキャスト 送信元 IP アドレスと一致するエントリを表示します。
group *group-ip-address*	（任意）マルチキャスト グループ IP アドレスと一致するエントリを表示します。
vlan *vlan-ID*	（任意）指定された VLAN のエントリを表示します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

オプションの引数を省略すると、**show ip igmp snooping membership** コマンドにより、すべてのホストに関するメンバーシップ情報が表示されます。

例

次に、**show ip igmp snooping membership vlan** コマンドの出力例を示します。

```
Device# show ip igmp  snooping membership vlan  70

Snooping Membership Summary for Vlan 70
----------------------------------------
Total number of channels: 10000
Total number of hosts   : 2

Source/Group                 Interface Reporter        Uptime   Last-Join    Last-Leave
-------------------------------------------------------------------------------------------

10.60.60.10/209.165.201.1     Gi2/0/36  192.0.2.2       00:00:45 00:00:45     -

10.60.60.10/209.165.201.1     Gi2/0/36  192.0.2.10     00:00:59 00:19:54     00:18:54

10.60.60.10/209.165.201.2     Gi2/0/36  192.0.2.2       00:00:45 00:00:45
```

関連コマンド

Command	Description
ip igmp snooping vlan explicit-tracking	IGMP のホスト、グループ、およびチャンネルの明示的なトラッキングが有効になります。

show ip igmp snooping mrouter

deviceまたは指定されたマルチキャスト VLAN の Internet Group Management Protocol（IGMP）スヌーピングの動的に学習され、手動で設定されたマルチキャストルータポートを表示するには、特権 EXEC モードで **show ip igmp snooping mrouter** コマンドを使用します。

show ip igmp snooping mrouter ［**vlan** *vlan-id*］

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。範囲は 1 ～ 1001 と 1006 ～ 4094 です。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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。

マルチキャストVLAN レジストレーション（MVR）がイネーブルの場合、**show ip igmp snooping mrouter** コマンドは MVR マルチキャストルータの情報および IGMP スヌーピング情報を表示します。

式では大文字と小文字が区別されます。たとえば、「| exclude output」と入力した場合、output を含む行は表示されませんが、Output を含む行は表示されます。

例

次に、**show ip igmp snooping mrouter** コマンドの出力例を示します。deviceのマルチキャスト ルータ ポートを表示する方法を示します。

```
デバイス# show ip igmp snooping mrouter

Vlan    ports
----    -----
   1    Gi2/0/1(dynamic)
```

show ip igmp snooping querier

device で設定されている IGMP クエリアの設定と操作情報を表示するには、ユーザ EXEC モードで **show ip igmp snooping querier** コマンドを使用します。

show ip igmp snooping querier ［**vlan** *vlan-id*］ ［**detail** ］

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。範囲は 1 ～ 1001 と 1006 ～ 4094 です。
detail	（任意）IGMP クエリアの詳細情報を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

IGMP クエリ メッセージを送信する検出デバイス（クエリアとも呼ばれます）の IGMP バージョンと IP アドレスを表示するには、**show ip igmp snooping querier** コマンドを使用します。サブネットは複数のマルチキャスト ルータを保有できますが、IGMP クエリアは 1 つしか保有できません。IGMPv2 を実行しているサブネットでは、マルチキャスト ルータの 1 つがクエリアとして設定されます。クエリアには、レイヤ 3 device を指定できます。

show ip igmp snooping querier コマンド出力では、クエリアが検出された VLAN およびインターフェイスも表示されます。クエリアが device の場合、出力の Port フィールドには「Router」と表示されます。クエリアがルータの場合、出力の Port フィールドにはクエリアを学習したポート番号が表示されます。

show ip igmp snooping querier detail ユーザ EXEC コマンドは、**show ip igmp snooping querier** コマンドに似ています。ただし、**show ip igmp snooping querier** コマンドでは、device クエリアによって最後に検出されたデバイスの IP アドレスのみが表示されます。

show ip igmp snooping querier detail コマンドでは、device クエリアによって最後に検出されたデバイスの IP アドレスのほか、次の追加情報が表示されます。

- VLAN で選択されている IGMP クエリア
- VLAN で設定された device クエリア（存在する場合）に関連する設定情報と動作情報

式では大文字と小文字が区別されます。たとえば、「|**exclude output**」と入力した場合、output を含む行は表示されませんが、Output を含む行は表示されます。

例

次に、**show ip igmp snooping querier** コマンドの出力例を示します。

```
デバイス> show ip igmp snooping querier
Vlan      IP Address     IGMP Version        Port
-----------------------------------------------
1         172.20.50.11   v3                  Gi1/0/1
2         172.20.40.20   v2                  Router
```

次に、**show ip igmp snooping querier detail** コマンドの出力例を示します。

```
デバイス> show ip igmp snooping querier detail

Vlan      IP Address     IGMP Version   Port
-------------------------------------------------------------
1         1.1.1.1        v2             Fa8/0/1
Global IGMP device querier status

-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 0.0.0.0
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
Vlan 1:   IGMP device querier status
-----------------------------------------------------------
elected querier is 1.1.1.1         on port Fa8/0/1
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 10.1.1.65
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
operational state              : Non-Querier
operational version            : 2
tcn query pending count        : 0
```

show ip igmp snooping vlan

Catalyst VLAN のスヌーピング情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip igmp snooping vlan** コマンドを使用します。

show ip igmp snooping vlan *vlan-ID*

構文の説明

vlan-ID	VLAN ID。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

例

次に、**show ip igmp snooping vlan** コマンドの出力例を示します。

```
Device# show ip igmp snooping vlan 77

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping              : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 77:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Explicit host tracking               : Enabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
Device#
```

出力では情報が分かりやすく示されます。

関連コマンド

Command	Description
ip igmp snooping vlan explicit-tracking	IGMP のホスト、グループ、およびチャンネルの明示的なトラッキングが有効になります。

show ip pim autorp

Auto-RP に関するグローバル情報を表示するには、特権 EXEC モードで **show ip pim autorp** コマンドを使用します。

show ip pim autorp

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

Auto RP は、デフォルトでは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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Auto-RP が有効になっているか、無効になっているかを表示します。

例

次に、Auto-RP が有効になっている場合のコマンドの出力例を示します。

```
デバイス# show ip pim autorp

AutoRP Information:
  AutoRP is enabled.
  RP Discovery packet MTU is 0.
  224.0.1.40 is joined on GigabitEthernet1/0/1.

PIM AutoRP Statistics: Sent/Received
  RP Announce: 0/0, RP Discovery: 0/0
```

show ip pim bsr-router

Protocol Independent Multicast（PIM）ブートストラップルータ（BSR）プロトコル処理に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip pim bsr-router** コマンドを使用します。

show ip pim bsr-router

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

Auto-RP に加えて、BSR RP メソッドを設定できます。BSR RP メソッドを設定すると、このコマンドで BSR ルータの情報が表示されます。

次に、 **show ip pim bsr-router** コマンドの出力例を示します。

```
デバイス# show ip pim bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim bsr

Protocol Independent Multicast（PIM）ブートストラップルータ（BSR）プロトコル処理に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip pim bsr** コマンドを使用します。

show ip pim bsr

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

Auto-RP に加えて、BSR RP メソッドを設定できます。BSR RP メソッドを設定すると、このコマンドで BSR ルータの情報が表示されます。

次に、 **show ip pim bsr** コマンドの出力例を示します。

```
デバイス# show ip pim bsr

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim tunnel

インターフェイス上の Protocol Independent Multicast（PIM）レジスタのカプセル化およびカプセル化解除トンネルに関する情報を表示するには、 **show ip pim tunnel** コマンドを使用します。

show ip pim ［**vrf** *vrf:*］ **tunnel** ［**Tunnel** 名前 インターフェイス番号 | **verbose**］

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
Tunnel *interface-number*	（任意）トンネル インターフェイス番号を指定します。
verbose	（任意）MAC カプセル化ヘッダーおよびプラットフォーム固有情報などの追加情報を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

PIM トンネルインターフェイスに関する情報を表示するには、 **show ip pim tunnel** を使用します。

PIM トンネル インターフェイスは、PIM スパース モード（PIM-SM）登録プロセスの IPv4 マルチキャスト転送情報ベース（MFIB）で使用されます。IPv4 MFIB では、2 種類の PIM トンネル インターフェイスが使用されます。

- PIM カプセル化トンネル（PIM Encap トンネル）
- PIM カプセル化解除トンネル（PIM Decap トンネル）

PIM Encap トンネルは、（Auto-RP、ブートストラップ ルータ（BSR）、またはスタティック RP の設定を介して）グループからランデブー ポイント（RP）へのマッピングを学習するたびに動的に作成されます。PIM Encap トンネルは、送信元が直接接続されているファーストホップ代表ルータ（DR）から送信されるマルチキャスト パケットをカプセル化するために使用されます。

PIM Encap トンネルと同様、PIM Decap トンネル インターフェイスは動的に作成されますが、グループから RP へのマッピングを学習するたびに RP 上でのみ作成されます。PIM Decap トンネル インターフェイスは、PIM レジスタのカプセル化解除メッセージのために RP によって使用されます。

（注） PIM トンネルは実行コンフィギュレーションには表示されません。

PIM トンネル インターフェイスが作成されると、次の syslog メッセージが表示されます。

```
* %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel<interface_number>,
changed state to up
```

次に、RP から取得した **show ip pim tunnel** の出力例を示します。この出力は、RP 上の PIM Encap および Decap トンネルを確認するために使用されます。

```
デバイス# show ip pim tunnel

Tunnel0
   Type  : PIM Encap
  RP    : 70.70.70.1*
  Source: 70.70.70.1
Tunnel1*
  Type  : PIM Decap
  RP    : 70.70.70.1*
  Source: -R2#
```

（注） アスタリスク（*）は、そのルータが RP であることを示します。RP には、PIM Encap トンネル インターフェイスおよび PIM Decap トンネル インターフェイスが常にあるとは限りません。

show mdns cache

deviceの mDNS キャッシュ情報を表示するには、特権 EXEC モードで **show mdns cache** コマンドを使用します。

show mdns cache [**interface** *type number* | **name** *record-name* [**type** *record-type*] | **type** *record-type*]

構文の説明

interface *type-number*	（任意）mDNS キャッシュ情報を表示する特定のインターフェイスのタイプと番号を指定します。
name *record-name*	（任意）mDNS キャッシュ情報を表示する特定の名前を指定します。
type *record-type*	（任意）mDNS キャッシュ情報を表示する特定のタイプを指定します。

コマンド デフォルト なし

コマンド モード 特権 EXEC

ユーザ EXEC

コマンド履歴

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

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、「|**exclude output**」と入力した場合、output を含む行は表示されませんが、Output を含む行は表示されます。

例

次に、キーワードを指定しない **show mdns cache** コマンドの出力例を示します。

```
デバイス# show mdns cache

==========================================================================================
[<NAME>]
[<TYPE>][<CLASS>][<TTL>/Remaining][Accessed][If-name][Mac Address][<RR Record Data>]

_airplay._tcp.local                    PTR     IN      4500/4455         0        Vl121
 b878.2e33.c7c5 CAMPUS APPLE TV1._airplay._tcp.local

CAMPUS APPLE TV1._airplay._tcp.local SRV     IN      120/75            2        Vl121
 b878.2e33.c7c5 CAMPUS-APPLE-TV1.local

CAMPUS-APPLE-TV1.local                 A       IN      120/75            2        Vl121
 b878.2e33.c7c5  121.1.0.254

CAMPUS APPLE TV1._airplay._tcp.local TXT     IN      4500/4455         2        Vl121
 b878.2e33.c7c5  (162) 'deviceid=B8:78:2E:33:C7:C6'

                 'features=0x5a7ffff7''flags=0x4'

                 'model=AppleT~'~

_ipp._tcp.local                        PTR     IN      4500/4465         2        Vl2
 2894.0fed.447f  EPSON XP-400 Series._ipp._tcp.local

EPSON XP-400 Series._ipp._tcp.local  SRV     IN      120/85            2        Vl2
 2894.0fed.447f  EPSONC053AA.local

EPSONC053AA.local                      A       IN      120/85            2        Vl2
 2894.0fed.447f  121.1.0.251

EPSON XP-400 Series._ipp._tcp.local  TXT     IN      4500/4465         2        Vl2
 2894.0fed.447f  (384)'txtvers=1' N XP-400 Series'

                 'usbFG=EPSON''usb_MDL=XP~'~

_smb._tcp.local                        PTR     IN      4500/4465         2        Vl2
 2894.0fed.447f  EPSON XP-400 Series._smb._tcp.local

EPSON XP-400 Series._smb._tcp.local  SRV     IN      120/85            2        Vl2
 2894.0fed.447f  EPSONC053AA.local

EPSON XP-400 Series._smb._tcp.local  TXT     IN      4500/4465         2        Vl2
 2894.0fed.447f  (1)'' R2-Access1#
```

show mdns requests

deviceのレコード名とレコードタイプ情報を含む、未処理の mDNS 要求の情報を表示するには、特権 EXEC モードで **show mdns requests** コマンドを使用します。

show mdns requests [**detail** | **name** *record-name* | **type** *record-type* [**name** *record-name*]]

構文の説明

detail	詳細な mDNS 要求の情報を表示します。
name *record-name*	名前に基づいた詳細な mDNS 要求の情報を表示します。
type *record-type*	タイプに基づいた詳細な mDNS 要求の情報を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

ユーザ EXEC

コマンド履歴

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

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、「|exclude output」と入力した場合、output を含む行は表示されませんが、Output を含む行は表示されます。

例

次に、キーワードを指定しない **show mdns requests** コマンドの出力例を示します。

```
デバイス# show mdns requests
MDNS Outstanding Requests
==================================================
Request name  :   _airplay._tcp.local
Request type  :   PTR
Request class :   IN
--------------------------------------------------
Request name  :   *.*
Request type  :   PTR
Request class :   IN
```

show mdns statistics

device の mDNS 統計を表示するには、特権 EXEC モードで **show mdns statistics** コマンドを使用します。

show mdns statistics {**all** | **service-list** *list-name* | **service-policy** {**all** | **interface** *type-number* }}

構文の説明

all	サービス ポリシー、サービス リスト、インターフェイス情報を表示します。
service-list *list-name*	サービス リスト情報を表示します。
service-policy	サービス ポリシー情報を表示します。
interface *type number*	インターフェイス情報を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

ユーザ EXEC

コマンド履歴

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

使用上のガイドライン

式では大文字と小文字が区別されます。たとえば、「| **exclude output**」と入力した場合、「output」を含む行は表示されませんが、「Output」を含む行は表示されます。

例

次に、**show mdns statistics all** コマンドの出力例を示します。

```
デバイス# show mdns statistics all

 mDNS Statistics
 mDNS packets sent       : 0
 mDNS packets received   : 0
 mDNS packets dropped    : 0
 mDNS cache memory in use: 64224(bytes)
```

show platform software fed switch ip multicast

プラットフォーム依存 IP マルチキャストテーブルおよびその他の情報を表示するには、特権 EXEC モードで **show platform software fed switch ip multicast** コマンドを使用します。

show platform software fed switch{*switch-number* | **active** | **standby**}**ip multicast**{**groups** | **hardware**[{**detail**}] | **interfaces** | **retry**}

構文の説明

switch {*switch_num* | **active** | **standby** }	情報を表示するデバイス。 • *switch_num*：スイッチ ID を入力します。指定されたスイッチに関する情報を表示します。 • **active**：アクティブスイッチの情報を表示します。 • **standby**：存在する場合、スタンバイスイッチの情報を表示します。
groups	グループごとの IP マルチキャスト ルートを表示します。
hardware [**detail**]	ハードウェアにロードされた IP マルチキャスト ルートを表示します。任意指定の **detail** キーワードは、宛先インデックスおよびルートインデックスのポートメンバを表示するために使用します。
interfaces	IP マルチキャスト インターフェイスを表示します。
retry	リトライ キューの IP マルチキャスト ルートを表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカル サポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

例

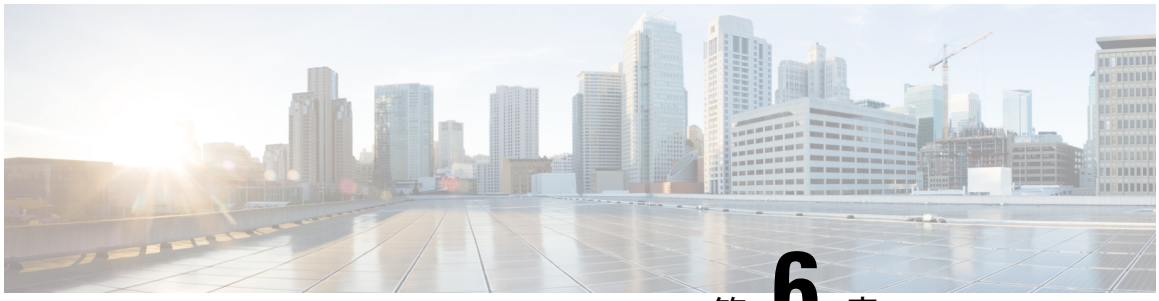
次に、グループごとのプラットフォーム IP マルチキャスト ルートを表示する例を示します。

```
デバイス# show platform software fed active ip multicast groups

Total Number of entries:3
MROUTE ENTRY vrf 0 (*, 224.0.0.0)
Token: 0x0000001f6  flags:  C
No RPF interface.
Number of OIF: 0
Flags: 0x10   Pkts : 0
OIF Details:No OIF interface.

DI details
----------
Handle:0x603cf7f8 Res-Type:ASIC_RSC_DI Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
Hardware Indices/Handles: index0:0x51f6  index1:0x51f6
```

```
Cookie length 56
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x4 0xe0 0x0 0x0 0x0 0x0 0x0

0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Detailed Resource Information (ASIC# 0)
---------------------------------------

al_rsc_di
RM:index = 0x51f6
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f6
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
---------------------------------------

al_rsc_di
RM:index = 0x51f6
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f6
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0

============================================================

<output truncated>
```

第 V 部

IPv6



第 6 章

IPv6 コマンド

ipv6 dhcp server vrf enable

DHCP for IPv6 サーバの VRF 認識型機能を有効にするには、グローバル コンフィギュレーション モードで **ipv6 dhcp server vrf 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。

ipv6 dhcp server vrf enable
no ipv6 dhcp server vrf 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

DHCPv6 サーバの VRF 認識型機能は有効になりません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

ipv6 dhcp server option vpn コマンドは DHCPv6 サーバの VRF 認識型機能をデバイス上でグローバルに有効にすることができます。

例

次に、DHCPv6 サーバの VRF 認識型機能をデバイス上でグローバルに有効にする例を示します。

```
デバイス(config)# ipv6 dhcp server option vpn
```

ipv6 flow monitor

このコマンドは、着信または発信トラフィックを分析するためにインターフェイスに割り当てることで、作成済みのフロー モニタをアクティブにします。

以前に作成したフローモニタをアクティブにするには、 **ipv6 flow monitor** コマンドを使用します。フローモニタを非アクティブにするには、このコマンドの **no** 形式を使用します。

ipv6 flow monitor *ipv6-monitor-name* [**sampler** *ipv6-sampler-name*] {**input** | **output**}
no ipv6 flow monitor *ipv6-monitor-name* [**sampler** *ipv6-sampler-name*] {**input** | **output**}

構文の説明

ipv6-monitor-name	着信または発信トラフィックを分析するためにインターフェイスに割り当てることで、作成済みのフローモニタをアクティブにします。
sampler *ipv6-sampler-name*	フロー モニタ サンプラーを適用します。
input	入力トラフィックにフロー モニタを適用します。
output	出力トラフィックにフロー モニタを適用します。

コマンド デフォルト

IPv6 フロー モニタは、インターフェイスに割り当てられるまでアクティブになりません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

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

使用上のガイドライン

ポート チャネル インターフェイスには NetFlow モニタを接続できません。サービス モジュールの両方のインターフェイスが EtherChannel の一部である場合、両方の物理インターフェイスにモニタを接続する必要があります。

次に、フロー モニタをインターフェイスに適用する例を示します。

```
デバイス(config)# interface gigabitethernet 1/1/2
デバイス(config-if)# ip flow monitor FLOW-MONITOR-1 input
デバイス(config-if)# ip flow monitor FLOW-MONITOR-2 output
デバイス(config-if)# end
```

show ipv6 dhcp binding

IPv6 サーバのバインディングテーブルの Dynamic Host Configuration Protocol（DHCP）から自動クライアントバインディングを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ipv6 dhcp binding** コマンドを使用します。

show ipv6 dhcp binding [*ipv6-address*] [**vrf** *vrf-name*]

構文の説明

ipv6-address	（任意）IPv6 クライアントの DHCP のアドレス。
vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

show ipv6 dhcp binding コマンドは、*ipv6-address* 引数を指定しないと、IPv6 サーバ バインディング テーブルの DHCP からすべての自動クライアントバインディングを表示します。*ipv6-address* 引数が指定されている場合、指定したクライアントのバインディングだけが表示されます。

vrf *vrf-name* キーワードと引数の組み合わせを使用すると、指定した VRF に属するすべてのバインディングが表示されます。

（注） 設定した VRF が機能するには、**ipv6 dhcp server vrf enable** コマンドをイネーブルにしておく必要があります。このコマンドが設定されていない場合、 **show ipv6 dhcp binding** コマンドの出力に設定した VRF が表示されず、デフォルトの VRF の詳細のみが表示されます。

例

次に、IPv6 サーバ バインディング テーブルの DHCP からすべての自動クライアント バインディングが表示された出力例を示します。

```
デバイス# show ipv6 dhcp binding

Client: FE80::A8BB:CCFF:FE00:300
  DUID: 00030001AABBCC000300
  Username : client_1
  Interface: Virtual-Access2.1
  IA PD: IA ID 0x000C0001, T1 75, T2 135
    Prefix: 2001:380:E00::/64
            preferred lifetime 150, valid lifetime 300
```

```
           expires at Dec 06 2007 12:57 PM (262 seconds)
Client: FE80::A8BB:CCFF:FE00:300 (Virtual-Access2.2)
  DUID: 00030001AABBCC000300
  IA PD: IA ID 0x000D0001, T1 75, T2 135
    Prefix: 2001:0DB8:E00:1::/64
           preferred lifetime 150, valid lifetime 300
           expires at Dec 06 2007 12:58 PM (288 seconds)
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *24 : show ipv6 dhcp binding* フィールドの説明

フィールド	説明
クライアント（Client）	指定したクライアントのアドレス。
DUID	DHCP 固有識別子（DUID）。
Virtual-Access2.1	最初の仮想クライアント。IPv6 DHCP クライアントが 2 つのプレフィックスを要求し、そのプレフィックスの DUID が同じで、プレフィックス委任（IAPD）に 2 つの異なるインターフェイスで異なる ID の関連付けがある場合、これらのプレフィックスは 2 つの異なるクライアント用として見なされ、両方のインターフェイス情報が保持されます。
Username : client_1	バインディングに関連付けられているユーザ名。
IA PD	クライアントに関連付けられているプレフィックスのコレクション。
IA ID	この IAPD の識別子。
Prefix	指定したクライアント上に指定された IAPD に委任されたプレフィックス。
preferred lifetime, valid lifetime	指定したクライアントの優先ライフタイムと有効なライフタイム設定（秒単位）。
Expires at	有効なライフタイムの有効期限が切れる日時。
Virtual-Access2.2	2 番目の仮想クライアント。IPv6 DHCP クライアントが 2 つのプレフィックスを要求し、そのプレフィックスの DUID が同じで IAID が 2 つの異なるインターフェイス上で異なる場合、これらのプレフィックスは 2 つの異なるクライアント用と見なされ、両方のインターフェイス情報が保持されます。

Cisco IOS DHCPv6 サーバの DHCPv6 プールを設定して、認証、認可、およびアカウンティング（AAA）サーバから委任のプレフィックスを取得すると、着信 PPP セッションから AAA サーバに PPP ユーザ名が送信され、プレフィックスを取得します。バインディングに関連付けられている PPP ユーザ名が **show ipv6 dhcp binding** コマンドの

出力に表示されます。バインディングに関連付けられている PPP ユーザ名がない場合、このフィールドには値として「unassigned」が表示されます。

次に、バインディングに関連付けられている PPP ユーザ名が「client_1」である例を示します。

```
デバイス# show ipv6 dhcp binding

Client: FE80::2AA:FF:FEBB:CC
  DUID: 0003000100AA00BB00CC
  Username : client_1
  Interface : Virtual-Access2
  IA PD: IA ID 0x00130001, T1 75, T2 135
    Prefix: 2001:0DB8:1:3::/80
            preferred lifetime 150, valid lifetime 300
            expires at Aug 07 2008 05:19 AM (225 seconds)
```

次に、バインディングに関連付けられている値が「unassigned」である例を示します。

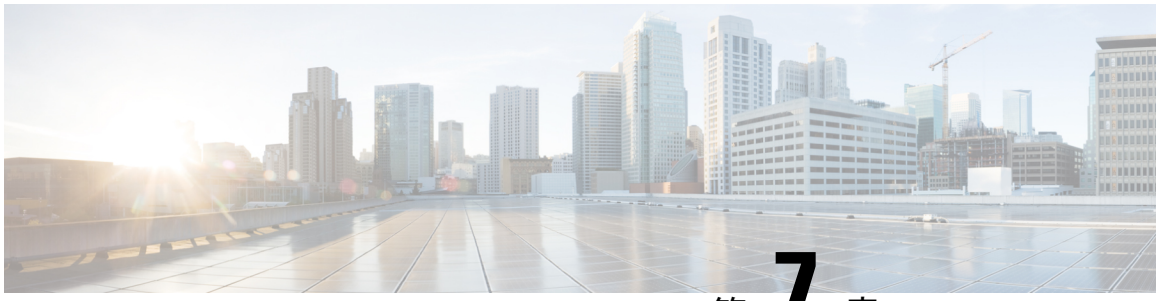
```
デバイス# show ipv6 dhcp binding

Client: FE80::2AA:FF:FEBB:CC
  DUID: 0003000100AA00BB00CC
  Username : unassigned
  Interface : Virtual-Access2
  IA PD: IA ID 0x00130001, T1 150, T2 240
    Prefix: 2001:0DB8:1:1::/80
            preferred lifetime 300, valid lifetime 300
            expires at Aug 11 2008 06:23 AM (233 seconds)
```

関連コマンド

Command	Description
ipv6 dhcp server vrf enable	DHCPv6 サーバ VRF 対応機能をイネーブルにします。
clear ipv6 dhcp binding	DHCP for IPv6 バインディング テーブルから自動クライアント バインディングを削除します。

第 VI 部

レイヤ 2/3



第 7 章

レイヤ 2/3 コマンド

channel-group

EtherChannel グループにイーサネットポートを割り当てる、EtherChannel モードをイネーブルにする、またはその両方を行うには、インターフェイス コンフィギュレーション モードで **channel-group** コマンドを使用します。EtherChannel グループからイーサネットポートを削除するには、このコマンドの **no** 形式を使用します。

channel-group { **auto** | *channel-group-number* **mode** {**active** | **auto** [**non-silent**] | **desirable** [**non-silent**] | **on** | **passive**} }
no channel-group

構文の説明

auto	個々のポート インターフェイスの auto-LAG 機能をイネーブルにします。 デフォルトでは、auto-LAG 機能は各ポート上でイネーブルになっています。
channel-group-number	チャネルグループ番号。指定できる範囲は 1 ～ 128 です。
mode	EtherChannel モードを指定します。

active	無条件に Link Aggregation Control Protocol（LACP）をイネーブルにします。
auto	Port Aggregation Protocol（PAgP）装置が検出された場合に限り、PAgP をイネーブルにします。
non-silent	（任意）PAgP 対応のパートナーに接続されたとき、インターフェイスを非サイレント動作に設定します。他の装置からのトラフィックが予想されている場合に PAgP モードで **auto** または **desirable** キーワードとともに使用されます。
desirable	無条件に PAgP をイネーブルにします。
on	on モードをイネーブルにします。
passive	LACP 装置が検出された場合に限り、LACP をイネーブルにします。

コマンド デフォルト

チャネルグループは割り当てることができません。

モードは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

レイヤ 2 の EtherChannel では、チャネルグループに最初の物理ポートが追加されると、**channel-group** コマンドがポートチャネル インターフェイスを自動的に作成します。ポートチャネル インターフェイスを手動で作成するためにグローバル コンフィギュレーション モードで **interface port-channel** コマンドを使用する必要はありません。最初にポートチャネル インターフェイスを作成する場合は、*channel-group-number* を *port-channel-number* と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポートチャネルを作成します。

チャネル グループの一部である物理ポートに割り当てられた IP アドレスをディセーブルにする必要はありませんが、これをディセーブルにすることを強く推奨します。

interface port-channel コマンドの次に **no switchport** 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、レイヤ3のポートチャネルを作成できます。インターフェイスをチャネル グループに適用する前に、ポート チャネルの論理インターフェイスを手動で設定してください。

EtherChannelを設定した後、ポートチャネルインターフェイスに加えられた設定の変更は、そのポートチャネルインターフェイスに割り当てられたすべての物理ポートに適用されます。物理ポートに適用された設定の変更は、設定を適用したポートだけに有効です。EtherChannel 内のすべてのポートのパラメータを変更するには、ポートチャネルインターフェイスに対してコンフィギュレーション コマンドを適用します。たとえば、spanning-tree コマンドを使用して、レイヤ 2 EtherChannel をトランクとして設定します。

active モードは、ポートをネゴシエーションステートにします。このステートでは、ポートは LACP パケットを送信することによって、他のポートとのネゴシエーションを開始します。チャネルは、active モードまたは passive モードの別のポートグループで形成されます。

auto モードは、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケットネゴシエーションを開始することはありません。チャネルは、desirable モードの別のポートグループでだけ形成されます。auto がイネーブルの場合、サイレント動作がデフォルトになります。

desirableモードは、ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、他のポートとのネゴシエーションを開始します。EtherChannel は、desirable モードまたは auto モードの別のポートグループで形成されます。desirable がイネーブルの場合、サイレント動作がデフォルトになります。

auto モードまたは desirable モードとともに non-silent を指定しなかった場合は、サイレントが指定されているものと見なされます。サイレントモードを設定するのは、PAgP 非対応で、かつほとんどパケットを送信しない装置に device を接続する場合です。サイレントパートナーの例は、トラフィックを生成しないファイルサーバ、またはパケットアナライザなどです。この場合、物理ポート上で稼働している PAgP は、そのポートを動作可能にしません。ただし、PAgP は動作可能で、チャネルグループにポートを付与したり、伝送用ポートを使用したりできます。リンクの両端はサイレントに設定することはできません。

onモードでは、使用可能なEtherChannelが存在するのは、両方の接続ポートグループがonモードになっている場合だけです。

注意 onモードの使用には注意が必要です。これは手動の設定であり、EtherChannelの両端のポートには、同一の設定が必要です。グループの設定を誤ると、パケット損失またはスパニングツリーループが発生することがあります。

passiveモードは、ポートをネゴシエーションステートにします。この場合、ポートは受信した LACP パケットに応答しますが、LACP パケットネゴシエーションを開始することはありません。チャネルは、active モードの別のポートグループでだけ形成されます。

EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP および LACP を実行している EtherChannel グループは、同一の device、またはスタックにある異なる devices 上で共存できます（クロススタック構成ではできません）。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。

channel-protocol インターフェイス コンフィギュレーション コマンドを使用してプロトコルを設定した場合、設定値は、**channel-group** インターフェイス コンフィギュレーション コマンドによっては上書きされません。

アクティブまたはまだアクティブでない EtherChannel メンバとなっているポートを、IEEE 802.1X ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1X 認証をイネーブルにしようとすると、エラー メッセージが表示され、IEEE 802.1X 認証はイネーブルになりません。

セキュアポートを EtherChannel の一部として、または EtherChannel ポートをセキュアポートとしては設定しないでください。

設定の注意事項の一覧については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

⚠

注意 物理 EtherChannel ポート上で、レイヤ 3 のアドレスをイネーブルにしないでください。物理 EtherChannel ポート上でブリッジグループを割り当てることは、ループが発生する原因になるため、行わないでください。

この例では、スタック内の 1 つの device に EtherChannel を設定する例を示します。VLAN 10 のスタティックアクセス ポート 2 つを PAgP モード desirable であるチャネル 5 に割り当てます。

```
デバイス# configure terminal
デバイス(config)# interface range GigabitEthernet 2/0/1 - 2
デバイス(config-if-range)# switchport mode access
デバイス(config-if-range)# switchport access vlan 10
デバイス(config-if-range)# channel-group 5 mode desirable
デバイス(config-if-range)# end
```

この例では、スタック内の 1 つの device に EtherChannel を設定する例を示します。VLAN 10 のスタティックアクセス ポート 2 つを LACP モード active であるチャネル 5 に割り当てます。

```
デバイス# configure terminal
デバイス(config)# interface range GigabitEthernet 2/0/1 - 2
デバイス(config-if-range)# switchport mode access
デバイス(config-if-range)# switchport access vlan 10
デバイス(config-if-range)# channel-group 5 mode active
デバイス(config-if-range)# end
```

次の例では、device スタックのクロススタック EtherChannel を設定する方法を示します。LACP パッシブモードを使用して、VLAN 10 内のスタティックアクセス ポートと

してスタックメンバ 2 のポートを 2 つ、スタックメンバ 3 のポートを 1 つチャネル 5 に割り当てます。

```
デバイス# configure terminal
デバイス(config)# interface range GigabitEthernet 2/0/4 - 5
デバイス(config-if-range)# switchport mode access
デバイス(config-if-range)# switchport access vlan 10
デバイス(config-if-range)# channel-group 5 mode passive
デバイス(config-if-range)# exit
デバイス(config)# interface GigabitEthernet 3/0/3
デバイス(config-if)# switchport mode access
デバイス(config-if)# switchport access vlan 10
デバイス(config-if)# channel-group 5 mode passive
デバイス(config-if)# exit
```

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

channel-protocol

ポート上で使用されるプロトコルを制限してチャネリングを管理するには、インターフェイス コンフィギュレーション モードで **channel-protocol** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

channel-protocol {**lacp** | **pagp**}
no channel-protocol

構文の説明

lacp	Link Aggregation Control Protocol（LACP）で EtherChannel を設定します。
pagp	Port Aggregation Protocol（PAgP）で EtherChannel を設定します。

コマンド デフォルト

EtherChannel に割り当てられているプロトコルはありません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

channel-protocol コマンドは、チャネルを LACP または PAgP に制限するためだけに使用します。**channel-protocol** コマンドを使用してプロトコルを設定する場合、設定は **channel-group** インターフェイス コンフィギュレーション コマンドで上書きされることはありません。

channel-group インターフェイス コンフィギュレーション コマンドは、EtherChannel のパラメータ設定に使用してください。また、**channel-group** コマンドは、EtherChannel に対しモードを設定することもできます。

EtherChannel グループ上で、PAgP および LACP モードの両方をイネーブルにすることはできません。

PAgP と LACP には互換性がありません。両方ともチャネルの終端は同じプロトコルを使用する必要があります。

クロススタック構成の PAgP を設定できません。

次の例では、EtherChannel を管理するプロトコルとして LACP を指定する方法を示します。

```
デバイス(config-if)# channel-protocol lacp
```

設定を確認するには、**show etherchannel** [*channel-group-number*] **protocol** 特権 EXEC コマンドを入力します。

clear lacp

Link Aggregation Control Protocol（LACP）チャネルグループカウンタをクリアするには、特権 EXEC モードで **clear lacp** コマンドを使用します。

clear lacp [*channel-group-number*] **counters**

構文の説明

channel-group-number	（任意）チャネルグループ番号。指定できる範囲は 1 ～ 128 です。
counters	トラフィックカウンタをクリアします。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

すべてのカウンタをクリアするには、**clear lacp counters** コマンドを使用します。また、指定のチャネルグループのカウンタのみをクリアするには、**clear lacp** *channel-group-number* **counters** コマンドを使用します。

次の例では、すべてのチャネルグループ情報をクリアする方法を示します。

```
デバイス# clear lacp counters
```

次の例では、グループ 4 の LACP トラフィックのカウンタをクリアする方法を示します。

```
デバイス# clear lacp 4 counters
```

情報が削除されたことを確認するには、**show lacp counters** または **show lacp** *channel-group-number* **counters** 特権 EXEC コマンドを使用します。

clear pagp

Port Aggregation Protocol（PAgP）チャネルグループ情報をクリアするには、特権 EXEC モードで **clear pagp** コマンドを使用します。

clear pagp [*channel-group-number*] **counters**

構文の説明

channel-group-number	（任意）チャネルグループ番号。指定できる範囲は 1 ～ 128 です。
counters	トラフィックカウンタをクリアします。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

すべてのカウンタをクリアするには、**clear pagp counters** コマンドを使用します。また、指定のチャネルグループのカウンタのみをクリアするには、**clear pagp** *channel-group-number* **counters** コマンドを使用します。

次の例では、すべてのチャネルグループ情報をクリアする方法を示します。

```
デバイス# clear pagp counters
```

次の例では、グループ 10 の PAgP トラフィックのカウンタをクリアする方法を示します。

```
デバイス# clear pagp 10 counters
```

情報が削除されたことを確認するには、**show pagp** 特権 EXEC コマンドを入力します。

clear spanning-tree counters

スパニングツリーのカウンタをクリアするには、特権EXECモードで**clear spanning-tree counters**コマンドを使用します。

clear spanning-tree counters ［**interface** *interface-id*］

構文の説明

interface *interface-id*	（任意）指定のインターフェイスのスパニングツリーカウンタをすべてクリアします。有効なインターフェイスとしては、物理ポート、VLAN、ポートチャネルなどがあります。 指定できる VLAN 範囲は 1 ～ 4094 です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

*interface-id*が指定されていない場合は、すべてのインターフェイスのスパニングツリーカウンタがクリアされます。

次の例では、すべてのインターフェイスのスパニングツリーカウンタをクリアする方法を示します。

```
デバイス# clear spanning-tree counters
```

clear spanning-tree detected-protocols

devicesでプロトコル移行プロセスを再開して、強制的にネイバーと再ネゴシエーションするには、特権 EXEC モードで **clear spanning-tree detected-protocols** コマンドを使用します。

clear spanning-tree detected-protocols [**interface** *interface-id*]

構文の説明	**interface** *interface-id*	（任意）指定されたインターフェイスでプロトコル移行プロセスを再開します。有効なインターフェイスとしては、物理ポート、VLAN、ポートチャネルなどがあります。 指定できる VLAN 範囲は 1 ～ 4094 です。 ポートチャネル範囲は 1 ～ 128 です。
コマンド デフォルト	なし	
コマンド モード	特権 EXEC	

コマンド履歴

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

使用上のガイドライン

Rapid Per-VLAN Spanning-Tree Plus（Rapid PVST+）プロトコルまたは Multiple Spanning Tree Protocol（MSTP）が稼働する device は、 組み込み済みのプロトコル移行方式をサポートしています。それによって、スイッチはレガシー IEEE 802.1D devices と相互に動作できるようになります。Rapid PVST+ または MSTP device が、プロトコルのバージョンが 0 に設定されているレガシー IEEE 802.1D コンフィギュレーションブリッジプロトコルデータユニット（BPDU）を受信した場合、その device はそのポートで IEEE 802.1D BPDU だけを送信します。マルチスパニングツリー（MST）device が、レガシー BPDU、別のリージョンに対応する MST BPDU（バージョン3）、または高速スパニングツリー（RST）BPDU（バージョン2）を受信したときは、そのポートがリージョンの境界にあることを検知します。

deviceは、IEEE 802.1D BPDU を受信しなくなった場合であっても、自動的には Rapid PVST+ モードまたはMSTPモードには戻りません。これは、レガシースイッチが指定スイッチでなければ、リンクから削除されたかどうかを学習できないためです。この状況では、**clear spanning-tree detected-protocols** コマンドを使用します。

次の例では、ポートでプロトコル移行プロセスを再開する方法を示します。

```
デバイス# clear spanning-tree detected-protocols interface gigabitethernet2/0/1
```

debug etherchannel

EtherChannel のデバッグをイネーブルにするには、特権 EXEC モードで **debug etherchannel** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug etherchannel [{**all** | **detail** | **error** | **event** | **idb** }]

no debug etherchannel [{**all** | **detail** | **error** | **event** | **idb** }]

構文の説明

all	（任意）EtherChannel デバッグ メッセージをすべて表示します。
detail	（任意）EtherChannel デバッグ メッセージの詳細を表示します。
error	（任意）EtherChannel エラー デバッグ メッセージを表示します。
event	（任意）EtherChannel イベント メッセージを表示します。
idb	（任意）PAgP インターフェイス記述子ブロック デバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

（注） **linecard** キーワードは、コマンドラインのヘルプに表示されますが、サポートされていません。

あるスタック上でデバッグをイネーブルにした場合、active switchでのみイネーブルになります。スタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してactive switchからセッションを開始します。スタンバイスイッチのコマンドラインプロンプトで **debug** コマンドを入力します。

active switchで最初にセッションを開始せずにスタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次の例では、すべての EtherChannel デバッグ メッセージを表示する方法を示します。

```
デバイス# debug etherchannel all
```

次の例では、EtherChannel イベント関連のデバッグ メッセージを表示する方法を示します。

```
デバイス# debug etherchannel event
```

debug lacp

Link Aggregation Control Protocol（LACP）アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug lacp** コマンドを使用します。LACP のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug lacp [{**all** | **event** | **fsm** | **misc** | **packet**}]
no debug lacp [{**all** | **event** | **fsm** | **misc** | **packet**}]

構文の説明

all	（任意）LACP デバッグ メッセージをすべて表示します。
event	（任意）LACP イベント デバッグ メッセージを表示します。
fsm	（任意） LACP有限状態マシン内の変更に関するメッセージを表示します。
misc	（任意）各種 LACP デバッグ メッセージを表示します。
packet	（任意）受信および送信 LACP 制御パケットを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

あるスタック上でデバッグをイネーブルにした場合、active switchでのみイネーブルになります。スタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してactive switchからセッションを開始します。スタンバイスイッチのコマンドラインプロンプトで **debug** コマンドを入力します。

active switchで最初にセッションを開始せずにスタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次の例では、すべての LACP デバッグ メッセージを表示する方法を示します。

```
デバイス# debug LACP all
```

次の例では、LACPイベントに関連するデバッグ メッセージを表示する方法を示します。

```
デバイス# debug LACP event
```

debug pagp

Port Aggregation Protocol（PAgP）アクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug pagp** コマンドを使用します。PAgP のデバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug pagp [{**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**}]
no debug pagp [{**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**}]

構文の説明

all	（任意）PAgP デバッグ メッセージをすべて表示します。
dual-active	（任意）デュアル アクティブ検出メッセージを表示します。
event	（任意）PAgP イベント デバッグ メッセージを表示します。
fsm	（任意）PAgP 有限状態マシン内の変更に関するメッセージを表示します。
misc	（任意）各種 PAgP デバッグ メッセージを表示します。
packet	（任意）送受信 PAgP 制御パケットを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

あるスタック上でデバッグをイネーブルにした場合、active switchでのみイネーブルになります。スタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してactive switchからセッションを開始します。スタンバイスイッチのコマンドラインプロンプトで **debug** コマンドを入力します。

active switchで最初にセッションを開始せずにスタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次の例では、すべての PAgP デバッグ メッセージを表示する方法を示します。

```
デバイス# debug pagp all
```

次の例では、PAgP イベントに関連するデバッグ メッセージを表示する方法を示します。

```
デバイス# debug pagp event
```

debug platform pm

プラットフォーム依存ポート マネージャ ソフトウェア モジュールのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform pm** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

構文の説明

all	すべてのポート マネージャ デバッグ メッセージを表示します。
counters	リモートプロシージャ コール（RPC）デバッグ メッセージのカウンタを表示します。
errdisable	error-disabled 関連イベント デバッグ メッセージを表示します。
if-numbers	インターフェイス番号移動イベントデバッグ メッセージを表示します。
link-status	インターフェイス リンク検出イベント デバッグ メッセージを表示します。
platform	ポート マネージャ関数イベント デバッグ メッセージを表示します。
pm-vectors	ポートマネージャ ベクトル関連イベントデバッグ メッセージを表示します。
detail	（任意）ベクトル関数の詳細を表示します。
vlans	VLAN 作成および削除イベント デバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

あるスタック上でデバッグをイネーブルにした場合、active switchでのみイネーブルになります。スタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してactive switchからセッションを開始します。スタンバイスイッチのコマンドラインプロンプトで **debug** コマンドを入力します。

active switchで最初にセッションを開始せずにスタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次に、VLAN の作成および削除に関するデバッグ メッセージを表示する例を示します。

```
デバイス# debug platform pm vlans
```

debug platform udld

プラットフォーム依存の単方向リンク検出（UDLD）ソフトウェアのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform udld** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

構文の説明

error	（任意）エラー条件デバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

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

debug spanning-tree

スパニングツリー アクティビティのデバッグをイネーブルにするには、EXEC モードで **debug spanning-tree** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug spanning-tree {**all** | **backbonefast** | **bpdu** | **bpdu-opt** | **config** | **etherchannel** | **events** | **exceptions** | **general** | **ha** | **mstp** | **pvst+** | **root** | **snmp** | **synchronization** | **switch** | **uplinkfast**}
no debug spanning-tree {**all** | **backbonefast** | **bpdu** | **bpdu-opt** | **config** | **etherchannel** | **events** | **exceptions** | **general** | **mstp** | **pvst+** | **root** | **snmp** | **synchronization** | **switch** | **uplinkfast**}

構文の説明

all	スパニングツリーのデバッグ メッセージをすべて表示します。
backbonefast	BackboneFast イベント デバッグ メッセージを表示します。
bpdu	スパニングツリーブリッジプロトコル データ ユニット（BPDU）デバッグ メッセージを表示します。
bpdu-opt	最適化された BPDU 処理デバッグ メッセージを表示します。
config	スパニングツリー設定変更デバッグ メッセージを表示します。
etherchannel	EtherChannel サポート デバッグ メッセージを表示します。
events	スパニングツリー トポロジ イベント デバッグ メッセージを表示します。
exceptions	スパニングツリー例外デバッグ メッセージを表示します。
general	一般的なスパニングツリーアクティビティデバッグ メッセージを表示します。
ha	高可用性スパニングツリー デバッグ メッセージを表示します。
mstp	Multiple Spanning Tree Protocol（MSTP）イベントをデバッグします。
pvst+	Per VLAN Spanning-Tree Plus（PVST+）イベント デバッグ メッセージを表示します。
root	スパニングツリー ルート イベント デバッグ メッセージを表示します。
snmp	スパニングツリーの Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）処理デバッグ メッセージを表示します。
switch	device シム コマンド デバッグ メッセージを表示します。このシムは、一般的なスパニングツリープロトコル（STP）コードと、各deviceプラットフォーム固有コードとの間のインターフェイスとなるソフトウェアモジュールです。

synchronization	スパニングツリー同期イベントデバッグメッセージを表示します。
uplinkfast	UplinkFast イベント デバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

undebug spanning-tree コマンドは **no debug spanning-tree** コマンドと同じです。

あるスタック上でデバッグをイネーブルにした場合、active switchでのみイネーブルになります。スタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **session** *switch-number* コマンドを使用してactive switchからセッションを開始します。スタンバイスイッチのコマンドラインプロンプトで **debug** コマンドを入力します。

active switchで最初にセッションを開始せずにスタンバイスイッチでデバッグをイネーブルにするには、特権 EXEC モードで **remote command** *switch-number LINE* コマンドを使用します。

次の例では、すべてのスパニングツリーデバッグ メッセージを表示する方法を示します。

```
デバイス# debug spanning-tree all
```

interface port-channel

ポートチャネルにアクセスするか、またはポートチャネルを作成するには、グローバル コンフィギュレーション モードで **interface port-channel** コマンドを使用します。ポートチャネルを削除するには、このコマンドの **no** 形式を使用します。

interface port-channel *port-channel-number*
no interface port-channel

構文の説明

port-channel-number	チャネルグループ番号。指定できる範囲は1～128です。

コマンド デフォルト

ポートチャネル論理インターフェイスは定義されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

レイヤ 2 EtherChannel では、物理ポートをチャネルグループに割り当てる前にポートチャネル インターフェイスを作成する必要はありません。代わりに、**channel-group** インターフェイス コンフィギュレーション コマンドを使用できます。このコマンドでは、チャネルグループが最初の物理ポートを獲得すると、ポートチャネル論理インターフェイスが自動的に作成されます。最初にポートチャネル インターフェイスを作成する場合は、*channel-group-number* を *port-channel-number* と同じ番号にしても、新しい番号にしてもかまいません。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポートチャネルを作成します。

interface port-channel コマンドの次に **no switchport** 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、レイヤ3のポートチャネルを作成できます。インターフェイスをチャネルグループに適用する前に、ポートチャネルの論理インターフェイスを手動で設定してください。

チャネル グループ内の 1 つのポートチャネルだけが許可されます。

⚠

注意 ポートチャネルインターフェイスをルーテッドポートとして使用する場合、チャネルグループに割り当てられた物理ポート上のレイヤ3に、アドレスを割り当てないようにしてください。

⚠

注意 レイヤ 3 のポートチャネル インターフェイスとして使用されているチャネルグループの物理ポート上で、ブリッジグループを割り当てることは、ループ発生の原因になるため行わないようにしてください。スパニングツリーもディセーブルにする必要があります。

interface port-channel コマンドを使用するときは、次のガイドラインに従ってください。

- Cisco Discovery Protocol（CDP）を使用する場合には、これを物理ポートで設定してください。ポートチャネル インターフェイスでは設定できません。
- EtherChannel のアクティブメンバであるポートを IEEE 802.1X ポートとしては設定しないでください。まだアクティブになっていない EtherChannel のポートで IEEE 802.1X をイネーブルにしても、ポートは EtherChannel に加入しません。

設定の注意事項の一覧については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Configuring EtherChannels」の章を参照してください。

次の例では、ポートチャネル番号 5 でポートチャネル インターフェイスを作成する方法を示します。

```
デバイス(config)# interface port-channel 5
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel** *channel-group-number* **detail** 特権 EXEC コマンドを入力します。

lacp max-bundle

ポートチャネルで許可されるアクティブ LACP ポートの最大数を定義するには、インターフェイス コンフィギュレーション モードで **lacp max-bundle** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp max-bundle *max_bundle_number*
no lacp max-bundle

構文の説明

max_bundle_number	ポートチャネルのアクティブ LACP ポートの最大数。指定できる範囲は 1 ～ 8 です。デフォルト値は 8 です。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

LACP チャネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 個をアクティブに、最大 8 個をホットスタンバイ モードにできます。LACP チャネルグループに 9 つ以上のポートがある場合、リンクの制御側終端にある device は、ポートプライオリティを使用して、チャネルにバンドルするポートおよびホットスタンバイモードに置くポートを判別します。他の device（リンクの非制御側終端）上のポートプライオリティは無視されます。

lacp max-bundle コマンドには、**port-channel min-links** コマンドで指定される数より大きい数を指定する必要があります。

ホットスタンバイモード（ポートステートフラグの H で出力に表示）にあるポートを判断するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

次に、ポート チャネル 2 で最大 5 個のアクティブ LACP ポートを指定する例を示します。

```
デバイス(config)# interface port-channel 2
デバイス(config-if)# lacp max-bundle 5
```

lacp port-priority

Link Aggregation Control Protocol（LACP）のポートプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **lacp port-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp port-priority *priority*
no lacp port-priority

構文の説明

priority	LACP のポート プライオリティ。指定できる範囲は 1 ～ 65535 です。

コマンド デフォルト

デフォルトは 32768 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

lacp port-priority インターフェイス コンフィギュレーション コマンドは、LACP チャネル グループに 9 つ以上のポートがある場合、バンドルされるポートと、ホットスタンバイ モードに置かれるポートを判別します。

LACP チャネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。

ポート プライオリティの比較では、数値が小さいほどプライオリティが高くなります。LACP チャネル グループに 9 つ以上のポートがある場合、LACP ポート プライオリティの数値が小さい（つまり、高いプライオリティ値の）8 つのポートがチャネル グループにバンドルされ、それより低いプライオリティのポートはホットスタンバイ モードに置かれます。LACP ポート プライオリティが同じポートが 2 つ以上ある場合（たとえば、そのいずれもデフォルト設定の 65535 に設定されている場合）、ポート番号の内部値によりプライオリティが決定されます。

（注） LACP リンクを制御する device 上にポートがある場合に限り、LACP ポートプライオリティは有効です。リンクを制御する device の判別については、**lacp system-priority** グローバル コンフィギュレーション コマンドを参照してください。

LACP ポートプライオリティおよび内部ポート番号値を表示するには、**show lacp internal** 特権 EXEC コマンドを使用します。

物理ポート上での LACP の設定については、このリリースに対応する構成ガイドを参照してください。

次の例では、ポートで LACP ポート プライオリティを設定する方法を示します。

```
デバイス# interface gigabitethernet2/0/1
デバイス(config-if)# lacp port-priority 1000
```

設定を確認するには、**show lacp** [*channel-group-number*] **internal** 特権 EXEC コマンドを入力します。

lacp rate

Link Aggregation Control Protocol（LACP）制御パケットが LACP がサポートされているインターフェイスに入力されるレートを設定するには、インターフェイス コンフィギュレーション モードで **lacp rate** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp rate {**normal** | **fast**}
no lacp rate

構文の説明

normal	LACP 制御パケットが通常レート（リンクのバンドル後、30 秒間隔）で入力されるように指定します。
fast	LACP 制御パケットが高速レート（1 秒に 1 回）で入力されるように指定します。

コマンド デフォルト

制御パケットのデフォルトの入力レートは、リンクがバンドルされた後、30 秒間隔です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.1	このコマンドが導入されました。

使用上のガイドライン

LACP タイムアウトの期間を変更するには、このコマンドを使用します。シスコ スイッチの LACP タイムアウト値はインターフェイスで LACP レートの 3 倍に設定されます。**lacp rate** コマンドを使用して、スイッチの LACP タイムアウト値として 90 秒または 3 秒のいずれかを選択できます。

このコマンドは、LACP がイネーブルになっているインターフェイスでのみサポートされます。

次に、インターフェイス GigabitEthernet 0/0 の高速（1 秒）入力レートを指定する例を示します。

```
デバイス(config)# interface gigabitEthernet 0/0
デバイス(config-if)# lacp rate fast
```

lacp system-priority

Link Aggregation Control Protocol（LACP）のシステムプライオリティを設定するには、deviceのグローバル コンフィギュレーション モードで **lacp system-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

lacp system-priority *priority*
no lacp system-priority

構文の説明

priority	LACP のシステム プライオリティ。指定できる範囲は 1 ～ 65535 です。

コマンド デフォルト

デフォルトは 32768 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

lacp system-priority コマンドでは、ポートプライオリティを制御する LACP リンクの device が判別されます。

LACP チャネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。LACP チャネルグループに 9 つ以上のポートがある場合、リンクの制御側終端にある device は、ポートプライオリティを使用して、チャネルにバンドルするポートおよびホットスタンバイモードに置くポートを判別します。他の device（リンクの非制御側終端）上のポートプライオリティは無視されます。

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。したがって、LACP システムプライオリティの数値が小さい（プライオリティ値の高い）システムが制御システムとなります。どちらの devices も同じ LACP システムプライオリティである場合（たとえば、どちらもデフォルト設定の 32768 が設定されている場合）、LACP システム ID（device の MAC アドレス）により制御する device が判別されます。

lacp system-priority コマンドは、device 上のすべての LACP EtherChannel に適用されます。

ホットスタンバイモード（ポートステートフラグの H で出力に表示）にあるポートを判断するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

次の例では、LACP のシステム プライオリティを設定する方法を示します。

```
デバイス(config)# lacp system-priority 20000
```

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

pagp learn-method

EtherChannel ポートから受信した着信パケットの送信元アドレスを学習するには、インターフェイス コンフィギュレーション モードで **pagp learn-method** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pagp learn-method {**aggregation-port** | **physical-port**}
no pagp learn-method

構文の説明

aggregation-port	論理ポート チャネルでのアドレス ラーニングを指定します。device は、EtherChannel のいずれかのポートを使用して送信元にパケットを送信します。この設定は、デフォルトです。集約ポート ラーニングの場合、どの物理ポートにパケットが届くかは重要ではありません。
physical-port	EtherChannel 内の物理ポートでのアドレス ラーニングを指定します。device は、送信元アドレスを学習したものと同じ EtherChannel 内のポートを使用して送信元へパケットを送信します。チャネルのもう一方の終端では、特定の宛先 MAC または IP アドレスに対してチャネル内の同じポートが使用されます。

コマンド デフォルト

デフォルトは、aggregation-port（論理ポート チャネル）です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

学習方式は、リンクの両端で同一の設定にする必要があります。

コマンドライン インターフェイス（CLI）で **physical-port** キーワードが指定された場合でも、device がサポートするのは集約ポートでのアドレスラーニングのみです。**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドは device のハードウェアには影響を及ぼしませんが、物理ポートによるアドレスラーニングのみをサポートしているデバイスと PAgP の相互運用性を確保するために必要です。

device のリンクパートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して物理ポートラーナーとして device を設定することを推奨します。また、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用して、送信元 MAC アドレスに基づいて負荷分散方式を設定することを推奨します。**pagp learn-method** インターフェイス コンフィギュレーション コマンドは、このような場合にのみ使用してください。

次の例では、EtherChannel 内の物理ポート上のアドレスを学習するように学習方式を設定する方法を示します。

```
デバイス(config-if)# pagp learn-method physical-port
```

次の例では、EtherChannel 内のポート チャネル上のアドレスを学習するように学習方式を設定する方法を示します。

```
デバイス(config-if)# pagp learn-method aggregation-port
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp** *channel-group-number* **internal** 特権 EXEC コマンドを入力します。

pagp port-priority

EtherChannel を経由してすべての Port Aggregation Protocol（PAgP）トラフィックが送信されるポートを選択するには、インターフェイス コンフィギュレーション モードで **pagp port-priority** コマンドを使用します。EtherChannel で使用されていないすべてのポートがホットスタンバイ モードにあり、現在選択されているポートやリンクに障害が発生した場合、これらのポートは稼働状態にできます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pagp port-priority *priority*
no pagp port-priority

構文の説明

priority	プライオリティ番号。有効な範囲は 0 ～ 255 です。

コマンド デフォルト

デフォルト値は 128 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

同じ EtherChannel 内で動作可能でメンバーシップを持つ物理ポートの中で最も高いプライオリティを持つポートが、PAgP 送信用として選択されます。

コマンドライン インターフェイス（CLI）で **physical-port** キーワードが指定された場合でも、deviceがサポートするのは集約ポートでのアドレスラーニングのみです。**pagp learn-method** および **pagp port-priority** インターフェイス コンフィギュレーション コマンドはdeviceのハードウェアには影響を及ぼしませんが、Catalyst 1900 スイッチなど、物理ポートによるアドレスラーニングのみをサポートしているデバイスと PAgP の相互運用性を確保するために必要です。

deviceのリンクパートナーが物理ラーナーである場合、**pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して物理ポートラーナーとしてdeviceを設定することを推奨します。また、**port-channel load-balance src-mac** グローバル コンフィギュレーション コマンドを使用して、送信元MACアドレスに基づいて負荷分散方式を設定することを推奨します。**pagp learn-method** インターフェイス コンフィギュレーション コマンドは、このような場合にのみ使用してください。

次の例では、ポート プライオリティを 200 に設定する方法を示します。

```
デバイス(config-if)# pagp port-priority 200
```

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show pagp** *channel-group-number* **internal** 特権 EXEC コマンドを入力します。

port-channel

自動作成された EtherChannel を手動チャネルに変換して、設定を EtherChannel に追加するには、特権 EXEC モードで **port-channel** コマンドを使用します。

port-channel {*channel-group-number* **persistent** | **persistent** }

構文の説明

channel-group-number	チャネルグループ番号。指定できる範囲は 1 ～ 128 です。
persistent	自動作成された EtherChannel を手動チャネルに変更し、EtherChannel への設定の追加を許可します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.2E	このコマンドが導入されました。

使用上のガイドライン

EtherChannel の情報を表示するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

例

この例では、自動作成されたEtherChannelを手動チャネルに変換する方法を示します。

```
デバイス# port-channel 1 persistent
```

port-channel auto

スイッチ上の Auto-LAG 機能をグローバルで有効にするには、グローバル コンフィギュレーション モードで **port-channel auto** コマンドを使用します。スイッチ上の Auto-LAG 機能をグローバルで無効にするには、このコマンドの **no** 形式を使用します。

port-channel auto
no port-channel auto

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、Auto-LAG 機能がグローバルで無効にされ、すべてのポート インターフェイス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

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.2E	このコマンドが導入されました。

使用上のガイドライン

EtherChannel が自動作成されたかどうかを確認するには、**show etherchannel auto** 特権 EXEC コマンドを使用します。

例

次に、スイッチの Auto-LAG 機能を有効にする例を示します。

```
デバイス(config)# port-channel auto
```

port-channel load-balance

EtherChannel のポート間での負荷分散方式を設定するには、グローバル コンフィギュレーション モードで **port-channel load-balance** コマンドを使用します。ロードバランシング メカニズムをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel load-balance {**dst-ip** | **dst-mac** | **dst-mixed-ip-port** | **dst-port** | **extended** | **src-dst-ip** | **src-dst-mac** | **src-dst-mixed-ip-port** | **src-dst-port** | **src-ip** | **src-mac** | **src-mixed-ip-port** | **src-port**}
no port-channel load-balance

構文の説明

dst-ip	宛先ホストの IP アドレスに基づいた負荷分散を指定します。
dst-mac	宛先ホストの MAC アドレスに基づいた負荷分散を指定します。同一の宛先に対するパケットは同一のポートに送信され、異なる宛先のパケットはチャネルの異なるポートに送信されます。

dst-mixed-ip-port	宛先 IPv4 または IPv6 アドレスと TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。
dst-port	宛先 TCP/UDP（レイヤ 4）と IPv4 と IPv6 の両方のポート番号に基づいて負荷分散を指定します。
extended	EtherChannel のポート間の拡張ロード バランス方式を設定します。**port-channel load-balance extended** コマンドを参照してください。
src-dst-ip	送信元および宛先ホストの IP アドレスに基づいて負荷分散を指定します。
src-dst-mac	送信元および宛先ホストの MAC アドレスに基づいた負荷分散を指定します。
src-dst-mixed-ip-port	送信元および宛先のホスト IP アドレスと TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。
src-dst-port	送信元および宛先の TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。
src-ip	送信元ホストの IP アドレスに基づいた負荷分散を指定します。
src-mac	送信元の MAC アドレスに基づいた負荷分散を指定します。異なるホストからのパケットは、チャネルで異なるポートを使用し、同一のホストからのパケットは同一のポートを使用します。
src-mixed-ip-port	送信元ホスト IP アドレスと TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。
src-port	TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。

コマンド デフォルト

デフォルトは **src-mac** です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel load-balance** 特権 EXEC コマンドを入力します。

例

次の例では、負荷分散方式を dst-mac に設定する方法を示します。

```
デバイス(config)# port-channel load-balance dst-mac
```

port-channel load-balance extended

EtherChannelのポート間での負荷分散方式の組み合わせを設定するには、グローバル コンフィギュレーション モードで **port-channel load-balance extended** コマンドを使用します。拡張ロードバランシング メカニズムをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel load-balance extended[{**dst-ip** | **dst-mac** | **dst-port** | **ipv6-label** | **l3-proto** | **src-ip** | **src-mac** | **src-port**}]
no port-channel load-balance extended

構文の説明

dst-ip	（任意）宛先ホストの IP アドレスに基づいて負荷分散を指定します。
dst-mac	（任意）宛先ホストの MAC アドレスに基づいて負荷分散を指定します。同一の宛先に対するパケットは同一のポートに送信され、異なる宛先のパケットはチャネルの異なるポートに送信されます。
dst-port	（任意）IPv4 と IPv6 両方の宛先 TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。
ipv6-label	（任意）送信元MACアドレスとIPv6フローラベルに基づいて負荷分散を指定します。
l3-proto	（任意）送信元 MAC アドレスとレイヤ 3 プロトコルに基づいて負荷分散を指定します。
src-ip	（任意）送信元ホストの IP アドレスに基づいて負荷分散を指定します。
src-mac	（任意）送信元の MAC アドレスに基づいて負荷分散を指定します。異なるホストからのパケットは、チャネルで異なるポートを使用し、同一のホストからのパケットは同一のポートを使用します。
src-port	（任意）TCP/UDP（レイヤ 4）ポート番号に基づいて負荷分散を指定します。

コマンド デフォルト

デフォルトは **src-mac** です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

どのような場合にこれらの転送方式を使用するかについては、このリリースの『*Layer 2/3 Configuration Guide (Catalyst 3650 Switches)*』を参照してください。

設定を確認するには、**show running-config** 特権 EXEC コマンドまたは **show etherchannel load-balance** 特権 EXEC コマンドを入力します。

例

次に、拡張負荷分散方式を設定する例を示します。

```
デバイス(config)# port-channel load-balance extended dst-ip dst-mac src-ip
```

port-channel min-links

ポートチャネルがアクティブになるように、リンクアップ状態で、EtherChannel にバンドルする必要がある LACP ポートの最小数を定義するには、インターフェイス コンフィギュレーション モードで **port-channel min-links** 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。

port-channel min-links *min_links_number*
no port-channel min-links

構文の説明

min_links_number	ポートチャネル内のアクティブな LACP ポートの最小数。指定できる範囲は 2 ～ 8 です。デフォルトは 1 です。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

LACP チャネル グループは、同じタイプのイーサネット ポートを 16 個まで保有できます。最大 8 個をアクティブに、最大 8 個をホットスタンバイ モードにできます。LACP チャネルグループに 9 つ以上のポートがある場合、リンクの制御側終端にある device は、ポートプライオリティを使用して、チャネルにバンドルするポートおよびホットスタンバイモードに置くポートを判別します。他の device（リンクの非制御側終端）上のポートプライオリティは無視されます。

port-channel min-links コマンドには、**lacp max-bundle** コマンドで指定される数より小さい数を指定する必要があります。

ホットスタンバイモード（ポートステートフラグの H で出力に表示）にあるポートを判断するには、**show etherchannel summary** 特権 EXEC コマンドを使用します。

次に、ポート チャネル 2 がアクティブになる前に、少なくとも 3 個のアクティブな LACP ポートを指定する例を示します。

```
デバイス(config)# interface port-channel 2
デバイス(config-if)# port-channel min-links 3
```

rep admin vlan

Resilient Ethernet Protocol（REP）の REP 管理 VLAN を設定して、ハードウェアフラッドレイヤ（HFL）メッセージを送信するには、グローバル コンフィギュレーション モードで **rep admin vlan** コマンドを使用します。VLAN 1 が管理 VLAN になるようにデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

rep admin vlan *vlan-id*
no rep admin vlan

構文の説明

vlan-id	48 ビット静的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 Denali 16.2.2	このコマンドが導入されました。

使用上のガイドライン

REP 管理 VLAN の範囲は 1 ～ 4094 です。

デバイスとセグメントで 1 つの管理 VLAN だけが可能です。

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

例

次に、VLAN 100 を REP 管理 VLAN として設定する例を示します。

```
デバイス(config)# rep admin vlan 100
```

関連コマンド

コマンド	説明
show interfaces rep detail	管理 VLAN を含め、すべてのインターフェイスまたは指定したインターフェイスの詳細 REP 設定およびステータスを表示します。

rep block port

Resilient Ethernet Protocol（REP）プライマリエッジポートで REP VLAN ロードバランシングを設定するには、インターフェイス コンフィギュレーション モードで **rep block port** コマンドを使用します。VLAN 1 が管理 VLAN になるようにデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

rep block port {id *port-id* | *neighbor-offset* | **preferred**} **vlan {***vlan-list* | **all**}
no rep block port {id *port-id* | *neighbor-offset* | **preferred**}

構文の説明

id *port-id*	REP を有効にすると自動的に生成される一意のポート ID を入力して VLAN ブロッキング代替ポートを指定します。REP ポート ID は、16 文字の 16 進数値です。
neighbor-offset	ネイバーのオフセット番号を入力することによる、VLAN ブロック代替ポート。範囲は -256 ～ +256 です。値 0 は無効です。
preferred	すでに VLAN ロード バランシングの優先代替ポートとして指定されている通常セグメント ポートを選択します。
vlan	ブロックされる VLAN を指定します。
vlan-list	表示される VLAN ID または VLAN ID の範囲。ブロックする VLAN ID（1 ～ 4094 の範囲）を入力するか、ブロックする LAN ID の範囲または連続番号（1-3、22、41-44 など）を入力します。
all	すべての VLAN をブロックします。

コマンド デフォルト

特権 EXEC モードで **rep preempt segment** コマンドを入力した後のデフォルト動作では（手動プリエンプションの場合）、プライマリエッジポートですべての VLAN をブロックします。この動作は、**rep block port** コマンドを設定するまで継続されます。

プライマリ エッジ ポートで代替ポートを判別できない場合は、デフォルトのアクションはプリエンプションなし、および VLAN ロード バランシングなしです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	このコマンドが導入されました。

使用上のガイドライン

オフセット番号を入力して代替ポートを選択する場合、オフセット番号はエッジポートのダウンストリーム ネイバー ポートを識別します。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。

負の番号は、セカンダリ エッジ ポート（オフセット番号 –1）とダウンストリーム ネイバーを識別します。

（注） 番号 1 はプライマリ エッジ ポート自体のオフセット番号なので、オフセット番号 1 は入力しないでください。

インターフェイス コンフィギュレーション モードで、**rep preempt delay seconds** コマンドを入力することでプリエンプション遅延時間を設定しており、リンク障害とリカバリが発生した場合、別のリンク障害が発生することなく設定したプリエンプション期間が経過すると、VLAN ロードバランシングが開始されます。ロードバランシング設定で指定された代替ポートは、設定された VLAN をブロックし、その他すべてのセグメント ポートのブロックを解除します。プライマリ エッジ ポートで VLAN バランシングの代替ポートを決定できない場合、デフォルトのアクションはプリエンプションなしになります。

セグメント内のポートごとに、一意のポート ID が割り当てられます。ポートのポート ID を判別するには、特権 EXEC モードで **show interfaces** *interface-id* **rep detail** コマンドを入力します。

例

次に、REP VLAN ロード バランシングを設定する例を示します。

```
デバイス(config)# interface TenGigabitEthernet 4/1
デバイス(config-if)# rep block port id 0009001818D68700 vlan 1-100
```

関連コマンド

コマンド	説明
show interfaces rep detail	管理 VLAN を含め、すべてのインターフェイスまたは指定したインターフェイスの詳細 REP 設定およびステータスを表示します。

rep lsl-age-timer

Resilient Ethernet Protocol（REP）リンクステータスレイヤ（LSL）のエージアウトタイマー値を設定するには、インターフェイス コンフィギュレーション モードで **rep lsl-age-timer** コマンドを使用します。デフォルトのエージアウトタイマー値に戻すには、このコマンドの **no** 形式を使用します。

rep lsl-age-timer *milliseconds*
no rep lsl-age-timer *milliseconds*

構文の説明

milliseconds	ミリ秒単位の REP LSL エージアウト タイマー値。範囲は 120 ～ 10000 の 40 の倍数です。

コマンド デフォルト デフォルトの LSL エージアウト タイマー値は 5 ミリ秒です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	このコマンドが導入されました。

使用上のガイドライン

REP の設定可能なタイマーを設定する際には、最初に REP LSL の再試行回数を設定し、その後、REP LSL のエージアウト タイマー値を設定することを推奨します。

例

次に、REP LSL エージアウト タイマー値を設定する例を示します。

```
デバイス(config)# interface TenGigabitEthernet 4/1
デバイス(config-if)# rep segment 1 edge primary
デバイス(config-if)# rep lsl-age-timer 2000
```

関連コマンド

コマンド	説明
interface interface-type interface-name	STCNを受信する物理インターフェイスまたはポート チャネルを指定します。
rep segment	インターフェイス上で REP をイネーブルにし、セグメント ID を割り当てます。

rep lsl-retries

REP リンクステータスレイヤ（LSL）の再試行回数を設定するには、インターフェイス コンフィギュレーション モードで **rep lsl-retries** コマンドを使用します。デフォルトの再試行回数に戻すには、このコマンドの **no** 形式を使用します。

rep lsl-retries *number-of-retries*
no rep lsl-retries *number-of-retries*

構文の説明

number-of-retries	LSL の再試行回数。再試行回数の範囲は、3 ～ 10 です。

コマンド デフォルト

デフォルトの再試行回数は 5 回です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	このコマンドが追加されました。

使用上のガイドライン

rep lsl-retries コマンドは、REP リンクを無効にする前に再試行回数を設定するために使用されます。REP の設定可能なタイマーを設定する際には、最初に REP LSL の再試行回数を設定し、その後、REP LSL のエージアウト タイマー値を設定することを推奨します。

次に、REP LSL の再試行回数を設定する例を示します。

```
デバイス(config)#  interface TenGigabitEthernet 4/1
デバイス(config-if)#  rep segment 2 edge primary
```

rep preempt delay

セグメントポートの障害およびリカバリの発生後、Resilient Ethernet Protocol（REP）VLAN ロードバランシングがトリガーされるまでの待機時間を設定するには、インターフェイス コンフィギュレーション モードで **rep preempt delay** コマンドを使用します。設定した遅延を削除するには、このコマンドの **no** 形式を使用します。

rep preempt delay *seconds*
no rep preempt delay

構文の説明

seconds	REP プリエンプションを遅延する秒数です。範囲は 15 ～ 300 秒です。デフォルトは遅延なしの手動プリエンプションです。

コマンド デフォルト

REP プリエンプション遅延は設定されていません。デフォルトは遅延なしの手動プリエンプションです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	このコマンドが導入されました。

使用上のガイドライン

REP プライマリ エッジ ポート上にこのコマンドを入力します。

リンク障害とリカバリ後に自動的に VLAN ロード バランシングをトリガーする場合は、このコマンドを入力してプリエンプション時間遅延を設定します。

VLAN ロード バランシングが設定されている場合、セグメント ポート障害とリカバリの後、VLAN ロード バランシングが発生する前に REP プライマリ エッジ ポートで遅延タイマーが起動されます。各リンク障害が発生した後にタイマーが再起動することに注意してください。タイマーが満了となると、（**rep block port** インターフェイス コンフィギュレーション コマンドを使用して設定された）VLAN ロードバランシングを実行するように REP プライマリエッジ ポートが代替ポートに通知し、新規トポロジ用のセグメントが準備されます。設定された VLAN リストは代替ポートでブロックされ、他のすべての VLAN はプライマリ エッジ ポートでブロックされます。

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

例

次に、プライマリ エッジ ポートで REP プリエンプション時間遅延を 100 秒に設定する例を示します。

```
デバイス(config)# interface TenGigabitEthernet 4/1
デバイス(config-if)# rep preempt delay 100
```

関連コマンド

コマンド	説明
rep block port	VLAN ロード バランシングを設定します。
show interfaces rep detail	管理 VLAN を含め、すべてのインターフェイスまたは指定したインターフェイスの詳細 REP 設定およびステータスを表示します。

rep preempt segment

Resilient Ethernet Protocol（REP）VLAN ロードバランシングがセグメントで手動で開始されるようにするには、特権 EXEC モードで **rep preempt segment** コマンドを使用します。

rep preempt segment *segment-id*

構文の説明

segment-id	REP セグメントの ID です。有効な範囲は 1 ～ 1024 です。

コマンド デフォルト

デフォルト動作は手動プリエンプションです。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	このコマンドが導入されました。

使用上のガイドライン

デバイスのプライマリ エッジ ポートがあるセグメントで、次のコマンドを入力します。

VLAN ロード バランシングのプリエンプションを設定する前に、他のすべてのセグメントの設定が完了していることを確認してください。VLAN ロードバランシングのプリエンプションはネットワークを中断する可能性があるため、**rep preempt segment** *segment-id* コマンドを入力すると、このコマンドの実行前に確認メッセージが表示されます。

プライマリエッジポートで、インターフェイス コンフィギュレーション モードから **rep preempt delay** *seconds* コマンドを入力せずに、プリエンプション時間遅延を設定する場合、デフォルト設定はセグメントでの VLAN ロードバランシングの手動トリガーです。

特権 EXEC モードで **show rep topology** コマンドを入力して、セグメント内のどのポートがプライマリエッジポートなのかを確認します。

VLAN ロードバランシングを設定しない場合、**rep preempt segment** *segment-id* コマンドを入力すると、デフォルトの動作が実行されます。つまりプライマリエッジポートがすべてのVLANをブロックします。

REP プライマリエッジポートのインターフェイス コンフィギュレーション モードで **rep block port** コマンドを入力して VLAN ロードバランシングを設定してから、手動でプリエンプションを開始できます。

例

次に、セグメント 100 で手動で REP プリエンプションをトリガーする例を示します。

```
デバイス# rep preempt segment 100
```

関連コマンド

コマンド	説明
rep block port	VLAN ロード バランシングを設定します。
rep preempt delay	ポート障害とリカバリの後から REP VLAN ロードバランシングがトリガーされるまでの待機期間を設定します。
show rep topology	セグメントまたはすべてのセグメントの REP トポロジ情報を表示します。

rep segment

インターフェイスで Resilient Ethernet Protocol（REP）を有効にし、そのインターフェイスにセグメント ID を割り当てるには、インターフェイス コンフィギュレーション モードで **rep segment** コマンドを使用します。インターフェイスで REP を無効にするには、このコマンドの **no** 形式を使用します。

rep segment *segment-id* **[edge [no-neighbor] [primary]] [preferred]**
no rep segment

構文の説明

segment-id	REP が有効になっているセグメント。セグメント ID をインターフェイスに割り当てます。有効な範囲は 1 ～ 1024 です。
edge	（任意）エッジ ポートとしてポートを設定します。各セグメントにあるエッジ ポートは 2 つだけです。
no-neighbor	（任意）セグメント エッジを外部 REP ネイバーなしに指定します。
primary	（任意）プライマリ エッジ ポート（VLAN ロード バランシングを設定できるポート）としてポートを指定します。1 セグメント内のプライマリ エッジ ポートは 1 つだけです。

preferred	（任意）ポートを優先代替ポートまたは VLAN ロード バランシングの優先ポートに指定します。 （注） ポートを優先ポートに設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。通常、前に障害が発生したポートが、代替ポートとなります。

コマンド デフォルト

REP はインターフェイスでディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	このコマンドが導入されました。

使用上のガイドライン

REP ポートは、レイヤ 2 IEEE 802.1Q ポートまたは 802.1AD ポートのいずれかである必要があります。各 REP セグメント上には、プライマリ エッジ ポートとセカンダリ エッジ ポートの 2 種類のエッジ ポートを設定しなければいけません。

REPがデバイスの2つのポートでイネーブルである場合、両方のポートが通常セグメント ポートまたはエッジ ポートのいずれかである必要があります。REP ポートは以下の規則に従います。

- セグメント内のデバイスにポートが 1 つだけ設定されている場合、そのポートはエッジ ポートになります。
- 1 つのデバイス上で 2 つのポートが同じセグメントに属する場合、どちらのポートも通常セグメント ポートである必要があります。
- 1 つのデバイス上で 2 つのポートが同じセグメントに属し、1 つがエッジ ポートとして設定され、もう 1 つが通常のセグメント ポートとして設定された場合（設定ミス）、エッジ ポートは通常セグメント ポートとして処理されます。

⚠

注意 REP インターフェイスはブロック ステートで起動し、安全にブロック解除可能と通知されるまでブロック ステートのままになります。突然の接続切断を避けるために、これを意識しておく必要があります。

REP がインターフェイスでイネーブルの場合、デフォルトでは通常のセグメント ポートであるポートに対してイネーブルになります。

例

次に、通常（非エッジ）セグメント ポートで REP を有効にする例を示します。

```
デバイス(config)# interface TenGigabitEthernet 4/1
デバイス(config-if)# rep segment 100
```

次に、ポートで REP をイネーブルし、そのポートを REP プライマリ エッジ ポートとして指定する例を示します。

```
デバイス(config)# interface TenGigabitEthernet 4/1
デバイス(config-if)# rep segment 100 edge primary
```

次に、ポートで REP をイネーブルし、そのポートを REP セカンダリ エッジ ポートとして指定する例を示します。

```
デバイス(config)# interface TenGigabitEthernet 4/1
デバイス(config-if)# rep segment 100 edge
```

次に、REP をネイバーなしのエッジ ポートとして有効にする例を示します。

```
デバイス(config)# interface TenGigabitEthernet 4/1
デバイス(config-if)# rep segment 1 edge no-neighbor primary
```

rep stcn

セグメントトポロジ変更通知（STCN）を他のインターフェイスまたは他のセグメントに送信するように Resilient Ethernet Protocol（REP）エッジポートを設定するには、インターフェイス コンフィギュレーション モードで **rep stcn** コマンドを使用します。インターフェイスまたはセグメントへの STCN の送信タス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。

rep stcn {**interface** *interface-id* | **segment** *segment-id-list*}
no rep stcn {**interface** | **segment**}

構文の説明

interface *interface-id*	STCN を受信する物理インターフェイスまたはポート チャネルを指定します。
segment *segment-id-list*	STCN を受信する 1 つの REP セグメントまたは REP セグメントの一覧を指定します。セグメントの範囲は 1 ～ 1024 です。また、一連のセグメント（たとえば3～5、77、100）を設定することもできます。

コマンド デフォルト

他のインターフェイスおよびセグメントへの STCN 送信は、無効になっています。

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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	このコマンドが導入されました。

使用上のガイドライン

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

例

次に、セグメント 25 ～ 50 に STCN を送信するように REP エッジ ポートを設定する例を示します。

```
デバイス(config)# interface TenGigabitEthernet 4/1
デバイス(config-if)# rep stcn segment 25-50
```

show etherchannel

チャネルの EtherChannel 情報を表示するには、ユーザ EXEC モードで **show etherchannel** コマンドを使用します。

show etherchannel [{*channel-group-number* | {**detail** | **port** | **port-channel** | **protocol** | **summary**}}] | [{**auto** | **detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**}]

構文の説明

channel-group-number	（任意）チャネルグループ番号。指定できる範囲は 1 ～ 128 です。
auto	（任意）Etherchannel が自動的に作成する情報を表示します。
detail	（任意）詳細な EtherChannel 情報を表示します。
load-balance	（任意）ポート チャネル内のポート間の負荷分散方式、またはフレーム配布方式を表示します。
port	（任意）EtherChannel ポートの情報を表示します。
port-channel	（任意）ポート チャネル情報を表示します。
protocol	（任意）EtherChannel で使用されるプロトコルを表示します。
summary	（任意）各チャネル グループのサマリーを 1 行で表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

コマンド履歴

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

使用上のガイドライン

チャネル グループ番号を指定しない場合は、すべてのチャネル グループが表示されます。

出力では、パッシブ ポート リスト フィールドはレイヤ 3 のポート チャネルだけで表示されます。このフィールドは、まだ起動していない物理ポートがチャネル グループ内で設定されていること（および間接的にチャネル グループ内で唯一のポート チャネルであること）を意味します。

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

```
device# show etherchannel auto
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SUA)        LACP      Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)
```

次に、**show etherchannel** *channel-group-number* **detail** コマンドの出力例を示します。

```
デバイス> show etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:      LACP
                   Ports in the group:
                   -------------------
Port: Gi1/0/1
------------
Port state    = Up Mstr In-Bndl
Channel group = 1         Mode  = Active        Gcchange = -
Port-channel  =           Po1GC = -             Pseudo port-channel = Po1
Port index    =           0Load = 0x00          Protocol = LACP

Flags: S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDU
       A - Device is in active mode.        P - Device is in passive mode.

Local information:
                         LACP port   Admin   Oper   Port   Port
Port     Flags   State   Priority    Key     Key    Number State
Gi1/0/1   SA      bndl     32768      0x1     0x1    0x101  0x3D
Gi1/0/2    A      bndl     32768      0x0     0x1    0x0    0x3D

Age of the port in the current state: 01d:20h:06m:04s

                   Port-channels in the group:
                   ----------------------

Port-channel: Po1   (Primary Aggregator)

Age of the Port-channel = 01d:20h:20m:26s
Logical slot/port = 10/1          Number of ports = 2
HotStandBy port   = null
Port state        = Port-channel Ag-Inuse
```

```
Protocol          = LACP

Ports in the Port-channel:

Index  Load   Port      EC state        No of bits
------+------+------+------------------+-----------
 0      00    Gi1/0/1    Active           0
 0      00    Gi1/0/2    Active           0

Time since last port bundled:   01d:20h:24m:44s   Gi1/0/2
```

次に、**show etherchannel** *channel-group-number* **summary** コマンドの出力例を示します。

```
デバイス> show etherchannel 1 summary
Flags: D - down P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3 S - Layer2
       u - unsuitable for bundling
       U - in use f - failed to allocate aggregator
       d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
 1     Po1(SU)       LACP        Gi1/0/1(P) Gi1/0/2(P)
```

次に、**show etherchannel** *channel-group-number* **port-channel** コマンドの出力例を示します。

```
デバイス> show etherchannel 1 port-channel
Port-channels in the group:
----------------------
Port-channel: Po1 (Primary Aggregator)
------------
Age of the Port-channel = 01d:20h:24m:50s
Logical slot/port = 10/1 Number of ports = 2
Logical slot/port = 10/1 Number of ports = 2
Port state = Port-channel Ag-Inuse
Protocol = LACP

Ports in the Port-channel:

Index  Load   Port   EC state           No of bits
------+------+------+------------------+-----------
 0      00    Gi1/0/1 Active             0
 0      00    Gi1/0/2 Active             0

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2
```

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

```
デバイス# show etherchannel protocol
Channel-group listing:
-----------------------
Group: 1
----------
Protocol: LACP
```

```
Group: 2
----------
Protocol: PAgP
```

show interfaces rep detail

管理 VLAN を含む、すべてのインターフェイスまたは指定されたインターフェイスの詳細な Resilient Ethernet Protocol（REP）の設定およびステータスを表示するには、特権 EXEC モードで **show interfaces rep detail** コマンドを使用します。

show interfaces [*interface-id*] **rep detail**

構文の説明

interface-id	（任意）ポート ID を表示するために使用される物理インターフェイス。

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 Denali 16.2.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、1 つ以上のセグメントまたは 1 つのインターフェイスに STCN を送信先するために、セグメント エッジ ポートで入力します。

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

例

次に、指定されたインターフェイスに関する REP 設定とステータスを表示する例を示します。

```
デバイス# show interfaces TenGigabitEthernet4/1 rep detail

TenGigabitEthernet4/1 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
```

```
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

関連コマンド

コマンド	説明
rep admin vlan	REP が HFL メッセージを送信するための REP 管理 VLAN を設定します。

show lacp

Link Aggregation Control Protocol（LACP）チャネルグループ情報を表示するには、ユーザ EXEC モードで **show lacp** コマンドを使用します。

show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor** | **sys-id**}

構文の説明

channel-group-number	（任意）チャネルグループ番号。指定できる範囲は 1 ～ 128 です。
counters	トラフィック情報を表示します。
internal	内部情報を表示します。
neighbor	ネイバーの情報を表示します。
sys-id	LACP によって使用されるシステム識別子を表示します。システム識別子は、LACP システムプライオリティとdevice MAC アドレスで構成されています。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

コマンド履歴

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

使用上のガイドライン

show lacp コマンドを入力すると、アクティブなチャネルグループの情報が表示されます。特定のチャネル情報を表示するには、チャネルグループ番号を指定して **show lacp** コマンドを入力します。

チャネル グループを指定しない場合は、すべてのチャネル グループが表示されます。

channel-group-number を入力すると、**sys-id** 以外のすべてのキーワードでチャネルグループを指定できます。

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

```
デバイス> show lacp counters
               LACPDUs         Marker      Marker Response   LACPDUs
Port         Sent  Recv     Sent  Recv      Sent  Recv      Pkts  Err
---------------------------------------------------------------------
Channel group:1
Gi2/0/1       19    10         0    0          0    0         0
Gi2/0/2       14    6          0    0          0    0         0
```

表 *25 : show lacp counters* のフィールドの説明

フィールド	説明
LACPDUs Sent および Recv	ポートによって送受信された LACP パケット数
Marker Sent および Recv	ポートによって送受信された LACP Marker パケット数
Marker Response Sent および Recv	ポートによって送受信された LACP Marker 応答パケット数
LACPDUs Pkts および Err	ポートの LACP によって受信された、未知で不正なパケット数

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

```
デバイス> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port     Port
Port      Flags   State     Priority      Key       Key     Number   State
Gi2/0/1    SA      bndl      32768         0x3       0x3       0x4    0x3D
Gi2/0/2    SA      bndl      32768         0x3       0x3       0x5    0x3D
```

次の表に、出力されるフィールドの説明を示します。

表 *26 : show lacp internal* のフィールドの説明

フィールド	説明
ステータス	特定のポートの状態。次に使用可能な値を示します。 • – : ポートの状態は不明です。 • **bndl**：ポートがアグリゲータに接続され、他のポートとバンドルされています。 • **susp**：ポートが中断されている状態で、アグリゲータには接続されていません。 • **hot-sby**：ポートがホットスタンバイの状態です。 • **indiv**：ポートは他のポートとバンドルできません。 • **indep**：ポートは独立状態です。バンドルされていませんが、データ トラフィックを処理することができます。この場合、LACP は相手側ポートで実行されていません。 • **down**：ポートがダウンしています。
LACP Port Priority	ポートのプライオリティ設定。ハードウェアの制限により互換性のあるすべてのポートを集約できない場合、LACP はポート プライオリティを使用してポートをスタンバイ モードにします。
Admin Key	ポートに割り当てられた管理用のキー。LACP は自動的に管理用のキー値を生成します（16 進数）。管理キーにより、他のポートとともに集約されるポートの機能が定義されます。ポートが他のポートと集約できるかどうかは、ポートの物理特性（たとえば、データ レートやデュプレックス機能）と設定に指定された制限によって決定されます。
Oper Key	ポートで使用される実行時の操作キー。LACP は自動的に値を生成します（16 進数）。
Port Number	ポート番号。

フィールド	説明
Port State	ポートの状態変数。1つのオクテット内で個々のビットとしてエンコードされ、次のような意味になります。 • bit0：LACP のアクティビティ • bit1：LACP のタイムアウト • bit2：集約 • bit3：同期 • bit4：収集 • bit5：配信 • bit6：デフォルト • bit7：期限切れ （注） 上のリストでは、bit7 が MSB で bit0 は LSB です。

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

```
デバイス> show lacp neighbor
Flags: S - Device is sending Slow LACPDUs  F - Device is sending Fast LACPDUs
       A - Device is in Active mode        P - Device is in Passive mode

Channel group 3 neighbors

Partner's information:

          Partner                Partner               Partner
Port      System ID              Port Number   Age     Flags
Gi2/0/1   32768,0007.eb49.5e80   0xC             19s    SP

          LACP Partner           Partner       Partner
          Port Priority          Oper Key      Port State
          32768                  0x3           0x3C

Partner's information:

          Partner                Partner               Partner
Port      System ID              Port Number   Age     Flags
Gi2/0/2   32768,0007.eb49.5e80   0xD             15s    SP

          LACP Partner           Partner       Partner
          Port Priority          Oper Key      Port State
          32768                  0x3           0x3C
```

次に、**show lacp sys-id** コマンドの出力例を示します。

```
デバイス> show lacp sys-id
32765,0002.4b29.3a00
```

システム ID は、システム プライオリティおよびシステム MAC アドレスで構成されています。最初の 2 バイトはシステム プライオリティ、最後の 6 バイトはグローバルに管理されているシステム関連の個々の MAC アドレスです。

show pagp

ポート集約プロトコル（PAgP）のチャネルグループ情報を表示するには、EXEC モードで **show pagp** コマンドを使用します。

show pagp [*channel-group-number*] {**counters** | **dual-active** | **internal** | **neighbor**}

構文の説明

channel-group-number	（任意）チャネルグループ番号。指定できる範囲は 1 ～ 128 です。
counters	トラフィック情報を表示します。
dual-active	デュアルアクティブ ステータスが表示されます。
internal	内部情報を表示します。
neighbor	ネイバーの情報を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

show pagp コマンドを入力すると、アクティブなチャネルグループの情報が表示されます。非アクティブポートチャネルの情報を表示するには、チャネルグループ番号を指定して **show pagp** コマンドを入力します。

例

次に、**show pagp 1 counters** コマンドの出力例を示します。

```
デバイス> show pagp 1 counters
             Information        Flush
Port         Sent   Recv     Sent   Recv
---------------------------------------
Channel group: 1
  Gi1/0/1    45     42       0      0
  Gi1/0/2    45     41       0      0
```

次に、**show pagp dual-active** コマンドの出力例を示します。

```
デバイス> show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1

Channel group 1
          Dual-Active     Partner              Partner   Partner
Port      Detect Capable  Name                 Port      Version
Gi1/0/1   No              デバイス              Gi3/0/3   N/A
Gi1/0/2   No              デバイス              Gi3/0/4   N/A

<output truncated>
```

次に、**show pagp 1 internal** コマンドの出力例を示します。

```
デバイス> show pagp 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Channel group 1
                                Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi1/0/1     SC    U6/S7   H       30s      1        128        Any      16
Gi1/0/2     SC    U6/S7   H       30s      1        128        Any      16
```

次に、**show pagp 1 neighbor** コマンドの出力例を示します。

```
デバイス> show pagp 1 neighbor

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.

Channel group 1 neighbors
            Partner              Partner          Partner           Partner Group
Port        Name                 Device ID        Port         Age  Flags   Cap.
Gi1/0/1     device-p2            0002.4b29.4600   Gi01//1        9s SC      10001
Gi1/0/2     device-p2            0002.4b29.4600   Gi1/0/2       24s SC      10001
```

show platform software fed etherchannel

プラットフォーム依存 EtherChannel 情報を表示するには、特権 EXEC モードで **show platform software fed etherchannel** コマンドを使用します。

show platform software fed etherchannel [**switch** *switch-number*] *channel-group-number* {**group-mask** | **load-balance mac** *src-mac dst-mac* [**ip** *src-ip dst-ip* [**port** *src-port dst-port*]]}

構文の説明

switch *switch-number*	（任意）スタック メンバを指定します。
channel-group-number	チャネルグループ番号。指定できる範囲は 1 ～ 128 です。
group-mask	EtherChannel グループ マスクを表示します。

load-balance	EtherChannel ロードバランシングのハッシュ アルゴリズムをテストします。
mac *src-mac dst-mac*	送信元と宛先の MAC アドレスを指定します。
ip *src-ip dst-ip*	（任意）送信元と宛先の IP アドレスを指定します。
port *src-port dst-port*	（任意）送信元と宛先のレイヤ ポート番号を指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。

テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show platform pm

プラットフォーム依存のポートマネージャ情報を表示するには、特権 EXEC モードで **show platform pm** コマンドを使用します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。

テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show rep topology

セグメント、またはセグメント内のプライマリおよびセカンダリエッジポートを含むすべてのセグメントの Resilient Ethernet Protocol（REP）トポロジ情報を表示するには、特権 EXEC モードで **show rep topology** コマンドを使用します。

show rep topology [segment *segment-id*] **[archive] [detail]**

構文の説明

segment *segment-id*	（任意）REP トポロジ情報を表示するセグメントを指定します。セグメント *ID* の範囲は 1 ～ 1024 です。
archive	（任意）セグメントの前のトポロジを表示します。このキーワードは、リンク障害のトラブルシューティングに役立ちます。
detail	（任意）REP トポロジの詳細情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.2.2	このコマンドが導入されました。

例

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

```
デバイス# show rep topology

REP Segment 1
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
10.64.106.63     Te5/4      Pri  Open
10.64.106.228    Te3/4           Open
10.64.106.228    Te3/3           Open
10.64.106.67     Te4/3           Open
10.64.106.67     Te4/4           Alt
10.64.106.63     Te4/4      Sec  Open

REP Segment 3
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
10.64.106.63     Gi50/1     Pri  Open
SVT_3400_2       Gi0/3           Open
SVT_3400_2       Gi0/4           Open
10.64.106.68     Gi40/2          Open
10.64.106.68     Gi40/1          Open
10.64.106.63     Gi50/2     Sec  Alt
```

次に、**show rep topology detail** コマンドの出力例を示します。

```
デバイス# show rep topology detail
```

```
REP Segment 1
10.64.106.63, Te5/4 (Primary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 1 / [-6]
10.64.106.228, Te3/4 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 2 / [-5]
10.64.106.228, Te3/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 00E
  Port Priority: 000
  Neighbor Number: 3 / [-4]
10.64.106.67, Te4/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1800
  Port Number: 008
  Port Priority: 000
  Neighbor Number: 4 / [-3]
10.64.106.67, Te4/4 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 0005.9b2e.1800
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 5 / [-2]
10.64.106.63, Te4/4 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 6 / [-1]
```

show udld

すべてのポートまたは指定されたポートの単方向リンク検出（UDLD）の管理ステータスおよび動作ステータスを表示するには、ユーザ EXEC モードで **show udld** コマンドを使用します。

show udld ［**Auto-Template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan**］ *interface_number*
show udld neighbors

構文の説明

Auto-Template	（任意）自動テンプレート インターフェイスの UDLD 動作ステータスを表示します。範囲は 1 ～ 999 です。
Capwap	（任意）CAPWAP インターフェイスの UDLD 動作ステータスを表示します。指定できる範囲は 0 ～ 2147483647 です。

GigabitEthernet	（任意）GigabitEthernet インターフェイスの UDLD 動作ステータスを表示します。範囲は 0 ～ 9 です。
GroupVI	（任意）グループ仮想インターフェイスの UDLD 動作ステータスを表示します。範囲は 1 ～ 255 です。
InternalInterface	（任意）内部インターフェイスの UDLD 動作ステータスを表示します。範囲は 0 ～ 9 です。
Loopback	（任意）ループバック インターフェイスの UDLD 動作ステータスを表示します。指定できる範囲は 0 ～ 2147483647 です。
Null	（任意）null インターフェイスの UDLD 動作ステータスを表示します。
Port-channel	（任意）イーサネット チャネル インターフェイスの UDLD 動作ステータスを表示します。有効な範囲は 1 ～ 128 です。
TenGigabitEthernet	（任意）10 ギガビット イーサネット インターフェイスの UDLD 動作ステータスを表示します。範囲は 0 ～ 9 です。
Tunnel	（任意）トンネル インターフェイスの UDLD 動作ステータスを表示します。指定できる範囲は 0 ～ 2147483647 です。
Vlan	（任意）VLAN インターフェイスの UDLD 動作ステータスを表示します。指定できる範囲は 1 ～ 4095 です。
interface-id	（任意）インターフェイスの ID およびポート番号です。有効なインターフェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。
neighbors	（任意）ネイバー情報だけを表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

コマンド履歴

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

使用上のガイドライン

インターフェイス ID を入力しない場合は、すべてのインターフェイスの管理上および運用上の UDLD ステータスが表示されます。

次の例では、**show udld** *interface-id* コマンドの出力を示します。ここでは、UDLD はリンクの両端でイネーブルに設定されていて、リンクが双方向であることを UDLD が検出します。次の表に、この出力で表示されるフィールドについて説明します。

```
デバイス> show udld gigabitethernet2/0/1
Interface gi2/0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
Entry 1
Expiration time: 146
Device ID: 1
Current neighbor state: Bidirectional
Device name: Switch-A
Port ID: Gi2/0/1
Neighbor echo 1 device: Switch-B
Neighbor echo 1 port: Gi2/0/2
Message interval: 5
CDP Device name: Switch-A
```

表 *27 : show udld* のフィールドの説明

フィールド	説明
Interface	UDLD に設定されたローカル デバイスのインターフェイス。
Port enable administrative configuration setting	ポートでの UDLD の設定方法。UDLD がイネーブルまたはディセーブルの場合、ポートのイネーブル設定は運用上のイネーブル ステートと同じです。それ以外の場合、イネーブル動作設定は、グローバルなイネーブル設定によって決まります。
Port enable operational state	このポートで UDLD が実際に稼働しているかどうかを示す動作ステート。
Current bidirectional state	リンクの双方向ステート。リンクがダウンしているか、または UDLD 非対応デバイスに接続されている場合は、unknown ステートが表示されます。リンクが UDLD 対応デバイスに通常どおり双方向接続されている場合は、bidirectional ステートが表示されます。その他の値が表示されている場合は、正しく配線されていません。

フィールド	説明
Current operational state	UDLD ステート マシンの現在のフェーズ。通常の双方向リンクの場合、多くは、ステート マシンはアドバタイズ フェーズです。
Message interval	ローカルデバイスからアドバタイズ メッセージを送信する頻度。単位は秒です。
Time out interval	検出ウィンドウ中に、UDLD がネイバー デバイスからのエコーを待機する期間（秒）。
Entry 1	最初のキャッシュ エントリの情報。このエントリには、ネイバーから受信されたエコー情報のコピーが格納されます。
Expiration time	このキャッシュ エントリの期限が切れるまでの存続期間（秒）。
Device ID	ネイバー デバイスの ID。
Current neighbor state	ネイバーの現在の状態。ローカル デバイスおよびネイバー装置の両方で UDLD が通常どおり稼働している場合、ネイバー ステートおよびローカル ステートは双方向です。リンクがダウンしているか、またはネイバーが UDLD 対応でない場合、キャッシュ エントリは表示されません。
デバイス名	装置名またはネイバーのシステム シリアル番号。装置名が設定されていないか、またはデフォルト（Switch）に設定されている場合、システムのシリアル番号が表示されます。
Port ID	UDLD に対してイネーブルに設定されたネイバーのポート ID。
Neighbor echo 1 device	エコーの送信元であるネイバーのネイバー デバイス名。
Neighbor echo 1 port	エコーの送信元であるネイバーのポート番号 ID。
Message interval	ネイバーがアドバタイズ メッセージを送信する速度（秒）。

フィールド	説明
CDP device name	CDP デバイス名またはシステム シリアル番号。装置名が設定されていないか、またはデフォルト（Switch）に設定されている場合、システムのシリアル番号が表示されます。

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

```
デバイス# show udld neighbors
Port     Device Name          Device ID  Port-ID  OperState
-------- -------------------- ---------- -------- --------------
Gi2/0/1  Switch-A             1          Gi2/0/1  Bidirectional
Gi3/0/1  Switch-A             2          Gi3/0/1  Bidirectional
```

switchport

レイヤ 3 モードになっているインターフェイスをレイヤ 2 設定用のレイヤ 2 モードに配置するには、インターフェイス コンフィギュレーション モードで **switchport** コマンドを使用します。インターフェイスをレイヤ 3 モードに配置するには、このコマンドの **no** 形式を使用します。

switchport
no switchport

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、すべてのインターフェイスがレイヤ 2 モードです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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* | **name** *vlan_name*}
no switchport access vlan

構文の説明

vlan-id	アクセス モード VLAN のVLAN ID。範囲は 1 ~ 4094。

コマンド デフォルト

デフォルトのアクセス VLAN およびトランク インターフェイス ネイティブ VLAN は、プラットフォームまたはインターフェイス ハードウェアに対応したデフォルト VLAN です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

リリース	変更内容
Cisco IOS XE Denali 16.2.1	**name** *vlan_name* キーワードが導入されました。

使用上のガイドライン

switchport access vlan コマンドを有効にするには、事前にポートをアクセス モードにする必要があります。

スイッチポートのモードが **access vlan** *vlan-id* に設定されている場合、ポートは指定された VLAN のメンバとして動作します。アクセス ポートを割り当てることができるのは、1 つの VLAN だけです。

no switchport access コマンドを使用すると、アクセス モード VLAN がデバイスに適したデフォルト VLAN にリセットされます。

例

次の例では、アクセス モードで動作するスイッチド ポート インターフェイスが、デフォルト VLAN ではなく VLAN 2 で動作するように変更します。

```
デバイス(config-if)# switchport access vlan 2
```

例

次の例では、最初に VLAN ID と VLAN 名を対応させて、その情報を VLAN データベースに格納し、その後、アクセス モードにあるインターフェイス上の VLAN を設定します（名前を使用）。設定を確認するには、特権 EXEC コマンドで **show interfaces** *interface-id* **switchport** を入力して、Access Mode VLAN：行の情報を調べます。

手順 1：VLAN データベースでのエントリの作成

```
デバイス# configure terminal
デバイス(config)# vlan 33
デバイス(config-vlan)# name test
デバイス(config-vlan)# end
デバイス#
```

手順 2：VLAN データベースの確認

```
デバイス # show vlan id 33
VLAN  Name   Status   Ports
---- -------------------------------- --------- -------------------------------

33    test   active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
33   enet  100033     1500   -      -      -        -   -       0      0

Remote SPAN VLAN
----------------
Disabled

Primary  Secondary Type              Ports
------- --------- -------------- -----------------------------------------
```

手順 3：VLAN 名を使用したインターフェイスへの VLAN の割り当て

```
デバイス # configure terminal
デバイス(config)# interface GigabitEthernet3/1/1
デバイス(config-if)# switchport mode access
デバイス(config-if)# switchport access vlan name test
デバイス(config-if)# end
デバイス#
```

手順 4：設定の確認

```
デバイス # show running-config interface GigabitEthernet3/1/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet3/1/1
switchport access vlan 33
switchport mode access
```

手順 5：インターフェイス スイッチポートの確認

```
デバイス # show interface GigabitEthernet3/1/1 switchport
Name: Gi3/1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 33 (test)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: None
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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
```

switchport nonegotiate

ダイナミック トランキング プロトコル（DTP）ネゴシエーションパケットがレイヤ2インターフェイス上で送信されないように指定するには、インターフェイス コンフィギュレーション モードで **switchport nonegotiate** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport nonegotiate
no switchport nonegotiate

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、トランキング ステータスを学習するために、DTP ネゴシエーションを使用します。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

no switchport nonegotiate コマンドは nonegotiate ステータスを解除します。

このコマンドが有効なのは、インターフェイス スイッチポート モードがアクセスまたはトランク（**switchport mode access** または **switchport mode trunk** インターフェイス コンフィギュレーション コマンドで設定）の場合だけです。dynamic（auto または desirable）モードでこのコマンドを実行しようとすると、エラーが返されます。

DTP をサポートしないインターネットワーキング デバイスでは、DTP フレームが正しく転送されず、設定に矛盾が生じることがあります。この問題を回避するには、**switchport nonegotiate** コマンドを使用して DTP をオフにし、DTP をサポートしていないデバイスに接続されたインターフェイスが DTP フレームを転送しないように設定します。

switchport nonegotiate コマンドを入力した場合、このインターフェイスでは DTP ネゴシエーションパケットが送信されません。デバイスがトランキングを実行するかどうかは、**mode** パラメータ（**access** または **trunk.**）によって決まります。

- 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上のトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。

次の例では、ポートに対してトランキング モードのネゴシエートを制限し、（モードの設定に応じて）トランク ポートまたはアクセス ポートとして動作させる方法を示します。

```
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# switchport nonegotiate
```

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

switchport voice vlan

ポートに音声 VLAN 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 voice vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport voice vlan {*vlan-id* | **dot1p** | **none** | **untagged** | **name** *vlan_name*}
no switchport voice vlan

構文の説明

vlan-id	音声トラフィックに使用する VLAN。指定できる範囲は 1 ～ 4094 です。デフォルトでは、Cisco IP Phone は IEEE 802.1Q プライオリティ 5 を使用して音声トラフィックを転送します。
dot1p	IEEE 802.1p プライオリティ タギングおよび VLAN 0（ネイティブ VLAN）を使用するように電話機を設定します。デフォルトでは、Cisco IP Phone は IEEE 802.1p プライオリティ 5 を使用して音声トラフィックを転送します。
none	音声 VLAN に関して IP Phone に指示しません。IP Phone のキー パッドから入力された設定を使用します。
untagged	タグなしの音声トラフィックを送信するように IP Phone を設定します。これが IP Phone のデフォルト設定になります。
name *vlan_name*	（任意）音声トラフィックに使用する VLAN 名を指定します。最大 128 文字を入力できます。

コマンド デフォルト

デフォルトでは、IP Phone を自動設定しません（**none**）。

デフォルトでは、IP Phone はフレームにタグを付けません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

リリース	変更内容
Cisco IOS XE Denali 16.2.1	音声 VLAN に VLAN 名を指定するオプション。「**name**」キーワードが追加されました。

使用上のガイドライン

レイヤ 2 アクセス ポート上で音声 VLAN を設定する必要があります。

device の Cisco IP 電話に接続しているスイッチポート上の Cisco Discovery Protocol（CDP）をイネーブルにし、Cisco IP 電話に設定情報を送信する必要があります。デフォルトでは、CDP はインターフェイス上でグローバルにイネーブルです。

音声 VLAN をイネーブルにする前に、**trust device cisco-phone** インターフェイス コンフィギュレーション コマンドを入力してインターフェイス上で Quality of Service（QoS）をイネーブルに設定しておくことを推奨します。Auto QoS 機能を使用すると、これらは自動的に設定されます。

VLAN ID を入力すると、IP Phone は IEEE 802.1Q フレームの音声トラフィックを指定された VLAN ID タグ付きで転送します。device は IEEE 802.1Q 音声トラフィックを音声 VLAN に入れます。

dot1p、**none**、または **untagged** を選択した場合、device は指定の音声トラフィックをアクセス VLAN に入れます。

すべての設定で、音声トラフィックはレイヤ 2 の IP precedence 値を運びます。音声トラフィックのデフォルトは 5 です。

音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュア アドレスを設定する必要があります。

アクセス VLAN で任意のポート セキュリティ タイプがイネーブルにされた場合、音声 VLAN でダイナミック ポート セキュリティは自動的にイネーブルになります。

音声 VLAN には、スタティック セキュア MAC アドレスを設定できません。

音声 VLAN を設定すると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

次の例では、最初に VLAN ID と VLAN 名を対応させて、その情報を VLAN データベースに格納し、その後、アクセスモードにあるインターフェイス上の VLAN を設定します（名前を使用）。設定を確認するには、特権 EXEC コマンドで **show interfaces** *interface-id* **switchport** を入力して、Voice VLAN: 行の情報を調べます。

パート 1 - VLAN データベースに入力する

```
デバイス# configure terminal
デバイス(config)# vlan 55
```

```
デバイス(config-vlan)# name test
デバイス(config-vlan)# end
デバイス#
```

パート 2 - VLAN データベースを確認する

```
デバイス# show vlan id 55
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
55 test active
VLAN Type  SAID   MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ------ ---- ------ ------ -------- --- -------- ------ ------
55   enet  100055 1500 -      -      -        -   -        0      0
Remote SPAN VLAN
----------------
Disabled
Primary Secondary Type Ports
------- --------- ----------------- ------------------------------------------
```

パート 3 - VLAN 名を使用して VLAN をインターフェイスに割り当てる

```
デバイス# configure terminal
デバイス(config)# interface gigabitethernet3/1/1
デバイス(config-if)# switchport mode access
デバイス(config-if)# switchport voice vlan name test
デバイス(config-if)# end
デバイス#
```

パート 4 - 設定を確認する

```
デバイス# show running-config
interface gigabitethernet3/1/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet3/1/1
switchport voice vlan 55
switchport mode access
Switch#
```

パート 5 - インターフェイス スイッチポートでも確認できる

```
デバイス# show interface GigabitEthernet3/1/1 switchport
Name: Gi3/1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 55 (test)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
```

```
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
デバイス#
```

udld

単方向リンク検出（UDLD）で、アグレッシブモードまたは通常モードをイネーブルにし、設定可能なメッセージタイマーの時間を設定するには、グローバル コンフィギュレーション モードで **udld** コマンドを使用します。すべての光ファイバポート上でアグレッシブモード UDLD または通常モード UDLDをディセーブルにするには、このコマンドの **no** 形式を使用します。

udld {**aggressive** | **enable** | **message time** *message-timer-interval*}
no udld {**aggressive** | **enable** | **message**}

構文の説明

aggressive	すべての光ファイバインターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。
enable	すべての光ファイバインターフェイスにおいて、通常モードでUDLD をイネーブルにします。
message time *message-timer-interval*	アドバタイズメント フェーズにあり、双方向と判別されたポートにおける UDLD プローブ メッセージ間の時間間隔を設定します。指定できる範囲は 1 ～ 90 秒です。デフォルトは 15 秒です。

コマンド デフォルト

すべてのインターフェイスで UDLD はディセーブルです。

メッセージ タイマーは 15 秒に設定されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

UDLD は、2 つの動作モードをサポートしています。通常（デフォルト）とアグレッシブです。ノーマルモードでは、UDLDは、光ファイバ接続において誤って接続されたインターフェイスによる単一方向リンクを検出します。アグレッシブ モードでは、UDLD はまた、光ファイバおよびツイストペア リンクの単一方向トラフィックによる単一方向リンク、および光ファイバ リンクにおいて誤って接続されたインターフェイスによる単一方向リンクを検出します。通常モードおよびアグレッシブモードについては、*Catalyst 2960-X* スイッチ *Layer 2* コンフィ

ギュレーション ガイド*Catalyst 2960-XR Switch Layer 2 Configuration Guide*『*Layer 2/3 Configuration Guide (Catalyst 3650 Switches)*』を参照してください。

プローブ パケット間のメッセージ時間を変更する場合、検出速度と CPU 負荷との折り合いをつけることになります。時間を減少させると、検出応答を高速にすることができますが、CPU の負荷も高くなります。

このコマンドが作用するのは、光ファイバインターフェイスだけです。他のインターフェイスタイプで UDLD をイネーブルにする場合は、**udld** インターフェイス コンフィギュレーション コマンドを使用します。

次のコマンドを使用して、UDLDによってシャットダウンされたインターフェイスをリセットできます。

- **udld reset** 特権 EXEC コマンド：UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- **shutdown** および **no shutdown** インターフェイス コンフィギュレーション モード コマンド。
- **no udld enable** グローバル コンフィギュレーション コマンドの後に **udld {aggressive | enable}** グローバル コンフィギュレーション コマンドを入力：グローバルに UDLD を再度イネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** または **udld port aggressive** インターフェイス コンフィギュレーション コマンドを入力：指定したインターフェイスで UDLD を再度イネーブルにします。
- **errdisable recovery cause udld** および **errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンド：自動的に UDLD error-disabled ステートから回復します。

次の例では、すべての光ファイバインターフェイスでUDLDをイネーブルにする方法を示します。

```
デバイス(config)# udld enable
```

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

udld port

個々のインターフェイスで単方向リンク検出（UDLD）をイネーブルにするか、または光ファイバインターフェイスが **udld** グローバル コンフィギュレーション コマンドによってイネーブルになるのを防ぐには、インターフェイス コンフィギュレーション モードで **udld port** コマンドを使用します。**udld** グローバル コンフィギュレーション コマンド設定に戻すか、または非光ファイバポートで入力された場合に UDLD をディセーブルにするには、このコマンドの **no** 形式を使用します。

udld port [**aggressive**]

no udld port [**aggressive**]

構文の説明

aggressive	（任意）指定されたインターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。

コマンド デフォルト

光ファイバインターフェイスでは、UDLDはディセーブルになっていますが、光ファイバインターフェイスは、**udld enable** または **udld aggressive** グローバル コンフィギュレーション コマンドのステートに応じて UDLD をイネーブルにします。

非光ファイバ インターフェイスでは、UDLD はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

UDLD 対応ポートが別の device の UDLD 非対応ポートに接続されている場合、このポートは単一方向リンクを検出できません。

UDLD は、2 つの動作モードをサポートしています。通常（デフォルト）とアグレッシブです。ノーマルモードでは、UDLDは、光ファイバ接続において誤って接続されたインターフェイスによる単一方向リンクを検出します。アグレッシブ モードでは、UDLD はまた、光ファイバおよびツイストペア リンクの単一方向トラフィックによる単一方向リンク、および光ファイバ リンクにおいて誤って接続されたインターフェイスによる単一方向リンクを検出します。

UDLD を通常モードでイネーブルにするには、**udld port** インターフェイス コンフィギュレーション コマンドを使用します。UDLD をアグレッシブモードでイネーブルにするには、**udld port aggressive** インターフェイス コンフィギュレーション コマンドを使用します。

UDLD の制御を **udld enable** グローバル コンフィギュレーション コマンドに戻したり、UDLD を非光ファイバポートでディセーブルにしたりする場合は、光ファイバポートで **no udld port** コマンドを使用します。

udld enable または **udld aggressive** グローバル コンフィギュレーション コマンドの設定を上書きする場合は、光ファイバポートで **udld port aggressive** コマンドを使用します。この設定を削除して UDLD イネーブル化の制御を **udld** グローバル コンフィギュレーション コマンドに戻したり、UDLDを非光ファイバポートでディセーブルにしたりする場合は、光ファイバポートで **no** 形式を使用します。

UDLDによってシャットダウンされたインターフェイスをリセットするのに、次のコマンドを使用します。

- **udld reset** 特権 EXEC コマンド：UDLD によってシャットダウンされたすべてのインターフェイスをリセットします。
- **shutdown** および **no shutdown** インターフェイス コンフィギュレーション モード コマンド。

- **no udld enable** グローバル コンフィギュレーション コマンドの後に **udld {aggressive | enable}** グローバル コンフィギュレーション コマンドを入力：グローバルに UDLD を再度イネーブルにします。
- **no udld port** インターフェイス コンフィギュレーション コマンドの後に **udld port** または **udld port aggressive** インターフェイス コンフィギュレーション コマンドを入力：指定したインターフェイスで UDLD を再度イネーブルにします。
- **errdisable recovery cause udld** および **errdisable recovery interval** *interval* グローバル コンフィギュレーション コマンド：自動的に UDLD error-disabled ステートから回復します。

次の例では、ポート上で UDLD をイネーブルにする方法を示します。

```
デバイス(config)# interface gigabitethernet6/0/1
デバイス(config-if)# udld port
```

次の例では、**udld** グローバル コンフィギュレーション コマンドの設定に関係なく、光ファイバインターフェイス上で UDLD をディセーブルにする方法を示します。

```
デバイス(config)# interface gigabitethernet6/0/1
デバイス(config-if)# no udld port
```

設定を確認するには、**show running-config** または **show udld** *interface* 特権 EXEC コマンドを入力します。

udld reset

単方向リンク検出（UDLD）によりディセーブルにされたインターフェイスをすべてリセットし、インターフェイスのトラフィックを再開させるには、特権 EXEC モードで **udld reset** コマンドを使用します（イネーブルの場合には、スパニングツリー、ポート集約プロトコル（PAgP）、ダイナミック トランキング プロトコル（DTP）などの他の機能を介することで有効になります）。

udld reset

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

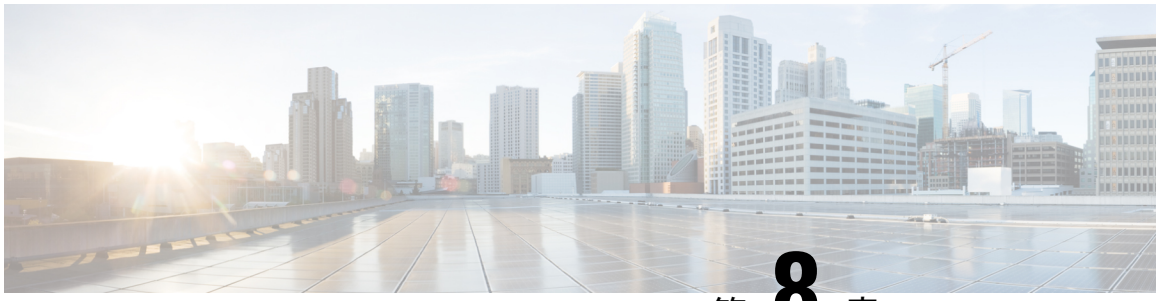
インターフェイスの設定で、UDLDがまだイネーブルである場合、これらのポートは再びUDLDの稼働を開始し、問題が修正されていない場合には同じ理由でディセーブルになります。

次の例では、UDLDによってディセーブルにされたすべてのインターフェイスをリセットする方法を示します。

```
デバイス# udld reset
1 ports shutdown by UDLD were reset.
```

第 VII 部

Multiprotocol Label Switching：マルチプロトコル ラベル スイッチング



第 8 章

MPLS コマンド

mpls ip default-route

IP デフォルトルートに関連付けられたラベルの配信を有効にするには、グローバル コンフィギュレーション モードで **mpls ip default-route** コマンドを使用します。

mpls ip default-route

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

IP デフォルト ルートのラベルの配信はありません。

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 Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

mpls ip default-route コマンドを使用する前に、ダイナミック ラベル スイッチング（つまり、ルーティングプロトコルに基づくラベルの配信）を有効にする必要があります。

