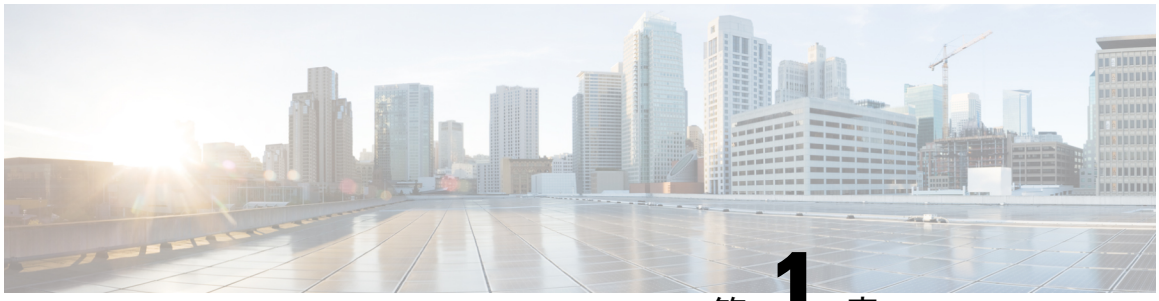
Cisco IOS XE Amsterdam 17.3.x（Catalyst 9300 スイッチ）IP マルチキャスト ルーティング コンフィギュレーション ガイド

初版：2020 年 7 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/

目 次



第 1 章

IP マルチキャスト ルーティング テクノロジーの概要

IP マルチキャスト テクノロジーに関する情報

ここでは、IP マルチキャストテクノロジーについて説明します。

IP マルチキャストについて

マルチキャスト グループに対する転送速度の制御はサポートされていません。

IP 通信の一端である IP ユニキャストでは、送信元 IP ホストが特定の宛先 IP ホストにパケットを送信します。この場合、IP パケットに指定される宛先アドレスは、IP ネットワーク上で一意に識別される単一ホストのアドレスです。これらの IP パケットは、ネットワーク上の送信元ホストから、一連のデバイスによって宛先ホストに転送されます。送信元と宛先間のパス上の各ポイントでは、デバイスがユニキャスト ルーティング テーブルを使用して、パケットの IP 宛先アドレスに基づきユニキャスト転送先を決定します。

IP 通信で IP ユニキャストの対極にある IP ブロードキャストでは、送信元ホストはネットワーク セグメント上のすべてのホストにパケットを送信します。IP ブロードキャスト パケットの宛先アドレスでは、宛先 IP アドレスのホスト部分がすべて 1 に設定され、ネットワーク部分がサブネットのアドレスに設定されています。一連の IP ホスト（デバイスを含む）は、宛先アドレスとして IP ブロードキャスト アドレスを指定されたパケットが、サブネット上のすべての IP ホスト向けであることを認識しています。特に設定しない限り、デバイスは IP ブロードキャスト パケットを転送しないので、一般的に IP ブロードキャスト通信はローカル サブネットに限定されます。

IP マルチキャストは、IP ユニキャスト通信と IP ブロードキャスト通信の中間に位置します。IP マルチキャスト通信によって、ホストは IP ネットワーク上の任意の場所にあるホストのグループに IP パケットを送信します。IP マルチキャスト通信では、特定のグループに情報を送信するために、IP マルチキャスト グループ アドレスという特殊な形式の IP 宛先アドレスを使

用します。IP マルチキャスト グループ アドレスは、パケットの IP 宛先アドレス フィールドに指定されます。

IP 情報をマルチキャストするには、レイヤ 3 スイッチおよびデバイスが IP マルチキャスト グループのメンバに接続する出力インターフェイスすべてに着信 IP パケットを転送する必要があります。

IP マルチキャストはビデオ会議と同じものとして考えられる傾向があります。ネットワークに初めて導入する IP マルチキャスト アプリケーションは多くの場合ビデオ会議ですが、ビデオは実用的で多様な IP マルチキャスト アプリケーションのひとつに過ぎません。生産性の向上につながる他の IP マルチキャスト アプリケーションとしては、マルチメディア会議、データ複製、リアルタイム データ マルチキャスト、シミュレーション アプリケーションなどがあります。

