Cisco IOS XE Everest 16.6x（Catalyst 9300 スイッチ）IPv6 コンフィギュレーション ガイド

初版：2017 年 07 月 31 日

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

【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。

目 次

第 1 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。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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 Cisco 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。特に指示がないかぎり、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。

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。

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、*Command Reference (Catalyst 9500 Series Switches)*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、2960-X、または 2960-CX 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。

トポロジ変更通知処理

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。

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 *1*：*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）	有効。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。

機能	デフォルト設定
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 スタックに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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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： `Device(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： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config** 例： `Device(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： `Device(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 スヌーピングのイネーブル化またはディセーブル化（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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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： `Device(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： `Device(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： `Device(config)# ipv6 mld`	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
	`snooping vlan 1`	

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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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： `Device(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。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Device(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：
	`Device# show ipv6 mld snooping address`
	または
	`Device# 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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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 vlan** *vlan-id* **mrouter interface** *interface-id* 例： `Device(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。指定できるポートチャネルの範囲は 1 ～ 48 です。
ステップ 3	**end** 例： `Device(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： `Device# 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（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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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： `Device(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。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Device(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： `Device# 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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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： `Device(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： `Device(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。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 mld snooping last-listener-query-count** *count* 例： `Device(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： `Device(config)# ipv6 mld snooping vlan 1 last-listener-query-count 7`	（任意）VLAN 単位でラストリスナー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** 間隔 例： `Device(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： `Device(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： `Device(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： `Device(config)# ipv6 mld snooping tcn flood query count`	（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。

	コマンドまたはアクション	目的
	5	
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： `Device(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（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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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： `Device(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： `Device(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** 例： `Device# 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 *2*：*MLD* スヌーピング情報表示用のコマンド

コマンド（Command）	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（Command）	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。

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

          1/0/1
Device(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。

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

          0/2
Device(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。

```
Device# configure terminal
Device(config)# ipv6 mld snooping vlan 130 immediate-leave
Device(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。

```
Device# configure terminal
Device(config)# ipv6 mld snooping robustness-variable 3
Device(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。

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

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

第 2 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。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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 Cisco 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 Network Advantage ライセンスを実行している必要があります。Network Essentials ライセンスを実行しているスイッチは、IPv6 スタティック ルーティングと IPv6 用の RIP をサポートしています。Network Advantage ライセンスを実行しているスイッチは、IPv6 に対し OSPF、EIGRP および BGP をサポートしています。

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 アドレス

スイッチがサポートするのは、IPv6 ユニキャスト アドレスのみです。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 http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-3e/ip6b-xe-3e-book.html 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

ここでは、スイッチでサポートされている IPv6 プロトコル機能について説明します。

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。

デフォルト ルータ プリファレンス

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 を使用すると、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 Configuration Guide*』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。

IPv6 のポリシーベース ルーティング

ポリシーベース ルーティング（PBR）は、トラフィック フローに定義ポリシーを設定し、ルートにおけるルーティング プロトコルへの依存度を軽くして、パケットのルーティングを柔軟に行えるようにします。したがって、PBR は、ルーティング プロトコルで提供される既存のメカニズムを拡張および補完することにより、ルーティングの制御を強化します。PBR を使用すると、IPv6 precedence を設定できます。単純なポリシーでは、これらのタスクのいずれかを使用し、複雑なポリシーでは、これらすべてのタスクを使用できます。高コストリンク上のプライオリティ トラフィックなど、特定のトラフィックのパスを指定することもできます。

PBR for IPv6 は、転送される IPv6 パケットおよび送信される IPv6 パケットの両方に適用できます。転送されるパケットの場合、PBR for IPv6 は、次の転送パスでサポートされる IPv6 入力インターフェイス機能として実装されます。

- プロセス
- シスコ エクスプレス フォワーディング（旧称 CEF）
- 分散型シスコ エクスプレス フォワーディング

ポリシーは、IPv6 アドレス、ポート番号、プロトコル、またはパケットのサイズに基づいて作成できます。

PBR を使用すると、次の作業を実行できます。

- 拡張アクセス リスト基準に基づいてトラフィックを分類する。リストにアクセスし、次に一致基準を設定します。
- 差別化されたサービス クラスをイネーブルにする機能をネットワークに与える IPv6 precedence ビットを設定する。
- 特定のトラフィック エンジニアリング パスにパケットをルーティングする。ネットワークを介して特定の Quality of Service（QoS）を得るためにパケットをルーティングする必要がある場合があります。

PBR を使用すると、ネットワークのエッジでパケットを分類およびマーキングできます。PBR では、precedence 値を設定することにより、パケットをマーキングします。precedence 値は、ネットワーク コアにあるデバイスが適切な QoS をパケットに適用するために直接使用でき、これにより、パケットの分類がネットワーク エッジで維持されます。

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 セットを実行しているスイッチは、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。

IPv6 の HSRP の設定

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。

（注） IPv6 の HSRP を設定する場合、インターフェイス上で HSRP version 2（HSRPv2）をイネーブルにする必要があります。

EIGRP IPv6

スイッチは、IPv6 の Enhanced Interior Gateway Routing Protocol（EIGRP）をサポートしています。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。IP Lite を実行しているスイッチは EIGRPv6 スタブ ルーティングをサポートします。

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 IPv6 アドレスを基にして作成されるため、すべての IPv6 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 ノードのみが含まれるネットワークで稼働するため、使用可能な IPv6 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。

EIGRPv6 スタブ ルーティング

EIGRPv6 スタブ ルーティング機能は、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの利用率を低減させます。

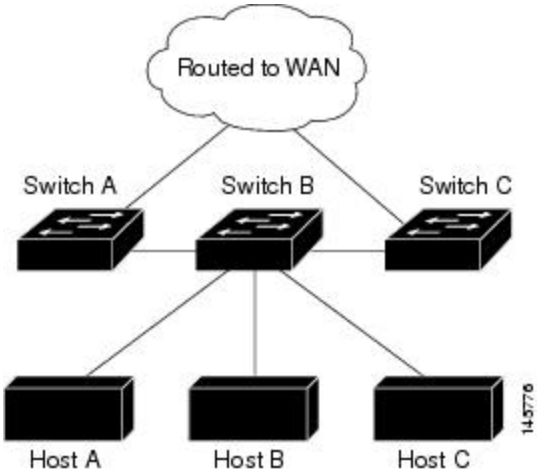
EIGRPv6 スタブ ルーティングを使用するネットワークでは、ユーザに対する IPv6 トラフィックの唯一の許容ルートは、EIGRPv6 スタブ ルーティングを設定しているスイッチ経由です。スイッチは、ユーザ インターフェイスとして設定されているインターフェイスまたは他のデバイスに接続されているインターフェイスにルーテッド トラフィックを送信します。

EIGRPv6 スタブ ルーティングを使用しているときは、EIGRPv6 を使用してスイッチだけをスタブとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。指定したルートだけがスイッチから伝播されます。スイッチは、サマリー、接続ルート、およびルーティング アップデートに対するすべてのクエリーに応答します。

スタブ ルータの状態を通知するパケットを受信した隣接ルータは、ルートについてはスタブ ルータに照会しません。また、スタブ ピアを持つルータは、そのピアについては照会しません。スタブ ルータは、ディストリビューション ルータを使用して適切なアップデートをすべてのピアに送信します。

次の図では、スイッチ B は EIGRPv6 スタブ ルータとして設定されています。スイッチ A および C は残りの WAN に接続されています。スイッチ B は、接続ルート、スタティック ルート、再配信ルート、およびサマリー ルートをスイッチ A と C にアドバタイズします。 スイッチ B は、スイッチ A から学習したルートをアドバタイズしません（逆の場合も同様です）。

図 *1*：*EIGRP* スタブ ルータ設定



EIGRPv6 スタブ ルーティングの詳細については、『*Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols, Release 12.4*』の「Implementing EIGRP for IPv6」を参照してください。

SNMP と Syslog、IPv6 による

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 上の 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 接続を確立するには、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 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
- 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 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。
- スイッチはソースルート IPv6 パケットに関する QoS 分類をハードウェアで適用できません。

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） スタック内で IPv6 パケットを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 セットが稼動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），（30 ページ）

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（IPv6 オプション）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 *3*：*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

機能	デフォルト設定
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	ディセーブル（IPv4 CEF および dCEF はデフォルトでイネーブル） （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 形式のアドレス	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, （28 ページ）
- **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 *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、**noipv6 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は、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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 preferdual-ipv4-and-ipv6** { **advanced** | **vlan**} 例： `Device(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 設定を最大化します。 （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 Base ライセンスでのみ使用できます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**reload** 例： `Device# reload`	オペレーティング システムをリロードします。

	コマンドまたはアクション	目的
ステップ 5	**configureterminal** 例： `Device# 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： `Device(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	**noswitchport** 例： `Device(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*
	
	例：
	`Device(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64`
	
	`Device(config-if)# ipv6 address 2001:0DB8:c18:1::/64`
	
	`Device(config-if)# ipv6 address 2001:0DB8:c18:1::`
		• 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。
		• 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。

	コマンドまたはアクション	目的
	link-local `Device(config-if)# ipv6 enable`	
ステップ 9	**exit** 例： `Device(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： `Device(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	**ipv6unicast-routing** 例： `Device(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： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 13	**show ipv6 interface** *interface-id* 例： `Device# show ipv6 interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 14	**copyrunning-configstartup-config** 例： `Device# 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 アドレスが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

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 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）。

	コマンドまたはアクション	目的
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** • **ipv6 address***WORD* • **ipv6 address***autoconfig* • **ipv6 address***dhcp*	• 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。 • 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。

	コマンドまたはアクション	目的
ステップ 10	**copyrunning-configstartup-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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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： `Device(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： `Device(config-if)# ipv6 nd`	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。

	コマンドまたはアクション	目的
	router-preference medium	
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**showipv6interface** 例： `Device# show ipv6 interface`	設定を確認します。
ステップ 6	**copyrunning-configstartup-config** 例： `Device# 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

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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： `Device(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）。有効な範囲は 0 ～ 2147483647 ミリ秒です。

	コマンドまたはアクション	目的
		• *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： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 4	**show ipv6 interface** [*interface-id*] 例： `Device# show ipv6 interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 5	**copyrunning-configstartup-config** 例： `Device# 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、ハードウェアによって distributed CEF（dCEF）が使用されます。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 は自動的にディセーブルになります。IPv6 CEF および dCEF は、設定中にディセーブルにできません。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

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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： `Device(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 進値の前にスラッシュ記号を付ける必要があります。 • *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

	コマンドまたはアクション	目的
		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： `Device(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*] [**detail**]][**recursive**] [**detail**] • **show ipv6 route static** [*updated*]	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。

	コマンドまたはアクション	目的

	例：
	`Device# show ipv6 static 2001:0DB8::/32 interface gigabitethernet2/0/1`
	または
	`Device# show ipv6 route static`
		• **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	**copyrunning-configstartup-config** 例： `Device# 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。

