Catalyst 2960-X スイッチ IPv6 コンフィギュレーション ガイド、Cisco IOS Release 15.0(2)EX

初版：2013 年 07 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-29036-01-J

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

© 2013 Cisco Systems, Inc. All rights reserved.

目 次

はじめに vii

表記法 vii

関連資料 ix

マニュアルの入手方法およびテクニカル サポート ix

コマンドライン インターフェイスの使用 1

コマンドライン インターフェイスの使用に関する情報 1

コマンド モード 1

ヘルプ システムの使用 5

コマンドの省略形 6

コマンドの no 形式および default 形式 6

CLI のエラー メッセージ 6

コンフィギュレーション ロギング 7

CLI を使用して機能を設定する方法 8

コマンド履歴の設定 8

コマンド履歴バッファ サイズの変更 8

コマンドの呼び出し 8

コマンド履歴機能のディセーブル化 9

編集機能のイネーブル化およびディセーブル化 9

キーストロークによるコマンドの編集 10

画面幅よりも長いコマンドラインの編集 12

show および more コマンド出力の検索およびフィルタリング 13

コンソール接続または Telnet による CLI アクセス 13

MLD スヌーピングの設定 15

機能情報の確認 15

IPv6 MLD スヌーピングの設定に関する情報 15

MLD スヌーピングの概要 16

MLD メッセージ 17
MLD クエリー 17
マルチキャスト クライアント エージングの堅牢性 18
マルチキャスト ルータ検出 18
MLD レポート 19
MLD Done メッセージおよび即時脱退 19
TCN 処理 20
スイッチ スタックでの MLD スヌーピング 20
IPv6 MLD スヌーピングの設定方法 20
MLD スヌーピングのデフォルト設定 20
MLD スヌーピング設定時の注意事項 21
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 22
VLAN に対する MLD スヌーピングのイネーブル化またはディセーブル化 23
スタティックなマルチキャスト グループの設定 24
マルチキャスト ルータ ポートの設定 25
MLD 即時脱退のイネーブル化 26
MLD スヌーピング クエリーの設定 26
MLD リスナー メッセージ抑制のディセーブル化 28
MLD スヌーピング情報の表示 29
MLD スヌーピングの設定例 31
スタティックなマルチキャスト グループの設定：例 31
マルチキャスト ルータ ポートの設定：例 31
MLD 即時脱退のイネーブル化：例 31
MLD スヌーピング クエリーの設定：例 31
IPv6 ユニキャスト ルーティングの設定 33
機能情報の確認 33
IPv6 ホスト機能の設定に関する情報 33
IPv6 の概要 34
IPv6 形式のアドレス 34
サポート対象の IPv6 ユニキャスト ルーティング機能 35
128 ビット幅のユニキャスト アドレス 35
IPv6 の DNS 36

ICMPv6 36
ネイバー探索 36
IPv6 のステートレス自動設定および重複アドレス検出 36
IPv6 アプリケーション 37
IPv4 と IPv6 の二重プロトコル スタック 37
IPv6 による SNMP と Syslog 38
IPv6 による HTTP（S） 39
IPv6 とスイッチ スタック 39
IPv6 のデフォルト設定 39
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 40
IPv6 ICMP レート制限の設定 42
IPv6 のスタティック ルーティングの設定 44
IPv6 の表示 46
IPv6 ユニキャスト ルーティングの設定例 47
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 47
IPv6 ICMP レート制限の設定：例 48
IPv6 のスタティック ルーティングの設定：例 48
IPv6 の表示：例 48
IPv6 ACL の設定 49
機能情報の確認 49
IPv6 ACL の設定に関する情報 49
IPv6 ACL の概要 50
サポートされる ACL 機能 50
IPv6 ACL の制限事項 51
IPv6 ACL の設定 52
IPv6 ACL のデフォルト設定 52
他の機能およびスイッチとの相互作用 52
IPv6 ACL の作成 53
インターフェイスへの IPv6 ACL の適用 57
IPv6 ACL の表示 58
IPv6 ACL の設定例 58
例：IPv6 ACL の作成 58

例：IPv6 ACL の適用 **58**

例：IPv6 ACL の表示 **59**

はじめに

ここでは、次のトピックを扱います。

- 表記法，vii ページ
- 関連資料，ix ページ
- マニュアルの入手方法およびテクニカル サポート，ix ページ

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。
太字の **`courier`** フォント	**太字の `courier`** フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。

