IPv6 コンフィギュレーション ガイド、Cisco IOS XE リリース 3SE（Catalyst 3650 スイッチ）

初版：2013 年 10 月 10 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/

Text Part Number: OL-30687-01-J

目 次

はじめに

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します （ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
bold フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
Italic フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*italic* フォントで示しています。
`courier` フォント	システムが表示するターミナル セッションおよび情報は、`courier` フォントで示しています。
`courier` フォント	太字の **`courier`** フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。

表記法	説明
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。 角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。 string の前後には引用符を使用しません。 引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

（注） 「注釈」です。 役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。 機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス　時間を節約する方法です。 ここに紹介している方法で作業を行うと、時間を短縮できます。

警告　**「警告」の意味です。 人身事故を予防するための注意事項が記述されています。**

関連資料

（注）　スイッチをインストールまたはアップグレードする前に、スイッチのリリース ノートを参照してください。

- 次の URL にある Cisco Catalyst 3650 スイッチ のマニュアル：

  http://www.cisco.com/go/cat3650_docs

- 次の URL にある Cisco SFP および SFP+ モジュールのマニュアル（互換性マトリクスを含む）：

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html

- 次の URL にあるエラー メッセージ デコーダ：

  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。 RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

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に関する情報

コマンド モード

Cisco IOS ユーザ インターフェイスは、いくつかのモードに分かれています。 使用できるコマンドの種類は、現在のモードによって異なります。 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。

CLI セッションはコンソール接続、Telnet、SSH、またはブラウザを使用することによって開始できます。

セッションを開始するときは、ユーザ モード（別名ユーザ EXEC モード）が有効です。 ユーザ EXEC モードでは、限られた一部のコマンドしか使用できません。 たとえばユーザ EXEC コマンドの大部分は、**show** コマンド（現在のコンフィギュレーション ステータスを表示する）、**clear** コマンド（カウンタまたはインターフェイスをクリアする）などのように、1 回限りのコマンドです。 ユーザ EXEC コマンドは、スイッチをリブートするときには保存されません。

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

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

ローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モードおよびライン コンフィギュレーション モードに移行できます。

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

表 *1*：コマンド モードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	Telnet、SSH、またはコンソールを使用してセッションを開始します。	`Switch>`	**logout** または **quit** を入力します。	このモードを使用して次の作業を行います。 • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードで、**enable** コマンドを入力します。	`Switch#`	**disable** を入力して終了します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure** コマンドを入力します。	`Switch(config)#`	終了して特権 EXEC モードに戻るには、**exit** または **end** コマンドを入力するか、Ctrl+Z を押します。	このモードは、スイッチ全体に適用するパラメータを設定する場合に使用します。
VLAN コンフィギュレーション	グローバル コンフィギュレーション モードで、**vlan** *vlan-id* コマンドを入力します。	`Switch(config-vlan)#`	グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを入力します。 特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	

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

ヘルプ システムの使用

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

手順の概要

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

手順の詳細

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

ステップ 2	*abbreviated-command-entry* **?**
	
	例：
	`Switch# di?`
	`dir disable disconnect`
		特定のストリングで始まるコマンドのリストを表示します。

ステップ 3	*abbreviated-command-entry* <Tab>
	
	例：
	`Switch# sh conf<tab>`
	`Switch# show configuration`
		特定のコマンド名を補完します。

ステップ 4	**?** 例： `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。
ステップ 5	*command* **?** 例： `Switch> show ?`	コマンドに関連するキーワードを一覧表示します。

	コマンドまたはアクション	目的

ステップ 6	*command keyword* **?**
	
	例：
	`Switch(config)# cdp holdtime ?`
	`  <10-255> Length of time (in sec) that receiver must keep this packet`
		キーワードに関連する引数を一覧表示します。

コマンドの省略形

スイッチでコマンドが一意に認識される長さまでコマンドを入力します。

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

```
Switch# show conf
```

コマンドの no 形式および default 形式

大部分のコンフィギュレーション コマンドに、**no** 形式があります。 **no** 形式は一般に、特定の機能または動作をディセーブルにする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスのシャットダウンが取り消されます。 **no** キーワードなしでコマンドを使用すると、ディセーブルにされた機能を再度イネーブルにしたり、デフォルトでディセーブルになっている機能をイネーブルにすることができます。

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、コマンドの設定値をデフォルトに戻します。 大部分のコマンドはデフォルトでディセーブルに設定されているので、**default** 形式は **no** 形式と同じになります。 ただし、デフォルトでイネーブルに設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。 これらのコマンドについては、**default** コマンドを使用すると、コマンドがイネーブルになり、変数がデフォルト値に設定されます。

CLI のエラー メッセージ

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 *2*：*CLI* の代表的なエラー メッセージ

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

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。

CLI を使用して機能を設定する方法

コマンド履歴の設定

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、スイッチは履歴バッファにコマンドライン10行を記録します。 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。 この手順は任意です。

手順の概要

1. **terminal history** [**size** *number-of-lines*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal history** [**size** *number-of-lines*] 例： `Switch# terminal history size 200`	特権 EXEC モードで現在のターミナル セッション中にスイッチが記録するコマンドラインの数を変更します。 サイズは 0 から 256 までの間で設定できます。

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。

手順の概要

1. **Ctrl+P** または**上矢印**キー
2. **Ctrl+N** または**下矢印**キー
3. **show history**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**Ctrl+P** または**上矢印**キー	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。
ステップ 2	**Ctrl+N** または**下矢印**キー	**Ctrl+P** または上矢印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。
ステップ 3	**show history** 例： `Switch# show history`	特権 EXEC モードで、直前に入力したコマンドをいくつか表示します。 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指定されます。

コマンド履歴機能のディセーブル化

コマンド履歴機能は、自動的にイネーブルになっています。 現在の端末セッションまたはコマンドラインでディセーブルにできます。 この手順は任意です。

手順の概要

1. **terminal no history**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal no history** 例： `Switch# terminal no history`	特権 EXEC モードで現在のターミナル セッション中のこの機能を無効化します。

編集機能のイネーブル化およびディセーブル化

拡張編集モードは自動的に有効に設定されますが、無効にでき、再び有効にもできます。

手順の概要

1. **terminal editing**
2. **terminal no editing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal editing** 例： `Switch# terminal editing`	特権 EXEC モードで現在のターミナルセッションにおける拡張編集モードを再び有効にします。
ステップ 2	**terminal no editing** 例： `Switch# terminal no editing`	特権 EXEC モードで現在のターミナルセッションにおける拡張編集モードを再び有効にします。

キー入力によるコマンドの編集

キーストロークは、コマンドラインの編集に役立ちます。 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 *3*：編集コマンド

編集コマンド	説明
Ctrl-B または**左矢印**キー	カーソルを 1 文字後退させます。
Ctrl-F または**右矢印**キー	カーソルを 1 文字前進させます。
Ctrl+A	コマンドラインの先頭にカーソルを移動します。
Ctrl+E	カーソルをコマンド ラインの末尾に移動します。
Esc B	カーソルを 1 単語後退させます。
Esc F	カーソルを 1 単語前進させます。

Ctrl+T	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。
Delete キーまたは **Backspace** キー	カーソルの左にある文字を消去します。
Ctrl+D	カーソル位置にある文字を削除します。
Ctrl+K	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	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	カーソルの左にある単語を削除します。
Esc D	カーソルの位置から単語の末尾までを削除します。
Esc C	カーソル位置のワードを大文字にします。
Esc L	カーソルの場所にある単語を小文字にします。
Esc U	カーソルの位置から単語の末尾までを大文字にします。
Ctrl+V または Esc Q	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。
Return キー	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。
Space バー	1 画面分下にスクロールします。
Ctrl+L または Ctrl+R	スイッチから画面に突然メッセージが出力された場合に、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。

次に、画面上で 1 行を超える長いコマンドラインを折り返す例を示します。

手順の概要

1. **access-list**
2. **Ctrl+A**
3. **Return** キー

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**access-list**
	
	例：
	`Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35`
	`Switch(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25`
	`Switch(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq`
	`Switch(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45`
		1 行分を超えるグローバル コンフィギュレーション コマンド入力を表示します。
		最初にカーソルが行末に達すると、その行は 10 文字分だけ左へシフトされ、再表示されます。 ドル記号（$）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。

ステップ 2	**Ctrl+A** 例： `Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$`	完全な構文をチェックします。 行末に表示されるドル記号（$）は、その行が右へスクロールされたことを表します。
ステップ 3	**Return** キー	コマンドを実行します。

	コマンドまたはアクション	目的
		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。

手順の概要

1. {**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	{**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*
	
	例：
	`Switch# show interfaces | include protocol`
	`Vlan1 is up, line protocol is up`
	`Vlan10 is up, line protocol is down`
	`GigabitEthernet1/0/1 is up, line protocol is down`
	`GigabitEthernet1/0/2 is up, line protocol is up`
		出力を検索およびフィルタリングします。
		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。

スイッチ スタックでの CLI へのアクセス

CLI にはコンソール接続、Telnet、SSH、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、active switch を経由して管理します。 スイッチごとにスタック メンバを管理することはできません。 1 つまたは複数のスタック メンバーのコンソールポートまたはイーサネット管理ポートを経由してへ接続できます。 で複数のCLIセッションを使用する場合は注意してください。 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。

スタンバイ スイッチをデバッグするには、アクティブなスイッチから **session standby ios** 特権 EXEC コマンドを使用してスタンバイ スイッチの IOS コンソールにアクセスします。 特定のスタック メンバをデバッグするには、アクティブなスイッチから **session switch** *stack-member-number* 特権 EXEC コマンドを使用して、スタック メンバの診断シェルにアクセスします。 これらのコマンドの詳細情報については、スイッチ コマンド リファレンスを参照してください。

コンソール接続または Telnet 経由での CLI へのアクセス

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。

スイッチがすでに設定されている場合は、ローカル コンソール接続またはリモート Telnet セッションによって CLI にアクセスできますが、このタイプのアクセスに対応できるように、先にスイッチを設定しておく必要があります。

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 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、または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 Secure Shell（SSH; セキュア シェル）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 2 章

Web グラフィカル ユーザ インターフェイスの使用

Web GUI の使用に関する前提条件

- GUI を使用する PC では、Windows 7、Windows XP SP1 以降のリリースまたは Windows 2000 SP4 以降のリリースが稼働している必要があります。
- スイッチGUI は、Microsoft Internet Explorer バージョン 10.x、Mozilla Firefox 20.x、または Google Chrome 26.x. と互換性があります。

Web GUI の使用に関する情報

Web ブラウザ、つまり、グラフィカル ユーザ インターフェイス（GUI）は、各スイッチに組み込まれています。

サービス ポート インターフェイスまたは管理インターフェイスを使用して GUI にアクセスできますが、 サービス ポート インターフェイスの使用をお勧めします。 GUI のページ上部にある [Help] をクリックすると、オンライン ヘルプが表示されます。 オンライン ヘルプを表示するには、ブラウザのポップアップ ブロッカを無効にする必要があります。

Web GUI の機能

スイッチWeb GUI は次の機能をサポートします。

構成ウィザード : IP アドレスおよびローカルユーザ名/パスワードの初期設定、または認証サーバでの認証（必須特権 15）の後、ウィザードは最初の無線設定を完了するための手順を提供します。 [Configuration] > [Wizard] を起動し、次のことを設定するために、9 ステップの手順に従います。

- 管理ユーザ
- SNMP システムの概要
- Management Port
- ワイヤレス管理
- RF Mobility と国番号
- モビリティ設定
- WLAN
- 802.11 設定
- Set Time

[Monitor] タブ:

- 概要のスイッチ、クライアント、アクセス ポイントの詳細を表示します。
- すべての無線および AP 接続統計情報を表示します。
- アクセス ポイントの電波品質を表示します。
- すべてのインターフェイスおよび CDP トラフィック情報の Cisco Discovery Protocol (CDP) のすべてのネイバーの一覧を表示します。
- 分類 Friendly、Malicious、Ad hoc、Classified、および Unclassified に基づいて、すべての不正アクセス ポイントを表示します。

[Configuration] タブ:

- Web設定ウィザードを使用して、すべての初期操作のためにスイッチを設定できます。 ウィザードでは、ユーザの詳細、管理インターフェイスなどを設定できます。
- システム、内部 DHCP サーバ、管理、およびモビリティ管理パラメータを設定できます。
- スイッチ、WLAN、無線を設定できます。
- スイッチで、セキュリティ ポリシーを設定できます。
- オペレーティング システム ソフトウェアの管理コマンドスイッチにアクセスできます。

[Administration] タブで、システム ログを設定できます。

スイッチ のコンソール ポートの接続

はじめる前に

基本的な動作ができるようにスイッチを設定するには、VT-100 ターミナル エミュレーション プログラム（HyperTerminal、ProComm、Minicom、Tip など）を実行する PC にコントローラを接続する必要があります。

ステップ 1 ヌルモデム シリアル ケーブルの一端をスイッチの RJ-45 コンソール ポートに接続し、もう一端を PC のシリアル ポートに接続します。

ステップ 2 AC 電源コードをスイッチに接続し、アース付き 100 ～ 240 VAC、50/60 Hz の電源コンセントに差し込みます。 電源を入れます。 起動スクリプトによって、オペレーティング システム ソフトウェアの初期化（コードのダウンロードおよび電源投入時自己診断テスト）および基本設定が表示されます。 スイッチの電源投入時自己診断テストに合格した場合は、起動スクリプトによって設定ウィザードが実行されます。画面の指示に従って、基本設定を入力してください。

ステップ 3 **yes** と入力します。 CLI セットアップ ウィザードの基本的な初期設定パラメータに進みます。 gigabitethernet 0/0 インターフェイスであるサービス ポートの IP アドレスを指定します。
構成ウィザードの設定パラメータを入力すると、Web GUI にアクセスできます。 これで、スイッチがサービス ポートの IP アドレスにより設定されます。

Web GUI へのログイン

ステップ 1 ブラウザのアドレス行にスイッチスイッチIPアドレスを入力します。 接続をセキュリティで保護するには、https://**ip-address** と入力します。 接続をセキュリティで保護しない場合は、http://**ip-address** と入力します。

ステップ 2 [Accessing Cisco AIR-CT3650] ページが表示されます。

Web モードおよびセキュア Web モードの有効化

ステップ 1 [Configuration] > [Switch] > [Management] > [Protocol Management] > [HTTP-HTTPS]を選択します。

[HTTP-HTTPS Configuration] ページが表示されます。

ステップ 2 Web モード（ユーザが「http://ip-address」を使用してスイッチ GUI にアクセスできます）を有効にするには、[HTTP Access] ドロップダウン リストから [Enabled] を選択します。 有効にしない場合は、[Disabled] を選択します。 Web モード（HTTP）の接続は、セキュリティで保護されません。

ステップ 3 セキュア Web モード（ユーザが「https://ip-address」を使用してスイッチ GUI にアクセスできます）を有効にするには、[HTTPS Access] ドロップダウン リストから [Enabled] を選択します。 有効にしない場合は、[Disabled] を選択します。 セキュア Web モード（HTTPS）の接続は、セキュリティで保護されています。

ステップ 4 [IP Device Tracking] チェックボックスで、デバイスを追跡することを選択します。

ステップ 5 [Enable] チェックボックスでトラスト ポイントをイネーブルにすることを選択します。

ステップ 6 [Trustpoints] ドロップダウン リストからトラストポイントを選択します。

ステップ 7 [HTTP Timeout-policy (1 to 600 sec)] テキスト ボックスに、非アクティブ化により Web セッションがタイムアウトするまでの時間を秒単位で入力します。
有効な範囲は 1 ～ 600 秒です。

ステップ 8 [Server Life Time (1 to 86400 sec)] テキスト ボックスにサーバのライフタイムを入力します。
有効な範囲は 1 ～ 86400 秒です。

ステップ 9 [Maximum number of Requests (1 to 86400)] テキスト ボックスに、サーバが受け入れる最大接続要求数を入力します。
指定できる接続数の範囲は、1 ～ 86400 です。

ステップ 10 **[Apply]** をクリックします。

ステップ 11 **[Save Configuration]** をクリックします。

スイッチ Web GUI の設定

設定ウィザードでは、スイッチ上での基本的な設定を行うことができます。 このウィザードは、スイッチを購入した直後やスイッチを工場出荷時のデフォルトにリセットした後に実行します。 設定ウィザードは、GUI と CLI の両方の形式で使用できます。

ステップ 1 PC をサービス ポートに接続し、スイッチと同じサブネットを使用するように IPv4 アドレスを設定します。 スイッチが IOS XE イメージとともにロードされ、サービス ポート インターフェイスが gigabitethernet 0/0 として設定されます。

ステップ 2 PC で Internet Explorer 10 以降、Firefox 2.0.0.11 以降、または Google Chrome を開始し、ブラウザ ウィンドウに管理インターフェイスの IP アドレスを入力します。 管理インターフェイスの IP アドレスは、gigabitethernet 0/0（別名、サービス ポート インターフェイス）と同じです。 初めてログインするときに、

HTTP のユーザ名およびパスワードを入力する必要があります。 デフォルトでは、ユーザ名は **admin**、パスワードは **cisco** です。
サービス ポート インターフェイスを使用するときは、HTTP と HTTPS の両方を使用できます。 HTTPS はデフォルトでイネーブルであり、HTTP をイネーブルにすることもできます。

初めてログインすると、[Accessing Cisco Switch <Model Number> <Hostname>] ページが表示されます。

ステップ 3 [Accessing Cisco Switch] ページで、スイッチ Web GUI の **[Home]** ページにアクセスするために、**[Wireless Web GUI]** リンクをクリックします。

ステップ 4 最初にスイッチの設定に必要なすべての手順を実行するために、[Configuration] > [Wizard]を選択します。 **[Admin Users]** ページが表示されます。

ステップ 5 **[Admin Users]** ページで、このスイッチに割り当てる管理者のユーザ名を [User Name] テキスト ボックスに入力し、このスイッチに割り当てる管理パスワードを [Password] テキスト ボックスおよび [Confirm Password] テキスト ボックスに入力します。 **[Next]** をクリックします。
デフォルトのユーザ名は **admin** で、デフォルトのパスワードは **cisco** です。 またはスイッチの新しい管理者ユーザを作成できます。 ユーザ名とパスワードには、最大 24 文字の ASCII 文字を入力できます。

[SNMP System Summary] ページが表示されます。

ステップ 6 **[SNMP System Summary]** ページで、スイッチの次の SNMP システム パラメータを入力し、**[Next]** をクリックします。

- [Location] テキスト ボックスでユーザ定義可能なスイッチの場所。
- [Contact] テキスト ボックスで名前や電話番号などのユーザ定義可能な連絡先の詳細。
- SNMP 通知をさまざまな SNMP トラップで送信するには、[SNMP Global Trap] ドロップダウン リストで **[Enabled]** を選択し、さまざまな SNMP トラップに対して SNMP 通知を送信しないようにするには **[Disabled]** を選択します。
- システム ログ メッセージを送信するには [SNMP Logging] ドロップダウン リストから **[Enabled]** を選択し、システム ログ メッセージを送信しない場合は **[Disabled]** を選択します。

（注） SNMP トラップ サーバは、ディストリビューション ポートから到達可能であることが必要です（gigabitethernet0/0 サービスまたは管理インターフェイスは経由しません）。

[Management Port] ページが表示されます。

ステップ 7 **[Management Port]** ページで、管理ポートのインターフェイス（gigabitethernet 0/0）の次のパラメータを入力し、**[Next]** をクリックします。

- [IP Address] テキスト ボックスでサービス ポートに割り当てたインターフェイスの IP アドレス。
- [Netmask]テキストボックスで、管理ポートのインターフェイスのネットワーク マスクのアドレス。
- [IPv4 DHCP Server] テキスト ボックスで選択されたポートの IPv4 Dynamic Host Configuration Protocol (DHCP) のアドレス。

[Wireless Management] ページが表示されます。

ステップ 8 **[Wireless Management]** ページでは、次のワイヤレス インターフェイス管理の詳細を入力し、**[Next]** をクリックします。

- [Select Interface] ドロップダウン リストから、インターフェイスとして VLAN または 10 ギガビット イーサネットを選択します。
- [VLAN ID] テキスト ボックスで VLAN タグの ID。VLAN タグがない場合は 0。
- [IP Address] テキスト ボックスで、アクセス ポイントが接続されたワイヤレス管理インターフェイスの IP アドレス。
- [Netmask] テキスト ボックスで、ワイヤレス管理インターフェイスのネットワーク マスクのアドレス。
- [IPv4 DHCP Server] テキスト ボックスで DHCP IPv4 IP アドレス。

インターフェイスとして VLAN を選択すると、[Switch Port Configuration] テキスト ボックスで指定されたリストから、ポートとしてトランク ポートまたはアクセス ポートを指定できます。

[RF Mobility and Country Code] ページが表示されます。

ステップ 9 **[RF Mobility and Country Code]** ページで、RF モビリティ ドメイン名を [RF Mobility] テキスト ボックスに入力し、[Country Code] ドロップダウン リストから現在の国コードを選択して、**[Next]** をクリックします。 GUI からは、1 つの国番号のみを選択できます。

（注） RF グループ化パラメータとモビリティ設定を設定する前に、必ず関連する概念のコンテンツを参照してから、設定に進むようにしてください。

[Mobility Configuration] ページが開き、モビリティのグローバル コンフィギュレーション設定が表示されます。

ステップ 10 **[Mobility Configuration]** ページで、次のモビリティのグローバル コンフィギュレーション設定を参照および入力し、**[Next]** をクリックします。

- [Mobility Role] ドロップダウン リストから、**[Mobility Controller]** または **[Mobility Agent]** を選択します。
  - [Mobility Agent] を選択した場合は、[Mobility Controller IP Address] テキスト ボックスにモビリティ コントローラの IP アドレス、[Mobility Controller Public IP Address] テキスト ボックスにモビリティ コントローラの IP アドレスを入力します。
  - [Mobility Controller] を選択すると、モビリティ コントローラの IP アドレスとモビリティ コントローラのパブリック IP アドレスがそれぞれのテキスト ボックスに表示されます。
- [Mobility Protocol Port] テキスト ボックスにモビリティ プロトコルのポート番号が表示されます。
- [Mobility Switch Peer Group Name] テキスト ボックスにモビリティ スイッチのピア グループ名が表示されます。
- [DTLS Mode] テキスト ボックスで、DTLS がイネーブルであるかどうかが示されます。

DTLS は、標準化過程にある TLS に基づくインターネット技術特別調査委員会（IETF）プロトコルです。

- [Mobility Domain ID for 802.11 radios] テキスト ボックスに、802.11 無線のモビリティ ドメイン ID が表示されます。
- [Mobility Keepalive Interval (1-30)sec] テキスト ボックスで、ピア スイッチに送信する各 ping 要求の間隔（秒単位）。

  有効範囲は 1 ～ 30 秒で、デフォルト値は 10 秒です。
- [Mobility Keep Alive Count（3-20）] テキスト ボックスで、ピア スイッチが到達不能と判断するまでに ping 要求を送信する回数。

  有効な範囲は 3 ～ 20 で、デフォルト値は 3 です。
- [Mobility Control Message DSCP Value (0-63)] テキスト ボックスで、モビリティ スイッチに設定される DSCP 値。

  有効な範囲は 0 ～ 63 で、デフォルト値は 0 です。
- [Switch Peer Group Members Configured] テキスト ボックスで設定したモビリティ スイッチ ピア グループ メンバーの数を表示します。

[WLANs] ページが表示されます。

ステップ 11 **[WLANs]** ページで、次の WLAN 設定パラメータを入力し、**[Next]** をクリックします。

- [WLAN ID] テキスト ボックスで WLAN 識別子。
- [SSID] テキスト ボックスで、クライアントに関連付けられている WLAN の SSID。
- [Profile Name] テキスト ボックスで、クライアントが使用する WLAN の名前。

[802.11 Configuration] ページが表示されます。

ステップ 12 **[802.11 Configuration]** ページで、[802.11a/n/ac] チェックボックスと [802.11b/g/n] チェックボックスのいずれかまたは両方をオンにして 802.11 無線をイネーブルにし、**[Next]** をクリックします。
[Set Time] ページが表示されます。

ステップ 13 **[Set Time]** ページで、次のパラメータに基づいてスイッチの日時を設定し、**[Next]** をクリックします。

- [Current Time] テキスト ボックスで、スイッチの現在のタイムスタンプが表示されます。
- [Mode] ドロップダウン リストから [Manual] または [NTP] を選択します。

  NTP サーバの使用時に、スイッチに接続されているすべてのアクセス ポイントが、使用可能な NTP サーバ設定に基づいて時間を同期します。
- [Year, Month, and Day] ドロップダウン リストからスイッチの日付を選択します。
- [Hours, Minutes, and Seconds] ドロップダウン リストから時間を選択します。
- 時間帯を [Zone] テキスト ボックスに入力し、スイッチで設定された現在の時刻と比較した場合に必要なオフセットを [Offset] ドロップダウン リストから選択します。

[Save Wizard] ページが表示されます。

ステップ 14 **[Save Wizard]** ページで、この手順を使用してスイッチで行った設定を確認できます。設定値を変更する場合は、**[Previous]** をクリックし、該当ページに移動します。
すべてのウィザードについて成功メッセージが表示された場合にのみ、ウィザードを使用して作成したスイッチ設定を保存できます。 **[Save Wizard]** ウィザード ページでエラーが表示された場合、スイッチの初期設定のためにウィザードを再実行する必要があります。

第 3 章

MLD スヌーピングの設定

このモジュールには、MLD スヌーピングの設定の詳細が含まれています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

IPv6 MLD スヌーピングの設定に関する情報

スイッチ上で Multicast Listener Discovery（MLD）スヌーピングを使用して、スイッチド ネットワーク内のクライアントおよびルータに IP Version 6（IPv6）マルチキャスト データを効率的に配信することができます。 特に明記しない限り、スイッチという用語は、スタンドアロン スイッチおよびスイッチ スタックを指します。

（注） Catalyst 2960-XR スイッチで IPv6 を使用するには、スイッチ上にデュアル IPv4 および IPv6 スイッチング データベース管理（SDM）テンプレートが設定されている必要があります。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスまたは手順に記載された Cisco IOS のマニュアルを参照してください。

MLD スヌーピングの概要

IP Version 4（IPv4）では、レイヤ 2 スイッチはインターネット グループ管理プロトコル（IGMP）スヌーピングを使用して、動的にレイヤ 2 インターフェイスを設定することにより、マルチキャスト トラフィックのフラッディングを抑制します。そのため、マルチキャスト トラフィックはIP マルチキャスト デバイスに対応付けられたインターフェイスにだけ転送されます。 IPv6 では、MLD スヌーピングが同様の機能を実行します。 MLD スヌーピングを使用すると、IPv6 マルチキャストデータはVLAN（仮想LAN）内のすべてのポートにフラッディングされるのではなく、データを受信するポートのリストに選択的に転送されます。 このリストは、IPv6 マルチキャスト制御パケットをスヌーピングすることにより構築されます。

MLD は IPv6 マルチキャスト ルータで使用されるプロトコルで、ルータに直接接続されたリンク上のマルチキャスト リスナー（IPv6マルチキャストパケットを受信するノード）の存在、および隣接ノードを対象とするマルチキャスト パケットを検出します。 MLD は IGMP から派生しています。MLD バージョン 1（MLDv1）は IGMPv2 と、MLD バージョン 2（MLDv2）は IGMPv3 とそれぞれ同等です。 MLD は Internet Control Message Protocol バージョン 6（ICMPv6）のサブプロトコルです。MLD メッセージは ICMPv6 メッセージのサブセットで、IPv6 パケット内で先頭の Next Header 値 58 により識別されます。

スイッチは、次の 2 つのバージョンの MLD スヌーピングをサポートします。

- MLDv1 スヌーピング：MLDv1 制御パケットを検出し、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックのブリッジングを設定します。
- MLDv2 基本スヌーピング（MBSS）：MLDv2 制御パケットを使用して、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックの転送を設定します。

スイッチは MLDv1 プロトコル パケットと MLDv2 プロトコル パケットの両方でスヌーピングでき、IPv6 宛先マルチキャスト アドレスに基づいて IPv6 マルチキャスト データをブリッジングします。

（注） スイッチは、IPv6 送信元および宛先マルチキャスト アドレスベースの転送を設定する MLDv2 拡張スヌーピングをサポートしません。

MLD スヌーピングは、グローバルまたは VLAN 単位でイネーブルまたはディセーブルに設定できます。 MLD スヌーピングがイネーブルの場合、VLAN 単位の IPv6 マルチキャスト アドレス テーブルはソフトウェアおよびハードウェアで構築されます。 その後、スイッチはハードウェアで IPv6 マルチキャストアドレスに基づくブリッジングを実行します。

IPv6 マルチキャスト標準に従い、スイッチは自身の MAC アドレスの下位 4 オクテットと MAC アドレス 33:33:00:00:00:00 の論理 OR を実行して、MAC マルチキャストアドレスを抽出します。 た

とえば、IPv6 の MAC アドレス FF02:DEAD:BEEF:1:3 は、イーサネットの MAC アドレス 33:33:00:01:00:03 にマッピングされます。

IPv6 宛先アドレスと MAC 宛先アドレスが一致しない場合、マルチキャスト パケットは一致しません。 スイッチは、一致しないパケットをハードウェア ベースの MAC アドレス テーブルによって転送します。 MAC 宛先アドレスが MAC アドレス テーブルにない場合、スイッチは受信したポートと同じ VLAN 内のすべてのポートにパケットをフラッディングします。

MLD メッセージ

MLDv1 は、次の 3 種類のメッセージをサポートします。

- Listener Query：IGMPv2 クエリーと同等で、General Query または Mulicast-Address-Specific Query（MASQ）のいずれかになります。
- Multicast Listener Report：IGMPv2 レポートと同等です。
- Multicast Listener Done メッセージ：IGMPv2 Leave メッセージと同等です。

MLDv2 では、MLDv1 レポートおよび Done メッセージに加えて、MLDv2 クエリーおよび MLDv2 レポートもサポートします。

メッセージの送受信の結果生じるメッセージ タイマーおよびステート移行は、IGMPv2 メッセージの場合と同じです。 リンクに対してローカルで有効な IPv6 送信元アドレスを持たない MLD メッセージは、MLD ルータおよび MLD スイッチで無視されます。

MLD クエリー

スイッチは MLD クエリーを送信し、IPv6 マルチキャスト アドレス データベースを構築し、MLD グループ固有クエリー、MLD グループおよび送信元固有クエリーを生成して、MLD Done メッセージに応答します。 また、スイッチはレポート抑制、レポートプロキシング、即時脱退機能、およびスタティックな IPv6 マルチキャスト グループ アドレス設定もサポートします。

MLD スヌーピングがディセーブルの場合、すべての MLD クエリーが入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合、受信された MLD クエリーが入力 VLAN でフラッディングされ、クエリーのコピーは CPU に送信され、処理されます。 MLD スヌーピングでは、受信されたクエリーから IPv6 マルチキャスト アドレス データベースを構築します。 MLD スヌーピングは、マルチキャストルータ ポートを検出して、タイマーを維持し、レポート応答時間を設定します。また、VLAN のクエリア IP 送信元アドレス、VLAN 内のクエリア ポートを学習して、マルチキャストアドレス エージングを維持します。

（注） IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、Catalyst 2960、2960-S、2960-C または 2960-X スイッチが VLAN 上でクエリーを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。 標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

グループが MLD スヌーピング データベースに存在する場合、スイッチは MLDv1 レポートを送信して、グループ固有のクエリーに応答します。 このグループが不明の場合、グループ固有のクエリーは入力 VLAN にフラッディングされます。

ホストがマルチキャスト グループから脱退する場合、MLD Done メッセージ（IGMP Leave メッセージと同等）を送信できます。 スイッチが MLDv1 Done メッセージを受信した際に、即時脱退がイネーブルでなければ、スイッチはメッセージを受信したポートに MASQ を送信して、ポートに接続する他のデバイスがマルチキャスト グループに残る必要があるかどうか判別します。

マルチキャスト クライアント エージングの堅牢性

クエリー数に基づいて、アドレスからのポート メンバーシップの削除を設定できます。 1 つのアドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対するレポートがない場合のみです。 デフォルトの回数は 2 回です。