例

次に、IP デフォルト ルートに関連付けられたラベルの配信を有効にする例を示します。

```
Switch# configure terminal
Switch(config)# mpls ip
Switch(config)# mpls ip default-route
```

関連コマンド

コマンド	説明
mpls ip （グローバル コンフィギュレーション）	プラットフォーム用に通常ルーティングされるパスに沿ってIPv4パケットのMPLS転送が行われるようにします。
mpls ip （インターフェイス コンフィギュレーション）	特定のインターフェイス用に通常ルーティングされるパスに沿ってIPv4パケットのMPLS転送が行われるようにします。

mpls ip（グローバル コンフィギュレーション）

プラットフォームの通常のルーテッドパスでの IPv4 および IPv6 パケットのマルチプロトコル ラベル スイッチング（MPLS）転送を有効にするには、グローバル コンフィギュレーション モードで **mpls ip** 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。

mpls ip
no mpls ip

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

プラットフォームの通常のルーテッド パスでの IPv4 および IPv6 パケットのラベル スイッチング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

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

通常のルーテッド パスでの IPv4 および IPv6 パケットの MPLS 転送（ダイナミック ラベル スイッチングと呼ばれることもある）は、このコマンドによって有効になります。ダイナミック ラベル スイッチングを実行するように指定されたインターフェイスには、そのインターフェイス用およびプラットフォーム用にこのスイッチング機能がイネーブルになっていなければなりません。

このコマンドの **no** 形式は、インターフェイスの設定に関係なく、すべてのプラットフォーム インターフェイスのダイナミック ラベル スイッチングを停止します。また、ダイナミック ラベル スイッチングのためのラベルの配信も停止します。ただし、このコマンドの no 形式は、

ラベル スイッチパス（LSP）トンネルを介してのラベルの付いたパケットの送信には影響しません。

例

次に、プラットフォームのダイナミック ラベル スイッチングをディセーブルにし、プラットフォームのすべてのラベル配信を停止させる例を示します。

```
Switch(config)# no mpls ip
```

関連コマンド

コマンド	説明
mpls ip （インターフェイス コンフィギュレーション）	関連付けられているインターフェイスの通常のルーテッド パスでの IPv4 および IPv6 パケットの MPLS 転送を有効にします。

mpls ip（インターフェイス コンフィギュレーション）

特定のインターフェイスの通常のルーテッドパスでの IPv4 パケットおよび IPv6 パケットのマルチプロトコル ラベル スイッチング（MPLS）フォワーディングを有効にするには、インターフェイス コンフィギュレーション モードで **mpls ip** 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。

mpls ip
no mpls ip

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

インターフェイスの通常のルーテッド パスで IPv4 パケットおよび IPv6 パケットを MPLS フォワーディングする機能は無効になっています。

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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

通常のルーテッド パスで IPv4 パケットおよび IPv6 パケットを MPLS フォワーディングする機能は、ダイナミック ラベル スイッチングとも呼ばれます。プラットフォームでダイナミック ラベル スイッチングがイネーブルになっている場合、インターフェイス上でこのコマンドを実行すると、ネイバー探索 HELLO メッセージの定期送信によりインターフェイスでラベル配布が開始されます。インターフェイスを経由してルーティングされる宛先の出ラベルがわかっている場合、宛先のパケットにその出ラベルが付され、インターフェイスを経由してフォワーディングされます。

このコマンドの**no**形式を使用すると、インターフェイスを経由してルーティングされるパケットはラベルなしで送信されます。また、インターフェイスのラベル配布も終了します。しかし、このインターフェイスを使用するリンクステートパケット（LSP）トンネルを経由するラベル付きパケットの送信が、コマンドの no 形式による影響を受けることはありません。

例

次に、イーサネットインターフェイスでラベルスイッチングを有効にする例を示します。

```
Switch(config)# configure terminal
Switch(config-if)# interface TenGigabitEthernet1/0/3
Switch(config-if)# mpls ip
```

次に、Cisco Catalyst スイッチの指定された VLAN インターフェイス（SVI）でラベルスイッチングを有効にする例を示します。

```
Switch(config)# configure terminal
Switch(config-if)# interface vlan 1
Switch(config-if)# mpls ip
```

mpls label protocol（グローバル コンフィギュレーション）

プラットフォームの Label Distribution Protocol（LDP; ラベル配布プロトコル）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 **mpls label protocol** コマンドを使用します。デフォルト LDP に戻すには、このコマンドの **no** 形式を使用します。

mpls label protocol ldp
no mpls label protocol ldp

構文の説明

ldp	LDP をデフォルトのラベル配布プロトコルとすることを指定します。

コマンド デフォルト

LDP がデフォルトのラベル配布プロトコルです。

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 Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

global mpls label protocol ldp コマンドまたは interface mpls label protocol ldp コマンドのどちらも使用されていない場合は、すべてのラベル配布セッションで LDP が使用されます。

例

次のコマンドは、LDP をプラットフォームのラベル配布プロトコルとして確立します。

```
Switch(config)# mpls label protocol ldp
```

mpls label protocol（インターフェイス コンフィギュレーション）

インターフェイスの Label Distribution Protocol（LDP; ラベル配布プロトコル）を指定するには、インターフェイス コンフィギュレーション モードで **mpls label protocol** コマンドを使用します。インターフェイスから LDP を削除するには、このコマンドの **no** 形式を使用します。

mpls label protocol ldp
no mpls label protocol ldp

構文の説明

ldp	LDP がインターフェイスで使用されるように指定します。

コマンド デフォルト

インターフェイスにプロトコルが明示的に設定されていない場合は、プラットフォームに設定された LDP が使用されます。プラットフォームの LDP を設定するには、グローバルの **mpls label protocol** コマンドを使用します。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

2 つのラベル スイッチ ルータ（LSR）を接続するリンクのラベル配布用のセッションを正常に確立するには、LSR のリンク インターフェイスが同じ LDP を使用するように設定されている必要があります。2 つの LSR を接続する複数のリンクがある場合は、2 つの LSR に接続しているすべてのリンク インターフェイスが同じプロトコルを使用するように設定されている必要があります。

例

次に、LDP をインターフェイスのラベル配布プロトコルとして確立する例を示します。

```
Switch(config-if)# mpls label protocol ldp
```

mpls label range

パケットインターフェイス上のマルチプロトコル ラベル スイッチング（MPLS）で使用できるローカルラベルの範囲を設定するには、グローバル コンフィギュレーション モードで **mpls label range** コマンドを使用します。プラットフォームをデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

mpls label range *minimum-value maximum-value* [**static** *minimum-static-value maximum-static-value*]
no mpls label range

構文の説明

minimum-value	ラベル スペースで許容される最小のラベルの値。デフォルトは 16 です。
maximum-value	ラベル スペースで許容される最大のラベルの値。デフォルトはプラットフォームによって異なります。
static	（任意）スタティック ラベル割り当てに使用するローカル ラベルのブロックを予約します。**static** キーワードと *minimum-static-value maximum-static-value* 引数を省略すると、スタティック割り当て用にラベルは予約されません。
minimum-static-value	（任意）スタティック ラベル割り当ての最小値。デフォルト値はありません。
maximum-static-value	（任意）スタティック ラベル割り当ての最大値。デフォルト値はありません。

コマンド デフォルト

プラットフォームのデフォルト値が使用されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

ラベル 0 ～ 15 は IETF によって予約されており（詳細については、RFC 3032「MPLS Label Stack Encoding」を参照）、**mpls label range** コマンドで指定する範囲に含めることはできません。コマンドに 0 を入力すると、コマンドが認識されなかったコマンドであることを示すメッセージが表示されます。

mpls label range コマンドで定義されたラベル範囲は、（ダイナミック ラベル スイッチング、MPLS、MPLS トラフィック エンジニアリング、MPLS バーチャル プライベート ネットワーク（VPN）などの）ローカルラベルを割り当てるすべての MPLS アプリケーションによって使用されます。

Label Distribution Protocol（LDP; ラベル配布プロトコル）などのラベル配布プロトコルを使用して、16 ～ 1048575 の汎用的なラベル範囲をダイナミック割り当て用に予約できます。

スタティック割り当て用にラベルを予約するには、オプションの **static** キーワードを指定します。MPLS スタティック ラベル機能では、スタティック割り当て用のラベルの範囲を設定する必要があります。スタティック バインディングは現在のスタティック範囲からのみ設定できます。スタティック範囲が設定されていないか、使い果たされている場合は、スタティック バインディングを設定できません。

ラベル値の範囲は、16～4096です。最大値のデフォルトは、4096です。たとえば、スタティック ラベル スペースを16～100、ダイナミック ラベル スペースを101 ～ 4096のように分割することができます。

最小スタティック ラベル値の上限と下限がヘルプ ラインに表示されます。たとえば、ダイナミック ラベルの最小値を16、最大値を100に設定すると、ヘルプ ラインには次のように表示されます。

```
Switch(config)# mpls label range 16 100 static ?
<100>  Upper Minimum static label value
<16>         Lower Minimum static label value
Reserved Label Range  --> 0    to 15
Available Label Range --> 16   to 4096
Static Label Range    --> 16   to 100
Dynamic Label Range   --> 101  to 4096
```

この例では、スタティックを16 ～ 100に設定できます。

下部の最小スタティック ラベル スペースが使用できない場合、最小値の下限はヘルプ ラインに表示されません。次に例を示します。

```
Switch(config)# mpls label range 16 100 static ?
  <16-100>  static label value range
```

例

次に、ローカル ラベル スペースのサイズを設定する例を示します。この例では、最小スタティック値が200に、最大スタティック値が4000に設定されています。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# mpls label range 200 4000
Switch(config)#
```

現在の範囲に重複する新しい範囲を指定すると（たとえば、新しい範囲の最小スタティック値を16、最大スタティック値を1000に設定する）、新しい範囲が即座に有効になります。

次に、ダイナミック ローカル ラベル スペースの最小スタティック値を100、最大スタティック値を1000に設定し、スタティック ラベル スペースの最小スタティック値を16、最大スタティック値を99に設定する例を示します。

```
Switch(config)# mpls label range 100 1000 static 16 99
Switch(config)#
```

リロード後に実行される **show mpls label range** コマンドの次の出力では、設定された範囲が有効になっていることが示されます。

```
Switch# show mpls label range
Downstream label pool: Min/Max label: 100/1000
Range for static labels: Min/Max/Number: 16/99
```

次に、ラベル範囲をデフォルト値に戻す例を示します。

```
Switch# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no mpls label range
Switch(config)# end
```

関連コマンド

コマンド	説明
show mpls label range	MPLS ローカル ラベル スペースの範囲を表示します。

show mpls label range

パケットインターフェイスで使用可能なローカルラベルの範囲を表示するには、特権 EXEC モードで **show mpls label range** コマンドを使用します。

show mpls label range

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

mpls label range コマンドを使用して、デフォルトの範囲とは異なるローカルラベルの範囲を設定できます。**show mpls label range** コマンドでは、現在使用中のラベル範囲と、スイッチの次のリロード後に使用されるラベル範囲の両方が表示されます。

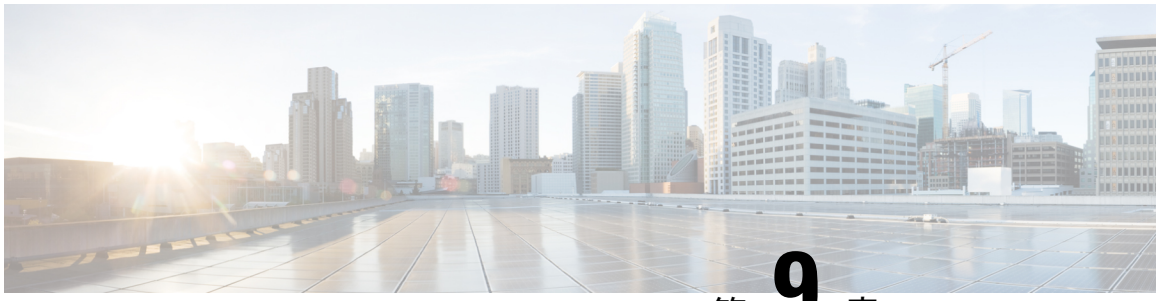
例

次に、最初のラベル範囲にオーバーラップしないラベル範囲を設定するために **mpls label range** コマンドを使用する前と後で、**show mpls label range** コマンドを使用した場合の出力例を示します。

```
Switch# show mpls label range
Downstream label pool: Min/Max label: 16/100
Switch# configure terminal
Switch(config)# mpls label range 101 4000
Switch(config)# exit
Switch# show mpls label range
Downstream label pool: Min/Max label: 101/4000
```

関連コマンド

コマンド	説明
mpls label range	ローカル ラベルとして使用する値の範囲を設定します。



第 9 章

マルチキャスト VPN コマンド

ip multicast-routing

IP マルチキャストルーティングをイネーブルにするには、グローバル コンフィギュレーション モードで **ip multicast-routing** コマンドを使用します。IP マルチキャストルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip multicast-routing [**vrf** *vrf-name*]
no ip multicast-routing [**vrf** *vrf-name*]

構文の説明

vrf *vrf-name*	（任意）*vrf-name* 引数に指定されたマルチキャスト VPN ルーティングおよび転送（MVRF）インスタンスのための IP マルチキャストルーティングを有効にします。

コマンド デフォルト

IP マルチキャストルーティングはディセーブルになっています。

コマンド モード

グローバル コンフィギュレーション（config）。

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン IP マルチキャスト ルーティングがディセーブルになっている場合、Cisco IOS ソフトウェアはどのマルチキャスト パケットも転送しません。

（注） IPマルチキャストの場合は、IPマルチキャストルーティングを有効にした後に、PIMをすべてのインターフェイスに設定する必要があります。IPマルチキャストルーティングを無効にしても PIM は削除されません。PIM は、インターフェイスの設定から明示的に削除する必要があります。

例

次に、IP マルチキャストルーティングをイネーブルにする例を示します。

```
Switch(config)# ip multicast-routing
```

次に、特定の VRF の IP マルチキャストルーティングを有効にする例を示します。

```
Switch(config)#
ip multicast-routing vrf vrf1
```

次に、IP マルチキャスト ルーティングをディセーブルにする例を示します。

```
Switch(config)#
no ip multicast-routing
```

次に、Cisco IOS XE リリース 3.3S で特定の VRF の MDS を有効にする例を示します。

```
Switch(config)#
ip multicast-routing vrf vrf1
```

関連コマンド

コマンド	説明
ip pim	インターフェイスに対してPIMをイネーブルにします。

ip multicast mrinfo-filter

マルチキャストルータ情報（mrinfo）要求パケットをフィルタ処理するには、グローバル コンフィギュレーション モードで **ip multicast mrinfo-filter** コマンドを使用します。mrinfo 要求のフィルタを削除するには、このコマンドの **no** 形式を使用します。

ip multicast [**vrf** *vrf-name*] **mrinfo-filter** *access-list*
no ip multicast [**vrf** *vrf-name*] **mrinfo-filter**

構文の説明

vrf	（任意）マルチキャストVPNルーティングおよび転送（VRF）インスタンスをサポートします。
vrf-name	（任意）VRF に割り当てられた名前。

access-list	どのネットワークまたはホストが **mrinfo** コマンドを使用して、ローカル マルチキャストデバイスをクエリできるかを判別するIP標準の番号付けまたは名前付けされたアクセスリスト。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

ip multicast mrinfo-filter コマンドは、指定されたアクセスリストによって拒否されたすべての送信元からの mrinfo 要求パケットをフィルタ処理します。つまり、アクセス リストが送信元を拒否すると、その送信元の mrinfo 要求は除外されます。ACL によって許可された送信元からの mrinfo 要求は処理が許可されます。

例

次に、ネットワーク 192.168.1.1 のすべてのホストからの mrinfo 要求パケットをフィルタ処理し、その他のホストからの要求は許可する例を示します。

```
ip multicast mrinfo-filter 51
access-list 51 deny 192.168.1.1
access list 51 permit any
```

関連コマンド

Command	Description
mrinfo	ピアリングしている隣接するマルチキャスト デバイスについて、マルチキャスト デバイスにクエリします。

mdt data

データマルチキャスト配信ツリー（MDT）プールで使用されるアドレス範囲を指定するには、VRF コンフィギュレーション モードまたは VRF アドレス ファミリ コンフィギュレーション モードで **mdt data** 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。

mdt data threshold *kb/s*
no mdt data threshold *kb/s*

構文の説明

threshold *kb/s*	（任意）帯域幅しきい値をキロビット/秒（kb/s）単位で定義します。範囲は 1 ～ 4294967 です。

コマンド デフォルト

データ MDT プールは設定されていません。

コマンド モード

VRF アドレス ファミリ コンフィギュレーション（config-vrf-af）

VRF コンフィギュレーション（config-vrf）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

データ MDT には、MVPN ごとに最大 256 のマルチキャスト グループを含めることができます。データ MDT の作成に使用されるマルチキャスト グループは、設定済み IP アドレスのプールからダイナミックに選択されます。

データ MDT プールで使用されるアドレス範囲を指定するには、 **mdt data** コマンドを使用します。しきい値は、kb/s 単位で指定されます。オプションの **list** キーワードと *access-list* 引数を使用して、データ MDT プールで使用する (S, G) MVPN エントリを定義できます。これによって、データ MDT プールの作成は、*access-list* 引数に指定されたアクセスリストで定義された特定の (S, G) MVPN エントリにさらに限定されます。

mdt data コマンドには、**ip vrf** 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できます。また、**mdt data** コマンドには、**vrf definition** グローバル コンフィギュレーション コマンドに続けて **address-family ipv4** VRF コンフィギュレーション コマンドを使用することでもアクセスできます。

例

次に、MDT データ プールのグループ アドレスの範囲を設定する例を示します。500 kb/s のしきい値が設定されています。つまり、マルチキャスト ストリームが 1 kb/s を超えると、データ MDT が作成されます。

```
ip vrf vrf1
 rd 1000:1
 route-target export 10:27
 route-target import 10:27
 mdt default 236.1.1.1
 mdt data 228.0.0.0 0.0.0.127 threshold 500 list 101
!
.
.
.
!
ip pim ssm default
ip pim vrf vrf1 accept-rp auto-rp
!
```

関連コマンド

コマンド	説明
mdt default	VPN VRF のデフォルトの MDT グループを設定します。

mdt default

バーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）のデフォルトのマルチキャスト配信ツリー（MDT）グループを設定するには、VRF コンフィギュレーションまたは VRF アドレス ファミリ コンフィギュレーション モードで **mdt default** 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。

mdt default*group-address*
no mdt default*group-address*

構文の説明

group-address	デフォルト MDT グループの IP アドレス同じグループ アドレスで設定されるプロバイダーエッジ（PE）デバイスはグループのメンバになるため、このアドレスはコミュニティの ID として機能し、これによってプロバイダーエッジ ルータ間で相互にパケットを送受信できるようになります。

コマンド デフォルト

このコマンドはディセーブルです。

コマンド モード

VRF アドレス ファミリ コンフィギュレーション（config-vrf-af）VRF コンフィギュレーション（config-vrf）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

デフォルト MDT グループは、同じ VPN に属するすべての PE デバイスに設定された同じグループである必要があります。

Source Specific Multicast（SSM; 送信元特定マルチキャスト）がデフォルト MDT のプロトコルとして使用されている場合、送信元 IP アドレスは、Border Gateway Protocol（BGP）セッションの送信元に使用されるアドレスです。

このコマンドによって、トンネルインターフェイスが作成されます。デフォルトでは、トンネル ヘッダーの宛先アドレスは、 *group-address* 引数です。

mdt default コマンドには、**ip vrf** 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できます。また、**mdt default** コマンドには、**vrf definition** グローバル コンフィギュレーション コマンドに続けて **address-family ipv4** VRF コンフィギュレーション コマンドを使用することでもアクセスできます。

例

次に、Protocol Independent Multicast（PIM）SSM をバックボーンに設定する例を示します。そのため、デフォルト グループとデータ MDT グループは、IP アドレスの SSM 範囲内に設定されています。VPN の内部では、PIM スパースモード（PIM-SM）が設定され、Auto-RP アナウンスのみが受け入れられます。

```
ip vrf vrf1
```

```
 rd 1000:1
 mdt default 236.1.1.1
 mdt data 228.0.0.0 0.0.0.127 threshold 50
 mdt data threshold 50
 route-target export 1000:1
 route-target import 1000:1
!
!
```

関連コマンド

コマンド	説明
mdt data	データ MDT グループ用にマルチキャスト グループのアドレス範囲を設定します。

mdt log-reuse

データマルチキャスト配信ツリー（MDT）の再利用の記録を有効にするには、VRF コンフィギュレーション モードまたは VRF アドレス ファミリ コンフィギュレーション モードで **mdt log-reuse** 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。

mdt log-reuse
no mdt log-reuse

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

このコマンドはディセーブルです。

コマンド モード

VRF アドレス ファミリ コンフィギュレーション（config-vrf-af）VRF コンフィギュレーション（config-vrf）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

mdt log-reuse コマンドは、データ MDT が再利用されるたびに Syslog メッセージを生成します。

mdt log-reuse コマンドには、**ip vrf** 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できます。また、**mdt log-reuse** コマンドには、**vrf definition** グローバル コンフィギュレーション コマンドに続けて **address-family ipv4** VRF コンフィギュレーション コマンドを使用することでもアクセスできます。

例

次に、MDT の再利用のログを有効にする例を示します。

```
mdt log-reuse
```

関連コマンド

コマンド	説明
mdt data	データ MDT グループ用にマルチキャスト グループのアドレス範囲を設定します。
mdt default	VPN VRF のデフォルトの MDT グループを設定します。

show ip pim mdt bgp

マルチキャスト配信ツリー（MDT）のデフォルト グループのルート識別子（RD）の Border Gateway Protocol（BGP）アドバタイズメントに関する詳細を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで show ip pim mdt bgp コマンドを使用します。

show ip pim [**vrf** *vrf-name*] **mdt bgp**

構文の説明

vrf *vrf-name*	（任意）*vrf-name* 引数に指定されたマルチキャスト バーチャル プライベート ネットワーク（MVPN）ルーティングおよび転送（MVRF）インスタンスに関連付けられた MDT デフォルト グループの RD の BGP アドバタイズメントに関する情報を表示します。

コマンド モード

ユーザ EXEC、特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

MDT デフォルト グループの RD の詳細な BGP アドバタイズメントを表示するには、このコマンドを使用します。

例

次に、 **show ip pim mdt bgp** コマンドの出力例を示します。

```
Device# show ip pim mdt bgp
MDT-default group 232.2.1.4
 rid:10.1.1.1 next_hop:10.1.1.1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 28 : show ip pim mdt bgp のフィールドの説明

フィールド	説明
MDT-default group	このルータにアドバタイズされた MDT デフォルト グループ。
rid:10.1.1.1	アドバタイズしたルータの BGP ルータ ID。
next_hop:10.1.1.1	アドバタイズメントに含まれていた BGP ネクスト ホップ アドレス。

show ip pim mdt history

再利用されているデータマルチキャスト配信ツリー（MDT）グループの履歴に関する情報を表示するには、特権 EXEC モードで **show ip pim mdt history** コマンドを使用します。

show ip pim vrf *vrf-name* **mdt history interval** *minutes*

構文の説明

vrf *vrf-name*	*vrf-name* 引数に指定されたマルチキャスト VPN（MVPN）ルーティングおよび転送（MVRF）インスタンス用に再利用されているデータ MDT グループの履歴を表示します。
interval *minutes*	再利用されているデータ MDT グループの履歴について情報を表示する間隔（分単位）を指定します。範囲は 1 ～ 71512 分（7 週間）です。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

show ip pim mdt history コマンドの出力には、**interval** キーワードと *minutes* 引数で指定された間隔の再利用された MDT データグループの履歴が表示されます。間隔は過去から現在まで、つまり、*minutes* 引数に指定された時間からコマンドが実行された時間までです。

例

次に、**show ip pim mdt history** コマンドの出力例を示します。

```
Device# show ip pim vrf vrf1 mdt history interval 20
   MDT-data send history for VRF - vrf1 for the past 20 minutes
MDT-data group        Number of reuse
     10.9.9.8           3
     10.9.9.9           2
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *29 : show ip pim mdt history* のフィールドの説明

フィールド	説明
MDT-data group	情報が表示されている MDT データ グループ。
Number of reuse	このグループで再利用されたデータ MDT の数。

show ip pim mdt receive

プロバイダーエッジ（PE）ルータから受信したデータマルチキャスト配信ツリー（MDT）グループマッピングを表示するには、特権 EXEC モードで **show ip pim mdt receive** コマンドを使用します。

show ip pim vrf *vrf-name* **mdt receive** [**detail**]

構文の説明

vrf *vrf-name*	*vrf-name* 引数に指定されたマルチキャスト VPN（MVPN）ルーティングおよび転送（MVRF）インスタンスのデータ MDT マッピングを表示します。
detail	（任意）受信されたデータ MDT アドバタイズメントの詳細な説明を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

ルータがデフォルトの MDT からデータ MDT に切り替えるときには、VRF 送信元、グループペア、およびトラフィックが送信されるグローバル マルチキャスト アドレスをアドバタイズします。リモートルータがこのデータを受信する場合は、このグローバルアドレスマルチキャスト グループに加入します。

例

次に、さらに情報を取得するために **detail** キーワードを使用した **show ip pim mdt receive** コマンドの出力例を示します。

```
Device# show ip pim vrf vpn8 mdt receive detail
Joined MDT-data groups for VRF:vpn8
group:172.16.8.0 source:10.0.0.100 ref_count:13
(10.101.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:26, OIF count:1, flags:TY
(10.102.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:27, OIF count:1, flags:TY
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *30 : show ip pim mdt receive* のフィールドの説明

フィールド	説明
group:172.16.8.0	データ MDT を作成したグループ
source:10.0.0.100	データ MDT を作成した VRF 送信元
ref_count:13	このデータ MDT を再利用している (S, G) ペアの数
OIF count:1	このマルチキャスト データを転送しているインターフェイスの数

フィールド	説明
flags:	エントリに関する情報です。 • A：候補となる Multicast Source Discovery Protocol（MSDP）アドバタイズメント • B：双方向グループ • D：デンス • C：接続済み • F：登録フラグ • I：受信した送信元固有のホスト レポート • J：最短パス送信元ツリー（SPT）の結合 • L：ローカル • M：MSDP が作成したエントリ • P：プルーニング済み • R：RP ビットが設定済み • S：スパース • s：Source Specific Multicast（SSM）グループ • T：SPT ビット セット • X：プロキシ結合タイマーの実行中 • U：URL Rendezvous Directory（URD） • Y：結合された MDT データ グループ • y：MDT データ グループに送信中 • Z：マルチキャスト トンネル

show ip pim mdt send

使用中のデータマルチキャスト配信ツリー（MDT）グループを表示するには、特権EXECモードで **show ip pim mdt send** コマンドを使用します。

show ip pim vrf *vrf-name* **mdt send**

構文の説明

vrf *vrf-name*	*vrf-name* 引数に指定されたマルチキャスト VPN（MVPN）ルーティングおよび転送（MVRF）インスタンスによって使用されているデータ MDT グループを表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

使用上のガイドライン

指定された MVRF によって使用されているデータ MDT グループを表示するには、このコマンドを使用します。

例

次に、**show ip pim mdt send** コマンドの出力例を示します。

```
Device# show ip pim vrf vpn8 mdt send
MDT-data send list for VRF:vpn8
  (source, group)                      MDT-data group      ref_count
  (10.100.8.10, 225.1.8.1)             232.2.8.0           1
  (10.100.8.10, 225.1.8.2)             232.2.8.1           1
  (10.100.8.10, 225.1.8.3)             232.2.8.2           1
  (10.100.8.10, 225.1.8.4)             232.2.8.3           1
  (10.100.8.10, 225.1.8.5)             232.2.8.4           1
  (10.100.8.10, 225.1.8.6)             232.2.8.5           1
  (10.100.8.10, 225.1.8.7)             232.2.8.6           1
  (10.100.8.10, 225.1.8.8)             232.2.8.7           1
  (10.100.8.10, 225.1.8.9)             232.2.8.8           1
  (10.100.8.10, 225.1.8.10)            232.2.8.9           1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *31 : show ip pim mdt send* のフィールドの説明

フィールド	説明
source, group	このルータがデータ MDT に切り替えた送信元とグループのアドレス
MDT-data group	これらのデータ MDT が送信されるマルチキャスト アドレス
ref_count	このデータ MDT を再利用している (S, G) ペアの数

第 VIII 部

ネットワーク管理

第 10 章

Flexible NetFlow

cache

フローモニタのフローキャッシュパラメータを設定するには、フローモニタ コンフィギュレーション モードで **cache** コマンドを使用します。フローモニタのフローキャッシュパラメータを削除するには、このコマンドの **no** 形式を使用します。

cache {**timeout** {**active** | **inactive**} *seconds* | **type** **normal**}
no **cache** {**timeout** {**active** | **inactive**} | **type**}

構文の説明

timeout	フロー タイムアウトを指定します。
active	アクティブ フロー タイムアウトを指定します。
inactive	非アクティブ フロー タイムアウトを指定します。
seconds	タイムアウト値（秒単位）。範囲は 1 ～ 604800 （7日）です。
type	フローキャッシュのタイプを指定します。

normal	通常キャッシュタイプを設定します。フローキャッシュ内のエントリは、**timeout active** *seconds* および **timeout inactive** *seconds* の設定に従って期限切れになります。これがデフォルトのキャッシュタイプです。

コマンド デフォルト

デフォルトのフロー モニタ フロー キャッシュ パラメータが使用されます。

フローモニタの以下のフロー キャッシュ パラメータがイネーブルになっています。

- キャッシュタイプ：normal
- アクティブ フロー タイムアウト：1800 秒
- 非アクティブ フロー タイムアウト：15 秒

コマンド モード

フロー モニタ コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

各フローモニタには、モニタするすべてのフローの保存に使用するキャッシュがあります。各キャッシュには、フローがキャッシュ内に留まることができる時間など、設定可能な要素があります。フローがタイムアウトするとキャッシュから削除され、対応するフローモニタ用に設定されている任意のエクスポータに送信されます。

cache timeout active コマンドでは、通常タイプのキャッシュのエージング動作を制御します。フローが長時間アクティブになっている場合、通常はエージアウト（そのフローの後続のパケット用の新しいフローを開始）することが望まれます。このエージアウトプロセスを行うことで、エクスポートを受信するモニタリングアプリケーションに最新の情報を反映し続けることができます。デフォルトでは、このタイムアウトは 1800 秒（30分）ですが、システム要件に応じて調整できます。大きい値を設定すると、存続時間の長いフローを単一のフローレコードに記録することができます。小さい値を設定すると、存続時間の長い新しいフローが開始されてから、そのフローのデータがエクスポートされるまでの遅延が短縮されます。アクティブ フロー タイムアウトを変更した場合、新しいタイムアウト値はただちに有効になります。

また、**cache timeout inactive** コマンドでも、通常タイプのキャッシュのエージング動作を制御できます。指定した時間内にフローでアクティビティが検出されない場合、そのフローはエージアウトされます。デフォルトでは、このタイムアウトは15秒ですが、この値は想定されるトラフィックのタイプに応じて調整できます。存続時間の短いフローが多数存在し、多くのキャッシュエントリが消費されている場合は、非アクティブタイムアウトを短縮することでこのオーバーヘッドを削減できます。多数のフローが、データを収集し終わる前に頻繁にエージアウトしている場合は、このタイムアウトを延長することでフローの相関関係を向上できます。非アクティブ フロー タイムアウトを変更した場合、新しいタイムアウト値はただちに有効になります。

cache type normal コマンドでは、通常キャッシュタイプを指定します。これがデフォルトのキャッシュタイプです。キャッシュのエントリは、**timeout active** *seconds* および **timeout inactive**

seconds の設定に従って、エージアウトされます。キャッシュエントリはエージアウトされると、キャッシュから削除され、そのキャッシュに対応するモニタ用に設定されているエクスポータによってエクスポートされます。

キャッシュをデフォルト設定に戻すには、**default cache** フロー モニタ コンフィギュレーション コマンドを使用します。

（注） キャッシュが一杯になると、新しいフローはモニタされません。

次に、フローモニタキャッシュのアクティブタイムアウトを設定する例を示します。

```
デバイス(config)# flow monitor FLOW-MONITOR-1
デバイス(config-flow-monitor)# cache timeout active 4800
```

次に、フローモニタキャッシュの非アクティブタイマーを設定する例を示します。

```
デバイス(config)# flow monitor FLOW-MONITOR-1
デバイス(config-flow-monitor)# cache timeout inactive 30
```

次に、通常キャッシュを設定する例を示します。

```
デバイス(config)# flow monitor FLOW-MONITOR-1
デバイス(config-flow-monitor)# cache type normal
```

clear flow exporter

Flexible Netflow フローエクスポータの統計情報をクリアするには、特権 EXEC モードで **clear flow exporter** コマンドを使用します。

clear flow exporter [[**name**] *exporter-name*] **statistics**

構文の説明

name	（任意）フローエクスポータの名前を指定します。
exporter-name	（任意）以前に設定されたフローエクスポータの名前。
statistics	フローエクスポータの統計情報をクリアします。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

clear flow exporter コマンドは、フローエクスポータからすべての統計情報を削除します。これらの統計情報はエクスポートされず、キャッシュ内に保存されていたデータは失われます。

show flow exporter statistics 特権 EXEC コマンドを使用して、フローエクスポータの統計情報を表示できます。

例

次の例では、deviceで設定されているすべてのフローエクスポータの統計情報をクリアします。

```
デバイス# clear flow exporter statistics
```

次の例では、FLOW-EXPORTER-1 という名前のフローエクスポータの統計情報をクリアします。

```
デバイス# clear flow exporter FLOW-EXPORTER-1 statistics
```

clear flow monitor

フローモニタキャッシュまたはフローモニタ統計情報をクリアし、フローモニタキャッシュ内のデータを強制的にエクスポートするには、特権 EXEC モードで **clear flow monitor** コマンドを使用します。

clear flow monitor [**name**] *monitor-name* [{[**cache**] **force-export** | **statistics**}]

構文の説明

name	フローモニタの名前を指定します。
monitor-name	以前に設定されたフローモニタの名前
cache	（任意）フローモニタキャッシュ情報をクリアします。
force-export	（任意）フローモニタキャッシュ統計情報を強制的にエクスポートします。
statistics	（任意）フローモニタの統計情報をクリアします。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

clear flow monitor cache コマンドを実行すると、フローモニタキャッシュからすべてのエントリが削除されます。キャッシュ内のエントリはエクスポートされ、キャッシュ内に保存されていたデータは失われます。

（注） クリアされたキャッシュエントリの統計情報は保持されます。

clear flow monitor force-export コマンドを実行すると、フローモニタキャッシュからすべてのエントリが削除され、それらのエントリはフローモニタに割り当てられているすべてのフローエクスポータを使用してエクスポートされます。このアクションにより、CPU使用率は一時的に増加します。このコマンドの使用には注意が必要です。

clear flow monitor statistics コマンドを実行すると、このフローモニタの統計情報がクリアされます。

（注） **clear flow monitor statistics** コマンドを実行しても、現在のエントリに関する統計情報はクリアされません。なぜなら、この情報はキャッシュ内に保存されているエントリ数のインジケータであり、キャッシュは、このコマンドによってクリアされないためです。

フローモニタの統計情報を表示するには、**show flow monitor statistics** 特権 EXEC コマンドを使用します。

例

次に、FLOW-MONITOR-1 という名前のフローモニタの統計情報とキャッシュエントリをクリアする例を示します。

```
Device# clear flow monitor name FLOW-MONITOR-1
```

次に、FLOW-MONITOR-1 という名前のフローモニタの統計情報とキャッシュエントリをクリアして、強制的にエクスポートする例を示します。

```
Device# clear flow monitor name FLOW-MONITOR-1 force-export
```

次に、FLOW-MONITOR-1 という名前のフローモニタのキャッシュをクリアして、強制的にエクスポートする例を示します。

```
Device# clear flow monitor name FLOW-MONITOR-1 cache force-export
```

次に、FLOW-MONITOR-1 という名前のフローモニタの統計情報をクリアする例を示します。

```
Device# clear flow monitor name FLOW-MONITOR-1 statistics
```

collect

フローモニタレコードの非キーフィールドを設定し、そのレコードによって作成されたフローの各フィールドへの値の取り込みを有効にするには、フロー レコード コンフィギュレーション モードで **collect** コマンドを使用します。

collect {**counter** | **interface** | **timestamp** | **transport**}

構文の説明

counter	フロー レコードの非キーフィールドとしてフロー内のバイト数またはパケット数を設定します。詳細については、collect counter （416 ページ）を参照してください。
interface	入力および出力インターフェイス名をフロー レコードの非キー フィールドとして設定します。詳細については、collect interface （416 ページ）を参照してください。
timestamp	フロー内の最初または最後に確認されたパケットの絶対時間をフロー レコードの非キー フィールドとして設定します。詳細については、collect timestamp absolute （417 ページ）を参照してください。
transport	フロー レコードからの転送 TCP フラグの収集を有効にします。詳細については、collect transport tcp flags （418 ページ）を参照してください。

コマンド デフォルト

フローモニタレコードの非キーフィールドは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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

非キーフィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キーフィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キーフィールドの値はフロー内の最初のパケットからのみ取得されます。

collect コマンドは、フローモニタレコードの非キーフィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キーフィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キーフィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キーフィールドの値はフロー内の最初のパケットからのみ取得されます。

（注） **flow username** キーワードは、コマンドラインのヘルプストリングには表示されますが、サポートされていません。

次に、フローの合計バイト数を非キーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter bytes long
```

collect counter

フロー レコードの非キーフィールドとしてフロー内のバイト数またはパケット数を設定するには、フロー レコード コンフィギュレーション モードで **collect counter** コマンドを使用します。フロー（カウンタ）内のバイト数またはパケット数をフロー レコードの非キーフィールドとして使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

コマンド デフォルト

フロー内のバイト数またはパケット数は、非キーフィールドとして設定されません。

コマンド モード

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

このコマンドをデフォルト設定に戻すには、**no collect counter** または **default collect counter** フロー レコード コンフィギュレーション コマンドを使用します。

次に、フローの合計バイト数を非キーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#collect counter bytes long
```

次に、フローからの合計パケット数を非キーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter packets long
```

collect interface

フローレコードの非キーフィールドとして入力インターフェイス名を設定するには、フロー レコード コンフィギュレーション モードで **collect interface** コマンドを使用します。入力インターフェイスをフローレコードの非キーフィールドとして使用する設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

collect interface input
no collect interface input

構文の説明

input	入力インターフェイス名を非キーフィールドとして設定し、フローから入力インターフェイスを収集します。

コマンド デフォルト

入力インターフェイス名は、非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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

Flexible NetFlow **collect** コマンドは、フローモニタレコードの非キーフィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キーフィールドの値は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キーフィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キーフィールドの値はフロー内の最初のパケットからのみ取得されます。

このコマンドをデフォルト設定に戻すには、**no collect interface** または **default collect interface** 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、非キーフィールドとして入力インターフェイスを設定します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect interface input
```

collect timestamp absolute

フロー内の最初または最後に確認されたパケットの絶対時間をフローレコードの非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 **collect timestamp absolute** コマンドを使用します。フロー内の最初または最後に確認されたパケットをフローレコードの非キーフィールドとして使用するのを無効にするには、このコマンドの **no** 形式を使用します。

collect timestamp absolute {**first** | **last**}
no collect timestamp absolute {**first** | **last**}

構文の説明

first	フロー内の最初に確認されたパケットの絶対時間を非キーフィールドとして設定し、フローからのタイムスタンプの収集を有効にします。
last	フロー内の最後に確認されたパケットの絶対時間を非キーフィールドとして設定し、フローからのタイムスタンプの収集を有効にします。

コマンド デフォルト

絶対時間フィールドは非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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

collect コマンドは、フローモニタレコードの非キーフィールドを設定し、そのレコードによって作成されたフローの各フィールドに値を取り込むために使用します。非キーフィールドの値

は、フロー内のトラフィックに関する追加情報を提供するためにフローに追加されます。非キーフィールドの値の変更によって新しいフローが作成されることはありません。ほとんどの場合、非キーフィールドの値はフロー内の最初のパケットからのみ取得されます。

次に、フロー内の最初に確認されたパケットの絶対時間に基づくタイム スタンプを非キーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect timestamp absolute first
```

次に、フロー内の最後に確認されたパケットの絶対時間に基づくタイム スタンプを非キーフィールドとして設定する例を示します。

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect timestamp absolute last
```

collect transport tcp flags

フローからの転送 TCP フラグの収集をイネーブルにするには、フロー レコード コンフィギュレーション モードで **collect transport tcp flags** コマンドを使用します。フローからの転送 TCP フラグの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。

collect transport tcp flags
no collect transport tcp flags

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

トランスポート層フィールドは非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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

トランスポート層フィールドの値は、フロー内のすべてのパケットから取得されます。収集する TCP フラグを指定することはできません。転送 TCP フラグの収集のみ指定できます。すべての TCP フラグはこのコマンドで収集されます。次の転送 TCP フラグを収集します。

- **ack**：TCP 確認応答フラグ
- **cwr**：TCP 輻輳ウィンドウ縮小フラグ
- **ece**：TCP ECN エコー フラグ
- **fin**：TCP 終了フラグ
- **psh**：TCP プッシュ フラグ

- **rst**：TCP リセット フラグ
- **syn**：TCP 同期フラグ
- **urg**：TCP 緊急フラグ

このコマンドをデフォルト設定に戻すには、**no collect collect transport tcp flags** または **default collect collect transport tcp flags** フロー レコード コンフィギュレーション コマンドを使用します。

次に、フローから TCP フラグを収集する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# collect transport tcp flags
```

datalink flow monitor

インターフェイスに Flexible NetFlow フローモニタを適用するには、インターフェイス コンフィギュレーション モードで **datalink flow monitor** コマンドを使用します。Flexible NetFlow フロー モニタ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。

datalink flow monitor *monitor-name* **sampler** *sampler-name* **input**
no datalink flow monitor *monitor-name* **sampler** *sampler-name* **input**

構文の説明

monitor-name	インターフェイスに適用するフロー モニタの名前。
sampler *sampler-name*	フロー モニタ用に指定したフロー サンプラーをイネーブルにします。
input	スイッチがインターフェイスで受信するトラフィックをモニタします。

コマンド デフォルト

フローモニタはイネーブルになっていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

datalink flow monitor コマンドを使用してインターフェイスにフローモニタを適用する前に、**flow monitor** 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フローモニタを作成し、**sampler** 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フローサンプラーを作成しておく必要があります。

フロー モニタ用のフロー サンプラーをイネーブルにするには、事前にサンプラーを作成しておく必要があります。

（注） **datalink flow monitor** コマンドは、非 IPv4 および非 IPv6 トラフィックだけをモニタします。IPv4 トラフィックをモニタするには、**ip flow monitor** コマンドを使用します。IPv6 トラフィックをモニタするには、**ipv6 flow monitor** コマンドを使用します。

次に、インターフェイス上での Flexible NetFlow データリンク モニタリングをイネーブルにする例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# datalink flow monitor FLOW-MONITOR-1 sampler FLOW-SAMPLER-1 input
```

debug flow exporter

Flexible NetFlow フローエクスポータのデバッグ出力をイネーブルにするには、特権 EXEC モードで **debug flow exporter** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug flow exporter [[**name**] *exporter-name*] [{**error** | **event** | **packets** *number*}]
no debug flow exporter [[**name**] *exporter-name*] [{**error** | **event** | **packets** *number*}]

構文の説明

name	（任意）フローエクスポータの名前を指定します。
exporter-name	（任意）前に設定されたフロー エクスポータの名前。
error	（任意）フロー エクスポータのエラーのデバッグをイネーブルにします。
event	（任意）フロー エクスポータのイベントのデバッグをイネーブルにします。
packets	（任意）フロー エクスポータのパケットレベルのデバッグをイネーブルにします。
number	（任意）フロー エクスポータのパケットレベルのデバッグでデバッグするパケット数。指定できる範囲は 1 ～ 65535 です。

コマンド モード

特権 EXEC

コマンド履歴

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

例

次の例は、フローエクスポータのパケットがプロセス送信用のキューに格納されたことを示しています。

```
Device# debug flow exporter
May 21 21:29:12.603: FLOW EXP: Packet queued for process send
```

debug flow monitor

Flexible NetFlow フローモニタのデバッグ出力をイネーブルにするには、特権 EXEC モードで **debug flow monitor** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug flow monitor [{**error** | [**name**] *monitor-name* [{**cache** [**error**] | **error** | **packets** *packets*}]}]
no debug flow monitor [{**error** | [**name**] *monitor-name* [{**cache** [**error**] | **error** | **packets** *packets*}]}]

構文の説明

error	（任意）すべてのフロー モニタまたは指定されたフロー モニタのフロー モニタ エラーのデバッグをイネーブルにします。
name	（任意）フロー モニタの名前を指定します。
monitor-name	（任意）事前に設定されたフロー モニタの名前。
cache	（任意）フロー モニタ キャッシュのデバッグをイネーブルにします。
cache error	（任意）フロー モニタ キャッシュ エラーのデバッグをイネーブルにします。
packets	（任意）フロー モニタのパケットレベルのデバッグをイネーブルにします。
パケット	（任意）フロー モニタのパケットレベルのデバッグでデバッグするパケットの数。指定できる範囲は 1 ～ 65535 です。

コマンド モード

特権 EXEC

コマンド履歴

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

例

次の例は、FLOW-MONITOR-1 のキャッシュが削除されたことを示しています。

```
Device# debug flow monitor FLOW-MONITOR-1 cache
May 21 21:53:02.839: FLOW MON:  'FLOW-MONITOR-1' deleted cache
```

debug flow record

Flexible NetFlow フローレコードのデバッグ出力をイネーブルにするには、特権 EXEC モードで **debug flow record** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug flow record [{[**name**] *record-name* | **options** {**sampler-table**} | [{**detailed** | **error**}]}]
no debug flow record [{[**name**] *record-name* | **options** {**sampler-table**} | [{**detailed** | **error**}]}]

構文の説明

name	（任意）フロー レコードの名前を指定します。
record-name	（任意）前に設定されたユーザ定義のフロー レコードの名前。
options	（任意）他のフロー レコードオプションに関する情報が含まれます。
sampler-table	（任意）サンプラー テーブルに関する情報が含まれます。
detailed	（任意）詳細情報を表示します。
error	（任意）エラーのみを表示します。

コマンド モード

特権 EXEC

コマンド履歴

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

例

次に、フロー レコードのデバッグを有効にする例を示します。

```
Device# debug flow record FLOW-record-1
```

debug sampler

Flexible NetFlow サンプラーのデバッグ出力をイネーブルにするには、特権 EXEC モードで **debug sampler** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sampler [{**detailed** | **error** | [**name**] *sampler-name* [{**detailed** | **error** | **sampling** *samples*}]}]
no debug sampler [{**detailed** | **error** | [**name**] *sampler-name* [{**detailed** | **error** | **sampling**}]}]

構文の説明

detailed	（任意）サンプラー要素の詳細デバッグをイネーブルにします。
error	（任意）サンプラー エラーのデバッグをイネーブルにします。
name	（任意）サンプラーの名前を指定します。
sampler-name	（任意）前に設定されたサンプラーの名前。
sampling *samples*	（任意）サンプリングのデバッグをイネーブルにし、デバッグするサンプルの数を指定します。

コマンド モード

特権 EXEC

コマンド履歴

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

例

次に、デバッグ プロセスが SAMPLER-1 というサンプラーの ID を取得した場合の出力例を示します。

```
Device# debug sampler detailed
*May 28 04:14:30.883: Sampler: Sampler(SAMPLER-1: flow monitor FLOW-MONITOR-1 (ip,Et1/0,O)
 get ID succeeded:1
*May 28 04:14:30.971: Sampler: Sampler(SAMPLER-1: flow monitor FLOW-MONITOR-1 (ip,Et0/0,I)
 get ID succeeded:1
```

description

フロー モニタ、フロー エクスポータ、またはフロー レコードの説明を設定するには、該当するコンフィギュレーション モードで **description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

description 説明
no description 説明

構文の説明

description	フロー モニタ、フロー エクスポータ、またはフロー レコードを説明するテキスト文字列。

コマンド デフォルト

フロー サンプラー、フロー モニタ、フロー エクスポータ、またはフロー レコードのデフォルトの説明は「ユーザ定義」です。

コマンド モード

次のコマンド モードがサポートされています。

フロー エクスポータ コンフィギュレーション

フロー モニタ コンフィギュレーション

フロー レコード コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

このコマンドをデフォルト設定に戻すには、該当するコンフィギュレーション モードで **no description** または **default description** コマンドを使用します。

次に、フロー モニタの説明を設定する例を示します。

```
デバイス(config)# flow monitor FLOW-MONITOR-1
デバイス(config-flow-monitor)# description Monitors traffic to 172.16.0.1 255.255.0.0
```

destination

フロー エクスポータのエクスポート宛先を設定するには、フロー エクスポータ コンフィギュレーション モードで **destination** コマンドを使用します。フロー エクスポータのエクスポート宛先を削除するには、このコマンドの **no** 形式を使用します。

destination {*hostnameip-address*}
no destination {*hostnameip-address*}

構文の説明

hostname	NetFlow 情報を送信するデバイスのホスト名。
ip-address	NetFlow情報を送信するワークステーションのIPv4アドレス。

コマンド デフォルト

エクスポート宛先は設定されていません。

コマンド モード

フロー エクスポータ コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

各フロー エクスポータには、宛先アドレスまたはホスト名を 1 つのみ指定できます。

デバイスのIPアドレスの代わりに、ホスト名を設定すると、ホスト名は直ちに解決され、IPv4アドレスが実行コンフィギュレーションに保存されます。ドメイン ネーム システム（DNS）の最初の名前解決に使用されたホスト名と IP アドレスのマッピングが DNS サーバ上で動的に変わる場合は、device でこれが検出されないため、エクスポートされたデータは最初の IP アドレスに送信され続け、データは失われます。

このコマンドをデフォルト設定に戻すには、フローエクスポータ コンフィギュレーション モードで **no destination** または **default destination** コマンドを使用します。

次の例に、宛先システムに キャッシュ エントリをエクスポートするようにネットワーク デバイスを設定する方法を示します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)# destination 10.0.0.4
```

dscp

フロー エクスポータ データグラムの Differentiated Services Code Point（DSCP; DiffServ コードポイント）の値を設定するには、フロー エクスポータ コンフィギュレーション モードで **dscp** コマンドを使用します。フロー エクスポータ データグラムの DSCP 値を削除するには、このコマンドの **no** 形式を使用します。

dscp *dscp*
no dscp *dscp*

構文の説明

dscp	エクスポートされたデータグラムの DSCP フィールドで使用される DSCP。指定できる範囲は 0 ～ 63 です。デフォルトは 0 です。

コマンド デフォルト

Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値は 0 です。

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドをデフォルト設定に戻すには、 **no dscp** または **default dscp** 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。

次に、エクスポートされたデータグラムの DSCP フィールドの値を 22 に設定する例を示します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)# dscp 22
```

export-protocol netflow-v9

NetFlow バージョン 9 エクスポートを Flexible NetFlow エクスポータのエクスポートプロトコルとして設定するには、フローエクスポータ コンフィギュレーションモードで**export-protocol netflow-v9** コマンドを使用します。

export-protocol netflow-v9

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

NetFlow バージョン 9 がイネーブルです。

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

device は NetFlow v5 エクスポートフォーマットをサポートしていません。NetFlow v9 エクスポートフォーマットのみがサポートされています。

次の例では、NetFlowバージョン9エクスポートをNetFlowエクスポータのエクスポートプロトコルとして設定します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)# export-protocol netflow-v9
```

exporter

フローモニタのフローエクスポータを追加するには、適切なコンフィギュレーションモードで **exporter** コマンドを使用します。フローモニタ用のフローエクスポータを削除するには、このコマンドの **no** 形式を使用します。

exporter *exporter-name*
no exporter *exporter-name*

構文の説明

exporter-name	事前に設定したフローエクスポータの名前

コマンド デフォルト

エクスポータは設定されていません。

コマンド モード

フロー モニタ コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

exporter コマンドを使用してフローモニタにフローエクスポータを適用するには、**flow exporter** コマンドを使用して事前にフローエクスポータを作成しておく必要があります。

このコマンドをデフォルト設定に戻すには、**no exporter** または **default exporter** フロー モニタ 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、フローモニタのエクスポータを設定します。

```
デバイス(config)# flow monitor FLOW-MONITOR-1
デバイス(config-flow-monitor)# exporter EXPORTER-1
```

flow exporter

フロー エクスポータを作成するか、既存の フロー エクスポータを変更して、 フロー エクスポータ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **flow exporter** コマンドを使用します。 フロー エクスポータを削除するには、このコマンドの **no** 形式を使用します。

flow exporter *exporter-name*

no flow exporter *exporter-name*

構文の説明

exporter-name	作成または変更するフローエクスポータの名前。

コマンド デフォルト

フロー エクスポータは、コンフィギュレーション内には存在しません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フローエクスポータでは、フロー モニタ キャッシュ内のデータをリモートシステム（たとえば、分析および保管のためにNetFlowコレクタを実行するサーバ）にエクスポートします。フローエクスポータは、コンフィギュレーションで別のエンティティとして作成されます。フローエクスポータは、フローモニタにデータエクスポート機能を提供するためにフローモニタに割り当てられます。複数のフローエクスポータを作成して、1 つまたは複数のフローモニタに適用すると、いくつかのエクスポート先を指定することができます。1つのフローエクスポータを作成し、いくつかのフローモニタに適用することができます。

例

次に、FLOW-EXPORTER-1 という名前のフロー エクスポータを作成し、 フロー エクスポータ コンフィギュレーション モードを開始する例を示します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)#
```

flow monitor

フローモニタを作成するか、または既存のフローモニタを変更して、フロー モニタ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **flow monitor** コマンドを使用します。フローモニタを削除するには、このコマンドの **no** 形式を使用します。

flow monitor *monitor-name*
no flow monitor *monitor-name*

構文の説明

monitor-name	作成または変更するフローモニタの名前。

コマンド デフォルト

フロー モニタはコンフィギュレーション内には存在しません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー モニタは、ネットワーク トラフィックのモニタリングを実行するためにインターフェイスに適用される コンポーネントです。フローモニタは、フローレコードとキャッシュで構成されます。フローモニタを作成した後に、フローモニタにレコードを追加します。フローモニタのキャッシュは、フローモニタが最初のインターフェイスに適用されると自動的に作成されます。フローデータは、モニタリングプロセス中にネットワークトラフィックから収集されます。このデータ収集は、フローモニタのレコード内のキーフィールドおよび非キーフィールドに基づいて実行され、フローモニタのキャッシュに保存されます。

例

次の例では、FLOW-MONITOR-1 という名前のフローモニタを作成し、フロー モニタ コンフィギュレーション モードを開始します。

```
デバイス(config)# flow monitor FLOW-MONITOR-1
デバイス(config-flow-monitor)#
```

flow record

フロー レコードを作成するか、既存のフロー レコードを変更して、フロー レコード コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **flow record** コマンドを使用します。 レコードを削除するには、このコマンドの **no** 形式を使用します。

flow record *record-name*
no flow record *record-name*

構文の説明

record-name	作成または変更するフローレコードの名前。

コマンド デフォルト

フロー レコードは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー レコードでは、フロー内のパケットを識別するために で使用するキーとともに、がフローについて収集する関連フィールドを定義します。キーと関連フィールドを任意の組み合わせで指定して、フロー レコードを定義できます。は、幅広いキー セットをサポートします。フローレコードでは、フロー単位で収集するカウンタのタイプも定義します。64 ビットのパケットまたはバイトカウンタを設定できます。

例

次に、FLOW-RECORD-1 という名前のフロー レコードを作成し、フロー レコード コンフィギュレーション モードを開始する例を示します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)#
```

ip flow monitor

deviceが受信するIPv4トラフィックのFlexible NetFlowフローモニタをイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip flow monitor** コマンドを使用します。フローモニタ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 flow monitor *monitor-name* [**sampler** *sampler-name*] **input**
no ip flow monitor *monitor-name* [**sampler** *sampler-name*] **input**

構文の説明

monitor-name	インターフェイスに適用するフロー モニタの名前。
sampler *sampler-name*	（任意）フローモニタ用に指定したフローサンプラーの名前をイネーブルにします。
input	device がインターフェイスで受信する IPv4トラフィックをモニタします。

コマンド デフォルト

フローモニタはイネーブルになっていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

ip flow monitor コマンドを使用して、任意のインターフェイスにフローモニタを適用するには、事前に **flow monitor** 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、フローモニタを作成しておく必要があります。

フローモニタにサンプラーを追加すると、その名前付きサンプラーによって選択されたパケットだけがキャッシュに保存され、フローを形成します。サンプラーを使用するたびに、その使用に対応する統計情報が別個に保存されます。

インターフェイスですでにイネーブルになっているフローモニタにサンプラーを追加することはできません。まず、そのフローモニタをインターフェイスから削除してから、同じフローモニタをサンプラーとともに追加する必要があります。

（注） 想定される使用状況を得るには、各フローの統計情報をスケールする必要があります。たとえば、100 パケットにつき 1 パケットをサンプリングするサンプラーを使用した場合は、パケットカウンタとバイトカウンタを 100 倍する必要があります。

次に、入力トラフィックのモニタリングのためにフローモニタをイネーブルにする例を示します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

次に、サンプラーによってサンプリングされる入力パケット数を制限した状態で、入力トラフィックをモニタするようにフローモニタをイネーブルにする例を示します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

次の例では、サンプラーなしでインターフェイスでイネーブルになっているフローモニタにサンプラーを追加する場合の動作を示します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

次の例では、フローモニタをサンプラーと一緒にイネーブルにできるようにするために、インターフェイスからいったん削除する方法を示します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# no ip flow monitor FLOW-MONITOR-1 input
デバイス(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

ipv6 flow monitor

device が受信する IPv6 トラフィックのフローモニタ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 flow monitor** コマンドを使用します。フローモニタ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 flow monitor *monitor-name* [**sampler** *sampler-name*] **input**
no ipv6 flow monitor *monitor-name* [**sampler** *sampler-name*] **input**

構文の説明

monitor-name	インターフェイスに適用するフロー モニタの名前。
sampler *sampler-name*	（任意）フローモニタ用に指定したフローサンプラーの名前をイネーブルにします。

input	device がインターフェイスで受信する IPv6 トラフィックをモニタします。

コマンド デフォルト

フローモニタはイネーブルになっていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

ipv6 flow monitor コマンドを使用して、任意のインターフェイスにフローモニタを適用するには、事前に **flow monitor** 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、フローモニタを作成しておく必要があります。

フローモニタにサンプラーを追加すると、その名前付きサンプラーによって選択されたパケットだけがキャッシュに保存され、フローを形成します。サンプラーを使用するたびに、その使用に対応する統計情報が別個に保存されます。

インターフェイスですでにイネーブルになっているフローモニタにサンプラーを追加することはできません。まず、そのフローモニタをインターフェイスから削除してから、同じフローモニタをサンプラーとともに追加する必要があります。

（注） 想定される使用状況を得るには、各フローの統計情報をスケールする必要があります。たとえば、100 パケットにつき 1 パケットをサンプリングするサンプラーを使用した場合は、パケットカウンタとバイトカウンタを 100 倍する必要があります。

次に、入力トラフィックのモニタリングのためにフローモニタをイネーブルにする例を示します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
```

次に、サンプラーによってサンプリングされる入力パケット数を制限した状態で、入力トラフィックをモニタするようにフローモニタをイネーブルにする例を示します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

次の例では、サンプラーなしでインターフェイスでイネーブルになっているフローモニタにサンプラーを追加する場合の動作を示します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

次の例では、フローモニタをサンプラーと一緒にイネーブルにできるようにするために、インターフェイスからいったん削除する方法を示します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# no ipv6 flow monitor FLOW-MONITOR-1 input
デバイス(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

match datalink ethertype

パケットの EtherType 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 datalink ethertype** コマンドを使用します。パケットの EtherType 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 datalink ethertype
no match datalink ethertype

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

パケットの EtherType はキー 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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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。

match datalink ethertype コマンドを使用して、パケットの EtherType をフロー レコードのキーフィールドとして設定すると、トラフィック フローは、インターフェイスに割り当てられたフロー モニタのタイプに基づいて作成されます。

- **datalink flow monitor** 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、データリンクフローモニタがインターフェイスに割り当てられると、異なるレイヤ2プロトコルに対して一意のフローが作成されます。
- **ip flow monitor** 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、IP フローモニタがインターフェイスに割り当てられると、異なる IPv4 プロトコルに対して一意のフローが作成されます。
- **ipv6 flow monitor** 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、IPv6 フローモニタがインターフェイスに割り当てられると、異なる IPv6 プロトコルに対して一意のフローが作成されます。

このコマンドをデフォルト設定に戻すには、**no match datalink ethertype** または **default match datalink ethertype** 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、パケットの EtherType を フロー レコードのキー フィールドとして設定しています。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match datalink ethertype
```

match datalink mac

フローレコードのキーフィールドとして MAC アドレス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 datalink mac** 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 MAC 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 datalink mac {destination address input | source address input}
no match datalink mac {destination address input | source address input}

構文の説明

destination address	キーフィールドとして宛先MACアドレスを使用するように設定します。
input	入力パケットの MAC アドレスを指定します。
source address	キーフィールドとして送信元MACアドレスを使用するように設定します。

コマンド デフォルト

MAC 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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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。

input キーワードを使用して、**match datalink mac** コマンドで使用する観測ポイントを指定し、ネットワークトラフィックの一意の MAC アドレスに基づいてフローを作成します。

（注） データリンク フロー モニタがインターフェイスまたは VLAN レコードに割り当てられている場合、非 IPv6 または非 IPv4 トラフィック用のフローだけが作成されます。

このコマンドをデフォルト設定に戻すには、**no match datalink mac** または **default match datalink mac** 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、フローレコードのキーフィールドとして、deviceによって受信されるパケットの宛先 MAC アドレスを使用するように設定します。

```
デバイス(config)# flow record FLOW-RECORD-1
デバイス(config-flow-record)# match datalink mac destination address input
```

match datalink vlan

VLAN ID 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 datalink vlan** コマンドを使用します。VLAN ID 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 datalink vlan input
no match datalink vlan input

構文の説明

input	deviceが受信しているトラフィックの VLAN ID 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

VLAN ID 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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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。

input キーワードは **match datalink vlan** コマンドがネットワークトラフィックに固有の VLAN ID に基づいてフローを作成するための観測点を指定するために使用されます。

次に、deviceが受信しているトラフィックの VLAN ID をフロー レコードのキー 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 datalink vlan input
```

match flow cts

フローレコードの CTS 送信元グループタグおよび宛先グループタグを設定するには、フローレコード コンフィギュレーション モードで **match flow cts** コマンドを使用します。グループタグ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 flow cts {**source** | **destination**} **group-tag**
no match flow cts {**source** | **destination**} **group-tag**

構文の説明

cts destination group-tag	CTS 宛先フィールド グループをキー フィールドとして設定します。
cts source group-tag	CTS 送信元フィールド グループをキー フィールドとして設定します。

コマンド デフォルト

CTS 宛先または送信元フィールド グループ、フロー方向およびフロー サンプラー ID 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

Flexible NetFlow フロー レコード コンフィギュレーション（config-flow-record）

ポリシー インライン コンフィギュレーション（config-if-policy-inline）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.7.3E	このコマンドが導入されました。
Cisco IOS XE Denali 16.2.1	このコマンドが再度導入されました。このコマンドは以下でサポートされていません：Cisco IOS XE Denali 16.1.x

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、送信元グループ タグをキー 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 flow cts source group-tag
```

match flow direction

フロー方向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 flow direction** コマンドを使用します。フロー方向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 flow direction
no match flow direction

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

フロー方向はキー 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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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。

match flow direction コマンドは、フローの方向をキーフィールドとしてキャプチャします。この機能は、入力フローと出力フローに対して単一のフローモニタが設定されている場合に最も役立ちます。また、入力と出力で 1 回ずつ、2 回モニタされているフローを見つけ、除外するために使用することができます。このコマンドは、2 つのフローが反対方向に流れている場合に、エクスポートされたデータ内のフローのペアを一致させるために役立つ場合もあります。

次に、フローがモニタされた方向をキー 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 flow direction
```

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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 （438 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 （439 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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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 （441 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 （442 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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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 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 3.3SE	このコマンドが導入されました。

使用上のガイドライン 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 3.3SE	このコマンドが導入されました。

使用上のガイドライン 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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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
```

mode random 1 out-of

ランダムサンプリングを有効にし、サンプラーのパケット間隔を指定するには、サンプラーコンフィギュレーション モードで **mode random 1 out-of** コマンドを使用します。サンプラーのパケット間隔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。

mode random 1 out-of *window-size*
no mode

構文の説明

window-size	パケットを選択するウィンドウサイズを指定します。指定できる範囲は2～1024です。

コマンド デフォルト

サンプラーのモードとパケット間隔は設定されていません。

コマンド モード

サンプラー コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

では、計4つの固有のサンプラーがサポートされています。パケットは、トラフィック パターンのバイアスを除外し、モニタリングを回避するためのユーザによる試行を無効にする方法で選択されます。

（注） **deterministic** キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

例

次の例では、ウィンドウ サイズ1000でランダム サンプリングをイネーブルにします。

```
デバイス(config)# sampler SAMPLER-1
デバイス(config-sampler)# mode random 1 out-of 1000
```

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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
```

record

フローモニタのフローレコードを追加するには、フロー モニタ コンフィギュレーション モードで **record** コマンドを使用します。 フローモニタのフローレコードを削除するには、このコマンドの **no** 形式を使用します。

record *record-name*
no record

構文の説明

record-name	事前に設定したユーザ定義のフロー レコードの名前。

コマンド デフォルト

フロー レコードは設定されていません。

コマンド モード

フロー モニタ コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

フロー モニタごとに、キャッシュ エントリの内容およびレイアウトを定義するレコードが必要です。フロー モニタがさまざまな事前定義済みレコード フォーマットの 1 つを使用することも、上級ユーザが独自のレコード フォーマットを作成することもできます。

（注） フローモニタで **record** コマンドのパラメータを変更する前に、**no ip flow monitor** コマンドを使用して、すべてのインターフェイスから適用済みのフローモニタを削除する必要があります。

例

次の例では、FLOW-RECORD-1 を使用するようにフロー モニタを設定します。

```
デバイス(config)# flow monitor FLOW-MONITOR-1
デバイス(config-flow-monitor)# record FLOW-RECORD-1
```

sampler

フローサンプラーを作成するか、または既存の フローサンプラーを変更し、サンプラー 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 **sampler** コマンドを使用します。サンプラーを削除するには、このコマンドの **no** 形式を使用します。

sampler *sampler-name*
no sampler *sampler-name*

構文の説明

sampler-name	作成または変更するフローサンプラーの名前。

コマンド デフォルト

フローサンプラーは設定されません。

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
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

フローサンプラーは分析されるパケット数を制限することで、トラフィックをモニタするために によってネットワークデバイスで生じる負荷を軽減するために使用されます。 パケットの範囲から1パケットの割合でサンプリング レートを設定します。フローサンプラーは、サンプリングされた を実装するためにフローモニタとともにインターフェイスに適用されます。

フロー サンプリングをイネーブルにするには、トラフィック分析に使用して、フロー モニタに割り当てるレコードを設定します。インターフェイスにサンプラーを含むフローモニタを適用すると、サンプリングされたパケットはサンプラーによって指定されたレートで分析され、フローモニタに対応するフロー レコードと比較されます。分析されるパケットがフロー レコードによって指定された条件を満たす場合、フロー モニタ キャッシュに追加されます。

例

次に、フロー サンプラーの名前 SAMPLER-1 を作成する例を示します。

```
デバイス(config)# sampler SAMPLER-1
デバイス(config-sampler)#
```

show flow exporter

フロー エクスポータのステータスと統計情報を表示するには、特権 EXEC モードで **show flow exporter** コマンドを使用します。

show flow exporter [{**export-ids netflow-v9** | [**name**] *exporter-name* [{**statistics** | **templates**}] | **statistics** | **templates**}]

構文の説明

export-ids netflow-v9	（任意）エクスポート可能なNetFlowバージョン9エクスポートフィールドとその ID を表示します。
name	（任意）フローエクスポータの名前を指定します。
exporter-name	（任意）以前に設定されたフローエクスポータの名前。
statistics	（任意）すべてのフローエクスポータまたは指定されたフローエクスポータの統計情報を表示します。
templates	（任意）すべてのフローエクスポータまたは指定されたフローエクスポータのテンプレート情報を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

次に、device で設定されているすべてのフロー エクスポータのステータスと統計情報を表示する例を示します。

```
デバイス# show flow exporter
Flow Exporter FLOW-EXPORTER-1:
  Description:              Exports to the datacenter
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 192.168.0.1
    Source IP address:      192.168.0.2
    Transport Protocol:     UDP
    Destination Port:       9995
    Source Port:            55864
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
```

次の表で、この出力に表示される重要なフィールドについて説明します。

表 *32 : show flow exporter* のフィールドの説明

フィールド	説明
Flow Exporter	設定したフロー エクスポータの名前。
Description	エクスポータに設定した説明、またはユーザ定義のデフォルトの説明。
Transport Configuration	このエクスポータのトランスポート設定フィールド。

フィールド	説明
Destination IP address	宛先ホストの IP アドレス。
Source IP address	エクスポートされたパケットで使用される送信元 IP アドレス。
Transport Protocol	エクスポートされたパケットで使用されるトランスポート層プロトコル。
Destination Port	エクスポートされたパケットが送信される宛先 UDP ポート。
Source Port	エクスポートされたパケットが送信される送信元 UDP ポート。
DSCP	Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値。
TTL	存続可能時間値。
Output Features	**output-features** コマンドが使用されたかどうかを指定します。このコマンドが使用されると、Flexible NetFlow エクスポート パケット上で出力機能が実行されます。

次に、device で設定されているすべてのフロー エクスポータのステータスと統計情報を表示する例を示します。

```
デバイス# show flow exporter name FLOW-EXPORTER-1 statistics
Flow Exporter FLOW-EXPORTER-1:
  Packet send statistics (last cleared 2w6d ago):
    Successfully sent:         0                     (0 bytes)
```

show flow interface

インターフェイスの 設定およびステータスを表示するには、特権 EXEC モードで **show flow interface** コマンドを使用します。

show flow interface [*type number*]

構文の説明

type	（任意）アカウンティング設定情報を表示するインターフェイスのタイプ。
number	（任意） アカウンティング設定情報を表示するインターフェイスの番号。

コマンド モード

特権 EXEC

コマンド履歴

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

例

次に、イーサネット インターフェイス 0/0 と 0/1 の アカウンティング設定を表示する例を示します。

```
デバイス# show flow interface gigabitethernet1/0/1

Interface Ethernet1/0
        monitor:         FLOW-MONITOR-1
        direction:       Output
        traffic(ip):     on
デバイス# show flow interface gigabitethernet1/0/2
Interface Ethernet0/0
        monitor:         FLOW-MONITOR-1
        direction:       Input
        traffic(ip):     sampler SAMPLER-2#
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *33 : show flow interface* のフィールドの説明

フィールド	説明
Interface	情報が適用されるインターフェイス。
monitor	インターフェイス上に設定されているフローモニタの名前。
direction:	フローモニタによってモニタされているトラフィックの方向。 次の値が可能です。 • Input：インターフェイスが受信しているトラフィック。 • Output：インターフェイスが送信しているトラフィック。
traffic(ip)	フローモニタが通常モードとサンプラーモードのどちらであるかを示します。 次の値が可能です。 • on：通常モード。 • sampler：サンプラー モード（サンプラーの名前も表示されます）。

show flow monitor

フローモニタのステータスと統計情報を表示するには、特権 EXEC モードで **show flow monitor** コマンドを使用します。

構文の説明

name	（任意）フロー モニタの名前を指定します。
monitor-name	（任意）事前に設定されたフロー モニタの名前。
cache	（任意）フロー モニタのキャッシュの内容を表示します。
format	（任意）ディスプレイ出力のフォーマット オプションのいずれかを使用することを指定します。
csv	（任意）フローモニタのキャッシュの内容をカンマ区切り値（CSV）形式で表示します。
record	（任意）フロー モニタのキャッシュの内容をレコード形式で表示します。
table	（任意）フロー モニタのキャッシュの内容を表形式で表示します。
statistics	（任意）フロー モニタの統計情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

cache キーワードでは、デフォルトでレコード形式が使用されます。

show flowmonitor *monitor-name* **cache** コマンドのディスプレイ出力に含まれる大文字のフィールド名は、フローの識別に が使用するキー フィールドです。**show flow monitor** *monitor-name* **cache** コマンドのディスプレイ出力に含まれる小文字のフィールド名は、 がキャッシュの追加データとして値を収集する非キー フィールドです。

例

次の例では、フロー モニタのステータスを表示します。

```
デバイス# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic traffic analysis
  Flow Record:       flow-record-1
  Flow Exporter:     flow-exporter-1
                     flow-exporter-2
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 311316 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *34 : show flow monitor monitor-name* フィールドの説明

フィールド	説明
Flow Monitor	設定したフロー モニタの名前。
Description	モニタに設定した説明、またはユーザ定義のデフォルトの説明。
Flow Record	フロー モニタに割り当てられたフロー レコード。
Flow Exporter	フロー モニタに割り当てられたエクスポータ。
Cache	フロー モニタのキャッシュに関する情報。
Type	フロー モニタのキャッシュ タイプ。この値は常に normal となります。これが唯一サポートされているキャッシュ タイプです。
Status	フロー モニタのキャッシュのステータス。 次の値が可能です。 • allocated：キャッシュが割り当てられています。 • being deleted：キャッシュが削除されています。 • not allocated：キャッシュが割り当てられていません。
Size	現在のキャッシュ サイズ。
Inactive Timeout	非アクティブ タイムアウトの現在の値（秒単位）。
Active Timeout	アクティブ タイムアウトの現在の値（秒単位）。

次の例では、FLOW-MONITOR-1 という名前のフロー モニタのステータス、統計情報、およびデータを表示します。

次の表で、この出力に表示される重要なフィールドを説明します。

次の例では、FLOW-MONITOR-1 という名前のフロー モニタのステータス、統計情報、およびデータを表形式で表示します。

次の例では、FLOW-MONITOR-IPv6 という名前のフロー モニタ（キャッシュに IPv6 データを格納）のステータス、統計情報、およびデータをレコード形式で表示します。

次の例では、フロー モニタのステータスと統計情報を表示します。

show flow record

フロー レコードのステータスと統計情報を表示するには、特権 EXEC モードで **show flow record** コマンドを使用します。

show flow record [{[**name**] *record-name*}]

構文の説明

name	（任意）フロー レコードの名前を指定します。
record-name	（任意）前に設定されたユーザ定義のフロー レコードの名前。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

次に、FLOW-RECORD-1 のステータスおよび統計情報を表示する例を示します。

```
デバイス# show flow record FLOW-RECORD-1
flow record FLOW-RECORD-1:
  Description:        User defined
  No. of users:       0
  Total field space:  24 bytes
  Fields:
    match ipv6 destination address
    match transport source-port
    collect interface input
```

show sampler

サンプラーのステータスと統計情報を表示するには、特権 EXEC モードで **show sampler** コマンドを使用します。

show sampler [{[**name**] *sampler-name*}]

構文の説明

name	（任意）サンプラーの名前を指定します。
sampler-name	（任意）前に設定されたサンプラーの名前。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

次に、設定されたフロー サンプラーすべてのステータスと統計情報を表示する例を示します。

```
デバイス# show sampler
Sampler SAMPLER-1:
  ID:             2083940135
  export ID:      0
  Description:    User defined
  Type:           Invalid (not in use)
  Rate:           1 out of 32
  Samples:        0
  Requests:       0
  Users (0):

Sampler SAMPLER-2:
  ID:             3800923489
  export ID:      1
  Description:    User defined
  Type:           random
  Rate:           1 out of 100
  Samples:        1
  Requests:       124
  Users (1):
    flow monitor FLOW-MONITOR-1 (datalink,vlan1)  0 out of 0
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *35 : show sampler* のフィールドの説明

フィールド	説明
ID	フロー サンプラーの ID 番号。
Export ID	フロー サンプラーのエクスポートの ID。
Description	フローサンプラーに設定した説明、またはユーザ定義のデフォルトの説明。
Type	フロー サンプラーに設定したサンプリング モード。
Rate	フローサンプラーに設定したウィンドウ サイズ（パケットの選択用）。指定できる範囲は 2 ～ 32768 です。
Samples	フローサンプラーを設定してから、または device を再起動してからサンプリングされたパケットの数。この数は、トラフィックのサンプリングが必要かどうかを決定するためにサンプラーが呼び出されたときに肯定応答を受信した回数と同じです。この表の Requests フィールドの説明を参照してください。

フィールド	説明
Requests	トラフィックのサンプリングが必要かどうかを決定するためにサンプラーが呼び出された回数。
Users	フロー サンプラーが設定されるインターフェイス。

source

フローエクスポータから送信されるすべてのパケットの送信元 IP アドレスのインターフェイスを設定するには、フロー エクスポータ コンフィギュレーション モードで **source** コマンドを使用します。 フローエクスポータから送信されるすべてのパケットの送信元 IP アドレスの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-type interface-number*
no source

構文の説明

interface-type	フローエクスポータから送信されるパケットの送信元 IP アドレス向けに使用する IP アドレスのインターフェイスのタイプ。
interface-number	フローエクスポータから送信されるパケットの送信元 IP アドレス向けに使用する IP アドレスのインターフェイス番号。

コマンド デフォルト

データグラムを送信するインターフェイスの IP アドレスが、送信元 IP アドレスとして使用されます。

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

が送信するデータグラムに一貫した送信元 IP アドレスを使用することの利点として、以下が含まれます。

- によりエクスポートされるデータグラムの送信元 IP アドレスは、データがどちらの device から到着するかを判断するために、宛先システムによって使用されます。device から宛先システムに データグラムを送信するのに使用できるパスがネットワークに複数あり、送信元 IP アドレスを取得する送信元インターフェイスが指定されていない場合、device はデータグラムが送信されるインターフェイスの IP アドレスを、データグラムの送信元 IP アドレスとして使用します。この場合、宛先システムは同じ device から送信元 IP アドレスが異なる データグラムを受信する場合があります。宛先システムが、異なる送信元 IP

アドレスを持つ同じdeviceから データグラムを受信すると、宛先システムは異なるdevices から送信されたものとして データグラムを処理します。宛先システムが データグラムを異なる devices から送信されたものとして処理しないようにするには、宛先システムが device ですべての可能な送信元 IP アドレスから受信する データグラムを単一の フローに集約するように、宛先システムを設定する必要があります。

- データグラムを宛先システムに送信するために使用できる複数のインターフェイスがdevice にあり、**source** コマンドを設定していない場合、トラフィックを許可するために作成するアクセスリストに、各インターフェイスの IP アドレスのエントリを追加する必要があります。既知の送信元からの トラフィックを許可し、不明な送信元からはブロックするためにアクセスリストを作成および維持することは、 トラフィックをエクスポートする device ごとに単一の IP アドレスに データグラムの送信元 IP アドレスを制限すると、より簡単に行えるようになります。

注意 **source** インターフェイスとして設定するインターフェイスには、設定された IP アドレスが必須であり、アップされている必要があります。

ヒント **source** コマンドで設定したインターフェイス上で一時的な停止が発生した場合、 エクスポータは、データグラムが送信されるインターフェイスの IP アドレスをデータグラムの送信元 IP アドレスとして使用するデフォルトの動作に戻ります。この問題を回避するには、*ループバック インターフェイス*を送信元インターフェイスとして使用します。これは、*ループバック インターフェイス*が物理インターフェイスで発生する可能性のある一時的な停止の影響を受けないためです。

このコマンドをデフォルト設定に戻すには、**no source** または **default source** 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。

例

次に、NetFlow トラフィックの送信元インターフェイスとして、*ループバック インターフェイス*を使用するように を設定する例を示します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)# source loopback 0
```

template data timeout

フローエクスポータ テンプレートデータの再送信のタイムアウト期間を指定するには、フローエクスポータ コンフィギュレーション モードで **template data timeout** コマンドを使用します。フローエクスポータの再送信のタイムアウトを削除するには、このコマンドの **no** 形式を使用します。

template data timeout *seconds*

no template data timeout *seconds*

構文の説明

seconds	秒単位のタイムアウト値です。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

デフォルトのフロー エクスポータ テンプレート再送信のタイムアウトは、600秒です。

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

フロー エクスポータのテンプレート データには、エクスポートされるデータ レコードが記述されています。対応するテンプレートなしでデータ レコードをデコードすることはできません。**template data timeout** コマンドを使用して、これらのテンプレートをエクスポートする頻度を制御します。

このコマンドをデフォルト設定に戻すには、**no template data timeout** または **default template data timeout** フロー レコード エクスポータ コマンドを使用します。

次の例では、1000秒というタイムアウトに基づいてテンプレートの再送信を設定します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)# template data timeout 1000
```

transport

のフロー エクスポータのトランスポート プロトコルを設定するには、フロー エクスポータ コンフィギュレーション モードで **transport** コマンドを使用します。フロー エクスポータのトランスポート プロトコルを削除するには、このコマンドの **no** 形式を使用します。

transport udp *udp-port*
no transport udp *udp-port*

構文の説明

udp *udp-port*	トランスポート プロトコルとして User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を指定し、UDP ポート番号を指定します。

コマンド デフォルト

フロー エクスポータでは、UDP をポート 9995 で使用します。

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドをデフォルト設定に戻すには、**no transport** または **default transport flow exporter** コンフィギュレーション コマンドを使用します。

次に、トランスポート プロトコルとして UDP を設定し、UDP ポート番号を 250 に設定する例を示します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)# transport udp 250
```

ttl

存続可能時間（TTL）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 **ttl** コマンドを使用します。TTL 値を削除するには、このコマンドの **no** 形式を使用します。

ttl *ttl*
no ttl *ttl*

構文の説明

ttl	エクスポートされたデータグラムの存続可能時間（TTL）値。指定できる範囲は 1 ～ 255 です。デフォルトは 255 です。

コマンド デフォルト

フロー エクスポータでは TTL 値 255 が使用されています。

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

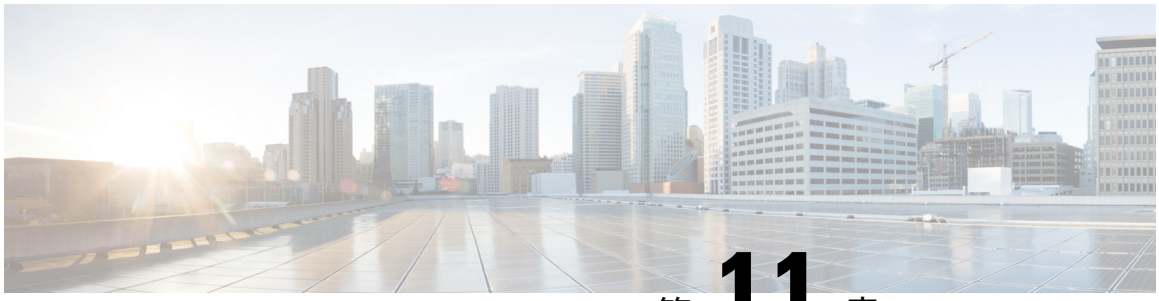
リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドをデフォルト設定に戻すには、**no ttl** または **default ttl** 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。

次に、TTL 値 15 を指定する例を示します。

```
デバイス(config)# flow exporter FLOW-EXPORTER-1
デバイス(config-flow-exporter)# ttl 15
```



第 11 章

ネットワーク管理

debug event manager auto-deploy

Embedded Event Manager（EEM）自動展開ポリシーのデバッグをイネーブルにするには、特権 EXEC モードで **debug event manager auto-deploy** コマンドを使用します。デバッグメッセージをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug event manager auto-deploy {**common** | **parser** | **schedule**}
no debug event manager auto-deploy {**common** | **parser** | **schedule**}

構文の説明

common	EEM 自動展開のインフラストラクチャ関連のデバッグのロギングをイネーブルにします。
parser	マニフェストファイル解析デバッグのロギングをイネーブルにします。
schedule	EEM ポリシー プロビジョニング デバッグのロギングをイネーブルにします。

コマンド デフォルト

デバッグはイネーブルになりません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

例

次に、スケジュール ログをイネーブルにする例を示します。

```
Device# debug event manager auto-deploy schedule

*Jul 26 16:45:22.731 IST: [fadpa]
*Jul 26 16:45:22.731 IST: [fadec]
*Jul 26 16:45:22.733 IST: fadpa: CLI execution is done
*Jul 26 16:45:22.733 IST:
*Jul 26 16:45:22.733 IST: Provisioned ENV A.ENV policy

*Jul 26 16:45:22.734 IST: [fadpl]
*Jul 26 16:45:22.734 IST: [fadv]
*Jul 26 16:45:22.734 IST: Successfully provisioned env vars
```

```
*Jul 26 16:45:22.734 IST: [fadpl]
*Jul 26 16:45:22.734 IST: [fadv]
*Jul 26 16:45:22.734 IST: [fadpfp]
*Jul 26 16:45:22.735 IST: [fadfxr]
*Jul 26 16:45:22.735 IST: [fadft]
*Jul 26 16:45:22.790 IST:
*Jul 26 16:45:22.790 IST: Downloaded APP policy
```

関連コマンド

コマンド	説明
event manager auto-deploy	EEM 自動展開プロファイルを設定します。

default

ポリシープロビジョニング コマンドをデフォルト状態に設定するには、自動展開コンフィギュレーション モードで default コマンドを使用します。

default {**enable** | **exit** | **log-url** | **manifest format xml url** | **retry count** *retry-count* **interval** *interval-duration* | **schedule start-in hours** *hours* **minutes** *minutes* {**oneshot** | **recurring** {**days** *days* | **hours** *hours* }} | **window** *minutes*}

構文の説明

enable	プロファイルを有効にします。
exit	自動展開コンフィギュレーション モードを終了します。
log-url	ポリシー プロビジョニングのログ ファイルを保存する場所を設定します。
manifest format xml url	マニフェストファイルの形式とマニフェスト ファイルをダウンロードする場所を設定します。
retry count *retry-count* **interval** *interval-duration*	ファイル転送が成功しない場合のファイル転送の再試行回数を設定します。
schedule start-in hours *hours* **minutes** *minutes*	指定時間後のポリシー プロビジョニングをスケジュールします。
oneshot	ポリシープロビジョニングをスケジュールします。
recurring days *days* **hours** *hours*	指定時間内に繰り返し実行されるポリシー プロビジョニングをスケジュールします。

window *minutes*	プロファイル プロビジョニングがトリガーされるランダム時間を設定します。ウィンドウ期間はスケジュールされた開始時間に追加され、ポリシープロビジョニングはスケジュールされた開始時間と設定されたウィンドウ期間の間の任意の時間に実行されます。

コマンド デフォルト　自動展開コマンドは有効になっていません。

コマンド モード　自動展開コンフィギュレーション モード（config-auto-deploy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

例

次に、コマンドをデフォルトに設定する例を示します。

```
Device(config)# event manager auto-deploy name deploy1
Device(auto-deploy)# default retry count 2 interval 3
```

関連コマンド

コマンド	説明
event-manager auto-deploy	EEM 自動展開プロファイルを設定します。

description（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元セッションを説明するには、ERSPAN モニタ送信元セッション コンフィギュレーション モードで **description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

description 説明
no description

構文の説明

description	このセッションのプロパティについて説明します。

コマンド デフォルト　説明は設定されていません。

コマンド モード　ERSPAN モニタ送信元セッション コンフィギュレーション モード（config-mon-erspan-src）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

description 引数は 240 文字以内で指定します。

例

次に、ERSPAN 送信元セッションを説明する例を示します。

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# description source1
```

関連コマンド

コマンド	説明
monitor session type erspan-source	ローカルのERSPAN送信元セッションを設定します。

destination（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元セッションの宛先を設定するには、ERSPAN モニタ送信元セッション コンフィギュレーション モードで **destination** コマンドを使用します。宛先セッションを削除するには、このコマンドの **no** 形式を使用します。

destination
no destination

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

送信元セッションの宛先は設定されていません。

コマンド モード

ERSPAN モニタ送信元セッション コンフィギュレーション モード（config-mon-erspan-src）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

ERSPAN トラフィックは、GRE カプセル化された SPAN トラフィックで、ERSPAN 宛先セッションによってだけ処理されます。

すべての ERSPAN 送信元セッション（最大 8）の宛先 IP アドレスが同一である必要はありません。ERSPAN 宛先セッションに IP アドレスを設定するには、**ip address** コマンドを入力します。

ERSPAN 送信元セッションの宛先 IP アドレスが（宛先スイッチ上のインターフェイスで設定される）、ERSPAN 宛先セッションが宛先ポートに送信するトラフィックの送信元です。**ip**

address コマンドを使用して、送信元セッションおよび宛先セッションの両方に同一のアドレスを設定します。

例

次に、ERSPAN 送信元セッションの宛先を設定し、ERSPAN モニタ宛先セッション コンフィギュレーション モードを開始して、宛先プロパティを指定する例を示します。

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)#ip address 10.1.1.1
Switch(config-mon-erspan-src-dst)#
```

次の **show monitor session all** の出力例には、送信元セッションの宛先の異なる IP アドレスが示されています。

```
Switch# show monitor session all

Session 1
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session1
Destination IP Address : 10.1.1.1


Session 2
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session2
Destination IP Address : 192.0.2.1


Session 3
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session3
Destination IP Address : 198.51.100.1

Session 4
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session4
Destination IP Address : 203.0.113.1


Session 5
---------
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session5
Destination IP Address : 209.165.200.225
```

関連コマンド

コマンド	説明
erspan-id	ERSPAN トラフィックを識別するため、宛先セッションで使用される ID を設定します。
ip ttl	ERSPAN トラフィックのパケットの TTL 値を設定します。
monitor session type erspan-source	ローカルの ERSPAN 送信元セッションを設定します。
origin	ERSPAN トラフィックの送信元として使用される IP アドレスを設定します。

enable

Embedded Event Manager（EEM; 組み込みイベントマネージャ）プロファイルを有効にするには、自動展開コンフィギュレーション モードで **enable** コマンドを使用します。EEM 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。

enable
no enable

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

EEM プロファイルは有効になっていません。

コマンド モード

自動展開コンフィギュレーション（config-auto-deploy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

設定済みのプロファイルを有効にしないかぎり、そのプロファイルはアクティブにならず、ポリシー プロビジョニングが開始されません。

例

次に、EEM プロファイルを有効にする例を示します。

```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# enable
```

関連コマンド

コマンド	説明
event-manager auto-deploy	EEM 自動展開プロファイルを設定します。

erspan-id

Encapsulated Remote Switched Port Analyzer（ERSPAN）トラフィックを識別するために宛先セッションが使用する ID を設定するには、ERSPAN モニタ宛先セッション コンフィギュレーション モードで **erspan-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。

erspan-id *erspan-ID*
no erspan-id *erspan-ID*

構文の説明

erspan-id	宛先セッションが使用する ERSPAN ID。有効値は 1 ～ 1023 です。

コマンド デフォルト

宛先セッションの ERSPAN ID は設定されていません。

コマンド モード

ERSPAN モニタ宛先セッション コンフィギュレーションモード（config-mon-erspan-src-dst）

コマンド履歴

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

例

次に、宛先セッションの ERSPAN ID を設定する例を示します。

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# erspan-id 3
```

関連コマンド

コマンド	説明
destination	ERSPAN 宛先セッションを設定し、宛先プロパティを指定します。
monitor session type erspan-source	ローカルの ERSPAN 送信元セッションを設定します。

event manager auto-deploy

Embedded Event Manager（EEM; 組み込みイベントマネージャ）の自動展開プロファイルを設定するには、グローバル コンフィギュレーション モードで **event manager auto-deploy** 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。

event manager auto-deploy name *profile-name*
no event manager auto-deploy name *profile-name*

構文の説明		
	name *profile-name*	自動展開プロファイルの名前を指定します。

コマンド デフォルト デフォルト プロファイル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 Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン このコマンドを設定すると、モードが自動展開コンフィギュレーションモードになります。自動展開コンフィギュレーション設定は、このモードで設定できます。どの時点でも複数のプロファイルを有効することはできません。

例

次に、EEM プロファイルの自動展開を設定する例を示します。

```
Device(config)# event manager auto-deploy name deploy1
```

関連コマンド	コマンド	説明
	show event-manager auto-deploy summary	自動展開プロファイルに関する情報を表示します。

event manager auto-deploy start

Embedded Event Manager（EEM; 組み込みイベントマネージャ）の自動展開を即座にトリガーしてポリシーの処理を開始するには、特権 EXEC モードで **event manager auto-deploy start** コマンドを使用します。

event manager auto-deploy start name *profile-name* {**now** | **window** *duration*}

構文の説明		
	name *profile-name*	自動展開プロファイルの名前を指定します。
	now	EEM 自動展開をすぐに開始するように指定します。
	window *duration*	指定されたウィンドウ期間のランダム時間に EEM 自動展開を開始するように指定します。*duration* 引数の有効値は 5 ー 30 分です。

コマンド デフォルト　EEM 自動展開は有効になっていません。

コマンド モード　特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

例

次に、ポリシー処理をすぐに開始する例を示します。

```
Device# event manager auto-deploy start name deploy1 now
```

次に、指定されたウィンドウ期間内の任意の時間にポリシー処理を開始する例を示します。

```
Device# event manager auto-deploy start name deploy1 window 20
```

filter（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元がトランクポートの場合に、ERSPAN 送信元 VLAN フィルタリングを設定するには、ERSPAN モニタ送信元セッション コンフィギュレーション モードで **filter** 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。

filter {**ip access-group** {*standard-access-list extended-access-list acl-name*} | **ipv6 access-group** *acl-name* | **mac access-group** *acl-name* | **sgt** *sgt-id* [{**,**}] [{**-**}] | **vlan** *vlan-id*[{**,**}] [{**-**}]}
no filter {**ip** [{**access-group** | [{*standard-access-list extended-access-list acl-name*}]}] | **ipv6** [{**access-group**}] | **mac** [{**access-group**}] | **sgt** *sgt-id* [{**,**}] [{**-**}] | **vlan** *vlan-id*[{**,**}] [{**-**}]}

構文の説明

ip	IP アクセス制御ルールを指定します。
access-group	アクセス制御グループを指定します。
standard-access-list	標準 IP アクセスリスト。
extended-access-list	拡張 IP アクセスリスト。
acl-name	アクセスリスト名。
ipv6	IPv6 アクセス制御ルールを指定します。
mac	Media Access Control（MAC）ルールを指定します。
sgt *sgt-ID*	セキュリティグループタグ（SGT）を指定します。有効値は 1 ～ 65535 です。

vlan *vlan-ID*	ERSPAN 送信元 VLAN を指定します。有効な値は 1 ～ 4094 です。
,	（任意）別の VLAN を指定します。
-	（任意）VLAN の範囲を指定します。

コマンド デフォルト

送信元 VLAN フィルタリングは設定されていません。

コマンド モード

ERSPAN モニタ送信元セッション コンフィギュレーション モード（config-mon-erspan-src）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.11.1	**sgt** キーワードが導入されました。

使用上のガイドライン

送信元 VLAN とフィルタ VLAN を同じセッションに含めることはできません。

モニタされたトランクインターフェイス上で **filter** コマンドを設定した場合、指定された VLAN セット上のトラフィックだけがモニタされます。

例

次に、送信元 VLAN フィルタリングを設定する例を示します。

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# filter vlan 3
```

関連コマンド

コマンド	説明
monitor session type erspan-source	ローカルの ERSPAN 送信元セッションを設定します。

header-type

カプセル化の ERSPAN ヘッダータイプを設定するには、ERSPAN モニタ送信元セッション コンフィギュレーション モードで **header-type** 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。

header-type *header-type*
no header-type *header-type*

構文の説明

header-type	ERSPAN ヘッダータイプ。有効なヘッダータイプは 2 および 3 です。

コマンド デフォルト

ERSPAN ヘッダータイプは 2 に設定されています。

コマンド モード

ERSPAN モニタ送信元セッション コンフィギュレーション モード（config-mon-erspan-src）

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、ERSPAN ヘッダータイプを 3 に変更する例を示します。

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# header-type 3
```

関連コマンド

コマンド	説明
monitor session type	ローカルのERSPAN送信元または宛先セッションを設定します。

ip dscp（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）トラフィックの DiffServ コードポイント（DSCP）値を設定するには、ERSPAN モニタ宛先セッション コンフィギュレーション モードで **ip dscp** コマンドを使用します。DSCP 値を削除するには、このコマンドの **no** 形式を使用します。

ip dscp *dscp-value*
no ip dscp *dscp-value*

構文の説明

dscp-value	DSCP 値。有効な値は 0 ～ 63 です。

コマンド デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

ERSPAN モニタ宛先セッション コンフィギュレーションモード（config-mon-erspan-src-dst）

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、ERSPAN トラフィックの DSCP 値を設定する例を示します。

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# ip dscp 15
```

関連コマンド

コマンド	説明
destination	ERSPAN宛先セッションを設定し、宛先プロパティを指定します。

コマンド	説明
monitor session type	ローカルの ERSPAN 送信元または宛先セッションを設定します。

ip ttl（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）トラフィックのパケットの存続可能時間（TTL）を設定するには、ERSPAN モニタ宛先セッション コンフィギュレーション モードで **ip ttl** コマンドを使用します。TTL 値を削除するには、このコマンドの **no** 形式を使用します。

ip ttl *ttl-value*
no ip ttl *ttl-value*

構文の説明

ttl-value	TTL の値。有効値は 2 ～ 255 です。

コマンド デフォルト

TTL 値は 255 として設定されます。

コマンド モード

ERSPAN モニタ宛先セッション コンフィギュレーションモード（config-mon-erspan-src-dst）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

例

次に、ERSPAN トラフィックの TTL 値を設定する例を示します。

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# ip ttl 32
```

関連コマンド

コマンド	説明
destination	ERSPAN 宛先セッションを設定し、宛先プロパティを指定します。
monitor session type erspan-source	ローカルの ERSPAN 送信元セッションを設定します。

ip wccp

Web キャッシュサービスをイネーブルにし、アプリケーションエンジンで定義されたダイナミックサービスに対応するサービス番号を指定するには、device で **ip wccp** グローバル コン

フィギュレーション コマンドを使用します。サービスを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 wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]
no ip wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]

構文の説明

web-cache	Web キャッシュ サービスを指定します（WCCP バージョン 1 とバージョン 2）。
service-number	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ～ 254 の範囲で指定できます。サービスの最大数（**web-cache** キーワードで指定する Web キャッシュサービスを含む）は 256 です。
group-address *groupaddress*	（任意）サービス グループに参加するために devices およびアプリケーション エンジンが使用するマルチキャスト グループ アドレスを指定します。
group-list *access-list*	（任意）マルチキャスト グループ アドレスが使用されない場合、サービス グループに加入しているアプリケーション エンジンに対応する有効な IP アドレスのリストを指定します。
redirect-list *access-list*	（任意）ホストから特定のホストまたは特定のパケットのリダイレクト サービスを指定します。
password *encryption-number password*	（任意）暗号化番号を指定します。指定できる範囲は 0 ～ 7 です。暗号化しない場合は 0、独自の場合は 7 を使用します。また、7 文字以内でパスワード名を指定します。device は、パスワードと MD5 認証値を組み合わせて、device とアプリケーション エンジンとの接続にセキュリティを確保します。デフォルトでは、パスワードは設定されておらず、認証も実行されていません。

コマンド デフォルト

WCCP サービスがデバイスでイネーブルにされていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

シスコ エクスプレス フォワーディング スイッチングがイネーブルのとき、WCCP の透過的キャッシングはネットワーク アドレス変換（NAT）をバイパスします。この状況に対処するには、発信方向で WCCP 透過キャッシングを設定し、コンテンツ エンジン インターフェイスで Cisco Express Forwarding スイッチングを有効にし、**ip wccp web-cache redirect out** コマンドを指定します。キャッシュに面するルータ インターフェイスで **ip wccp redirect exclude in** コマンドを指定し、内部インターフェイスの着信方向に WCCP を設定します。この設定は、そのインターフェイスに到着したパケットのリダイレクションを回避します。

サービス グループを設定するときにリダイレクト リストを含めることもできます。指定されたリダイレクト リストは、NAT（送信元）IP アドレスを含むパケットを拒否して、リダイレクションを阻止します。

このコマンドは、指定されたサービス番号または Web キャッシュ サービス名のサポートをイネーブルまたはディセーブルにするよう device に指示します。サービス番号は 0 ～ 254 の範囲で指定できます。サービス番号または名前がイネーブルになると、ルータはサービス グループの確立に参加できます。

no ip wccp コマンドが入力されると、device はサービスグループへの参加を終了し、引き続きサービスが設定されているインターフェイスがなければ領域の割り当てを解除し、他のサービスが設定されていなければ WCCP タスクを終了します。

web-cache に続くキーワードと *service-number* 引数はオプションで、任意の順序で指定できますが、1 回しか指定できません。

例

次に、Web キャッシュ、アプリケーション エンジンまたはサーバに接続されたインターフェイス、およびクライアントに接続するインターフェイスを設定する例を示します。

```
デバイス(config)# ip wccp web-cache
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# no switchport
デバイス(config-if)# ip address 172.20.10.30 255.255.255.0
デバイス(config-if)# no shutdown
デバイス(config-if)# exit
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# no switchport
デバイス(config-if)#
*Dec  6 13:11:29.507: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to
down

デバイス(config-if)# ip address 175.20.20.10 255.255.255.0
デバイス(config-if)# no shutdown
デバイス(config-if)# ip wccp web-cache redirect in
デバイス(config-if)# ip wccp web-cache group-listen
デバイス(config-if)# exit
```

log-url

プロビジョニングログを保存する場所を指定するには、自動展開コンフィギュレーションモードで **log-url** 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。

log-url *URL*
no log-url

構文の説明

URL	ステータス ログの保存場所。

コマンド デフォルト

ステータス ログの URL は指定されていません。

コマンド モード

自動展開コンフィギュレーション（config-auto-deploy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

ログの URL は、マニフェストファイル内で、または **log-url** コマンドを使用して設定できます。両方の方法でログの URL が設定されている場合は、マニフェスト ファイルのログの URL が使用されます。*URL* 引数の有効値は、次のとおりです。

- flash:
- ftp:
- http:
- https:
- tftp:

例

次に、ステータス ログを記録するための URL を指定する例を示します。

```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# log-url tftp://10.106.16.20/folder1/EEM
```

関連コマンド

コマンド	説明
event-manager auto-deploy	EEM 自動展開プロファイルを設定します。

manifest format

マニフェストファイルの形式と場所の詳細情報を指定するには、自動展開コンフィギュレーション モードで **manifest format** 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。

manifest format xml url *URL*
no manifest format xml url

構文の説明

xml	マニフェストファイルの形式としてXMLを指定します。
url *URL*	マニフェスト ファイルを保存する場所を指定します。

コマンド デフォルト

マニフェスト ファイルの詳細情報は指定されていません。

コマンド モード

自動展開コンフィギュレーション（config-auto-deploy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

URL 引数の有効値は、次のとおりです。

- flash:
- ftp:
- http:
- https:
- tftp:

例

次に、マニフェスト ファイルの形式と場所の詳細情報を指定する例を示します。

```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# manifest format xml url tftp://10.106.16.20/folder1/123.xml
```

関連コマンド

コマンド	説明
event-manager auto-deploy	EEM自動展開プロファイルを設定します。

map platform-type

パラメータマップ属性フィルタ基準をプラットフォームタイプに設定するには、パラメータマップ フィルタ モードで **map platform-type** コマンドを使用します。この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。

map-number **map platform-type** {{**eq** | **not-eq** | **regex**} *platform-type*}
no *map-number* **map platform-type** {{**eq** | **not-eq** | **regex**} *platform-type*}

map-number	パラメータ マップ番号を指定します。
eq	フィルタタイプ名がプラットフォームタイプ名と同じであることを指定します。
not-eq	フィルタタイプ名がプラットフォームタイプ名と同じでないことを指定します。
regex	フィルタタイプ名が正規表現であることを指定します。
platform-type	パラメータマップ属性フィルタ基準のプラットフォームタイプを指定します。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

パラメータ マップ フィルタ モード（config-parameter-map-filter）

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、パラメータマップ属性フィルタ基準をプラットフォームタイプに設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para
Device(config-parameter-map-filter)# 10 map platform-type eq C9xxx
```

match platform-type

プラットフォームタイプに基づいて制御クラスを評価するには、コントロール クラスマップ フィルタ モードで **match platform-type** コマンドを使用します。この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 platform-type *platform-name*

no match platform-type *platform-name*

構文の説明

platform-name	プラットフォームの名前を指定します。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

コントロール クラスマップ フィルタ 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 16.12.1	このコマンドが導入されました。

例

次に、クラスマップフィルタをプラットフォームタイプと一致するように設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# class-map type control subscriber match-all DOT1X_NO_AGENT
Device(config-filter-control-classmap)# match platform-type C9xxx
```

monitor capture (interface/control plane)

接続ポイントおよびパケットフロー方向を指定してモニタキャプチャポイントを設定する、またはキャプチャポイントに接続ポイントを追加するには、特権EXECモードで **monitor capture** コマンドを使用します。指定した接続ポイントおよびパケットフロー方向でモニタキャプチャを無効にする、またはキャプチャポイント上の複数の接続ポイントのいずれかを無効にするには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*}{**interface** *interface-type interface-id* | **control-plane**}{**in** | **out** | **both**}
no monitor capture {*capture-name*}{**interface** *interface-type interface-id* | **control-plane**}{**in** | **out** | **both**}

構文の説明

capture-name	定義するキャプチャの名前。
interface *interface-type interface-id*	*interface-type* および *interface-id* とのインターフェイスを接続ポイントとして指定します。引数の意味は次のとおりです。
control-plane	コントロール プレーンを接続ポイントとして指定します。
in | **out** | **both**	キャプチャするトラフィックの方向を指定します。

コマンド デフォルト

Wireshark キャプチャは設定されていません。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

接続ポイントがこのコマンドを使用してキャプチャポイントに関連付けられると、方向を変更する唯一の方法は、このコマンドの **no** 形式を使用して接続ポイントを削除し、新しい方向に接続ポイントを再接続することです。接続ポイントの方向は上書きできません。

接続ポイントがキャプチャ ポイントから削除され、1 つの接続ポイントのみが関連付けられている場合、キャプチャ ポイントは効率的に削除されます。

このコマンドを別の接続ポイントで再実行することで、複数の接続ポイントをキャプチャ ポイントと関連付けることができます。次に例を示します。

複数のキャプチャ ポイントを定義できますが、一度にアクティブにできるのは1つだけです。つまり、1 つ開始するには 1 つ停止する必要があります。

インターフェイスの出力方向にキャプチャされたパケットは、スイッチの書き換えによって行われた変更（TTL、VLAN タグ CoS、チェックサム、および MAC アドレス、DSCP、プレシデント、UP など）が反映されないこともあります。

特定の順序はキャプチャ ポイントを定義する場合には適用されません。任意の順序でキャプチャ ポイント パラメータを定義できます。Wireshark CLI では、単一行のパラメータ数に制限はありません。これはキャプチャ ポイントを定義するために必要なコマンドの数を制限します。

VRF、管理ポート、プライベート VLAN はいずれも接続ポイントとして使用することはできません。

Wireshark は宛先 SPAN ポートでパケットをキャプチャできません。

VLAN が Wireshark の接続ポイントとして使用されている場合、パケットは、入力方向でのみキャプチャされます。

例

物理インターフェイスを接続ポイントとして使用してキャプチャ ポイントを定義するには次を実行します。

```
デバイス# monitor capture mycap interface GigabitEthernet1/0/1 in
デバイス# monitor capture mycap match ipv4 any any
```

（注） 2 つ目のコマンドは、キャプチャ ポイントのコア フィルタを定義します。これは、キャプチャ ポイントで CAPWAP トンネリング接続ポイントを使用している場合を除いて、キャプチャ ポイントが機能するために必要です。

キャプチャ ポイントで CAPWAP トンネリング接続ポイントを使用している場合、コア フィルタを使用できません。

複数の接続ポイントを持つキャプチャ ポイントを定義するには次を実行します。

```
デバイス# monitor capture mycap interface GigabitEthernet1/0/1 in
デバイス# monitor capture mycap match ipv4 any any
デバイス# monitor capture mycap control-plane in
デバイス# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap control-plane in
```

複数の接続ポイントで定義されたキャプチャ ポイントから接続ポイントを削除するには次を実行します。

```
デバイス# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap control-plane in
デバイス# no monitor capture mycap control-plane
デバイス# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
```

CAPWAP 接続ポイントでキャプチャ ポイントを定義するには次を実行します。

```
デバイス# show capwap summary

CAPWAP Tunnels General Statistics:
  Number of Capwap Data Tunnels       = 1
  Number of Capwap Mobility Tunnels   = 0
  Number of Capwap Multicast Tunnels  = 0


Name   APName                           Type PhyPortIf Mode      McastIf
------ -------------------------------- ---- --------- --------- -------
Ca0    AP442b.03a9.6715                 data Gi3/0/6   unicast   -


Name   SrcIP           SrcPort DestIP          DstPort DtlsEn MTU   Xact
------ --------------- ------- --------------- ------- ------ ----- ----
Ca0    10.10.14.32     5247    10.10.14.2      38514   No     1449  0

デバイス# monitor capture mycap interface capwap 0 both
デバイス# monitor capture mycap file location flash:mycap.pcap
デバイス# monitor capture mycap file buffer-size 1
デバイス# monitor capture mycap start

*Aug 20 11:02:21.983: %BUFCAP-6-ENABLE: Capture Point mycap enabled.on

デバイス# show monitor capture mycap parameter
   monitor capture mycap interface capwap  0 in
   monitor capture mycap interface capwap  0 out
   monitor capture mycap file location flash:mycap.pcap buffer-size 1
デバイス#
デバイス# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
    Ingress:
 0
    Egress:
 0
   Status : Active
  Filter Details:
```

```
    Capture all packets
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 1
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
デバイス#
デバイス# show monitor capture file flash:mycap.pcap
  1   0.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  2   0.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  3   2.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  4   2.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  5   3.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  6   4.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  7   4.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  8   5.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
  9   5.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 10   6.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 11   8.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 12   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 13   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 14   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 15   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 16   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 17   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 18   9.236987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 19  10.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 20  10.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 21  12.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 22  12.239993   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 23  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 24  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 25  12.250994   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 26  12.256990   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 27  12.262987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 28  12.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
 29  12.802012   10.10.14.3 -> 10.10.14.255 NBNS Name query NB WPAD.<00>
 30  13.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0,
FN=0, Flags=........
```

monitor capture buffer

モニタキャプチャ（WireShark）のバッファを設定するには、特権 EXEC モードで **monitor capture buffer** コマンドを使用します。モニタキャプチャバッファを無効にする、またはバッファを循環バッファからデフォルトの線形バッファに戻すには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*} **buffer** {**circular** [**size** *buffer-size*] | **size** *buffer-size*}
no monitor capture {*capture-name*} **buffer** [**circular**]

構文の説明

capture-name	バッファが設定されるキャプチャの名前。
circular	バッファが循環タイプであることを指定します。循環タイプのバッファは、バッファが消費された後も以前にキャプチャされたデータを上書きすることでデータのキャプチャを継続します。
size *buffer-size*	（任意）バッファのサイズを指定します。範囲は 1 ～ 100 MB です。

コマンド デフォルト

線形バッファが設定されます。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

最初に WireShark のキャプチャを設定すると、小規模の循環バッファが提案されます。

例

1 MB のサイズの循環バッファを設定する場合は次を実行します。

```
デバイス# monitor capture mycap buffer circular size 1
```

monitor capture clear

モニタキャプチャ（WireShark）バッファをクリアするには、特権 EXEC モードで **monitor capture clear** コマンドを使用します。

monitor capture {*capture-name*} **clear**

構文の説明

capture-name	バッファがクリアされるキャプチャの名前。

コマンド デフォルト バッファのコンテンツはクリアされません。

コマンド モード 特権 EXEC

コマンド履歴

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

使用上のガイドライン キャプチャ中、または 1 つ以上の最終条件が満たされたか **monitor capture stop** コマンドを入力したためにキャプチャが停止された後に、**monitor capture clear** コマンドを使用します。キャプチャが停止した後に **monitor capture clear** コマンドを入力した場合、バッファにキャプチャされたパケットがないため、ファイルへのキャプチャされたパケットのコンテンツの保存に使用された **monitor capture export** コマンドには影響はありません。

パケットをバッファ内に保存する複数のキャプチャがある場合、メモリ ロスを避けるため、新しいキャプチャを開始する前にバッファをクリアしてください。

例

mycap をキャプチャするためにバッファ コンテンツをクリアするには次を実行します。

```
デバイス# monitor capture mycap clear
```

monitor capture export

ファイルにモニタキャプチャ（WireShark）をエクスポートするには、特権 EXEC モードで **monitor capture export** コマンドを使用します。

monitor capture {*capture-name*} **export** *file-location* **:** *file-name*

構文の説明

capture-name	エクスポートするキャプチャの名前。
file-location :*file-name*	（任意）キャプチャ ストレージ ファイルの場所およびファイル名を指定します。*file-location* に使用可能な値は次のとおりです。 • flash：オンボード フラッシュ ストレージ • (usbflash0:)：USB ドライブ

コマンド デフォルト キャプチャされたパケットは保存されません。

コマンド モード 特権 EXEC

コマンド履歴

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

使用上のガイドライン

ストレージの宛先がキャプチャバッファである場合にのみ **monitor capture export** コマンドを使用します。ファイルはリモートにもローカルにも保存できます。キャプチャ中またはパケットキャプチャ停止後にこのコマンドを使用します。パケットキャプチャは、1つ以上の終了条件が満たされた場合、または **monitor capture stop** コマンドを入力すると停止します。

WireSharkがスタック内のスイッチで使用される場合、パケットキャプチャは前述の*file-location*で指定されたアクティブスイッチに接続されるデバイス上にのみ保存されます。例：flash1 はアクティブなスイッチに接続されています。flash2はセカンダリスイッチに接続されています。この場合、パケット キャプチャの保存に使用できるのは flash1 だけです。

（注） サポートされていないデバイスまたはアクティブなスイッチに接続されていないデバイスにパケット キャプチャを保存しようとするとエラーが発生する可能性があります。

例

キャプチャ バッファの内容を flash ドライブの mycap.pcap にエクスポートするには次を実行します。

```
デバイス# monitor capture mycap export flash:mycap.pcap
```

monitor capture file

モニタキャプチャ（WireShark）ストレージファイル属性を設定するには、特権 EXEC モードで **monitor capture file** コマンドを使用します。ストレージファイル属性を削除するには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*} **file**{ [**buffer-size** *temp-buffer-size*] [**location** *file-location* **:** *file-name*] [**ring** *number-of-ring-files*] [**size** *total-size*] }
no monitor capture {*capture-name*} **file**{ [**buffer-size**] [**location**] [**ring**] [**size**] }

構文の説明

capture-name	変更するキャプチャの名前。
buffer-size *temp-buffer-size*	（任意）一時バッファのサイズを指定します。*temp-buffer-size* の範囲は 1 ～ 100 MB です。これはパケット損失を削減するために指定されます。

location *file-location* : *file-name*	（任意）キャプチャ ストレージ ファイルの場所およびファイル名を指定します。*file-location* に使用可能な値は次のとおりです。 • flash：オンボード フラッシュ ストレージ • (usbflash0:)：USB ドライブ
ring *number-of-ring-files*	（任意）キャプチャが循環ファイルチェーンに保存されること、およびファイル リング内のファイル数を指定します。
size *total-size*	（任意）キャプチャ ファイルの合計サイズを指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

ストレージの宛先がファイルである場合にのみ **monitor capture file** コマンドを使用します。ファイルはリモートにもローカルにも保存できます。パケット キャプチャの停止後にこのコマンドを使用します。パケットキャプチャは、1 つ以上の終了条件が満たされた場合、または **monitor capture stop** コマンドを入力すると停止します。

WireShark がスタック内のスイッチで使用される場合、パケットキャプチャは前述の *file-location* で指定されたアクティブスイッチに接続されるデバイス上にのみ保存されます。例：flash1 はアクティブなスイッチに接続されています。flash2 はセカンダリスイッチに接続されています。この場合、パケット キャプチャの保存に使用できるのは flash1 だけです。

（注） サポートされていないデバイスまたはアクティブなスイッチに接続されていないデバイスにパケット キャプチャを保存しようとするとエラーが発生する可能性があります。

例

フラッシュ ドライブに保管されているファイル名が mycap.pcap であることを指定するには次を実行します。

```
デバイス# monitor capture mycap file location flash:mycap.pcap
```

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*] [**packet-length** *size*] [**packets** *num*]}
no monitor capture {*capture-name*} **limit** [**duration**] [**packet-length**] [**packets**]

構文の説明

capture-name	キャプチャ制限を割り当てられるキャプチャの名前。
duration *seconds*	（任意）キャプチャ期間（秒）を指定します。範囲は 1 ～ 1000000 です。
packet-length *size*	（任意）パケット長（バイト）を指定します。実際のパケットが特定の長さより長い場合、数がバイト引数によって示される最初のセットのバイトのみが保存されます。
packets *num*	（任意）キャプチャに対して処理されるパケット数を指定します。

コマンド デフォルト

キャプチャ制限は設定されません。

コマンド モード

特権 EXEC

コマンド履歴

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

例

60 秒のセッション制限および 400 バイトのパケット セグメント長を設定するには次を実行します。

```
デバイス# monitor capture mycap limit duration 60 packet-len 400
```

monitor capture match

（注） CAPWAP トンネルをキャプチャする場合は、このコマンドを使用しないでください。また、コントロール プレーンおよび CAPWAP トンネルが混在している場合、このコマンドには効果がありません。

モニタ（Wireshark）キャプチャに対して明示的にインラインコアフィルタを定義するには、特権 EXEC モードで **monitor capture match** コマンドを使用します。このフィルタを削除するには、このコマンドの **no** 形式を使用します。

monitor capture {*capture-name*} **match** {**any** | **mac** *mac-match-string* | **ipv4** {**any** | **host** | **protocol**}{**any** | **host**} | **ipv6** {**any** | **host** | **protocol**}{**any** | **host**}}
no monitor capture {*capture-name*} **match**

構文の説明

capture-name	コア フィルタを割り当てられるキャプチャの名前。
any	すべてのパケットを指定します。
mac *mac-match-string*	レイヤ 2 パケットを指定します。
ipv4	IPv4 パケットを指定します。
host	ホストを指定します。
protocol	プロトコルを指定します。
ipv6	IPv6 パケットを指定します。

コマンド デフォルト

コア フィルタは設定されていません。

コマンド モード

特権 EXEC

コマンド履歴

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

例

ソースまたは宛先上の任意の IP バージョン 4 パケットに一致するキャプチャ ポイントに対してキャプチャ ポイントおよびコア フィルタを定義するには、次を実行します。

```
デバイス# monitor capture mycap interface GigabitEthernet1/0/1 in
デバイス# monitor capture mycap match ipv4 any any
```

monitor capture start

トラフィック トレース ポイントでパケットデータのバッファへのキャプチャを開始するには、特権 EXEC モードで **monitor capture start** コマンドを使用します。

monitor capture {*capture-name*} **start**

構文の説明

capture-name	開始するキャプチャの名前。

コマンド デフォルト

バッファのコンテンツはクリアされません。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

キャプチャポイントが定義された後にパケットデータキャプチャを有効にするには、**monitor capture clear** コマンドを使用します。パケットデータのキャプチャを停止するには、**monitor capture stop** コマンドを使用します。

CPU およびメモリなどのシステム リソースがキャプチャの開始前に使用可能であることを確認します。

例

バッファ コンテンツのキャプチャを開始するには次を実行します。

```
デバイス#  monitor capture mycap start
```

monitor capture stop

トラフィック トレース ポイントでパケットデータのキャプチャを停止するには、特権 EXEC モードで **monitor capture stop** コマンドを使用します。

monitor capture {*capture-name*} **stop**

構文の説明

capture-name	停止するキャプチャの名前。

コマンド デフォルト

パケット データ キャプチャが進行中です。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

monitor capture stop コマンドを使用して、**monitor capture start** コマンドによって開始したパケットデータのキャプチャを停止します。線形および循環の 2 つのタイプのキャプチャ バッファを設定できます。線形バッファがいっぱいになった場合、データ キャプチャは自動的に停止します。循環バッファがいっぱいになると、データ キャプチャは最初から開始し、データは上書きされます。

