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。

（注） RFC 4291 によると、FF0x::/12（IPv6 宛先アドレスの T フラグが 0 に設定されている）は、永続的に割り当てられた（「既知の」）IPv6 マルチキャストアドレス範囲です。

Cisco Catalyst 9200 シリーズ スイッチでは、このアドレス範囲のパケットのデフォルトの動作は、入力 VLAN でのフラッドです。

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。

プロトコル独立マルチキャスト

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。

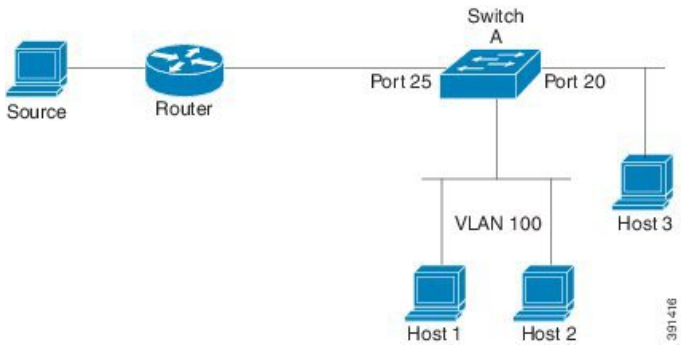
PIM スタブ ルーティングを使用しているときは、IPv6 マルチキャスト ルーティングを使用し、スイッチだけを PIM スタブ ルータとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。スイッチは分散ルータ間の伝送トラフィックをルーティングしません。スイッチのルーテッドアップリンク ポートも設定する必要があります。SVI の場合は、スイッチのアップリンク ポートを使用できません。

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 *1 : PIM* スタブ ルータ設定



ランデブー ポイント

IPv6 PIM では、組み込み RP がサポートされています。組み込み RP サポートを利用すると、デバイスは、静的に設定されている RP の代わりに、マルチキャスト グループ宛先アドレスを使用して RP 情報を学習できるようになります。デバイスが RP である場合、RP として静的に設定する必要があります。

デバイスは、MLD レポート内、または PIM メッセージおよびデータ パケット内の組み込み RP グループアドレスを検索します。このようなアドレスが見つかったら、デバイスはアドレス自体からグループの RP を学習します。この学習された RP は、グループのすべてのプロトコル

アクティビティに使用されます。デバイスが RP である場合、組み込み RP を RP として設定する必要があり、デバイスはそのようにアドバタイズされます。

組み込み RP よりも優先するスタティック RP を選択するには、特定の組み込み RP グループ範囲またはマスクをスタティック RP のアクセス リストに設定する必要があります。PIM がスパースモードで設定されている場合は、RP として動作する 1 つ以上のデバイス選択も必要です。RP は、共有配布ツリーの選択ポイントに配置された単一の共通ルートであり、各ボックスでスタティックに設定されます。

PIM DR は、共有ツリーの下位方向に配布するために、直接接続されているマルチキャスト送信元から RP にデータを転送します。データは次の 2 つの方法のいずれかを使用して RP に転送されます。

- データは、登録パケットにカプセル化され、DR として動作するファーストホップデバイスによって直接 RP にユニキャストされます。
- RP 自身が送信元ツリーに加入している場合は、PIM スパース モードの項で説明したように、RPF 転送アルゴリズムに従ってマルチキャスト転送されます。

RP アドレスは、パケットをグループに送信するホストの代わりに PIM Register メッセージを送信するためにファーストホップデバイスによって使用されます。また、RP アドレスは、ラストホップデバイスによって PIM join および prune メッセージを RP に送信してグループメンバーシップについて通知するためにも使用されます。すべてのデバイス（RP デバイスを含む）で RP アドレスを設定する必要があります。

1 台の PIM デバイスを、複数のグループの RP にできます。特定のグループの PIM ドメイン内で一度に使用できる RP アドレスは 1 つだけです。アクセスリストで指定されている条件によって、デバイスがどのグループの RP であるかが判別されます。

IPv6 マルチキャストでは、PIM accept register 機能がサポートされています。これは、RP で PIM-SM register メッセージのフィルタリングを実行するための機能です。ユーザは、アクセスリストを照合するか、または登録されている送信元の AS パスとルート マップに指定されている AS パスを比較できます。

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） 分散型 MFIB は、アクティブスイッチがスタック内の他のメンバースイッチに 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。 MFIB には、ラインカード全体の複製に関するプラットフォーム固有の情報も含めることができます。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 VRF Lite