情報配信における IP マルチキャストの役割

IP マルチキャストは、単一の情報ストリームを何千もの潜在的な企業および家庭に同時に配信することによってトラフィックを削減する帯域幅節約テクノロジーです。マルチキャストを利用するアプリケーションには、ビデオ会議、企業コミュニケーション、通信教育、およびソフトウェア、株価情報、ニュースの配信などが含まれます。

IP マルチキャスト ルーティングにより、ホスト（ソース）は、IP マルチキャスト グループ アドレスと呼ばれる特別な形式の IP アドレスを使用して、IP ネットワーク内の任意の場所にあるホスト（レシーバ）にパケットを送信できます。ソースのホストは、マルチキャスト グループ アドレスをパケットの宛先 IP アドレス フィールドに挿入します。IP マルチキャスト ルータおよびマルチレイヤ スイッチは、受信した IP マルチキャスト パケットを、マルチキャスト グループのメンバにつながるすべてのインターフェイスから転送します。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受信します。

IP マルチキャスト ルーティング プロトコル

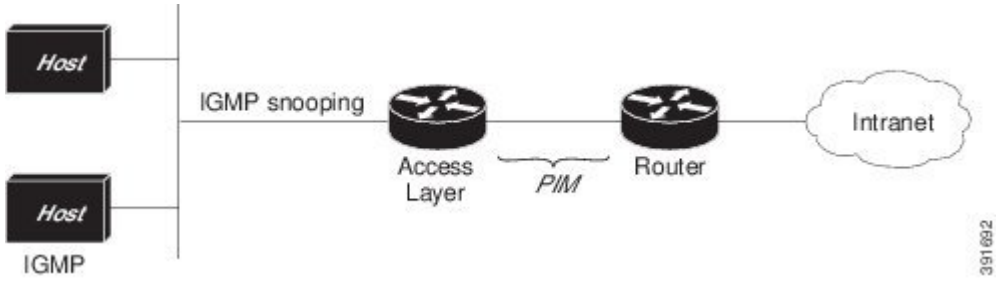
ソフトウェアでは、IP マルチキャスト ルーティングを実装するため、次のプロトコルがサポートされています。

- IGMP を LNA 上のホストとその LAN上のルータ（およびマルチレイヤデバイス）間で使用して、ホストがメンバになっているマルチキャストグループを追跡します。IP マルチキャスティングに参加するには、マルチキャストホスト、ルータ、およびマルチレイヤデバイスで Internet Group Management Protocol（IGMP）が動作している必要があります。
- 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ルータ間で使用されます。
- IGMP スヌーピングは、レイヤ 2 スイッチング環境でのマルチキャストに使用します。レイヤ 2 インターフェイスを動的に設定し、マルチキャスト トラフィックが IP マルチキャ

ストデバイスと関連付けられたインターフェイスにだけ転送されるようにすることによって、マルチキャスト トラフィックのフラッディングを削減します。

次の図に、これらのプロトコルが IP マルチキャスト環境内のどの部分で動作するかを示します。

図 *1 : IP* マルチキャスト ルーティング プロトコル



IPv4 マルチキャスト標準に従い、MAC 宛先マルチキャスト アドレスは 0100:5e で始まり、IP アドレスの末尾 23 ビットが付加されます。たとえば、IP 宛先アドレスが 239.1.1.39 の場合、MAC 宛先アドレスは 0100:5e01:0127 となります。

IPv4 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。デバイスは、ハードウェア内の一致しないパケットを MAC アドレステーブルに基づいて転送します。MAC 宛先アドレスが MAC アドレステーブルにない場合、デバイス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。

Internet Group Management Protocol（インターネット グループ管理プロトコル）

IP マルチキャスト ホストは IGMP メッセージを使用して、ローカルのレイヤ 3 スイッチまたはルータに要求を送信し、特定のマルチキャスト グループに加入して、マルチキャスト トラフィックの受信を開始します。IGMPv2 の一部の拡張機能を使用すると、IP ホストはレイヤ 3 スイッチまたはルータに対し、IP マルチキャスト グループを脱退してマルチキャスト グループ トラフィックを受信しないように求める要求も送信します。