例

バッファ コンテンツのキャプチャを停止するには次を実行します。

```
デバイス# monitor capture mycap stop
```

monitor session

ポート間のトラフィック分析のために、イーサネットスイッチドポートアナライザ（SPAN）セッション、リモートスイッチドポートアナライザ（RSPAN）セッション、またはEncapsulated Remote Switched Port Analyzer（ERSPAN）セッションのコンフィギュレーションを新規作成するか、既存のセッションのコンフィギュレーションに追加するには、**monitor session** グローバル コンフィギュレーション コマンドを使用します。セッションをクリアするには、このコマンドの **no** 形式を使用します。

monitor session *session-number* {**destination** | **filter** | **source** | **type** {**erspan-destination** | **erspan-source**}}
no monitor session {*session-number* [**destination** | **filter** | **source** | **type** {**erspan-destination** | **erspan-source**}] | **all** | **local** | **range** *session-range* | **remote**}

構文の説明

session-number	セッションで識別されるセッション番号。指定できる範囲は 1 ～ 66 です。
all	すべてのモニタ セッションをクリアします。
local	すべてのローカルモニタセッションをクリアします。
range *session-range*	指定された範囲のモニタ セッションをクリアします。
remote	すべてのリモートモニタセッションをクリアします。

コマンド デフォルト

モニタ セッションは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.11.1	**type** {**erspan-destination** | **erspan-source**} キーワードが導入されました。

使用上のガイドライン

2 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチまたはスイッチスタック上で、合計 66 の SPAN、RSPAN、および ERSPAN セッションを保有できます。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、FRSPAN、および ERSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

例

次に、ローカル SPAN セッション 1 を作成して Po13（EtherChannel ポート）のトラフィックをモニタし、セッションの SPAN トラフィックを VLAN 1281 のみに限定する例を示します。出力トラフィックは送信元を複製します。入力転送はイネーブルになりません。

```
Device(config)# monitor session 1 source interface Po13
Device(config)# monitor session 1 filter vlan 1281
Device(config)# monitor session 1 destination interface GigabitEthernet2/0/36 encapsulation
 replicate
Device(config)# monitor session 1 destination interface GigabitEthernet3/0/36 encapsulation
 replicate
```

次に、これらのセットアップ手順を完了した後の **show monitor session all** コマンドの出力を示します。

```
Device# show monitor session all

Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Po13
Destination Ports      : Gi2/0/36,Gi3/0/36
    Encapsulation      : Replicate
          Ingress      : Disabled
Filter VLANs           : 1281
...
```

monitor session destination

新規にスイッチドポートアナライザ（SPAN）セッションまたはリモート SPAN（RSPAN）宛先セッションを開始し、ネットワーク セキュリティ デバイス（Cisco IDS Sensor アプライアンスなど）の宛先ポート上の入力トラフィックをイネーブルにし、既存の SPAN または RSPAN セッションでインターフェイスを追加または削除するには、**monitor session destination** グローバル コンフィギュレーション コマンドを使用します。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから宛先インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

monitor session *session-number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**replicate** | **dot1q**}] {**ingress** [**dot1q** | **untagged**] } | {**remote**} **vlan** *vlan-id*

no monitor session *session-number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**replicate** | **dot1q**}] {**ingress** [**dot1q** | **untagged**] } | {**remote**} **vlan** *vlan-id*

構文の説明

session-number	
interface *interface-id*	SPAN または RSPAN セッションの宛先または送信元インターフェイスを指定します。有効なインターフェイスは物理ポート（タイプ、スタック メンバ、モジュール、ポート番号を含む）です。送信元インターフェイスの場合は、ポート チャネルも有効なインターフェイス タイプであり、指定できる範囲は 1 ～ 128 です。
,	（任意）複数のインターフェイスまたはVLANを指定します。または、前の範囲からインターフェイスまたは VLAN の範囲を分離します。カンマの前後にスペースを入れます。
-	（任意）インターフェイスまたは VLAN の範囲を指定します。ハイフンの前後にスペースを入れます。
encapsulation replicate	（任意）宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 次のキーワードは、ローカル SPAN にだけ有効です。RSPAN、RSPAN VLAN ID は元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。**encapsulation** オプションは、**no** 形式では無視されます。
encapsulation dot1q	（任意）宛先インターフェイスが IEEE 802.1Q カプセル化の送信元インターフェイスの着信パケットを受け入れるように指定します。 次のキーワードは、ローカル SPAN にだけ有効です。RSPAN、RSPAN VLAN ID は元の VLAN ID を上書きするため、パケットは常にタグなしで送信されます。**encapsulation** オプションは、**no** 形式では無視されます。
ingress	入力トラフィック転送をイネーブルにします。

dot1q	（任意）指定された VLAN をデフォルト VLAN として、IEEE 802.1Q カプセル化された着信パケットを受け入れます。
untagged	（任意）指定された VLAN をデフォルト VLAN として、タグなしカプセル化された着信パケットを受け入れます。
isl	ISL カプセル化を使用して入力トラフィックを転送するように指定します。
remote	RSPAN 送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。 RSPAN VLAN は VLAN 1（デフォルトの VLAN）、または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN に予約済）になることはできません。
vlan *vlan-id*	**ingress** キーワードとのみ使用された場合、入力トラフィックに対するデフォルトの VLAN を設定します。

コマンド デフォルト

モニタ セッションは設定されていません。

ローカル SPAN の宛先ポートで **encapsulation replicate** が指定されなかった場合、パケットはカプセル化のタグなしのネイティブ形式で送信されます。

入力転送は宛先ポートではディセーブルになっています。

all、**local**、**range** *session-range*、**remote** を **no monitor session** コマンドに指定することで、すべての SPAN および RSPAN、すべてのローカル SPAN、範囲、すべての RSPAN セッションをクリアできます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

8 つのローカル SPAN セッションおよび RSPAN 送信元セッションを組み合わせた最大値を設定することができます。スイッチまたはスイッチ スタック上で、合計 66 の SPAN および RSPAN セッションを保有できます。

SPAN または RSPAN の宛先は物理ポートである必要があります。

スイッチ上またはスイッチ スタック上で、最大 64 の宛先ポートを保有できます。

各セッションには複数の入力または出力の送信元ポートまたは VLAN を含めることができますが、1 つのセッション内で送信元ポートと送信元 VLAN を組み合わせることはできません。各セッションは複数の宛先ポートを保有できます。

VLAN-based SPAN（VSPAN）を使用して、VLAN または一連の VLAN 内のネットワーク トラフィックを解析する場合、送信元 VLAN のすべてのアクティブ ポートが SPAN または RSPAN セッションの送信元ポートになります。トランク ポートは VSPAN の送信元ポートとして含まれ、モニタリングされた VLAN ID のパケットだけが宛先ポートに送信されます。

1 つのポート、1 つの VLAN、一連のポート、一連の VLAN、ポート範囲、VLAN 範囲でトラフィックをモニタできます。**[,|-]** オプションを使用して、複数または一定範囲のインターフェイスまたは VLAN を指定します。

一連の VLAN またはインターフェイスを指定するときは、カンマ（,）の前後にスペースが必要です。VLAN またはインターフェイスの範囲を指定するときは、ハイフン（-）の前後にスペースが必要です。

EtherChannel ポートは、SPAN または RSPAN 宛先ポートとして設定することは。EtherChannel グループのメンバである物理ポートは、宛先ポートとして使用できます。ただし、SPAN の宛先として機能する間は、EtherChannel グループに参加できません。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 宛先ポートであるポート上で IEEE 802.1X 認証をイネーブルにすることはできますが、ポートが SPAN 宛先として削除されるまで IEEE 802.1X 認証はディセーブルです。IEEE 802.1X 認証がポート上で使用できない場合、スイッチはエラー メッセージを返します。SPAN または RSPAN 送信元ポートでは IEEE 802.1X 認証をイネーブルにすることができます。

入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。

宛先ポートは次のような動作を設定できます。

- **monitor session** *session_number* **destination interface** *interface-id* を他のキーワードなしで入力すると、出力のカプセル化はタグなしとなり、入力転送はイネーブルになりません。
- **monitor session** *session_number* **destination interface** *interface-id* **ingress** を入力した場合は、出力カプセル化はタグなしで、入力カプセル化はそのあとに続くキーワードが **dot1q** と **untagged** のいずれであるかによって決まります。
- **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate** を他のキーワードなしで入力すると、出力のカプセル化はソースインターフェイスのカプセル化を複製し、入力転送はイネーブルになりません（これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。
- **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate ingress** を入力した場合は、出力カプセル化は送信元インターフェイスカプセル化を複製し、入力カプセル化はそのあとに続くキーワードが **dot1q** と **untagged** のいずれであるかによって

決まります（これはローカル SPAN だけに適用します。RSPAN はカプセル化の複製をサポートしていません）。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバ 1 の送信元ポート 1 からスタック メンバ 2 の宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
デバイス(config)# monitor session 1 source interface gigabitethernet1/0/1 both
デバイス(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

次の例では、宛先ポートを既存のローカル SPAN セッションから削除する方法を示します。

```
デバイス(config)# no monitor session 2 destination interface gigabitethernet1/0/2
```

次の例では、ある送信元インターフェイスをモニタリングする RSPAN 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示します。

```
デバイス(config)# monitor session 1 source interface gigabitethernet1/0/1
デバイス(config)# monitor session 1 destination remote vlan 900
デバイス(config)# end
```

次の例では、モニタリングされたトラフィックを受信するスイッチに、RSPAN 宛先セッション 10 を設定する方法を示します。

```
デバイス(config)# monitor session 10 source remote vlan 900
デバイス(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

次の例では、IEEE 802.1Q カプセル化をサポートするセキュリティ装置を使用して、VLAN 5 の入力トラフィックに対応する宛先ポートを設定する方法を示します。出力トラフィックは送信元のカプセル化を複製します。入力トラフィックは IEEE 802.1Q カプセル化を使用します。

```
デバイス(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
 dot1q ingress dot1q vlan 5
```

次の例では、カプセル化をサポートしないセキュリティ デバイスを使用して、VLAN 5 上の入力トラフィックの宛先ポートを設定する方法を示します。出力トラフィックおよび入力トラフィックはタグなしです。

```
デバイス(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress
untagged vlan 5
```

monitor session filter

フローベース SPAN（FSPAN）セッションやフローベース RSPAN（FRSPAN）送信元または宛先セッションを新しく開始する、または特定の VLAN に対して SPAN 送信元トラフィックを制限（フィルタ処理）するには、**monitor session filter** グローバル コンフィギュレーション コマンドを使用します。SPAN または RSPAN セッションからフィルタを削除するには、このコマンドの **no** 形式を使用します。

monitor session *session-number* **filter** {**vlan** *vlan-id* [**,** | **-**] }
no monitor session *session-number* **filter** {**vlan** *vlan-id* [**,** | **-**] }

構文の説明

session-number	
vlan *vlan-id*	SPAN 送信元トラフィックを特定の VLAN に制限するため、トランクの送信元ポート上のフィルタとしてVLANのリストを指定します。*vlan-id* で指定できる範囲は 1 ～ 4094 です。
,	任意）複数の VLAN を指定します。または VLAN 範囲を前の範囲から区切ります。カンマの前後にスペースを入れます。
-	（任意）VLAN の範囲を指定します。ハイフンの前後にスペースを入れます。

コマンド デフォルト

モニタ セッションは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

1 つの VLAN、または複数のポートや VLAN、特定範囲のポートや VLAN でトラフィックをモニタできます。複数または一定範囲の VLAN を指定するには、[,|-] オプションを使用します。

複数の VLAN を指定するときは、カンマ（,）の前後にスペースが必要です。VLAN の範囲を指定するときは、ハイフン（-）の前後にスペースが必要です。

VLAN のフィルタリングは、トランクの送信元ポート上で選択された一連の VLAN のネットワーク トラフィック解析を参照します。デフォルトでは、すべての VLAN がトランクの送信

元ポートでモニタリングされます。**monitor session** *session_number* **filter vlan** *vlan-id* コマンドを使用すると、トランク送信元ポートの SPAN トラフィックを指定された VLAN だけに限定できます。

VLAN のモニタリングおよび VLAN のフィルタリングは相互に排他的な関係です。VLAN が送信元の場合、VLANのフィルタリングはイネーブルにできません。VLANのフィルタリングが設定されている場合、VLAN は送信元になることができません。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

例

次の例では、既存のセッションの SPAN トラフィックを指定の VLAN だけに制限する方法を示します。

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

次に、ローカル SPAN セッション 1 を作成してスタック メンバ 1 の送信元ポート 1 とスタック メンバ 2 の宛先ポートの送受信両方のトラフィックをモニタし、FSPAN セッションでアクセス リスト番号 122 を使用して IPv4 トラフィックをフィルタする例を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 1 filter ip access-group 122
```

monitor session source

スイッチドポートアナライザ（SPAN）セッションまたはリモート SPAN（RSPAN）送信元セッションを開始する、または既存の SPAN または RSPAN セッションでインターフェイスを追加または削除するには、**monitor session source** グローバル コンフィギュレーション コマンドを使用します。SPAN または RSPAN セッションを削除したり、SPAN または RSPAN セッションから送信元インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

monitor session *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [**,** | **-**] [**both** | **rx** | **tx**]}
no monitor session *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [**,** | **-**] [**both** | **rx** | **tx**]}

構文の説明

session_number

interface *interface-id*	SPAN または RSPAN セッションの送信元インターフェイスを指定します。有効なインターフェイスは物理ポート（タイプ、スタック メンバ、モジュール、ポート番号を含む）です。送信元インターフェイスの場合は、ポートチャネルも有効なインターフェイスタイプであり、指定できる範囲は 1 ～ 48 です。
,	（任意）複数のインターフェイスまたはVLANを指定します。または、前の範囲からインターフェイスまたは VLAN の範囲を分離します。カンマの前後にスペースを入れます。
-	（任意）インターフェイスまたは VLAN の範囲を指定します。ハイフンの前後にスペースを入れます。
both | **rx** | **tx**	（任意）モニタリングするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは送受信のトラフィックを送信します。
remote	（任意）RSPAN送信元または宛先セッションのリモート VLAN を指定します。指定できる範囲は 2 ～ 1001 または 1006 ～ 4094 です。 RSPAN VLAN は VLAN 1（デフォルトの VLAN）、またはVLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN に予約済）になることはできません。
vlan *vlan-id*	**ingress** キーワードだけで使用された場合、入力トラフィックにデフォルトの VLAN を設定します。

コマンド デフォルト

モニタ セッションは設定されていません。

送信元インターフェイスのデフォルトでは、受信トラフィックと送信トラフィックの両方をモニタリングします。

送信元ポートとして使用されるトランク インターフェイス上では、すべての VLAN がモニタリングされます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

送信元ポートまたは送信元 VLAN を出入りするトラフィックは、SPAN または RSPAN を使用してモニタできます。送信元ポートまたは送信元 VLAN にルーティングされるトラフィックはモニタできません。

物理ポート、ポート チャネル、VLAN が送信元になることができます。

各セッションには複数の入力または出力の送信元ポートまたは VLAN を含めることができますが、1 つのセッション内で送信元ポートと送信元 VLAN を組み合わせることはできません。各セッションは複数の宛先ポートを保有できます。

VLAN-based SPAN（VSPAN）を使用して、VLAN または一連の VLAN 内のネットワーク トラフィックを解析する場合、送信元 VLAN のすべてのアクティブ ポートが SPAN または RSPAN セッションの送信元ポートになります。トランク ポートは VSPAN の送信元ポートとして含まれ、モニタリングされた VLAN ID のパケットだけが宛先ポートに送信されます。

1 つのポート、1 つの VLAN、一連のポート、一連の VLAN、ポート範囲、VLAN 範囲でトラフィックをモニタできます。[,|-] オプションを使用して、複数または一定範囲のインターフェイスまたは VLAN を指定します。

一連の VLAN またはインターフェイスを指定するときは、カンマ（,）の前後にスペースが必要です。VLAN またはインターフェイスの範囲を指定するときは、ハイフン（-）の前後にスペースが必要です。

個々のポートはそれらが EtherChannel に参加している間もモニタリングすることができます。また、RSPAN 送信元インターフェイスとして **port-channel** 番号を指定することで EtherChannel バンドル全体をモニタリングすることができます。

宛先ポートとして使用しているポートは、SPAN または RSPAN 送信元ポートにすることはできません。また、同時に複数のセッションの宛先ポートにすることはできません。

SPAN または RSPAN 送信元ポートでは IEEE 802.1X 認証をイネーブルにすることができます。

設定を確認するには、**show monitor** 特権 EXEC コマンドを入力します。**show running-config** 特権 EXEC コマンドを入力すると、スイッチの SPAN、RSPAN、FSPAN、および FRSPAN の設定を表示することができます。SPAN 情報は出力の最後付近に表示されます。

例

次の例では、ローカル SPAN セッション 1 を作成し、スタック メンバ 1 の送信元ポート 1 からスタック メンバ 2 の宛先ポート 2 に送受信するトラフィックをモニタする方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

次の例では、複数の送信元インターフェイスをモニタリングする RSPAN 送信元セッション 1 を設定し、さらに宛先 RSPAN VLAN 900 を設定する方法を示します。

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

monitor session type

ローカルの Encapsulated Remote Switched Port Analyzer（ERSPAN）セッションを設定するには、グローバル コンフィギュレーション モードで **monitor session type** コマンドを使用します。ERSPAN 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。

monitor session *span-session-number* **type** {**erspan-destination** | **erspan-source**}
no monitor session *span-session-number* **type** {**erspan-destination** | **erspan-source**}

構文の説明

span-session-number	ローカル ERSPAN セッションの番号。有効値は 1 ～ 66 です。

コマンド デフォルト

ERSPAN 送信元または宛先セッションは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.11.1	**erspan-destination** キーワードが導入されました。

使用上のガイドライン

span-session-number およびセッションタイプは、設定後は変更できません。セッションを削除するには、このコマンドの **no** 形式を使用し、新しいセッション ID または新しいセッションタイプでセッションを再作成します。

ERSPAN 送信元セッションの宛先 IP アドレスが（宛先スイッチ上のインターフェイスで設定される必要がある）、ERSPAN宛先セッションが宛先ポートに送信するトラフィックの送信元です。ERSPAN モニタ宛先セッション コンフィギュレーション モードで **ip address** コマンドを使用して、送信元セッションと宛先セッションの両方に同じアドレスを設定できます。

ERSPAN ID により、同じ宛先 IP アドレスに着信する ERSPAN トラフィックと異なる ERSPAN 送信元セッションとが区別されます。

ローカル ERSPAN 送信元セッションの最大数は 8 に制限されています。

例

次に、ERSPAN 送信元セッション番号を設定する例を示します。

```
Device(config)# monitor session 55 type erspan-source
Device(config-mon-erspan-src)#
```

関連コマンド

コマンド	説明
monitor session type	ERSPAN 送信元セッション番号または宛先セッション番号を作成するか、セッションに対して ERSPAN セッション コンフィギュレーション モードを開始します。
show capability feature monitor	モニタ機能に関する情報を表示します。
show monitor session	ERSPAN、SPAN、RSPAN のセッションに関する情報を表示します。

mtu（ERSPAN）

ERSPAN 切り捨ての最大伝送ユニット（MTU）サイズを設定するには、ERSPAN モニタ宛先セッション コンフィギュレーション モードで **mtu** コマンドを使用します。MTU 値を元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。

mtu *bytes*
no mtu

構文の説明

bytes	MTUサイズ（バイト単位）。MTUのデフォルト値は9000バイトです。

コマンド モード

ERSPAN モニタ宛先セッション コンフィギュレーションモード（config-mon-erspan-src-dst）

コマンド履歴

コマンド履歴

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

例

次に、1000 バイトの MTU を指定する例を示します。

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# mtu 1000
```

関連コマンド

コマンド	説明
destination	ERSPAN宛先セッションを設定し、宛先プロパティを指定します。
monitor session type	ローカルの ERSPAN 送信元または宛先セッションを設定します。

origin

Encapsulated Remote Switched Port Analyzer（ERSPAN）トラフィックの送信元として使用するIP アドレスを設定するには、ERSPAN モニタ宛先セッション コンフィギュレーション モードで **origin** 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。

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

構文の説明

ip-address	ERSPAN 送信元セッションの宛先 IP アドレスを指定します。

コマンド デフォルト

送信元 IP アドレスは設定されていません。

コマンド モード

ERSPAN モニタ宛先セッション コンフィギュレーションモード（config-mon-erspan-src-dst）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

スイッチの ERSPAN 送信元セッションは、**origin** コマンドを使用して、さまざまな送信元 IP アドレスを使用できます。

例

次に、ERSPAN 送信元セッションの IP アドレスを設定する例を示します。

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# origin ip-address 203.0.113.2
```

次の **show monitor session all** コマンドの出力例では、異なる送信元 IP アドレスの ERSPAN 送信元セッションが表示されます。

```
Session 3
---------
Type : ERSPAN Source Session
Status : Admin Enabled
Source Ports :
Both : Gi1/0/13
Destination IP Address : 10.10.10.10
Origin IP Address : 10.10.10.10


Session 4
---------
Type : ERSPAN Source Session
Status : Admin Enabled
Destination IP Address : 192.0.2.1
Origin IP Address : 203.0.113.2
```

関連コマンド

コマンド	説明
destination	ERSPAN 宛先セッションを設定し、宛先プロパティを指定します。
monitor session type erspan-source	ローカルの ERSPAN 送信元セッションを設定します。

retry count

ファイル転送が成功しない場合のファイル転送の再試行回数を設定するには、自動展開コンフィギュレーション モードで **retry count** 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。

retry count *retry-count* **interval** *interval-duration*
no retry count *retry-count* **interval** *interval-duration*

構文の説明

retry-count	ファイル転送が成功しない場合のファイル転送の再試行回数。有効な値は 1 ～ 3 です。
interval *interval-duration*	再試行の間隔を指定します。有効な値は 2 ～ 4 分です。

コマンド デフォルト

デフォルトは 0 です。

コマンド モード

自動展開コンフィギュレーション（config-auto-deploy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

例

次に、転送が成功しないファイルの再試行回数を設定する例を示します。

```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# retry count 3 interval 3
```

関連コマンド

コマンド	説明
event-manager auto-deploy	EEM 自動展開プロファイルを設定します。

schedule start-in

ポリシーのプロビジョニングをスケジュールするには、自動展開コンフィギュレーションモードで **schedule start-in** コマンドを使用します。スケジュ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。

schedule start-in hours *hours* **minutes** *minutes* {**oneshot** | **recurring** {**days** *days* | **hours** *hours* }}
no schedule start-in hours *hours* **minutes** *minutes* {**oneshot** | **recurring** {**days** *days* | **hours** *hours* }}

構文の説明

hours *hours*	ポリシー プロビジョニングを開始するタイミング（時）を指定します。有効な値は 0 ～ 23 です。
minutes *minutes*	ポリシー プロビジョニングを開始するタイミング（分）を指定します。有効な値は 0 ～ 59 です。
oneshot	ポリシー プロビジョニングが 1 回だけ実行されるようにスケジュールします。
recurring	ポリシー プロビジョニングが繰り返し実行されるようにスケジュールします。
days *days*	ポリシー プロビジョニングを繰り返すタイミング（日単位）を指定します。有効な値は 1 ～ 30 です。
hours *hours*	ポリシー プロビジョニングを繰り返すタイミング（時間単位）を指定します。有効な値は 12 ～ 168 です。

コマンド デフォルト

ポリシー プロビジョニングのスケジュールは有効になっていません。

コマンド モード

自動展開コンフィギュレーション（config-auto-deploy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

例

次に、ポリシー プロビジョニングが 1 回だけ実行されるようにスケジュールする例を示します。

```
Device(config)# event manager auto-deploy name deploy1
```

```
Device(config-auto-deploy)# schedule start-in hours 2 minutes 30 oneshot
```

次に、ポリシープロビジョニングが繰り返し実行されるようにスケジュールする例を示します。

```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# schedule start-in hours 2 minutes 30 recurring days 2
```

関連コマンド

コマンド	説明
event-manager auto-deploy	EEM 自動展開プロファイルを設定します。

show capability feature monitor

モニタ機能に関する情報を表示するには、特権 EXEC モードで **show capability feature monitor** コマンドを使用します。

show capability feature monitor {**erspan-destination** | **erspan-source**}

構文の説明

erspan-destination	設定済みの Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元セッションに関する情報を表示します。
erspan-source	すべての設定済みのグローバル組み込みテンプレートを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

例

次に、**show capability feature monitor erspan-source** コマンドの出力例を示します。

```
Switch# show capability feature monitor erspan-source

ERSPAN Source Session Supported: true
No of Rx ERSPAN source session: 8
No of Tx ERSPAN source session: 8
ERSPAN Header Type supported: II
ACL filter Supported: true
Fragmentation Supported: true
Truncation Supported: false
Sequence number Supported: false
QOS Supported: true
```

次に、**show capability feature monitor erspan-destination** コマンドの出力例を示します。

```
Switch# show capability feature monitor erspan-destination

ERSPAN Destination Session Supported: false
```

関連コマンド

コマンド	説明
monitor session type erspan-source	ERSPAN 送信元セッション番号を作成するか、セッションに対して ERSPAN セッション コンフィギュレーション モードを開始します。

show class-map type control subscriber

設定されている制御ポリシーのクラスマップ統計情報を表示するには、特権 EXEC モードで **show class-map type control subscriber** コマンドを使用します。

show class-map type control subscriber {all | name *control-class-name***}**

構文の説明

all	すべての制御ポリシーのクラスマップ統計情報を表示します。
name *control-class-name*	指定した制御ポリシーのクラスマップ統計情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

例

次に、**show class-map type control subscriber name** *control-class-name* コマンドの出力例を示します。

```
Device# show class-map type control subscriber name platform

Class-map                 Action                       Exec  Hit  Miss  Comp
---------                 ------                       ----  ---  ----  ----
match-all platform        match platform-type C9xxx    0     0    0     0
Key:
  "Exec" - The number of times this line was executed
  "Hit"  - The number of times this line evaluated to TRUE
  "Miss" - The number of times this line evaluated to FALSE
  "Comp" - The number of times this line completed the execution of its
       condition without a need to continue on to the end
```

show event manager auto-deploy summary

自動展開プロファイル情報のサマリーを表示するには、特権EXECモードで**show event manager auto-deploy summary** コマンドを使用します。

show event manager auto-deploy summary

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが変更されました。

使用上のガイドライン

例

次に、**show event manager auto-deploy summary** コマンドの出力例を示します。

```
Device# show event manager auto-deploy summary

EEM Auto-Deploy Profile details:

    Profile Name  : test
    Status        : Enabled
    Running       : Yes
    Status Syslog : No
    Schedule      : start in 0 hours 5 mins oneshot
    Window        : 5
    Manifest URL  : tftp://10.106.16.20/folder1/123.xml
    Log URL       : tftp://10.106.16.20/folder1/EEM
```

下の表に、ディスプレイ内に表示される重要なフィールドのリストを示します。

表 *36 : show event manager auto-deploy summary* のフィールドの説明

フィールド	説明
プロファイル名	プロファイルに指定された名前。
Status	プロファイル プロビジョニングのステータス（Enabled または Disabled のいずれか）。
Running	有効になっているプロファイルが実行されているかどうか。
Schedule	ポリシー プロビジョニングのスケジュール。

フィールド	説明
Window	ポリシー プロビジョニング時間に追加されるウィンドウ期間。ポリシープロビジョニングは、ポリシープロビジョニング時間と設定されたウィンドウ期間（分単位）の間のランダム時間に実行されます。
Manifest URL	マニフェスト ファイルの場所。
Log URL	デバッグ ログが保存される場所。

関連コマンド

コマンド	説明
event-manager auto-deploy	EEM 自動展開プロファイルを設定します。

show ip sla statistics

Cisco IOS IP サービスレベル契約（SLA）のすべての動作または指定された動作の現在または集約された動作ステータスおよび統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip sla statistics** コマンドを使用します。

show ip sla statistics ［ *operation-number* ［**details**］ | **aggregated** ［ *operation-number* | **details**］ | **details**］

構文の説明

operation-number	（任意）動作ステータスおよび統計情報を表示する動作の番号。受け入れられる値の範囲は 1 ～ 2147483647 です。
details	（任意）詳細出力を指定します。
aggregated	（任意）IP SLA 集約統計を指定します。

コマンド デフォルト

稼働しているすべての IP SLA 動作の出力を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

動作の残りの継続時間、動作がアクティブかどうか、完了時刻など、IP SLA 動作の現在の状態を表示するには、 **show ip sla statistics** を使用します。出力には、最後の（最近完了した）動作に対して返されたモニタリング データも含まれます。この生成された操作 ID は、基本マ

ルチキャスト操作に対して、また操作全体の要約統計の一部として **show ip sla** コンフィギュレーション コマンドを使用すると表示されます。

あるレスポンダに対して詳細を表示するには、その特定の操作IDに**show**コマンドを入力します。

例

次に、 **show ip sla statistics** コマンドの出力例を示します。

```
デバイス# show ip sla statistics

Current Operational State
Entry Number: 3
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
Operational State of Entry: active
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200  OK
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707
```

show monitor

すべてのスイッチドポートアナライザ（SPAN）およびリモート SPAN（RSPAN）セッションに関する情報を表示するには、EXEC モードで **show monitor** コマンドを使用します。

show monitor ［**session** {*session_number* | **all** | **local** | **range** *list* | **remote**} ［**detail**］］

構文の説明

session	（任意）指定された SPAN セッションの情報を表示します。
session_number	
all	（任意）すべての SPAN セッションを表示します。
local	（任意）ローカル SPAN セッションだけを表示します。

range *list*	（任意）一定範囲の SPAN セッションを表示します。*list* は有効なセッションの範囲です。range は単一のセッション、または 2 つの数字を小さい数字からハイフンで区切ったセッションの範囲です。カンマ区切りのパラメータ間、またはハイフン指定の範囲にスペースは入力しません。 （注） このキーワードは、特権 EXEC モードの場合だけ使用可能です。
remote	（任意）リモート SPAN セッションだけを表示します。
detail	（任意）指定されたセッションの詳細情報を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

show monitor コマンドと **show monitor session all** コマンドの出力は同じです。

例

次に、**show monitor** ユーザ EXEC コマンドの出力例を示します。

```
デバイス# show monitor
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
Session 2
---------
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

次の例では、ローカル SPAN 送信元セッション 1 に対する **show monitor** ユーザ EXEC コマンドの出力を示します。

```
デバイス# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

次の例では、入力トラフィック転送をイネーブルにした場合の **show monitor session all** ユーザ EXEC コマンドの出力を示します。

```
デバイス# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
---------
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/012
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

show monitor capture

モニタキャプチャ（WireShark）の内容を表示するには、特権 EXEC モードで **show monitor capture file** コマンドを使用します。

show monitor capture [*capture-name* [**buffer**] | **file** *file-location* : *file-name*][**brief** | **detailed** | **display-filter** *display-filter-string*]

構文の説明

capture-name	（任意）表示するキャプチャの名前を指定します。
buffer	（任意）指定されたキャプチャに関連するバッファが表示されることを指定します。
file *file-location* : *file-name*	（任意）表示するキャプチャ ストレージ ファイルのファイル位置と名前を指定します。

brief	（任意）表示内容の概要を指定します。
detailed	（任意）詳細な表示内容を指定します。
display-filter *display-filter-string*	*display-filter-string* に従って表示内容をフィルタ処理します。

コマンド デフォルト

すべてのキャプチャの内容を表示します。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

none

例

mycap という名前のキャプチャのキャプチャを表示するには次を実行します。

```
デバイス# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
    Ingress:
 0
    Egress:
 0
   Status : Active
  Filter Details:
    Capture all packets
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 1
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

show monitor session

スイッチドポートアナライザ（SPAN）、リモート SPAN（RSPAN）、および Encapsulated Remote Switched Port Analyzer（ERSPAN）のセッションに関する情報を表示するには、EXEC モードで **show monitor session** コマンドを使用します。

show monitor session {*session_number* | **all** | **erspan-destination** | **erspan-source** | **local** | **range** *list* | **remote**} [**detail**]

構文の説明

session_number	SPAN または RSPAN セッションで識別されるセッション番号。指定できる範囲は 1 ～ 66 です。
all	すべての SPAN セッションを表示します。
erspan-source	送信元 ERSPAN セッションだけを表示します。
erspan-destination	宛先 ERSPAN セッションだけを表示します。
local	ローカル SPAN セッションだけを表示します。
range *list*	一定範囲の SPAN セッションを表示します。*list* は有効なセッションの範囲です。range は単一のセッション、または 2 つの数字を小さい数字からハイフンで区切ったセッションの範囲です。カンマ区切りのパラメータ間、またはハイフン指定の範囲にスペースは入力しません。 （注） このキーワードは、特権 EXEC モードの場合だけ使用可能です。
remote	リモート SPAN セッションだけを表示します。
detail	（任意）指定されたセッションの詳細情報を表示します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.11.1	**erspan-destination** コマンドが導入されました。

使用上のガイドライン

ローカルの ERSPAN 送信元セッションの最大数は 8 です。

例

次に、ローカル SPAN 送信元セッション 1 に対する **show monitor session** コマンドの出力例を示します。

```
Device# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

次に、入力トラフィックの転送が有効になっている場合の **show monitor session all** コマンドの出力例を示します。

```
Device# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
---------
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/012
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

次に、**show monitor session erspan-source** コマンドの出力例を示します。

```
Device# show monitor session erspan-source

Type : ERSPAN Source Session
Status : Admin Enabled
Source Ports :
RX Only : Gi1/4/33
Destination IP Address : 20.20.163.20
Destination ERSPAN ID : 110
Origin IP Address : 10.10.10.216
IPv6 Flow Label : None
```

次に、**show monitor session erspan-destination** コマンドの出力例を示します。

```
Device# show monitor session erspan-destination

Type                    : ERSPAN Destination Session
Status                  : Admin Enabled
Source IP Address       : 10.10.10.210
Source ERSPAN ID        : 40
```

show parameter-map type subscriber attribute-to-service

パラメータマップの統計を表示するには、特権 EXEC モードで **show parameter-map type subscriber attribute-to-service** コマンドを使用します。

show parameter-map type subscriber attribute-to-service {all | name *parameter-map-name***}**

構文の説明

all	すべてのパラメータマップの統計を表示します。
name *parameter-map-name*	指定したパラメータマップの統計を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

例

次に、**show parameter-map type subscriber attribute-to-service name** *parameter-map-name* コマンドの出力例を示します。

```
Device# show parameter-map type subscriber attribute-to-service name platform


Parameter-map name: platform
 Map: 10 platform-type regex "C9xxx"
  Action(s):
     10 interface-template critical
```

show platform software fed switch ip wccp

プラットフォーム依存 Web Cache Communication Protocol（WCCP）情報を表示するには、**show platform software fed switch ip wccp** 特権 EXEC コマンドを使用します。

```
show platform software fed switch{switch-number|active|standby}ip
wccp{cache-engines |interfaces |service-groups}
```

構文の説明

switch {*switch_num* | **active** | **standby**}	情報を表示するデバイス。 • *switch_num*：スイッチ ID を入力します。指定されたスイッチに関する情報を表示します。 • **active**：アクティブスイッチの情報を表示します。 • **standby**：存在する場合、スタンバイスイッチの情報を表示します。
cache-engines	WCCP キャッシュ エンジンを表示します。
interfaces	WCCP インターフェイスを表示します。
service-groups	WCCP サービス グループを表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

このコマンドは、deviceが IP サービス フィーチャ セットを実行している場合だけ使用可能です。

次に、WCCP インターフェイスを表示する例を示します。

```
デバイス# show platform software fed switch 1 ip wccp interfaces

WCCP Interface Info

=====================

**** WCCP Interface: Port-channel13 iif_id: 000000000000007c (#SG:3),  VRF: 0 Ingress
WCCP ****
port_handle:0x20000f9

List of Service Groups on this interface:
* Service group id:90 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority:
 35
Promiscuous mode (no ports).


* Service group id:70 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority:
 35
Promiscuous mode (no ports).
```

```
* Service group id:60 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority:
 35
Promiscuous mode (no ports).


**** WCCP Interface: Port-channel14 iif_id: 000000000000007e (#SG:3),  VRF: 0 Ingress
WCCP ****
port_handle:0x880000fa

List of Service Groups on this interface:
* Service group id:90 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority:
 35
Promiscuous mode (no ports).


* Service group id:70 vrf_id:0 (ref count:24)
type: Dynamic     Open service      prot: PROT_TCP    l4_type: Dest ports     priority:
 35
Promiscuous mode (no ports).
<output truncated>
```

show platform software swspan

スイッチドポートアナライザ（SPAN）情報を表示するには、特権EXECモードで **show platform software swspan** コマンドを使用します。

show platform software swspan {**switch**} {{{**F0** | **FP active**} **counters**} | **R0** | **RP active**} {**destination sess-id** *session-ID* | **source sess-id** *session-ID*}

構文の説明

switch	スイッチに関する情報を表示します。
F0	Embedded Service Processor（ESP）スロット0に関する情報を表示します。
FP	ESPに関する情報を表示します。
active	ESPまたはルートプロセッサ（RP）のアクティブインスタンスに関する情報を表示します。
counters	SWSPANメッセージカウンタを表示します。
R0	RPスロット0に関する情報を表示します。
RP	RPに関する情報を表示します。
destination sess-id *session-ID*	指定された宛先セッションに関する情報を表示します。
source sess-id *session-ID*	指定された送信元セッションに関する情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドは、Cisco IOS Release 16.1.1 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

セッション番号が存在しないか、SPAN セッションがリモート接続先セッションの場合、コマンド出力には「% Error: No Information Available」のメッセージが表示されます。

例

次に、**show platform software swspan FP active source** コマンドの出力例を示します。

```
Switch# show platform software swspan FP active source sess-id 0

Showing SPAN source detail info

Session ID : 0
Intf Type : PORT
Port dpidx : 30
PD Sess ID : 1
Session Type : Local
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 579
AOM Object Status : Done
Parent AOM object Id : 118
Parent AOM object Status : Done

Session ID : 9
Intf Type : PORT
Port dpidx : 8
PD Sess ID : 0
Session Type : Local
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 578
AOM Object Status : Done
Parent AOM object Id : 70
Parent AOM object Status : Done
```

次に、**show platform software swspan RP active destination** コマンドの出力例を示します。

```
Switch# show platform software swspan RP active destination

Showing SPAN destination table summary info

Sess-id IF-type IF-id Sess-type
--------------------------------------
1 PORT 19 Remote
```

snmp-server enable traps

deviceでネットワーク管理システム（NMS）にインフォーム要求やさまざまなトラップのSimple Network Management Protocol（SNMP）通知を送信可能にするには、グローバル コンフィギュレーション モードで **snmp-server enable traps** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps ［**auth-framework** ［**sec-violation**］ | **bridge** | **call-home** | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp** ］
no snmp-server enable traps ［**auth-framework** ［**sec-violation**］ | **bridge** | **call-home** | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp** ］

構文の説明

auth-framework	（任意）SNMP CISCO-AUTH-FRAMEWORK-MIB トラップをイネーブルにします。
sec-violation	（任意）SNMP camSecurityViolationNotif 通知をイネーブルにします。
bridge	（任意）SNMP STP ブリッジ MIB トラップをイネーブルにします。*
call-home	（任意）SNMP CISCO-CALLHOME-MIB トラップをイネーブルにします。*
cluster	（任意）SNMP クラスタ トラップをイネーブルにします。
config	（任意）SNMP 設定トラップをイネーブルにします。
config-copy	（任意）SNMP 設定コピー トラップをイネーブルにします。
config-ctid	（任意）SNMP設定CTID トラップをイネーブルにします。
copy-config	（任意）SNMPコピー設定トラップをイネーブルにします。
cpu	（任意）CPU 通知トラップをイネーブルにします。*
dot1x	（任意）SNMP dot1x トラップをイネーブルにします。*

energywise	（任意）SNMP energywise トラップをイネーブルにします。*
entity	（任意）SNMP エンティティ トラップをイネーブルにします。
envmon	（任意）SNMP 環境モニタ トラップをイネーブルにします。*
errdisable	（任意）SNMP エラーディセーブル トラップをイネーブルにします。*
event-manager	（任意）SNMP 組み込みイベント マネージャ トラップをイネーブルにします。
flash	（任意）SNMP フラッシュ通知トラップをイネーブルにします。*
fru-ctrl	（任意）エンティティ現場交換可能ユニット（FRU）制御トラップを生成します。deviceスタックでは、このトラップはスタックにおけるdeviceの挿入/取り外しを意味します。
license	（任意）ライセンス トラップをイネーブルにします。*
mac-notification	（任意）SNMP MAC 通知トラップをイネーブルにします。*
port-security	（任意）SNMP ポート セキュリティ トラップをイネーブルにします。*
power-ethernet	（任意）SNMP パワーイーサネット トラップをイネーブルにします。*
rep	（任意）SNMP レジリエント イーサネット プロトコル トラップをイネーブルにします。
snmp	（任意）SNMP トラップをイネーブルにします。*
stackwise	（任意）SNMP StackWise トラップをイネーブルにします。*
storm-control	（任意）SNMP ストーム制御トラップ パラメータをイネーブルにします。
stpx	（任意）SNMP STPX MIB トラップをイネーブルにします。*
syslog	（任意）SNMP syslog トラップをイネーブルにします。

transceiver	（任意）SNMP トランシーバ トラップをイネーブルにします。*
tty	（任意）TCP接続トラップを送信します。この設定はデフォルトでイネーブルになっています。
vlan-membership	（任意）SNMP VLAN メンバーシップ トラップをイネーブルにします。
vlancreate	（任意）SNMP VLAN作成トラップをイネーブルにします。
vlandelete	（任意）SNMP VLAN削除トラップをイネーブルにします。
vstack	（任意）SNMP スマートインストール トラップをイネーブルにします。*
vtp	（任意）VLAN トランキング プロトコル（VTP）トラップをイネーブルにします。

コマンド デフォルト

SNMP トラップの送信をディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

上記の表のアスタリスクが付いているコマンド オプションにはサブ コマンドがあります。これらのサブ コマンドの詳細については、関連コマンドの項を参照してください。

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

トラップまたは情報がサポートされている場合に、これらの送信をイネーブルにするには、**snmp-server enable traps** コマンドを使用します。

（注） **fru-ctrl, insertion** および **removal**キーワードは、コマンドラインのヘルプストリングに表示されますが、deviceでサポートされていません。**snmp-server enable informs** グローバル コンフィギュレーション コマンドは、サポートされていません。SNMP情報通知の送信をイネーブルにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと **snmp-server host** *host-addr* **informs** グローバル コンフィギュレーション コマンドを組み合わせて使用します。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、複数の SNMP トラップ タイプをイネーブルにする例を示します。

```
デバイス(config)# snmp-server enable traps cluster
デバイス(config)# snmp-server enable traps config
デバイス(config)# snmp-server enable traps vtp
```

snmp-server enable traps bridge

STP ブリッジ MIB トラップを生成するには、グローバル コンフィギュレーション モードで **snmp-server enable traps bridge** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps bridge ［**newroot**］［**topologychange**］
no snmp-server enable traps bridge ［**newroot**］［**topologychange**］

構文の説明

newroot	（任意）SNMP STP ブリッジ MIB 新規ルート トラップをイネーブルにします。
topologychange	（任意）SNMP STP ブリッジ MIB トポロジ変更トラップをイネーブルにします。

コマンド デフォルト

ブリッジ SNMP トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次の例では、NMS にブリッジ新規ルート トラップを送信する方法を示します。

```
デバイス(config)# snmp-server enable traps bridge newroot
```

snmp-server enable traps bulkstat

データ収集 MIB トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps bulkstat** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps bulkstat [**collection** | **transfer**]
no snmp-server enable traps bulkstat [**collection** | **transfer**]

構文の説明

collection	（任意）データ収集MIB収集トラップをイネーブルにします。
transfer	（任意）データ収集MIB送信トラップをイネーブルにします。

コマンド デフォルト

データ収集 MIB トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、データ収集 MIB 収集トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps bulkstat collection
```

snmp-server enable traps call-home

SNMP CISCO-CALLHOME-MIB トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps call-home** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps call-home ［**message-send-fail** | **server-fail**］
no snmp-server enable traps call-home ［**message-send-fail** | **server-fail**］

構文の説明

message-send-fail	（任意）SNMP メッセージ送信失敗トラップをイネーブルにします。
server-fail	（任意）SNMP サーバ障害トラップをイネーブルにします。

コマンド デフォルト

SNMP CISCO-CALLHOME-MIB トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP メッセージ送信失敗トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps call-home message-send-fail
```

snmp-server enable traps cef

SNMP Cisco Express Forwarding（CEF）トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps cef** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]
no snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]

構文の説明

inconsistency	（任意）SNMP CEF 矛盾トラップをイネーブルにします。
peer-fib-state-change	（任意）SNMP CEF ピア FIB ステート変更トラップをイネーブルにします。
peer-state-change	（任意）SNMP CEF ピア ステート変更トラップをイネーブルにします。
resource-failure	（任意）SNMP リソース障害トラップをイネーブルにします。

コマンド デフォルト

SNMP CEF トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP CEF 矛盾トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps cef inconsistency
```

snmp-server enable traps cpu

CPU通知をイネーブルにするには、グローバルコンフィギュレーションモードで**snmp-server enable traps cpu** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps cpu [**threshold**]

no snmp-server enable traps cpu ［**threshold**］

構文の説明

threshold	（任意）CPU しきい値通知をイネーブルにします。

コマンド デフォルト

CPU 通知の送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、CPU しきい値通知を生成する例を示します。

```
デバイス(config)# snmp-server enable traps cpu threshold
```

snmp-server enable traps envmon

SNMP 環境トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps envmon** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps envmon ［**fan**］［**shutdown**］［**status**］ ［**supply**］［**temperature**］
no snmp-server enable traps envmon ［**fan**］［**shutdown**］［**status**］ ［**supply**］［**temperature**］

構文の説明

fan	（任意）ファン トラップをイネーブルにします。
shutdown	（任意）環境シャットダウン モニタ トラップをイネーブルにします。
status	（任意）SNMP 環境ステータス変更トラップをイネーブルにします。
supply	（任意）環境電源モニタ トラップをイネーブルにします。

temperature	（任意）環境温度モニタ トラップをイネーブルにします。

コマンド デフォルト

環境 SNMP トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、ファン トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps envmon fan
```

snmp-server enable traps errdisable

エラーディセーブルのSNMP通知をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps errdisable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps errdisable ［**notification-rate** *number-of-notifications*］
no snmp-server enable traps errdisable ［**notification-rate** *number-of-notifications*］

構文の説明

notification-rate *number-of-notifications*	（任意）通知レートとして 1 分当たりの通知の数を指定します。受け入れられる値の範囲は 0 ～ 10000 です。

コマンド デフォルト

エラー ディセーブルの SNMP 通知送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、エラー ディセーブルの SNMP 通知数を 2 に設定する例を示します。

```
デバイス(config)# snmp-server enable traps errdisable notification-rate 2
```

snmp-server enable traps flash

SNMP フラッシュ通知をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps flash** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps flash ［**insertion**］［**removal**］
no snmp-server enable traps flash ［**insertion**］［**removal**］

構文の説明		
	insertion	（任意）SNMP フラッシュ挿入通知をイネーブルにします。
	removal	（任意）SNMP フラッシュ取り出し通知をイネーブルにします。

コマンド デフォルト

SNMP フラッシュ通知の送信はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

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

使用上のガイドライン **snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP フラッシュ挿入通知を生成する例を示します。

```
デバイス(config)# snmp-server enable traps flash insertion
```

snmp-server enable traps isis

Intermediate System-to-Intermediate System（IS-IS）リンクステート ルーティング プロトコル トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps isis** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps isis ［**errors** | **state-change**］
no snmp-server enable traps isis ［**errors** | **state-change**］

構文の説明

errors	（任意）IS-IS エラー トラップをイネーブルにします。
state-change	（任意）IS-IS ステート変更トラップをイネーブルにします。

コマンド デフォルト IS-IS のトラップ送信はディセーブルになります。

コマンド モード グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン **snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、IS-IS エラー トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps isis errors
```

snmp-server enable traps license

ライセンストラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps license** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps license [**deploy**] [**error**] [**usage**]
no snmp-server enable traps license [**deploy**] [**error**] [**usage**]

構文の説明

deploy	（任意）ライセンス導入トラップをイネーブルにします。
error	（任意）ライセンスエラートラップをイネーブルにします。
usage	（任意）ライセンス使用トラップをイネーブルにします。

コマンド デフォルト

ライセンス トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、ライセンス導入トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps license deploy
```

snmp-server enable traps mac-notification

SNMP MAC 通知トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps mac-notification** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps mac-notification ［**change**］［**move**］［**threshold**］
no snmp-server enable traps mac-notification ［**change**］［**move**］［**threshold**］

構文の説明

change	（任意）SNMP MAC 変更トラップをイネーブルにします。
move	（任意）SNMP MAC 移動トラップをイネーブルにします。
threshold	（任意）SNMP MAC しきい値トラップをイネーブルにします。

コマンド デフォルト

SNMP MAC 通知トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP MAC 通知変更トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps mac-notification change
```

snmp-server enable traps ospf

SNMP の Open Shortest Path First（OSPF）トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps ospf** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time max-number-of-traps* | **retransmit** | **state-change**]
no snmp-server enable traps ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time max-number-of-traps* | **retransmit** | **state-change**]

構文の説明

cisco-specific	（任意）シスコ固有のトラップをイネーブルにします。
errors	（任意）エラー トラップをイネーブルにします。
lsa	（任意）リンクステート アドバタイズメント（LSA）トラップをイネーブルにします。
rate-limit	（任意）レート制限トラップをイネーブルにします。
rate-limit-time	（任意）レート制限トラップの時間の長さを秒数で指定します。指定できる値は 2 ～ 60 です。
max-number-of-traps	（任意）設定した時間内に送信するレート制限トラップの最大数を指定します。
retransmit	（任意）パケット再送信トラップをイネーブルにします。
state-change	（任意）状態変更トラップをイネーブルにします。

コマンド デフォルト

OSPF SNMP トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、LSA トラップをイネーブルにする例を示します。

```
デバイス(config)# snmp-server enable traps ospf lsa
```

snmp-server enable traps pim

SNMP プロトコル独立型マルチキャスト（PIM）トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps pim** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps pim ［**invalid-pim-message**］［**neighbor-change**］［**rp-mapping-change**］
no snmp-server enable traps pim
［**invalid-pim-message**］［**neighbor-change**］［**rp-mapping-change**］

構文の説明

invalid-pim-message	（任意）無効な PIM メッセージ トラップをイネーブルにします。
neighbor-change	（任意）PIM ネイバー変更トラップをイネーブルにします。
rp-mapping-change	（任意）ランデブー ポイント（RP）マッピング変更トラップをイネーブルにします。

コマンド デフォルト

PIM SNMP トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、無効な PIM メッセージ トラップをイネーブルにする例を示します。

```
デバイス(config)# snmp-server enable traps pim invalid-pim-message
```

snmp-server enable traps port-security

SNMP ポートセキュリティトラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps port-security** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps port-security ［**trap-rate** *value*］
no snmp-server enable traps port-security ［**trap-rate** *value*］

構文の説明

trap-rate *value*	（任意）1 秒間に送信するポート セキュリティ トラップの最大数を設定します。指定できる範囲は 0 ～ 1000 です。デフォルトは 0 です（制限はなく、トラップは発生するたびに送信されます）。

コマンド デフォルト

ポート セキュリティ SNMP トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、1 秒当たり 200 の速度でポート セキュリティ トラップをイネーブルにする例を示します。

```
デバイス(config)# snmp-server enable traps port-security trap-rate 200
```

snmp-server enable traps power-ethernet

SNMP の Power over Ethernet（PoE）トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps power-ethernet** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps power-ethernet {**group** *number* | **police**}
no snmp-server enable traps power-ethernet {**group** *number* | **police**}

構文の説明

group *number*	指定したグループ番号に対するインライン パワー グループベース トラップをイネーブルにします。受け入れられる値の範囲は 1 ～ 9 です。
police	インライン パワー ポリシング トラップをイネーブルにします。

コマンド デフォルト

Power over Ethernet の SNMP トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、グループ 1 の Power over Ethernet（PoE）トラップをイネーブルにする例を示します。

```
デバイス(config)# snmp-server enable traps poower-over-ethernet group 1
```

snmp-server enable traps snmp

SNMP トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps snmp** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps snmp ［**authentication** ］［**coldstart** ］［**linkdown** ］［**linkup** ］［**warmstart**］
no snmp-server enable traps snmp ［**authentication** ］［**coldstart** ］［**linkdown** ］［**linkup** ］［**warmstart**］

構文の説明

authentication	（任意）認証トラップをイネーブルにします。
coldstart	（任意）コールドスタート トラップをイネーブルにします。
linkdown	（任意）リンクダウン トラップをイネーブルにします。
linkup	（任意）リンクアップ トラップをイネーブルにします。
warmstart	（任意）ウォームスタート トラップをイネーブルにします。

コマンド デフォルト

SNMP トラップの送信をディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、ウォーム スタートの SNMP トラップをイネーブルにする例を示します。

```
デバイス(config)# snmp-server enable traps snmp warmstart
```

snmp-server enable traps stackwise

SNMP StackWise トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps stackwise** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps stackwise [**GLS**] [**ILS**] [**SRLS**]
[**insufficient-power**] [**invalid-input-current**]
[**invalid-output-current**] [**member-removed**] [**member-upgrade-notification**]
[**new-master**] [**new-member**] [**port-change**] [**power-budget-warning**] [**power-invalid-topology**]
[**power-link-status-changed**] [**power-oper-status-changed**]
[**power-priority-conflict**] [**power-version-mismatch**] [**ring-redundant**]
[**stack-mismatch**] [**unbalanced-power-supplies**] [**under-budget**] [**under-voltage**]
no snmp-server enable traps stackwise [**GLS**] [**ILS**] [**SRLS**]
[**insufficient-power**] [**invalid-input-current**]
[**invalid-output-current**] [**member-removed**] [**member-upgrade-notification**]
[**new-master**] [**new-member**] [**port-change**] [**power-budget-warning**] [**power-invalid-topology**]
[**power-link-status-changed**] [**power-oper-status-changed**]
[**power-priority-conflict**] [**power-version-mismatch**] [**ring-redundant**]
[**stack-mismatch**] [**unbalanced-power-supplies**] [**under-budget**] [**under-voltage**]

構文の説明

GLS	（任意）StackWise スタック電源 GLS トラップをイネーブルにします。
ILS	（任意）StackWise スタック電源 ILS トラップをイネーブルにします。
SRLS	（任意）StackWise スタック電源 SRLS トラップをイネーブルにします。
insufficient-power	（任意）Stackwise スタック電源の不平衡電源トラップをイネーブルにします。
invalid-input-current	（任意）Stackwise スタック電源の無効入力電流トラップをイネーブルにします。
invalid-output-current	（任意）Stackwise スタック電源の無効出力電流トラップをイネーブルにします。
member-removed	（任意）StackWise スタック メンバ削除トラップをイネーブルにします。
member-upgrade-notification	（任意）StackWise メンバのアップグレード用リロード トラップをイネーブルにします。
new-master	（任意）StackWise の新規マスター トラップをイネーブルにします。

new-member	（任意）StackWise の新規メンバ トラップをイネーブルにします。
port-change	（任意）StackWise のスタック ポート変更トラップをイネーブルにします。
power-budget-warning	（任意）StackWise スタック電源バジェット警告トラップをイネーブルにします。
power-invalid-topology	（任意）Stackwise スタック電源の無効トポロジ トラップをイネーブルにします。
power-link-status-changed	（任意）StackWise スタック電源リンク ステータス変更トラップをイネーブルにします。
power-oper-status-changed	（任意）StackWise スタック電源ポート動作ステータス変更トラップをイネーブルにします。
power-priority-conflict	（任意）StackWise スタック電源のプライオリティ競合トラップをイネーブルにします。
power-version-mismatch	（任意）StackWise スタック電源のバージョン不一致トラップをイネーブルにします。
ring-redundant	（任意）StackWise のリング冗長トラップをイネーブルにします。
stack-mismatch	（任意）StackWise スタック不一致トラップをイネーブルにします。
unbalanced-power-supplies	（任意）Stackwise スタック電源の不平衡電源トラップをイネーブルにします。
under-budget	（任意）StackWise スタック電源の不足バジェット トラップをイネーブルにします。
under-voltage	（任意）Stackwise スタック電源の不足電圧トラップをイネーブルにします。

コマンド デフォルト

SNMP StackWise トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、StackWise スタック電源の GLS トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps stackwise GLS
```

snmp-server enable traps storm-control

SNMP ストーム制御トラップパラメータをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps storm-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps storm-control {**trap-rate** *number-of-minutes*}
no snmp-server enable traps storm-control {**trap-rate**}

構文の説明

trap-rate *number-of-minutes*	（任意）SNMP ストーム制御トラップ レートを分単位で指定します。受け入れられる値の範囲は 0 ～ 1000 です。

コマンド デフォルト

SNMP ストーム制御トラップ パラメータの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP ストーム制御トラップレートを 1 分あたり 10 トラップに設定する例を示します。

```
デバイス(config)# snmp-server enable traps storm-control trap-rate 10
```

snmp-server enable traps stpx

SNMP STPX MIB トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps stpx** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps stpx [**inconsistency**] [**loop-inconsistency**] [**root-inconsistency**]
no snmp-server enable traps stpx [**inconsistency**] [**loop-inconsistency**] [**root-inconsistency**]

構文の説明

inconsistency	（任意）SNMP STPX MIB 矛盾更新トラップをイネーブルにします。
loop-inconsistency	（任意）SNMP STPX MIB ループ矛盾更新トラップをイネーブルにします。
root-inconsistency	（任意）SNMP STPX MIB ルート矛盾更新トラップをイネーブルにします。

コマンド デフォルト

SNMP STPX MIB トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP STPX MIB 矛盾更新トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps stpx inconsistency
```

snmp-server enable traps transceiver

SNMP トランシーバトラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps transceiver** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps transceiver {**all**}
no snmp-server enable traps transceiver {**all**}

構文の説明

all	（任意）すべてのSNMPトランシーバ トラップをイネーブルにします。

コマンド デフォルト

SNMP トランシーバ トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、すべての SNMP トランシーバ トラップを設定する例を示します。

```
デバイス(config)# snmp-server enable traps transceiver all
```

snmp-server enable traps vrfmib

SNMP vrfmib トラップを許可するには、グローバル コンフィギュレーション モードで **snmp-server enable traps vrfmib** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps vrfmib [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]
no snmp-server enable traps vrfmib [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]

構文の説明

vnet-trunk-down	（任意）vrfmib trunk ダウン トラップをイネーブルにします。
vnet-trunk-up	（任意）vrfmib trunk アップ トラップをイネーブルにします。
vrf-down	（任意）vrfmib vrf ダウン トラップをイネーブルにします。
vrf-up	（任意）vrfmib vrf アップ トラップをイネーブルにします。

コマンド デフォルト

SNMP vrfmib トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

この例は、vrfmib trunk ダウン トラップを生成する方法を示しています。

```
デバイス(config)# snmp-server enable traps vrfmib vnet-trunk-down
```

snmp-server enable traps vstack

SNMP スマートインストール トラップをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps vstack** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

snmp-server enable traps vstack ［**addition**］［**failure**］［**lost**］［**operation**］
no snmp-server enable traps vstack ［**addition**］［**failure**］［**lost**］［**operation**］

構文の説明

addition	（任意）クライアントによって追加されたトラップをイネーブルにします。
failure	（任意）ファイルのアップロードとダウンロード障害トラップをイネーブルにします。
lost	（任意）クライアントの損失トラップをイネーブルにします。
operation	（任意）動作モード変更トラップをイネーブルにします。

コマンド デフォルト

SNMP スマート インストール トラップの送信はディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

snmp-server host グローバル コンフィギュレーション コマンドを使用して、トラップを受信するホスト（NMS）を指定します。トラップ タイプを指定しない場合は、すべてのトラップ タイプが送信されます。

（注） SNMPv1 では、情報はサポートされていません。

複数のトラップタイプをイネーブルにするには、トラップタイプごとに **snmp-server enable traps** コマンドを個別に入力する必要があります。

例

次に、SNMP スマートインストール クライアント追加トラップを生成する例を示します。

```
デバイス(config)# snmp-server enable traps vstack addition
```

snmp-server engineID

SNMP のローカルコピーまたはリモートコピーに名前を設定するには、グローバル コンフィギュレーション モードで **snmp-server engineID** コマンドを使用します。

snmp-server engineID {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}

構文の説明

local *engineid-string*	SNMP コピーの名前に 24 文字の ID 文字列を指定します。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジン ID のうちゼロのみが続く箇所を除いた部分だけです。
remote *ip-address*	リモート SNMP コピーを指定します。SNMP のリモート コピーを含むデバイスの *ip-address* を指定します。
udp-port *port-number*	（任意）リモート デバイスのユーザ データグラム プロトコル（UDP）ポートを指定します。デフォルトは 162 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

なし

例

次の例では、ローカル エンジン ID 1234000000000000000000000 を設定します。

```
デバイス(config)# snmp-server engineID local 1234
```

snmp-server host

Simple Network Management Protocol（SNMP）通知操作の受信者（ホスト）を指定するには、deviceで **snmp-server host** グローバル コンフィギュレーション コマンドを使用します。指定したホストを削除するには、このコマンドの **no** 形式を使用します。

snmp-server host {*host-addr*} [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }
no snmp-server host {*host-addr*} [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }

構文の説明

host-addr	ホスト（ターゲットとなる受信側）の名前またはインターネットアドレスです。
vrf *vrf-instance*	（任意）仮想プライベートネットワーク（VPN）ルーティングインスタンスとこのホストの名前を指定します。
informs | **traps**	（任意）このホストに SNMP トラップまたは情報を送信します。
version 1 | **2c** | **3**	（任意）トラップの送信に使用する SNMP のバージョンを指定します。 **1**：SNMPv1。情報の場合は、このオプションを使用できません。 **2c**：SNMPv2C。 **3**：SNMPv3。認証キーワードの 1 つ（次の表の行を参照）が、バージョン 3 キーワードに従っている必要があります。
auth | **noauth** | **priv**	**auth**（任意）：Message Digest 5（MD5）およびセキュア ハッシュ アルゴリズム（SHA）パケット認証をイネーブルにします。 **noauth**（デフォルト）：noAuthNoPriv セキュリティ レベル。**auth** | **noauth** | **priv** キーワードの選択が指定されていない場合、これがデフォルトとなります。 **priv**（任意）：データ暗号規格（DES）によるパケット暗号化（「プライバシー」ともいう）をイネーブルにします。
community-string	通知処理にともなって送信される、パスワードと類似したコミュニティ ストリングです。**snmp-server host** コマンドを使用してこのストリングを設定できますが、このストリングを定義するには、**snmp-server community** グローバル コンフィギュレーション コマンドを使用してから、**snmp-server host** コマンドを使用することを推奨します。 （注） コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティ ストリングの一部として @ 記号を使用しないでください。

notification-type （任意）ホストに送信される通知のタイプです。タイプが指定されていない場合、すべての通知が送信されます。通知タイプには、次のキーワードの 1 つまたは複数を指定できます。

- **auth-framework**：SNMP CISCO-AUTH-FRAMEWORK-MIB トラップを送信します。
- **bridge**：SNMP スパニング ツリー プロトコル（STP）ブリッジ MIB トラップを送信します。
- **bulkstat**：データ収集 MIB 収集通知トラップを送信します。
- **call-home**：SNMP CISCO-CALLHOME-MIB トラップを送信します。
- **cef**：SNMP CEF トラップを送信します。
- **config**：SNMP 設定トラップを送信します。
- **config-copy**：SNMP config-copy トラップを送信します。
- **config-ctid**：SNMP config-ctid トラップを送信します。
- **copy-config**：SNMP コピー設定トラップを送信します。
- **cpu**：CPU 通知トラップを送信します。
- **cpu threshold**：CPU しきい値通知トラップを送信します。
- **entity**：SNMP エントリ トラップを送信します。

- **envmon**：環境モニタ トラップを送信します。
- **errdisable**：SNMP errdisable 通知トラップを送信します。
- **event-manager**：SNMP Embedded Event Manager トラップを送信します。
- **flash**：SNMP FLASH 通知を送信します。
- **flowmon**：SNMP flowmon 通知トラップを送信します。
- **ipmulticast**：SNMP IP マルチキャスト ルーティング トラップを送信します。
- **ipsla**：SNMP IP SLA トラップを送信します。
- **license**：ライセンス トラップを送信します。
- **local-auth**：SNMP ローカル認証トラップを送信します。
- **mac-notification**：SNMP MAC 通知トラップを送信します。
- **pim**：SNMP プロトコル独立型マルチキャスト（PIM）トラップを送信します。
- **power-ethernet**：SNMP パワー イーサネット トラップを送信します。
- **snmp**：SNMP タイプ トラップを送信します。
- **storm-control**：SNMP ストーム制御トラップを送信します。
- **stpx**：SNMP STP 拡張 MIB トラップを送信します。
- **syslog**：SNMP syslog トラップを送信します。
- **transceiver**：SNMP トランシーバ トラップを送信します。
- **tty**：TCP 接続トラップを送信します。
- **vlan-membership**：SNMP VLAN メンバーシップ トラップを送信します。
- **vlancreate**：SNMP VLAN 作成のトラップを送信します。
- **vlandelete**：SNMP VLAN 削除トラップを送信します。
- **vrfmib**：SNMP vrfmib トラップを送信します。
- **vtp**：SNMP VLAN Trunking Protocol（VTP）トラップを送信します。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。通知は送信されません。

キーワードを指定しないでこのコマンドを入力した場合は、デフォルトで、すべてのトラップタイプがホストに送信されます。情報はこのホストに送信されません。

version キーワードがない場合、デフォルトはバージョン 1 になります。

バージョン 3 を選択し、認証キーワードを入力しなかった場合は、デフォルトで **noauth**（noAuthNoPriv）セキュリティレベルになります。

（注） **fru-ctrl** キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

SNMP通知は、トラップまたは情報要求として送信できます。トラップを受信しても受信側は確認応答を送信しないため、トラップは信頼できません。送信側では、トラップが受信されたかどうかを判別できません。ただし、情報要求を受信したSNMPエンティティは、SNMP応答PDUを使用してメッセージに確認応答します。送信側が応答を受信しない場合、インフォーム要求を再送信して、インフォームが目的の宛先に到達する可能性を向上できます。

ただし、情報はエージェントおよびネットワークのリソースをより多く消費します。送信と同時に破棄されるトラップと異なり、インフォーム要求は応答を受信するまで、または要求がタイムアウトになるまで、メモリ内に保持する必要があります。また、トラップの送信は1回限りですが、情報は数回にわたって再試行が可能です。再送信の回数が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因にもなります。

snmp-server host コマンドを入力しなかった場合は、通知が送信されません。SNMP 通知を送信するように device を設定するには、**snmp-server host** コマンドを少なくとも 1 つ入力する必要があります。キーワードを指定しないでこのコマンドを入力した場合、そのホストではすべてのトラップ タイプがイネーブルになります。複数のホストをイネーブルにするには、ホストごとに **snmp-server host** コマンドを個別に入力する必要があります。コマンドには複数の通知タイプをホストごとに指定できます。

ローカルユーザがリモートホストと関連付けられていない場合、device は **auth**（authNoPriv）および **priv**（authPriv）の認証レベルの情報を送信しません。

同じホストおよび同じ種類の通知（トラップまたは情報）に対して複数の **snmp-server host** コマンドを指定した場合は、後に入力されたコマンドによって前のコマンドが上書きされます。最後の **snmp-server host** コマンドだけが有効です。たとえば、ホストに **snmp-server host inform** コマンドを入力してから、同じホストに別の **snmp-server host inform** コマンドを入力した場合は、2 番目のコマンドによって最初のコマンドが置き換えられます。

snmp-server host コマンドは、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと組み合わせて使用します。グローバルに送信される SNMP 通知を指定するには、**snmp-server enable traps** コマンドを使用します。1 つのホストでほとんどの通知を受信する場合は、このホストに対して、少なくとも 1 つの **snmp-server enable traps** コマンドと **snmp-server host** コマンドをイネーブルにする必要があります。一部の通知タイプは、**snmp-server enable traps** コマンドで制御できません。たとえば、ある通知タイプは常にイネーブルですが、別の通知タイプはそれぞれ異なるコマンドによってイネーブルになります。

キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。情報をディセーブルにするには、**no snmp-server host informs** コマンドを使用してください。

例

次の例では、トラップに対して一意の SNMP コミュニティ ストリング comaccess を設定し、このストリングによる、アクセス リスト 10 を介した SNMP ポーリング アクセスを禁止します。

```
デバイス(config)# snmp-server community comaccess ro 10
デバイス(config)# snmp-server host 172.20.2.160 comaccess
デバイス(config)# access-list 10 deny any
```

次の例では、名前 myhost.cisco.com で指定されたホストに SNMP トラップを送信する方法を示します。コミュニティ ストリングは、comaccess として定義されています。

```
デバイス(config)# snmp-server enable traps
デバイス(config)# snmp-server host myhost.cisco.com comaccess snmp
```

次の例では、コミュニティストリング public を使用して、すべてのトラップをホスト myhost.cisco.com に送信するように device をイネーブルにする方法を示します。

```
デバイス(config)# snmp-server enable traps
デバイス(config)# snmp-server host myhost.cisco.com public
```

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

source（ERSPAN）

Encapsulated Remote Switched Port Analyzer（ERSPAN）送信元インターフェイスまたはVLAN、およびモニタするトラフィックの方向を設定するには、ERSPAN モニタ送信元セッション コンフィギュレーション モードで **source** 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。

source {**interface** *type number* | **vlan** *vlan-ID*}[{**,** | **-** | **both** | **rx** | **tx**}]

構文の説明

interface *type number*	インターフェイスのタイプおよび番号を指定します。
vlan *vlan-ID*	ERSPAN 送信元セッション番号と VLAN を関連付けます。有効な値は 1 ～ 4094 です。
,	（任意）別のインターフェイスを指定します。
-	（任意）インターフェイスの範囲を指定します。
both	（任意）ERSPAN の送受信トラフィックをモニタします。
rx	（任意）受信トラフィックのみモニタします。
tx	（任意）送信トラフィックのみモニタします。

コマンド デフォルト

送信元インターフェイスまたは VLAN が設定されていません。

コマンド モード ERSPAN モニタ送信元セッション コンフィギュレーション モード（config-mon-erspan-src）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン 送信元 VLAN とフィルタ VLAN を同じセッションに含めることはできません。

例

次に、ERSPAN 送信元セッションのプロパティの設定例を示します。

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# source interface fastethernet 0/1 rx
```

関連コマンド

コマンド	説明
monitor session type erspan-source	ローカルのERSPAN送信元セッションを設定します。

status syslog

プロビジョニングポリシーのステータスをsyslogに送信するには、自動展開コンフィギュレーション モードで **status syslog** 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。

status syslog
no status syslog

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 syslog デバッグは有効になっていません。

コマンド モード 自動展開コンフィギュレーション（config-auto-deploy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

例

次に、syslog デバッグ を有効にする例を示します。

```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# status syslog
```

関連コマンド

コマンド	説明
event-manager auto-deploy	EEM 自動展開プロファイルを設定します。

switchport mode access

トランキングなし、タグなしの単一VLANイーサネットインターフェイスとしてインターフェイスを設定するには、テンプレート コンフィギュレーション モードで **switchport mode access** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport mode access
no switchport mode access

構文の説明

switchport mode access	トランキングなし、タグなしの単一VLANイーサネットインターフェイスとして、インターフェイスを設定します。

コマンド デフォルト

アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。アクセス ポートは、デフォルトで、VLAN 1 のトラフィックを送受信します。

コマンド モード

テンプレート コンフィギュレーション

コマンド履歴

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

例

次に、単一 VLAN インターフェイスを設定する例を示します。

```
デバイス(config-template)# switchport mode access
```

switchport voice vlan

指定された VLAN からのすべての音声トラフィックを転送するように指定するには、テンプレート コンフィギュレーション モードで **switchport voice vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport voice vlan*vlan_id*
no switchport voice vlan

構文の説明

switchport voice vlan*vlan_id*	すべての音声トラフィックを指定されたVLAN経由で転送するように指定します。

コマンド デフォルト 1 ～ 4094 の値を指定できます。

コマンド モード テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、指定された VLAN からのすべての音声トラフィックを転送するように指定する例を示します。

```
デバイス(config-template)# switchport voice vlan 20
```

window

プロファイルプロビジョニングがトリガーされるランダム時間を設定するには、自動展開コンフィギュレーションモードで**window** 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。

window *minutes*
no window *minutes*

構文の説明

minutes	分単位の時間。有効値は1～60です。

コマンド デフォルト ポリシー プロビジョニング ウィンドウは有効になっていません。

コマンド モード 自動展開コンフィギュレーション（config-auto-deploy）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン ウィンドウ期間は、**schedule start-in** コマンドによって設定された時間に追加されます。プロファイルプロビジョニングは、指定されたスケジュールと設定されたウィンドウ期間の間のランダム時間にトリガーされます。

例

次に、ポリシープロビジョニングのランダム時間を設定する例を示します。この例では、ポリシー プロビジョニングのスケジュールされた開始時刻は 2 時間 30 分です。ウィンドウ期間を 10 分に設定すると、この時間が 2 時間 30 分に追加されます。ポリ

シープロビジョニングは、2時間30分より後の任意の時間（ただし、ウィンドウ期間として指定された10分以内）に開始されます。

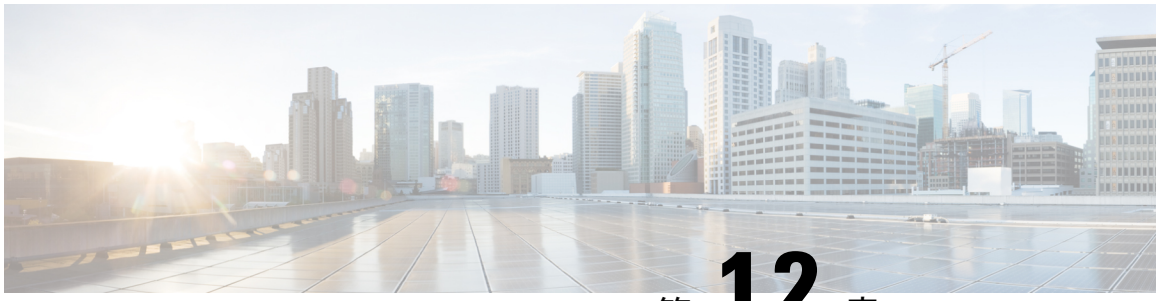
```
Device(config)# event manager auto-deploy name deploy1
Device(config-auto-deploy)# schedule start-in hours 2 minutes 30 oneshot
Device(config-auto-deploy)# window 10
```

関連コマンド

コマンド	説明
event-manager auto-deploy	EEM自動展開プロファイルを設定します。

第 IX 部

QoS



第 12 章

QoS

この章では、次の QoS コマンドについて説明します。

auto qos classify

QoS ドメイン内で信頼できないデバイスの Quality of Service（QoS）の分類を自動的に設定するには、インターフェイス コンフィギュレーション モードで **auto qos classify** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

auto qos classify [**police**]

no auto qos classify [**police**]

構文の説明

police	（任意）信頼できないデバイスのQoSポリシングを設定します。

コマンド デフォルト

auto-QoS 分類は、すべてのポートでディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

QoS ドメイン内の信頼インターフェイスに QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、device、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジ デバイスなどが含まれます。

auto-QoSがイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケット ラベルの割り当て、および入力/出力キューの設定を行います。

表 *37 :* 出力キューに対する *auto-QoS* の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キュー ウェイト（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100イーサネットポートのキュー（バッファ）サイズ
プライオリティ（シェイプド）	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

auto-QoS は、device が信頼インターフェイスと接続するように設定します。着信パケットのQoSラベルは信頼されます。非ルーテッドポートの場合は、着信パケットのCoS値が信頼されます。ルーテッドポートでは、着信パケットの DSCP 値が信頼されます。

auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。auto-QoSをイネーブルにした後で、auto-QoSを調整できます。

（注） device は、コマンドライン インターフェイス（CLI）からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、device をリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシーマップや集約ポリサーを変更しないでください。ポリシーマップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシーマップやポリサーを変更します。生成されたポリシーマップの代わりに新しいポリシーマップを使用するには、生成したポリシーマップをインターフェイスから削除して、新しいポリシーマップを適用します。

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。**debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッギングがイネーブルになります。

auto qos classify コマンドおよび **auto qos classify police** コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ（**auto qos classify police** コマンドの場合）：

- AutoQos-4.0-Classify-Police-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ：

- AutoQos-4.0-Multimedia-Conf-Class（match-any）
- AutoQos-4.0-Bulk-Data-Class（match-any）
- AutoQos-4.0-Transaction-Class（match-any）
- AutoQos-4.0-Scavanger-Class（match-any）
- AutoQos-4.0-Signaling-Class（match-any）
- AutoQos-4.0-Default-Class（match-any）
- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）

- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

ポートの auto-QoS をディセーブルにするには、**no auto qos classify** インターフェイス コンフィギュレーション コマンドを使用します。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos classify** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

例

次の例では、信頼できないデバイスの auto-QoS 分類をイネーブルにし、トラフィックをポリシングする方法を示します。

```
デバイス(config)# interface gigabitEthernet1/0/6
デバイス(config-if)# auto qos classify police
デバイス(config-if)# end
デバイス# show policy-map interface gigabitEthernet1/0/6
GigabitEthernet1/0/6

  Service-policy input: AutoQos-4.0-Classify-Police-Input-Policy

    Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp af41
      police:
          cir 5000000 bps, bc 156250 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
      0 packets
      Match: access-group name AutoQos-4.0-Acl-Bulk-Data
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp af11
      police:
          cir 10000000 bps, bc 312500 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          set-dscp-transmit dscp table policed-dscp
        conformed 0000 bps, exceed 0000 bps

    Class-map: AutoQos-4.0-Transaction-Class (match-any)
      0 packets
```

```
  Match: access-group name AutoQos-4.0-Acl-Transactional-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af21
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Scavanger-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Scavanger
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs1
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Signaling-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Signaling
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
      cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Default
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp default
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
```

```
Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
    Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
    0 packets
    Match:  dscp af41 (34) af42 (36) af43 (38)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  4
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
    0 packets
    Match:  dscp af21 (18) af22 (20) af23 (22)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  2
      0 packets, 0 bytes
      5 minute rate 0 bps
```

```
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

設定を確認するには、 **show auto qos interface** *interface-id* 特権 EXEC コマンドを入力します。

auto qos trust

QoS ドメイン内の信頼インターフェイスの Quality of Service（QoS）を自動的に設定するには、インターフェイス コンフィギュレーション モードで **auto qos trust** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

auto qos trust {**cos** | **dscp**}
no auto qos trust {**cos** | **dscp**}

構文の説明

cos	CoS パケット分類を信頼します。
dscp	DSCP パケット分類を信頼します。

コマンド デフォルト

auto-QoS 信頼は、すべてのポートでディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

QoS ドメイン内の信頼インターフェイスに QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、device、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジ デバイスなどが含まれます。auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケットラベルの割り当て、および入力/出力キューの設定を行います。

表 *38 :* トラフィックタイプ、パケットラベル、およびキュー

	VoIP データ トラフィック	VOIP コントロール トラフィック	ルーティング プロトコル トラフィック	STP[3] BPDU[4] トラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラフィック	
DSCP[5]	46	24、26	48	56	34	–	
CoS[6]	5	3	6	7	3	–	
CoS から出力キューへのマッピング	4、5（キュー 1）	2、3、6、7（キュー 2）			0（キュー 3）	2（キュー 3）	0、1（キュー 4）

[3] STP = スパニング ツリー プロトコル
[4] BPDU = ブリッジ プロトコル データ ユニット
[5] DSCP = DiffServ コードポイント

[6] CoS = サービスクラス

表 *39 :* 出力キューに対する *auto-QoS* の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キュー ウェイト（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネットポートのキュー（バッファ）サイズ
プライオリティ（シェイプド）	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

（注） device は、コマンドライン インターフェイス（CLI）からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、device をリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシーマップや集約ポリサーを変更しないでください。ポリシーマップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシーマップやポリサーを変更します。生成されたポリシーマップの代わりに新しいポリシーマップを使用するには、生成したポリシーマップをインターフェイスから削除して、新しいポリシーマップを適用します。

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。**debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッギングがイネーブルになります。

auto qos trust cos コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ：

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ：

- class-default（match-any）

- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos trust dscp コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ：

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ：

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

ポートの auto-QoS をディセーブルにするには、**no auto qos trust** インターフェイス コンフィギュレーション コマンドを使用します。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos trust** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

例

次に、特定の CoS 分類を持つ信頼できるインターフェイスの auto-QoS を有効にする方法を示します。

```
デバイス(config)# interface gigabitEthernet1/0/17
```

```
デバイス(config-if)# auto qos trust cos
デバイス(config-if)# end
デバイス# show policy-map interface GigabitEthernet1/0/17
GigabitEthernet1/0/7

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

    Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
      0 packets
      Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue-limit dscp 16 percent 80
      queue-limit dscp 24 percent 90
      queue-limit dscp 48 percent 100
      queue-limit dscp 56 percent 100

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 10%

      queue-buffers ratio 10

    Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
      0 packets
      Match:  dscp af41 (34) af42 (36) af43 (38)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  4
        0 packets, 0 bytes
        5 minute rate 0 bps
```

```
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
```

```
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

次に、特定の DSCP 分類を持つ信頼できるインターフェイスの auto-QoS を有効にする方法を示します。

```
デバイス(config)# interface GigabitEthernet1/0/18
デバイス(config-if)# auto qos trust dscp
デバイス(config-if)# end
デバイス#show policy-map interface GigabitEthernet1/0/18
GigabitEthernet1/0/18

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

    Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
      0 packets
      Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue-limit dscp 16 percent 80
      queue-limit dscp 24 percent 90
```

```
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
```

```
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

設定を確認するには、 **show auto qos interface** *interface-id* 特権 EXEC コマンドを入力します。

auto qos video

QoS ドメイン内のビデオの Quality Of Service（QoS）を自動的に設定するには、インターフェイス コンフィギュレーション モードで **auto qos video** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

auto qos video {**cts** | **ip-camera** | **media-player**}
no auto qos video {**cts** | **ip-camera** | **media-player**}

構文の説明

cts	Cisco TelePresence System に接続されるポートを指定し、自動的にビデオの QoS を設定します。
ip-camera	Cisco IP カメラに接続されるポートを指定し、自動的にビデオの QoS を設定します。
media-player	Cisco Digital Media Player に接続されるポートを指定し、自動的にビデオの QoS を設定します。

コマンド デフォルト

Auto-QoS ビデオは、ポート上でディセーブルに設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

QoS ドメイン内のビデオトラフィックに適切な QoS を設定するには、このコマンドを使用します。QoS ドメインには、device、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジ デバイスなどが含まれます。auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケットラベルの割り当て、および入力/出力キューの設定を行います。詳細については、この項の最後にあるキューテーブルを参照してください。

auto-QoS は、Cisco TelePresence システム、Cisco IP カメラ、または Cisco Digital Media Player へのビデオ接続用に device を設定します。

auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。auto-QoS をイネーブルにした後で、auto-QoS を調整できます。

device は、コマンドライン インターフェイス（CLI）からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、device をリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

これが auto-QoS をイネーブルにする最初のポートの場合は、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドに続いてインターフェイス コンフィギュレーション コマンドが実行されます。別のポートで auto-QoS をイネーブルにすると、そのポートに対して auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが実行されます。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシーマップや集約ポリサーを変更しないでください。ポリシーマップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシーマップやポリサーを変更します。生成されたポリシーマップの代わりに新しいポリシーマップを使用するには、生成したポリシーマップをインターフェイスから削除して、新しいポリシーマップを適用します。

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。**debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッギングがイネーブルになります。

auto qos video cts コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ：

- AutoQos-4.0-Trust-Cos-Input-Policy

- AutoQos-4.0-Output-Policy

クラスマップ

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos video ip-camera コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ：

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ：

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos video media-player コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ：

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ：

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

ポートの auto-QoS をディセーブルにするには、**no auto qos video** インターフェイス コンフィギュレーション コマンドを使用します。このポートに対して、auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos video** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

表 *40*：トラフィックタイプ、パケットラベル、およびキュー

	VoIP データ トラフィック	VOIP コントロール トラフィック	ルーティング プロトコル トラフィック	STP[7] BPDU[8] トラフィック	リアルタイム ビデオ トラフィック	その他すべてのトラフィック	
DSCP[9]	46	24、26	48	56	34	–	
CoS[10]	5	3	6	7	3	–	
CoS から出力キューへのマッピング	4、5（キュー 1）	2、3、6、7（キュー 2）	2、3、6、7（キュー 2）	2、3、6、7（キュー 2）	0（キュー 3）	2（キュー 3）	0、1（キュー 4）

[7] STP = スパニング ツリー プロトコル
[8] BPDU = ブリッジ プロトコル データ ユニット
[9] DSCP = DiffServ コードポイント
[10] CoS = サービスクラス

表 *41* : 出力キューに対する *auto-QoS* の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キュー ウェイト（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネットポートのキュー（バッファ）サイズ
プライオリティ（シェイプド）	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

例

次に、**auto qos video cts** コマンドと、適用されるポリシーとクラスマップの例を示します。

```
デバイス(config)# interface gigabitEthernet1/0/12
デバイス(config-if)# auto qos video cts
デバイス(config-if)# end
デバイス# show policy-map interface gigabitEthernet1/0/12
GigabitEthernet1/0/12

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1
```

```
Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10
```

```
  Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
    0 packets
    Match:  dscp cs1 (8)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
    0 packets
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

次に、**auto qos video ip-camera** コマンドと、適用されるポリシーとクラスマップの例を示します。

```
デバイス(config)# interface GigabitEthernet1/0/9
デバイス(config-if)# auto qos video ip-camera
デバイス(config-if)# end
デバイス# show policy-map interface GigabitEthernet1/0/9
GigabitEthernet1/0/9

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1
```

```
  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match:  dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
```

```
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
    0 packets
    Match:  dscp af11 (10) af12 (12) af13 (14)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  1
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 4%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
    0 packets
    Match:  dscp cs1 (8)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
    0 packets
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

次に、**auto qos video media-player** コマンドと、適用されるポリシーとクラスマップの例を示します。

```
デバイス(config)# interface GigabitEthernet1/0/7
デバイス(config-if)# auto qos video media-player
デバイス(config-if)# end
デバイス# show policy-map interface GigabitEthernet1/0/7
```

```
GigabitEthernet1/0/25

  Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp dscp table AutoQos-4.0-Trust-Dscp-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match:  dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,

      Priority Level: 1

    Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
      0 packets
      Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  3
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue-limit dscp 16 percent 80
      queue-limit dscp 24 percent 90
      queue-limit dscp 48 percent 100
      queue-limit dscp 56 percent 100

      (total drops) 0
      (bytes output) 0
      bandwidth remaining 10%

      queue-buffers ratio 10

    Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
      0 packets
      Match:  dscp af41 (34) af42 (36) af43 (38)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  4
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing

      (total drops) 0
```

```
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
```

```
(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25
```

設定を確認するには、 **show auto qos video interface** *interface-id* 特権 EXEC コマンドを入力します。

auto qos voip

QoS ドメイン内の Voice over IP（VoIP）の Quality of Service（QoS）を自動的に設定するには、インターフェイス コンフィギュレーション モードで **auto qos voip** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

auto qos voip {**cisco-phone** | **cisco-softphone** | **trust**}
no auto qos voip {**cisco-phone** | **cisco-softphone** | **trust**}

構文の説明

cisco-phone	Cisco IP Phone に接続されるポートを指定し、自動的にビデオの VoIP を設定します。着信パケットの QoS ラベルが信頼されるのは、IP Phone が検知される場合に限ります。
cisco-softphone	Cisco SoftPhone が動作している装置に接続されるポートを指定し、自動的にビデオの VoIP を設定します。
trust	信頼できる device に接続されるポートを指定し、自動的にビデオの VoIP を設定します。着信パケットの QoS ラベルは信頼されます。非ルーテッドポートの場合は、着信パケットの CoS 値が信頼されます。ルーテッドポートでは、着信パケットの DSCP 値が信頼されます。

コマンド デフォルト

auto-QoS は、すべてのポートでディセーブルです。

auto-QoS がイネーブルの場合は、入力パケットのラベルを使用して、トラフィックの分類、パケットラベルの割り当て、および入力/出力キューの設定を行います。

コマンド デフォルト

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

QoS ドメイン内の VoIP トラフィックに適切な QoS を設定する場合は、このコマンドを使用します。QoS ドメインには、device、ネットワーク内部、QoS の着信トラフィックを分類することのできるエッジ デバイスなどが含まれます。

Auto-QoS は、device とルーテッド ポート上の Cisco IP Phone を使用した VoIP と、Cisco SoftPhone アプリケーションが動作する装置に対して device を設定します。これらのリリースは Cisco IP

SoftPhone バージョン 1.3(3)以降だけをサポートします。接続される装置は Cisco Call Manager バージョン 4 以降を使用する必要があります。

auto-QoS のデフォルトを利用するには、auto-QoS をイネーブルにしてから、その他の QoS コマンドを設定する必要があります。auto-QoS をイネーブルにした後で、auto-QoS を調整できます。

（注） device は、コマンドライン インターフェイス（CLI）からコマンドが入力された場合と同じように、auto-QoS によって生成されたコマンドを適用します。既存のユーザ設定では、生成されたコマンドの適用に失敗することがあります。また、生成されたコマンドで既存の設定が上書きされることもあります。これらのアクションは、警告を表示せずに実行されます。生成されたコマンドがすべて正常に適用された場合、上書きされなかったユーザ入力の設定は実行コンフィギュレーション内に残ります。上書きされたユーザ入力の設定は、現在の設定をメモリに保存せずに、device をリロードすると復元できます。生成されたコマンドの適用に失敗した場合は、前の実行コンフィギュレーションが復元されます。

これが auto-QoS をイネーブルにする最初のポートの場合は、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドに続いてインターフェイス コンフィギュレーション コマンドが実行されます。別のポートで auto-QoS をイネーブルにすると、そのポートに対して auto-QoS によって生成されたインターフェイス コンフィギュレーション コマンドだけが実行されます。

Cisco IP Phone に接続されたネットワークエッジのポートで **auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力すると、device により信頼境界の機能が有効になります。device は、Cisco Discovery Protocol（CDP）を使用して、Cisco IP Phone の存在を検出します。Cisco IP Phone が検出されると、ポートの入力分類は、パケットで受け取った QoS ラベルを信頼するように設定されます。また、device はポリシングを使用してパケットがプロファイル内か、プロファイル外かを判断し、パケットに対するアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、device は DSCP 値を 0 に変更します。Cisco IP Phone が存在しない場合、ポートの入力分類は、パケットで受け取った QoS ラベルを信頼しないように設定されます。ポリシングがポリシーマップ分類と一致したトラフィックに適用された後で、deviceが信頼境界の機能をイネーブルにします。

-
- Cisco SoftPhone が動作するデバイスに接続されたネットワーク エッジにあるポートに **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを入力した場合、device はポリシングを使用してパケットがプロファイル内かプロファイル外かを判断し、パケットに対するアクションを指定します。パケットに 24、26、または 46 という DSCP 値がない場合、またはパケットがプロファイル外にある場合、device は DSCP 値を 0 に変更します。
- ネットワーク内部に接続されたポート上で **auto qos voip trust** インターフェイス コンフィギュレーション コマンドを入力すると、非ルーテッド ポートの場合は入力パケット内の CoS 値、ルーテッド ポートの場合は入力パケット内の DSCP 値が device で信頼されます

（前提条件は、トラフィックがすでに他のエッジデバイスによって分類されていることです）。

スタティックポート、ダイナミックアクセスポート、音声 VLAN アクセスポート、およびトランクポートで auto-QoS をイネーブルにすることができます。ルーテッドポートで Cisco IP Phone の自動 QoS を有効にすると、スタティック IP アドレスを IP Phone に割り当てます。

（注） Cisco SoftPhone が稼働するデバイスが device またはルーテッドポートに接続されている場合、device はポートごとに 1 つの Cisco SoftPhone アプリケーションだけをサポートします。

auto-QoS をイネーブルにした後、名前に *AutoQoS* を含むポリシーマップや集約ポリサーを変更しないでください。ポリシーマップや集約ポリサーを変更する必要がある場合、そのコピーを作成し、コピーしたポリシーマップやポリサーを変更します。生成されたポリシーマップの代わりに新しいポリシーマップを使用するには、生成したポリシーマップをインターフェイスから削除して、新しいポリシーマップを適用します。

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。**debug auto qos** 特権 EXEC コマンドを使用すると、auto-QoS のデバッギングがイネーブルになります。

auto qos voip trust コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ：

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ：

- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos voip cisco-softphone コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ：

- AutoQos-4.0-CiscoSoftPhone-Input-Policy
- AutoQos-4.0-Output-Policy

クラスマップ：

- AutoQos-4.0-Voip-Data-Class（match-any）
- AutoQos-4.0-Voip-Signal-Class（match-any）
- AutoQos-4.0-Multimedia-Conf-Class（match-any）
- AutoQos-4.0-Bulk-Data-Class（match-any）
- AutoQos-4.0-Transaction-Class（match-any）
- AutoQos-4.0-Scavanger-Class（match-any）
- AutoQos-4.0-Signaling-Class（match-any）
- AutoQos-4.0-Default-Class（match-any）
- class-default（match-any）
- AutoQos-4.0-Output-Priority-Queue（match-any）
- AutoQos-4.0-Output-Control-Mgmt-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Conf-Queue（match-any）
- AutoQos-4.0-Output-Trans-Data-Queue（match-any）
- AutoQos-4.0-Output-Bulk-Data-Queue（match-any）
- AutoQos-4.0-Output-Scavenger-Queue（match-any）
- AutoQos-4.0-Output-Multimedia-Strm-Queue（match-any）

auto qos voip cisco-phone コマンドを実行する場合、次のポリシーマップおよびクラスマップが作成され、適用されます。

ポリシーマップ：

- service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
- service-policy output AutoQos-4.0-Output-Policy

クラスマップ：

- class AutoQos-4.0-Voip-Data-CiscoPhone-Class
- class AutoQos-4.0-Voip-Signal-CiscoPhone-Class
- class AutoQos-4.0-Default-Class

ポートの auto-QoS をディセーブルにするには、**no auto qos voip** インターフェイス コンフィギュレーション コマンドを使用します。このポートに対して、auto-QoS によって生成された

インターフェイス コンフィギュレーション コマンドだけが削除されます。auto-QoS をイネーブルにした最後のポートで、**no auto qos voip** コマンドを入力すると、auto-QoS によって生成されたグローバル コンフィギュレーション コマンドが残っている場合でも、auto-QoS はディセーブルと見なされます（グローバル コンフィギュレーションによって影響を受ける他のポートでのトラフィックの中断を避けるため）。

device は、このテーブルの設定にしたがってポートの出力キューを設定します。

表 *42* : 出力キューに対する *auto-QoS* の設定

出力キュー	キュー番号	CoS からキューへのマッピング	キュー ウェイト（帯域幅）	ギガビット対応ポートのキュー（バッファ）サイズ	10/100 イーサネット ポートのキュー（バッファ）サイズ
プライオリティ（シェイプド）	1	4、5	最大 100%	25%	15%
SRR 共有	2	2、3、6、7	10%	25%	25%
SRR 共有	3	0	60%	25%	40%
SRR 共有	4	1	20%	25%	20%

例

次に、**auto qos voip trust** コマンドと、適用されるポリシーとクラスマップの例を示します。

```
デバイス(config)# interface gigabitEthernet1/0/31
デバイス(config-if)# auto qos voip trust
デバイス(config-if)# end
デバイス# show policy-map interface GigabitEthernet1/0/31
GigabitEthernet1/0/31

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
      priority level 1

      (total drops) 0
      (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
```

```
  Match:  dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
```

```
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

次に、**auto qos voip cisco-phone** コマンドと、適用されるポリシーとクラスマップの例を示します。

```
デバイス(config)# interface gigabitEthernet1/0/5
デバイス(config-if)# auto qos voip cisco-phone
デバイス(config-if)# end
デバイス# show policy-map interface gigabitEthernet1/0/5
GigabitEthernet1/0/5

  Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

    Class-map: AutoQos-4.0-Voip-Data-CiscoPhone-Class (match-any)
      0 packets
      Match: cos  5
```

```
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp ef
    police:
        cir 128000 bps, bc 8000 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
      conformed 0000 bps, exceed 0000 bps

  Class-map: AutoQos-4.0-Voip-Signal-CiscoPhone-Class (match-any)
    0 packets
    Match: cos  3
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp cs3
    police:
        cir 32000 bps, bc 8000 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
      conformed 0000 bps, exceed 0000 bps

  Class-map: AutoQos-4.0-Default-Class (match-any)
    0 packets
    Match: access-group name AutoQos-4.0-Acl-Default
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp default

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
    Match:  dscp cs4 (32) cs5 (40) ef (46)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Match: cos  5
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

  Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
    0 packets
```

```
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
```

```
    0 packets
    Match:  dscp cs1 (8)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

  Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
    0 packets
    Match:  dscp af31 (26) af32 (28) af33 (30)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps
    Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25
```

次に、**auto qos voip cisco-softphone** コマンドと、適用されるポリシーとクラスマップの例を示します。

```
デバイス(config)# interface gigabitEthernet1/0/20
デバイス(config-if)# auto qos voip cisco-softphone
デバイス(config-if)# end
デバイス# show policy-map interface gigabitEthernet1/0/20
GigabitEthernet1/0/21

  Service-policy input: AutoQos-4.0-CiscoSoftPhone-Input-Policy

    Class-map: AutoQos-4.0-Voip-Data-Class (match-any)
      0 packets
      Match:  dscp ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos  5
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp ef
      police:
          cir 128000 bps, bc 8000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
```

```
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Voip-Signal-Class (match-any)
  0 packets
  Match:  dscp cs3 (24)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
      cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af41
  police:
      cir 5000000 bps, bc 156250 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Bulk-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af11
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Transaction-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Transactional-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af21
  police:
      cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
```

```
      conformed 0000 bps, exceed 0000 bps

  Class-map: AutoQos-4.0-Scavanger-Class (match-any)
    0 packets
    Match: access-group name AutoQos-4.0-Acl-Scavanger
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp cs1
    police:
        cir 10000000 bps, bc 312500 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        drop
      conformed 0000 bps, exceed 0000 bps

  Class-map: AutoQos-4.0-Signaling-Class (match-any)
    0 packets
    Match: access-group name AutoQos-4.0-Acl-Signaling
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp cs3
    police:
        cir 32000 bps, bc 8000 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        drop
      conformed 0000 bps, exceed 0000 bps

  Class-map: AutoQos-4.0-Default-Class (match-any)
    0 packets
    Match: access-group name AutoQos-4.0-Acl-Default
      0 packets, 0 bytes
      5 minute rate 0 bps
    QoS Set
      dscp default
    police:
        cir 10000000 bps, bc 312500 bytes
      conformed 0 bytes; actions:
        transmit
      exceeded 0 bytes; actions:
        set-dscp-transmit dscp table policed-dscp
      conformed 0000 bps, exceed 0000 bps

  Class-map: class-default (match-any)
    0 packets
    Match: any
      0 packets, 0 bytes
      5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 0
    (bytes output) 0

  Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
    0 packets
```

```
  Match:  dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match:  dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match:  dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match:  dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos  2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match:  dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
```

```
    5 minute rate 0 bps
  Match: cos  1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match:  dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match:  dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

設定を確認するには、 **show auto qos interface** *interface-id* 特権 EXEC コマンドを入力します。

class

指定されたクラスマップ名のトラフィックを分類する一致基準を定義するには、ポリシーマップ コンフィギュレーション モードで **class** コマンドを使用します。既存のクラス マップを削除する場合は、このコマンドの **no** 形式を使用します。

class {*class-map-name* | **class-default**}

no class {*class-map-name* | **class-default**}

構文の説明

class-map-name	クラスマップ名。
class-default	分類されていないパケットに一致するシステムのデフォルトクラスを参照します。

コマンド デフォルト

ポリシーマップクラスマップは定義されていません。

コマンド モード

ポリシー マップ コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

class コマンドを使用する前に、**policy-map** グローバル コンフィギュレーション コマンドを使用してポリシー マップを識別し、ポリシーマップ コンフィギュレーション モードを開始する必要があります。ポリシーマップを指定すると、ポリシーマップ内で新規クラスのポリシーを設定したり、既存クラスのポリシーを変更したりすることができます。**service-policy** インターフェイス コンフィギュレーション コマンドを使用して、ポリシーマップをポートへ添付することができます。

class コマンドを入力すると、ポリシーマップ クラス コンフィギュレーション モードが開始されます。使用できるコンフィギュレーション コマンドは、次のとおりです。

- **admit**：コールアドミッション制御（CAC）の要求を許可します。
- **bandwidth**：クラスに割り当てられる帯域幅を指定します。
- **exit**：ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシー マップ コンフィギュレーション モードに戻ります。
- **no**：コマンドをデフォルト設定に戻します。
- **police**：分類したトラフィックにポリサーまたは集約ポリサーを定義します。ポリサーは、帯域幅の限度およびその限度を超過した場合に実行するアクションを指定します。このコマンドの詳細については、Cisco.com で入手可能な『*Cisco IOS Quality of Service Solutions Command Reference*』を参照してください。
- **priority**：ポリシーマップに属するトラフィックのクラスにスケジューリング プライオリティを割り当てます。
- **queue-buffers**：クラスのキューバッファを設定します。
- **queue-limit**：ポリシーマップに設定されたクラスポリシー用にキューが保持できる最大パケット数を指定します。
- **service-policy**：QoS サービスポリシーを設定します。

- **set**：分類したトラフィックに割り当てる値を指定します。詳細については、set（613 ページ）を参照してください。
- **shape**：平均またはピーク レート トラフィック シェーピングを指定します。このコマンドの詳細については、Cisco.com で入手可能な『*Cisco IOS Quality of Service Solutions Command Reference*』を参照してください。

ポリシーマップ コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

class コマンドは、**class-map** グローバル コンフィギュレーション コマンドと同じ機能を実行します。他のポートと共有していない新しい分類が必要な場合は、**class** コマンドを使用します。多数のポート間でマップを共有する場合には、**class-map** コマンドを使用します。

class class-default ポリシーマップ コンフィギュレーション コマンドを使用して、デフォルト クラスを設定できます。分類されていないトラフィック（トラフィック クラスで指定された一致基準を満たさないトラフィック）は、デフォルト トラフィックとして処理されます。

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

例

次に、policy1 という名前のポリシーマップを作成する例を示します。このコマンドが入力方向に添付された場合、class1 で定義されたすべての着信トラフィックの照合を行い、IP DiffServ コード ポイント（DSCP）を 10 に設定し、平均レート 1 Mb/s、バースト 20 KB のトラフィックをポリシングします。プロファイルを超えるトラフィックは、ポリシング設定 DSCP マップから取得した DSCP 値がマークされてから送信されます。

```
デバイス(config)# policy-map policy1
デバイス(config-pmap)# class class1
デバイス(config-pmap-c)# set dscp 10
デバイス(config-pmap-c)# police 1000000 20000 conform-action
デバイス(config-pmap-c)# police 1000000 20000 exceed-action
デバイス(config-pmap-c)# exit
```

次に、ポリシーマップにデフォルトのトラフィック クラスを設定する例を示します。また、**class-default** が最初に設定された場合でも、デフォルトのトラフィック クラスをポリシーマップ pm3 の終わりに自動的に配置する方法も示します。

```
デバイス# configure terminal
デバイス(config)# class-map cm-3
デバイス(config-cmap)# match ip dscp 30
デバイス(config-cmap)# exit

デバイス(config)# class-map cm-4
デバイス(config-cmap)# match ip dscp 40
デバイス(config-cmap)# exit

デバイス(config)# policy-map pm3
デバイス(config-pmap)# class class-default
デバイス(config-pmap-c)# set dscp 10
デバイス(config-pmap-c)# exit
```

```
デバイス(config-pmap)# class cm-3
デバイス(config-pmap-c)# set dscp 4
デバイス(config-pmap-c)# exit

デバイス(config-pmap)# class cm-4
デバイス(config-pmap-c)# set precedence 5
デバイス(config-pmap-c)# exit
デバイス(config-pmap)# exit

デバイス# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class cm-4
    set precedence 5
  Class class-default
    set dscp af11
```

class-map

名前を指定したクラスとパケットの照合に使用するクラスマップを作成し、クラスマップ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **class-map** コマンドを使用します。既存のクラスマップを削除し、グローバル コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

class-map *class-map name* {**match-any** | **match-all**}
no class-map *class-map name* {**match-any** | **match-all**}

構文の説明

match-any	（任意）このクラスマップ内の一致ステートメントの論理和をとります。1つ以上の条件が一致していなければなりません。
match-all	（任意）このクラスマップ内の一致ステートメントの論理積をとります。すべての条件に一致する必要があります。
class-map-name	クラスマップ名。

コマンド デフォルト

クラスマップは定義されていません。

コマンド モード

グローバル コンフィギュレーション

ポリシー マップ コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

クラスマップ一致基準を作成または変更するクラスの名前を指定し、クラス マップ コンフィギュレーション モードを開始する場合は、このコマンドを使用します。

ポートごとに適用される、グローバルに名前が付けられたサービスポリシーの一部として、パケットの分類、マーキング、および集約ポリシングを定義する場合は、**class-map** コマンドおよびそのサブコマンドを使用します。

Quality of Service（QoS）クラスマップ コンフィギュレーション モードでは、次のコンフィギュレーション コマンドを利用することができます。

- **description**：クラスマップを説明します（最大 200 文字）。**show class-map** 特権 EXEC コマンドは、クラスマップの説明と名前を表示します。
- **exit**：QoS クラスマップ コンフィギュレーション モードを終了します。
- **match**：分類基準を設定します。
- **no**：クラスマップから一致ステートメントを削除します。

match-any キーワードを入力した場合、**match access-group** クラスマップ コンフィギュレーション コマンドで名前付き拡張アクセスコントロールリスト（ACL）を指定するためにのみ使用できます。

物理ポート単位でパケット分類を定義するために、クラスマップごとに 1 つの **match** コマンドのみがサポートされています。

ACL には複数のアクセス コントロール エントリ（ACE）を含めることができます。

例

次に、クラスマップ class1 に 1 つの一致基準（アクセス リスト 103）を設定する例を示します。

```
Device(config)# access-list 103 permit ip any any dscp 10
Device(config)# class-map class1
Device(config-cmap)# match access-group 103
Device(config-cmap)# exit
```

次に、クラスマップ class1 を削除する例を示します。

```
Device(config)# no class-map class1
```

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

debug auto qos

Automatic Quality of Service（auto-QoS; 自動 QoS）機能のデバッグをイネーブルにするには、特権 EXEC モードで **debug auto qos** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

debug auto qos

no debug auto qos

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

auto-QoS デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

auto-QoS がイネーブルのときに自動的に生成される QoS の設定を表示するには、auto-QoS をイネーブルにする前にデバッグをイネーブルにします。デバッグをイネーブルにするには、**debug auto qos** 特権 EXEC コマンドを入力します。

undebug auto qos コマンドは **no debug auto qos** コマンドと同じです。

あるdevice スタック上でデバッグをイネーブルにした場合、アクティブdevice でのみイネーブルになります。スタック メンバのデバッグをイネーブルにする場合は、**session** *switch-number* 特権EXECコマンドでアクティブ deviceからセッションを開始してください。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバ device のデバッグをイネーブルにするには、アクティブ device上で **remote command** *stack-member-number LINE* 特権 EXEC コマンドを使用することもできます。

例

次の例では、auto-QoS がイネーブルの場合に自動的に生成される QoS 設定を表示する方法を示します。

```
デバイス# debug auto qos
AutoQoS debugging is on
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# auto qos voip cisco-phone
```

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 3.3SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**class-map** *class-map-name*、**cos** *cos-value*、**qos-group** *qos-group-value*、および **vlan** *vlan-id* キーワードが追加されました。

リリース	変更内容
Cisco IOS XE Everest 16.6.1	**class-map** *class-map-name* キーワードは削除されました。 **mpls** *experimental-value*、**non-client-nrt**、**protocol** *protocol-name*、および **wlan** *wlan-id* キーワードが追加されました。

使用上のガイドライン

パケットを分類するために着信パケットのどのフィールドを調べるのかを指定する場合は、**match** コマンドを使用します。IP アクセス グループまたは MAC アクセス グループの Ether Type/Len のマッチングだけがサポートされています。

class-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 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 3.3SE	このコマンドが導入されました。

使用上のガイドライン なし

次に、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
```

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン **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。

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

Kb/s	（任意）プライオリティ トラフィック向けの保証帯域幅（キロビット/秒（kbps））。帯域幅の量は、使用中のインターフェイスとプラットフォームによって異なります。保証帯域幅を超えると、非プライオリティ トラフィックがなくならないようにするため、プライオリティ トラフィックが輻輳のイベントでドロップされます。値は 1 ～ 2,000,000 kbps である必要があります。

burst -in-bytes	（任意）バイト単位のバースト サイズ。バースト サイズは、トラフィックの一時的なバーストに対応するネットワークを設定します。デフォルトバースト値は、設定されている帯域幅レートで、200 ミリ秒のトラフィックとして計算され、burst引数が指定されていない場合に使用されます。バーストの範囲は 32 ～ 2000000 バイトです。
level *level-value*	（任意）プライオリティ レベルを割り当てます。*level-value* の有効値は 1 と 2 です。レベル 1 はレベル 2 よりもプライオリティが高くなります。レベル 1 は帯域幅を予約して最初に送信を行うため、遅延は非常に低くなります。
percent *percentage*	（任意）保証帯域幅の量が、使用可能な帯域幅の割合（%）によって指定されることを、指定します。

コマンド デフォルト

プライオリティは設定されません。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	*Kbps*、*burst -in-bytes*、および **percent** *percentage* キーワードが追加されました。

使用上のガイドライン

priority コマンドを使用すると、（User Datagram Ports（UDP）ポートだけではなく）さまざまな基準に基づいてクラスと設定し、プライオリティを割り当てることができます。これは、シリアル インターフェイスと相手先固定接続（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
```

queue-buffers ratio

クラスのキュー バッファを設定するには、ポリシーマップ クラス コンフィギュレーション モードで **queue-buffers ratio** コマンドを使用します。比率制限を削除するには、このコマンドの **no** 形式を使用します。

queue-buffers ratio *ratio limit*
no queue-buffers ratio *ratio limit*

構文の説明

ratio limit	（任意）クラスのキュー バッファを設定します。キュー バッファの比率制限（0 ～ 100）を入力します。

コマンド デフォルト

クラスのキュー バッファは定義されていません。

コマンド モード

ポリシーマップ クラス コンフィギュレーション（config-pmap-c）

コマンド履歴

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

使用上のガイドライン

このコマンドを使用する前に、**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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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
```

service-policy（有線）

物理ポートまたはスイッチ仮想インターフェイス（SVI）にポリシーマップを適用するには、インターフェイス コンフィギュレーション モードで **service-policy** コマンドを使用します。ポリシーマップとポートの対応付けを削除するには、このコマンドの **no** 形式を使用します。

service-policy {**input** | **output**} *policy-map-name*
no service-policy {**input** | **output**} *policy-map-name*

構文の説明

input *policy-map-name*	物理ポートまたはSVIの入力に、指定したポリシーマップを適用します。
output *policy-map-name*	物理ポートまたはSVIの出力に、指定したポリシーマップを適用します。

コマンド デフォルト

ポートにポリシーマップは適用されていません。

コマンド モード

WLAN インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

ポリシーマップは、**policy map** コマンドによって定義されます。

1 つのポートごとに入力と出力に関して 1 つのポリシーマップだけがサポートされます。つまり、いずれのポートにおいても、1 つの入力ポリシーと 1 つの出力ポリシーだけを使用できます。

ポリシー マップは、物理ポートまたは SVI 上の着信トラフィックに適用できます。『*QoS Configuration Guide (Catalyst 3650 Switches)*』

（注） **history** キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。このキーワードが収集した統計情報は無視します。

例

次の例では、物理入力ポートに plcmap1 を適用する方法を示します。

```
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# service-policy input plcmap1
```

次の例では、物理ポートから plcmap2 を削除する方法を示します。

```
デバイス(config)# interface gigabitethernet2/0/2
```

```
デバイス(config-if)# no service-policy input plcmap2
```

次の例では、VLANのポリサー設定を表示します。この設定の最後に、QoSのインターフェイスに VLAN ポリシーマップを適用します。

```
デバイス# configure terminal
デバイス(config)# class-map vlan100
デバイス(config-cmap)# match vlan 100
デバイス(config-cmap)# exit
デバイス(config)# policy-map vlan100
デバイス(config-pmap)# policy-map class vlan100
デバイス(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
デバイス(config-pmap-c-police)# end
デバイス# configure terminal
デバイス(config)# interface gigabitEthernet1/0/5
デバイス(config-if)#  service-policy input vlan100
```

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

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**
set cos
{*cos-value*} | {**cos** | **dscp** | **precedence** | **qos-group**} [{**table** *table-map-name*}]
set dscp
{*dscp-value*} | {**cos** | **dscp** | **precedence** | **qos-group**} [{**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*}]}

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。 • （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。 • （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。

コマンド デフォルト

トラフィックの分類は定義されていません。

コマンド モード

ポリシー マップ クラス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。
Cisco IOS XE 3.3SE	**cos**、**dscp**、**qos-group**、**wlantable** *table-map-name* の各キーワードが追加されました。

使用上のガイドライン

set dscp *dscp-value* コマンド、**set cos** *cos-value* コマンド、および **set ip precedence** *precedence-value* コマンドの場合は、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。

show auto qos

automatic QoS（auto-QoS）が有効になっているインターフェイスに入力された Quality of Service（QoS）コマンドを表示するには、特権 EXEC モードで **show auto qos** コマンドを使用します。

show auto qos [**interface** [*interface-id*]]

構文の説明

interface [*interface-id*]	（任意）指定されたポートまたはすべてのポートの auto-QoS 情報を表示します。有効なインターフェイスには、物理ポートが含まれます。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

show auto qos コマンド出力には、各インターフェイスに入力された **auto qos** コマンドだけが表示されます。**show auto qos interface** *interface-id* コマンド出力には、特定のインターフェイス上に入力された **auto qos** コマンドが表示されます。

auto-QoS設定およびユーザ変更を表示する場合は、**show running-config** 特権EXECコマンドを使用します。

Cisco IOS リリース 12.2(40)SE 以降、**show auto qos** コマンドの出力には、Cisco IP Phone のサービスポリシー情報が表示されます。

例

次の例では、**auto qos voip cisco-phone** および **auto qos voip cisco-softphone** インターフェイス コンフィギュレーション コマンドを入力した場合の **show auto qos** コマンドの出力を示します。

```
デバイス# show auto qos
GigabitEthernet2/0/4
auto qos voip cisco-softphone

GigabitEthernet2/0/5
auto qos voip cisco-phone


GigabitEthernet2/0/6
auto qos voip cisco-phone
```

次に、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドが入力された場合の **show auto qos interface** *interface-id* コマンドの出力例を示します。

```
デバイス# show auto qos interface gigabitethernet 2/0/5
GigabitEthernet2/0/5
auto qos voip cisco-phone
```

次に、**auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドが入力された場合の **show auto qos interface** *interface-id* コマンドの出力例を示します。

```
デバイス# show auto qos interface gigabitethernet1/0/2
GigabitEthernet1/0/2
auto qos voip cisco-phone
```

次の例では、auto-QoS がインターフェイスでディセーブルになっている場合の **show auto qos interface** *interface-id* コマンドの出力を示します。

```
デバイス# show auto qos interface gigabitethernet3/0/1
AutoQoS is disabled
```

show class-map

トラフィックを分類するための一致基準を定義するサービス品質（QoS）クラスマップを表示するには、**show class-map** コマンドを EXEC モードで使用します。

show class-map [*class-map-name* | **type control subscriber** {**all** | *class-map-name*}]

構文の説明

class-map-name	（任意）クラス マップ名。
type control subscriber	（任意）コントロール クラス マップに関する情報を表示します。
all	（任意）すべてのコントロールクラスマップに関する情報を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

例

次に、**show class-map** コマンドの出力例を示します。

```
デバイス# show class-map
 Class Map match-any videowizard_10-10-10-10 (id 2)
   Match access-group name videowizard_10-10-10-10

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-any dscp5 (id 3)
   Match ip dscp 5
```

show platform hardware fed switch

デバイス固有のハードウェア情報を表示するには、**show platform hardware fed switch***switch_number* コマンドを使用します。

このトピックでは、QoS 特有のオプション、つまり **show platform hardware fed switch** {*switch_num* | **active** | **standby** } **qos** コマンドで使用可能なオプションのみについて詳しく説明します。

show platform hardware fed switch {*switch_num* | **active** | **standby**} **qos** {**afd** | {**config type***type* | [{**asic** *asic_num*}] | **stats clients** {**all** | **bssid** *id* | **wlanid***id*}} | **dscp-cos counters** {**iifd_id** *id* | **interface***typenumber*} | **le-info** | {**iifd_id***id* | **interface** *typenumber*} | **policer config** {**iifd_id** *id* | **interface** *type number*} | **queue** | {**config** | {**iifd_id** *id* | **interface** *type number* | **internal port-type***type*{**asic** *number*[{**port_num**}]}} | **label2qmap** | [{**aqmrepqostbl** | **iqslabeltable** | **sqslabeltable**}] | {**asic***number*} | **stats** | {**iifd_id***id* | **interface** *typenumber* | **internal** {**cpu policer** | **port-type** *type***asic** *number*}{**asic***number*[{**port_num**}]}}} | **resource**}

構文の説明

switch {*switch_num* | **active** | **standby** }	情報を表示するスイッチ。次の選択肢があります。 • *switch_num*：スイッチの ID。 • **active**：アクティブなスイッチに関する情報を表示します。 • **standby**：存在する場合、スタンバイスイッチに関する情報を表示します。
qos	QoS ハードウェア情報を表示します。次のオプションの中から選択する必要があります。 • **afd** ：ハードウェアの Approximate Fair Drop（AFD）の情報を表示します。 • **dscp-cos**：各ポートの DSCP-COS カウンタの情報を表示します。 • **leinfo**：論理エンティティ情報を表示します。 • **policer**：ハードウェアの QoS ポリサー情報を表示します。 • **queue**：ハードウェアのキュー情報を表示します。 • **resource**：ハードウェアのリソース情報を表示します。
afd {**config type** | **stats client** }	**config type** または **stats client** のオプションから選択する必要があります。 **config type**: • **client**：ワイヤレス クライアント情報を表示します。 • **port**：ポート固有の情報を表示します。 • **radio**：ワイヤレス無線情報を表示します。 • **ssid**：ワイヤレス SSID 情報を表示します。 **stats client** : • **all**：すべてのクライアントの統計を表示します。 • **bssid**：有効な範囲は 1 ～ 4294967295 です。 • **wlanid**：有効な範囲は 1 ～ 4294967295 です。

asic*asic_num*	（任意）ASIC 番号。有効な範囲は 0 ～ 255 です。
dscp-cos counters { **iifd_id** *id* | **interface** *type number* }	ポートごとの DSCP-COS カウンタを表示します。**dscp-cos counters** の次のオプションから選択する必要があります。 • **iif_id** *id*：ターゲット インターフェイスの ID です。有効な範囲は 1 ～ 4294967295 です。 • **interface** *type number*：ターゲットインターフェイスのタイプおよび ID です。
leinfo	**dscp-cos counters** の次のオプションから選択する必要があります。 • **iif_id** *id*：ターゲット インターフェイスの ID です。有効な範囲は 1 ～ 4294967295 です。 • **interface** *type number*：ターゲットインターフェイスのタイプおよび ID です。
policer config	ハードウェアのポリサーに関連する設定情報を表示します。次のオプションの中から選択する必要があります。 • **iif_id** *id*：ターゲット インターフェイスの ID です。有効な範囲は 1 ～ 4294967295 です。 • **interface** *type number*：ターゲットインターフェイスのタイプおよび ID です。

queue {**config** {**iif_id** *id* | **interface** *type number* | **internal**} | **label2qmap** | **stats**}	ハードウェアのキュー情報を表示します。次のオプションの中から選択する必要があります。 • **config**：設定情報です。次のオプションの中から選択する必要があります。 • **iif_id** *id*：ターゲット インターフェイスの ID です。有効な範囲は 1 ～ 4294967295 です。 • **interface** *type number*：ターゲットインターフェイスのタイプおよび ID です。 • **internal**：内部キューの関連情報を表示します。 • **label2qmap**：キューマッピング情報にハードウェア ラベルを表示します。次のオプションの中から選択できます。 • （任意）**aqmrepqostbl**：AQM REP QoS ラベルテーブルのルックアップ。 • （任意）**iqslabeltable**：IQS QoS ラベルテーブルのルックアップ。 • （任意）**sqslabeltable**：SQS およびローカル QoS ラベルテーブルのルックアップ。 • **stats**：キューの統計情報を表示します。次のオプションの中から選択する必要があります。 • **iif_id** *id*：ターゲット インターフェイスの ID です。有効な範囲は 1 ～ 4294967295 です。 • **interface** *type number*：ターゲットインターフェイスのタイプおよび ID です。 • **internal** {**cpu policer** | **port_type** *port_type* **asic** *asic_num* [**port_num** *port_num*] }：内部キューの関連情報を表示します。
resource	ハードウェア リソースの使用情報を表示します。次のキーワードを入力する必要があります。 **usage**

