CHAPTER 41

IPv6 マルチキャストの実装

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。

ここでは、IPv6 マルチキャストを設定する方法について説明します。コマンド リファレンスについては、『Cisco IOS IPv6 Command Reference』を参照してください。

IPv6 マルチキャストの実装に関する情報

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。

（注）　IPv6 マルチキャスト ルーティングは、IP ベース イメージでのみサポートされます。

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。

マルチキャスト リスナー ディスカバリ プロトコル（IPv6）

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 クエリアおよびホストの違いは次のとおりです。

- 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。
- ホストは、レポート メッセージを送信して、クエリアにホスト メンバーシップを通知する受信側（スイッチを含む）です。

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 では、次の 3 種類のメッセージが使用されます。

- クエリー：一般、グループ固有、およびマルチキャスト アドレス固有。MLD から一般クエリーが送信されると、マルチキャスト アドレス フィールドは 0 に設定されます。一般クエリーでは、接続されているリンク上にリスナーが存在するマルチキャスト アドレスを学習します。

グループ固有のクエリーとマルチキャスト アドレス固有のクエリーはどちらも、マルチキャスト アドレス フィールドをクエリーされているアドレスに設定します。グループ アドレスはマルチキャスト アドレスです。

- レポート：レポート メッセージでは、マルチキャスト アドレス フィールドは、送信側がリッスンしている特定の IPv6 マルチキャスト アドレスのフィールドになります。
- Done：Done メッセージでは、マルチキャスト アドレス フィールドは、MLD メッセージの送信元がすでにリッスンしていない特定の IPv6 マルチキャスト アドレスのフィールドになります。

（注）　MLD バージョン 2 には、Done メッセージはありません。

MLD レポートの送信には、有効な IPv6 リンクローカル送信元アドレスを使用するか、または送信側インターフェイスが有効なリンクローカル アドレスをまだ取得していない場合は未指定アドレス（::）を使用する必要があります。未指定アドレスでのレポートの送信は、ネイバー探索プロトコルでの IPv6 マルチキャストの使用をサポートできます。

ステートレス自動設定で Duplicate Address Detection（DAD; 重複アドレス検出）を実行するためには、ノードは複数の IPv6 マルチキャスト グループに加入する必要があります。DAD を実行する前は、インターフェイスの送信用にレポーティング ノードが使用するアドレスは一時的なアドレスのみであり、通信には使用できません。そのため、未指定アドレスを使用する必要があります。

MLD バージョン 2 または MLD バージョン 1 のメンバーシップ レポートから生成される MLD ステートは、グローバルに、またはインターフェイス単位で制限できます。MLD グループ制限機能は、MLD パケットによって生じる Denial of Service（DoS; サービス拒絶）攻撃に対する保護を提供します。設定されている制限を超過するメンバーシップ レポートは MLD キャッシュには格納されず、これらの超過メンバーシップ レポートのトラフィックは転送されません。

MLD では、送信元フィルタリングがサポートされています。送信元フィルタリングにより、特定の送信元アドレスからのパケット（SSM をサポートするのに必要）、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特定のマルチキャスト アドレスに送信されたパケットをリッスンする対象をノードがレポートできるようになります。

MLD を使用するホストが Leave メッセージを送信した場合、スイッチはクエリー メッセージを送信することによって、このホストがグループに加入した最後のホストであることを再確認する必要があります。再確認後、トラフィックの転送を停止できます。この処理には約 2 秒かかります。この「脱退遅延」は、IPv4 マルチキャスト対応 IGMP バージョン 2 にも存在します。

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。

IPv6 マルチキャスト ユーザ認証およびプロファイル サポート

IPv6 マルチキャストは、ネットワーク内の任意のホストがマルチキャスト グループの受信側または送信元になれる設計になっています。したがって、ネットワークのマルチキャスト トラフィックを制御するには、マルチキャスト アクセス コントロールが必要です。アクセス コントロール機能は、主に、送信元のアクセス コントロールとアカウンティング、受信側のアクセス コントロールとアカウンティング、およびこのアクセス コントロール メカニズムのプロビジョニングで構成されます。