インターフェイスでの IPv6 PBR の有効化

IPv6 のポリシーベース ルーティング（PBR）を有効にするには、パケットの一致基準と目的のポリシールーティングアクションを指定する、ルートマップを作成する必要があります。次に、そのルート マップを必要なインターフェイスに関連付けます。指定されたインターフェイスに到着し、match 句に一致するすべてのパケットに対して、PBR が実行されます。

PBR では、**setvrf** コマンドにより Virtual Routing and Forwarding（VRF）インスタンスとインターフェイス アソシエーションを切り離し、既存の PBR またはルート マップ設定を使用して、アクセス コントロール リスト（ACL）ベースの分類に基づいて VRF を選択できるようになります。このコマンドは、1 つのルータに複数ルーティング テーブルを提供し、ACL 分類に基づいてルートを選択できるようにします。ルータは、ACLに基づいてパケットを分類し、ルーティングテーブルを選択し、宛先アドレスを検索し、パケットをルーティングします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map rip-to-ospf permit`	ルーティング プロトコル間でルートを再配布する条件を定義するか、ポリシー ルーティングを有効にしてルートマップ 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	次のいずれかを実行します。
	• **matchlength***minimum-length maximum-length*
	• **matchipv6address** {**prefix-list** *prefix-list-name* | *access-list-name*}
	
	例：
	
	`Device(config-route-map)# match length 3 200`
	
	例：
	
	`Device(config-route-map)# match ipv6 address marketing`
		一致基準を指定します。
		• 次のうちの任意の項目またはすべてを指定できます。
		• レベル 3 のパケット長とのマッチング。
		• 指定された IPv6 アクセス リストとのマッチング。
		• **match** コマンドを指定しない場合、ルートマップはすべてのパケットに適用されます。

ステップ 5	次のいずれかを実行します。 • **setipv6precedence** *precedence-value* • **setipv6next-hop***global-ipv6-address* [*global-ipv6-address...*] • **setinterface** *type number* [*...type number*] • **setipv6defaultnext-hop** *global-ipv6-address* [*global-ipv6-address...*] • **setdefaultinterface** *type number* [*...type number*] • **setvrf** *vrf-name*	基準に一致したパケットに適用するアクション（1 つまたは複数）を指定します。 • 次のうちの任意の項目またはすべてを指定できます。 • IPv6 ヘッダーに precedence 値を設定します。 • パケットのルーティング先となるネクストホップを設定します（ネクストホップは隣接している必要があります）。 • パケットの出力インターフェイスを設定します。

	コマンドまたはアクション	目的

	例：
	`Device(config-route-map)# set ipv6 precedence 1`
	例：
	`Device(config-route-map)# set ipv6 next-hop 2001:DB8:2003:1::95`
	例：
	`Device(config-route-map)# set interface GigabitEthernet 0/0/1`
	例：
	`Device(config-route-map)# set ipv6 default next-hop 2001:DB8:2003:1::95`
	例：
	`Device(config-route-map)# set default interface GigabitEthernet 0/0/0`
	例：
	`Device(config-route-map)# set vrf vrfname`
		• 宛先への明示的なルートがない場合に、パケットのルーティング先となるネクスト ホップを設定します。
		• 宛先への明示的なルートがない場合に、パケットの出力インターフェイスを設定します。
		• ポリシーベース ルーティング VRF の選択のために、ルートマップ内に VRF インスタンス選択を設定します。

ステップ 6	**exit** 例： `Device(config-route-map)# exit`	ルート マップ 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。
ステップ 7	**interface** *type number* 例： `Device(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、ルータ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 8	**ipv6policyroute-map** *route-map-name* 例： `Device(config-if)# ipv6 policy-route-map interactive`	インターフェイスで IPv6 PBR に使用するルート マップを特定します。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-if)# end`	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、特権 EXEC モードに戻ります。

ローカル PBR for IPv6 の有効化

デバイスが生成したパケットに対して、通常はポリシーによるルーティングは行われません。これらのパケットのためのローカル IPv6 ポリシーベース ルーティング（PBR）をイネーブルにするには、この作業を実行して、どのルート マップをデバイスで使用するべきかを示します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# 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	**ipv6localpolicyroute-map** *route-map-name* 例： `Device(config)# ipv6 local policy route-map pbr-src-90`	デバイスによって生成されるパケットに対する IPv6 PBR を設定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

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

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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** 名前 例： `Device(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： `Device(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： `Device(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： `Device(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。

	コマンドまたはアクション	目的
ステップ 6	**ipv6 rip** 名前**enable** 例： `Device(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： `Device(config-if)# ipv6 rip cisco default-information only`	（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。 （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**：このインターフェイスから送信するアップデートに、デフォルト ルートを格納し、その他のすべてのルートを含めない場合に選択します。 • **originate**：このインターフェイスから送信するアップデートに、デフォルト ルートおよびその他のすべてのルートを格納する場合に選択します。
ステップ 8	**end** 例： `Device(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： `Device# show ipv6 rip cisco interface gigabitethernet2/0/1`	• 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。

	コマンドまたはアクション	目的
	または `Device# show ipv6 rip`	
ステップ 10	**copyrunning-configstartup-config** 例： `Device# 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

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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： `Device(config)# ipv6 router`	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

	コマンドまたはアクション	目的
	ospf 21	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： `Device(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）アドバタイズするアドレス範囲ステータスを設定し、タイプ 3 のサマリー リンクステート アドバタイズメント（LSA）を生成します。 • **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： `Device(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： `Device(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。

	コマンドまたはアクション	目的
ステップ 6	**interface** *interface-id* 例： `Device(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： `Device(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： `Device(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 ospf** [*process-id*] [*area-id*] **interface** [*interface-id*]
	• **show ipv6 ospf** [*process-id*] [*area-id*]
	
	例：
	`Device# show ipv6 ospf 21 interface gigabitethernet2/0/1`
	
	または
	`Device# show ipv6 ospf 21`
		• OSPFインターフェイスに関する情報を表示します。
		• 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	**copyrunning-configstartup-config** 例： `Device# 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 global configuration** 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 global** 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 ユニキャスト リバース パス転送の設定

ユニキャスト リバース パス転送（ユニキャスト RPF）機能は、検証可能な送信元 IP アドレスが不足している IP パケットを廃棄することで、間違ったまたは偽造（スプーフィングされた）送信元 IP アドレスがネットワークに流れて発生する問題を軽減するのに役立ちます。たとえば、Smurf や Tribal Flood Network（TFN）など、多くの一般的なタイプの DoS 攻撃は、偽造された、または次々に変わる送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタすることを攻撃者が阻止できるようにします。パブリック アクセスを提供するインターネット サービス プロバイダー（ISP）の場合、uRPF が IP ルーティング テーブルと整合性の取れた有効な送信元アドレスを持つパケットだけを転送することによって、そのような攻撃をそらします。この処理により、ISP のネットワーク、その顧客、および残りのインターネットが保護されます。

（注）

- ユニキャスト RPF は、IP サービスでのみでサポートされます。
- スイッチが複数のスイッチ タイプが混在する混合ハードウェア スタック内にある場合は、ユニキャスト RPF を設定しないでください。

IP ユニキャスト RPF 設定の詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「*Other Security Features*」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 *4* : ***IPv6*** をモニタリングするコマンド

コマンド（**Command**）	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	スイッチの IPv6 ルーティング プロトコルのリストを表示します。
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 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 *5* : ***EIGRP IPv6*** 情報を表示するためのコマンド

コマンド（**Command**）	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 interface[*as-number*] *traffic*	送受信される EIGRP IPv6 パケット数を表示します。
show ipv6 eigrptopology [*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

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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： `Device(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。プール名は、記号文字列（Engineering など）または整数（0 など）です。
ステップ 3	**address prefix** *IPv6-prefix* {**lifetime**} {*t1 t1* | **infinite**} 例： `Device(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な状態を維持するタイム インターバル（秒）を指定します。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： `Device(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。

	コマンドまたはアクション	目的
		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。
ステップ 5	**vendor-specific** *vendor-id* 例： `Device(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： `Device(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： `Device(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： `Device(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： `Device(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	**ipv6dhcpserver** [*poolname* | **automatic**] [**rapid-commit**] [**preference** *value*] [**allow-hint**] 例： `Device(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。プール名は、記号文字列（Engineering など）または整数（0 など）です。

	コマンドまたはアクション	目的
		• **automatic**：（任意）サーバが、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つのメッセージを交換する方式を許可します。 • **preference** 値：（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 オプションで指定するプリファレンス値を設定します。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 メッセージに含まれるクライアントの提案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： `Device(config)# end`	特権 EXEC モードに戻ります。

ステップ 12	次のいずれかを実行します。
	• **show ipv6 dhcp pool**
	• **show ipv6 dhcp interface**
	例：
	`Device# show ipv6 dhcp pool`
	または
	`Device# 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	**copyrunning-configstartup-config** 例： `Device# 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

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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： `Device(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： `Device(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）アドレス割り当てに 2 つのメッセージを交換する方式を許可します。
ステップ 4	**ipv6 dhcp client request** [**vendor-specific**] 例： `Device(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： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showipv6dhcpinterface** 例： `Device# 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。

```
Device(config)# ipv6 unicast-routing
Device(config)# interface gigabitethernet1/0/11
Device(config-if)# no switchport
Device(config-if)# ipv6 address 2001:0DB8:c18:1::/64 eui 64
Device(config-if)# end
Device# 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。

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

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

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

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

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

```
Device(config)# interface gigabitethernet2/0/1
Device(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。

```
Device(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。

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

例：インターフェイスでの PBR のイネーブル化

次の例では、pbr-dest-1 という名前のルートマップを作成および設定し、パケット一致基準および目的のポリシー ルーティング アクションを指定します。次に、PBR が GigabitEthernet インターフェイス 0/0/1 でイネーブルにされます。

```
ipv6 access-list match-dest-1
  permit ipv6 any 2001:DB8:2001:1760::/32
route-map pbr-dest-1 permit 10
  match ipv6 address match-dest-1
  set interface GigabitEthernet 0/0/0
interface GigabitEthernet0/0/1
  ipv6 policy-route-map interactive
```

例：ローカル PBR for IPv6 の有効化

次の例では、宛先 IPv6 アドレスがアクセス リスト pbr-src-90 で許可されている IPv6 アドレス範囲に一致するパケットが、IPv6 アドレス 2001:DB8:2003:1::95 のデバイスに送信されています。

```
ipv6 access-list src-90
  permit ipv6 host 2001:DB8:2003::90 2001:DB8:2001:1000::/64
route-map pbr-src-90 permit 10
  match ipv6 address src-90
  set ipv6 next-hop 2001:DB8:2003:1::95
ipv6 local policy route-map pbr-src-90
```

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。