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
	このコマンドが導入されました。

次に、**show platform hardware fed switch***switch_number***qos queue stats internal cpu policer** コマンドの出力例を示します。

```
デバイス#show platform hardware fed switch 3 qos queue stats internal cpu policer

                                                    (default)  (set)
QId PlcIdx  Queue Name                 Enabled       Rate     Rate       Drop
----------------------------------------------------------------------------
0    11     DOT1X Auth                  No          1000      1000          0
1    1      L2 Control                  No          500       500           0
2    14     Forus traffic               No          1000      1000          0
3    0      ICMP GEN                    Yes         200       200           0
4    2      Routing Control             Yes         1800      1800          0
5    14     Forus Address resolution    No          1000      1000          0
6    3      ICMP Redirect               No          500       500           0
7    6      WLESS PRI-5                 No          1000      1000          0
8    4      WLESS PRI-1                 No          1000      1000          0
9    5      WLESS PRI-2                 No          1000      1000          0
10   6      WLESS PRI-3                 No          1000      1000          0
11   6      WLESS PRI-4                 No          1000      1000          0
12   0      BROADCAST                   Yes         200       200           0
13   10     Learning cache ovfl         Yes         100       100           0
14   13     Sw forwarding               Yes         1000      1000          0
15   8      Topology Control            No          13000     13000         0
16   12     Proto Snooping              No          500       500           0
17   16     DHCP Snooping               No          1000      1000          0
18   9      Transit Traffic             Yes         500       500           0
19   10     RPF Failed                  Yes         100       100           0
20   15     MCAST END STATION           Yes         2000      2000          0
21   13     LOGGING                     Yes         1000      1000          0
22   7      Punt Webauth                No          1000      1000          0
23   10     Crypto Control              Yes         100       100           0
24   10     Exception                   Yes         100       100           0
25   3      General Punt                No          500       500           0
26   10     NFL SAMPLED DATA            Yes         100       100           0
27   2      SGT Cache Full              Yes         1800      1800          0
28   10     EGR Exception               Yes         100       100           0
29   16     Show frwd                   No          1000      1000          0
30   9      MCAST Data                  Yes         500       500           0
31   10     Gold Pkt                    Yes         100       100           0
```

show policy-map

着信トラフィックの分類基準を定義するサービス品質（QoS）のポリシーマップを表示するには、EXEC モードで **show policy-map** コマンドを使用します。

show policy-map [{*policy-map-name* | **interface** *interface-id*}]

show policy-map interface {**Auto-template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Lspvif** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan** | **brief** | **class** | **input** | **output**

構文の説明

policy-map-name	（任意）ポリシーマップの名前。

interface *interface-id*	（任意）インターフェイスに適用された入力ポリシーと出力ポリシーの統計情報と設定を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

ポリシーマップには、帯域幅制限および制限を超過した場合の対処法を指定するポリサーを格納できます。

（注） **control-plane**、**session**、および **type** キーワードは、コマンドラインのヘルプ ストリングには表示されますが、サポートされていません。表示されている統計情報は無視してください。

次に、**show policy-map interface** コマンドの出力例を示します。

```
デバイス# show policy-map interface gigabitethernet1/0/48GigabitEthernet1/0/48

  Service-policy output: port_shape_parent

    Class-map: class-default (match-any)
      191509734 packets
      Match: any
      Queueing

      (total drops) 524940551420
      (bytes output) 14937264500
      shape (average) cir 250000000, bc 2500000, be 2500000
      target shape rate 250000000

      Service-policy : child_trip_play

        queue stats for all priority classes:
          Queueing
          priority level 1

          (total drops) 524940551420
          (bytes output) 14937180648

        queue stats for all priority classes:
          Queueing
          priority level 2

          (total drops) 0
          (bytes output) 0

        Class-map: dscp56 (match-any)
```

```
191508445 packets
Match:  dscp cs7 (56)
  0 packets, 0 bytes
  5 minute rate 0 bps
Priority: Strict,

Priority Level: 1
police:
    cir 10 %
    cir 25000000 bps, bc 781250 bytes
  conformed 0 bytes; actions: >>>>>counters not supported
    transmit
  exceeded 0 bytes; actions:
    drop
  conformed 0000 bps, exceeded 0000 bps  >>>>>counters not supported
```

show tech-support qos

テクニカルサポートに使用する Quality of Service（QoS）関連の情報を表示するには、特権 EXEC モードで **show tech-support qos** コマンドを使用します。

show tech-support qos [{**switch** {*switch-number* | **active** | **all** | **standby**} |[{**control-plane** | **interface** { *interface-name* | **all**}}]}]

構文の説明

switch *switch-number*	（任意）特定のスイッチのQoS関連情報を表示します。
active	（任意）スイッチのアクティブインスタンスのQoS関連情報を表示します。
all	（任意）スイッチのすべてのインスタンスのQoS関連情報を表示します。
standby	（任意）スイッチのスタンバイインスタンスのQoS関連情報を表示します。
control-plane	（任意）コントロールプレーンのQoS関連情報を表示します。
interface *interface-name*	（任意）指定したインターフェイスのQoS関連情報を表示します。
all	（任意）すべてのインターフェイスのQoS関連情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support qos | redirect flash:***filename*）。

show tech-support qos コマンドの出力には、一連のコマンドとその出力が表示されます。これらのコマンドは、プラットフォームによって異なります。

例

次に、**show tech-support qos** コマンドの出力例を示します。

```
Device# show tech-support qos
.
.
.
------------------ show platform software fed switch 1 qos policy target brief
------------------


TCG summary for policy: system-cpp-policy

Loc Interface              IIF-ID           Dir tccg Child #m/p/q  State:(cfg,opr)
--- ---------------------- ---------------- --- ---- ----- ------- ---------------
?:255 Control Plane        0x00000001000001 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4da31c8
?:0 CoPP-Queue-0           0x0000000100000d OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4da41e8
?:0 CoPP-Queue-1           0x0000000100000e OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4dbede8
?:0 CoPP-Queue-2           0x0000000100000f OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4dc2df8
?:0 CoPP-Queue-3           0x00000001000010 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4dc6e08
?:0 CoPP-Queue-4           0x00000001000011 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4dcae18
?:0 CoPP-Queue-5           0x00000001000012 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4dcee28
?:0 CoPP-Queue-6           0x00000001000013 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4dd2e38
?:0 CoPP-Queue-7           0x00000001000014 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4dd6e48
?:0 CoPP-Queue-8           0x00000001000015 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4ddae58
?:0 CoPP-Queue-9           0x00000001000016 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4ddee68
?:0 CoPP-Queue-10          0x00000001000017 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4de2e78
?:0 CoPP-Queue-11          0x00000001000018 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4de6e88
?:0 CoPP-Queue-12          0x00000001000019 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4deae98
?:0 CoPP-Queue-13          0x0000000100001a OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4deeea8
?:0 CoPP-Queue-14          0x0000000100001b OUT   22     0 0/17/0  VALID,SET_INHW
```

```
0xffe4df2eb8
?:0 CoPP-Queue-15         0x0000000100001c OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4df6ec8
?:0 CoPP-Queue-16         0x0000000100001d OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4dfaed8
?:0 CoPP-Queue-17         0x0000000100001e OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4dfeee8
?:0 CoPP-Queue-18         0x0000000100001f OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4e02ef8
?:0 CoPP-Queue-19         0x00000001000020 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4e06f08
?:0 CoPP-Queue-20         0x00000001000021 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4e0ae88
?:0 CoPP-Queue-21         0x00000001000022 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4e0ee98
?:0 CoPP-Queue-22         0x00000001000023 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4e12ea8
?:0 CoPP-Queue-23         0x00000001000024 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4e16eb8
?:0 CoPP-Queue-24         0x00000001000025 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4e1aec8
?:0 CoPP-Queue-25         0x00000001000026 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4e1eed8
?:0 CoPP-Queue-26         0x00000001000027 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4e22ee8
?:0 CoPP-Queue-27         0x00000001000028 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4e26ef8
?:0 CoPP-Queue-28         0x00000001000029 OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4e2af08
?:0 CoPP-Queue-29         0x0000000100002a OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4e2ef18
?:0 CoPP-Queue-30         0x0000000100002b OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4e32f28
?:0 CoPP-Queue-31         0x0000000100002c OUT   22     0 0/17/0  VALID,SET_INHW
0xffe4e36f38

------------------ show platform software fed switch 1 qos policy summary
------------------


Policymap Summary: (counters)
  CGID     Clases Targets Child CfgErr InHw  OpErr Policy Name
---------- ------ ------- ----- ------ ----- ----- ------------------
15212688   22     33      0     0      33    0     system-cpp-policy
.
.
.
```

出力フィールドの意味は自明です。

trust device

インターフェイスに接続されているサポートデバイスに対する信頼を設定するには、インターフェイス コンフィギュレーション モードで **trust device** コマンドを使用します。接続デバイスに対する信頼を無効にするには、このコマンドの **no** 形式を使用します。

trust device {**cisco-phone** | **cts** | **ip-camera** | **media-player**}
no trust device {**cisco-phone** | **cts** | **ip-camera** | **media-player**}

構文の説明

cisco-phone	Cisco IP Phone を設定します。
cts	Cisco TelePresence System を設定します。
ip-camera	Video Surveillance IP カメラ（IPVSC）を設定します。
media-player	Cisco Digital Media Player（DMP）を設定します。

コマンド デフォルト

信頼はディセーブルに設定

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

trust device コマンドは、次のタイプのインターフェイスに使用します。

- **Auto**：自動テンプレート インターフェイス
- **Capwap**：Capwap トンネル インターフェイス
- **GigabitEthernet**：Gigabit Ethernet IEEE 802
- **GroupVI**：グループ仮想インターフェイス
- **Internal Interface**：内部インターフェイス
- **Loopback**：ループバック インターフェイス
- **Null**：ヌル インターフェイス
- **Port-channel**：イーサネット チャネル インターフェイス
- **TenGigabitEthernet**：10 ギガビット イーサネット
- **Tunnel**：トンネル インターフェイス
- **Vlan**：Catalyst VLAN
- **range**：**interface range** コマンド

例

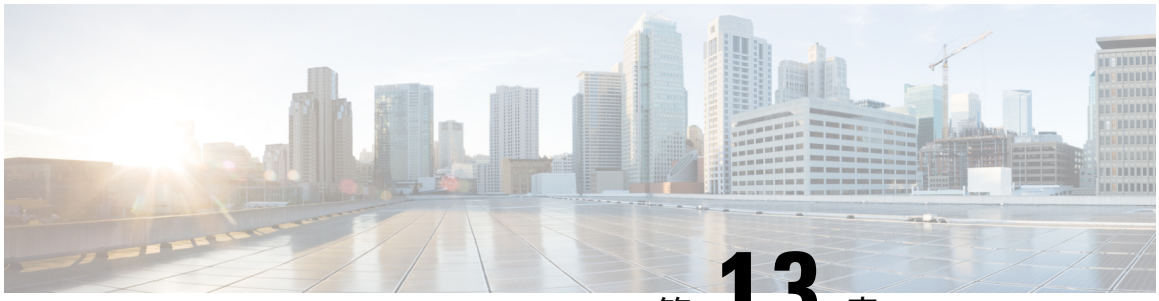
次に、インターフェイス GigabitEthernet 1/0/1 で Cisco IP Phone の信頼を設定する例を示します。

```
デバイス(config)# interface GigabitEthernet1/0/1
デバイス(config-if)# trust device cisco-phone
```

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

第 X 部

Routing



第 13 章

双方向フォワーディング検出

authentication（BFD）

シングルホップセッション用の Bidirectional Forwarding Detection（BFD）テンプレートで認証を設定するには、BFD コンフィギュレーション モードで **authentication** コマンドを使用します。シングルホップセッション用の BFD テンプレートで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。

authentication *authentication-type* **keychain** *keychain-name*
no authentication *authentication-type* **keychain** *keychain-name*

構文の説明

authentication-type	認証タイプ。有効な値は、md5、meticulous-md5、meticulous-sha1、および sha-1 です。
keychain *keychain-name*	指定された名前で認証キーチェーンを設定します。この名前の長さは最大 32 文字です。

コマンド デフォルト

シングルホップセッション用の BFD テンプレートでは認証が有効になっていません。

コマンド モード

BFD 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 Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

シングルホップテンプレートで認証を設定できます。セキュリティを強化するために認証を設定することをお勧めします。認証は、BFDの送信元と宛先のペアごとに設定する必要があり、認証パラメータは両方のデバイスで同じである必要があります。

例

次に、BFDシングルホップテンプレートのtemplate1で認証を設定する例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# bfd-template single-hop template1
デバイス(config-bfd)# authentication sha-1 keychain bfd-singlehop
```

bfd

インターフェイスに対してベースライン Bidirectional Forwarding Detection（BFD）セッションパラメータを設定するには、インターフェイス コンフィギュレーション モードで **bfd** コマンドを使用します。ベースライン BFD セッション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。

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*
no bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

構文の説明

interval *milliseconds*	BFD 制御パケットが BFD ピアに送信される速度（ミリ秒単位）を指定します。milliseconds 引数の有効範囲は 50 ～ 9999 です。
min_rx *milliseconds*	BFD 制御パケットが BFD ピアで受信されるものと期待される速度（ミリ秒単位）を指定します。milliseconds 引数の有効範囲は 50 ～ 9999 です。
multiplier *multiplier-value*	BFD ピアから連続して紛失してよい BFD 制御パケットの数を指定します。この数に達すると、BFD はそのピアが利用不可になっていることを宣言し、レイヤ 3 BFD ピアに障害が伝えられます。multiplier-value 引数の有効範囲は 3 ～ 50 です。

コマンド デフォルト

ベースライン BFD セッションパラメータの設定はありません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

bfd コマンドは、SVI、イーサネット、およびポートチャネル インターフェイスで設定できます。

BFD がポート チャネル インターフェイスで実行されている場合は、BFD には、250 * 3 ミリ秒のタイマー値制限があります。

bfd interval 設定は次のような場合には削除されません。

- IPv4 アドレスがインターフェイスから削除された場合
- IPv6 アドレスがインターフェイスから削除された場合
- IPv6 がインターフェイスからディセーブルにされた場合
- インターフェイスがシャットダウンされた場合
- インターフェイスで IPv4 CEF がグローバルまたはローカルでディセーブルにされた場合
- インターフェイスで IPv6 CEF がグローバルまたはローカルでディセーブルにされた場合

bfd interval 設定は、それを設定したサブインターフェイスが削除されたときに削除されます。

（注） インターフェイス コンフィギュレーション モードで bfd interval コマンドを設定すると、デフォルトで BFD エコー モードが有効になります。インターフェイス コンフィギュレーション モードで no ip redirect（BFD エコーが必要な場合）または no bfd echo のいずれかを有効にする必要があります。

CPU 使用率の上昇を避けるために、BFD エコー モードを使用する前に、no ip redirect コマンドを入力して、インターネット制御メッセージ プロトコル（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

次に、ギガビットイーサネット 1/0/3 の BFD セッションパラメータを設定する例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# interface gigabitethernet 1/0/3
デバイス(config-if)# bfd interval 100 min_rx 100 multiplier 3
```

bfd all-interfaces

ルーティングプロセスに参加しているすべてのインターフェイスの Bidirectional Forwarding Detection（BFD）を有効にするには、ルータ コンフィギュレーション モードまたはアドレス ファミリ インターフェイス コンフィギュレーション モードで **bfd all-interfaces** コマンドを使用します。1つのインターフェイスですべてのネイバーの BFD を無効にするには、このコマンドの **no** 形式を使用します。

bfd all-interfaces
no bfd all-interfaces

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

ルーティングプロセスに参加しているインターフェイスの BFD が無効になっています。

コマンド モード

ルータ コンフィギュレーション（config-router）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

すべてのインターフェイスの BFD を有効にするには、ルータ コンフィギュレーション モードで bfd all-interfaces コマンドを入力します。

例

次に、すべての Enhanced Interior Gateway Routing Protocol（EIGRP）ネイバーの BFD を有効にする例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# router eigrp 123
デバイス(config-router)# bfd all-interfaces
デバイス(config-router)# end
```

次に、すべての Intermediate System-to-Intermediate System（IS-IS）ネイバーの BFD を有効にする例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# router isis tag1
デバイス(config-router)# bfd all-interfaces
デバイス(config-router)# end
```

bfd check-ctrl-plane-failure

Intermediate System-to-Intermediate System（IS-IS）ルーティングプロトコルの Bidirectional Forwarding Detection（BFD）コントロールプレーン障害チェックを有効にするには、ルータ コンフィギュレーション モードで **bfd check-control-plane-failure** コマンドを使用します。コントロールプレーン障害検出を無効にするには、このコマンドの **no** 形式を使用します。

bfd check-ctrl-plane-failure
no bfd check-ctrl-plane-failure

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

BFD コントロールプレーン障害チェックが無効になっています。

コマンド モード

ルータ コンフィギュレーション（config-router）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

bfd check-ctrl-plane-failure コマンドは、IS-IS ルーティングプロセスについてのみ設定できます。このコマンドは、他のプロトコルではサポートされていません。

スイッチが再起動すると、見せかけの BFD セッション障害が発生する場合があります。このとき、隣接ルータは、転送障害が本当に発生したかのように動作します。ただし、スイッチで bfd check-control-plane-failure コマンドが有効になっていると、ルータはコントロールプレーン関連の BFD セッション障害を無視できます。ルータを再起動する予定がある場合は、直前にすべての隣接ルータの設定にこのコマンドを追加し、再起動が完了したときにすべての隣接ルータからこのコマンドを削除することをお勧めします。

例

次に、IS-IS ルーティングプロトコルの BFD コントロールプレーン障害チェックを有効にする例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# router isis
デバイス(config-router)# bfd check-ctrl-plane-failure
デバイス(config-router)# end
```

bfd echo

Bidirectional Forwarding Detection（BFD）エコーモ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 **bfd echo** コマンドを使用します。BFD エコーモードを無効にするには、このコマンドの **no** 形式を使用します。

bfd echo
no bfd echo

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

インターフェイス コンフィギュレーション モードで bfd interval コマンドを使用して BFD を設定している場合は、BFD エコー モードがデフォルトで有効になります。

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（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

エコーモードはデフォルトでイネーブルになっています。キーワードを指定せずに **no bfd echo** コマンドを入力すると、エコーパケットの送信がオフになり、スイッチがBFDネイバースイッチから受信したエコーパケットを転送しないことを示します。

エコーモードを有効にすると、必要最短エコー送信間隔と必要最短送信間隔の値が **bfd interval***milliseconds***min_rx***milliseconds* パラメータから取得されます。

（注） CPU 使用率の上昇を避けるために、BFD エコーモードを使用する前に、**no ip redirects** コマンドを入力して、インターネット制御メッセージプロトコル（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

次に、BFD ネイバー間でエコーモードを設定する例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# interface GigabitEthernet 1/0/3
デバイス(config-if)# bfd echo
```

show bfd neighbors details コマンドの次の出力は、BFD セッションネイバーが BFD エコーモードで稼働しているところを示します。この出力では、対応するコマンド出力が太字で表示されています。

```
デバイス# show bfd neighbors details
OurAddr      NeighAddr   LD/RD  RH/RS  Holdown(mult) State Int
172.16.1.2   172.16.1.1  1/6    Up     0 (3 )        Up    Fa0/1
Session state is UP and using echo function with 100 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 1
             Min tx interval: 1000000   - Min rx interval: 1000000
             Min Echo interval: 50000
```

bfd slow-timers

Bidirectional Forwarding Detection（BFD） スロータイマー値を設定するには、インターフェイス コンフィギュレーション モードで **bfd slow-timers** コマンドを使用します。BFD によって使用されるスロータイマーを変更するには、このコマンドの **no** 形式を使用します。

bfd slow-timers ［*milliseconds*］

no bfd slow-timers

コマンド デフォルト

BFD スロータイマー値は 1000 ミリ秒です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

例

次に、BFD スロータイマー値を 14,000 ミリ秒に設定する例を示します。

```
デバイス(config)# bfd slow-timers 14000
```

show bfd neighbors details コマンドの次の出力は、BFD スロータイマー値 14,000 ミリ秒が実装されているところを示します。MinTxInt および MinRxInt の値は BFD スロータイマーの設定値に対応しています。関連するコマンド出力は太字で示されています。

```
デバイス# show bfd neighbors details
OurAddr      NeighAddr   LD/RD  RH/RS  Holdown(mult) State Int
172.16.1.2   172.16.1.1  1/6    Up     0 (3 )        Up    Fa0/1
Session state is UP and using echo function with 100 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 14000, MinRxInt: 14000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3600(0), Hello (hits): 1200(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
Uptime: 00:05:00
Last packet: Version: 1            - Diagnostic: 0
             State bit: Up         - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 3         - Length: 24
             My Discr.: 6          - Your Discr.: 1
             Min tx interval: 1000000   - Min rx interval: 1000000
             Min Echo interval: 50000
```

（注）

- BFDセッションがダウンすると、BFD制御パケットがスロータイマー間隔で送信されます。
- BFDセッションが稼働している場合、エコーが有効になっていれば、BFD制御パケットがネゴシエートされたスロータイマー間隔で送信され、エコーパケットがネゴシエートされた設定済みのBFD間隔で送信されます。エコーが有効になっていない場合は、BFD制御パケットがネゴシエートされた設定済みの間隔で送信されます。

bfd template

Bidirectional Forwarding Detection（BFD）テンプレートを設定し、BFD 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 **bfd-template** コマンドを使用します。BFD テンプレートを削除するには、このコマンドの **no** 形式を使用します。

bfd template *template-name*
no bfd template *template-name*

コマンド デフォルト

BFD テンプレートはインターフェイスにバインドされません。

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 Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

bfd-template コマンドを使用してテンプレートを作成していない場合でも、インターフェイスでテンプレート名を設定できますが、テンプレートを定義するまでテンプレートは無効と見なされます。テンプレート名を再設定する必要はありません。名前は自動的に有効になります。

例

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# interface Gigabitethernet 1/3/0
デバイス(config-if)# bfd template template1
```

bfd-template single-hop

シングルホップ Bidirectional Forwarding Detection（BFD）テンプレートをインターフェイスにバインドするには、インターフェイス コンフィギュレーション モードで **bfd template** コマンドを使用します。シングルホップ BFD テンプレートをインターフェイスからアンバインドするには、このコマンドの **no** 形式を使用します。

bfd-template single-hop *template-name*
no bfd-template single-hop *template-name*

構文の説明

single-hop	シングルホップBFDテンプレートを作成します。
template-name	テンプレート名。

コマンド デフォルト

BFD テンプレートは存在しません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

bfd template コマンドを使用すると BFD テンプレートを作成し、デバイスを BFD コンフィギュレーション モードにすることができます。テンプレートは一連の BFD 間隔値を指定するために使用できます。BFD テンプレートの一部として指定される BFD 間隔値は、1 つのインターフェイスに限定されるものではありません。

例

次に、BFD テンプレートを作成し、BFD 間隔値を指定する例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# bfd-template single-hop node1
デバイス(bfd-config)#interval min-tx 100 min-rx 100 multiplier 3
デバイス(bfd-config)#echo
```

次に、BFD シングルホップテンプレートを作成し、BFD間隔値と認証キーチェーンを設定する例を示します。

```
デバイス> enable
デバイス# configuration terminal
デバイス(config)# bfd-template single-hop template1
デバイス(bfd-config)#interval min-tx 200 min-rx 200 multiplier 3
デバイス(bfd-config)#authentication keyed-sha-1 keychain bfd_singlehop
```

（注） デフォルトでは、BFDテンプレート設定でBFDエコーは有効になっていません。これは明示的に設定する必要があります。

ip route static bfd

スタティックルートの Bidirectional Forwarding Detection（BFD）ネイバーを指定するには、グローバル コンフィギュレーション モードで **ip route static bfd** コマンドを使用します。スタティックルートの BFD ネイ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。

ip route static bfd {*interface-type interface-number ip-address* | **vrf** *vrf-name*} [**group** *group-name*] **[passive] [unassociate]**
no ip route static bfd {*interface-type interface-number ip-address* | **vrf** *vrf-name*} [**group** *group-name*] **[passive] [unassociate]**

構文の説明

interface-type interface-number	インターフェイスのタイプと番号。
ip-address	A.B.C.D形式のゲートウェイの IP アドレス。

vrf *vrf-name*	Virtual Routing and Forwarding（VRF）インスタンスと宛先の vrf 名を指定します。
group *group-name*	（任意）BFD グループを割り当てます。group-name は BFD グループ名を指定する最大 32 文字の文字列です。
unassociate	（任意）BFD に設定されたスタティック ルートの関連付けを解除します。

コマンド デフォルト

スタティック ルート BFD ネイバーは指定されていません。

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 Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

スタティック ルート BFD ネイバーを指定するには、ip route static bfd コマンドを使用します。設定に指定されている同一のインターフェイスとゲートウェイを保持するスタティック ルートはすべて、到達可能性通知を得るために同一の BFD セッションを共有します。

interface-type interface-number および ip-address 引数に同じ値が指定されているスタティック ルートはすべて、自動的に BFD を使用して、ゲートウェイの到達可能性を判別し、高速障害検出を利用します。

group キーワードは BFD グループを割り当てます。スタティック BFD 設定は、インターフェイスが関連付けられている VPN ルーティングおよび転送（VRF）インスタンスに追加されます。**passive** キーワードは、グループのパッシブメンバを指定します。passive キーワードなしでグループにスタティック BFD を追加すると、BFD がグループのアクティブメンバになります。グループの BFD セッションをトリガーするために、スタティック ルートをアクティブ BFD 設定によって追跡する必要があります。特定のグループのすべてのスタティック BFD 設定（アクティブとパッシブ）を削除するには、**no ip route static bfd** コマンドを使用して、BFD グループ名を指定します。

unassociate キーワードは、BFD ネイバーがスタティック ルートに関連付けられることなく、インターフェイスに BFD が設定されている場合に BFD セッションが要求されることを指定します。これは IPv4 スタティック ルートがない BFDv4 セッションを起動するために役立ちます。unassociate キーワードを指定しない場合は、IPv4 スタティック ルートが BFD セッションに関連付けられます。

BFD では、両方のエンドポイント デバイス BFD セッションが開始されている必要があります。そのため、このコマンドは各エンドポイント デバイスで設定する必要があります。

スイッチ仮想インターフェイス（SVI）の BFD スタティック セッションは、その SVI 上で無効だった **bfd interval***milliseconds***min_rx***milliseconds***multiplier***multiplier-value* コマンドが有効化された後にのみ確立されます。

スタティック BFD セッションを有効にするには、次の手順を実行します。

1. SVI で BFD タイマーを有効にします。

   bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

2. スタティック IP ルートの BFD を有効にします。

   ip route static bfd *interface-type interface-number ip-address*

3. SVI で BFD タイマーを無効にし、再度有効にします。

   no bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

   bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

例

次に、指定したネイバー、グループおよびグループのアクティブメンバを介してすべてのスタティック ルートの BFD を設定する例を示します。

```
デバイス# configuration terminal
デバイス(config)# ip route static bfd GigabitEthernet 1/0/1 10.1.1.1 group group1
```

次に、指定したネイバー、グループおよびグループのパッシブメンバを介してすべてのスタティック ルートの BFD を設定する例を示します。

```
デバイス# configuration terminal
デバイス(config)# ip route static bfd GigabitEthernet 1/0/1 10.2.2.2 group group1 passive
```

次に、group および passive キーワードを指定せず、無関係なモードですべてのスタティック ルートの BFD を設定する例を示します。

```
デバイス# configuration terminal
デバイス(config)# ip route static bfd GigabitEthernet 1/0/1 10.2.2.2 unassociate
```

ipv6 route static bfd

スタティックルートの Bidirectional Forwarding Detection for IPv6（BFDv6）ネイバーを指定するには、グローバル コンフィギュレーション モードで **ipv6 route static bfd** コマンドを使用します。スタティックルートの BFDv6 ネイ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。

ipv6 route static bfd ［**vrf** *vrf-name*］ *interface-type interface-number ipv6-address* **[unassociated]**
no ipv6 route static bfd

構文の説明

vrf *vrf-name*	（任意）スタティック ルートを指定する必要がある Virtual Routing and Forwarding（VRF）インスタンスの名前。
interface-type interface-number	インターフェイスのタイプと番号。
ipv6-address	ネイバーの IPv6 アドレス。
unassociated	（任意）スタティック BFD ネイバーを関連付けられたモードから無関係なモードに移行します。

コマンド デフォルト

スタティック ルートの BFDv6 ネイバーは指定されていません。

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 Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

スタティック ルートのネイバーを指定するには、ipv6 route static bfd コマンドを使用します。設定に指定されている同一のインターフェイスとゲートウェイを保持するスタティック ルートはすべて、到達可能性通知を得るために同一の BFDv6 セッションを共有します。BFDv6 では、両方のエンドポイントのルータで BFDv6 セッションが開始されている必要があります。そのため、このコマンドは各エンドポイント ルータで設定する必要があります。IPv6 スタティック BFDv6 ネイバーは、インターフェイスとネイバーアドレスで完全に指定される必要があり、直接接続されている必要があります。

vrf vrf-name、interface-type interface-number および *ipv6-address* に同じ値が指定されているスタティック ルートはすべて、自動的に BFDv6 を使用して、ゲートウェイの到達可能性を判別し、高速障害検出を利用します。

例

次に、アドレスが 2001::1 のイーサネット インターフェイス 0/0 でネイバーを作成する例を示します。

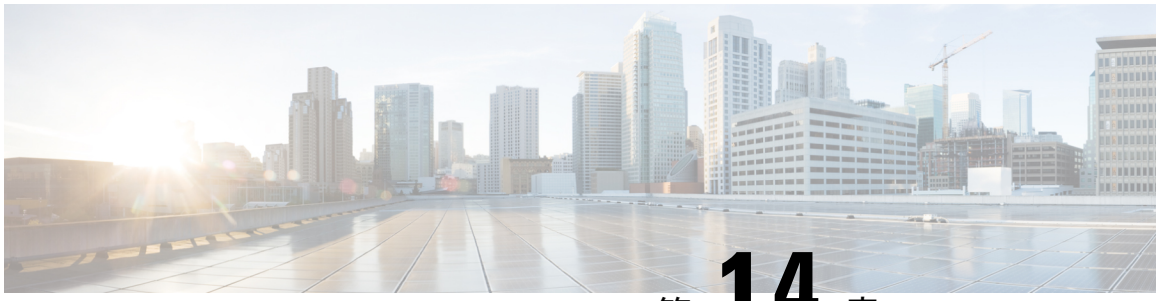
```
デバイス# configuration terminal
デバイス(config)# ipv6 route static bfd ethernet 0/0 2001::1
```

次に、ネイバーを無関係なモードに変換する例を示します。

```
デバイス# configuration terminal
デバイス(config)# ipv6 route static bfd ethernet 0/0 2001::1 unassociated
```

第 XI 部

セキュリティ



第 14 章

セキュリティ

aaa accounting

RADIUS または TACACS+ を使用する場合に、課金やセキュリティ目的で、要求されたサービスの認証、許可、およびアカウンティング（AAA）アカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting** コマンドを使用します。AAA アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accouting {**auth-proxy** | **system** | **network** | **exec** | **connections** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*
no aaa accouting {**auth-proxy** | **system** | **network** | **exec** | **connections** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*

構文の説明

auth-proxy	すべての認証済みプロキシユーザイベントに関する情報を出力します。
system	リロードなどのユーザに関連付けられていないシステムレベルのすべてのイベントのアカウンティングを実行します。

network	ネットワークに関連するあらゆるサービス要求にアカウンティングを実行します。
exec	EXEC シェルセッションのアカウンティングを実行します。このキーワードは、**autocommand** コマンドによって生成される情報などのユーザプロファイル情報を返すことができます。
connection	ネットワーク アクセス サーバから確立されたすべてのアウトバウンド接続に関する情報を提供します。
commands *level*	指定した特権レベルですべてのコマンドのアカウンティングを実行します。有効な特権レベル エントリは 0 ～ 15 の整数です。
default	この引数のあとにリストされるアカウンティング方式を、アカウンティングサービスのデフォルトリストとして使用します。
list-name	次に記載されているアカウンティング方式のうち、少なくとも 1 つを含むリストの名前を付けるために使用する文字列です：
start-stop	プロセスの開始時に "start" accounting 通知を送信し、プロセスの終了時に "stop" accounting 通知を送信します。"start" アカウンティングレコードはバックグランドで送信されます。要求されたユーザプロセスは、"start" accounting 通知がアカウンティングサーバで受信されたかどうかに関係なく開始されます。
stop-only	要求されたユーザ プロセスの終了時に、"stop" アカウンティング通知を送信します。
none	この回線またはインターフェイスでアカウンティングサービスをディセーブルにします。
broadcast	（任意）複数の AAA サーバへのアカウンティングレコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウンティングレコードを同時に送信します。最初のサーバが使用できない場合、そのグループ内で定義されたバックアップサーバを使用してフェールオーバーが発生します。
group groupname	次に記述されているキーワードの 1 つ以上を使用します： 表 43 : AAA アカウンティングの方式 （651 ページ）

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

アカウンティングを有効にし、回線別またはインターフェイス別に特定のアカウンティング方式を定義する名前付き方法リストを作成するには、**aaa accounting** コマンドを使用します。

表 *43 : AAA* アカウンティングの方式

キーワード	Description
group radius	**aaa group server radius** コマンドで定義されるすべての RADIUS サーバのリストを認証に使用します。
group tacacs+	**aaa group server tacacs+** コマンドで定義されるすべての TACACS+ サーバのリストを認証に使用します。
group *group-name*	group-name サーバグループで定義したように、アカウンティングのための RADIUS サーバまたは TACACS+ サーバのサブセットを使用します。

表 43 : AAA アカウンティングの方式 （651 ページ） では、**group radius** 方式および **group tacacs+** 方式は、以前に定義した一連の RADIUS サーバまたは TACACS+ サーバを参照します。ホストサーバを設定するには、**radius server** および **tacacs server** コマンドを使用します。特定のサーバグループを作成するには、 **aaa group server radius** および **aaa group server tacacs+** コマンドを使用します。

Cisco IOS ソフトウェアは次の 2 つのアカウンティング方式をサポートします。

- RADIUS：ネットワークアクセスサーバは、アカウンティングレコードの形式でRADIUSセキュリティサーバに対してユーザアクティビティを報告します。各アカウンティングレコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティサーバに格納されます。
- TACACS+：ネットワークアクセスサーバは、アカウンティングレコードの形式でTACACS+セキュリティサーバに対してユーザアクティビティを報告します。各アカウンティングレコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティサーバに格納されます。

アカウンティングの方式リストは、アカウンティングの実行方法を定義します。名前付きアカウンティング方式リストにより、特定の回線またはインターフェイスで、特定の種類のアカウンティングサービスに使用する特定のセキュリティプロトコルを指定できます。*list-name* および *method* を入力してリストを作成します。*list-name* にはこのリストの名前として使用する任意の文字列（radius や tacacs+ などの方式名を除く）を指定し、*method* には指定されたシーケンスで試行する方式を指定します。

特定のアカウンティングの種類の **aaa accounting** コマンドを、名前付き方式リストを指定しないで発行した場合、名前付き方式リストが明示的に定義されているものを除いて、すべてのインターフェイスまたは回線（このアカウンティングの種類が適用される）にデフォルトの方式リストが自動的に適用されます（定義済みの方式リストは、デフォルトの方式リストに優先し

ます）。デフォルトの方式リストが定義されていない場合、アカウンティングは実行されません。

（注） システムアカウンティングでは名前付きアカウンティングリストは使用されず、システムアカウンティングのためのデフォルトのリストだけを定義できます。

最小のアカウンティングの場合、**stop-only** キーワードを指定して、要求されたユーザプロセスの終了時にstopレコードアカウンティング通知を送信します。詳細なアカウンティングの場合、**start-stop** キーワードを指定することで、RADIUS または TACACS+ が要求されたプロセスの開始時に start アカウンティング通知を送信し、プロセスの終了時に stop アカウンティング通知を送信するようにできます。アカウンティングはRADIUS またはTACACS+サーバにだけ保存されます。noneキーワードは、指定した回線またはインターフェイスのアカウンティングサービスをディセーブルにします。

AAA アカウンティングがアクティブにされると、ネットワークアクセスサーバは、ユーザが実装したセキュリティ方式に応じて、接続に関係する RADIUS アカウンティング属性または TACACS+ AV ペアをモニタします。ネットワークアクセスサーバはこれらの属性をアカウンティングレコードとしてレポートし、アカウンティングレコードはその後セキュリティサーバのアカウンティングログに保存されます。サポートされるRADIUSアカウンティング属性の一覧については、『*Cisco IOS Security Configuration Guide*』の付録「RADIUS Attributes」を参照してください。サポートされるTACACS+アカウンティングのAVペアの一覧については、『*Cisco IOS Security Configuration Guide*』の付録「TACACS+ Attributes-Value Pairs」を参照してください。

（注） このコマンドは、TACACS または拡張 TACACS には使用できません。

次の例では、デフォルトのコマンドアカウンティング方式リストを定義しています。この例のアカウンティング サービスはTACACS+セキュリティ サーバによって提供され、stop-only 制限で特権レベル 15 コマンドに設定されています。

```
デバイス(config)# aaa accounting commands 15 default stop-only group TACACS+
```

次の例では、アカウンティング サービスが TACACS+ セキュリティ サーバで提供され、stop-only 制限があるデフォルトの auth-proxy アカウンティング方式リストの定義を示します。aaa accounting コマンドは認証プロキシアカウンティングをアクティブにします。

```
デバイス(config)# aaa new model
デバイス(config)# aaa authentication login default group TACACS+
デバイス(config)# aaa authorization auth-proxy default group TACACS+
デバイス(config)# aaa accounting auth-proxy default start-stop group TACACS+
```

aaa accounting dot1x

認証、認可、およびアカウンティング（AAA）アカウンティングをイネーブルにして、IEEE 802.1Xセッションの特定のアカウンティング方式を、回線単位またはインターフェイス単位で定義する方式リストを作成するには **aaa accounting dot1x** グローバル コンフィギュレーション コマンドを使用します。IEEE 802.1X アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting dot1x {*name* | **default** } **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} **. . .**] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} **. . .**]}
no aaa accounting dot1x {*name* | **default** }

構文の説明

name	サーバ グループ名。これは、**broadcast group** および **group** キーワードの後に入力する場合に使用するオプションです。
default	デフォルトリストにあるアカウンティング方式を、アカウンティングサービス用に指定します。
start-stop	プロセスの開始時に start accounting 通知を送信し、プロセスの終了時に stop accounting 通知を送信します。start アカウンティングレコードはバックグラウンドで送信されます。アカウンティング サーバが start accounting 通知を受け取ったかどうかには関係なく、要求されたユーザプロセスが開始されます。
broadcast	複数の AAA サーバに送信されるアカウンティングレコードをイネーブルにして、アカウンティングレコードを各グループの最初のサーバに送信します。最初のサーバが利用できない場合、スイッチはバックアップサーバのリストを使用して最初のサーバを識別します。
group	アカウンティングサービスに使用するサーバグループを指定します。有効なサーバグループ名は次のとおりです。 • *name*：サーバグループの名前。 • **radius** ：すべての RADIUS ホストのリスト。 • **tacacs+** ：すべての TACACS+ ホストのリスト。 **broadcast group** および **group** キーワードの後に入力する場合、**group** キーワードはオプションです。オプションの **group** キーワードより多くの値を入力できます。
radius	（任意）RADIUS アカウンティングをイネーブルにします。
tacacs+	（任意）TACACS+ アカウンティングをイネーブルにします。

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

このコマンドは、RADIUS サーバへのアクセスが必要です。

インターフェイスに IEEE 802.1X RADIUS アカウンティングを設定する前に、**dot1x reauthentication** インターフェイス コンフィギュレーション コマンドを入力することを推奨します。

次の例では、IEEE 802.1X アカウンティングを設定する方法を示します。

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

aaa accounting identity

IEEE 802.1X、MAC 認証バイパス（MAB）、および Web 認証セッションの認証、認可、およびアカウンティング（AAA）をイネーブルにするには、グローバル コンフィギュレーション モードで、**aaa accounting identity** コマンドを使用します。IEEE 802.1X アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting identity {*name* | **default** } **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} **. . .**] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} **. . .**]}
no aaa accounting identity {*name* | **default** }

構文の説明

name	サーバ グループ名。これは、**broadcast group** および **group** キーワードの後に入力する場合に使用するオプションです。
default	デフォルトリストにあるアカウンティング方式を、アカウンティングサービス用に使用します。
start-stop	プロセスの開始時に start accounting 通知を送信し、プロセスの終了時に stop accounting 通知を送信します。start アカウンティングレコードはバックグラウンドで送信されます。アカウンティングサーバが start アカウンティング通知を受け取ったかどうかには関係なく、要求されたユーザプロセスが開始されます。
broadcast	複数の AAA サーバに送信されるアカウンティングレコードをイネーブルにして、アカウンティングレコードを各グループの最初のサーバに送信します。最初のサーバが利用できない場合、スイッチはバックアップサーバのリストを使用して最初のサーバを識別します。

group	アカウンティングサービスに使用するサーバグループを指定します。有効なサーバグループ名は次のとおりです。 • *name*：サーバグループの名前。 • **radius** ：すべての RADIUS ホストのリスト。 • **tacacs+** ：すべての TACACS+ ホストのリスト。 **broadcast group** および **group** キーワードの後に入力する場合、**group** キーワードはオプションです。オプションの**group**キーワードより多くの値を入力できます。
radius	（任意）RADIUS 認証をイネーブルにします。
tacacs+	（任意）TACACS+ アカウンティングをイネーブルにします。

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

AAA アカウンティング アイデンティティをイネーブルにするには、ポリシー モードをイネーブルにする必要があります。ポリシー モードを有効にするには、特権 EXEC モードで **authentication display new-style** コマンドを入力します。

次の例では、IEEE 802.1X アカウンティング アイデンティティを設定する方法を示します。

```
デバイス# authentication display new-style

Please note that while you can revert to legacy style
configuration at any time unless you have explicitly
entered new-style configuration, the following caveats
should be carefully read and understood.

(1) If you save the config in this mode, it will be written
    to NVRAM in NEW-style config, and if you subsequently
    reload the router without reverting to legacy config and
    saving that, you will no longer be able to revert.

(2) In this and legacy mode, Webauth is not IPv6-capable. It
    will only become IPv6-capable once you have entered new-
    style config manually, or have reloaded with config saved
    in 'authentication display new' mode.

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

aaa authentication dot1x

IEEE 802.1X 認証に準拠するポートで使用する認証、認可、およびアカウンティング（AAA）方式を指定するには、スタンドアロンスイッチ上のグローバル コンフィギュレーション モードで **aaa authentication dot1x** コマンドを使用します。認証を無効にするには、このコマンドの **no** 形式を使用します。

aaa authentication dot1x {**default**} *method1*
no aaa authentication dot1x {**default**} *method1*

構文の説明

default	ユーザがログインするときのデフォルトの方法。この引数に続いてリストされた認証方式が使用されます。
method1	サーバ認証を指定します。認証用にすべての RADIUS サーバの一覧を使用するには、**group radius** キーワードを入力します。 （注） コマンドラインのヘルプストリングには他のキーワードも表示されますが、サポートされるのは **default** および **group radius** キーワードのみです。

コマンド デフォルト

認証は実行されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

method 引数には、認証アルゴリズムがクライアントからのパスワードを確認するために特定の順序で試みる方式を指定します。IEEE 802.1X に準拠している唯一の方式は、クライアントデータが RADIUS 認証サーバに対して確認される **group radius** 方式です。

group radius を指定した場合、**radius-server host** グローバル コンフィギュレーション コマンドを入力して RADIUS サーバを設定する必要があります。

設定された認証方式の一覧を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

次の例では AAA をイネーブルにして IEEE 802.1X 準拠の認証リストを作成する方法を示します。この認証は、最初に RADIUS サーバとの交信を試みます。この動作でエラーが返信された場合、ユーザはネットワークへのアクセスが許可されません。

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

aaa authorization network

IEEE 802.1x VLAN 割り当てなどのすべてのネットワーク関連サービス要求に対してユーザ RADIUS 認証を使用するようにスイッチを設定するには、グローバル コンフィギュレーション モードで **aaa authorization network** コマンドを使用します。RADIUS ユーザ認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization network default group radius
no aaa authorization network default

構文の説明

default group radius	デフォルトの認証リストとして、サーバグループ内のすべての RADIUS ホストのリストを使用します。

コマンド デフォルト

認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

スイッチが、デフォルトの認証リスト内にある RADIUS サーバから IEEE 802.1x 認証パラメータをダウンロードできるようにするには、**aaa authorization network default group radius** 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。認証パラメータは、VLAN 割り当てなど、RADIUS サーバからパラメータを取得する機能で使用されます。

設定された認証方式リストを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

この例では、すべてのネットワーク関連サービス要求に対してユーザ RADIUS 認証を行うようスイッチを設定する方法を示します。

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

aaa new-model

認証、認可、およびアカウンティング（AAA）アクセス制御モデルを有効にするには、グローバル コンフィギュレーション モードで **aaa new-model** コマンドを使用します。AAA アクセス制御モデルを無効にするには、このコマンドの **no** 形式を使用します。

aaa new-model
no aaa new-model

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

AAA が有効になっていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

このコマンドにより、AAA アクセス制御システムが有効になります。

仮想端末回線（VTY）に関して **login local** コマンドが設定されている場合で、かつ **aaa new-model** コマンドが削除されている場合は、スイッチをリロードして、デフォルト設定または **login** コマンドを取得する必要があります。スイッチをリロードしない場合、スイッチは、VTY ではデフォルトで **login local** コマンドに設定されます。

（注） **aaa new-model** コマンドを削除することは推奨されません。

次に、この制限の例を示します。

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

line vty 0 4
 login local  !<=== Login local instead of "login"
line vty 5 15
 login local
!
```

例

次に、AAA を初期化する例を示します。

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

関連コマンド

Command	Description
aaa accounting	課金またはセキュリティ目的のために、要求されたサービスの AAA アカウンティングをイネーブルにします。

Command	Description
aaa authentication arap	TACACS+ を使用する ARAP の AAA 認証方式を有効にします。
aaa authentication enable default	ユーザが特権コマンドレベルにアクセスできるかどうかを決定する AAA 認証を有効にします。
aaa authentication login	ログイン時の AAA 認証を設定します。
aaa authentication ppp	PPP を実行しているシリアルインターフェイス上で使用する 1 つまたは複数の AAA 認証方式を指定します。
aaa authorization	ネットワークへのユーザアクセスを制限するパラメータを設定します。

aaa policy interface-config allow-subinterface

認証、認可、およびアカウンティング（AAA）Link Control Protocol（LCP）インターフェイス設定ポリシーパラメータを有効にするには、グローバル コンフィギュレーション モードで **aaa policy interface-config allow-subinterface** コマンドを発行します。LCP インターフェイス設定ポリシー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。

aaa policy interface-config allow-subinterface
no aaa policy interface-config allow-subinterface

構文の説明

interface-config	LCP インターフェイス設定ポリシー パラメータを指定します。
allow-subinterface	デフォルトではフル仮想アクセス インターフェイスを作成しないことを指定します。

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 3.6.0E	このコマンドが導入されました。

使用上のガイドライン

セッションに関連付けられている仮想アクセスインターフェイスでインターフェイス コンフィギュレーション モードのコマンドを適用するには、interface-config キーワードを使用します。

例

次に、AAA LCP インターフェイス設定ポリシー パラメータを有効にする例を示します。

```
Device# configure terminal
Device(config)# aaa new-model
```

```
Device(config)# aaa policy interface-config allow-subinterface
```

関連コマンド

Command	Description
aaa new-model	AAAアクセスコントロールモデルをイネーブルにします。

authentication host-mode

ポートで認証マネージャモードを設定するには、インターフェイス コンフィギュレーション モードで **authentication host-mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

authentication host-mode {**multi-auth** | **multi-domain** | **multi-host** | **single-host**}
no authentication host-mode

構文の説明

multi-auth	ポートのマルチ認証モード（multi-auth モード）をイネーブルにします。
multi-domain	ポートのマルチドメインモードをイネーブルにします。
multi-host	ポートのマルチホストモードをイネーブルにします。
single-host	ポートのシングルホストモードをイネーブルにします。

コマンド デフォルト

シングルホストモードがイネーブルにされています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

接続されているデータホストが1つだけの場合は、シングルホストモードを設定する必要があります。シングルホストポートでの認証のために音声デバイスを接続しないでください。ポートで音声 VLAN が設定されていないと、音声デバイスの許可が失敗します。

データホストが IP フォン経由でポートに接続されている場合は、マルチドメインモードを設定する必要があります。音声デバイスを認証する必要がある場合は、マルチドメインモードを設定する必要があります。

ハブの背後にデバイスを配置し、それぞれを認証してポートアクセスのセキュリティを確保できるようにするには、マルチ認証モードに設定する必要があります。音声 VLAN が設定されている場合は、このモードで認証できる音声デバイスは 1 つだけです。

マルチホストモードでも、ハブ越しの複数ホストのためのポートアクセスが提供されますが、マルチホストモードでは、最初のユーザが認証された後でデバイスに対して無制限のポートアクセスが与えられます。

次の例では、ポートのマルチ認証モードをイネーブルにする方法を示します。

```
デバイス(config-if)# authentication host-mode multi-auth
```

次の例では、ポートのマルチドメインモードをイネーブルにする方法を示します。

```
デバイス(config-if)# authentication host-mode multi-domain
```

次の例では、ポートのマルチホストモードをイネーブルにする方法を示します。

```
デバイス(config-if)# authentication host-mode multi-host
```

次の例では、ポートのシングルホストモードをイネーブルにする方法を示します。

```
デバイス(config-if)# authentication host-mode single-host
```

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

authentication mac-move permit

device 上での MAC 移動をイネーブルにするには、グローバル コンフィギュレーション モードで **authentication mac-move permit** コマンドを使用します。MAC 移動をディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication mac-move permit
no authentication mac-move permit

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

MAC 移動は無効になっています。

コマンド モード

グローバル コンフィギュレーション

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

使用上のガイドライン

このコマンドを使用すると、device 上のポート間で認証ホストを移動できます。たとえば、認証されたホストとポートの間にデバイスがあり、そのホストが別のポートに移動した場合、認証セッションは最初のポートから削除され、ホストは新しいポート上で再認証されます。

MAC 移動がディセーブルで、認証されたホストが別のポートに移動した場合、そのホストは再認証されず、違反エラーが発生します。

次の例では、device 上で MAC 移動をイネーブルにする方法を示します。

```
デバイス(config)# authentication mac-move permit
```

authentication priority

プライオリティリストに認証方式を追加するには、インターフェイス コンフィギュレーション モードで **authentication priority** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

authentication priority ［**dot1x** | **mab**］｛**webauth**｝
no authentication priority ［**dot1x** | **mab**］｛**webauth**｝

構文の説明		
	dot1x	（任意）認証方式の順序に 802.1X を追加します。
	mab	（任意）認証方式の順序に MAC 認証バイパス（MAB）を追加します。
	webauth	認証方式の順序に Web 認証を追加します。

コマンド デフォルト

デフォルトのプライオリティは、802.1X 認証、MAC 認証バイパス、Web 認証の順です。

コマンド モード

インターフェイス コンフィギュレーション

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

使用上のガイドライン

順序付けでは、スイッチがポートに接続された新しいデバイスを認証しようとするときに試行する方式の順序を設定します。

ポートにフォールバック方式を複数設定するときは、Web 認証（webauth）を最後に設定してください。

異なる認証方式にプライオリティを割り当てることにより、プライオリティの高い方式を、プライオリティの低い進行中の認証方式に割り込ませることができます。

（注） クライアントがすでに認証されている場合に、プライオリティの高い方式の割り込みが発生すると、再認証されることがあります。

認証方式のデフォルトのプライオリティは、実行リストの順序におけるその位置と同じで、802.1X 認証、MAC 認証バイパス（MAB）、Web 認証の順です。このデフォルトの順序を変更するには、キーワード **dot1x**、**mab**、および **webauth** を使用します。

次の例では、802.1X を最初の認証方式、Web 認証を 2 番めの認証方式として設定する方法を示します。

```
デバイス(config-if)# authentication priority dotx webauth
```

次の例では、MAB を最初の認証方式、Web 認証を 2 番めの認証方式として設定する方法を示します。

```
デバイス(config-if)# authentication priority mab webauth
```

関連コマンド

コマンド	説明
authentication control-direction	ポート モードを単一方向または双方向に設定します。
authentication event fail	認証マネージャが認証エラーを認識されないユーザクレデンシャルの結果として処理する方法を指定します。
authentication event no-response action	認証マネージャが認証エラーを応答のないホストの結果として処理する方法を指定します。
authentication event server alive action reinitialize	以前に到達不能であった認証、許可、アカウンティングサーバが使用可能になったときに認証マネージャセッションを再初期化します。
authentication event server dead action authorize	認証、許可、アカウンティングサーバが到達不能になったときに認証マネージャセッションを許可します。
authentication fallback	Web 認証のフォール バック方式をイネーブルにします。

コマンド	説明
authentication host-mode	ホストの制御ポートへのアクセスを許可します。
authentication open	ポートでオープンアクセスをイネーブルにします。
authentication order	認証マネージャがポート上のクライアントの認証を試みる順序を指定します。
authentication periodic	ポートの自動再認証をイネーブルにします。
authentication port-control	制御ポートの許可ステートを設定します。
authentication timer inactivity	機能しない認証マネージャセッションを強制終了するまでの時間を設定します。
authentication timer reauthenticate	認証マネージャが許可ポートの再認証を試みる間隔を指定します。
authentication timer restart	認証マネージャが無許可ポートの認証を試みる間隔を指定します。
authentication violation	ポート上でセキュリティ違反が生じた場合に取るアクションを指定します。
mab	ポートのMAC認証バイパスをイネーブルにします。
show authentication registrations	認証マネージャに登録されている認証方式に関する情報を表示します。
show authentication sessions	現在の認証マネージャセッションに関する情報を表示します。
show authentication sessions interface	特定のインターフェイスの認証マネージャに関する情報を表示します。

authentication violation

新しいデバイスがポートに接続されたとき、または最大数のデバイスがポートに接続されている状態で新しいデバイスがポートに接続されたときに発生する違反モードを設定するには、インターフェイス コンフィギュレーション モードで **authentication violation** コマンドを使用します。

authentication violation { **protect** | **replace** | **restrict** | **shutdown** }
no authentication violation { **protect** | **replace** | **restrict** | **shutdown** }

構文の説明

protect	予期しない着信 MAC アドレスをドロップします。syslog エラーは生成されません。
replace	現在のセッションを削除し、新しいホストによる認証を開始します。
restrict	違反エラーの発生時に Syslog エラーを生成します。
shutdown	エラーによって、予期しない MAC アドレスが発生するポートまたは仮想ポートがディセーブルになります。

コマンド デフォルト

Authentication violation shutdown モードがイネーブルにされています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

ポート上でセキュリティ違反が発生したときに実行するアクションを指定するには、**authentication violation** コマンドを使用します。

次の例では、新しいデバイスがポートに接続する場合に、errdisable になり、シャットダウンするように IEEE 802.1X 対応ポートを設定する方法を示します。

```
デバイス(config-if)# authentication violation shutdown
```

次の例では、新しいデバイスがポートに接続する場合に、システムエラーメッセージを生成して、ポートを制限モードに変更するように802.1X対応ポートを設定する方法を示します。

```
デバイス(config-if)# authentication violation restrict
```

次の例では、新しいデバイスがポートに接続するときに、そのデバイスを無視するように 802.1X 対応ポートを設定する方法を示します。

```
デバイス(config-if)# authentication violation protect
```

次の例では、新しいデバイスがポートに接続するときに、現在のセッションを削除し、新しいデバイスによる認証を開始するように802.1X対応ポートを設定する方法を示します。

```
デバイス(config-if)# authentication violation replace
```

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

cisp enable

スイッチ上で Client Information Signalling Protocol（CISP）を有効にして、サプリカントスイッチのオーセンティケータとして機能し、オーセンティケータスイッチのサプリカントとして機能するようにするには、**cisp enable** グローバル コンフィギュレーション コマンドを使用します。

cisp enable
no cisp enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドはCisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされません。

使用上のガイドライン

オーセンティケータとサプリカントスイッチの間のリンクはトランクです。両方のスイッチで VTP をイネーブルにする場合は、VTP ドメイン名が同一であり、VTP モードがサーバである必要があります。

VTPモードを設定する場合にMD5チェックサムの不一致エラーにならないようにするために、次の点を確認してください。

- VLAN が異なる 2 台のスイッチに設定されていないこと。同じドメインに VTP サーバが 2 台存在することがこの状態の原因になることがあります。
- 両方のスイッチで、設定のリビジョン番号が異なっていること。

次の例では、CISP をイネーブルにする方法を示します。

```
デバイス(config)# cisp enable
```

関連コマンド

コマンド	説明
dot1x credentialsプロファイル	プロファイルをサプリカント スイッチに設定します。
dot1x supplicant force-multicast	802.1X サプリカントがマルチキャストパケットを送信するように強制します。
dot1x supplicant controlled transient	802.1X サプリカントによる制御アクセスを設定します。
show cisp	指定されたインターフェイスの CISP 情報を表示します。

clear errdisable interface vlan

error-disabled 状態になっていた VLAN を再びイネーブルにするには、特権 EXEC モードで **clear errdisable interface** コマンドを使用します。

clear errdisable interface *interface-id* **vlan** [*vlan-list*]

構文の説明

interface-id	インターフェイスを指定します。
vlan list	（任意）再びイネーブルにする VLAN のリストを指定します。VLAN リストを指定しない場合は、すべての VLAN が再びイネーブルになります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

shutdown および **no shutdown** のインターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにするか、**clear errdisable** インターフェイスコマンドを使用して VLAN の error-disabled をクリアできます。

次の例では、ギガビット イーサネット ポート 4/0/2 で errdisable になっているすべての VLAN を再びイネーブルにする方法を示します。

```
デバイス# clear errdisable interface gigabitethernet4/0/2 vlan
```

関連コマンド

コマンド	説明
errdisable detect cause	特定の原因、またはすべての原因に対して errdisable 検出をイネーブルにします。
errdisable recovery	回復メカニズム変数を設定します。
show errdisable detect	errdisable 検出ステータスを表示します。
show errdisable recovery	errdisable 回復タイマーの情報を表示します。
show interfaces status err-disabled	errdisable ステートになっているインターフェイスのリストのインターフェイス ステータスを表示します。

clear mac address-table

特定のダイナミックアドレス、特定のインターフェイス上のすべてのダイナミックアドレス、スタックメンバ上のすべてのダイナミックアドレス、または特定の VLAN 上のすべてのダイナミックアドレスを MAC アドレステーブルから削除するには、**clear mac address-table** コマンドを特権 EXEC モードで使用します。このコマンドはまた MAC アドレス通知グローバル カウンタもクリアします。

clear mac address-table {**dynamic** [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*] | **move update** | **notification**}

構文の説明

dynamic	すべてのダイナミック MAC アドレスを削除します。
address *mac-addr*	（任意）指定されたダイナミック MAC アドレスを削除します。
interface *interface-id*	（任意）指定された物理ポートまたはポートチャネル上のすべてのダイナミック MAC アドレスを削除します。
vlan *vlan-id*	（任意）指定された VLAN のすべてのダイナミック MAC アドレスを削除します。指定できる範囲は 1 ～ 4094 です。
move update	MAC アドレステーブルの move-update カウンタをクリアします。

notification	履歴テーブルの通知をクリアし、カウンタをリセットします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

情報が削除されたことを確認するには、**show mac address-table** 特権 EXEC コマンドを入力します。

次の例では、ダイナミック アドレス テーブルから特定の MAC アドレスを削除する方法を示します。

```
デバイス# clear mac address-table dynamic address 0008.0070.0007
```

関連コマンド

コマンド	説明
mac address-table notification	MAC アドレス通知機能をイネーブルにします。
mac address-table move update {**receive** | **transmit**}	スイッチ上の MAC アドレス テーブル移行更新を設定します。
show mac address-table	MAC アドレス テーブルのスタティック エントリおよびダイナミック エントリを表示します。
show mac address-table move update	スイッチに MAC アドレス テーブル移行更新情報を表示します。
show mac address-table notification	**interface** キーワードが追加されると、すべてのインターフェイスまたは指定されたインターフェイスに対する MAC アドレス通知設定を表示します。
snmp trap mac-notification change	特定のインターフェイスの SNMP MAC アドレス通知トラップをイネーブルにします。

deny（MAC アクセス リスト コンフィギュレーション）

条件が一致した場合に非 IP トラフィックが転送されるのを防止するには、スイッチスタックまたはスタンドアロンスイッチ上で **deny** MAC アクセスリスト コンフィギュレーション コマンドを使用します。名前付き MAC アクセス リストから拒否条件を削除するには、このコマンドの **no** 形式を使用します。

deny {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**] [**cos** *cos*]
no deny {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**] [**cos** *cos*]

構文の説明

any	すべての送信元または宛先MACアドレスを拒否します。
host *src-MAC-addr* | *src-MAC-addr mask*	ホスト MAC アドレスと任意のサブネット マスクを定義します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP トラフィックは拒否されます。
host *dst-MAC-addr* | *dst-MAC-addr mask*	宛先 MAC アドレスと任意のサブネット マスクを定義します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。
type mask	（任意）パケットのEtherType番号と、Ethernet IIまたはSNAPカプセル化を指定して、パケットのプロトコルを識別します。 type には、0 ～ 65535 の 16 進数を指定できます。 mask は、一致をテストする前に EtherType に適用される don’t care ビットのマスクです。
aarp	（任意）データリンク アドレスをネットワーク アドレスにマッピングする EtherType AppleTalk Address Resolution Protocol を指定します。

amber	（任意）EtherType DEC-Amber を指定します。
appletalk	（任意）EtherType AppleTalk/EtherTalk を指定します。
dec-spanning	（任意）EtherType Digital Equipment Corporation（DEC）スパニングツリーを指定します。
decnet-iv	（任意）EtherType DECnet Phase IV プロトコルを指定します。
diagnostic	（任意）EtherType DEC-Diagnostic を指定します。
dsm	（任意）EtherType DEC-DSM を指定します。
etype-6000	（任意）EtherType 0x6000 を指定します。
etype-8042	（任意）EtherType 0x8042 を指定します。
lat	（任意）EtherType DEC-LAT を指定します。
lavc-sca	（任意）EtherType DEC-LAVC-SCA を指定します。
lsap *lsap-number mask*	（任意）パケットの LSAP 番号（0 ～ 65535）と 802.2 カプセル化を使用して、パケットのプロトコルを指定します。 *mask* は、一致をテストする前に LSAP 番号に適用される don’t care ビットのマスクです。
mop-console	（任意）EtherType DEC-MOP Remote Console を指定します。
mop-dump	（任意）EtherType DEC-MOP Dump を指定します。
msdos	（任意）EtherType DEC-MSDOS を指定します。
mumps	（任意）EtherType DEC-MUMPS を指定します。
netbios	（任意）EtherType DEC-Network Basic Input/Output System（NetBIOS）を指定します。
vines-echo	（任意）Banyan Systems による EtherType Virtual Integrated Network Service（VINES）Echo を指定します。

vines-ip	（任意）EtherType VINES IP を指定します。
xns-idp	（任意）10 進数、16 進数、または 8 進数の任意の Ethertype である EtherType Xerox Network Systems（XNS）プロトコル スイート（0 ～ 65535）を指定します。
cos *cos*	（任意）プライオリティを設定するため、0 ～ 7 までのサービス クラス（CoS）値を指定します。CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。**cos** オプションが設定されているかどうかを確認する警告メッセージが表示されます。

コマンド デフォルト

このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルト アクションは拒否です。

コマンド モード

MAC アクセス リスト コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

mac access-list extended グローバル コンフィギュレーション コマンドを使用して、MAC アクセス リスト コンフィギュレーション モードを開始します。

host キーワードを使用した場合、アドレスマスクは入力できません。**host** キーワードを使用しない場合は、アドレスマスクを入力する必要があります。

アクセス コントロール エントリ（ACE）がアクセスコントロールリストに追加された場合、リストの最後には暗黙の **deny-any-any** 条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap** *lsap mask* キーワードを使用します。Novell 用語と Cisco IOS 用語での IPX カプセル化タイプに対応するフィルタ条件を表に一覧表示します。

表 *44 : IPX* フィルタ基準

IPX カプセル化タイプ		**フィルタ基準**
Cisco IOS 名	**Novel 名**	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137

IPX カプセル化タイプ		フィルタ基準
Cisco IOS 名	**Novel 名**	
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

次の例では、すべての送信元から MAC アドレス 00c0.00a0.03fa への NETBIOS トラフィックを拒否する名前付き MAC 拡張アクセス リストを定義する方法を示します。このリストに一致するトラフィックは拒否されます。

```
デバイス(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

次の例では、名前付き MAC 拡張アクセス リストから拒否条件を削除する方法を示します。

```
デバイス(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

次の例では、EtherType 0x4321 のすべてのパケットを拒否します。

```
デバイス(config-ext-macl)# deny any any 0x4321 0
```

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

関連コマンド

コマンド	説明
mac access-list extended	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
permit	MAC アクセスリスト コンフィギュレーションから許可します。 条件が一致した場合に非 IP トラフィックが転送されるのを許可します。
show access-lists	スイッチに設定されたアクセス コントロール リストを表示します。

device-role（IPv6 スヌーピング）

ポートに接続されているデバイスのロールを指定するには、IPv6 スヌーピング コンフィギュレーション モードで **device-role** コマンドを使用します。

device-role {**node** | **switch**}

構文の説明

node	接続されたデバイスのロールをノードに設定します。
switch	接続されたデバイスのロールをスイッチに設定します。

コマンド デフォルト

デバイスのロールはノードです。

コマンド モード

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

device-role コマンドは、ポートに接続されているデバイスのロールを指定します。デフォルトでは、デバイスのロールはノードです。

switch キーワードは、リモートデバイスがスイッチであり、ローカル スイッチがマルチスイッチ モードで動作していることを示します。ポートで学習したバインディング エントリは、trunk_port プリファレンス レベルでマークされます。ポートが trusted ポートに設定されている場合、バインディング エントリは trunk_trusted_port プリファレンス レベルでマークされます。

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、デバイスを IPv6 スヌーピング コンフィギュレーション モードにし、デバイスをノードとして設定する例を示します。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)# device-role node
```

device-role（IPv6 ND インスペクション）

ポートに接続されているデバイスのロールを指定するには、ネイバー探索（ND）インスペクション ポリシー コンフィギュレーション モードで **device-role** コマンドを使用します。

device-role {**host** | **switch**}

構文の説明

host	接続されたデバイスのロールをホストに設定します。
switch	接続されたデバイスのロールをスイッチに設定します。

コマンド デフォルト

デバイスのロールはホストです。

コマンド モード

ND インスペクション ポリシー コンフィギュレーション

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

使用上のガイドライン

device-role コマンドは、ポートに接続されているデバイスのロールを指定します。デフォルトでは、デバイスのロールはホストであるため、すべての着信ルータ アドバタイズメントとリダイレクト メッセージはブロックされます。

switch キーワードは、リモートデバイスがスイッチであり、ローカル スイッチがマルチスイッチ モードで動作していることを示します。ポートで学習したバインディング エントリは、trunk_port プリファレンス レベルでマークされます。ポートが trusted ポートに設定されている場合、バインディングエントリは trunk_trusted_port プリファレンス レベルでマークされます。

次に、Neighbor Discovery Protocol（NDP）ポリシー名を policy1 と定義し、デバイスを ND インスペクション ポリシー コンフィギュレーション モードにして、デバイスをホストとして設定する例を示します。

```
デバイス(config)#  ipv6 nd inspection policy policy1
デバイス(config-nd-inspection)# device-role host
```

device-tracking policy

スイッチ統合型セキュリティ機能（SISF）ベースの IP デバイス トラッキング ポリシーを設定するには、グローバル コンフィギュレーション モードで **device-tracking** コマンドを使用します。デバイス トラッキング ポリシーを削除するには、このコマンドの **no** 形式を使用します。

device -tracking policy *policy-name*
no device-tracking policy *policy-name*

構文の説明

policy-name	デバイス トラッキング ポリシーのユーザ定義名。ポリシー名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。

コマンド デフォルト

デバイス トラッキング ポリシーは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

デバイス トラッキング ポリシーを作成するには、SISF ベースの **device-tracking policy** コマンドを使用します。**device-tracking policy** コマンドがイネーブルの場合、コンフィギュレーション モードが デバイストラッキング コンフィギュレーション モードに変更されます。このモードでは、管理者が次のファーストホップ セキュリティ コマンドを設定できます。

- （任意）**device-role**{**node**] | **switch**}：ポートに接続されたデバイスの役割を指定します。デフォルトは **node** です。
- （任意）**limit address-count** *value*：ターゲットごとに許可されるアドレス数を制限します。
- （任意）**no**：コマンドを無効にするか、またはそのデフォルトに設定します。
- （任意）**destination-glean**{**recovery**| **log-only**}[**dhcp**]}：データ トラフィックの送信元アドレス グリーニングによるバインディング テーブルの回復をイネーブルにします。
- （任意）**data-glean**{**recovery**| **log-only**}[**dhcp** | **ndp**]}：送信元アドレスまたはデータ アドレスのグリーニングを使用したバインディング テーブルの回復をイネーブルにします。
- （任意）**security-level**{**glean**|**guard**|**inspect**}：この機能によって適用されるセキュリティのレベルを指定します。デフォルトは **guard** です。

  glean：メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。

  guard：アドレスを収集し、メッセージを検査します。さらに、RA および DHCP サーバ メッセージを拒否します。これがデフォルトのオプションです。

  inspect：アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。
- （任意）**tracking** {**disable** | **enable**}：トラッキング オプションを指定します。
- （任意）**trusted-port**：信頼できるポートを設定します。これにより、該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。

次に、デバイストラッキング ポリシーを設定する例を示します。

```
デバイス(config)# device-tracking policy policy1
デバイス(config-device-tracking)# trusted-port
```

dot1x critical（グローバル コンフィギュレーション）

IEEE 802.1X クリティカル認証パラメータを設定するには、グローバル コンフィギュレーション モードで **dot1x critical** コマンドを使用します。

dot1x critical eapol

構文の説明

eapol	スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。

コマンド デフォルト

eapol はディセーブルです

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

次に、スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するよう指定する例を示します。

```
デバイス(config)# dot1x critical eapol
```

dot1x pae

Port Access Entity（PAE）タイプを設定するには、インターフェイス コンフィギュレーション モードで **dot1x pae** コマンドを使用します。設定された PAE タイプをディセーブルにするには、コマンドの **no** 形式を入力します。

dot1x pae {**supplicant** | **authenticator** | **both**}
no dot1x pae {**supplicant** | **authenticator** | **both**}

構文の説明

supplicant	インターフェイスはサプリカントとしてだけ機能し、オーセンティケータ向けのメッセージに応答しません。
authenticator	インターフェイスはオーセンティケータとしてだけ動作し、サプリカント向けのメッセージに応答しません。
both	（任意）インターフェイスは、サプリカントおよびオーセンティケータとして動作するため、すべての dot1x メッセージに応答します。

コマンド デフォルト

PAE タイプは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドはCisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされません。

使用上のガイドライン

IEEE 802.1X 認証をポート上でディセーブルにする場合は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

dot1x port-control インターフェイス コンフィギュレーション コマンドを入力するなどしてポート上で IEEE 802.1x 認証を設定した場合、スイッチは自動的にポートを IEEE 802.1x オーセンティケータとして設定します。オーセンティケータの PAE 動作は、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを入力した後でディセーブルになります。

次に、インターフェイスがサプリカントとして動作するように設定されている例を示します。

```
デバイス(config)# interface g1/0/3
デバイス(config-if)# dot1x pae supplicant
```

dot1x supplicant controlled transient

認証中に 802.1X サプリカントポートへのアクセスを制御するには、グローバル コンフィギュレーション モードで **dot1x supplicant controlled transient** コマンドを使用します。認証中にサプリカントのポートを開くには、このコマンドの **no** 形式を使用します。

dot1x supplicant controlled transient
no dot1x supplicant controlled transient

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

認証中に 802.1x サプリカントのポートへのアクセスが許可されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドはCisco IOS XE Denali 16.1.x およびCisco IOS XE Denali 16.2.x ではサポートされません。

使用上のガイドライン

デフォルトでは、BPCU ガードがイネーブルにされたオーセンティケータ スイッチにサプリカントのスイッチを接続する場合、オーセンティケータのポートはサプリカント スイッチが認証する前にスパニングツリープロトコル（STP）のブリッジプロトコルデータユニット（BPDU）を受信した場合、errdisable 状態になる可能性があります。Cisco IOS Release 15.0(1) SE 以降では、認証中にサプリカントのポートから送信されるトラフィックを制御できます。**dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証が完了する前にオーセンティケータポートがシャットダウンすることがないように、認証中に一時的にサプリカントのポートがブロックされます。認証に失敗すると、サプリカントのポートが開きます。**no dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証期間中にサプリカントポートが開きます。これはデフォルトの動作です。

BPDU ガードが **spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドによりオーセンティケータ スイッチ ポートでイネーブルになっている場合、サプリカントスイッチで **dot1x supplicant controlled transient** コマンドを使用することを強く推奨します。

次に、認証の間にスイッチの 802.1x サプリカントのポートへのアクセスを制御する例を示します。

```
デバイス(config)# dot1x supplicant controlled transient
```

dot1x supplicant force-multicast

サプリカントスイッチでマルチキャストまたはユニキャストの Extensible Authentication Protocol over LAN（EAPOL）パケットを受信した場合に、常にマルチキャスト EAPOL パケットのみを送信するように強制するには、グローバル コンフィギュレーション モードで **dot1x supplicant force-multicast** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x supplicant force-multicast
no dot1x supplicant force-multicast

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

サプリカント スイッチは、ユニキャスト EAPOL パケットを受信すると、ユニキャスト EAPOL パケットを送信します。同様に、マルチキャスト EAPOL パケットを受信すると、EAPOL パケットを送信します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドは Cisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされません。

使用上のガイドライン

Network Edge Access Topology（NEAT）がすべてのホスト モードで機能するようにするには、サプリカント スイッチ上でこのコマンドをイネーブルにします。

次の例では、サプリカント スイッチがオーセンティケータ スイッチにマルチキャスト EAPOL パケットを送信するように設定する方法を示します。

```
デバイス(config)# dot1x supplicant force-multicast
```

関連コマンド

コマンド	説明
cisp enable	スイッチの Client Information Signalling Protocol（CISP）をイネーブルにすることで、スイッチがサプリカント スイッチに対するオーセンティケータとして動作するようにします。
dot1x credentials	ポートに 802.1x サプリカント資格情報を設定します。
dot1x pae supplicant	インターフェイスがサプリカントとしてだけ機能するように設定します。

dot1x test eapol-capable

すべてのスイッチポート上の IEEE 802.1x のアクティビティをモニタリングして、IEEE 802.1x をサポートするポートに接続しているデバイスの情報を表示するには、スイッチスタックまたはスタンドアロンスイッチ上で特権 EXEC モードで **dot1x test eapol-capable** コマンドを使用します。

dot1x test eapol-capable ［**interface** *interface-id*］

構文の説明

interface *interface-id*	（任意）クエリー対象のポートです。

コマンド デフォルト

デフォルト設定はありません。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

スイッチ上のすべてのポートまたは特定のポートに接続するデバイスの IEEE 802.1X 機能をテストするには、このコマンドを使用します。

このコマンドには、no 形式はありません。

次の例では、スイッチ上で IEEE 802.1X の準備チェックをイネーブルにして、ポートに対してクエリーを実行する方法を示します。また、ポートに接続しているデバイスを確認するためのクエリーの実行対象ポートから受信した応答が IEEE 802.1X 対応であることを示します。

```
デバイス# dot1x test eapol-capable interface gigabitethernet1/0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL
 capable
```

関連コマンド

コマンド	説明
dot1x test timeout *timeout*	IEEE 802.1X 準備クエリーに対する EAPOL 応答を待機するために使用されるタイムアウトを設定します。

dot1x test timeout

IEEE 802.1x 準備状態を照会しているポートからの EAPOL 応答の待機に使用されるタイムアウトを設定するには、スイッチスタックまたはスタンドアロンスイッチ上でグローバル コンフィギュレーション モードで **dot1x test timeout** コマンドを使用します。

dot1x test timeout *timeout*

構文の説明

timeout	EAPOL 応答を待機する時間（秒）。指定できる範囲は 1 ～ 65535 秒です。

コマンド デフォルト

デフォルト設定は 10 秒です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

EAPOL 応答を待機するために使用されるタイムアウトを設定するには、このコマンドを使用します。

このコマンドには、no 形式はありません。

次の例では、EAPOL 応答を 27 秒間待機するようにスイッチを設定する方法を示します。

```
デバイス# dot1x test timeout 27
```

タイムアウト設定のステータスを確認するには、**show run** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
dot1x test eapol-capable [**interface** *interface-id*]	すべての、または指定された IEEE 802.1X 対応ポートに接続するデバイスで IEEE 802.1X の準備が整っているかを確認します。

dot1x timeout

再試行タイムアウトの値を設定するには、グローバル コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで **dot1x timeout** コマンドを使用します。再試行タイムアウトをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

dot1x timeout {**auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds* | **ratelimit-period** *seconds* | **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds*}

構文の説明

auth-period *seconds*	サプリカントで保留ステートが維持される秒数（つまり、サプリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。

held-period *seconds*	サプリカントで保留ステートが維持される秒数（つまり、サプリカントが試行に失敗した場合に再度クレデンシャルを送信するまでに待機する時間）を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 60 です。
quiet-period *seconds*	認証情報の交換に失敗したあと、クライアントの再認証を試みるまでにオーセンティケータ（サーバ）が待機状態（HELD 状態）を続ける秒数を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 60 です。
ratelimit-period *seconds*	動作の不正なクライアント PC（たとえば、スイッチ処理電力の無駄につながる、EAP-START パケットを送信する PC）から送信される EAP-START パケットを抑制します。 • オーセンティケータはレート制限時間中、認証に成功したクライアントからの EAPOL-Start パケットを無視します。 • 有効な範囲は 1 ～ 65535 です。デフォルトでは、レート制限はディセーブルになっています。
server-timeout *seconds*	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 • 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。 サーバが指定時間内に 802.1X パケットへの応答を送信しない場合、パケットは再度送信されます。
start-period *seconds*	連続して送信される 2 つの EAPOL-Start フレーム間の間隔（秒単位）を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。 Cisco IOS リリース 15.2(5)E では、サプリカント モードでのみこのコマンドを使用できます。その他のモードでこのコマンドを適用すると、設定からそのコマンドが失われます。
supp-timeout *seconds*	EAP 要求 ID 以外のすべての EAP メッセージについて、オーセンティケータからホストへの再送信時間を設定します。 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。

tx-period *seconds*	クライアントに EAP 要求 ID パケットを再送信する間隔を（応答が受信されないものと仮定して）秒数で設定します。 • 有効な範囲は 1 ～ 65535 です。デフォルトは 30 です。 • 802.1X パケットがサプリカントに送信され、そのサプリカントが再試行期間後に応答しなかった場合、そのパケットは再度送信されます。

コマンド デフォルト

定期的な再認証と定期的なレート制限が行われます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

dot1x reauthentication インターフェイス コンフィギュレーション コマンドを使用して定期的な再認証をイネーブルにしただけの場合、**dot1x timeout reauth-period** インターフェイス コンフィギュレーション コマンドは、スイッチの動作に影響します。

待機時間の間、スイッチはどのような認証要求も受け付けず、開始もしません。デフォルトよりも小さい数を入力することによって、ユーザへの応答時間を短縮できます。

ratelimit-period が 0（デフォルト）に設定された場合、スイッチは認証に成功したクライアントからの EAPOL パケットを無視し、それらを RADIUS サーバに転送します。

次に、さまざまな 802.1X 再送信およびタイムアウト時間が設定されている例を示します。

```
デバイス(config)# configure terminal
デバイス(config)# interface g1/0/3
デバイス(config-if)# dot1x port-control auto
デバイス(config-if)# dot1x timeout auth-period 2000
デバイス(config-if)# dot1x timeout held-period 2400
デバイス(config-if)# dot1x timeout quiet-period 600
デバイス(config-if)# dot1x timeout start-period 90
デバイス(config-if)# dot1x timeout supp-timeout 300
デバイス(config-if)# dot1x timeout tx-period 60
デバイス(config-if)# dot1x timeout server-timeout 60
```

イネーブルパスワード

さまざまな権限レベルへのアクセスを制御するローカルパスワードを設定するには、グローバル コンフィギュレーション モードで **enable password** コマンドを使用します。パスワード要件を削除するには、このコマンドの **no** 形式を使用します。

enable password [**level** *level*] {[**0**] *unencrypted-password* | [*encryption-type*] *encrypted-password*}
no enable password [**level** *level*]

構文の説明

level *level*	（任意）パスワードが適用されるレベル。0 ～ 15 の数字を使用して最大 16 個の権限レベルを指定できます。レベル 1 は、通常の EXEC モード ユーザ権限です。この引数がコマンドで、またはコマンドの **no** 形式で指定されていない場合、権限レベルはデフォルトの 15（従来のイネーブル権限）になります。
0	（任意）暗号化されていないクリアテキストパスワードを指定します。パスワードはセキュア ハッシュ アルゴリズム（SHA）256 シークレットに変換されてデバイスに保存されます。
unencrypted-password	イネーブルモードを開始するためにユーザが入力するパスワード。
encryption-type	（任意）パスワードの暗号化に使用するシスコ独自のアルゴリズム。*encryption-type* を指定する場合、入力する次の引数は暗号化されたパスワード（すでに Cisco デバイスによって暗号化されたパスワード）である必要があります。非表示のパスワードが続くことを示すタイプ 7 を指定できます。
encrypted-password	別のデバイス設定からコピーして入力する暗号化パスワード。

コマンド デフォルト

パスワードは定義されていません。デフォルトはレベル 15 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 16.11.1	このコマンドが導入されました。

使用上のガイドライン

⚠

注意 enable password コマンドと enable secret コマンドのいずれも設定されていない場合で、かつコンソールの回線パスワードが設定されている場合、コンソールの回線パスワードがすべての VTY（Telnet およびセキュアシェル（SSH））セッションのイネーブルパスワードとして機能します。

特定の権限レベルのパスワードを定義するには、このコマンドを **level** オプションを指定して使用します。レベルとパスワードを設定したら、このレベルにアクセスする必要のあるユーザにパスワードを供与します。さまざまなレベルでアクセスできるコマンドを指定するには、**privilege level** コンフィギュレーション コマンドを使用します。

通常、暗号化タイプは入力しません。通常、暗号化タイプは、Cisco デバイスによってすでに暗号化されているパスワードをコピーしてこのコマンドに貼り付ける場合にのみ入力します。

⚠

注意 暗号化タイプを指定してクリアテキストパスワードを入力した場合は、再びイネーブルモードを開始することはできません。いずれの方法で暗号化したパスワードも、忘れた場合は回復できません。

service password-encryption コマンドが設定されている場合、**more nvram:startup-config** コマンドを入力すると、**enable password** コマンドで作成するパスワードが暗号化された形式で表示されます。

service password-encryption コマンドを使用して、パスワードの暗号化を有効または無効にすることができます。

イネーブルパスワードの定義は次のとおりです。

- 1 ～ 25 文字の大文字と小文字の英数字を含める必要があります。
- 先頭にスペースを指定できますが、無視されます。ただし、中間および末尾のスペースは認識されます。
- パスワードを作成するときに、Crtl+V キーの組み合わせを押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、*abc?123* というパスワードを作成するには、次の手順を実行します。
  - **abc** を入力します。
  - **Crtl-v** と入力します。
  - **?123** を入力します。

システムからイネーブル パスワードを入力するように求められた場合、疑問符の前に Ctrl+v を入力する必要はなく、パスワードのプロンプトにそのまま abc?123 と入力できます。

例

次に、特権レベル 2 のパスワード「pswd2」を有効にする例を示します。

```
Device(config)# enable password level 2 pswd2
```

次に、暗号化タイプ 7 を使用して、デバイスのコンフィギュレーション ファイルからコピーした権限レベル 2 の暗号化パスワード「1i5Rkls3LoyxzS8t9」を設定する例を示します。

```
Device(config)# enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

関連コマンド

Command	Description
enable secret	**enable password** コマンドよりも強化したセキュリティレイヤを指定します。

enable secret

enable password コマンドよりも強化したセキュリティレイヤを指定するには、グローバル コンフィギュレーション モードで **enable secret** コマンドを使用します。**enable secret** の機能をオフにするには、このコマンドの **no** 形式を使用します。

enable secret [**level** *level*] {[**0**] *unencrypted-password* | *encryption-type encrypted-password*}
no enable secret [**level** *level*] [*encryption-type encrypted-password*]

構文の説明

level *level*	（任意）パスワードが適用されるレベルを指定します。1 ～ 15 の数字を使用して最大 15 個の権限レベルを指定できます。レベル 1 は、通常の EXEC モード ユーザ権限です。引数 *level* がコマンドまたはコマンドの **no** 形式で指定されていない場合、権限レベルはデフォルトの 15（従来のイネーブル権限）になります。
0	（任意）暗号化されていないクリアテキストパスワードを指定します。パスワードはセキュア ハッシュ アルゴリズム（SHA）256 シークレットに変換されてデバイスに保存されます。
unencrypted-password	イネーブルモードを開始するためにユーザが入力するパスワード。このパスワードは、**enable password** コマンドで作成したパスワードとは異なるものにする必要があります。
encryption-type	パスワードのハッシュに使用するシスコ独自のアルゴリズム。 • **5**：メッセージ ダイジェスト アルゴリズム 5 （MD5）で暗号化されたシークレットを指定します。 • **8**：パスワードベースキー派生関数 2（PBKDF2）の SHA-256 でハッシュされたシークレットを指定します。 • **9**：スクリプトでハッシュされたシークレットを指定します。
encrypted-password	別のデバイス設定からコピーしたハッシュパスワード。

コマンド デフォルト

パスワード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（config）

コマンド履歴

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

使用上のガイドライン

注意 **enable password** コマンドと **enable secret** コマンドのいずれも設定されていない場合で、かつコンソールの回線パスワードが設定されている場合、コンソールの回線パスワードがすべてのVTY（Telnet およびセキュアシェル（SSH））セッションのイネーブルパスワードとして機能します。

enable secret コマンドは、イネーブルパスワードよりも強化したセキュリティレイヤを指定するために使用します。**enable secret** コマンドでは、不可逆的な暗号化関数を使用してイネーブルシークレットパスワードを保存することでセキュリティを向上させます。この追加のセキュリティ暗号化レイヤは、パスワードがネットワークで送信される環境や TFTP サーバに保存される環境において役立ちます。

通常、暗号化タイプは、デバイスのコンフィギュレーションファイルからコピーした暗号化パスワードをこのコマンドに貼り付ける場合にのみ入力します。

注意 暗号化タイプを指定してクリアテキストパスワードを入力した場合は、再びイネーブルモードを開始することはできません。いずれの方法で暗号化したパスワードも、忘れた場合は回復できません。

enable password コマンドと **enable secret** コマンドに同じパスワードを使用した場合、推奨されない方法であることを警告するエラーメッセージが表示されますが、パスワードは受け入れられます。ただし、同じパスワードを使用すると、**enable secret** コマンドによって提供される追加のセキュリティが損なわれます。

（注） **enable secret** コマンドを使用してパスワードを設定したあとは、 **enable secret** がディセーブルになっている場合、または Cisco IOS ソフトウェアの古いバージョンが使用されている（古い rxboot イメージを実行しているときなど）場合にのみ、**enable password** コマンドを使用して設定されたパスワードは機能します。また、いずれの方法で暗号化したパスワードも、忘れた場合は回復できません。

service password-encryption コマンドが設定されている場合、**more nvram:startup-config** コマンドを入力すると、作成するパスワードが暗号化された形式で表示されます。

service password-encryption コマンドを使用して、パスワードの暗号化を有効または無効にすることができます。

イネーブルパスワードの定義は次のとおりです。

- 1 ～ 25 文字の大文字と小文字の英数字を含める必要があります。
- 先頭にスペースを指定できますが、無視されます。ただし、中間および末尾のスペースは認識されます。

- パスワードを作成するときに、Crtl+V キーの組み合わせを押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、*abc?123* というパスワードを作成するには、次の手順を実行します。
  - **abc** を入力します。
  - **Crtl-v** を押します。
  - **?123** を入力します。

システムからイネーブルパスワードを入力するように求められた場合、疑問符の前に Ctrl+v を入力する必要はなく、パスワードのプロンプトに **abc?123** と入力できます。

（注） タイプ 8 またはタイプ 9 のパスワードを使用していて、タイプ 8 およびタイプ 9 のパスワードをサポートしていない古いバージョンの Cisco IOS ソフトウェアにダウングレードする場合は、ダウングレードする前にタイプ 5 ハッシュを使用するようパスワードを再設定する必要があります。これを行わないと、デバイスからロックアウトされ、パスワードの回復が必要になります。外部 AAA サーバを使用して特権レベルを管理している場合は、デバイスからロックアウトされません。

例

次に、**enable secret** コマンドを使用してパスワードを指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable secret password
```

enable secret コマンドを使用してパスワードを指定した後、ユーザはこのパスワードを入力してアクセスする必要があります。**enable password** コマンドを使用して設定されたパスワードは機能しなくなります。

```
Password: password
```

次に、暗号化タイプ 4 を使用して、デバイスのコンフィギュレーション ファイルからコピーした権限レベル 2 の暗号化パスワード「1FaD0$Xyti5Rkls3LoyxzS8」を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 4 $1$FaD0$Xyti5Rkls3LoyxzS8
```

次に、ユーザが **enable secret 4** *encrypted-password* コマンドを入力したときに表示される警告メッセージの例を示します。

```
Device# configure terminal
Device(config)# enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

WARNING: Command has been added to the configuration but Type 4 passwords have been
```

```
deprecated.
Migrate to a supported password type

Device(config)# end
Device# show running-config | inc secret

enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
```

関連コマンド

コマンド	説明
enable password	さまざまな権限レベルへのアクセスを制御するローカルパスワードを設定します。
more nvram:startup-config	NVRAM に保管されている、または CONFIG_FILE 環境変数によって指定されているスタートアップ コンフィギュレーション ファイルを表示します。
service password-encryption	パスワードを暗号化します。

epm access-control open

アクセスコントロールリスト（ACL）が設定されていないポートにオープンディレクティブを設定するには、グローバル コンフィギュレーション モードで **epm access-control open** コマンドを使用します。オープンディレクティブをディセーブルにするには、このコマンドの **no** 形式を使用します。

epm access-control open
no epm access-control open

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

デフォルトのディレクティブが適用されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

スタティック ACL が設定されたアクセスポートに、認可ポリシーのないホストを許可するオープンディレクティブを設定するには、このコマンドを使用します。このコマンドを設定しない場合、ポートは設定された ACL のポリシーをトラフィックに適用します。ポートにスタティック ACL が設定されていない場合、デフォルトおよびオープンの両方のディレクティブがポートへのアクセスを許可します。

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

次の例では、オープンディレクティブを設定する方法を示します。

```
デバイス(config)# epm access-control open
```

関連コマンド

コマンド	説明
show running-config	現在実行されているコンフィギュレーション ファイルの内容を表示します

ip access-list role-based

ロールベース（セキュリティグループ）アクセスコントロールリスト（RBACL）を作成して、ロールベース ACL 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 access-list role-based** 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。

ip access-list role-based *access-list-name*
no ip access-list role-based *access-list-name*

構文の説明

access-list-name	セキュリティ グループ アクセス コントロール リスト（SGACL）の名前。

コマンド デフォルト

ロールベースの ACL 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 Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

SGACL ロギングの場合は、**permit ip log** コマンドを設定する必要があります。また、このコマンドは、ダイナミック SGACL のロギングを有効にするために、Cisco Identity Services Engine（ISE）でも設定する必要があります。

次に、IPv4トラフィックに適用できる SGACL を定義し、ロールベース アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
Switch(config)# ip access-list role-based rbacl1
Switch(config-rb-acl)# permit ip log
```

関連コマンド

コマンド	説明
permit ip log	設定されたエントリに一致するロギングを許可します。
show ip access-list	現在のすべてのIPアクセスリストの内容を表示します。

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 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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 admission name

Web認証をイネーブルにするには、グローバル コンフィギュレーション モードで**ip admission name** コマンドを使用します。Web 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip admission name *name* {**consent** | **proxy http**} [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** {*acl* | *acl-name*} | **service-policy type tag** *service-policy-name*]
no ip admission name *name* {**consent** | **proxy http**} [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** {*acl* | *acl-name*} | **service-policy type tag** *service-policy-name*]

構文の説明

name	ネットワークアドミッション制御ルールの名前。
consent	認証プロキシ同意 Web ページを *admission-name* 引数で指定された IP アドミッションルールに対応させます。
proxy http	Web 認証のカスタムページを設定します。
absolute-timer 分	（任意）外部サーバがタイムアウトするまでの経過時間（分）。
inactivity-time 分	（任意）外部ファイルサーバが到達不能であると見なされるまでの経過時間（分）。
list	（任意）指定されたルールをアクセス コントロール リスト（ACL）に関連付けます。
acl	標準、拡張リストを指定のアドミッション制御ルールに適用します。値の範囲は 1～199、または拡張範囲で 1300 から 2699 です。
acl-name	名前付きのアクセスリストを指定のアドミッション制御ルールに適用します。
service-policy type tag	（任意）コントロール プレーン サービス ポリシーを設定できます。
service-policy-name	**policy-map type control tag***policyname* コマンド、キーワード、および引数を使用して設定されたコントロールプレーンタグのサービスポリシー。このポリシーマップは、タグを受信したときのホストでの処理を適用するために使用されます。

コマンド デフォルト

Web 認証はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

ip admission name コマンドにより、スイッチ上で Web 認証がグローバルにイネーブルになります。

スイッチ上で Web 認証をイネーブルにしてから、**ip access-group in** および **ip admission web-rule** インターフェイス コンフィギュレーション コマンドを使用して、特定のインターフェイス上で Web 認証をイネーブルにします。

例

次に、スイッチ ポートで Web 認証のみを設定する例を示します。

```
デバイス# configure terminal
デバイス(config) ip admission name http-rule proxy http
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 101 in
デバイス(config-if)# ip admission rule
デバイス(config-if)# end
```

次の例では、スイッチ ポートでのフォールバック メカニズムとして、Web 認証とともに IEEE 802.1X 認証を設定する方法を示します。

```
デバイス# configure terminal
デバイス(config)# ip admission name rule2 proxy http
デバイス(config)# fallback profile profile1
デバイス(config)# ip access group 101 in
デバイス(config)# ip admission name rule2
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# dot1x port-control auto
デバイス(config-if)# dot1x fallback profile1
デバイス(config-if)# end
```

関連コマンド

コマンド	説明
dot1x fallback	IEEE 802.1X 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
fallback profile	Web 認証のフォールバック プロファイルを作成します。

コマンド	説明
ip admission	ポートで Web 認証をイネーブルにします。
show authentication sessions interface *interface* **detail**	Web 認証セッションのステータスに関する情報を表示します。
show ip admission	NAC のキャッシュされたエントリまたはNAC設定についての情報を表示します。

ip dhcp snooping database

Dynamic Host Configuration Protocol（DHCP）のスヌーピングデータベースを設定するには、グローバル コンフィギュレーション モードで **ip dhcp snooping database** コマンドを使用します。DHCP スヌーピングサーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

no ip dhcp snooping database ［ **timeout** | **write-delay** ］

構文の説明

flash:*url*	flash を使用して、エントリを格納するためのデータベースの URL を指定します。
ftp:*url*	FTP を使用して、エントリを格納するためのデータベースの URL を指定します。
http:*url*	HTTP を使用して、エントリを格納するためのデータベースの URL を指定します。
https:*url*	セキュア HTTP（HTTPS）を使用して、エントリを格納するためのデータベースの URL を指定します。
rcp:*url*	リモートコピー（RCP）を使用して、エントリを格納するためのデータベースの URL を指定します。

scp:*url*	セキュアコピー（SCP）を使用して、エントリを格納するためのデータベースの URL を指定します。
tftp:*url*	TFTP を使用して、エントリを格納するためのデータベースの URL を指定します。
timeout *seconds*	中断タイムアウトインターバルを指定します。有効値は 0 ～ 86,400 秒です。
write-delay *seconds*	ローカル DHCP スヌーピングデータベースにデータが追加されてから、DHCP スヌーピングエントリを外部サーバに書き込みするまでの時間を指定します。有効値は 15 ～ 86,400 秒です。

コマンド デフォルト

DHCP スヌーピングデータベースは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

このコマンドを入力する前に、インターフェイス上でDHCPスヌーピングをイネーブルにする必要があります。DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping** コマンドを使用します。

次に、TFTP を使用してデータベースの URL を指定する例を示します。

```
デバイス(config)#  ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```

次に、DHCP スヌーピングエントリを外部サーバに書き込むまでの時間を指定する例を示します。

```
デバイス(config)#  ip dhcp snooping database write-delay 15
```

ip dhcp snooping information option format remote-id

オプション 82 リモート ID サブオプションを設定するには、スイッチのグローバル コンフィギュレーション モードで **ip dhcp snooping information option format remote-id** コマンドを使用します。デフォルトのリモート ID サブオプションを設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping information option format remote-id {**hostname** | **string** *string*}
no ip dhcp snooping information option format remote-id {**hostname** | **string** *string*}

構文の説明

hostname	スイッチのホスト名をリモート ID として指定します。
string *string*	1 ～ 63 の ASCII 文字（スペースなし）を使用して、リモート ID を指定します。

コマンド デフォルト

スイッチの MAC アドレスは、リモート ID です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

DHCP スヌーピング設定を有効にするには、**ip dhcp snooping** グローバル コンフィギュレーション コマンドを使用して DHCP スヌーピングをグローバルにイネーブルにする必要があります。

オプション 82 機能がイネーブルの場合、デフォルトのリモート ID サブオプションはスイッチの MAC アドレスです。このコマンドを使用すると、スイッチのホスト名または 63 個の ASCII 文字列（スペースなし）のいずれかをリモート ID として設定できます。

（注） ホスト名が 63 文字を超える場合、リモート ID 設定では 63 文字以降は省略されます。

次の例では、オプション 82 リモート ID サブオプションを設定する方法を示します。

```
デバイス(config)# ip dhcp snooping information option format remote-id hostname
```

ip dhcp snooping verify no-relay-agent-address

DHCP クライアントメッセージのリレーエージェントアドレス（giaddr）が信頼できないポート上のクライアント ハードウェア アドレスに一致することを確認して、DHCP スヌーピング

機能をディセーブルにするには、グローバル コンフィギュレーション モードで **ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。検証をイネーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping verify no-relay-agent-address
no ip dhcp snooping verify no-relay-agent-address

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

DHCP スヌーピング機能では、信頼できないポート上の DHCP クライアント メッセージのリレー エージェント IP アドレス（giaddr）フィールドが 0 であることを確認します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

デフォルトでは、DHCP スヌーピング機能では、信頼できないポート上の DHCP クライアント メッセージのリレーエージェントの IP アドレス（giaddr）フィールドが 0 であることを確認します。giaddr フィールドが 0 でない場合、メッセージはドロップされます。検証をディセーブルにするには、**ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。検証を再度イネーブルにするには、**no ip dhcp snooping verify no-relay-agent-address** コマンドを使用します。

次に、DHCP クライアントメッセージの giaddr 検証をイネーブルにする例を示します。

```
デバイス(config)# no ip dhcp snooping verify no-relay-agent-address
```

ip http access-class

HTTP サーバへのアクセスを制限するために使用するアクセスリストを指定するには、グローバル コンフィギュレーション モードで **ip http access-class** コマンドを使用します。以前に設定したアクセスリストの関連付けを削除するには、このコマンドの **no** 形式を使用します。

（注） 既存の **ip http access-class** *access-list-number* コマンドは、現在サポートされていますが、廃止される予定です。代わりに、**ip http access-class ipv4** {*access-list-number* | *access-list-name*} および **ip http access-class ipv6** *access-list-name* を使用してください。

ip http access-class { *access-list-number* | **ipv4** { *access-list-number* | *access-list-name* } | **ipv6** *access-list-name* }

no ip http access-class { *access-list-number* | **ipv4** { *access-list-number* | *access-list-name* } | **ipv6** *access-list-name* }

構文の説明

ipv4	セキュア HTTP サーバへのアクセスを制限するように IPv4 アクセス リストを指定します。
ipv6	セキュア HTTP サーバへのアクセスを制限するように IPv6 アクセス リストを指定します。
access-list-number	グローバル コンフィギュレーション コマンド **access-list** を使用して設定される、0 ～ 99 の標準 IP アクセスリスト番号。
access-list-name	**ip access-list** コマンドで設定された標準 IPv4 アクセスリストの名前。

コマンド デフォルト

アクセス リストは、HTTP サーバには適用されません。

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 Denali 16.3.1	このコマンドが変更されました。**ipv4** および **ipv6** キーワードが追加されました。
Cisco IOS XE Release 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドが設定されていると、指定されたアクセス リストはHTTPサーバに割り当てられます。HTTPサーバは、接続を受け入れる前にアクセス リストを確認します。確認に失敗すると、HTTP サーバは接続要求を承認しません。

例

次に、アクセス リストを 20 に定義して、HTTP サーバに割り当てる例を示します。

```
Device(config)# ip access-list standard 20
Device(config-std-nacl)# permit 209.165.202.130 0.0.0.255
Device(config-std-nacl)# permit 209.165.201.1 0.0.255.255
Device(config-std-nacl)# permit 209.165.200.225 0.255.255.255
Device(config-std-nacl)# exit
Device(config)# ip http access-class 20
```

次に、IPv4 の指定済みアクセス リストを定義して、HTTP サーバに割り当てる例を示します。

```
Device(config)# ip access-list standard Internet_filter
Device(config-std-nacl)# permit 1.2.3.4
```

```
Device(config-std-nacl)# exit

Device(config)# ip http access-class ipv4 Internet_filter
```

関連コマンド

コマンド	説明
ip access-list	IDをアクセスリストに割り当て、アクセスリストのコンフィギュレーションモードを開始します。
ip http server	HTTP 1.1 サーバ（Cisco Web ブラウザ ユーザ インターフェイスを含む）をイネーブルにします。

ip radius source-interface

すべての発信 RADIUS パケットに対して指定されたインターフェイスの IP アドレスを使用するように RADIUS 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 radius source-interface** コマンドを使用します。すべての発信 RADIUS パケットに対して指定されたインターフェイスの IP アドレスを使用しないように RADIUS を設定するには、このコマンドの no 形式を使用します。

ip radius source-interface *interface-name* [**vrf** *vrf-name*]
no ip radius source-interface

構文の説明

interface-name	RADIUSがすべての発信パケットに使用するインターフェイスの名前です。
vrf *vrf-name*	（任意）Virtual Route Forwarding（VRF）単位の設定です。

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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、すべての発信 RADIUS パケットの送信元アドレスとして使用するインターフェイスの IP アドレスを設定する場合に使用します。インターフェイスがアップ状態である限り、この IP アドレスが使用されます。RADIUS サーバでは、IP アドレスのリストを保持する代わりに、すべてのネットワーク アクセス クライアントに対して 1 つの IP アドレスエントリを使用できます。インターフェイスがアップ状態であるかダウン状態であるかに関係なく、関連付けられているインターフェイスの IP アドレスが使用されます。

特に、ルータに多数のインターフェイスがあり、特定のルータからのすべてのRADIUSパケットに同一の IP アドレスが含まれるようにする場合は、**ip radius source-interface** コマンドが役立ちます。

指定されたインターフェイスに有効な IP アドレスがあり、アップ状態でないと、設定は有効になりません。指定されたインターフェイスに有効な IP アドレスがない場合やダウン状態である場合、RADIUS によって AAA サーバへの最適なルートに対応するローカル IP が選択されます。これを回避するには、インターフェイスに有効な IP アドレスを追加するか、そのインターフェイスをアップ状態にします。

このコマンドを VRF 単位で設定するには、**vrf** *vrf-name* キーワードと引数を使用します。これにより、ユーザのルートに別のユーザのルートとの相互関係がない複数のルーティングテーブルまたは転送テーブルを使用できます。

例

次に、すべての発信 RADIUS パケットに対してインターフェイス s2 の IP アドレスを使用するように RADIUS を設定する例を示します。

```
ip radius source-interface s2
```

次に、VRF の定義に対してインターフェイス Ethernet0 の IP アドレスを使用するように RADIUS を設定する例を示します。

```
ip radius source-interface Ethernet0 vrf vrf1
```

ip source binding

スタティック IP ソース バインディング エントリを追加するには、**ip source binding** コマンドを使用します。スタティック IP ソース バインディング エントリを削除するには、このコマンドの **no** 形式を使用します。

ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*
no ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

構文の説明

mac-address	バインディング対象MACアドレスです。
vlan *vlan-id*	レイヤ 2 VLAN ID を指定します。有効な値は 1～4094 です。
ip-address	バインディング対象 IP アドレスです。
interface *interface-id*	物理インターフェイスの ID です。

コマンド デフォルト

IP 送信元バインディングは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

このコマンドは、スタティック IP ソース バインディング エントリだけを追加するために使用できます。

no 形式は、対応する IP ソース バインディング エントリを削除します。削除が正常に実行されるためには、すべての必須パラメータが正確に一致しなければなりません。各スタティック IP バインディング エントリは MAC アドレスと VLAN 番号がキーであることに注意してください。コマンドに既存の MAC アドレスと VLAN 番号が含まれる場合、別のバインディング エントリが作成される代わりに既存のバインディングエントリが新しいパラメータで更新されます。

次の例では、スタティック IP ソース バインディング エントリを追加する方法を示します。

```
デバイス# configure terminal
デバイスconfig) ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface
gigabitethernet1/0/1
```

ip ssh source-interface

インターフェイスのIPアドレスをセキュアシェル（SSH）クライアントデバイスの送信元アドレスとして指定するには、グローバル コンフィギュレーション モードで **ip ssh source-interface** コマンドを使用します。送信元アドレスとして指定した IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

ip ssh source-interface *interface*
no ip ssh source-interface *interface*

構文の説明

interface	アドレスをSSHクライアントの送信元アドレスとして使用するインターフェイス。

コマンド デフォルト

宛先に最も近いインターフェイスのアドレスが送信元アドレスとして使用されます（最も近いインターフェイスは SSH パケットが送信される出力インターフェイスです）。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1 Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを指定することにより、SSH クライアントの送信元アドレスとして送信元インターフェイスの IP アドレスを使用するように強制できます。

例

次の例では、GigabitEthernet インターフェイス 1/0/1 に割り当てられた IP アドレスが SSH クライアントの送信元アドレスとして使用されます。

```
Device> enable
Device# configure terminal
Device(config)# ip ssh source-interface GigabitEthernet 1/0/1
Device(config)# exit
```

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 [**mac-check**]
no ip verify source

mac-check	（任意）MAC アドレス検証による IP ソース ガードをイネーブルにします。

コマンド デフォルト

IP 送信元ガードはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

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

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

例

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

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

次の例では、MAC アドレスの検証による IP ソース ガードをイネーブルにする方法を示します。

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

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

ipv6 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 Denali 16.3.1	このコマンドが再度導入されました。このコマンドはCisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされません。

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 snooping policy

（注） すべての既存の IPv6 スヌーピング コマンド（Cisco IOS XE Denali 16.1.1 より前）には、対応する SISF ベースのデバイス トラッキング コマンドが用意され、IPv4 と IPv6 の両方のアドレス ファミリに設定を適用できるようになりました。詳細については、「device-tracking policy」を参照してください。

IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 snooping policy** コマンドを使用します。IPv6 スヌーピング ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ipv6 snooping policy *snooping-policy*
no ipv6 snooping policy *snooping-policy*

構文の説明

snooping-policy	スヌーピング ポリシーのユーザ定義名。ポリシー名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。

コマンド デフォルト

IPv6 スヌーピング ポリシーは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

IPv6 スヌーピング ポリシーを作成するには、**ipv6 snooping policy** コマンドを使用します。**ipv6 snooping policy** コマンドがイネーブルの場合、コンフィギュレーション モードが IPv6 スヌーピング コンフィギュレーション モードに変更されます。このモードでは、管理者が次の IPv6 ファーストホップ セキュリティ コマンドを設定できます。

- **device-role** コマンドは、ポートに接続されているデバイスのロールを指定します。
- **limit address-count** *maximum* コマンドは、ポートで使用できる IPv6 アドレスの数を制限します。
- **protocol** コマンドは、アドレスを Dynamic Host Configuration Protocol（DHCP）または Neighbor Discovery Protocol（NDP）で収集する必要があることを指定します。
- **security-level** コマンドは、適用されるセキュリティのレベルを指定します。
- **tracking** コマンドは、ポートのデフォルトのトラッキング ポリシーを上書きします。
- **trusted-port** コマンドは、ポートを信頼できるポートとして設定します。つまり、メッセージを受信したときに検証が限定的に実行されるか、まったく実行されません。

次に、IPv6 スヌーピング ポリシーを設定する例を示します。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)#
```

key chain macsec

事前共有キー（PSK）を取得するためにデバイスインターフェイスの MACsec キーチェーンの名前を設定するには、グローバル コンフィギュレーション モードで **key chain macsec** コマンドを使用します。CDP 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。

key chain *name***macsec** {**description** | **key** | **exit**}

構文の説明

name	キーを取得するために使用するキー チェーンの名前。
description	MACsec キー チェーンの説明を入力します。
key	MACsec キーを設定します。
exit	MACsec キーチェーン コンフィギュレーション モードを終了します。
no	コマンドを無効にするか、またはデフォルト値を設定します。

コマンド デフォルト

key chain macsec は無効になっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、128 ビットの事前共有キー（PSK）を取得するために MACsec キー チェーンを設定する例を示します。

```
Switch#configure terminal
Switch(config)#key chain kc1 macsec
Switch(config-keychain-macsec)#key 1000
Switch(config-keychain-macsec)#cryptographic-algorithm aes-128-cmac
Switch(config-keychain-macsec-key)# key-string fb63e0269e2768c49bab8ee9a5c2258f
Switch(config-keychain-macsec-key)#end
Switch#
```

次に、256 ビットの事前共有キー（PSK）を取得するために MACsec キー チェーンを設定する例を示します。

```
Switch#configure terminal
Switch(config)#key chain kc1 macsec
Switch(config-keychain-macsec)#key 2000
Switch(config-keychain-macsec)#cryptographic-algorithm aes-256-cmac
Switch(config-keychain-macsec-key)# key-string
c865632acb269022447c417504a1bf5db1c296449b52627ba01f2ba2574c2878
Switch(config-keychain-macsec-key)#end
Switch#
```

key config-key password-encrypt

タイプ 6 の暗号キーをプライベート NVRAM に保存するには、グローバル コンフィギュレーション モードで **key config-key password-encrypt** コマンドを使用します。暗号化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。

key config-key password-encrypt [*text*]
no key config-key password-encrypt [*text*]

構文の説明

text	（任意）**Password** または **master** キー。 （注） 事前共有キーがどこにも出力されないようにするために、*text* 引数は使用せず、代わりにインタラクティブモードを使用（**key config-key password-encrypt** コマンドを入力した後に enter キーを使用）することを推奨します。

コマンド デフォルト

タイプ 6 パスワード暗号化なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

コマンドラインインターフェイス（CLI）を使用して、プレーンテキストのパスワードをタイプ6形式でNVRAMに安全に保存できます。タイプ6のパスワードは暗号化されています。暗号化されたパスワード自体を、確認したり取得したりすることは可能ですが、それを復号化して実際のパスワードを特定することは困難です。**key config-key password-encrypt** コマンドを **password encryption aes** コマンドとともに使用すると、パスワードを設定してイネーブルにできます（キーの暗号化には対称キー暗号である高度暗号化規格（AES）が使用されます）。**key config-key password-encrypt** コマンドを使用して設定されたパスワード（キー）は、デバイス内のその他すべてのキーを暗号化するマスター暗号キーとして使用されます。

password encryption aes コマンドを設定する際、同時に **key config-key password-encrypt** コマンドを設定しないと、**show running-config** コマンドや **copy running-config startup-config** コマンドなどが設定されている起動時や不揮発性生成（NVGEN）プロセス中に次のようなメッセージが出力されます。

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

パスワードの変更

key config-key password-encryption コマンドを使用してパスワード（マスターキー）が変更された場合、または再暗号化された場合には、リストレジストリから、タイプ6暗号が使用されているアプリケーションモジュールへ、変更前のキーと変更後のキーが渡されます。

パスワードの削除

key config-key password-encrypt コマンドを使用して設定されたマスターキーがシステムから削除されると、タイプ6のパスワードすべてが使用不可になるという内容の警告が出力されます（同時に、確認用のプロンプトも表示されます）。セキュリティを確保するため、暗号化されたパスワードがCisco IOSソフトウェアによって復号化されることはありません。ただし、すでに説明したように、パスワードを再暗号化することはできます。

⚠

注意 **key config-key password-encrypt** コマンドを使用して設定されたパスワードは、一度失われると回復できません。パスワードは、安全な場所に保存することを推奨します。

パスワード暗号化の設定解除

no password encryption aes コマンドを使用してパスワード暗号化の設定を解除しても、既存のタイプ6パスワードはすべて変更されずに残されます。**key config-key password-encryption** コマンドを使用して設定したパスワード（マスターキー）があれば、アプリケーションで必要に応じてタイプ6パスワードを復号化できます。

パスワードの保存

（**key config-key password-encrypt** コマンドを使用して設定された）パスワードは誰にも「判読」できないため、デバイスからパスワードを取得する方法はありません。既存の管理ステー

ションでは、その内部にキーが格納されるよう強化されることで初めて、パスワードの内容を「知る」ことができます。その場合、パスワードは管理ステーション内部に安全に保存する必要があります。TFTP を使用して保存された設定は、スタンドアロンではないため、デバイスにはロードできません。設定をデバイスにロードする前後には、（**key config-key password-encrypt** コマンドを使用して）パスワードを手動で追加する必要があります。このパスワードは、保存された設定に手動で追加できますが、それによって設定内のすべてのパスワードを誰もが復号化できるようになるため、手動によるパスワードの追加は行わないことを推奨します。

新規パスワードまたは不明パスワードの設定

入力またはカット アンド ペーストした暗号文は、それがマスター キーに適合しない場合やマスター キーが存在しない場合でも、受理または保存されます。ただしこの場合にはアラート メッセージが出力されます。アラート メッセージの内容は次のとおりです。

```
“ciphertext>[for username bar>] is incompatible with the configured master key.”
```

マスターキーを新規に設定すると、プレーンテキストのキーはすべて暗号化され、タイプ 6 のキーになります。すでにタイプ 6 であるキーは暗号化されず、現在の状態が維持されます。

既存のマスターキーが失われた場合、またはその内容が不明の場合は、**no key config-key password-encrypt** コマンドを使用してそのマスターキーを削除できます。**no key config-key password-encrypt** コマンドを使用してマスターキーを削除しても、既存の暗号化パスワードは、暗号化された状態のままデバイス設定内に保持されます。これらのパスワードは復号化されません。

例

次に、タイプ 6 の暗号キーを NVRAM に保存する例を示します。

```
Device (config)# key config-key password-encrypt
```

関連コマンド

コマンド	説明
password encryption aes	タイプ 6 の暗号化事前共有キーをイネーブルにします。

limit address-count

ポートで使用できる IPv6 アドレスの数を制限するには、Neighbor Discovery Protocol（NDP）インスペクション ポリシー コンフィギュレーション モードまたは IPv6 スヌーピング コンフィギュレーション モードで **limit address-count** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

limit address-count *maximum*
no limit address-count

構文の説明

maximum	ポートで許可されているアドレスの数。範囲は 1 ～ 10000 です。

コマンド デフォルト デフォルト設定は無制限です。

コマンド モード ND インスペクション ポリシーの設定

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

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

使用上のガイドライン **limit address-count** コマンドは、ポリシーが適用されているポートで使用できる IPv6 アドレスの数を制限します。ポート上の IPv6 アドレスの数を制限すると、バインディング テーブル サイズの制限に役立ちます。範囲は 1 ～ 10000 です。

次に、NDP ポリシー名を policy1 と定義し、スイッチを NDP インスペクション ポリシー コンフィギュレーション モードにし、ポートで使用できる IPv6 アドレスの数を 25 に制限する例を示します。

```
デバイス(config)# ipv6 nd inspection policy policy1
デバイス(config-nd-inspection)# limit address-count 25
```

次に、IPv6 スヌーピング ポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、ポートで使用できる IPv6 アドレスの数を 25 に制限する例を示します。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)# limit address-count 25
```

mab request format attribute 32

スイッチ上でVLAN IDベースのMAC認証をイネーブルにするには、グローバル コンフィギュレーション モードで **mab request format attribute 32 vlan access-vlan** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mab request format attribute 32 vlan access-vlan
no mab request format attribute 32 vlan access-vlan

構文の説明 このコマンドには引数またはキーワードはありません。

コマンド デフォルト VLAN-ID ベースの MAC 認証はディセーブルです。

コマンド モード グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

RADIUS サーバがホスト MAC アドレスと VLAN に基づいて新しいユーザを認証できるようにするには、このコマンドを使用します。

Microsoft IAS RADIUS サーバを使用したネットワークでこの機能を使用します。Cisco ACS はこのコマンドを無視します。

次の例では、スイッチで VLAN-ID ベースの MAC 認証をイネーブルにする方法を示します。

```
デバイス(config)# mab request format attribute 32 vlan access-vlan
```

関連コマンド

コマンド	説明
authentication event	特定の認証イベントのアクションを設定します。
authentication fallback	IEEE 802.1X 認証をサポートしないクライアント用のフォールバック方式として Web 認証を使用するようポートを設定します。
authentication host-mode	ポートで認証マネージャモードを設定します。
authentication open	ポートでオープンアクセスをイネーブルまたはディセーブルにします。
authentication order	ポートで使用する認証方式の順序を設定します。
authentication periodic	ポートで再認証をイネーブルまたはディセーブルにします。
authentication port-control	ポートの認証ステートの手動制御をイネーブルにします。
authentication priority	ポートプライオリティリストに認証方式を追加します。
authentication timer	802.1X 対応ポートのタイムアウトパラメータと再認証パラメータを設定します。