マルチキャスト ルータ検出

IGMP スヌーピングと同様に、MLD スヌーピングでは次の特性を持つマルチキャスト ルータ検出を行います。

- ユーザにより設定されたポートには、期限切れがありません。
- ダイナミックなポート学習は、MLDv1 スヌーピング クエリーおよび IPv6 PIMv2 パケットにより行われます。
- 複数のルータが同じレイヤ 2 インターフェイス上にある場合、MLD スヌーピングではポート上の単一のマルチキャスト ルータ（直前にルータ制御パケットを送信したルータ）を追跡します。
- マルチキャスト ルータ ポートのダイナミックなエージングは、デフォルト タイマーの 5 分に基づきます。ポート上で制御パケットが 5 分間受信されない場合、マルチキャスト ルータはルータのポート リストから削除されます。
- IPv6 マルチキャスト ルータ検出が実行されるのは、MLD スヌーピングがスイッチでイネーブルの場合のみです。
- 受信された IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネーブルかどうかにかかわらず、常に入力 VLAN にフラッディングされます。

- 最初の IPv6 マルチキャスト ルータ ポートが検出された後は、不明の IPv6 マルチキャスト データは、検出されたルータ ポートに対してのみ転送されます（それまでは、すべての IPv6 マルチキャスト データは入力 VLAN にフラッディングされます）。

MLD レポート

MLDv1 join メッセージは、本質的には IGMPv2 と同じように処理されます。 IPv6 マルチキャスト ルータが VLAN で検出されない場合は、レポートが処理されないか、またはスイッチから転送されません。 IPv6 マルチキャスト ルータが検出され、MLDv1 レポートが受信されると、IPv6 マルチキャスト グループ アドレスが VLAN の MLD データベースに入力されます。 その後、VLAN 内のグループに対するすべての IPv6 マルチキャスト トラフィックが、このアドレスを使用して転送されます。 MLD スヌーピングがディセーブルの場合、レポートは入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合は、MLD レポート抑制（リスナー メッセージ抑制）は自動的にイネーブルになります。 レポート抑制により、スイッチはグループで受信された最初の MLDv1 レポートを IPv6 マルチキャスト ルータに転送します。グループのそれ以降のレポートはルータに送信されません。 MLD スヌーピングがディセーブルの場合は、レポート抑制がディセーブルになり、すべての MLDv1 レポートは入力 VLAN にフラッディングされます。

スイッチは、MLDv1 プロキシ レポーティングもサポートします。 MLDv1 MASQ が受信されると、スイッチに他のポートのグループが存在する場合、およびクエリーを受信したポートとアドレスの最後のメンバ ポートが異なる場合は、スイッチはクエリーを受信したアドレスに関する MLDv1 レポートで応答します。

MLD Done メッセージおよび即時脱退

即時脱退機能がイネーブルの場合にホストが MLDv1 Done メッセージ（IGMP Leave メッセージと同等）を送信すると、Done メッセージを受信したポートはグループからただちに削除されます。 VLAN で即時脱退をイネーブルにする場合は（IGMP スヌーピングと同様に）、ポートに単一のホストが接続されている VLAN でのみこの機能を使用します。 ポートがグループの最後のメンバである場合、グループも削除され、検出された IPv6 マルチキャスト ルータに脱退情報が転送されます。

VLAN で即時脱退がイネーブルでない場合に（1 つのポート上にグループのクライアントが複数ある場合）、Done メッセージがポートで受信されると、このポートで MASQ が生成されます。 ユーザは、既存アドレスのポート メンバーシップが削除される時期を MASQ 数の観点から制御できます。 アドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対する MLDv1 レポートがない場合です。

生成される MASQ 数は、 **ipv6 mld snooping last-listener-query count** グローバル コンフィギュレーション コマンドにより設定されます。 デフォルトの回数は 2 回です。

MASQ は、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信されます。 スイッチの最大応答時間内に MASQ で指定された IPv6 マルチキャスト アドレスにレポートが送信されなければ、MASQ が送信されたポートは IPv6 マルチキャスト アドレス データベースから削除されます。 最大応答時間は、 **ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュ

レーション コマンドにより設定します。 削除されたポートがマルチキャスト アドレスの最後のメンバである場合は、マルチキャスト アドレスも削除され、スイッチは検出されたマルチキャスト ルータすべてにアドレス脱退情報を送信します。

即時脱退がイネーブルでない場合に、ポートが MLD Done メッセージを受信すると、スイッチはポートで MASQ を生成して、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信します。 ポートがマルチキャスト グループから削除される前に、送信される MASQ 数およびスイッチが応答を待機する時間を任意で設定できます。

MLDv1 即時脱退をイネーブルにした場合、スイッチはポートで MLD Done メッセージを検出するとただちに、マルチキャスト グループからポートを削除します。 即時脱退機能を使用するのは、VLAN の各ポート上にレシーバが 1 つだけ存在する場合に限定してください。 同一ポートにマルチキャスト グループのクライアントが複数ある場合は、VLAN で即時脱退をイネーブルにしてはなりません。

TCN 処理

ipv6 mld snooping tcn query solicit 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、トポロジ変更通知（TCN）送信請求をイネーブルにすると、MLDv1 スヌーピングは、設定された数の MLDv1 クエリーによりすべての IPv6 マルチキャスト トラフィックをフラッディングするよう VLAN に設定してから、選択されたポートにのみマルチキャスト データの送信を開始します。 この値は、 **ipv6 mld snooping tcn flood query count** 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します。 デフォルトでは、2 つのクエリーが送信されます。 スイッチが VLAN 内の STP ルートになる場合、またはスイッチがユーザにより設定された場合は、リンクに対してローカルで有効な IPv6 送信元アドレスを持つ MLDv1 グローバル Done メッセージも生成されます。 これは IGMP スヌーピングの場合と同じです。

スイッチ スタックでの MLD スヌーピング

MLD IPv6 グループ アドレス データベースは、どのスイッチが IPv6 マルチキャスト グループを学習するかに関係なく、スタック内のすべてのスイッチ上で保持されます。 レポート抑制とプロキシ レポーティングは、スタック全体で行われます。 最大応答時間の間、1 つのグループに受信したレポートでマルチキャスト ルータに転送されるのは、どのスイッチにそのレポートが到達したかに関係なく、1 つだけです。

新しいスタック マスターの選択は、IPv6マルチキャストデータの学習やブリッジングには影響しません。IPv6マルチキャストデータのブリッジングは、スタック マスターの再選択中にも停止しません。 新しいスイッチがスタックに追加されると、スタック マスターからの学習済み IPv6 マルチキャスト情報との同期が取られます。 同期が完了するまでは、新しく追加されたスイッチでのデータ入力は、不明マルチキャスト データとして扱われます。

IPv6 MLD スヌーピングの設定方法

MLD スヌーピングのデフォルト設定

表 *4* : ***MLD*** スヌーピングのデフォルト設定

機能	デフォルト設定
MLD スヌーピング（グローバル）	ディセーブル
MLD スヌーピング（VLAN 単位）	イネーブル VLAN MLD スヌーピングが実行されるためには、MLD スヌーピングがグローバルにイネーブルである必要があります。
IPv6 マルチキャスト アドレス	未設定
IPv6 マルチキャスト ルータ ポート	未設定
MLD スヌーピング即時脱退	ディセーブル
MLD スヌーピングの堅牢性変数	グローバル：2、VLAN 単位：0 （注） VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー カウント	グローバル：2、VLAN 単位：0 （注） VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー インターバル	グローバル：1000（1 秒）、VLAN：0 （注） VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバルのインターバルを使用します。
TCN クエリー送信請求	ディセーブル
TCN クエリー カウント	2
MLD リスナー抑制	ディセーブル

MLD スヌーピング設定時の注意事項

MLD スヌーピングの設定時は、次の注意事項に従ってください。

- MLD スヌーピングの特性はいつでも設定できますが、設定を有効にする場合は、 **ipv6 mld 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 MLD 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。
- IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、スイッチが VLAN 上でクエリーを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。
- MLD スヌーピングと IGMP スヌーピングは相互に独立して動作します。 スイッチで両方の機能を同時にイネーブルにできます。
- スイッチまたはスイッチ スタックで保持可能なマルチキャスト エントリの最大数は、設定された SDM テンプレートによって決まります。
- スイッチまたはスイッチ スタックに保持可能なアドレス エントリの最大数は 4000 です。

スイッチでのMLDスヌーピングのイネーブル化またはディセーブル化（CLI）

デフォルトでは、IPv6 MLD スヌーピングはスイッチではグローバルにディセーブルで、すべての VLAN ではイネーブルです。 MLD スヌーピングがグローバルにディセーブルの場合は、すべての VLAN でもディセーブルです。 MLD スヌーピングをグローバルにイネーブルにすると、VLAN 設定はグローバル設定を上書きします。 つまり、MLD スヌーピングはデフォルト ステート（イネーブル）の VLAN インターフェイスでのみイネーブルになります。

VLAN 単位または VLAN 範囲で MLD スヌーピングをイネーブルおよびディセーブルにできますが、MLD スヌーピングをグローバルにディセーブルにした場合は、すべての VLAN でディセーブルになります。 グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

スイッチで MLD スヌーピングをグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping** 例： `Switch(config)# ipv6 mld snooping`	スイッチで MLD スヌーピングをイネーブルにします。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config** 例： `Switch(config)# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 5	**reload** 例： `Switch(config)# reload`	OS（オペレーティング システム）をリロードします。

VLAN での MLD スヌーピングの有効化または無効化（CLI）

VLAN で MLD スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping** 例： `Switch(config)# ipv6 mld snooping`	スイッチで MLD スヌーピングをイネーブルにします。
ステップ 3	**ipv6 mld snooping vlan** *vlan-id* 例： `Switch(config)# ipv6 mld snooping vlan 1`	VLAN で MLD スヌーピングをイネーブルにします。 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 （注） VLAN スヌーピングをイネーブルにするには、MLD スヌーピングがグローバルにイネーブルである必要があります。
ステップ 4	**end** 例： `Switch(config)# ipv6 mld snooping vlan 1`	特権 EXEC モードに戻ります。

スタティック マルチキャスト グループの設定（CLI）

ホストまたはレイヤ 2 ポートは、通常マルチキャスト グループにダイナミックに加入しますが、VLAN に IPv6 マルチキャスト アドレスおよびメンバ ポートをスタティックに設定することもできます。

マルチキャスト グループのメンバとしてレイヤ 2 ポートを追加するには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **static** *ipv6_multicast_address* **interface** *interface-id* 例： `Switch(config)# ipv6 mld snooping vlan 1 static FF12::3 interface gigabitethernet 0/1`	マルチキャスト グループのメンバとしてレイヤ 2 ポートにマルチキャスト グループを設定します。 • *vlan-id* は、マルチキャスト グループの VLAN ID です。 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • *ipv6_multicast_address* は、128 ビットのグループ IPv6 アドレスです。 このアドレスは RFC 2373 で指定された形式でなければなりません。 • *interface-id* は、メンバ ポートです。 物理インターフェイスまたはポート チャネル（1～48）に設定できます。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

ステップ 4	次のいずれかを使用します。
	• **show ipv6 mld snooping address**
	• **show ipv6 mld snooping address vlan** *vlan-id*
	
	例：
	`Switch# show ipv6 mld snooping address`
	または
	`Switch# show ipv6 mld snooping vlan 1`
		スタティック メンバ ポートおよび IPv6 アドレスを確認します。

マルチキャスト ルータ ポートの設定（CLI）

（注） マルチキャスト ルータへのスタティック接続は、スイッチ ポートに限りサポートされます。

VLAN にマルチキャスト ルータ ポートを追加するには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **mrouter interface** *interface-id* 例： `Switch(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet 0/2`	マルチキャスト ルータの VLAN ID を指定して、マルチキャスト ルータにインターフェイスを指定します。 • 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • このインターフェイス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。 ポート チャネル範囲は 1 ～ 48 です。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping mrouter** [**vlan** *vlan-id*] 例： `Switch# show ipv6 mld snooping mrouter vlan 1`	VLAN インターフェイスで IPv6 MLD スヌーピングがイネーブルになっていることを確認します。

MLD 即時脱退の有効化（CLI）

MLDv1 即時脱退をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 mld snooping vlan** *vlan-id* **immediate-leave** 例： `Switch(config)# ipv6 mld snooping vlan 1 immediate-leave`	VLAN インターフェイスで MLD 即時脱退をイネーブルにします。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping vlan** *vlan-id* 例： `Switch# show ipv6 mld snooping vlan 1`	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。

MLD スヌーピング クエリーの設定（CLI）

スイッチまたは VLAN に MLD スヌーピング クエリーの特性を設定するには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ipv6 mld snooping robustness-variable** *value* 例： `Switch(config)# ipv6 mld snooping robustness-variable 3`	（任意）スイッチが一般クエリーに応答しないリスナー（ポート）を削除する前に、送信されるクエリー数を設定します。指定できる範囲は 1 ～ 3 です。デフォルトは 2 です。
ステップ 3	**ipv6 mld snooping vlan** *vlan-id* **robustness-variable** *value* 例： `Switch(config)# ipv6 mld snooping vlan 1 robustness-variable 3`	（任意）VLAN 単位でロバストネス変数を設定します。これにより、MLD レポート応答がない場合にマルチキャスト アドレスがエージング アウトされるまでに、MLD スヌーピングが送信する一般クエリー数が決定されます。 指定できる範囲は 1 ～ 3 です。デフォルトは 0 です。 0 に設定すると、使用される数はグローバルな堅牢性変数の値になります。
ステップ 4	**ipv6 mld snooping last-listener-query-count** *count* 例： `Switch(config)# ipv6 mld snooping last-listener-query-count 7`	（任意）MLD クライアントがエージング アウトされる前にスイッチが送信する MASQ 数を設定します。 指定できる範囲は 1 ～ 7 です。デフォルトは 2 です。 クエリーは 1 秒後に送信されます。
ステップ 5	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-count** *count* 例： `Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-count 7`	（任意）VLAN 単位で last-listener クエリー カウントを設定します。 この値はグローバルに設定された値を上書きします。指定できる範囲は 1 ～ 7 です。デフォルトは 0 です。 0 に設定すると、グローバルなカウント値が使用されます。 クエリーは 1 秒後に送信されます。
ステップ 6	**ipv6 mld snooping last-listener-query-interval** *interval* 例： `Switch(config)# ipv6 mld snooping last-listener-query-interval 2000`	（任意）スイッチが MASQ を送信したあと、マルチキャスト グループからポートを削除するまで待機する最大応答時間を設定します。 指定できる範囲は、100 ～ 32,768 ミリ秒です。デフォルト値は 1000（1 秒）です。
ステップ 7	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-interval** *interval* 例： `Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 2000`	（任意）VLAN 単位で last-listener クエリー インターバルを設定します。 この値はグローバルに設定された値を上書きします。 指定できる範囲は、0 ～ 32,768 ミリ秒です。 デフォルトは 0 です。 0 に設定すると、グローバルな最後のリスナー クエリー インターバルが使用されます。
ステップ 8	**ipv6 mld snooping tcn query solicit** 例： `Switch(config)# ipv6 mld snooping tcn query solicit`	（任意）トポロジ変更通知（TCN）をイネーブルにします。これにより、VLAN は設定された数のクエリーに関する IPv6 マルチキャスト トラフィックすべてをフラッディングしてから、マルチキャストデータをマルチキャストデータの受信を

	コマンドまたはアクション	目的
		要求するポートに対してのみ送信します。 デフォルトでは、TCN はディセーブルに設定されています。
ステップ 9	**ipv6 mld snooping tcn flood query count** *count* 例： `Switch(config)# ipv6 mld snooping tcn flood query count 5`	（任意）TCN がイネーブルの場合、送信される TCN クエリー数を指定します。 指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**show ipv6 mld snooping querier** ［ **vlan** *vlan-id*］ 例： `Switch(config)# show ipv6 mld snooping querier vlan 1`	（任意）スイッチまたは VLAN の MLD スヌーピング クエリア情報を確認します。

MLD リスナー メッセージ抑制の無効化（CLI）

デフォルトでは、MLD スヌーピング リスナー メッセージ抑制はイネーブルに設定されています。この機能がイネーブルの場合、スイッチはマルチキャスト ルータ クエリーごとに 1 つの MLD レポートのみを転送します。 メッセージ抑制がディセーブルの場合は、複数のマルチキャスト ルータに MLD レポートが転送されます。

MLD リスナー メッセージ抑制をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no ipv6 mld snooping listener-message-suppression** 例： `Switch(config)# no ipv6 mld snooping listener-message-suppression`	MLD メッセージ抑制をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 mld snooping** 例： `Switch# show ipv6 mld snooping`	IPv6 MLD スヌーピング レポート抑制がディセーブルであることを確認します。

MLD スヌーピング情報の表示

ダイナミックに学習された、あるいはスタティックに設定されたルータ ポートおよびVLANインターフェイスの MLD スヌーピング情報を表示できます。 また、MLD スヌーピング用に設定された VLAN の IPv6 グループ アドレス マルチキャスト エントリを表示することもできます。

表 *5*：*MLD* スヌーピング情報表示用のコマンド

コマンド	目的
show ipv6 mld snooping [**vlan** *vlan-id*]	スイッチのすべての VLAN または指定された VLAN の MLD スヌーピング設定情報を表示します。 （任意）個々のVLANに関する情報を表示するには、 **vlan** *vlan-id* を入力します。 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping mrouter [**vlan** *vlan-id*]	ダイナミックに学習され、手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。 MLD スヌーピングをイネーブルにすると、スイッチはマルチキャストルータの接続先であるインターフェイスを自動的に学習します。 これらのインターフェイスは動的に学習されます。 （任意）個々のVLANに関する情報を表示するには **vlan** *vlan-id* を入力します。 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。

コマンド	目的
show ipv6 mld snooping querier [**vlan** *vlan-id*]	VLAN 内で直前に受信した MLD クエリー メッセージの IPv6 アドレスおよび着信ポートに関する情報を表示します。 （任意） **vlan** *vlan-id* を入力して、単一の VLAN 情報を表示します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping address [**vlan** *vlan-id*] [**count** ｜ **dynamic** ｜ **user**]	すべての IPv6 マルチキャスト アドレス情報あるいはスイッチまたは VLAN の特定の IPv6 マルチキャスト アドレス情報を表示します。 • **count** を入力して、スイッチまたは VLAN のグループ数を表示します。 • **dynamic** を入力して、スイッチまたは VLAN の MLD スヌーピング学習済みグループ情報を表示します。 • **user** を入力して、スイッチまたは VLAN の MLD スヌーピング ユーザ設定グループ情報を表示します。
show ipv6 mld snooping address vlan *vlan-id* [*ipv6-multicast-address*]	指定の VLAN および IPv6 マルチキャスト アドレスの MLD スヌーピングを表示します。

MLD スヌーピングの設定例

スタティックなマルチキャスト グループの設定：例

次に、IPv6 マルチキャスト グループをスタティックに設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 2 static FF12::3 interface gigabitethernet

          1/0/1
Switch(config)# end
```

マルチキャスト ルータ ポートの設定：例

次に、VLAN 200 にマルチキャスト ルータ ポートを追加する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet

          0/2
Switch(config)# exit
```

MLD 即時脱退のイネーブル化：例

次に、VLAN 130 で MLD 即時脱退をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 130 immediate-leave
Switch(config)# exit
```

MLD スヌーピング クエリーの設定：例

次に、MLD スヌーピングのグローバルな堅牢性変数を 3 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# exit
```

次に、VLAN の MLD スヌーピングの最後のリスナー クエリー カウントを 3 に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
Switch(config)# exit
```

次に、MLD スヌーピングの最後のリスナー クエリー インターバル（最大応答時間）を 2000（2 秒）に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
Switch(config)# exit
```

第 4 章

IPv6 ユニキャスト ルーティングの設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

IPv6 ユニキャスト ルーティングの設定について

この章では、スイッチに IPv6 ユニキャスト ルーティングを設定する方法について説明します。

（注） この章のすべての IPv6 機能を使用するには、スイッチまたはスタック マスターが IP サービス フィーチャ セットを実行している必要があります。 IP ベースのフィーチャ セットを実行しているスイッチは、IPv6 スタティック ルーティング、IPv6 の RIP、および OSPF をサポートします。 LAN ベースのフィーチャ セットが稼働しているスイッチは、IPv6 ホスト機能だけをサポートします。

IPv6 の概要

IPv4 ユーザは IPv6 に移行することができ、エンドツーエンドのセキュリティ、Quality of Service（QoS）、およびグローバルに一意なアドレスのようなサービスを利用できます。 IPv6 アドレス スペースによって、プライベートアドレスの必要性が低下し、ネットワークエッジの境界ルータで Network Address Translation（NAT; ネットワーク アドレス変換）処理を行う必要性も低下します。

シスコの IPv6 の実装方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6553/products_ios_technology_home.html

IPv6 およびこの章のその他の機能については、

- 『*Cisco IOS IPv6 Configuration Library*』を参照してください。
- Cisco.com の [Search] フィールドを使用して、Cisco IOS ソフトウェア マニュアルを特定します。 たとえば、スタティック ルートについての情報が必要な場合は、[Search] フィールドで *Implementing Static Routes for IPv6* と入力すると、スタティック ルートについて調べられます。

IPv6 形式のアドレス

スイッチがサポートするのは、IPv6ユニキャストアドレスだけです。 サイトローカルなユニキャスト アドレスおよびマルチキャスト アドレスはサポートされません。

IPv6 の 128 ビットアドレスは、コロンで区切られた一連の 8 つの 16 進フィールド（n:n:n:n:n:n:n:n. の形式）で表されます。 次に、IPv6 アドレスの例を示します。

2031:0000:130F:0000:0000:09C0:080F:130B

実装を容易にするために、各フィールドの先行ゼロは省略可能です。 上記アドレスは、先行ゼロを省略した次のアドレスと同じです。

2031:0:130F:0:0:9C0:80F:130B

2 つのコロン（::）を使用して、ゼロが連続する 16 進フィールドを表すことができます。ただし、この短縮形を使用できるのは、各アドレス内で 1 回のみです。

2031:0:130F::09C0:080F:130B

IPv6 アドレス形式、アドレス タイプ、および IPv6 パケット ヘッダーの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library* 』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

「Information About Implementing Basic Connectivity for IPv6」の章では、次の項の内容がスイッチに適用されます。

- IPv6 アドレス形式
- IPv6 アドレス タイプ：ユニキャスト
- IPv6 アドレス タイプ：マルチキャスト

- IPv6 アドレスの出力表示
- 簡易 IPv6 パケット ヘッダー

サポート対象の IPv6 ユニキャスト ルーティング機能

スイッチは、ソフトウェアでルーティングされるホップ単位の拡張ヘッダー パケットをサポートします。

スイッチは、IPv6 の Routing Information Protocol（RIP）、および Open Shortest Path First（OSPF）バージョン 3 プロトコルによる IPv6 ルーティング機能を提供します。 等コスト ルートは 16 個までサポートされ、IPv4 および IPv6 フレームを回線レートで同時に転送できます。

128 ビット幅のユニキャスト アドレス

スイッチは集約可能なグローバル ユニキャスト アドレスおよびリンクに対してローカルなユニキャストアドレスをサポートします。 サイトに対してローカルなユニキャストアドレスはサポートされていません。

- 集約可能なグローバル ユニキャスト アドレスは、集約可能グローバル ユニキャスト プレフィックスの付いた IPv6 アドレスです。 このアドレス構造を使用すると、ルーティング プレフィックスを厳格に集約することができ、グローバルルーティング テーブル内のルーティング テーブル エントリ数が制限されます。 これらのアドレスは、組織を経由して最終的にインターネット サービス プロバイダーに至る集約リンク上で使用されます。

  これらのアドレスはグローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID によって定義されます。 現在のグローバル ユニキャスト アドレス割り当てには、バイナリ値 001（2000::/3）で開始するアドレス範囲が使用されます。 プレフィックスが 2000::/3（001）～ E000::/3（111）のアドレスには、Extended Unique Identifier（EUI）64 フォーマットの 64 ビット インターフェイス ID を設定する必要があります。

- リンクに対してローカルなユニキャストアドレスをすべてのインターフェイスに自動的に設定するには、修飾EUIフォーマット内で、リンクに対してローカルなプレフィックスFE80::/10（1111 1110 10）およびインターフェイスIDを使用します。 ネイバー探索プロトコル（NDP）およびステートレス自動設定プロセスでは、リンクに対してローカルなアドレスが使用されます。 ローカル リンク上のノードは、リンクに対してローカルなアドレスを使用します。 通信する場合に、グローバルに一意なアドレスは不要です。 IPv6ルータは、リンクに対してローカルな送信元または宛先アドレスを持つパケットをその他のリンクに転送しません。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library* 』の「Implementing IPv6 Addressing and Basic Connectivity」の章にある IPv6 ユニキャスト アドレスに関する項を参照してください。

IPv6 の DNS

IPv6 は、ドメイン ネーム システム（DNS）のレコード タイプを、DNS 名前/アドレスおよびアドレス/名前の検索プロセスでサポートします。 DNS AAAA リソース レコード タイプは IPv6 アド

レスをサポートし、IPv4 の A アドレス レコードと同等です。 スイッチは IPv4 および IPv6 の DNS 解決をサポートします。

IPv6 ユニキャストのパス MTU ディスカバリ

スイッチはシステム最大伝送単位（MTU）の IPv6 ノードへのアドバタイズおよびパス MTU ディスカバリをサポートします。 パス MTU ディスカバリを使用すると、ホストは指定されたデータパスを通るすべてのリンクの MTU サイズを動的に検出して、サイズに合せて調整できます。 IPv6 では、パスを通るリンクの MTU サイズが小さくてパケット サイズに対応できない場合、パケットの送信元がフラグメンテーションを処理します。

ICMPv6

IPv6 のインターネット制御メッセージプロトコル（ICMP）は、ICMP 宛先到達不能メッセージなどのエラー メッセージを生成して、処理中に発生したエラーや、その他の診断機能を報告します。 IPv6 では、ネイバー探索プロトコルおよびパス MTU ディスカバリに ICMP パケットも使用されます。

ネイバー探索

スイッチは、IPv6 対応の NDP、ICMPv6 の最上部で稼働するプロトコル、および NDP をサポートしない IPv6 ステーション対応のスタティック ネイバー エントリをサポートします。 IPv6 ネイバー探索プロセスは ICMP メッセージおよび送信請求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを判別し、ネイバーに到達できるかどうかを確認し、近接ルータを追跡します。

スイッチは、マスク長が 64 未満のルートに対して ICMPv6 リダイレクトをサポートしています。 マスク長が 64 ビットを超えるホスト ルートまたは集約ルートでは、ICMP リダイレクトがサポートされません。

ネイバー探索スロットリングにより、IPv6 パケットをルーティングするためにネクストホップ転送情報を取得するプロセス中に、スイッチ CPU に不必要な負荷がかかりません。 IPv6 パケットのネクスト ホップがスイッチによってアクティブに解決しようとしている同じネイバーである場合は、そのようなパケットが追加されると、スイッチはそのパケットをドロップします。 このドロップにより、CPU に余分な負荷がかからないようになります。

DRP

スイッチは、ルータのアドバタイズメント メッセージの拡張機能である、IPv6 Default Router Prefernce（DRP）をサポートします。 DRP では、特にホストがマルチホーム構成されていて、ルータが異なるリンク上にある場合に、ホストが適切なルータを選択する機能が向上しました。 スイッチは、Route Information Option（RFC 4191）をサポートしません。

IPv6 ホストは、オフリンク宛先へのトラフィック用にルータを選択する、デフォルトルータ リストを維持します。 次に、宛先用に選択されたルータは、宛先キャッシュに格納されます。 IPv6 NDP では、到達可能であるルータまたは到達可能性の高いルータが、到達可能性が不明または低いルータよりも優先されます。 NDP は、到達可能または到達可能の可能性があるルータとして、

常に同じルータを選択するか、またはルータ リストから繰り返し使用できます。 DRP を使用することにより、IPv6 ホストが、両方ともが到達可能または到達可能の可能性がある 2 台のルータを差別化するように設定できます。

DRP for IPv6 の詳細情報については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 のステートレス自動設定および重複アドレス検出

スイッチではステートレス自動設定が使用されているため、ホストやモバイル IP アドレスの管理のような、リンク、サブネット、およびサイト アドレス指定の変更を管理することができます。ホストはリンクに対してローカルな独自アドレスを自動的に設定します。起動元ノードはルータに送信請求を送信して、インターフェイス設定をアドバタイズするようルータに要求します。

自動設定および重複アドレス検出の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 アプリケーション

スイッチは、次のアプリケーションについて IPv6 をサポートします。

- Ping、traceroute、Telnet、および TFTP
- IPv6 トランスポートによるセキュア シェル（SSH）
- IPv6 トランスポートによる HTTP サーバ アクセス
- IPv4 トランスポートによる AAAA の DNS レゾルバ
- IPv6 アドレスの Cisco Discovery Protocol（CDP）サポート

これらのアプリケーションの管理に関する詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

DHCP for IPv6 アドレスの割り当て

DHCPv6 により、DHCP サーバは IPv6 ネットワーク アドレスなどの設定パラメータを IPv6 クライアントに渡すことができます。 このアドレス割り当て機能により、ホストが接続するネットワークに基づいて、適切なプレフィックス内での重複しないアドレス割り当てが管理されます。アドレスは、1 つまたは複数のプレフィックス プールから割り当てることができます。 デフォルトのドメインおよび DNS ネーム サーバ アドレスなど、その他のオプションは、クライアントに戻すことができます。アドレスプールは、特定のインターフェイス、複数のインターフェイス上で使用する場合に割り当てられます。または、サーバが自動的に適切なプールを検出できます。

これらの機能の詳細および設定方法については、『*Cisco IOS IPv6* コンフィギュレーション ガイド』を参照してください。

このマニュアルでは、DHCPv6 のアドレス割り当てについてだけ説明します。 DHCPv6 クライアント、サーバ、またはリレーエージェント機能の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing DHCP for IPv6」の章を参照してください。

IPv6 のスタティック ルート

スタティック ルートは手動で設定され、2 つのネットワーキング デバイス間のルートを明示的に定義します。 スタティック ルートが有効なのは、外部ネットワークへのパスが 1 つしかない小規模ネットワークの場合、または大規模ネットワークで特定のトラフィック タイプにセキュリティを設定する場合です。

スタティック ルートの詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

RIP for IPv6

IPv6 の Routing Information Protocol（RIP）は、ルーティング メトリックとしてホップ カウントを使用するディスタンスベクトル プロトコルです。 IPv6 アドレスおよびプレフィックスのサポート、すべての RIP ルータを含むマルチキャスト グループ アドレス FF02::9 を RIP アップデート メッセージの宛先アドレスとして使用する機能などがあります。

IPv6 の RIP の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

OSPF for IPv6

IP Base フィーチャ セットを実行中のスイッチは、IPv6 の Open Shortest Path First（OSPF）（IP のリンクステート プロトコル）をサポートします。 詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

HSRP for IPv6

IPServices および IPBase フィーチャ セットを実行中のスイッチは、IPv6 のホットスタンバイ ルータ プロトコル（HSRP）をサポートします。 HSRP は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。 IPv6 ホストは、IPv6 ネイバー探索ルータのアドバタイズメント メッセージによって使用可能なルータを学習します。 これらのメッセージは定期的にマルチキャストされるか、ホストにより送信請求されます。

HSRP IPv6 グループには、HSRP グループ番号に基づく仮想 MAC アドレス、およびデフォルトで HSRP 仮想 MAC アドレスに基づく HSRP の仮想 IPv6 リンクローカル アドレスがあります。 HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカル アドレスに送信されます。 グループがアクティブ ステートでなくなった場合、これらのメッセージは最後のメッセージが送信されたあとで停止します。

HSRP for IPv6 の設定に関する詳細については、「HSRP for IPv6」の項を参照してください。

EIGRP IPv6

IP サービス フィーチャ セットを実行中のスイッチは、IPv6 の Enhanced Interior Gateway Routing Protocol（EIGRP）をサポートします。 IPv6 の EIGRP は稼働するインターフェイス上で設定されるため、グローバルな IPv6 アドレスは不要です。