表記法	説明
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[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 安全上の重要事項

「危険」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。 機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。 各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。 （日本語版は削除）

これらの注意事項を保管しておいてください。

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、リリース ノートを参照してください。

- 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

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，1 ページ
- CLI を使用して機能を設定する方法，8 ページ

コマンドライン インターフェイスの使用に関する情報

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

コマンド モード

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 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。
`% Incomplete command.`	コマンドに必須のキーワードまたは値が、一部入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。
`% Invalid input detected at '^' marker.`	コマンドの入力ミスです。 間違っている箇所をキャレット（^）記号で示しています。	疑問符（?）を入力すると、そのコマンド モードで使用できるすべてのコマンドが表示されます。 コマンドとともに使用できるキーワードが表示されます。

コンフィギュレーション ロギング

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 セッションにおけるこの機能をディセーブルにします。

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、ディセーブルにして再びイネーブルにできます。

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イネーブルにします。
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ディセーブルにします。

キーストローク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 行分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。

コンソール接続または Telnet による CLI アクセス

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

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

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，15 ページ
- IPv6 MLD スヌーピングの設定に関する情報，15 ページ
- IPv6 MLD スヌーピングの設定方法，20 ページ
- MLD スヌーピング情報の表示，29 ページ
- MLD スヌーピングの設定例，31 ページ

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

（注） この IPv6 MLD スヌーピングを使用するには、スイッチが LAN Base イメージを実行している必要があります。

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） スタック構成をサポートしているのは、LAN Base イメージを実行している Catalyst 2960-X スイッチだけです。

（注） Catalyst 2960-X 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。

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。

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。

機能	デフォルト設定
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	イネーブル

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 スタックに保持可能なアドレス エントリの最大数は 1000 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

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。

	コマンドまたはアクション	目的
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 に対する MLD スヌーピングのイネーブル化またはディセーブル化

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。

スタティックなマルチキャスト グループの設定

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*	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。

	コマンドまたはアクション	目的

	例：
	`Switch# show ipv6 mld snooping address`
	または
	`Switch# show ipv6 mld snooping vlan 1`	

マルチキャスト ルータ ポートの設定

（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。

	コマンドまたはアクション	目的
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 即時脱退のイネーブル化

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

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。
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。

	コマンドまたはアクション	目的
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 メッセージ抑制のディセーブル化

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。
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。

コマンド	目的
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。
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 3 章

IPv6 ユニキャスト ルーティングの設定

- 機能情報の確認，33 ページ
- IPv6 ホスト機能の設定に関する情報，33 ページ
- IPv6 ユニキャスト ルーティングの設定例，47 ページ

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 ホスト機能の設定に関する情報

この章では、Catalyst 2960、2960-S、2960-C、2960-X スイッチで IPv6 ホスト機能を設定する方法について説明します。

（注） IPv6 ホスト機能を使用するには、スイッチが LAN Base イメージを実行している必要があります。

IPv6 Multicast Listener Discovery（MLD）スヌーピングの設定については、*MLD* スヌーピング設定を参照してください。

Catalyst 2960 スイッチでデュアル スタック環境（IPv4 と IPv6 の両方をサポートする）をイネーブルにするには、スイッチング データベース管理（SDM）テンプレートをデュアル IPv4 および IPv6

テンプレートに設定する必要があります。 「デュアル IPv4 および IPv6 プロトコル スタック」の章を参照してください。 このテンプレートは、Catalyst 2960-S スイッチではサポートされません。

（注） この章で使用しているコマンドの完全な構文と使用方法については、手順の中で参照している Cisco IOS のマニュアルを参照してください。

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。 スイッチはサイトローカルなユニキャスト アドレス、エニキャスト アドレス、またはマルチキャスト アドレスをサポートしません。

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。

「Implementing Addressing and Basic Connectivity」の章では、次の項の内容がCatalyst 2960、2960-S、2960-C、2960-X スイッチに適用されます。

- IPv6 アドレス形式
- 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

スイッチでは、拡張アドレス機能、ヘッダー フォーマットの単純化、拡張子およびオプションのサポートの改善、および拡張ヘッダーのハードウェア解析などがサポートされています。 また、ホップ単位の拡張ヘッダー パケットもサポートし、これらをソフトウェアでルーティングまたはブリッジングします。

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。

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。

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、および Telnet
- 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