（注） IPv6 マルチキャスト VRF Lite をサポートするためには、スイッチで Network Advantage ライセンスを実行している必要があります。

IPv6 マルチキャスト VRF Lite 機能は、複数の仮想ルーティングおよび転送（VRF）コンテキストに対する IPv6 マルチキャスト サポートを提供します。これらの VRF の範囲は、VRF が定義されているデバイスに制限されています。

この機能により、別の VRF に属するデバイス間の通信は、明示的に設定されていない限り許可されないため、より高いレベルのセキュリティでのルーティングと転送の切り分けができます。IPv6 マルチキャスト VRF Lite 機能は、特定の VRF に属するトラフィックの管理とトラブルシューティングを容易にします。

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 マルチキャストでの NSF と SSO のサポート

Network Advantage ライセンスを実行しているスイッチは、IPv6 のノン ストップ フォワーディング（NSF）およびステートフル スイッチオーバー（SSO）をサポートします。

詳細については、『*Stack Manager and High Availability Configuration Guide*』の「*Configuring NSF with SSO*」を参照してください。

IPv6 対応の NTP

ネットワーク タイム プロトコル（NTP）は、マシンのネットワークの時刻同期を行うように設計されたプロトコルです。NTP は UDP 上で動作し、UDP は IPv4 上で動作します。NTP バージョン 4（NTPv4）は、NTP バージョン 3 を拡張したもので、IPv4 と IPv6 の両方をサポートします。

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 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

IPV6 マルチキャストルーティングを有効にするには、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： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	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-routing** 例： デバイス(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 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 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

インターフェイスの MLD をカスタマイズして確認するには、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： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	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： デバイス(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 join-group** [*group-address*] [**include** | **exclude**] {*source-address* | **source-list** [*acl*]} 例： `デバイス(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。
ステップ 5	**ipv6 mld access-group** *access-list-name* 例： `デバイス(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 6	**ipv6 mld static-group** [*group-address*] [**include** | **exclude**] {*source-address* | source-list [*acl*]} 例： `デバイス(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 7	**ipv6 mld query-max-response-time** *seconds* 例： `デバイス(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： `デバイス(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 mld groups [link-local]** [*group-name* | *group-address*] [*interface-type interface-number*] [**detail** | **explicit**] 例： `デバイス# 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： `デバイス# 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。
ステップ 11	**show ipv6 mld interface** [*type number*] 例：	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
	デバイス# **show ipv6 mld interface GigabitEthernet 1/0/1**	
ステップ 12	**debug ipv6 mld** [*group-name* | *group-address* | *interface-type*] 例： デバイス# **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： デバイス# **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

MLD グループ制限をグローバルに実装するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 mld** [*vrf vrf-name*] **state-limit** *number*
4. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： デバイス# **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： デバイス(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

MLD グループ制限をインターフェイスごとに実装するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type** *number*
4. **ipv6 mld limit** *number* [**except**]*access-list*
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **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： デバイス(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： デバイス(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。

受信側の明示的トラッキングを設定してホストの動作を追跡するには、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： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	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： デバイス(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 mld explicit-tracking** *access-list-name* 例： デバイス(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 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。

MLD トラフィック カウンタのリセット

MLD トラフィックカウンタをリセットするには、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： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **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	**clear ipv6 mld traffic** 例： デバイス# **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 4	**show ipv6 mld traffic** 例： デバイス# **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 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。

MLD インターフェイス カウンタのクリア

MLD インターフェイスカウンタをクリアするには、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： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **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 3	**clear ipv6 mld counters** *interface-type* 例： デバイス# **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 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。

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

PIM-SM を設定し、グループ範囲の PIM-SM 情報を表示するには、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： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **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 pim **rp-address** *ipv6-address*[*group-access-list*] 例： デバイス(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 4	**exit** 例： デバイス(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 5	**show ipv6 pim interface** [state-on] [**state-off**] [*type-number*] 例：	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。

	コマンドまたはアクション	目的
	デバイス# **show ipv6 pim interface**	
ステップ 6	**show ipv6 pim group-map** [*group-name* | group-address] | [*group-range* | *group-mask*] [**info-source {bsr** | **default** | **embedded-rp** | **static**}] 例： デバイス# **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 7	**show ipv6 pim neighbor** [**detail**] [*interface-type interface-number* | **count**] 例： デバイス# **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 8	**show ipv6 pim range-list** [**config**] [*rp-address* | *rp-name*] 例： デバイス# **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。
ステップ 9	**show ipv6 pim tunnel** [*interface-type interface-number*] 例： デバイス# **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 10	**debug ipv6 pim** [*group-name* | *group-address* | **interface** *interface-type* | **bsr** | **group** | **mvpn** | **neighbor**] 例： デバイス# **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 11	**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