（注） IP ベース フィーチャ セットを実行中のスイッチでは、IPv6 EIGRP スタブ ルーティングを含め、IPv6 EIGRP 機能はすべてサポートされません。

EIGRP IPv6 インスタンスでは、実行する前に暗示的または明示的なルータ ID が必要です。 暗示的なルータ ID はローカルの IPv4 アドレスを基にして作成されるため、すべての IPv4 ノードには常に使用可能なルータ ID があります。 ただし、EIGRP IPv6 は IPv6 ノードだけが含まれるネットワークで稼働するため、使用可能な IPv4 ルータ ID がない場合があります。

EIGRP for IPv6 の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 による SNMP と Syslog

IPv4 と IPv6 の両方をサポートするには、IPv6 のネットワーク管理で IPv4 および IPv6 のトランスポートが必要になります。 IPv6 による Syslog は、このトランスポートのアドレス データ タイプをサポートします。

IPv6 による SNMP および Syslog は、次の機能を提供します。

- IPv4 と IPv6 両方のサポート
- SNMP に対する IPv6 トランスポート、および SNMP 変更による IPv6 ホストのトラップのサポート
- IPv6 アドレス指定をサポートするための SNMP および Syslog に関連する MIB
- IPv6 ホストをトラップ レシーバとして設定

IPv6 に関連するサポートでは、SNMP は既存の IP トランスポート マッピングを変更して、IPv4 と IPv6 を同時にサポートします。 次の SNMP 動作は、IPv6 トランスポート管理をサポートします。

- デフォルト設定のユーザ データグラム プロトコル（UDP）SNMP ソケットを開く
- *SR_IPV6_TRANSPORT* と呼ばれる新しいトランスポート メカニズムを提供
- IPv6 トランスポートによる SNMP 通知の送信
- IPv6 トランスポートの SNMP 名のアクセス リストのサポート
- IPv6 トランスポートを使用した SNMP プロキシ転送のサポート
- SNMP マネージャ機能と IPv6 トランスポートの連動確認

設定手順を含む、IPv6 による SNMP については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順を含む、IPv6 による Syslog については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv6 による HTTP（S）

HTTP クライアントは要求を IPv4 HTTP サーバと IPv6 HTTP サーバの両方に送信し、これらのサーバは IPv4 HTTP クライアントと IPv6 HTTP クライアントの両方からの要求に応答します。 IPv6 アドレスを含む URL は、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

受信ソケット コールは、IPv4 アドレス ファミリまたは IPv6 アドレス ファミリを選択します。 受信ソケットは、IPv4 ソケットまたは IPv6 ソケットのいずれかです。 リスニング ソケットは、接続を示す IPvv4 と IPv6 の両方の信号を待ち受け続けます。 IPv6 リスニング ソケットは、IPv6 ワイルドカード アドレスにバインドされています。

基本 TCP/IP スタックは、デュアル スタック環境をサポートします。 HTTP には、TCP/IP スタック、およびネットワーク層相互作用を処理するためのソケットが必要です。

HTTP 接続が確立するためには、基本ネットワーク接続（**ping**）がクライアントとサーバ ホストとの間に存在する必要があります。

詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

サポートされていない IPv6 ユニキャスト ルーティング機能

スイッチは、次の IPv6 機能をサポートしません。

- IPv6 ポリシーベース ルーティング
- IPv6 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）テーブルのサポート
- Multiprotocol ボーダー ゲートウェイ プロトコル（BGP）、および Intermediate System-to-Intermediate System（IS-IS）ルーティングの IPv6 ルーティング プロトコルのサポート
- サイトローカルなアドレス宛ての IPv6 パケット
- IPv4/IPv6 や IPv6/IPv4 などのトンネリング プロトコル
- IPv4/IPv6 または IPv6/IPv4 トンネリング プロトコルをサポートするトンネル エンドポイントとしてのスイッチ
- IPv6 ユニキャスト Reverse-Path Forwarding
- IPv6 Web Cache Communication Protocol（WCCP）

IPv6 機能の制限

スイッチでは IPv6 はハードウェアに実装されるため、ハードウェア メモリ内の IPv6 圧縮アドレスによる制限がいくつか発生します。 これらのハードウェア制限により、機能の一部が失われて、制限されます。

機能の制限は次のとおりです。

- スイッチはハードウェアで SNAP カプセル化 IPv6 パケットを転送できません。 これらはソフトウェアで転送されます。
- スイッチはハードウェアでソース ルーテッド IPv6 パケットに QoS 分類を適用できません。

IPv6 とスイッチ スタック

スイッチにより、スタック全体で IPv6 転送がサポートされ、スタック マスターで IPv6 ホスト機能がサポートされます。 スタック マスターは IPv6 ユニキャスト ルーティング プロトコルを実行してルーティング テーブルを計算します。 スタック メンバー スイッチはテーブルを受信して、転送用にハードウェア IPv6 ルートを作成します。 スタック マスターも、すべての IPv6 アプリケーションを実行します。

（注） IPv6 パケットをスタック内でルーティングするには、スタック内のすべてのスイッチで IP Base フィーチャ セットが実行されている必要があります。

新しいスイッチがスタック マスターになる場合、新しいマスターは IPv6 ルーティング テーブルを再計算してこれをメンバー スイッチに配布します。 新しいスタック マスターが選択中およびリセット中の間には、スイッチ スタックによる IPv6 パケットの転送は行われません。 スタック MAC アドレスが変更され、これによって IPv6 アドレスが変更されます。 **ipv6 address** *ipv6-prefix/prefix length* **eui-64** 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、拡張固有識別子（EUI）でスタック IPv6 アドレスを指定する場合、アドレスは、インターフェイス MAC アドレスに基づきます。 IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化（CLI），（50 ページ）を参照してください。

スタック上で永続的な MAC アドレスを設定し、スタック マスターが変更された場合、スタック MAC アドレスは、約 4 分間、変更されません。

IPv6 スタック マスターおよびメンバーの機能は次のとおりです。

- スタック マスター
  - IPv6 ルーティングプロトコルの実行
  - ルーティング テーブルの生成
  - dCEFv6 を使用するスタック メンバーへのルーティング テーブルの配布
  - IPv6 ホスト機能および IPv6 アプリケーションの実行
- スタック メンバー（IP サービス フィーチャ セットを実行している必要があります）
  - スタック マスターからの CEFv6 ルーティング テーブルの受信
  - ハードウェアへのルートのプログラミング

（注） IPv6 パケットに例外（IPv6Options）がなく、スタック内のスイッチでハードウェア リソースが不足していない場合、IPv6 パケットがスタック全体にわたってハードウェアでルーティングされます。

- マスターの再選択での CEFv6 テーブルのフラッシュ

IPv6 のデフォルト設定

表 *6* : *IPv6* のデフォルト設定

機能	デフォルト設定
SDM テンプレート	アドバンス デスクトップ。 デフォルトは拡張テンプレートです
IPv6 ルーティング	すべてのインターフェイスでグローバルにディセーブル
CEFv6 または dCEFv6	（注） IPv6 ルーティングがイネーブルの場合、CEFv6 および dCEF6 は自動的にイネーブル
IPv6 アドレス	未設定

IPv6アドレッシングの設定とIPv6ルーティングのイネーブル化（CLI）

ここでは、IPv6 アドレスを各レイヤ 3 インターフェイスに割り当てて、IPv6 トラフィックをスイッチ上でグローバル転送する方法を説明します。

スイッチ上の IPv6 を設定する前に、次の注意事項に従ってください。

- スイッチでは、この章で説明されたすべての機能がサポートされるわけではありません。 サポートされていない IPv6 ユニキャスト ルーティング機能, （48 ページ）を参照してください。
-
- **ipv6 address** インターフェイス コンフィギュレーション コマンドでは、16 ビット値を使用したコロン区切りの 16 進形式で指定したアドレスで指定した *ipv6-address* 変数および *ipv6-prefix* 変数を入力する必要があります。 *prefix-length* 変数（スラッシュ（/）で始まる）は、プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。

インターフェイス上の IPv6 トラフィックを転送するには、そのインターフェイス上でグローバル IPv6 アドレスを設定する必要があります。 インターフェイス上で IPv6 アドレスを設定すると、リンクに対してローカルなアドレスの設定、およびそのインターフェイスに対する IPv6 のアクティブ化が自動的に行われます。 設定されたインターフェイスは、次に示す、該当リンクの必須マルチキャスト グループに自動的に参加します。

- インターフェイスに割り当てられた各ユニキャスト アドレスの送信要求ノード マルチキャスト グループ FF02:0:0:0:0:1:ff00::/104（このアドレスはネイバー探索プロセスで使用される）
- すべてのノードを含む、ルータリンクに対してローカルなマルチキャスト グループ FF02::1
- すべてのルータを含む、リンクに対してローカルなマルチキャスト グループ FF02::2

インターフェイスから IPv6 アドレスを削除するには、**no ipv6 address** *ipv6-prefix/prefix length* **eui-64** または **no ipv6 address** *ipv6-address* **link-local** 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手動で設定したすべての IPv6 アドレスを削除するには、**no ipv6 address** インターフェイス コンフィギュレーション コマンドを引数なしで使用します。 IPv6 アドレスで明示的に設定されていないインターフェイスで IPv6 処理をディセーブルにするには、**no ipv6 enable** 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 ルーティングをグローバルにディセーブルにするには、**no ipv6 unicast-routing** 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。

IPv6 ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Addressing and Basic Connectivity for IPv6」の章を参照してください。

レイヤ 3 インターフェイスに IPv6 アドレスを割り当てて、IPv6 ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**sdm prefer dual-ipv4-and-ipv6** {**advanced** | **vlan**} 例： `Switch(config)# sdm prefer dual-ipv4-and-ipv6 default`	IPv4 および IPv6 をサポートする SDM テンプレートを選択します。 • **advanced**：スイッチをデフォルト テンプレートに設定して、システム リソースを均衡化します。 • **vlan**：ハードウェアでのルーティングをサポートしないスイッチでの VLAN 設定を最適化します。 （注） advanced はすべてのライセンス レベルで使用できます。 VLAN テンプレートは LAN ベースでのみ使用できます。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**reload** 例： `Switch# reload`	オペレーティング システムをリロードします。
ステップ 5	**configure terminal** 例： `Switch# configure terminal`	スイッチのリロード後、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	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、設定するレイヤ 3 インターフェイスを指定します。インターフェイスは物理インターフェイス、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できます。
ステップ 7	**no switchport** 例： `Switch(config-if)# no switchport`	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 8	次のいずれかを使用します。 • **ipv6 address** *ipv6-prefix/prefix length* **eui-64** • **ipv6 address** *ipv6-address/prefix length* • **ipv6 address** *ipv6-address* **link-local** • **ipv6 enable** • **ipv6 address***WORD* • **ipv6 address***autoconfig* • **ipv6 address***dhcp*	• IPv6 アドレスの下位 64 ビットの拡張固有識別子（EUI）を使用して、グローバル IPv6 アドレスを指定します。ネットワーク プレフィックスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。これにより、インターフェイス上で IPv6 処理がイネーブルになります。 • インターフェイスの IPv6 アドレスを手動で設定します。 • インターフェイスで IPv6 がイネーブルな場合に自動設定されるリンクローカルなアドレスでなく、インターフェイス上の特定のリンクローカルなアドレスを使用するように指定します。このコマンドにより、インターフェイス上で IPv6 処理がイネーブルになります。

	コマンドまたはアクション	目的

	例：
	`Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64`
	`Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64`
	`Switch(config-if)# ipv6 address 2001:0DB8:c18:1:: link-local`
	`Switch(config-if)# ipv6 enable`
		• インターフェイスに IPv6 リンクローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。 リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合だけです。

ステップ 9	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**ip routing** 例： `Switch(config)# ip routing`	スイッチ上で IP ルーティングをイネーブルにします。
ステップ 11	**ipv6 unicast-routing** 例： `Switch(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データ パケットの転送をイネーブルにします。
ステップ 12	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show ipv6 interface** *interface-id* 例： `Switch# show ipv6 interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 14	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv4 および IPv6 プロトコル スタックの設定（CLI）

IPv4 および IPv6 を両方サポートし、IPv6 ルーティングがイネーブルになるようにレイヤ 3 インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

（注） IPv6 アドレスを設定されていないインターフェイスで IPv6 処理をディセーブルにするには、**no ipv6 enable** 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。

手順の概要

1. **configure terminal**
2. **ip routing**
3. **ipv6 unicast-routing**
4. **interface** *interface-id*
5. **no switchport**
6. **ip address** *ip-address mask* [**secondary**]
7. 次のいずれかを使用します。
   - **ipv6 address** *ipv6-prefix/prefix length* **eui-64**
   - **ipv6 address** *ipv6-address/prefix length*
   - **ipv6 address** *ipv6-address* **link-local**
   - **ipv6 enable**
   - **ipv6 address***WORD*
   - **ipv6 address***autoconfig*
   - **ipv6 address***dhcp*
8. **end**
9. 次のいずれかを使用します。
   - **show interface** *interface-id*
   - **show ip interface** *interface-id*
   - **show ipv6 interface** *interface-id*
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing** 例： `Switch(config)# ip routing`	スイッチ上でルーティングをイネーブルにします。
ステップ 3	**ipv6 unicast-routing** 例： `Switch(config)# ipv6 unicast-routing`	スイッチ上で IPv6 データ パケットの転送をイネーブルにします。
ステップ 4	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	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、設定するレイヤ 3 インターフェイスを指定します。
ステップ 5	**no switchport** 例： `Switch(config-if)# no switchport`	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 6	**ip address** *ip-address mask* [**secondary**] 例： `Switch(config-if)# ip address 10.1.2.3 255.255.255`	インターフェイスのプライマリまたはセカンダリ IPv4 アドレスを指定します。
ステップ 7	次のいずれかを使用します。 • **ipv6 address** *ipv6-prefix/prefix length* **eui-64** • **ipv6 address** *ipv6-address/prefix length* • **ipv6 address** *ipv6-address* **link-local** • **ipv6 enable**	• グローバル IPv6 アドレスを指定します。 ネットワーク プレフィックスだけを指定します。最終の 64 ビットは、スイッチの MAC アドレスから自動的に計算されます。 • インターフェイスで IPv6 がイネーブルな場合に自動設定されるリンクローカルなアドレスでなく、インターフェイス上のリンクローカルなアドレスを使用するように指定します。

	コマンドまたはアクション	目的
	• **ipv6 address***WORD* • **ipv6 address***autoconfig* • **ipv6 address***dhcp*	• インターフェイスに IPv6 リンクローカルなアドレスを自動設定し、インターフェイスでの IPv6 処理をイネーブルにします。 リンクに対してローカルなアドレスを使用できるのは、同じリンク上のノードと通信する場合だけです。 （注） インターフェイスから手動で設定したすべての IPv6 アドレスを削除するには、**no ipv6 address** インターフェイス コンフィギュレーション コマンドを引数なしで使用します。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	次のいずれかを使用します。 • **show interface** *interface-id* • **show ip interface** *interface-id* • **show ipv6 interface** *interface-id*	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト ルータ プリファレンスの設定（CLI）

ルータ アドバタイズメント（RA）メッセージは、**ipv6 nd router-preference** インターフェイス コンフィギュレーション コマンドによって設定される DRP とともに送信されます。 DRP が設定されていない場合は、RA は中小規模のプリファレンスとともに送信されます。

リンク上の 2 つのルータが等価ではあっても、等コストではないルーティングを提供する可能性がある場合、およびポリシーでホストがいずれかのルータを選択するよう指示された場合は、DRP が有効です。

IPv6 の DRP の設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addresses and Basic Connectivity」の章を参照してください。

インターフェイス上のルータに DRP を設定するには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	インターフェイス コンフィギュレーション モードを開始して、DRP を指定するレイヤ 3 インターフェイスを特定します。
ステップ 3	**ipv6 nd router-preference** {**high** | **medium** | **low**} 例： `Switch(config-if)# ipv6 nd router-preference medium`	スイッチ インターフェイス上のルータに DRP を指定します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 interface** 例： `Switch# show ipv6 interface`	設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 ICMP レート制限の設定（CLI）

ICMP レート制限はデフォルトでイネーブルです。エラー メッセージのデフォルト間隔は 100 ミリ秒、デフォルト バケット サイズ（バケットに格納される最大トークン数）は 10 です。

ICMP レート制限パラメータを変更するには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 icmp error-interval** *interval* [*bucketsize*] 例： `Switch(config)# ipv6 icmp error-interval 50 20`	IPv6 ICMP エラー メッセージの間隔とバケット サイズを設定します。 • *interval*：バケットに追加されるトークンの間隔（ミリ秒）。 指定できる範囲は 0 ～ 2147483647 ミリ秒です。 • *bucketsize*：（任意）バケットに格納される最大トークン数。 範囲は 1 ～ 200 です。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 interface** [*interface-id*] 例： `Switch# show ipv6 interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 5	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 の CEF および dCEF の設定

シスコエクスプレスフォワーディング（CEF）は、ネットワーク パフォーマンスを最適化するためのレイヤ 3 IP スイッチング テクノロジーです。 CEF には高度な IP 検索および転送アルゴリズムが実装されているため、レイヤ 3 スイッチングのパフォーマンスを最大化できます。 高速スイッチング ルート キャッシュよりも CPU にかかる負担が少ないため、CEF はより多くの CPU 処理能力をパケット転送に振り分けることができます。 スイッチスタックでは、ハードウェアがスタック内で Distributed CEF（dCEF）を使用します。 IPv4 CEF および dCEF はデフォルトでイネーブルです。 IPv6 CEF および dCEF はデフォルトでディセーブルですが、IPv6 ルーティングを設定すると自動的にイネーブルになります。

IPv6 ルーティングが設定されていない場合は、IPv6 CEF および dCEF は自動的に無効になります。 IPv6 CEF および dCEF は、設定中に無効にできません。 IPv6 ステータスを確認するには、**show ipv6 cef** 特権 EXEC コマンドを入力します。

IPv6 ユニキャスト パケットをルーティングするには、最初に **ipv6 unicast-routing** 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、IPv6ユニキャストパケットの転送をグローバルに設定してから、**ipv6 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、特定のインターフェイスに IPv6 アドレスおよび IPv6 処理を設定する必要があります。

CEF および dCEF の設定に関する詳細情報については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 のスタティック ルーティングの設定（CLI）

スタティック IPv6 ルートを設定する前に、**ip routing** 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ルーティングをイネーブルにし、**ipv6 unicast-routing** 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 IPv6 パケットの転送をイネーブルにし、インターフェイスに IPv6 アドレスを設定して少なくとも 1 つのレイヤ 3 インターフェイス上で IPv6 をイネーブルにする必要があります。

スタティック IPv6 ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing Static Routes for IPv6」の章を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 route** *ipv6-prefix/prefix length* {*ipv6-address* | *interface-id*	スタティック IPv6 ルートを設定します。

	コマンドまたはアクション	目的
	[*ipv6-address*]} [*administrative distance*] 例： `Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130`	• *ipv6-prefix*：スタティック ルートの宛先となる IPv6 ネットワーク。スタティック ホスト ルートを設定する場合は、ホスト名も設定できます。 • */prefix length*：IPv6 プレフィックスの長さ。 プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。 10 進数値の前にスラッシュ記号が必要です。 • *ipv6-address*：指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレス。 ネクスト ホップの IPv6 アドレスを直接接続する必要はありません。再帰処理が実行されて、直接接続されたネクスト ホップの IPv6 アドレスが検出されます。 このアドレスは RFC 2373 に記載された形式（16 ビット値を使用したコロン区切りの 16 進表記で指定）で設定する必要があります。 • *interface-id*：Point-To-Point（ポイントツーポイント）インターフェイスおよびブロードキャスト インターフェイスからのダイレクト スタティック ルートを指定します。 ポイントツーポイント インターフェイスの場合、ネクスト ホップの IPv6 アドレスを指定する必要はありません。 ブロードキャスト インターフェイスの場合は、常にネクスト ホップの IPv6 アドレスを指定するか、または指定したプレフィックスをリンクに割り当てて、リンクに対してローカルなアドレスをネクスト ホップとして指定する必要があります。 パケットの送信先となるネクスト ホップの IPv6 アドレスを指定することもできます。 （注） リンクに対してローカルなアドレスをネクスト ホップとして使用する場合は、*interface-id* を指定する必要があります（リンクに対してローカルなネクスト ホップを隣接ルータに設定する必要もあります）。 • *administrative distance*：（任意）アドミニストレーティブ ディスタンス。 指定できる範囲は 1 ～ 254 です。デフォルト値は 1 で、この場合、接続されたルートを除くその他のどのルート タイプよりも、スタティック ルートが優先します。 フローティング スタティック ルートを設定する場合は、ダイナミック ルーティング プロトコルよりも大きなアドミニストレーティブ ディスタンスを使用します。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	次のいずれかを使用します。	IPv6 ルーティング テーブルの内容を表示して、設定を確認します。

	コマンドまたはアクション	目的

	• **show ipv6 static** [*ipv6-address* | *ipv6-prefix/prefix length*] [**interface** *interface-id*] [**detail**]][**recursive**] [**detail**]
	• **show ipv6 route static** [*updated*]
	
	例：
	`Switch# show ipv6 static 2001:0DB8::/32 interface gigabitethernet2/0/1`
	または
	`Switch# show ipv6 route static`
		• **interface** *interface-id*：（任意）出力インターフェイスとして指定されたインターフェイスを含むスタティック ルートのみを表示します。
		• **recursive**：（任意）再帰スタティック ルートのみを表示します。**recursive** キーワードは **interface** キーワードと相互に排他的です。ただし、コマンド構文に IPv6 プレフィックスが指定されているかどうかに関係なく、使用することができます。
		• **detail**：（任意）次に示す追加情報を表示します。
		◦有効な再帰ルートの場合、出力パス セットおよび最大分解深度
		◦無効なルートの場合、ルートが無効な理由

ステップ 5	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

RIP for IPv6 の設定（CLI）

IPv6 RIP を実行するようにスイッチを設定する前に、**ip routing** 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ルーティングをイネーブルにし、**ipv6 unicast-routing** 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 IPv6 パケットの転送をイネーブルにして、IPv6 RIP をイネーブルにするレイヤ 3 インターフェイス上で IPv6 をイネーブルにする必要があります。

IPv6 の RIP ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing RIP for IPv6」の章を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 router rip** *name* 例： `Switch(config)# ipv6 router rip cisco`	IPv6 RIP ルーティング プロセスを設定し、このプロセスに対してルータ コンフィギュレーションモードを開始します。
ステップ 3	**maximum-paths** *number-paths* 例： `Switch(config-router)# maximum-paths 6`	（任意）IPv6 RIP がサポートできる等コスト ルートの最大数を定義します。 指定できる範囲は 1 ～ 32 で、デフォルトは 16 ルートです。
ステップ 4	**exit** 例： `Switch(config-router)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	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、設定するレイヤ 3 インターフェイスを指定します。
ステップ 6	**ipv6 rip** *name* **enable** 例： `Switch(config-if)# ipv6 rip cisco enable`	指定された IPv6 RIP ルーティング プロセスをインターフェイス上でイネーブルにします。
ステップ 7	**ipv6 rip** *name* **default-information** {**only** | **originate**} 例： `Switch(config-if)# ipv6 rip cisco`	（任意）IPv6 デフォルト ルート（::/0）を RIP ルーティング プロセス アップデートに格納して、指定インターフェイスから送信します。

	コマンドまたはアクション	目的
	default-information only	（注） 任意のインターフェイスから IPv6 デフォルト ルート（::/0）を送信したあとに、ルーティング ループが発生しないようにするために、ルーティング プロセスは任意のインターフェイスで受信したすべてのデフォルト ルートを無視します。 • **only**：デフォルトルートを送信し、現在のインターフェイスで送信されたアップデート内のその他のすべてのルートを抑制するように選択します。 • **originate**：デフォルト ルート、および現在のインターフェイスで送信されたアップデート内のその他のすべてのルートを送信するように選択します。
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

ステップ 9	次のいずれかを使用します。
	• **show ipv6 rip** [*name*] [**interface***interface-id*] [**database**] [**next-hops**]
	• **show ipv6 rip**
	例：
	`Switch# show ipv6 rip cisco interface gigabitethernet2/0/1`
	または
	`Switch# show ipv6 rip`
		• 現在の IPv6 RIP プロセスに関する情報を表示します。
		• IPv6 ルーティング テーブルの現在の内容を表示します。

ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

OSPF for IPv6 の設定（CLI）

ネットワークでは、IPv6 の OSPF をカスタマイズできます。 ただし、IPv6 の OSPF のデフォルト設定は、ほとんどのカスタマーおよび機能の要件を満たします。

次の注意事項に従ってください。

- IPv6 コマンドのデフォルト設定を変更する場合は注意してください。 デフォルト設定を変更すると、IPv6 ネットワークの OSPF に悪影響が及ぶことがあります。
- インターフェイスで IPv6 OSPF をイネーブルにする前に、**ip routing** 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ルーティングをイネーブルにし、**ipv6 unicast-routing** 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 IPv6 パケットの転送をイネーブルにし、IPv6 OSPF をイネーブルにするレイヤ 3 インターフェイスで IPv6 をイネーブルにする必要があります。

IPv6 の OSPF ルーティングの設定の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing OSPF for IPv6」の章を参照してください。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 router ospf** *process-id* 例： `Switch(config)# ipv6 router ospf 21`	プロセスに対して OSPF ルータ コンフィギュレーション モードをイネーブルにします。 プロセス ID は、IPv6 OSPF ルーティング プロセスをイネーブルにする場合に管理上割り当てられる番号です。 この ID はローカルに割り当てられ、1 ～ 65535 の正の整数を指定できます。
ステップ 3	**area** *area-id* **range** {*ipv6-prefix/prefix length*} [**advertise** | **not-advertise**] [**cost** *cost*] 例： `Switch(config)# area .3 range 2001:0DB8::/32 not-advertise`	（任意）エリア境界でルートを統合および集約します。 • *area-id*：ルートをサマライズするエリアの ID。 10 進数または IPv6 プレフィックスのどちらかを指定できます。 • *ipv6-prefix/prefix length*：宛先 IPv6 ネットワーク、およびプレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進数。 10 進値の前にスラッシュ（/）を付加する必要があります。 • **advertise**：（任意）Type 3 サマリー LSA をアドバタイズおよび生成するように、アドレス範囲ステータスを設定します。

	コマンドまたはアクション	目的
		• **not-advertise**：（任意）アドレス範囲ステータスを DoNotAdvertise に設定します。 Type3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。 • **cost** *cost*：（任意）現在のサマリールートのメトリックまたはコストを設定します。宛先への最短パスを判別する場合に、OSPF SPF 計算で使用します。 指定できる値は 0 ～ 16777215 です。
ステップ 4	**maximum paths** *number-paths* 例： `Switch(config)# maximum paths 16`	（任意）IPv6 OSPF がルーティング テーブルに入力する必要がある、同じ宛先への等コスト ルートの最大数を定義します。指定できる範囲は 1 ～ 32 で、デフォルトは 16 です。
ステップ 5	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	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、設定するレイヤ 3 インターフェイスを指定します。
ステップ 7	**ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*] 例： `Switch(config-if)# ipv6 ospf 21 area .3`	インターフェイスで IPv6 の OSPF をイネーブルにします。 • **instance** *instance-id*：（任意）インスタンス ID
ステップ 8	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	次のいずれかを使用します。	• OSPF インターフェイスに関する情報を表示します。

	コマンドまたはアクション	目的

	• **show ipv6 ospf** [*process-id*] [*area-id*] **interface** [*interface-id*]
	• **show ipv6 ospf** [*process-id*] [*area-id*]
	
	例：
	`Switch# show ipv6 ospf 21 interface gigabitethernet2/0/1`
	または
	`Switch# show ipv6 ospf 21`
		• OSPF ルーティング プロセスに関する一般情報を表示します。

ステップ 10	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 の EIGRP の設定

IPv6 EIGRP を実行するようにスイッチを設定する前に、**ip routing** 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ルーティングをイネーブルにし、**ipv6 unicast-routing** 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 IPv6 パケットの転送をイネーブルにして、IPv6 EIGRP をイネーブルにするレイヤ 3 インターフェイス上で IPv6 をイネーブルにします。

明示的なルータ ID を設定するには、**show ipv6 eigrp** コマンドを使用して設定済みのルータ ID を確認してから、**router-id** コマンドを使用します。

EIGRP IPv4 の場合と同様に、EIGRPv6 を使用して EIGRP IPv6 インターフェイスを指定し、これらのサブセットを受動インターフェイスとして選択できます。 **passive-interface** コマンドを使用してインターフェイスをパッシブに設定してから、選択したインターフェイスで **no passive-interface** コマンドを使用してこれらのインターフェイスをアクティブにします。 受動インターフェイスでは、EIGRP IPv6 を設定する必要がありません。

設定手順の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing EIGRP for IPv6」の章を参照してください。

IPv6 の表示

次のコマンドの構文および使用方法の詳細については、Cisco IOS のコマンド リファレンスを参照してください。

表 *7* : ***IPv6*** のモニタリング用コマンド

コマンド	目的
show ipv6 access-list	アクセス リストのサマリーを表示します。
show ipv6 cef	IPv6 の Cisco エクスプレス フォワーディングを表示します。
show ipv6 interface *interface-id*	IPv6 インターフェイスのステータスと設定を表示します。
show ipv6 mtu	宛先キャッシュごとに IPv6 MTU を表示します。
show ipv6 neighbors	IPv6 ネイバー キャッシュ エントリを表示します。
show ipv6 ospf	IPv6 OSPF 情報を表示します。
show ipv6 prefix-list	IPv6 プレフィックス リストを表示します。
show ipv6 protocols	スイッチ上の IPv6 ルーティング プロトコルを表示します。
show ipv6 rip	IPv6 RIP ルーティング プロトコル ステータスを表示します。
show ipv6 route	IPv6 ルート テーブル エントリを表示します。
show ipv6 routers	ローカル IPv6 ルータを表示します。
show ipv6 static	IPv6 スタティック ルートを表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

表 *8*：*EIGRP IPv6* 情報を表示するためのコマンド

コマンド	目的
show ipv6 eigrp [*as-number*] *interface*	EIGRP IPv6 用に設定されたインターフェイスの情報を表示します。
show ipv6 eigrp [*as-number*] *neighbor*	EIGRP IPv6 で検出されたネイバーを表示します。
show ipv6 eigrp [*as-number*] *traffic*	送受信される EIGRP IPv6 パケット数を表示します。
show ipv6 eigrp topology [*as-number* | *ipv6-address*] [**active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors**| **Base**]	IPv6 トポロジ テーブルの EIGRP エントリを表示します。

DHCP for IPv6 アドレス割り当ての設定

DHCPv6 アドレス割り当てのデフォルト設定

デフォルトで、DHCPv6 機能はスイッチに設定されています。

DHCPv6 アドレス割り当ての設定時の注意事項

DHCPv6 アドレス割り当てを設定する場合は、次の注意事項に従ってください。

- 以下の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
  - DHCPv6 IPv6 ルーティングは、レイヤ 3 インターフェイス上でイネーブルである必要があります。
  - SVI：**interface vlan** *vlan_id* コマンドを使用して作成された VLAN インターフェイスです。
  - レイヤ 3 モードの EtherChannel ポート チャネル：**interface port-channel port-channel-number** コマンドを使用して作成されたポートチャネル論理インターフェイス。
- スイッチは、DHCPv6 クライアント、サーバ、またはリレーエージェントとして動作できます。 DHCPv6 クライアント、サーバ、およびリレー機能は、インターフェイスで相互に排他的です。

- DHCPv6 クライアント、サーバ、またはリレーエージェントは、マスタースイッチ上でだけ稼働します。 スタックマスターの再選出があった場合、新しいマスタースイッチはDHCPv6 設定を維持します。 ただし、DHCP サーバ データベース リース情報のローカルの RAM コピーは、維持されません。

DHCPv6 サーバ機能のイネーブル化（CLI）

DHCPv6 プールの特性を変更するには、**no** 形式の DHCP プール コンフィギュレーション モードコマンドを使用します。 インターフェイスに対して DHCPv6 サーバ機能をディセーブルにするには、**no ipv6 dhcp server** 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。