レイヤ 3 スイッチまたはルータは、IGMP によって得た情報を使用して、マルチキャスト グループ メンバーシップのリストをインターフェイス単位で維持します。インターフェイス上で少なくとも 1 つのホストが、マルチキャスト グループ トラフィックを受信するための IGMP 要求を送信している限り、そのインターフェイスのマルチキャスト グループ メンバーシップはアクティブです。

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）がプロトコルに依存しない理由は、使用されている任意のユニキャスト ルーティング プロトコルを利用してルーティングテーブルへの書き込みを行い（Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、Border Gateway Protocol（BGP）、およびスタティックルートを含む）、IP マルチキャストをサポートするからです。

PIM はさらに、完全に独立したマルチキャスト ルーティング テーブルを作成する代わりに、ユニキャスト ルーティング テーブルを使用して Reverse Path Forwarding（RPF）チェック機能を実行します。PIM は、他のルーティング プロトコルが行うような、ルータ間でのマルチキャスト ルーティング アップデートの送受信は行いません。

PIM スパース モード（PIM-SM）

PIM スパース モード（PIM-SM）は、プル モデルを使用してマルチキャスト トラフィックを配信します。明示的にデータを要求した、アクティブな受信者のいるネットワークだけにトラフィックが転送されます。PIM-SM は、デスクトップ ビデオ会議や企業コンピューティングなど、少数の受信者がそれぞれ異なるマルチキャストを一般に同時使用するネットワークでの使用を目的としています。

ランデブー ポイント

また、PIM をスパース モードで動作するよう構成する場合は、1 つまたは複数のデバイスをランデブー ポイント（RP）とするよう選択する必要があります。マルチキャスト グループへの送信者は、RP を使用してその存在を通知します。マルチキャストパケットの受信者は、RP を使用して新しい送信者について学習します。1 つのマルチキャスト グループのパケットが 1 つまたは複数の RP を使用できるように Cisco IOS ソフトウェアを構成できます。

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。同じグループの 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は、（異なるグループが異なる RP を持つことが可能なため）デバイスがいずれのグループの RP であるかを決定します。

IGMP スヌーピング

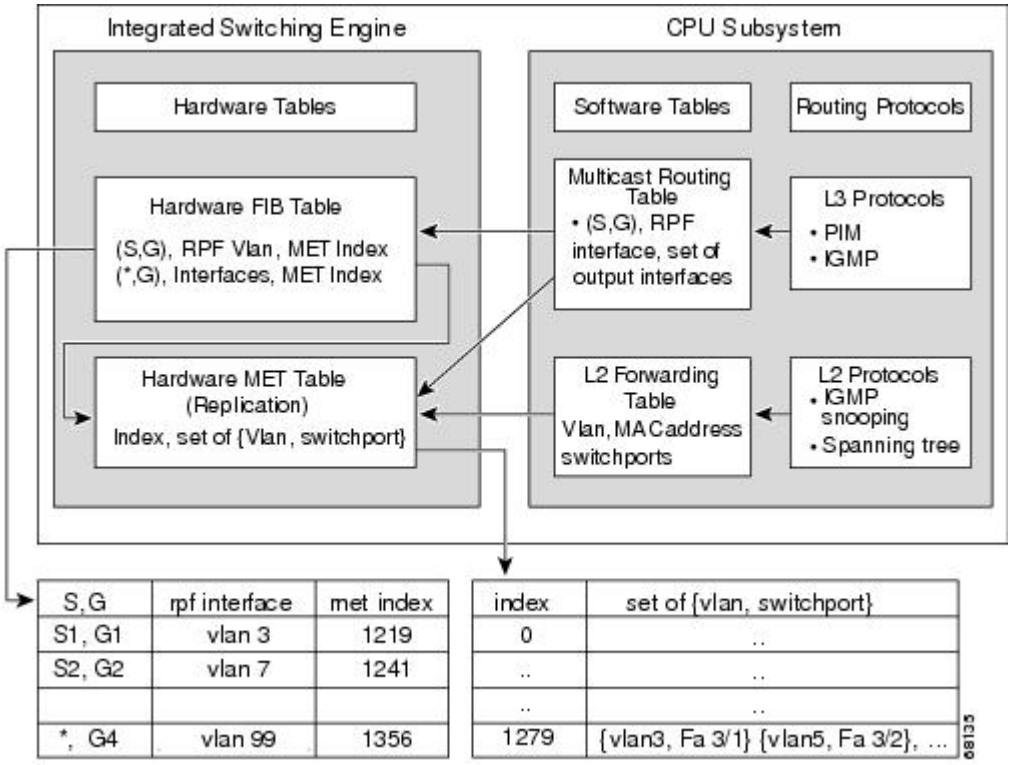
IGMP スヌーピングは、レイヤ 2 スイッチング環境でのマルチキャストに使用します。IGMP スヌーピングを使用する場合、レイヤ 3 スイッチまたはルータは、ホストとデバイス間で転送される IGMP パケットのレイヤ 3 情報を検証します。スイッチが特定のマルチキャスト グループのホストから IGMP Host Report を受信すると、スイッチはそのホストのポート番号を対応するマルチキャスト テーブル エントリに追加します。スイッチがホストから IGMP Leave Group メッセージを受信すると、スイッチはテーブル エントリからそのホストのポートを削除します。