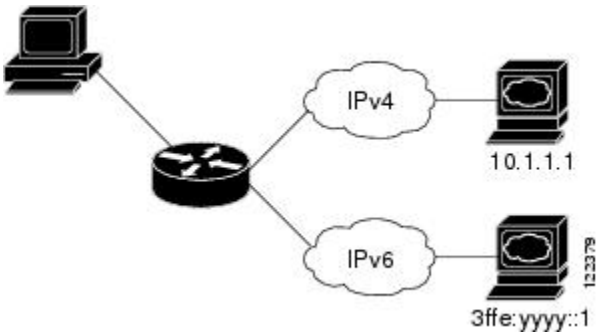
これらのアプリケーションの管理の詳細については、Cisco.com から『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章および「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

IPv4 と IPv6 の二重プロトコル スタック

Catalyst 2960-X スイッチで、IPv4 および IPv6 プロトコルの両方で Ternary Content Addressable Memory（TCAM）の使用を割り当てるには、デュアル IPv4/IPv6 テンプレートを使用する必要があります。

この図に、IP パケットおよび宛先アドレスに基づいて、同じインターフェイスを介して IPv4 および IPv6 トラフィックを転送するルータを示します。

図 *1*：インターフェイス上での *IPv4/IPv6* のデュアル サポート



デュアル IPv4 および IPv6 スイッチ データベース管理（SDM）テンプレートを使用して、IPv6 のルーティング デュアル スタック環境（IPv4 および IPv6 の両方をサポートする）をイネーブルにします。デュアル IPv4/IPv6 SDM テンプレートの詳細については、「*SDM* テンプレートの設定」を参照してください。

デュアル IPv4 および IPv6 テンプレートを使用すると、デュアル スタック環境でスイッチを使用できるようになります。

- デュアル IPv4/IPv6 テンプレートを最初に選択しないで IPv6 を設定しようとすると、警告メッセージが表示されます。

- IPv4 専用環境のスイッチは、IPv4 パケットをルーティングし、IPv4 の QoS および ACL をハードウェアで適用します。 IPv6 パケットはサポートされません。
- デュアル IPv4/IPv6 環境で、スイッチは IPv4 QoS および ACL をハードウェアで適用します。
- IPv6 QoS および ACL はサポートされていません。
- デュアル スタック テンプレートを使用すると、各リソースのハードウェア メモリ容量が少なくなるため、IPv6 を使用する予定がない場合はこのテンプレートを使用しないでください。

IPv4/IPv6 プロトコル スタックについての詳細は、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 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。

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 マスターにより、IPv6 ホスト機能および IPv6 アプリケーションが実行されます。

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 ホストのイネーブル化」の章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。 詳細については、「スイッチ スタックの管理」の「永続的な MAC アドレスのイネーブル化」の章を参照してください。

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	デフォルト デスクトップ
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

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。

- 必ずデュアル IPv4/IPv6 SDM テンプレートを選択してください。
- **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

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。

IPv6 アドレスをレイヤ 3 インターフェイスに割り当てて IPv6 転送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。

	コマンドまたはアクション	目的
ステップ 2	**sdm prefer dual-ipv4-and-ipv6** {**default**} 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。 • **default**：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。
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。
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**	• 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。

	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。
		• 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 8	**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 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**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 11	**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

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。

手順の概要

1. **configure terminal**
2. **ipv6 icmp error-interval** *interval* [*bucketsize*]
3. **end**
4. **show ipv6 interface** [*interface-id*]
5. **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 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 dhcp 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 のスタティック ルーティングの設定

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* [*ipv6-address*]} [*administrative distance*] 例： `Switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet2/0/1 130`	スタティック IPv6 ルートを設定します。 • *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。

	コマンドまたはアクション	目的
		（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。
	• **show ipv6 static** [*ipv6-address* | *ipv6-prefix/prefix length*] [**interface** *interface-id*] [**recursive**] [**detail**]
	• **show ipv6 route static** [*updated*]
	例：
	`Switch# show ipv6 static 2001:0DB8::/32 interface gigabitethernet2/0/1 130`
	または
	`Switch# show ipv6 route static`
		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。
		• **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。

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 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 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 route	IPv6 ルート テーブル エントリを表示します。
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* : ***IPv4*** および ***IPv6*** のアドレス タイプの表示用コマンド

コマンド	目的
show ip http server history	アクセスした IP アドレス、接続が終了したときの時間を含む、最近 20 回の HTTP サーバへの接続を表示します。
show ip http server connection	アクセスしているローカルおよびリモート IP アドレスを含む、HTTP サーバへの現在の接続を表示します。