インターフェイスで DHCPv6 サーバをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 dhcp pool** *poolname* 例： `Switch(config)# ipv6 dhcp pool 7`	DHCP プール コンフィギュレーション モードを開始して、IPv6 DHCP プールの名前を定義します。 プール名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。
ステップ 3	**address prefix** *IPv6-prefix* {**lifetime**} {*t1 t1* | **infinite**} 例： `Switch(config-dhcpv6)# address prefix 2001:1000::0/64 lifetime 3600`	（任意）アドレス割り当て用のアドレス プレフィックスを指定します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。 **lifetime** *t1 t1*：IPv6 アドレス プレフィックスが有効ステートを維持するタイム インターバル（秒）を指定します。 指定できる範囲は 5 ～ 4294967295 秒です。 間隔を指定しない場合は、**infinite** を指定します。
ステップ 4	**link-address** *IPv6-prefix* 例： `Switch(config-dhcpv6)# link-address 2001:1002::0/64`	（任意）link-address IPv6 プレフィックスを指定します。 着信インターフェイス上のアドレスまたはパケットのリンクアドレスが指定した IPv6 プレフィックスに一致する場合、サーバは設定情報プールを使用します。 このアドレスは、16 ビット値をコロンで区切った 16 進数で指定する必要があります。

	コマンドまたはアクション	目的
ステップ 5	**vendor-specific** *vendor-id* 例： `Switch(config-dhcpv6)# vendor-specific 9`	（任意）ベンダー固有のコンフィギュレーション モードを開始して、ベンダー固有の ID 番号を指定します。 この番号は、ベンダーの IANA プライベート エンタープライズ番号です。 指定できる範囲は 1 ～ 4294967295 です。
ステップ 6	**suboption** *number* {**address** *IPv6-address* | **ascii** *ASCII-string* | **hex** *hex-string*} 例： `Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::`	（任意）ベンダー固有のサブオプション番号を入力します。 指定できる範囲は 1 ～ 65535 です。 IPv6 アドレス、ASCII テキスト、または16進文字列をサブオプション パラメータで定義されているように入力します。
ステップ 7	**exit** 例： `Switch(config-dhcpv6-vs)# exit`	DHCP プール コンフィギュレーション モードに戻ります。
ステップ 8	**exit** 例： `Switch(config-dhcpv6)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	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、設定するインターフェイスを指定します。
ステップ 10	**ipv6 dhcp server** [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**] 例： `Switch(config-if)# ipv6 dhcp server automatic`	インターフェイスに対して DHCPv6 サーバ機能をイネーブルにします。 • *poolname*：（任意）IPv6 DHCP プールのユーザ定義の名前 プール名には象徴的な文字列（Engineering など）または整数（0 など）を使用できます。 • **automatic**：（任意）システムが、クライアントにアドレスを割り当てるときに使用するプールを自動的に決定できるようにします。 • **rapid-commit**：（任意）2 つのメッセージの交換方法を許可します。

	コマンドまたはアクション	目的
		• **preference** *value*：（任意）サーバによって送信されるアドバタイズメントメッセージ内のプリファレンスオプションで指定されるプリファレンス値を設定します。 有効な範囲は 0 ～ 255 です。 デフォルトのプリファレンス値は 0 です。 • **allow-hint**：（任意）サーバが、SOLICIT メッセージ内のクライアントからの指示を考慮するかどうかを指定します。デフォルトでは、サーバはクライアントのヒントを無視します。
ステップ 11	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

ステップ 12	次のどちらかを実行します。
	• **show ipv6 dhcp pool**
	• **show ipv6 dhcp interface**
	例：
	`Switch# show ipv6 dhcp pool`
	または
	`Switch# show ipv6 dhcp interface`
		• DHCPv6 プール設定を確認します。
		• DHCPv6 サーバ機能がインターフェイス上でイネーブルであることを確認します。

ステップ 13	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

DHCPv6 クライアント機能のイネーブル化（CLI）

このタスクでは、インターフェイスに対して DHCPv6 クライアントをイネーブルにする方法を説明します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet 1/0/1`	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、設定するインターフェイスを指定します。
ステップ 3	**ipv6 address dhcp** [**rapid-commit**] 例： `Switch(config-if)# ipv6 address dhcp rapid-commit`	インターフェイスで DHCPv6 サーバから IPv6 アドレスを取得できるようにします。 **rapid-commit**：（任意）アドレス割り当てで、2 つのメッセージの交換方法を許可します。
ステップ 4	**ipv6 dhcp client request** [**vendor-specific**] 例： `Switch(config-if)# ipv6 dhcp client request vendor-specific`	（任意）インターフェイスでベンダー固有のオプションを要求できるようにします。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ipv6 dhcp interface** 例： `Switch# show ipv6 dhcp interface`	DHCPv6 クライアントがインターフェイスでイネーブルになっていることを確認します。

IPv6 ユニキャスト ルーティングの設定例

IPv6 アドレッシングの設定と IPv6 ルーティングのイネーブル化：例

次に、IPv6 プレフィックス 2001:0DB8:c18:1::/64 に基づく、リンクに対してローカルなアドレスおよびグローバル アドレスを使用して、IPv6 をイネーブルにする例を示します。 EUI-64 インターフェイス ID が、両方のアドレスの下位 64 ビットで使用されます。 **show ipv6 interface** EXEC コマンドの出力は、インターフェイスのリンクに対してローカルなプレフィックス FE80::/64 にインターフェイス ID（20B:46FF:FE2F:D940）を付加する方法を示すために追加されています。

```
Switch(config)# ipv6 unicast-routing
Switch(config)# interface gigabitethernet1/0/11
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
Switch# show ipv6 interface gigabitethernet1/0/11
GigabitEthernet1/0/11 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
  2001:0DB8:c18:1:20B:46FF:FE2F:D940, subnet is 2001:0DB8:c18:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
```

デフォルト ルータ プリファレンスの設定：例

次に、インターフェイス上のルータに高い DRP を設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ipv6 nd router-preference high
Switch(config-if)# end
```

IPv4 および IPv6 プロトコル スタックの設定：例

次に、インターフェイス上で IPv4 および IPv6 ルーティングをイネーブルにする例を示します。

```
Switch(config)# ip routing
Switch(config)# ipv6 unicast-routing
```

```
Switch(config)# interface fastethernet1/0/11
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.99.1 255.255.255.0
Switch(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Switch(config-if)# end
```

DHCPv6 サーバ機能のイネーブル化：例

次の例では、*engineering* という IPv6 アドレス プレフィックスを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool engineering
Switch(config-dhcpv6)#address prefix 2001:1000::0/64
Switch(config-dhcpv6)# end
```

次に、3 リンクアドレスおよび IPv6 アドレス プレフィックスを持つ *testgroup* と呼ばれるプールを設定する例を示します。

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

次の例では、*350* というベンダー固有オプションを持つプールを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool 350
Switch(config-dhcpv6)# address prefix 2001:1005::0/48
Switch(config-dhcpv6)# vendor-specific 9
Switch(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Switch(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Switch(config-dhcpv6-vs)# end
```

DHCPv6 クライアント機能のイネーブル化：例

次に、IPv6 アドレスを取得して、rapid-commit オプションをイネーブルにする例を示します。

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ipv6 address dhcp rapid-commit
```

IPv6 ICMP レート制限の設定：例

次に、IPv6 ICMP エラー メッセージ間隔を 50 ミリ秒に、バケット サイズを 20 トークンに設定する例を示します。

```
Switch(config)#ipv6 icmp error-interval 50 20
```

IPv6 のスタティック ルーティングの設定：例

次に、アドミニストレーティブ ディスタンスが 130 のフローティング スタティック ルートをインターフェイスに設定する例を示します。

```
Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130
```

IPv6 の RIP の設定：例

次に、最大 8 の等コスト ルートにより RIP ルーティング プロセス *cisco* をイネーブルにし、インターフェイス上でこれをイネーブルにする例を示します。

```
Switch(config)# ipv6 router rip cisco
Switch(config-router)# maximum-paths 8
Switch(config)# exit
Switch(config)# interface gigabitethernet2/0/11
Switch(config-if)# ipv6 rip cisco enable
```

IPv6 の表示：例

次に、**show ipv6 interface** 特権 EXEC コマンドの出力例を示します。

```
Switch# show ipv6 interface
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::20B:46FF:FE2F:D940
  Global unicast address(es):
    3FFE:C000:0:1:20B:46FF:FE2F:D940, subnet is 3FFE:C000:0:1::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF2F:D940
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
<output truncated>
```

第 5 章

IPv6 クライアント IP アドレス ラーニングの設定

IPv6 クライアント アドレス ラーニングの前提条件

IPv6 クライアント アドレス ラーニングを設定する前に、IPv6 をサポートするようにワイヤレス クライアントを設定します。

関連トピック

RA ガード ポリシーの設定（CLI），（85 ページ）

IPv6 クライアント アドレス ラーニングについて

クライアントアドレスラーニングは、アソシエーション、再アソシエーション、非認証、タイムアウト時に、ワイヤレス クライアントの IPv4 および IPv6 アドレス、スイッチによって維持されるクライアント遷移ステートについて学習するために、スイッチで設定されます。

IPv6 クライアントで IPv6 アドレスを取得するには、次の 3 つの方法があります。

- ステートレス アドレス自動設定（SLACC）
- ステートフル DHCPv6
- 静的設定

これらの方法のいずれの場合も、IPv6 クライアントは常にネイバー送信要求 DAD（重複アドレス検出）要求を送信して、ネットワークに重複する IP アドレスがないようにします。 スイッチはクライアントの NDP および DHCPv6 パケットをスヌープして、そのクライアント IP アドレスについて学習します。

SLAAC アドレス割り当て

IPv6 クライアント アドレス割り当て用の最も一般的な方法は、ステートレス アドレス自動設定（SLAAC）です。 SLAAC はクライアントが IPv6 プレフィクスに基づいてアドレスを自己割り当てするシンプルなプラグ アンド プレイ接続を提供します。 このプロセスが実現しました。

次のように、ステートレス アドレス自動設定（SLAAC）は設定されています。

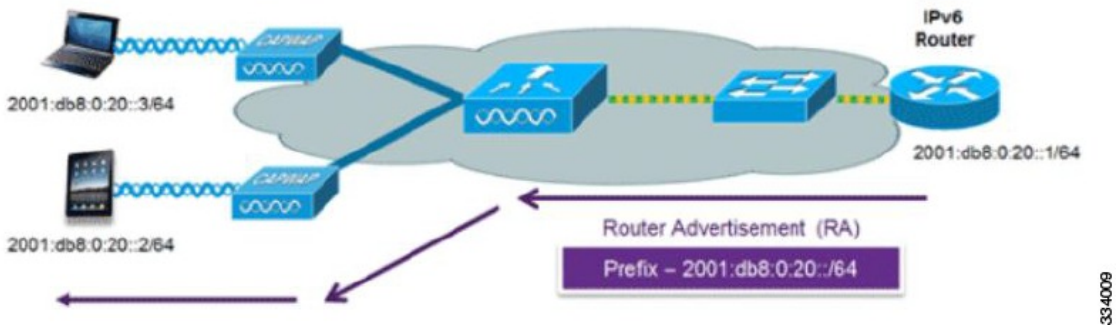
- ホストは、ルータ送信要求メッセージを送信します。
- ホストは、ルータ アドバタイズメント メッセージを待機します。
- ホストは、ルータ アドバタイズメント メッセージから IPv6 プレフィックスの最初の 64 ビットを取得し、これを 64 ビット EUI-64 アドレス（イーサネットの場合、MAC アドレスから作成されます）と組み合わせて、グローバル ユニキャスト メッセージを作成します。 ホストは、デフォルト ゲートウェイとして、ルータ アドバタイズメント メッセージの IP ヘッダーに含まれる送信元 IP アドレスも使用します。
- 重複アドレス検出は、選択されるランダム アドレスが他のクライアントと重複しないように、IPv6 クライアントによって実行されます。

- アルゴリズムの選択はクライアントに依存し、多くの場合は設定できます。

次の 2 種類のアルゴリズムに基づいて IPv6 アドレスの最後の 64 ビットが学習可能です。

- インターフェイスの MAC アドレスに基づく EUI-64、または
- ランダムに生成されるプライベート アドレス。

図 *1*：*SLAAC* アドレス割り当て



Cisco 対応 IPv6 ルータからの次の Cisco IOS コンフィギュレーション コマンドを使用して、SLAAC のアドレッシングとルータ アドバタイズメントを有効にします。

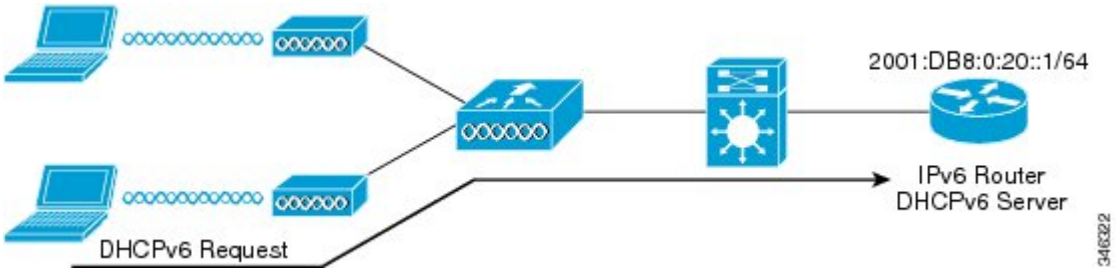
```
ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end
```

関連トピック

IPv6 スヌーピングの設定（CLI），（90 ページ）
DHCP プールの設定（CLI），（94 ページ）
DHCP を使用しないステートレス自動アドレス設定の設定（CLI），（95 ページ）
DHCP によるステートレス自動アドレス設定の設定（CLI），（96 ページ）
ステートフル DHCP のローカルな設定（CLI），（98 ページ）
ステートフル DHCP の外部的設定（CLI），（100 ページ）

ステートフル DHCPv6 アドレス割り当て

図 *2*：ステートフル *DHCPv6* アドレス割り当て



DHCPv6の使用は、SLAACがすでに導入されている場合は、IPv6クライアント接続で要求されません。 DHCPv6 にはステートレスおよびステートフルという 2 種類の動作モードがあります。

DHCPv6 ステートレス モードは、ルータ アドバタイズメントで使用できない追加のネットワーク情報をクライアントに提供するために使用しますが、これはIPv6アドレスではありません。すでに SLAAC によって提供されているためです。 この情報には DNS ドメイン名、DNS サーバ、その他の DHCP ベンダー固有オプションを含めることができます。 このインターフェイス設定は、SLAAC をイネーブルにしてステートレス DHCPv6 を実装する Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
ipv6 address 2001:DB8:0:20::1/64
end
```

マネージド モードとも呼ばれる DHCPv6 ステートフル オプションは、DHCPv4 に対して同じように動作します。つまり固有のアドレスを、SLAAC のとおりにアドレスの最後の 64 ビットを生成するクライアントではなく、それぞれのクライアントに割り当てます。 このインターフェイス設定は、ローカル Switchのステートフル DHCPv6 を実装している Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
end
```

このインターフェイス設定は、外部 DHCP サーバのステートフル DHCPv6 を実装している Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp_relay destination 2001:DB8:0:20::2
end
```

関連トピック

IPv6 スヌーピングの設定（CLI），（90 ページ）
DHCP プールの設定（CLI），（94 ページ）
DHCP を使用しないステートレス自動アドレス設定の設定（CLI），（95 ページ）
DHCP によるステートレス自動アドレス設定の設定（CLI），（96 ページ）
ステートフル DHCP のローカルな設定（CLI），（98 ページ）
ステートフル DHCP の外部的設定（CLI），（100 ページ）

静的 IP アドレス割り当て

クライアントにスタティックに設定されたアドレス。

ルータ要求

ルータ送信要求メッセージは、ローカル ルーティングに関する情報を入手できる、またはステートレス自動設定を設定できるルータ アドバタイズメントを送信するようにローカルルータを促進するために、ホスト コントローラによって発行されます。 ルータ アドバタイズメントは定期的に送信され、起動時または再起動操作後などに、ホストはルータ送信要求を使用して即時ルータ アドバタイズメントを要求します。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI），（91 ページ）

Router Advertisement

ルータ アドバタイズメント メッセージは、ルータから定期的に送信されるか、ホストからのルータ送信要求メッセージへの応答として送信されます。 これらのメッセージに含まれる情報は、ホストでステートレス自動設定を実行し、ルーティング テーブルを変更するために使用されます。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI），（91 ページ）

ネイバー探索

IPv6 ネイバー ディスカバリとは、近隣のノード間の関係を決定するメッセージとプロセスのことです。 ネイバー ディスカバリは、IPv4 で使用されていた ARP、ICMP ルータ探索、および ICMP リダイレクトに代わるものです。

信頼できるバインディング テーブル データベースを構築するために、IPv6 ネイバー ディスカバリ検査によってネイバー ディスカバリ メッセージが分析され、準拠しない IPv6 ネイバー ディスカバリ パケットはドロップされます。 スイッチ内のネイバー バインディング テーブルでは、各 IPv6 アドレスと、アソシエートされた MAC アドレスが追跡されます。 クライアントは、ネイバー バインディング タイマーに従って、テーブルから消去されます。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI），（91 ページ）

ネイバー探索抑制

ワイヤレス クライアントの IPv6 アドレスは、スイッチによってキャッシュされます。 スイッチが IPv6 アドレスを検索する NS マルチキャストを受信して、スイッチによって特定された目的のアドレスがクライアントのいずれかに属している場合、スイッチはクライアントに代わって NA メッセージで応答します。 このプロセスによって IPv4 のアドレス解決プロトコル（ARP）テーブルと同等のテーブルが生成されますが、より効率的であり、たいていの場合、使用されるメッセージは少なくなります。

（注） スイッチがプロキシのように動作し NA で応答するのは、**ipv6 nd suppress** コマンドが設定されている場合だけです。

スイッチにワイヤレス クライアントの IPv6 アドレスがない場合、スイッチは NA で応答せず、NS パケットをワイヤレス側に転送します。 この問題を解決するために、NS マルチキャスト フォワーディング ノブが用意されています。 このノブがイネーブルの場合、スイッチは存在しない（キャッシュ欠落）IPv6 アドレスの NS パケットを取得し、ワイヤレス側に転送します。 このパケットは、目的のワイヤレス クライアントに到達し、クライアントは NA で応答します。

このキャッシュ ミス シナリオが発生するのはまれで、完全な IPv6 スタックが実装されていないクライアントが、NDP 時にそれらの IPv6 アドレスをアドバタイズしない可能性はほとんどありません。

関連トピック

IPv6 ND 抑制ポリシーの設定（CLI），（91 ページ）

RA Guard

IPv6 クライアントは、IPv6 アドレスを設定し、IPv6 ルータ アドバタイズメント（RA）パケットに基づいてルータ テーブルにデータを入力します。 RA ガード機能は、有線ネットワークの RA ガード機能に類似しています。 RA ガードは、ワイヤレス クライアントから発信される不要な、または不正な RA パケットをドロップすることによって、IPv6 ネットワークのセキュリティを強化します。 この機能が設定されていないと、悪意のある IPv6 ワイヤレス クライアントが、多くの場合は高い優先順位で、それ自体をネットワークのルータとして通知する可能性があり、そのため、正規の IPv6 ルータよりも優先されることになります。

また、RA ガードは、着信 RA を調べて、メッセージまたはスイッチ設定で検出された情報のみに基づいて、それらをスイッチするかブロックするかを決定します。 受信したフレームで使用できる情報は、RA の検証に有用です。

- フレームが受信されるポート
- IPv6 送信元アドレス
- プレフィックス リスト

スイッチで作成された次の設定情報は、受信した RA フレームで検出された情報に対して検証するときに RA ガードで使用できます。

- RA ガード メッセージの受信用に信頼できる/信頼できないポート
- RA 送信者の信頼できる/信頼できない送信元 IPv6 アドレス
- 信頼できる/信頼できないプレフィックス リストおよびプレフィックス範囲
- ルータ プリファレンス

RA ガードはスイッチで行われます。 スイッチで RA メッセージをドロップするようにスイッチを設定できます。 すべての IPv6 RA メッセージがドロップされ、それによって他のワイヤレス クライアントおよびアップストリーム有線ネットワークが悪意のある IPv6 クライアントから保護されます。

```
//Create a policy for RA Guard//
ipv6 nd raguard policy raguard-router
trusted-port
device-role router
//Applying the RA Guard Policy on port/interface//
interface tengigabitethernet1/0/1 (Katana)
interface gigabitethernet1/0/1 (Edison)