```
Device(config)# ipv6 router rip cisco
```

```
Device(config-router)# maximum-paths 8
Device(config)# exit
Device(config)# interface gigabitethernet2/0/11
Device(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。

```
Device# 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 3 章

IPv6 マルチキャストの実装

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。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表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 Cisco 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 マルチキャスト ルーティングの実装に関する情報

この章では、スイッチにIPv6マルチキャストルーティングを実装する方法について説明します。

従来の IP 通信では、ホストはパケットを単一のホスト（ユニキャスト伝送）またはすべてのホスト（ブロードキャスト伝送）に送信できます。IPv6 マルチキャストは、第三の方式を提供するものであり、ホストが単一のデータ ストリームをすべてのホストのサブセット（グループ伝送）に同時に送信できるようにします。

IPv6 マルチキャストの概要

IPv6マルチキャストグループは、特定のデータ ストリームを受信する受信側の任意のグループです。このグループには、物理的境界または地理的境界はありません。受信側は、インターネット

上または任意のプライベート ネットワーク内の任意の場所に配置できます。特定のグループへのデータ フローの受信に関与する受信側は、ローカル スイッチに対してシグナリングすることによってそのグループに加入する必要があります。このシグナリングは、MLDプロトコルを使用して行われます。

スイッチは、MLDプロトコルを使用して、直接接続されているサブネットにグループのメンバが存在するかどうかを学習します。ホストは、MLD レポート メッセージを送信することによってマルチキャスト グループに加入します。ネットワークでは、各サブネットでマルチキャストデータのコピーを 1 つだけ使用して、潜在的に無制限の受信側にデータが伝送されます。トラフィックの受信を希望する IPv6 ホストはグループ メンバと呼ばれます。

グループ メンバに伝送されるパケットは、単一のマルチキャスト グループ アドレスによって識別されます。マルチキャストパケットは、IPv6ユニキャストパケットと同様に、ベストエフォート型の信頼性を使用してグループに伝送されます。

マルチキャスト環境は、送信側と受信側で構成されます。どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージをリッスンして受信できます。

マルチキャスト アドレスがマルチキャスト グループの受信先として選択されます。送信者は、データグラムの宛先アドレスとしてグループのすべてのメンバに到達するためにそのアドレスを使用します。

マルチキャスト グループ内のメンバーシップはダイナミックです。ホストはいつでも加入および脱退できます。マルチキャスト グループ内のメンバの場所または数に制約はありません。ホストは、一度に複数のマルチキャスト グループのメンバにすることができます。

マルチキャスト グループがどの程度アクティブであるか、その期間、およびメンバーシップはグループおよび状況によって異なります。メンバを含むグループにアクティビティがない場合もあります。

IPv6 マルチキャスト ルーティングの実装

Cisco IOS ソフトウェアでは、IPv6 マルチキャスト ルーティングを実装するため、次のプロトコルがサポートされています。

- MLD は、直接接続されているリンク上のマルチキャスト リスナー（特定のマルチキャスト アドレスを宛先としたマルチキャストパケットを受信するために使用するノード）を検出するために IPv6 スイッチで使用されます。MLD には 2 つのバージョンがあります。MLD バージョン 1 はバージョン 2 のインターネット グループ管理プロトコル（IGMP）for IPv4 をベースとしています。MLD バージョン 2 はバージョン 3 の IGMP for IPv4 をベースとしています。Cisco IOS ソフトウェアの IPv6 マルチキャストでは、MLD バージョン 2 と MLD バージョン 1 の両方が使用されます。MLD バージョン 2 は、MLD バージョン 1 と完全な下位互換性があります（RFC 2710 で規定）。MLD バージョン 1 だけをサポートするホストは、MLD バージョン 2 を実行しているスイッチと相互運用します。MLD バージョン 1 ホストと MLD バージョン 2 ホストの両方が混在する LAN もサポートされています。
- PIM-SM は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにスイッチ間で使用されます。

- PIM in Source Specific Multicast（PIM-SSM）は PIM-SM と類似していますが、IP マルチキャストアドレスを宛先とした特定の送信元アドレス（または特定の送信元アドレスを除くすべてのアドレス）からのパケットを受信する対象をレポートする機能を別途備えています。

IPv6 マルチキャスト リスナー ディスカバリ プロトコル

キャンパス ネットワークでマルチキャストの実装を開始するには、ユーザは最初に、誰がマルチキャストを受信するかを定義する必要があります。MLDプロトコルは、直接接続されているリンク上のマルチキャストリスナー（たとえば、マルチキャストパケットを受信するノード）の存在を検出するため、およびこれらのネイバーノードを対象にしている特定のマルチキャストアドレスを検出するために、IPv6スイッチによって使用されます。これは、ローカル グループおよび送信元固有のグループ メンバーシップの検出に使用されます。

MLD プロトコルは、特別なマルチキャスト クエリアおよびホストを使用して、ネットワーク全体でマルチキャスト トラフィックのフローを自動的に制御および制限する手段を提供します。

マルチキャスト クエリアとマルチキャスト ホスト

マルチキャスト クエリアは、クエリー メッセージを送信して、特定のマルチキャスト グループのメンバーであるネットワーク デバイスを検出するネットワーク デバイス（スイッチなど）です。

マルチキャストホストは、受信側（スイッチを含む）としてレポートメッセージを送信し、クエリアにホスト メンバーシップを通知します。

同じ送信元からのマルチキャストデータ ストリームを受信する一連のクエリアおよびホストは、マルチキャスト グループと呼ばれます。クエリアおよびホストは、MLD レポートを使用して、マルチキャストグループに対する加入および脱退を行ったり、グループ トラフィックの受信を開始したりします。

MLD では、メッセージの伝送にインターネット制御メッセージ プロトコル（ICMP）が使用されます。すべての MLD メッセージはホップ制限が 1 のリンクローカルであり、すべてにスイッチ アラート オプションが設定されています。スイッチ アラート オプションは、ホップバイホップ オプション ヘッダーの実装を意味します。

MLD アクセス グループ

MLD アクセス グループは、Cisco IOS IPv6 マルチキャスト スイッチでの受信側アクセス コントロールを実現します。この機能では、受信側が加入できるグループのリストを制限し、SSM チャネルへの加入に使用される送信元を許可または拒否します。

受信側の明示的トラッキング

明示的トラッキング機能を使用すると、スイッチがIPv6ネットワーク内のホストの動作を追跡できるようになります。また、この機能により、高速脱退メカニズムを MLD バージョン 2 のホスト レポートで使用できるようになります。

Protocol Independent Multicast

PIM（Protocol Independent Multicast）は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにスイッチ間で使用されます。PIM は、ユニキャスト ルーティング プロトコルとは独立して動作し、他のプロトコルと同様に、マルチキャスト ルート アップデートの送受信を実行します。ユニキャスト ルーティング テーブルに値を入力するために LAN でどのユニキャスト ルーティング プロトコルが使用されているかどうかにかかわらず、Cisco IOS PIM では、独自のルーティング テーブルを構築および管理する代わりに、既存のユニキャスト テーブル コンテンツを使用して、Reverse Path Forwarding（RPF）チェックを実行します。

PIM-SM または PIM-SSM のいずれかを使用するように IPv6 マルチキャストを設定することも、ネットワークで PIM-SM と PIM-SSM の両方を使用することもできます。

PIM スパース モード

IPv6 マルチキャストでは、PIM-SM を使用したドメイン内マルチキャスト ルーティングがサポートされています。PIM-SM は、ユニキャスト ルーティングを使用して、マルチキャスト ツリー構築用のリバースパス情報を提供しますが、特定のユニキャスト ルーティング プロトコルには依存しません。

PIM-SM は、トラフィックに対して明示的な要求がある場合を除いて、各マルチキャストに関与しているスイッチの数が比較的少なく、これらのスイッチがグループのマルチキャスト パケットを転送しないときに、マルチキャスト ネットワークで使用されます。PIM-SM は、共有ツリー上のデータ パケットを転送することによって、アクティブな送信元に関する情報を配布します。PIM-SM は最初に共有ツリーを使用しますが、これには RP の使用が必要となります。

要求は、ツリーのルート ノードに向けてホップバイホップで送信される PIM join を使用して行われます。PIM-SM のツリーのルート ノードは、共有ツリーの場合は RP、最短パス ツリー（SPT）の場合はマルチキャスト送信元に直接接続されているファーストホップ スイッチになります。RP はマルチキャスト グループを追跡し、マルチキャスト パケットを送信するホストはそのホストのファーストホップ スイッチによって RP に登録されます。

PIM join がツリーの上位方向に送信されると、要求されたマルチキャスト トラフィックがツリーの下位方向に転送されるように、パス上のスイッチがマルチキャスト転送ステートを設定します。マルチキャスト トラフィックが不要になったら、スイッチはルート ノードに向けてツリーの上位方向に PIM prune を送信し、不必要なトラフィックをプルーニング（削除）送信します。この PIM prune がホップごとにツリーを上位方向に移動する際、各スイッチはその転送状態を適切に更新します。最終的に、マルチキャスト グループまたは送信元に関連付けられている転送ステートは削除されます。

マルチキャスト データの送信側は、マルチキャスト グループを宛先としたデータを送信します。送信側の指定スイッチ（DR）は、これらのデータ パケットを受け取り、ユニキャストでカプセル化し、RP に直接送信します。RP は、カプセル化されたこれらのデータ パケットを受信し、カプセル化を解除し、共有ツリー上に転送します。そのあと、パケットは、RP ツリー上のスイッチの（*,G）マルチキャスト ツリー ステートに従って、RP ツリー ブランチの任意の場所に複製され、そのマルチキャスト グループのすべての受信側に最終的に到達します。RP へのデータ パケット

のカプセル化のプロセスは登録と呼ばれ、カプセル化されたパケットはPIM レジスタ パケットと呼ばれます。

IPv6 BSR：RP マッピングの設定

ドメイン内の PIM スイッチは、各マルチキャスト グループを正しい RP アドレスにマッピングできる必要があります。PIM-SM 対応の BSR プロトコルは、グループと RP のマッピング情報をドメイン全体に迅速に配布するためのダイナミック適応メカニズムを備えています。IPv6 BSR 機能を使用すると、到達不能になった RP が検出され、マッピング テーブルが変更されます。これにより、到達不能な RP が今後使用されなくなり、新しいテーブルがドメイン全体に迅速に配布されるようになります。

すべての PIM-SM マルチキャスト グループを RP の IP または IPv6 アドレスに関連付ける必要があります。新しいマルチキャスト送信側が送信を開始すると、そのローカル DR がこれらのデータ パケットを PIM register メッセージにカプセル化し、そのマルチキャスト グループの RP に送信します。新しいマルチキャスト受信側が加入すると、そのローカル DR がそのマルチキャスト グループの RP に PIM join メッセージを送信します。PIM スイッチは、（*, G）join メッセージを送信するとき、RP 方向への次のスイッチを認識して、G（グループ）がそのスイッチにメッセージを送信できるようにする必要があります。また、PIM スイッチは、（*, G）ステートを使用してデータ パケットを転送するとき、G を宛先としたパケットの正しい着信インターフェイスを認識する必要があります。これは、他のインターフェイスに着信するパケットを拒否する必要があるためです。

ドメイン内の少数のスイッチが候補ブートストラップ スイッチ（C-BSR）として設定され、単一のBSRがそのドメイン用に選択されます。また、ドメイン内の一連のスイッチが候補RP（C-RP）として設定されます。通常、これらのスイッチは、C-BSRとして設定されているものと同じスイッチです。候補RPは、候補RPアドバタイズメント（C-RP-Adv）メッセージをそのドメインのBSRに定期的にユニキャストし、RP になる意思をアドバタイズします。C-RP-Adv メッセージには、アドバタイズを行っている C-RP のアドレス、およびグループ アドレスとマスク長のフィールドの任意のリストが含まれています。これらのフィールドは、立候補のアドバタイズの対象となるグループ プレフィックスを示します。BSR は、定期的に発信するブートストラップ メッセージ（BSM）にこれらの一連の C-RP とそれに対応するグループ プレフィックスを含めます。BSM は、ドメイン全体にホップバイホップで配布されます。

双方向 BSR がサポートされているため、双方向 RP を C-RP メッセージおよび BSM の双方向範囲でアドバタイズできます。システム内のすべてのスイッチは、BSMで双方向範囲を使用できる必要があります。使用できない場合は、双方向 RP 機能が機能しません。

PIM-Source Specific Multicast (PIM-SSM)

PIM-SSMは、SSMの実装をサポートするルーティング プロトコルであり、PIM-SMから派生したものです。ただし、PIM-SM では PIM join を受けてすべてのマルチキャスト送信元からデータが送信されるのに対し、SSM 機能では、受信側が明示的に加入しているマルチキャスト送信元だけからその受信側にデータグラム トラフィックが転送されます。これにより、帯域利用率が最適化され、不要なインターネット ブロードキャスト トラフィックが拒否されます。さらに、SSM では、RPと共有ツリーを使用する代わりに、マルチキャスト グループの送信元アドレスで見つかっ

た情報を使用します。この情報は、MLD メンバーシップ レポートによってラストホップ スイッチにリレーされる送信元アドレスを通して受信側から提供されます。その結果として、送信元に直接つながる最短パス ツリーが得られます。

SSM では、データグラムは（S, G）チャネルに基づいて配信されます。1 つの（S, G）チャネルのトラフィックは、IPv6 ユニキャスト送信元アドレス S とマルチキャスト グループ アドレス G を IPv6 宛先アドレスとして使用するデータグラムで構成されます。システムは、（S, G）チャネルのメンバになることによって、このトラフィックを受信します。シグナリングは不要ですが、受信側は特定の送信元からのトラフィックを受信する場合は（S,G）チャネルに加入し、トラフィックを受信しない場合はチャネルから脱退する必要があります。

SSM を動作させるには、MLD バージョン 2 が必要です。MLD を使用すると、ホストが送信元の情報を提供できるようになります。MLD を使用して SSM を動作させるには、Cisco IOS IPv6 スイッチ、アプリケーションが実行されているホスト、およびアプリケーション自体で SSM がサポートされている必要があります。

ルーティング可能アドレスの hello オプション

IPv6 内部ゲートウェイ プロトコルを使用してユニキャスト ルーティング テーブルを構築する場合、アップストリーム スイッチ アドレスを検出するための手順では、PIM ネイバーとネクストホップ スイッチが同じスイッチを表しているかぎり、これらのアドレスは常に同じであるものと想定されます。ただし、スイッチがリンク上に複数のアドレスを持つ場合は、このことが当てはまるとはかぎりません。

この状況は IPv6 において、2 つの一般的な状況で発生することがあります。1 つめの状況は、ユニキャスト ルーティング テーブルが IPv6 内部ゲートウェイ プロトコル（マルチキャスト BGP など）によって構築されない場合に発生します。2 つめの状況は、RP のアドレスがダウンストリーム スイッチとサブネット プレフィックスを共有している場合に発生します（RP スイッチ アドレスはドメインワイドにする必要があるため、リンクローカル アドレスにはできないことに注意してください）。

ルーティング可能アドレスの hello オプションによって、PIM プロトコルでこのような状況を回避できます。このためには、PIM hello メッセージがアドバタイズされるインターフェイス上のすべてのアドレスを含む PIM hello メッセージ オプションを追加します。PIM スイッチが何らかのアドレスのアップストリーム スイッチを検出すると、RPF 計算の結果は、PIM ネイバーのアドレス自体に加えて、このオプションのアドレスとも比較されます。このオプションにはそのリンク上の PIM スイッチの考えられるアドレスがすべて含まれているため、対象の PIM スイッチがこのオプションをサポートしている場合、常に RPF 計算の結果が含まれます。