PIM オプションを設定するには、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：	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	デバイス> **enable**	
ステップ 2	**configure terminal** 例： デバイス# **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 pim spt-threshold infinity** [**group-list** *access-list-name*] 例： デバイス(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 4	**ipv6 pim accept-register** { **list** *access-list* | **route-map** *map-name*} 例： デバイス(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。
ステップ 5	**interface** *type number* 例： デバイス(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 6	**ipv6 pim dr-priority** *value* 例： デバイス(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 7	**ipv6 pim hello-interval** *seconds* 例： デバイス(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 8	**ipv6 pim join-prune-interval** *seconds* 例： デバイス(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。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： デバイス(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 10	**ipv6 pim join-prune statistic** [*interface-type*] 例： デバイス(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 11	**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。

PIM トラフィックカウンタをリセットするには、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： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **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	**clear ipv6 pim traffic** 例： デバイス# **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 4	**show ipv6 pim traffic** 例：	PIM トラフィック カウンタを表示します。

	コマンドまたはアクション	目的
	デバイス# **show ipv6 pim traffic**	
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。

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。

PIM トポロジテーブルをクリアして MRIB 接続をリセットするには、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： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **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	**clear ipv6 pim topology** [*group-name* | *group-address*] 例： デバイス# **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 4	**show ipv6 mrib client** [**filter**] [**name** {*client-name* | *client-name* **: client-id**}] 例： デバイス# **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。
ステップ 5	**show ipv6 mrib route** {**link-local** | **summary** | [*sourceaddress-or-name* | *] [*groupname-or-address*[*prefix-length*]]] 例： デバイス# **show ipv6 mrib route**	MRIB ルート情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	**show ipv6 pim topology** [*groupname-or-address* [*sourceaddress-or-name*] | **link-local** | **route-count** [**detail**]] 例： デバイス# **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 7	**debug ipv6 mrib client** 例： デバイス# **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 8	**debug ipv6 mrib io** 例： デバイス# **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 9	**debug ipv6 mrib proxy** 例： デバイス# **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 10	**debug ipv6 mrib route** [*group-name* | *group-address*] 例： デバイス# **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 11	**debug ipv6 mrib table** 例： デバイス# **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 12	**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。詳細については、「*EIGRP* スタブルーティング」の項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

次の表に、デバイス の IPv6 PIM ルーティングのデフォルト設定を示します。

表 *1:* 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
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

IPV6 PIM スタブルーティングをイネーブルにするには、次の手順を実行します。

始める前に

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 multicast pim-passive-enable**
4. **interface** *interface-id*
5. **ipv6 pim**
6. **ipv6 pim** {**bsr**} | {**dr-priority** | *value*} | {**hello-interval** | *seconds*} | {**join-prune-interval** | *seconds*} | {**passive**}
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# 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： `デバイス(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： `デバイス(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。 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

	コマンドまたはアクション	目的
		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。
ステップ 5	**ipv6 pim** 例： `デバイス(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： `デバイス(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 優先順位を設定します。 **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：	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
	デバイス(config-if)# **end**	

IPv6 PIM スタブ ルーティングのモニタ

表 *2 : PIM* スタブ設定の *show* コマンド

コマンド	目的
show ipv6 pim interface デバイス# **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 デバイス# **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 デバイス# **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。

IPv6 PIM での組み込み RP サポートのディセーブル化

ドメイン内のすべてのデバイスが組み込み RP をサポートしていない場合、必要に応じて、インターフェイスで組み込み RP サポートを無効化できます。

（注） この作業では、IPv6 PIM での組み込み RP サポートだけでなく、PIM を完全にディセーブルにします。

IPv6 PIM の組み込み RP サポートを無効化するには、次の手順を実行します。

手順の概要

1. **enable**
2. **enable**
3. **configure terminal**
4. **no ipv6 pim** [**vrf** *vrf-name*] **rp embedded**
5. **interface** *type number*
6. **no ipv6 pim**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 3	**configure terminal** 例： `デバイス# 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 4	**no ipv6 pim** [**vrf** *vrf-name*] **rp embedded** 例： `デバイス(config)# no ipv6 pim rp embedded`	IPv6 PIM での組み込み RP サポートをディセーブルにします。
ステップ 5	**interface** *type number* 例： `デバイス(config)# interface FastEthernet 1/0`	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 6	**no ipv6 pim** 例： `デバイス(config-if)# no ipv6 pim`	指定したインターフェイスで IPv6 PIM をオフにします。