ipv6 nd raguard attach-policy raguard-router
```

関連トピック

RA ガード ポリシーの設定（CLI），（85 ページ）
RA ガード ポリシーの適用（CLI），（86 ページ）
RA スロットル ポリシーの設定（CLI），（87 ページ）
VLAN への RA スロットル ポリシーの適用（CLI），（89 ページ）

RA スロットリング

RA スロットリングは、コントローラがワイヤレス ネットワーク宛ての RA パケットを強制的に制限できるようにします。 RA スロットリングを有効にすることにより、多数の RA パケットを送信するルータを最小限の頻度に調整することができ、その場合も IPv6 クライアントの接続は維持されます。 クライアントが RS パケットを送信すると、RA がクライアントに返送されます。 この RA は、コントローラを通過でき、クライアントにユニキャストされます。 このプロセスによって、新しいクライアントやローミング クライアントが RA スロットリングの影響を受けないようにすることができます。

関連トピック

RA ガード ポリシーの設定（CLI），（85 ページ）
RA ガード ポリシーの適用（CLI），（86 ページ）
RA スロットル ポリシーの設定（CLI），（87 ページ）
VLAN への RA スロットル ポリシーの適用（CLI），（89 ページ）

IPv6 ユニキャストの設定（CLI）

IPv6 ユニキャストはスイッチとコントローラで常にイネーブルにする必要があります。 IPv6 ユニキャスト ルーティングはディセーブルに設定されています。

はじめる前に

IPv6 ユニキャスト データグラムの転送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 unicast-routing** コマンドを使用します。 IPv6 ユニキャスト データグラムの転送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。

手順の概要

1. **configure terminal**
2. **ipv6 unicast routing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ipv6 unicast routing** 例： `Switch (config)# ipv6 unicast routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。

RA ガード ポリシーの設定（CLI）

IPv6 クライアント アドレスを追加し、IPv6 ルータ アドバタイズメント パケットに基づいてルータ テーブルに入力するには、スイッチで RA ガード ポリシーを設定します。

はじめる前に

手順の概要

1. **configure terminal**
2. **ipv6 nd raguard policy** raguard-router
3. **trustedport**
4. **device-role router**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 nd raguard policy** raguard-router 例： `Switch(config)# ipv6 nd raguard policy raguard-router`	RA ガードポリシー名を定義して、RA ガードポリシーコンフィギュレーション モードを開始します。
ステップ 3	**trustedport** 例： `Switch(config-ra-guard)# trustedport`	（任意）このポリシーが信頼できるポートに適用されることを指定します。

	コマンドまたはアクション	目的
ステップ 4	**device-role router** 例： `Switch(config-ra-guard)# device-role router`	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。
ステップ 5	**exit** 例： `Switch(config-ra-guard)# exit`	RA ガードポリシー コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。

関連トピック

IPv6 クライアント アドレス ラーニングの前提条件，（78 ページ）
RA Guard，（83 ページ）
RA スロットリング，（84 ページ）
RA ガード ポリシーの適用（CLI），（86 ページ）
RA スロットル ポリシーの設定（CLI），（87 ページ）
VLAN への RA スロットル ポリシーの適用（CLI），（89 ページ）

RA ガード ポリシーの適用（CLI）

スイッチで RA ガード ポリシーを適用すると、すべての信頼できない RA がブロックされます。

はじめる前に

手順の概要

1. **configure terminal**
2. **interface tengigabitethernet** 1/0/1
3. **ipv6 nd raguard attach-policy** raguard-router
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface tengigabitethernet** 1/0/1 例： `Switch (config)# interface tengigabitethernet 1/0/1`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 3	**ipv6 nd raguard attach-policy** raguard-router 例： `Switch(config-if)# ipv6 nd raguard attach-policy raguard-router`	指定したインターフェイスに IPv6 RA ガード機能を適用します。
ステップ 4	**exit** 例： `Switch(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

関連トピック

RA ガード ポリシーの設定（CLI），（85 ページ）
RA Guard,（83 ページ）
RA スロットリング,（84 ページ）
RA スロットル ポリシーの設定（CLI），（87 ページ）
VLAN への RA スロットル ポリシーの適用（CLI），（89 ページ）

RA スロットル ポリシーの設定（CLI）

強制的に制限できるように RA スロットル ポリシーを設定します。

はじめる前に

手順の概要

1. **configure terminal**
2. **ipv6 nd ra-throttler policy** ra-throttler1
3. **throttleperiod**500
4. **max-through**10
5. **allow-atleast** 5 **at-most** 10

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 nd ra-throttler policy** ra-throttler1 例： `Switch(config)# ipv6 nd ra-throttler policy ra-throttler1`	ルータ アドバタイズメント（RA）スロットラ ポリシー名を定義して、IPv6 RA スロットル ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**throttleperiod**500 例： `Switch(config-nd-ra-throttle)# throttleperiod 500`	IPv6 RA スロットラ ポリシーのスロットル期間を設定します。
ステップ 4	**max-through**10 例： `Switch(config-nd-ra-throttle)# max-through 500`	スロットル期間ごとに、VLAN あたりのマルチキャスト RA を制限します。
ステップ 5	**allow-atleast** 5 **at-most** 10 例： `Switch(config-nd-ra-throttle)# allow-atleast 5 at-most 10`	RA スロットラ ポリシーのスロットル期間ごとに、デバイスあたりのマルチキャスト RA 数を制限します。

関連トピック

RA ガード ポリシーの設定（CLI），（85 ページ）
RA ガード ポリシーの適用（CLI），（86 ページ）

RA Guard, （83 ページ）
RA スロットリング, （84 ページ）
VLAN への RA スロットル ポリシーの適用（CLI）, （89 ページ）

VLAN への RA スロットル ポリシーの適用（CLI）

VLAN に RA スロットル ポリシーを適用します。 RA スロットリングを有効にすることにより、多数の RA パケットを送信するルータを最小限の頻度に調整することができ、その場合も IPv6 クライアントの接続は維持されます。

はじめる前に

手順の概要

1. **configure terminal**
2. **vlan configuration** 1
3. **ipv6 nd ra throttler attach-policy** ra-throttler1

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration** 1 例： `Switch(config)# vlan configuration 1`	VLAN または VLAN の集合を設定して、VLAN コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd ra throttler attach-policy** ra-throttler1 例： `Switch(config-vlan)# ipv6 nd ra throttler attach-policy ra-throttler1`	VLAN または VLAN の集合に IPv6 RA スロットル ポリシーを接続します。

関連トピック

RA ガード ポリシーの設定（CLI）, （85 ページ）
RA ガード ポリシーの適用（CLI）, （86 ページ）
RA スロットル ポリシーの設定（CLI）, （87 ページ）

RA Guard, （83 ページ）
RA スロットリング, （84 ページ）

IPv6 スヌーピングの設定（CLI）

IPv6 スヌーピングはスイッチとコントローラで常にイネーブルにする必要があります。

はじめる前に

クライアント マシンで IPv6 をイネーブルにします。

手順の概要

1. **vlan configuration 1**
2. **ipv6 snooping**
3. **ipv6 nd suppress**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**vlan configuration 1** 例： `Switch(config)# vlan configuration 1`	Vlan コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 snooping** 例： `Switch(config-vlan)# ipv6 snooping`	Vlan で IPv6 スヌーピングをイネーブルにします。
ステップ 3	**ipv6 nd suppress** 例： `Switch(config-vlan-config)# ipv6 nd suppress`	Vlan で IPv6 ND 抑制をイネーブルにします。
ステップ 4	**exit** 例： `Switch(config-vlan-config)# exit`	設定を保存し、Vlan コンフィギュレーション モードを終了します。

関連トピック

SLAAC アドレス割り当て, （78 ページ）

ステートフル DHCPv6 アドレス割り当て，（80 ページ）

IPv6 ND 抑制ポリシーの設定（CLI）

IPv6 ネイバー探索（ND）マルチキャスト抑制機能では、ドロップする（およびターゲットに代わって送信要求に応答する）、またはユニキャスト トラフィックに変換することで、できるだけ多くの ND マルチキャスト ネイバー送信要求（NS）メッセージを停止します。 この機能は、レイヤ 2 スイッチまたはワイヤレス コントローラで実行され、適切なリンクの処理に必要な制御トラフィックの量を減らすために使用されます。

アドレスがバインディングテーブルに挿入されると、マルチキャストアドレスに送信されたアドレス解決要求が代行受信され、デバイスはアドレスの所有者に代わって応答するか、レイヤ 2 で要求をユニキャスト メッセージに変換して宛先に転送します。

はじめる前に

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 nd suppress policy**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch(config)# enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**ipv6 nd suppress policy** 例： `Switch (config)# ipv6 nd suppress policy`	ND 制御ポリシー名を定義して ND 制御ポリシー コンフィギュレーション モードを開始します。

関連トピック

ルータ要求，（81 ページ）

Router Advertisement, （81 ページ）
ネイバー探索, （82 ページ）
ネイバー探索抑制, （82 ページ）

VLAN/PortChannel での IPv6 スヌーピングの設定

ネイバー探索（ND）抑制は、VLAN またはスイッチ ポートでイネーブルまたはディセーブルにできます。

はじめる前に

手順の概要

1. **vlan config901**
2. **ipv6 nd suppress**
3. **end**
4. **interface gi1/0/1**
5. **ipv6 nd suppress**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**vlan config901** 例： `Switch(config)# vlan config901`	VLAN を作成し、VLAN コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 nd suppress** 例： `Switch(config-vlan)# ipv6 nd suppress`	VLAN に IPv6 nd 抑制を適用します。
ステップ 3	**end** 例： `Switch(config-vlan)# end`	VLAN 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 モードを開始します。
ステップ 4	**interface gi1/0/1** 例： `Switch (config)# interface gi1/0/1`	ギガビット イーサネット ポート インターフェイスを作成します。
ステップ 5	**ipv6 nd suppress** 例： `Switch(config-vlan)# ipv6 nd suppress`	インターフェイスに IPv6 nd 抑制を適用します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Switch(config-vlan)# end`	VLAN 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 モードを開始します。

Switch での IPv6 の設定（CLI）

インターフェイス上の IPv6 を設定するには、この設定例を使用します。

はじめる前に

クライアント上の IPv6 および有線インフラストラクチャ上の IPv6 サポートをイネーブルにします。

手順の概要

1. **interface vlan** 1
2. **ip address** fe80::1 link-local
3. **ipv6 enable**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interface vlan** 1 例： `Switch(config)# interface vlan 1`	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ip address** fe80::1 link-local
	
	例：
	`Switch(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Switch(config-if)# ipv6 address fe80::1 link-local`
	`Switch(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Switch(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。

ステップ 3	**ipv6 enable** 例： `Switch(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	インターフェイス モードを終了します。

DHCP プールの設定（CLI）

手順の概要

1. **ipv6 dhcp pool** Vlan21
2. **address prefix** 2001:DB8:0:1:FFFF:1234::/64 **lifetime** 300 10
3. **dns-server** 2001:100:0:1::1
4. **domain-name** example.com
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ipv6 dhcp pool** Vlan21 例： `Switch(config)# ipv6 dhcp pool vlan1`	コンフィギュレーションモードを開始し、VLANの IPv6 DHCP プールを設定します。
ステップ 2	**address prefix** 2001:DB8:0:1:FFFF:1234::/64 **lifetime** 300 10 例： `Switch(config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10`	コンフィギュレーション DHCP モードを開始し、VLANのアドレスプールとそのライフタイムを設定します。
ステップ 3	**dns-server** 2001:100:0:1::1 例： `Switch(config-dhcpv6)# dns-server 2001:20:21::1`	DHCP プールの DNS サーバを設定します。
ステップ 4	**domain-name** example.com 例： `Switch(config-dhcpv6)# domain-name example.com`	完全な非修飾ホスト名になるようにドメイン名を設定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

SLAAC アドレス割り当て，（78 ページ）
ステートフル DHCPv6 アドレス割り当て，（80 ページ）

DHCP を使用しないステートレス自動アドレス設定の設定（CLI）

手順の概要

1. **interface vlan** 1
2. **ip address** fe80::1 link-local
3. **ipv6 enable**
4. **no ipv6 nd managed-config-flag**
5. **no ipv6 nd other-config-flag**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interface vlan** 1 例： `Switch(config)# interface vlan 1`	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ip address** fe80::1 link-local
	
	例：
	`Switch(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Switch(config-if)# ipv6 address fe80::1 link-local`
	`Switch(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Switch(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 enable** 例： `Switch(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。

ステップ 4	**no ipv6 nd managed-config-flag**
	
	例：
	`Switch(config)#interface vlan 1`
	`Switch(config-if)# no ipv6 nd managed-config-flag`
		接続されたホストで、アドレスの取得にステートフル自動設定が使用されないようにします。

ステップ 5	**no ipv6 nd other-config-flag** 例： `Switch(config-if)# no ipv6 nd other-config-flag`	接続されたホストで、DHCP からの非アドレス オプションの取得に（ドメインなど）ステートフル自動設定が使用されないようにします。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

SLAAC アドレス割り当て，（78 ページ）
ステートフル DHCPv6 アドレス割り当て，（80 ページ）

DHCPによるステートレス自動アドレス設定の設定（CLI）

手順の概要

1. **interface vlan** 1
2. **ip address** fe80::1 link-local
3. **ipv6 enable**
4. **no ipv6 nd managed-config-flag**
5. **ipv6 nd other-config-flag**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interface vlan** 1 例： `Switch(config)# interface vlan 1`	インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ip address** fe80::1 link-local
	
	例：
	`Switch(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Switch(config-if)# ipv6 address fe80::1 link-local`
	`Switch(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Switch(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		リンクローカルオプションを使用してインターフェイスで IPv6 アドレスを設定します。

ステップ 3	**ipv6 enable** 例： `Switch(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。

ステップ 4	**no ipv6 nd managed-config-flag**
	
	例：
	`Switch(config)#interface vlan 1`
	`Switch(config-if)# no ipv6 nd managed-config-flag`
		接続されたホストで、アドレスの取得にステートフル自動設定が使用されないようにします。

ステップ 5	**ipv6 nd other-config-flag** 例： `Switch(config-if)# no ipv6 nd other-config-flag`	接続されたホストで、DHCP からの非アドレス オプションの取得に（ドメインなど）ステートフル自動設定が使用されないようにします。
ステップ 6	**end** 例： `Switch(config)# end`	インターフェイス モードを終了します。

関連トピック

SLAAC アドレス割り当て，（78 ページ）
ステートフル DHCPv6 アドレス割り当て，（80 ページ）

ステートフル DHCP のローカルな設定（CLI）

このインターフェイス設定は、ローカル Switchのステートフル DHCPv6 を実装している Cisco IOS IPv6 ルータ用です。

はじめる前に

手順の概要

1. **configure terminal**
2. **ipv6 unicast-routing**
3. **ipv6 dhcp pool** IPv6_DHCPPOOL
4. **address prefix** 2001:DB8:0:1:FFFF:1234::/64
5. **dns-server** 2001:100:0:1::1
6. **domain-name** example.com
7. **exit**
8. **interface** vlan1
9. **description IPv6-DHCP-Stateful**
10. **ipv6 address** 2001:DB8:0:20::1/64
11. **ip address** 192.168.20.1 255.255.255.0
12. **ipv6 nd prefix** 2001:db8::/64 **no-advertise**
13. **ipv6 nd managed-config-flag**
14. **ipv6 nd other-config-flag**
15. **ipv6 dhcp server** IPv6_DHCPPOOL

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 unicast-routing** 例： `Switch(config)# ipv6 unicast-routing`	ユニキャスト用に IPv6 を設定します。
ステップ 3	**ipv6 dhcp pool** IPv6_DHCPPOOL 例： `Switch (config)# ipv6 dhcp pool IPv6_DHCPPOOL`	コンフィギュレーションモードを開始し、VLAN の IPv6 DHCP プールを設定します。

	コマンドまたはアクション	目的
ステップ 4	**address prefix** 2001:DB8:0:1:FFFF:1234::/64 例： `Switch (config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64`	プールに入力するアドレス範囲を指定します。
ステップ 5	**dns-server** 2001:100:0:1::1 例： `Switch (config-dhcpv6)# dns-server 2001:100:0:1::1`	DHCP クライアントに DNS サーバのオプションを提供します。
ステップ 6	**domain-name** example.com 例： `Switch (config-dhcpv6)# domain-name example.com`	DHCP クライアントにドメイン名オプションを提供します。
ステップ 7	**exit** 例： `Switch (config-dhcpv6)# exit`	前のモードに戻ります。
ステップ 8	**interface** vlan1 例： `Switch (config)# interface vlan 1`	インターフェイス モードを開始して、ステートフル DHCP を設定します。
ステップ 9	**description IPv6-DHCP-Stateful** 例： `Switch (config-if)# description IPv6-DHCP-Stateful`	ステートフル IPv6 DHCP の説明を入力します。
ステップ 10	**ipv6 address** 2001:DB8:0:20::1/64 例： `Switch (config-if)# ipv6 address 2001:DB8:0:20::1/64`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 11	**ip address** 192.168.20.1 255.255.255.0 例： `Switch (config-if)# ip address 192.168.20.1 255.255.255.0`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 12	**ipv6 nd prefix** 2001:db8::/64 **no-advertise** 例： `Switch (config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise`	アドバタイズしてはならない、IPv6 ルーティング プレフィックス アドバタイズメントを設定します。

	コマンドまたはアクション	目的
ステップ 13	**ipv6 nd managed-config-flag** 例： `Switch (config-if)# ipv6 nd managed-config-flag`	ホストでアドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 14	**ipv6 nd other-config-flag** 例： `Switch (config-if)# ipv6 nd other-config-flag`	ホストで非アドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 15	**ipv6 dhcp server** IPv6_DHCPPOOL 例： `Switch (config-if)# ipv6 dhcp server IPv6_DHCPPOOL`	インターフェイスにDHCPサーバを設定します。

関連トピック

SLAAC アドレス割り当て，（78 ページ）
ステートフル DHCPv6 アドレス割り当て，（80 ページ）

ステートフル DHCP の外部的設定（CLI）

このインターフェイス設定は、外部 DHCP サーバのステートフル DHCPv6 を実装している Cisco IOS IPv6 ルータ用です。

はじめる前に

手順の概要

1. **configure terminal**
2. **ipv6 unicast-routing**
3. **dns-server** 2001:100:0:1::1
4. **domain-name** example.com
5. **exit**
6. **interface** vlan1
7. **description IPv6-DHCP-Stateful**
8. **ipv6 address** 2001:DB8:0:20::1/64
9. **ip address** 192.168.20.1 255.255.255.0
10. **ipv6 nd prefix** 2001:db8::/64 **no-advertise**
11. **ipv6 nd managed-config-flag**
12. **ipv6 nd other-config-flag**
13. **ipv6 dhcp_relaydestination** 2001:DB8:0:20::2

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 unicast-routing** 例： `Switch(config)# ipv6 unicast-routing`	ユニキャスト用に IPv6 を設定します。
ステップ 3	**dns-server** 2001:100:0:1::1 例： `Switch (config-dhcpv6)# dns-server 2001:100:0:1::1`	DHCP クライアントに DNS サーバのオプションを提供します。
ステップ 4	**domain-name** example.com 例： `Switch (config-dhcpv6)# domain-name example.com`	DHCP クライアントにドメイン名オプションを提供します。
ステップ 5	**exit** 例： `Switch (config-dhcpv6)# exit`	前のモードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**interface** vlan1 例： `Switch (config)# interface vlan 1`	インターフェイス モードを開始して、ステートフル DHCP を設定します。
ステップ 7	**description IPv6-DHCP-Stateful** 例： `Switch (config-if)# description IPv6-DHCP-Stateful`	ステートフル IPv6 DHCP の説明を入力します。
ステップ 8	**ipv6 address** 2001:DB8:0:20::1/64 例： `Switch (config-if)# ipv6 address 2001:DB8:0:20::1/64`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 9	**ip address** 192.168.20.1 255.255.255.0 例： `Switch (config-if)# ip address 192.168.20.1 255.255.255.0`	ステートフル IPv6 DHCP の IPv6 アドレスを入力します。
ステップ 10	**ipv6 nd prefix** 2001:db8::/64 **no-advertise** 例： `Switch (config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise`	アドバタイズしてはならない、IPv6 ルーティング プレフィックス アドバタイズメントを設定します。
ステップ 11	**ipv6 nd managed-config-flag** 例： `Switch (config-if)# ipv6 nd managed-config-flag`	ホストでアドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 12	**ipv6 nd other-config-flag** 例： `Switch (config-if)# ipv6 nd other-config-flag`	ホストで非アドレス設定に DHCP を使用できるように、IPv6 インターフェイス ネイバー探索を設定します。
ステップ 13	**ipv6 dhcp_relaydestination** 2001:DB8:0:20::2 例： `Switch (config-if)# ipv6 dhcp_relay destination 2001:DB8:0:20::2`	インターフェイスにDHCPサーバを設定します。

関連トピック

SLAAC アドレス割り当て，（78 ページ）
ステートフル DHCPv6 アドレス割り当て，（80 ページ）

IPv6 クライアントのモニタリング（GUI）

Switchに関連づけられた IPv6 クライアントを表示する方法

はじめる前に

[Monitor] > [Clients] を選択します。
[Clients] ページが表示されます。 [Clients] ページには、次の詳細が含まれます。

- Client MAC Address：クライアントの MAC アドレスを表示します。
- AP Name：クライアントが接続されているアクセス ポイント名を表示します。
- WLAN：クライアントに関連付けられている WLAN を表示します。
- State：クライアント認証を表示します。
- Protocol：使用されるプロトコルを表示します。

クライアント関連の一般的な詳細を表示するには、[Clients] ページの **[Client MAC Address]** パラメータをクリックします。 **[Client > Detail]** ページの **[General]** タブの下にクライアントの IPv6 アドレスが表示されます。

IPv6 アドレス ラーニング設定の確認

次に、**show ipv6 dhcp pool** コマンドの出力例を示します。 このコマンドは、スイッチ上の IPv6 サービス設定を表示します。 vlan 21 の設定済みプールの詳細には、プールからアドレスを現在使用している 6 つのクライアントが表示されます。

手順の概要

1. **show ipv6 dhcp pool**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**show ipv6 dhcp pool**
	
	例：
	`Switchshow ipv6 dhcp pool`
	`DHCPv6 pool: vlan21`
	`Address allocation prefix: 2001:DB8:0:1:FFFF:1234::/64 valid`
		スイッチ上の IPv6 サービス設定を表示します。

	コマンドまたはアクション	目的

	`86400 preferred 86400 (6 in use, 0 conflicts)`
	`DNS server: 2001:100:0:1::1`
	`Domain name: example.com`
	`Active clients: 6`	

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	*IPv6 コマンド リファレンス (Catalyst 3650 スイッチ)*
IP コマンド リファレンス	*IP Command Reference (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

説明	リンク
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB のダウンロードには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングに役立てていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 クライアント アドレス ラーニングの機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 クライアント アドレス ラーニング機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 6 章

IPv6 WLAN セキュリティの設定

IPv6 WLAN セキュリティの前提条件

クライアント VLAN をスイッチで設定された WLAN にマッピングする必要があります。

IPv6 WLAN セキュリティの制限

RADIUS サーバのサポート

- 冗長性を保つために複数の RADIUS サーバが設定されている場合、バックアップが適切に機能するようにするには、すべてのサーバでユーザ データベースを同一にする必要があります。

Radius ACS サポート

- Cisco Secure Access Control Server（ACS）とスイッチの両方で、RADIUS を設定する必要があります。
- RADIUS は、Cisco Secure ACS バージョン 3.2 以降のリリースでサポートされます。

IPv6 WLAN セキュリティについて

RADIUS について

Remote Authentication Dial-In User Service（RADIUS）とは、ネットワークへの管理アクセス権を取得しようとするユーザに対して中央管理されたセキュリティ機能を提供する、クライアント/サーバプロトコルです。 これは、ローカルEAPに類似したバックエンドデータベースとして機能し、認証サービスおよびアカウンティング サービスを提供します。

- 認証：スイッチにログインしようとするユーザを検証するプロセス。

  スイッチで RADIUS サーバに対してユーザが認証されるようにするには、ユーザは有効なユーザ名とパスワードを入力する必要があります。 複数のデータベースを設定する場合は、バックエンド データベースを試行する順序を指定します。

- アカウンティング：ユーザによる処理と変更を記録するプロセス。

  ユーザによる処理が正常に実行される度に、RADIUSアカウンティング サーバでは、変更された属性、変更を行ったユーザのユーザ ID、ユーザがログインしたリモート ホスト、コマンドが実行された日付と時刻、ユーザの認可レベル、および実行された処理と入力された値の説明がログに記録されます。 RADIUSアカウンティング サーバが到達不能の場合、ユーザは中断なく、セッションを続行できます。

ユーザ データグラム プロトコル：RADIUS では、その転送にユーザ データグラム プロトコル（UDP）を使用します。 RADIUS では、1 つのデータベースが保持されます。そして、UDP ポート 1812 で受信認証要求がリッスンされ、UDP ポート 1813 で受信アカウンティング要求がリッスンされます。 アクセスコントロールを要求するスイッチは、クライアントとして動作し、サーバから AAA サービスを要求します。 スイッチとサーバ間のトラフィックは、プロトコルで定義されるアルゴリズムと、両方のデバイスにおいて設定される共有秘密キーによって暗号化されます。

複数の RADIUS アカウンティングおよび認証サーバを設定します。 たとえば、1 台の RADIUS 認証サーバを中央に配置し、複数の RADIUS アカウンティング サーバを異なる地域に配置できます。 同じタイプのサーバを複数設定すると、最初のサーバで障害が発生したり、接続不能になったりしても、コントローラは、必要に応じて 2 台目や 3 台目あるいはそれ以降のサーバへの接続を自動的に試行します。

RADIUS 方式が WLAN に対して設定されている場合、スイッチは WLAN に対して設定されている RADIUS 方式を使用します。 ローカル EAP を使用するように WLAN を設定すると、WLAN で設定されている RADIUS 方式はローカルをポイントします。 WLANには、使用するローカルEAPプロファイルの名前を設定する必要もあります。

RADIUS 方式が WLAN に対して設定されていない場合、スイッチはグローバル モードで定義されているデフォルトの RADIUS 方式を使用します。

ローカル EAP について

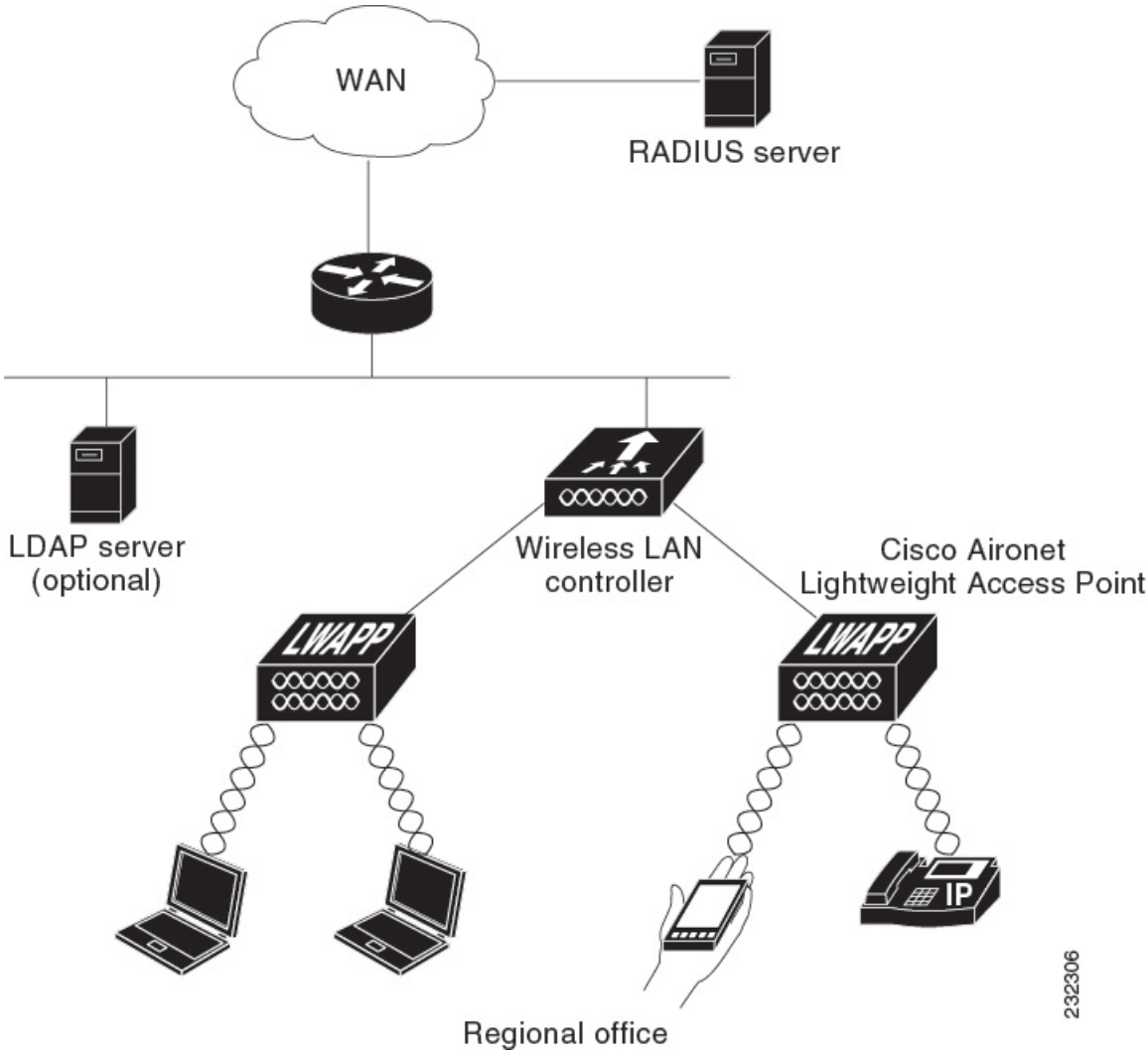
ローカルEAPは、ユーザおよびワイヤレスクライアントのローカル認証を可能にする認証方式です。 この方式は、バックエンドシステムが妨害されたり、外部認証サーバが停止した場合でも、ワイヤレスクライアントへの接続を維持できるように、リモートオフィスで使用する目的で設計

されています。 ローカルEAPを有効にすると、スイッチは認証サーバおよびローカルユーザデータベースとして機能するため、外部認証サーバに依存する必要がなくなります。 ローカル EAP は、ローカル ユーザ データベースまたは LDAP バックエンド データベースからユーザのクレデンシャルを取得して、ユーザを認証します。 ローカル EAP では、コントローラとワイヤレス クライアント間で、LEAP、EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC 認証方式をサポートします。

（注） LDAPバックエンドデータベースでは、ローカルEAP方式として、EAP-TLS、EAP-FAST/GTC、および PEAPv1/GTC がサポートされます。 LEAP、EAP-FAST/MSCHAPv2、および PEAPv0。 MSCHAPv2は平文のパスワードを返すようにLDAPサーバが設定されている場合にのみサポートされます。

（注） スイッチは、Microsoft Active Directory や Novell の eDirectory などの外部 LDAP データベースに対するローカルEAP認証をサポートしています。 Novellの eDirectoryに対するローカルEAP認証用にコントローラを設定する方法の詳細については、『Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database』ホワイトペーパーを参照してください。

図 *3*：ローカル *EAP* の例



関連トピック

ローカル ユーザの作成, （111 ページ）
クライアント VLAN とインターフェイスの作成, （112 ページ）
EAP プロファイルの設定, （113 ページ）
クライアント VLAN の作成, （127 ページ）
外部 RADIUS サーバを使用した 802.1x WLAN の作成, （128 ページ）

IPv6 WLAN セキュリティの設定方法

ローカル認証の設定

ローカル ユーザの作成

手順の概要

1. **configure terminal**
2. **username** aaa_test
3. **password 0** aaa_test
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**username** aaa_test 例： `Switch(config)# username aaa_test`	ユーザ名を作成します。
ステップ 3	**password 0** aaa_test 例： `Switch(config)# usernameaaa_test password 0 aaa_test`	ユーザ名のパスワードを割り当てます。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバルコンフィギュレーションモードを終了できます。

```
Switch# configure terminal
Switch(config)# username aaa_test password 0 aaa_test
Switch(config)# end
```

関連トピック

IPv6 WLAN セキュリティについて，（108 ページ）

クライアント VLAN とインターフェイスの作成

手順の概要

1. **configure terminal**
2. **vlan**
3. **exit**
4. **interface vlan** vlan_ID
5. **ip address**
6. **ipv6 address**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**vlan** 例： `Switch(config)# vlan 137`	VLAN を作成します。
ステップ 3	**exit** 例： `Switch (config-vlan)# exit`	VLAN コンフィギュレーション モードを終了します。
ステップ 4	**interface vlan** vlan_ID 例： `Switch (config)# interface vlan 137`	インターフェイスに VLAN を関連付けます。
ステップ 5	**ip address** 例： `Switch(config-if)# ip address 10.7.137.10 255.255.255.0`	VLAN インターフェイスに IP アドレスを割り当てます。
ステップ 6	**ipv6 address** 例： `Switch(config-if)#ipv6 address 2001:db8::20:1/64`	VLAN インターフェイスに IPv6 アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Switch# configure terminal
Switch(config)# vlan 137
Switch(config-vlan)#exit
Switch(config)#interface vlan 137
Switch(config-if)#ip address 10.7.137.10 255.255.255.0
Switch(config-if)#ipv6 address 2001:db8::20:1/64
Switch(config-if)#end
```

関連トピック

IPv6 WLAN セキュリティについて，（108 ページ）

EAP プロファイルの設定

手順の概要

1. **eap profile** name
2. **method leap**
3. **method tls**
4. **method peap**
5. **method mschapv2**
6. **method md5**
7. **method gtc**
8. **method fast profile** my-fast
9. **description** my_local**eap profile**
10. **exit**
11. **eap method fast profile**myFast
12. **authority-id** [identity|information]
13. **local-key 0** key-name
14. **pac-password 0** password
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**eap profile** name 例： `Switch(config)# eap profile wcm_eap_prof`	EAP プロファイルを作成します。
ステップ 2	**method leap** 例： `Switch(config-eap-profile)# method leap`	プロファイルで EAP-LEAP 方式を設定します。
ステップ 3	**method tls** 例： `Switch(config-eap-profile)# method tls`	プロファイルでEAP-TLS方式を設定します。
ステップ 4	**method peap** 例： `Switch(config-eap-profile)# method peap`	プロファイルで PEAP 方式を設定します。
ステップ 5	**method mschapv2** 例： `Switch(config-eap-profile)# method mschapv2`	プロファイルで EAP-MSCHAPV2 方式を設定します。
ステップ 6	**method md5** 例： `Switch(config-eap-profile)# method md5`	プロファイルでEAP-MD5方式を設定します。
ステップ 7	**method gtc** 例： `Switch(config-eap-profile)# method gtc`	プロファイルでEAP-GTC方式を設定します。

ステップ 8	**method fast profile** my-fast
	
	例：
	`Switch(config-eap-profile)# eap method fast profile my-fast`
	`Switch (config-eap-profile)#description my_local eap profile`
		my-fast というEAP プロファイルを作成します。

ステップ 9	**description** my_local**eap profile** 例： `Switch (config-eap-profile)#description my_local eap profile`	ローカルプロファイルの説明を指定します。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： `Switch (config-eap-profile)# exit`	eap 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。
ステップ 11	**eap method fast profile**myFast 例： `Switch (config)# eap method fast profile myFast`	EAP 方式プロファイルを設定します。

ステップ 12	**authority-id** [identity|information]
	
	例：
	`Switch(config-eap-method-profile)# authority-id identity my_identity`
	`Switch(config-eap-method-profile)#authority-id information my_information`
		EAP 方式プロファイルの認証局 ID および情報を設定します。

ステップ 13	**local-key 0** key-name 例： `Switch(config-eap-method-profile)# local-key 0 test`	ローカル サーバ キーを設定します。
ステップ 14	**pac-password 0** password 例： `Switch(config-eap-method-profile)# pac-password 0 test`	手動の PAC プロビジョニング用の PAC パスワードを設定します。
ステップ 15	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Switch(config)#eap profile wcm_eap_prof
Switch(config-eap-profile)#method leap
Switch(config-eap-profile)#method tls
Switch(config-eap-profile)#method peap
Switch(config-eap-profile)#method mschapv2
Switch(config-eap-profile)#method md5
Switch(config-eap-profile)#method gtc
Switch(config-eap-profile)#eap method fast profile my-fast
Switch (config-eap-profile)#description my_local eap profile
Switch(config-eap-profile)# exit
Switch (config)# eap method fast profile myFast
Switch(config-eap-method-profile)#authority-id identity my_identity
Switch(config-eap-method-profile)#authority-id information my_information
Switch(config-eap-method-profile)#local-key 0 test
Switch(config-eap-method-profile)#pac-password 0 test
Switch(config-eap-method-profile)# end
```

関連トピック

IPv6 WLAN セキュリティについて，（108 ページ）

ローカル認証モデルの作成

手順の概要

1. **aaa** new-model
2. **authentication dot1x default local**
3. **dot1x** method_list **local**
4. **aaa authentication dot1x** dot1x_name **local**
5. **aaa authorization credential-download** name **local**
6. **aaa local authentication** auth-name **authorization** authorization-name
7. セッション **ID**
8. **dot1x system-auth-control**

手順の詳細

	コマンドまたはアクション	目的
ステップ **1**	**aaa** new-model 例： `Switch(config)# aaa new-model`	AAA 認証モデルを作成します。
ステップ **2**	**authentication dot1x default local** 例： `Switch(config)# aaa authentication dot1x default local`	他の方法が見つからない場合、dot1x でデフォルトのローカル RADIUS を使用する必要があることを意味します。
ステップ **3**	**dot1x** method_list **local** 例： `Switch(config)# aaa authentication dot1x wcm_local local`	wcm_local 方式リスト用のローカル認証を割り当てます。
ステップ **4**	**aaa authentication dot1x** dot1x_name **local** 例： `Switch(config)# aaa authentication dot1x aaa_auth local`	dot1x 方式用のローカル認証を設定します。
ステップ **5**	**aaa authorization credential-download** name **local** 例： `Switch(config)# aaa authorization credential-download wcm_author local`	Local/RADIUS/LDAP から EAP クレデンシャルをダウンロードするようにローカル データベースを設定します。
ステップ **6**	**aaa local authentication** auth-name **authorization** authorization-name	ローカル認証および許可を選択します。

	コマンドまたはアクション	目的
	例： `Switch(config)# aaa local authentication wcm_local authorization wcm_author`	
ステップ 7	**セッション ID** 例： `Switch(config)# aaa session-id common`	AAA のセッション ID を設定します。
ステップ 8	**dot1x system-auth-control** 例： `Switch(config)# dot1x system-auth-control`	dot.1x システム認証制御をイネーブルにします。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default local
Switch(config)# aaa authentication dot1x wcm-local local
Switch(config)# aaa authentication dot1x aaa_auth local
Switch(config)# aaa authorization credential-download wcm_author local
Switch(config)# aaa local authentication wcm_local authorization wcm_author
Switch(config)# aaa session-id common
Switch(config)# dot1x system-auth-control
```

クライアント WLAN の作成

（注） この例では、ダイナミック WEP の 802.1x を使用しています。 ワイヤレス クライアントでサポートされ、スイッチで設定可能な他の任意のセキュリティ メカニズムも使用できます。

手順の概要

1. **configure terminal**
2. **wlan** wlan name **<identifier>** SSID
3. **broadcast-ssid**
4. **no security wpa**
5. **security dot1x**
6. **security** dot1x authentication-list *wcm-local*
7. **local-auth** wcm_eap_prof
8. **client vlan** *137*
9. **no shutdown**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**wlan** wlan name **<identifier>** SSID 例： `Switch(config)# wlan wlanProfileName 1 ngwcSSID`	WLAN を作成します。
ステップ 3	**broadcast-ssid** 例： `Switch(config-wlan)# broadcast-ssid`	WLAN で SSID をブロードキャストするように設定します。
ステップ 4	**no security wpa** 例： `Switch(config-wlan)# no security wpa`	WLAN の wpa をディセーブルにして、802.1x をイネーブルにします。
ステップ 5	**security dot1x** 例： `Switch(config-wlan)# security dot1x`	WLAN の 802.1x 暗号化セキュリティを設定します。
ステップ 6	**security** dot1x authentication-list *wcm-local* 例： `Switch(config-wlan)# security dot1x authentication-list wcm-local`	dot1x 認証用に WLAN へのサーバ グループ マッピングを設定します。
ステップ 7	**local-auth** wcm_eap_prof 例： `Switch (config-wlan)# local-auth wcm_eap_profile`	ローカル認証用に WLAN に eap プロファイルを設定します。
ステップ 8	**client vlan** *137* 例： `Switch(config-wlan)# client vlan 137`	WLAN に VLAN を関連付けます。
ステップ 9	**no shutdown** 例： `Switch(config-wlan)# no shutdown`	WLAN をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 10	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Switch# config terminal
Switch(config)#wlan wlanProfileName 1 ngwcSSID
Switch(config-wlan)#broadcast-ssid
Switch(config-wlan)#no security wpa
Switch(config-wlan)#security dot1x
Switch(config-wlan)#security dot1x authentication-list wcm-local
Switch (config-wlan)# local-auth wcm_eap_prof
Switch(config-wlan)#client vlan 137
Switch(config-wlan)#no shutdown
Switch(config-wlan)#end
Switch#
```

関連トピック

WPA2+AES 用クライアント VLAN の作成, （121 ページ）

WPA2+AES でのローカル認証の設定

手順の概要

1. **configure terminal**
2. **aaa** new model
3. **dot1x system-auth-control**
4. **aaa authentication dot1x default local**
5. **aaa local authorization credential-download default local**
6. **aaa local authentication default authorization default**
7. **eap profile** wcm_eap_profile
8. **method leap**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**aaa** new model 例： `Switch(config)# aaa new-model`	AAA 認証モデルを作成します。
ステップ 3	**dot1x system-auth-control** 例： `Switch(config)# dot1x system-auth-control`	dot1x システム認証制御をイネーブルにします。
ステップ 4	**aaa authentication dot1x default local** 例： `Switch(config)# aaa authentication dot1x default local`	デフォルト dot1x 方式用のローカル認証を設定します。
ステップ 5	**aaa local authorization credential-download default local** 例： `Switch(config)# aaa authorization credential-download default local`	ローカル サーバから EAP クレデンシャルをダウンロードするようにデフォルト データベースを設定します。
ステップ 6	**aaa local authentication default authorization default** 例： `Switch(config)# aaa local authentication default authorization default`	デフォルトのローカル認証および許可を選択します。
ステップ 7	**eap profile** wcm_eap_profile 例： `Switch(config)#eap profile wcm_eap_profile`	EAP プロファイルを作成します。
ステップ 8	**method leap** 例： `Switch(config)# method leap`	プロファイルで EAP-LEAP 方式を設定します。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# dot1x system-auth-control
Switch(config)# aaa authentication dot1x default local
Switch(config)# aaa authorization credential-download default local
Switch(config)# aaa local authentication default authorization default
Switch(config)#eap profile wcm_eap_profile
```

```
Switch(config)# method leap
Switch(config)# end
```