IGMP 制御メッセージはマルチキャスト パケットとして送信されるので、レイヤ 2 ヘッダーだけが検証される場合は、マルチキャスト データと区別できません。IGMP スヌーピングが稼働しているスイッチは、すべてのマルチキャスト データ パケットについて、関連する IGMP 制御情報が含まれているかどうかを調べます。低速の CPU を搭載したローエンドのスイッチに IGMP スヌーピングを実装すると、データを高速で送信する場合、パフォーマンスに重大な影響が出る可能性があります。

IP マルチキャスト テーブル

次に、デバイスがハードウェアで IP マルチキャスト パケットを転送する目的で使用する主なデータ構造図を示します。

図 *2 : IP* マルチキャスト テーブルおよびプロトコル



Integrated Switching Engine は、個々の IP マルチキャスト ルートを識別する目的で、ハードウェア FIB テーブルを維持します。各エントリは、宛先グループの IP アドレスおよびオプションの送信元 IP アドレスで構成されます。マルチキャスト トラフィックは、主に（S,G）および（*,G）の 2 種類のルート上を流れます。（S,G）ルートは、マルチキャスト送信元の IP アドレスと、マルチキャスト グループ宛先の IP アドレスに基づいて、送信元からグループへ流れます。（*,G）ルートのトラフィックは、PIM RP からグループ G のすべての受信者へ流れます。（*,G）ルートを使用するのは、スパース モード グループだけです。Integrated Switching Engine ハードウェアには、合計 128,000 のルート用のスペースが準備されています。これらがユニキャスト ルート、マルチキャスト ルート、およびマルチキャスト高速ドロップ エントリによって共有されます。

出力インターフェイスのリストは、Multicast Expansion Table（MET）に保存されます。MET には、最大 32,000 の出力インターフェイス リスト用のスペースがあります（RET には、最大 102 K エントリ（フラッディング セットに 32 K、マルチキャスト エントリに 70,000 使用）が可能です）。MET リソースは、レイヤ 3 マルチキャスト ルートおよびレイヤ 2 マルチキャスト エントリによって共有されます。ハードウェアで使用できる出力インターフェイス リストの実際の数は、設定によって異なります。マルチキャスト ルートの総数が 32,000 を超えると、Integrated Switching Engine によってマルチキャスト パケットをスイッチングできなくなる場合がありま