マルチキャスト アクセス コントロールは、マルチキャストと認証、認可、アカウンティング（AAA）間のインターフェイスを提供し、ラストホップ スイッチ、マルチキャストにおける受信側アクセス コントロール機能、およびマルチキャストにおけるグループまたはチャネル ディセーブル化機能でのプロビジョニング、認可、およびアカウンティングを実現します。

新しいマルチキャスト サービス環境を展開する場合、ユーザ認証を追加し、インターフェイス単位でユーザ プロファイルのダウンロードを行う必要があります。AAA と IPv6 マルチキャストを使用すると、マルチキャスト環境でのユーザ認証とユーザ プロファイルのダウンロードがサポートされます。

RADIUS サーバからアクセス スイッチへのマルチキャスト アクセス コントロール プロファイルのダウンロードをトリガーするイベントは、アクセス スイッチへの MLD join の着信です。このイベントが発生すると、ユーザは認可キャッシュのタイム アウトを発生させて定期的なダウンロードを要求するか、または適切な multicast clear コマンドを使用してプロファイルが変更された場合に新規ダウンロードをトリガーできます。

アカウンティングは RADIUS アカウンティングを使用して行われます。開始および停止アカウンティング レコードは、アクセス スイッチから RADIUS サーバに送信されます。リソースの消費をストリーム単位で追跡できるように、これらのアカウンティング レコードには、マルチキャスト送信元およびグループに関する情報が含まれています。ラストホップ スイッチが新しい MLD レポートを受信すると、開始レコードが送信され、MLD leave を受信するか、何らかの理由によりグループまたはチャネルが削除されると、停止レコードが送信されます。

IPv6 MLD プロキシ

MLD プロキシ機能は、スイッチのアップストリーム インターフェイス上で、スイッチがすべての（*, G）および（S, G）エントリに対して MLD メンバーシップ レポートを生成するか、またはこれらのエントリのユーザ定義サブセットを生成するメカニズムを提供します。MLD プロキシ機能により、デバイスは、プロキシ グループ メンバーシップ情報を学習し、その情報に基づいてマルチキャスト パケットを転送できるようになります。

スイッチが mroute プロキシ エントリの RP として動作する場合、これらのエントリの MLD メンバーシップ レポートを、ユーザが指定したプロキシ インターフェイス上で生成できます。

プロトコル独立マルチキャスト

プロトコル独立マルチキャスト（PIM）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。

指定スイッチ

Cisco スイッチは、LAN セグメント上に複数のスイッチが存在する場合、PIM-SM を使用してマルチキャスト トラフィックを転送し、選択プロセスに従って指定スイッチを選択します。

指定スイッチは、PIM register メッセージ、PIM join メッセージ、および PIM prune メッセージを RP に送信し、アクティブな送信元およびホスト グループ メンバーシップに関する情報を通知します。

LAN 上に複数の PIM-SM スイッチが存在する場合は、指定スイッチを選択して、接続されているホストに対するマルチキャスト トラフィックの重複を回避する必要があります。**ipv6 pim dr-priority** コマンドを使用して DR の選択を強制することを選択しない限り、最も大きい IPv6 アドレスの PIM スイッチが LAN の DR になります。このコマンドでは、LAN セグメント上の各スイッチの DR プライオリティ（デフォルトのプライオリティ = 1）を指定して、最もプライオリティの高いスイッチが DR として選択されるようにすることができます。LAN セグメント上のすべてのスイッチのプライオリティが同じ場合にも、最上位 IPv6 アドレスを持つスイッチが使用されます。

DR で障害が発生した場合、PIM-SM はスイッチ A の障害を検出し、フェールオーバー DR を選択する手段を提供します。DR（スイッチ A）が動作不能になった場合、スイッチ A とネイバーとの隣接関係がタイムアウトすると、スイッチ B はその状況を検出します。スイッチ B はホスト A から MLD メンバーシップ レポートを受けているため、このインターフェイスでグループ A の MLD ステートをすでに持ち、新しい DR になると即座に RP に join を送信します。この段階で、スイッチ B を経由する共有ツリーの新しいブランチの下位方向へのトラフィック フローが再び確立されます。また、ホスト A がトラフィックを送信していた場合、スイッチ B は、ホスト A から次のマルチキャスト パケットを受信した直後に、新しい登録プロセスを開始します。このアクションがトリガーとなって、RP は、スイッチ B を経由する新しいブランチを介して、ホスト A への SPT に加入します。