PIM メッセージにサイズ制限があることと、ルーティング可能アドレスの hello オプションが単一の PIM hello メッセージ内に収まる必要があるため、インターフェイスで設定できるアドレスの制限は 16 個になっています。

PIM IPv6 スタブ ルーティング

PIM スタブ ルーティング機能は、エンド ユーザの近くにルーテッド トラフィックを移動し、リソースの利用率を軽減します。

PIM スタブ ルーティングを使用するネットワークでは、ユーザに対する IPv6 トラフィックの唯一の許容ルートは、PIM スタブ ルーティングを設定しているスイッチ経由です。PIM 受動インターフェイスは、VLAN などのレイヤ 2 アクセス ドメイン、または他のレイヤ 2 デバイスに接続されているインターフェイスに接続されます。直接接続されたマルチキャスト レシーバおよび送信元のみが、レイヤ 2 アクセス ドメインで許可されます。PIM 受動インターフェイスは、受信した PIM 制御パケットを送信または処理しません。

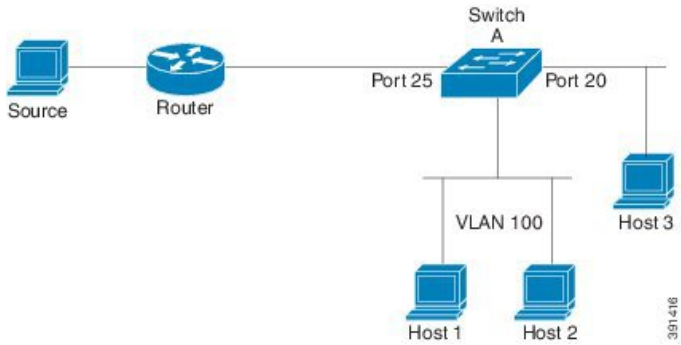
PIM スタブ ルーティングを使用しているときは、IPv6 マルチキャスト ルーティングを使用し、スイッチだけを PIM スタブ ルータとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。スイッチは分散ルータ間の伝送トラフィックをルーティングしません。スイッチのルーテッド アップリンク ポートも設定する必要があります。SVI の場合は、スイッチのアップリンク ポートを使用できません。

また、PIM スタブ ルーティングをスイッチに設定するときは、EIGRP スタブ ルーティングも設定する必要があります。

冗長 PIM スタブ ルータ トポロジーはサポートされません。単一のアクセス ドメインにマルチキャスト トラフィックを転送している複数の PIM ルータがある場合、冗長トポロジーが存在します。PIM メッセージはブロックされ、PIM アサートおよび指定されたルータ選出メカニズムは PIM 受動インターフェイスではサポートされません。PIM スタブ機能では、非冗長アクセス ルータ トポロジーだけがサポートされます。非冗長トポロジーを使用することで、PIM 受動インターフェイスはそのアクセス ドメインで唯一のインターフェイスおよび指定ルータであると想定します。

次に示す図では、スイッチ A ルーテッド アップリンク ポート 25 がルータに接続され、PIM スタブ ルーティングが VLAN 100 インターフェイスとホスト 3 でイネーブルになっています。この設定により、直接接続されたホストはマルチキャスト発信元からトラフィックを受信できます。

図 *2*：*PIM* スタブ ルータ設定



スタティック mroute

IPv6 スタティック mroute は、RPF チェックを変化させるために使用する IPv4 スタティック mroute とほぼ同様に動作します。IPv6 スタティック mroute は、IPv6 スタティック ルートと同じデータベースを共有し、RPF チェックに対するスタティック ルート サポートを拡張することによって実装されます。スタティック mroute では、等コスト マルチパス mroute がサポートされています。また、ユニキャスト専用スタティック ルートもサポートされています。

MRIB

マルチキャストルーティング情報ベース（MRIB）は、マルチキャスト ルーティング プロトコル（ルーティング クライアント）によってインスタンス化されるマルチキャスト ルーティング エントリのプロトコル非依存リポジトリです。その主要機能は、ルーティング プロトコルとマルチキャスト転送情報ベース（MFIB）間の非依存性を実現することです。また、クライアント間の調整および通信ポイントとしても機能します。

ルーティング クライアントは、MRIB が提供するサービスを使用して、ルーティング エントリをインスタンス化し、他のクライアントによってルーティング エントリに加えられた変更を取得します。MRIB では、ルーティング クライアント以外に、転送クライアント（MFIB インスタンス）や特別なクライアント（MLD など）も扱われます。MFIB は、MRIB からその転送エントリを取得し、パケットの受信に関連するイベントについて MRIB に通知します。これらの通知は、ルーティング クライアントによって明示的に要求されることも、MFIB によって自発的に生成されることもあります。

MRIB のもう 1 つの重要な機能は、同じマルチキャスト セッション内でマルチキャスト接続を確立する際に、複数のルーティング クライアントの調整を可能にすることです。また、MRIB では、MLD とルーティング プロトコル間の調整も可能です。

MFIB

MFIB は、IPv6 ソフトウェア用のプラットフォーム非依存およびルーティング プロトコル非依存ライブラリです。その主な目的は、転送テーブルが変更されたときに、Cisco IOS プラットフォームに、IPv6 マルチキャスト転送テーブルおよび通知を読み取るインターフェイスを提供することです。MFIB が提供する情報には、明確に定義された転送セマンティクスが含まれています。この情報は、プラットフォームが特定のハードウェアまたはソフトウェア転送メカニズムに容易に変換できる設計になっています。

ネットワーク内でルーティングまたはトポロジが変更されると、IPv6 ルーティング テーブルがアップデートされ、これらの変更が MFIB に反映されます。MFIB は、IPv6 ルーティング テーブル内の情報に基づいて、ネクストホップ アドレス情報を管理します。MFIB エントリとルーティング テーブル エントリの間には 1 対 1 の相互関係があるため、MFIB には既知のすべてのルートが含まれ、高速スイッチングや最適スイッチングなどのスイッチング パスに関連付けられているルート キャッシュ管理の必要がなくなります。

MFIB

（注） 分散 MFIB は、マスターが他のスタック メンバーに MFIB 情報を配布するスタック環境でのみ意味を持ちます。次のセクションでは、ラインカードは単にスタックのメンバー スイッチです。

MFIB（MFIB）は、分散型プラットフォーム上でマルチキャスト IPv6 パケットをスイッチングするために使用されます。また、MFIB には、ラインカード間での複製に関するプラットフォーム固

有の情報も含まれることがあります。転送ロジックのコアを実装する基本 MFIB ルーチンは、すべての転送環境に共通です。

MFIB は、次の機能を実装します。

- ラインカードで生成されたデータ駆動型プロトコル イベントを PIM にリレーします。
- MFIB プラットフォーム アプリケーション プログラム インターフェイス（API）を提供し、ハードウェア アクセラレーション エンジンのプログラミングを担っている、プラットフォーム固有のコードに MFIB の変更を伝播します。また、この API には、ソフトウェアでパケットをスイッチングしたり（パケットがデータ駆動型イベントのトリガーとなっている場合に必要）、ソフトウェアにトラフィックの統計情報をアップロードしたりするエントリ ポイントも含まれています。

また、MFIB および MRIB サブシステムを組み合わせて使用すると、スイッチが各ラインカードでMFIBデータベースの「カスタマイズ」コピーを保有したり、MFIB関連のプラットフォーム固有の情報を RP からラインカードに転送したりできるようになります。

IPv6マルチキャストのプロセス スイッチングおよび高速スイッチング

統合 MFIB は、IPv6 マルチキャストでの PIM-SM および PIM-SSM に対するファスト スイッチングおよびプロセス スイッチングの両サポートを提供するために使用されます。プロセス スイッチングでは、の が各パケットの調査、書き換え、および転送を行う必要があります。最初にパケットが受信され、システム メモリにコピーされます。次に、スイッチがルーティング テーブル内でレイヤ 3 ネットワーク アドレスを検索します。そのあと、レイヤ 2 フレームがネクストホップの宛先アドレスで書き換えられ、発信インターフェイスに送信されます。また、は、巡回冗長検査（CRC）も計算します。このスイッチング方式は、IPv6 パケットをスイッチングする方式の中でスケーラビリティが最も低い方式です。

IPv6 マルチキャストの高速スイッチングを使用すると、スイッチは、プロセス スイッチングよりも高いパケット転送パフォーマンスを実現できます。従来ルート キャッシュに格納される情報は、IPv6 マルチキャスト スイッチング用にいくつかのデータ構造に格納されます。これらのデータ構造では、ルックアップが最適化され、パケット転送を効率的に行えるようになっています。

IPv6 マルチキャスト転送では、PIM プロトコル ロジックで許可されていれば、最初のパケットのファスト スイッチングが行われます。IPv6 マルチキャストの高速スイッチングでは、MAC カプセル化ヘッダーが事前に計算されます。IPv6 マルチキャストの高速スイッチングでは、MFIB を使用して、IPv6 送信先プレフィックス ベースのスイッチング判定が行われます。IPv6 マルチキャストの高速スイッチングでは、MFIB に加えて、隣接関係テーブルを使用して、レイヤ2アドレッシング情報が付加されます。隣接関係テーブルでは、すべての MFIB エントリのレイヤ 2 ネクストホップ アドレスが管理されます。

隣接が検出されると、隣接関係テーブルにそのデータが入力されます。（ARP などを使用して）隣接エントリが作成されるたびに、その隣接ノードのリンク層ヘッダーが事前に計算され、隣接関係テーブルに格納されます。ルートが決定されると、そのヘッダーはネクスト ホップおよび対応する隣接エントリを指します。そのあと、そのヘッダーはパケット スイッチング時のカプセル化に使用されます。

ロードバランシングと冗長性の両方に対応するようにスイッチが設定されている場合など、ルートには送信先プレフィックスへの複数のパスが存在することがあります。解決されたパスごとに、そのパスのネクストホップ インターフェイスに対応する隣接へのポインタが追加されます。このメカニズムは、複数のパスでのロード バランシングに使用されます。

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP

IPv6 マルチキャスト アドレス ファミリのマルチプロトコル BGP 機能では、マルチプロトコル BGP for IPv6 拡張を提供し、IPv4 BGP と同じ機能と機能性をサポートします。マルチキャスト BGP に対する IPv6 拡張には、IPv6 マルチキャスト アドレス ファミリ、ネットワーク層到達可能性情報（NLRI）、およびIPv6アドレスを使用するネクストホップ（宛先へのパス内の次のスイッチ）属性のサポートが含まれています。

マルチキャスト BGP は、ドメイン間 IPv6 マルチキャストの配布を可能にする、拡張された BGP です。マルチプロトコル BGP では、複数のネットワーク層プロトコル アドレス ファミリ（IPv6 アドレス ファミリなど）および IPv6 マルチキャスト ルートに関するルーティング情報を伝送します。IPv6 マルチキャスト アドレス ファミリには、IPv6 PIM プロトコルによる RPF ルックアップに使用される複数のルートが含まれており、マルチキャストBGP IPv6は、同じドメイン間転送を提供します。ユニキャスト BGP が学習したルートは IPv6 マルチキャストには使用されないため、ユーザは、BGP で IPv6 マルチキャストを使用する場合は、マルチプロトコル BGP for IPv6 マルチキャストを使用する必要があります。

マルチキャスト BGP 機能は、個別のアドレス ファミリ コンテキストを介して提供されます。Subsequent Address Family Identifier（SAFI）では、属性で伝送されるネットワーク層到達可能性情報のタイプに関する情報を提供します。マルチプロトコルBGPユニキャストではSAFI 1 メッセージを使用し、マルチプロトコル BGP マルチキャストでは SAFI 2 メッセージを使用します。SAFI 1 メッセージは、ルートは IP ユニキャストだけに使用でき、IP マルチキャストには使用できないことを示します。この機能があるため、IPv6 ユニキャスト RIB 内の BGP ルートは、IPv6 マルチキャスト RPF ルックアップでは無視される必要があります。

IPv6 マルチキャスト RPF ルックアップを使用して、異なるポリシーおよびトポロジ（IPv6 ユニキャストとマルチキャストなど）を設定するよう、個別のBGPルーティングテーブルが維持されています。マルチキャスト RPF ルックアップは、IP ユニキャスト ルート ルックアップと非常によく似ています。

IPv6 マルチキャスト BGP テーブルと関連付けられている MRIB はありません。ただし、必要な場合、IPv6 マルチキャスト BGP は、ユニキャスト IPv6 RIB で動作します。マルチキャスト BGP では、IPv6 ユニキャスト RIB へのルートの挿入や更新は行いません。

IPv6 マルチキャストの実装

IPv6 マルチキャスト ルーティングのイネーブル化

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal**	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 multicast-routing** 例： `Device (config)# ipv6 multicast-routing`	すべての IPv6 対応インターフェイスでマルチキャスト ルーティングをイネーブルにし、イネーブルになっているすべてのスイッチ インターフェイスで PIM および MLD に対してマルチキャスト転送をイネーブルにします。
ステップ 3	**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。

MLD プロトコルのカスタマイズおよび確認

インターフェイスでの MLD のカスタマイズおよび確認

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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** *type number* 例： `(config)# interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチ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 mld join-group** [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** [*acl*]} 例： `(config-if) # ipv6 mld join-group FF04::10`	指定したグループおよび送信元に対して MLD レポートを設定します。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 mld access-group** *access-list-name* 例： `(config-if) # ipv6 access-list acc-grp-1`	ユーザに IPv6 マルチキャストの受信側アクセス コントロールの実行を許可します。
ステップ 5	**ipv6 mld static-group** [*group-address*] [**include** | **exclude**] {*source-address* | source-list [*acl*]} 例： `(config-if) # ipv6 mld static-group ff04::10 include 100::1`	指定したインターフェイスにマルチキャスト グループのトラフィックをスタティックに転送し、MLD ジョイナがインターフェイスに存在するかのようにインターフェイスが動作するようにします。
ステップ 6	**ipv6 mld query-max-response-time** 秒 例： `(config-if) # ipv6 mld query-max-response-time 20`	MLD キューにアドバタイズされる最大応答時間を設定します。
ステップ 7	**ipv6 mld query-timeout** 秒 例： `(config-if) # ipv6 mld query-timeout 130`	スイッチがインターフェイスのクエリアとして引き継ぐまでのタイムアウト値を設定します。
ステップ 8	**exit** 例： `(config-if) # exit`	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 9	**show ipv6 mldgroups [link-local]** [*group-name* | *group-address*] [*interface-type interface-number*] [**detail** | **explicit**] 例： `# show ipv6 mld groups GigabitEthernet 1/0/1`	スイッチに直接接続されており、MLD を介して学習したマルチキャスト グループを表示します。
ステップ 10	**show ipv6 mld groups summary** 例： `# show ipv6 mld groups summary`	MLD キャッシュに存在する (*, G) および (S, G) メンバーシップ レポートの番号を表示します。

	コマンドまたはアクション	目的
ステップ 11	**show ipv6 mldinterface** [*type number*] 例： `# show ipv6 mld interface GigabitEthernet 1/0/1`	インターフェイスのマルチキャスト関連情報を表示します。
ステップ 12	**debug ipv6 mld** [*group-name* | *group-address* | *interface-type*] 例： `# debug ipv6 mld`	MLD プロトコル アクティビティに対するデバッグをイネーブルにします。
ステップ 13	**debug ipv6 mld explicit** [*group-name* | *group-address* 例： `# debug ipv6 mld explicit`	ホストの明示的トラッキングに関連する情報を表示します。