コマンド	目的
show ip http client connection	HTTP サーバへの HTTP クライアント接続の設定値を表示します。
show ip http client history	サーバに対して HTTP クライアントが行った最後の 20 回の要求のリストを表示します。

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)# sdm prefer dual-ipv4-and-ipv6 default

Switch(config)# interface gigabitethernet1/0/11

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.
```

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 4 章

IPv6 ACL の設定

- 機能情報の確認，49 ページ
- IPv6 ACL の設定に関する情報，49 ページ
- IPv6 ACL の設定，52 ページ
- IPv6 ACL の設定例，58 ページ

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 ACL の設定に関する情報

IP バージョン 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 バージョン 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。 レイヤ 3 管理トラフィックをフィルタリングするために、入力ルータ ACL を作成し、適用することもできます。

（注） IPv6 を使用するには、デュアル IPv4 および IPv6 スイッチング データベース管理（SDM）テンプレートがスイッチに設定されている必要があります。 テンプレートの選択は、**sdm prefer {default | dual-ipv4-and-ipv6}** グローバル コンフィギュレーション コマンドで行います。

（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。

IPv6 ACL の概要

スイッチ イメージは、次の 2 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL：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送信トラフィックまたは着信トラフィックでサポートされます。 経路選択済みの IPv6 パケットだけに適用されます。

- IPv6 ポート ACL：レイヤ 2 インターフェイスの着信トラフィックでだけサポートされます。インターフェイスに届くすべての IPv6 パケットに適用されます。

（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。

サポートされる ACL 機能

スイッチの IPv6 ACL には、次の特性があります。

- 分割フレーム（IPv4 では fragments キーワード）がサポートされます。
- IPv6 ACL では、IPv4 と同じ統計情報がサポートされます。
- スイッチの Ternary CAM（TCAM）スペースが不足している場合、ACL ラベルに対応付けられたパケットは CPU に転送され、ACL はソフトウェアで適用されます。
- ホップバイホップ オプションがあるルーテッド パケットまたはブリッジド パケットには、ソフトウェアで適用される IPv6 ACL が設定されます。
- ロギングは、ルータ ACL ではサポートされますが、ポート ACL ではサポートされません。

IPv6 ACL の制限事項

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。

- IPv6 送信元および宛先アドレス：ACL 照合は、Extended Universal Identifier（EUI）-64 形式の /0 ～/64 のプレフィックスおよびホスト アドレス（/128）だけでサポートされます。 スイッチは、情報損失のない次のホスト アドレスだけをサポートします。

  集約グローバル ユニキャスト アドレス

  リンク ローカル アドレス

- 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。
- スイッチは再起 ACL（**reflect** キーワード）をサポートしません。
- このリリースが IPv6 用にサポートしているのは、ポート ACL およびルータ ACL だけです。 VLAN ACL（VLAN マップ）はサポートしていません。
- スイッチは IPv6 フレームに MAC ベース ACL を適用しません。
- レイヤ 2 EtherChannel に IPv6 ポート ACL を適用できません。
- スイッチは出力ポート ACL をサポートしません。
- IPv6 の出力ルータ ACL および入力ポート ACL は、だけでサポートされます。 スイッチは、コントロール プレーン（着信）IPv6 ACL だけをサポートします。
- 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接続されている ACL に ACE が追加されるのを許可しません。

IPv6 ACL の設定

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。

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

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	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。

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	**ipv6access-list***access-list-name* 例： `ipv6 access-list access-list-name`	IPv6 アクセス リスト名を定義し、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。

	コマンドまたはアクション	目的
		• 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。

	コマンドまたはアクション	目的
		• （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。 • （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。

	コマンドまたはアクション	目的
ステップ 6	**{deny|permit} icmp** 例： `{deny | permit} icmp {source-ipv6-prefix/prefix-length | any | 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]`	（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 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。

インターフェイスへの IPv6 ACL 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 3 インターフェイスで発信または着信トラフィックに、あるいはレイヤ 2 インターフェイスで着信トラフィックに ACL を適用できます。

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 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`	ルータ ACL を適用する場合は、インターフェイスをレイヤ 2 モード（デフォルト）からレイヤ 3 モードに変更します。
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。 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。
ステップ 5	**ipv6 traffic-filter** *access-list-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。 **out** キーワードはレイヤ 2インターフェイス（ポート ACL）ではサポートされません。
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**	アクセス リストの設定を確認します。
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。

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。
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。

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。