（注）
- 2 つの PIM スイッチが直接接続されている場合、これらのスイッチはネイバーになります。PIM ネイバーを表示するには、**show ipv6 pim neighbor** 特権 EXEC コマンドを使用します。
- DR 選択プロセスは、マルチアクセス LAN のみで必要です。

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、スイッチは、スタティックに設定されている 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。スイッチが RP である場合、RP としてスタティックに設定する必要があります。

スイッチは、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、スイッチ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。スイッチが 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、スイッチ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 つ以上のスイッチを選択する必要もあります。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 スイッチによって直接 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、ファーストホップ スイッチによって PIM register メッセージを送信するために使用されます。また、RP アドレスは、ラストホップ スイッチによって 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。すべてのスイッチ（RP スイッチを含む）で RP アドレスを設定する必要があります。

1 つの PIM スイッチを複数のグループの RP にすることができます。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、スイッチがどのグループの 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。

PIMv6 エニーキャスト RP ソリューションの概要

IPv6 PIM のエニーキャスト RP ソリューションは、IPv6 ネットワークによる PIM-SM RP のエニーキャスト サービスのサポートを可能にします。これにより、PIM のみを実行するドメイン内でエニーキャスト RP を使用できるようになります。この機能は、ドメイン間接続が不要な場合に便利です。エニーキャスト RP は、IPv4 および IPv6 で使用できますが、IPv4 だけで動作する Multicast Source Discovery Protocol（MSDP）には依存しません。

エニーキャスト RP は、PIM RP のデバイスに障害が発生した場合に、高速コンバージェンスを取得するために ISP ベースのバックボーンが使用するメカニズムです。受信側および送信元が最も近くの RP にランデブーできるようにするには、送信元からのパケットがすべての RP に到達して、加入している受信側を検出する必要があります。

ユニキャスト IP アドレスは RP アドレスとして選択されます。このアドレスは、静的に設定されるか、またはダイナミック プロトコルを使用して、ドメイン全体のすべての PIM デバイスに配信されます。ドメイン内の一連のデバイスが、この RP アドレスの RP として動作するように選択されます。これらのデバイスは、エニーキャスト RP セットと呼ばれます。エニーキャスト RP セット内の各デバイスは、RP アドレスを使用してループバック インターフェイスで設定されます。また、エニーキャスト RP セット内の各デバイスには、RP 間の通信に使用する別の物理 IP アドレスも必要です。

RP アドレス、または RP アドレスに対応するプレフィックスは、ドメイン内部のユニキャスト ルーティング システムに挿入されます。エニーキャスト RP セット内の各デバイスは、エニーキャスト RP セット内のその他すべてのデバイスのアドレスで設定されます。また、この設定は、セット内のすべての RP で一致している必要があります。

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、Candidate-RP-Advertisement（C-RP-Adv; 候補 RP アドバタイズメント）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 Bootstrap Message（BSM; ブートストラップ メッセージ）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 送信元固有マルチキャスト

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。

IPv6 用の SSM マッピング

IPv6 用の SSM マッピングでは、MLD バージョン 1 の受信側用にスタティックとダイナミックの両方のドメイン ネーム システム（DNS）マッピングがサポートされています。この機能を使用すると、TCP/IP ホスト スタックおよび IP マルチキャスト受信アプリケーションで MLD バージョン 2 サポートを提供できないホストで IPv6 SSM を展開できます。

SSM マッピングにより、スイッチは実行コンフィギュレーションまたは DNS サーバのいずれかでマルチキャスト MLD バージョン 1 レポートの送信元を検索できるようになります。そのあと、スイッチは送信元に対する（S, G）join を開始できます。

PIM 共有ツリーおよび送信元ツリー（最短パス ツリー）

デフォルトでは、グループのメンバは、RP をルートとする単一のデータ配布ツリーを通じて、送信側からグループへのデータを受信します。このタイプの配布ツリーは、共有ツリーまたはランデブー ポイント ツリー（RPT）と呼ばれます（下の図を参照）。送信側からのデータは、RP に配信され、その共有ツリーに加入しているグループ メンバに配布されます。