ステップ 14	**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。

MLD グループ制限の実装

インターフェイス単位の MLD 制限とグローバル MLD 制限は相互に独立して機能します。インターフェイス単位の MLD 制限とグローバル MLD 制限の両方を同じスイッチで設定できます。MLD制限の数は、グローバルの場合もインターフェイス単位の場合も、デフォルトでは設定されません。ユーザが制限を設定する必要があります。インターフェイス単位のステート制限またはグローバル ステート制限を超えるメンバーシップ レポートは無視されます。

MLD グループ制限のグローバルな実装

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	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	**configureterminal** 例： `Device# 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 mld** [*vrf vrf-name*] **state-limit** *number* 例： `Device(config)# ipv6 mld state-limit 300`	MLD ステートの数をグローバルに制限します。
ステップ 4	**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。

MLD グループ制限のインターフェイス単位での実装

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	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	**configureterminal** 例： `Device# 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	**interface type** *number* 例： `Device(config)# interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチ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。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 mld limit** *number* [**except**]*access-list* 例： `Device(config-if)# ipv6 mld limit 100`	MLD ステートの数をインターフェイス単位で制限します。
ステップ 5	**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。

受信側の明示的トラッキングによってホストの動作を追跡するための設定

明示的トラッキング機能を使用すると、スイッチが IPv6 ネットワーク内のホストの動作を追跡できるようになります。また、高速脱退メカニズムを MLD バージョン 2 のホスト レポートで使用できるようになります。

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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** *type number* 例： `(config)# interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチ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 mld explicit-tracking** *access-list-name* 例： `(config-if)# ipv6 mld explicit-tracking list1`	ホストの明示的トラッキングをイネーブルにします。
ステップ 4	**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。

MLD トラフィック カウンタのリセット

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 mldtraffic** 例： `# clear ipv6 mld traffic`	すべての MLD トラフィック カウンタをリセットします。
ステップ 2	**show ipv6 mldtraffic** 例： `# show ipv6 mld traffic`	MLD トラフィック カウンタを表示します。
ステップ 3	**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。

MLD インターフェイス カウンタのクリア

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 mldcounters** *interface-type* 例： `# clear ipv6 mld counters Ethernet1/0`	MLDインターフェイス カウンタをクリアします。
ステップ 2	**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。

PIM の設定

ここでは、PIM の設定方法について説明します。

PIM-SM の設定およびグループ範囲の PIM-SM 情報の表示

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 pim **rp-address** *ipv6-address*[*group-access-list*] 例： `(config) # ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C acc-grp-1`	特定のグループ範囲の PIM RP のアドレスを設定します。
ステップ 3	**exit** 例： `(config) # exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 4	**show ipv6 piminterface** [state-on] [**state-off**] [*type-number*] 例： `# show ipv6 pim interface`	PIM に対して設定されたインターフェイスに関する情報を表示します。
ステップ 5	**show ipv6 pimgroup-map** [*group-name* | group-address] | [*group-range* | *group-mask*] [**info-source {bsr** | **default** | **embedded-rp** | **static**}] 例： `# show ipv6 pim group-map`	IPv6 マルチキャスト グループ マッピング テーブルを表示します。
ステップ 6	**show ipv6 pimneighbor** [**detail**] [*interface-type interface-number* | **count**] 例： `# show ipv6 pim neighbor`	Cisco IOS ソフトウェアで検出された PIM ネイバーを表示します。
ステップ 7	**show ipv6 pimrange-list** [**config**] [*rp-address* | *rp-name*] 例： `# show ipv6 pim range-list`	IPv6 マルチキャスト範囲リスト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
ステップ 8	**show ipv6 pimtunnel** [*interface-type interface-number*] 例： `# show ipv6 pim tunnel`	インターフェイス上の PIM レジスタのカプセル化およびカプセル化解除トンネルに関する情報を表示します。
ステップ 9	**debug ipv6 pim** [*group-name* | *group-address* | **interface** *interface-type* | **bsr** | **group** | **mvpn** | **neighbor**] 例： `# debug ipv6 pim`	PIM プロトコル アクティビティに対するデバッグをイネーブルにします。
ステップ 10	**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。

PIM オプションの設定

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 pimspt-threshold infinity** [**group-list** *access-list-name*] 例： `(config) # ipv6 pim spt-threshold infinity group-list acc-grp-1`	PIM リーフ スイッチが指定したグループの SPT に加入するタイミングを設定します。
ステップ 3	**ipv6 pimaccept-register** {**list** *access-list* | **route-map** *map-name*} 例： `(config) # ipv6 pim accept-register route-map reg-filter`	RP のレジスタを許可または拒否します。

	コマンドまたはアクション	目的
ステップ 4	**interface** *type number* 例： `(config) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチ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 5	**ipv6 pim dr-priority** *value* 例： `(config-if) # ipv6 pim dr-priority 3`	PIM スイッチの DR プライオリティを設定します。
ステップ 6	**ipv6 pim hello-interval** 秒 例： `(config-if) # ipv6 pim hello-interval 45`	インターフェイスにおける PIM hello メッセージの頻度を設定します。
ステップ 7	**ipv6 pim join-prune-interval** 秒 例： `(config-if) # ipv6 pim join-prune-interval 75`	指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。
ステップ 8	**exit** 例： `(config-if) # exit`	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 9	**ipv6 pimjoin-prune statistic** [*interface-type*] 例： `(config-if) # show ipv6 pim join-prune statistic`	各インターフェイスの最後の集約パケットに関する平均 join-prune 集約を表示します。
ステップ 10	**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。

PIM トラフィック カウンタのリセット

PIM が誤動作する場合、または予想される PIM パケット数が送受信されていることを確認するために、ユーザは PIM トラフィック カウンタをクリアできます。トラフィック カウンタがクリア

されたら、ユーザは show ipv6 pim traffic コマンドを入力して、PIM が正しく機能していること、および PIM パケットが正しく送受信されていることを確認できます。

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 pimtraffic** 例： `# clear ipv6 pim traffic`	PIM トラフィック カウンタをリセットします。
ステップ 2	**show ipv6 pimtraffic** 例： `# show ipv6 pim traffic`	PIM トラフィック カウンタを表示します。
ステップ 3	**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。

PIM トポロジ テーブルをクリアすることによる MRIB 接続のリセット

MRIB を使用するのに設定は不要です。ただし、特定の状況においては、ユーザは PIM トポロジ テーブルをクリアして MRIB 接続をリセットし、MRIB 情報を確認する必要がある場合があります。

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 pimtopology** [*group-name* | *group-address*] 例： `# clear ipv6 pim topology FF04::10`	PIM トポロジテーブルをクリアします。
ステップ 2	**show ipv6 mribclient** [**filter**] [**name** {*client-name* | *client-name***: client-id**}] 例： `# show ipv6 mrib client`	インターフェイスのマルチキャスト関連情報を表示します。

	コマンドまたはアクション	目的
ステップ 3	**show ipv6 mribroute** {**link-local** | **summary** | [*sourceaddress-or-name* | *] [*groupname-or-address*[*prefix-length*]]] 例： `# show ipv6 mrib route`	MRIB ルート情報を表示します。
ステップ 4	**show ipv6 pimtopology** [*groupname-or-address* [*sourceaddress-or-name*] | **link-local** | **route-count** [**detail**]] 例： `# show ipv6 pim topology`	特定のグループまたはすべてのグループの PIM トポロジテーブル情報を表示します。
ステップ 5	**debug ipv6 mribclient** 例： `# debug ipv6 mrib client`	MRIB クライアント管理アクティビティに対するデバッグをイネーブルにします。
ステップ 6	**debug ipv6 mribio** 例： `# debug ipv6 mrib io`	MRIB I/O イベントに対するデバッグをイネーブルにします。
ステップ 7	**debug ipv6 mrib proxy** 例： `# debug ipv6 mrib proxy`	分散型スイッチプラットフォームにおけるスイッチプロセッサとラインカード間の MRIB プロキシアクティビティに対するデバッグをイネーブルにします。
ステップ 8	**debug ipv6 mribroute** [*group-name* | *group-address*] 例： `# debug ipv6 mrib route`	MRIB ルーティング エントリ関連のアクティビティに関する情報を表示します。
ステップ 9	**debug ipv6 mribtable** 例： `# debug ipv6 mrib table`	MRIB テーブル管理アクティビティに対するデバッグをイネーブルにします。
ステップ 10	**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。

PIM IPv6 スタブ ルーティングの設定

PIM スタブ ルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャスト ルーティングをサポートします。サポート対象の PIM インターフェイスは、アップリンク PIM インターフェイスと PIM パッシブ インターフェイスの 2 種類です。PIM パッシブ モードに設定されているルーテッド インターフェイスは、PIM 制御トラフィックの通過も転送も行いません。通過させたり転送したりするのは MLD トラフィックだけです。

PIM IPv6 スタブ ルーティングの設定時の注意事項

- PIM スタブ ルーティングを設定する前に、スタブ ルータと中央のルータの両方に IPv6 マルチキャスト ルーティングが設定されている必要があります。また、スタブ ルータのアップリンク インターフェイス上に、PIM モード（スパースモード）が設定されている必要があります。
- PIM スタブ ルータは、ディストリビューション ルータ間の伝送トラフィックのルーティングは行いません。ユニキャスト（EIGRP）スタブ ルーティングではこの動作が強制されます。PIM スタブ ルータの動作を支援するためにユニキャスト スタブ ルーティングを設定する必要があります。詳細は、EIGRPv6 スタブ ルーティング, （26 ページ）のセクションを参照してください。
- 直接接続されたマルチキャスト（MLD）レシーバおよび送信元だけが、レイヤ 2 アクセス ドメインで許可されます。アクセス ドメインでは、PIM プロトコルはサポートされません。
- 冗長 PIM スタブ ルータ トポロジーはサポートされません。

IPv6 PIM ルーティングのデフォルト設定

この表に、Device用の IPv6 PIM ルーティングのデフォルト設定について示します。

表 *6*：マルチキャスト ルーティングのデフォルト設定

機能	デフォルト設定
マルチキャスト ルーティング	すべてのインターフェイスでディセーブル
PIM のバージョン	バージョン 2
PIM モード	モードは未定義
PIM スタブ ルーティング	未設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル。

機能	デフォルト設定
PIM マルチキャスト境界	なし。
候補 BSR	ディセーブル。
候補 RP	ディセーブル。
SPT しきい値レート	0 kb/s
PIM ルータ クエリー メッセージ インターバル	30 秒

IPv6 PIM スタブ ルーティングのイネーブル化

はじめる前に