コマンド	説明
authentication violation	新しいデバイスがポートに接続するか、ポートにすでに最大数のデバイスが接続しているときに、新しいデバイスがポートに接続した場合に発生する違反モードを設定します。
mab	ポートの MAC-based 認証をイネーブルにします。
mab eap	Extensible Authentication Protocol（EAP）を使用するようポートを設定します。
show authentication	スイッチの認証マネージャ イベントに関する情報を表示します。

macsec network-link

アップリンク インターフェイスの MKA MACsec 設定を有効にするには、インターフェイスで **macsec network-link** コマンドを使用します。CDP 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。

macsec network-link

構文の説明

macsec network-link	EAP-TLS 認証プロトコルを使用してデバイス インターフェイスの MKA MACsec 設定を有効にします。

コマンド デフォルト

macsec network-link は無効になっています。

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
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

次に、EAP-TLS 認証プロトコルを使用して、インターフェイスに MACsec MKA を設定する例を示します。

```
Switch#configure terminal
Switch(config)# int G1/0/20
Switch(config-if)# macsec network-link
Switch(config-if)# end
Switch#
```

match（アクセス マップ コンフィギュレーション）

1つまたは複数のアクセス リストをパケットと照合するようにVLANマップを設定するには、スイッチ スタックまたはスタンドアロン スイッチのアクセスマップ コンフィギュレーション モードで **match** コマンドを使用します。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*}]. . . | **ipv6 address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]. . . | **mac address** {*name*} [{*name*}] [{*name*}]. . .}
no match {**ip address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]. . . | **ipv6 address** {*namenumber*} [{*namenumber*}] [{*namenumber*}]. . . | **mac address** {*name*} [{*name*}] [{*name*}]. . .}

構文の説明

ip address	パケットを IP アドレス アクセス リストと照合するようにアクセス マップを設定します。
ipv6 address	パケットを IPv6 アドレス アクセス リストと照合するようにアクセス マップを設定します。
mac address	パケットを MAC アドレス アクセス リストと照合するようにアクセス マップを設定します。
name	パケットを照合するアクセス リストの名前です。
number	パケットを照合するアクセス リストの番号です。このオプションは、MACアクセス リストに対しては無効です。

コマンド デフォルト

デフォルトのアクションでは、一致パラメータは VLAN マップに適用されません。

コマンド モード

アクセス マップ コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

vlan access-map グローバル コンフィギュレーション コマンドを使用して、アクセスマップ コンフィギュレーション モードを開始します。

1 つのアクセス リストの名前または番号を入力する必要があります。その他は任意です。パケットは、1つまたは複数のアクセス リストに対して照合できます。いずれかのリストに一致すると、エントリの一致としてカウントされます。

アクセス マップ コンフィギュレーション モードでは、**match** コマンドを使用して、VLAN に適用される VLAN マップの一致条件を定義できます。**action** コマンドを使用すると、パケットが条件に一致したときに実行するアクションを設定できます。

パケットは、同じプロトコル タイプのアクセス リストに対してだけ照合されます。IP パケットは、IP アクセス リストに対して照合され、IPv6 パケットは IPv6 アクセス リストに対して照合され、その他のパケットはすべて MAC アクセス リストに対して照合されます。

同じマップ エントリに、IP アドレス、IPv6 アドレスおよび MAC アドレスを指定できます。

次の例では、VLAN アクセス マップ vmap4 を定義して VLAN 5 と VLAN 6 に適用する方法を示します。このアクセス マップでは、パケットがアクセス リスト al2 に定義された条件に一致すると、インターフェイスは IP パケットをドロップします。

```
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。

mka policy（グローバル コンフィギュレーション）

MACsec Key Agreement（MKA）プロトコルのポリシーを作成して MKA 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 **mka policy** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

mka policy *policy-name*
no mka policy *policy-name*

構文の説明

policy-name	MKA ポリシーを指定して、MKA ポリシー コンフィギュレーション モードを開始します。ポリシー名の長さは最大で 16 文字です。

コマンド デフォルト

作成されている MKA ポリシーはありません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

既存のポリシーの名前を入力した場合は、そのポリシーを変更すると、そのポリシーが適用されているすべてのアクティブな MKA セッションが削除されることを示す警告が表示されます。MKA ポリシーを変更すると必ず、そのポリシーが適用されているアクティブな MKA セッ

ションはクリアされます。17文字以上でポリシー名を作成しようとすると、警告メッセージが表示され、ポリシーは作成されません。

no mka policy *policy-name* コマンドを入力して、少なくとも1つのインターフェイスに適用されているポリシーを削除しようとすると、そのポリシーが適用されているすべてのインターフェイスからポリシーを削除してから、コマンドを再入力するように求められます。ポリシーを削除するときにそのポリシー名が存在しない場合は、ユーザに通知されます。

MKA ポリシー モードを開始すると、次のコマンドが使用可能になります。

- confidentiality-offset：機密性オフセットを設定して MACsec を動作させます。
- replay-protection：MACsec 動作にリプレイ保護を使用するように MKA を設定します。

例

次の例は、MKAポリシーを設定するときにすでに存在するポリシー名でポリシーを作成しようとした場合のコマンドの出力を示しています。

```
Device(config)# mka policy test-policy
Device(config-mka-policy)# exit
Device(config)# mka policy test-policy
%MKA policy "test-policy" may have associated active MKA Sessions.
 Changes to MKA Policy "test-policy" values
 will cause all associated active MKS Sessions to be cleared.
```

関連コマンド

コマンド	説明
mka policy（インターフェイス コンフィギュレーション）	MKAポリシーをインターフェイスに適用します。
show mka policy	定義されているMKAプロトコルのポリシーに関する情報を表示します。

mka pre-shared-key

事前共有キー（PSK）を使用してデバイスインターフェイスのMKA MACsec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 **mka pre-shared-key key-chain** *key-chain name* コマンドを使用します。CDP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。

mka pre-shared-key key-chain *key-chain-name*

構文の説明

mka pre-shared-key key-chain	PSK を使用してデバイス インターフェイスの MACsec MKA 設定を有効にします。

コマンド デフォルト

mka pre-shared-key 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 Denali 16.3.1	このコマンドが導入されました。

次に、PSK を使用して、インターフェイスの MKA MACsec を設定する例を示します。

```
Switch#
Switch(config)# int G1/0/20
Switch(config-if)# mka pre-shared-key key-chain kc1
Switch(config-if)# end
Switch#
```

authentication logging verbose

認証システムメッセージから詳細情報をフィルタリングするには、スイッチスタックまたはスタンドアロンスイッチ上で **authentication logging verbose** コマンドをグローバル コンフィギュレーション モードで使用します。

authentication logging verbose
no authentication logging verbose

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

システムメッセージの詳細ログ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 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、認証システムメッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose 認証システムメッセージをフィルタリングするには、次の手順に従います。

```
デバイス(config)# authentication logging verbose
```

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

関連コマンド

コマンド	説明
authentication logging verbose	認証システムメッセージから詳細情報をフィルタリングします。
dot1x logging verbose	802.1Xシステムメッセージから詳細情報をフィルタリングします。
mab logging verbose	MAC認証バイパス（MAB）システムメッセージから詳細情報をフィルタリングします。

dot1x logging verbose

802.1xシステムメッセージから詳細情報をフィルタリングするには、スイッチスタックまたはスタンドアロンスイッチ上で **dot1x logging verbose** コマンドをグローバル コンフィギュレーション モードで使用します。

dot1x logging verbose
no dot1x logging verbose

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

システムメッセージの詳細ログ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 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、802.1Xシステムメッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose 802.1x システム メッセージをフィルタリングするには、次の手順に従います。

```
デバイス(config)# dot1x logging verbose
```

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

関連コマンド

コマンド	説明
authentication logging verbose	認証システムメッセージから詳細情報をフィルタリングします。

コマンド	説明
dot1x logging verbose	802.1Xシステムメッセージから詳細情報をフィルタリングします。
mab logging verbose	MAC認証バイパス（MAB）システムメッセージから詳細情報をフィルタリングします。

mab logging verbose

MAC 認証バイパス（MAB）のシステムメッセージから詳細情報をフィルタリングするには、スイッチスタックまたはスタンドアロンスイッチ上で **mab logging verbose** コマンドをグローバル コンフィギュレーション モードで使用します。

mab logging verbose
no mab logging verbose

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

システムメッセージの詳細ログ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 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドにより、MAC認証バイパス（MAB）システムメッセージから、予測される成功などの詳細情報がフィルタリングされます。失敗メッセージはフィルタリングされません。

verbose MAB システム メッセージをフィルタリングするには、次の手順に従います。

```
デバイス(config)# mab logging verbose
```

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

関連コマンド

コマンド	説明
authentication logging verbose	認証システムメッセージから詳細情報をフィルタリングします。
dot1x logging verbose	802.1Xシステムメッセージから詳細情報をフィルタリングします。

コマンド	説明
mab logging verbose	MAC認証バイパス（MAB）システムメッセージから詳細情報をフィルタリングします。

password encryption aes

タイプ6の暗号化事前共有キー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 **password encryption aes** コマンドを使用します。パスワードの暗号化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。

password encryption aes
no password encryption aes

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

事前共有キーは暗号化されていません。

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 16.11.1	このコマンドが導入されました。

使用上のガイドライン

コマンドラインインターフェイス（CLI）を使用して、プレーンテキストのパスワードをタイプ6形式でNVRAMに安全に保存できます。タイプ6のパスワードは暗号化されています。暗号化されたパスワード自体を、確認したり取得したりすることは可能ですが、それを復号化して実際のパスワードを特定することは困難です。**key config-key password-encrypt** コマンドを **password encryption aes** コマンドとともに使用すると、パスワードを設定してイネーブルにできます（キーの暗号化には対称キー暗号である高度暗号化規格（AES）が使用されます）。**key config-key password-encrypt** コマンドを使用して設定されたパスワード（キー）は、ルータ内のその他すべてのキーを暗号化するマスター暗号キーとして使用されます。

password encryption aes コマンドを設定する際、同時に **key config-key password-encrypt** コマンドを設定しないと、**show running-config** コマンドや **copy running-config startup-config** コマンドなどが設定されている起動時や不揮発性生成（NVGEN）プロセス中に次のようなメッセージが出力されます。

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

パスワードの変更

key config-key password-encrypt コマンドを使用してパスワード（マスターキー）が変更された場合、または再暗号化された場合には、リストレジストリから、タイプ6暗号が使用されているアプリケーションモジュールへ、変更前のキーと変更後のキーが渡されます。

パスワードの削除

key config-key password-encrypt コマンドを使用して設定されたマスターキーがシステムから削除されると、タイプ6のパスワードすべてが使用不可になるという内容の警告が出力されます（同時に、確認用のプロンプトも表示されます）。セキュリティを確保するため、暗号化されたパスワードが Cisco IOS ソフトウェアによって復号化されることはありません。ただし、すでに説明したように、パスワードを再暗号化することはできます。

⚠

注意 **key config-key password-encrypt** コマンドを使用して設定されたパスワードは、一度失われると回復できません。パスワードは、安全な場所に保存することを推奨します。

パスワード暗号化の設定解除

no password encryption aes コマンドを使用してパスワード暗号化の設定を解除しても、既存のタイプ 6 パスワードはすべて変更されずに残されます。**key config-key password-encrypt** コマンドを使用して設定したパスワード（マスターキー）があれば、アプリケーションで必要に応じてタイプ 6 パスワードを復号化できます。

パスワードの保存

（**key config-key password-encrypt** コマンドを使用して設定された）パスワードは誰にも「判読」できないため、ルータからパスワードを取得する方法はありません。既存の管理ステーションでは、その内部にキーが格納されるよう強化されることで初めて、パスワードの内容を「知る」ことができます。その場合、パスワードは管理ステーション内部に安全に保存する必要があります。TFTP を使用して保存された設定は、スタンドアロンではないため、ルータにはロードできません。設定をルータにロードする前後には、（**key config-key password-encrypt** コマンドを使用して）パスワードを手動で追加する必要があります。このパスワードは、保存された設定に手動で追加できますが、それによって設定内のすべてのパスワードを誰もが復号化できるようになるため、手動によるパスワードの追加は行わないことを推奨します。

新規パスワードまたは不明パスワードの設定

入力またはカット アンド ペーストした暗号文は、それがマスター キーに適合しない場合やマスター キーが存在しない場合でも、受理または保存されます。ただしこの場合にはアラート メッセージが出力されます。アラート メッセージの内容は次のとおりです。

```
"ciphertext>[for username bar>] is incompatible with the configured master key."
```

マスターキーを新規に設定すると、プレーンテキストのキーはすべて暗号化され、タイプ6のキーになります。すでにタイプ 6 であるキーは暗号化されず、現在の状態が維持されます。

既存のマスターキーが失われた場合、またはその内容が不明の場合は、**no key config-key password-encrypt** コマンドを使用してそのマスターキーを削除できます。**no key config-key password-encrypt** コマンドを使用してマスターキーを削除しても、既存の暗号化パスワードは、暗号化された状態のままルータ設定内に保持されます。これらのパスワードは復号化されません。

例

次に、タイプ 6 の暗号化事前共有キーをイネーブルにする例を示します。

```
Device (config)# password encryption aes
```

関連コマンド

コマンド	説明
key config-key password-encrypt	タイプ 6 の暗号キーをプライベート NVRAM に保存します。

permit（MACアクセス リストコンフィギュレーション）

条件が一致した場合に非 IP トラフィックの転送を許可するには、スイッチスタックまたはスタンドアロンスイッチ上で **permit** MAC アクセスリスト コンフィギュレーション コマンドを使用します。拡張 MAC アクセス リストから許可条件を削除するには、このコマンドの **no** 形式を使用します。

{**permit** {**any** | **host***src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host***dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap***lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**] [**cos***cos*]
nopermit {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**] [**cos***cos*]

構文の説明

any	すべての送信元または宛先MACアドレスを拒否します。
host *src-MAC-addr* |*src-MAC-addr mask*	ホスト MAC アドレスと任意のサブネット マスクを指定します。パケットの送信元アドレスが定義されたアドレスに一致する場合、そのアドレスからの非 IP トラフィックは拒否されます。
host *dst-MAC-addr* | *dst-MAC-addr mask*	宛先 MAC アドレスと任意のサブネット マスクを指定します。パケットの宛先アドレスが定義されたアドレスに一致する場合、そのアドレスへの非 IP トラフィックは拒否されます。

type mask	（任意）パケットの EtherType 番号と、Ethernet II または SNAP カプセル化を指定して、パケットのプロトコルを識別します。 • *type* には、0 ～ 65535 の 16 進数を指定できます。 • *mask* は、一致をテストする前に EtherType に適用される don't care ビットのマスクです。
aarp	（任意）データリンク アドレスをネットワーク アドレスにマッピングする EtherType AppleTalk Address Resolution Protocol を指定します。
amber	（任意）EtherType DEC-Amber を指定します。
appletalk	（任意）EtherType AppleTalk/EtherTalk を指定します。
dec-spanning	（任意）EtherType Digital Equipment Corporation（DEC）スパニングツリーを指定します。
decnet-iv	（任意）EtherType DECnet Phase IV プロトコルを指定します。
diagnostic	（任意）EtherType DEC-Diagnostic を指定します。
dsm	（任意）EtherType DEC-DSM を指定します。
etype-6000	（任意）EtherType 0x6000 を指定します。
etype-8042	（任意）EtherType 0x8042 を指定します。
lat	（任意）EtherType DEC-LAT を指定します。
lavc-sca	（任意）EtherType DEC-LAVC-SCA を指定します。
lsap *lsap-number mask*	（任意）パケットの LSAP 番号（0 ～ 65535）と 802.2 カプセル化を使用して、パケットのプロトコルを指定します。 *mask* は、一致をテストする前に LSAP 番号に適用される don't care ビットのマスクです。
mop-console	（任意）EtherType DEC-MOP Remote Console を指定します。

mop-dump	（任意）EtherType DEC-MOP Dump を指定します。
msdos	（任意）EtherType DEC-MSDOS を指定します。
mumps	（任意）EtherType DEC-MUMPS を指定します。
netbios	（任意）EtherType DEC-Network Basic Input/Output System（NetBIOS）を指定します。
vines-echo	（任意）Banyan Systems による EtherType Virtual Integrated Network Service（VINES）Echo を指定します。
vines-ip	（任意）EtherType VINES IP を指定します。
xns-idp	（任意）EtherType Xerox Network Systems（XNS）プロトコル スイートを指定します。
cos *cos*	（任意）プライオリティを設定するため、0～7 までの任意の Class of Service（CoS）値を指定します。CoS に基づくフィルタリングは、ハードウェアでだけ実行可能です。**cos** オプションが設定されているかどうかを確認する警告メッセージが表示されます。

コマンド デフォルト

このコマンドには、デフォルトはありません。ただし、名前付き MAC ACL のデフォルト アクションは拒否です。

コマンド モード

MAC アクセス リスト コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

appletalk は、コマンドラインのヘルプストリングには表示されますが、一致条件としてはサポートされていません。

mac access-list extended グローバル コンフィギュレーション コマンドを使用して、MAC アクセス リスト コンフィギュレーション モードを開始します。

host キーワードを使用した場合、アドレスマスクは入力できません。**any** キーワードまたは **host** キーワードを使用しない場合は、アドレスマスクを入力する必要があります。

アクセス コントロール エントリ（ACE）がアクセスコントロールリストに追加された場合、リストの最後には暗黙の**deny-any-any**条件が存在します。つまり、一致がない場合にはパケットは拒否されます。ただし、最初の ACE が追加される前に、リストはすべてのパケットを許可します。

IPX トラフィックをフィルタリングするには、使用されている IPX カプセル化のタイプに応じて、*type mask* または **lsap** *lsap mask* キーワードを使用します。Novell 用語と Cisco IOS 用語での IPX カプセル化タイプに対応するフィルタ条件を、次の表に一覧表示します。

表 *45 : IPX* フィルタ基準

IPX カプセル化タイプ		**フィルタ基準**
Cisco IOS 名	**Novell 名**	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

次の例では、あらゆる送信元からMACアドレス00c0.00a0.03faへのNetBIOSトラフィックを許可する名前付き MAC 拡張アクセス リストを定義する方法を示します。このリストに一致するトラフィックは許可されます。

```
デバイス(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

次の例では、名前付き MAC 拡張アクセス リストから許可条件を削除する方法を示します。

```
デバイス(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

次の例では、EtherType 0x4321 のすべてのパケットを許可します。

```
デバイス(config-ext-macl)# permit any any 0x4321 0
```

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

関連コマンド

コマンド	説明
deny	MACアクセスリストコンフィギュレーションを拒否します。条件が一致した場合に非IPトラフィックが転送されるのを拒否します。

コマンド	説明
mac access-list extended	非 IP トラフィック用に MAC アドレス ベースのアクセス リストを作成します。
show access-lists	スイッチに設定されたアクセス コントロール リストを表示します。

protocol（IPv6 スヌーピング）

アドレスを Dynamic Host Configuration Protocol（DHCP）または Neighbor Discovery Protocol（NDP）で収集する必要があることを指定するか、プロトコルを IPv6 プレフィックス リストに対応させるには、**protocol** コマンドを使用します。DHCP または NDP によるアドレス収集をディセーブルにするには、このコマンドの **no** 形式を使用します。

protocol {**dhcp** | **ndp**}
no protocol {**dhcp** | **ndp**}

構文の説明

dhcp	アドレスをダイナミック ホスト コンフィギュレーション プロトコル（DHCP）パケットで収集する必要があることを指定します。
ndp	アドレスをネイバー探索プロトコル（NDP）パケットで収集する必要があることを指定します。

コマンド デフォルト

スヌーピングとリカバリは DHCP および NDP の両方を使用して試行します。

コマンド モード

IPv6 スヌーピング コンフィギュレーション モード

コマンド履歴

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

使用上のガイドライン

アドレスが 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
```

radius server

（注） Cisco IOS 15.2(5)E リリース以降では、Cisco IOS リリース 15.2(5)E より前のリリースで使用されていた **radius-server host** コマンドが **radius server** コマンドに置き換えられました。古いコマンドは廃止されました。

RADIUS アカウンティングと RADIUS 認証を含む RADIUS サーバのパラメータを設定するには、スイッチスタックまたはスタンドアロンスイッチで **radius server** コンフィギュレーション サブモード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius server *name*
address {ipv4 | ipv6} *ip{address | hostname}* **auth-port** *udp-port* **acct-port** *udp-port*
key *string*
automate tester *name* | **retransmit** *value* | **timeout** *seconds*
no radius server *name*

構文の説明

address {ipv4 | ipv6} *ip{address | hostname}*	RADIUS サーバの IP アドレスを指定します。
auth-port *udp-port*	（任意）RADIUS 認証サーバの UDP ポートを指定します。指定できる範囲は 0 ～ 65536 です。
acct-port *udp-port*	（任意）RADIUS アカウンティング サーバの UDP ポートを指定します。指定できる範囲は 0 ～ 65536 です。
key *string*	（任意）スイッチおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。 （注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。必ずこのコマンドの最終項目として key を設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。key にスペースが含まれる場合は、引用符が key の一部でない限り、key を引用符で囲まないでください。

automate tester *name*	（任意）RADIUS サーバ ステータスの自動サーバ テストをイネーブルにし、使用されるユーザ名を指定します。
retransmit *value*	（任意）サーバが応答しない、または応答が遅い場合に、RADIUS要求をリセットする回数を指定します。指定できる範囲は 1 ～ 100 です。この設定は、radius-server retransmit グローバル コンフィギュレーション コマンドによる設定を上書きします。
timeout *seconds*	（任意）スイッチが要求を再送信する前に RADIUS サーバからの応答を待機する時間間隔を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、radius-server timeout グローバル コンフィギュレーション コマンドによる設定を上書きします。
no radius server *name*	デフォルト設定に戻します。

コマンド デフォルト

- RADIUS アカウンティング サーバの UDP ポートは 1646 です。
- RADIUS 認証サーバの UDP ポートは 1645 です。
- 自動サーバ テストはディセーブルです。
- タイムアウトは 60 分（1 時間）です。
- 自動テストがイネーブルの場合、UDPポートのアカウンティングおよび認証時にテストが実行されます。
- 認証キーおよび暗号キー（string）は設定されていません。

コマンド モード

RADIUS サーバ サブモード コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	**radius-server host** コマンドを置き換える目的でこのコマンドが追加されました。

使用上のガイドライン

- RADIUS アカウンティング サーバおよび RADIUS 認証サーバの UDP ポートをデフォルト以外の値に設定することを推奨します。
- **key** *string* サブモード コンフィギュレーション コマンドを使用すると、認証および暗号キーを設定できます。必ずこのコマンドの最終項目として key を設定してください。
- RADIUS サーバステータスの自動サーバテストをイネーブルにし、使用されるユーザ名を指定するには、**automate-tester** *name* キーワードを使用します。

次の例では、認証サーバの UDP ポートを 1645、アカウンティング サーバの UDP ポートを 1646 に設定し、文字列を設定する例を示します。

```
デバイス(config)# radius server ISE
デバイス(config-radius-server)# address ipv4 10.1.1.1 auth-port 1645 acct-port 1646
デバイス(config-radius-server)# key cisco123
```

sap mode-list (cts manual)

2 個のインターフェイスの間のリンク暗号化をネゴシエートするために使用される Security Association Protocol（SAP）の認証と暗号化モード（最高から最低に優先順位付けされた）を選択するには、CTS dot1x インターフェイス コンフィギュレーション モードで **sap mode-list** コマンドを使用します。モードリストを削除してデフォルトに戻すには、このコマンドの **no** 形式を使用します。

2 個のインターフェイス間で MACsec のリンク暗号化をネゴシエートするために、ペアワイズ マスターキー（PMK）と Security Association Protocol（SAP）の認証および暗号化モードを手動で指定するには、**sap mode-list** 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。

sap pmk mode-list {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]
no sap pmk mode-list {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]

構文の説明

pmk *hex_value*	16 進数データ PMK を指定します（先行する 0x なし。偶数の16 進数文字を入力する。そうでない場合は、最後の文字に 0 のプレフィックスが付加される）。
mode-list	アドバタイズされたモードのリストを指定します（最高から最低に優先順位付け）。
gcm-encrypt	GMAC認証、GCM暗号化を指定します。
gmac	GMAC 認証だけを指定し、暗号化を指定しません。
no-encap	カプセル化を指定しません。
null	カプセル化あり、認証なし、暗号化なしを指定します。

コマンド デフォルト

デフォルトのカプセル化は **sap pmk mode-list gcm-encrypt null** です。ピア インターフェイスが 802.1AE MACsec または 802.REV レイヤ 2 リンク暗号化をサポートしない場合、デフォルトの暗号化は **null** です。

コマンド モード

CTS 手動インターフェイス コンフィギュレーション（config-if-cts-manual）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

使用上のガイドライン

認証と暗号化方式を指定するには、**sap pmk mode-list** コマンドを使用します。

セキュリティアソシエーションプロトコル（SAP）は802.11iIEEEプロトコルのドラフトバージョンに基づいた暗号キーの取得および交換プロトコルです。SAPはMACsecをサポートするインターフェイス間の 802.1AE リンク間暗号化（MACsec）を確立および管理するために使用します。

SAP およびペアワイズマスターキー（PMK）は、**sap pmk mode-list** コマンドを使用して、2 個のインターフェイス間に手動で設定することもできます。802.1X 認証を使用する場合、両方（サプリカントおよびオーセンティケータ）が Cisco Secure Access Control Server からピアのポートの PMK および MAC アドレスを受信します。

デバイスがCTS対応ソフトウェアを実行していて、ハードウェアがCTS非対応である場合は、**sap mode-list no-encap** コマンドを使用してカプセル化を拒否します。

例

次に、ギガビット イーサネット インターフェイスで SAP を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk FFFEE mode-list gcm-encrypt
```

関連コマンド

コマンド	説明
cts manual	CTS のインターフェイスを有効にします。
propagate sgt (cts manual)	Cisco TrustSec Security（CTS）インターフェイスのレイヤ 2 でのセキュリティ グループ タグ（SGT）の伝達を有効にします。
show cts interface	Cisco TrustSec インターフェイス設定の統計情報を表示します。

security level（IPv6 スヌーピング）

適用されるセキュリティのレベルを指定するには、IPv6 スヌーピング ポリシー コンフィギュレーション モードで **security-level** コマンドを使用します。

security level {**glean** | **guard** | **inspect**}

構文の説明

glean	アドレスをメッセージから抽出し、検証を行わずにそれらをバインディング テーブルにインストールします。
guard	収集と検査の両方を実行します。さらに、信頼できるポートで受信されていない場合、または別のポリシーによって許可されていない場合、RA メッセージおよび DHCP サーバ メッセージは拒否されます。
inspect	メッセージの一貫性と準拠度を検証します。特に、アドレス所有権が強制されます。無効なメッセージはドロップされます。

コマンド デフォルト

デフォルトのセキュリティ レベルは guard です。

コマンド モード

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	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
```

server-private（RADIUS）

グループサーバに対して、プライベートRADIUSサーバのIPアドレスを設定するには、RADIUS サーバグループ コンフィギュレーション モードで **server-private** コマンドを使用します。関連付けられたプライベートサーバを認証、許可、およびアカウンティング（AAA）グループサーバから削除するには、このコマンドの **no** 形式を使用します。

server-private *ip-address* [{**auth-port** *port-number* | **acct-port** *port-number*}] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
no server-private *ip-address* [{**auth-port** *port-number* | **acct-port** *port-number*}] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

構文の説明

ip-address	プライベート RADIUS サーバホストの IP アドレス。

auth-port *port-number*	（任意）認証要求に対するユーザ データグラム プロトコル（UDP）宛先ポート。デフォルト値は 1645 です。
acct-port *port-number*	（任意）アカウンティング要求に対する UDP 宛先ポート。デフォルト値は 1646 です。
non-standard	（任意）RADIUS サーバでベンダー独自の RADIUS 属性を使用。
timeout *seconds*	（任意）ルータが RADIUS サーバの応答を待機し、再送信するまでの時間間隔（秒単位）。この設定は **radius-server timeout** コマンドのグローバル値を上書きします。タイムアウト値が指定されていない場合は、グローバル値が使用されます。
retransmit *retries*	（任意）サーバが応答しない、または応答が遅い場合に RADIUS 要求をサーバに再送信する回数。この設定は **radius-server retransmit** コマンドのグローバル設定を上書きします。
key *string*	（任意）ルータと RADIUS サーバ上で稼働する RADIUS デーモン間で使用される認証および暗号キー。このキーは **radius-server key** コマンドのグローバル設定を上書きします。キー文字列を指定しない場合、グローバル値が使用されます。 *string* には、**0**（暗号化されていないキーが続くことを指定）、**6**（Advanced Encryption Scheme（AES）暗号化キーが続くことを指定）**7**（非公開のキーが続くことを指定）または暗号化されていない（クリアテキスト）サーバキーを指定する行を指定できます。

コマンド デフォルト

server-private パラメータが指定されていない場合は、グローバル コンフィギュレーションが使用されます。グローバル コンフィギュレーションが指定されていない場合は、デフォルト値が使用されます。

コマンド モード

RADIUS サーバグループ コンフィギュレーション（config-sg-radius）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

server-private コマンドを使用して、特定のプライベートサーバと定義済みのサーバグループを関連付けます。Virtual Route Forwarding（VRF）インスタンス間でプライベートアドレスが重複する可能性を防ぐには、プライベートサーバ（プライベートアドレスを持つサーバ）をサーバグループ内で定義し、他のグループには示されないようにします。この場合も、グローバルプール（デフォルトの「radius」サーバグループなど）内のサーバは、IP アドレスとポート番号を使って参照できます。このように、サーバグループ内のサーバのリストには、グローバル コンフィギュレーションにおけるホストの参照情報とプライベート サーバの定義が含まれます。

（注）

- **radius-server directed-request** コマンドが設定されている場合、**server-private**（RADIUS）コマンドを設定してプライベートRADIUSサーバをグループサーバとして使用することはできません。
- プライベート RADIUS サーバの AAA サーバ統計情報レコードの作成または更新はサポートされていません。プライベートRADIUSサーバが使用されている場合、エラーメッセージとトレースバックが発生しますが、これらのエラーメッセージやトレースバックはAAA RADIUS機能には影響しません。これらのエラーメッセージとトレースバックを回避するには、プライベートRADIUSサーバの代わりにパブリック RADIUS サーバを設定します。

タイプ 6 AES 暗号化キーを設定するには、**password encryption aes** コマンドを使用します。

例

次に、sg_water RADIUS グループサーバを定義してプライベートサーバを関連付ける例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius sg_water
Device(config-sg-radius)# server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
Device(config-sg-radius)# server-private 10.2.2.2 timeout 5 retransmit 3 key xyz
```

関連コマンド

コマンド	説明
aaa group server	各種のサーバ ホストを別個のリストと別個の方式にグループ化します。
aaa new-model	AAA アクセス コントロール モデルをイネーブルにします。
password encryption aes	タイプ 6 の暗号化事前共有キーをイネーブルにします。
radius-server host	RADIUS サーバ ホストを指定します。
radius-server directed-request	ユーザが NAS にログインして認証用の RADIUS サーバを選択できるようにします。

show aaa clients

AAA クライアントの統計情報を表示するには、**show aaa clients** コマンドを使用します。

show aaa clients ［**detailed**］

構文の説明

detailed	（任意）詳細なAAAクライアントの統計情報を示します。

コマンド モード

ユーザ EXEC

コマンド履歴

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

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

```
デバイス# show aaa clients

Dropped request packets: 0
```

show aaa command handler

AAA コマンドハンドラの統計情報を表示するには、**show aaa command handler** コマンドを使用します。

show aaa command handler

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC

コマンド履歴

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

次に、**show aaa command handler** コマンドの出力例を示します。

```
デバイス# show aaa command handler

AAA Command Handler Statistics:
    account-logon: 0, account-logoff: 0
    account-query: 0, pod: 0
    service-logon: 0, service-logoff: 0
    user-profile-push: 0, session-state-log: 0
    reauthenticate: 0, bounce-host-port: 0
    disable-host-port: 0, update-rbacl: 0
    update-sgt: 0, update-cts-policies: 0
    invalid commands: 0
    async message not sent: 0
```

show aaa local

AAA ローカル方式オプションを表示するには、**show aaa local** コマンドを使用します。

show aaa local {**netuser** {*name* | **all** } | **statistics** | **user lockout**}

構文の説明

netuser	AAA ローカル ネットワークまたはゲスト ユーザ データベースを指定します。
name	ネットワーク ユーザ名。
all	ネットワークおよびゲスト ユーザ情報を指定します。
statistics	ローカル認証の統計情報を表示します。
user lockout	AAA ローカルのロックアウトされたユーザを指定します。

コマンド モード

ユーザ EXEC

コマンド履歴

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

次に、**show aaa local statistics** コマンドの出力例を示します。

```
デバイス# show aaa local statistics

Local EAP statistics

EAP Method         Success       Fail
---------------------------------------
Unknown                  0          0
EAP-MD5                  0          0
EAP-GTC                  0          0
LEAP                     0          0
PEAP                     0          0
EAP-TLS                  0          0
EAP-MSCHAPV2             0          0
EAP-FAST                 0          0

Requests received from AAA:                0
Responses returned from EAP:               0
Requests dropped (no EAP AVP):             0
Requests dropped (other reasons):          0
Authentication timeouts from EAP:          0

Credential request statistics
Requests sent to backend:                  0
Requests failed (unable to send):          0
Authorization results received

  Success:                                 0
```

```
Fail:                                    0
```

show aaa servers

AAA サーバの MIB によって認識されるすべての AAA サーバを表示するには、**show aaa servers** コマンドを使用します。

show aaa servers ［ **private** | **public** | ［**detailed**］］

構文の説明

detailed	（任意）AAA サーバの MIB によって認識されるプライベート AAA サーバを表示します。
public	（任意）AAA サーバの MIB によって認識されるパブリック AAA サーバを表示します。
detailed	（任意）詳細な AAA サーバの統計情報を表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

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

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

```
デバイス# show aaa servers
RADIUS: id 1, priority 1, host 172.20.128.2, auth-port 1645, acct-port 1646
State: current UP, duration 9s, previous duration 0s
Dead: total time 0s, count 0
Quarantined: No
Authen: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Account: request 0, timeouts 0, failover 0, retransmission 0
Request: start 0, interim 0, stop 0
Response: start 0, interim 0, stop 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 0m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
```

```
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

show aaa sessions

AAA セッション MIB によって認識される AAA セッションを表示するには、**show aaa sessions** コマンドを使用します。

show aaa sessions

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

ユーザ EXEC

コマンド履歴

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

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

```
デバイス# show aaa sessions
Total sessions since last reload: 7
Session Id: 4007
   Unique Id: 4025
   User Name: *not available*
   IP Address: 0.0.0.0
   Idle Time: 0
   CT Call Handle: 0
```

show authentication brief

特定のインターフェイスの認証セッションに関する概要情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show authentication brief** コマンドを使用します。

`show authentication brief[switch{`*switch-number*`|active|standby}{R0}]`

構文の説明

switch-number	*switch-number* 変数の有効な値は 1 ～ 9 です。
R0	ルート プロセッサ（RP）スロット 0 に関する情報を表示します。
active	アクティブ インスタンスを指定します。

standby	スタンバイ インスタンスを指定します。

コマンド モード

特権 EXEC（#）

ユーザ EXEC (>)

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドは 16.9.1 よりも前のリリースで導入されました。

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

```
Device# show authentication brief

Interface  MAC Address     AuthC           AuthZ                    Fg  Uptime
-------------------------------------------------------------------------------
Gi2/0/14   0002.0002.0001  m:NA d:OK       AZ: SA-                  X     281s
Gi2/0/14   0002.0002.0002  m:NA d:OK       AZ: SA-                  X     280s
Gi2/0/14   0002.0002.0003  m:NA d:OK       AZ: SA-                  X     279s
Gi2/0/14   0002.0002.0004  m:NA d:OK       AZ: SA-                  X     278s
Gi2/0/14   0002.0002.0005  m:NA d:OK       AZ: SA-                  X     278s
Gi2/0/14   0002.0002.0006  m:NA d:OK       AZ: SA-                  X     277s
Gi2/0/14   0002.0002.0007  m:NA d:OK       AZ: SA-                  X     276s
Gi2/0/14   0002.0002.0008  m:NA d:OK       AZ: SA-                  X     276s
Gi2/0/14   0002.0002.0009  m:NA d:OK       AZ: SA-                  X     275s
Gi2/0/14   0002.0002.000a  m:NA d:OK       AZ: SA-                  X     275s
Gi2/0/14   0002.0002.000b  m:NA d:OK       AZ: SA-                  X     274s
Gi2/0/14   0002.0002.000c  m:NA d:OK       AZ: SA-                  X     274s
Gi2/0/14   0002.0002.000d  m:NA d:OK       AZ: SA-                  X     273s
Gi2/0/14   0002.0002.000e  m:NA d:OK       AZ: SA-                  X     273s
Gi2/0/14   0002.0002.000f  m:NA d:OK       AZ: SA-                  X     272s
Gi2/0/14   0002.0002.0010  m:NA d:OK       AZ: SA-                  X     272s
Gi2/0/14   0002.0002.0011  m:NA d:OK       AZ: SA-                  X     271s
Gi2/0/14   0002.0002.0012  m:NA d:OK       AZ: SA-                  X     271s
Gi2/0/14   0002.0002.0013  m:NA d:OK       AZ: SA-                  X     270s
Gi2/0/14   0002.0002.0014  m:NA d:OK       AZ: SA-                  X     270s
Gi2/0/14   0002.0002.0015  m:NA d:OK       AZ: SA-                  X     269s
```

次に、アクティブインスタンスに対する **show authentication brief** コマンドの出力例を示します。

```
Device# show authentication brief switch active R0

Interface  MAC Address     AuthC           AuthZ                    Fg  Uptime
-------------------------------------------------------------------------------
Gi2/0/14   0002.0002.0001  m:NA d:OK       AZ: SA-                  X       1s
Gi2/0/14   0002.0002.0002  m:NA d:OK       AZ: SA-                  X       0s
Gi2/0/14   0002.0002.0003  m:NA d:OK       AZ: SA-                  X     299s
Gi2/0/14   0002.0002.0004  m:NA d:OK       AZ: SA-                  X     298s
Gi2/0/14   0002.0002.0005  m:NA d:OK       AZ: SA-                  X     298s
Gi2/0/14   0002.0002.0006  m:NA d:OK       AZ: SA-                  X     297s
Gi2/0/14   0002.0002.0007  m:NA d:OK       AZ: SA-                  X     296s
Gi2/0/14   0002.0002.0008  m:NA d:OK       AZ: SA-                  X     296s
Gi2/0/14   0002.0002.0009  m:NA d:OK       AZ: SA-                  X     295s
Gi2/0/14   0002.0002.000a  m:NA d:OK       AZ: SA-                  X     295s
Gi2/0/14   0002.0002.000b  m:NA d:OK       AZ: SA-                  X     294s
Gi2/0/14   0002.0002.000c  m:NA d:OK       AZ: SA-                  X     294s
```

```
Gi2/0/14   0002.0002.000d  m:NA d:OK      AZ: SA-                X     293s
Gi2/0/14   0002.0002.000e  m:NA d:OK      AZ: SA-                X     293s
Gi2/0/14   0002.0002.000f  m:NA d:OK      AZ: SA-                X     292s
Gi2/0/14   0002.0002.0010  m:NA d:OK      AZ: SA-                X     292s
Gi2/0/14   0002.0002.0011  m:NA d:OK      AZ: SA-                X     291s
Gi2/0/14   0002.0002.0012  m:NA d:OK      AZ: SA-                X     291s
Gi2/0/14   0002.0002.0013  m:NA d:OK      AZ: SA-                X     290s
Gi2/0/14   0002.0002.0014  m:NA d:OK      AZ: SA-                X     290s
Gi2/0/14   0002.0002.0015  m:NA d:OK      AZ: SA-                X     289s
Gi2/0/14   0002.0002.0016  m:NA d:OK      AZ: SA-                X     289s
```

次に、スタンバイインスタンスに対する **show authentication brief** コマンドの出力例を示します。

```
Device# show authentication brief switch standby R0

No sessions currently exist
```

次の表で、この出力で表示される重要なフィールドについて説明します。

表 *46 : show authentication brief* フィールドの説明

フィールド	説明
Interface	認証インターフェイスのタイプと番号。
MAC アドレス	クライアントの MAC アドレス。
AuthC	認証ステータス。
authz	承認ステータス。
FG	現在のステータスを示すフラグ。有効な値は次のとおりです。 • A：ポリシーの適用中（詳細は複数行のステータスを参照） • D：取り外し待ち • F：最終の取り外しの進行中 • I：IIF ID の割り当て待ち • P：セッションをプッシュ済み • R：ユーザプロファイルの削除中（詳細は複数行のステータスを参照） • U：ユーザプロファイルの適用中（詳細は複数行のステータスを参照） • X：不明なブロック
Uptime	セッションが起動してからの経過時間。

show authentication sessions

現在の認証マネージャセッションに関する情報を表示するには、**show authentication sessions** コマンドを使用します。

show authentication sessions ［**database**］［**handle** *handle-id*［**details**］］［**interface** *type number*［**details**］［**mac** *mac-address*［**interface** *type number*］［**method** *method-name*［**interface** *type number*［**details**］［**session-id** *session-id* ［**details**］］

構文の説明

database	（任意）セッションデータベースに格納されているデータだけを示します。
handle *handle-id*	（任意）認証マネージャ情報を表示する特定のハンドルを指定します。
details	（任意）詳細情報を表示します。
interface *type number*	（任意）認証マネージャ情報を表示する特定のインターフェイスのタイプと番号を指定します。
mac *mac-address*	（任意）情報を表示する特定の MAC アドレスを指定します。
method *method-name*	（任意）認証マネージャ情報を表示する特定の認証方法を指定します。方式を指定する場合（**dot1x**、**mab**、または **webauth**）、インターフェイスも指定できます。
session-id *session-id*	（任意）認証マネージャ情報を表示する特定のセッションを指定します。

コマンド モード

ユーザ EXEC

コマンド履歴

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

使用上のガイドライン

現在のすべての認証マネージャセッションに関する情報を表示するには、**show authentication sessions** コマンドを使用します。特定の認証マネージャ セッションに関する情報を表示するには、1 つ以上のキーワードを使用します。

このテーブルは、報告された認証セッションで想定される動作状態を示します。

表 *47*：認証方式の状態

状態	説明
Not run	このセッションの方式は実行されていません。

状態	説明
Running	このセッションの方式が実行中です。
Failed over	この方式は失敗しました。次の方式が結果を出すことが予期されています。
Success	この方式は、セッションの成功した認証結果を提供しました。
Authc Failed	この方式は、セッションの失敗した認証結果を提供しました。

次の表に、使用できる認証方式を示します。

表 *48 :* 認証方式の状態

状態	説明
dot1x	802.1X
mab	MAC 認証バイパス
webauth	Web 認証

次に、スイッチ上のすべての認証セッションを表示する例を示します。

```
デバイス# show authentication sessions
Interface    MAC Address     Method   Domain   Status         Session ID
Gi1/0/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/0/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/0/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

次に、インターフェイス上のすべての認証セッションを表示する例を示します。

```
デバイス# show authentication sessions interface gigabitethernet2/0/47
            Interface:  GigabitEthernet2/0/47
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Guest Vlan
          Vlan Policy:  20
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000000002763C
      Acct Session ID:  0x00000002
              Handle:  0x25000000
Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Failed over
```

```
----------------------------------------
            Interface:  GigabitEthernet2/0/47
          MAC Address:  0005.5e7c.da05
           IP Address:  Unknown
            User-Name:  00055e7cda05
               Status:  Authz Success
               Domain:  VOICE
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000010002A238
      Acct Session ID:  0x00000003
               Handle:  0x91000001
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

show cisp

指定されたインターフェイスの CISP 情報を表示するには、特権 EXEC モードで **show cisp** コマンドを使用します。

show cisp { [**clients** | **interface** *interface-id*] | **registrations** | **summary**}

構文の説明

clients	（任意）CISP クライアントの詳細を表示します。
interface *interface-id*	（任意）指定されたインターフェイスの CISP 情報を表示します。有効なインターフェイスには、物理ポートとポート チャネルが含まれます。
registrations	CISP の登録情報を表示します。
summary	（任意）CISP のサマリー情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

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

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが再度導入されました。このコマンドはCisco IOS XE Denali 16.1.x および Cisco IOS XE Denali 16.2.x ではサポートされません。

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

```
デバイス# show cisp interface fast 0
CISP not enabled on specified interface
```

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

```
デバイス# show cisp registrations
Interface(s) with CISP registered user(s):
-----------------------------------------
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
Auth Mgr (Authenticator)
Gi2/0/13
Auth Mgr (Authenticator)
Gi3/0/3
Gi3/0/5
Gi3/0/23
```

関連コマンド

コマンド	説明
cisp enable	Client Information Signalling Protocol（CISP）をイネーブルにします。
dot1x credentials *profile*	サプリカント スイッチでプロファイルを設定します。

show dot1x

スイッチまたは指定されたポートのIEEE 802.1x統計情報、管理ステータス、および動作ステータスを表示するには、ユーザ EXEC モードで **show dot1x** コマンドを使用します。

show dot1x ［**all** ［**count** | **details** | **statistics** | **summary**］］［**interface** *type number*［**details** | **statistics**］］［**statistics**］

構文の説明

all	（任意）すべてのインターフェイスのIEEE 802.1X情報を表示します。
count	（任意）許可されたクライアントと無許可のクライアントの総数を表示します。
details	（任意）IEEE 802.1Xインターフェイスの詳細を表示します。
statistics	（任意）すべてのインターフェイスのIEEE 802.1X統計情報を表示します。
summary	（任意）すべてのインターフェイスのIEEE 802.1Xサマリー情報を表示します。
interface *type number*	（任意）指定したポートのIEEE 802.1Xステータスを表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

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

次に、**show dot1x all** コマンドの出力例を示します。

```
デバイス# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            3
```

次に、**show dot1x all count** コマンドの出力例を示します。

```
デバイス# show dot1x all count
Number of Dot1x sessions
------------------------------
Authorized Clients        = 0
UnAuthorized Clients      = 0
```

```
Total No of Client        = 0
```

次に、**show dot1x all statistics** コマンドの出力例を示します。

```
デバイス# show dot1x statistics
Dot1x Global Statistics for
-------------------------------------------
RxStart = 0     RxLogoff = 0    RxResp = 0      RxRespID = 0
RxReq = 0       RxInvalid = 0   RxLenErr = 0
RxTotal = 0

TxStart = 0     TxLogoff = 0    TxResp = 0
TxReq = 0       ReTxReq = 0     ReTxReqFail = 0
TxReqID = 0     ReTxReqID = 0   ReTxReqIDFail = 0
TxTotal = 0
```

show eap pac peer

拡張可能認証プロトコル（EAP）のセキュアトンネリングを介したフレキシブル認証（FAST）ピアの格納済み Protected Access Credential（PAC）を表示するには、特権 EXEC モードで **show eap pac peer** コマンドを使用します。

show eap pac peer

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

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

次に、**show eap pac peers** 特権 EXEC コマンドの出力例を示します。

```
デバイス> show eap pac peers
No PACs stored
```

関連コマンド

コマンド	説明
clear eap sessions	スイッチまたは指定されたポートの EAP のセッション情報をクリアします。

show ip dhcp snooping statistics

DHCP スヌーピング統計情報を概要形式または詳細形式で表示するには、ユーザ EXEC モードで **show ip dhcp snooping statistics** コマンドを使用します。

show ip dhcp snooping statistics ［**detail** ］

構文の説明

detail	（任意）詳細な統計情報を表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

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

使用上のガイドライン

スイッチ スタックでは、すべての統計情報がスタック マスターで生成されます。新しいアクティブスイッチが選定された場合、統計カウンタはリセットされます。

次に、**show ip dhcp snooping statistics** コマンドの出力例を示します。

```
デバイス> show ip dhcp snooping statistics

 Packets Forwarded                                = 0
 Packets Dropped                                  = 0
 Packets Dropped From untrusted ports             = 0
```

次に、**show ip dhcp snooping statistics detail** コマンドの出力例を示します。

```
デバイス> show ip dhcp snooping statistics detail

 Packets Processed by DHCP Snooping               = 0
 Packets Dropped Because
   IDB not known                                  = 0
   Queue full                                     = 0
   Interface is in errdisabled                    = 0
   Rate limit exceeded                            = 0
   Received on untrusted ports                    = 0
   Nonzero giaddr                                 = 0
   Source mac not equal to chaddr                 = 0
   Binding mismatch                               = 0
   Insertion of opt82 fail                        = 0
   Interface Down                                 = 0
   Unknown output interface                       = 0
   Reply output port equal to input port          = 0
   Packet denied by platform                      = 0
```

次の表に、DHCP スヌーピング統計情報およびその説明を示します。

表 *49 : DHCP* スヌーピング統計情報

DHCP スヌーピング統計情報	**説明**
Packets Processed by DHCP Snooping	転送されたパケットおよびドロップされたパケットも含めて、DHCP スヌーピングによって処理されたパケットの合計数。
Packets Dropped Because IDB not known	パケットの入力インターフェイスを判断できないエラーの数。
Queue full	パケットの処理に使用される内部キューが満杯であるエラーの数。非常に高いレートでDHCPパケットを受信し、入力ポートでレート制限がイネーブルになっていない場合、このエラーが発生することがあります。
Interface is in errdisabled	errdisable としてマークされたポートでパケットを受信した回数。これが発生する可能性があるのは、ポートが errdisable ステートである場合にパケットが処理キューに入り、そのパケットが後で処理される場合です。
Rate limit exceeded	ポートで設定されているレート制限を超えて、インターフェイスが errdisable ステートになった回数。
Received on untrusted ports	信頼できないポートで DHCP サーバ パケット（OFFER、ACK、NAK、LEASEQUERY のいずれか）を受信してドロップした回数。
Nonzero giaddr	信頼できないポートで受信した DHCP パケットのリレー エージェント アドレス フィールド（giaddr）がゼロ以外だった回数。または **no ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを設定しておらず、信頼できないポートで受信したパケットにオプション 82 データが含まれていた回数。
Source mac not equal to chaddr	DHCP パケットのクライアント MAC アドレス フィールド（chaddr）がパケットの送信元 MAC アドレスと一致せず、**ip dhcp snooping verify mac-address** グローバル コンフィギュレーション コマンドが設定されている回数。

DHCP スヌーピング統計情報	説明
Binding mismatch	MACアドレスとVLANのペアのバインディングになっているポートとは異なるポートで、RELEASEパケットまたはDECLINEパケットを受信した回数。これは、誰かが本来のクライアントをスプーフィングしようとしている可能性があることを示しますが、クライアントがスイッチの別のポートに移動してRELEASEまたはDECLINEを実行したことを表すこともあります。MAC アドレスは、イーサネットヘッダーの送信元MACアドレスではなく、DHCP パケットの chaddr フィールドから採用されます。
Insertion of opt82 fail	パケットへのオプション82挿入がエラーになった回数。オプション82データを含むパケットがインターネットの単一物理パケットのサイズを超えた場合、挿入はエラーになることがあります。
Interface Down	パケットが DHCP リレー エージェントへの応答であるが、リレー エージェントの SVI インターフェイスがダウンしている回数。DHCP サーバへのクライアント要求の送信と応答の受信の間で SVI がダウンした場合に発生するエラーですが、めったに発生しません。
Unknown output interface	オプション 82 データまたは MAC アドレス テーブルのルックアップのいずれかで、DHCP 応答パケットの出力インターフェイスを判断できなかった回数。パケットはドロップされます。オプション82が使用されておらず、クライアントMACアドレスが期限切れになった場合に発生することがあります。ポートセキュリティ オプションで IPSG がイネーブルであり、オプション 82 がイネーブルでない場合、クライアントのMACアドレスは学習されず、応答パケットはドロップされます。
Reply output port equal to input port	DHCP 応答パケットの出力ポートが入力ポートと同じであり、ループの可能性の原因となった回数。ネットワークの設定の誤り、またはポートの信頼設定の誤用の可能性を示します。
Packet denied by platform	プラットフォーム固有のレジストリによってパケットが拒否された回数。

show macsec

802.1ae Media Access Control Security（MACsec）情報を表示するには、特権 EXEC モードで **show macsec** コマンドを使用します。

show macsec {**interface***interface-id* | **summary**}

構文の説明

interface *interface-id*	MACsec インターフェイスの詳細を表示します。
summary	MACsec サマリー情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

例

次の例では、インターフェイスに確立された MACsec セッションがない場合の **show macsec interface** コマンドの出力を示します。

```
Switch# show macsec interface gigabitethernet 1/0/1
 MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
 Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128
 No Transmit Secure Channels
 No Receive Secure Channels
```

次の例では、セッションが確立された後の **show macsec interface** コマンドの出力を示します。

```
Switch# show macsec interface gigabitethernet 1/0/1
MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
 Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128
 Transmit Secure Channels
  SCI : 0022BDCF9A010002
   Elapsed time : 00:00:00
   Current AN: 0   Previous AN: -1
```

```
   SC Statistics
    Auth-only (0 / 0)
    Encrypt (1910 / 0)
 Receive Secure Channels
  SCI : 001B2140EC4C0000
   Elapsed time : 00:00:00
   Current AN: 0   Previous AN: -1
   SC Statistics
    Notvalid pkts 0      Invalid pkts 0
    Valid pkts 1         Late pkts 0
    Uncheck pkts 0       Delay pkts 0
  Port Statistics
   Ingress untag pkts  0        Ingress notag pkts 1583
   Ingress badtag pkts 0        Ingress unknownSCI pkts 0
   Ingress noSCI pkts 0         Unused pkts 0
   Notusing pkts 0              Decrypt bytes 80914
   Ingress miss pkts 1492
```

次の例では、すべての確立されたMACsecセッションを表示する**show macsec summary**コマンドの出力を示します。

```
Switch# show macsec summary
Interface                   Transmit SC          Receive SC
GigabitEthernet1/0/18             0                    0
GigabitEthernet1/0/20             1                    1
GigabitEthernet1/0/21             0                    0
GigabitEthernet1/0/22             1                    1
GigabitEthernet4/0/19             0                    0
GigabitEthernet4/0/20             1                    1
GigabitEthernet4/0/22             0                    0
```

関連コマンド

コマンド	説明
macsec	インターフェイスで MACsec をイネーブルにします。

show mka policy

すべての定義された MACsec Key Agreement（MKA）プロトコル ポリシーのサマリー（MKA デフォルトポリシーを含む）を表示する、または指定されたポリシーを表示するには、特権 EXEC モードで **show mka policy** コマンドを使用します。

show mka policy ［ *policy-name* ［**detail**］［**sessions**］］

構文の説明

policy-name	（任意）ポリシーの名前を指定します。

detail	（任意）指定された MKA ポリシーの詳細な設定情報（そのポリシーが適用された物理インターフェイスの名前を含む）を表示します。この出力は、各設定オプションのデフォルト値を示します。 **session** キーワードの後に入力された場合、指定されたポリシー名を持つ、すべてのアクティブな MKA セッションに関する詳細なステータス情報を表示します。
sessions	（任意）指定されたポリシー名を持つ、すべてのアクティブなMKAセッションのサマリーを表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

例

次に、**show mka policy** コマンドの出力例を示します。

```
Switch# show mka policy
MKA Policy Summary...
Policy            KS       Delay   Replay  Window     Conf   Interfaces
Name              Priority Protect Protect Size       Offset Applied
============================================================================
*DEFAULT POLICY*  0        NO      YES     0          0      Gi1/0/1
MkaPolicy-1       0        NO      YES     1000       0      Gi1/0/2  Gi1/0/3
MkaPolicy-2       0        NO      YES     0          50
MkaPolicy-3       0        YES     YES     64         30     Gi1/0/4  Gi1/0/5
                                                             Gi1/0/6
my_policy         0        NO      YES     4294967295 0
test-policy       0        NO      YES     10000      0
```

表 *50 : show mka policy* の出力フィールド

フィールド	説明
[Policy Name]	ポリシーのストリング識別情報。

フィールド	説明
KS Priority	キーサーバ（KS）になるための、プライオリティの設定値。有効範囲は0～255です。0は最高のプライオリティを、255は最小のプライオリティを示します。値0は、スイッチが常にキー サーバとして動作しようとすることを意味し、値255は、スイッチがサーバとして動作しようとしないことを意味します。この値は設定可能です。
Delay Protect	実施された遅延保護の設定値。この値は設定可能です。
Replay Protect	実施されたリプレイ保護の設定済みの値（これは、replay-protection window-sizeコマンドを入力することで設定可能です）。
Window Size	パケットごとのフレーム数で表される、リプレイ保護ウィンドウの設定済みサイズ。リプレイ保護がオフであれば、値は0です。リプレイ保護がオンで、値が0であれば、MACsecフレームの厳密な順序検証が発生します（これは、replay-protection window-sizeコマンドを入力することで設定可能です）。
Conf Offset	機密性オフセットの設定済みの値（MACsecの各フレームに保護または暗号化をオフセットするバイト数）。設定済みの値は、0（オフセットなし）、30、または50バイト。
Interfaces Applied	ポリシーが適用されたインターフェイスの短い名前。どのインターフェイスにも適用されていない場合、ストリングは空です。

次に、**show mka policy detail** コマンドの出力例を示します。

```
Switch# show mka policy MkaPolicy detail
MKA Policy Configuration ("MkaPolicy-3")
========================
MKA Policy Name........ MkaPolicy-3
Key Server Priority.... 0
Delay Protection....... NO
Replay Protection...... YES
Replay Window Size..... 64
Confidentiality Offset. 30
Applied Interfaces...
  GigabitEthernet1/0/4    GigabitEthernet1/0/5
  GigabitEthernet1/0/6
```

次に、**show mka policy sessions** コマンドの出力例を示します。

```
Switch# show mka policy replay-policy sessions
Summary of All Active MKA Sessions with MKA Policy "replay-policy"...
Interface Peer-RxSCI          Policy-Name      Audit-Session-ID
Port-ID   Local-TxSCI         Key-Svr Status   CKN
================================================================================
Gi1/0/25  001b.2140.ec3c/0000 replay-policy    0A05783B0000001700448BA8
2         001e.bdfe.6d99/0002 YES     Secured  3808F996026DFB8A2FCEC9A88BBD0680
```

関連コマンド

コマンド	説明
mka policy（グローバル コンフィギュレーション）	MKA ポリシーを作成して、MKA ポリシー コンフィギュレーション モードを開始します。
mka policy（インターフェイス コンフィギュレーション）	MKA ポリシーをインターフェイスに適用します。

show mka session

アクティブな MACsec Key Agreement（MKA）プロトコルセッションのサマリーを表示するには、特権 EXEC モードで **show mka session** コマンドを使用します。

show mka session ［**interface***interface-id*］［**port-id***port-id*］］［**local-sci***sci*］［**detail**］

構文の説明

interface *interface-id*	（任意）インターフェイス上のアクティブな MAK セッションのステータス情報を表示します。
port-id *port-id*	（任意）指定されたポート ID を持つインターフェイスで実行中のアクティブな MKA セッションのサマリーを表示します。ポート ID を表示するには、**show mka session interface** *interface-id* コマンドを使用します。ポート ID の値は、2 から始まり、同じ物理インターフェイスの仮想ポートを使用する新しいセッションごとに単調に増加します。
local-sci *sci*	（任意）Local TX-SCI で指定される MKA セッションのステータス情報を表示します。指定したセッションの Local TX-SCI を確認するには、show mka session コマンドをキーワードなしで入力します。SCI の長さは、8 個のオクテット（16 個の 16 進数）である必要があります。

detail	（任意）すべてのアクティブなMKAセッション、指定されたインターフェイス、または、指定されたポート ID を持つ特定のインターフェイスのすべてのセッションに関する詳細なステータス情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

例

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

```
Switch# show mka session
Total MKA Sessions..... 1
      Secured Sessions... 1
      Pending Sessions... 0
===============================================================================
Interface Peer-RxSCI          Policy-Name      Audit-Session-ID
Port-ID   Local-TxSCI         Key-Svr Status   CKN
===============================================================================
Gi1/0/1   001b.213d.28ed/0000 *DEFAULT POLICY* 02020202000000000000EAA6
2         001e.bdfe.8402/0002 YES     Secured  3A06ECB1183E42BB4D7817EB2B949D0E
Gi1/0/1   001a.323a.38ef/0000 *DEFAULT POLICY* 02020314000000000000EAB9
3         001e.bdfe.8402/0003 YES     Pending  CFB1E3B513344AB3417E17FBCB449D3A
Gi1/0/2   001c.113f.2d3a/0000 MkaPolicy-1      02020533000000000000EC81
2         001e.bdfe.8402/0002 YES     Secured  F103EABB133F4AB3497312EF2A949A03
```

表 ***51 : show mka session*** の出力フィールド

フィールド	説明
Interface	MKAセッションがアクティブである物理インターフェイスの短い名前。
Peer-RxSCI	ピアの 16 ビット ポート ID と連結した、ピアのインターフェイスの MAC アドレス。
Policy-name	セッション開始時に初期設定値の設定に使用されるポリシーの名前。
Audit session ID	セッション ID。
Port-ID	Local-TX-SCI で使用されるポート ID。
Local-TxSCI	16 ビット ポート ID と連結した、物理インターフェイスの MAC アドレス。

フィールド	説明
Key Server Status	キーサーバは、MKAセッションがキーサーバであれば「Y」を、それ以外の場合は「N」の値を持ちます。
CKN	Connectivity Association Key（CAK）の名前。

次に、**show mka session detail** コマンドの出力例を示します。

```
Switch# show mka session detail
MKA Detailed Status for MKA Session
==================================
Status: SECURED - Secured MKA Session with MACsec
Local Tx-SCI............. 0022.bdcf.9a01/0002
Interface MAC Address.... 0022.bdcf.9a01
MKA Port Identifier...... 2
Interface Name........... GigabitEthernet1/0/1
Audit Session ID......... 0B0B0B3D0000034F050FA69B
CAK Name (CKN)........... 46EFE9FE85199FE404FB7AFA3FD0732E
Member Identifier (MI)... D7B00EDA353242704CC6B0DB
Message Number (MN)...... 7
Authenticator............ YES
Key Server............... YES
Latest SAK Status........ Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (KN)....... D7B00EDA353242704CC6B0DB00000001 (1)
Old SAK Status........... FIRST-SAK
Old SAK AN............... 0
Old SAK KI (KN).......... FIRST-SAK (0)
SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
MKA Policy Name.......... *DEFAULT POLICY*
Key Server Priority...... 0
Delay Protection......... NO
Replay Protection........ YES
Replay Window Size....... 0
Confidentiality Offset... 0
Algorithm Agility........ 80C201
Cipher Suite............. 0080020001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES
# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 1
Live Peers List:
  MI                       MN          Rx-SCI (Peer)
  -----------------------------------------------------------
  DA296D3E62E0961234BF39A6  7          001b.2140.ec4c/0000
Potential Peers List:
  MI                       MN          Rx-SCI (Peer)
  -----------------------------------------------------------
```

次に、**show mka session interface** コマンドの出力例を示します。

```
Switch# show mka session interface gigabitethernet1/0/25
Summary of All Currently Active MKA Sessions on Interface GigabitEthernet1/0/25.
Interface Peer-RxSCI          Policy-Name      Audit-Session-ID
Port-ID   Local-TxSCI         Key-Svr Status   CKN
================================================================================
```

```
Gi1/0/25  001b.2140.ec3c/0000 replay-policy    0A05783B0000001700448BA8
2         001e.bdfe.6d99/0002 YES     Secured  3808F996026DFB8A2FCEC9A88BBD0680
```

関連コマンド

コマンド	説明
clear mka sessions	すべての MKA セッション（ポート ID、インターフェイス、または Local TX-SCI 上の MKA セッション）をクリアします。
macsec	インターフェイスで MACsec をイネーブルにします。

show mka statistics

グローバル MACsec Key Agreement（MKA）プロトコル統計情報およびアクティブな MKA セッションと以前の MKA セッションのエラーカウンタを表示するには、特権 EXEC モードで **show mka statistics** コマンドを使用します。

show mka statistics ［**interface***interface-id***port-id***port-id*］ | ［**local-sci***sci*］}

構文の説明

interface *interface-id*	（任意）インターフェイス上の MKA セッションの統計情報を表示します。物理インターフェイスだけが有効です。
port-id *port-id*	指定されたポート ID を持つインターフェイスで実行中のアクティブな MKA セッションのサマリーを表示します。ポート ID を表示するには、show mka session または **show mka session interface** *interface-id* コマンドを入力します。ポート ID の値は、2 から始まり、同じ物理インターフェイスの仮想ポートを使用する新しいセッションごとに単調に増加します。
local-sci *sci*	（任意）Local TX-SCI で指定される MKA セッションの統計情報を表示します。セッションの Local TX-SCI を確認するには、show mka session detail コマンドを入力します。SCI の長さは、8 個のオクテット（16 個の 16 進数）である必要があります。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

例

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

```
Switch# show mka statistics
MKA Global Statistics
=====================
MKA Session Totals
   Secured..................... 32
   Reauthentication Attempts.. 31
   Deleted (Secured).......... 1
   Keepalive Timeouts......... 0
CA Statistics
   Pairwise CAKs Derived...... 32
   Pairwise CAK Rekeys........ 31
   Group CAKs Generated....... 0
   Group CAKs Received........ 0
SA Statistics
   SAKs Generated............. 32
   SAKs Rekeyed............... 31
   SAKs Received.............. 0
   SAK Responses Received..... 32
MKPDU Statistics
   MKPDUs Validated & Rx...... 580
      "Distributed SAK"..... 0
      "Distributed CAK"..... 0
   MKPDUs Transmitted......... 597
      "Distributed SAK"..... 32
      "Distributed CAK"..... 0
MKA Error Counter Totals
========================
Bring-up Failures.................. 0
Reauthentication Failures.......... 0
SAK Failures
   SAK Generation.................. 0
   Hash Key Generation............. 0
   SAK Encryption/Wrap............. 0
   SAK Decryption/Unwrap........... 0
CA Failures
   Group CAK Generation............ 0
   Group CAK Encryption/Wrap....... 0
   Group CAK Decryption/Unwrap..... 0
   Pairwise CAK Derivation......... 0
   CKN Derivation.................. 0
   ICK Derivation.................. 0
   KEK Derivation.................. 0
   Invalid Peer MACsec Capability.. 2
MACsec Failures
   Rx SC Creation.................. 0
   Tx SC Creation.................. 0
   Rx SA Installation.............. 0
   Tx SA Installation.............. 0
MKPDU Failures
   MKPDU Tx........................ 0
   MKPDU Rx Validation............. 0
   MKPDU Rx Bad Peer MN............ 0
```

```
MKPDU Rx Non-recent Peerlist MN.. 0
```

表 *52 : show mka Global Statistics* の出力フィールド（続く）

フィールド	説明
Reauthentications	802.1x からの再認証。
Pairwise CAKs Derived	EAP 認証によって取得されたペアの Secure Connectivity Association Key（CAK）。
Pairwise CAK Rekeys	再認証後に再生成されたペアの CAK。
Group CAKs Generated	グループ CA のキー サーバとして動作中に生成されたグループ CAK。
Group CAKs Received	グループ CA の非キー サーバ メンバとして動作中に受信したグループ CAK。
SAK Rekeys	キー サーバとして開始された、または非キー サーバ メンバとして受信した Secure Association Key（SAK）のキー再生成。
SAKs Generated	任意の CA でキー サーバとして動作している間に生成された SAK。
SAKs Received	任意の CA で非キー サーバ メンバとして動作中に受信した SAK。
MPDUs Validated & Rx	受信し、検証された MACsec Key Agreement Protocol Data Units（MPDU）。
MPDUs Transmitted	送信された MPDU。

関連コマンド

コマンド	説明
clear mka statistics	すべての MKA 統計情報（特定のインターフェイス、ポート ID、または Local TX-SCI 上の MKA 統計情報）をクリアします。

show mka summary

MACsec Key Agreement（MKA）セッションのサマリーおよびグローバル統計情報を表示するには、特権 EXEC モードで **show mka summary** コマンドを使用します。

show mka summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.1	このコマンドが導入されました。

例

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

```
Switch# show mka summary
Summary of All Currently Active MKA Sessions...
===============================================
Total MKA Sessions..... 1
Initializing (Waiting for Peer)..... 0
Pending (Waiting for Peer MACsec Reply).... 0
Secured (Secured MKA Session with MACsec).. 1
Reauthenticating MKA Sessions..... 0
Interface Peer-RxSCI Policy-Name Audit-Session-ID
Port-ID Local-TxSCI Key-Svr Status CKN
================================================================================
Gi1/0/25 001b.2140.ec3c/0000 replay-policy 0A05783B0000001700448BA8
2 001e.bdfe.6d99/0002 YES Secured 3808F996026DFB8A2FCEC9A88BBD0680
MKA Global Statistics
=====================
MKA Session Totals
Secured..... 36
Reauthentications..... 23
Deleted (Secured)..... 0
Keepalive Timeouts..... 4
MACsec SAK-Use Timeouts.. 0
CA Statistics
Pairwise CAKs Derived.... 33
Pairwise CAK Rekeys..... 23
Group CAKs Generated..... 0
Group CAKs Received..... 0
SA Statistics
SAKs Generated..... 61
SAKs Rekeyed..... 54
SAKs Received..... 0
SAK Responses Received... 59
MKPDU Statistics
MKPDUs Validated & Rx.... 75774
"Distributed SAK"..... 0
"Distributed CAK"..... 0
MKPDUs Transmitted..... 75049
"Distributed SAK"..... 96
"Distributed CAK"..... 0
MKA Error Counter Totals
========================
Internal Failures..... 0
Session Failures
Failed while Initializing..... 6
Failed while Pending MACsec... 2
Reauthentication Failure..... 0
SAK Failures
SAK Generation..... 0
```

```
Hash Key Generation.......... 0
SAK Encryption/Wrap.......... 0
SAK Decryption/Unwrap........ 0
CA Failures
Group CAK Generation......... 0
Group CAK Encryption/Wrap..... 0
Group CAK Decryption/Unwrap... 0
Pairwise CAK Derivation...... 0
CKN Derivation............... 0
ICK Derivation............... 0
KEK Derivation............... 0
MACsec Failures
Rx SC Creation............... 2
Tx SC Creation............... 2
Rx SA Installation........... 2
Tx SA Installation........... 0
MKPDU Failures
MKPDU Tx..................... 0
MKPDU Rx Validation.......... 13
Bad Peer MN (anti-replay).. 0
Non-recent Peerlist MN..... 0
MKA Policy Summary...
Policy KS Delay Replay Window Conf Interfaces
Name Priority Protect Protect Size Offset Applied
================================================================================
*DEFAULT POLICY* 0 NO YES 0 0 Gi1/0/26 Gi1/0/29
replay-policy 0 NO YES 300 0 Gi1/0/25
Incredible-59#sh mka policy replay-policy
MKA Policy Summary...
Policy KS Delay Replay Window Conf Interfaces
Name Priority Protect Protect Size Offset Applied
================================================================================
replay-policy 0 NO YES 300 0 Gi1/0/25
```

表 ***53 : show mka summary*** の出力フィールド

フィールド	説明
Reauthentications	802.1x からの再認証。
Pairwise CAKs Derived	EAP 認証によって取得されたペアの Secure Connectivity Association Key（CAK）。
Pairwise CAK Rekeys	再認証後に再生成されたペアの CAK。
Group CAKs Generated	グループ CA のキー サーバとして動作中に生成されたグループ CAK。
Group CAKs Received	グループ CA の非キー サーバ メンバとして動作中に受信したグループ CAK。
SAK Rekeys	キー サーバとして開始された、または非キー サーバ メンバとして受信した Secure Association Key（SAK）のキー再生成。
SAKs Generated	任意の CA でキー サーバとして動作している間に生成された SAK。

フィールド	説明
SAKs Received	任意の CA で非キー サーバ メンバとして動作中に受信した SAK。
MPDUs Validated & Rx	受信し、検証された MACsec Key Agreement Protocol Data Units（MPDU）。
MPDUs Transmitted	送信された MPDU。

関連コマンド

コマンド	説明
show mka policy	定義されている MKA プロトコルのポリシーに関する情報を表示します。
show mka session	アクティブな MKA セッションのサマリーを表示します。
show mka statistics	グローバルな MKA 統計情報を表示します。

show radius server-group

RADIUS サーバグループのプロパティを表示するには、**show radius server-group** コマンドを使用します。

show radius server-group {*name* | **all**}

構文の説明

name	サーバ グループの名前。サーバグループの名前の指定に使用する文字列は、**the aaa group server radius** コマンドを使用して定義する必要があります。
all	すべてのサーバ グループのプロパティを表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

aaa group server radius コマンドで定義したサーバグループを表示するには、**show radius server-group** コマンドを使用します。

次に、**show radius server-group all** コマンドの出力例を示します。

```
デバイス# show radius server-group all
Server group radius
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *54 : show radius server-groups* コマンドのフィールドの説明

フィールド	説明
Server group	サーバ グループの名前。
Sharecount	このサーバ グループを共有している方式リストの数。たとえば、1 つの方式リストが特定のサーバ グループを使用する場合、sharecount は 1 です。2 つの方式リストが同じサーバ グループを使用する場合、sharecount は 2 です。
sg_unconfigured	サーバ グループが設定解除されました。
Type	タイプは、standard または nonstandard のいずれかです。タイプはグループ内のサーバが非標準の属性を受け入れるかどうかを示します。グループ内のすべてのサーバに非標準のオプションが設定されている場合、タイプは「nonstandard」と表示されます。
Memlocks	メモリ内にあるサーバ グループ構造の内部参照の数。この数は、このサーバ グループへの参照を保持している内部データ構造パケットまたはトランザクションがいくつあるかを表します。Memlocks はメモリ管理のために内部的に使用されます。

show storm-control

スイッチまたは指定のインターフェイス上で、ブロードキャスト、マルチキャストまたはユニキャストストーム制御の設定を表示する、またはストーム制御の履歴を表示するには、ユーザ EXEC モードで **show storm-control** コマンドを使用します。

show storm-control [{*interface-id*}] [{**broadcast** | **multicast** | **unicast**}]

構文の説明

interface-id	（任意）物理ポートのインターフェイスID（タイプ、スタック構成可能なスイッチのスタック メンバ、モジュール、ポート番号を含む）。
broadcast	（任意）ブロードキャスト ストームのしきい値設定を表示します。
multicast	（任意）マルチキャスト ストームのしきい値設定を表示します。
unicast	（任意）ユニキャスト ストームのしきい値設定を表示します。

コマンド モード

ユーザ EXEC

コマンド履歴

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

使用上のガイドライン

インターフェイス ID を入力すると、指定されたインターフェイスのストーム制御しきい値が表示されます。

インターフェイス ID を入力しない場合、スイッチ上のすべてのポートに対して 1 つのトラフィック タイプの設定が表示されます。

トラフィック タイプを入力しない場合は、ブロードキャスト ストーム制御の設定が表示されます。

次の例では、キーワードを指定せずに入力した **show storm-control** コマンドの出力の一部を示します。トラフィック タイプのキーワードが入力されてないため、ブロードキャスト ストーム制御の設定が表示されます。

```
デバイス> show storm-control
Interface Filter State  Upper      Lower     Current
--------- ------------- ---------- --------- ---------
Gi1/0/1   Forwarding    20 pps     10 pps    5 pps
Gi1/0/2   Forwarding    50.00%     40.00%    0.00%
<output truncated>
```

次の例では、指定したインターフェイスの **show storm-control** コマンドの出力を示します。トラフィック タイプのキーワードが入力されてないため、ブロードキャスト ストーム制御の設定が表示されます。

```
デバイス> show storm-control gigabitethernet 1/0/1
Interface Filter State  Upper      Lower     Current
--------- ------------- ---------- --------- ---------
Gi1/0/1   Forwarding    20 pps     10 pps    5 pps
```

次の表に、show storm-control の出力に表示されるフィールドの説明を示します。

表 *55 : show storm-control* のフィールドの説明

フィールド	説明
Interface	インターフェイスの ID を表示します。
Filter State	フィルタのステータスを表示します。 • blocking：ストーム制御はイネーブルであり、ストームが発生しています。 • forwarding：ストーム制御はイネーブルであり、ストームは発生していません。 • Inactive：ストーム制御はディセーブルです。
Upper	上限抑制レベルを利用可能な全帯域幅のパーセンテージとして、毎秒のパケット数または毎秒のビット数で表示します。
Lower	下限抑制レベルを利用可能な全帯域幅のパーセンテージとして、毎秒のパケット数または毎秒のビット数で表示します。
Current	ブロードキャスト トラフィックまたは指定されたトラフィック タイプ（ブロードキャスト、マルチキャスト、ユニキャスト）の帯域幅の使用状況を、利用可能な全帯域幅のパーセンテージで表示します。このフィールドは、ストーム制御がイネーブルの場合だけ有効です。

show tech-support acl

テクニカルサポートに使用するアクセスコントロールリスト（ACL）関連の情報を表示するには、特権 EXEC モードで **show tech-support acl** コマンドを使用します。

show tech-support acl

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

show tech-support acl コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support acl | redirect flash:***show_tech_acl.txt*）。

このコマンドの出力には次のコマンドが表示されます。

（注） スタック可能なプラットフォームでは、これらのコマンドはスタック内のすべてのスイッチで実行されます。Catalyst 9400 シリーズ スイッチなどのモジュール型のプラットフォームでは、これらのコマンドはアクティブスイッチでのみ実行されます。

（注） 次のコマンドのリストは、出力で使用可能なコマンドの例です。これらはプラットフォームによって異なる場合があります。

- **show clock**
- **show version**
- **show running-config**
- **show module**
- **show interface**
- **show access-lists**
- **show logging**
- **show platform software fed switch** *switch-number* **acl counters hardware**
- **show platform software fed switch** *switch-number* **ifm mapping**
- **show platform hardware fed switch** *switch-number* **fwd-asic drops exceptions**
- **show platform software fed switch** *switch-number* **acl info**
- **show platform software fed switch** *switch-number* **acl**
- **show platform software fed switch** *switch-number* **acl usage**
- **show platform software fed switch** *switch-number* **acl policy intftype all cam**
- **show platform software fed switch** *switch-number* **acl cam brief**
- **show platform software fed switch** *switch-number* **acl policy intftype all vcu**
- **show platform hardware fed switch** *switch-number* **acl resource usage**
- **show platform hardware fed switch** *switch-number* **fwd-asic resource tcam table acl**
- **show platform hardware fed switch** *switch-number* **fwd-asic resource tcam utilization**
- **show platform software fed switch** *switch-number* **acl counters hardware**

- **show platform software classification switch** *switch-number* **all F0 class-group-manager class-group**
- **show platform software process database forwarding-manager switch** *switch-number* **R0 summary**
- **show platform software process database forwarding-manager switch** *switch-number* **F0 summary**
- **show platform software object-manager switch** *switch-number* **F0 pending-ack-update**
- **show platform software object-manager switch** *switch-number* **F0 pending-issue-update**
- **show platform software object-manager switch** *switch-number* **F0 error-object**
- **show platform software peer forwarding-manager switch** *switch-number* **F0**
- **show platform software access-list switch** *switch-number* **f0 statistics**
- **show platform software access-list switch** *switch-number* **r0 statistics**
- **show platform software trace message fed switch** *switch-number*
- **show platform software trace message forwarding-manager switch** *switch-number* **F0**
- **show platform software trace message forwarding-manager switch R0** *switch-number* **R0**

例

次に、**show tech-support acl** コマンドの出力例を示します。

```
Device# show tech-support acl

.
.
.
------------------ show platform software fed switch 1 acl cam brief ------------------

Printing entries for region ACL_CONTROL (143) type 6 asic 0
=============================================================
TAQ-4 Index-0 (A:0,C:0) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Output IPv4 VACL

 VCU Result: Not In-Use

 L3 Length: 0000, L3 Protocol: 17 (UDP), L3 Tos: 00

 Source Address/Mask
 0.0.0.0/0.0.0.0
 Destination Address/Mask
 0.0.0.0/0.0.0.0

 Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

 L4 Source Port/Mask   L4 Destination Port/Mask
 0x0044 (68)/0xffff     0x0043 (67)/0xffff

 TCP Flags: 0x00 ( NOT SET )

 ACTIONS:  Forward L3, Forward L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)

----------------------------------------
TAQ-4 Index-1 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output IPv4 VACL
```

```
 VCU Result: Not In-Use

 L3 Length: 0000, L3 Protocol: 17 (UDP), L3 Tos: 00

 Source Address/Mask
 0.0.0.0/0.0.0.0
 Destination Address/Mask
 0.0.0.0/0.0.0.0

 Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

 L4 Source Port/Mask   L4 Destination Port/Mask
 0x0043 (67)/0xffff     0x0044 (68)/0xffff

 TCP Flags: 0x00 ( NOT SET )

 ACTIONS:  Forward L3, Forward L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)

----------------------------------------
TAQ-4 Index-2 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output IPv4 VACL

 VCU Result: Not In-Use

 L3 Length: 0000, L3 Protocol: 17 (UDP), L3 Tos: 00

 Source Address/Mask
 0.0.0.0/0.0.0.0
 Destination Address/Mask
 0.0.0.0/0.0.0.0

 Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

 L4 Source Port/Mask   L4 Destination Port/Mask
 0x0043 (67)/0xffff     0x0043 (67)/0xffff

 TCP Flags: 0x00 ( NOT SET )

 ACTIONS:  Forward L3, Forward L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)

----------------------------------------
TAQ-4 Index-3 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Input IPv4 PACL

 VCU Result: Not In-Use

 L3 Length: 0000, L3 Protocol: 00 (HOPOPT), L3 Tos: 00

 Source Address/Mask
 0.0.0.0/0.0.0.0
 Destination Address/Mask
 0.0.0.0/0.0.0.0

 Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

 L4 Source Port/Mask   L4 Destination Port/Mask
 0x0000 (0)/0x0000     0x0000 (0)/0x0000

 TCP Flags: 0x00 ( NOT SET )

 ACTIONS:  Drop L3, Drop L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)
```

```
----------------------------------------
TAQ-4 Index-4 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output IPv4 PACL

 VCU Result: Not In-Use

 L3 Length: 0000, L3 Protocol: 00 (HOPOPT), L3 Tos: 00

 Source Address/Mask
 0.0.0.0/0.0.0.0
 Destination Address/Mask
 0.0.0.0/0.0.0.0

 Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled

 L4 Source Port/Mask   L4 Destination Port/Mask
 0x0000 (0)/0x0000     0x0000 (0)/0x0000

 TCP Flags: 0x00 ( NOT SET )

 ACTIONS:  Drop L3, Drop L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)

----------------------------------------
TAQ-4 Index-5 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output MAC PACL

 VLAN ID/MASK : 0x000 (000)/0x000

 Source MAC/Mask : 0000.0000.0000/0000.0000.0000

 Destination MAC/Mask : 0000.0000.0000/0000.0000.0000

 isSnap: Disabled, isLLC: Disabled

 ACTIONS:  Drop L3, Drop L2, Logging Disabled
 ACL Priority: 2 (15 is Highest Priority)

.
.
.
```

出力フィールドの意味は自明です。

show tech-support identity

テクニカルサポートに使用するアイデンティティ/802.1X 関連の情報を表示するには、特権 EXEC モードで **show tech-support identity** コマンドを使用します。

show tech-support identity mac *mac-address* **interface** *interface-name*

構文の説明

mac *mac-address*	クライアント MAC アドレスに関する情報を表示します。
interface *interface-name*	クライアントインターフェイスに関する情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 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

show tech-support platform コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support identity mac** *mac-address* **interface** *interface-name* **| redirect flash:***filename*）。

このコマンドの出力には次のコマンドが表示されます。

- **show clock**
- **show module**
- **show version**
- **show switch**
- **show redundancy**
- **show dot1x statistics**
- **show ip access-lists**
- **show interface**
- **show ip interface brief**
- **show vlan brief**
- **show running-config**
- **show logging**
- **show interface controller**
- **show platform authentication sbinfo interface**
- **show platform host-access-table**
- **show platform pm port-data**
- **show spanning-tree interface**
- **show access-session mac detail**
- **show platform authentication session mac**
- **show device-tracking database mac details**
- **show mac address-table address**
- **show access-session event-logging mac**
- **show authentication sessions mac details R0**

- **show ip admission cache R0**
- **show platform software wired-client R0**
- **show platform software wired-client F0**
- **show platform software process database forwarding-manager R0 summary**
- **show platform software process database forwarding-manager F0 summary**
- **show platform software object-manager F0 pending-ack-update**
- **show platform software object-manager F0 pending-issue-update**
- **show platform software object-manager F0 error-object**
- **show platform software peer forwarding-manager R0**
- **show platform software peer forwarding-manager F0**
- **show platform software VP R0 summary**
- **show platform software VP F0 summary**
- **show platform software fed punt cpuq**
- **show platform software fed punt cause summary**
- **show platform software fed inject cause summary**
- **show platform hardware fed fwd-asic drops exceptions**
- **show platform hardware fed fwd-asic resource tcam table acl**
- **show platform software fed acl counter hardware**
- **show platform software fed matm macTable**
- **show platform software fed ifm mappings**
- **show platform software trace message fed reverse**
- **show platform software trace message forwarding-manager R0 reverse**
- **show platform software trace message forwarding-manager F0 reverse**
- **show platform software trace message smd R0 reverse**
- **show authentication sessions mac details**
- **show platform software wired-client**
- **show platform software process database forwarding-manager summary**
- **show platform software object-manager pending-ack-update**
- **show platform software object-manager pending-issue-update**
- **show platform software object-manager error-object**
- **show platform software peer forwarding-manager**
- **show platform software VP summary**

- **show platform software trace message forwarding-manager reverse**
- **show ip admission cache**
- **show platform software trace message smd reverse**
- **show platform software fed punt cpuq**
- **show platform software fed punt cause summary**
- **show platform software fed inject cause summary**
- **show platform hardware fed fwd-asic drops exceptions**
- **show platform hardware fed fwd-asic resource tcam table acl**
- **show platform software fed acl counter hardware**
- **show platform software fed matm macTable**
- **show platform software fed ifm mappings**
- **show platform software trace message fed reverse**

例

次に、**show tech-support identity** コマンドの出力例を示します。

```
Device# show tech-support identity mac 0000.0001.0003 interface gigabitethernet1/0/1

.
.
.
------------------ show platform software peer forwarding-manager R0  ------------------

IOSD Connection Information:

  MQIPC (reader) Connection State: Connected, Read-selected
    Connections: 1, Failures: 22
    3897 packet received (0 dropped), 466929 bytes
    Read attempts: 2352, Yields: 0
  BIPC Connection state: Connected, Ready
    Accepted: 1, Rejected: 0, Closed: 0, Backpressures: 0
    36 packets sent, 2808 bytes

SMD Connection Information:

  MQIPC (reader) Connection State: Connected, Read-selected
    Connections: 1, Failures: 30
    0 packet received (0 dropped), 0 bytes
    Read attempts: 1, Yields: 0
  MQIPC (writer) Connection State: Connected, Ready
    Connections: 1, Failures: 0, Backpressures: 0
    0 packet sent, 0 bytes

FP Peers Information:

  Slot: 0
    Peer state: connected
    OM ID: 0, Download attempts: 638
      Complete: 638, Yields: 0, Spurious: 0
      IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
    Back-Pressure asserted for IPC: 0, IPC-Log: 1
    Number of FP FMAN peer connection expected: 7
```

```
  Number of FP FMAN online msg received: 1
  IPC state: unknown

  Config IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf3d48e8, BIPC FD: 36, Peer Context: 0xdf3e7158
    Tx Packets: 688, Messages: 2392, ACKs: 36
    Rx Packets: 37, Bytes: 2068

    IPC Log:
      Peer name: fman-log-bay0-peer0
      Flags: Recovery-Complete
      Send Seq: 36, Recv Seq: 36, Msgs Sent: 0, Msgs Recovered: 0

  Upstream FMRP IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf3e7308, BIPC FD: 37, Peer Context: 0xdf3e7158
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0

  Upstream FMRP-IOSd IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf3f9c38, BIPC FD: 38, Peer Context: 0xdf3e7158
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 37, Bytes: 2864
    Rx ACK Requests: 1, Tx ACK Responses: 1

  Upstream FMRP-SMD IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf40c568, BIPC FD: 39, Peer Context: 0xdf3e7158
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-WNCD_0 IPC Context:
    State: Connected
    BIPC Handle: 0xdf4317c8, BIPC FD: 41, Peer Context: 0xdf3e7158
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-WNCMGRD IPC Context:
    State: Connected
    BIPC Handle: 0xdf41ee98, BIPC FD: 40, Peer Context: 0xdf3e7158
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-MOBILITYD IPC Context:
    State: Connected
    BIPC Handle: 0xdf4440f8, BIPC FD: 42, Peer Context: 0xdf3e7158
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

Slot: 1
Peer state: connected
  OM ID: 1, Download attempts: 1
    Complete: 1, Yields: 0, Spurious: 0
    IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
  Back-Pressure asserted for IPC: 0, IPC-Log: 0
  Number of FP FMAN peer connection expected: 7
  Number of FP FMAN online msg received: 1
  IPC state: unknown
```

```
    Config IPC Context:
      State: Connected, Read-selected
      BIPC Handle: 0xdf45e4d8, BIPC FD: 48, Peer Context: 0xdf470e18
      Tx Packets: 20, Messages: 704, ACKs: 1
      Rx Packets: 2, Bytes: 108

      IPC Log:
        Peer name: fman-log-bay0-peer1
        Flags: Recovery-Complete
        Send Seq: 1, Recv Seq: 1, Msgs Sent: 0, Msgs Recovered: 0

    Upstream FMRP IPC Context:
      State: Connected, Read-selected
      BIPC Handle: 0xdf470fc8, BIPC FD: 49, Peer Context: 0xdf470e18
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0

    Upstream FMRP-IOSd IPC Context:
      State: Connected, Read-selected
      BIPC Handle: 0xdf4838f8, BIPC FD: 50, Peer Context: 0xdf470e18
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0
      Rx ACK Requests: 0, Tx ACK Responses: 0

    Upstream FMRP-SMD IPC Context:
      State: Connected, Read-selected
      BIPC Handle: 0xdf496228, BIPC FD: 51, Peer Context: 0xdf470e18
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0
      Rx ACK Requests: 0, Tx ACK Responses: 0

    Upstream FMRP-WNCD_0 IPC Context:
      State: Connected
      BIPC Handle: 0xdf4bb488, BIPC FD: 53, Peer Context: 0xdf470e18
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0
      Rx ACK Requests: 0, Tx ACK Responses: 0

    Upstream FMRP-WNCMGRD IPC Context:
      State: Connected
      BIPC Handle: 0xdf4a8b58, BIPC FD: 52, Peer Context: 0xdf470e18
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0
      Rx ACK Requests: 0, Tx ACK Responses: 0

    Upstream FMRP-MOBILITYD IPC Context:
      State: Connected
      BIPC Handle: 0xdf4cddb8, BIPC FD: 54, Peer Context: 0xdf470e18
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0
      Rx ACK Requests: 0, Tx ACK Responses: 0



------------------ show platform software peer forwarding-manager R0  ------------------

IOSD Connection Information:

  MQIPC (reader) Connection State: Connected, Read-selected
    Connections: 1, Failures: 22
    3897 packet received (0 dropped), 466929 bytes
    Read attempts: 2352, Yields: 0
```

```
  BIPC Connection state: Connected, Ready
    Accepted: 1, Rejected: 0, Closed: 0, Backpressures: 0
    36 packets sent, 2808 bytes

SMD Connection Information:

  MQIPC (reader) Connection State: Connected, Read-selected
    Connections: 1, Failures: 30
    0 packet received (0 dropped), 0 bytes
    Read attempts: 1, Yields: 0
  MQIPC (writer) Connection State: Connected, Ready
    Connections: 1, Failures: 0, Backpressures: 0
    0 packet sent, 0 bytes

FP Peers Information:

  Slot: 0
    Peer state: connected
    OM ID: 0, Download attempts: 638
      Complete: 638, Yields: 0, Spurious: 0
      IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
    Back-Pressure asserted for IPC: 0, IPC-Log: 1
    Number of FP FMAN peer connection expected: 7
    Number of FP FMAN online msg received: 1
    IPC state: unknown

    Config IPC Context:
      State: Connected, Read-selected
      BIPC Handle: 0xdf3d48e8, BIPC FD: 36, Peer Context: 0xdf3e7158
      Tx Packets: 688, Messages: 2392, ACKs: 36
      Rx Packets: 37, Bytes: 2068

      IPC Log:
        Peer name: fman-log-bay0-peer0
        Flags: Recovery-Complete
        Send Seq: 36, Recv Seq: 36, Msgs Sent: 0, Msgs Recovered: 0

    Upstream FMRP IPC Context:
      State: Connected, Read-selected
      BIPC Handle: 0xdf3e7308, BIPC FD: 37, Peer Context: 0xdf3e7158
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0

    Upstream FMRP-IOSd IPC Context:
      State: Connected, Read-selected
      BIPC Handle: 0xdf3f9c38, BIPC FD: 38, Peer Context: 0xdf3e7158
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 37, Bytes: 2864
      Rx ACK Requests: 1, Tx ACK Responses: 1

    Upstream FMRP-SMD IPC Context:
      State: Connected, Read-selected
      BIPC Handle: 0xdf40c568, BIPC FD: 39, Peer Context: 0xdf3e7158
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0
      Rx ACK Requests: 0, Tx ACK Responses: 0

    Upstream FMRP-WNCD_0 IPC Context:
      State: Connected
      BIPC Handle: 0xdf4317c8, BIPC FD: 41, Peer Context: 0xdf3e7158
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0
      Rx ACK Requests: 0, Tx ACK Responses: 0
```

```
  Upstream FMRP-WNCMGRD IPC Context:
    State: Connected
    BIPC Handle: 0xdf41ee98, BIPC FD: 40, Peer Context: 0xdf3e7158
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-MOBILITYD IPC Context:
    State: Connected
    BIPC Handle: 0xdf4440f8, BIPC FD: 42, Peer Context: 0xdf3e7158
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

Slot: 1
Peer state: connected
  OM ID: 1, Download attempts: 1
    Complete: 1, Yields: 0, Spurious: 0
    IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
  Back-Pressure asserted for IPC: 0, IPC-Log: 0
  Number of FP FMAN peer connection expected: 7
  Number of FP FMAN online msg received: 1
  IPC state: unknown

  Config IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf45e4d8, BIPC FD: 48, Peer Context: 0xdf470e18
    Tx Packets: 20, Messages: 704, ACKs: 1
    Rx Packets: 2, Bytes: 108

    IPC Log:
      Peer name: fman-log-bay0-peer1
      Flags: Recovery-Complete
      Send Seq: 1, Recv Seq: 1, Msgs Sent: 0, Msgs Recovered: 0

  Upstream FMRP IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf470fc8, BIPC FD: 49, Peer Context: 0xdf470e18
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0

  Upstream FMRP-IOSd IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf4838f8, BIPC FD: 50, Peer Context: 0xdf470e18
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-SMD IPC Context:
    State: Connected, Read-selected
    BIPC Handle: 0xdf496228, BIPC FD: 51, Peer Context: 0xdf470e18
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-WNCD_0 IPC Context:
    State: Connected
    BIPC Handle: 0xdf4bb488, BIPC FD: 53, Peer Context: 0xdf470e18
    TX Packets: 0, Bytes: 0, Drops: 0
    Rx Packets: 0, Bytes: 0
    Rx ACK Requests: 0, Tx ACK Responses: 0

  Upstream FMRP-WNCMGRD IPC Context:
    State: Connected
```

```
      BIPC Handle: 0xdf4a8b58, BIPC FD: 52, Peer Context: 0xdf470e18
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0
      Rx ACK Requests: 0, Tx ACK Responses: 0

    Upstream FMRP-MOBILITYD IPC Context:
      State: Connected
      BIPC Handle: 0xdf4cddb8, BIPC FD: 54, Peer Context: 0xdf470e18
      TX Packets: 0, Bytes: 0, Drops: 0
      Rx Packets: 0, Bytes: 0
      Rx ACK Requests: 0, Tx ACK Responses: 0



------------------ show platform software VP R0 summary ------------------


Forwarding Manager Vlan Port Information

  Vlan    Intf-ID   Stp-state
  ------------------------------------------------------------------------------
  1       7           Forwarding
  1       9           Forwarding
  1       17          Forwarding
  1       27          Forwarding
  1       28          Forwarding
  1       29          Forwarding
  1       30          Forwarding
  1       31          Forwarding
  1       40          Forwarding
  1       41          Forwarding


Forwarding Manager Vlan Port Information

  Vlan    Intf-ID   Stp-state
  ------------------------------------------------------------------------------
  1       49          Forwarding
  1       51          Forwarding
  1       63          Forwarding
  1       72          Forwarding
  1       73          Forwarding
  1       74          Forwarding



------------------ show platform software VP R0 summary ------------------


Forwarding Manager Vlan Port Information

  Vlan    Intf-ID   Stp-state
  ------------------------------------------------------------------------------
  1       7           Forwarding
  1       9           Forwarding
  1       17          Forwarding
  1       27          Forwarding
  1       28          Forwarding
  1       29          Forwarding
  1       30          Forwarding
  1       31          Forwarding
  1       40          Forwarding
  1       41          Forwarding
```

```
Forwarding Manager Vlan Port Information

  Vlan    Intf-ID   Stp-state
  ------------------------------------------------------------------------------
  1       49          Forwarding
  1       51          Forwarding
  1       63          Forwarding
  1       72          Forwarding
  1       73          Forwarding
  1       74          Forwarding
.
.
.
```

show vlan access-map

特定の VLAN アクセス マップまたはすべての VLAN アクセス マップに関する情報を表示するには、特権 EXEC モードで **show vlan access-map** コマンドを使用します。

show vlan access-map [*map-name*]

構文の説明

map-name	（任意）特定の VLAN アクセスマップ名。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

次に、**show vlan access-map** コマンドの出力例を示します。

```
デバイス# show vlan access-map
Vlan access-map "vmap4"  10
  Match clauses:
    ip  address: al2
  Action:
    forward
Vlan access-map "vmap4"  20
  Match clauses:
    ip  address: al2
  Action:
    forward
```

show vlan filter

すべての VLAN フィルタ、または特定の VLAN または VLAN アクセス マップに関する情報を表示するには、特権 EXEC モードで **show vlan filter** コマンドを使用します。

show vlan filter {**access-map** *name* | **vlan** *vlan-id*}

構文の説明

access-map *name*	（任意）指定された VLAN アクセス マップのフィルタリング情報を表示します。
vlan *vlan-id*	（任意）指定された VLAN のフィルタリング情報を表示します。指定できる範囲は 1 ～ 4094 です。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

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

```
デバイス# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

show vlan group

VLAN グループにマッピングされている VLAN を表示するには、特権 EXEC モードで **show vlan group** コマンドを使用します。

show vlan group [{**group-name** *vlan-group-name* [**user_count**]}]

構文の説明

group-name *vlan-group-name*	（任意）指定した VLAN グループにマッピングされている VLAN を表示します。
user_count	（任意）特定の VLAN グループにマッピングされている各 VLAN のユーザ数を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

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

使用上のガイドライン

show vlan group コマンドは既存の VLAN グループを表示し、各 VLAN グループのメンバである VLAN および VLAN の範囲を示します。**group-name** キーワードを入力すると、指定した VLAN グループのメンバのみが表示されます。

次の例では、特定の VLAN グループのメンバを表示する方法を示します。

```
デバイス# show vlan group group-name group2
vlan group group1 :40-45
```

次に、グループ内の各 VLAN のユーザ数を表示する例を示します。

```
デバイス# show vlan group group-name group2 user_count
  VLAN     : Count
-------------------
  40         : 5
  41         : 8
  42         : 12
  43         : 2
  44         : 9
  45         : 0
```

storm-control

ブロードキャスト、マルチキャスト、またはユニキャストストーム制御をイネーブルにして、インターフェイスのしきい値レベルを設定するには、インターフェイスコンフィギュレーション モードで **storm-control** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

storm-control {**action** {**shutdown** | **trap**} | {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]}}
no storm-control {**action** {**shutdown** | **trap**} | {**broadcast** | **multicast** | **unicast**} **level**}

構文の説明

action	ポートでストームが発生した場合に実行されるアクションを指定します。デフォルト アクションは、トラフィックをフィルタリングし、簡易ネットワーク管理プロトコル（SNMP）トラップを送信しません。
shutdown	ストームの間、ポートをディセーブルにします。
trap	ストームが発生した場合に SNMP トラップを送信します。
broadcast	インターフェイス上でブロードキャスト ストーム制御をイネーブルにします。
multicast	インターフェイス上でマルチキャスト ストーム制御をイネーブルにします。

unicast	インターフェイス上でユニキャスト ストーム制御をイネーブルにします。
level	上限および下限抑制レベルをポートの全帯域幅の割合で指定します。
level	上限抑制レベル（小数点以下第2位まで）。指定できる範囲は0.00～100.00です。指定した level の値に達した場合、ストーム パケットのフラッディングをブロックします。
level-low	（任意）下限抑制レベル（小数点以下第 2 位まで）。指定できる範囲は 0.00 ～ 100.00 です。この値は上限抑制値より小さいか、または等しくなければなりません。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。
level bps	上限および下限抑制レベルを、ポートで受信するトラフィックの速度（ビット/秒）で指定します。
bps	上限抑制レベル（小数点以下第1位まで）。指定できる範囲は0.0～10000000000.0です。指定した bps の値に達した場合、ストーム パケットのフラッディングをブロックします。 大きい数値のしきい値には、k、m、g などのメトリック サフィクスを使用できます。
bps-low	（任意）下限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。この値は上限抑制値に等しいか、または小さくなければなりません。 大きい数値のしきい値には、k、m、g などのメトリック サフィクスを使用できます。
level pps	上限および下限抑制レベルを、ポートで受信するトラフィックの速度（パケット/秒）で指定します。
pps	上限抑制レベル（小数点以下第1位まで）。指定できる範囲は0.0～10000000000.0です。指定した pps の値に達した場合、ストーム パケットのフラッディングをブロックします。 大きい数値のしきい値には、k、m、g などのメトリック サフィクスを使用できます。
pps-low	（任意）下限抑制レベル（小数点以下第 1 位まで）。指定できる範囲は 0.0 ～ 10000000000.0 です。この値は上限抑制値に等しいか、または小さくなければなりません。 大きい数値のしきい値には、k、m、g などのメトリック サフィクスを使用できます。

コマンド デフォルト

ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御はディセーブルです。

デフォルト アクションは、トラフィックをフィルタリングし、SNMP トラップを送信しません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

ストーム制御抑制レベルは、ポートの全帯域幅の割合、またはトラフィックを受信する速度（1秒あたりのパケット数、または 1 秒あたりのビット数）で入力できます。

全帯域幅の割合で指定した場合、100% の抑制値は、指定したトラフィック タイプに制限が設定されていないことを意味します。**level 0 0** の値は、ポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャストトラフィックをブロックします。ストーム制御は、上限抑制レベルが 100% 未満の場合にだけイネーブルになります。他のストーム制御設定が指定されていない場合、デフォルトアクションは、ストームの原因となっているトラフィックをフィルタリングし、SNMP トラップを送信しません。

（注） マルチキャスト トラフィックのストーム制御しきい値に達した場合、ブリッジプロトコルデータ ユニット（BPDU）および Cisco Discovery Protocol（CDP）フレームなどの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。ただし、スイッチは、Open Shortest Path First（OSPF）および通常のマルチキャスト データ トラフィック間のように、ルーティング アップデート間を区別しないため、両方のタイプのトラフィックがブロックされます。

trap および **shutdown** オプションは、互いに独立しています。

パケットストームが検出されたときにシャットダウンを行う（ストームの間、ポートが error-disabled になる）ようにアクションを設定する場合、インターフェイスをこのステートから解除するには **no shutdown** インターフェイス コンフィギュレーション コマンドを使用する必要があります。**shutdown** アクションを指定しない場合、アクションを **trap**（ストーム検出時にスイッチがトラップを生成する）に指定してください。

ストームが発生し、実行されるアクションがトラフィックのフィルタリングである場合、下限抑制レベルが指定されていないと、トラフィック レートが上限抑制レベルより低くなるまでスイッチはすべてのトラフィックをブロックします。下限抑制レベルが指定されている場合、トラフィック レートがこのレベルより低くなるまでスイッチはトラフィックをブロックします。

（注） ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ブロードキャスト ストームが発生し、実行されるアクションがトラフィックのフィルタである場合、スイッチはブロードキャスト トラフィックだけをブロックします。

詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

次の例では、75.5% の上限抑制レベルでブロードキャスト ストーム制御をイネーブルにする方法を示します。

```
デバイス(config-if)# storm-control broadcast level 75.5
```

次の例では、87% の上限抑制レベルと 65% の下限抑制レベルのポートでユニキャスト ストーム制御をイネーブルにする方法を示します。

```
デバイス(config-if)# storm-control unicast level 87 65
```

次の例では、2000 パケット/秒の上限抑制レベルと 1000 パケット/秒の下限抑制レベルのポートでマルチキャスト ストーム制御をイネーブルにする方法を示します。

```
デバイス(config-if)# storm-control multicast level pps 2k 1k
```

次の例では、ポートで **shutdown** アクションをイネーブルにする方法を示します。

```
デバイス(config-if)# storm-control action shutdown
```

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

switchport port-security aging

セキュアアドレスエントリのエージングタイムおよびタイプを設定する、または特定のポートのセキュアアドレスのエージング動作を変更するには、インターフェイス コンフィギュレーション モードで **switchport port-security aging** コマンドを使用します。ポート セキュリティ エージングをディセーブルにする、またはパラメータをデフォルトの状態に設定するには、このコマンドの **no** 形式を使用します。

switchport port-security aging {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}
no switchport port-security aging {**static** | **time** | **type**}

構文の説明

static	このポートに静的に設定されたセキュア アドレスのエージングをイネーブルにします。
time *time*	このポートのエージング タイムを指定します。指定できる範囲は 0 ～ 1440 分です。time が 0 の場合、このポートのエージングはディセーブルです。
type	エージング タイプを設定します。
absolute	absolute エージング タイプを設定します。このポートのすべてのセキュア アドレスは、指定された時間（分）が経過した後に期限切れとなり、セキュア アドレス リストから削除されます。

inactivity	inactivityエージング タイプを設定します。指定された時間内にセキュア送信元アドレスからのデータ トラフィックがない場合だけ、このポートのセキュア アドレスが期限切れになります。

コマンド デフォルト

ポート セキュリティ エージング機能はディセーブルです。デフォルトの時間は 0 分です。

デフォルトのエージング タイプは absolute です。

デフォルトのスタティック エージング動作はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

特定のポートのセキュア アドレス エージングをイネーブルにするには、ポート エージング タイムを 0 以外の値に設定します。

特定のセキュアアドレスに時間を限定してアクセスできるようにするには、エージングタイプを **absolute** に設定します。エージング タイムの期限が切れると、セキュア アドレスが削除されます。

継続的にアクセスできるセキュアアドレス数を制限するには、エージングタイプを **inactivity** に設定します。このようにすると、非アクティブになったセキュアアドレスが削除され、他のアドレスがセキュアになることができます。

セキュアアドレスへのアクセス制限を解除するには、セキュアアドレスとして設定し、**no switchport port-security aging static** インターフェイス コンフィギュレーション コマンドを使用して、静的に設定されたセキュアアドレスのエージングをディセーブルにします。

次の例では、ポートのすべてのセキュア アドレスに対して、エージング タイプを absolute、エージング タイムを 2 時間に設定します。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# switchport port-security aging time 120
```

次の例では、ポートに設定されたセキュア アドレスに対して、エージング タイプを inactivity、エージング タイムを 2 分に設定します。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# switchport port-security aging time 2
デバイス(config-if)# switchport port-security aging type inactivity
デバイス(config-if)# switchport port-security aging static
```

次の例では、設定されたセキュア アドレスのエージングをディセーブルにする方法を示します。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# no switchport port-security aging static
```

switchport port-security mac-address

セキュアMACアドレスまたはスティッキMACアドレスラーニングを設定するには、**switchport port-security mac-address** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security mac-address {*mac-address* [{**vlan** {*vlan-id* {**access** | **voice**}}}] | **sticky** [{*mac-address* | **vlan** {*vlan-id* {**access** | **voice**}}}]}
no switchport port-security mac-address {*mac-address* [{**vlan** {*vlan-id* {**access** | **voice**}}}] | **sticky** [{*mac-address* | **vlan** {*vlan-id* {**access** | **voice**}}}]}

構文の説明

mac-address	48 ビット MAC アドレスの入力によって指定するインターフェイスのセキュア MAC アドレス。設定された最大数まで、セキュア MAC アドレスを追加できます。
vlan *vlan-id*	（任意）トランク ポート上でだけ、VLAN ID および MAC アドレスを指定します。VLAN ID を指定しない場合は、ネイティブ VLAN が使用されます。
vlan access	（任意）アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。
vlan voice	（任意）アクセス ポートでだけ、VLAN を音声 VLAN として指定します。 （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。
sticky	スティッキ ラーニングのインターフェイスをイネーブルにします。スティッキ ラーニングをイネーブルにすると、インターフェイスは動的に学習したすべてのセキュア MAC アドレスを実行コンフィギュレーションに追加して、これらのアドレスをスティッキ セキュア MAC アドレスに変換します。
mac-address	（任意）スティッキ セキュア MAC アドレスを指定する MAC アドレス。

コマンド デフォルト

セキュア MAC アドレスは設定されていません。

スティッキ ラーニングはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることはできますが、ダイナミック アクセス ポートには設定できません。
- セキュア ポートはルーテッド ポートにはできません。
- セキュア ポートは保護ポートにはできません。
- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。
- セキュア ポートをギガビットまたは 10 ギガビット EtherChannel ポート グループに含めることはできません。
- 音声 VLAN では、スタティック セキュアまたはスティッキ セキュア MAC アドレスを設定できません。
- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュア アドレスを設定する必要があります。
- 音声 VLAN はアクセス ポート上でだけサポートされます。トランク ポート上ではサポートされません。

スティッキ セキュア MAC アドレスには、次の特性があります。

- **switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイス上でスティッキラーニングをイネーブルにした場合、インターフェイスはすべてのダイナミックセキュア MAC アドレス（スティッキラーニングがイネーブルになる前に動的に学習されたアドレスを含む）を、スティッキセキュア MAC アドレスに変換し、すべてのスティッキセキュア MAC アドレスを実行コンフィギュレーションに追加します。
- **no switchport port-security mac-address sticky** インターフェイス コンフィギュレーション コマンドを使用して、スティッキラーニングをディセーブルする場合、または実行コンフィギュレーションを削除する場合は、スティッキセキュア MAC アドレスは実行コンフィギュレーションの一部に残りますが、アドレステーブルからは削除されます。削除されたアドレスはダイナミックに再設定することができ、ダイナミック アドレスとしてアドレス テーブルに追加されます。
- **switchport port-security mac-address sticky** *mac-address* インターフェイス コンフィギュレーション コマンドを使用して、スティッキセキュア MAC アドレスを設定する場合、これらのアドレスはアドレステーブルおよび実行コンフィギュレーションに追加されます。ポート セキュリティがディセーブルの場合、スティッキ セキュア MAC アドレスは実行コンフィギュレーションに残ります。

- スティッキ セキュア MAC アドレスがコンフィギュレーション ファイルに保存されていると、スイッチの再起動時、またはインターフェイスのシャットダウン時に、インターフェイスはこれらのアドレスを再学習しなくてすみます。スティッキ セキュア アドレスを保存しない場合、アドレスは失われます。スティッキ ラーニングがディセーブルの場合、スティッキ セキュア MAC アドレスはダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。
- スティッキラーニングをディセーブルにして、**switchport port-security mac-address sticky** *mac-address* インターフェイス コンフィギュレーション コマンドを入力した場合、エラーメッセージが表示され、スティッキセキュア MAC アドレスは実行コンフィギュレーションに追加されません。

設定を確認するには、**show port-security** 特権 EXEC コマンドを使用します。

次の例では、ポートでセキュア MAC アドレスと VLAN ID を設定する方法を示します。

```
デバイス(config)# interface gigabitethernet 2/0/2
デバイス(config-if)# switchport mode trunk
デバイス(config-if)# switchport port-security
デバイス(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

次の例では、スティッキ ラーニングをイネーブルにして、ポート上で 2 つのスティッキ セキュア MAC アドレスを入力する方法を示します。

```
デバイス(config)# interface gigabitethernet 2/0/2
デバイス(config-if)# switchport port-security mac-address sticky
デバイス(config-if)# switchport port-security mac-address sticky 0000.0000.4141
デバイス(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

switchport port-security maximum

セキュア MAC アドレスの最大数を設定するには、インターフェイス コンフィギュレーション モードで **switchport port-security maximum** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security maximum *value* [**vlan** [{*vlan-list* | [{**access** | **voice**}]}]]
no switchport port-security maximum *value* [**vlan** [{*vlan-list* | [{**access** | **voice**}]}]]

構文の説明

value	インターフェイスのセキュア MAC アドレスの最大数を設定します。 デフォルトの設定は 1 秒です。
vlan	（任意）トランク ポートの場合、VLAN ごとまたは一定範囲の VLAN のセキュア MAC アドレスの最大数を設定します。**vlan** キーワードが入力されていない場合、デフォルト値が使用されます。

vlan-list	（任意）カンマで区切られたVLANの範囲またはハイフンで区切られた一連のVLAN。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。
access	（任意）アクセス ポートでだけ、VLAN をアクセス VLAN として指定します。
voice	（任意）アクセス ポートでだけ、VLAN を音声 VLAN として指定します。 （注） **voice** キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。

コマンド デフォルト

ポートセキュリティをイネーブルにしてキーワードを入力しない場合、デフォルトのセキュア MAC アドレスの最大数は 1 です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

スイッチまたはスイッチ スタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されているMACアドレスの最大数によって決まります。この数字はアクティブなSwitch Database Management（SDM）テンプレートによって決められます。**sdm prefer** コマンドを参照してください。この数字は、インターフェイスで設定された他のレイヤ 2 機能やその他のセキュア MAC アドレスなど、利用可能な MAC アドレスの合計数を示します。

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることができますが、ダイナミック アクセス ポートには設定できません。
- セキュア ポートはルーテッド ポートにはできません。
- セキュア ポートは保護ポートにはできません。
- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。
- セキュア ポートをギガビットまたは 10 ギガビット EtherChannel ポート グループに含めることはできません。
- 音声 VLAN が設定されたインターフェイス上でポート セキュリティをイネーブルにする場合は、ポートの最大セキュア アドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。2 台以上の PC を Cisco IP Phone に接続する場合、各 PC に 1 つ、さらに Cisco IP Phone に 1 つ割り当てるよう十分なセキュア アドレスを設定する必要があります。

音声 VLAN はアクセス ポート上でだけサポートされます。トランク ポート上ではサポートされません。

- インターフェイスのセキュアアドレスの最大値を入力する場合、新しい値が前回の値より大きいと、新しい値によって前回の設定値が上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュア アドレス数が新しい値より大きい場合、コマンドは拒否されます。

  アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、確実にデバイスがポートの帯域幅を完全に使用できます。

インターフェイスのセキュア アドレスの最大値を入力すると、次の事象が発生します。

- 新しい値が前回の値より大きい場合、新しい値によって前回の設定値が上書きされます。
- 新しい値が前回の値より小さく、インターフェイスで設定されているセキュアアドレス数が新しい値より大きい場合、コマンドは拒否されます。

設定を確認するには、**show port-security** 特権 EXEC コマンドを使用します。

次の例では、ポートでポートセキュリティをイネーブルにし、セキュアアドレスの最大数を 5 に設定する方法を示します。違反モードはデフォルトで、セキュア MAC アドレスは設定されていません。

```
デバイス(config)# interface gigabitethernet 2/0/2
デバイス(config-if)# switchport mode access
デバイス(config-if)# switchport port-security
デバイス(config-if)# switchport port-security maximum 5
```

switchport port-security violation

セキュア MAC アドレスの違反モード、またはポートセキュリティに違反した場合に実行するアクションを設定するには、インターフェイス コンフィギュレーション モードで **switchport port-security violation** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security violation {**protect** | **restrict** | **shutdown** | **shutdown vlan**}
no switchport port-security violation {**protect** | **restrict** | **shutdown** | **shutdown vlan**}

構文の説明

protect	セキュリティ違反保護モードを設定します。
restrict	セキュリティ違反制限モードを設定します。
shutdown	セキュリティ違反シャットダウン モードを設定します。
shutdown vlan	VLAN ごとのシャットダウンにセキュリティ違反モードを設定します。

コマンド デフォルト

デフォルトの違反モードは **shutdown** です。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

セキュリティ違反保護モードでは、ポートのセキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。ドロップすることでセキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。セキュリティ違反が起こっても、ユーザには通知されません。

（注） トランク ポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。

セキュリティ違反制限モードでは、セキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされます。セキュア MAC アドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。

セキュリティ違反シャットダウン モードでは、違反が発生し、ポートの LED がオフになると、インターフェイスが errdisable になります。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。セキュア ポートが errdisable ステートの場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力してこのステートを解除するか、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力して手動で再びイネーブルにできます。

セキュリティ違反モードが VLAN ごとのシャットダウンに設定されると、違反が発生した VLAN のみが errdisable になります。

セキュア ポートに関する制限事項は、次のとおりです。

- セキュア ポートはアクセス ポートまたはトランク ポートにすることができますが、ダイナミック アクセス ポートには設定できません。
- セキュア ポートはルーテッド ポートにはできません。
- セキュア ポートは保護ポートにはできません。
- セキュア ポートをスイッチド ポート アナライザ（SPAN）の宛先ポートにすることはできません。

- セキュア ポートをギガビットまたは 10 ギガビット EtherChannel ポート グループに含めることはできません。

  セキュア MAC アドレスの最大値がアドレス テーブルに存在し、アドレス テーブルに存在しない MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合、または別のセキュア ポートのセキュア MAC アドレスとして設定された MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合に、セキュリティ違反が起こります。

  セキュアポートが errdisable ステートの場合は、**errdisable recovery cause** *psecure-violation* グローバル コンフィギュレーション コマンドを入力して、このステートから回復させることができます。**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力するか、**clear errdisable interface** 特権 EXEC コマンドを使用して、ポートを手動で再びイネーブルにすることができます。

設定を確認するには、**show port-security** 特権 EXEC コマンドを使用します。

次の例では、MAC セキュリティ違反が発生した場合に VLAN のみをシャットダウンするようポートを設定する方法を示します。

```
デバイス(config)# interface gigabitethernet2/0/2
デバイス(config)# switchport port-security violation shutdown vlan
```

tacacs server

IPv6 または IPv4 用に TACACS+ サーバを設定し、TACACS+ サーバ 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 **tacacs server** 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。

tacacs server *name*
no tacacs server

構文の説明

name	プライベート TACACS+ サーバ ホストの名前。

コマンド デフォルト

TACACS+ サーバは構成されていません。

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 3.3SE	このコマンドが導入されました。

使用上のガイドライン

tacacs server コマンドは、*name* 引数を使用して TACACS サーバを設定し、TACACS+ サーバ コンフィギュレーション モードを開始します。設定が完了し、TACACS+ サーバ コンフィギュレーション モードを終了すると、設定が適用されます。

例

次の例は、名前 server1 を使用して TACACS サーバを設定し、さらに設定を行うために TACACS+ サーバ コンフィギュレーション モードを開始する方法を示しています。