データしきい値で保証される場合、共有ツリー上のリーフ スイッチは、送信元をルートとするデータ配布ツリーへの切り替えを開始できます。このタイプの配布ツリーは、最短パス ツリーまたは送信元ツリーと呼ばれます。デフォルトでは、Cisco IOS ソフトウェアは、送信元から最初のデータ パケットを受信した時点で、送信元ツリーへの切り替えを行います。

次に、共有ツリーから送信元ツリーに切り替わるプロセスの詳細を示します。

1. 受信側がグループに加入します。リーフ スイッチ C が RP に join メッセージを送信します。
2. RP がスイッチ C へのリンクを発信インターフェイス リストに登録します。
3. 送信元がデータを送信します。スイッチ A が register にデータをカプセル化し、それを RP に送信します。
4. RP が共有ツリーの下位方向のスイッチ C にデータを転送し、送信元に join メッセージを送信します。この時点で、データはスイッチ C に 2 回（カプセル化された状態で 1 回、ネイティブの状態で 1 回）着信する可能性があります。
5. データがネイティブの（カプセル化されていない）状態で RP に着信すると、RP はスイッチ A に register-stop メッセージを送信します。
6. デフォルトでは、最初のデータ パケット受信時に、スイッチ C が Join メッセージを送信元に送信するよう要求します。
7. スイッチ C は、（S, G）でデータを受信すると、共有ツリーの上位方向にある送信元に prune メッセージを送信します。
8. RP が（S, G）の発信インターフェイスからスイッチ C へのリンクを削除します。
9. RP が送信元への prune メッセージをトリガーします。

送信元および RP に join および prune メッセージが送信されます。これらのメッセージはホップバイホップで送信され、送信元または RP へのパス上にある各 PIM スイッチで処理されます。register および register-stop メッセージは、ホップバイホップで送信されません。これらのメッセージは、送信元に直接接続されている指定スイッチによって送信され、グループの RP によって受信されます。

Reverse Path Forwarding

Reverse Path Forwarding は、マルチキャスト データグラムの転送に使用されます。これは、次のように機能します。

- スイッチで、送信元へのユニキャスト パケットの送信に使用しているインターフェイスでデータグラムを受信すると、パケットは RPF インターフェイスに着信しています。
- パケットが RPF インターフェイスに着信した場合、スイッチは、マルチキャスト ルーティング テーブル エントリの発信インターフェイス リストに存在するインターフェイスにパケットを転送します。
- パケットが RPF インターフェイスに着信しない場合、パケットはループを回避するためにサイレントにドロップされています。

PIM では、送信元ツリーと RP をルートとする共有ツリーの両方を使用してデータグラムを転送します。RPF チェックは、次のようにそれぞれ異なる方法で実行されます。

- PIM スイッチが送信元ツリー ステートである場合（つまり、(S, G）エントリがマルチキャスト ルーティング テーブル内にある場合)、マルチキャスト パケットの送信元の IPv6 アドレスに対して RPF チェックが実行されます。
- PIM スイッチが共有ツリー ステートである場合（および送信元ツリー ステートが明示されていない場合)、（メンバがグループに加入している場合は既知である）RP のアドレスに対して RPF チェックが実行されます。

空間モード PIM では、RPF ルックアップ機能を使用して、join および prune の送信先を決定します。(S, G）join（送信元ツリー ステート）は送信元に向けて送信されます。(*, G）join（共有ツリー ステート）は RP に向けて送信されます。

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。

双方向 PIM

双方向 PIM により、マルチキャスト スイッチは、PIM-SM の単方向共有ツリーと比較して、保持するステート情報を減らすことができます。双方向共有ツリーは、データを送信元からランデブー ポイント アドレス（RPA）に伝送し、それらを RPA から受信側に配布します。PIM-SM とは異なり、双方向 PIM は送信元ツリーへの切り替えは実行しません。また、送信元から RP へのデータの登録カプセル化は行われません。