WPA2+AES 用クライアント VLAN の作成

ローカル認証の WPA2+AES タイプの VLAN を作成します。 この VLAN は、後で WLAN にマッピングされます。

手順の概要

1. **configure terminal**
2. **vlan** vlan_ID
3. **exit**
4. **interface** vlan vlan_ID
5. **ip address**
6. **ipv6 address**
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**vlan** vlan_ID 例： `Switch (config)# vlan 105`	VLAN を作成します。
ステップ 3	**exit** 例： `Switch (config-vlan)# exit`	VLAN モードを終了します。
ステップ 4	**interface** vlan vlan_ID 例： `Switch(config)# interface vlan 105`	インターフェイスに VLAN を関連付けます。
ステップ 5	**ip address** 例： `Switch(config-if)# ip address 10.8.105.10 255.255.255.0`	VLAN インターフェイスに IP アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 6	**ipv6 address** 例： `Switch(config-if)#ipv6 address 2001:db8::10:1/64`	VLAN インターフェイスに IPv6 アドレスを割り当てます。
ステップ 7	**exit** 例： `Switch (config-if)# exit`	インターフェイス モードを終了します。

```
Switch# configure terminal
Switch(config)# vlan105
Switch (config-vlan)# exit
Switch (config)# interface vlan 105
Switch(config-if)#ip address 10.8.105.10 255.255.255.0
Switch(config-if)#ipv6 address 2001:db8::10:1/64
Switch(config-if)#exit
Switch(config)#
```

関連トピック

クライアント WLAN の作成，（117 ページ）

WPA2+AES 用 WLAN の作成

WLAN を作成し、WPA2+AES 用に作成されたクライアント VLAN にマッピングします。

手順の概要

1. **configure terminal**
2. **wlan** wpas2-aes-wlan 1 wpas2-aes-wlan
3. **client vlan** 105
4. **local-auth** wcm_eap_profile
5. **security dot1x authentication-list default**
6. **no shutdown**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**wlan** wpas2-aes-wlan 1 wpas2-aes-wlan
	
	例：
	`Switch(config)#wlan wpa2-aes-wlan 1 wpa2-aes-wlan`
	`Switch(config-wlan)#`
		WLAN を作成します。

ステップ 3	**client vlan** 105
	
	例：
	`Switch(config-wlan)#client vlan 105`
	`Switch(config-wlan)#`
		クライアント VLAN に WLAN をマッピングします。

ステップ 4	**local-auth** wcm_eap_profile 例： `Switch(config-wlan)#local-auth wcm_eap_profile`	WLAN に EAP プロファイルを作成し、設定します。
ステップ 5	**security dot1x authentication-list default** 例： `Switch(config-wlan)#security dot1x authentication-list default`	デフォルトの dot1x 認証リストを使用します。

ステップ 6	**no shutdown**
	
	例：
	`Switch(config-wlan)#no shutdown`
	`Switch(config-wlan)#`
		WLAN をイネーブルにします。

ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバルコンフィギュレーション モードを終了できます。

```
Switch# configure terminal
Switch(config)#wlan wpa2-aes-wlan 1 wpa2-aes-wlan
Switch(config-wlan)#client vlan 105
Switch(config-wlan)#local-auth wcm_eap_profile
Switch(config-wlan)#security dot1x authentication-list default
Switch(config-wlan)#no shutdown
Switch(config-wlan)# exit
```

外部 RADIUS サーバの設定

RADIUS 認証サーバ ホストの設定

手順の概要

1. **configure terminal**
2. **radius server One**
3. **address ipv4** address **auth-port**auth_port_number **acct-port** acct_port_number
4. **address ipv6** address **auth-port**auth_port_number **acct-port** acct_port_number
5. **key** 0cisco
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**radius server One** 例： `Switch (config)# radius server One`	RADIUS サーバを作成します。
ステップ 3	**address ipv4** address **auth-port**auth_port_number **acct-port** acct_port_number 例： `Switch (config-radius-server)# address ipv4 10.10.10.10 auth-port 1812 acct-port 1813`	RADIUS サーバの IPv4 アドレスを設定します。
ステップ 4	**address ipv6** address **auth-port**auth_port_number **acct-port** acct_port_number 例： `Switch (config-radius-server)# address ipv6 2001:db8::25:2 auth-port 1812 acct-port 1813`	RADIUS サーバの IPv6 アドレスを設定します。
ステップ 5	**key** 0cisco 例： `Switch (config-radius-server)# key 0 cisco`	**exit**

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Switch (config-radius-server)# exit`	RADIUS サーバ モードを終了します。

```
Switch# configure terminal
Switch (config)# radius server One
Switch (config-radius-server)# address ipv4 10.10.10.10 auth-port 1812 acct-port 1813
Switch (config-radius-server)# address ipv6 2001:db8::25:2 auth-port 1812 acct-port 1813
Switch (config-radius-server)# key 0 cisco
Switch (config-radius-server)#exit
```

関連トピック

RADIUS 認証サーバ グループの設定，（125 ページ）

RADIUS 認証サーバ グループの設定

手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **aaa group server radius** wcm_rad
4. **server** <ip address>**auth-port**1812**acct-port**1813
5. **aaa authentication dot1x** method_list **group** wcm_rad
6. **dot1x system-auth-control**
7. **aaa session-idcommon**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**aaa new-model** 例： `Switch(config)#aaa new-model`	AAA 認証モデルを作成します。

	コマンドまたはアクション	目的

ステップ 3	**aaa group server radius** wcm_rad
	
	例：
	`Switch(config)# aaa group server radius wcm_rad`
	`Switch(config-sg-radius)#`
		RADIUS サーバ グループを作成します。

ステップ 4	**server** <ip address>**auth-port**1812**acct-port**1813
	
	例：
	`Switch(config-sg-radius)# server One auth-port 1812 acct-port 1813`
	`Switch(config-sg-radius)# server Two auth-port 1812 acct-port 1813`
	`Switch(config-sg-radius)# server Three auth-port 1812 acct-port 1813`
		手順 3 で作成した RADIUS グループにサーバを追加します。 RADIUS アカウンティング サーバおよび認証サーバの UDP ポートを設定します。

ステップ 5	**aaa authentication dot1x** method_list **group** wcm_rad 例： `Switch(config)# aaa authentication dot1x method_list group wcm_rad`	RADIUS グループに方式リストをマッピングします。
ステップ 6	**dot1x system-auth-control** 例： `Switch(config)# dot1x system-auth-control`	RADIUS グループのシステム認証制御をイネーブルにします。
ステップ 7	**aaa session-idcommon** 例： `Switch(config)# aaa session-id common`	RADIUS グループから、特定のコールに対して送信されるすべてのセッション ID 情報が同じであることを確認します。

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa group server radius wcm_rad
Switch(config-sg-radius)# server One auth-port 1812 acct-port 1813
Switch(config-sg-radius)# server Two auth-port 1812 acct-port 1813
Switch(config-sg-radius)# server Three auth-port 1812 acct-port 1813
Switch(config)# aaa authentication dot1x method_list group wcm_rad
Switch(config)# dot1x system-auth-control
Switch(config)# aaa session-id common
Switch(config)#
```

関連トピック

RADIUS 認証サーバ ホストの設定，（124 ページ）

クライアント VLAN の作成

手順の概要

1. **configure terminal**
2. **vlan** 137
3. **exit**
4. **interface vlan** 137
5. **ip address** 10.7.137.10 255.255.255.0
6. **ipv6 address** 2001:db8::30:1/64
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。
ステップ 2	**vlan** 137 例： `Switch(config)# vlan 137`	VLAN を作成してインターフェイスに関連付けます。
ステップ 3	**exit** 例： `Switch (config-vlan)# exit`	VLAN モードを終了します。
ステップ 4	**interface vlan** 137 例： `Switch (config)# interface vlan 137`	インターフェイスに VLAN を割り当てます。
ステップ 5	**ip address** 10.7.137.10 255.255.255.0 例： `Switch(config-if)# ip address 10.7.137.10 255.255.255.0`	VLAN インターフェイスに IPv4 アドレスを割り当てます。
ステップ 6	**ipv6 address** 2001:db8::30:1/64 例： `Switch(config-if)# ipv6 address 2001:db8::30:1/64`	VLAN インターフェイスに IPv6 アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Switch# configure terminal
Switch(config)# vlan137
Switch(config-vlan)# exit
Switch(config)# interface vlan137
Switch(config-if)# ip address 10.7.137.10 255.255.255.0
Switch(config-if)# ipv6 address 2001:db8::30:1/64
Switch(config-if)# end
```

関連トピック

IPv6 WLAN セキュリティについて, （108 ページ）
外部 RADIUS サーバを使用した 802.1x WLAN の作成, （128 ページ）

外部 RADIUS サーバを使用した 802.1x WLAN の作成

手順の概要

1. **configure terminal**
2. **wlan** ngwc-1x**<ssid>**ngwc-1x
3. **broadcast-ssid**
4. **no security wpa**
5. **security dot1x**
6. **security dot1x authentication-list** wcm-rad
7. **client vlan** 137
8. **no shutdown**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**wlan** ngwc-1x**<ssid>**ngwc-1x 例： `Switch(config)# wlan ngwc_8021x 2 ngwc_8021x`	802.1x 認証用の新しい WLAN を作成します。
ステップ 3	**broadcast-ssid** 例： `Switch(config-wlan)# broadcast-ssid`	WLAN で SSID をブロードキャストするように設定します。
ステップ 4	**no security wpa** 例： `Switch(config-wlan)# no security wpa`	WLAN の WPA をディセーブルにして、802.1x をイネーブルにします。
ステップ 5	**security dot1x** 例： `Switch(config-wlan)# security dot1x`	WLAN の 802.1x 暗号化セキュリティを設定します。
ステップ 6	**security dot1x authentication-list** wcm-rad 例： `Switch(config-wlan)# security dot1x authentication-list wcm-rad`	dot1x 認証用に WLAN へのサーバ グループ マッピングを設定します。
ステップ 7	**client vlan** 137 例： `Switch(config-wlan)# client vlan 137`	WLAN に VLAN を関連付けます。
ステップ 8	**no shutdown** 例： `Switch(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Switch# configure terminal
Switch(config)#wlan ngwc_8021x 2 ngwc_8021x
Switch(config-wlan)# broadcast-ssid
Switch(config-wlan)# no security wpa
Switch(config-wlan)# security dot1x
Switch(config-wlan)# security dot1x authentication-list wcm-rad
Switch(config-wlan)# client vlan 137
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

関連トピック

クライアント VLAN の作成，（127 ページ）
IPv6 WLAN セキュリティについて，（108 ページ）

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	*IPv6 コマンド リファレンス (Catalyst 3650 スイッチ)*
WLAN コマンド リファレンス	*WLAN コマンド リファレンス、Cisco IOS XE Release 3SE（Catalyst 3650 スイッチ）*
WLAN の設定	*WLAN コンフィギュレーション ガイド、Cisco IOS XE Release 3SE（Catalyst 3650 スイッチ）*

エラー メッセージ デコーダ

説明	リンク
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB のダウンロードには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングに役立てていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 WLAN セキュリティの機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 WLAN セキュリティ機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 7 章

IPv6 ACL の設定

IPv6 ACL の前提条件

IP Version 6（IPv6）アクセス コントロール リスト（ACL）を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP Version 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。 また、スイッチで IP ベース フィーチャ セットが稼働している場合、入力ルータ ACL を作成しそれを適用してレイヤ 3 管理トラフィックをフィルタリングすることもできます。

関連トピック

IPv6 ACL の作成，（138 ページ）

IPv6 ACL の制限

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。 IPv6 がサポートするのは名前付き ACL だけです。

スイッチは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- スイッチは、**flowlabel**、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- スイッチは再帰 ACL（**reflect** キーワード）をサポートしません。
- スイッチは IPv6 フレームに MAC ベース ACL を適用しません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。 ハードウェア転送が必要なインターフェイス（物理ポートまたはSVI）にACLを適用する場合、スイッチはインターフェイスで ACL がサポートされるかどうかを判別します。 サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロールエントリ（ACE）を追加しようとする場合、スイッチは現在インターフェイスに適用されている ACL に ACE が追加されることを許可しません。

IPv6 ACL について

アクセスコントロールリスト（ACL）は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです（たとえば、無線クライアントからコントローラの管理インターフェイスにpingが実行されるのを制限する場合などに使用されます）。スイッチで設定したACLは、管理インターフェイス、AP マネージャ インターフェイス、任意の動的インターフェイス、またはワイヤレス クライアントとやり取りするデータ トラフィックの制御用の WLAN、あるいは中央処理装置（CPU）宛のすべてのトラフィックの制御用のコントローラ CPU に適用できます。

Web 認証用に事前認証 ACL を作成することもできます。 このような ACL は、認証が完了するまでに特定のタイプのトラフィックを許可するために使用されます。

IPv6 ACL は、送信元、宛先、送信元ポート、宛先ポートなど、IPv4 ACL と同じオプションをサポートします。

（注） ネットワーク内で IPv4 トラフィックだけを有効にするには、IPv6 トラフィックをブロックします。 つまり、すべての IPv6 トラフィックを拒否するように IPv6 ACL を設定し、これを特定またはすべての WLAN 上で適用します。

IPv6 ACL の概要

スイッチは、次の 2 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL は、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できるレイヤ 3 インターフェイスのアウトバウンド トラフィッ

クまたはインバウンド トラフィックでサポートされます。 IPv6 ルータ ACL は、ルーティングされる IPv6 パケットに対してだけ適用されます。

- IPv6 ポート ACL は、レイヤ 2 インターフェイスのインバウンド トラフィックでだけサポートされます。 IPv6 ポート ACL は、インターフェイスに着信するすべての IPv6 パケットに対して適用されます。

IP ベース フィーチャ セットが稼働しているスイッチは、入力ルータ IPv6 ACL だけをサポートします。 ポート ACL または出力ルータ IPv6 ACL はサポートされません。

（注） サポートされない IPv6 ACL を設定した場合、エラー メッセージが表示され、その設定は有効になりません。

スイッチは、IPv6 トラフィックの Virtual LAN（VLAN）ACL（VLAN マップ）をサポートしません。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。 IPv4 ACL の場合と同様に、IPv6 ポート ACL はルータ ACL よりも優先されます。

- SVI に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに着信したパケットはポート ACL によってフィルタリングされます。 その他のポートに着信したルーテッド IP パケットは、ルータ ACL によってフィルタリングされます。 他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに

  着信したパケットはポート ACL によってフィルタリングされます。 発信ルーテッド IPv6 パケットは、ルータ ACL によってフィルタリングされます。 他のパケットはフィルタリングされません。

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

関連トピック

IPv6 ACL の作成, （138 ページ）
インターフェイスへの IPv6 の適用, （143 ページ）
WLAN IPv6 ACL の作成, （144 ページ）
IPv6 ACL の表示, （145 ページ）

ACL のタイプ

ユーザあたりの IPv6 ACL

ユーザあたりの ACL の場合、テキスト文字列として、完全アクセス制御エントリ（ACE）が ACS で設定されます。

ACE はコントローラで設定されません。 ACE は `Access-Accept` 属性でスイッチに送信され、クライアント用に直接適用されます。 ワイヤレスクライアントが外部スイッチにローミングするときに、ACE が、AAA 属性としてモビリティ ハンドオフ メッセージで外部スイッチに送信されます。

フィルタ ID IPv6 ACL

filter-Id ACL の場合、完全な ACE および `acl name(filter-id)` がスイッチで設定され、`filter-id` のみが ACS で設定されます。 `filter-id` は Access-Accept 属性でスイッチに送信され、スイッチは ACE の filter-id をルックアップしてから、クライアントに ACE を適用します。 クライアント L2 が外部スイッチにローミングするときに、filter-id だけがモビリティ ハンドオフ メッセージで外部スイッチに送信されます。 外部スイッチは filter-id と ACE を事前に設定する必要があります。

ダウンロード可能 IPv6 ACL

ダウンロード可能 ACL（dACL）の場合、完全な ACE および `dacl` 名はすべて ACS だけで設定されます。

（注） コントローラは ACL を設定しません。

ACS は `dacl` 名をスイッチに対しその `ACCESS-Accept` 属性で送信します。さらに `dacl` 名を使用して、ACE のために `dACL` 名が ACS に、`access-request` 属性によって戻されます。

ACS は `access-accept` 属性でスイッチの対応する ACE に応答します。 ワイヤレス クライアントが外部スイッチにローミングするときに、`dacl` 名だけがモビリティ ハンドオフ メッセージで外部スイッチに送信されます。 外部スイッチは、`dacl` 名の ACS サーバにアクセスして ACE を取得します。

IPv6 ACL とスイッチ スタック

スタック マスターは IPv6 ACL をハードウェアでサポートし、IPv6 ACL をスタック メンバーに配信します。

（注） スイッチ スタック内で IPv6 を完全に機能させるには、すべてのスタック メンバーで拡張 IP サービス フィーチャ セットが稼働している必要があります。

新しいスイッチがスタック マスターを引き継ぐと、ACL 設定がすべてのスタック メンバーに配信されます。 メンバ スイッチは、新しいスタック マスターによって配信された設定との同期をとり、不要なエントリを一掃します。

ACL の修正、インターフェイスへの適用、またはインターフェイスからの解除が行われると、スタック マスターは変更内容をすべてのスタック メンバーに配信します。

IPv6 ACL の設定

IPv6 トラフィックをフィルタリングする場合は、次の手順を実行します

はじめる前に

IPv6 ACL を設定する場合は、事前にデュアル IPv4 および IPv6 SDM テンプレートのいずれかを選択する必要があります。

手順の概要

1. IPv6 ACL を作成し、IPv6 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。
2. IPv6 ACL が、トラフィックをブロックする（拒否）または通過させる（許可）よう設定します。
3. トラフィックをフィルタリングする必要があるインターフェイスに IPv6 ACL を適用します。
4. インターフェイスに IPv6 ACL を適用します。 ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	IPv6 ACL を作成し、IPv6 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。	
ステップ 2	IPv6 ACL が、トラフィックをブロックする（拒否）または通過させる（許可）よう設定します。	
ステップ 3	トラフィックをフィルタリングする必要があるインターフェイスに IPv6 ACL を適用します。	
ステップ 4	インターフェイスに IPv6 ACL を適用します。 ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。	

IPv6 ACL のデフォルト設定

デフォルトでは、IPv6 ACL は設定または適用されていません。

他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージプロトコル（ICMP）キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチ スタックに作成したり、同一インターフェイスに適用できます。 各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

  IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（たとえば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラー メッセージが表示されます。

- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。 MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェア メモリが満杯の場合、設定済みの ACL を追加すると、パケットは CPU に転送され、ACL はソフトウェアで適用されます。ハードウェアが一杯になると、ACL がアンロードされたことを示すメッセージがコンソールに出力され、パケットはインターフェイスでドロップされます。

（注） 追加できなかった ACL と同じタイプのパケットのみ（ipv4、ipv6、MAC）がインターフェイスでドロップされます。

IPv6 ACL の設定方法

IPv6 ACL の作成

IPv6 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **ipv6 access-list** *acl_name*
3. **{deny|permit} protocol**
4. **{deny|permit} tcp**
5. **{deny|permit} udp**
6. **{deny|permit} icmp**
7. **end**
8. **show ipv6 access-list**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 access-list** *acl_name* 例： `ipv6 access-list access-list-name`	名前を使用して IPv6 アクセス リストを定義し、IPv6 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。
ステップ 3	**{deny|permit} protocol** 例： `{deny | permit} protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |host destination-ipv6-address} [operator [port-number]][dscp value] [fragments][log] [log-input] [routing][sequence value] [time-range name]`	条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。 次に、条件について説明します。 • protocol には、インターネット プロトコルの名前または番号を入力します。ahp、esp、icmp、ipv6、pcp、stcp、tcp、udp、または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。 • source-ipv6-prefix/prefix-length または destination-ipv6-prefix/ prefix-length は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。 • IPv6 プレフィックス ::/0 の短縮形として、any を入力します。 • host source-ipv6-address または destination-ipv6-address には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホスト

	コマンドまたはアクション	目的
		アドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 • （任意）operator には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。 オペランドには、lt（より小さい）、gt（より大きい）、eq（等しい）、neq（等しくない）、range（包含範囲）があります。 source-ipv6-prefix/prefix-length 引数のあとの operator は、送信元ポートに一致する必要があります。destination-ipv6- prefix/prefix-length 引数のあとの operator は、宛先ポートに一致する必要があります。 • （任意）port-number は、0 ～ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。 TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。 UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。 • （任意）dscp value を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コード ポイント値を照合します。 指定できる範囲は 0 ～ 63 です。 • （任意）fragments を入力して、先頭ではないフラグメントを確認します。 このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。 • （任意）log を指定すると、エントリと一致するパケットに関するログ メッセージがコンソールに送信されます。 log-input を指定すると、ログ エントリに入力インターフェイスが追加されます。 ロギングはルータ ACL でだけサポートされます。 • （任意）routing を入力して、IPv6 パケットのルーティングを指定します。 • （任意）sequence value を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。 指定できる範囲は 1 ～ 4294967295 です。

	コマンドまたはアクション	目的
		• （任意）time-range name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。
ステップ 4	**{deny|permit} tcp** 例： `{deny | permit} tcp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |hostdestination-ipv6-address} [operator [port-number]][ack] [dscp value][established] [fin] [log][log-input] [neq {port |protocol}] [psh] [range{port | protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]`	（任意）TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は tcp を入力します。 パラメータはステップ 3 で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。 • ack：確認応答（ACK）ビット セット • established：確立された接続。 TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • fin：終了ビット セット。送信元からのデータはそれ以上ありません。 • neq {port | protocol}：所定のポート番号上にないパケットだけを照合します。 • psh：プッシュ機能ビット セット • range {port | protocol}：ポート番号の範囲内のパケットだけを照合します。 • rst：リセット ビット セット • syn：同期ビット セット • urg：緊急ポインタ ビット セット

ステップ 5	**{deny|permit} udp**
	
	例：
	`{deny | permit} udp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][dscp value] [log][log-input]`
	
	`[neq {port |protocol}] [range {port |protocol}] [routing][sequence value][time-range name]`
		（任意）UDP アクセス リストおよびアクセス条件を定義します。
		
		ユーザ データグラム プロトコルの場合は、udp を入力します。 UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator [port]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。UDP の場合、established パラメータは無効です。

ステップ 6	**{deny|permit} icmp** 例： `{deny | permit} icmp {source-ipv6-prefix/prefix-length | any |`	（任意）ICMP アクセス リストおよびアクセス条件を定義します。 インターネット制御メッセージプロトコルの場合は、icmp を入力します。 ICMP パラメータはステップ 3a

	コマンドまたはアクション	目的

	`hostsource-ipv6-address}`
	`[operator [port-number]]`
	`{destination-ipv6-prefix/prefix-length | any |`
	`hostdestination-ipv6-address}`
	`[operator [port-number]][icmp-type [icmp-code]`
	`|icmp-message] [dscpvalue] [log] [log-input]`
	`[routing] [sequence value][time-range name]`
		の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。 オプションのキーワードの意味は次のとおりです。
		• icmp-type：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。
		• icmp-code：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0～255 です。
		• icmp-message：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージ タイプとコード名でフィルタリングする場合に入力します。 ICMP メッセージのタイプ名およびコード名のリストについては、?キーを使用するか、またはこのリリースのコマンド リファレンスを参照してください。

ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**show ipv6 access-list** 例： `show ipv6 access-list`	アクセス リストの設定を確認します。
ステップ 9	**copy running-config startup-config** 例： `copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IPv6 ACL の前提条件, （133 ページ）
IPv6 ACL の概要, （134 ページ）
インターフェイスへの IPv6 の適用, （143 ページ）
WLAN IPv6 ACL の作成, （144 ページ）
IPv6 ACL の表示, （145 ページ）

インターフェイスへの IPv6 の適用

ここでは、ネットワーク インターフェイスに IPv6 ACL を適用する手順について説明します。 レイヤ 2 およびレイヤ 3 インターフェイスの発信または着信トラフィックに IPv6 ACL を適用できます。 IPv6 ACL はレイヤ 3 インターフェイスの着信管理トラフィックにだけ適用できます。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface** interface_id
3. **no switchport**
4. **ipv6 address** *ipv6_address*
5. **ipv6 traffic-filter** *acl_name*
6. **end**
7. **show running-config interface tenGigabitEthernet 1/0/3**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** interface_id 例： `Switch# interface interface-id`	アクセス リストを適用するレイヤ 2 インターフェイス（ポート ACL 用）またはレイヤ 3 スイッチ仮想インターフェイス（ルータ ACL 用）を特定して、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。
ステップ 3	**no switchport** 例： `Switch# no switchport`	レイヤ 2 モード（デフォルト）からレイヤ 3 モードにインターフェイスを変更します（ルータ ACL を適用する場合のみ）。
ステップ 4	**ipv6 address** *ipv6_address* 例： `Switch# ipv6 address ipv6-address`	レイヤ 3 インターフェイス（ルータ ACL 用）で IPv6 アドレスを設定します。 （注） このコマンドは、レイヤ 2 インターフェイスでは、またはインターフェイスに明示的な IPv6 アドレスが設定されている場合には、必要ありません。

	コマンドまたはアクション	目的
ステップ 5	**ipv6 traffic-filter** *acl_name* 例： `Switch# ipv6 traffic-filter access-list-name {in | out}`	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ステップ 7	**show running-config interface tenGigabitEthernet 1/0/3**
	
	例：
	`Switch# show running-config interface tenGigabitEthernet 1/0/3`
	`.....`
	`.....`
	`Building configuration .....`
	`.....`
	`Current configuration : 98 bytes`
	`!`
	`interface TenGigabitEthernet1/0/3`
	` switchport mode trunk`
	` ipv6 traffic-filter MyFilter out`
	`end`
		設定の概要を示します。

ステップ 8	**copy running-config startup-config** 例： `copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

関連トピック

IPv6 ACL の作成, （138 ページ）
IPv6 ACL の概要, （134 ページ）
WLAN IPv6 ACL の作成, （144 ページ）
IPv6 ACL の表示, （145 ページ）

WLAN IPv6 ACL の作成

手順の概要

1. **ipv6 traffic-filter acl** *acl_name*
2. **ipv6 traffic-filter acl web**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ipv6 traffic-filter acl** *acl_name* 例： `Switch(config-wlan)# ipv6 traffic-filter acl <acl_name>`	名前付き WLAN ACL を作成します。
ステップ 2	**ipv6 traffic-filter acl web** 例： `Switch(config-wlan)# ipv6 traffic-filter acl web <acl_name-preauth>`	WLAN ACL の事前認証を作成します。

```
Switch(config-wlan)# ipv6 traffic-filter acl <acl_name>
Switch(config-wlan)#ipv6 traffic-filter acl web <acl_name-preauth>
```

関連トピック

IPv6 ACL の作成，（138 ページ）
インターフェイスへの IPv6 の適用，（143 ページ）
IPv6 ACL の概要，（134 ページ）
IPv6 ACL の表示，（145 ページ）

IPv6 ACL の確認

IPv6 ACL の表示

1 つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示できます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show access-list** 例： `Switch# show access-lists`	スイッチに設定されたすべてのアクセスリストを表示します。

	コマンドまたはアクション	目的
ステップ 2	**show ipv6 access-list** *acl_name* 例： `Switch# show ipv6 access-list [access-list-name]`	設定済みのすべての IPv6 アクセス リストまたは名前付けされたアクセス リストを表示します。

関連トピック

IPv6 ACL の作成，（138 ページ）
インターフェイスへの IPv6 の適用，（143 ページ）
WLAN IPv6 ACL の作成，（144 ページ）
IPv6 ACL の概要，（134 ページ）

IPv6 ACL の設定例

例：IPv6 ACL の作成

次に、CISCO と名前が付けられた IPv6 アクセス リストを設定する例を示します。 リスト内の最初の拒否エントリは、宛先 TCP ポート番号が 5000 より大きいパケットをすべて拒否します。 2 番めの拒否エントリは、送信元 UDP ポート番号が 5000 未満のパケットを拒否します。 また、この 2 番めの拒否エントリは、すべての一致をコンソールに表示します。 リスト内の最初の許可エントリは、すべての ICMP パケットを許可します。 リスト内の 2 番めの許可エントリは、その他のすべてのトラフィックを許可します。 暗黙の全否定の条件が各 IPv6 アクセス リストの末尾にあるため、2 番めの許可エントリは必要です。

（注） ロギングは、レイヤ 3 インターフェイスでのみサポートされます。

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
```

例：IPv6 ACL の適用

次に、レイヤ 3 インターフェイスの発信トラフィックに対して、アクセス リスト Cisco を適用する例を示します。

```
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

例：IPv6 ACL の表示

次に、**show access-lists** 特権 EXEC コマンドの出力例を示します。 出力には、スイッチまたはスイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
Switch #show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

次に、show ipv6 access-lists 特権 EXEC コマンドの出力例を示します。 出力には、スイッチまたはスイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
Switch# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30

IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```

例：RA スロットリングと NS 抑制の設定

このタスクでは、省電力のワイヤレス クライアントが頻繁な非請求の定期的 RA に影響されないように、RA スロットルポリシーを作成する方法について説明します。 非請求タイプのマルチキャスト RA は、コントローラによってスロットルされます。

はじめる前に

クライアント マシンで IPv6 をイネーブルにします。

手順の概要

1. **configure terminal**
2. **ipv6 nd ra-throttler policy** Mythrottle
3. **throttle-period** 20
4. **max-through** 5
5. **allow at-least** 3 **at-most** 5
6. **switch (config)# vlan configuration 100**
7. **ipv6 nd suppress**
8. **ipv6 nd ra-th attach-policy** attach-policy_name
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 nd ra-throttler policy** Mythrottle 例： `Switch (config)# ipv6 nd ra-throttler policy Mythrottle`	Mythrottle という RA スロットラ ポリシーを作成します。
ステップ 3	**throttle-period** 20 例： `Switch (config-nd-ra-throttle)# throttle-period 20`	スロットリングを適用する時間間隔セグメントを特定します。
ステップ 4	**max-through** 5 例： `Switch (config-nd-ra-throttle)# max-through 5`	許容する初期 RA の数を特定します。
ステップ 5	**allow at-least** 3 **at-most** 5 例： `Switch (config-nd-ra-throttle)# allow at-least 3 at-most 5`	初期 RA が送信された後に、間隔セグメントの終了まで許容される RA の数を特定します。
ステップ 6	**switch (config)# vlan configuration 100** 例： `Switch (config)# vlan configuration 100`	VLAN あたりの設定を作成します。
ステップ 7	**ipv6 nd suppress** 例： `Switch (config)# ipv6 nd suppress`	VLAN でネイバー探索をディセーブルにします。
ステップ 8	**ipv6 nd ra-th attach-policy** attach-policy_name 例： `Switch (config)# ipv6 nd ra-throttle attach-policy attach-policy_name`	ルータ アドバタイズメント スロットリングをイネーブルにします。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例：RA ガード ポリシーの設定

手順の概要

1. **ipv6 nd raguard policy** MyPloicy
2. **trusted-port**
3. **device-role router**
4. **interface tenGigabitEthernet** 1/0/1
5. **ipv6 nd raguard attach-policy**MyPolicy
6. **vlan configuration** 19-21,23
7. **ipv6 nd suppress**
8. **ipv6 snooping**
9. **ipv6 nd raguard attach-policy** MyPolicy
10. **ipv6 nd ra-throttler attach-policy** Mythrottle

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ipv6 nd raguard policy** MyPloicy 例： `Switch (config)# ipv6 nd raguard policy MyPolicy`	
ステップ 2	**trusted-port** 例： `Switch (config-nd-raguard)# trusted-port`	上記で作成したポリシーの信頼できるポートを設定します。

ステップ 3	**device-role router**
	
	例：
	`Switch (config-nd-raguard)# device-role [host|monitor|router|switch]`
	`Switch (config-nd-raguard)# device-role router`
		上記で作成した信頼できるポートに RA を送信可能な信頼できるデバイスを定義します。

ステップ 4	**interface tenGigabitEthernet** 1/0/1 例： `Switch (config)# interface tenGigabitEthernet 1/0/1`	信頼できるデバイスにインターフェイスを設定します。
ステップ 5	**ipv6 nd raguard attach-policy**MyPolicy 例： `Switch (config-if)# ipv6 nd raguard attach-policy Mypolicy`	ポートから受信した RA を信頼するようにポリシーを設定し、接続します。