す。そのパケットは、CPUサブシステムによってきわめて低い速度で転送されることになります

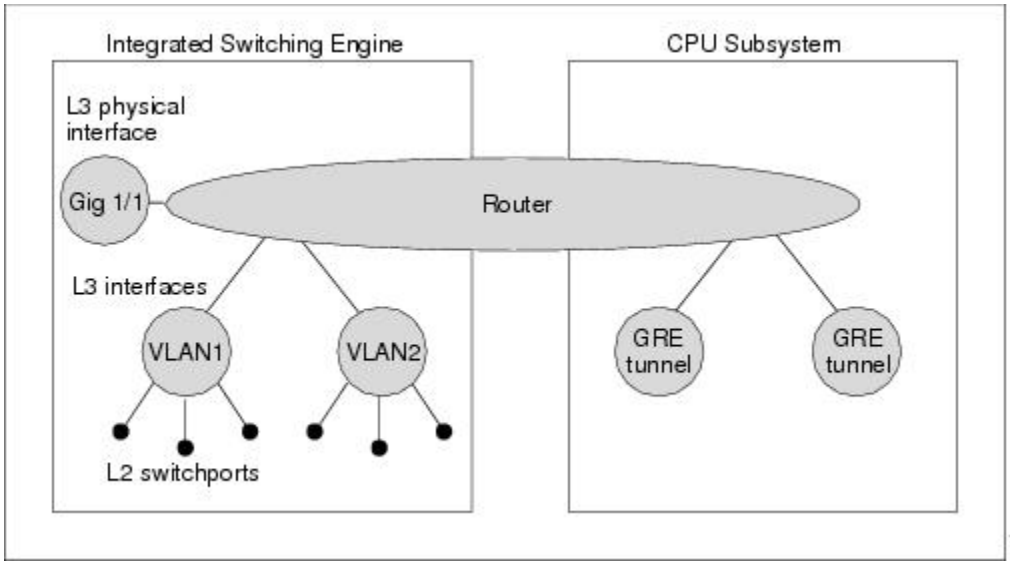
（注） （RET では 102 K エントリまでサポートされます（フラッディング セットに 32K、multicast エントリに 70 K を使用））。

ハードウェアおよびソフトウェアによる転送

Integrated Switching Engine は通常、パケットをハードウェアで非常に高速で転送します。CPU サブシステムは、例外パケットをソフトウェアで転送します。Integrated Switching Engine が大部分のパケットをハードウェアで転送していることは、統計レポートからわかります。

次に、ハードウェアとソフトウェアの転送コンポーネントの概念図を示します。

図 *3:* ハードウェアおよびソフトウェアの転送コンポーネント



Integrated Switching Engine は、通常の動作モードでは、ハードウェアで VLAN 間ルーティングを実行します。CPU サブシステムは、ソフトウェアによる転送のために、総称ルーティング カプセル化（GRE）トンネルをサポートしています。

複製は、パケットの 1 コピーを送信する代わりに、パケットを複製して複数のコピーを送信する転送の一種です。レイヤ 3 で複製が行われるのは、マルチキャスト パケットに限られます。ユニキャスト パケットが複数のレイヤ 3 インターフェイス用に複製されることはありません。IP マルチキャスト動作では、着信した IP マルチキャスト パケットごとに、そのパケットの多くの複製が送信されます。

IP マルチキャスト パケットを伝送するルートのタイプは、次のとおりです。

- ハードウェア ルート

- ソフトウェア ルート
- 部分的なルート

ハードウェア ルートは、Integrated Switching Engine ハードウェアがパケットのすべての複製を転送する場合に発生します。ソフトウェア ルートは、CPU サブシステム ソフトウェアがパケットのすべての複製を転送する場合に発生します。部分的なルートは、Integrated Switching Engine が一部の複製をハードウェアで転送し、CPU サブシステムが一部の複製をソフトウェアで転送する場合に発生します。

部分的なルート

（注） 以下に記載する条件が成立する場合、CPU サブシステム ソフトウェアによって複製が転送されますが、ハードウェアによる複製の転送パフォーマンスに影響はありません。

あるルートに対するパケットの複製の一部が CPU サブシステムによって転送される条件は、次のとおりです。

- **ip igmp join-group** コマンドを使用して、マルチキャスト送信元の RPF インターフェイス上の IP マルチキャストグループのメンバとしてスイッチを設定している場合。
- スイッチが PIM スパース モードの送信元へのファースト ホップである場合。スイッチは RP に PIM Register メッセージを送信する必要があります。