指定された単一のフォワーダ（DF）が、双方向 PIM ドメイン内のすべてのリンク（マルチアクセスおよびポイントツーポイント リンクを含む）の各 RPA 用に存在しています。唯一の例外は、DF が存在しない RPL です。DF は、MRIB が提供するメトリックとの比較で決定される、RPA への最適なルートを持つリンク上のスイッチです。指定された RPA の DF は、リンクにダウンストリーム トラフィックを転送し、リンクからのアップストリーム トラフィックをランデブー ポイント リンク（RPL）に転送します。DF は、RPA にマップするすべての双方向グループに対してこの機能を実行します。また、リンク上の DF は、リンク上のダウンストリーム スイッチからの Join メッセージを処理するとともに、MLD などのローカル メンバーシップ メカニズムによって検出されたローカル受信者にパケットが転送されることを保証します。

双方向 PIM は、中レートまたは低レートの送信元が多数存在する場合に役立ちます。ただし、双方向共有ツリーの遅延特性は、PIM-SM で構築された送信元ツリーよりもさらに劣る可能性があります（トポロジに依存）。

IPv6 では、双方向 RP のスタティック設定だけがサポートされています。

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

Multicast Routing Information Base（MRIB; マルチキャスト ルーティング情報ベース）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 Multicast Forwarding Information Base（MFIB; マルチキャスト転送情報ベース）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。

分散型 MFIB

Distributed MFIB（dMFIB; 分散型 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、dMFIB 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。

dMFIB は、次の機能を実装します。

- ラインカードに MFIB のコピーを配布します。
- 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。
- RP に存在するクライアントがオンデマンドでトラフィックの統計情報を読み取れるようにするフックを提供します （dMFIB はこれらの統計情報を RP に定期的にアップロードすることはありません）。

また、dMFIB 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

IPv6 マルチキャスト VRF Lite 機能は、複数の Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）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 のスコープは、VRF が定義されているスイッチ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、ルート プロセッサ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、RP 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）を設定するために、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 マルチキャストでの NSF と SSO のサポート

IPv6 マルチキャストでは、Nonstop Forwarding（NSF; ノンストップ フォワーディング）およびステートフル スイッチオーバー（SSO）がサポートされています。

IPv6 マルチキャストの帯域幅ベースの CAC

IPv6 マルチキャストの帯域幅ベースのコール アドミッション制御（CAC）機能は、コスト乗数を使用してインターフェイス単位の mroute ステート リミッタをカウントする手段を実装します。この機能を使用すると、マルチキャスト フローで異なる量の帯域幅が使用されるネットワーク環境で、インターフェイス単位の帯域幅ベースの CAC を提供できます。

この機能では、IPv6 マルチキャスト ステートを詳細に制限および考慮します。この機能を設定すると、IPv6 マルチキャスト PIM トポロジの着信インターフェイスまたは発信インターフェイスとして使用できる回数にインターフェイスを制限できます。

この機能を使用すると、スイッチ管理者はアクセス リストと一致するステートに対してグローバル制限コスト コマンドを設定して、インターフェイス制限に対してこのようなステートを考慮するときに使用するコスト乗数を指定できます。この機能では、異なる帯域幅要件に応じてコスト乗数を適切に調整することによって、帯域幅ベースのローカル CAC ポリシーを柔軟に実装できます。

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。

	コマンド	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 multicast-routing** [**vrf** *vrf-name*] 例： `Switch(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。

	コマンド	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： `Switch(config)# interface FastEthernet 1/0`	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： `Switch(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 4	**ipv6 mld access-group** *access-list-name* 例： `Switch(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。

	コマンド	目的
ステップ 5	**ipv6 mld static-group** *group-address*] [**include**| **exclude**] {*source-address* | source-list [*acl*]} **例：** `Switch(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** *seconds* **例：** `Switch(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** *seconds* **例：** `Switch(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：** `Switch(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** [**vrf** *vrf-name*] **groups** [**link-local**] [*group-name* | *group-address*] [*interface-type interface-number*] [**detail** | **explicit**] **例：** `Switch# show ipv6 mld groups FastEthernet 2/1`	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：** `Switch# 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** [**vrf** *vrf-name*] **interface** [*type number*] **例：** `Switch# show ipv6 mld interface FastEthernet 2/1`	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：** `Switch# 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：** `Switch# 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

特権 EXEC モードで次の手順を実行します。

	コマンド	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 mld** [vrf *vrf-name*] **state**-limit *number* **例：** `Switch(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 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 グループ制限のインターフェイス単位での実装