	コマンドまたはアクション	目的
ステップ 6	**vlan configuration** 19-21,23 例： `Switch (config)# vlan configuration 19-21,23`	ワイヤレス クライアントの VLAN を設定します。
ステップ 7	**ipv6 nd suppress** 例： `Switch (config-vlan-config)# ipv6 nd suppress`	無線上で ND メッセージを抑制します。
ステップ 8	**ipv6 snooping** 例： `Switch (config-vlan-config)# ipv6 snooping`	IPv6 トラフィックをキャプチャします。
ステップ 9	**ipv6 nd raguard attach-policy** MyPolicy 例： `Switch (config-vlan-config)# ipv6 nd raguard attach-policy Mypolicy`	ワイヤレス クライアントの VLAN に RA ガード ポリシーを接続します。
ステップ 10	**ipv6 nd ra-throttler attach-policy** Mythrottle 例： `Switch (config-vlan-config)#ipv6 nd ra-throttler attach-policy Mythrottle`	ワイヤレス クライアントの VLAN に RA スロットリング ポリシーを接続します。

例：IPv6 ネイバー バインディングの設定

手順の概要

1. **ipv6 neighbor binding** [vlan]19 2001:db8::25:4 **interface tenGigabitEthernet** 1/0/3 aaa.bbb.ccc

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ipv6 neighbor binding** [vlan]19 2001:db8::25:4 **interface tenGigabitEthernet** 1/0/3 aaa.bbb.ccc 例： `Switch (config)# ipv6 neighbor binding vlan 19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc`	送信元 MAC アドレスとして aaa.bbb.ccc が設定されたインターフェイス te1/0/3 を介して VLAN 19 で送信する場合にのみ有効なネイバー 2001:db8::25: 4 を設定して検証します。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	*IPv6 コマンド リファレンス (Catalyst 3650 スイッチ)*
ACL 設定	セキュリティ コンフィギュレーション ガイド *(Catalyst 3650 スイッチ)*

エラー メッセージ デコーダ

説明	リンク
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB のダウンロードには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングに役立てていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 ACL の機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 ACL 機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 8 章

IPv6 Web 認証の設定

IPv6 Web 認証の前提条件

次の設定を、IPv6 Web 認証を開始する前に行う必要があります。

- IPv6 デバイス トラッキング。
- IPv6 DHCP スヌーピング。
- wlan 上の 802.1x タイプのセキュリティをディセーブルにします。
- 各 WLAN には、vlan が関連付けられている必要があります。
- デフォルト wlan 設定を **shutdown** から **no shutdown** に変更します。

関連トピック

WLAN のセキュリティのイネーブル化，（157 ページ）

IPv6 Web 認証の制限

次の制限は、IPv6 Web 認証の使用時に適用されます。

関連トピック

WLAN のセキュリティのイネーブル化, （157 ページ）

IPv6 Web 認証について

Web 認証は、レイヤ 3 セキュリティ機能です。スイッチでは、有効なユーザー名とパスワードを入力するまで、特定のクライアントからの IP トラフィック（DHCP および DNS 関連パケットを除く）を拒否します。 これはサプリカントまたはクライアントユーティリティを必要としないシンプルな認証方式です。 一般に Web 認証は、ゲスト アクセス ネットワークを展開する顧客が使用します。 HTTP と HTTPS の両方からのトラフィックで、ページがログイン ページを表示できるようにします。

（注） Web 認証は、データ暗号化を提供せず、通常は、接続が常に重要になるホット スポットまたはキャンパス環境用のシンプルなゲスト アクセスとして使用されます。

WLAN は、Web ベース認証の**セキュリティ WebAuth** として設定されます。 スイッチは次のタイプの Web ベース認証をサポートしています。

- Web 認証：クライアントが Web ページにクレデンシャルを入力し、次に Wlan コントローラによって検証されます。
- Web 同意：Wlan コントローラは、[Accept/Deny] ボタンが用意されたポリシー ページを提供します。 ネットワークにアクセスするには、[Accept] ボタンをクリックします。

一般に Wlan はオープン認証用に設定されます。つまり、レイヤ 2 認証なしで、Web ベースの認証メカニズムが使用されるときに設定されます。

Web 認証プロセス

次のイベントは、WLAN が Web 認証用に設定されている場合に発生します。

- ユーザは、Web ブラウザを開き、URL アドレスとして、たとえば、*http://www.example.com* を入力します。 クライアントは、この URL の DNS 要求を送信して、宛先の IP アドレスを取得します。 スイッチは DNS 要求を DNS サーバにバイパスし、サーバは宛先 *www.example.com* の IP アドレスが含まれている DNS 応答で応答します。 次にこれがワイヤレス クライアントに転送されます。
- クライアントは、宛先 IP アドレスで TCP 接続を開こうとします。 *www.example.com* の IP アドレス宛ての TCP SYN パケットを送信します。
- スイッチにはクライアントに設定されたルールがあり、*www.example.com* のプロキシとして機能できません。 *www.example.com* の IP アドレスとしての送信元とともにクライアントに TCP SYN-ACK パケットを戻します。 クライアントは、スリーウェイ TCP ハンドシェイクを完了するために TCP ACK パケットを戻し、TCP 接続が完全に確立されます。

- クライアントは、*www.example.com* 宛ての HTTP GET パケットを送信します。 スイッチはこのパケットをインターセプトし、リダイレクト処理用に送信します。 HTTP アプリケーション ゲートウェイは、クライアントによって要求された HTTP GET への応答として、HTML 本文を準備し送信します。 この HTML では、クライアントはスイッチのデフォルトの Web ページ（たとえば、*http://<Virtual-Server-IP>/login.html*）に転送されます。
- クライアントは、たとえば、*www.example.com* などの IP アドレスとの TCP 接続を閉じます。
- クライアントは仮想 IP に移動する場合に、スイッチの仮想 IP アドレスで TCP 接続を開こうとします。 スイッチに、仮想 IP 用の TCP SYN パケットを送信します。
- スイッチは TCP SYN-ACK で返答し、クライアントはハンドシェイクを完了するために、TCP ACK をスイッチに戻します。
- クライアントは、ログイン ページの要求のために、仮想 IP 宛ての */login.html* 用に HTTP GET を送信します。
- この要求は、スイッチの Web サーバで許可され、サーバはデフォルト ログイン ページで応答します。 クライアントは、ユーザがログインできるブラウザ ウィンドウでログイン ページを受信します。

関連トピック

WPA の無効化, （155 ページ）
WLAN のセキュリティのイネーブル化, （157 ページ）
WLAN のパラメータ マップのイネーブル化, （157 ページ）
WLAN の認証リストの有効化, （158 ページ）
グローバル Web 認証 WLAN パラメータ マップの設定, （158 ページ）
WLAN の設定, （159 ページ）
グローバル コンフィギュレーション モードの IPv6 のイネーブル化, （161 ページ）
パラメータ マップの確認, （162 ページ）
認証リストの確認, （162 ページ）

IPv6 Web 認証の設定方法

WPA の無効化

はじめる前に

802.1x を無効にします。 一般的な Web 認証では、レイヤ 2 セキュリティを使用しません。 レイヤ 2 セキュリティを削除するには、この設定を使用します。

手順の概要

1. **configure terminal**
2. **wlan** test1 2 test1
3. **no security** wpa

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** test1 2 test1 例： `Switch(config)# wlan test1 2 test1`	WLAN を作成し、SSID を割り当てます。
ステップ 3	**no security** wpa 例： `Switch(config-wlan)# no security wpa`	WLAN に対して WPA のサポートを無効にします。

次の作業

次を有効にします。

- セキュリティ Web 認証。
- パラメータ ローカル。
- 認証リスト。

関連トピック

Web 認証プロセス，（154 ページ）

WLAN のセキュリティのイネーブル化

手順の概要

1. **parameter-map type web-auth global**
2. **virtual-ip ipv4** 192.0.2.1
3. **virtual-ip ipv6** 2001:db8::24:2

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**parameter-map type web-auth global** 例： `Switch(config)# parameter-map type web-auth global`	すべての Web 認証 wlan にパラメータ マップを適用します。
ステップ 2	**virtual-ip ipv4** 192.0.2.1 例： `Switch(config-params-parameter-map)# virtual-ip ipv4 192.0.2.1`	仮想ゲートウェイの IPv4 アドレスを定義します。
ステップ 3	**virtual-ip ipv6** 2001:db8::24:2 例： `Switch(config-params-parameter-map)# virtual-ip ipv6 2001:db8::24:2`	仮想ゲートウェイの IPv6 アドレスを定義します。

関連トピック

IPv6 Web 認証の前提条件, （153 ページ）
IPv6 Web 認証の制限, （153 ページ）
Web 認証プロセス, （154 ページ）

WLAN のパラメータ マップのイネーブル化

手順の概要

1. **security web-auth parameter-map** <mapname>

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**security web-auth parameter-map** <mapname> 例： `Switch(config-wlan)# security web-auth parameter-map webparalocal`	WLAN 用の Web 認証をイネーブルにし、パラメータ マップを作成します。

関連トピック

Web 認証プロセス，（154 ページ）

WLAN の認証リストの有効化

手順の概要

1. **security web-auth authentication-list** webauthlistlocal

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**security web-auth authentication-list** webauthlistlocal 例： `Switch(config-wlan)# security web-auth`	WLAN 用の Web 認証を有効にし、ローカル Web 認証リストを作成します。

関連トピック

Web 認証プロセス，（154 ページ）

グローバル Web 認証 WLAN パラメータ マップの設定

この例を使用して、グローバル Web 認証 WLAN を設定し、パラメータ マップを追加します。

手順の概要

1. **parameter-map type webauth global**
2. **virtual-ip ipv6** 2001:db8:4::1
3. **ratelimit init-state-sessions** 120
4. **max-https-conns** 70

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**parameter-map type webauth global** 例： `Switch (config)# parameter-map type webauth global`	グローバル Web 認証を設定し、パラメータ マップを追加します。
ステップ 2	**virtual-ip ipv6** 2001:db8:4::1 例： `Switch (config-params-parameter-map)# virtual-ip ipv6 2001:db8:4::1`	認証用のワイヤレス クライアントに表示される仮想ゲートウェイ IP アドレスを定義します。
ステップ 3	**ratelimit init-state-sessions** 120 例： `Switch (config-params-parameter-map)# ratelimit init-state-sessions 120`	グローバル レート制限を設定して、スイッチで Web クライアントが使用できる帯域幅を制限し、オーバーフラッディング攻撃を防止します。
ステップ 4	**max-https-conns** 70 例： `Switch (config-params-parameter-map)# max-http-conns 70`	オーバーフラッディング攻撃を防止するため、スイッチで試行される http 接続の最大数を設定します。

関連トピック

Web 認証プロセス，（154 ページ）
WLAN の設定，（159 ページ）

WLAN の設定

はじめる前に

- WLAN は、Vlan が関連付けられている必要があります。 デフォルトでは、新しい WLAN は常に設定要件に応じて変更できる VLAN 1 に関連付けられます。

- WLAN を *no shutdown* に設定して、イネーブルにします。デフォルトでは、WLAN は *shutdown* パラメータで設定され、ディセーブルです。

手順の概要

1. **wlan** *1*
2. **client vlan** *interface ID*
3. **security web-auth authentication list** webauthlistlocal
4. **security web-auth parameter-map** global
5. **no security wpa**
6. **no shutdown**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**wlan** *1* 例： `Switch(config-wlan)# wlan 1 name vicweb ssid vicweb`	WLAN を作成し、SSID を割り当てます。
ステップ 2	**client vlan** *interface ID* 例： `Switch(config-wlan)# client vlan VLAN0136`	クライアントを VLAN インターフェイスに割り当てます。
ステップ 3	**security web-auth authentication list** webauthlistlocal 例： `Switch(config-wlan)# security web-auth authentication-list webauthlistlocal`	WLAN 用の Web 認証を設定します。
ステップ 4	**security web-auth parameter-map** global 例： `Switch(config-wlan)# security web-auth parameter-map global`	WLAN にパラメータ マップを設定します。
ステップ 5	**no security wpa** 例： `Switch(config-wlan)# no security wpa`	WLAN のセキュリティ ポリシーを設定します。これにより WLAN がイネーブルになります。
ステップ 6	**no shutdown** 例： `Switch(config-wlan)# no shutdown`	WLAN を設定して、イネーブルにします。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

グローバル Web 認証 WLAN パラメータ マップの設定，（158 ページ）
Web 認証プロセス，（154 ページ）
グローバル コンフィギュレーション モードの IPv6 のイネーブル化，（161 ページ）

グローバル コンフィギュレーション モードの IPv6 のイネーブル化

Web 認証用にグローバル コンフィギュレーションの IPv6 をイネーブルにします。

手順の概要

1. **configure terminal**
2. **web-auth global**
3. **virtual IPv6**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**web-auth global** 例： `Switch(config)# parameter-map type webauth global`	パラメータ マップのタイプを Web 認証としてグローバルに設定します。
ステップ 3	**virtual IPv6** 例： `Switch(config-params-parameter-map)# virtual-ip ipv6`	Web 認証用の仮想 IP として IPv6 を選択します。 （注） Web 認証用の優先 IP として IPv4 を選択することもできます。

関連トピック

WLAN の設定, （159 ページ）
Web 認証プロセス, （154 ページ）
パラメータ マップの確認, （162 ページ）

IPv6 Web 認証の確認

パラメータ マップの確認

WLAN に対して設定したパラメータ マップを確認するには、**show running configuration** コマンドを使用します。

手順の概要

1. **show running config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show running config** 例： `Switchshow running config`	スイッチの実行コンフィギュレーション全体を表示します。パラメータ マップのグレップを行い結果を表示します。

```
wlan alpha 2 alpha
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 security web-auth authentication-list webauthlistlocal
 security web-auth parameter-map webparalocal
```

関連トピック

グローバル コンフィギュレーション モードの IPv6 のイネーブル化, （161 ページ）
Web 認証プロセス, （154 ページ）
認証リストの確認, （162 ページ）

認証リストの確認

WLAN に対して設定した認証リストを確認するには、**show running configuration** コマンドを使用します。

手順の概要

1. **show running configuration**
2. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show running configuration** 例： `Switch#show running-config`	WLAN の設定を表示します。 `Switch# show running-config`
ステップ 2	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Switch#show running-config
 ..................................
 ..................................
 ..................................
 wlan alpha 2 alpha
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 security web-auth authentication-list webauthlistlocal
 security web-auth parameter-map webparalocal
 ..................................
 ..................................
 ..................................
```

関連トピック

パラメータ マップの確認, （162 ページ）
Web 認証プロセス, （154 ページ）

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	*IPv6 コマンド リファレンス (Catalyst 3650 スイッチ)*

関連項目	マニュアル タイトル
Web 認証設定	セキュリティ コンフィギュレーション ガイド *(Catalyst 3650 スイッチ)*

エラー メッセージ デコーダ

説明	リンク
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB のダウンロードには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングに役立てていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 Web 認証の機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 Web 認証機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 9 章

IPv6 クライアント モビリティの設定

IPv6 クライアント モビリティの前提条件

ワイヤレス IPv6 クライアント接続をイネーブルにするには、基礎となる有線ネットワークで、SLAAC または DHCPv6 などの IPv6 ルーティングおよびアドレス割り当て機能をサポートしている必要があります。 スイッチは IPv6 ルータに対する L2 隣接関係が必要です。また、VLAN はパケットがスイッチに着信するときにタグを付ける必要があります。 AP は、IPv6 ネットワーク上で接続を必要としません。すべてのトラフィックが AP とスイッチ間の IPv4 CAPWAP トンネル内でカプセル化されるためです。

IPv6 クライアント モビリティの制限

- IPv6 クライアント モビリティを使用する場合、クライアントはスタティック ステートレス自動設定（Windows XP クライアントなど）またはステートフル DHCPv6 IP アドレッシング（Windows 7 クライアントなど）とともに IPv6 をサポートする必要があります。

- ステートフル DHCPv6 IP アドレッシングが円滑に動作できるようにするには、DHCPv6 サーバとして動作するように設定された DHCP for IPv6 機能をサポートするスイッチまたはルータ（スイッチなど）、または組み込み DHCPv6 サーバを備えた Windows 2008 サーバなどの

専用サーバが必要です。 Cisco Catalyst 3850 スイッチおよび Cisco Catalyst 5700 スイッチは、（内部的に）DHCPv6 サーバとして機能できます。

（注） Cisco Catalyst 3850 スイッチに SDM IPv6 テンプレートをロードするには、**sdm prefer dual-ipv4** および **v6** デフォルト コマンドを入力し、スイッチをリセットします。

IPv6 クライアント モビリティについて

スイッチは、IPv6 専用ノードまたはデュアル スタック ノードに対し IPv6 モビリティをサポートします。 IPv6 クライアント モビリティは次のレイヤに分かれます。

- リンク層および
- ネットワーク層

リンク層は、リンク層接続を失うことなく、同じ SSID で識別される同一 BSS（基本サービスセット）の任意の AP にクライアントがローミングできるようにする 802.11 プロトコルによって処理されます。

ただし、リンク層モビリティは、ローミング中にワイヤレス クライアントのレイヤ 3 アプリケーションがシームレスに動作を継続するには十分ではありません。 Cisco IOSd のワイヤレス モビリティ モジュールは、モビリティ トンネリングを使用して、クライアントが異なるスイッチ上の異なるサブネット間をローミングするときに、クライアントのレイヤ 3 PoP（Point of Presence）用のシームレスな接続を維持します。

IPv6 は、プロトコルの TCP/IP スイートの IPv4 に代わることを目的とした次世代ネットワーク層インターネット プロトコルです。 この新しいバージョンでは、一意のグローバル IP アドレスを必要とするユーザとアプリケーションに対応するためのインターネット グローバルアドレス空間を増大させます。 IPv6 は、128 ビットの送信元アドレスおよび宛先アドレスを組み込むことにより、32 ビットの IPv4 アドレスよりも格段に多くのアドレスを提供します。

コントローラをまたいだ IPv6 クライアントをサポートするには、IPv6 クライアントが同じレイヤ 3 ネットワーク上にとどまるように、ICMPv6 メッセージを特別に処理する必要があります。 スイッチは、ICMPv6 メッセージを代行受信することで IPv6 クライアントを追跡し、シームレスなモビリティを提供して、ネットワーク攻撃からネットワークを保護します。 NDP（ネイバーディスカバリ パケット）パケットは、マルチキャストからユニキャストに変換され、クライアントごとに個別に配信されます。 この固有なソリューションによって、ネイバー ディスカバリ パケットとルータ アドバタイズメント パケットの VLAN 間でのリークを防止できます。 クライアントは、特定のネイバー ディスカバリ パケットおよびルータ アドバタイズメント パケットを受信することで IPv6 アドレス指定が適切であることを確認し、不要なマルチキャスト トラフィックを回避します。

IPv6 モビリティの設定は、IPv4 モビリティと同一であり、シームレスなローミングを実現するためにクライアント側で別個のソフトウェアを使用する必要はありません。 スイッチは、同じモビリティ グループに属している必要があります。 IPv4 と IPv6 の両クライアント モビリティが、デフォルトで有効になります。

IPv6 クライアント モビリティは次のことに使用されます。

- レイヤ 2 およびレイヤ 3 ローミングでのクライアント IPv6 複数アドレスの維持。
- IPv6 ネイバー探索プロトコル（NDP）パケットの管理。
- クライアントの IPv6 アドレスの学習。

ルータ アドバタイズメントの使用

ネイバー探索プロトコル（NDP）はリンク層で動作し、リンク上の他のノードの検出を行います。他のノードのリンク層アドレスを特定し、使用可能なルータを検索し、他のアクティブなネイバーノードのパスに関する到達可能性情報を維持します。

ルータ アドバタイズメント（RA）は、使用可能なルータを検出し、IPv6 アドレス、リンク MTU などを生成するネットワーク プレフィクスを取得するためにホストで使用される IPv6 ネイバー探索プロトコル（NDP）パケットの 1 つです。 ルータは、定期的またはホスト ルータ送信要求メッセージへの応答として RA を送信します。

IPv6 ワイヤレス クライアント モビリティは IPv6 RA パケットを管理します。 集約アクセススイッチは、リンクローカル全ノード マルチキャスト RA パケットをローカルおよび RA が受信される同じ VLAN にマップされたローミング ワイヤレス ノードに転送します。

図 4 では、ワイヤレス ノード モビリティでのリンクローカル全ノード マルチキャスト RA の転送の問題について説明します。

図 *4*：ルータ *2* から無効な *RA* を受け取るローミング クライアント

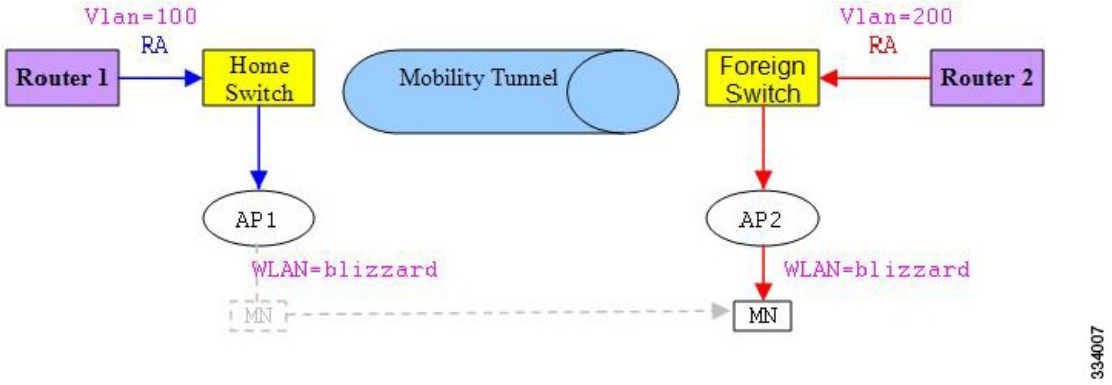
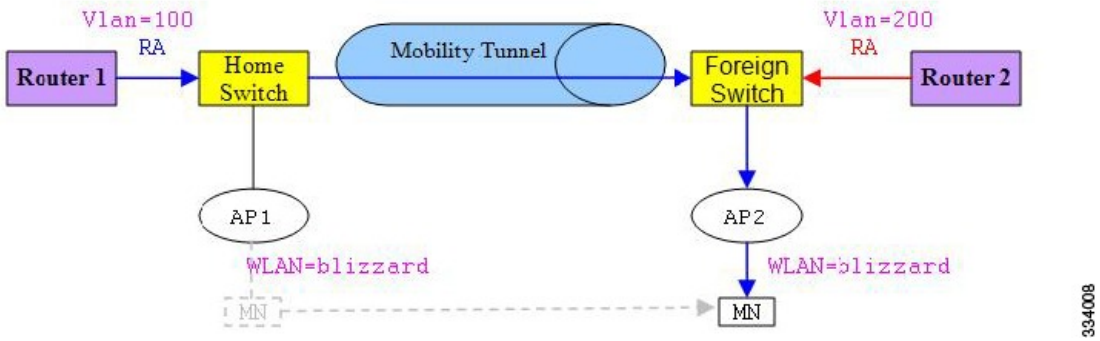


図 5 では、ローミング クライアント「MN」が外部スイッチで VLAN 200 から RA をどのように受信するか、および新しい IP アドレスを取得してどのように L3 モビリティの PoP（Point of Presence）に入るかを示しています。

図 *5*：ルータ *1* から有効な *RA* を受け取るローミング クライアント



関連トピック

IPv6 クライアント モビリティの確認，（172 ページ）
IPv6 クライアント モビリティのモニタリング，（173 ページ）

RA スロットリングと NS 抑制

頻繁な非請求タイプの定期的 RA による制約を受けないように省電力ワイヤレス クライアントを保護するため、コントローラで非請求タイプのマルチキャスト RA をスロットルできます。

関連トピック

IPv6 クライアント モビリティの確認，（172 ページ）
IPv6 クライアント モビリティのモニタリング，（173 ページ）

IPv6 アドレス ラーニング

IPv6 クライアントで IPv6 アドレスを取得するには、次の 3 つの方法があります。

- ステートレス アドレス自動設定（SLAAC）
- ステートフル DHCPv6
- 静的設定

これらの方法の場合、IPv6 クライアントは常に NS DAD（重複アドレス検出）要求を送信して、ネットワークに重複する IP アドレスがないようにします。 スイッチはクライアントの NDP および DHCPv6 パケットをスヌープして、そのクライアント IP アドレスについて学習し、コントロー

ラ データベースを更新します。 データベースは、クライアントの新しい IP アドレスについてコントローラに通知します。

関連トピック

IPv6 クライアント モビリティの確認, （172 ページ）
IPv6 クライアント モビリティのモニタリング, （173 ページ）

複数の IP アドレスの処理

RUN 状態後に新しい IP アドレスが受信されると、追加の場合も削除の場合も、コントローラは表示目的でそのローカル データベース上の新しい IP アドレスを更新します。 基本的に、IPv6 は既存または IPv4 の場合と同じ PEM ステート マシン コードフローを使用します。 IP アドレスが、たとえば、外部エンティティによって Prime Infrastructure から要求されると、コントローラは、すべての使用可能な IP アドレス、IPv4 および IPv6 を外部エンティティへの API/SPI インターフェイスに含めます。

IPv6 クライアントは、様々な目的でスタックから複数の IP アドレスを取得できます。 たとえば、リンクローカル トラフィックのリンクローカルアドレスおよびルーティング可能な固有のローカル アドレスまたはグローバル アドレスがあります。

クライアントが DHCP 要求状態にあり、コントローラが IPv4 または IPv6 アドレス用にデータベースから最初の IP アドレスの通知を受信すると、PEM はクライアントを RUN 状態に移行させます。

RUN 状態後に新しい IP アドレスが受信されるときは、追加の場合も削除の場合も、コントローラは表示目的でそのローカル データベース上の新しい IP アドレスを更新します。

IP アドレスが、たとえば、外部エンティティによって Prime Infrastructure から要求されると、コントローラは、使用可能な IP アドレス、IPv4 および IPv6 を外部エンティティに提供します。

関連トピック

IPv6 クライアント モビリティの確認, （172 ページ）
IPv6 クライアント モビリティのモニタリング, （173 ページ）

IPv6 Configuration

スイッチは IPv4 クライアントと同様にシームレスに IPv6 クライアントをサポートします。 管理者は、IPV6、IPv6 スヌーピングおよびスロットリング機能を有効にするには、Vlan を手動で設定する必要があります。 これにより、スイッチとそのさまざまなクライアント間でのスロットリングを NDP パケットで行えます。

関連トピック

IPv6 クライアント モビリティの確認, （172 ページ）
IPv6 クライアント モビリティのモニタリング, （173 ページ）

ハイ アベイラビリティ

スイッチはクライアント IP アドレスが学習しにくいときにワイヤレス クライアントと同期します。 スイッチオーバーが発生すると、IPv6 ネイバー バインディング テーブルがスタンバイ ステートに同期されます。 ただし、スイッチオーバーが完了し、ネイバー バインディング テーブルがそのクライアントの最新情報で更新されると、ワイヤレス クライアント自体はアソシエート解除され、新しいアクティブ ステートに再アソシエートされます。

再アソシエーション時に、クライアントが他の AP に移動すると、バインディング テーブル内の元のエントリがしばらくの間ダウンとマークされ、期限切れになります。

別の AP からスイッチを結合する新しいエントリの場合は、新しい IP アドレスが学習されて、コントローラのデータベースに通知されます。

（注） この機能は、Cisco Catalyst 3850 スイッチでのみ使用できます。

関連トピック

IPv6 クライアント モビリティの確認, （172 ページ）
IPv6 クライアント モビリティのモニタリング, （173 ページ）

IPv6 クライアント モビリティの確認

表 1 に示すコマンドは、IPv6 クライアント モビリティに適用されます。

表 *9*：*Cisco 5760 WLC* の *IPv6* クライアント モビリティを確認するためのコマンド

コマンド	説明
debug mobility ipv6	すべてのワイヤレス クライアント IPv6 モビリティのデバッグをイネーブルにします。
debug クライアント **mac-address** (mac-addr)	ワイヤレスクライアントのデバッグを表示します。 デバッグ情報の MAC アドレスを入力します。

関連トピック

ルータ アドバタイズメントの使用, （169 ページ）
RA スロットリングと NS 抑制, （170 ページ）
IPv6 アドレス ラーニング, （170 ページ）
複数の IP アドレスの処理, （171 ページ）

IPv6 Configuration, （171 ページ）
IPv6 クライアント モビリティのモニタリング, （173 ページ）
ハイ アベイラビリティ, （172 ページ）

IPv6 クライアント モビリティのモニタリング

表 2 のコマンドは、スイッチで IPv6 クライアント モビリティをモニタリングするために使用されます。

表 *10* : *IPv6* クライアント モビリティ コマンドのモニタリング

コマンド	説明
show wireless client summary	アクティブなクライアントのワイヤレス固有設定を表示します。
show wireless client mac-address (mac-addr)	アクティブなクライアントのワイヤレス固有設定をその MAC アドレスに基づいて表示します。

関連トピック

IPv6 クライアント モビリティの確認, （172 ページ）
ルータ アドバタイズメントの使用, （169 ページ）
RA スロットリングと NS 抑制, （170 ページ）
IPv6 アドレス ラーニング, （170 ページ）
複数の IP アドレスの処理, （171 ページ）
IPv6 Configuration, （171 ページ）
ハイ アベイラビリティ, （172 ページ）

その他の関連資料

関連資料

関連項目	マニュアル タイトル
『IPv6 Command Reference』	*IPv6* コマンド リファレンス *(Catalyst 3650* スイッチ*)*
モビリティ設定	*Mobility* コンフィギュレーション ガイド、*Cisco IOS XE Release 3SE*（*Catalyst 3650* スイッチ）

エラー メッセージ デコーダ

説明	リンク
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB のダウンロードには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングに役立てていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 クライアント モビリティの機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 クライアント モビリティ機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 10 章

IPv6 モビリティの設定

IPv6 モビリティの前提条件

モビリティとその関連のインフラストラクチャを設定して使用できるようにする必要があります。

IPv6 モビリティについて

モビリティ（ローミング）は、できるだけ低遅延で、確実かつスムーズに、あるアクセス ポイントから別のアクセス ポイントへのアソシエーションを維持する無線 LAN クライアントの機能です。 この項では、スイッチが無線ネットワークに存在する場合のモビリティの動作について説明します。

あるワイヤレス クライアントがアクセス ポイントにアソシエートして認証すると、アクセス ポイントのスイッチは、クライアント データベースにそのクライアントに対するエントリを設定します。 このエントリには、クライアントの MAC アドレス、IP アドレス、セキュリティ コンテキストおよびアソシエーション、Quality of Service（QoS）コンテキスト、WLAN、およびアソシエートされたアクセスポイントが含まれます。 スイッチはこの情報を使用してフレームを転送し、ワイヤレス クライアントで送受信されるトラフィックを管理します。

ワイヤレス クライアントがそのアソシエーションをあるアクセス ポイントから別のアクセス ポイントへ移動する場合、スイッチは新たにアソシエートするアクセス ポイントでクライアントのデータベースをアップデートするだけです。 必要に応じて、新たなセキュリティ コンテキストと

アソシエーションも確立されます。 しかし、クライアントが 1 つのスイッチに接続されたアクセスポイントから別のスイッチに接続されたアクセスポイントにローミングする際には、プロセスはより複雑になります。 また、同一のサブネット上でこれらのスイッチが動作しているかどうかによっても異なります。

コントローラ間ローミング

クライアントが新たなスイッチに接続されたアクセス ポイントへアソシエートする場合、新たなスイッチはモビリティ メッセージを元のスイッチと交換し、スティッキアンカリングがディセーブルの場合に、クライアントのデータベース エントリは新たなスイッチに移動されます。

関連トピック

IPv6 モビリティのモニタリング, （179 ページ）

スティッキ アンカリングでのサブネット内ローミング、およびサブネット間ローミング

サブネット間ローミングは、スイッチがクライアントのローミングに関するモビリティ メッセージを交換する点でコントローラ間ローミングと似ています。 ただし、クライアントのデータベースエントリを新しいスイッチに移動するのではなく、元のスイッチのクライアントデータベース内で該当クライアントに「アンカー」エントリのマークが付けられます。 このデータベースエントリが新しいスイッチのクライアント データベースにコピーされ、新しいスイッチ内で「外部」エントリのマークが付けられます。 ローミングはワイヤレスクライアントには透過的なまま行われ、クライアントは元の IP アドレスを保持します。

サブネット間ローミングでは、アンカーと外部の両スイッチの WLAN に、ソースベースのルーティングやソースベースのファイアウォールは設定せずに同一のネットワーク アクセス権限を設定する必要があります。 そのようにしない場合、ハンドオフ後クライアントにネットワーク接続上の問題が発生することがあります。

モビリティの設定の詳細については、『Cisco 5700 Wireless LAN Controller Mobility Configuration Guide, Cisco IOS XE, Release 3.2SE』を参照してください。

関連トピック

IPv6 モビリティのモニタリング, （179 ページ）

IPv6 モビリティの設定方法

IPv6 モビリティのモニタリング

この章では、モビリティ関連 IPv6 設定を表示します。 モビリティ関連の設定を確認するには、『Cisco 5700 Wireless LAN Controller Mobility Configuration Guide, Cisco IOS XE 3.2SE』を参照してください。

手順の概要

1. **show ipv6 neighbors binding mac** C0C1.C06B.C4E2

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ipv6 neighbors binding mac** C0C1.C06B.C4E2 例： `Switch# show ipv6 neighbors binding mac C0C1.C06B.C4E2`	IPv6 関連のモビリティ設定を表示します。