PIM スタブ ルーティングは IPv6 ではデフォルトでディセーブルです。インターフェイス上で PIM スタブ 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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 multicast pim-passive-enable** 例： `Device(config-if)# ipv6 multicast pim-passive-enable`	スイッチで IPv6 マルチキャスト PIM ルーティングをイネーブルにします。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 9/0/6`	PIM スタブ ルーティングをイネーブルにする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。

	コマンドまたはアクション	目的
		次のいずれかのインターフェイスを指定する必要があります。 • ルーテッドポート：レイヤ3ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを MLD スタティック グループに結合する必要があります。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース モードをイネーブルにして、静的に接続されたメンバーとして VLAN を MLD スタティック グループに結合し、VLAN、MLD スタティック グループ、および物理インターフェイスで MLD スヌーピングをイネーブルにする必要があります。 これらのインターフェイスには、IPv6 アドレスを割り当てる必要があります。

	コマンドまたはアクション	目的
ステップ 5	**ipv6 pim** 例： `Device(config-if)# ipv6 pim`	インターフェイスで PIM をイネーブルにします。
ステップ 6	**ipv6 pim** {**bsr**} | {**dr-priority** | *value*} | {**hello-interval** | *seconds*} | {**join-prune-interval** | *seconds*} | {**passive**} 例： `Device(config-if)# ipv6 pim bsr|dr-priority|hello-interval|join-prune-interval|passive`	インターフェイスでさまざまな PIM スタブ機能を設定します。 **bsr** を入力して PIM スイッチの BSR を設定します。 **dr-priority** を入力して、PIM スイッチの DR プライオリティを設定します。 **hello-interval** を入力して、インターフェイスの PIM hello メッセージの頻度を設定します。 **join-prune-interval** を入力して、指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。 **passive** を入力して、パッシブ モードの PIM を設定します。
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

IPv6 PIM スタブ ルーティングのモニタ

表 *7*：*PIM* スタブ設定の *show* コマンド

コマンド（Command）	目的
show ipv6 pim interface `Device# show ipv6 pim interface`	各インターフェイスで有効になっている PIM スタブを表示します。
show ipv6 mld groups `Device# show ipv6 mld groups`	特定のマルチキャスト グループを結合した対象クライアントを表示します。
show ipv6 mroute `Device# show ipv6 mroute`	ソースから対象クライアントへのマルチキャスト ストリーム転送を確認します。

BSR の設定

ここでの作業について、以下に説明します。

BSR の設定および BSR 情報の確認

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 pimbsr candidate bsr** *ipv6-address*[*hash-mask-length*] [**priority** *priority-value*] 例： `(config) # ipv6 pim bsr candidate bsr 2001:DB8:3000:3000::42 124 priority 10`	候補 BSR になるようにスイッチを設定します。
ステップ 3	**interface** *type number* 例： `(config) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチ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。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 pim bsr border** 例： `(config-if) # ipv6 pim bsr border`	インターフェイスのタイプと番号を指定し、スイッチ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 5	**exit** 例： `(config-if) # exit`	このコマンドを2回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 6	**show ipv6 pim** bsr {**election** | **rp-cache** | **candidate-rp**} 例： `(config-if) # show ipv6 pim bsr election`	PIM BSR プロトコル処理に関連する情報を表示します。
ステップ 7	**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。

BSR への PIM RP アドバタイズメントの送信

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 pim bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** seconds] 例： `(config) # ipv6 pim bsr candidate rp 2001:DB8:3000:3000::42 priority 0`	BSR に PIM RP アドバタイズメントを送信します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* 例： `(config) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチ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 4	**ipv6 pim bsr border** 例： `(config-if) # ipv6 pim bsr border`	指定したインターフェイスの任意のスコープの全BSMに対して境界を設定します。
ステップ 5	**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。

限定スコープ ゾーン内で BSR を使用できるようにするための設定

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 pim bsr candidate rp** *ipv6-address* [*hash-mask-length*] [**priority** priority-value] 例： `(config) # ipv6 pim bsr candidate bsr 2001:DB8:1:1:4`	候補 BSR になるようにスイッチを設定します。
ステップ 3	**ipv6 pim bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** seconds] 例： `(config) # ipv6 pim bsr candidate rp 2001:DB8:1:1:1 group-list list scope 6`	BSR に PIM RP アドバタイズメントを送信するように候補 RP 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	**interface** *type number* 例： `(config-if) # interface GigabitEthernet 1/0/1`	インターフェイスのタイプと番号を指定し、スイッチ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 5	**ipv6 multicast boundary scope** *scope-value* 例： `(config-if) # ipv6 multicast boundary scope 6`	指定されたスコープのインターフェイスでマルチキャスト境界を設定します。
ステップ 6	**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。

BSR スイッチにスコープと RP のマッピングをアナウンスさせるための設定

IPv6 BSR スイッチは、スコープと RP のマッピングを候補 RP メッセージから学習するのではなく、直接アナウンスするようにスタティックに設定できます。ユーザは、スコープと RP のマッピングをアナウンスするように BSR スイッチを設定して、BSR をサポートしていない RP がその BSR にインポートされるように設定できます。この機能をイネーブルにすると、ローカルの候補 BSR スイッチの既知のリモート RP が、企業の BSR ドメインの外部に配置されている RP を学習できるようになります。

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 pim bsr announced rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] 例： `(config)# ipv6 pim bsr announced rp 2001:DB8:3000:3000::42 priority 0`	指定した候補 RP の BSR からスコープと RP のマッピングを直接アナウンスします。
ステップ 3	**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。

SSM マッピングの設定

SSM マッピング機能をイネーブルにすると、DNS ベースの SSM マッピングが自動的にイネーブルになります。つまり、スイッチは、マルチキャスト MLD バージョン 1 レポートの送信元を DNS サーバから検索するようになります。

スイッチ設定に応じて、DNS ベースのマッピングまたはスタティック SSM マッピングのいずれかを使用できます。スタティック SSM マッピングを使用する場合は、複数のスタティック SSM マッピングを設定できます。複数のスタティック SSM マッピングを設定すると、一致するすべてのアクセス リストの送信元アドレスが使用されるようになります。

（注） DNS ベースの SSM マッピングを使用するには、スイッチは正しく設定されている DNS サーバを少なくとも 1 つ見つける必要があります。スイッチは、その DNS サーバに直接接続される可能性があります。

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 mldssm-map enable** 例： `(config) # ipv6 mld ssm-map enable`	設定済みの SSM 範囲内のグループに対して SSM マッピング機能をイネーブルにします。
ステップ 3	**no ipv6 mldssm-map query dns** 例： `(config) # no ipv6 mld ssm-map query dns`	DNS ベースの SSM マッピングをディセーブルにします。
ステップ 4	**ipv6 mldssm-map static** *access-list source-address* 例： `(config-if) # ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1`	スタティック SSM マッピングを設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `(config-if) # exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 6	**show ipv6 mldssm-map** [*source-address*] 例： `(config-if) # show ipv6 mld ssm-map`	SSM マッピング情報を表示します。
ステップ 7	**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。

スタティック mroute の設定

IPv6 のスタティック マルチキャスト ルート（mroute）は、IPv6 スタティック ルートの拡張として実装できます。スイッチを設定する際には、ユニキャスト ルーティング専用としてスタティック ルートを使用するか、マルチキャスト RPF 選択専用としてスタティック マルチキャスト ルートを使用するか、またはユニキャスト ルーティングとマルチキャスト RPF 選択の両方にスタティック ルートを使用するように設定できます。

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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-type interface-number ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | *unicast* | *multicast*] [**tag** *tag*] 例： `(config) # ipv6 route 2001:DB8::/64 6::6 100`	スタティック IPv6 ルートを確立します。この例は、ユニキャスト ルーティングとマルチキャスト RPF 選択の両方に使用されるスタティック ルートを示しています。

	コマンドまたはアクション	目的
ステップ 3	**exit** 例： `# exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 4	**show ipv6 mroute** [link-local | [*group-name* | *group-address* [*source-address* | *source-name*]] **[summary]** [**count**] 例： `# show ipv6 mroute ff07::1`	IPv6 マルチキャスト ルーティング テーブルの内容を表示します。
ステップ 5	**show ipv6 mroute** [**link-local** | *group-name* | *group-address*] **active** [*kbps*] 例： `(config-if) # show ipv6 mroute active`	スイッチ上のアクティブなマルチキャスト ストリームを表示します。
ステップ 6	**show ipv6 rpf** [*ipv6-prefix*] 例： `(config-if) # show ipv6 rpf 2001::1:1:2`	特定のユニキャスト ホスト アドレスおよびプレフィックスの RPF 情報を確認します。
ステップ 7	**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 マルチキャストでの MFIB の使用

IPv6 マルチキャスト ルーティングをイネーブルにすると、マルチキャスト転送が自動的にイネーブルになります。

IPv6 マルチキャストでの MFIB の動作の確認

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**show ipv6 mfib** [**linkscope** | **verbose** | *group-address-name* | *ipv6-prefix / prefix-length* | *source-address-name* | **count** | **interface** | **status** | **summary**] 例： `# show ipv6 mfib`	IPv6 MFIB での転送エントリおよびインターフェイスを表示します。
ステップ 2	**show ipv6 mfib** [all | linkscope | group-name | group-address [source-name | source-address]] **count** 例： `# show ipv6 mfib ff07::1`	IPv6 マルチキャスト ルーティング テーブルの内容を表示します。
ステップ 3	**show ipv6 mfib interface** 例： `# show ipv6 mfib interface`	IPv6マルチキャスト対応インターフェイスとその転送ステータスに関する情報を表示します。
ステップ 4	**show ipv6 mfib status** 例： `# show ipv6 mfib status`	一般的なMFIB設定と動作ステータスを表示します。
ステップ 5	**show ipv6 mfibsummary** 例： `# show ipv6 mfib summary`	IPv6 MFIB エントリおよびインターフェイスの数に関するサマリー情報を表示します。
ステップ 6	**debug ipv6 mfib** [*group-name* | *group-address*] [**adjacency** | **db** | **fs** | **init** | **interface** | **mrib** [**detail**] | **nat** | **pak** | **platform** | **ppr** | **ps** | **signal** | **table**] 例： `# debug ipv6 mfib FF04::10 pak`	IPv6 MFIB に対するデバッグ出力をイネーブルにします。