特権 EXEC モードで次の手順を実行します。

	コマンド	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：** `Switch(config)# interface FastEthernet 1/0`	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 limit** *number* [**except** *access-list* **例：** `Switch(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 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。

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。

	コマンド	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：** `Switch(config)# interface FastEthernet 1/0`	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：** `Switch(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。

マルチキャスト ユーザ認証およびプロファイル サポートの設定

マルチキャスト ユーザ認証およびプロファイル サポートを設定する前に、次の制約事項を認識しておく必要があります。

- ポート、インターフェイス、VC、または VLAN ID がユーザまたは加入者アイデンティティになります。ホスト名、ユーザ ID、またはパスワードを使用したユーザ アイデンティティはサポートされていません。
- IPv6 マルチキャストに対する AAA アクセス コントロールのイネーブル化
- 方式リストの指定およびマルチキャスト アカウンティングのイネーブル化
- スイッチでの未認証マルチキャスト トラフィックの受信のディセーブル化
- MLD インターフェイスでの認可ステータスのリセット

IPv6 マルチキャストに対する AAA アクセス コントロールのイネーブル化

特権 EXEC モードで次の手順を実行します。

	コマンド	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	**aaa new-model** **例：** `Switch(config)# aaa new-model`	AAA アクセス コントロール システム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。

方式リストの指定およびマルチキャスト アカウンティングのイネーブル化

次の作業では、AAA 認可およびアカウンティングに使用される方式リストを指定する方法、およびインターフェイス上の指定したグループまたはチャネルでマルチキャスト アカウンティングをイネーブルにする方法を示します。

特権 EXEC モードで次の手順を実行します。

	コマンド	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	**aaa authorization multicast default** [*method3* | *method4*] **例：** `Switch(config)# aaa authorization multicast default`	AAA 認可をイネーブルにし、IPv6 マルチキャスト ネットワークへのユーザ アクセスを制限するパラメータを設定します。
ステップ 3	**aaa accounting multicast default** [**start-stop** | **stop-only**] [**broadcast**] [*method1*] [*method2*] [*method3*] [*method4*] **例：** `Switch(config)# aaa accounting multicast default`	課金、または RADIUS を使用する際のセキュリティのために、IPv6 マルチキャスト サービスの AAA アカウンティングをイネーブルにします。
ステップ 4	**interface** *type number* **例：** `Switch(config)# interface FastEthernet 1/0`	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 aaa account receive** *access-list-name* [**throttle** *throttle-number*] **例：** `Switch(config-if)# ipv6 multicast aaa account receive list1`	指定したグループまたはチャネルで AAA アカウンティングをイネーブルにします。
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。

スイッチでの未認証マルチキャスト トラフィックの受信のディセーブル化

状況によっては、アクセス コントロール プロファイルに従って加入者の認証とチャネルの認可が行われていないかぎり、マルチキャスト トラフィックの受信を防止することが必要となる場合があります。つまり、アクセス コントロール プロファイルで特に指定がなければ、トラフィックを完全になくす必要があります。

未認証グループまたは未認可チャネルからマルチキャスト トラフィックをスイッチが受信しないようにするには、次の作業を実行します。

特権 EXEC モードで次の手順を実行します。

	コマンド	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 multicast** [vrf *vrf-name*] **group-range**[*access-list-name*] **例：** `Switch(config)# ipv6 multicast group-range`	スイッチのすべてのインターフェイスで未認可グループまたはチャネルのマルチキャスト プロトコル アクションおよびトラフィック転送をディセーブルにします。
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。

IPv6 での MLD プロキシのイネーブル化

特権 EXEC モードで次の手順を実行します。

	コマンド	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 mld host-proxy** [*group-acl*] **例：** `Switch(config)# ipv6 mld host-proxy proxy-group`	MLD プロキシ機能をイネーブルにします。
ステップ 3	**ipv6 mld host-proxy interface** [*group-acl*] **例：** `Switch(config)# ipv6 mld host-proxy interface Ethernet 0/0`	RP 上の指定したインターフェイス上で MLD プロキシ機能をイネーブルにします。
ステップ 4	**show ipv6 mld host-proxy** [*interface-type interface-number*] **group** [*group-address*]] **例：** `Switch(config)# show ipv6 mld host-proxy Ethernet0/0`	IPv6 MLD ホスト プロキシ情報を表示します。
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 インターフェイスでの認可ステータスのリセット