ソフトウェア ルート

（注） RPF インターフェイスまたは出力インターフェイスの設定について次の条件が 1 つでも成立すると、出力のすべての複製はソフトウェアで実行されます。

あるルートに対するパケットの複製の一部が CPU サブシステム ソフトウェアによって転送される条件は、次のとおりです。

- インターフェイスがマルチキャスト ヘルパーを使用して設定されている場合
- インターフェイスが GRE トンネルまたはディスタンス ベクトル マルチキャスト ルーティング プロトコル（DVMRP）トンネルである場合
- インターフェイスが高等研究計画局（ARPA）以外のカプセル化を使用している場合

次のパケットは、常にソフトウェアによって転送されます。

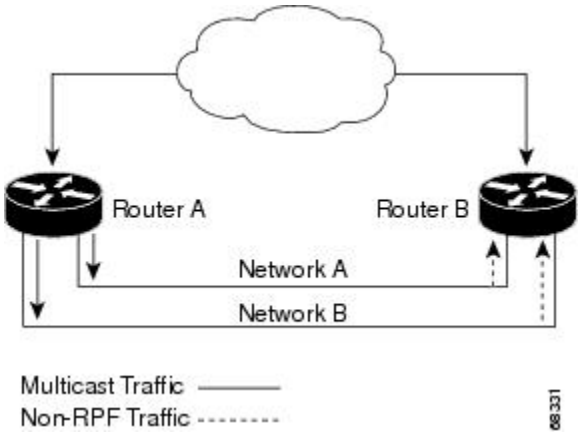
- 224.0.0.*（* は 0 ～ 255）の範囲のマルチキャスト グループに送信されるパケット。この範囲は、ルーティング プロトコルが使用します。レイヤ 3 スイッチングでは、この範囲以外のすべてのマルチキャスト グループ アドレスがサポートされています。
- IP オプション付きのパケット

非リバース パス フォワーディング トラフィック

Reverse Path Forwarding（RPF）チェックに失敗したトラフィックを、非RPF トラフィックといいます。Integrated Switching Engine は、非 RPF トラフィックをフィルタリング（持続的にドロップ）するか、またはレート制限して転送します。

複数のレイヤ 3 スイッチまたはルータが同一の LAN セグメントに接続されている冗長な構成で、送信元から発信インターフェイス上の受信側へマルチキャスト トラフィックを転送するのは、1 台の装置だけです。次の図に、一般的なネットワーク構成で非 RPF トラフィックが発生した状況を示します。

図 *4:* スタブ ネットワークにおける冗長マルチキャスト ルータの構成



この種のトポロジでは、PIM 指定ルータ（PIM DR）であるルータ A だけが共通の VLAN にデータを転送します。ルータ B は転送されたマルチキャスト トラフィックを受信しますが、このトラフィックをドロップします。不正なインターフェイスでこのトラフィックが着信したので、RPF チェックに失敗するためです。このように RPF チェックに失敗するトラフィックを、「非 RPF トラフィック」といいます。