MFIB トラフィック カウンタのリセット

特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**clear ipv6 mfibcounters** [*group-name* | **group-address** [*source-address* | *source-name*]] 例： `# clear ipv6 mfib counters FF04::10`	アクティブなすべての MFIB トラフィック カウンタをリセットします。

第 4 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 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），（102 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、 クライアントの IPv4 および IPv6 アドレス、デバイス 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、デバイス 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。デバイスはクライアントの 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。

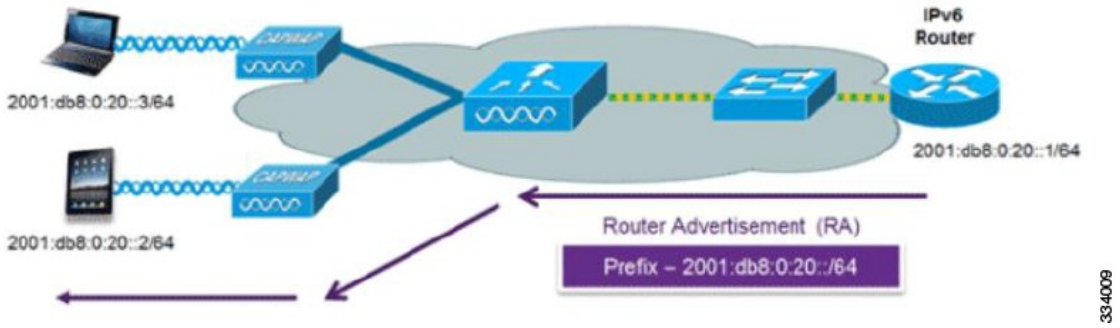
- ホストは、ルータ送信要求メッセージを送信します。
- ホストは、ルータ アドバタイズメント メッセージを待機します。
- ホストは、ルータ アドバタイズメント メッセージから IPv6 プレフィックスの最初の 64 ビットを取得し、これを 64 ビット EUI-64 アドレス（イーサネットの場合、MAC アドレスから作成されます）と組み合わせて、グローバル ユニキャスト メッセージを作成します。ホストは、デフォルト ゲートウェイとして、ルータ アドバタイズメント メッセージの IP ヘッダーに含まれる送信元 IP アドレスも使用します。
- 重複アドレス検出は、選択されるランダム アドレス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 *3*：*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イネーブルにします。

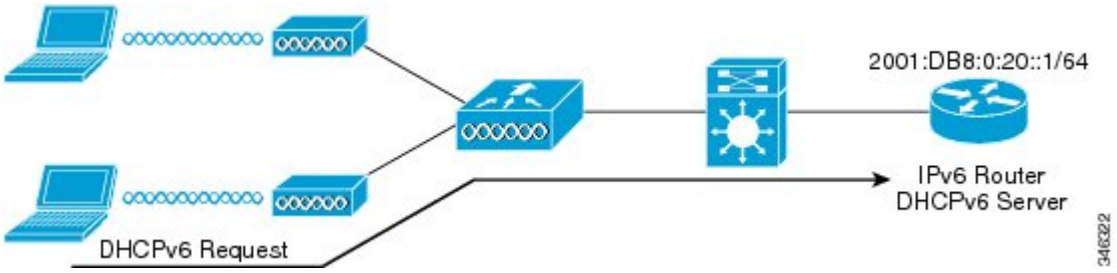
```
ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end
```

関連トピック

IPv6 スヌーピングの設定（CLI），（104 ページ）
DHCP プールの設定（CLI），（108 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），（109 ページ）
DHCP を使用したステートレス自動アドレス設定の設定（CLI），（110 ページ）
ステートフル DHCP のローカル設定（CLI），（111 ページ）
ステートフル DHCP の外部的設定（CLI），（113 ページ）

ステートフル DHCPv6 アドレス割り当て

図 *4*：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Device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），（104 ページ）
DHCP プールの設定（CLI），（108 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），（109 ページ）
DHCP を使用したステートレス自動アドレス設定の設定（CLI），（110 ページ）
ステートフル DHCP のローカル設定（CLI），（111 ページ）
ステートフル DHCP の外部的設定（CLI），（113 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），（105 ページ）

ルータ アドバタイズメント

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），（105 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。 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），（105 ページ）

ネイバー探索抑制

クライアントの IPv6 アドレスは、デバイス によってキャッシュされます。デバイスが IPv6 アドレスを検索する NS マルチキャストを受信して、デバイス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、デバイス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） デバイス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。

デバイス に クライアントの IPv6 アドレスがない場合、デバイス は NA で応答せず、NS パケットを転送します。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、デバイス 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、転送します。このパケットは、目的の 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），（105 ページ）

RA ガード

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、 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 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（IPv6 source address）
- 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 ガードはデバイスで行われます。デバイスで RA メッセージをドロップするようにデバイスを設定できます。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 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），（102 ページ）
RA ガード ポリシーの適用（CLI），（103 ページ）
RA スロットル ポリシーの設定（CLI）
VLAN への RA スロットル ポリシーの適用（CLI）

IPv6 ユニキャストの設定（CLI）

IPv6 ユニキャストはスイッチ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

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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： `Device (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、デバイスで RA ガード ポリシーを設定します。

はじめる前に

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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 nd raguard policy** raguard-router 例： `Device(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： `Device(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。
ステップ 4	**device-role router** 例： `Device(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： `Device(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

RA ガード, （101 ページ）
RA スロットリング
RA ガード ポリシーの適用（CLI）, （103 ページ）
RA スロットル ポリシーの設定（CLI）
VLAN への RA スロットル ポリシーの適用（CLI）
IPv6 クライアント アドレス ラーニングの前提条件, （96 ページ）

RA ガード ポリシーの適用（CLI）

デバイスで 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

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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： `Device (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： `Device(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： `Device(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），（102 ページ）
RA ガード，（101 ページ）
RA スロットリング
RA スロットル ポリシーの設定（CLI）
VLAN への RA スロットル ポリシーの適用（CLI）

IPv6 スヌーピングの設定（CLI）

IPv6 スヌーピングはスイッチ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

	コマンドまたはアクション	目的
ステップ 1	**vlan configuration 1** 例： `Device(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： `Device(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： `Device(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	**[終了(exit)]** 例： `Device(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，（96 ページ）
ステートフル DHCPv6 アドレス割り当て，（98 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device(config)# enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# 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： `Device (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，（99 ページ）
ルータ アドバタイズメント，（99 ページ）
ネイバー探索，（100 ページ）
ネイバー探索抑制，（100 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

	コマンドまたはアクション	目的
ステップ 1	**vlan config901** 例： `Device(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。

	コマンドまたはアクション	目的
ステップ 2	**ipv6 nd suppress** 例： `Device(config-vlan)# ipv6 nd suppress`	VLAN に IPv6 nd 抑制を適用します。
ステップ 3	**end** 例： `Device(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： `Device (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： `Device(config-vlan)# ipv6 nd suppress`	インターフェイスに IPv6 nd 抑制を適用します。
ステップ 6	**end** 例： `Device(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。

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

	コマンドまたはアクション	目的
ステップ 1	**interface vlan** 1 例： `Device(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。

	コマンドまたはアクション	目的

ステップ 2	**ip address** fe80::1 link-local
	
	例：
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(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： `Device(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	終了 例： `Device(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

	コマンドまたはアクション	目的
ステップ 1	**ipv6 dhcp pool** Vlan21 例： `Device(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： `Device(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： `Device(config-dhcpv6)# dns-server 2001:20:21::1`	DHCP プールの DNS サーバを設定します。

	コマンドまたはアクション	目的
ステップ 4	**domain-name** example.com 例： `Device(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。
ステップ 5	**end** 例： `Device(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，（96 ページ）
ステートフル DHCPv6 アドレス割り当て，（98 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

	コマンドまたはアクション	目的
ステップ 1	**interface vlan** 1 例： `Device(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：
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(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： `Device(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	**no ipv6 nd managed-config-flag**
	
	例：
	`Device(config)#interface vlan 1`
	`Device(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： `Device(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： `Device(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，（96 ページ）
ステートフル DHCPv6 アドレス割り当て，（98 ページ）

DHCP を使用したステートレス自動アドレス設定の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**interface vlan** 1 例： `Device(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：
	`Device(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Device(config-if)# ipv6 address fe80::1 link-local`
	`Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Device(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： `Device(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：
	`Device(config)#interface vlan 1`
	`Device(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： `Device(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	終了 例： `Device(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，（96 ページ）
ステートフル DHCPv6 アドレス割り当て，（98 ページ）

ステートフル DHCP のローカル設定（CLI）

このインターフェイス設定は、ローカル のステートフル DHCPv6 を実装している Cisco IOS Ipv6 ルータ用です。Device

はじめる前に