インターフェイスを指定しない場合は、すべての MLD インターフェイスで認可がリセットされます。

特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**clear ipv6 multicast aaa authorization** [*interface-type interface-number*] **例：** `Switch# clear ipv6 multicast aaa authorization FastEthernet 1/0`	IPv6 マルチキャスト ネットワークへのユーザ アクセスを制限するパラメータをクリアします。
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。

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。

	コマンド	目的
ステップ 1	clear ipv6 mld [vrf vrf-name] traffic 例： `Switch# 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 mld** [vrf *vrf-name*] **traffic** 例： `Switch# 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。

	コマンド	目的
ステップ 4	**clear ipv6 mld** [vrf *vrf-name*] **counters** *interface-type* 例： `Switch# 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 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 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。

	コマンド	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 [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] [**bidir**] 例： `Switch(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。

	コマンド	目的
ステップ 3	**exit** **例：** `Switch(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 pim** [**vrf** *vrf-name*] **interface** [state-on] [**state-off**] [*type number*] **例：** `Switch# 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 pim** [**vrf** *vrf-name*] **group-map** [*group-name* | group-address] | [*group-range* | *group-mask*] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}] **例：** `Switch# 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 pim** [vrf *vrf-name*] **neighbor** [**detail**] [*interface-type interface-number* | **count**] **例：** `Switch# 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 pim** [**vrf** *vrf-name*] **range-list**[**config**] [*rp-address* | *rp-name*] **例：** `Switch# 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 8	**show ipv6 pim** [**vrf** *vrf-name*] **tunnel** [*interface-type interface-number*] **例：** `Switch# 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：** `Switch# 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。

	コマンド	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** [**vrf** *vrf-name*] **spt-threshold infinity** [**group-list** *access-list-name*] **例：** `Switch(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 pim** [vrf *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*} **例：** `Switch(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 4	**interface** *type number* **例：** `Switch(config)# interface FastEthernet 1/0`	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：** `Switch(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** *seconds* **例：** `Switch(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** *seconds* **例：** `Switch(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：** `Switch(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 pim** [vrf *vrf-name*] **join-prune statistic** [*interface-type*] **例：** `Switch# 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。

双方向 PIM の設定および双方向 PIM 情報の表示

特権 EXEC モードで次の手順を実行します。

	コマンド	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** [*vrf vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] [**bidir**] **例：** `Switch(config)# ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C bidir`	特定のグループ範囲の PIM RP のアドレスを設定します。**bidir** キーワードを使用すると、そのグループ範囲が双方向共有ツリー転送に使用されるようになります。
ステップ 3	**exit** **例：** `Switch(config-if)# exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 4	**show ipv6 pim** [**vrf** *vrf-name*] **df** [*interface-type interface-number*] [*rp-address*] **例：** `Switch# show ipv6 pim df`	RP の各インターフェイスの指定フォワーダ（DF）選択ステートを表示します。
ステップ 5	**show ipv6 pim** [vrf *vrf-name*] **df winner**[*interface-type interface-number*] [*rp-address*] **例：** `Switch# show ipv6 pim df winner ethernet 1/0 200::1`	各 RP の各インターフェイスの DF 選択ウィナーを表示します。
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。

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。

	コマンド	目的
ステップ 1	**clear ipv6 pim** [**vrf** *vrf-name*] **traffic** **例：** `Switch# 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 pim** [**vrf** *vrf-name*] **traffic** **例：** `Switch# 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。

	コマンド	目的
ステップ 1	**clear ipv6 pim** [**vrf** *vrf-name*] **topology** [*group-name* | *group-address*] **例：** `Switch# 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 mrib** [**vrf** *vrf-name*] **client** [**filter**] [**name** {*client-name* | *client-name* **:** **client-id**}] **例：** `Switch# 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 3	**show ipv6 mrib** [**vrf** *vrf-name*] **route [link-local**| **summary** | [*sourceaddress-or-name* | *] [*groupname-or-address* [*prefix-length*]]] **例：** `Switch# show ipv6 mrib route`	MRIB ルート情報を表示します。
ステップ 4	**show ipv6 pim** [**vrf** *vrf-name*] **topology** [*groupname-or-address* [*sourcename-or-address*] | **link-local** | **route-count** [**detail**]] **例：** `Switch# 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 mrib** [**vrf** *vrf-name*] **client** **例：** `Switch# 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 mrib** [vrf *vrf-name*] **io** **例：** `Switch# 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：** `Switch# 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 mrib** [vrf *vrf-name*] **route** [*group-name* | *group-address*] **例：** `Switch# 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 mrib** [**vrf** *vrf-name*] **table** **例：** `Switch# 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。