```
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
```

索 引

数字

128 ビット 34

A

ACL 49

D

DNS 36
　IPv6 36

E

EUI 35
「EUI」を参照 35
Extended Universal Identifier 35
　「EUI」を参照 35

I

ICMP 36
　IPv6 36
ICMPv6 36
IGMP 26, 28, 29
　スヌーピング 29
　脱退処理、イネーブル化 26
　レポート抑制 28
　　ディセーブル化 28
IGMP スヌーピング 20, 21, 22, 29
　イネーブル化またはディセーブル化 22
　デフォルト設定 20, 21
　モニタリング 29
IPv4 および IPv6 37
IPv6 15, 34, 35, 36, 37, 39, 40, 46, 49
　ACL 49
　ICMP 36
　SDM テンプレート 15
　アドレス 34
　アドレス形式 34
　アドレスの割り当て 40
　アプリケーション 37
　サポートされる機能 35
　自動設定 36
　スタック マスターは、次に示す機能を実行します。 39
　ステートレス自動設定 36
　定義 34
　デフォルト設定 39
　とスイッチ スタック 39
　ネイバー探索 36
　フォワーディング 40
　モニタリング 46
IPv6 ICMP レート制限の設定：コマンド例 48
IPv6 アドレスの割り当て 40
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：コマンド例 47
IPv6 による HTTP（S） 39
IPv6 による SNMP と Syslog 38
IPv6 のスタティック ルーティングの設定：コマンド例 48
IPv6 の表示：コマンド例 48
IPv6 ルーティング 39
「IPv6」を参照 34
IP アドレス 34
　128 ビット 34
　IPv6 34
IP ユニキャスト ルーティング 35
　IPv6 35
ISL 35
　および IPv6 35

M

MLDv1 Done メッセージ 19
MLD クエリー 17
MLD スヌーピング 16
MLD スヌーピング クエリー コマンドの設定例 31
MLD スヌーピング クエリーの設定：コマンド例 31
MLD 即時脱退のイネーブル化：コマンド例 31
MLD メッセージ 17
MLD レポート 19

S

SDM テンプレート 15
SDM テンプレートのサポート 37

T

TCN 処理 20

あ

アドレス 34
　IPv6 34
アドレス形式 34
アドレスの割り当て 40
アプリケーション 37

い

イネーブル化 26
イネーブル化またはディセーブル化 22
インターネット プロトコル バージョン 6 34
　「IPv6」を参照 34

お

および IPv6 35

こ

コンフィギュレーション コマンド例 47

さ

サポートされる機能 35

し

自動設定 36
集約グローバル ユニキャスト アドレス 35

す

スイッチ スタック 20
スタック、スイッチ 39
　IPv6 39
スタックの変更 39
　への効果 39
　　IPv6 ルーティング 39
スタック マスター 39
　IPv6 39
スタック マスターは、次に示す機能を実行します。 39
スタック メンバ 39
　IPv6 39
スタティック結合 24
スタティックなマルチキャスト グループの設定：コマンド例 31
ステートレス自動設定 36
スヌーピング 29

そ

即時脱退、IGMP 26
　イネーブル化 26

た

脱退処理、イネーブル化 26

て

定義 34
ディセーブル化 28
デフォルト設定 20, 21, 39
　IGMP スヌーピング 20, 21
　IPv6 39

デュアル IPv4/IPv6 テンプレート 37
デュアル プロトコル スタック 37
IPv4 および IPv6 37
SDM テンプレートのサポート 37

と

とスイッチ スタック 39

ね

ネイバー探索 36
ネイバー探索、IPv6 36

ふ

フォワーディング 40

へ

への効果 39
IPv6 ルーティング 39

ま

マルチキャスト クライアント エージングの堅牢性 18
マルチキャスト グループ 24
スタティック結合 24
マルチキャスト ルータ検出 18
マルチキャスト ルータ ポートの設定：コマンド例 31

も

モニタリング 29, 46
IGMP 29
スヌーピング 29
IPv6 46

り

リンク ローカル ユニキャスト アドレス 35

れ

レイヤ 3 インターフェイス 40
IPv6 アドレスの割り当て 40
レポート抑制 28
ディセーブル化 28
レポート抑制、IGMP 28
ディセーブル化 28