```
Switch# show ipv6 neighbors binding mac C0C1.C06B.C4E2
Binding Table has 45 entries, 37 dynamic (limit 100)
Codes: L - Local, S - Static, ND - Neighbor Discovery, DH - DHCP, PKT - Other Packet, API
- API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    IPv6 address                            Link-Layer addr Interface vlan prlvl  age
state    Time left
L   FE80:20:25::16                          2037.064C.BA71  Vl25        25  0100 3137mn
REACHABLE
L   FE80:20:24::16                          2037.064C.BA41  Vl24        24  0100 3137mn
REACHABLE
L   FE80:20:23::16                          2037.064C.BA44  Vl23        23  0100 3137mn
REACHABLE
ND  FE80:20:23::13                          2037.0653.6BC4  Te1/0/1     23  0005   85s
REACHABLE  223 s try 0
ND  FE80:20:22::17                          2037.064D.06F6  Te1/0/1     22  0005    3mn
REACHABLE  92 s try 0
L   FE80:20:22::16                          2037.064C.BA76  Vl22        22  0100 3137mn
REACHABLE
ND  FE80:20:22::13                          2037.0653.6BF6  Te1/0/1     22  0005  165s
REACHABLE  136 s try 0
ND  FE80:20:22::12                          2037.064C.94F6  Te1/0/1     22  0005   23s
REACHABLE  281 s try 0
ND  FE80:20:22::2                           0022.550E.8FC3  Te1/0/1     22  0005   18s
REACHABLE  295 s try 0
ND  FE80:20:21::17                          2037.064D.06E8  Te1/0/1     21  0005    4mn
REACHABLE  60 s try 0
L   FE80:20:21::16                          2037.064C.BA68  Vl21        21  0100 3137mn
```

```
REACHABLE
ND  FE80:20:21::13                          2037.0653.6BE8  Te1/0/1     21  0005   57s
REACHABLE  252 s try 0
ND  FE80:20:21::12                          2037.064C.94E8  Te1/0/1     21  0005    4s
REACHABLE  297 s
ND  FE80:20:21::2                           0022.550E.8FC2  Te1/0/1     21  0005    2s
REACHABLE  307 s try 0
ND  FE80::F866:8BE0:12E4:39CF               C0C1.C06B.C4E2  Ca4         21  0005    3mn
REACHABLE  89 s try 0
ND  FE80::6D0A:DB33:D69E:91C7               0050.B606.A6CE  Te1/0/1     22  0005  135s
REACHABLE  171 s try 0
ND  FE80::985:8189:9937:BB05                8CA9.8295.09CC  Ca0         21  0005   15s
REACHABLE  287 s
ND  FE80::20:24:13                          2037.0653.6BC1  Te1/0/1     24  0005  155s
REACHABLE  145 s try 0
L   2001:20:23::16                          2037.064C.BA44  Vl23        23  0100 3137mn
REACHABLE
DH  2001:20:22:0:C96C:AF29:5DDC:2689        0050.B606.A6CE  Te1/0/1     22  0024   19s
REACHABLE  286 s try 0(16574
DH  2001:20:22:0:A46B:90B2:F0DB:F952        0050.B606.A6CE  Te1/0/1     22  0024 2339mn
STALE      32401 s
DH  2001:20:22:0:7DFD:14EC:B1E4:1172        0050.B606.A6CE  Te1/0/1     22  0024 2339mn
STALE      24394 s
DH  2001:20:22:0:7CB3:D6DD:FD6A:50F         0050.B606.A6CE  Te1/0/1     22  0024 2333mn
STALE      29195 s
DH  2001:20:22:0:6D32:AF24:FDE1:2504        0050.B606.A6CE  Te1/0/1     22  0024  509mn
STALE      118821 s
DH  2001:20:22:0:5106:5AD:FE98:A2F0         0050.B606.A6CE  Te1/0/1     22  0024 2328mn
STALE      31362 s
ND  2001:20:22::201:13                      0050.B606.A6CE  Te1/0/1     22  0005   49s
REACHABLE  264 s try 0
L   2001:20:22::16                          2037.064C.BA76  Vl22        22  0100 3137mn
REACHABLE
ND  2001:20:22::13                          2037.0653.6BF6  Te1/0/1     22  0005  175s
REACHABLE  131 s try 0
ND  2001:20:22::2                           0022.550E.8FC3  Te1/0/1     22  0005   28s
REACHABLE  274 s try 0
ND  2001:20:21:0:F866:8BE0:12E4:39CF        C0C1.C06B.C4E2  Ca4         21  0005    4mn
REACHABLE  21 s try 0
ND  2001:20:21:0:C085:9D4C:4521:B777        0021.CC73.AA17  Te1/0/1     21  0005   11s
REACHABLE  290 s try 0
ND  2001:20:21:0:6233:4BFF:FE1A:744C        6033.4B1A.744C  Ca4         21  0005    3mn
REACHABLE  108 s try 0
ND  2001:20:21:0:447E:745D:2F48:1C68        8CA9.8295.09CC  Ca0         21  0005   34s
REACHABLE  276 s
ND  2001:20:21:0:3920:DDE8:B29:AD51         C0C1.C06B.C4E2  Ca4         21  0005    3mn
REACHABLE  87 s try 0
ND  2001:20:21:0:1016:A333:FAD5:6E66        0021.CC73.AA17  Te1/0/1     21  0005    4mn
REACHABLE  18 s try 0
ND  2001:20:21:0:C42:E317:BA9B:EB17         6033.4B1A.744C  Ca4         21  0005    4mn
REACHABLE  61 s try 0
ND  2001:20:21:0:985:8189:9937:BB05         8CA9.8295.09CC  Ca0         21  0005  135s
REACHABLE  173 s try 0
ND  2001:20:21::201:20                      0021.CC73.AA17  Te1/0/1     21  0005    4mn
REACHABLE  43 s try 0
ND  2001:20:21::17                          2037.064D.06E8  Te1/0/1     21  0005    4mn
REACHABLE  50 s try 0
L   2001:20:21::16                          2037.064C.BA68  Vl21        21  0100 3137mn
REACHABLE
ND  2001:20:21::13                          2037.0653.6BE8  Te1/0/1     21  0005   67s
REACHABLE  237 s try 0
ND  2001:20:21::12                          2037.064C.94E8  Te1/0/1     21  0005    5mn
REACHABLE  512 ms try 0
ND  2001:20:21::2                           0022.550E.8FC2  Te1/0/1     21  0005   12s
REACHABLE  294 s try 0
```

関連トピック

コントローラ間ローミング, （178 ページ）

スティッキ アンカリングでのサブネット内ローミング、およびサブネット間ローミング，（178 ページ）

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	*IPv6 コマンド リファレンス (Catalyst 3650 スイッチ)*
モビリティ設定	*Mobility コンフィギュレーション ガイド、Cisco IOS XE Release 3SE（Catalyst 3650 スイッチ）*

エラー メッセージ デコーダ

説明	リンク
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB のダウンロードには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングに役立てていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 モビリティの機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 モビリティ機能	Cisco IOS XE 3.3SE	この機能が導入されました。

第 11 章

IPv6 NetFlow の設定

IPv6 NetFlow の前提条件

ネットワーキング デバイスで、Cisco IOS Flexible NetFlow がサポートされた Cisco IOSd リリースを実行している必要があります。

IPv6 トラフィック

- 次のいずれかがルータ、および Flexible NetFlow をイネーブルにするインターフェイスでイネーブルになっている必要があります。
  - シスコ エクスプレス フォワーディング IPv6
  - 分散型シスコ エクスプレス フォワーディング IPv6

IPv6 NetFlow の制限

次の制限は、IPv6 Netflow 設定に適用されます。

- ローカルで生成されたトラフィック（Flexible NetFlow 出力アカウンティング機能が設定されているルータ、Cisco WLC 5760、によって生成されるトラフィック）は、Output Flexible NetFlow Accounting 機能のフロー トラフィックとしてカウントされません。
- Flexible NetFlow 出力アカウンティング機能によって、CEF スイッチド パケットのみがカウントされます。 プロセス スイッチド中継パケットはカウントされません。

IPv6 NetFlow について

NetFlowは、ネットワーク モニタリング、ユーザのモニタリングとプロファイリング、ネットワーク プランニング、セキュリティの分析、課金とアカウンティング、データ ウェアハウジングとデータ マイニングのためにカスタマー アプリケーションで使用されるモニタ機能です。 アップリンク ポートで Flexible NetFlow を使用すれば、ユーザ定義フローのモニタリング、フロー統計情報の収集、フロー単位のポリシングの実行が可能です。 Flexible NetFlowは、フロー統計情報を収集してコレクタ デバイスにエクスポートします。

（注） Flexible NetFlowは、IPベースまたはIPサービス フィーチャ セットを実行しネットワーク サービスモジュールが装備されているCatalyst 3750-Xスイッチおよび3560-Xスイッチだけでサポートされます。 NPEまたはLANベースイメージを実行しているスイッチではサポートされません。

（注） コマンド リファレンスに記載されているすべての Flexible NetFlow コマンドがスイッチで使用できるわけではありません。 サポートされていないコマンドは、表示されないか、入力するとエラー メッセージが生成されます。

Flexible NetFlow の概要

Flexible NetFlow では、トラフィックが処理され、パケットはフローに分類されます。 新しいフローはNetFlowテーブルに挿入され、統計情報は自動的に更新されます。 入力および出力NetFlowモニタの両方を設定する必要があります。 ネットワーク サービス モジュールにより、方向ごとにインターフェイスあたり 1 個のモニタをサポートします。

Flexible NetFlow は、次のコンポーネントで構成されます。

- レコード：Flexible NetFlow モニタをモニタリングして、データの保存に使用されるキャッシュを定義するために割り当てられるキーおよび非キー フィールドの組み合わせです。
- フロー モニタ：インターフェイスに適用され、ネットワーク トラフィック モニタリングを実行します。 フロー モニタには、ユーザ定義のレコード、オプションのフロー エクスポータ、およびモニタが最初のインターフェイスに適用されるときに自動的に作成されるキャッ

シュで構成されます。 スイッチは、設定に従って期限切れになる通常のキャッシュをサポートします。

- フロー エクスポータ：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、NetFlow コレクタを実行するサーバ）にエクスポートします。
- フローサンプラー：分析す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 Flexible NetFlow によってネットワーキング デバイスで生じる負荷を軽減します。

単方向フロー（宛先または送信元アドレスベースのフロー）、およびフローエージングを設定できます。 次の機能が、ネットワーク サービス モジュールでサポートされます。

- レイヤ 2 スイッチング（非ルーティング）トラフィック、レイヤ 3（CAPWAP）IPv4 および IPv6 トラフィック、レイヤ 4 TCP、IGMP、および ICMP トラフィックの統計情報収集の設定。
- NetFlow カウント、メンテナンス、トラブルシューティング（デバッグ コマンド）。
- NetFlow 分析は、ネットワーク サービス モジュール上の物理インターフェイスを通るトラフィックに対して実行されます。 スイッチは、転送判断を実行した後、出力（発信）トラフィックを処理します。 プライベート VLAN または保護ポートを設定することで、ローカルにスイッチングまたはルーティングされたトラフィックが、サービス モジュール ポートの通過を強制されます。

次の NetFlow の特性はサポートされていません。

- Netflow-5 プロトコル
- あらかじめ定義されたフロー レコード
- ISL
- ポリシーベースの NetFlow
- Cisco TrustSec モニタリング

スイッチに取り付けることができる他のモジュールは 1 ギガビットおよび 10 ギガビット アップリンク インターフェイスを搭載していますが、NetFlow はネットワーク サービス モジュールだけでサポートされます。

IPv6 Netflow

Flexible Netflow（FNF）では、事前定義済みフィールドの大規模なコレクションからフィールドを選択し、CLI コンフィギュレーション コマンドを使用して、特定のアプリケーションに最適なフロー レコード（対象となるキー、非キー、カウンタ、およびタイムスタンプ フィールドのセット）を定義することができます。

事前定義されたフィールドのコレクションには次のフィールドが含まれます。

- データリンク層（L2）のヘッダー フィールド
- IPv6 ヘッダーのフィールド

- トランスポート層（L4）のヘッダー フィールド
- アプリケーション層（L5）のヘッダー フィールド
- ルーティング属性（汎用、IPv4、IPv6）
- インターフェイス フィールド
- カウンタ フィールド
- タイムスタンプ フィールド

関連トピック

カスタマイズしたフロー レコードの設定，（186 ページ）
フロー エクスポータの設定，（189 ページ）
カスタマイズしたフロー モニタの設定，（195 ページ）
インターフェイスへのフロー モニタの適用，（197 ページ）
フロー サンプリングの設定およびイネーブル化，（199 ページ）

IPv6 NetFlow の設定方法

カスタマイズしたフロー レコードの設定

フロー レコードの次のフィールドに一致させることができます。

- IPv4 または IPv6 宛先アドレス
- 直接接続されたホストの MAC アドレスを示す、インターフェイスで受信または送信されるトラフィックのレイヤ 2 送信元と宛先アドレスおよび VLAN を識別するデータリンク フィールド。 サービス クラス（CoS）および Ethertype データリンク ヘッダー フィールドも使用できます。
- アプリケーションのタイプ（ICMP、IGMP、または TCP トラフィック）を識別するトランスポート フィールドの送信元および宛先ポート。

フロー レコードの次のフィールドを収集できます。

- 合計バイト数、エクスポータによって送信されるまたはフローまたはパケット（exporter）、または 64 ビット カウンタのバイト数またはパケット数（long）。 最初のパケットの送信時間または最新（最後）のパケットが見つかった時間からのシステム稼働時間に基づくタイムスタンプ。
- 入力または出力インターフェイスの SNMP インデックス。 サービス モジュールに出入りするトラフィックのインターフェイスは、スイッチの転送キャッシュに基づいています。 このフィールドは、一般にデータ リンク、IPv4 および IPv6 アドレスとともに使用され、直接接続されたホストの実際のファースト ホップのインターフェイスを提供します。
  - 値 0 は、インターフェイス情報がキャッシュにないことを意味します。

- 一部の NetFlow コレクタでは、フロー レコードにこの情報が必要です。

次の手順で、カスタマイズされたフロー レコードを設定します。

手順の概要

1. **configure terminal**
2. **flow record** recordname
3. **description** description
4. **match** {ipv4 | ipv6} {destination | hop-limit | protocol | source | traffic-class| version} **address**
5. **match datalink** [dot1q | ethertype | mac | vlan]
6. **match transport** [destination-port | icmp | source-port]
7. **match interface** [input |output]
8. **match flow direction**
9. **collect counter** {bytes [layer2 | long] | packets [long]}
10. **collect timestamp absolute** [first | last]
11. **collect interface** [input | output]
12. **collect transport tcp flags** {ack | cwr | ece | fin | psh | rst | syn | urg}
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**flow record** recordname 例： `Switch(config)# flow record TestRecordName`	フロー レコードを作成し、Flexible NetFlow フロー レコード コンフィギュレーション モードを開始します。 このコマンドで、既存のフロー レコードを変更することもできます。
ステップ 3	**description** description 例： `Switch(config-flow-record)# description SampleNetflowDescription`	（任意）フロー レコードの説明を作成します。
ステップ 4	**match** {ipv4 | ipv6} {destination | hop-limit | protocol | source | traffic-class| version} **address** 例： `Switch(config-flow-record)# match ipv6 destination address`	フロー レコードの主要 ipv4 および ipv6 フィールドを設定します。

	コマンドまたはアクション	目的
ステップ 5	**match datalink** [dot1q | ethertype | mac | vlan] 例： `Switch(config-flow-record)# match datalink [dot1q | ethertype | mac | vlan]`	フロー レコードの主要データリンク（レイヤ2）フィールドを設定します。
ステップ 6	**match transport** [destination-port | icmp | source-port] 例： `Switch(config-flow-record)# match transport [destination-port | icmp | source-port]`	フロー レコードの主要トランスポート レイヤ フィールドを設定します。
ステップ 7	**match interface** [input |output] 例： `Switch(config-flow-record)# match interface input`	フロー レコードの主要インターフェイス フィールドを設定します。
ステップ 8	**match flow direction** 例： `Switch(config-flow-record)# match flow direction`	フロー レコードの主要フロー アイデンティティ フィールドを設定します。
ステップ 9	**collect counter** {bytes [layer2 | long] | packets [long]} 例： `Switch(config-flow-record)#collect counter bytes layer2 long`	フロー レコードのカウンタ主要フィールドを設定します。
ステップ 10	**collect timestamp absolute** [first | last] 例： `Switch(config-flow-record)# collect timestamp absolute [first | last ]`	フロー レコードのタイムスタンプ主要フィールドを設定します。
ステップ 11	**collect interface** [input | output] 例： `Switch(config-flow-record)# collect interface [input | output]`	フロー レコードのインターフェイス主要フィールドを設定します。
ステップ 12	**collect transport tcp flags** {ack | cwr | ece | fin | psh | rst | syn | urg} 例： `Switch(config-flow-record)# collect transport tcp flags ack`	フロー レコードのトランスポート tcp フラグ フィールドを設定します。
ステップ 13	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Switch(config)# flow record
Switch(config-flow-record)# description record to monitor network traffic
Switch(config-flow-record)# match ipv6 destination address
Switch(config-flow-record)# match datalink [dot1q | ethertype | mac | vlan]
Switch(config-flow-record)# match transport [destination-port | icmp |igmp | source-port]
Switch(config-flow-record)# match interface input
Switch(config-flow-record)# match flow direction
Switch(config-flow-record)#collect counter bytes layer2 long
Switch(config-flow-record)# collect timestamp absolute first
Switch(config-flow-record)# collect interface [input | output]
Switch(config-flow-record)# collect transport tcp flags ack
Switch(config-flow-record)# end
```

関連トピック

IPv6 Netflow, （185 ページ）
フロー エクスポータの設定 , （189 ページ）
カスタマイズしたフロー モニタの設定, （195 ページ）
インターフェイスへのフロー モニタの適用, （197 ページ）
フロー サンプリングの設定およびイネーブル化 , （199 ページ）

フロー エクスポータの設定

次の手順を使用して NetFlow エクスポータを設定します。

（注） 任意の export-protocol フロー エクスポータ コンフィギュレーション コマンドは、エクスポータで使用される NetFlow エクスポート プロトコルを指定します。 スイッチは netflow-v9 だけをサポートします。 CLI ヘルプに記載されていますが、netflow-5 はサポートされません。

手順の概要

1. **configure terminal**
2. **flow exporter** exporter-name
3. **description** description
4. **destination** {hostname | ip-address} **vrf** vrf-name
5. **dscp** <0-63>
6. **source** interface-id
7. **option** {exporter-stats | interface-table | sampler-table} **timeout** seconds]
8. **export-protocolnetflow-v9**
9. **template data timeout** seconds
10. **transport udp** udp-port
11. **ttl** seconds
12. **end**

手順の詳細

	コマンドまたはアクション
ステップ 1	**configure terminal** 例： `Switch# configure terminal`
ステップ 2	**flow exporter** exporter-name 例： `Switch(config)# flow exporter TestNetFlowExporterName`
ステップ 3	**description** description 例： `Switch(config-flow-exporter)# description SampleNetFlowExporterDescription`

	コマンドまたはアクション
ステップ 4	**destination** {hostname | ip-address} **vrf** vrf-name 例： `Switch(config-flow-exporter)# destination 198.51.100.120 vrf SampleVrfName`
ステップ 5	**dscp** <0-63> 例： `Switch(config-flow-exporter)# dscp 23`

ステップ 6	**source** interface-id
	
	例：
	`Switch(config-flow-exporter)# source {`
	`Auto-Template|Capwap|GigabitEthernet|GroupVI|InternalInterface|Loopback|Null|Port-channel|TenGigabitEthernet|Tu`

	コマンドまたはアクション
ステップ 7	**option** {exporter-stats | interface-table | sampler-table} **timeout** seconds] 例： `Switch(config-flow-exporter)# option exporter-stats timeout 600`
ステップ 8	**export-protocolnetflow-v9** 例： `Switch(config-flow-exporter)# export-protocol netflow-v9`

	コマンドまたはアクション

ステップ 9	**template data timeout** seconds
	
	例：
	`Switch(config-flow-exporter)# template data timeout 600`
	`Switch(config-flow-exporter)#`

ステップ 10	**transport udp** udp-port 例： `Switch(config-flow-exporter)# transport udp 67`
ステップ 11	**ttl** seconds 例： `Switch(config-flow-exporter)# ttl 100`

	コマンドまたはアクション
ステップ 12	**end** 例： `Switch(config)# end`

```
Switch(config)# flow exporter QoS-Collector
Switch(config-flow-exporter)# description QoS Collector Bldg 19
Switch(config-flow-exporter)# destination 172.20.244.28
Switch(config-flow-exporter)# source vlan 1
Switch(config-flow-exporter)# dscp 3
Switch(config-flow-exporter)# transport udp 2055
Switch(config-flow-exporter)# end
```

次の作業

カスタマイズしたフロー モニタの設定。

関連トピック

カスタマイズしたフロー レコードの設定，（186 ページ）
IPv6 Netflow,（185 ページ）

カスタマイズしたフロー モニタの設定

次の手順を使用して NetFlow モニタを設定します。

手順の概要

1. **configure terminal**
2. **flow monitor** monitor -name
3. **description** description
4. **record** {TestNetflowRecordName|TestRecord}
5. **cache** {timeout [active| inactive|update] (seconds) | type (normal)}
6. **cache** {timeout [active| inactive|update] (seconds) | type (normal)}
7. **exporter** TestNetFlowExporterName
8. **cache** {timeout [active| inactive|update] (seconds) | type (normal)}
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**flow monitor** monitor -name 例： `Switch(config)# flow monitor SampleMonitorName`	フロー モニタを作成し、Flexible NetFlow 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。 このコマンドを使用して既存のフローモニタを変更することもできます。
ステップ 3	**description** description 例： `Switch(config-flow-monitor)# Description SampleNetFlowMonitorName`	（任意）フロー モニタの説明を設定します。
ステップ 4	**record** {TestNetflowRecordName|TestRecord} 例： `Switch(config-flow-monitor)#record TestNetflowRecordName`	フロー モニタのレコードを指定します。

	コマンドまたはアクション	目的
ステップ 5	**cache** {timeout [active| inactive|update] (seconds) | type (normal)} 例： `Switch(config-flow-monitor)# cache type normal`	（任意）フローモニタ キャッシュ パラメータ（タイムアウト値、キャッシュ エントリ数、キャッシュ タイプなど）を変更します。 • **timeout active** *seconds*：アクティブ フロー タイムアウトを設定します。これは、トラフィック分析の細かさを定義します。指定できる範囲は 1 ～ 604800 秒です。デフォルト値は 1800 です。一般的な値は 60 または 300 秒です。推奨値については、『Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters』を参照してください。 • **type normal**：フロー キャッシュからの通常のフロー削除を設定します。 （注） コマンドラインのヘルプには記載されていますが、entries キーワードとタイムアウト inactive および update はサポートされません。
ステップ 6	**cache** {timeout [active| inactive|update] (seconds) | type (normal)} 例： `Switch(config-flow-monitor)# cache type normal`	フロー モニタの追加キャッシュ パラメータを設定するには、ステップ 5 を繰り返します。
ステップ 7	**exporter** TestNetFlowExporterName 例： `Switch(config-flow-monitor)# exporter TestNetFlowExporterName`	（任意）事前に作成されたエクスポータの名前を指定します。
ステップ 8	**cache** {timeout [active| inactive|update] (seconds) | type (normal)} 例： `Switch(config-flow-monitor)# cache type normal`	フロー モニタの追加キャッシュ パラメータを設定するには、ステップ 5 を繰り返します。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Switch(config)# flow monitor FLOW-MONITOR-1
Switch(config-flow-monitor)# Used for ipv6 traffic analysis
Switch(config-flow-monitor)# record FLOW-RECORD-1
Switch(config-flow-monitor)# cache timeout active 300
Switch(config-flow-monitor)# cache type normal
Switch(config-flow-monitor)# exporter EXPORTER-1
Switch(config-flow-monitor)# exit
```

次の作業

インターフェイスへのフロー モニタの適用

関連トピック

カスタマイズしたフロー レコードの設定，（186 ページ）
フロー エクスポータの設定，（189 ページ）
IPv6 Netflow，（185 ページ）
インターフェイスへのフロー モニタの適用，（197 ページ）
フロー サンプリングの設定およびイネーブル化，（199 ページ）

インターフェイスへのフロー モニタの適用

次の手順を使用して、インターフェイスに NetFlow モニタを設定します。

手順の概要

1. **configure terminal**
2. **interface** interface-id
3. **wlan** ssid
4. [ip | ipv6 | datalink] **flow monitor** monitor -name **sampler** [sampler | input | output]
5. **exit**
6. ステップ 2 および 3 を繰り返します。
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** interface-id 例： `Switch(config)# interface tengigabitEthernet 1/0/1`	インターフェイスを指定し、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。 Flexible NetFlow は、サービス モジュールの 1 ギガビットまたは 10 ギガビット イーサネット インターフェイスのみでサポートされます。 （注） 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。

	コマンドまたはアクション	目的
ステップ 3	**wlan** ssid 例： `Switch (config)# wlan test 1 test`	WLAN のフロー モニタを設定します。
ステップ 4	[ip | ipv6 | datalink] **flow monitor** monitor -name **sampler** [sampler | input | output] 例： `Switch(config-if)# ipv6 flow monitor SampleMonitorName input`	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。 • ip：IPv4 IP アドレスに一致するレコードを入力します。 • ipv6：IPv6 IP アドレスに一致するレコードを入力します。 （注） このキーワードは、デュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートがスイッチに設定されている場合にだけ表示されます。 • 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。 • sampler：（任意）フロー モニタ サンプラーを適用します。

ステップ 5	**exit**
	
	例：
	`Switch(config-if)# exit`
	`Switch(config)#`
		グローバル コンフィギュレーション モードに戻ります。

ステップ 6	ステップ 2 および 3 を繰り返します。 例：	フロー モニタの追加キャッシュ パラメータを設定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Switch(config)# interface tengigabitethernet 1/0/1
Switch(config-if)# ip flow monitor FLOW-MONITOR-1 input
Switch(config-if)# ip flow monitor FLOW-MONITOR-2 output
Switch(config-if)# end
```

関連トピック

カスタマイズしたフロー レコードの設定，（186 ページ）
フロー エクスポータの設定，（189 ページ）
カスタマイズしたフロー モニタの設定，（195 ページ）

IPv6 Netflow, （185 ページ）
フロー サンプリングの設定およびイネーブル化 , （199 ページ）

フロー サンプリングの設定およびイネーブル化

次の手順を使用して、フロー サンプリングを設定してイネーブルにします。

手順の概要

1. **configure terminal**
2. **sampler** sampler -name
3. **description** description
4. **mode** {deterministic|random} (<1-1>)**out-of** <2-1024>
5. **end**
6. **interface** interface-id
7. **wlan** ssid
8. {ip | ipv6 | datalink] **flow monitor** monitor-name **sampler** sampler-name {input | output}
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**sampler** sampler -name 例： `Switch(config)# sampler SampleNameForSAMPLER`	フロー モニタを作成し、Flexible NetFlow サンプラー コンフィギュレーション モードを開始します。 このコマンドを使用して既存のサンプラーを変更することもできます。
ステップ 3	**description** description 例： `Switch(config-sampler)#description SamplerName_1`	（任意）サンプラーの説明を設定します。
ステップ 4	**mode** {deterministic|random} (<1-1>)**out-of** <2-1024> 例： `Switch(config-sampler)#mode random 1 out-of 2`	パケットを選択するモードとウィンドウ サイズを指定します。 ウィンドウ サイズの範囲は 2 ～ 1024 です。 （注） CLI ヘルプには記載されていますが、mode deterministic キーワードはサポートされません。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Switch(config-sampler)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface** interface-id 例： `Switch(config)# interface tengigabitethernet 1/0/1`	インターフェイスを指定し、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。
ステップ 7	**wlan** ssid 例： `Switch(config)# wlan test 1 test`	WLAN のフロー サンプラーを適用するように設定します。
ステップ 8	{ip | ipv6 | datalink] **flow monitor** monitor-name **sampler** sampler-name {input | output} 例： `Switch(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLE-1 input`	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 IPv4 または IPv6 フロー モニタをアクティブにします。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

```
Switch(config)# sampler SAMPLER-1
Switch(config-sampler)# description Sample at 50
Switch(config-sampler)# mode random 1 out-of 2
Switch(config-sampler)# exit
Switch(config)# interface tengigabitethernet 1/0/1
Switch(config)# wlan test 1 test
Switch(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLE-1 input
```

次の作業

NetFlow v9 for IPv6 の設定方法。

関連トピック

カスタマイズしたフロー レコードの設定，（186 ページ）
フロー エクスポータの設定，（189 ページ）
カスタマイズしたフロー モニタの設定，（195 ページ）
インターフェイスへのフロー モニタの適用，（197 ページ）
IPv6 Netflow，（185 ページ）

IPv6 NetFlow の確認

この項では、IPv6 の Netflow 関連の **show** コマンドについて説明します。 次のコマンドが、スイッチ上の Netflow の確認に使用できます。

コマンド	目的
show flow record	フロー レコードのステータスを表示します。
show flow ssid <ssid_name>	SSID インターフェイスの情報を表示します。
show flow monitor {monitor name} {cache|provisioning|statistics}	フロー モニタ情報を表示します。
show flow exporter exporter-name	フロー エクスポータのステータスを表示します。
show flow monitor monitor -name	フロー モニタの現在のステータスを表示します。
show flow interface interface-id	Flexible NetFlow がインターフェイスに設定されていることを確認します。
show flow monitor monitor -name cache format [csv | record | table}	フロー モニタ キャッシュ内のデータを表示します。
show sampler sampler -name	フローサンプラーの現在のステータスを表示します。

IPv6 NetFlow のモニタリング

このセクションでは、IPv6 の Netflow コマンドについて説明します。次のコマンドを使用して、スイッチ上の NetFlow をモニタリングできます。

コマンド	目的
show running-config flow record	設定済みフロー レコードを表示します。
show running-config flow exporter exporter-name	設定済みフロー エクスポータを確認します。
show running-config flow monitor monitor -name	フロー モニタ設定を確認します。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	*IPv6 コマンド リファレンス (Catalyst 3650 スイッチ)*
Flexible NetFlow コマンド リファレンス	*Cisco Flexible NetFlow Command Reference (Catalyst 3650 Switches)*
Flexible NetFlow 設定	*Cisco Flexible NetFlow Configuration Guide (Catalyst 3650 Switches)*

エラー メッセージ デコーダ

説明	リンク
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB のダウンロードには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングに役立てていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 NetFlow の機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 NetFlow 機能	Cisco IOS XE 3.3SE	この機能が導入されました。

索 引

数字

A

C

D

E

I

M

O

R

S

T

あ

い

お

き

く

こ

さ

し

す

せ

そ

た

て

と

ね

は

ふ

へ

ま

も

り

る

れ