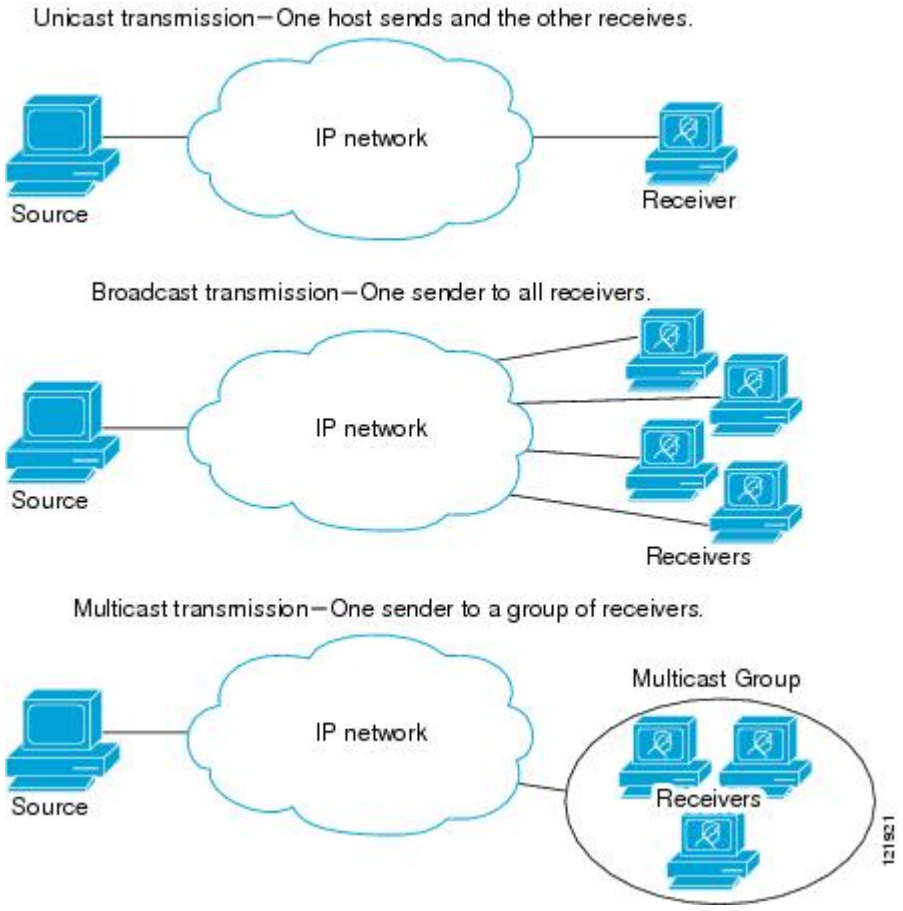
マルチキャスト グループ伝送方式

IP通信は、最初の図に示すように、トラフィックの送信者として機能するホストと、レシーバとして機能するホストで構成されます。送信者はソースと呼ばれます。従来の IP 通信は、単一のホスト ソースがパケットを別の単一ホスト（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）に送信することによって行われます。IPマルチキャストは第三の方式を提供するものであり、ホストはすべてのホストのサブセットにパケットを送信できます（マルチキャスト伝送）。受信側のホストのこのサブセットをマルチキャスト グループと呼びます。マルチキャスト グループに属するホストは、グループ メンバと呼ばれます。

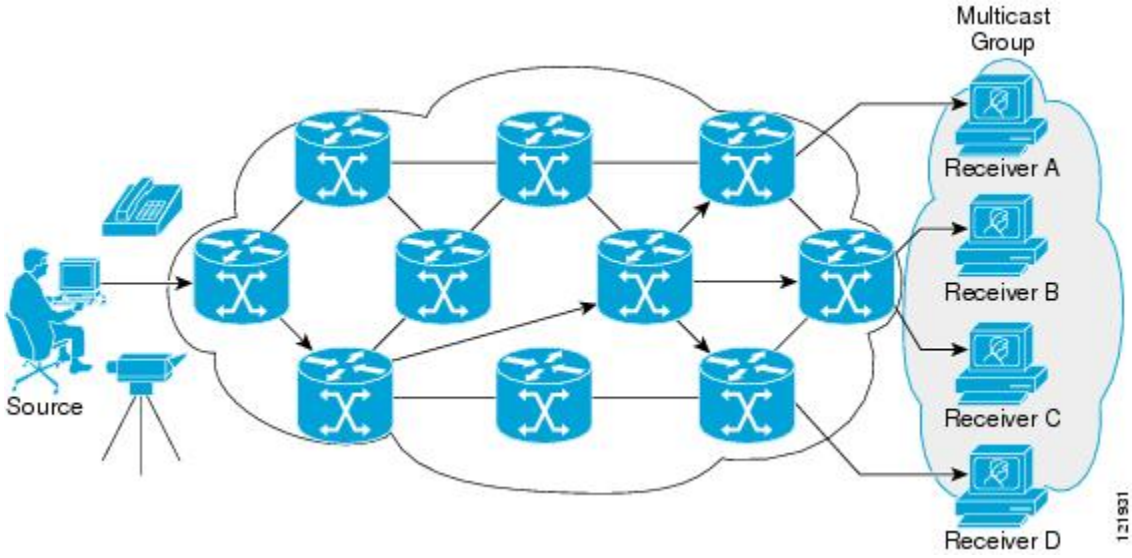
マルチキャストは、このグループの概念に基づいています。マルチキャスト グループは、特定のデータ ストリームを受信するためにグループに加入する任意の数のレシーバです。このマルチキャスト グループには、物理的境界または地理的境界はありません。ホストは、インターネット上または任意のプライベート ネットワーク上のどこにでも配置できます。ソースから特定のグループに対するデータを受信する必要があるホストはそのグループに加入する必要があ