```
Device(config)# tacacs server server1
Device(config-server-tacacs)#
```

関連コマンド

Command	Description
address ipv6 (TACACS+)	TACACS+ サーバの IPv6 アドレスを設定します。
key (TACACS+)	TACACS+ サーバでサーバ単位の暗号キーを設定します。
port (TACACS+)	TACACS+ 接続に使用する TCP ポートを指定します。
send-nat-address (TACACS+)	クライアントの NAT 後のアドレスを TACACS+ サーバに送信します。
single-connection **(TACACS+)**	単一の TCP 接続を使用してすべての TACACS パケットを同じサーバに送信できるようにします。
timeout **(TACACS+)**	指定された TACACS サーバからの応答を待機する時間を設定します。

tracking（IPv6 スヌーピング）

ポートでデフォルトのトラッキングポリシーを上書きするには、IPv6 スヌーピング ポリシー コンフィギュレーション モードで **tracking** コマンドを使用します。

tracking {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}

構文の説明

enable	トラッキングをイネーブルにします。
reachable-lifetime	（任意）到達可能という証明がない状態で、到達可能なエントリが直接的または間接的に到達可能であると判断される最大時間を指定します。 • **reachable-lifetime** キーワードを使用できるのは、**enable** キーワードが指定されている場合のみです。 • **reachable-lifetime** キーワードを使用すると、 **ipv6 neighbor binding reachable-lifetime** コマンドで設定されたグローバルな到達可能ライフタイムが上書きされます。

value	秒単位のライフタイム値。指定できる範囲は 1 ～ 86400 で、デフォルトは 300 です。
infinite	エントリを無限に到達可能状態またはステイル状態に維持します。
disable	トラッキングをディセーブルにします。
stale-lifetime	（任意）時間エントリをステイル状態に維持します。これによりグローバルの stale-lifetime 設定が上書きされます。 • ステイル ライフタイムは 86,400 秒です。 • **stale-lifetime** キーワードを使用できるのは、**disable** キーワードが指定されている場合のみです。 • **stale-lifetime** キーワードを使用すると、**ipv6 neighbor binding stale-lifetime** コマンドで設定されたグローバルなステイルライフタイムが上書きされます。

コマンド デフォルト

時間のエントリは到達可能な状態に維持されます。

コマンド モード

IPv6 スヌーピング コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

tracking コマンドは、このポリシーが適用されるポート上で **ipv6 neighbor tracking** コマンドによって設定されたデフォルトのトラッキングポリシーに優先します。この機能は、たとえば、エントリを追跡しないが、バインディングテーブルにエントリを残して盗難を防止する場合などに、信頼できるポート上で有用です。

reachable-lifetime キーワードは、到達可能という証明がない状態で、あるエントリがトラッキングにより直接的に、または IPv6 スヌーピングにより間接的に到達可能であると判断される最大時間を示します。**reachable-lifetime** 値に到達すると、エントリはステイル状態に移行します。tracking コマンドで **reachable-lifetime** キーワードを使用すると、**ipv6 neighbor binding reachable-lifetime** コマンドで設定されたグローバルな到達可能ライフタイムが上書きされます。

stale-lifetime キーワードは、エントリが削除されるか、直接または間接的に到達可能であると証明される前にテーブルに保持される最大時間です。**tracking** コマンドで **reachable-lifetime** キーワードを使用すると、**ipv6 neighbor binding stale-lifetime** コマンドで設定されたグローバルなステイルライフタイムが上書きされます。

次に、IPv6 スヌーピングポリシー名を policy1 と定義し、スイッチを IPv6 スヌーピング ポリシー コンフィギュレーション モードにし、エントリを信頼できるポート上で無限にバインディング テーブルに保存するように設定する例を示します。

```
デバイス(config)# ipv6 snooping policy policy1
デバイス(config-ipv6-snooping)# tracking disable stale-lifetime infinite
```

trusted-port

あるポートを信頼できるポートとして設定するには、IPv6 スヌーピング ポリシー モードまたは ND 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 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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
```

username

ユーザ名ベースの認証システムを確立するには、グローバル 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。確立されたユーザ名ベースの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。

username *name* [**aaa attribute list** *aaa-list-name*]
username *name* [**access-class** *access-list-number*]
username *name* [**algorithm-type** {**md5** | **scrypt** | **sha256** }]
username *name* [**autocommand** *command*]
username *name* [**callback-dialstring** *telephone-number*]
username *name* [**callback-line** [**tty**] *line-number* [*ending-line-number*]]
username *name* [**callback-rotary** *rotary-group-number*]
username *name* [**common-criteria-policy** *policy-name*]
username *name* [**dnis**]
username *name* [**mac**]
username *name* [**nocallback-verify**]
username *name* [**noescape**]
username *name* [**nohangup**]
username *name* [{**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}]
username *name* [**one-time** {**password** {**0** | **6** | **7** |*password* } | **secret** {**0** | **5** | **8** | **9** |*password*}}]
username *name* [**password** *secret*]
username *name* [**privilege** *level*]
username *name* [**secret** {**0** | **5** |*password*}]
username *name* [**serial-number**]
username *name* [**user-maxlinks** *number*]
username *name* [**view** *view-name*]
no username *name*

構文の説明

name	ホスト名、サーバ名、ユーザ ID、またはコマンド名。*name* 引数には 1 つの単語だけ使用できます。空白や引用符は使用できません。
aaa attribute list *aaa-list-name*	（任意）指定した認証、許可、およびアカウンティング（AAA）方式リストを使用します。

access-class *access-list-number*	（任意）ライン コンフィギュレーション モードで使用可能な **access-class** コマンドで指定されたアクセスリストをオーバーライドする発信アクセスリストを指定します。これはユーザのセッションで使用されます。
algorithm-type	（任意）ユーザのプレーンテキストのシークレットをハッシュするために使用するアルゴリズムを指定します。 • **md5**：MD5アルゴリズムを使用してパスワードをエンコードします。 • **scrypt**：SCRYPT ハッシュアルゴリズムを使用してパスワードをエンコードします。 • **sha256**：PBKDF2 ハッシュアルゴリズムを使用してパスワードをエンコードします。
autocommand *command*	（任意）指定したコマンドがユーザのログイン後に自動的に発行されるようにします。コマンドが完了するとセッションが終了します。このコマンドは任意の長さにすることができ、途中にスペースを含めることもできるため、**autocommand** キーワードを使用するコマンドは行の最後のオプションにする必要があります。
callback-dialstring *telephone-number*	（任意）非同期コールバックの場合のみ、DCEデバイスに渡す電話番号を指定できます。
callback-line *line-number*	（任意）非同期コールバックの場合のみ、特定のユーザ名をコールバックに対して有効にする端末回線（または連続したグループの最初の回線）の相対番号。番号はゼロから始まります。
ending-line-number	（任意）特定のユーザ名をコールバックに対して有効にする連続したグループの最後の回線の相対番号。キーワード（**tty** など）を省略した場合 、line-number および ending-line-number は相対回線番号ではなく絶対回線番号となります。
tty	（任意）非同期コールバックの場合のみ、標準の非同期回線。
callback-rotary *rotary-group-number*	（任意）非同期コールバックの場合のみ、特定のユーザ名をコールバックに対して有効にするロータリーグループ番号を指定できます。ロータリーグループで次に使用可能な回線が選択されます。範囲は1～100です。
common-criteria-policy	（任意）コモンクライテリアポリシーの名前を指定します。
dnis	（任意）着信番号識別サービス（DNIS）から取得された場合にパスワードを不要にします。
mac	（任意）MAC アドレスをローカルで実行される MAC フィルタリングのユーザ名として使用できるようにします。

nocallback-verify	（任意）指定した回線の EXEC コールバックに認証が不要であることを指定します。
noescape	（任意）ユーザが接続されているホストでエスケープ文字を使用できないようにします。
nohangup	（任意）自動コマンド（**autocommand** キーワードを使用して設定）の完了後に Cisco IOS ソフトウェアでユーザを切断しないようにします。ユーザには、代わりに別の EXEC プロンプトが表示されます。
nopassword	（任意）このユーザがログインする際のパスワードを不要にします。通常、このキーワードは **autocommand** キーワードを使用する場合に組み合わせて使用すると役立ちます。
password	（任意）*name* 引数にアクセスするためのパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。
password	ユーザが入力するパスワード。
encryption-type	直後のテキストが暗号化されるかどうか、および暗号化される場合は使用される暗号化タイプを定義する 1 桁の数字。定義されている暗号化タイプは、0（直後のテキストは暗号化されない）および 6 と 7（テキストはシスコが定義した暗号化アルゴリズムを使用して暗号化される）です。
encrypted-password	ユーザが入力する暗号化パスワード。
one-time	（任意）ユーザ名とパスワードが 1 回だけ有効であることを指定します。この設定は、デフォルトのクレデンシャルがユーザ設定に残らないようにするために使用されます。 • **0**：暗号化されていないパスワードまたはシークレット（設定に依存）が続くことを指定します。 • **6**：暗号化パスワードが続くことを指定します。 • **7**：非表示のパスワードが続くことを指定します。 • **5**：MD5 でハッシュされたシークレットが続くことを指定します。 • **8**：PBKDF2 でハッシュされたシークレットが続くことを指定します。 • **9**：SCRYPT でハッシュされたシークレットが続くことを指定します。
secret	（任意）ユーザのシークレットを指定します。

secret	チャレンジハンドシェイク認証プロトコル（CHAP）認証の場合：ローカルデバイスまたはリモートデバイスのシークレットを指定します。シークレットはローカルデバイスに暗号化されて格納されます。最大11文字のASCII文字からなる任意の文字列で構成できます。指定できるユーザ名とパスワードの組み合わせの数に制限はないため、任意の数のリモートデバイスを認証できます。
privilege *privilege-level*	（任意）ユーザの特権レベルを設定します。範囲：1 ～ 15。
serial-number	（任意）シリアル番号を指定します。
user-maxlinks *number*	（任意）ユーザに許可されるインバウンドリンクの最大数を指定します。
view *view-name*	（任意）CLI ビューの場合のみ、**parser view** コマンドで指定されたCLI ビュー名をローカル AAA データベースに関連付けます。

コマンド デフォルト

ユーザ名に基づく認証システムは確立されません。

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 16.11.1	このコマンドが導入されました。

使用上のガイドライン

username コマンドは、ログインだけを目的としてユーザ名、パスワード、またはその両方の認証を行います。

複数の **username** コマンドを使用して、単一ユーザのオプションを指定できます。

ローカルデバイスと通信を行う、認証が必要になるリモートシステムごとに、ユーザ名のエントリを追加します。リモートデバイスには、ローカルデバイスのユーザ名のエントリが必要です。このエントリは、そのリモートデバイスに対応するローカルデバイスのエントリと同じパスワードにする必要があります。

このコマンドは、特殊な取り扱いが必要なユーザ名を定義する場合に便利です。たとえば、このコマンドを使用すると、パスワードが不要で、ユーザを汎用の情報サービスに接続する「info」ユーザ名を定義できます。

username コマンドは、CHAP の設定の一部として必要です。ローカルデバイスが認証を必要とするリモートシステムごとにユーザ名のエントリを追加します。

（注）　ローカルデバイスをリモートのCHAPチャレンジに応答できるようにするには、一方の**username** *name*エントリを他方のデバイスにすでに割り当てられている**hostname**エントリと同じにする必要があります。

- 権限レベル1のユーザが上位の権限レベルを開始する状況を回避するには、ユーザ単位の権限レベルを1以外に設定します（たとえば0または2 ～ 15）。
- ユーザ単位の権限レベルは仮想端末の権限レベルよりも優先されます。

CLI ビューと合法的傍受ビュー

CLI ビューと合法的傍受ビューは、どちらも特定のコマンドと設定情報へのアクセスを制限します。合法的傍受ビューを使用すると、ユーザは、コールとユーザに関する情報を保存する簡易ネットワーク管理プロトコル（SNMP）コマンドの特別なセットである TAP-MIB 内に保持された合法的傍受コマンドへのアクセスを保護できます。

lawful-intercept キーワードを使用して指定されたユーザは、他の権限レベルまたはビュー名が明示的に指定されていない場合、デフォルトで合法的傍受ビューになります。

secret 引数に値が指定されていない場合、 **debug serial-interface** コマンドが有効になっていると、リンクの確立時にエラーが表示され、CHAP チャレンジは実装されません。CHAP デバッグ情報は、**debug ppp negotiation**、**debug serial-interface**、および **debug serial-packet** コマンドを使用して確認できます。

例

次に、ログインプロンプトで入力できる UNIX の **who** コマンドに似た、デバイスの現在のユーザを一覧表示するサービスを実装する例を示します。

```
Device(config)# username who nopassword nohangup autocommand show users
```

次に、パスワードを使用する必要がない情報サービスを実装する例を示します。コマンドは次の形式になります。

```
Device(config)# username info nopassword noescape autocommand telnet nic.ddn.mil
```

次に、すべての TACACS+ サーバが切断された場合でも機能する ID を実装する例を示します。コマンドは次の形式になります。

```
Device(config)# username superuser password superpassword
```

次に、「server_1」のシリアルインターフェイス 0 で CHAP を有効にする例を示します。「server_r」という名前のリモートサーバのパスワードも定義しています。

```
hostname server_1
username server_r password theirsystem
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

次に、暗号化されたパスワードを表示する **show running-config** コマンドの出力を示します。

```
hostname server_1
username server_r password 7 121F0A18
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

次の例では、権限レベル 1 のユーザが 1 よりも高い権限レベルへのアクセスを拒否されています。

```
Device(config)# username user privilege 0 password 0 cisco
Device(config)# username user2 privilege 2 password 0 cisco
```

次に、user2 のユーザ名ベースの認証を削除する例を示します。

```
Device(config)# no username user2
```

関連コマンド

Command	Description
debug ppp negotiation	PPP の始動時に、PPP オプションをネゴシエートするために送信された PPP パケットを表示します。
debug serial-interface	シリアル接続の障害に関する情報を表示します。
debug serial-packet	**debug serial interface** コマンドを使用して取得できる情報よりも詳しいシリアルインターフェイスのデバッグ情報を表示します。

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 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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 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 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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
```

第 XII 部

スタック マネージャおよびハイ アベイラビリティ

第 15 章

スタック マネージャおよびハイ アベイラビリティ

debug platform stack-manager

スタック マネージャ ソフトウェアのデバッグをイネーブルにするには、特権 EXEC モードで **debug platform stack-manager** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug platform stack-manager {**all** | **rpc** | **sdp** | **sim** | **ssm** | **trace**}
no debug platform stack-manager {**all** | **rpc** | **sdp** | **sim** | **ssm** | **trace**}

構文の説明

all	すべてのスタック マネージャ デバッグ メッセージを表示します。
rpc	スタック マネージャ リモート プロシージャ コール（RPC）使用状況のデバッグ メッセージを表示します。
sdp	スタック ディスカバリ プロトコル（SDP）のデバッグ メッセージを表示します。
sim	スタック情報モジュールのデバッグ メッセージを表示します。
ssm	スタック ステートマシンのデバッグ メッセージを表示します。
trace	スタック マネージャの入口と出口のデバッグ メッセージを追跡します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

このコマンドは、スタック対応スイッチのみでサポートされています。

undebug platform stack-manager コマンドは **no debug platform stack-manager** コマンドと同じです。

あるスイッチ スタック上でデバッグをイネーブルにした場合は、スタック マスターでのみイネーブルになります。スタックメンバのデバッグをイネーブルにする場合は、**session** *switch-number* EXEC コマンドを使用してスタックマスターからセッションを開始してください。スタックメンバのコマンドラインプロンプトで **debug** コマンドを入力します。最初にセッションを開始せずにメンバスイッチのデバッグをイネーブルにするには、スタックマススイッチ上で **remote command** *stack-member-number LINE* EXEC コマンドを使用します。

mode sso

冗長モードをステートフルスイッチオーバー（SSO）に設定するには、冗長コンフィギュレーション モードで **mode sso** コマンドを使用します。

mode sso

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

冗長コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

mode sso コマンドは、冗長コンフィギュレーション モードでのみ入力できます。

システムを SSO モードに設定する場合は、次の注意事項に従ってください。

- SSO モードをサポートするために、スタック内のスイッチでは同一の Cisco IOS イメージを使用する必要があります。Cisco IOS リリース間の相違のために、冗長機能が動作しない場合があります。
- モジュールの活性挿抜（OIR）を実行する場合、モジュールの状態が移行状態（Ready 以外の状態）である場合にだけ、ステートフル スイッチオーバーの間にスイッチはリセットし、ポート ステートは再起動します。
- 転送情報ベース（FIB）テーブルはスイッチオーバー時に消去されます。ルーテッド トラフィックは、ルート テーブルが再コンバージェンスするまで中断されます。

次の例では、冗長モードを SSO に設定する方法を示します。

```
デバイス(config)# redundancy
デバイス(config-red)# mode sso
デバイス(config-red)#
```

main-cpu

冗長メイン コンフィギュレーション サブモードを開始し、スタンバイスイッチをイネーブルにするには、冗長コンフィギュレーション モードで **main-cpu** コマンドを使用します。

main-cpu

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト なし

コマンド モード 冗長コンフィギュレーション（config-red）

コマンド履歴

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

使用上のガイドライン 冗長メイン コンフィギュレーション サブモードから、**standby console enable** コマンドを使用してスタンバイスイッチをイネーブルにします。

次に、冗長メインコンフィギュレーションサブモードを開始し、スタンバイスイッチをイネーブルにする例を示します。

```
デバイス(config)# redundancy
デバイス(config-red)# main-cpu
デバイス(config-r-mc)# standby console enable
デバイス#
```

policy config-sync prc reload

Parser Return Code（PRC）の障害がコンフィギュレーションの同期中に発生した場合にスタンバイスイッチをリロードするには、冗長コンフィギュレーション モードで **policy config-sync reload** コマンドを使用します。Parser Return Code（PRC）の障害が発生した場合にスタンバイスイッチがリロードしないように指定するには、このコマンドの **no** 形式を使用します。

policy config-sync {**bulk** | **lbl**} **prc reload**
no policy config-sync {**bulk** | **lbl**} **prc reload**

構文の説明

bulk	バルク コンフィギュレーション モードを指定します。
lbl	1行ごと（lbl）のコンフィギュレーションモードを指定します。

コマンド デフォルト このコマンドは、デフォルトではイネーブルです。

コマンド モード 冗長コンフィギュレーション（config-red）

コマンド履歴

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

次に、Parser Return Code（PRC）の障害がコンフィギュレーションの同期化中に発生した場合に、スタンバイスイッチがリロードされないように指定する例を示します。

```
デバイス(config-red)# no policy config-sync bulk prc reload
```

mode sso

冗長モードをステートフルスイッチオーバー（SSO）に設定するには、冗長コンフィギュレーション モードで **mode sso** コマンドを使用します。

mode sso

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

冗長コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

mode sso コマンドは、冗長コンフィギュレーション モードでのみ入力できます。

システムを SSO モードに設定する場合は、次の注意事項に従ってください。

- SSO モードをサポートするために、スタック内のスイッチでは同一の Cisco IOS イメージを使用する必要があります。Cisco IOS リリース間の相違のために、冗長機能が動作しない場合があります。
- モジュールの活性挿抜（OIR）を実行する場合、モジュールの状態が移行状態（Ready 以外の状態）である場合にだけ、ステートフル スイッチオーバーの間にスイッチはリセットし、ポート ステートは再起動します。
- 転送情報ベース（FIB）テーブルはスイッチオーバー時に消去されます。ルーテッド トラフィックは、ルート テーブルが再コンバージェンスするまで中断されます。

次の例では、冗長モードを SSO に設定する方法を示します。

```
デバイス(config)# redundancy
デバイス(config-red)# mode sso
デバイス(config-red)#
```

policy config-sync prc reload

Parser Return Code（PRC）の障害がコンフィギュレーションの同期中に発生した場合にスタンバイスイッチをリロードするには、冗長コンフィギュレーション モードで **policy config-sync reload** コマンドを使用します。Parser Return Code（PRC）の障害が発生した場合にスタンバイスイッチがリロードしないように指定するには、このコマンドの **no** 形式を使用します。

policy config-sync {**bulk** | **lbl**} **prc reload**

no policy config-sync {bulk | lbl} prc reload

構文の説明

bulk	バルク コンフィギュレーション モードを指定します。
lbl	1行ごと（lbl）のコンフィギュレーションモードを指定します。

コマンド デフォルト

このコマンドは、デフォルトではイネーブルです。

コマンド モード

冗長コンフィギュレーション（config-red）

コマンド履歴

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

次に、Parser Return Code（PRC）の障害がコンフィギュレーションの同期化中に発生した場合に、スタンバイスイッチがリロードされないように指定する例を示します。

```
デバイス(config-red)# no policy config-sync bulk prc reload
```

redundancy config-sync mismatched-commands

アクティブスイッチとスタンバイスイッチの間に設定の不一致があるときにスタンバイスイッチのスタックへの参加を許可するには、特権 EXEC モードで **redundancy config-sync mismatched-commands** コマンドを使用します。

redundancy config-sync {ignore | validate} mismatched-commands

構文の説明

ignore	Mismatched Command List を無視します。
validate	修正した実行コンフィギュレーションに基づいて Mismatched Command List を再確認します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

スタンバイスイッチの起動中にアクティブスイッチの実行コンフィギュレーションのコマンド構文チェックが失敗した場合、**redundancy config-sync mismatched-commands** コマンドを使用して、アクティブスイッチの Mismatched Command List（MCL）を表示し、スタンバイスイッチをリブートします。

次に、不一致コマンドのログ エントリの例を示します。

```
00:06:31: Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
 full list of mismatched commands via:
show redundancy config-sync failures mcl
00:06:31: Config Sync: Starting lines from MCL file:
interface GigabitEthernet7/7
! <submode> "interface"
- ip address 192.0.2.0 255.255.255.0
! </submode> "interface"
```

すべての不一致コマンドを表示するには、**show redundancy config-sync failures mcl** コマンドを使用します。

MCL を消去するには、次の手順を実行します。

1. アクティブスイッチの実行コンフィギュレーションからすべての不一致コマンドを除外します。
2. **redundancy config-sync validate mismatched-commands** コマンドを使用して、修正した実行コンフィギュレーションに基づいて MCL を再確認します。
3. スタンバイスイッチをリロードします。

次の手順に従って、MCL を無視することもできます。

1. **redundancy config-sync ignore mismatched-commands** コマンドを入力します。
2. スタンバイスイッチをリロードします。システムは SSO モードに移行します。

（注） 不一致コマンドを無視する場合、アクティブスイッチとスタンバイスイッチの同期していないコンフィギュレーションは存在したままです。

3. 無視された MCL は、**show redundancy config-sync ignored mcl** コマンドを使用して確認できます。

コンフィギュレーションファイルの互換性の問題が原因で、アクティブスイッチとスタンバイスイッチ間で SSO モードを確立できない場合、Mismatched Command List（MCL）がアクティブスイッチで生成され、スタンバイスイッチに対して Route Processor Redundancy（RPR）モードへのリロードが強制されます。

次の例に、変更したコンフィギュレーションとの Mismatched Command List を再検証する方法を示します。

```
デバイス# redundancy config-sync validate mismatched-commands
デバイス#
```

redundancy

冗長コンフィギュレーションモードを開始するには、グローバル コンフィギュレーション モードで **redundancy** コマンドを使用します。

redundancy

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

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

使用上のガイドライン

冗長コンフィギュレーションモードは、スタンバイスイッチをイネーブルにするために使用されるメイン CPU サブモードを開始するために使用されます。

メイン CPU サブモードを開始するには、冗長コンフィギュレーション モードで **main-cpu** コマンドを使用します。

スタンバイスイッチを有効にするには、メイン CPU サブモードから **standby console enable** コマンドを使用します。

冗長コンフィギュレーション モードを終了するには、**exit** コマンドを使用します。

次に、冗長コンフィギュレーション モードを開始する例を示します。

```
デバイス(config)# redundancy
デバイス(config-red)#
```

次の例では、メイン CPU サブモードを開始する方法を示します。

```
デバイス(config)# redundancy
デバイス(config-red)# main-cpu
デバイス(config-r-mc)#
```

redundancy force-switchover

アクティブスイッチとスタンバイスイッチのスイッチオーバーを強制的に実行するには、スイッチスタックの特権 EXEC モードで **redundancy force-switchover** コマンドを使用します。

redundancy force-switchover

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト なし

コマンド モード 特権 EXEC

コマンド履歴

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

使用上のガイドライン 手動で冗長スイッチに切り替えるには、**redundancy force-switchover** コマンドを使用します。冗長スイッチは Cisco IOS イメージを実行する新しいアクティブスイッチになり、モジュールはデフォルト設定にリセットされます。

古いアクティブスイッチは新しいイメージで再起動し、スタックに参加します。

アクティブスイッチで **redundancy force-switchover** コマンドを使用すると、アクティブスイッチのスイッチポートがダウン状態になります。

部分リング スタック内のスイッチにこのコマンドを使用すると、次の警告メッセージが表示されます。

```
デバイス# redundancy force-switchover
Stack is in Half ring setup; Reloading a switch might cause stack split
This will reload the active unit and force switchover to standby[confirm]
```

次の例では、アクティブ スーパーバイザ エンジンからスタンバイ スーパーバイザ エンジンに手動で切り替える方法を示します。

```
デバイス# redundancy force-switchover
デバイス#
```

redundancy reload

スタック内のいずれか、またはすべてのスイッチを強制リロードするには、特権EXECモードで **redundancy reload** コマンドを使用します。

redundancy reload {**peer** | **shelf**}

構文の説明

peer	ピア ユニットをリロードします。
shelf	スタック内のすべてのスイッチが再起動します。

コマンド デフォルト なし

コマンド モード 特権 EXEC

コマンド履歴

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

使用上のガイドライン

このコマンドを使用する前に、詳細情報について『*Stacking Configuration Guide (Catalyst 3650 Switches)*』の「Performing a Software Upgrade」の項を参照してください。

スタック内のすべてのスイッチをリブートするには、**redundancy reload shelf** コマンドを使用します。

次に、手動でスタック内のすべてのスイッチをリロードする例を示します。

```
デバイス# redundancy reload shelf
デバイス#
```

reload

スタックメンバをリロードし、設定変更を適用するには、特権 EXEC モードで **reload** コマンドを使用します。

reload [{**/noverify** | **/verify**}] [{*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**}]

構文の説明

/noverify	（任意）リロードの前にファイル シグニチャを確認しないように指定します。
/verify	（任意）リロードの前にファイル シグニチャを確認します。
LINE	（任意）リセットの理由。
at	（任意）リロードを実行する時間を hh:mm 形式で指定します。
cancel	（任意）保留中のリロードをキャンセルします。
in	（任意）リロードを実行する間隔を指定します。
slot	（任意）指定したスタックメンバに変更を保存し、再起動します。
stack-member-number	
standby-cpu	（任意）スタンバイ ルートプロセッサ（RP）をリロードします。

コマンド デフォルト

スタック メンバをただちにリロードし、設定の変更を有効にします。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

スイッチスタックに複数のスイッチがある場合に **reload slot** *stack-member-number* コマンドを入力すると、設定の保存を要求するプロンプトが表示されません。

例

次の例では、スイッチ スタックをリロードする方法を示します。

```
デバイス# reload
System configuration has been modified. Save? [yes/no]: yes
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm] yes
```

次の例では、特定のスタック メンバをリロードする方法を示します。

```
デバイス# reload slot 6
Proceed with reload? [confirm] y
```

次の例では、単一スイッチのスイッチ スタック（メンバ スイッチが 1 つだけ）をリロードする方法を示します。

```
デバイス# reload slot 3
System configuration has been modified. Save? [yes/no]: y
Proceed to reload the whole Stack? [confirm] y
```

reload

スタックメンバをリロードし、設定変更を適用するには、特権 EXEC モードで **reload** コマンドを使用します。

reload [{**/noverify** | **/verify**}] [{*LINE* | **at** | **cancel** | **in** | **slot** *stack-member-number* | **standby-cpu**}]

構文の説明

/noverify	（任意）リロードの前にファイル シグニチャを確認しないように指定します。
/verify	（任意）リロードの前にファイル シグニチャを確認します。
LINE	（任意）リセットの理由。
at	（任意）リロードを実行する時間を hh:mm 形式で指定します。
cancel	（任意）保留中のリロードをキャンセルします。
in	（任意）リロードを実行する間隔を指定します。
slot	（任意）指定したスタックメンバに変更を保存し、再起動します。
stack-member-number	

standby-cpu	（任意）スタンバイ ルート プロセッサ（RP）をリロードします。

コマンド デフォルト

スタック メンバをただちにリロードし、設定の変更を有効にします。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

スイッチスタックに複数のスイッチがある場合に **reload slot** *stack-member-number* コマンドを入力すると、設定の保存を要求するプロンプトが表示されません。

例

次の例では、スイッチ スタックをリロードする方法を示します。

```
デバイス# reload
System configuration has been modified. Save? [yes/no]: yes
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm] yes
```

次の例では、特定のスタック メンバをリロードする方法を示します。

```
デバイス# reload slot 6
Proceed with reload? [confirm] y
```

次の例では、単一スイッチのスイッチ スタック（メンバ スイッチが 1 つだけ）をリロードする方法を示します。

```
デバイス# reload slot 3
System configuration has been modified. Save? [yes/no]: y
Proceed to reload the whole Stack? [confirm] y
```

session

特定のスタックメンバにアクセスするには、スタックマスターの特権 EXEC モードで **session** コマンドを使用します。

session *stack-member-number*

構文の説明

stack-member-number	active switch からアクセスするスタック メンバの番号。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

メンバにアクセスすると、メンバの番号がシステム プロンプトに追加されます。

メンバデバイスにアクセスするには、マスターから **session** コマンドを使用します。

内部コントローラにアクセスするには、マスターまたはスタンドアロンスイッチから、**processor 1** を指定して **session** コマンドを使用します。スタンドアロンデバイスは常にメンバ 1 です。

例

次の例では、スタック メンバ 3 にアクセスする方法を示します。

```
デバイス# session 3
デバイス-3#
```

session

特定のスタックメンバにアクセスするには、スタックマスターの特権 EXEC モードで **session** コマンドを使用します。

session *stack-member-number*

構文の説明

stack-member-number	active switch からアクセスするスタック メンバの番号。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

メンバにアクセスすると、メンバの番号がシステム プロンプトに追加されます。

メンバデバイスにアクセスするには、マスターから **session** コマンドを使用します。

内部コントローラにアクセスするには、マスターまたはスタンドアロンスイッチから、**processor 1** を指定して **session** コマンドを使用します。スタンドアロンデバイスは常にメンバ 1 です。

例

次の例では、スタック メンバ 3 にアクセスする方法を示します。

```
デバイス# session 3
デバイス-3#
```

set platform software fed switch

SVL ポート単位のパケットキャッシュ数を設定するには、特権 EXEC モードまたはユーザ EXEC モードで **set platform software fed switch** コマンドを使用します。

set platform software fed switch {*switch-number* | **active** | **standby**} {**F0** | **F1 active**} **fss pak-cache** *count*

構文の説明

switch {*switch-number* | **active** | **standby**}	スイッチに関する情報を指定します。次の選択肢があります。 • *switch-number*。 • **active** ：アクティブなスイッチに関する情報を表示します。 • **standby**：存在する場合、スタンバイスイッチに関する情報を表示します。
F0	Embedded Service Processor スロット 0 に関する情報を表示します。
FP active	アクティブな Embedded Service Processor に関する情報を表示します。
pak-cache *count*	パケットキャッシュ数を指定します。範囲は 10 ～ 600 です。デフォルトは 10 です。

コマンド デフォルト

ポート単位のパケットキャッシュ数のデフォルトは 10 です。

コマンド モード

ユーザ EXEC（>）

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

なし

例

次に、SVL ポート単位のパケットキャッシュ数を設定する例を示します。

```
Device# set platform software fed switch active F1 active fss pak-cache 40
```

set platform software nif-mgr switch

SVL ポート単位のパケットキャッシュ数を設定するには、特権 EXEC モードまたはユーザ EXEC モードで **set platform software nif-mgr switch** コマンドを使用します。

set platform software nif-mgr switch {*switch-number* | **active** | **standby** }**R0 pak-cache** *count*

構文の説明

switch {*switch-number* | **active** | **standby**}	スイッチに関する情報を指定します。次の選択肢があります。 • *switch-number*。 • **active** ：アクティブなスイッチに関する情報を表示します。 • **standby**：存在する場合、スタンバイスイッチに関する情報を表示します。
R0	ルートプロセッサ（RP）スロット 0 に関する情報を指定します。
pak-cache *count*	パケットキャッシュ数を指定します。範囲は 10 ～ 600 です。デフォルトは 10 です。

コマンド デフォルト

ポート単位のパケットキャッシュ数のデフォルトは 10 です。

コマンド モード

ユーザ EXEC（>）

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

なし

例

次に、SVL ポート単位のパケットキャッシュ数を設定する例を示します。

```
Device# set platform software nif_mgr switch active R0 pak-cache 40
```

show platform software fed

FED と Network Interface Manager（NIF Mgr）のソフトウェアプロセス間におけるポート単位の SDP/LMP 制御パケット交換履歴を表示するには、特権 EXEC モードで **show platform software fed** コマンドを使用します。

show platform software fed switch {*switch-number* | **active** | **standby**} **fss** {**counters** | **interface-counters interface** {*interface-type interface-number*} | **lmp-packets interface** {*interface-type interface-number*} | **sdp-packets**

構文の説明

switch {*switch-number* | **active** | **standby**}	スイッチに関する情報を表示します。次の選択肢があります。 • *switch-number*。 • **active** ：アクティブなスイッチに関する情報を表示します。 • **standby**：存在する場合、スタンバイスイッチに関する情報を表示します。 （注） このキーワードはサポートされていません。
fss	前面スタック構成（FSS）に関する情報を指定します。
counters	SDP、LMP、OOB1/2、EMP、および LOOPBACK タイプの TX パケットと RX パケットの数を表示します。
interface-counters	すべてのインターフェイスについて、TX パケットと RX パケットの数を表示します。特定の SVL インターフェイスについての情報を表示するように出力をフィルタ処理するには、**interface-counters interface** {*interface-type interface-number*} コマンドを使用します。
lmp-packets	すべての SVL インターフェイスについて、FED と NIF Manager の間でやり取りされた LMP パケットトランザクションの詳細を表示します。特定の SVL インターフェイスについての情報を表示するように出力をフィルタ処理するには、**lmp-packets interface** {*interface-type interface-number*} コマンドを使用します。
sdp-packets	すべての SVL インターフェイスについて、FED と NIF Manager の間で送信された SDP パケットの詳細を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 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

デフォルトでは、**show platform software fed switch active fss sdp-packets** コマンドの出力にパケットキャッシュ数が 10 と表示されます。ポート単位のパケットキャッシュ数は、**set platform software fed switch** コマンドを使用して最大 600 に設定できます。

例

次に、**show platform software fed switch active fss lmp-packets interface** *interface-type interface-number* コマンドの出力例を示します。

```
Device# show platform software fed switch active fss lmp-packets interface
fortygigabitethernet1/0/1

Interface: fortygigabitethernet1/0/1 IFID:0x1d
FED FSS LMP packets max 10:

FED --> Nif Mgr
Timestamp                    Local    Peer       Seq
                             LPN      LPN        Num
-----------------------------------------------------
Tue Sep 18 12:45:13 2018     11       11         4329
Tue Sep 18 12:45:14 2018     11       11         4330
```

次に、**show platform software fed switch active fss sdp-packets** コマンドの出力例を示します。

```
Device# show platform software fed switch active fss sdp-packets
FED FSS SDP packets max 10:
-------------------------

FED-> Nif Mgr
Timestamp                        Src Mac                  Dst Mac.                 Seq Num
-------------------------------------------------------------------------------------------
Thu Oct  4 05:54:04 2018         e4aa:5d54:8aa8           ffff:ffff:ffff           262
Thu Oct  4 05:54:08 2018         e4aa:5d54:8aa8           ffff:ffff:ffff           263
Thu Oct  4 05:54:12 2018         e4aa:5d54:8aa8           ffff:ffff:ffff           264
```

次に、**show platform software fed switch active fss counters** コマンドの出力例を示します。

```
Device# show platform software fed switch active fss counters
FSS Packet Counters
       SDP                                          LMP
TX  |              RX                       TX  |              RX
---------------------                      ---------------------
1493             1494                      4988             4988

       OOB1                                         OOB2
TX  |              RX                       TX  |              RX
---------------------                      ---------------------
22                  8                      134858         133833

       EMP
TX  |              RX                              LOOPBACK
----------------------                     --------------------
0                     0                              71
```

次に、**show platform software fed switch active fss interface-counters interface** *interface-type interface-number* コマンドの出力例を示します。

```
Device# show platform software fed switch active fss interface-counters
fortygigabitethernet1/0/1

Interface fortygigabitethernet1/0/1 IFID: 0x1d Counters
       LMP
  TX    |    RX
----------------------
6391        6389
```

関連コマンド

コマンド	説明
set platform software fed switch	SVL インターフェイスのポート単位のパケットキャッシュ数を設定します。

show platform software nif-mgr switch

Network Interface Manager（NIF Mgr）ソフトウェアプロセスと StackWise Virtual リンク（SVL）インターフェイスの間における制御パケット交換履歴を表示するには、特権 EXEC モードで **show platform software nif-mgr switch** コマンドを使用します。

show platform software nif-mgr switch {*switch-number* | **active** | **standby**} **R0**{**counters** [**lpn** *lpn-index*] | **packets** [**lpn** *lpn-index*] | **switch-info**}

show platform software nif-mgr switch {*switch-number* | **active** | **standby**} **R0counters**{**slot***slot-number* }{**port** *port-number* }**packets**{**slot***slot-number* }{**port** *port-number* }{**switch-info**}

構文の説明

switch {*switch-number* | **active** | **standby**}	スイッチに関する情報を表示します。次の選択肢があります。 • *switch-number*。 • **active** ：アクティブなスイッチに関する情報を表示します。 • **standby**：存在する場合、スタンバイスイッチに関する情報を表示します。 （注） このキーワードはサポートされていません。
R0	ルート プロセッサ（RP）スロット 0 に関する情報を表示します。
counters	LMP および SDP タイプの TX パケットと RX パケットの数を表示します。
lpn *lpn-index*	ローカルポート番号（LPN）を指定します。範囲は 1 ～ 96 です。 *lpn-index* に関する情報については **show platform software nif-mgr switch active R0 switch-info** コマンドを使用してください。

packets	LMP および SDP タイプの TX パケットと RX パケットの詳細を表示します。
switch-info	NIF Manager の運用データベースに関する情報を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 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

show platform software nif-mgr switch active R0 counters コマンドの出力には、送信された LMP および SDP パケットのカウンタが表示されます。

show platform software nif-mgr switch active R0 switch-info コマンドの出力には、SVL リンクの詳細と各リンクにおけるプロトコルのフラップ数が表示されます。

- LMP から FED
- SDP から FED
- FED から LMP
- FED から SDP
- Stack Manager から SDP
- SDP から Stack Manager

show platform software nif-mgr switch active R0 packets コマンドの出力には、送信された LMP および SDP パケットのタイムスタンプの詳細が表示されます。

- FED からの最後の 10 個の LMP フレームのタイムスタンプ
- FED への最後の 10 個の LMP フレームのタイムスタンプ
- Stack Manager からの最後の 10 個の SDP フレームのタイムスタンプ
- Stack Manager への最後の 10 個の SDP フレームのタイムスタンプ

デフォルトでは、ブートアップ時の SVL ポート単位のパケットキャッシュ数は 10 です。ポート単位のパケットキャッシュ数を設定するには、**set platform software nif-mgr switch** コマンドを使用します。

例

次に、**show platform software nif-mgr switch active R0 counters** コマンドの出力例を示します。

```
デバイス# show platform software nif-mgr switch active R0 counters
NIF Manager Counters
 Counters:
################################################
Stack Link : 1
================================================
FED to NIF Mgr
---------------
Number of LMP RX Packets : 749
NIF Mgr to FED
---------------
Number of LMP TX Packets : 758
Stack Link : 2
================================================
FED to NIF Mgr
---------------
Number of LMP RX Packets : 0
NIF Mgr to FED
---------------
Number of LMP TX Packets : 0

NIF Mgr to Stack Mgr
-----------------------
Number of SDP Success Packets - 1854
Number of SDP Fail Packets - 0
Stack Mgr to NIF Mgr
---------------------
Number of SDP Success Packets - 1850
Number of SDP Fail Packets - 0
```

次に、**show platform software nif-mgr switch active R0 counters lpn** *lpn-index* コマンドの出力例を示します。

```
デバイス# Switch#sh platform software nif_mgr switch active r0 counters lpn 1
Counters:
################################################
LPN : 1 Stack Link : 1 port 1
================================================
FED to NIF Mgr
---------------
Number of LMP RX Packets : 760
NIF Mgr to FED
---------------
Number of LMP TX Packets : 768
```

次に、**show platform software nif-mgr switch active R0 packets** コマンドの出力例を示します。

```
デバイス# show platform software nif-mgr switch active R0 packets
NIF manager packets max 10:

Stack Link :   1
LMP
------------------------
FED->
Nif Mgr
Timestamp                      Local    Peer     Seq
                               LPN      LPN      Num
-------------------------------------------------------------
Wed Jun 20 02:20:49 2018       3        3        1050
Wed Jun 20 02:20:50 2018       3        3        1051
```

```
Wed Jun 20 02:20:41 2018       3       3       1042
Wed Jun 20 02:20:42 2018       3       3       1043
Wed Jun 20 02:20:43 2018       3       3       1044
Wed Jun 20 02:20:44 2018       3       3       1045
Wed Jun 20 02:20:45 2018       3       3       1046
Wed Jun 20 02:20:46 2018       3       3       1047
Wed Jun 20 02:20:47 2018       3       3       1048
Wed Jun 20 02:20:48 2018       3       3       1049

Nif Mgr->
FED
Timestamp              Local   Peer    Seq
                               LPN     LPN     Num
-----------------------------------------------------------
Wed Jun 20 02:20:49 2018       3       3       1050
Wed Jun 20 02:20:50 2018       3       3       1051
Wed Jun 20 02:20:41 2018       3       3       1042
Wed Jun 20 02:20:42 2018       3       3       1043
Wed Jun 20 02:20:43 2018       3       3       1044
Wed Jun 20 02:20:44 2018       3       3       1045
Wed Jun 20 02:20:45 2018       3       3       1046
Wed Jun 20 02:20:46 2018       3       3       1047
Wed Jun 20 02:20:47 2018       3       3       1048
Wed Jun 20 02:20:48 2018       3       3       1049

SDP
------------------------
Nif Mgr->
Stack Mgr
Timestamp                      Src Mac        Dst Mac        Seq Num
-------------------------------------------------------------------------
Wed Jun 20 02:20:40 2018       40ce:2499:aa90 ffff:ffff:ffff 320
Wed Jun 20 02:20:44 2018       40ce:2499:aa90 ffff:ffff:ffff 321
Wed Jun 20 02:20:48 2018       40ce:2499:aa90 ffff:ffff:ffff 322
Wed Jun 20 02:20:12 2018       40ce:2499:aa90 ffff:ffff:ffff 313
Wed Jun 20 02:20:16 2018       40ce:2499:aa90 ffff:ffff:ffff 314
Wed Jun 20 02:20:20 2018       40ce:2499:aa90 ffff:ffff:ffff 315
Wed Jun 20 02:20:24 2018       40ce:2499:aa90 ffff:ffff:ffff 316
Wed Jun 20 02:20:28 2018       40ce:2499:aa90 ffff:ffff:ffff 317
Wed Jun 20 02:20:32 2018       40ce:2499:aa90 ffff:ffff:ffff 318
Wed Jun 20 02:20:36 2018       40ce:2499:aa90 ffff:ffff:ffff 319

Stack Mgr->
Nif Mgr
Timestamp                      Src Mac        Dst Mac        Seq Num
-------------------------------------------------------------------------
Wed Jun 20 02:20:17 2018       40ce:2499:a9d0 ffff:ffff:ffff 310
Wed Jun 20 02:20:21 2018       40ce:2499:a9d0 ffff:ffff:ffff 311
Wed Jun 20 02:20:25 2018       40ce:2499:a9d0 ffff:ffff:ffff 312
Wed Jun 20 02:20:29 2018       40ce:2499:a9d0 ffff:ffff:ffff 313
Wed Jun 20 02:20:33 2018       40ce:2499:a9d0 ffff:ffff:ffff 314
Wed Jun 20 02:20:37 2018       40ce:2499:a9d0 ffff:ffff:ffff 315
Wed Jun 20 02:20:41 2018       40ce:2499:a9d0 ffff:ffff:ffff 316
Wed Jun 20 02:20:45 2018       40ce:2499:a9d0 ffff:ffff:ffff 317
Wed Jun 20 02:20:49 2018       40ce:2499:a9d0 ffff:ffff:ffff 318
Wed Jun 20 02:20:13 2018       40ce:2499:a9d0 ffff:ffff:ffff 309
```

関連コマンド

コマンド	説明
set platform software nif-mgr switch	SVLインターフェイスのポート単位のパケットキャッシュ数を設定します。

show platform stack-manager

プラットフォーム依存スイッチスタック情報を表示するには、特権EXECモードで**show platform stack-manager** コマンドを使用します。

show platform stack-manager {**oir-states** | **sdp-counters** | **sif-counters**} **switch** *stack-member-number*

構文の説明

oir-states	活性挿抜（OIR）状態の情報を表示します。
sdp-counters	スタックディスカバリプロトコル（SDP）カウンタ情報を表示します。
sif-counters	スタック情報（SIF）カウンタ情報を表示します。
switch *stack-member-number*	スタック マネージャ情報を表示するスタック メンバを指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

スイッチスタックのデータと統計を収集するには、**show platform stack-manager** コマンドを使用します。

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show platform stack-manager

プラットフォーム依存スイッチスタック情報を表示するには、特権EXECモードで**show platform stack-manager** コマンドを使用します。

show platform stack-manager {**oir-states** | **sdp-counters** | **sif-counters**} **switch** *stack-member-number*

構文の説明

oir-states	活性挿抜（OIR）状態の情報を表示します。
sdp-counters	スタックディスカバリ プロトコル（SDP）カウンタ情報を表示します。
sif-counters	スタック情報（SIF）カウンタ情報を表示します。
switch *stack-member-number*	スタック マネージャ情報を表示するスタック メンバを指定します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

スイッチスタックのデータと統計を収集するには、**show platform stack-manager** コマンドを使用します。

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show redundancy config-sync

コンフィギュレーション同期障害情報または無視された Mismatched Command List（MCL）（存在する場合）を表示するには、EXEC モードで **show redundancy config-sync** コマンドを使用します。

show redundancy config-sync {**failures** {**bem** | **mcl** | **prc**} | **ignored failures mcl**}

構文の説明

failures	MCL エントリまたはベスト エフォート方式（BEM）/パーサー リターン コード（PRC）の障害を表示します。
bem	BEM 障害コマンド リストを表示し、スタンバイスイッチを強制的にリブートします。
mcl	スイッチの実行コンフィギュレーションに存在するがスタンバイスイッチのイメージでサポートされていないコマンドを表示し、スタンバイスイッチを強制的にリブートします。
prc	PRC 障害コマンドリストを表示し、スタンバイスイッチを強制的にリブートします。

ignored failures mcl	無視された MCL 障害を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

2 つのバージョンの Cisco IOS イメージが含まれている場合は、それぞれのイメージによってサポートされるコマンドセットが異なる可能性があります。このような不一致コマンドのいずれかがアクティブスイッチで実行された場合、スタンバイスイッチでそのコマンドを認識できない可能性があり、これにより設定の不一致状態が発生します。バルク同期中にスタンバイスイッチでコマンドの構文チェックが失敗すると、コマンドはMCLに移動し、スタンバイスイッチはリセットされます。すべての不一致コマンドを表示するには、**show redundancy config-sync failures mcl** コマンドを使用します。

MCL を消去するには、次の手順を実行します。

1. アクティブスイッチの実行コンフィギュレーションから、不一致コマンドをすべて削除します。
2. **redundancy config-sync validate mismatched-commands** コマンドを使用して、修正した実行コンフィギュレーションに基づいて MCL を再確認します。
3. スタンバイスイッチをリロードします。

または、次の手順を実行して MCL を無視することもできます。

1. **redundancy config-sync ignore mismatched-commands** コマンドを入力します。
2. スタンバイスイッチをリロードします。システムは SSO モードに遷移します。

（注） 不一致コマンドを無視する場合、アクティブスイッチとスタンバイスイッチの同期していないコンフィギュレーションは存在したままです。

3. 無視された MCL は、**show redundancy config-sync ignored mcl** コマンドを使用して確認できます。

各コマンドでは、そのコマンドを実装するアクション機能において戻りコードが設定されます。この戻りコードは、コマンドが正常に実行されたかどうかを示します。アクティブスイッチは、コマンドの実行後に PRC を維持します。スタンバイスイッチはコマンドを実行し、アクティブスイッチに PRC を返します。これら 2 つの PRC が一致しないと、PRC 障害が発生します。バルク同期または 1 行ごとの（LBL）同期中にスタンバイスイッチで PRC エラーが生

じた場合、スタンバイスイッチはリセットされます。すべてのPRC障害を表示するには、**show redundancy config-sync failures prc** コマンドを使用します。

ベスト エフォート方式（BEM）エラーを表示するには、**show redundancy config-sync failures bem** コマンドを使用します。

次に、BEM 障害を表示する例を示します。

```
デバイス> show redundancy config-sync failures bem
BEM Failed Command List
-----------------------

 The list is Empty
```

次に、MCL 障害を表示する例を示します。

```
デバイス> show redundancy config-sync failures mcl
Mismatched Command List
-----------------------

The list is Empty
```

次に、PRC 障害を表示する例を示します。

```
デバイス# show redundancy config-sync failures prc
PRC Failed Command List
-----------------------

 The list is Empty
```

show redundancy

冗長ファシリティ情報を表示するには、特権 EXEC モードで **show redundancy** コマンドを使用します。

show redundancy [{**clients** | **config-sync** | **counters** | **history** [{**reload** | **reverse**}] | **slaves**[*slave-name*] {**clients** | **counters**} | **states** | **switchover history** [**domain default**]}]

構文の説明

clients	（任意）冗長ファシリティ クライアントに関する情報を表示します。
config-sync	（任意）コンフィギュレーション同期の失敗または無視されたMismatched Command List（MCL）を表示します。詳細については、show redundancy config-sync （827 ページ）を参照してください。
counters	（任意）冗長ファシリティ カウンタに関する情報を表示します。
history	（任意）冗長ファシリティの過去のステータスのログおよび関連情報を表示します。
history reload	（任意）冗長ファシリティの過去のリロード情報を表示します。

history reverse	（任意）冗長ファシリティの過去のステータスおよび関連情報のログを逆順で表示します。
slaves	（任意）冗長ファシリティのすべてのスレーブを表示します。
slave-name	（任意）特定の情報を表示する冗長ファシリティ スレーブの名前。指定スレーブのすべてのクライアントまたはカウンタを表示するには、追加でキーワードを入力します。
clients	指定スレーブのすべての冗長ファシリティ クライアントを表示します。
counters	指定スレーブのすべてのカウンタを表示します。
states	（任意）冗長ファシリティの状態（ディセーブル、初期化、スタンバイ、アクティブなど）に関する情報を表示します。
switchover history	（任意）冗長ファシリティのスイッチオーバー履歴に関する情報を表示します。
domain default	（任意）スイッチオーバー履歴を表示するドメインとしてデフォルト ドメインを表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

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

次の例では、冗長ファシリティに関する情報を表示する方法を示します。

```
デバイス# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 6 days, 9 hours, 23 minutes
Switchovers system experienced = 0
             Standby failures = 0
        Last switchover reason = not known

                 Hardware Mode = Simplex
    Configured Redundancy Mode = SSO
     Operating Redundancy Mode = SSO
              Maintenance Mode = Disabled
                Communications = Down      Reason: Simplex mode

Current Processor Information :
-------------------------------
               Active Location = slot 1
        Current Software state = ACTIVE
       Uptime in current state = 6 days, 9 hours, 23 minutes
                 Image Version = Cisco IOS Software, IOS-XE Software, Catalyst 3
850 L3 Switch Software (CAT3850-UNIVERSALK9-M), Version 03.08.59.EMD EARLY DEPLO
YMENT ENGINEERING NOVA_WEEKLY BUILD, synced to DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_11
```

```
05
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 16-S
        Configuration register = 0x102

Peer (slot: 0) information is not available because it is in 'DISABLED' state
デバイス#
```

次の例では、冗長ファシリティクライアント情報を表示する方法を示します。

```
デバイス# show redundancy clients
Group ID =     1
     clientID = 20002    clientSeq =     4    EICORE HA Client
     clientID = 24100    clientSeq =     5    WCM_CAPWAP
     clientID = 24101    clientSeq =     6    WCM RRM HA
     clientID = 24103    clientSeq =     8    WCM QOS HA
     clientID = 24105    clientSeq =    10    WCM_MOBILITY
     clientID = 24106    clientSeq =    11    WCM_DOT1X
     clientID = 24107    clientSeq =    12    WCM_APFROGUE
     clientID = 24110    clientSeq =    15    WCM_CIDS
     clientID = 24111    clientSeq =    16    WCM_NETFLOW
     clientID = 24112    clientSeq =    17    WCM_MCAST
     clientID = 24120    clientSeq =    18    wcm_comet
     clientID = 24001    clientSeq =    21    Table Manager Client
     clientID = 20010    clientSeq =    24    SNMP SA HA Client
     clientID = 20007    clientSeq =    27    Installer HA Client
     clientID =    29    clientSeq =    60    Redundancy Mode RF
     clientID =   139    clientSeq =    61    IfIndex
     clientID =  3300    clientSeq =    62    Persistent Variable
     clientID =    25    clientSeq =    68    CHKPT RF
     clientID = 20005    clientSeq =    74    IIF-shim
     clientID = 10001    clientSeq =    82    QEMU Platform RF

<output truncated>
```

出力には、次の情報が表示されます。

- clientID には、クライアントの ID 番号が表示されます。
- clientSeq には、クライアントの通知シーケンス番号が表示されます。
- 現在の冗長ファシリティの状態。

次の例では、冗長ファシリティカウンタ情報を表示する方法を示します。

```
デバイス# show redundancy counters
Redundancy Facility OMs

               comm link up = 0
             comm link down = 0
          invalid client tx = 0
          null tx by client = 0
                tx failures = 0
      tx msg length invalid = 0

      client not rxing msgs = 0
 rx peer msg routing errors = 0
           null peer msg rx = 0
         errored peer msg rx = 0

                 buffers tx = 0
```

```
     tx buffers unavailable = 0
                buffers rx = 0
      buffer release errors = 0

 duplicate client registers = 0
  failed to register client = 0
       Invalid client syncs = 0

デバイス#
```

次の例では、冗長ファシリティ履歴情報を表示する方法を示します。

```
デバイス# show redundancy history
00:00:00 *my state = INITIALIZATION(2) peer state = DISABLED(1)
00:00:00 RF_EVENT_INITIALIZATION(524) op=0 rc=0
00:00:00 *my state = NEGOTIATION(3) peer state = DISABLED(1)
00:00:01 client added: Table Manager Client(24001) seq=21
00:00:01 client added: SNMP SA HA Client(20010) seq=24
00:00:06 client added: WCM_CAPWAP(24100) seq=5
00:00:06 client added: WCM QOS HA(24103) seq=8
00:00:07 client added: WCM_DOT1X(24106) seq=11
00:00:07 client added: EICORE HA Client(20002) seq=4
00:00:09 client added: WCM_MOBILITY(24105) seq=10
00:00:09 client added: WCM_NETFLOW(24111) seq=16
00:00:09 client added: WCM_APFROGUE(24107) seq=12
00:00:09 client added: WCM RRM HA(24101) seq=6
00:00:09 client added: WCM_MCAST(24112) seq=17
00:00:09 client added: WCM_CIDS(24110) seq=15
00:00:09 client added: wcm_comet(24120) seq=18
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) First Slave(0) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6107) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6109) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6128) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8897) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8898) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8901) op=0 rc=0
00:00:22 RF_EVENT_SLAVE_STATUS_DONE(523) First Slave(0) op=405 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Redundancy Mode RF(29) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) IfIndex(139) op=0 rc=0

<output truncated>
```

次の例では、冗長ファシリティスレーブに関する情報を表示する方法を示します。

```
デバイス# show redundancy slaves
Group ID =   1
Slave/Process ID =  6107   Slave Name = [installer]
Slave/Process ID =  6109   Slave Name = [eicored]
Slave/Process ID =  6128   Slave Name = [snmp_subagent]
Slave/Process ID =  8897   Slave Name = [wcm]
Slave/Process ID =  8898   Slave Name = [table_mgr]
Slave/Process ID =  8901   Slave Name = [iosd]

デバイス#
```

次の例では、冗長ファシリティの状態に関する情報を表示する方法を示します。

```
デバイス# show redundancy states
         my state = 13 -ACTIVE
       peer state =  1 -DISABLED
            Mode = Simplex
```

```
         Unit ID = 1

 Redundancy Mode (Operational) = SSO
  Redundancy Mode (Configured) = SSO
              Redundancy State = Non Redundant
                    Manual Swact = disabled (system is simplex (no peer unit))

  Communications = Down      Reason: Simplex mode

    client count = 75
  client_notification_TMR = 360000 milliseconds
           keep_alive TMR = 9000 milliseconds
         keep_alive count = 0
     keep_alive threshold = 18
            RF debug mask = 0
```

デバイス#

show switch

スタックメンバまたはスイッチスタックに関連した情報を表示するには、EXECモードで**show switch**コマンドを使用します。

show switch [{*stack-member-number* | **detail** | **neighbors** | **stack-ports** [{**summary**}]}]

構文の説明

stack-member-number	（任意）スタック メンバ数。指定できる範囲は 1 ～ 9 です。
detail	（任意）スタック リングの詳細情報を表示します。
neighbors	（任意）スイッチ スタック全体のネイバーを表示します。
stack-ports	（任意）スイッチ スタック全体のポート情報を表示します。
summary	（任意）スタック ケーブルの長さ、スタック リンクのステータス、およびループバックのステータスを表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

このコマンドでは、次のステートが表示されます。

- Initializing：スイッチはスタックに追加されたばかりで、ready 状態になるための基本的な初期化が完了していません。
- HA Sync in Progress：スタンバイが選出されると、同期が終了するまで対応するスイッチはこの状態のままになります。
- Syncing：既存のスタックに追加されたスイッチは、スイッチ追加シーケンスが完了するまでこの状態のままになります。
- Ready：メンバがシステム レベルおよびインターフェイス レベルの設定のロードを完了し、トラフィックを転送できるようになっています。
- V-Mismatch：Version-Mismatch モードのスイッチ。Version-Mismatch モードは、スタックに参加したスイッチのソフトウェアバージョンがアクティブスイッチと非互換である場合です。
- Provisioned：スイッチ スタックのアクティブ メンバになる前にすでに設定されていたスイッチの状態です。プロビジョニングされたスイッチでは、MAC アドレスおよびプライオリティ番号は、常に 0 と表示されます。
- Unprovisioned：プロビジョニングされたスイッチ番号が **no switch** *switch-number* **provision** コマンドを使用してプロビジョニング解除された場合の状態です。
- Removed：スタックに存在していたスイッチが、**reload slot** コマンドを使用して除外された場合です。
- Sync not started：複数のスイッチが既存のスタックに同時に追加された場合、アクティブスイッチが 1 台ずつ追加します。追加中のスイッチは Syncing 状態になります。まだ追加されていないスイッチは Sync not started 状態になります。
- Lic-Mismatch：スイッチのライセンスレベルがアクティブスイッチと異なります。

スタックメンバ（アクティブスイッチを含む）の代表的なステート遷移は、Waiting > Initializing > Ready です。

Version Mismatch（VM）モードのスタックメンバの代表的なステート遷移は、Waiting > Ver Mismatch です。

スイッチスタックにプロビジョニングされたスイッチが存在するかどうかを識別するには、**show switch** コマンドを使用できます。**show running-config** および **show startup-config** 特権 EXEC コマンドでは、この情報は提供されません。

永続的 MAC アドレスがイネーブルになっている場合、スタックの MAC-persistency wait-time も表示されます。

例

次に、スタック情報の概要を表示する例を示します。

```
デバイス# show switch
Switch/Stack Mac Address : 6400.f124.e900
                                           H/W   Current
Switch#   Role    Mac Address     Priority Version  State
```

```
-----------------------------------------------------------
 1       Member   0000.0000.0000     0      0       Provisioned
 2       Member   0000.0000.0000     0      0       Removed
*3       Active   6400.f124.e900     2      0       Ready
 8       Member   0000.0000.0000     0      0       Unprovisioned
```

次に、スタック情報の詳細を表示する例を示します。

```
デバイス# show switch detail
Switch/Stack Mac Address : 2037.06ce.3f80 - Local Mac Address
Mac persistency wait time: Indefinite
                                           H/W   Current
Switch#   Role   Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Active 2037.06ce.3f80     1      0       Ready
 2       Member 0000.000.0000      0      0       Provisioned
 6       Member 2037.06ce.1e00     1      0       Ready

           Stack Port Status             Neighbors
Switch#   Port 1     Port 2           Port 1   Port 2
-----------------------------------------------------------
  1       Ok         Down             6        None
  6       Down       Ok               None       1
```

次に、メンバ 6 の要約情報を表示する例を示します。

```
デバイス# show switch 6
Switch#  Role      Mac Address     Priority     State
-----------------------------------------------------------
 6       Member     0003.e31a.1e00     1         Ready
```

次に、スタックに関するネイバー情報を表示する例を示します。

```
デバイス# show switch neighbors
  Switch #    Port A       Port B
  --------    ------       ------
      6         None          8
      8          6           None
```

次に、スタック ポート情報を表示する例を示します。

```
デバイス# show switch stack-ports
  Switch #    Port A       Port B
  --------    ------       ------
    6          Down          Ok
    8           Ok           Down
```

次に、**show switch stack-ports summary** コマンドの出力例を示します。次の表に、この出力で表示されるフィールドについて説明します。

表 *56 : show switch stack-ports summary* コマンドの出力

フィールド	説明
Switch#/Port#	メンバー番号と、そのスタックポート番号。

フィールド	説明
スタックポートのステータス	スタックポートのステータス。 • Down：ケーブルは検出されましたが、接続されたネイバーがアップになっていないか、スタックポートがディセーブルになっています。 • OK：ケーブルが検出され、接続済みのネイバーが起動しています。
ネイバー	スタックケーブルの接続先の、アクティブなメンバーのスイッチの数。
ケーブル長	有効な長さは 50 cm、1 m、または 3 m です。 スイッチがケーブルの長さを検出できない場合は、値は *no cable* になります。ケーブルが接続されていないか、リンクが信頼できない可能性があります。
リンク OK	スタックケーブルが接続され機能しているかどうか。相手側には、接続されたネイバーが存在する場合も、そうでない場合もあります。 リンクパートナーは、ネイバースイッチ上のスタックポートのことです。 • No：このポートに接続されているスタックケーブルがないか、スタックケーブルが機能していません。 • Yes：このポートには正常に機能するスタックケーブルが接続されています。
リンクアクティブ	スタックケーブル相手側にネイバーが接続されているかどうか。 • No：相手側にネイバーが検出されません。ポートは、このリンクからトラフィックを送信できません。 • Yes：相手側にネイバーが検出されました。ポートは、このリンクからトラフィックを送信できます。
同期 OK	リンクパートナーが、スタックポートに有効なプロトコルメッセージを送信するかどうか。 • No：リンクパートナーからスタックポートに有効なプロトコルメッセージが送信されません。 • Yes：リンクの相手側は、ポートに有効なプロトコルメッセージを送信します。
# Changes to LinkOK	リンクの相対的安定性。 短期間で多数の変更が行われた場合は、リンクのフラップが発生することがあります。

フィールド	説明
ループバック内	スタックケーブルがメンバのスタックポートに接続されているかどうか。 • No：メンバ上の少なくとも 1 つのスタックポートに接続済みのスタックケーブルがあります。 • Yes：メンバーのどのスタック ポートにも、スタックケーブルが接続されていません。

show redundancy config-sync

コンフィギュレーション同期障害情報または無視された Mismatched Command List（MCL）（存在する場合）を表示するには、EXEC モードで **show redundancy config-sync** コマンドを使用します。

show redundancy config-sync {**failures** {**bem** | **mcl** | **prc**} | **ignored failures mcl**}

構文の説明

failures	MCL エントリまたはベスト エフォート方式（BEM）/パーサー リターン コード（PRC）の障害を表示します。
bem	BEM 障害コマンド リストを表示し、スタンバイスイッチを強制的にリブートします。
mcl	スイッチの実行コンフィギュレーションに存在するがスタンバイスイッチのイメージでサポートされていないコマンドを表示し、スタンバイスイッチを強制的にリブートします。
prc	PRC 障害コマンドリストを表示し、スタンバイスイッチを強制的にリブートします。
ignored failures mcl	無視された MCL 障害を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

2 つのバージョンの Cisco IOS イメージが含まれている場合は、それぞれのイメージによってサポートされるコマンドセットが異なる可能性があります。このような不一致コマンドのいず

れかがアクティブスイッチで実行された場合、スタンバイスイッチでそのコマンドを認識できない可能性があり、これにより設定の不一致状態が発生します。バルク同期中にスタンバイスイッチでコマンドの構文チェックが失敗すると、コマンドはMCLに移動し、スタンバイスイッチはリセットされます。すべての不一致コマンドを表示するには、**show redundancy config-sync failures mcl** コマンドを使用します。

MCL を消去するには、次の手順を実行します。

1. アクティブスイッチの実行コンフィギュレーションから、不一致コマンドをすべて削除します。
2. **redundancy config-sync validate mismatched-commands** コマンドを使用して、修正した実行コンフィギュレーションに基づいて MCL を再確認します。
3. スタンバイスイッチをリロードします。

または、次の手順を実行して MCL を無視することもできます。

1. **redundancy config-sync ignore mismatched-commands** コマンドを入力します。
2. スタンバイスイッチをリロードします。システムは SSO モードに遷移します。

（注） 不一致コマンドを無視する場合、アクティブスイッチとスタンバイスイッチの同期していないコンフィギュレーションは存在したままです。

3. 無視された MCL は、**show redundancy config-sync ignored mcl** コマンドを使用して確認できます。

各コマンドでは、そのコマンドを実装するアクション機能において戻りコードが設定されます。この戻りコードは、コマンドが正常に実行されたかどうかを示します。アクティブスイッチは、コマンドの実行後に PRC を維持します。スタンバイスイッチはコマンドを実行し、アクティブスイッチに PRC を返します。これら 2 つの PRC が一致しないと、PRC 障害が発生します。バルク同期または 1 行ごとの（LBL）同期中にスタンバイスイッチで PRC エラーが生じた場合、スタンバイスイッチはリセットされます。すべてのPRC障害を表示するには、**show redundancy config-sync failures prc** コマンドを使用します。

ベスト エフォート方式（BEM）エラーを表示するには、**show redundancy config-sync failures bem** コマンドを使用します。

次に、BEM 障害を表示する例を示します。

```
デバイス> show redundancy config-sync failures bem
BEM Failed Command List
-----------------------

 The list is Empty
```

次に、MCL 障害を表示する例を示します。

```
デバイス> show redundancy config-sync failures mcl
Mismatched Command List
------------------------

The list is Empty
```

次に、PRC 障害を表示する例を示します。

```
デバイス# show redundancy config-sync failures prc
PRC Failed Command List
------------------------

 The list is Empty
```

show tech-support stack

テクニカルサポートに使用するスイッチスタック関連のすべての情報を表示するには、特権 EXEC モードで **show tech-support stack** コマンドを使用します。

show tech-support stack

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.12.1	このコマンドの出力が拡張され、より多くのスタック関連情報が含まれるようになりました。

使用上のガイドライン

show tech-support stack コマンドは、スタック構成の状態のスナップショットをキャプチャし、問題のデバッグに役立つ情報を提供します。このコマンドは、スタック構成に関する問題（スタックケーブルの問題、サイレントリロード、スイッチが準備完了にならない、スタックのクラッシュなど）が発生した場合に使用します。

show tech-support stack コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします（たとえば、**show tech-support stack | redirect flash:***filename*）。

show tech stack コマンドの出力には次のコマンドが表示されます。

- **show clock**
- **show version**
- **show running-config**
- **show redundancy switchover history**

- **show switch stack-ports summary**
- **show switch stack-mode**
- **show switch stack-ring speed**
- **show switch stack-bandwidth**
- **show switch detail**
- **show switch neighbors**

次のコマンドは、待受開始状態のスタック構成のスイッチでのみ使用できます。

- **show platform software stack-mgr switch**
- **show platform software sif switch**
- **show platform hardware fed switch**
- **dir crashinfo:**
- **dir flash:/core**

例

次に、**show tech-support stack** コマンドの出力例を示します。

```
Device# show tech-support stack

.
.
.
 ------------------ show switch stack-ports summary ------------------


Sw#/Port#  Port Status  Neighbor  Cable Length   Link OK   Link Active   Sync OK
#Changes to LinkOK  In Loopback
-------------------------------------------------------------------------------------------------
1/1        OK           3         50cm           Yes       Yes           Yes       1
                No
1/2        OK           2         50cm           Yes       Yes           Yes       1
                No
2/1        OK           1         50cm           Yes       Yes           Yes       1
                No
2/2        OK           3         50cm           Yes       Yes           Yes       1
                No
3/1        OK           2         50cm           Yes       Yes           Yes       1
                No
3/2        OK           1         50cm           Yes       Yes           Yes       1
                No


------------------ show switch stack-mode ------------------


Switch#  Role    Mac Address     Version   Mode  Configured  State
-------------------------------------------------------------------------------
*1       Active   046c.9d1e.f380           N+1     None       Ready
 2       Member   0c75.bd11.5d80    V01     N+1     None       Ready
 3       Standby  0c75.bd11.59ff    P1A     N+1     None       Ready
```

```
------------------ show switch stack-bandwidth ------------------

                   Stack       Current
Switch#   Role     Bandwidth   State
-----------------------------------------------------------
*1       Active    480G        Ready
 2       Member    480G        Ready
 3       Standby   480G        Ready



------------------ show switch stack-ring speed ------------------


Stack Ring Speed        : 480G
Stack Ring Configuration: Full
Stack Ring Protocol     : StackWise


------------------ show switch detail ------------------


Switch/Stack Mac Address : 046c.9d1e.f380 - Local Mac Address
Mac persistency wait time: Indefinite
                                           H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-----------------------------------------------------------------------------------------
*1       Active   046c.9d1e.f380     1             Ready
 2       Member   0c75.bd11.5d80     1      V01    Ready
 3       Standby  0c75.bd11.59ff     1      P1A    Ready


         Stack Port Status             Neighbors
Switch#  Port 1     Port 2           Port 1   Port 2
---------------------------------------------------------
  1         OK         OK               3        2
  2         OK         OK               1        3
  3         OK         OK               2        1


------------------ show switch neighbors ------------------


  Switch #    Port 1       Port 2
  --------    ------       ------
      1         3            2
      2         1            3
      3         2            1


------------------ show platform software stack-mgr switch 1 R0 oir-states --

Switch#       OIR State               Type                    Provisioned
-----------------------------------------------------------------------
1             CHASSIS_COMPATIBLE      C9300-24U               YES
```

```
2             CHASSIS_COMPATIBLE      C9300-48U              YES
3             CHASSIS_COMPATIBLE      C9300-48U              YES


------------------ show platform software stack-mgr switch 1 R0 sdp-counters --

Stack Discovery Protocol (SDP) Counters

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

Message                 Tx Success    Tx Fail       Rx Success    Rx Fail
------------------------------------------------------------------------------
Discovery               16            0             27            0
Neighbor                5             1             5             2
Keepalive               473           0             945           0
SEPPUKU                 0             0             0             0
Standby Elect Req       1             0             0             0
Standby Elect Ack       0             0             1             0
Standby IOS State       0             0             2             0
Reload Req              0             0             0             0
Reload Ack              0             0             0             0
SESA Mesg               0             0             0             0
RTU Msg                 1             0             4             0
Disc Timer Stop         1             0             2             0

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

------------------ show platform software sif switch 1 R0 counters ------------------

Stack Interface (SIF) Counters

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

Stack Discovery Protocol (SDP) Messages
---------------------------------------
Message                 Tx Success    Tx Fail       Rx Success    Rx Fail
------------------------------------------------------------------------------
Discovery               0             0             0             0
Neighbor                0             0             0             0
Forward                 516           0             1040          0

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

SIF Management Messages
-----------------------
Message                 Success       Fail
-------------------------------------------------
Link Status             4             0
Link Management         0             0
Chassis Num             1             0
Topo Change             2             0
Active Declare          1             0
Template set            0             0

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

------------------ show platform software sif switch 1 R0 counters oob ------------------
```

```
SIF OOB Statistics
----------------------
Message                 Count
-----------------------------------
TX LSMPI                524
TX Enq Failed           0
TX Copy Failed          0
TX Ring Full            0
TX Iter                 516
TX Enq Success          526
RX Process              1042
RX Exception            0
RX Total                1042
Dequeue Attempts        986
Dequeue Success         1043

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

SIF Netdrv OOB Statistics
Unicast Messages
----------------------
Switch        Count
--------------------------
2             42228
3             79287
----------------------
Broadcast messages count: 4

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


------------------ show platform software sif switch 1 R0 counters cable ------------------


SIF Cable Statistics
--------------------
Direction     Remove        Insert
-----------------------------------------
East          0             1
West          0             1

-----------------------------------
SIF Link Statistics
--------------------
ASIC          Port          State         Changes
-------------------------------------------------------
0             1             1             2
1             2             1             2

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


------------------ show platform software sif switch 1 R0 exceptions ------------------


------------------ show platform software sif switch 1 R0 topo ------------------


Stack Interface (SIF) Topology

------------------------------
```

```
Stacked Switch List
-------------------------------------
Chassis#      MAC Adress              Role
-----------------------------------------------------
3             0c75.bd11.59ff
2             0c75.bd11.5d80
1             046c.9d1e.f380          L,A

L: Local Switch;  A: Active Switch;
-------------------------------------
.
.
.
```

出力フィールドの意味は自明です。

stack-mac update force

スタック MAC アドレスをアクティブスイッチの MAC アドレスに更新するには、アクティブスイッチの EXEC モードで **stack-mac update force** コマンドを使用します。

stack-mac update force

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

デフォルトでは、ハイ アベイラビリティ（HA）フェールオーバー時に、スタックの MAC アドレスは新しいアクティブスイッチの MAC アドレスに変更されません。スタック MAC アドレスが新しいアクティブスイッチの MAC アドレスに強制的に変更されるようにするには、**stack-mac update force** コマンドを使用します。

スタック MAC アドレスと同じ MAC アドレスを持つスイッチが現在そのスタックのメンバである場合、**stack-mac update force** コマンドは無効です（スタック MAC アドレスはアクティブスイッチの MAC アドレスに更新されません）。

（注） スタック MAC アドレスを変更しない場合、レイヤ 3 インターフェイスのフラップが発生しません。これは、未知の MAC アドレス（スタック内のスイッチに属さない MAC アドレス）がスタック MAC アドレスになる可能性があることを意味します。この未知の MAC アドレスを持つスイッチが別のスタックにアクティブスイッチとして参加すると、2 つのスタックが同じスタック MAC アドレスを持つことになります。**stack-mac update force** コマンドを使用して、この競合を解決する必要があります。

次に、スタック MAC アドレスをアクティブスイッチの MAC アドレスに更新する例を示します。

```
デバイス> stack-mac update force
デバイス>
```

設定を確認するには、**show switch** 特権 EXEC コマンドを入力します。スタック MAC アドレスには、MAC アドレスがローカルと未知のどちらであるかも含まれます。

standby console enable

スタンバイ スイッチ コンソールへのアクセスをイネーブルにするには、冗長メイン コンフィギュレーション サブモードで **standby console enable** コマンドを使用します。スタンバイ スイッチ コンソールへのアクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

standby console enable
no standby console enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

スタンバイ スイッチ コンソールへのアクセスはディセーブルです。

コマンド モード

冗長メイン コンフィギュレーション サブモード

コマンド履歴

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

使用上のガイドライン

このコマンドは、スタンバイ コンソールに関する特定のデータを収集し、確認するために使用されます。コマンドは、主にシスコのテクニカル サポート担当がスイッチのトラブルシューティングを行うのに役立ちます。

次に、冗長メイン コンフィギュレーション サブモードを開始し、スタンバイ コンソール スイッチへのアクセスをイネーブルにする例を示します。

```
デバイス(config)# redundancy
デバイス(config-red)# main-cpu
デバイス(config-r-mc)# standby console enable
デバイス(config-r-mc)#
```

switch stack port

メンバの指定されたスタックポートをディセーブルまたはイネーブルにするには、スタックメンバの特権 EXEC モードで **switch** コマンドを使用します。

switch *stack-member-number* **stack port** *port-number* {**disable** | **enable**}

構文の説明

stack-member-number	
stack port *port-number*	メンバ上のスタック ポートを指定します。指定できる範囲は 1 ～ 2 です。
disable	指定したポートをディセーブルにします。
enable	指定されたポートをイネーブルにします。

コマンド デフォルト

スタック ポートはイネーブルです。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

スタックが次の状態 スタックが full-ring 状態になるのは、すべてのスタック メンバがスタック ポートを使用して接続され、ready 状態になっている場合です。

スタックが次の状態 スタックが partial-ring 状態になるのは、次が発生したときです。

- すべてのメンバがスタック ポートを通じて接続されたが、一部が ready ステートではない。
- スタック ポートを通じて接続されていないメンバーがある。

（注） **switch** *stack-member-number* **stack port** *port-number* **disable** コマンドを使用するときは注意してください。スタック ポートをディセーブルにすると、スタックは半分の帯域幅で稼働します。

switch *stack-member-number* **stack port** *port-number* **disable** 特権 EXEC コマンドを入力し、スタックが full-ring 状態にある場合、ディセーブルにできるスタックポートは 1 つだけです。次のメッセージが表示されます。

```
Enabling/disabling a stack port may cause undesired stack changes. Continue?[confirm]
```

switch *stack-member-number* **stack port** *port-number* **disable** 特権 EXEC コマンドを入力し、スタックが partial-ring 状態にある場合、ポートはディセーブルにできません。次のメッセージが表示されます。

```
Disabling stack port not allowed with current stack configuration.
```

例

次に、member 4 上の stack port 2 をディセーブルにする方法の例を示します。

```
デバイス# switch 4 stack port 2 disable
```

switch priority

スタックメンバ のプライオリティ値を変更するには、active switchの EXEC モードで **switch priority** コマンドを使用します。

switch *stack-member-number* **priority** *new-priority-value*

構文の説明

stack-member-number	
new-priority-value	スタック メンバの新しいプライオリティ値指定できる範囲は 1 ～ 15 です。

コマンド デフォルト

デフォルトのプライオリティ値は 1 です。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

新しいプライオリティ値は、新しい active switch 選定の要素になります。プライオリティ値を変更しても、active switch がただちに変更されることはありません。

例

次の例では、スタック メンバ 6 のプライオリティ値を 8 に変更する方法を示します。

```
デバイス# switch 6 priority 8
Changing the Switch Priority of Switch Number 6 to 8
Do you want to continue?[confirm]
```

switch provision

新しいスイッチがスイッチスタックに追加される前に構成設定するには、active switchのグローバル コンフィギュレーション モードで **switch provision** コマンドを使用します。除外されたスイッチ（スタックを離れたスタック メンバ）に対応するすべての設定情報を削除するには、このコマンドの **no** 形式を使用します。

switch *stack-member-number* **provision** *type*
no switch *stack-member-number* **provision**

構文の説明

stack-member-number	
type	新しいスイッチがスタックに加入する前の、このスイッチのタイプ。

コマンド デフォルト

スイッチは、プロビジョニングされていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

type には、コマンドライン ヘルプ ストリングに示されたサポート対象のスイッチのモデル番号を入力します。

エラー メッセージを受信しないようにするには、このコマンドの **no** 形式を使用してプロビジョニングされた設定を削除する前に、スイッチ スタックから指定のスイッチを削除する必要があります。

スイッチ タイプを変更する場合も、スイッチ スタックから指定のスイッチを削除する必要があります。スイッチ タイプを変更しない場合でも、スイッチ スタック内に物理的に存在するプロビジョニングされたスイッチのスタック メンバ番号を変更できます。

プロビジョニングされたスイッチのタイプが、スタック上のプロビジョニングされた設定のスイッチ タイプと一致しない場合、スイッチ スタックはプロビジョニングされたスイッチにデフォルト設定を適用し、これをスタックに追加します。スイッチスタックでは、デフォルト設定を適用する場合にメッセージを表示します。

プロビジョニング情報は、スイッチスタックの実行コンフィギュレーションで表示されます。**copy running-config startup-config** 特権 EXEC コマンドを入力すると、プロビジョニングされた設定がスイッチスタックのスタートアップ コンフィギュレーション ファイルに保存されます。

⚠

注意 **switch provision** コマンドを使用すると、プロビジョニングされた設定にメモリが割り当てられます。新しいスイッチタイプが設定されたときに、以前割り当てられたメモリのすべてが解放されるわけではありません。そのため、このコマンドをおおよそ200回を超えて使用しないようにしてください。スイッチのメモリが不足し、予期せぬ動作が発生する可能性があります。

例

次に、スタック メンバー番号2が設定されたスイッチをスイッチ スタックに割り当てる例を示します。**show running-config** コマンドの出力は、プロビジョニングされたスイッチに関連付けられたインターフェイスを示します。

```
デバイス(config)# switch 2 provision WS-xxxx
デバイス(config)# end
デバイス# show running-config | include switch 2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
<output truncated>
```

また、**show switch** ユーザ EXEC コマンドを入力すると、スイッチ スタックのプロビジョニングされたステータスを表示できます。

次の例では、スイッチがスタックから削除される場合に、スタック メンバ5についてのすべての設定情報が削除される方法を示します。

```
デバイス(config)# no switch 5 provision
```

プロビジョニングされたスイッチが、実行コンフィギュレーションで追加または削除されたことを確認するには、**show running-config** 特権 EXEC コマンドを入力します。

switch renumber

スタックメンバ 番号を変更するには、active switchの EXEC モードで **switch renumber** コマンドを使用します。

switch *current-stack-member-number* **renumber** *new-stack-member-number*

構文の説明

current-stack-member-number
new-stack-member-number

コマンド デフォルト デフォルトのスタック メンバ番号は 1 です。

コマンド モード ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

指定したメンバ番号をすでに他のスタック メンバが使用している場合、スタック メンバをリロードする際に active switch は使用可能な一番低い番号を割り当てます。

（注） スタック メンバ番号を変更し、新しいスタック メンバ番号がどの設定にも関連付けされていない場合、そのスタック メンバは現在の設定を廃棄してリセットを行い、デフォルトの設定に戻ります。

プロビジョニングされたスイッチでは、**switch** *current-stack-member-number* **renumber** *new-stack-member-number* コマンドを使用しないでください。使用すると、コマンドは拒否されます。

スタックメンバをリロードし、設定変更を適用するには、**reload slot** *current stack member number* 特権 EXEC コマンドを使用します。

例

次の例では、スタック メンバ 6 のメンバ番号を 7 に変更する方法を示しています。

```
デバイス# switch 6 renumber 7
WARNING:Changing the switch number may result in a configuration change for that switch.
The interface configuration associated with the old switch number will remain as a
provisioned configuration.
Do you want to continue?[confirm]
```

switch renumber

スタックメンバ 番号を変更するには、active switchの EXEC モードで **switch renumber** コマンドを使用します。

switch *current-stack-member-number* **renumber** *new-stack-member-number*

構文の説明

current-stack-member-number
new-stack-member-number

コマンド デフォルト

デフォルトのスタック メンバ番号は 1 です。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

指定したメンバ番号をすでに他のスタック メンバが使用している場合、スタック メンバをリロードする際に active switch は使用可能な一番低い番号を割り当てます。

（注） スタック メンバ番号を変更し、新しいスタック メンバ番号がどの設定にも関連付けされていない場合、そのスタックメンバは現在の設定を廃棄してリセットを行い、デフォルトの設定に戻ります。

プロビジョニングされたスイッチでは、**switch** *current-stack-member-number* **renumber** *new-stack-member-number* コマンドを使用しないでください。使用すると、コマンドは拒否されます。

スタックメンバをリロードし、設定変更を適用するには、**reload slot** *current stack member number* 特権 EXEC コマンドを使用します。

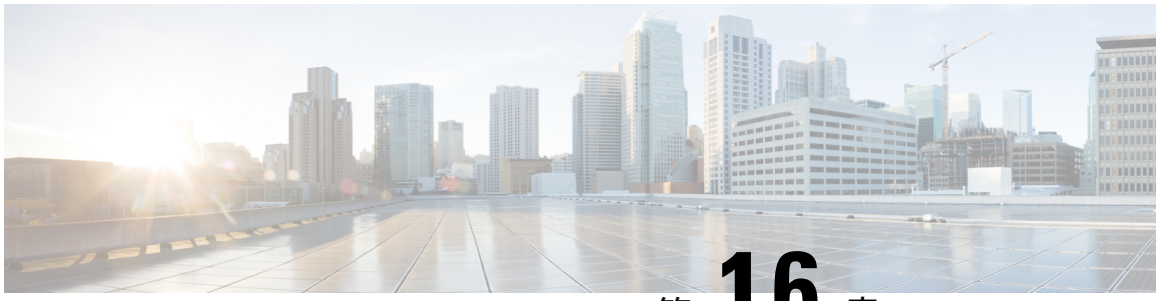
例

次の例では、スタック メンバ 6 のメンバ番号を 7 に変更する方法を示しています。

```
デバイス# switch 6 renumber 7
WARNING:Changing the switch number may result in a configuration change for that switch.
The interface configuration associated with the old switch number will remain as a
provisioned configuration.
Do you want to continue?[confirm]
```

第 XIII 部

システム管理



第 16 章

システム管理コマンド

arp

Address Resolution Protocol（ARP）テーブルの内容を表示するには、ブートローダモードで **arp** コマンドを使用します。

arp [*ip_address*]

構文の説明

ip_address	（任意）ARP テーブルまたは特定の IP アドレスのマッピングを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

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

使用上のガイドライン

ARP テーブルには、IP アドレスと MAC アドレスのマッピングが示されます。

例

次に、ARP テーブルを表示する例を示します。

```
デバイス: arp 172.20.136.8
arp'ing 172.20.136.8...
172.20.136.8 is at 00:1b:78:d1:25:ae, via port 0
```

boot

実行可能イメージをロードおよびブートして、コマンドライン インターフェイス（CLI）を表示するには、ブートローダモードで **boot** コマンドを使用します。

boot ［**-post** | **-n** | **-p** | *flag*］ *filesystem:/file-url...*

構文の説明

-post	（任意）拡張および総合POSTによってロードされたイメージを実行します。このキーワードを使用すると、POST の完了に要する時間が長くなります。
-n	（任意）起動後すぐに、Cisco IOS デバッガが休止します。
-p	（任意）イメージのロード後すぐに、JTAG デバッガが休止します。
filesystem:	ファイルシステムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。USB メモリスティックには **usbflash0:** を使用します。
/file-url	ブート可能なイメージのパス（ディレクトリ）および名前。各イメージ名はセミコロンで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

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

使用上のガイドライン

引数を何も指定しないで **boot** コマンドを入力した場合、deviceは、BOOT 環境変数が設定されていればその中の情報を使用して、システムを自動的にブートしようとします。

file-url 変数にイメージ名を指定した場合、**boot** コマンドは指定されたイメージをブートしようとします。

ブートローダ **boot** コマンドのオプションを設定した場合は、このコマンドがただちに実行され、現在のブートローダセッションだけに適用されます。

これらの設定が保存されて次回のブート処理に使用されることはありません。

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

例

次の例では、*new-image.bin* イメージを使用してdeviceをブートする方法を示します。

```
デバイス: set BOOT flash:/new-images/new-image.bin
デバイス: boot
```

このコマンドを入力すると、セットアッププログラムを開始するように求められます。

cat

1つ以上のファイルの内容を表示するには、ブートローダモードで**cat**コマンドを使用します。

cat *filesystem:/file-url...*

構文の説明

filesystem:	ファイルシステムを指定します。
/file-url	表示するファイルのパス（ディレクトリ）と名前を指定します。ファイル名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

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

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

ファイルのリストを指定した場合は、各ファイルの内容が順に表示されます。

例

次の例では、イメージファイルの内容を表示する方法を示します。

```
デバイス: cat flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

clear location

特定の電波による個体識別（RFID）タグまたはデータベース全体のすべてのRFIDタグ情報をクリアするには、EXEC モードで **clear location** コマンドを使用します。

clear location [mac-address *mac-address* | **rfid]**

構文の説明

mac-address *mac-address*	特定の RFID タグの MAC アドレス。
rfid	データベース上のすべてのRFIDタグを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

次に、データベースからすべての RFID タグ情報をクリアする例を示します。

```
デバイス> clear location rfid
```

clear location statistics

電波による個体識別（RFID）の統計情報をクリアするには、**clear location statistics** コマンドを使用します。

clear location statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

次に、**clear location rfid** コマンドの出力例と、RFID 統計情報をクリアする例を示します。

```
デバイス> clear location statistics
```

copy

ファイルをコピー元からコピー先にコピーするには、ブートローダモードで **copy** コマンドを使用します。

copy *filesystem:/source-file-url filesystem:/destination-file-url*

構文の説明

filesystem:	ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。
/source-file-url	コピー元のパス（ディレクトリ）およびファイル名です。
/destination-file-url	コピー先のパス（ディレクトリ）およびファイル名です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

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

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

スラッシュ（/）間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

指定できるファイル名は最大127文字です。ファイル名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

ファイルを別のディレクトリにコピーする場合は、そのディレクトリが存在していなければなりません。

例

次の例では、ルートにあるファイルをコピーする方法を示します。

```
デバイス: copy usbflash0:test1.text usbflash0:test4.text
File "usbflash0:test1.text" successfully copied to "usbflash0:test4.text"
```

ファイルがコピーされたかどうかを確認するには、**dir** *filesystem:* ブートローダコマンドを入力します。

copy startup-config tftp:

スイッチから TFTP サーバに設定をコピーするには、特権 EXEC モードで **copy startup-config tftp:** コマンドを使用します。

copy startup-config tftp: *remote host {ip-address}/{name}*

構文の説明

remote host {ip-address}/{name}	リモートホストのホスト名または IP アドレス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 16.1	このコマンドが導入されました。

使用上のガイドライン

スイッチから現在の設定をコピーするには、**copy startup-config tftp:** コマンドを実行し、続く指示に従います。設定が TFTP サーバにコピーされます。

次に、別のスイッチへログインし、**copy tftp: startup-config** コマンドを実行して、続く指示に従います。これで、設定は別のスイッチにコピーされます。

例

次に、TFTP サーバに設定をコピーする例を示します。

```
デバイス: copy startup-config tftp:
Address or name of remote host []?
```

copy tftp: startup-config

TFTP サーバから新しいスイッチに設定をコピーするには、新しいスイッチ上で、特権 EXEC モードで **copy tftp: startup-config** コマンドを使用します。

copy tftp: startup-config *remote host {ip-address}/{name}*

構文の説明

remote host {ip-address}/{name}	リモートホストのホスト名または IP アドレス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 16.1	このコマンドが導入されました。

使用上のガイドライン

設定をコピーした後、その設定を保存するには、**write memory** コマンドを使用し、その後スイッチをリロードするか、または **copy startup-config running-config** コマンドを実行します。

例

次に、TFTP サーバからスイッチに設定をコピーする例を示します。

```
デバイス: copy tftp: startup-config
Address or name of remote host []?
```

debug platform condition feature multicast controlplane

Internet Group Management Protocol（IGMP）およびマルチキャストリスナー検出（MLD）のスヌーピング機能の放射線トレースを有効にするには、特権 EXEC モードで **debug platform condition feature multicast controlplane** コマンドを使用します。放射線トレー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。

debug platform condition feature multicast controlplane {{igmp-debug | pim} group-ip {*ipv4 address* | *ipv6 address***} | {mld-snooping | igmp-snooping} mac** *mac-address* **ip {***ipv4 address* | *ipv6 address***} vlan** *vlan-id* **} level {debug | error | info | verbose | warning}**
no debug platform condition feature multicast controlplane {{igmp-debug | pim} group-ip {*ipv4 address* | *ipv6 address***} | {mld-snooping | igmp-snooping} mac** *mac-address* **ip {***ipv4 address* | *ipv6 address***} vlan** *vlan-id* **} level {debug | error | info | verbose | warning}**

構文の説明

igmp-debug	IGMP制御の放射線トレースを有効にします。
pim	Protocol Independent Multicast（PIM）制御の放射線トレースを有効にします。
mld-snooping	MLD スヌーピング制御の放射線トレースを有効にします。
igmp-snooping	IGMP スヌーピング制御の放射線トレースを有効にします。
mac *mac-address*	受信者の MAC アドレス。
group-ip {*ipv4 address* | *ipv6 address***}**	igmp-debug または pim グループの IPv4 または IPv6 アドレス。

ip {*ipv4 address* | *ipv6 address*}	mld-snooping または igmp-snooping グループの IPv4 または IPv6 アドレス。
vlan *vlan-id*	VLAN ID。指定できる範囲は 1 ～ 4094 です。
level	デバッグの重大度レベルを有効にします。
debug	デバッグレベルを有効にします。
error	エラーデバッグを有効にします。
info	情報デバッグを有効化します。
verbose	詳細デバッグを有効にします。
warning	警告デバッグを有効にします。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

次に、IGMP スヌーピングの放射線トレース有効にする例を示します。

```
Device# debug platform condition feature multicast controlplane igmp-snooping mac
000a.f330.344a ip 10.1.1.10 vlan 550 level warning
```

関連コマンド

Command	Description
clear debug platform condition all	プラットフォームに適用されているデバッグ条件を削除します。
debug platform condition	指定した条件に基づいて **debug** コマンドのデバッグ出力をフィルタリングします。
debug platform condition start	システムの条件付きデバッグを開始します。
debug platform condition stop	システムの条件付きデバッグを停止します。

Command	Description
show platform condition	現在アクティブなデバッグ設定を表示します。

debug platform condition mac

MAC ラーニングの放射線トレースを有効にするには、特権 EXEC モードで **debug platform condition mac** コマンドを使用します。MAC ラーニングの放射線トレー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。

debug platform condition mac {*mac-address* **{control-plane | egress | ingress} | access-list** *access-list name* **{egress | ingress}}**
no debug platform condition mac {*mac-address* **{control-plane | egress | ingress} | access-list** *access-list name* **{egress | ingress}}**

構文の説明

mac *mac-address*	指定されたMACアドレスに基づいて出力をフィルタリングします。
access-list *access-list name*	指定されたアクセスリストに基づいて出力をフィルタリングします。
control-plane	コントロールプレーンのルーチンに関するメッセージを表示します。
egress	発信パケットに基づいて出力をフィルタリングします。
ingress	着信パケットに基づいて出力をフィルタリングします。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

次に、MAC アドレスに基づいてデバッグ出力をフィルタリングする例を示します。

```
Device# debug platform condition mac bc16.6509.3314 ingress
```

関連コマンド

Command	Description
show platform condition	現在アクティブなデバッグ設定を表示します。
debug platform condition	指定した条件に基づいて **debug** コマンドのデバッグ出力をフィルタリングします。
debug platform condition start	システムの条件付きデバッグを開始します。
debug platform condition stop	システムの条件付きデバッグを停止します。
clear debug platform condition all	プラットフォームに適用されているデバッグ条件を削除します。

debug platform rep

Resilient Ethernet Protocol（REP）機能のデバッグをイネーブルにするには、特権 EXEC モードで **debug platform rep** コマンドを使用します。指定した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。

debug platform rep {all | error | event | packet | verbose}
no debug platform rep {all | error | event | packet | verbose}

構文の説明

all	すべての REP デバッグ機能をイネーブルにします。
error	REP エラーデバッグをイネーブルにします。
event	REP イベントデバッグをイネーブルにします。
packet	REP パケットデバッグをイネーブルにします。
verbose	REP 詳細デバッグをイネーブルにします。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

次に、すべての機能のデバッグをイネーブルにする例を示します。

```
Device# debug platform rep all

debug platform rep verbose debugging is on
debug platform rep control pkt handle debugging is on
debug platform rep error debugging is on
debug platform rep event debugging is on
```

関連コマンド

Command	Description
show platform condition	現在アクティブなデバッグ設定を表示します。
debug platform condition	指定した条件に基づいて **debug** コマンドのデバッグ出力をフィルタリングします。
debug platform condition start	システムの条件付きデバッグを開始します。
debug platform condition stop	システムの条件付きデバッグを停止します。
clear debug platform condition all	プラットフォームに適用されているデバッグ条件を削除します。

debug voice diagnostics mac-address

音声クライアントの音声診断のデバッグを有効にするには、特権 EXEC モードで **debug voice diagnostics mac-address** コマンドを使用します。デバッグを無効にするには、このコマンドの **no** 形式を使用します。

debug voice diagnostics mac-address *mac-address1* **verbose mac-address** *mac-address2* **verbose**
nodebug voice diagnostics mac-address *mac-address1* **verbose mac-address** *mac-address2* **verbose**

構文の説明

voice diagnostics	音声クライアントの音声のデバッグを設定します。
mac-address *mac-address1* **mac-address** *mac-address2*	音声クライアントのMACアドレスを指定します。
verbose	音声診断の冗長モードを有効にします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

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

以下は、**debug voice diagnostics mac-address** コマンドの出力例で、MAC アドレスが 00:1f:ca:cf:b6:60 である音声クライアントの音声診断のデバッグを有効にする手順を示しています。

```
デバイス# debug voice diagnostics mac-address 00:1f:ca:cf:b6:60
```

delete

指定されたファイルシステムから 1 つ以上のファイルを削除するには、ブートローダモードで **delete** コマンドを使用します。

delete *filesystem:/file-url...*

構文の説明

filesystem:	ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。
/file-url...	削除するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

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

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

各ファイルを削除する前に確認を求めるプロンプトがdeviceによって表示されます。

例

次の例では、2 つのファイルを削除します。

```
デバイス: delete usbflash0:test2.text usbflash0:test5.text
Are you sure you want to delete "usbflash0:test2.text" (y/n)?y
File "usbflash0:test2.text" deleted
Are you sure you want to delete "usbflash0:test5.text" (y/n)?y
File "usbflash0:test2.text" deleted
```

ファイルが削除されたことを確認するには、**dir usbflash0:** ブートローダコマンドを入力します。

dir

指定されたファイルシステムのファイルおよびディレクトリのリストを表示するには、ブートローダモードで **dir** コマンドを使用します。

dir *filesystem:/file-url*

構文の説明

filesystem:	ファイルシステムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。USB メモリスティックには **usbflash0:** を使用します。
/file-url	（任意）表示するコンテンツが格納されているパス（ディレクトリ）およびディレクトリの名前です。ディレクトリ名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

特権 EXEC

コマンド履歴

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

使用上のガイドライン

ディレクトリ名では、大文字と小文字が区別されます。

例

次の例では、フラッシュメモリ内のファイルを表示する方法を示します。

```
デバイス: dir flash:
Directory of flash:/
    2  -rwx         561   Mar 01 2013 00:48:15  express_setup.debug
    3  -rwx     2160256   Mar 01 2013 04:18:48  c2960x-dmon-mz-150-2r.EX
    4  -rwx        1048   Mar 01 2013 00:01:39  multiple-fs
    6  drwx         512   Mar 01 2013 23:11:42  c2960x-universalk9-mz.150-2.EX
  645 drwx         512   Mar 01 2013 00:01:11  dc_profile_dir
  647 -rwx        4316   Mar 01 2013 01:14:05  config.text
  648 -rwx           5   Mar 01 2013 00:01:39  private-config.text

   96453632 bytes available (25732096 bytes used)
```

表 *57 : dir* のフィールドの説明

フィールド	説明
2	ファイルのインデックス番号

フィールド	説明
-rwx	ファイルのアクセス権（次のいずれか、またはすべて） • d：ディレクトリ • r：読み取り可能 • w：書き込み可能 • x：実行可能
1644045	ファイルのサイズ
<date>	最終変更日
env_vars	ファイル名

emergency-install

システムで緊急インストールを実行するには、ブートローダモードで**emergency-install**コマンドを使用します。

emergency-install *url://<url>*

構文の説明

<url> 緊急インストールバンドルイメージが格納されているファイルのURLと名前です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

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

使用上のガイドライン

インストール操作時にブートフラッシュが消去されます。緊急インストール操作を実行した後、ブートローダモードで**boot flash:packages.conf**コマンドを手動で実行してシステムを起動します。

例

次に、イメージファイルの内容を使用して緊急インストール操作を実行する例を示します。

```
デバイス: emergency-install tftp:<url>
The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery (tftp:<url> ...
```

```
Reading full image into memory.....................done
Nova Bundle Image
--------------------------------------
Kernel Address    : 0x6042d5c8
Kernel Size       : 0x317ccc/3243212
Initramfs Address : 0x60745294
Initramfs Size    : 0xdc6774/14444404
Compression Format: .mzip

Bootable image at @ ram:0x6042d5c8
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range          \
[0x80180000, 0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)



Initiating Emergency Installation of bundle                                      \
tftp:<url>


Downloading bundle tftp:<url>...

Validating bundle tftp:<url>...
Installing bundle tftp:<url>...
Verifying bundle tftp:<url>...
Package cat3k_caa-base.SPA.03.02.00SE.pkg is Digitally Signed
Package cat3k_caa-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-infra.SPA.03.02.00SE.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg is Digitally Signed
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-wcm.SPA.10.0.100.0.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.\ufffd


Booting...(use DDR clock 667 MHz)Initializing and Testing RAM                     \
+++@@@@####...++@@++@@++@@++@@++@@++@@++@@++@@done.
Memory Test Pass!

Base ethernet MAC Address: 20:37:06:ce:25:80
Initializing Flash...

flashfs[7]: 0 files, 1 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 6784000
flashfs[7]: Bytes used: 1024
flashfs[7]: Bytes available: 6782976
flashfs[7]: flashfs fsck took 1 seconds....done Initializing Flash.

The system is not configured to boot automatically. The
following command will finish loading the operating system
software:

    boot
```

exit

以前のモードに戻るか、CLI EXEC モードを終了するには、**exit** コマンドを使用します。

exit

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

グローバル コンフィギュレーション

コマンド履歴

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

次に、コンフィギュレーション モードを終了する例を示します。

```
デバイス(config)# exit
デバイス#
```

factory-reset

出荷時以降にデバイスに追加されたすべてのお客様固有のデータを削除するには、特権EXEC モードで **factory-reset** コマンドを使用します。

factory-reset {**all** | **config** | **boot-vars**}

構文の説明

all	設定データ、クラッシュ情報、ログファイル、ブート変数、コアファイル、現在のブートイメージを含むIOSイメージなどのすべてのデータをデバイスから削除します。
config	ユーザデータ、スタートアップ、実行コンフィギュレーションなどのすべての設定データを削除します。
boot-vars	ブート変数をリセットします。

コマンド デフォルト

このコマンドにはデフォルトはありません。

コマンド モード

特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS XE 16.6.1	このコマンドが導入されました。

使用上のガイドライン

factory-reset コマンドを使用するために必要なシステム設定はありません。すべてのオプションを有効にしてコマンドを使用してください。

factory-reset コマンドにより、IOS イメージ、ブート変数、設定データ、およびすべてのユーザデータが消去されます。設定、ログファイル、ブート変数、およびコアファイル形式のデータが対象です。

システムはリロードされ、初期設定にリセットされて、ROMMON モードで起動します。

factory reset コマンドを実行した後に、USB または TFTP を使用して ROMMON から IOS イメージをロードできます。

（注） 電源コードを抜いたり、初期設定へのリセットを中断したりしないでください。

このコマンドは、次の 2 つのシナリオで使用されます。

- デバイスの返品許可（RMA）：RMA のためにデバイスをシスコに返送する必要がある場合は、そのデバイスの RMA 証明書を取得する前に、お客様固有のデータをすべて削除してください。
- 侵害を受けたデバイスのリカバリ：デバイスに保存されているキーマテリアルまたはクレデンシャルが侵害を受けた場合は、デバイスを初期設定にリセットし、デバイスを再設定してください。

flash_init

flash: ファイルシステムを再初期化するには、ブートローダモードで **flash_init** コマンドを使用します。

flash_init

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

flash: ファイルシステムは、通常のシステム動作中に自動的に初期化されます。

コマンド モード

ブートローダ

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

使用上のガイドライン flash: ファイルシステムは、通常のブート プロセス中に自動的に初期化されます。

このコマンドは、flash: ファイルシステムを手動で初期化します。たとえば、パスワードを忘れた場合には、回復手順中にこのコマンドを使用します。

help

利用可能なコマンドを表示するには、ブートローダモードで **help** コマンドを使用します。

help

構文の説明 このコマンドには引数またはキーワードはありません。

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード ブートローダ

コマンド履歴

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

例

次に、利用可能なブートローダコマンドのリストを表示する例を示します。

```
デバイス:help
? -- Present list of available commands
arp -- Show arp table or arp-resolve an address
boot -- Load and boot an executable image
cat -- Concatenate (type) file(s)
copy -- Copy a file
delete -- Delete file(s)
dir -- List files in directories
emergency-install -- Initiate Disaster Recovery
...
...
...
unset -- Unset one or more environment variables
version -- Display boot loader version
```

install

ソフトウェア メンテナンス アップグレード（SMU）パッケージをインストールするには、特権 EXEC モードで **install** コマンドを使用します。

install {**abort** | **activate** | **file** {**bootflash:** | **flash:** | **harddisk:** | **webui:**} [{**auto-abort-timer timer** *timer* **prompt-level** {**all** | **none**}}] | **add file** {**bootflash:** | **flash:** | **ftp:** | **harddisk:** | **http:** | **https:** | **pram:** | **rcp:** | **scp:** | **tftp:** | **webui:**} [{**activate** [{**auto-abort-timer** *timer***prompt-level** {**all** |

none}**commit**}]}] | **commit** | **auto-abort-timer stop** | **deactivate file** {**bootflash:** | **flash:** | **harddisk:** | **webui:**} | **label** *id*{**description** *description* | **label-name** *name*} | **remove** {**file** {**bootflash:** | **flash:** | **harddisk:** | **webui:**} | **inactive** } | **rollback to** {**base** | **committed** | **id** {*install-ID* } | **label** {*label-name*}}}

構文の説明

abort	現在のインストール操作を中止します。
activate	**install add** コマンドを通じて SMU が追加されているかどうかを検証します。 このキーワードは、互換性チェックを実行し、パッケージ ステータスを更新します。パッケージを再起動できる場合はポストインストール スクリプトをトリガーして必要なプロセスを再起動するか、または再起動できないパッケージの場合はリロードをトリガーします。
file	アクティブにするパッケージを指定します。
{**bootflash:** | **flash:** | **harddisk:** | **webui:**}	インストールしたパッケージのロケーションを指定します。
auto-abort-timer *timer*	（任意）自動アボートタイマーをインストールします。
prompt-level {**all** | **none**}	（任意）インストール アクティビティについてのプロンプトをユーザに表示します。 たとえば、**activate** キーワードはリロードが必要なパッケージに対してリロードを自動的にトリガーします。パッケージをアクティブにする前に、続行するかどうかについてユーザに確認するプロンプトが表示されます。 **all** キーワードを使用するとプロンプトをイネーブルにすることができます。**none** キーワードはプロンプトをディセーブルにします。

add	リモートのロケーションから（FTP、TFTP 経由で）デバイスにファイルをコピーし、プラットフォームとイメージ バージョンにソフトウェア メンテナンス アップグレード（SMU）を実行します。 このキーワードは、指定したパッケージがプラットフォームで必ずサポートされるように基本の互換性チェックを実行します。また、パッケージ ファイル内にエントリを追加することで、ステータスを監視し、維持できるようにします。
{ **bootflash:** | **flash:** |**ftp:** |**harddisk:** |**http:** |**https:** | **pram:** |**rcp:** | **scp:** | **tftp:** |**webui:**}	追加するパッケージを指定します。
commit	リロード後も SMU の変更が持続されるようにします。 パッケージをアクティブにした後、システムがアップ状態にある間、または最初のリロード後にコミットを実行できます。パッケージがアクティブになっていてもコミットされていない場合は、最初のリロード後はアクティブの状態を保ちますが、2回目のリロード後はアクティブ状態を保ちません。
auto-abort-timer stop	自動アボートタイマーを停止します。
deactivate	インストールしたパッケージを非アクティブにします。 また、パッケージを非アクティブにすると、パッケージ ステータスが更新され、プロセスが再起動またはリロードされます。
label *id*	ラベルを付けるインストール ポイントの ID を指定します。
description	指定したインストール ポイントに説明を追加します。
label-name *name*	指定したインストール ポイントに説明を追加します。

remove	インストールしたパッケージを削除します。 パッケージ ファイルがファイル システムから削除されます。**remove** キーワードは、現在非アクティブ状態のパッケージでのみ使用できます。
inactive	非アクティブ状態のパケージをデバイスから削除します。
rollback	データモデルインターフェイス（DMI）パッケージ（DMP）SMU をベース バージョン、最後にコミットされたバージョン、または既知のコミット ID にロールバックします。
to base	ベース イメージに戻します。
committed	最後のコミット操作が実行されたときのインストール状態に戻します。
id *install-ID*	特定のインストールポイント ID に戻します。有効な値は、1 ～ 4294967295 です。

コマンド デフォルト

パッケージはインストールされません。

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 Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

SMUは、システムにインストールしてパッチ修正やセキュリティ解決をリリースされたイメージに提供ができるパッケージです。このパッケージには、パッケージの内容を記述するいくつかのメタデータとともに、リリースにパッチを適用するための最小限の一連のファイルが含まれています。

パッケージは、SMU をアクティブにする前に追加する必要があります。

パッケージは、ブートフラッシュから削除する前に非アクティブにする必要があります。削除したパッケージは、もう一度追加する必要があります。

例

次に、インストール パッケージをデバイスに追加する例を示します。

```
Device# install add file tftp://172.16.0.1//tftpboot/folder1/cat3k-
universalk9.2017-01-10_13.15.1.CSCxxxxxxx.SSA.dmp.bin

install_add: START Sun Feb 26 05:57:04 UTC 2017
Downloading file tftp://172.16.0.1//tftpboot/folder1/cat3k-universalk9.2017-01-10_13.15.1.
```

```
CSCvb12345.SSA.dmp.bin
Finished downloading file
tftp://172.16.0.1//tftpboot/folder1/cat3k-universalk9.2017-01-10_13.15.1.
CSCxxxxxxx.SSA.dmp.bin to
bootflash:cat3k-universalk9.2017-01-10_13.15.1.CSCxxxxxxx.SSA.dmp.bin
SUCCESS: install_add /bootflash/cat3k-universalk9.2017-01-10_13.15.1.CSCxxxxxxx.SSA.dmp.bin

Sun Feb 26 05:57:22 UTC 2017
```

次に、インストールパッケージをアクティブにする例を示します。

```
Device# install activate file bootflash:cat3k-universalk9.2017-01-10_13.15.1.
CSCxxxxxxx.SSA.dmp.bin

install_activate: START Sun Feb 26 05:58:41 UTC 2017
DMP package.
Netconf processes stopped
SUCCESS: install_activate
/bootflash/cat3k-universalk9.2017-01-10_13.15.1.CSCxxxxxxx.SSA.dmp.bin
Sun Feb 26 05:58:58 UTC 2017
*Feb 26 05:58:47.655: %DMI-4-CONTROL_SOCKET_CLOSED:  SIP0: nesd:
Confd control socket closed Lost connection to ConfD (45): EOF on socket to ConfD.
*Feb 26 05:58:47.661: %DMI-4-SUB_READ_FAIL:  SIP0: vtyserverutild:
Confd subscription socket read failed Lost connection to ConfD (45):
EOF on socket to ConfD.
*Feb 26 05:58:47.667: %DMI-4-CONTROL_SOCKET_CLOSED:  SIP0: syncfd:
Confd control socket closed Lost connection to ConfD (45): EOF on socket to ConfD.
*Feb 26 05:59:43.269: %DMI-5-SYNC_START:  SIP0: syncfd:
External change to running configuration detected.
The running configuration will be synchronized to the NETCONF running data store.
*Feb 26 05:59:44.624: %DMI-5-SYNC_COMPLETE:  SIP0: syncfd:
The running configuration has been synchronized to the NETCONF running data store.
```

次に、インストールしたパッケージをコミットする例を示します。

```
Device# install commit

install_commit: START Sun Feb 26 06:46:48 UTC 2017
SUCCESS: install_commit  Sun Feb 26 06:46:52 UTC 2017
```

次に、ベース SMU パッケージにロールバックする例を示します。

```
Device# install rollback to base

install_rollback: START Sun Feb 26 06:50:29 UTC 2017
7 install_rollback: Restarting impacted processes to take effect
7 install_rollback: restarting confd

*Feb 26 06:50:34.957: %DMI-4-CONTROL_SOCKET_CLOSED:  SIP0: syncfd:
Confd control socket closed Lost connection to ConfD (45): EOF on socket to ConfD.
*Feb 26 06:50:34.962: %DMI-4-CONTROL_SOCKET_CLOSED:  SIP0: nesd:
Confd control socket closed Lost connection to ConfD (45): EOF on socket to ConfD.
*Feb 26 06:50:34.963: %DMI-4-SUB_READ_FAIL:  SIP0: vtyserverutild:
Confd subscription socket read failed Lost connection to ConfD (45):
EOF on socket to ConfD.Netconf processes stopped
7 install_rollback: DMP activate complete
SUCCESS: install_rollback  Sun Feb 26 06:50:41 UTC 2017
*Feb 26 06:51:28.901: %DMI-5-SYNC_START:  SIP0: syncfd:
External change to running configuration detected.
The running configuration will be synchronized to the NETCONF running data store.
*Feb 26 06:51:30.339: %DMI-5-SYNC_COMPLETE:  SIP0: syncfd:
```

```
The running configuration has been synchronized to the NETCONF running data store.
```

関連コマンド

コマンド	説明
show install	インストール パッケージに関する情報を表示します。

l2 traceroute

レイヤ 2 トレースルートサーバを有効にするには、グローバル コンフィギュレーション モードで **l2 traceroute** コマンドを使用します。レイヤ 2 トレースルートサーバを無効にするには、このコマンドの **no** 形式を使用します。

l2 traceroute
no l2 traceroute

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

グローバル コンフィギュレーション（config#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SE	このコマンドが追加されました。

使用上のガイドライン

レイヤ 2 トレースルートはデフォルトでは有効になっており、ユーザ データグラム プロトコル（UDP）ポート 2228 でリスニングソケットが開きます。UDP ポート 2228 を閉じてレイヤ 2 トレースルートを無効にするには、グローバル コンフィギュレーション モードで **no l2 traceroute** コマンドを使用します。

次に、**l2 traceroute** コマンドを使用してレイヤ 2 トレースルートを設定する例を示します。

```
Device# configure terminal
Device(config)# l2 traceroute
```

license boot level

デバイスで新しいソフトウェアライセンスを起動するには、グローバル コンフィギュレーション モードで **license boot level** コマンドを使用します。すべてのソフトウェアライセンスをデバイスから削除するには、このコマンドの **no** 形式を使用します。

license boot level *base-license-level* **addon** *addon-license-level*
no license boot level

構文の説明

base-license-level	スイッチの起動レベル。例： **ipservice** 使用可能な基本ライセンスは次のとおりです。 • LAN ベース • IP Base • IP サービス
addon-license-level	3年、5年、または7年の固定期間で登録できる追加ライセンス。 使用可能なアドオンライセンスは次のとおりです。 • Digital Networking Architecture（DNA）Essentials • DNA Advantage（DNA Essentials を含む）

コマンド デフォルト

設定されたイメージでスイッチが起動します。

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 Fuji 16.9.1	このコマンドが導入されました。

使用上のガイドライン

license boot level コマンドは次の目的に使用します。

- ライセンスのダウングレードとアップグレード
- 評価ライセンスと拡張ライセンスの有効化と無効化
- アップグレードライセンスのクリア

このコマンドは、特定のモジュールのライセンスインフラストラクチャで保持されているライセンス階層ではなく、設定されたライセンスレベルで起動するようにライセンスインフラストラクチャを設定します。

- スイッチをリロードすると、ライセンスインフラストラクチャでスタートアップコンフィギュレーションの設定にライセンスがあるかどうかが確認されます。設定にライセンスがある場合、そのライセンスでスイッチが起動します。ライセンスがない場合、ライセンスインフラストラクチャでイメージ階層に従ってライセンスが確認されます。
- 強制ブート評価ライセンスが期限切れの場合、ライセンスインフラストラクチャで通常の階層に従ってライセンスが確認されます。
- 設定されたブートライセンスがすでに期限切れになっている場合、ライセンスインフラストラクチャで階層に従ってライセンスが確認されます。

例

次に、スイッチの次回リロード時に *ipbase* ライセンスを有効化する例を示します。

```
デバイス(config)# license boot level ipbase
```

license smart conversion start

デバイスにインストールされている従来のライセンスを Cisco Smart Software Manager（CSSM）にすべて移行するには、特権 EXEC モードで **license smart conversion start** コマンドを使用します。

license smart conversion　start

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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

使用上のガイドライン

license smart conversion start コマンドを実行すると、デバイスの従来のライセンスが変換され、移行データが CSSM に送信されます。CSSM でライセンス資格が作成され、ユーザアカウントに付与されます。

（注）　ライセンスの変換が完了するまでには 1 時間以上かかります。

例

次に、ライセンスの変換を開始する方法を示します。

```
デバイス# license smart conversion start
```

関連コマンド

コマンド	説明
license smart conversion stop	ライセンスの変換をキャンセルします。
show license status	ライセンスのコンプライアンスステータスを表示します。
show license usage	ライセンス使用情報を表示します。

license smart conversion stop

ネットワーク障害が発生した場合にライセンスの変換をキャンセルするには、特権 EXEC モードで **license smart conversion stop** コマンドを使用します。

license smart conversion　stop

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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、ライセンスの変換を中止する例を示します。

```
デバイス# license smart conversion stop
Some Smart Licensing Conversion jobs stopped successfully.
```

関連コマンド

コマンド	説明
license smart conversion start	ライセンスの変換を開始します。
show license status	ライセンスのコンプライアンスステータスを表示します。
show license usage	ライセンス使用情報を表示します。

license smart deregister

Cisco Smart Software Manager（CSSM）への device の登録をキャンセルするには、特権 EXEC モードで **license smart deregister** コマンドを使用します。

license　smart　deregister

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

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

使用上のガイドライン

license smart deregister コマンドは次の目的に使用します。

- デバイスをインベントリから外すとき
- デバイスを再配置のために別の場所に出荷するとき

• デバイスを交換のために返品許可（RMA）プロセスを使用してシスコに返却するとき

例

次に、CSSM への device の登録を解除する例を示します。

```
デバイス# license smart deregister
*Jun 25 00:20:13.291 PDT: %SMART_LIC-6-AGENT_DEREG_SUCCESS: Smart Agent for Licensing
De-registration with the Cisco Smart Software Manager or satellite was successful
*Jun 25 00:20:13.291 PDT: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Jun 25 00:20:13.291 PDT: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled
features is Not Allowed for udi PID:ISR4461/K9,SN:FDO2213A0GL
```

関連コマンド

コマンド	説明
license smart register idtoken	CSSM に device を登録します。
show license all	権限付与情報を表示します。
show license status	ライセンスのコンプライアンスステータスを表示します。
show license summary	すべてのアクティブなライセンスの要約を表示します。
show license usage	ライセンス使用情報を表示します。

license smart register idtoken

Cisco Smart Software Manager（CSSM）からトークンが生成された device を登録するには、特権 EXEC モードで **license smart register idtoken** コマンドを使用します。

license smart register idtoken *token_ID* {**force**}

構文の説明

token_ID	CSSM からトークンが生成されたデバイス。
force	デバイスが登録されているかどうかに関わらずデバイスを強制的に登録します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、CSSM に device を登録する例を示します。

```
デバイス# license smart register idtoken
$Tl4UytrNXBzbEs1ck8veUtWaG5abnZJOFdDa1FwbVRa%0AblRMbz0%3D%0A
Registration process is in progress. Use the 'show license status' command to check the
 progress and result
Device#% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 0 seconds)
```

関連コマンド

コマンド	説明
license smart deregister	CSSM への device の登録をキャンセルします。
show license all	権限付与情報を表示します。
show license status	ライセンスのコンプライアンスステータスを表示します。
show license summary	すべてのアクティブなライセンスの要約を表示します。
show license usage	ライセンス使用情報を表示します。

license smart renew

Cisco Smart Software Manager（CSSM）で device の ID または承認を手動で更新するには、特権 EXEC モードで **license smart renew** コマンドを使用します。

license smart renew {**auth** | **id**}

構文の説明

auth	承認を更新します。
id	ID を更新します。

コマンド デフォルト

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

使用上のガイドライン

認証期間は、スマートライセンスシステムによって 30 日ごとに更新されます。ライセンスが「承認済み」または「コンプライアンス違反」の状態にある限り、認証期間が更新されます。猶予期間は、認証期間が過ぎると開始されます。猶予期間中、またはライセンスが「期限切

れ」状態になると、システムは引き続き認証期間の更新を試行します。再試行に成功すると、新しい認証期間が開始されます。

例

次に、device のライセンスを更新する例を示します。

```
デバイス# license smart renew auth
```

関連コマンド

コマンド	説明
show license all	権限付与情報を表示します。
show license status	ライセンスのコンプライアンスステータスを表示します。
show license usage	ライセンス使用情報を表示します。

location

エンドポイントのロケーション情報を設定するには、グローバル コンフィギュレーション モードで **location** コマンドを使用します。ロケーション情報を削除するには、このコマンドの **no** 形式を使用します。

location {**admin-tag** *string* | **civic-location identifier** {**host***id*} | **civic-location identifier** {**host***id*} | **elin-location** {*string* | **identifier** *id*} | **geo-location identifier** {**host***id*} | **prefer** {**cdp weight** *priority-value* | **lldp-med weight** *priority-value* | **static config weight** *priority-value*}
no location {**admin-tag** *string* | **civic-location identifier** {**host***id*} | **civic-location identifier** {**host***id*} | **elin-location** {*string* | **identifier** *id*} | **geo-location identifier** {**host***id*} | **prefer** {**cdp weight** *priority-value* | **lldp-med weight** *priority-value* | **static config weight** *priority-value*}

構文の説明

admin-tag*string*	管理タグまたはサイト情報を設定します。英数字形式のサイト情報またはロケーション情報。
civic-location	都市ロケーション情報を設定します。
identifier	都市ロケーション、緊急ロケーション、地理的な場所の名前を指定します。
host	ホストの都市ロケーションや地理空間的な場所を定義します。

id	都市ロケーション、緊急ロケーション、地理的な場所の名前。 （注） LLDP-MED スイッチ TLV での都市ロケーションの ID は 250 バイト以下に制限されます。スイッチ設定中に使用できるバッファ スペースに関するエラー メッセージを回避するには、各都市ロケーション ID に指定されたすべての都市ロケーション情報の全体の長さが 250 バイトを超えないようにします。
elin-location	緊急ロケーション情報 (ELIN) を設定します。
geo-location	地理空間的なロケーション情報を設定します。
prefer	ロケーション情報のソースのプライオリティを設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

location civic-location identifier グローバル コンフィギュレーション コマンドを入力後、都市ロケーション コンフィギュレーション モードが開始されます。**location geo-location identifier** グローバル コンフィギュレーション コマンドを入力後、ジオ ロケーション コンフィギュレーション モードが開始されます。

都市ロケーション ID は 250 バイトを超えてはなりません。

ホスト ID はホストの都市ロケーションや地理空間的な場所を設定します。ID がホストではない場合、ID はインターフェイスで参照できる地理空間的なテンプレートまたは都市ロケーションだけを定義します。

host キーワードは、デバイスの場所を定義します。**identifier** と **host** キーワードを使用して設定可能な都市ロケーションオプションは同じです。都市ロケーション コンフィギュレーション モードで次の都市ロケーション オプションを指定できます。

- **additional-code**：追加都市ロケーション コードを設定します。
- **additional-location-information**：追加都市ロケーション情報を設定します。
- **branch-road-name**：ブランチのロード名を設定します。
- **building**：建物の情報を設定します。
- **city**：都市名を設定します。
- **country**：2 文字の ISO 3166 の国コードを設定します。

- **county**：郡名を設定します。
- **default**：コマンドをデフォルト値に設定します。
- **division**：市の地区の名前を設定します。
- **exit**：都市ロケーション コンフィギュレーション モードを終了します。
- **floor**：階数を設定します。
- **landmark**：目印となる建物の情報を設定します。
- **leading-street-dir**：町名番地に付与される方角を設定します。
- **name**：居住者名を設定します。
- **neighborhood**：ネイバーフッド情報を設定します。
- **no**：指定された都市ロケーション データを拒否し、デフォルト値を設定します。
- **number**：町名番地を設定します。
- **post-office-box**：私書箱を設定します。
- **postal-code**：郵便番号を設定します。
- **postal-community-name**：郵便コミュニティ名を設定します。
- **primary-road-name**：主要道路の名前を設定します。
- **road-section**：道路の区間を設定します。
- **room**：部屋の情報を設定します。
- **seat**：座席の情報を設定します。
- **state**：州の名前を設定します。
- **street-group**：町名番地のグループを設定します。
- **street-name-postmodifier**：町名番地の名前のポストモディファイアを設定します。
- **street-name-premodifier**：町名番地の名前のプレモディファイアを設定します。
- **street-number-suffix**：町名番地の番号のサフィックスを設定します。
- **street-suffix**：町名番地のサフィックスを設定します。
- **sub-branch-road-name**：支線からさらに分岐した道路名を設定します。
- **trailing-street-suffix**：後に続く町名番地のサフィックスを設定します。
- **type-of-place**：場所のタイプを設定します。
- **unit**：単位を設定します。

地理的ロケーション コンフィギュレーション モードで次の地理空間的なロケーション情報を指定できます。

- **altitude**：高さの情報を階数、メートル、またはフィート単位で設定します。
- **latitude**：度、分、秒の緯度情報を設定します。範囲は -90 ～ 90 度です。正の値は、赤道より北側の位置を示します。
- **longitude**：度、分、秒の経度の情報を設定します。範囲は -180 ～ 180 度です。正の値は、グリニッジ子午線の東側の位置を示します。
- **resolution**：緯度と経度の分解能を設定します。分解能値を指定しない場合、10 m のデフォルト値が緯度と経度の分解能パラメータに適用されます。緯度と経度の場合、分解能の単位はメートルで測定されます。分解能の値は小数単位でも指定できます。
- **default**：デフォルトの属性によって、地理的位置を設定します。
- **exit**：地理的ロケーション コンフィギュレーション モードを終了します。

• **no**：指定された地理的パラメータを拒否し、デフォルト値を設定します。

ロケーション TLV をディセーブルにするには、**no lldp med-tlv-select location information** インターフェイスコンフィギュレーションコマンドを使用します。デフォルトでは、ロケーション TLV はイネーブルに設定されています。

次の例では、スイッチに都市ロケーション情報を設定する方法を示します。

```
デバイス(config)# location civic-location identifier 1
デバイス(config-civic)# number 3550
デバイス(config-civic)# primary-road-name "Cisco Way"
デバイス(config-civic)# city "San Jose"
デバイス(config-civic)# state CA
デバイス(config-civic)# building 19
デバイス(config-civic)# room C6
デバイス(config-civic)# county "Santa Clara"
デバイス(config-civic)# country US
デバイス(config-civic)# end
```

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

次の例では、スイッチ上で緊急ロケーション情報を設定する方法を示します。

```
デバイス(config)# location elin-location 14085553881 identifier 1
```

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

次に、スイッチに、地理空間ロケーション情報を設定する例を示します。

```
デバイス(config)# location geo-location identifier host
デバイス(config-geo)# latitude 12.34
デバイス(config-geo)# longitude 37.23
デバイス(config-geo)# altitude 5 floor
デバイス(config-geo)# resolution 12.34
```

設定された地理空間的な場所の詳細を表示するには、**show location geo-location identifier** コマンドを使用します。

location plm calibrating

調整クライアントのパス損失測定（CCX S60）要求を設定するには、グローバル コンフィギュレーション モードで **location plm calibrating** コマンドを使用します。

location plm calibrating {**multiband** | **uniband**}

構文の説明

multiband	関連付けられた 802.11a または 802.11b/g 無線での調整クライアントのパス損失測定要求を指定します。

uniband	関連付けられた 802.11a/b/g 無線での調整クライアントのパス損失測定要求を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

単一の無線クライアントには、（無線がデュアルバンドで、2.4 GHz と 5 GHz の両方の帯域でも動作できるとしても）uniband が役立ちます。複数の無線クライアントには、multiband が役立ちます。

次に、関連付けられた 802.11a/b/g 無線での調整クライアントのパス損失測定要求を設定する例を示します。

```
デバイス# configure terminal
デバイス(config)# location plm calibrating uniband
デバイス(config)# end
```

mac address-table move update

MAC アドレステーブル移行更新機能を有効にするには、スイッチスタックまたはスタンドアロンスイッチのグローバル コンフィギュレーション モードで **mac address-table move update** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac address-table move update {**receive** | **transmit**}
no mac address-table move update {**receive** | **transmit**}

構文の説明

receive	スイッチが MAC アドレス テーブル移行更新メッセージを処理するように指定します。
transmit	プライマリ リンクがダウンし、スタンバイ リンクが起動した場合、スイッチが MACアドレステーブル移行更新メッセージをネットワークの他のスイッチに送信するように指定します。

コマンド デフォルト

デフォルトでは、MAC アドレステーブル移行更新機能はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

コマンド履歴

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

使用上のガイドライン

MAC アドレステーブル移行更新機能により、プライマリ（フォワーディング）リンクがダウンし、スタンバイ リンクがトラフィックのフォワーディングを開始した場合、スイッチは高速双方向コンバージェンスを提供できます。

プライマリ リンクがダウンし、スタンバイ リンクが起動した場合、アクセス スイッチがMAC アドレステーブル移行更新メッセージを送信するように設定できます。アップリンク スイッチが、MAC アドレステーブル移行更新メッセージを受信および処理するように設定できます。

例

次の例では、アクセス スイッチが MAC アドレス テーブル移行更新メッセージを送信するように設定する方法を示します。

```
デバイス# configure terminal
デバイス(config)# mac address-table move update transmit
デバイス(config)# end
```

次の例では、アップリンク スイッチが MAC アドレス テーブル移行更新メッセージを取得および処理するように設定する方法を示します。

```
デバイス# configure terminal
デバイス(config)# mac address-table move update receive
デバイス(config)# end
```

設定を確認するには、**show mac address-table move update** 特権 EXEC コマンドを入力します。

mgmt_init

イーサネット管理ポートを初期化するには、ブートローダモードで **mgmt_init** コマンドを使用します。

mgmt_init

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

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

使用上のガイドライン イーサネット管理ポートのデバッグ中にのみ、**mgmt_init** コマンドを使用します。

例

次の例では、イーサネット管理ポートを初期化する方法を示します。

```
デバイス: mgmt_init
```

mkdir

指定されたファイルシステムに1つ以上のディレクトリを作成するには、ブートローダモードで **mkdir** コマンドを使用します。

mkdir *filesystem:/directory-url...*

構文の説明

filesystem:	ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。
/directory-url...	作成するディレクトリの名前です。ディレクトリ名はスペースで区切ります。

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード ブートローダ

コマンド履歴

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

使用上のガイドライン ディレクトリ名では、大文字と小文字が区別されます。

スラッシュ（/）間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

例

次の例では、ディレクトリ Saved_Configs を作成する方法を示します。

```
デバイス: mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```

more

1 つ以上のファイルの内容を表示するには、ブートローダモードで **more** コマンドを使用します。

more *filesystem:/file-url...*

構文の説明

filesystem:	ファイルシステムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。
/file-url...	表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

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

使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

ファイルのリストを指定した場合は、各ファイルの内容が順に表示されます。

例

次に、ファイルの内容を表示する例を示します。

```
デバイス: more flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

no debug all

スイッチのデバッグを無効にするには、特権 EXEC モードで **no debug all** コマンドを使用します。

no debug all

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード 特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 16.1	このコマンドが導入されました。

例

次に、スイッチでデバッグを無効にする例を示します。

```
デバイス: no debug all
All possible debugging has been turned off.
```

rename

ファイルの名前を変更するには、ブート コンフィギュレーション モードで **rename** コマンドを使用します。

rename *filesystem:/source-file-url filesystem:/destination-file-url*

構文の説明

filesystem:	ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。
/source-file-url	元のパス（ディレクトリ）およびファイル名です。
/destination-file-url	新しいパス（ディレクトリ）およびファイル名です。

コマンド デフォルト デフォルトの動作や値はありません。

コマンド モード ブートローダ

コマンド履歴

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

使用上のガイドライン ファイル名およびディレクトリ名は、大文字と小文字を区別します。

スラッシュ（/）間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

指定できるファイル名は最大127文字です。ファイル名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

例

次の例では、ファイル *config.text* の名前を *config1.text* に変更します。

```
デバイス: rename usbflash0:config.text usbflash0:config1.text
```

ファイルの名前が変更されたかどうかを確認するには、**dir** *filesystem:* ブートローダコマンドを入力します。

request consent-token accept-response shell-access

以前に生成されたチャレンジに対する同意トークン応答を送信するには、**request consent-token accept-response shell-access** コマンドを使用します。

request consent-token accept-response shell-access *response-string*

構文の説明

構文	説明
response-string	応答を表す文字列を指定します。

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 16.11.1	このコマンドが導入されました。

使用上のガイドライン

応答文字列は、チャレンジの生成から30分以内に入力する必要があります。入力しないとチャレンジが期限切れになり、新しいチャレンジの要求が必要になります。

例

次に、**request consent-token accept-response shell-access** *response-string* コマンドの出力例を示します。

```
Device# request consent-token accept-response shell-access
[redacted]
% Consent token authorization success
*Jan 18 02:51:37.807: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (authentication success:
 Shell access 0).
```

request consent-token generate-challenge shell-access

システムシェルアクセスに対する同意トークンチャレンジを生成するには、**request consent-token generate-challenge shell-access** コマンドを使用します。

request consent-token generate-challenge shell-access auth-timeout *time-validity-slot*

構文の説明

構文	説明
auth-timeout *time-validity-slot*	シェルアクセスを要求するタイムスロット（分）を指定します。

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 16.11.1	このコマンドが導入されました。

使用上のガイドライン

システムシェルに対する要求したタイムスロットが期限切れになると、セッションは自動的に終了します。

システムシェルアクセスの最大承認タイムアウトは 7 日間です。

例

次に、**request consent-token generate-challenge shell-access auth-timeout** *time-validity-slot* コマンドの出力例を示します。

```
Device# request consent-token generate-challenge shell-access auth-timeout 900
zSSdrAAAAQEBAQAAAABAgAEAAAAAAMACH86csUhmD10BAAQ0FvdJ7CxqRYUeoD7B4AwW7QUABAAAG8GAAhDVEFfREVNTwAGENUQ9ERU1PX0NUQ9ISUdOSU5HX0tFWQgAC0M5ODAwLUNMUs5CQALOVpQUEVSE5KRkI=
Device#
*Jan 18 02:47:06.733: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (challenge generation
 attempt: Shell access 0).
```

request consent-token terminate-auth

システムシェルに対する同意トークンベースの承認を終了するには、**request consent-token terminate-auth** コマンドを使用します。

request consent-token terminate-auth

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 16.11.1	このコマンドが導入されました。

使用上のガイドライン

システムシェルアクセスのシナリオでは、シェルを終了しても、承認タイムアウトが発生するまで承認は終了しません。

システムシェルアクセスの目的を達成したら、**request consent-token terminate-auth** コマンドを明示的に発行することによって、システムシェルの承認を強制終了することを推奨します。

request consent-token terminate-auth コマンドを使用して現在の認証を終了した場合、ユーザがシステムシェルにアクセスする際に再度認証プロセスが必要になります。

例

次に、**request consent-token terminate-auth** コマンドの出力例を示します。

```
Device# request consent-token terminate-auth shell-access
% Consent token authorization termination success

Device#
*Mar 13 01:45:39.197: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (terminate
authentication: Shell access 0).
Device#
```

request platform software console attach switch

メンバスイッチでセッションを開始するには、特権 EXEC モードで **request platform software console attach switch** コマンドを使用します。

（注） スタッキングスイッチ（Catalyst 3650/3850/9200/9300 スイッチ）では、このコマンドはスタンバイコンソールでセッションを開始する場合にのみ使用できます。Catalyst 9500 スイッチでは、このコマンドは Stackwise Virtual セットアップでのみサポートされます。メンバスイッチでセッションを開始することはできません。デフォルトでは、すべてのコンソールはすでにアクティブであるため、アクティブなコンソールでセッションを開始する要求はエラーになります。

request platform software console attach switch { *switch-number* **| active | standby } { 0/0 | R0 }**

構文の説明

switch-number	スイッチ番号を指定します。指定できる範囲は 1 ～ 9 です。
active	アクティブスイッチを指定します。 （注） この引数は、Catalyst 9500 スイッチではサポートされていません。
standby	スタンバイスイッチを指定します。
0/0	SPA-Inter-Processor スロットが 0 で、ベイが 0 であることを指定します。 （注） このオプションをスタッキングスイッチとともに使用しないでください。それはエラーになります。
R0	ルート プロセッサ スロットが 0 であることを指定します。

コマンド デフォルト

デフォルトでは、スタック内のすべてのスイッチはアクティブです。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

スタンバイスイッチでセッションを開始するには、最初に設定で有効にする必要があります。

例

次に、スタンバイスイッチとのセッションを行う例を示します。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device(config-r-mc)# end
Device# request platform software console attach switch standby R0
#
# Connecting to the IOS console on the route-processor in slot 0.
# Enter Control-C to exit.
#
Device-stby> enable
Device-stby#
```

request platform software package clean

不要なメディアファイルを削除するには、特権 EXEC モードで **request platform software package clean** コマンドを使用します。

request platform software package clean [{file *URL*| pattern *URL*| switch *switch-ID* {file *URL*| pattern *URL*}}]

構文の説明

file *URL*	（任意）ファイルの URL を指定します。URL には、ファイルシステム、ディレクトリ、およびファイル名を含めます。
pattern *URL*	（任意）内容を消去する 1 つ以上のパスに一致するパターンを指定します。

switch *switch-ID*	（任意）プロビジョニングするスイッチを指定します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

例

次に、使用していないメディアファイルをデバイスから消去する例を示します。

```
Device# request platform software package clean

This operation may take several minutes...
Running command on switch 1
Cleaning up unnecessary package files
No path specified, will use booted path consolidated:packages.conf
Cleaning sw/isos
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat3k_caa-guestshell.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
    cat3k_caa-rpbase.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
    cat3k_caa-rpcore.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
    packages.conf
      File is in use, will not delete.
  done.

SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
```

関連コマンド

コマンド	説明
request platform software package install file	統合パッケージまたはサブパッケージをアップグレードします。
request platform software package install rollback	以前のソフトウェアアップグレードをロールバックします。

request platform software package copy

Cisco IOS XE イメージファイルをコピーするには、特権 EXEC モードで **request platform software package copy** コマンドを使用します。

request platform software package copy switch *switch-ID* **file** *file-URL* **to** *file-URL*

構文の説明

switch *switch-ID*	プロビジョニングするスイッチを指定します。
file *file-URL*	統合パッケージまたはサブパッケージの URL。
to	ファイルをコピーする展開先URLを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

例

次に、イメージファイルを展開先ディレクトリにコピーする例を示します。

```
Device# request platform software package copy switch all file
tftp://10.10.11.250/cat3k_caa-universalk9.16.08.05.SPA.bin to
ftp:cat3k_caa-universalk9.16.08.05.SPA.bin
```

コマンド	説明
request platform software package install file	統合パッケージまたはサブパッケージをアップグレードします。
request platform software package install rollback	以前のソフトウェアアップグレードをロールバックします。

request platform software package describe file

個々のモジュールまたは Cisco IOS-XE イメージファイルに関する説明情報を収集するには、特権 EXEC モードまたは診断モードで **request platform software package describe file** コマンドを使用します。

request platform software package describe file *URL* [**detail**] [**verbose**]

構文の説明

URL	ファイルの URL を指定します。*URL*には、ファイルシステム、ディレクトリ、およびファイル名を含めます。
detail	（任意）詳細出力を指定します。
verbose	（任意）詳細情報を表示します。ファイルに関するすべての情報がコンソールに表示されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、個々のモジュールおよび Cisco IOS-XE イメージファイルの情報を収集するためにのみ使用できます。このコマンドを使用して他のファイルの情報を収集しても出力は生成されますが、役に立つ情報は出力されません。

このコマンドの出力は、次の目的に使用できます。

- Cisco IOS-XE イメージに含まれる個々のモジュールファイルを確認する。
- ファイルがブート可能かどうかを確認する。
- ファイルをリロードまたは起動する必要があるコンテキストを確認する。
- ファイルが破損していないかどうかを確認する。
- ファイルとヘッダーのサイズ、ビルド日付、およびその他の一般的な情報を確認する。

例

次の例では、このコマンドを入力して、bootflash: ファイルシステムにある個々の SIP ベースモジュールファイルに関する情報を収集しています。

```
Device# request platform software package describe file
bootflash:cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin

Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
  Size: 36954316
  Timestamp: 2018-11-07 15:36:27 UTC
  Canonical path: /bootflash/cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin

  Raw disk-file SHA1sum:
    3ee37cdbe276316968866b16df7d8a5733a1502e

  Computed SHA1sum:
    f2db80416a1245a5b1abf2988088860b38ce7898
  Contained SHA1sum:
    f2db80416a1245a5b1abf2988088860b38ce7898
```

```
  Hashes match. Package is valid.

  Header size:     204 bytes
  Package type:    10000
  Package flags:   0
  Header version:  0

  Internal package information:
    Name: cc
    BuildTime: 2018-11-07_05.24
    ReleaseDate: Wed 07-Nov-18 01:00
    RouteProcessor: rp1
    Platform: Cat3XXX
    User: mcpre
    PackageName: ipbasek9
    Build: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin


  Package is bootable on SIP when specified
  by packages provisioning file.
```

次の例では、このコマンドを使用して、bootflash: ファイルシステムにある Cisco IOS-XE イメージに関する情報を収集しています。

```
Device# request platform software package describe file
bootflash:cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin

Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
  Size: 218783948
  Timestamp: 2018-11-07 17:14:09 UTC
  Canonical path: /bootflash/cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin

  Raw disk-file SHA1sum:
    d2999fc7e27e01344903a42ffacd62c156eba4cc

  Computed SHA1sum:
    5f8cda8518d01d8282d80ecd34f7715783f4a813
  Contained SHA1sum:
    5f8cda8518d01d8282d80ecd34f7715783f4a813
  Hashes match. Package is valid.

  Header size:     204 bytes
  Package type:    30000
  Package flags:   0
  Header version:  0

  Internal package information:
    Name: rp_super
    BuildTime: 2018-11-07_05.24
    ReleaseDate: Wed 07-Nov-18 01:00
    RouteProcessor: rp1
    Platform: Cat3XXX
    User: mcpre
    PackageName: ipbasek9
    Build: cat3k_caa-universalk9_universalk9.16.09.02


  Package is bootable from media and tftp.
  Package contents:

  Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
    Size: 52072652
    Timestamp: 2018-11-07 13:33:13 UTC
```

```
  Raw disk-file SHA1sum:
    f1aad6d687256aa327a4efa84deab949fbed12b8

  Computed SHA1sum:
    15502fd1b8f9ffd4af4014ad4d8026c837929fe6
  Contained SHA1sum:
    15502fd1b8f9ffd4af4014ad4d8026c837929fe6
  Hashes match. Package is valid.

  Header size:     204 bytes
  Package type:    20000
  Package flags:   0
  Header version:  0

  Internal package information:
    Name: fp
    BuildTime: 2018-11-07_05.24
    ReleaseDate: Wed 07-Nov-18 01:00
    RouteProcessor: rp1
    Platform: Cat3XXX
    User: mcpre
    PackageName: ipbasek9
    Build: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin


  Package is bootable on ESP when specified
  by packages provisioning file.

Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
  Size: 21844172
  Timestamp: 2018-11-07 13:33:01 UTC

  Raw disk-file SHA1sum:
    025e6159dd91cef9d254ca9fff2602d8ce065939

  Computed SHA1sum:
    ea1b358324ba5815b9ea623b453a98800eae1c78
  Contained SHA1sum:
    ea1b358324ba5815b9ea623b453a98800eae1c78
  Hashes match. Package is valid.

  Header size:     204 bytes
  Package type:    30004
  Package flags:   0
  Header version:  0

  Internal package information:
    Name: ipbasek9
    BuildTime: 2018-11-07_05.24
    ReleaseDate: Wed 07-Nov-07 01:00
    RouteProcessor: rp1
    Platform: Cat3XXXX
    User: mcpre
    PackageName: ipbasek9
    Build: 16.9.20180925:160127


  Package is not bootable.

Package: cat3k_caa-universalk9.16.09.02.SPA.bin
  Size: 21520588
  Timestamp: 2007-12-04 13:33:06 UTC
```

```
  Raw disk-file SHA1sum:
    432dfa61736d8a51baefbb2d70199d712618dcd2

  Computed SHA1sum:
    83c0335a3adcea574bff237a6c8640a110a045d4
  Contained SHA1sum:
    83c0335a3adcea574bff237a6c8640a110a045d4
  Hashes match. Package is valid.

  Header size:     204 bytes
  Package type:    30001
  Package flags:   0
  Header version:  0

  Internal package information:
    Name: rp_base
    BuildTime: 2007-12-04_05.24
    ReleaseDate: Tue 04-Dec-07 01:00
    RouteProcessor: rp1
    Platform: Cat3XXX
    User: mcpre
    PackageName: ipbasek9
    Build: v_16.9.20180925:160127


  Package is bootable on RP when specified
  by packages provisioning file.

Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
  Size: 24965324
  Timestamp: 2018-11-07 13:33:08 UTC

  Raw disk-file SHA1sum:
    eb964b33d4959c21b605d0989e7151cd73488a8f

  Computed SHA1sum:
    19b58886f97c79f885ab76c1695d1a6f4348674e
  Contained SHA1sum:
    19b58886f97c79f885ab76c1695d1a6f4348674e
  Hashes match. Package is valid.

  Header size:     204 bytes
  Package type:    30002
  Package flags:   0
  Header version:  0

  Internal package information:
    Name: rp_daemons
    BuildTime: 2018-11-07_05.24
    ReleaseDate: Wed 07-Nov-07 01:00
    RouteProcessor: rp1
    Platform: Cat3XXX
    User: mcpre
    PackageName: ipbasek9
    Build: v_16.9.20180925:160127


  Package is not bootable.

Package: cat3k_caa-universalk9.16.09.02.SPA.bin
  Size: 48515276
  Timestamp: 2007-12-04 13:33:13 UTC

  Raw disk-file SHA1sum:
```

```
    bc13462d6a4af7a817a7346a44a0ef7270e3a81b

  Computed SHA1sum:
    f1235d703cc422e53bce850c032ff3363b587d70
  Contained SHA1sum:
    f1235d703cc422e53bce850c032ff3363b587d70
  Hashes match. Package is valid.

  Header size:     204 bytes
  Package type:    30003
  Package flags:   0
  Header version:  0

  Internal package information:
    Name: rp_iosd
    BuildTime: 2007-12-04_05.24
    ReleaseDate: Tue 04-Dec-07 01:00
    RouteProcessor: rp1
    Platform: Cat3XXX
    User: mcpre
    PackageName: ipbasek9
    Build: v_16.9.20180925:160127


  Package is not bootable.

Package: cat3k_caa-universalk9.16.09.02.SPA.bin
  Size: 36954316
  Timestamp: 2007-12-04 13:33:11 UTC

  Raw disk-file SHA1sum:
    3ee37cdbe276316968866b16df7d8a5733a1502e

  Computed SHA1sum:
    f2db80416a1245a5b1abf2988088860b38ce7898
  Contained SHA1sum:
    f2db80416a1245a5b1abf2988088860b38ce7898
  Hashes match. Package is valid.

  Header size:     204 bytes
  Package type:    10000
  Package flags:   0
  Header version:  0

  Internal package information:
    Name: cc
    BuildTime: 2007-12-04_05.24
    ReleaseDate: Tue 04-Dec-07 01:00
    RouteProcessor: rp1
    Platform: Cat3XXX
    User: mcpre
    PackageName: ipbasek9
    Build: v_16.9.20180925:160127


  Package is bootable on SIP when specified
  by packages provisioning file.

Package: cat3k_caa-universalk9.16.09.02.SPA.bin
  Size: 19933388
  Timestamp: 2007-12-04 13:33:06 UTC

  Raw disk-file SHA1sum:
    44b6d15cba31fb0e9b27464665ee8a24b92adfd2
```

```
Computed SHA1sum:
  b1d5faf093b183e196c7c8e1023fe1f7aafdd36d
Contained SHA1sum:
  b1d5faf093b183e196c7c8e1023fe1f7aafdd36d
Hashes match. Package is valid.

Header size:     204 bytes
Package type:    10001
Package flags:   0
Header version:  0

Internal package information:
  Name: cc_spa
  BuildTime: 2007-12-04_05.24
  ReleaseDate: Tue 04-Dec-07 01:00
  RouteProcessor: rp1
  Platform: Cat3XXX
  User: mcpre
  PackageName: ipbasek9
  Build: v_16.9.20180925:160127


Package is not bootable.
```

関連コマンド

コマンド	説明
request platform software package install file	個々のパッケージまたはスーパーパッケージファイルをアップグレードします。

request platform software package expand

Cisco IOS-XE イメージから個々のモジュールを展開するには、特権 EXEC モードで **request platform software package expand** コマンドを使用します。

request platform software package expand {**file** *source-url* | **switch** *switch-ID* **file** *source-URL*}[**to** *destination-URL*] [**auto-copy**] [**force**] [**overwrite**] [**retain-source-file**] [**verbose**] [**wipe**]

構文の説明

source-URL	内容を展開する Cisco IOS-XE ファイルの URL を指定します。
switch *switch-ID*	スイッチ ID を指定します。
to *destination-URL*	（任意）Cisco IOS-XE ファイルから展開したファイルを操作の完了後に格納する展開先 URL を指定します。 このオプションが入力されていない場合、Cisco IOS-XE イメージファイルが現在格納されているディレクトリと同じディレクトリに Cisco IOS-XE イメージファイルの内容が展開されます。
auto-copy	（任意）プロビジョニング ディレクトリにパッケージをコピーします。

force	（任意）強制的に操作を実行し、警告メッセージに関係なくアップグレードを続行するように指定します。
over-write	（任意）同一でないパッケージと未使用のプロビジョニングファイルを上書きします。
retain-to-source	（任意）展開後にソースファイルを保持します。
verbose	（任意）詳細情報を表示します。プロセス中にコンソールに表示できるすべての出力が表示されます。
wipe	（任意）ファイルを展開してスナップショットディレクトリに格納する前に、展開先スナップショット ディレクトリの内容をすべて消去します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドで実行されるのは、Cisco IOS-XE イメージからの個々のモジュールファイルとプロビジョニングファイルの展開だけです。これらのプロビジョニングファイルや個々のモジュールをルータの起動と実行に使用するには、追加の設定が必要です。

このコマンドを使用すると、Cisco IOS-XE イメージ内の各モジュールとプロビジョニングファイルがコピーされ、それらのコピーが展開先ディレクトリに格納されます。操作の完了後に Cisco IOS-XE イメージファイルが変更されることはありません。

to オプションが入力されていない場合、Cisco IOS-XE イメージが現在格納されているディレクトリと同じディレクトリに Cisco IOS-XE イメージの内容が展開されます。

このコマンドを使用して個々のモジュールファイルを展開する際、ディレクトリにすでに個々のモジュールファイルが格納されていると、展開先デバイスにディレクトリが自動的に作成されてファイルが展開されます。

例

次に、個々のモジュールおよびプロビジョニングファイルがすでに格納されているディレクトリを展開先に指定して、Cisco IOS-XE イメージから個々のモジュールおよびプロビジョニングファイルを展開する例を示します。

ファイルが展開されたことを確認できるように、展開前と展開後のディレクトリの出力を示してあります。

```
Device# dir bootflash:

Directory of bootflash:/
   11  drwx       16384   Dec 4 2018 11:26:07 +00:00  lost+found
14401  drwx        4096   Dec 4 2018 11:27:41 +00:00  .installer
```

```
   12  -rw-   218783948   Dec 4 2018 12:12:16 +00:00 cat3k_caa-universalk9.16.09.02.SPA.bin

Device# request platform software package expand file
bootflash:cat3k_caa-universalk9.16.09.02.SPA.bin

Verifying parameters
Validating package type
Copying package files

Device# dir bootflash:

Directory of bootflash:/
   11  drwx       16384   Dec 4 2018 11:26:07 +00:00  lost+found
14401  drwx        4096   Dec 4 2018 11:27:41 +00:00  .installer
   12  -rw-   218783948   Dec 4 2018 12:12:16 +00:00
cat3k_caa-universalk9.16.09.02.SPA.bin
28802  -rw-        7145   Dec 4 2018 12:14:22 +00:00  packages.conf
928833536 bytes total (483700736 bytes free)
```

関連コマンド

コマンド	説明
request platform software package install file	個々のモジュールまたは Cisco IOS-XE ファイルをアップグレードします。

request platform software package install auto-upgrade

互換性のないすべてのスイッチでソフトウェアの自動アップグレードを開始するには、特権 EXEC モードで **request platform software package install auto-upgrade** コマンドを使用します。

request platform software package install auto-upgrade

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

例

次に、ソフトウェアを自動的にアップグレードする例を示します。

```
Device# request platform software package install auto-upgrade
```

関連コマンド

コマンド	説明
request platform software package install file	統合パッケージまたはサブパッケージをアップグレードします。
request platform software package install rollback	以前のソフトウェアアップグレードをロールバックします。

request platform software package install commit

ロールバックタイマーをキャンセルしてソフトウェアアップグレードをコミットするには、特権 EXEC モードで **request platform software package install commit** コマンドを使用します。

request platform software package install switch *switch-ID***commit** [**verbose**]

構文の説明

switch *switch-ID*	スイッチ ID を指定します。
verbose	（任意）詳細情報を表示します。プロセス中にコンソールに表示できるすべての情報が表示されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC（#）

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、 **request platform software package install switch** *switch-ID* **file auto-rollback** コマンドを使用して個別のサブパッケージまたは統合パッケージのアップグレードを開始した後に入力します。**auto-rollback** *minutes* オプションが使用されている場合、 **request platform software package install switch** *switch-ID* **commit** コマンドを入力してアップグレードをコミットしないと、*minutes* で指定した時間が経過した時点でアップグレードをキャンセルするロールバックタイマーによってアップグレードがキャンセルされます。

ロールバックタイマーが切れると、アップグレードは完了せず、デバイスでは以前のサブパッケージまたは統合パッケージが引き続き実行されます。

例

次に、アップグレードをコミットする例を示します。

```
Device# request platform software package install switch all commit
```

関連コマンド

コマンド	説明
request platform software package install file	統合パッケージまたはサブパッケージをアップグレードします。
request platform software package install rollback	以前のソフトウェアアップグレードをロールバックします。

request platform software package install file

統合パッケージまたは個々のサブパッケージをアップグレードするには、特権EXECモードで **request platform software package install file** コマンドを使用します。

request platform software package install switch *switch-ID* **file** *file-URL* [**auto-rollback** *minutes*] [**interface-module-delay** *seconds*] [**provisioning-file** *provisioning-file-URL*] [**slot** *slot-number*] [**bay** *bay-number*] [**auto-copy**] [**force**] [**ignore-compact-check**] [**mdr**] [**new**] [**on-reboot**] [**retain-source-file**] [**verbose**]

構文の説明

switch *switch-ID*	プロビジョニングするスイッチを指定します。
file-URL	統合パッケージまたはサブパッケージの URL。
auto-rollback *minutes*	（任意）ロールバックタイマーの設定を指定し、ロールバックタイマーが切れるまでの時間（分）を設定します。
interface-module-delay *seconds*	（任意）インターフェイスモジュールの再起動タイムアウト遅延を指定します。
provisioning-file *provisioning-file-URL*	（任意）プロビジョニングファイルの URL を指定します。プロビジョニングファイルは、個々のサブパッケージを使用してデバイスを起動する場合にのみ使用されます。
slot *slot-number*	（任意）共有ポート アダプタ インターフェイス プロセッサ（SIP）を取り付けることができるデバイスのスロット番号を指定します。
bay *bay-number*	（任意）SIP 内の共有ポートアダプタ（SPA）ベイ番号を指定します。
auto-copy	（任意）パッケージをプロビジョニング ディレクトリに自動的にコピーするように指定します。
force	（任意）強制的に操作を実行し、警告メッセージに関係なくアップグレードを続行するように指定します。
ignore-compact-check	（任意）互換性チェックを無視するように指定します。

mdr	（任意）Minimal Disruptive Restart を使用するように指定します。
new	（任意）新しいパッケージ プロビジョニング ファイルを作成します。
on-reboot	（任意）RP の次回の再起動時までインストールを完了しないように指定します。
retain-source-file	（任意）インストール後にソースファイルを保持します。
verbose	（任意）詳細情報を表示します。プロセス中にコンソールに表示できるすべての出力が表示されます。

コマンド デフォルト

request platform software package install file コマンドを入力しないと、デバイスで統合パッケージまたはサブパッケージのアップグレードは開始されません。

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 Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、統合パッケージおよび個別のサブパッケージをアップグレードする場合に使用します。

auto-rollback *minutes* オプションが使用されている場合、アップグレードを完了するには、ロールバックタイマーが切れる前に **request platform software package install switch** *switch-ID* **commit** コマンドを入力する必要があります。このコマンドが入力されていない場合、デバイスは以前のソフトウェアバージョンにロールバックします。ロールバックタイマーは *minutes* で指定された時間が経過すると切れます。**auto-rollback** *minutes* オプションが使用されていない場合は、アップグレードが自動的に行われます。

次の例では、**request platform software package install** コマンドを使用して統合パッケージをアップグレードしています。また、すべてのプロンプトを無視して（すでに同じ統合パッケージがインストールされている場合など）強制的にアップグレードを実行する **force** オプションを使用しています。

```
Device# request platform software package install rp 0 file
bootflash:cat3k_caa-universalk9.16.03.05.SPA.bin force

--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Verifying image file locations
Locating image files and validating name syntax
Inspecting image file types
Processing image file constraints
```

```
Extracting super package content
Verifying parameters
Validating package type
Copying package files
Checking and verifying packages contained in super package
Creating candidate provisioning file

  WARNING:
  WARNING: Candidate software will be installed upon reboot
  WARNING:

Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
Determining whether installation is valid
Determining whether installation is valid ... skipped
Checking IPC compatibility with running software
Checking IPC compatibility with running software ... skipped
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
Finished compatibility testing
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
SUCCESS: Software provisioned.  New software will load on reboot.

Device# reload
```

（注） この手順を終了するにはリロードを実行する必要があります。

関連コマンド

コマンド	説明
request platform software package install commit	ロールバックタイマーをキャンセルし、ソフトウェアアップグレードをコミットします。
request platform software package install rollback	以前のソフトウェアアップグレードをロールバックします。
request platform software package install snapshot	統合パッケージから抽出されたすべてのファイルを格納するスナップショット ディレクトリを作成します。

request platform software package install rollback

以前のソフトウェアアップグレードをロールバックするには、特権 EXEC モードで **request platform software package install rollback** コマンドを使用します。

request platform software package install switch *switch-ID* **rollback** [{**as-booted** | **provisioning-file** *provisioning-file-URL*}] [**auto-copy**] [**force**] [**ignore-compact-check**] [**new**] [**on-reboot**] [**retain-source-file**] [**verbose**]

構文の説明

switch *switch-ID*	プロビジョニングするスイッチを指定します。
as-booted	（任意）ソフトウェアアップデートは実行せず、前回の再起動時と同じ手順を使用してデバイスを起動するように指定します。
provisioning-file *provisioning-file-URL*	（任意）ソフトウェアアップデートは実行せず、指定したプロビジョニングファイルを使用してデバイスを起動するように指定します。
auto-copy	（任意）パッケージをプロビジョニング ディレクトリに自動的にコピーするように指定します。
force	（任意）強制的に操作を実行し、警告メッセージに関係なくアップグレードを続行するように指定します。
ignore-compact-check	（任意）互換性チェックを無視するように指定します。
new	（任意）新しいパッケージ プロビジョニング ファイルを作成します。
on-reboot	（任意）次回の再起動時までインストールを完了しないように指定します。
retain-source-file	（任意）インストール後にソースファイルを保持します。
verbose	（任意）詳細情報を表示します。プロセス中にコンソールに表示できるすべての出力が表示されます。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ロールバックタイマーがアクティブになっている設定をロールバックします。アクティブなロールバックタイマーは、**request platform software package install file** コマンドを使用したソフトウェアのアップグレード時に **auto-rollback** オプションが入力されている場合に使用されます。

例

次の例では、ロールバックタイマーを使用したアップグレードが以前の設定にロールバックされます。

```
Device# request platform software package install switch all rollback
```

関連コマンド

コマンド	説明
request platform software package install commit	ロールバックタイマーをキャンセルし、ソフトウェアアップグレードをコミットします。
request platform software package install file	統合パッケージまたは個々のサブパッケージをアップグレードします。

request platform software package install snapshot

統合パッケージから展開したすべてのファイルを格納するスナップショットディレクトリを作成するには、特権 EXEC モードで **request platform software package install snapshot** コマンドを使用します。

request platform software package install switch *switch-ID* **snapshot to** *URL* [**as** *snapshot-provisioning-filename*] [**force**] [**verbose**] [**wipe**]

構文の説明

switch *switch-ID*	プロビジョニングするスイッチを指定します。
snapshot to *URL*	ディレクトリを作成し、統合パッケージのすべてのファイルをそのディレクトリに展開します。ディレクトリの名前は、*URL_FS* の一部としてコマンドラインで指定します。 *URL_FS* がファイルシステムとして指定されている場合、統合パッケージ内のファイルはファイルシステム上のディレクトリではなくファイルシステム上に展開されます。
as *snapshot-provisioning-filename*	（任意）スナップショット ディレクトリ内のプロビジョニングファイルの名前を変更します。 このオプションを使用しない場合は、統合パッケージ内のプロビジョニングファイルの既存のプロビジョニングファイル名が使用されます。

wipe	（任意）ファイルを展開してスナップショット ディレクトリに格納する前に、展開先スナップショット ディレクトリの内容をすべて消去します。
force	（任意）強制的に操作を実行し、警告メッセージに関係なくアップグレードを続行するように指定します。
verbose	（任意）詳細情報を表示します。プロビジョニングプロセス中にすべての出力がコンソールに表示されます。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、展開先デバイスにディレクトリを作成し、そのディレクトリに統合パッケージ内の個々のサブパッケージを展開するために使用します。

これ以外に統合パッケージから個々のサブパッケージを展開するために使用できるコマンドは **request platform software package expand** コマンドだけです。

例

次の例では、snapdir1_snap という名前のスナップショット ディレクトリが bootflash: ファイルシステムに作成され、そのスナップショットディレクトリに統合パッケージの個々のサブパッケージファイルが展開されます。

例の 2 番目の部分では、最初に、スナップショット ディレクトリ内のファイルを使用して再起動するようにルータを設定しています（以前のすべての boot system コマンドを削除し、コンフィギュレーション レジスタを設定してから、展開したプロビジョニングファイルを使用してブートするために boot system コマンドを入力）。その後、新しい設定を保存してから、展開したプロビジョニングファイルを使用して起動するためにデバイスを再起動しています。これにより、展開した個々のサブパッケージファイルを使用してルータを実行できます。

```
Device# request platform software package install switch all snapshot to
bootflash:snapdir1_snap

--- Starting active image file snapshot --- Validating snapshot parameters Creating
destination directory
Copying files to destination media
   Copied provisioning file as packages.conf
Moving files into final location Finished active image file snapshot
Device(config)# no boot system
Device(config)# config-register 0x1
Device(config)# boot system harddisk:snapdir1_snap/packages.conf
Device(config)# exit
*May 11 01:31:04.815: %SYS-5-CONFIG_I: Configured from console by con
Device# write memory
```

```
Building configuration...
[OK]

Device# reload
```

関連コマンド

コマンド	説明
request platform software package install file	統合パッケージまたは個々のサブパッケージをアップグレードします。

request platform software package verify

In-Service Software Upgrade（ISSU）ソフトウェアパッケージの互換性を確認するには、特権 EXEC モードで **requestplatform software package verify** コマンドを使用します。

request platform software package verify switch *switch-ID* **file** *file-URL* [**bay** *bay-number*] [**slot** *slot-number*] [**auto-copy**] [**force**] [**mdr**]

構文の説明

switch *switch-ID*	プロビジョニングするスイッチを指定します。
file-URL	統合パッケージまたはサブパッケージの URL。
bay *bay-number*	（任意）SIP 内の共有ポートアダプタ（SPA）ベイ番号を指定します。
slot *slot-number*	（任意）共有ポート アダプタ インターフェイス プロセッサ（SIP）を取り付けることができるデバイスのスロット番号を指定します。
auto-copy	（任意）パッケージをプロビジョニング ディレクトリに自動的にコピーするように指定します。
force	（任意）強制的に操作を実行し、警告メッセージに関係なくアップグレードを続行するように指定します。
mdr	（任意）Minimal Disruptive Restart を使用するように指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

例

次に、Cisco IOS XE イメージを確認する例を示します。

```
Device# request platform software package verify switch all file
bootflash:cat3k_caa-universalk9.16.03.05.SPA.bin
```

関連コマンド

コマンド	説明
request platform software package install commit	ロールバックタイマーをキャンセルし、ソフトウェアアップグレードをコミットします。
request platform software package install rollback	以前のソフトウェアアップグレードをロールバックします。
request platform software package install snapshot	統合パッケージから抽出されたすべてのファイルを格納するスナップショット ディレクトリを作成します。

request platform software package uninstall

ソフトウェアパッケージをアンインストールするには、特権 EXEC モードで **request platform software package uninstall** コマンドを使用します。

request platform software package uninstall switch *switch-ID* **file** *file-URL* [**bay** *bay-number*] [**slot** *slot-number*] [**auto-copy**] [**force**] [**mdr**]

構文の説明

switch *switch-ID*	プロビジョニングするスイッチを指定します。
file-URL	統合パッケージまたはサブパッケージの URL。
bay *bay-number*	（任意）SIP 内の共有ポートアダプタ（SPA）ベイ番号を指定します。
slot *slot-number*	（任意）共有ポート アダプタ インターフェイス プロセッサ（SIP）を取り付けることができるデバイスのスロット番号を指定します。
auto-copy	（任意）パッケージをプロビジョニング ディレクトリに自動的にコピーするように指定します。
force	（任意）強制的に操作を実行し、警告メッセージに関係なくアップグレードを続行するように指定します。
mdr	（任意）Minimal Disruptive Restart を使用するように指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

例

次に、ソフトウェアパッケージをアンインストールする例を示します。

```
Device# request platform software package uninstall
```

関連コマンド

コマンド	説明
request platform software package install commit	ロールバックタイマーをキャンセルし、ソフトウェアアップグレードをコミットします。
request platform software package install rollback	以前のソフトウェアアップグレードをロールバックします。
request platform software package install snapshot	統合パッケージから抽出されたすべてのファイルを格納するスナップショット ディレクトリを作成します。

reset

システムでハードリセットを実行するには、ブートローダモードで **reset** コマンドを実行します。ハードリセットを行うと、deviceの電源切断後に電源を投入する手順と同様に、プロセッサ、レジスタ、およびメモリの内容が消去されます。

reset

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

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

例

次の例では、システムをリセットする方法を示します。

```
デバイス: reset
Are you sure you want to reset the system (y/n)? y
System resetting...
```

rmdir

指定されたファイルシステムから1つ以上の空のディレクトリを削除するには、ブートローダモードで **rmdir** コマンドを使用します。

rmdir *filesystem:/directory-url...*

構文の説明

filesystem:	ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。
/directory-url...	削除する空のディレクトリのパス（ディレクトリ）および名前です。ディレクトリ名はスペースで区切ります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴

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

使用上のガイドライン

スラッシュ（/）間に指定できるディレクトリ名は最大 45 文字で、大文字と小文字の区別があります。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、およびコロンは使用できません。

ディレクトリを削除する前に、まずディレクトリ内のファイルをすべて削除する必要があります。

device は、各ディレクトリを削除する前に、確認を求めるプロンプトを出します。

例

次の例では、ディレクトリを 1 つ削除する方法を示します。

```
デバイス: rmdir usbflash0:Test
```

ディレクトリが削除されたかどうかを確認するには、**dir** *filesystem:* ブートローダコマンドを入力します。

sdm prefer

スイッチで使用するSDMテンプレートを指定するには、グローバル コンフィギュレーション モードで **sdm prefer** コマンドを使用します。

sdm prefer
{**advanced**}

構文の説明

advanced	NetFlowなどの高度な機能をサポートします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

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

使用上のガイドライン

device スタックでは、すべてのスタック メンバが、アクティブな device に保存された同一のSDM テンプレートを使用する必要があります。

新規 device がスタックに追加されると、アクティブ device に保存された SDM コンフィギュレーションは、個々の device に設定されているテンプレートを上書きします。

例

次に、高度なテンプレートを設定する例を示します。

```
デバイス(config)# sdm prefer advanced
デバイス(config)# exit
デバイス# reload
```

set

環境変数を設定または表示するには、ブートローダモードで **set** コマンドを使用します。環境変数は、ブートローダまたはdeviceで稼働している他のソフトウェアを制御するために使用できます。

set *variable value*

構文の説明

変数	値
	variable および *value* の適切な値には、次のいずれかのキーワードを使用します。
	MANUAL_BOOT：device の起動を自動で行うか手動で行うかどうかを決定します。
	有効な値は 1/Yes と 0/No です。0 または No に設定されている場合、ブート ローダはシステムを自動的に起動します。他の値に設定されている場合は、ブート ローダモードから手動で device を起動する必要があります。
	BOOT *filesystem:/file-url*：自動起動時にロードおよび実行される実行可能ファイルのセミコロン区切りリストを識別します。
	BOOT 環境変数が設定されていない場合、システムは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT 変数が設定されていても、指定されたイメージをロードできなかった場合、システムはフラッシュ ファイル システムで最初に検出した起動可能なファイルを起動しようとします。
	ENABLE_BREAK：ユーザがコンソールの **Break** キーを押すと自動起動プロセスを中断できるようになります。
	有効な値は 1、Yes、On、0、No、および Off です。1、Yes、または On に設定されている場合は、フラッシュ ファイル システムの初期化後にコンソール上で Break キーを押すことで、自動起動プロセスを中断できます。
	HELPER *filesystem:/file-url*：ブート ローダの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストを識別します。ヘルパー ファイルは、ブートローダの機能を拡張したり、パッチを当てたりします。
	PS1 *prompt*：ブート ローダ モードの場合に、コマンドライン プロンプトとして使用する文字列を指定します。
	CONFIG_FILE flash: */file-url*：Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名を指定します。
	BAUD *rate*：コンソールのボー レートに使用するビット数/秒（b/s）を指定します。コンフィギュレーション ファイルに別の設定が指定されていない限り、Cisco IOS ソフトウェアはブートローダからボー レート設定を継承し、この値を引き続き使用します。指定できる範囲は 0 ～ 128000 b/s です。有効値は、50、75、110、150、300、600、1200、1800、2000、2400、3600、4800、7200、9600、14400、19200、28800、38400、56000、57600、115200、および 128000 です。
	最も一般的な値は、300、1200、2400、9600、19200、57600、および 115200 です。
	SWITCH_NUMBER *stack-member-number*：スタック メンバのメンバ番号を変更します。
	SWITCH_PRIORITY *priority-number*：スタック メンバのプライオリティ値を変更します。

コマンド デフォルト

環境変数のデフォルト値は、次のとおりです。

MANUAL_BOOT: No (0)

BOOT：ヌル ストリング

ENABLE_BREAK：No（Off または 0）（コンソール上で Break キーを押して自動起動プロセスを中断することはできません）。

HELPER: デフォルト値はありません（ヘルパー ファイルは自動的にロードされません）。

PS1 device：

CONFIG_FILE: config.text

BAUD：9600 b/s

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1

（注） 値が設定された環境変数は、各ファイルのフラッシュ ファイル システムに保管されます。ファイルの各行には、環境変数名と等号に続いて、その変数の値が指定されます。

このファイルに表示されていない変数には値がありません。表示されていればヌル ストリングであっても値があります。ヌル ストリング（たとえば“”）が設定されている変数は、値が設定された変数です。

多くの環境変数は事前に定義されており、デフォルト値が設定されています。

コマンド モード

ブートローダ

コマンド履歴

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

使用上のガイドライン

環境変数は大文字と小文字の区別があり、指定どおりに入力する必要があります。

値を持つ環境変数は、フラッシュ ファイル システムの外にあるフラッシュ メモリに保管されます。

通常の環境では、環境変数の設定を変更する必要はありません。

MANUAL_BOOT 環境変数は、**boot manual** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

BOOT 環境変数は、**boot system** *filesystem:/file-url* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

ENABLE_BREAK 環境変数は、**boot enable-break** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

HELPER 環境変数は、**boot helper** *filesystem: /file-url* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

CONFIG_FILE 環境変数は、**boot config-file flash:** */file-url* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

SWITCH_NUMBER 環境変数は、**switch** *current-stack-member-number* **renumber** *new-stack-member-number* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

SWITCH_PRIORITY 環境変数は、device *stack-member-number* **priority** *priority-number* グローバル コンフィギュレーション コマンドを使用して設定することもできます。

ブート ローダのプロンプト ストリング（PS1）には、等号（=）を除く、出力可能な文字列を 120 文字まで指定できます。

例

次に、SWITCH_PRIORITY 環境変数を設定する例を示します。

```
デバイス: set SWITCH_PRIORITY 2
```

設定を確認するには、**set** ブートローダコマンドを使用します。

show avc client

上位アプリケーションの数に関する情報を表示するには、特権 EXEC モードで **show avc client** コマンドを使用します。

show avc client *client-mac* **top** *n* **application**［**aggregate** | **upstream** | **downstream**］

構文の説明

client *client-mac*	クライアントの MAC アドレスを指定します。
top *n* **application**	特定のクライアントの上位「N」個のアプリケーションの数を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

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

次に、**show avc client** コマンドの出力例を示します。

```
デバイス# sh avc client 0040.96ae.65ec top 10 application aggregate
```

```
Cumulative Stats:

No.  AppName      Packet-Count    Byte-Count       AvgPkt-Size     usage%
-------------------------------------------------------------------------
1    skinny          7343           449860           61              94
2    unknown         99             13631            137             3
3    dhcp            18             8752             486             2
4    http            18             3264             181             1
5    tftp            9              534              59              0
6    dns             2              224              112             0

Last Interval(90 seconds) Stats:

No.  AppName     Packet-Count     Byte-Count       AvgPkt-Size      usage%
-------------------------------------------------------------------------
1    skinny          9              540              60               100
```

show cable-diagnostics tdr

タイムドメイン反射率計（TDR）の結果を表示するには、特権 EXEC モードで **show cable-diagnostics tdr** コマンドを使用します。

show cable-diagnostics tdr interface *interface-id*

構文の説明

interface-id	TDRが実行されているインターフェイスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

TDR は、銅線のイーサネット 10/100/100 ポートだけでサポートされます。10 ギガビット イーサネット ポート、および Small Form-Factor Pluggable（SFP）モジュール ポートではサポートされません。

例

次に、deviceに対する **show cable-diagnostics tdr interface** *interface-id* コマンドの出力例を示します。

```
デバイス# show cable-diagnostics tdr interface gigabitethernet1/0/23
  TDR test last run on: March 01 00:04:08
  Interface  Speed  Local pair  Pair length         Remote pair   Pair status
  ---------  -----  ----------  ------------------  -----------  --------------------
  Gi1/0/23   1000M  Pair A      1    +/- 1 meters   Pair A       Normal
                    Pair B      1    +/- 1 meters   Pair B       Normal
```

```
Pair C      1    +/- 1 meters   Pair C        Normal
Pair D      1    +/- 1 meters   Pair D        Normal
```

表 *58 : show cable-diagnostics tdr* コマンドで出力されるフィールドの説明

フィールド	説明
Interface	TDR が実行されているインターフェイス。
Speed	接続速度。
Local pair	ローカル インターフェイスで TDR がテストを実行するワイヤ ペア名。
Pair length	device に関するケーブルの問題の場所。次のいずれかの場合に限り、TDR は場所を特定できます。 • ケーブルが正しく接続され、リンクがアップ状態で、インターフェイス速度が 1000 Mb/s である場合 • ケーブルが断線している場合 • ケーブルがショートしている場合
Remote pair	ローカル ペアが接続されたワイヤ ペア名。ケーブルが正しく接続されリンクがアップ状態である場合だけ、TDR はリモート ペアについて確認します。
Pair status	TDR が実行されているワイヤ ペアのステータス • Normal：ワイヤ ペアが正しく接続されています。 • Not completed：テストは実行中で、完了していません。 • Not supported：インターフェイスは TDR をサポートしません。 • Open：ワイヤ ペアが断線しています。 • Shorted：ワイヤ ペアがショートしています。 • ImpedanceMis：インピーダンスが一致しません。 • Short/Impedance Mismatched：インピーダンスが一致しないかケーブルがショートしています。 • InProgress：診断テストが進行中です。

次の例では、TDR が実行されているときの **show interface** *interface-id* コマンドの出力を示します。

```
デバイス# show interface gigabitethernet1/0/2
  gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

次の例では、TDR が実行されていないときの **show cable-diagnostics tdr interface** *interface-id* コマンドの出力を示します。

```
デバイス# show cable-diagnostics tdr interface gigabitethernet1/0/2
```

```
% TDR test was never issued on gigabitethernet1/0/2
```

インターフェイスでTDRがサポートされない場合、次のメッセージが表示されます。

```
% TDR test is not supported on device 1
```

show debug

スイッチで使用できるすべての debug コマンドを表示するには、特権 EXEC モードで **show debug** コマンドを使用します。

show debug

show debug condition *Condition identifier* | *All conditions*

構文の説明

Condition identifier	使用される条件識別子の値を設定します。範囲は、1 ～ 1000 です。
All conditions	使用可能なすべての条件付きデバッグ オプションを表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 16.1	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、debug コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、debug コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用するのが最良です。このような時間帯を選んでデバッグを実行すると、debug コマンドの処理の負担によってシステム利用が影響を受ける可能性が少なくなります。

例

次に、**show debug** コマンドの出力例を示します。

```
デバイス# show debug condition all
```

デバッグを無効にするには、**no debug all** コマンドを使用します。

show env

スイッチ（スタンドアロンスイッチ、スタックマスター、またはスタックメンバ）のファン、温度、および電源情報を表示するには、EXEC モードで **show env** コマンドを使用します。

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

構文の説明

all	ファン、温度、および電源環境のステータスを表示します。
fan	スイッチのファンの状態を表示します。
power	電源装置のステータスを表示します。
all	（任意）すべての電源装置のステータスを表示します。
switch *switch-number*	（任意）特定のスイッチの電源装置のステータスを表示します。
stack *switch-number*	（任意）スタックの各スイッチまたは指定されたスイッチのすべての環境ステータスを表示します。指定できる範囲は、スタック内のスイッチ メンバ番号に従って 1 ～ 9 です。
temperature	スイッチの温度ステータスを表示します。
status	（任意）温度ステータスとしきい値を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

使用上のガイドライン

任意のメンバスイッチからスタック内のスイッチに関する情報を表示するには、**show env stack** [*switch-number*] コマンドを使用します。

スイッチの温度ステータスとしきい値レベルを表示するには、**show env temperature status** コマンドを使用します。

例

次の例では、マスター スイッチからスタック メンバ 1 に関する情報を表示する方法を示します。

```
デバイス> show env stack 1
デバイス 1:
デバイス Fan 1 is OK
デバイス Fan 2 is OK
デバイス Fan 3 is OK
FAN-PS1 is OK
FAN-PS2 is NOT PRESENT
デバイス 1: SYSTEM TEMPERATURE is OK
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius

デバイス>
```

次に、温度値、状態、およびしきい値を表示する例を示します。

```
デバイス> show env temperature status
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius

デバイス>
```

表 *59 : show env temperature status* コマンド出力のステート

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

show env xps

Cisco eXpandable Power System（XPS）2200 のバジェット配分、設定、電力、およびシステム電源情報を表示するには、特権 EXEC モードで **show env xps** コマンドを使用します。

show env xps { **budgeting** | **configuration** | **port** [**all** | *number*] | **power** | **system** | **thermal** | **upgrade** | **version** }

構文の説明

budgeting	XPS 電力バジェットの配分（電源スタックに含まれるすべてのスイッチに対する電力の割り当て量とバジェット量）を表示します。
configuration	power xps 特権 EXEC コマンドを実行した結果の設定を表示します。XPS 設定は XPS に保存されます。show env xps configuration コマンドを入力すると、デフォルト以外の設定が取得されます。
port ［**all** ｜ *number* ］	すべてのポートまたは指定の XPS ポートの設定とステータスを表示します。ポート番号は、1 ～ 9 です。
power	XPS 電源装置のステータスを表示します。
system	XPS システム ステータスを表示します。
thermal	XPS 温度ステータスを表示します。
upgrade	XPS アップグレード ステータスを表示します。
version	XPS バージョンの詳細を表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
12.2(55)SE1	このコマンドが導入されました。

使用上のガイドライン

XPS 2200 の情報を表示するには、**show env xps** 特権 EXEC コマンドを使用します。

例

次に、show env xps budgeting コマンドの出力例を示します。

```
Switch#
=======


XPS 0101.0100.0000 :
============================================================
Data                  Current    Power     Power Port  Switch #  PS A  PS B  Role-State
 Committed
Budget
----  --------  ----  ----  ---------- ---------  ------ 1     -        -    715  SP-PS
      223
    1543
2     -        -    -    SP-PS      223       223
3     -        -    -    -          -         -
4     -        -    -    -          -         -
5     -        -    -    -          -         -
6     -        -    -    -          -         -
7     -        -    -    -          -         -
8     -        -    -    -          -         -
```

```
9     1        1100 -    RPS-NB     223        070
XPS  -         -    1100  -          -
```

次に、show env xps configuration コマンドの出力例を示します。

```
Switch# show env xps configuration
===============================================
XPS 0101.0100.0000 :
===============================================
power xps port 4 priority 5
power xps port 5 mode disable
power xps port 5 priority 6
power xps port 6 priority 7
power xps port 7 priority 8
power xps port 8 priority 9
power xps port 9 priority 4
```

次に、show env xps port all コマンドの出力例を示します。

```
Switch#
XPS 010



----------------------------------------
Port name          : -
Connected          : Yes
Mode               : Enabled (On)
Priority           : 1
Data stack switch # : - Configured role    : Auto-SP
Run mode            : SP-PS : Stack Power Power-Sharing Mode
Cable faults        : 0x0 XPS 0101.0100.0000 Port 2
----------------------------------------
Port name          : -
Connected          : Yes
Mode               : Enabled (On)
Priority           : 2
Data stack switch # : - Configured role    : Auto-SP
Run mode            : SP-PS : Stack Power Power-Sharing Mode
Cable faults        : 0x0 XPS 0101.0100.0000 Port 3
----------------------------------------
Port name          : -
Connected          : No
Mode               : Enabled (On)
Priority           : 3
Data stack switch # : - Configured role    : Auto-SP Run mode            : -
Cable faults
<output truncated>
```

次に、show env xps power コマンドの出力例を示します。

```
================================================================================
XPS 0101.0100.0000 :
================================================================================
Port-Supply SW PID                 Serial#     Status         Mode Watts
----------- -- ------------------  ----------- --------------  ----  -----
XPS-A           Not present
XPS-B           NG3K-PWR-1100WAC   LIT13320NTV OK             SP   1100
1-A         -  -                   -           -
1-B         -  -                   -           -               SP    715
2-A         -  -                   -           -
2-B         -  -                   -           -
9-A                      100WAC    LIT141307RK OK              RPS  1100
9-B                   esent
```

次に、show env xps system コマンドの出力例を示します。

```
Switch#
=======


XPS 0101.0100.0000 :
================================================================================
XPS                        Cfg  Cfg      RPS Switch  Current    Data Port  XPS Port Name

Mode Role    Pri Conn    Role-State  Switch #
----  --------------------  ---- -------  --- ------  ----------  --------
1     -                     On   Auto-SP  1   Yes     SP-PS      -
2     -                     On   Auto-SP  2   Yes     SP-PS      -
3     -                     On   Auto-SP  3   No      -          -
4     none                  On   Auto-SP  5   No      -          -
5     -                     Off  Auto-SP  6   No      -          -
6     -                     On   Auto-SP  7   No      -          -
7     -                     On   Auto-SP  8   No      -          -
8     -                     On   Auto-SP  9   No      -
9     test                  On   Auto-SP  4   Yes     RPS-NB
```

次に、show env xps thermal コマンドの出力例を示します。

```
Switch#
=======



XPS 0101.0100.0000 :
============================================
Fan  Status
----  -----------
1     OK
2     OK
3     NOT PRESENT PS-1  NOT PRESENT PS-2  OK Temperature is OK
```

次に、アップグレードが実行されていない場合の show env xps upgrade コマンドの出力例を示します。

```
Switch# show env xps upgrade
No XPS is connected and upgrading.
```

次に、アップグレードが進行中の場合の show env xps upgrade コマンドの出力例を示します。

```
Switch# show env xps upgrade
XPS Upgrade Xfer

SW Status Prog
-- ----------- ----
1 Waiting 0%
Switch#
*Mar 22 03:12:46.723: %PLATFORM_XPS-6-UPGRADE_START: XPS 0022.bdd7.9b14 upgrade has
started through the Service Port.
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Receiving 1%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
```

```
1 Receiving 5%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Reloading 100%
Switch#
*Mar 22 03:16:01.733: %PLATFORM_XPS-6-UPGRADE_DONE: XPS 0022.bdd7.9b14 upgrade has
completed and the XPS is reloading.
```

次に、show env xps version コマンドの出力例を示します。

```
Switch# show env xps version
============================================
XPS 0022.bdd7.9b14:
============================================
Serial Number: FDO13490KUT
Hardware Version: 8
Bootloader Version: 7
Software Version: 18
```

表 *60*：関連コマンド

コマンド	Description
power xps（グローバル コンフィギュレーション コマンド）	XPS と XPS ポートの名前を設定します。
power xps（特権 EXEC コマンド）	XPS ポートとシステムを設定します。

show flow monitor

フローモニタのステータスと統計情報を表示するには、特権EXECモードで**show flow monitor**コマンドを使用します。

構文の説明

name	（任意）フロー モニタの名前を指定します。
monitor-name	（任意）事前に設定されたフロー モニタの名前。
cache	（任意）フロー モニタのキャッシュの内容を表示します。
format	（任意）ディスプレイ出力のフォーマット オプションのいずれかを使用することを指定します。
csv	（任意）フローモニタのキャッシュの内容をカンマ区切り値（CSV）形式で表示します。
record	（任意）フロー モニタのキャッシュの内容をレコード形式で表示します。
table	（任意）フロー モニタのキャッシュの内容を表形式で表示します。
statistics	（任意）フロー モニタの統計情報を表示します。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

cache キーワードでは、デフォルトでレコード形式が使用されます。

show flowmonitor *monitor-name* **cache** コマンドのディスプレイ出力に含まれる大文字のフィールド名は、フローの識別に が使用するキー フィールドです。**show flow monitor** *monitor-name* **cache** コマンドのディスプレイ出力に含まれる小文字のフィールド名は、 がキャッシュの追加データとして値を収集する非キー フィールドです。

例

次の例では、フロー モニタのステータスを表示します。

```
デバイス# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic traffic analysis
  Flow Record:       flow-record-1
  Flow Exporter:     flow-exporter-1
                     flow-exporter-2
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 311316 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 61 : show flow monitor monitor-name フィールドの説明

フィールド	説明
Flow Monitor	設定したフロー モニタの名前。
Description	モニタに設定した説明、またはユーザ定義のデフォルトの説明。
Flow Record	フロー モニタに割り当てられたフロー レコード。
Flow Exporter	フロー モニタに割り当てられたエクスポータ。
Cache	フロー モニタのキャッシュに関する情報。
Type	フロー モニタのキャッシュ タイプ。この値は常に normal となります。これが唯一サポートされているキャッシュ タイプです。

フィールド	説明
Status	フロー モニタのキャッシュのステータス。 次の値が可能です。 • allocated：キャッシュが割り当てられています。 • being deleted：キャッシュが削除されています。 • not allocated：キャッシュが割り当てられていません。
Size	現在のキャッシュ サイズ。
Inactive Timeout	非アクティブ タイムアウトの現在の値（秒単位）。
Active Timeout	アクティブ タイムアウトの現在の値（秒単位）。

次の例では、FLOW-MONITOR-1 という名前のフロー モニタのステータス、統計情報、およびデータを表示します。

次の表で、この出力に表示される重要なフィールドを説明します。

次の例では、FLOW-MONITOR-1 という名前のフロー モニタのステータス、統計情報、およびデータを表形式で表示します。

次の例では、FLOW-MONITOR-IPv6 という名前のフロー モニタ（キャッシュに IPv6 データを格納）のステータス、統計情報、およびデータをレコード形式で表示します。

次の例では、フロー モニタのステータスと統計情報を表示します。

show install

インストールパッケージに関する情報を表示するには、特権 EXEC モードで **show install** コマンドを使用します。

show install {**active** | **committed** | **inactive** | **log** | **package** {**bootflash:** | **flash:** | **webui:**} | **rollback** | **summary** | **uncommitted**}

構文の説明

active	アクティブなパッケージに関する情報を表示します。
committed	永続的なパッケージのアクティベーションを表示します。
inactive	非アクティブなパッケージを表示します。
log	ログ インストレーション バッファに格納されているエントリを表示します。

package	説明、再起動情報、パッケージ内のコンポーネントなど、パッケージに関するメタデータ情報を表示します。
{**bootflash:** | **flash:** | **harddisk:** |**webui:**}	インストール パッケージのロケーションを指定します。
rollback	保存されているインストレーションに関連付けられたソフトウェア セットを表示します。
summary	アクティブ、非アクティブ、コミット済み、廃止されたパッケージのリストに関する情報を表示します。
uncommitted	非永続的なパッケージのアクティベーションを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

インストール パッケージのステータスを表示するには、show コマンドを使用します。

例

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

```
Device# show install package bootflash:cat3k-universalk9.2017-01-10_13.15.1.
CSCxxx.SSA.dmp.bin
Name:  cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SS
Version:  16.6.1.0.199.1484082952..Everest
Platform:  Catalyst3k
Package Type:  dmp
Defect ID:  CSCxxx
Package State:  Added
Supersedes List:  {}
Smu ID:  1
```

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

```
Device# show install summary

Active Packages:
    bootflash:cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Inactive Packages:
   No packages
Committed Packages:
    bootflash:cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Uncommitted Packages:
   No packages
```

```
Device#
```

下の表に、ディスプレイ内に表示される重要なフィールドのリストを示します。

表 *62 : show install summary* フィールドの説明

フィールド	説明
Active Packages	アクティブなインストール パッケージの名前。
Inactive Packages	非アクティブなパッケージのリスト。
Committed Packages	変更がリロード以降も存続するように、ハードディスクに変更を保存またはコミットしたインストール パッケージ。
Uncommitted Packages	非永続的なインストール パッケージのアクティベーション。

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

```
Device# show install log

[0|install_op_boot]: START Fri Feb 24 19:20:19 Universal 2017
[0|install_op_boot]: END SUCCESS  Fri Feb 24 19:20:23 Universal 2017
[3|install_add]: START Sun Feb 26 05:55:31 UTC 2017
[3|install_add( FATAL)]: File path (scp) is not yet supported for this command
[4|install_add]: START Sun Feb 26 05:57:04 UTC 2017
[4|install_add]: END SUCCESS
/bootflash/cat3k-universalk9.2017-01-10_13.15.1.CSCvb12345.SSA.dmp.bin
Sun Feb 26 05:57:22 UTC 2017
[5|install_activate]: START Sun Feb 26 05:58:41 UTC 2017
```

関連コマンド

コマンド	説明
install	SMUパッケージをインストールします。

show license all

権限付与情報を表示するには、特権 EXEC モードで **show license all** コマンドを使用します。

show license all

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドでは、スマートライセンスが有効になっているかどうか、関連付けられているすべてのライセンス証明書、コンプライアンスステータスなども表示されます。

例

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

```
デバイス# show license all
Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: BU Production Test
  Virtual Account: DLC-VA1
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jul 09 10:08:19 2018 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Jan 05 10:08:19 2019 UTC
  Registration Expires: Jul 09 10:02:35 2019 UTC

License Authorization:
  Status: AUTHORIZED on Jul 09 11:16:10 2018 UTC
  Last Communication Attempt: SUCCEEDED on Jul 09 11:16:10 2018 UTC
  Next Communication Attempt: Aug 08 11:16:09 2018 UTC
  Communication Deadline: Oct 07 11:10:28 2018 UTC

License Conversion:
  Automatic Conversion Enabled: False
  Active: PID:WS-C3850-24P,SN:FOC1842U0FC
  Status: Successful on Jul 09 11:16:06 2018 UTC
  Standby: PID:WS-C3850-24P,SN:FOC1842U0CZ
  Status: Successful on Jul 09 11:16:06 2018 UTC
  Member: PID:WS-C3850-24P,SN:FOC1842X0FD
  Status: Successful on Jul 09 11:16:06 2018 UTC

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

License Usage
=============

C3850-DNA-E-24 (C3850-24 DNA Essentials):
  Description: C3850-DNA-E
  Count: 3
  Version: 1.0
  Status: AUTHORIZED

C3850_24_Lanbase (C3850-24 LAN Base):
  Description: C3850 24 Port Lanbase
  Count: 3
```

```
  Version: 1.0
  Status: AUTHORIZED

Product Information
===================
UDI: PID:WS-C3850-24P,SN:FOC1842U0FC

HA UDI List:
    Active:PID:WS-C3850-24P,SN:FOC1842U0FC
    Standby:PID:WS-C3850-24P,SN:FOC1842U0CZ
    Member:PID:WS-C3850-24P,SN:FOC1842X0FD

Agent Version
=============
Smart Agent for Licensing: 4.4.13_rel/116
Component Versions: SA:(1_3_dev)1.0.15, SI:(dev22)1.2.1, CH:(rel5)1.0.3, PK:(dev18)1.0.3

Reservation Info
================
License reservation: DISABLED
```

関連コマンド

コマンド	説明
show license status	ライセンスのコンプライアンスステータスを表示します。
show license summary	すべてのアクティブなライセンスの要約を表示します。
show license udi	UDI を表示します。
show license usage	ライセンス使用情報を表示します。
show tech-support license	デバッグ出力を表示します。

show license status

ライセンスのコンプライアンスステータスを表示するには、特権 EXEC モードで **show license status** コマンドを使用します。

show license status

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

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

```
デバイス# show license status
Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: REGISTERED
  Smart Account: BU Production Test
  Virtual Account: DLC-VA1
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jul 09 10:08:19 2018 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Jan 05 10:08:19 2019 UTC
  Registration Expires: Jul 09 10:02:35 2019 UTC

License Authorization:
  Status: AUTHORIZED on Jul 09 11:16:10 2018 UTC
  Last Communication Attempt: SUCCEEDED on Jul 09 11:16:10 2018 UTC
  Next Communication Attempt: Aug 08 11:16:09 2018 UTC
  Communication Deadline: Oct 07 11:10:28 2018 UTC

License Conversion:
  Automatic Conversion Enabled: False
  Active: PID:WS-C3850-24P,SN:FOC1842U0FC
  Status: Successful on Jul 09 11:16:06 2018 UTC
  Standby: PID:WS-C3850-24P,SN:FOC1842U0CZ
  Status: Successful on Jul 09 11:16:06 2018 UTC
  Member: PID:WS-C3850-24P,SN:FOC1842X0FD
  Status: Successful on Jul 09 11:16:06 2018 UTC
```

関連コマンド

コマンド	説明
show license all	権限付与情報を表示します。
show license summary	すべてのアクティブなライセンスの要約を表示します。
show license udi	UDI を表示します。
show license usage	ライセンス使用情報を表示します。
show tech-support license	デバッグ出力を表示します。

show license summary

すべてのアクティブなライセンスの要約を表示するには、特権 EXEC モードで **show license summary** コマンドを使用します。

show license summary

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

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

```
デバイス# show license summary
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: BU Production Test
  Virtual Account: DLC-VA1
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Jan 05 10:08:20 2019 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Aug 08 11:16:10 2018 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  C3850-DNA-E-24          (C3850-24 DNA Essentials)         3 AUTHORIZED
  C3850_24_Lanbase        (C3850-24 LAN Base)               3 AUTHORIZED
```

関連コマンド

コマンド	説明
show license all	権限付与情報を表示します。
show license status	ライセンスのコンプライアンスステータスを表示します。
show license udi	UDI を表示します。
show license usage	ライセンス使用情報を表示します。
show tech-support license	デバッグ出力を表示します。

show license udi

固有デバイス識別子（UDI）を表示するには、特権 EXEC モードで **show license udi** コマンドを使用します。

show license udi

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

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

```
デバイス# show license udi
UDI: PID:WS-C3850-24P,SN:FOC1842U0FC

HA UDI List:
    Active:PID:WS-C3850-24P,SN:FOC1842U0FC
    Standby:PID:WS-C3850-24P,SN:FOC1842U0CZ
    Member:PID:WS-C3850-24P,SN:FOC1842X0FD
```

関連コマンド

コマンド	説明
show license all	権限付与情報を表示します。
show license status	ライセンスのコンプライアンスステータスを表示します。
show license summary	すべてのアクティブなライセンスの要約を表示します。
show license usage	ライセンス使用情報を表示します。
show tech-support license	デバッグ出力を表示します。

show license usage

ライセンス使用情報を表示するには、特権 EXEC モードで **show license usage** コマンドを使用します。

show license usage

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

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

```
デバイス# show license usage
License Authorization:
  Status: AUTHORIZED on Jul 09 11:16:10 2018 UTC

C3850-DNA-E-24 (C3850-24 DNA Essentials):
  Description: C3850-DNA-E
  Count: 3
  Version: 1.0
  Status: AUTHORIZED

C3850_24_Lanbase (C3850-24 LAN Base):
  Description: C3850 24 Port Lanbase
  Count: 3
  Version: 1.0
  Status: AUTHORIZED
```

関連コマンド

コマンド	説明
show license all	権限付与情報を表示します。
show license status	ライセンスのコンプライアンスステータスを表示します。
show license summary	すべてのアクティブなライセンスの要約を表示します。
show license udi	UDI を表示します。
show tech-support license	デバッグ出力を表示します。

show location

ロケーション情報を表示するには、特権EXECモードで**show location** コマンドを使用します。

show location {**detail** *mac-addr* | **plm** | **statistics**| **summary** **rfid** | **rfid** {**client** | **config** | **detail** *mac-addr* | **summary**}}

構文の説明

detail *mac-addr*	特定のクライアントの RSSI テーブルとともに詳細なロケーション情報を表示します。

plm	ロケーション パス損失測定（CCX S60）の設定を表示します。
statistics	ロケーションベースのシステム統計情報を表示します。
summary	ロケーションベースのシステム概要情報を表示します。
rfid	RFID タグ トラッキング情報を表示します。
client	クライアントである RFID タグの概要を表示します。
config	RFID タグ トラッキングの設定オプションを表示します。
detail *mac-addr*	1 つの RFID タグの詳細情報を表示します。
summary	既知のすべての RFID タグの概要情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

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

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

```
デバイス# show location plm
Location Path Loss Configuration

Calbration client      : Disabled, Radio: Multiband
Normal clients         : Disabled
Burst interval         : 60
```

show location ap-detect

指定されたアクセスポイントで検出されたロケーション情報を表示するには、特権EXECモードで **show location ap-detect** コマンドを使用します。

show location ap-detect {**all** | **client** | **rfid** | **rogue-ap** | **rogue-client**} *ap-name*

構文の説明

all	クライアント、RFID、不正アクセス ポイント、不正クライアントの情報を表示します。
client	クライアント情報を表示します。
rfid	RFID 情報を表示します。
rogue-ap	不正アクセス ポイントの情報を表示します。

rogue-client	不正クライアントの情報を表示します。
ap-name	特定のアクセス ポイント名。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

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

次に、**show location ap-detect client** コマンドの出力例を示します。

```
デバイス# show location ap-detect client AP02
Clients

MAC Address       Status            Slot  Antenna     RSSI
------------------------------------------------------------
2477.0389.96ac    Associated           1        0      -60
2477.0389.96ac    Associated           1        1      -61
2477.0389.96ac    Associated           0        0      -46
2477.0389.96ac    Associated           0        1      -41


RFID Tags



Rogue AP's



Rogue Clients

MAC Address         State               Slot     Rssi
------------------------------------------------------------
0040.96b3.bce6      Alert               1        -58
586d.8ff0.891a      Alert               1        -72
```

show logging onboard switch uptime

システム内のすべてのモジュールまたはスイッチのすべてのリセット理由の履歴を表示するには、**show logging onboard switch uptime** コマンドを使用します。

show logging onboard switch { *switch-number* | **active** | **standby** } **uptime** [[[**continuous** | **detail**] [**start** *hour day month* [*year*] [**end** *hour day month year*]]] | **summary**]

構文の説明

switch *switch-number*	スイッチを指定します。スイッチ番号を入力します。
active	アクティブ インスタンスを指定します。
standby	スタンバイ インスタンスを指定します。
continuous	（任意）連続データを表示します。
detail	（任意）詳細データを表示します。
start *hour day month year*	（任意）データを表示する開始時刻を指定します。
end *hour day month year*	（任意）データを表示する終了時刻を指定します。
summary	（任意）要約データを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。
Cisco IOS XE Gibraltar 16.11.1	このコマンドの出力が更新され、スタック内のメンバのリロード理由が表示されるようになりました。

次に例を示します。

次に、**show logging onboard switch active uptime continuous** コマンドの出力例を示します。

```
Device# show logging onboard switch active uptime continuous
--------------------------------------------------------------------------------
UPTIME CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Time Stamp          | Reset                       | Uptime
MM/DD/YYYY HH:MM:SS | Reason                      | years weeks days hours minutes
--------------------------------------------------------------------------------
06/17/2018 19:42:56   Reload                        0     0     0     0     5
06/17/2018 19:56:31   Reload                        0     0     0     0     5
06/17/2018 20:10:46   Reload                        0     0     0     0     5
06/17/2018 20:23:48   Reload                        0     0     0     0     5
06/17/2018 20:37:20   Reload Command                0     0     0     0     5
06/18/2018 17:09:23   Reload Command                0     0     0     20    5
06/18/2018 17:18:39   redundancy force-switchover   0     0     0     0     5
06/18/2018 18:33:33   Reload                        0     0     0     1     5
06/18/2018 19:03:05   Reload                        0     0     0     0     5
06/18/2018 19:40:30   Reload                        0     0     0     0     5
06/18/2018 20:37:47   Reload                        0     0     0     0     5
06/18/2018 20:51:13   Reload                        0     0     0     0     5
06/18/2018 21:04:08   Reload                        0     0     0     0     5
06/18/2018 21:18:23   Reload                        0     0     0     0     5
```

```
06/18/2018 21:31:25   Reload                         0     0     0     0     5
06/18/2018 21:45:15   Reload                         0     0     0     0     5
06/18/2018 21:59:02   Reload                         0     0     0     0     5
06/18/2018 22:11:41   Reload                         0     0     0     0     5
06/18/2018 22:24:27   Reload                         0     0     0     0     5
06/18/2018 22:39:14   Reload Command                 0     0     0     0     4
06/19/2018 00:01:59   Reload Command                 0     0     0     1     5
06/19/2018 00:13:21   redundancy force-switchover    0     0     0     0     5
06/19/2018 01:05:42   redundancy force-switchover    0     0     0     0     5
06/20/2018 02:37:16   redundancy force-switchover    0     0     1     1     5
06/20/2018 02:50:03   redundancy force-switchover    0     0     0     0     5
06/20/2018 03:02:13   redundancy force-switchover    0     0     0     0     5
06/20/2018 03:14:26   redundancy force-switchover    0     0     0     0     5
06/20/2018 03:26:44   redundancy force-switchover    0     0     0     0     5
06/20/2018 03:38:58   redundancy force-switchover    0     0     0     0     5
06/20/2018 03:52:43   redundancy force-switchover    0     0     0     0     5
06/20/2018 04:05:16   redundancy force-switchover    0     0     0     0     5
.
.
.
```

次に、**show logging onboard switch active uptime detail** コマンドの出力例を示します。

```
Device# show logging onboard switch active uptime detail

--------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
--------------------------------------------------------------------------------
First customer power on : 06/10/2017 09:28:22
Total uptime            :  0  years  50 weeks  4  days  13 hours  38 minutes
Total downtime          :  0  years  15 weeks  4  days  11 hours  52 minutes
Number of resets        : 75
Number of slot changes  : 9
Current reset reason    : PowerOn
Current reset timestamp : 09/17/2018 10:59:57
Current slot            : 1
Chassis type            : 0
Current uptime          :  0  years  0  weeks  0  days  0  hours  0  minutes
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
UPTIME CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Time Stamp          | Reset                        | Uptime
MM/DD/YYYY HH:MM:SS | Reason                       | years weeks days hours minutes
--------------------------------------------------------------------------------
06/10/2017 09:28:22   Reload                         0     0     0     0     0
<snip>
09/17/2018 09:07:44   PowerOn                        0     0     3     15    5
09/17/2018 10:16:26   Reload Command                 0     0     0     1     5
09/17/2018 10:59:57   PowerOn                        0     0     0     0     5
```

次に、**show logging onboard switch standby uptime detail** コマンドの出力例を示します。

```
Device# show logging onboard switch standby uptime detail

--------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
--------------------------------------------------------------------------------
First customer power on : 06/10/2017 11:51:26
Total uptime            :  0  years  46 weeks  0  days  11 hours  44 minutes
Total downtime          :  0  years  20 weeks  1  days  10 hours  45 minutes
Number of resets        : 79
Number of slot changes  : 13
```

```
Current reset reason    : PowerOn
Current reset timestamp : 09/17/2018 10:59:57
Current slot            : 2
Chassis type            : 0
Current uptime          :  0  years  0  weeks  0  days  0  hours  5  minutes
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
UPTIME CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Time Stamp          | Reset                        | Uptime
MM/DD/YYYY HH:MM:SS | Reason                       | years weeks days hours minutes
--------------------------------------------------------------------------------
06/10/2017 11:51:26   Reload                         0     0     0     0     0
<snip>
08/10/2018 09:13:58   LocalSoft                      0     0     2     5     4
08/28/2018 14:21:42   Reload Slot Command            0     0     0     3     5
08/28/2018 14:34:29   System requested reload        0     0     0     0     0
09/11/2018 09:08:15   Reload                         0     0     1     8     5
09/11/2018 19:15:06   redundancy force-switchover    0     0     0     9     4
09/13/2018 16:50:18   Reload Command                 0     0     1     21    6
09/17/2018 10:55:09   PowerOn                        0     0     0     0     5
```

次に、**show logging onboard switch active uptime summary** コマンドの出力例を示します。

```
Device# show logging onboard switch active uptime summary
--------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
--------------------------------------------------------------------------------
First customer power on : 04/26/2018 21:45:39
Total uptime            :  0  years  20 weeks  2  days  12 hours  22 minutes
Total downtime          :  0  years  2  weeks  2  days  8  hours  40 minutes
Number of resets        : 1900
Number of slot changes  : 18
Current reset reason    : Reload Command
Current reset timestamp : 09/26/2018 20:43:15
Current slot            : 1
Chassis type            : 91
Current uptime          :  0  years  0  weeks  5  days  22 hours  5  minutes
--------------------------------------------------------------------------------
```

show mac address-table move update

device 上の MAC アドレステーブル移動更新情報を表示するには、EXEC モードで **show mac address-table move update** コマンドを使用します。

show mac address-table move update

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

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

例

次に、**show mac address-table move update** コマンドの出力例を示します。

```
デバイス# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

show platform integrity

起動段階のチェックサムレコードを表示するには、特権EXECモードで**show platform integrity**コマンドを使用します。

show platform integrity ［**sign** ［**nonce** <*nonce*>］］

構文の説明

sign	（任意）署名を表示します。
nonce	（任意）ナンス値を入力します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

例

次に、起動段階のチェックサム レコードを表示する例を示します。

```
デバイス# show platform integrity sign

PCR0: EE47F8644C2887D9BD4DE3E468DD27EB93F4A606006A0B7006E2928C50C7C9AB
PCR8: E7B61EC32AFA43DA1FF4D77F108CA266848B32924834F5E41A9F6893A9CB7A38
Signature version: 1
Signature:
816C5A29741BBAC1961C109FFC36DA5459A44DBF211025F539AFB4868EF91834C05789
5DAFBC7474F301916B7D0D08ABE5E05E66598426A73E921024C21504383228B6787B74
8526A305B17DAD3CF8705BACFD51A2D55A333415CABC73DAFDEEFD8777AA77F482EC4B
731A09826A41FB3EFFC46DC02FBA666534DBEC7DCC0C029298DB8462A70DBA26833C2A
1472D1F08D721BA941CB94A418E43803699174572A5759445B3564D8EAEE57D64AE304
EE1D2A9C53E93E05B24A92387E261199CED8D8A0CE7134596FF8D2D6E6DA773757C70C
D3BA91C43A591268C248DF32658999276FB972153ABE823F0ACFE9F3B6F0AD1A00E257
4A4CC41C954015A59FB8FE
Platform: WS-C3650-12X48UZ
```

show platform software fed switch punt cause

インターフェイスで受信したパケットがルータプロセッサ（RP）にパントされている理由に関する情報を表示するには、特権 EXEC モードで **show platform software fed switch punt cpuq cause** コマンドを使用します。

show platform software fed switch {*switch-number* | **active** | **standby**} **punt**{*cause_id* | **clear** | **summary**}

構文の説明

switch {*switch-number* | **active** | **standby**}	スイッチに関する情報を表示します。次の選択肢があります。 • *switch-number*。 • **active** ：アクティブなスイッチに関する情報を表示します。 • **standby**：存在する場合、スタンバイスイッチに関する情報を表示します。 （注） このキーワードはサポートされていません。
cause_id	詳細を表示する必要がある原因の ID を指定します。
clear	すべての原因の統計をクリアします。原因をクリアすると、統計に矛盾が生じる可能性があります。
summary	パント理由の概要を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴	リリース	変更内容
	Cisco IOS XE 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 なし

例

次に、**show platform software fed switch active punt cause summary** コマンドの出力例を示します。

```
Device# show platform software fed switch active punt cause summary
Statistics for all causes

Cause  Cause Info                       Rcvd                 Dropped
-------------------------------------------------------------------------------
7      ARP request or response          1                    0
21     RP<->QFP keepalive               22314                0
55     For-us control                   12                   0
60     IP subnet or broadcast packet    21                   0
96     Layer2 control protocols         133808               0
-------------------------------------------------------------------------------
```

次に、**show platform software fed switch active punt cause** *cause-id* コマンドの出力例を示します。

```
Device# show platform software fed switch active punt cause 21
Detailed Statistics

Sub Cause       Rcvd                 Dropped
-------------------------------------------
0               22363                0

-------------------------------------------
```

show platform software fed switch punt cpuq

CPU キューのパントトラフィックに関する情報を表示するには、特権 EXEC モードで **show platform software fed switch punt cpuq** コマンドを使用します。

show platform software fed switch {*switch-number* | **active** | **standby**} **punt cpuq** {*cpuq_id* | **all** | **brief** | **clear** | **rates**}

構文の説明

switch {*switch-number* **active standby**}	スイッチに関する情報を表示します。次の選択肢があります。 • *switch-number*。 • **active** ：アクティブなスイッチに関する情報を表示します。 • **standby**：存在する場合、スタンバイスイッチに関する情報を表示します。 （注） このキーワードはサポートされていません。
punt	パント情報を表示します。
cpuq	CPU 受信キューに関する情報を表示します。
cpuq_id	特定の CPU キューに固有の詳細を指定します。
all	すべての CPU キューの統計を表示します。
brief	受信およびドロップされたパントパケットの詳細など、すべてのキューの要約された統計を表示します。
clear	すべての CPU キューの統計をクリアします。CPU キューをクリアすると、統計に矛盾が生じる可能性があります。
rates	パケットのパントレートを表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE 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

なし

例

次に、**show platform software fed switch active punt cpuq brief** コマンドの出力例を示します。

```
Device#show platform software fed switch active punt cpuq brief

Punt CPU Q Statistics Brief
================================================================================================
 Q  |          Queue             |  Rx    |  Rx    |  Rx    |  Drop  |  Drop   |  Drop
 no |          Name              |  prev  |  cur   |  delta |  prev  |  cur    |  delta
================================================================================================
 0  CPU_Q_DOT1X_AUTH                0        0        0        0        0        0

 1  CPU_Q_L2_CONTROL                 0        6772     6772     0        0        0

 2  CPU_Q_FORUS_TRAFFIC              0        0        0        0        0        0

 3  CPU_Q_ICMP_GEN                   0        0        0        0        0        0

 4  CPU_Q_ROUTING_CONTROL            0        12       12       0        0        0

 5  CPU_Q_FORUS_ADDR_RESOLUTION      0        1        1        0        0        0

 6  CPU_Q_ICMP_REDIRECT              0        0        0        0        0        0

 7  CPU_Q_INTER_FED_TRAFFIC          0        0        0        0        0        0

 8  CPU_Q_L2LVX_CONTROL_PKT          0        0        0        0        0        0

 9  CPU_Q_EWLC_CONTROL               0        0        0        0        0        0

 10 CPU_Q_EWLC_DATA                  0        0        0        0        0        0

 11 CPU_Q_L2LVX_DATA_PKT             0        0        0        0        0        0

 12 CPU_Q_BROADCAST                  0        21       21       0        0        0

 13 CPU_Q_LEARNING_CACHE_OVFL        0        0        0        0        0        0

 14 CPU_Q_SW_FORWARDING              0        0        0        0        0        0

 15 CPU_Q_TOPOLOGY_CONTROL           0        127300   127300   0        0        0

 16 CPU_Q_PROTO_SNOOPING             0        0        0        0        0        0

 17 CPU_Q_BFD_LOW_LATENCY            0        0        0        0        0        0

 18 CPU_Q_TRANSIT_TRAFFIC            0        0        0        0        0        0

 19 CPU_Q_RPF_FAILED                 0        0        0        0        0        0

 20 CPU_Q_MCAST_END_STATION_SERVICE  0        0        0        0        0        0

 21 CPU_Q_LOGGING                    0        0        0        0        0        0

 22 CPU_Q_PUNT_WEBAUTH               0        0        0        0        0        0

 23 CPU_Q_HIGH_RATE_APP              0        0        0        0        0        0

 24 CPU_Q_EXCEPTION                  0        0        0        0        0        0

 25 CPU_Q_SYSTEM_CRITICAL            0        0        0        0        0        0

 26 CPU_Q_NFL_SAMPLED_DATA           0        0        0        0        0        0

 27 CPU_Q_LOW_LATENCY                0        0        0        0        0        0

 28 CPU_Q_EGR_EXCEPTION              0        0        0        0        0        0
```

```
 29 CPU_Q_FSS                        0         0         0         0         0         0

 30 CPU_Q_MCAST_DATA                 0         0         0         0         0         0

 31 CPU_Q_GOLD_PKT                   0         0         0         0         0         0

------------------------------------------------------------------------------------------
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *63 : show platform software fed switch active punt cpuq brief* フィールドの説明

フィールド	説明
Q no	キューの ID。
Queue Name	キューの名前。
Rx	受信されたパケット数。
ドロップ	ドロップされたパケットの数

次に、**show platform software fed switch active punt cpuq cpuq_id** コマンドの出力例を示します。

```
Device#show platform software fed switch active punt cpuq 1

Punt CPU Q Statistics
=============================================

CPU Q Id                        : 1
CPU Q Name                      : CPU_Q_L2_CONTROL
Packets received from ASIC      : 6774
Send to IOSd total attempts     : 6774
Send to IOSd failed count       : 0
RX suspend count                : 0
RX unsuspend count              : 0
RX unsuspend send count         : 0
RX unsuspend send failed count  : 0
RX consumed count               : 0
RX dropped count                : 0
RX non-active dropped count     : 0
RX conversion failure dropped   : 0
RX INTACK count                 : 6761
RX packets dq'd after intack    : 0
Active RxQ event                : 6761
RX spurious interrupt           : 0

Replenish Stats for all rxq:
---------------------------------------------
Number of replenish             : 61969
Number of replenish suspend     : 0
Number of replenish un-suspend  : 0
---------------------------------------------
```

show platform sudi certificate

特定のSUDIのチェックサムレコードを表示するには、特権EXECモードで**show platform sudi certificate**コマンドを使用します。

show platform sudi certificate [**sign** [**nonce** <*nonce*>]]

構文の説明

sign	（任意）署名を表示します。
nonce	（任意）ナンス値を入力します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.3.2	このコマンドが導入されました。

例

次に、特定の SUDI のチェックサム レコードを表示する例を示します。

```
デバイス# show platform sudi certificate

-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUl4F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1aO6g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQMqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
```

```
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcCl0lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KNDl5618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIDctWkMA0GCSqGSIb3DQEBCwUAMCcxDjAMBgNVBAoTBUNp
c2NvMRUwEwYDVQQDEwxBQ1QyIFNVREkgQ0EwHhcNMTUwODA2MDgwODI5WhcNMjUw
ODA2MDgwODI5WjBzMSwwKgYDVQQFEyNQSUQ6V1MtQzM2NTAtMTJYNDhVWiBTTjpG
RE8xOTMyWDAwQzEOMAwGA1UEChMFQ2lzY28xGDAWBgNVBAsTD0FDVC0yIExpdGUg
U1VESTEZMBcGA1UEAxMQV1MtQzM2NTAtMTJYNDhVWjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANZxOGYI0eUl4HcSwjL4HO75qTjl9C2BHG3ufce9ikkN
xwGXi8qg8vKxuB9tRYRaJC5bP1WMoq7+ZJtQA079xE4X14soNbkq5NaUhh7RB1wD
iRUJvTfCOzVICbNfbzvtB30I75tCarFNmpd0K6AFrIa41U988QGqaCj7R1JrYNaj
nC73UXXM/hC0HtNR5mhyqer5Y2qjjzo6tHZYqrrx2eS1XOa262ZSQriAxmaH/KLC
K97ywyRBdJlxBRX3hGtKlog8nASB8WpXqB9NVCERzUajwU3L/kg2BsCqw9Y2m7HW
U1cerTxgthuyUkdNI+Jg6iGApm2+s8E9hsHPBPMCdIsCAwEAAaNvMG0wDgYDVR0P
AQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwTQYDVR0RBEYwRKBCBgkrBgEEAQkVAgOg
NRMzQ2hpcElEPVVZSk5ORmRRRlFvN1ZIVmxJRTlqZENBeU9DQXhPRG93TlRveE1T
QVg5eWc9MA0GCSqGSIb3DQEBCwUAA4IBAQBKicTRZbVCRjVIR5MQcWXUT086v6Ej
HahDHTts3YpQoyAVfioNg2x8J6EXcEau4voyVu+eMUuoNL4szPhmmDcULfiCGBcA
/R3EFuoVMIzNT0geziytsCf728KGw1oGuosgVjNGOOahUELu4+F/My7bIJNbH+PD
KjIFmhJpJg0F3q17yClAeXvd13g3W393i35d00Lm5L1WbBfQtyBaOLAbxsHvutrX
u1VZ5sdqSTwTkkO9vKMaQjh7a8J/AmJi93jvzM69pe5711P1zqZfYfpiJ3cyJ0xf
I4brQ1smdczloFD4asF7A+1vor5e4VDBP0ppmeFAJvCQ52JTpj0M0o1D
-----END CERTIFICATE-----
```

show sdm prefer

特定の機能用のシステムリソースを最大にするために使用できるテンプレートに関する情報を表示するには、特権 EXEC モードで **show sdm prefer** コマンドを使用します。現在のテンプレートを表示するには、キーワードを指定せずにコマンドを使用します。

show sdm prefer［**advanced**］

構文の説明

advanced	（任意）高度なテンプレートに関する情報を表示します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

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

使用上のガイドライン

sdm prefer グローバル コンフィギュレーション コマンドを入力後にスイッチをリロードしていない場合、**show sdm prefer** 特権 EXEC コマンドでは、新しく設定されたテンプレートでなく現在使用中のテンプレートが表示されます。

各テンプレートで表示される番号は、各機能のリソースにおけるおおよその最大数になります。他に設定された機能の実際の数字にもよるため、実際の数字とは異なる場合があります。たとえば、deviceに 16 を超えるルーテッド インターフェイス（サブネット VLAN）がある場合、デフォルトのテンプレートでは、可能なユニキャスト MAC アドレスの数は 6000 未満になることがあります。

例

次に、**show sdm prefer** コマンドの出力例を示します。

```
デバイス# show sdm prefer

Showing SDM Template Info

This is the Advanced template.
 Number of VLANs:                            4094
 Unicast MAC addresses:                      32768
 Overflow Unicast MAC addresses:             512
 IGMP and Multicast groups:                  8192
 Overflow IGMP and Multicast groups:         512
 Directly connected routes:                  32768
 Indirect routes:                            7680
 Security Access Control Entries:            3072
 QoS Access Control Entries:                 3072
 Policy Based Routing ACEs:                  1024
 Netflow ACEs:                               1024
 Input Microflow policer ACEs:               256
 Output Microflow policer ACEs:              256
 Flow SPAN ACEs:                             256
 Tunnels:                                    256
 Control Plane Entries:                      512
 Input Netflow flows:                        8192
 Output Netflow flows:                      16384
 SGT/DGT entries:                            4096
 SGT/DGT Overflow entries:                   512
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.

デバイス#
```

show tech-support license

デバッグ出力を表示するには、特権 EXEC モードで **show license tech support** コマンドを使用します。

show tech-support license

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　特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show tech-support license** コマンドの出力例を示します。

```
デバイス# show tech-support license
Load for five secs: 5%/0%; one minute: 7%; five minutes: 6%
No time source, 12:36:46.732 EDT Tue Jul 17 2018


------------------ show clock ------------------

Load for five secs: 5%/0%; one minute: 7%; five minutes: 6%
No time source, 12:36:46.733 EDT Tue Jul 17 2018

12:36:46.733 EDT Tue Jul 17 2018


------------------ show version ------------------

Load for five secs: 5%/0%; one minute: 7%; five minutes: 6%
No time source, 12:36:46.734 EDT Tue Jul 17 2018
Cisco IOS XE Software, Version BLD_V169_THROTTLE_LATEST_20180712_092155_2
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
Experimental Version 16.9.20180712:083903
[v169_throttle-/scratch/mcpre/BLD-BLD_V169_THROTTLE_LATEST_20180712_092155 143]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 12-Jul-18 06:52 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
!
!
!
```

関連コマンド

コマンド	説明
show license all	権限付与情報を表示します。
show license status	ライセンスのコンプライアンスステータスを表示します。
show license summary	すべてのアクティブなライセンスの要約を表示します。

コマンド	説明
show license udi	UDI を表示します。
show license usage	ライセンス使用情報を表示します。

show tech-support platform evpn_vxlan

テクニカルサポートに使用するイーサネット VPN（EVPN）Virtual Extensible LAN（VXLAN）関連のプラットフォーム情報を表示するには、特権 EXEC モードで **show tech-support platform evpn_vxlan** コマンドを使用します。

show tech-support platform evpn_vxlan switch *switch-number*

構文の説明

switch *switch-number*	指定されたスイッチに関する情報を表示します。有効な値は 1 ～ 9 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 16.11.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support platform evpn_vxlan switch 1 | redirect flash:***filename*）。

例

次に、**show tech-support platform evpn_vxlan** コマンドの出力例を示します。

```
Device# show tech-support platform evpn_vxlan switch 1
.
.
.
    "show clock"
    "show version"
    "show running-config"switch no: 1


----- sh sdm prefer -----

Showing SDM Template Info

This is the Advanced template.
  Number of VLANs:                                4094
  Unicast MAC addresses:                          32768
  Overflow Unicast MAC addresses:                 512
  L2 Multicast entries:                           4096
  Overflow L2 Multicast entries:                  512
```

```
  L3 Multicast entries:                                4096
  Overflow L3 Multicast entries:                       512
  Directly connected routes:                           16384
  Indirect routes:                                     7168
  STP Instances:                                       4096
  Security Access Control Entries:                     3072
  QoS Access Control Entries:                          2560
  Policy Based Routing ACEs:                           1024
  Netflow ACEs:                                        768
  Flow SPAN ACEs:                                      512
  Tunnels:                                             256
  LISP Instance Mapping Entries:                       256
  Control Plane Entries:                               512
  Input Netflow flows:                                 8192
  Output Netflow flows:                                16384
  SGT/DGT (or) MPLS VPN entries:                       4096
  SGT/DGT (or) MPLS VPN Overflow entries:              512
  Wired clients:                                       2048
  MACSec SPD Entries:                                  256
  MPLS L3 VPN VRF:                                     127
  MPLS Labels:                                         2048
  MPLS L3 VPN Routes VRF Mode:                         7168
  MPLS L3 VPN Routes Prefix Mode:                      3072
  MVPN MDT Tunnels:                                    256
  L2 VPN EOMPLS Attachment Circuit:                    256
  MAX VPLS Bridge Domains :                            64
  MAX VPLS Peers Per Bridge Domain:                    8
  MAX VPLS/VPWS Pseudowires :                          256
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.
* values can be modified by sdm cli.


----- show platform software fed switch 1 ifm interfaces nve -----



----- show platform software fed switch 1 ifm interfaces efp -----



----- show platform software fed switch 1 matm macTable -----


Total Mac number of addresses:: 0
*a_time=aging_time(secs)  *e_time=total_elapsed_time(secs)
Type:
MAT_DYNAMIC_ADDR           0x1  MAT_STATIC_ADDR            0x2  MAT_CPU_ADDR
    0x4  MAT_DISCARD_ADDR           0x8
MAT_ALL_VLANS             0x10  MAT_NO_FORWARD            0x20  MAT_IPMULT_ADDR
   0x40  MAT_RESYNC                0x80
MAT_DO_NOT_AGE           0x100  MAT_SECURE_ADDR          0x200  MAT_NO_PORT
  0x400  MAT_DROP_ADDR            0x800
MAT_DUP_ADDR            0x1000  MAT_NULL_DESTINATION    0x2000  MAT_DOT1X_ADDR
 0x4000  MAT_ROUTER_ADDR         0x8000
MAT_WIRELESS_ADDR      0x10000  MAT_SECURE_CFG_ADDR    0x20000  MAT_OPQ_DATA_PRESENT
0x40000  MAT_WIRED_TUNNEL_ADDR  0x80000
MAT_DLR_ADDR          0x100000  MAT_MRP_ADDR          0x200000  MAT_MSRP_ADDR
0x400000  MAT_LISP_LOCAL_ADDR   0x800000
```

```
MAT_LISP_REMOTE_ADDR 0x1000000  MAT_VPLS_ADDR        0x2000000
Device#
```

出力フィールドの意味は自明です。

関連コマンド

コマンド	説明
show tech-support platform	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。

show tech-support platform fabric

スイッチファブリックに関する情報を表示するには、特権 EXEC モードで **show tech-support platform fabric** コマンドを使用します。

show tech-support platform fabric [{**display-cli** | **vrf** *vrf-name* {**ipv4 display-cli** | **ipv6 display-cli** | **source instance-id** *instance-id* {**ipv4** *ip-address*/*ip-prefix* | **ipv6** *ipv6-address*/*ipv6-prefix* | **mac** *mac-address*} {**dest instance-id** *instance-id* } {**ipv4** *ip-address*/*ip-prefix* | **ipv6** *ipv6-address*/*ipv6-prefix* | **mac** *mac-address*} [{**display-cli**}]}}]

構文の説明

display-cli	（任意）このコマンドの出力で使用可能な show コマンドのリストを表示します。
vrf *vrf-name*	（任意）指定した Virtual Routing and Forwarding（VRF）インスタンスのファブリック関連情報を表示します。
ipv4 *ip-address*/*ip-prefix*	（任意）送信元または宛先 IP VRF のファブリック関連情報を表示します。
ipv6 *ipv6-address*/*ipv6-prefix*	（任意）送信元または宛先 IPv6 VRF のファブリック関連情報を表示します。
source	（任意）送信元 VRF のファブリック関連情報を表示します。
instance-id *instance-id*	（任意）送信元のエンドポイント識別子（EID）に関する情報を表示します。

mac *mac-address*	（任意）レイヤ2拡張展開の送信元および宛先 MAC VRF のファブリック関連情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

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

使用上のガイドライン

このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support platform fabric | redirect flash:***filename*）。

このコマンドの出力には、一連のコマンドとその出力が表示されます。これらのコマンドは、プラットフォームによって異なる場合があります。

例

次に、**show tech-support platform fabric vrf source instance-id ipv4 dest instance-id ipv4** コマンドの出力例を示します。

```
Device# show tech-support platform fabric vrf DEFAULT_VN source instance-id
4098 ipv4 10.1.1.1/32 dest instance-id 4098 ipv4 10.12.12.12/32

.
.
.
-----show ip lisp eid-table vrf DEFAULT_VN forwarding  eid remote 10.12.12.12-----


Prefix                 Fwd action  Locator status bits   encap_iid
10.12.12.12/32         encap       0x00000001            N/A
  packets/bytes       1/576
  path list 7F44EEC2C188, 4 locks, per-destination, flags 0x49 [shble, rif, hwcn]
    ifnums:
      LISP0.4098(78): 192.0.2.2
    1 path
      path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
        nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2
7F44F8E86CE8
    1 output chain
      chain[0]: IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
                IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378


-----show lisp instance-id 4098 ipv4 map-cache-----


LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries

0.0.0.0/0, uptime: 02:46:01, expires: never, via static-send-map-request
  Encapsulating to proxy ETR
10.1.1.0/24, uptime: 02:46:01, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
  Locator  Uptime    State      Pri/Wgt     Encap-IID
```

```
  192.0.2.2  02:45:54  up          10/10        -


-----show lisp instance-id 4098 ipv4  map-cache detail-----


LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries

0.0.0.0/0, uptime: 02:46:01, expires: never, via static-send-map-request
  Sources: static-send-map-request
  State: send-map-request, last modified: 02:46:01, map-source: local
  Exempt, Packets out: 2(676 bytes) (~ 02:45:38 ago)
  Configured as EID address space
  Encapsulating to proxy ETR
101.1.0/24, uptime: 02:46:01, expires: never, via dynamic-EID, send-map-request
  Sources: NONE
  State: send-map-request, last modified: 02:46:01, map-source: local
  Exempt, Packets out: 0(0 bytes)
  Configured as EID address space
  Configured as dynamic-EID address space
  Encapsulating dynamic-EID traffic
  Encapsulating to proxy ETR
10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 02:45:54, map-source: 10.0.1.2
  Idle, Packets out: 1(576 bytes) (~ 02:45:38 ago)
  Locator  Uptime    State      Pri/Wgt     Encap-IID
  192.0.2.2  02:45:54  up          10/10        -
    Last up-down state change:         02:45:54, state change count: 1
    Last route reachability change:    02:45:54, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            02:45:54 (rtt 1ms)


-----show lisp instance-id 4098 ipv4 map-cache  10.12.12.12/32-----


LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries

10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 02:45:54, map-source: 10.0.1.2
  Idle, Packets out: 1(576 bytes) (~ 02:45:38 ago)
  Locator  Uptime    State      Pri/Wgt     Encap-IID
  192.0.2.2  02:45:54  up          10/10        -
    Last up-down state change:         02:45:54, state change count: 1
    Last route reachability change:    02:45:54, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            02:45:54 (rtt 1ms)


-----show ip cef vrf DEFAULT_VN 10.12.12.12/32 internal-----


10.12.12.12/32, epoch 1, flags [sc, lisp elig], refcnt 6, per-destination sharing
  sources: LISP, IPL
  feature space:
    Broker: linked, distributed at 1st priority
  subblocks:
    SC owned,sourced: LISP remote EID - locator status bits 0x00000001
    LISP remote EID: 1 packets 576 bytes fwd action encap, cfg as EID space
    LISP source path list
```

```
      path list 7F44EEC2C188, 4 locks, per-destination, flags 0x49 [shble, rif, hwcn]
        ifnums:
          LISP0.4098(78): 192.0.2.2
        1 path
          path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
            nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2
 7F44F8E86CE8
        1 output chain
          chain[0]: IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
                    IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378
      Dependent covered prefix type LISP, cover 0.0.0.0/0
    2 IPL sources [no flags]
  ifnums:
    LISP0.4098(78): 192.0.2.2
  path list 7F44EEC2C188, 3 locks, per-destination, flags 0x49 [shble, rif, hwcn]
    path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
      nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2
7F44F8E86CE8
  output chain:
    PushCounter(LISP:10.12.12.12/32) 7F44F3C8B8D8
    IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
    IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378
switch no: 1
.
.
.

Device# show tech-support platform fabric vrf Campus_VN source instance-id 8189
mac 00b7.7128.00a1 dest instance-id 8189 mac 00b7.7128.00a0   | i show

------------------ show clock ------------------
------------------ show version ------------------
------------------ show running-config ------------------
------------------ show device-tracking database ------------------
------------------ show lisp site ------------------
-------------------- show mac address-table address 00B7.7128.00A0-----
-------------------- show ip arp vrf Campus_VN-----
Device#
```

出力フィールドの意味は自明です。

関連コマンド

コマンド	説明
show tech-support platform	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。

show tech-support platform igmp_snooping

グループに関する Internet Group Management Protocol（IGMP）スヌーピング情報を表示するには、特権 EXEC モードで **show tech-support platform igmp_snooping** コマンドを使用します。

show tech-support platform igmp_snooping [{**Group_ipAddr** *ipv4-address* | [{**vlan** *vlan-ID*}]}]

構文の説明

Group_ipAddr	（任意）指定したグループアドレスに関するスヌーピング情報を表示します。
ipv4-address	（任意）グループの IPv4 アドレス。
vlan *vlan-ID*	（任意）IGMP スヌーピング VLAN情報を表示します。有効な値は 1 ～ 4094 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 16.11.1	このコマンドが導入されました。

このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします（たとえば、**show tech-support platform igmp_snooping | redirect flash:***filename*）。

例

次に、**show tech-support platform igmp_snooping** コマンドの出力例を示します。

```
Device# show tech-support platform igmp_snooping GroupIPAddr 226.6.6.6 vlan

.
.
.
----- show ip igmp snooping groups | i 226.6.6.6 -----

5         226.6.6.6               user                    Gi1/0/8, Gi1/0/27, Gi1/0/28,



----- show ip igmp snooping groups count -----

Total number of groups:   2


----- show ip igmp snooping mrouter -----


Vlan    ports
----    -----
  23    Router
  24    Router
  25    Router


----- show ip igmp snooping querier -----
```

```
Vlan      IP Address              IGMP Version   Port
-----------------------------------------------------------
23        10.1.1.1                v2             Router
24        10.1.2.1                v2             Router
25        10.1.3.1                v2             Router


----- show ip igmp snooping vlan 5 -----


Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
Global PIM Snooping          : Disabled
IGMPv3 snooping              : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 5:
--------
IGMP snooping                       : Enabled
Pim Snooping                        : Disabled
IGMPv2 immediate leave              : Disabled
Explicit host tracking              : Enabled
Multicast router learning mode      : pim-dvmrp
CGMP interoperability mode          : IGMP_ONLY
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000


----- show ip igmp snooping groups vlan 5 -----

Vlan      Group                   Type        Version     Port List
------------------------------------------------------------------------------
5         226.6.6.6               user                    Gi1/0/8, Gi1/0/27, Gi1/0/28,

                                                          Gi2/0/7, Gi2/0/8, Gi2/0/27,
                                                          Gi2/0/28
5         238.192.0.1             user                    Gi2/0/28


----- show platform software fed active ip igmp snooping vlan 5 -----


Vlan 5
---------
 IGMPSN Enabled  : On
 PIMSN Enabled   : Off
 Flood Mode      : On
 I-Mrouter       : Off
 Oper State      : Up
 STP TCN Flood   : Off
 Routing Enabled : Off
 PIM Enabled     : Off
 PVLAN           : No
```

```
 In Retry        : 0x0
 L3mcast Adj      :
 Mrouter PortQ   :
 Flood PortQ     :


----- show platform software fed active ip igmp snooping groups | begin 226.6.6.6 -----

Vlan:5 Group:226.6.6.6
---------------------------------
Member ports   :
CAPWAP ports   :
Host Type Flags: 0
Failure Flags  : 0
DI handle      : 0x7f11151cbad8
REP RI handle  : 0x7f11151cc018
SI handle      : 0x7f11151cd198
HTM handle     : 0x7f11151cd518

si hdl : 0x7f11151cd198 rep ri hdl : 0x7f11151cc018 di hdl :  0x7f11151cbad8 htm hdl :
0x7f11151cd518
.
.
.
Device#
```

出力フィールドの意味は自明です。

関連コマンド

コマンド	説明
ip igmp snooping	IGMP スヌーピングをグローバルまたはインターフェイスで有効にします。
show ip igmp snooping	デバイスの IGMP スヌーピング設定を表示します。
show tech-support platform	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。

show tech-support platform mld_snooping

グループに関するマルチキャストリスナー検出（MLD）スヌーピング情報を表示するには、特権 EXEC モードで **show tech-support platform mld_snooping** コマンドを使用します。

show tech-support platform mld_snooping [{**Group_ipv6Addr** *ipv6-address*}][{**vlan** *vlan-ID*}]

構文の説明

Group_ipv6Addr	（任意）指定したグループアドレスに関するスヌーピング情報を表示します。

ipv6-address	（任意）グループの IPv6 アドレス。
vlan *vlan-ID*	（任意）MLD スヌーピング VLAN情報を表示します。有効な値は 1 ～ 4094 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 16.11.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support platform mld_snooping | redirect flash:***filename*）。

例

次に、**show tech-support platform mld_snooping** コマンドの出力例を示します。

```
Device# show tech-support platform mld_snooping GroupIPv6Addr FF02::5:1

.
.
.
------------------ show running-config ------------------


Building configuration...