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

BSR 情報を設定および確認するには、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： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **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 pim bsr candidate bsr** *ipv6-address*[*hash-mask-length*] [**priority** *priority-value*] 例： デバイス(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 4	**interface** *type number* 例： デバイス(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 bsr border** 例： デバイス(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 6	**exit** 例： デバイス(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 7	**show ipv6 pim** bsr {**election** | **rp-cache** | **candidate-rp**} 例： デバイス(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 8	**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

BSR に PIM RP アドバタイズメントを送信するには、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： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **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 pim bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] **[priority** *priority-value*] [**interval** seconds] 例： デバイス(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。
ステップ 4	**interface** *type number* 例： デバイス(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 bsr border** 例： デバイス(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 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。

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

スコープゾーン内で使用する BSR を設定するには、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： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： デバイス# **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 pim bsr candidate rp** *ipv6-address* [*hash-mask-length*] [**priority** priority-value] 例： デバイス(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 4	**ipv6 pim bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** seconds] 例： デバイス(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。
ステップ 5	**interface** *type number* 例： デバイス(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 6	**ipv6 multicast boundary scope** *scope-value* 例： デバイス(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 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 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。

スコープと RP のマッピングをアナウンスするように BSR スイッチを設定するには、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： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **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 pim bsr announced rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] 例： デバイス(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 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。

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。

SSM マッピングを設定するには、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： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： デバイス# **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 ssm-map enable** 例： デバイス(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 4	**no ipv6 mld ssm-map query dns** 例： デバイス(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 5	**ipv6 mld ssm-map static** *access-list source-address* 例： デバイス(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。
ステップ 6	**exit** 例： デバイス(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 7	**show ipv6 mld ssm-map** [*source-address*] 例： デバイス(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 8	**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。

静的 mroute を設定するには、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**： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **例**： デバイス# **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 route** {*ipv6-prefix / prefix-length ipv6-address* | *interface-type interface-number ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | *unicast* | *multicast*] [**tag** *tag*] **例**： デバイス(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。
ステップ 4	**exit** **例**： デバイス# **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 5	**show ipv6 mroute** [link-local | [*group-name* | *group-address* [*source-address* | *source-name*]] **[summary]** [**count**] **例**： デバイス# **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。

	コマンドまたはアクション	目的
ステップ 6	**show ipv6 mroute** [**link-local** | *group-name* | *group-address*] **active** [*kbps*] 例： `デバイス(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 7	**show ipv6 rpf** [*ipv6-prefix*] 例： `デバイス(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 8	**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

IPv6 マルチキャストで MFIB の動作を確認するには、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： `デバイス> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**show ipv6 mfib** [| **verbose** | *group-address-name* | *ipv6-prefix / prefix-length* | *source-address-name* | **count** | **interface** | **status** | **summary**] 例： `デバイス# 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 3	**show ipv6 mfib** [all | linkscope | group-name | group-address [source-name | source-address]] **count** 例： `デバイス# 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。

	コマンドまたはアクション	目的
ステップ 4	**show ipv6 mfib interface** 例： デバイス# **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 5	**show ipv6 mfib status** 例： デバイス# **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 6	**show ipv6 mfib summary** 例： デバイス# **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 7	**debug ipv6 mfib** [*group-name* | *group-address*] [**adjacency** | **db** | **fs** | **init** | **interface** | **mrib** [**detail**] | **nat** | **pak** | **platform** | **ppr** | **ps** | **signal** | **table**] 例： デバイス# **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

MFIB トラフィックカウンタをリセットするには、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： デバイス> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**clear ipv6 mfib counters** [*group-name* | **group-address** [*source-address* | *source-name*]] 例： デバイス# **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。

その他の参考資料

標準および RFC

標準/RFC	タイトル
RFC 4292	*IP* 転送テーブル
RFC 4293	『*Management Information Base for the Internet Protocol (IP)*』

IPv6 マルチキャストの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *3 : IPv6* マルチキャストの機能情報

機能名	リリース	機能情報
IPv6 マルチキャスト	Cisco IOS XE Fuji 16.9.2	IPv6 向けマルチキャスト機能