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。

	コマンド	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** [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address*[*hash-mask-length*] [**priority** *priority-value*] **例：** `Switch(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：** `Switch(config)# interface FastEthernet 1/0`	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：** `Switch(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	**exit** **例：** `Switch(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** [**vrf** *vrf-name*] bsr {**election** | **rp-cache** | **candidate-rp**} **例：** `Switch# 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。

	コマンド	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** [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**] 例： `Switch(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 3	**interface** *type number* 例： `Switch(config)# interface FastEthernet 1/0`	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： `Switch(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。

	コマンド	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** [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] 例： `Switch(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** [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**] 例： `Switch(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 4	**interface** *type number* 例： `Switch(config)# interface FastEthernet 1/0`	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	目的
ステップ 5	**ipv6 multicast boundary scope** *scope-value* **例：** `Switch(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。

	コマンド	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** [**vrf** *vrf-name*] **bsr announced rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**bidir**] [**scope** *scope-value*] **例：** `Switch(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。

	コマンド	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 mld** [**vrf** *vrf-name*] **ssm-map enable** 例： `Switch(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 mld** [**vrf** *vrf-name*] **ssm-map query dns** 例： `Switch(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 mld** [**vrf** *vrf-name*] **ssm-map static** *access-list source-address* 例： `Switch(config)# 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 5	**exit** 例： `Switch(config-if)# exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 6	show ipv6 mld [**vrf** *vrf-name*] **ssm-map** [*source-address*] 例： `Switch# 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。

	コマンド	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：** `Switch(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 3	**exit** **例：** `Switch(config-if)# exit`	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 4	**show ipv6 mroute** [**vrf** *vrf-name*] [link-local | [*group-name* | *group-address* [*source-address* | *source-name*]] [**summary**] [**count**] **例：** `Switch# 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** [**vrf** *vrf-name*] [**link-local** | *group-name* | *group-address*] **active**[*kbps*] **例：** `Switch# 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** [**vrf** *vrf-name*] *ipv6-prefix* **例：** `Switch# show ipv6 rpf 2001:DB8::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。

	コマンド	目的
ステップ 1	**show ipv6 mfib** [**vrf** *vrf-name*] [**link-local** | **verbose** | *group-address-name* | *ipv6-prefix* / *prefix-length* | *source-address-name*| **active** | **count** | **interface** | **status** | **summary**] 例： `Switch# 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** [**vrf** *vrf-name*] [**link-local**| *group-name* | *group-address*] **active** [*kbps*] 例： `Switch# show ipv6 mfib active`	アクティブな送信元からマルチキャスト グループへの送信レートを表示します。
ステップ 3	**show ipv6 mfib** [**vrf** *vrf-name*] [**all** | **linkscope**| *group-name* | *group-address* [*source-name* | *source-address*]] **count** 例： `Switch# show ipv6 mfib count`	MFIB からのグループおよび送信元に関するサマリー トラフィック統計情報を表示します。
ステップ 4	**show ipv6 mfib interface** 例： `Switch# 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： `Switch# 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** [**vrf** *vrf-name*] **summary** 例： `Switch# 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** [**vrf** *vrf-name*] [*group-name*| *group-address*] [**adjacency** | **db** | **fs** | **init** | **interface** | **mrib** [**detail**] | **nat** | **pak** | **platform** | **ppr** | **ps** | **signal** | **table**] 例： `Switch# 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。
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。

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。

	コマンド	目的
ステップ 1	**clear ipv6 mfib** [**vrf** *vrf-name*] **counters** [*group-name* | **group-address** [*source-address* | *source-name*]] **例：** `Switch# 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。
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。