Current configuration : 11419 bytes
!
! Last configuration change at 09:17:04 UTC Thu Sep 6 2018
!
version 16.10
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
no platform punt-keepalive disable-kernel-core
!
hostname Switch
!
!
vrf definition Mgmt-vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
no aaa new-model
switch 1 provision ws-c3650-12x48uq
!
```

```
!
!
!
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact
email address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "profile-1"
  active
  destination transport-method http
  no destination transport-method email
!
!
!
!
!
ip admission watch-list expiry-time 0
!
!
!
login on-success log
!
!
!
!
!
no device-tracking logging theft
!
crypto pki trustpoint TP-self-signed-559433368
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-559433368
 revocation-check none
 rsakeypair TP-self-signed-559433368
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-559433368
 certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 35353934 33333336 38301E17 0D313531 32303331 32353432
  325A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3535 39343333
  33363830 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  AD8C9C3B FEE7FFC8 986837D2 4C126172 446C3C53 E040F798 4BA61C97 7506FDCE
  46365D0A E47E3F4F C774CA5B 73E2A8DD B72A2E98 C66DB196 94E8150F 0B669CF6
  AA5BC4CD FC2E02F6 FE08B17F 0164FC19 7DC84ABB C99D91D6 398233FF 814EF6DA
  6DC8FC20 CA12C0D6 1CB28EDA 6ADD6DFA 7E3E8281 4A189A9A AA44FCC0 BA9BD8A5
  02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
  23041830 16801448 668D668E C92914BB 69E9BA64 F61228DE 132E2030 1D060355
  1D0E0416 04144866 8D668EC9 2914BB69 E9BA64F6 1228DE13 2E20300D 06092A86
  4886F70D 01010505 00038181 0000F1D3 3DD1E5F1 EB714A95 D5819933 CAD0C943
  59927D55 9D70CAD0 D64830EB D54380AD D2B5B613 F8AF7A5B 1F801134 246F760D
  5E5515DB D098304F 5086F6CE 88E8B576 F6B93A88 F458FDCF 91A42D7E FA741908
  5C892D78 600FB655 E6C5A4D0 6C1F1B9A 3AECA550 E3DC0881 01C4D004 7AB65BC3
  88CF24DE DAA19474 51B535A5 0C
   quit
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
```

```
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
   quit
!
!
!
diagnostic bootup level minimal
diagnostic monitor syslog
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
!
redundancy
 mode sso
!
!
!
!
!
!
class-map match-any system-cpp-police-topology-control
  description Topology control
class-map match-any system-cpp-police-sw-forward
  description Sw forwarding, L2 LVX data, LOGGING
class-map match-any system-cpp-default
  description EWLC control, EWLC data, Inter FED
class-map match-any system-cpp-police-sys-data
  description Learning cache ovfl, High Rate App, Exception, EGR Exception, NFL SAMPLED
 DATA, RPF Failed
class-map match-any AutoQos-4.0-RT1-Class
 match dscp ef
 match dscp cs6
class-map match-any system-cpp-police-punt-webauth
  description Punt Webauth
class-map match-any AutoQos-4.0-RT2-Class
 match dscp cs4
 match dscp cs3
 match dscp af41
class-map match-any system-cpp-police-l2lvx-control
```

```
  description L2 LVX control packets
class-map match-any system-cpp-police-forus
  description Forus Address resolution and Forus traffic
class-map match-any system-cpp-police-multicast-end-station
  description MCAST END STATION
class-map match-any system-cpp-police-multicast
  description Transit Traffic and MCAST Data
class-map match-any system-cpp-police-l2-control
  description L2 control
class-map match-any system-cpp-police-dot1x-auth
  description DOT1X Auth
class-map match-any system-cpp-police-data
  description ICMP redirect, ICMP_GEN and BROADCAST
class-map match-any system-cpp-police-stackwise-virt-control
  description Stackwise Virtual
class-map match-any system-cpp-police-control-low-priority
  description ICMP redirect and general punt
class-map match-any system-cpp-police-wireless-priority1
  description Wireless priority 1
class-map match-any system-cpp-police-wireless-priority2
  description Wireless priority 2
class-map match-any system-cpp-police-wireless-priority3-4-5
  description Wireless priority 3,4 and 5
class-map match-any non-client-nrt-class
class-map match-any system-cpp-police-routing-control
  description Routing control and Low Latency
class-map match-any system-cpp-police-protocol-snooping
  description Protocol snooping
class-map match-any system-cpp-police-dhcp-snooping
  description DHCP snooping
class-map match-any system-cpp-police-system-critical
  description System Critical and Gold Pkt
!
policy-map system-cpp-policy
 class system-cpp-police-data
  police rate 200 pps
 class system-cpp-police-routing-control
  police rate 500 pps
 class system-cpp-police-control-low-priority
 class system-cpp-police-wireless-priority1
 class system-cpp-police-wireless-priority2
 class system-cpp-police-wireless-priority3-4-5
policy-map port_child_policy
 class non-client-nrt-class
  bandwidth remaining ratio 10
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 no ip address
 speed 1000
 negotiation auto
!
interface GigabitEthernet1/0/1
 switchport mode access
 macsec network-link
```

```
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/0/3
!
interface TenGigabitEthernet1/1/1
!
interface TenGigabitEthernet1/1/2
!
interface TenGigabitEthernet1/1/3
!
interface TenGigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
ip access-list extended AutoQos-4.0-wlan-Acl-Bulk-Data
 permit tcp any any eq 22
 permit tcp any any eq 465
 permit tcp any any eq 143
 permit tcp any any eq 993
 permit tcp any any eq 995
 permit tcp any any eq 1914
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 permit tcp any any eq smtp
 permit tcp any any eq pop3
ip access-list extended AutoQos-4.0-wlan-Acl-MultiEnhanced-Conf
 permit udp any any range 16384 32767
 permit tcp any any range 50000 59999
ip access-list extended AutoQos-4.0-wlan-Acl-Scavanger
 permit tcp any any range 2300 2400
 permit udp any any range 2300 2400
 permit tcp any any range 6881 6999
 permit tcp any any range 28800 29100
 permit tcp any any eq 1214
 permit udp any any eq 1214
 permit tcp any any eq 3689
 permit udp any any eq 3689
 permit tcp any any eq 11999
ip access-list extended AutoQos-4.0-wlan-Acl-Signaling
 permit tcp any any range 2000 2002
 permit tcp any any range 5060 5061
 permit udp any any range 5060 5061
ip access-list extended AutoQos-4.0-wlan-Acl-Transactional-Data
 permit tcp any any eq 443
 permit tcp any any eq 1521
 permit udp any any eq 1521
 permit tcp any any eq 1526
 permit udp any any eq 1526
 permit tcp any any eq 1575
 permit udp any any eq 1575
 permit tcp any any eq 1630
 permit udp any any eq 1630
 permit tcp any any eq 1527
 permit tcp any any eq 6200
 permit tcp any any eq 3389
 permit tcp any any eq 5985
```

```
 permit tcp any any eq 8080
!
!
!
ipv6 access-list preauth_ipv6_acl
 permit udp any any eq domain
 permit tcp any any eq domain
 permit icmp any any nd-ns
 permit icmp any any nd-na
 permit icmp any any router-solicitation
 permit icmp any any router-advertisement
 permit icmp any any redirect
 permit udp any eq 547 any eq 546
 permit udp any eq 546 any eq 547
 deny ipv6 any any
!
control-plane
 service-policy input system-cpp-policy
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
line vty 5 15
 login
!
!
mac address-table notification mac-move
!
!
!
!
!
end


-----show switch | Include Ready-----

*1       Active   188b.9dfc.eb00     1      V00     Ready


----- show ipv6 mld snooping address | i FF02::5:1 -----

Vlan      Group                    Type        Version     Port List
------------------------------------------------------------------------------
123       FF02::5:1                mld         v2          Gi2/0/1

Device#
```

出力フィールドの意味は自明です。

関連コマンド

コマンド	説明
ipv6 mld snooping	MLDv2 プロトコルスヌーピングをグローバルに有効にします。
show ipv6 mld snooping	MLDv2 スヌーピング情報を表示します。

コマンド	説明
show tech-support platform	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。

show tech-support platform layer3

レイヤ 3 プラットフォーム転送情報を表示するには、特権 EXEC モードで **show tech-support platform layer3** コマンドを使用します。

show tech-support platform layer3 {**multicast Group_ipAddr** *ipv4-address* **switch** *switch-number* **srcIP** *ipv4-address* | **unicast** {**dstIP** *ipv4-address* **srcIP** *ipv4-address* | **vrf** *vrf-name* **destIP** *ipv4-address* **srcIP** *ipv4-address*}}

構文の説明

multicast	マルチキャスト情報を表示します。
Group_ipv6Addr *ipv4-address*	指定したマルチキャストグループアドレスに関する情報を表示します。
switch *switch-number*	指定したスイッチに関する情報を表示します。有効な値は 1 ～ 9 です。
srcIP *ipv4-address*	指定した送信元アドレスに関する情報を表示します。
unicast	ユニキャスト関連の情報を表示します。
dstIP *ipv4-address*	指定した宛先アドレスに関する情報を表示します。
vrf *vrf-name*	ユニキャスト関連の Virtual Routing and Forwarding（VRF）情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support platform layer3 multicast group 224.1.1.1 switch 1 srcIP 10.10.0.2 | redirect flash:***filename*）。

例

次に、**show tech-support platform layer3 multicast group** コマンドの出力例を示します。

```
Device# show tech-support platform layer3 multicast group_ipAddr 224.1.1.1
switch 1 srcIp 10.10.0.2

.
.
.
destination IP: 224.1.1.1
source IP: 10.10.0.2
switch no: 1


----- show ip mroute 224.1.1.1 10.10.0.2 -----


IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group, c - PFP-SA cache created entry
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(10.10.0.2, 224.1.1.1), 00:00:22/00:02:37, flags: LFT
  Incoming interface: GigabitEthernet1/0/10, RPF nbr 0.0.0.0, Registering
  Outgoing interface list:
    Vlan20, Forward/Sparse, 00:00:22/00:02:37, A



----- show ip mfib 224.1.1.1 10.10.0.2 -----


Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
                ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
                MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
                MS  - MoFRR  Entry in Sync, MC - MoFRR entry in MoFRR Client.
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept, A2 - Accept backup,
                RA2 - MRIB Accept backup, MA2 - MFIB Accept backup
```

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
Default
 (10.10.0.2,224.1.1.1) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 1/1/0
   HW Forwarding:   NA/NA/NA/NA, Other: NA/NA/NA
   GigabitEthernet1/0/10 Flags: A
   Vlan20 Flags: F IC
     Pkts: 0/0
   Tunnel0 Flags: F
     Pkts: 0/0



----- show platform software fed switch 1 ip multicast interface summary -----

Multicast Interface database

VRF  Interface                IF ID               PIM Status  State               RI
Handle           SVI
------------------------------------------------------------------------------------------------------
0    GigabitEthernet1/0/10    0x000000000000005f  enabled     0x0000000000000010
0x00007fb414b1f108  false
0    Vlan20                   0x0000000000000060  enabled     0x0000000000000010
0x00007fb414b31a98  true



----- show platform software fed switch 1 ip multicast groups summary -----

Multicast Groups database

Mvrf_id: 0  Mroute: (*, 224.0.1.40/32)  Flags:  C IC
  Htm: 0x00007fb414b23ce8  Si: 0x00007fb414b23a08  Di: 0x00007fb414b240e8  Rep_ri:
  0x00007fb414b245f8

Mvrf_id: 0  Mroute: (*, 224.0.0.0/4)  Flags:  C
  Htm: 0x00007fb4143549e8  Si: 0x00007fb414b20a48  Di: 0x00007fb414b1fe78  Rep_ri:
  0x00007fb414b20428

Mvrf_id: 0  Mroute: (*, 224.1.1.1/32)  Flags:  C IC
  Htm: 0x00007fb414b2cc98  Si: 0x00007fb414b2b678  Di: 0x00007fb414b2ab98  Rep_ri:
  0x00007fb414b2b0c8

Mvrf_id: 0  Mroute: (10.10.0.2, 224.1.1.1/32)  Flags:  IC
  Htm: 0x00007fb414b2f348  Si: 0x00007fb414b321d8  Di: 0x00007fb414b2dba8  Rep_ri:
  0x00007fb414b30ed8



----- show platform software fed switch 1 ip multicast groups count -----


Total Number of entries:4



----- show platform software fed switch 1 ip multicast groups 224.1.1.1/32
source 10.10.0.2 detail -----


MROUTE ENTRY vrf 0 (10.10.0.2, 224.1.1.1/32)
```

```
  HW Handle: 140411418055080 Flags:  IC
RPF interface: GigabitEthernet1/0/10(95)):
  HW Handle:140411418055080 Flags:A
Number of OIF: 3
Flags: 0x4   Pkts : 0
OIF Details:
     Tunnel0      Adj: 0xf8000636    F
     Vlan20      Adj: 0xf8000601  F IC
     GigabitEthernet1/0/10        A
Htm: 0x7fb414b2f348  Si: 0x7fb414b321d8  Di: 0x7fb414b2dba8  Rep_ri: 0x7fb414b30ed8


DI details
----------
Handle:0x7fb414b2dba8 Res-Type:ASIC_RSC_DI Res-Switch-Num:255 Asic-Num:255
Feature-ID:AL_FID_L3_
MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x538e
mtu_index/l3u_ri_index0:0x0  index1:0x538e  mtu_index/l3u_ri_index1:0x0
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00
00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
----------------------------------------

Destination Index (DI) [0x538e]
portMap = 0x00000000                0
cmi1 = 0x385
rcpPortMap = 0

al_rsc_cmi
CPU Map Index (CMI) [0x385]
ctiLo0 = 0x9
ctiLo1 = 0
ctiLo2 = 0
cpuQNum0 = 0x9e
cpuQNum1 = 0
cpuQNum2 = 0
npuIndex = 0
strip_seg = 0x0
copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
----------------------------------------

Destination Index (DI) [0x538e]
portMap = 0x00000000                0
cmi1 = 0x385
rcpPortMap = 0

al_rsc_cmi
CPU Map Index (CMI) [0x385]
ctiLo0 = 0x9
ctiLo1 = 0
ctiLo2 = 0
cpuQNum0 = 0x9e
cpuQNum1 = 0
cpuQNum2 = 0
npuIndex = 0
strip_seg = 0x0
copy_seg = 0x0

============================================================
```

```
RI details
----------
Handle:0x7fb414b30ed8 Res-Type:ASIC_RSC_RI_REP Res-Switch-Num:255 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x5
mtu_index/l3u_ri_index0:0x0
index1:0x5  mtu_index/l3u_ri_index1:0x0
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00
00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
----------------------------------------

Detailed Resource Information (ASIC# 1)
----------------------------------------


============================================================

SI details
----------
Handle:0x7fb414b321d8 Res-Type:ASIC_RSC_SI_STATS Res-Switch-Num:255 Asic-Num:255
Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x4004
mtu_index/l3u_ri_index0:
0x0  sm handle 0:0x7fb414b2df98  index1:0x4004  mtu_index/l3u_ri_index1:0x0
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00
00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
----------------------------------------
Detailed Resource Information (ASIC# 1)
----------------------------------------

============================================================

HTM details
-----------
Handle:0x7fb414b2f348 Res-Type:ASIC_RSC_HASH_TCAM Res-Switch-Num:0 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_SG ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: handle0:0x7fb414b2f558
Detailed Resource Information (ASIC# 0)
----------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x7fb414b2f558)

KEY - src_addr:10.10.0.2 starg_station_index: 16387
MASK - src_addr:0.0.0.0 starg_station_index: 0
AD: use_starg_match: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0 rpf_valid: 1 rpf_le_ptr:
 0
afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1 cpp_type: 0 dest_mod_index: 0
rp_index:
0 priority: 5 rpf_le: 36 station_index: 16388 capwap_mgid_present: 0 mgid 0

============================================================
```

次に、**show tech-support platform layer3 unicast vrf** コマンドの出力例を示します。

```
Device# show tech-support platform layer3 unicast vrf vr1 dstIP 10.0.0.20
srcIP 10.0.0.10
```

```
.
.
.
destination IP: 10.0.0.20
source IP: 10.0.0.10
vrf name :

Switch/Stack Mac Address : 5006.ab89.0280 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------------------------------
*1       Active   5006.ab89.0280     1      V02     Ready




----- show switch -------



10.0.0.10 -> 10.0.0.20 =>IP adj out of GigabitEthernet1/0/7, addr 10.0.0.20


----- show ip cef    exact-route platform  10.0.0.10 10.0.0.20 -----



nexthop is 10.0.0.20


Protocol Interface                 Address
IP       GigabitEthernet1/0/7      10.0.0.20(8)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 0
                                   Encap length 14
                                   00211BFDE6495006AB8902C00800
                                   L2 destination address byte offset 0
                                   L2 destination address byte length 6
                                   Link-type after encap: ip
                                   ARP


----- show adjacency 10.0.0.20 detail -----



Routing entry for 10.0.0.0/24
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via GigabitEthernet1/0/7
      Route metric is 0, traffic share count is 1


----- show ip route   10.0.0.20 -----



10.0.0.20/32, epoch 3, flags [attached]
  Adj source: IP adj out of GigabitEthernet1/0/7, addr 10.0.0.20 FF90E67820
    Dependent covered prefix type adjfib, cover 10.0.0.0/24
```

```
  attached to GigabitEthernet1/0/7


----- show ip cef   10.0.0.20 detail -----


ip prefix: 10.0.0.20/32


Forwarding Table

10.0.0.20/32 -> OBJ_ADJACENCY (29), urpf: 30
Connected Interface: 31
Prefix Flags: Directly L2 attached
OM handle: 0x10205416d8


----- show platform software ip switch 1 R0 cef prefix  10.0.0.20/32 detail -----


OBJ_ADJACENCY found: 29


Number of adjacency objects: 5

Adjacency id: 0x1d (29)
  Interface: GigabitEthernet1/0/7, IF index: 31, Link Type: MCP_LINK_IP
  Encap: 0:21:1b:fd:e6:49:50:6:ab:89:2:c0:8:0
  Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
  Flags: no-l3-inject
  Incomplete behavior type: None
  Fixup: unknown
  Fixup_Flags_2: unknown
  Nexthop addr: 10.0.0.20
  IP FRR MCP_ADJ_IPFRR_NONE 0
  OM handle: 0x1020541348



----- show platform software adjacency switch 1 R0 index 29 -----


Forwarding Table

10.0.0.20/32 -> OBJ_ADJACENCY (29), urpf: 30
Connected Interface: 31
Prefix Flags: Directly L2 attached
aom id: 393, HW handle: (nil) (created)


----- show platform software ip switch 1 F0 cef prefix  10.0.0.20/32 detail -----


OBJ_ADJACENCY found: 29


Number of adjacency objects: 5
```

```
Adjacency id: 0x1d (29)
  Interface: GigabitEthernet1/0/7, IF index: 31, Link Type: MCP_LINK_IP
  Encap: 0:21:1b:fd:e6:49:50:6:ab:89:2:c0:8:0
  Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
  Flags: no-l3-inject
  Incomplete behavior type: None
  Fixup: unknown
  Fixup_Flags_2: unknown
  Nexthop addr: 10.0.0.20
  IP FRR MCP_ADJ_IPFRR_NONE 0
  aom id: 391, HW handle: (nil) (created)



----- show platform software adjacency switch 1 F0 index 29 -----



found aom id: 391

Object identifier: 391
  Description: adj 0x1d, Flags None
  Status: Done, Epoch: 0, Client data: 0xc6a747a8



----- show platform software object-manager switch 1 F0 object 391 -----


Object identifier: 66
  Description: intf GigabitEthernet1/0/7, handle 31, hw handle 31, HW dirty: NONE AOM
dirty NONE
  Status: Done



----- show platform software object-manager switch 1 F0 object 391  parents -----


Object identifier: 393
  Description: PREFIX 10.0.0.20/32 (Table id 0)
  Status: Done
.
.
.
```

出力フィールドの意味は自明です。

関連コマンド

コマンド	説明
show tech-support platform	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。

show tech-support port

テクニカルサポートに使用するポート関連の情報を表示するには、特権 EXEC モードで **show tech-support port** コマンドを使用します。

show tech-support 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 モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

show tech-support port コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support port | redirect flash:***filename*）。

このコマンドの出力には次のコマンドが表示されます。

- **show clock**
- **show version**
- **show module**
- **show inventory**
- **show interface status**
- **show interface counters**
- **show interface counters errors**
- **show interfaces**
- **show interfaces capabilities**
- **show controllers**
- **show controllers utilization**
- **show idprom interface**
- **show controller ethernet-controller phy detail**
- **show switch**
- **show platform software fed switch active port summary**
- **show platform software fed switch ifm interfaces ethernet**
- **show platform software fed switch ifm mappings**

- **show platform software fed switch ifm mappings lpn**
- **show platform software fed switch ifm mappings gpn**
- **show platform software fed switch ifm mappings port-le**
- **show platform software fed switch ifm if-id**
- **show platform software fed switch active port if_id**

例

次に、**show tech-support port** コマンドの出力例を示します。

```
Device# show tech-support port
.
.
.
  ----- show controllers utilization -----

Port       Receive Utilization  Transmit Utilization
Gi1/0/1       0   0
Gi1/0/2       0   0
Gi1/0/3       0   0
Gi1/0/4       0   0
Gi1/0/5       0   0
Gi1/0/6       0   0
Gi1/0/7       0   0
Gi1/0/8       0   0
Gi1/0/9       0   0
Gi1/0/10       0   0
Gi1/0/11       0   0
Gi1/0/12       0   0
Gi1/0/13       0   0
Gi1/0/14       0   0
Gi1/0/15       0   0
Gi1/0/16       0   0
Gi1/0/17       0   0
Gi1/0/18       0   0
Gi1/0/19       0   0
Gi1/0/20       0   0
Gi1/0/21       0   0
Gi1/0/22       0   0
Gi1/0/23       0   0
Gi1/0/24       0   0
Gi1/0/25       0   0
Gi1/0/26       0   0
Gi1/0/27       0   0
Gi1/0/28       0   0
Gi1/0/29       0   0
Gi1/0/30       0   0
Gi1/0/31       0   0
Gi1/0/32       0   0
Gi1/0/33       0   0
Gi1/0/34       0   0
Gi1/0/35       0   0
Gi1/0/36       0   0
Te1/0/37       0   0
Te1/0/38       0   0
Te1/0/39       0   0
Te1/0/40       0   0
Te1/0/41       0   0
Te1/0/42       0   0
```

```
Te1/0/43        0    0
Te1/0/44        0    0
Te1/0/45        0    0
Te1/0/46        0    0
Te1/0/47        0    0
Te1/0/48        0    0
Te1/1/1        0    0
Te1/1/2        0    0
Te1/1/3        0    0
Te1/1/4        0    0

Total Ports : 52
Total Ports Receive Bandwidth Percentage Utilization  : 0
Total Ports Transmit Bandwidth Percentage Utilization : 0

Average Switch  Percentage Utilization : 0


----- show idprom interface Gi1/0/1 -----


*Sep  7 08:57:24.249:  No module is present
.
.
.
```

出力フィールドの意味は自明です。

show tech-support platform

テクニカルサポートに使用するプラットフォームに関する詳細情報を表示するには、特権EXECモードで **show tech-support platform** コマンドを使用します。

show tech-support platform

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、プラットフォーム固有のデバッグに使用されます。出力には、CPU使用率、Ternary Content Addressable Memory（TCAM）の使用率、容量、メモリ使用率など、プラットフォームに関する詳細情報が表示されます。

show tech-support platform コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support platform | redirect flash:***filename*）。

show tech-support platform コマンドの出力には、一連のコマンドとその出力が表示されます。これらのコマンドは、プラットフォームによって異なる場合があります。

例

次に、**show tech-support platform** コマンドの出力例を示します。

```
Device# show tech-support platform

.
.
.
------------------ show platform hardware capacity ------------------


Load Average
 Slot  Status  1-Min  5-Min 15-Min
1-RP0 Healthy   0.25   0.17   0.12

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
1-RP0 Healthy  3964428  2212476 (56%)  1751952 (44%)   3420472 (86%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
1-RP0    0   1.40   0.90   0.00  97.60   0.00   0.10   0.00
         1   2.00   0.20   0.00  97.79   0.00   0.00   0.00
         2   0.20   0.00   0.00  99.80   0.00   0.00   0.00
         3   0.79   0.19   0.00  99.00   0.00   0.00   0.00
         4   5.61   0.50   0.00  93.88   0.00   0.00   0.00
         5   2.90   0.40   0.00  96.70   0.00   0.00   0.00



 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                   IHQ       IQD       OHQ       OQD      RXBS      RXPS
  TXBS      TXPS      TRTL
------------------------------------------------------------------------------------------------

  Vlan1                         0         0         0         0         0         0
     0         0         0
* GigabitEthernet0/0            0     10179         0         0      2000         4
     0         0         0
  GigabitEthernet1/0/1          0         0         0         0         0         0
     0         0         0
  GigabitEthernet1/0/2          0         0         0         0         0         0
     0         0         0
  GigabitEthernet1/0/3          0         0         0         0         0         0
     0         0         0
  GigabitEthernet1/0/4          0         0         0         0         0         0
     0         0         0
  GigabitEthernet1/0/5          0         0         0         0         0         0
     0         0         0
  GigabitEthernet1/0/6          0         0         0         0         0         0
     0         0         0
  GigabitEthernet1/0/7          0         0         0         0         0         0
     0         0         0
  GigabitEthernet1/0/8          0         0         0         0         0         0
```

```
   0         0         0
GigabitEthernet1/0/9          0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/10         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/11         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/12         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/13         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/14         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/15         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/16         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/17         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/18         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/19         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/20         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/21         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/22         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/23         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/24         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/25         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/26         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/27         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/28         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/29         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/30         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/31         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/32         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/33         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/34         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/35         0         0         0         0         0         0
   0         0         0
GigabitEthernet1/0/36         0         0         0         0         0         0
   0         0         0
Te1/0/37                      0         0         0         0         0         0
   0         0         0
Te1/0/38                      0         0         0         0         0         0
   0         0         0
Te1/0/39                      0         0         0         0         0         0
   0         0         0
Te1/0/40                      0         0         0         0         0         0
```

```
     0          0          0
  Te1/0/41                        0          0          0          0          0          0
     0          0          0
  Te1/0/42                        0          0          0          0          0          0
     0          0          0
  Te1/0/43                        0          0          0          0          0          0
     0          0          0
  Te1/0/44                        0          0          0          0          0          0
     0          0          0
  Te1/0/45                        0          0          0          0          0          0
     0          0          0
  Te1/0/46                        0          0          0          0          0          0
     0          0          0
  Te1/0/47                        0          0          0          0          0          0
     0          0          0
  Te1/0/48                        0          0          0          0          0          0
     0          0          0
  Te1/1/1                         0          0          0          0          0          0
     0          0          0
  Te1/1/2                         0          0          0          0          0          0
     0          0          0
  Te1/1/3                         0          0          0          0          0          0
     0          0          0
  Te1/1/4                         0          0          0          0          0          0
     0          0          0
ASIC 0 Info
------------
ASIC 0 HASH Table 0 Software info:  FSE 0
 MAB 0: Unicast MAC addresses srip 0 1
 MAB 1: Unicast MAC addresses srip 0 1
 MAB 2: Unicast MAC addresses srip 0 1
 MAB 3: Unicast MAC addresses srip 0 1
 MAB 4: Unicast MAC addresses srip 0 1
 MAB 5: Unicast MAC addresses srip 0 1
 MAB 6: Unicast MAC addresses srip 0 1
 MAB 7: Unicast MAC addresses srip 0 1
ASIC 0 HASH Table 1 Software info:  FSE 0
 MAB 0: Unicast MAC addresses srip 0 1
 MAB 1: Unicast MAC addresses srip 0 1
 MAB 2: Unicast MAC addresses srip 0 1
 MAB 3: Unicast MAC addresses srip 0 1
 MAB 4: Unicast MAC addresses srip 0 1
 MAB 5: Unicast MAC addresses srip 0 1
 MAB 6: Unicast MAC addresses srip 0 1
 MAB 7: Unicast MAC addresses srip 0 1
ASIC 0 HASH Table 2 Software info:  FSE 1
 MAB 0: L3 Multicast entries srip 2 3
 MAB 1: L3 Multicast entries srip 2 3
 MAB 2: SGT_DGT         srip 0 1
 MAB 3: SGT_DGT         srip 0 1
 MAB 4: (null)          srip
 MAB 5: (null)          srip
 MAB 6: (null)          srip
 MAB 7: (null)          srip
.
.
.
```

出力フィールドの意味は自明です。

関連コマンド

コマンド	説明
show tech-support platform evpn_vxlan	EVPN-VXLAN 関連のプラットフォーム情報を表示します。
show tech-support platform fabric	スイッチファブリックに関する詳細情報を表示します。
show tech-support platform igmp_snooping	グループに関する IGMP スヌーピング情報を表示します。
show tech-support platform layer3	レイヤ3プラットフォーム転送情報を表示します。
show tech-support platform mld_snooping	グループに関する MLD スヌーピング情報を表示します。

show version

現在ロードされているソフトウェアの情報とハードウェアおよびデバイス情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show version command** を使用します。

```
show version
```

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが変更され、スタック内のすべてのスイッチの最新のリロード理由が出力に表示されるようになりました。
Cisco IOS XE 3.3SE	このコマンドが以下に実装されました。 Cisco Catalyst 3650 シリーズスイッチ

例：

```
Device# show version

Cisco IOS XE Software, Version BLD_POLARIS_DEV_LATEST_20180713_195337
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
Experimental Version 16.11.20180713:191831
[polaris_dev-/nobackup/mcpre/BLD-BLD_POLARIS_DEV_LATEST_20180713_195337 124]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Fri 13-Jul-18 17:11 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
```

```
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON
BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.66, engineering software
(D)

 --More--         Switch uptime is 14 hours, 23 minutes
Uptime for this control processor is 14 hours, 26 minutes
System returned to ROM by Power Failure or Unknown
System image file is "flash:packages.conf"
Last reload reason: Power Failure or Unknown



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

 --More--
Technology Package License Information:

------------------------------------------------------------------------------
Technology-package                                      Technology-package
Current                       Type                         Next reboot
------------------------------------------------------------------------------
ipservicesk9         Smart License                    ipservicesk9
None                 Subscription Smart License       None

cisco WS-C3650-48FQM (MIPS) processor (revision PP) with 829450K/6147K bytes of memory.
Processor board ID FDO2011V00A
1 Virtual Ethernet interface
198 Gigabit Ethernet interfaces
46 Ten Gigabit Ethernet interfaces
2 Forty Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
255037K bytes of Crash Files at crashinfo:.
150009K bytes of Crash Files at crashinfo-2:.
150009K bytes of Crash Files at crashinfo-3:.
 --More--         250456K bytes of Crash Files at crashinfo-5:.
3417161K bytes of Flash at flash:.
3544695K bytes of Flash at flash-2:.
3544695K bytes of Flash at flash-3:.
1609272K bytes of Flash at flash-5:.
0K bytes of WebUI ODM Files at webui:.
```

```
250456K bytes of Crash Files at crashinfo-4:.
1609272K bytes of Flash at flash-4:.

Base Ethernet MAC Address          : cc:46:d6:c5:2a:00
Motherboard Assembly Number        : 73-17734-02
Motherboard Serial Number          : FDO200608QX
Model Revision Number              : PP
Motherboard Revision Number        : 05
Model Number                       : WS-C3650-48FQM
System Serial Number               : FDO200608QX


Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
*    1 52    WS-C3650-48FQM     16.11.1           CAT3K_CAA-UNIVERSALK9 INSTALL
     2 58    WS-C3650-12X48UZ   16.11.1           CAT3K_CAA-UNIVERSALK9 INSTALL
     3 56    WS-C3650-12X48UR   16.11.1           CAT3K_CAA-UNIVERSALK9 INSTALL
     4 52    WS-C3650-48PD      16.11.1           CAT3K_CAA-UNIVERSALK9 INSTALL
     5 28    WS-C3650-24PS      16.11.1           CAT3K_CAA-UNIVERSALK9 INSTALL


Switch 02
---------
Switch uptime                      : 14 hours, 26 minutes

Base Ethernet MAC Address          : 58:97:bd:59:58:00
Motherboard Assembly Number        : 73-100820-03
Motherboard Serial Number          : FDO20080L3B
Model Revision Number              : PP
Motherboard Revision Number        : 03
Model Number                       : WS-C3650-12X48UZ
System Serial Number               : FDO20080L3B
Last reload reason                 : Power Failure or Unknown

Switch 03
---------
Switch uptime                      : 14 hours, 26 minutes

Base Ethernet MAC Address          : 00:f6:63:8a:45:00
Motherboard Assembly Number        : 73-100818-03
 --More--         Motherboard Serial Number          : FDO20261CMV
Model Revision Number              : A0
Motherboard Revision Number        : A0
Model Number                       : WS-C3650-12X48UR
System Serial Number               : FDO20261CMV
Last reload reason                 : Power Failure or Unknown

Switch 04
---------
Switch uptime                      : 13 hours, 42 minutes

Base Ethernet MAC Address          : 70:db:98:01:42:00
Motherboard Assembly Number        : 73-15897-06
Motherboard Serial Number          : FDO210722MV
Model Revision Number              : Q0
Motherboard Revision Number        : A0
Model Number                       : WS-C3650-48PD
System Serial Number               : FDO210722MV
Last reload reason                 : Power Failure or Unknown

Switch 05
---------
Switch uptime                      : 14 hours, 26 minutes
 --More--
```

```
Base Ethernet MAC Address          : f8:72:ea:0d:cc:00
Motherboard Assembly Number        : 73-15128-05
Motherboard Serial Number          : FDO17331P6G
Model Revision Number              : A0
Motherboard Revision Number        : A0
Model Number                       : WS-C3650-24PS
System Serial Number               : FDO17331P6G
Last reload reason                 : Power Failure or Unknown

Configuration register is 0x102
```

system env temperature threshold yellow

イエローのしきい値を決定する、イエローとレッドの温度しきい値の差を設定するには、グローバル コンフィギュレーション コマンドで **system env temperature threshold yellow** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

system env temperature threshold yellow *value*
no system env temperature threshold yellow *value*

構文の説明

value	イエローとレッドのしきい値の差を指定します（摂氏）。指定できる範囲は 10 ～ 25 です。

コマンド デフォルト

デフォルト値は次のとおりです。

表 *64* : 温度しきい値のデフォルト値

デバイス	イエローとレッドの差	レッド[11]
Catalyst 3650	14 °C	60 °C

[11] レッドの温度しきい値を設定することはできません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

グリーンとレッドのしきい値を設定することはできませんが、イエローのしきい値を設定することはできます。イエローとレッドのしきい値の差を指定して、イエローのしきい値を設定するには、 **system env temperature threshold yellow** *value* グローバル コンフィギュレーション コマンドを使用します。たとえば、レッドしきい値が 66 °C の場合に、イエローしきい値を 51 °C に設定するには、しきい値の差を 15 に設定するために、 **system env temperature threshold yellow 15** コマンドを使用します。たとえば、レッドしきい値が 60 °C の場合に、イエローし

きい値を 51 ℃ に設定するには、しきい値の差を 9 に設定するために、 **system env temperature threshold yellow 9** コマンドを使用します。

（注） device 内部の温度センサーでシステム内の温度を測定するため、±5 ℃の差が生じる可能性があります。

例

次の例では、イエローとレッドのしきい値の差を 15 に設定する方法を示します。

```
デバイス(config)# system env temperature threshold yellow 15
デバイス(config)#
```

test cable-diagnostics tdr

インターフェイス上でタイムドメイン反射率計（TDR）機能を実行するには、特権 EXEC モードで **test cable-diagnostics tdr** コマンドを使用します。

test cable-diagnostics tdr interface *interface-id*

構文の説明

interface-id	TDR を実行するインターフェイス。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

TDR は、銅線のイーサネット 10/100/100 ポートだけでサポートされます。10 ギガビット イーサネット ポートまたは Small Form-Factor Pluggable（SFP）モジュール ポートではサポートされません。

test cable-diagnostics tdr interface *interface-id* コマンドを使用して TDR を実行した後、**show cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを使用して結果を表示します。

次の例では、インターフェイス上で TDR を実行する方法を示します。

```
デバイス# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results
```

インターフェイスのリンクステータスがアップ状態で速度が 10 Mb/s または 100 Mb/s である場合、**test cable-diagnostics tdr interface** *interface-id* コマンドを入力すると、次のメッセージが表示されます。

```
デバイス# test cable-diagnostics tdr interface gigabitethernet1/0/3
TDR test on Gi1/0/9 will affect link state and traffic
TDR test started on interface Gi1/0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

traceroute mac

指定の送信元 MAC アドレスから指定の宛先 MAC アドレスまでをパケットが通過するレイヤ 2 パスを表示するには、特権 EXEC モードで **traceroute mac** コマンドを使用します。

traceroute mac [**interface** *interface-id*] *source-mac-address* [**interface** *interface-id*] *destination-mac-address* [**vlan** *vlan-id*] [**detail**]

構文の説明

interface *interface-id*	（任意）送信元または宛先 device 上のインターフェイスを指定します。
source-mac-address	送信元 device の 16 進形式の MAC アドレス。
destination-mac-address	宛先 device の 16 進形式の MAC アドレス。
vlan *vlan-id*	（任意）送信元 device から宛先 device までをパケットが通過するレイヤ 2 のパスをトレースする VLAN を指定します。指定できる VLAN ID の範囲は 1 ～ 4094 です。
detail	（任意）詳細情報を表示するよう指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

レイヤ 2 のトレースルートを適切に機能させるには、Cisco Discovery Protocol（CDP）がネットワークのすべての device でイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。

device がレイヤ 2 パス内でレイヤ 2 トレースルートをサポートしていないデバイスを検知した場合、device はレイヤ 2 トレースクエリを送信し続け、タイムアウトにします。

パス内で識別可能な最大ホップ数は 10 です。

レイヤ 2 traceroute はユニキャスト トラフィックだけをサポートします。マルチキャストの送信元または宛先 MAC アドレスを指定しても、物理的なパスは識別されず、エラー メッセージが表示されます。

指定された送信元および宛先アドレスが同じ VLAN にある場合、**traceroute mac** コマンド出力はレイヤ 2 パスを表示します。

異なる VLAN にある送信元および宛先アドレスを指定した場合、レイヤ 2 パスは識別されず、エラー メッセージが表示されます。

送信元または宛先 MAC アドレスが複数の VLAN に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。

VLAN を指定しないと、パスは識別されず、エラー メッセージが表示されます。

複数の装置がハブを介して 1 つのポートに接続されている場合（たとえば、複数の CDP ネイバーがポートで検出されるなど）、レイヤ 2 traceroute 機能はサポートされません。

複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。

この機能は、トークンリング VLAN ではサポートされません。

例

次の例では、送信元および宛先 MAC アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
デバイス# traceroute mac 0000.0201.0601 0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

次の例では、**detail** キーワードを使用することで、レイヤ 2 のパスを表示する方法を示します。

```
デバイス# traceroute mac 0000.0201.0601 0000.0201.0201 detail
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 / WS-C3750E-24PD / 2.2.6.6 :
          Gi0/0/2 [auto, auto] => Gi0/0/3 [auto, auto]
  con5 / WS-C2950G-24-EI / 2.2.5.5 :
          Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
  con1 / WS-C3550-12G / 2.2.1.1 :
          Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
          Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

次の例では、送信元および宛先 device のインターフェイスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
デバイス# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
 0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                 (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

次の例では、device が送信元 device に接続されていない場合のレイヤ 2 のパスを示します。

```
デバイス# traceroute mac 0000.0201.0501 0000.0201.0201 detail
  Source not directly connected, tracing source .....
  Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
  con5 / WS-C3750E-24TD / 2.2.5.5 :
         Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
  con1 / WS-C3550-12G / 2.2.1.1 :
         Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
         Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

次の例では、device が送信元 MAC アドレスの宛先ポートを検出できない場合のレイヤ 2 のパスを示します。

```
デバイス# traceroute mac 0000.0011.1111 0000.0201.0201
  Error:Source Mac address not found.
  Layer2 trace aborted.
```

次の例では、送信元および宛先デバイスが異なる VLAN にある場合のレイヤ 2 のパスを示します。

```
デバイス# traceroute mac 0000.0201.0601 0000.0301.0201
  Error:Source and destination macs are on different vlans.
  Layer2 trace aborted.
```

次の例では、宛先 MAC アドレスがマルチキャスト アドレスの場合のレイヤ 2 のパスを示します。

```
デバイス# traceroute mac 0000.0201.0601 0100.0201.0201
  Invalid destination mac address
```

次の例では、送信元および宛先 device が複数の VLAN にある場合のレイヤ 2 のパスを示します。

```
デバイス# traceroute mac 0000.0201.0601 0000.0201.0201
  Error:Mac found on multiple vlans.
  Layer2 trace aborted.
```

traceroute mac ip

指定の送信元 IP アドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名を通過するパケットのレイヤ 2 パスを表示するには、特権 EXEC モードで **traceroute mac ip** コマンドを使用します。

traceroute mac ip {*source-ip-address source-hostname*} {*destination-ip-address destination-hostname*} [**detail**]

構文の説明

source-ip-address	32 ビットの値（ドット付き 10 進表記）で指定された送信元 device の IP アドレス。
source-hostname	送信元 device の IP ホスト名。
destination-ip-address	32 ビットの値（ドット付き 10 進表記）で指定された宛先 device の IP アドレス。
destination-hostname	宛先 device の IP ホスト名。
detail	（任意）詳細情報を表示するよう指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

レイヤ2のトレースルートを適切に機能させるには、Cisco Discovery Protocol（CDP）がネットワークの各 device でイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。

device がレイヤ 2 パス内でレイヤ 2 トレースルートをサポートしていないデバイスを検知した場合、device はレイヤ 2 トレースクエリを送信し続け、タイムアウトにします。

パス内で識別可能な最大ホップ数は 10 です。

指定された送信元および宛先の IP アドレスが同一のサブネット内にある場合、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。

IP アドレスを指定した場合、device は Address Resolution Protocol（ARP）を使用し、IP アドレスとそれに対応する MAC アドレスおよび VLAN ID を対応させます。

- 指定の IP アドレスの ARP のエントリが存在している場合、device は関連付けられた MAC アドレスを使用し、物理パスを識別します。
- ARP のエントリが存在しない場合、device は ARP クエリを送信し、IP アドレスを解決しようと試みます。IP アドレスは同一のサブネットにある必要があります。IP アドレスが解決されない場合は、パスは識別されず、エラー メッセージが表示されます。

複数の装置がハブを介して 1 つのポートに接続されている場合（たとえば、複数の CDP ネイバーがポートで検出されるなど）、レイヤ 2 traceroute 機能はサポートされません。

複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラー メッセージが表示されます。

この機能は、トークンリング VLAN ではサポートされません。

例

次の例では、**detail** キーワードを使用して、送信元と宛先の IP アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
デバイス# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C3750E-24TD / 2.2.6.6 :
        Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先ホスト名を指定することで、レイヤ 2 のパスを表示する方法を示します。

```
デバイス# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/2
```

```
con2                 (2.2.2.2        )  :    Gi0/0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

次の例では、ARP が送信元 IP アドレスと対応する MAC アドレスを関連付けられない場合の、レイヤ 2 のパスを示します。

```
デバイス# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

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 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

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:
```

unset

1つ以上の環境変数をリセットするには、ブートローダモードで**unset**コマンドを使用します。

unset *variable...*

構文の説明

variable	*variable* には、次に示すキーワードのいずれかを使用します。 **MANUAL_BOOT**：device の起動を自動で行うか手動で行うかどうかを指定します。
	BOOT：自動起動時に、実行可能ファイルのリストをリセットして、ロードおよび実行します。BOOT環境変数が設定されていない場合、システムは、フラッシュ ファイル システム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT変数が設定されていても、指定されたイメージをロードできなかった場合、システムはフラッシュ ファイル システムで最初に検出した起動可能なファイルを起動しようとします。
	ENABLE_BREAK：フラッシュファイルシステムの初期化後に、コンソール上の **Break** キーを使用して自動ブートプロセスを中断できるかどうかを指定します。
	HELPER：ブート ローダの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストを識別します。ヘルパー ファイルは、ブートローダの機能を拡張したり、パッチを当てたりします。
	PS1：ブート ローダ モードの場合に、コマンドライン プロンプトとして使用する文字列を指定します。
	CONFIG_FILE：Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名をリセットします。
	BAUD：コンソールで使用される速度（ビット/秒（b/s）単位）をリセットします。コンフィギュレーション ファイルに別の設定が指定されていない限り、Cisco IOS ソフトウェアはブートローダからボー レート設定を継承し、この値を引き続き使用します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

ブートローダ

コマンド履歴	リリース	変更内容
	Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

通常の環境では、環境変数の設定を変更する必要はありません。

MANUAL_BOOT 環境変数は、**no boot manual** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

BOOT 環境変数は、**no boot system** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

ENABLE_BREAK 環境変数は、**no boot enable-break** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

HELPER 環境変数は、**no boot helper** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

CONFIG_FILE 環境変数は、**no boot config-file** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

例

次に、SWITCH_PRIORITY 環境変数をリセットする例を示します。

```
デバイス: unset SWITCH_PRIORITY
```

version

ブートローダのバージョンを表示するには、ブートローダモードで **version** コマンドを使用します。

version

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

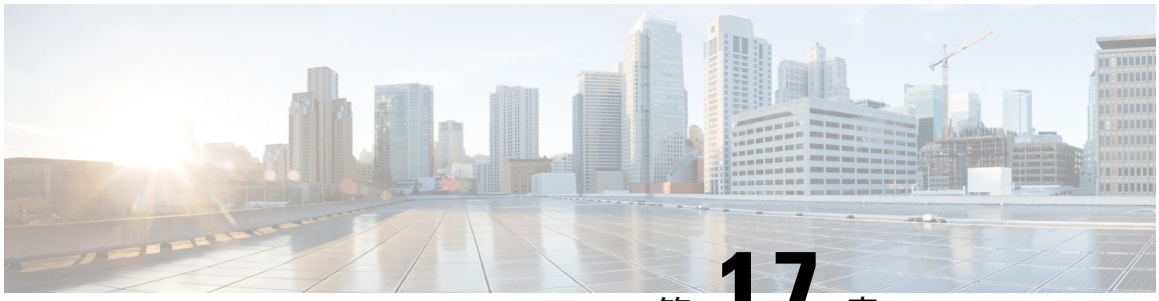
ブートローダ

コマンド履歴	リリース	変更内容
	Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

例

次に、deviceのブートローダのバージョンを表示する例を示します。

デバイス: **version**
```
CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 1.2, RELEASE SOFTWARE (P)
Compiled Sun Jul 14 20:22:00 PDT 2013 by rel
```



第 17 章

トレース

set platform software trace

プロセス内の特定のモジュールのトレースレベルを設定するには、特権 EXEC モードまたはユーザ EXEC モードで **set platform software trace** コマンドを使用します。

set platform software trace *process slot module trace-level*

構文の説明	*process*	トレース レベルが設定されているプロセス。次のオプションがあります。 • **chassis-manager**：Chassis Manager プロセス。 • **cli-agent**：CLI Agent プロセス。 • **dbm**：Database Manager プロセス。 • **emd**：Environmental Monitoring プロセス。 • **fed**：Forwarding Engine Driver プロセス。 • **forwarding-manager**：Forwarding Manager プロセス。 • **host-manager**：Host Manager プロセス。 • **iomd**：Input/Output Module daemon（IOMd）プロセス。 • **ios**：IOS プロセス。 • **license-manager**：License Manager プロセス。 • **logger**：Logging Manager プロセス。 • **platform-mgr**：Platform Manager プロセス。 • **pluggable-services**：Pluggable Services プロセス。 • **replication-mgr**：Replication Manager プロセス。 • **shell-manager**：Shell Manager プロセス。 • **smd**：Session Manager プロセス。 • **table-manager**：Table Manager サーバ。 • **wireshark**：Embedded Packet Capture（EPC）Wireshark プロセス。

slot	トレース レベルが設定されているプロセスを実行中のハードウェア スロット。次のオプションがあります。 • *number*：トレース レベルが設定されているハードウェア モジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。 • *SIP-slot / SPA-bay*：SIP スイッチ スロットの数とその SIP の共有ポート アダプタ（SPA）ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。 • **F0**：スロット 0 の Embedded-Service-Processor。 • **FP active**：アクティブな Embedded-Service-Processor。 • **R0**：スロット 0 のルート プロセッサ。 • **RP active**：アクティブなルート プロセッサ。 • **switch** <*number*> ：指定された番号を持つスイッチ。 • **switch active**：アクティブなスイッチ。 • **switch standby**：スタンバイスイッチ。
module	トレース レベルが設定されているプロセス内のモジュール。

trace-level	トレース レベルです。次のオプションがあります。 • **debug**：デバッグ レベルのトレーシング。デバッグレベルのトレース メッセージは、モジュールに関する大量の詳細を提供する緊急でないメッセージです。 • **emergency**：緊急事態レベルのトレーシング。緊急レベルのトレース メッセージは、システムが使用不能であることを示すメッセージです。 • **error**：エラー レベルのトレーシング。エラーレベルのトレース メッセージは、システム エラーを示すメッセージです。 • **info**：情報レベルのトレーシング。情報レベルのトレース メッセージは、システムに関する情報を提供する緊急でないメッセージです。 • **noise**：ノイズ レベルのトレーシング。ノイズ レベルは、常に可能なトレース レベルの中の最高レベルに相当し、考えられるすべてのトレース メッセージを生成します。 ノイズ レベルは、モジュールに関して可能な最高レベルのトレース メッセージに相当します。これは、このコマンドの将来の拡張で、ユーザが寄り高いトレース レベルを設定できるオプションが追加された場合にも、当てはまります。 • **notice**：重大な問題に関するメッセージです。ただし、スイッチは通常どおり動作しています。 • **verbose**：詳細レベルのトレーシング。トレース レベルが verbose に設定されている場合は、考えられるすべてのトレース メッセージが送信されます。 • **warning**：警告メッセージ。

コマンド デフォルト

すべてのモジュールのデフォルトのトレースレベルは **notice** です。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

module オプションは、プロセスおよび *hardware-module* によって異なります。このコマンドを入力する際に、各キーワード シーケンスで使用可能な *module* オプションを確認するには、? オプションを使用します。

トレースメッセージを表示するには、**show platform software trace message** コマンドを使用します。

トレース ファイルは、harddisk: ファイル システムのトレースログ ディレクトリに保存されます。これらのファイルは、スイッチの動作に影響を与えずに削除できます。

トレース ファイル出力は、デバッグに使用されます。トレース レベルは、モジュールに関するどのぐらいの量の情報をトレース ファイルに保存するかを決定する設定です。

例

次に、dbm プロセスのすべてのモジュールのトレース レベルを設定する例を示します。

```
デバイス# set platform software trace dbm R0 all-modules debug
```

show platform software trace filter-binary

特定のモジュールの最新のトレース情報を表示するには、特権EXECモードまたはユーザEXECモードで **show platform software trace filter-binary** コマンドを使用します。

show platform software trace filter-binary*modules* ［**context** *mac-address*］

構文の説明

context*mac-address*	フィルタ処理に使用されるコンテキストを表します。また、モジュール名とトレース レベルに基づいてフィルタ処理できます。コンテキスト キーワードは、タグが付いているトレースに基づき MAC アドレスまたは他の引数を受け入れます。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、モジュールに関連するすべてのプロセス全体で `/tmp/.../` に存在するすべてのログを照合してソートします。指定されたモジュールに関連するすべてのプロセスのトレース ログがコンソールに出力されます。このコマンドでは、同じコンテンツの `collated_log_{system time}` という名前のファイルも `/crashinfo/tracelogs` ディレクトリに生成されます。

show platform software trace message

プロセスのトレース メッセージを表示するには、特権 EXEC モードまたはユーザ EXEC モードで **set platform software trace** コマンドを使用します。

show platform software trace message *process slot*

構文の説明	*process*	設定されているトレース レベル。次のオプションがあります。 • **chassis-manager**：Chassis Manager プロセス。 • **cli-agent**：CLI Agent プロセス。 • **cmm**：CMM プロセス。 • **dbm**：Database Manager プロセス。 • **emd**：Environmental Monitoring プロセス。 • **fed**：Forwarding Engine Driver プロセス。 • **forwarding-manager**：Forwarding Manager プロセス。 • **geo**：Geo Manager プロセス。 • **host-manager**：Host Manager プロセス。 • **interface-manager**：Interface Manager プロセス。 • **iomd**：Input/Output Module daemon（IOMd）プロセス。 • **ios**：IOS プロセス。 • **license-manager**：License Manager プロセス。 • **logger**：Logging Manager プロセス。 • **platform-mgr**：Platform Manager プロセス。 • **pluggable-services**：Pluggable Services プロセス。 • **replication-mgr**：Replication Manager プロセス。 • **shell-manager**：Shell Manager プロセス。 • **sif**：Stack Interface（SIF）Manager プロセス。 • **smd**：Session Manager プロセス。 • **stack-mgr**：Stack Manager プロセス。 • **table-manager**：Table Manager サーバ。 • **thread-test**：Multithread Manager プロセス。 • **virt-manager**：Virtualization Manager プロセス。

slot

トレース レベルが設定されているプロセスを実行中のハードウェア スロット。次のオプションがあります。

- *number*：トレース レベルが設定されているハードウェア モジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。
- *SIP-slot / SPA-bay*：SIP スイッチ スロットの数とその SIP の共有ポート アダプタ（SPA）ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。
- **F0**：Embedded Service Processor スロット 0。
- **FP active**：アクティブな Embedded Service Processor。
- **R0**：スロット 0 のルート プロセッサ。
- **RP active**：アクティブなルート プロセッサ。
- **switch** <*number*> ：指定された番号を持つスイッチ。
- **switch active**：アクティブなスイッチ。
- **switch standby**：スタンバイスイッチ。
  - *number*：トレース レベルが設定されているハードウェア モジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。
  - *SIP-slot / SPA-bay*：SIP スイッチ スロットの数とその SIP の共有ポート アダプタ（SPA）ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。
  - **F0**：スロット 0 の Embedded Service Processor。
  - **FP active**：アクティブな Embedded Service Processor。
  - **R0**：スロット 0 のルート プロセッサ。
  - **RP active**：アクティブなルート プロセッ

サ。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

例

次に、Stack Manager プロセスおよび Forwarding Engine Driver プロセスのトレース メッセージを表示する例を示します。

```
デバイス# show platform software trace message stack-mgr switch active R0
10/30 09:42:48.767 [btrace] [8974]: (note): Successfully registered module [97] [uiutil]
10/30 09:42:48.762 [btrace] [8974]: (note): Successfully registered module [98]
[tdl_cdlcore_message]
10/29 13:28:19.023 [stack_mgr] [8974]: (note): Examining peer state
10/29 13:28:19.023 [stack_mgr] [8974]: (note): no switch eligible for standby election
presently
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Posting event
stack_fsm_event_wait_standby_elect_timer_expired, curstate stack_fsm_state_active_ready
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Timer HDL - STACK_WAIT_STANDBY_ELECT_TIMER
 expired
10/29 13:26:46.584 [btrace] [8974]: (note): Successfully registered module [99]
[tdl_ui_message]
10/29 13:26:46.582 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:36.582 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect
10/29 13:26:36.582 [evutil] [8974]: (ERR): Asynchronous connect failed for [uipeer uplink
 to slot 1] (fd == -1)
10/29 13:26:36.581 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:26.581 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect

デバイス# show platform software trace message fed switch active
11/02 10:55:01.832 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered
module [86] [uiutil]
11/02 10:55:01.848 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Single message size is
greater than 1024
11/02 10:55:01.822 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered
module [87] [tdl_cdlcore_message]
11/01 09:54:41.474 [btrace]: [12312]:  UUID: 0, ra: 0 (note): Successfully registered
module [88] [tdl_ngwc_gold_message]
11/01 09:54:11.228 [btrace]: [12312]:  UUID: 0, ra: 0 (note): Successfully registered
module [89] [tdl_doppler_iosd_matm_type]
11/01 09:53:37.454 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered
module [90] [tdl_ui_message]
11/01 09:53:37.382 [bipc]: [11310]:  UUID: 0, ra: 0 (note): Pending connection to server
 10.129.1.0
11/01 09:53:34.227 [xcvr]: [18846]:  UUID: 0, ra: 0 (ERR): FRU hardware authentication
Fail, result = 1.
11/01 09:53:33.775 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR): SMART COOKIE: SCC I2C
receive failed: rc=10
11/01 09:53:33.775 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR):
```

```
SMART COOKIE receive failed, try again
11/01 09:53:33.585 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR):
```

show platform software trace level

特定のプロセスですべてのモジュールのトレース レベルを表示するには、特権 EXEC モードまたはユーザ EXEC モードで **show platform software trace level** コマンドを使用します。

show platform software trace level *process slot*

構文の説明	*process*	トレース レベルが設定されているプロセス。次のオプションがあります。 • **chassis-manager**：Chassis Manager プロセス。 • **cli-agent**：CLI Agent プロセス。 • **cmm**：CMM プロセス。 • **dbm**：Database Manager プロセス。 • **emd**：Environmental Monitoring プロセス。 • **fed**：Forwarding Engine Driver プロセス。 • **forwarding-manager**：Forwarding Manager プロセス。 • **geo**：Geo Manager プロセス。 • **host-manager**：Host Manager プロセス。 • **interface-manager**：Interface Manager プロセス。 • **iomd**：Input/Output Module daemon（IOMd）プロセス。 • **ios**：IOS プロセス。 • **license-manager**：License Manager プロセス。 • **logger**：Logging Manager プロセス。 • **platform-mgr**：Platform Manager プロセス。 • **pluggable-services**：Pluggable Services プロセス。 • **replication-mgr**：Replication Manager プロセス。 • **shell-manager**：Shell Manager プロセス。 • **sif**：Stack Interface（SIF）Manager プロセス。 • **smd**：Session Manager プロセス。 • **stack-mgr**：Stack Manager プロセス。 • **table-manager**：Table Manager サーバ。 • **thread-test**：Multithread Manager プロセス。 • **virt-manager**：Virtualization Manager プロセス。

slot	トレース レベルが設定されているプロセスを実行中のハードウェア スロット。次のオプションがあります。 • *number*：トレース レベルが設定されているハードウェア モジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。 • *SIP-slot / SPA-bay*：SIP スイッチ スロットの数とその SIP の共有ポート アダプタ（SPA）ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。 • **F0**：スロット 0 の Embedded Service Processor。 • **F1**：スロット 1 の Embedded Service Processor。 • **FP active**：アクティブな Embedded Service Processor。 • **R0**：スロット 0 のルート プロセッサ。 • **RP active**：アクティブなルート プロセッサ。 • **switch** <*number*> ：指定された番号を持つスイッチ。 • **switch active**：アクティブなスイッチ。 • **switch standby**：スタンバイスイッチ。 • *number*：トレース レベルが設定されているハードウェア モジュールの SIP スロットの数。たとえば、スイッチの SIP スロット 2 の SIP を指定する場合は、「2」と入力します。 • *SIP-slot / SPA-bay*：SIP スイッチ スロットの数とその SIP の共有ポート アダプタ（SPA）ベイの数。たとえば、スイッチ スロット 3 の SIP のベイ 2 の SPA を指定する場合は、「3/2」と入力します。 • **F0**：スロット 0 の Embedded Service Processor。 • **FP active**：アクティブな Embedded Service Processor。 • **R0**：スロット 0 のルート プロセッサ。 • **RP active**：アクティブなルート プロセッサ。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

例

次に、トレース レベルを表示する例を示します。

```
デバイス# show platform software trace level dbm switch active R0
Module Name                      Trace Level
----------------------------------------------------
binos                            Notice
binos/brand                      Notice
bipc                             Notice
btrace                           Notice
bump_ptr_alloc                   Notice
cdllib                           Notice
chasfs                           Notice
dbal                             Informational
dbm                              Debug
evlib                            Notice
evutil                           Notice
file_alloc                       Notice
green-be                         Notice
ios-avl                          Notice
klib                             Debug
services                         Notice
sw_wdog                          Notice
syshw                            Notice
tdl_cdlcore_message              Notice
tdl_dbal_root_message            Notice
tdl_dbal_root_type               Notice
```

request platform software trace archive

スイッチ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 Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン 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 日以降にスイッチ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
```

request platform software trace rotate all

現在のインメモリトレースログを crashinfo パーティションに循環させ、プロセスごとの新しいインメモリトレースログを開始するには、特権 EXEC モードまたはユーザ EXEC モードで **request platform software trace rotate all** コマンドを使用します。

request platform software trace rotate all

コマンド モード ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン トレース ログ ファイルは読み取り専用を目的としています。ファイルの内容は編集しないでください。特定のログ セットを表示するために、ファイルの内容を削除する必要がある場合は、このコマンドを使用して新しいトレース ログ ファイルを開始します。

例

次に、過去1日以降にスイッチで実行されているプロセスのすべてのインメモリ トレース ログを循環させる例を示します。

```
デバイス# request platform software trace slot switch active R0 archive last 1 days target
 flash:test
```

request platform software trace filter-binary

トレースログ サブディレクトリに存在するすべてのアーカイブログを照合して並べ替えるには、特権 EXEC モードまたはユーザ EXEC モードで **request platform software trace filter-binary** コマンドを使用します。

request platform software trace filter-binary *modules* ［**context** *mac-address*］

構文の説明	**context** *mac-address*	フィルタ処理に使用されるコンテキストを表します。また、モジュール名とトレース レベルに基づいてフィルタ処理できます。コンテキスト キーワードは、タグが付いているトレースに基づき MAC アドレスまたは他の引数を受け入れます。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

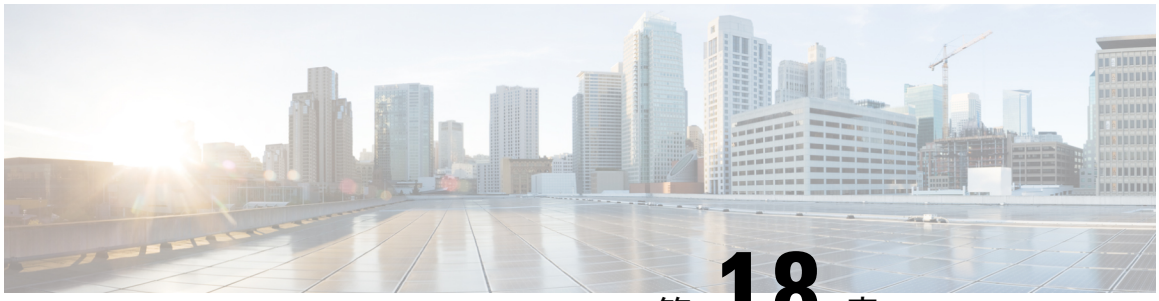
リリース	変更内容
Cisco IOS XE Denali 16.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、モジュールに関連するすべてのプロセスを対象に、トレースログ サブディレクトリに存在するすべてのアーカイブされたログを照合して並べ替えます。このコマンドでは、同じコンテンツの `collated_log_{system time}` という名前のファイルも `/crashinfo/tracelogs` ディレクトリに生成されます。

第 XIV 部

VLAN



第 18 章

VLAN

client vlan

WLAN インターフェイスまたはインターフェイスグループを設定するには、 **client vlan** コマンドを使用します。WLAN インターフェイスをディセーブルにするには、このコマンドの **no** 形式を使用します。

client vlan *interface-id-name-or-group-name*
no client vlan

構文の説明

interface-id-name-or-group-name	インターフェイス ID、名前、または VLAN グループ名。インターフェイス ID は、複数桁で指定することもできます。

コマンド デフォルト

デフォルト インターフェイスが設定されています。

コマンド モード

WLAN の設定

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにする必要があります。WLAN をディセーブルにする方法の詳細については、「関連コマンド」の項を参照してください。

次に、WLAN のクライアント VLAN をイネーブルにする例を示します。

```
デバイス# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
デバイス(config)# wlan wlan1
デバイス(config-wlan)# client vlan client-vlan1
デバイス(config-wlan)# end
```

次に、WLAN 上のクライアント VLAN をディセーブルにする例を示します。

```
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)# no client vlan
デバイス(config-wlan)# end
```

clear vtp counters

VLAN Trunking Protocol（VTP）およびプルーニングカウンタをクリアするには、特権 EXEC モードで **clear vtp counters** コマンドを使用します。

clear vtp counters

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

次の例では、VTP カウンタをクリアする方法を示します。

```
デバイス# clear vtp counters
```

情報が削除されたことを確認するには、**show vtp counters** 特権 EXEC コマンドを入力します。

debug platform vlan

VLANマネージャソフトウェアのデバッグをイネーブルにするには、特権EXECモードで**debug platform vlan** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug platform vlan [{**error** | **event**}] [**switch** *switch-number*]
no debug platform vlan [{**error** | **event**}] [**switch** *switch-number*]

構文の説明

error	（任意）VLAN エラー デバッグ メッセージを表示します。
event	（任意）VLAN プラットフォーム イベント デバッグ メッセージを表示します。
switch *switch-number*	（任意）VLAN マネージャ ソフトウェアのデバッグをイネーブルにするスタック メンバ番号を指定します。 このキーワードは、スタック対応スイッチでのみサポートされています。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

undebug platform vlan コマンドは **no debug platform vlan** コマンドと同じです。

次の例では、VLAN エラー デバッグ メッセージを表示する方法を示します。

```
デバイス# debug platform vlan error
```

debug sw-vlan

VLAN マネージャアクティビティのデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sw-vlan {**badpmcookies** | **cfg-vlan** {**bootup** | **cli**} | **events** | **ifs** | **management** | **mapping** | **notification** | **packets** | **redundancy** | **registries** | **vtp**}
no debug sw-vlan {**badpmcookies** | **cfg-vlan** {**bootup** | **cli**} | **events** | **ifs** | **management** | **mapping** | **notification** | **packets** | **redundancy** | **registries** | **vtp**}

構文の説明

badpmcookies	不良ポート マネージャ クッキーの VLAN マネージャ インシデントに関するデバッグ メッセージを表示します。
cfg-vlan	VLAN 設定デバッグ メッセージを表示します。
bootup	スイッチが起動すると、メッセージが表示されます。
cli	コマンドライン インターフェイス（CLI）が VLAN コンフィギュレーション モードである場合のメッセージを表示します。
events	VLAN マネージャ イベントのデバッグ メッセージを表示します。
ifs	VLAN マネージャ IOS ファイル システム（IFS）のデバッグ メッセージを表示します。詳細については、「debug sw-vlan ifs （1023 ページ）」を参照してください。
management	内部 VLAN の VLAN マネージャ管理のデバッグ メッセージを表示します。
mapping	VLAN マッピングのデバッグ メッセージを表示します。
notification	VLAN マネージャ通知のデバッグ メッセージを表示します。詳細については、「debug sw-vlan notification （1024 ページ）」を参照してください。
packets	パケット処理およびカプセル化プロセスのデバッグ メッセージを表示します。
redundancy	VTP VLAN 冗長性のデバッグ メッセージを表示します。
registries	VLAN マネージャ レジストリのデバッグ メッセージを表示します。
vtp	VLAN Trunking Protocol（VTP）コードのデバッグ メッセージを表示します。詳細については、「debug sw-vlan vtp （1025 ページ）」を参照してください。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

undebug sw-vlan コマンドは **no debug sw-vlan** コマンドと同じです。

次に、VLAN マネージャ イベントのデバッグ メッセージを表示する例を示します。

```
デバイス# debug sw-vlan events
```

debug sw-vlan ifs

VLAN マネージャ IOS File System（IFS）エラーテストのデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan ifs** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sw-vlan ifs {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}
no debug sw-vlan ifs {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

構文の説明

open read	VLAN マネージャ IFS ファイル読み取り動作のデバッグ メッセージを表示します。
open write	VLAN マネージャ IFS ファイル書き込み動作のデバッグ メッセージを表示します。
read	指定されたエラーテスト（**1**、**2**、**3**、または **4**）に関するファイル読み取り動作のデバッグメッセージを表示します。
write	ファイル書き込み動作のデバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

undebug sw-vlan ifs コマンドは **no debug sw-vlan ifs** コマンドと同じです。

ファイルの読み取り処理に処理 **1** を選択すると、ヘッダー検証ワードおよびファイルバージョン番号が格納されたファイルヘッダーが読み込まれます。処理 **2** を指定すると、ドメインおよび VLAN 情報の大部分が格納されたファイル本体が読み取られます。処理 **3** を指定すると、Type Length Version（TLV）記述子構造が読み取られます。処理 **4** を指定すると、TLV データが読み取られます。

次の例では、ファイル書き込み動作のデバッグ メッセージを表示する方法を示します。

```
デバイス# debug sw-vlan ifs write
```

debug sw-vlan notification

VLANマネージャ通知のデバッグをイネーブルにするには、特権EXECモードで**debug sw-vlan notification** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sw-vlan notification {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **pruningcfgchange** | **statechange**}
no debug sw-vlan notification {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **pruningcfgchange** | **statechange**}

構文の説明

accfwdchange	集約アクセス インターフェイス スパニングツリー転送変更に関するVLAN マネージャ通知のデバッグ メッセージを表示します。
allowedvlancfgchange	許可 VLAN の設定変更に関する VLAN マネージャ通知のデバッグ メッセージを表示します。
fwdchange	スパニングツリー転送変更に関する VLAN マネージャ通知のデバッグ メッセージを表示します。
linkchange	インターフェイス リンクステート変更のVLANマネージャ通知のデバッグ メッセージを表示します。
modechange	インターフェイス モード変更の VLAN マネージャ通知のデバッグ メッセージを表示します。
pruningcfgchange	プルーニング設定変更の VLAN マネージャ通知のデバッグ メッセージを表示します。
statechange	インターフェイス ステート変更のVLANマネージャ通知のデバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

undebug sw-vlan notification コマンドは **no debug sw-vlan notification** コマンドと同じです。

次に、インターフェイス モード変更の VLAN マネージャ通知のデバッグ メッセージを表示する例を示します。

```
デバイス# debug sw-vlan notification
```

debug sw-vlan vtp

VLAN Trunking Protocol（VTP）コードのデバッグをイネーブルにするには、特権 EXEC モードで **debug sw-vlan vtp** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sw-vlan vtp {**events** | **packets** | **pruning** [{**packets** | **xmit**}] | **redundancy** | **xmit**}
no debug sw-vlan vtp {**events** | **packets** | **pruning** | **redundancy** | **xmit**}

構文の説明

events	汎用の論理フローのデバッグ メッセージおよびVTP コード内の VTP_LOG_RUNTIME マクロによって生成された VTP メッセージの詳細を表示します。
packets	Cisco IOS VTP プラットフォーム依存層から VTP コードに渡されたすべての着信 VTP パケット（プルーニング パケットを除く）の内容のデバッグ メッセージを表示します。
pruning	VTP コードのプルーニング セグメントによって生成されるデバッグ メッセージを表示します。
packets	（任意）Cisco IOS VTP プラットフォーム依存層から VTP コードに渡されたすべての着信VTPプルーニング パケットの内容のデバッグ メッセージを表示します。
xmit	（任意）VTP コードが Cisco IOS VTP プラットフォーム依存層に送信するように要求したすべての発信 VTP パケットの内容のデバッグ メッセージを表示します。
redundancy	VTP 冗長性のデバッグ メッセージを表示します。
xmit	VTP コードが Cisco IOS VTP プラットフォーム依存層に送信するように要求したすべての発信VTPパケット（プルーニング パケットを除く）の内容のデバッグ メッセージを表示します。

コマンド デフォルト

デバッグはディセーブルです。

コマンド モード

特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン **undebug sw-vlan vtp** コマンドは **no debug sw-vlan vtp** コマンドと同じです。

pruning キーワードの後に追加のパラメータを入力しない場合は、VTP プルーニング デバッグ メッセージが表示されます。これらのメッセージは、VTP プルーニング コード内の VTP_PRUNING_LOG_NOTICE、VTP_PRUNING_LOG_INFO、VTP_PRUNING_LOG_DEBUG、VTP_PRUNING_LOG_ALERT、および VTP_PRUNING_LOG_WARNING マクロによって生成されます。

次に、VTP 冗長性のデバッグ メッセージを表示する例を示します。

```
デバイス# debug sw-vlan vtp redundancy
```

interface vlan

ダイナミック スイッチ仮想インターフェイス（SVI）を作成するか、既存のダイナミック SVI にアクセスし、インターフェイス コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **interface vlan** コマンドを使用します。SVI を削除するには、このコマンドの **no** 形式を使用します。

interface vlan *vlan-id*
no interface vlan *vlan-id*

構文の説明		
	vlan-id	VLAN 番号。指定できる範囲は 1 ～ 4094 です。

コマンド デフォルト デフォルトの VLAN インターフェイスは VLAN 1 です。

コマンド モード グローバル コンフィギュレーション

コマンド履歴	リリース	変更内容
	Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン SVI は、特定の VLAN に対して最初に **interface vlan** *vlan-id* コマンドを入力したときに作成されます。*vlan-id* は、IEEE 802.1Q カプセル化トランク上のデータ フレームに対応する VLAN タグ、またはアクセス ポート用に設定された VLAN ID に対応します。

（注） 物理ポートと関連付けられていない場合、SVI を作成してもアクティブにはなりません。

no interface vlan *vlan-id* コマンドを使用して削除した SVI は、**show interfaces** 特権 EXEC コマンドの出力に表示されなくなります。

（注） VLAN 1 インターフェイスを削除することはできません。

削除されたインターフェイスに対して **interface vlan** *vlan-id* コマンドを入力すると、削除されたSVIを元に戻すことができます。インターフェイスはバックアップとなりますが、それまでの設定は削除されます。

スイッチまたはスイッチスタック上で設定されたSVIの数と、設定された他の機能の数の相互関係によっては、ハードウェア制限により、CPU使用率に影響が出る可能性があります。**sdm prefer** グローバル コンフィギュレーション コマンドを使用して、システムのハードウェア リソースを、テンプレートおよび機能テーブルに基づいて再度割り当てることができます。

設定を確認するには、**show interfaces** および **show interfaces vlan** *vlan-id* 特権 EXEC コマンドを入力します。

次の例では、VLAN ID 23 の新しいSVIを作成し、インターフェイス コンフィギュレーション モードを開始する方法を示します。

```
デバイス(config)# interface vlan 23
デバイス(config-if)#
```

show platform vlan

プラットフォーム依存 VLAN 情報を表示するには、**show platform vlan** 特権 EXEC コマンドを使用します。

show platform vlan [*vlan-id*] [**switch** *switch-number*]

構文の説明

vlan-id	（任意）VLAN の ID。指定できる範囲は 1 ～ 4094 です。
switch *switch-number*	（任意）指定されたスタック メンバのVLANのみを表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

次の例では、プラットフォーム依存 VLAN 情報を表示する方法を示します。

```
デバイス# show platform vlan
```

show vlan

設定されたすべての VLAN またはスイッチ上の 1 つの VLAN（VLAN ID または名前を指定した場合）のパラメータを表示するには、特権 EXEC モードで **show vlan** コマンドを使用します。

show vlan [{**brief** | **group** | **id** *vlan-id* | **mtu** | **name** *vlan-name* | **remote-span** | **summary**}]

構文の説明

brief	（任意）VLAN ごとに VLAN 名、ステータス、およびポートを 1 行で表示します。
group	（任意）VLAN グループについての情報を表示します。
id *vlan-id*	（任意）VLAN ID 番号で特定された 1 つの VLAN に関する情報を表示します。*vlan-id* に指定できる範囲は 1 ～ 4094 です。
mtu	（任意）VLAN のリストと、VLAN のポートに設定されている最小および最大伝送単位（MTU）サイズを表示します。
name *vlan-name*	（任意）VLAN 名で特定された 1 つの VLAN に関する情報を表示します。VLAN 名は、1 ～ 32 文字の ASCII 文字列です。
remote-span	（任意）Remote SPAN（RSPAN）VLAN に関する情報を表示します。
summary	（任意）VLAN サマリー情報を表示します。

（注） **ifindex** キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

show vlan mtu コマンド出力では、MTU_Mismatch 列に VLAN 内のすべてのポートに同じ MTU があるかどうかを示します。この列に yes が表示されている場合、VLAN の各ポートに別々の MTU があり、パケットが、大きい MTU を持つポートから小さい MTU を持つポートにスイッチングされると、ドロップされることがあります。VLAN に SVI がない場合、ハイフン（-）記号が SVI_MTU 列に表示されます。MTU-Mismatch 列に yes が表示されている場合、MiniMTU と MaxMTU を持つポート名が表示されます。

次に、**show vlan** コマンドの出力例を示します。次の表に、この出力で表示されるフィールドについて説明します。

```
デバイス> show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                Gi1/0/23, Gi1/0/24, Gi1/0/25
                                                Gi1/0/26, Gi1/0/27, Gi1/0/28
                                                Gi1/0/29, Gi1/0/30, Gi1/0/31
                                                Gi1/0/32, Gi1/0/33, Gi1/0/34
                                                Gi1/0/35, Gi1/0/36, Gi1/0/37
                                                Gi1/0/38, Gi1/0/39, Gi1/0/40
                                                Gi1/0/41, Gi1/0/42, Gi1/0/43
                                                Gi1/0/44, Gi1/0/45, Gi1/0/46
                                                Gi1/0/47, Gi1/0/48
2    VLAN0002                         active
40   vlan-40                          active
300  VLAN0300                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
300  enet  100300     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
2000 enet  102000     1500  -      -      -        -    -        0      0
3000 enet  103000     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
```

```
2000,3000

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

表 *65 : show vlan* コマンドの出力フィールド

フィールド	説明
VLAN	VLAN 番号。
Name	VLAN の名前（設定されている場合）。
Status	VLAN のステータス（active または suspend）。
Ports	VLAN に属するポート。
Type	VLAN のメディア タイプ。
SAID	VLAN のセキュリティ アソシエーション ID 値。
MTU	VLAN の最大伝送単位サイズ。
Parent	親 VLAN（存在する場合）。
RingNo	VLAN のリング番号（該当する場合）。
BrdgNo	VLAN のブリッジ番号（該当する場合）。
Stp	VLAN で使用されるスパニングツリー プロトコル タイプ。
BrdgMode	この VLAN のブリッジング モード：可能な値はソースルート ブリッジング（SRB）およびソースルート トランスペアレント（SRT）で、デフォルトは SRB です。
Trans1	トランスレーション ブリッジ 1。
Trans2	トランスレーション ブリッジ 2。
Remote SPAN VLANs	設定されている RSPAN VLAN を識別します。

次に、**show vlan summary** コマンドの出力例を示します。

```
デバイス> show vlan summary
Number of existing VLANs              : 45
 Number of existing VTP VLANs         : 45
 Number of existing extended VLANS    : 0
```

次に、**show vlan id** コマンドの出力例を示します。

```
デバイス# show vlan id 2
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    VLAN0200                         active    Gi1/0/7, Gi1/0/8
```

```
2    VLAN0200                         active    Gi2/0/1, Gi2/0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
Disabled
```

show vtp

VLAN Trunking Protocol（VTP）管理ドメイン、ステータス、およびカウンタに関する一般情報を表示するには、EXEC モードで **show vtp** コマンドを使用します。

show vtp {**counters** | **devices** [**conflicts**] | **interface** [*interface-id*] | **password** | **status**}

構文の説明

counters	device の VTP 統計情報を表示します。
devices	ドメイン内のすべての VTP バージョン 3 デバイスに関する情報を表示します。このキーワードは、device が VTP バージョン 3 を実行していない場合だけ適用されます。
conflicts	（任意）競合するプライマリ サーバを持つ VTP バージョン 3 デバイスに関する情報を表示します。device が VTP トランスペアレントモードまたは VTP オフモードにある場合、このコマンドは無視されます。
interface	すべてのインターフェイスまたは指定されたインターフェイスに対する VTP のステータスおよび設定を表示します。
interface-id	（任意）VTP ステータスおよび設定を表示するインターフェイス。ここには物理インターフェイスまたはポート チャネルを指定できます。
password	設定された VTP パスワードを表示します（特権 EXEC モードでのみ使用可能）。
status	VTP 管理ドメインのステータスに関する一般情報を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

device が VTP バージョン 3 を実行中に **show vtp password** コマンドを入力すると、表示は次のルールに従います。

- **password** *password* グローバル コンフィギュレーション コマンドで **hidden** キーワードを指定せず、device 上で暗号化がイネーブルでない場合、パスワードはクリアテキストで表示されます。
- **password** *password*コマンドで **hidden** キーワードを指定せず、device 上で暗号化がイネーブルの場合、暗号化されたパスワードが表示されます。
- **password** *password* コマンドに **hidden** キーワードが含まれていた場合、16 進数の秘密キーが表示されます。

次に、**show vtp devices** コマンドの出力例を示します。**Conflict** 列の **Yes** は、応答するサーバがその機能のローカル サーバと競合していることを示します。つまり、同じドメイン内の 2 つの devices は、データベースに対して同じプライマリ サーバを持ちません。

```
デバイス# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf device ID      Primary Server Revision   System Name
             lict
------------ ---- --------------- -------------- ---------- ----------------------
VLAN         Yes  00b0.8e50.d000 000c.0412.6300 12354      main.cisco.com
MST          No   00b0.8e50.d000 0004.AB45.6000 24         main.cisco.com
VLAN         Yes  000c.0412.6300=000c.0412.6300 67         qwerty.cisco.com
```

次に、**show vtp counters** コマンドの出力例を示します。次の表に、この出力で表示される各フィールドについて説明します。

```
デバイス> show vtp counters
VTP statistics:
Summary advertisements received    : 0
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 0
Subset advertisements transmitted  : 0
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Gi1/0/47              0                0                0
Gi1/0/48              0                0                0
Gi2/0/1               0                0                0
Gi3/0/2               0                0                0
```

表 *66 : show vtp counters* のフィールドの説明

フィールド	説明
Summary advertisements received	トランクポート上でこの device が受信するサマリーアドバタイズメントの数。サマリー アドバタイズには、管理ドメイン名、コンフィギュレーション リビジョン番号、更新タイムスタンプと ID、認証チェックサム、および関連するサブセット アドバタイズの数が含まれます。
Subset advertisements received	トランクポート上でこの device が受信するサブセット アドバタイズメントの数。サブセット アドバタイズには、1 つ以上の VLAN に関する情報がすべて含まれています。
Request advertisements received	トランクポート上でこの device が受信するアドバタイズメント要求の数。アドバタイズ要求は、通常、すべての VLAN 上に関する情報を要求します。また、VLAN のサブセットに関する情報も要求できます。
Summary advertisements transmitted	トランクポート上でこの device が送信するサマリーアドバタイズメントの数。サマリー アドバタイズには、管理ドメイン名、コンフィギュレーション リビジョン番号、更新タイムスタンプと ID、認証チェックサム、および関連するサブセット アドバタイズの数が含まれます。
Subset advertisements transmitted	トランクポート上でこの device が送信するサブセット アドバタイズメントの数。サブセット アドバタイズには、1 つ以上の VLAN に関する情報がすべて含まれています。
Request advertisements transmitted	トランクポート上でこの device が送信するアドバタイズメント要求の数。アドバタイズ要求は、通常、すべての VLAN 上に関する情報を要求します。また、VLAN のサブセットに関する情報も要求できます。

フィールド	説明
Number of configuration revision errors	リビジョン エラーの数。 新しい VLAN の定義、既存 VLAN の削除、中断、または再開、あるいは既存 VLAN のパラメータ変更を行うと、device のコンフィギュレーション リビジョン番号が増加します。 リビジョン番号が device のリビジョン番号と一致するにもかかわらず、MD5 ダイジェスト値が一致しないアドバタイズメントを device が受信すると、リビジョンエラーが増加します。このエラーは、2 つの devices の VTP パスワードが異なるか、または devices の設定が異なることを意味します。 これらのエラーは、device が受信アドバタイズメントをフィルタしていて、これにより VTP データベースがネットワーク全体で同期されていない状態になっていることを示しています。
Number of configuration digest errors	MD5 ダイジェスト エラーの数。 サマリーパケット内の MD5 ダイジェストと、device によって計算された受信済みアドバタイズメントの MD5 ダイジェストが一致しない場合は、ダイジェストエラーが増加します。このエラーは、通常、2 つの devices の VTP パスワードが異なることを意味します。この問題を解決するには、すべての devices で VTP パスワードが同じになるようにします。 これらのエラーは、device が受信アドバタイズメントをフィルタしていて、これにより VTP データベースがネットワーク全体で同期されていない状態になっていることを示しています。

フィールド	説明
Number of V1 summary errors	バージョン 1 エラーの数。 VTP V2 モードの device が VTP バージョン 1 フレームを受信すると、バージョン1サマリー エラーが増加します。これらのエラーは、少なくとも 1 つの近接 device で、V2 モードがディセーブルにされた VTP バージョン 1、または VTP バージョン 2 が実行されていることを示しています。この問題を解決するには、VTP V2 モードの devices の設定をディセーブルに変更します。
Join Transmitted	トランク上で送信された VTP プルーニング メッセージの数。
Join Received	トランク上で受信された VTP プルーニング メッセージの数。
Summary Advts Received from non-pruning-capable device	トランク上で受信された、プルーニングをサポートしていないデバイスからの VTP サマリー メッセージの数。

次に、**show vtp status** コマンドの出力例を示します。次の表に、この出力で表示される各フィールドについて説明します。

```
デバイス> show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 2037.06ce.3580
Configuration last modified by 192.168.1.1 at 10-10-12 04:34:02
Local updater ID is 192.168.1.1 on interface LIIN0 (first layer3 interface found
)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 2
MD5 digest                        : 0xA0 0xA1 0xFE 0x4E 0x7E 0x5D 0x97 0x41
                                    0x89 0xB9 0x9B 0x70 0x03 0x61 0xE9 0x27
```

表 *67 : show vtp status* のフィールドの説明

フィールド	説明
VTP Version capable	device 上で動作できる VTP バージョンを表示します。

フィールド	説明
VTP Version running	device 上で動作中の VTP バージョンを表示します。デフォルトでは、device はバージョン 1 を実行しますが、バージョン 2 に設定することもできます。
VTP Domain Name	device の管理ドメインを特定する名前。
VTP Pruning Mode	プルーニングがイネーブルかまたはディセーブルかを表示します。VTP サーバでプルーニングをイネーブルにすると、管理ドメイン全体でプルーニングが有効になります。プルーニングを使用すると、トラフィックが適切なネットワーク デバイスにアクセスするために使用しなければならないトランク リンクへのフラッディング トラフィックが制限されます。
VTP Traps Generation	VTP トラップをネットワーク管理ステーションに送信するかどうかを表示します。
Device ID	ローカル デバイスの MAC アドレスを表示します。
Configuration last modified	最後に行った設定変更の日付と時刻を表示します。データベースの設定変更の原因となった device の IP アドレスを表示します。

フィールド	説明
VTP Operating Mode	VTP 動作モード（サーバ、クライアント、またはトランスペアレント）を表示します。 **Server**：VTP サーバモードの device は VTP に対してイネーブルであり、アドバタイズメントを送信します。スイッチで VLAN を設定できます。この device を使用すると、起動後に、現在の VTP データベース内のすべての VLAN 情報を、NVRAM から復元できます。デフォルトでは、すべての device が VTP サーバです。 （注） device が設定を NVRAM に書き込んでいる間に障害を検出し、NVRAM が機能するまでサーバモードに戻ることができない場合、スイッチは VTP サーバモードから VTP クライアントモードに自動的に変わります。 **Client**：VTP クライアントモードの device は VTP に対してイネーブルであり、アドバタイズメントを送信できますが、VLAN 設定を格納するために十分な不揮発性ストレージがありません。スイッチでは VLAN を設定できません。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。 **Transparent**：VTP トランスペアレントモードの device は、VTP に対してディセーブルであり、アドバタイズメントの送信や、他のデバイスから送信されたアドバタイズメントの学習を行いません。また、ネットワーク内の他のデバイスの VLAN 設定にも影響しません。device は VTP アドバタイズメントを受信し、アドバタイズメントを受信したトランクポートを除くすべてのトランクポートにこれを転送します。
Maximum VLANs Supported Locally	ローカルにサポートされている VLAN の最大数。
Number of Existing VLANs	既存の VLAN 数。

フィールド	説明
Configuration Revision	この device の現在のコンフィギュレーション リビジョン番号。
MD5 Digest	VTP 設定の 16 バイト チェックサム。

次の例では、VTP バージョン 3 を実行する device に対する **show vtp status** コマンドの出力を示します。

```
デバイス> show vtp status
VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : Cisco
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0021.1bcd.c700

Feature VLAN:
--------------
VTP Operating Mode : Server
Number of existing VLANs : 7
Number of existing extended VLANs : 0
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature MST:
--------------
VTP Operating Mode : Client
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature UNKNOWN:
----------------
```

switchport priority extend

着信したタグなしフレームのポートプライオリティ、または指定されたポートに接続された IP フォンが受信するフレームのプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **switchport priority extend** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

switchport priority extend {**cos** *value* | **trust**}
no switchport priority extend

構文の説明

cos *value*	PC から受信したか、または指定した Class of Service（CoS）値を持つ接続装置から受信した IEEE 802.1p プライオリティを上書きするよう IP Phone ポートを設定します。指定できる範囲は 0 ～ 7 です。7 が最も高いプライオリティです。デフォルトは 0 です。
trust	PC または接続装置から受信した IEEE 802.1p プライオリティを信頼するように IP Phone のポートを設定します。

コマンド デフォルト

ポートで受信したタグなしフレームには、デフォルト ポート プライオリティは、CoS 値 0 で設定されています。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

音声 VLAN をイネーブルにした場合、device を設定して、Cisco Discovery Protocol（CDP）パケットを送信し、Cisco IP 電話のアクセスポートに接続される装置からデータパケットを送信する方法を IP 電話に指示できます。Cisco IP 電話に設定を送信するには、Cisco IP 電話に接続している device ポートの CDP をイネーブルにする必要があります（デフォルトでは、CDP はすべての device インターフェイスでグローバルにイネーブルです）。

device アクセスポート上で音声 VLAN を設定する必要があります。

音声 VLAN をイネーブルにする前に、**trust device cisco-phone** インターフェイス コンフィギュレーション コマンドを入力してインターフェイス上で Quality of Service（QoS）をイネーブルに設定しておくことを推奨します。Auto QoS 機能を使用すると、これらは自動的に設定されます。

次の例では、受信した IEEE 802.1p プライオリティを信頼するように、指定されたポートに接続された IP Phone を設定する方法を示します。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# switchport priority extend trust
```

設定を確認するには、 **show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

switchport trunk

インターフェイスがトランキングモードの場合、トランクの特性を設定するには、インターフェイス コンフィギュレーション モードで **switchport trunk** コマンドを使用します。トランキング特性をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

switchport trunk {**allowed vlan** *vlan-list* | **native vlan** *vlan-id* | **pruning vlan** *vlan-list* }

no switchport trunk {**allowed vlan** | **native vlan** | **pruning vlan**}

構文の説明

allowed vlan *vlan-list*	トランキング モードの場合に、このインターフェイス上でタグ付き形式のトラフィックを送受信できる許可VLANのリストを設定します。*vlan-list*の選択については、「使用上のガイドライン」を参照してください。
native vlan *vlan-id*	インターフェイスが IEEE 802.1Q トランキング モードの場合に、タグなしトラフィックを送受信するようにネイティブ VLAN を設定します。指定できる範囲は 1 ～ 4094 です。
pruning vlan *vlan-list*	トランキング モードの場合に、VTP プルーニングに適格な VLAN のリストを設定します。*vlan-list*の選択については、「使用上のガイドライン」を参照してください。

コマンド デフォルト

VLAN 1 は、ポートのデフォルトのネイティブ VLAN ID です。

すべての VLAN リストのデフォルトには、すべての VLAN が含まれます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

vlan-list の形式は、**all | none | [add | remove | except]** *vlan-atom* [*,vlan-atom...*] です。:

- **all** 1 ～ 4094 のすべての VLAN を指定します。これはデフォルトです。このキーワードは、リストのすべての VLAN を同時に設定することを許可しないコマンド上では使用できません。
- **none** 空のリストを指定します。特定の VLAN を設定するか、または少なくとも 1 つの VLAN を設定する必要があるコマンドでは、このキーワードを使用できません。
- **add** リストを置き換えるのではなく、現在設定されている VLAN に VLAN の定義済みリストを追加します。有効な ID は 1 ～ 1005 です。場合によっては、拡張範囲 VLAN（VLAN ID が 1005 より上）を使用できます。

  （注） 許可 VLAN リストに拡張範囲 VLAN を追加できますが、プルーニング適格 VLAN リストには追加できません。

  カンマを使い、連続しない VLAN ID を区切ります。ID の範囲を指定するには、ハイフンを使用します。
- **remove** リストを置き換えるのではなく、現在設定されている VLAN から VLAN の定義済みリストを削除します。有効な ID は 1 ～ 1005 です。場合によっては、拡張範囲 VLAN ID を使用できます。

（注） 許可VLANリストから拡張範囲VLANを削除できますが、プルーニング適格リストからは削除できません。

- **except** 定義済み VLAN リスト以外の、計算する必要がある VLAN を示します（指定されている VLAN 以外の VLAN が追加されます）。有効な ID の範囲は 1 ～ 1005 です。カンマを使い、連続しない VLAN ID を区切ります。ID の範囲を指定するには、ハイフンを使用します。
- *vlan-atom* は、1 ～ 4094 内の単一の VLAN 番号、または 2 つの VLAN 番号で指定された連続した範囲の VLAN で、小さい方の値を先頭にハイフンで区切ります。

ネイティブ VLAN：

- IEEE 802.1Q トランク ポートで受信されたすべてのタグなしトラフィックは、ポートに設定されたネイティブ VLAN によって転送されます。
- パケットの VLAN ID が送信側ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信します。
- **native vlan** コマンドの **no** 形式は、ネイティブモード VLAN を、デバイスに適したデフォルト VLAN にリセットします。

許可 VLAN：

- スパニングツリー ループまたはストームのリスクを減らすには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートの VLAN 1 をディセーブルにできます。トランク ポートから VLAN 1 を削除した場合、インターフェイスは管理トラフィック（Cisco Discovery Protocol（CDP）、ポート集約プロトコル（PAgP）、Link Aggregation Control Protocol（LACP）、ダイナミック トランキング プロトコル（DTP）、および VLAN 1 の VLAN トランキング プロトコル（VTP））を送受信し続けます。
- **allowed vlan** コマンドの **no** 形式は、リストをデフォルトリスト（すべての VLAN を許可）にリセットします。

トランク プルーニング：

- プルーニング適格リストは、トランク ポートだけに適用されます。
- トランク ポートごとに独自の適格リストがあります。
- VLAN をプルーニングしない場合は、プルーニング適格リストから VLAN を削除します。プルーニング不適格の VLAN は、フラッディング トラフィックを受信します。
- VLAN 1、VLAN 1002 ～ 1005、および拡張範囲 VLAN（VLAN 1006 ～ 4094）は、プルーニングできません。

次の例では、すべてのタグなしトラフィックを送信するポートのデフォルトとして、VLAN 3 を設定する方法を示します。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# switchport trunk native vlan 3
```

次の例では、許可リストに VLAN 1、2、5、および 6 を追加する方法を示します。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

次の例では、プルーニング適格リストから VLAN 3 および 10 ～ 15 を削除する方法を示します。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# switchport trunk pruning vlan remove 3,10-15
```

設定を確認するには、 **show interfaces** *interface-id* **switchport** 特権 EXEC コマンドを入力します。

vlan

VLAN を追加して、VLAN コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **vlan** コマンドを使用します。VLAN を削除するには、このコマンドの **no** 形式を使用します。

vlan *vlan-id*
no vlan *vlan-id*

構文の説明

vlan-id	追加および設定する VLAN の ID。指定できる範囲は 1 ～ 4094 です。1 つの VLAN ID、それぞれをカンマで区切った一連の VLAN ID、またはハイフンを間に挿入した VLAN ID の範囲を入力できます。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

通常範囲の VLAN（VLAN ID 1 ～ 1005）や拡張範囲 VLAN（VLAN ID 1006 ～ 4094）を追加するには、**vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用します。通常範囲の VLAN の設定情報は常に VLAN データベースに保存されます。この情報を表示するには、**show vlan** 特権 EXEC コマンドを入力します。VTP モードがトランスペアレントである場合、通常

範囲の VLAN の VLAN 設定情報も device の実行コンフィギュレーション ファイルに保存されます。拡張範囲の VLAN ID は VLAN データベースに保存されず、スイッチの実行コンフィギュレーションファイルに保存されます。また、設定をスタートアップ コンフィギュレーション ファイルに保存できます。

VTP バージョン 3 は拡張範囲 VLAN の伝播をサポートしています。VTP バージョン 1 および 2 で伝播する範囲は、VLAN 1 ～ 1005 だけです。

VLAN および VTP 設定をスタートアップ コンフィギュレーション ファイルに保存して device をリブートすると、設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

無効な VLAN ID を入力すると、エラー メッセージが表示され、VLAN コンフィギュレーション モードを開始できません。

VLAN ID を指定して **vlan** コマンドを入力すると、VLAN コンフィギュレーション モードがイネーブルになります。既存の VLAN の VLAN ID を入力すると、新しい VLAN は作成されませんが、その VLAN の VLAN パラメータを変更できます。指定された VLAN は、VLAN コンフィギュレーション モードを終了したときに追加または変更されます。（VLAN 1 ～ 1005 の）**shutdown** コマンドだけがただちに有効になります。

（注） すべてのコマンドが表示されますが、拡張範囲 VLAN でサポートされる VLAN コンフィギュレーション コマンドは **remote-span** だけです。拡張範囲 VLAN の場合、他のすべての特性はデフォルト ステートのままにしておく必要があります。

次のコンフィギュレーション コマンドを VLAN コンフィギュレーション モードで利用できます。各コマンドの **no** 形式を使用すると、特性がそのデフォルト ステートに戻ります。

- **are** *are-number*：この VLAN の全ルート エクスプローラ（ARE）ホップの最大数を定義します。このキーワードは、TrCRF VLAN だけに適用されます。指定できる範囲は 0 ～ 13 です。デフォルト値は 7 です。値が入力されない場合、最大数は 0 であると見なされます。
- **backupcrf**：バックアップ CRF モードを指定します。このキーワードは、TrCRF VLAN だけに適用されます。
  - **enable**：この VLAN のバックアップ CRF モード。

- **disable**：この VLAN のバックアップ CRF モード（デフォルト）。

- **bridge** {*bridge-number* | **type**}：論理分散ソース ルーティング ブリッジ、つまり、FDDI-NET、トークンリング NET、および TrBRF VLAN 内で親 VLAN としてこの VLAN を持つすべての論理リングと相互接続するブリッジを指定します。指定できる範囲は 0 ～ 15 です。FDDI-NET、TrBRF、およびトークン リング NET VLAN については、デフォルトのブリッジ番号は 0（ソース ルーティング ブリッジなし）です。**type** キーワードは、TrCRF VLAN だけに適用され、次のうちのいずれかです。

  - **srb**：ソースルート ブリッジング。

  - **srt**：（ソースルート トランスペアレント）ブリッジング VLAN

- **exit**：変更を適用し、VLAN データベース リビジョン番号（VLAN 1 ～ 1005）を増加させ、VLAN コンフィギュレーション モードを終了します。

- **media**：VLAN メディア タイプを定義します。タイプは次のいずれかになります。

  （注） device がサポートするのは、イーサネット ポートだけです。FDDI およびトークン リング メディア固有の特性は、別の devices に対する VLAN Trunking Protocol（VTP）グローバル アドバタイズメントに限って設定します。これらの VLAN はローカルに停止されます。

  - **ethernet**：イーサネット メディア タイプ（デフォルト）。

  - **fd-net**：FDDI ネットワーク エンティティ タイトル（NET）メディア タイプ。

  - **fddi**：FDDI メディア タイプ。

  - **tokenring**：VTP v2 モードがディセーブルの場合は、トークン リング メディア タイプ。VTP バージョン 2（v）モードがイネーブルの場合は、TrCRF。

  - **tr-net**：VTP v2 モードがディセーブルの場合は、トークン リング ネットワーク エンティティ タイトル（NET）メディア タイプ。VTP v2 モードがイネーブルの場合は、TrBRF メディア タイプ。

  さまざまなメディア タイプで有効なコマンドおよび構文については、下の表を参照してください。

- **name** *vlan-name*：管理ドメイン内で一意である 1 ～ 32 文字の ASCII 文字列で VLAN に名前を付けます。デフォルトは VLANxxxx です。ここで、xxxx は VLAN ID 番号と同じ 4 桁の数字（先行ゼロを含む）です。

- **no**：コマンドを無効にするか、またはデフォルト設定に戻します。

- **parent** *parent-vlan-id*：既存の FDDI、トークンリング、または TrCRF VLAN の親 VLAN を指定しますこのパラメータは、TrCRF が所属する TrBRF を識別するもので、TrCRF を

定義するときに必要です。指定できる範囲は 0 ～ 1005 です。デフォルトの親 VLAN ID は、FDDI およびトークンリング VLAN では 0（親 VLAN なし）です。トークンリングおよび TrCRF VLAN の両方で、親 VLAN ID はデータベースにすでに存在していて、トークンリング NET または TrBRF VLAN と関連付けられている必要があります。

- **remote-span**：VLAN をリモート SPAN（RSPAN）VLAN として設定します。RSPAN 機能が既存の VLAN に追加される場合、まず VLAN は削除され、次に RSPAN 機能とともに再生されます。RSPAN 機能が削除されるまで、どのアクセス ポートも非アクティブになります。VTP がイネーブルの場合、新しい RSPAN VLAN は、1024 より小さい数字の VLAN ID の VTP により伝播されます。ラーニングは VLAN 上でディセーブルになります。

- **ring** *ring-number*：FDDI、トークンリング、または TrCRF VLAN の論理リングを定義します。指定できる範囲は 1 ～ 4095 です。トークンリング VLAN のデフォルト値は 0 です。FDDI VLAN には、デフォルト設定はありません。

- **said** *said-value*：IEEE 802.10 に記載されているセキュリティ アソシエーション ID（SAID）を指定します。指定できる ID は、1 ～ 4294967294 です。この数字は、管理ドメイン内で一意である必要があります。デフォルト値は、100000 に VLAN ID 番号を加算した値です。

- **shutdown**：VLAN 上で VLAN スイッチングをシャットダウンします。このコマンドはただちに有効になります。他のコマンドは、VLAN コンフィギュレーション モードを終了したときに有効になります。

- **state**：VLAN の状態を指定します。
  - **active** VLAN が稼働中であることを意味します（デフォルト）。
  - **suspend** VLAN が停止していることを意味します。停止している VLAN はパケットを通過させません。

- **ste** *ste-number*：スパニングツリーエクスプローラ（STE）ホップの最大数を定義します。このキーワードは、TrCRF VLAN だけに適用されます。指定できる範囲は 0 ～ 13 です。デフォルト値は 7 です。

- **stp type**：FDDI-NET、トークンリング NET、または TrBRF VLAN のスパニングツリー タイプを定義します。FDDI-NET VLAN の場合、デフォルトの STP タイプは ieee です。トークン リング NET VLAN の場合、デフォルトの STP タイプは ibm です。FDDI およびトークン リング VLAN の場合、デフォルトのタイプは指定されていません。
  - **ieee**：ソースルート トランスペアレント（SRT）ブリッジングを実行している IEEE イーサネット STP。
  - **ibm**：ソースルート ブリッジング（SRB）を実行している IBM STP。
  - **auto**：ソースルート トランスペアレント（SRT）ブリッジング（IEEE）およびソースルート ブリッジング（IBM）の組み合わせを実行している STP。

- **tb-vlan1** *tb-vlan1-id* および **tb-vlan2** *tb-vlan2-id*：この VLAN にトランスレーショナル ブリッジングが行われている 1 番めおよび 2 番めの VLAN を指定します。トランスレーショ

ナルVLANは、たとえばFDDIまたはトークンリングをイーサネットに変換します。指定できる範囲は0～1005です。値が指定されないと、0（トランスレーショナルブリッジングなし）と見なされます。

表 *68 :* さまざまなメディア タイプで指定できるコマンドと構文

メディア タイプ	指定できる構文
イーサネット	**name** *vlan-name*, **media ethernet**, **state** {**suspend** | **active**}, **said** *said-value*, **remote-span**, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
FDDI	**name** *vlan-name*, **media fddi**, **state** {**suspend** | **active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
FDDI-NET	**name** *vlan-name*, **media fd-net** , **state** {**suspend** | **active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee** | **ibm** | **auto**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id* VTP v2 モードがディセーブルの場合は、**stp type** を **auto.** に設定しないでください
Token Ring	VTP v1 モードはイネーブルです。 **name** *vlan-name*, **media tokenring**, **state** {**suspend** | **active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
トークンリング コンセントレータ リレー機能（TrCRF）	VTP v2 モードはイネーブルです。 **name** *vlan-name*, **media tokenring**, **state** {**suspend** | **active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **bridge type** {**srb** | **srt**}, **are** *are-number*, **ste** *ste-number*, **backupcrf** {**enable** | **disable**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
トークンリング NET	VTP v1 モードはイネーブルです。 **name** *vlan-name*, **media tr-net**, **state** {**suspend** | **active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee** | **ibm**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
トークンリング ブリッジ リレー機能（TrBRF）	VTP v2 モードはイネーブルです。 **name** *vlan-name*, **media tr-net**, **state** {**suspend** | **active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee** | **ibm** | **auto**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*

次の表に、VLAN の設定ルールを示します。

表 *69 : VLAN* 設定ルール

設定	ルール
VTP v2 モードがイネーブルで、TrCRF VLAN メディア タイプを設定している場合	すでにデータベースに存在している TrBRF の親 VLAN ID を指定します。 リング番号を指定します。このフィールドを空白のままにしないでください。 TrCRF VLAN に同じ親 VLAN ID がある場合には一意のリング番号を指定します。1 つのバックアップ コンセントレータ リレー機能（CRF）だけをイネーブルにすることができます。
VTP v2 モードがイネーブルで、TrCRF メディア タイプ以外の VLAN を設定している場合	バックアップ CRF を指定しないでください。
VTP v2 モードがイネーブルで、TrBRF VLAN メディア タイプを設定している場合	ブリッジ番号を指定します。このフィールドを空白のままにしないでください。
VTP v1 モードがイネーブルの場合	VLAN の STP タイプを auto に設定しないでください。 このルールは、イーサネット、FDDI、FDDI-NET、トークンリング、およびトークンリング NET VLAN に適用されます。

設定	ルール
トランスレーショナル ブリッジングが必要な VLAN を追加する場合（値は 0 に設定されない）	使用されるトランスレーショナル ブリッジング VLAN ID は、すでにデータベースに存在している必要があります。 （たとえば、イーサネットは FDDI をポイントし、FDDI はイーサネットをポイントするというように）コンフィギュレーションがポイントしているトランスレーショナル ブリッジング VLAN ID にも、トランスレーショナル ブリッジング パラメータの 1 つに元の VLAN へのポインタが含まれている必要があります。 コンフィギュレーションがポイントするトランスレーショナル ブリッジング VLAN ID は、（たとえば、イーサネットはトークンリングをポイントすることができるというように）元の VLAN とは異なるメディア タイプである必要があります。 両方のトランスレーショナル ブリッジング VLAN ID が設定されている場合、（たとえば、イーサネットは FDDI およびトークンリングをポイントすることができるというように）これらの VLAN は異なるメディア タイプである必要があります。

次の例では、デフォルトのメディア特性を持つイーサネット VLAN を追加する方法を示します。デフォルトには VLAN *xxxx* の *vlan-name* が含まれています。ここで、*xxxx* は VLAN ID 番号と同じ 4 桁の数字（先行ゼロを含む）です。デフォルトの media は ethernet です。state は active です。デフォルトの said-value は、100000 に VLAN ID を加算した値です。mtu-size 変数は 1500、stp-type は ieee です。**exit** VLAN コンフィギュレーション コマンドを入力した場合、VLAN がまだ存在していなかった場合にはこれが追加されます。そうでない場合、このコマンドは何も作用しません。

次に、新しい VLANをすべてデフォルトの特性で 作成し、VLAN コンフィギュレーション モードを開始する例を示します。

```
デバイス(config)# vlan 200
デバイス(config-vlan)# exit
デバイス(config)#
```

次に、新しい拡張範囲 VLAN をすべてデフォルトの特性で作成して、VLAN コンフィギュレーション モードを開始し、新しい VLAN を device のスタートアップ コンフィギュレーション ファイルに保存する例を示します。

```
デバイス(config)# vlan 2000
デバイス(config-vlan)# end
```

```
デバイス# copy running-config startup config
```

設定を確認するには、**show vlan** 特権 EXEC コマンドを入力します。

vtp（グローバル コンフィギュレーション）

VLAN トランキングプロトコル（VTP）設定の特性を設定するか、または変更するには、グローバル コンフィギュレーション モードで **vtp** コマンドを使用します。この設定を削除したりデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

vtp {**domain** *domain-name* | **file** *filename* | **interface** *interface-name* [**only**] | **mode** {**client** | **off** | **server** | **transparent**} [{**mst** | **unknown** | **vlan**}] | **password** *password* [{**hidden** | **secret**}] | **pruning** | **version** *number*}
no vtp {**file** | **interface** | **mode** [{**client** | **off** | **server** | **transparent**}] [{**mst** | **unknown** | **vlan**}] | **password** | **pruning** | **version**}

構文の説明

domain *domain-name*	VTP ドメイン名を device の VTP 管理ドメインを識別する 1 ～ 32 文字の ASCII 文字列で指定します。ドメイン名では大文字と小文字が区別されます。
file *filename*	VTP VLAN 設定が保存されている Cisco IOS ファイル システム ファイルを指定します。
interface *interface-name*	このデバイスで更新された VTP ID を提供するインターフェイスの名前を指定します。
only	（任意）VTP IP アップデータとしてこのインターフェイスの IP アドレスだけを使用します。
mode	VTP デバイス モードをクライアント、サーバ、またはトランスペアレントに指定します。
client	device を VTP クライアントモードにします。VTP クライアントモードの device は VTP に対してイネーブルであり、アドバタイズメントを送信できますが、VLAN 設定を格納するための十分な不揮発性メモリがありません。VTP クライアントでは、VLAN を設定できません。VLAN は、ドメインに含まれる、他のサーバ モードの device で設定します。VTP クライアントが起動すると、VTP クライアントはその VLAN データベースを初期化するアドバタイズを受信するまで、VTP アドバタイズを送信しません。
off	device を VTP オフモードにします。VTP オフモードの device は、トランクポート上で VTP アドバタイズメントを転送しないことを除いて、VTP トランスペアレントデバイスと同様に機能します。

server	device を VTP サーバモードにします。VTP サーバモードの device は VTP に対してイネーブルであり、アドバタイズメントを送信します。device で VLAN を設定できます。device は、再起動後に、不揮発性メモリから現在の VTP データベース内のすべての VLAN 情報を回復できます。
transparent	device を VTP トランスペアレントモードにします。VTP トランスペアレントモードの device は、VTP に対してディセーブルであり、アドバタイズメントの送信や、他のデバイスから送信されたアドバタイズメントからの学習を行いません。また、ネットワーク内の他のデバイスの VLAN 設定に影響を与えることはありません。device は VTP アドバタイズメントを受信し、アドバタイズメントを受信したトランクポートを除くすべてのトランクポートにこれを転送します。 VTP モードがトランスペアレントである場合、モードおよびドメイン名は device の実行コンフィギュレーション ファイルに保存されます。この情報を device のスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup config** 特権 EXEC コマンドを入力します。
mst	（任意）マルチ スパニングツリー（MST）VTP データベース（VTP バージョン 3 に限る）にモードを設定します。
unknown	（任意）未知の VTP データベース（VTP バージョン 3 に限る）にモードを設定します。
vlan	（任意）VLAN VTP データベースにモードを設定します。これがデフォルトです（VTP バージョン 3 に限る）。
password *password*	VTP アドバタイズメントで送信され、受信 VTP アドバタイズメントを確認するための MD5 ダイジェスト計算で使用される 16 バイトの秘密値を生成するための管理ドメイン パスワードを設定します。パスワードは、1 ～ 32 文字の ASCII 文字列です。パスワードでは大文字と小文字が区別されます。
hidden	（任意）パスワード文字列から生成されたキーが VLAN データベース ファイルに保存されることを指定します。**hidden** キーワードを指定しない場合、パスワード文字列はクリアテキストに保存されます。hidden パスワードを入力した場合、そのパスワードを再入力し、ドメイン内でコマンドを実行する必要があります。このキーワードは、VTP バージョン 3 だけでサポートされています。
secret	（任意）ユーザがパスワードの秘密キーを直接設定できるようにします（VTP バージョン 3 に限る）。
pruning	device 上で VTP プルーニングをイネーブルにします。
version *number*	VTP バージョンをバージョン 1、バージョン 2、またはバージョン 3 に設定します。

コマンド デフォルト　デフォルトのファイル名は *flash:vlan.dat* です。

デフォルト モードはサーバ モードで、デフォルトのデータベースは VLAN です。

VTP バージョン 3 では、MST データベースのデフォルト モードはトランスペアレントです。

ドメイン名またはパスワードは定義されていません。

パスワードは設定されていません。

プルーニングはディセーブルです。

デフォルトのバージョンはバージョン 1 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

VTP モード、ドメイン名、および VLAN 設定を device のスタートアップ コンフィギュレーション ファイルに保存して、device を再起動すると、VTP および VLAN 設定は次の条件によって選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントであり、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。

新規データベースをロードするのに **vtp file** *filename* を使用することはできません。これは、既存のデータベースが保存されているファイルの名前を変更するだけです。

VTP ドメイン名を設定するときには、次の注意事項に従ってください。

- ドメイン名を設定するまで、device は非管理ドメインステートの状態です。非管理ドメインステートの間は、ローカル VLAN 設定に変更が生じても、device は VTP アドバタイズメントを送信しません。device は、トランキングを行っているポートで最初の VTP サマリーパケットを受信した後、または **vtp domain** コマンドでドメイン名を設定した後で、非管理ドメインステートから抜け出します。device は、サマリーパケットからドメインを受信した場合、そのコンフィギュレーション リビジョン番号を 0 にリセットします。device が非管理ドメインステートから抜け出したあと、NVRAM をクリアしてソフトウェアをリロードするまで、スイッチがこのステートに再び入るよう設定することはできません。
- ドメイン名では、大文字と小文字が区別されます。
- 設定したドメイン名は、削除できません。別のドメインに再度割り当てるしかありません。

VTP モードを設定するときには、次の注意事項に従ってください。

- **no vtp mode** コマンドを使用すると、device を VTP サーバモードに戻すことができます。
- **vtp mode server** コマンドは、device がクライアントモードまたはトランスペアレントモードでない場合にエラーを返さないことを除けば、**no vtp mode** と同じです。
- 受信 device がクライアントモードである場合、クライアント device はその設定を変更して、サーバの設定をコピーします。クライアントモードの devices がある場合には、必ずサーバモードの device ですべての VTP または VLAN 設定変更を行ってください。サーバモードのスイッチの方が、保持している VTP コンフィギュレーション リビジョン番号が大きいためです。受信 device がトランスペアレントモードである場合、その device の設定は変更されません。
- トランスペアレントモードの device は、VTP に参加しません。トランスペアレントモードの device で VTP または VLAN 設定の変更を行った場合、その変更はネットワーク内の他の devices には伝播されません。
- サーバモードの device で VTP または VLAN 設定を変更した場合、その変更は同じ VTP ドメインのすべての devices に伝播されます。
- **vtp mode transparent** コマンドは、ドメインの VTP をディセーブルにしますが、device からドメインを削除しません。
- VTP バージョン 1 および 2 では、VTP および VLAN 情報を実行コンフィギュレーション ファイルに保存する場合には、VTP モードはトランスペアレントに設定してください。
- VTP バージョン 1 および 2 では、拡張範囲 VLAN がスイッチで設定されている場合には、VTP モードをクライアントまたはサーバに変更できません。VTP モードは、VTP バージョン 3 で拡張 VLAN を使用することにより変更できます。
- 拡張範囲 VLAN を追加したり、VTP および VLAN 情報を実行コンフィギュレーション ファイルに保存したりする場合には、VTP モードはトランスペアレントに設定してください。
- ダイナミック VLAN 作成がディセーブルの場合、VTP に設定できるモードは、サーバ モードまたはクライアント モードのいずれかに限ります。
- **vtp mode off** コマンドを使用すると、デバイスをオフに設定します。**no vtp mode off** コマンドを使用すると、デバイスを VTP サーバモードにリセットします。

VTP パスワードを設定するときには、次の注意事項に従ってください。

- パスワードは大文字と小文字が区別されます。パスワードは、同じドメイン内のすべての devices で一致している必要があります。
- device をパスワードが設定されていない状態に戻す場合は、このコマンドの **no vtp password** 形式を使用します。
- **hidden** および **secret** キーワードは、VTP バージョン 3 だけでサポートされています。VTP バージョン 2 から VTP バージョン 3 に変換する場合、変換前に hidden または secret キーワードを削除する必要があります。

VTP プルーニングを設定するときには、次の注意事項に従ってください。

- VTP プルーニングは、プルーニング適格 VLAN に所属するステーションがない場合、その VLAN の情報を VTP 更新から削除します。
- VTP サーバでプルーニングをイネーブルにすると、プルーニングは VLAN ID 1 ～ 1005 の管理ドメイン全体でイネーブルになります。
- プルーニング適格リストに指定された VLAN だけが、プルーニングの対象になります。
- プルーニングは、VTP バージョン 1 およびバージョン 2 でサポートされています。

VTP バージョンを設定するときには、次の注意事項に従ってください。

- バージョン 2（v2）モード ステートを切り替えると、ある一定のデフォルト VLAN のパラメータが変更されます。
- 各 VTP device は他のすべての VTP デバイスの機能を自動的に検出します。VTP バージョン 2 を使用するには、ネットワーク内のすべての VTP devices でバージョン 2 がサポートされている必要があります。そうでない場合、VTP バージョン 1 モードで稼働するよう設定する必要があります。
- ドメイン内のすべての devices が VTP バージョン 2 対応である場合、1 つの device でバージョン 2 を設定すれば、バージョン番号は、VTP ドメイン内の他のバージョン 2 対応 devices に伝播されます。
- トークンリング環境で VTP を使用している場合、VTP バージョン 2 もイネーブルである必要があります。
- Token Ring Bridge Relay Function（TrBRF）または Token Ring Concentrator Relay Function（TrCRF）VLAN メディア タイプを設定している場合には、バージョン 2 を使用してください。
- トークンリングまたはトークンリング NET VLAN メディア タイプを設定している場合には、バージョン 1 を使用してください。
- VTP バージョン 3 では、VLAN データベース情報だけでなく、すべてのデータベース VTP 情報がその VTP ドメイン全体に伝播します。
- VTP バージョン 3 の 2 つのリージョンが、VTP バージョン 1 または VTP バージョン 2 のリージョン経由で通信できるのは、トランスペアレントモードの場合に限られます。

device コンフィギュレーション ファイルにパスワード、プルーニング、およびバージョン コンフィギュレーションを保存することはできません。

次の例では、VTP コンフィギュレーション ストレージのファイル名を vtpfilename に変更する方法を示します。

```
デバイス(config)# vtp file vtpfilename
```

次の例では、デバイス ストレージのファイル名をクリアする方法を示します。

```
デバイス(config)# no vtp file vtpconfig
Clearing device storage filename.
```

次の例では、このデバイスの VTP アップデータ ID を提供するインターフェイスの名前を指定する方法を示します。

```
デバイス(config)# vtp interface gigabitethernet
```

次の例では、deviceの管理ドメインを設定する方法を示します。

```
デバイス(config)# vtp domain OurDomainName
```

次の例では、deviceを VTP トランスペアレントモードにする方法を示します。

```
デバイス(config)# vtp mode transparent
```

次の例では、VTP ドメイン パスワードを設定する方法を示します。

```
デバイス(config)# vtp password ThisIsOurDomainsPassword
```

次の例では、VLAN データベースでのプルーニングをイネーブルにする方法を示します。

```
デバイス(config)# vtp pruning
Pruning switched ON
```

次の例では、VLAN データベースのバージョン 2 モードをイネーブルにする方法を示します。

```
デバイス(config)# vtp version 2
```

設定を確認するには、**show vtp status** 特権 EXEC コマンドを入力します。

vtp（インターフェイス コンフィギュレーション）

ポート単位で VLAN Trunking Protocol（VTP）をイネーブルにするには、インターフェイス コンフィギュレーション モードで **vtp** コマンドを使用します。インターフェイスで VTP をディセーブルにするには、このコマンドの **no** 形式を使用します。

vtp
no vtp

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、トランキング モードのインターフェイスでのみ入力してください。

このコマンドは、device が VTP バージョン 3 を実行している場合にのみサポートされます。

次の例では、インターフェイス上で VTP をイネーブルにする方法を示します。

```
デバイス(config-if)# vtp
```

次の例では、インターフェイス上で VTP をディセーブルにする方法を示します。

```
デバイス(config-if)# no vtp
```

vtp primary

device を VLAN Trunking Protocol（VTP）プライマリサーバとして設定するには、特権 EXEC モードで **vtp primary** コマンドを使用します。

vtp primary [{**mst** | **vlan**}] [**force**]

構文の説明

mst	（任意）device をマルチ スパニング ツリー（MST）機能のプライマリ VTP サーバとして設定します。
vlan	（任意）device を VLAN のプライマリ VTP サーバとして設定します。
force	（任意）プライマリサーバを設定するときに device が競合するデバイスをチェックしないように設定します。

コマンド デフォルト

device は VTP セカンダリサーバです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	このコマンドが導入されました。

使用上のガイドライン

VTP プライマリ サーバはデータベース情報をアップデートし、システム内のすべてのデバイスによって行われるアップデートを送信します。VTP セカンダリ サーバは、プライマリ サーバから受信したアップデートされた VTP のコンフィギュレーションを NVRAM にバックアップすることだけができます。

デフォルトでは、すべてのデバイスはセカンダリ サーバとして起動します。プライマリ サーバのステータスは、管理者がドメイン内のテイクオーバー メッセージを発行する場合のデータ

ベース アップデートのためだけに必要です。プライマリ サーバなしで実用 VTP ドメインを持つことができます。

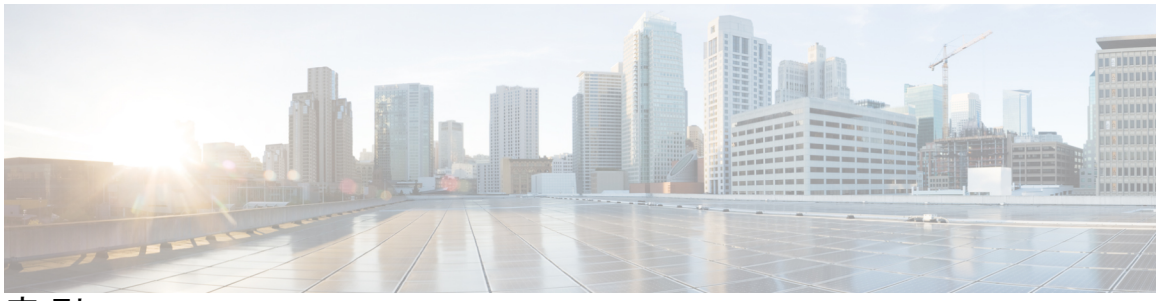
デバイスがリロードするかドメイン パラメータが変更された場合、プライマリ サーバのステータスは失われます。

（注） このコマンドは、device が VTP バージョン 3 を実行している場合にのみサポートされます。

次の例では、device を VLAN のプライマリ VTP サーバとして設定する方法を示します。

```
デバイス# vtp primary vlan
Setting device to VTP TRANSPARENT mode.
```

設定を確認するには、**show vtp status** 特権 EXEC コマンドを入力します。



索 引

A

B

C

D

E

F

H

I

L

M

N

O

P

Q

R

S

T

U

V

す

は

ふ

り