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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： `Device(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： `Device (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。
ステップ 4	**address prefix** 2001:DB8:0:1:FFFF:1234::/64 例： `Device (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： `Device (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： `Device (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： `Device (config-dhcpv6)# exit`	前のモードに戻ります。
ステップ 8	**interface** vlan1 例： `Device (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： `Device (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： `Device (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。

	コマンドまたはアクション	目的
ステップ 11	**ip address** 192.168.20.1 255.255.255.0 例： `Device (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： `Device (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 13	**ipv6 nd managed-config-flag** 例： `Device (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： `Device (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： `Device (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，（96 ページ）
ステートフル DHCPv6 アドレス割り当て，（98 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

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# 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： `Device(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： `Device (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： `Device (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： `Device (config-dhcpv6)# exit`	前のモードに戻ります。
ステップ 6	**interface** vlan1 例： `Device (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： `Device (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： `Device (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： `Device (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。

	コマンドまたはアクション	目的
ステップ 10	**ipv6 nd prefix** 2001:db8::/64**no-advertise** 例： `Device (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： `Device (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： `Device (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： `Device (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，（96 ページ）
ステートフル DHCPv6 アドレス割り当て，（98 ページ）

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、デバイス上の 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

	コマンドまたはアクション	目的

ステップ 1	**show ipv6 dhcp pool**
	
	例：
	`Deviceshow ipv6 dhcp pool`
	`DHCPv6 pool: vlan21`
	`Address allocation prefix:`
	`2001:DB8:0:1:FFFF:1234::/64 valid 86400 preferred`
		デバイス上の 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 (6 in use, 0 conflicts) DNS server: 2001:100:0:1::1 Domain name: example.com Active clients: 6	

その他の参考資料

関連資料

関連項目	参照先
IPv6 コマンド リファレンス	
IP コマンド リファレンス	

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 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 を探してダウンロードするには、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お役立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、Product Alert Tool（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	変更箇所
IPv6 クライアント アドレス ラーニング機能	Cisco IOS XE Everest 16.5.1a	この機能が導入されました。

第 5 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 Network Essentials ライセンス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，（124 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。

デバイスは 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。

- デバイスは、**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。
- デバイスは再帰 ACL（**reflect** キーワード）をサポートしません。
- デバイスは 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、デバイス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、デバイス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）とは、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ルール セットのことです。ACLは デバイス に設定され、管理インターフェイスおよび任意の動的インターフェイスに適用されます。

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。

Network Essentials ライセンスを稼働中のスイッチは、入力ルータ IPv6 ACL だけをサポートしています。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，（124 ページ）
インターフェイスへの IPv6 の適用，（129 ページ）
IPv6 ACL の表示，（130 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。

フィルタ ID IPv6 ACL

filter-Id ACL の場合、完全な ACE および `acl name(filter-id)` がデバイスで設定され、`filter-id` のみが ACS で設定されます。

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` 名をデバイスに対しその `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。

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 メンバで Network Advantage ライセンスを実行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

	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（例えば、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。

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

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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）。

	コマンドまたはアクション	目的
		• 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 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

	コマンドまたはアクション	目的
		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。 • （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

	コマンドまたはアクション	目的
		• 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 | hostsource-ipv6-address} [operator [port-number]] {destination-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 の IP プロトコルの説明にあるパ

	コマンドまたはアクション	目的
	hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] |icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value][time-range name]	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： `Device(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，（119 ページ）
IPv6 ACL の概要，（120 ページ）
インターフェイスへの IPv6 の適用，（129 ページ）
IPv6 ACL の表示，（130 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管理には、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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： `Device# 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： `Device# 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： `Device# 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。
ステップ 5	**ipv6 traffic-filter** *acl_name* 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(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：
	`Device# 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，（124 ページ）
IPv6 ACL の概要，（120 ページ）
IPv6 ACL の表示，（130 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

	コマンドまたはアクション	目的
ステップ 1	**show access-list** 例： `Device# show access-lists`	デバイス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： `Device# 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，（124 ページ）
インターフェイスへの IPv6 の適用，（129 ページ）
IPv6 ACL の概要，（120 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。

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

```
Device(config)# interface TenGigabitEthernet 1/0/3

Device(config-if)# no switchport
Device(config-if)# ipv6 address 2001::/64 eui-64
Device(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。

```
Device #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。

```
Device# 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 ガード ポリシーの設定

手順

	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： `Device (config)# ipv6 nd raguard policy MyPolicy`	
ステップ 2	**trusted-port** 例： `Device (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： `Device (config-nd-raguard)# device-role [host|monitor|router|switch]`	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。

	コマンドまたはアクション	目的
	`Device (config-nd-raguard)# device-role router`	
ステップ 4	**interface tenGigabitEthernet** 1/0/1 例： `Device (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： `Device (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。
ステップ 6	**vlan configuration** 19-21,23 例： `Device (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： `Device (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： `Device (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： `Device (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： `Device (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

	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： `Device (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。

その他の参考資料

関連資料

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 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 を探してダウンロードするには、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お役立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、Product Alert Tool（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	変更箇所
IPv6 ACL 機能	Cisco IOS XE Everest 16.5.1a	この機能が導入されました。

通告

Trademarks