ります。グループに加入するには、ホスト レシーバで Internet Group Management Protocol（IGMP）を使用します。

マルチキャスト環境では、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、そのグループに送信されたパケットはグループのメンバだけが受信できます。IP ユニキャスト パケットと同様、マルチキャスト パケットは、ベストエフォート型の信頼性を使用してグループに配信されます。



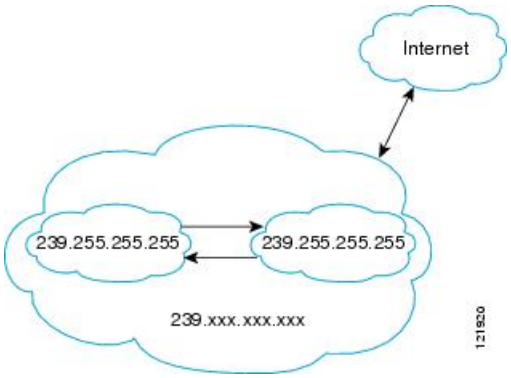
次の図では、レシーバ（指定したマルチキャスト グループ）がソースからのビデオ データ ストリームを受信する必要があります。これらのレシーバは、ネットワーク内のルータに IGMP ホスト レポートを送信することによってその意思を示します。この場合、ルータがソースからレシーバへのデータの配信を担います。ルータは、Protocol Independent Multicast（PIM）を使用して、マルチキャスト配信ツリーを動的に作成します。その後、ソースとレシーバ間のパスにあるネットワーク セグメントにのみ、ビデオ データ ストリームが配信されます。



IP マルチキャスト境界

図に示すように、アドレス スコーピングは、同じ IP アドレスを持つ RP が含まれるドメインが相互にデータを漏出させることのないように、ドメイン境界を定義します。スコーピングは、大きなドメイン内のサブネット境界や、ドメインとインターネットの間の境界で実行されます。

図 *5:* 境界でのアドレス スコーピング



マルチキャスト グループ アドレッシングのインターフェイスに管理スコープの境界を設定するには、**ip multicast boundary** コマンドと *access-list* 引数を使用します。影響を受けるアドレス範囲は、標準アクセス リストによって定義されます。境界が設定されると、マルチキャスト データ パケットは境界を越えて出入りできなくなります。境界を定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

Internet Assigned Numbers Authority（IANA）は、マルチキャスト アドレス範囲 239.0.0.0 ～ 239.255.255.255 を管理スコープ アドレスとして指定しています。この範囲のアドレスは、さまざまな組織で管理されるドメイン内で再使用されます。これらは、グローバルに一意ではなくローカルとみなされます。

filter-autorp キーワードを設定して、管理用スコープの境界で Auto-RP 検出と通知メッセージを検査し、フィルタできます。境界のアクセス コントロール リスト（ACL）に拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

IP マルチキャスト グループ アドレッシング

マルチキャスト グループは、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、そのマルチキャスト グループ アドレスに配信されます。単一のホストを独自に識別するユニキャスト アドレスとは異なり、マルチキャスト IP アドレスは特定のホストを識別しません。マルチキャストアドレスに送信されるデータを受信するには、アドレスが識別するグループにホストが参加する必要があります。データは、マルチキャストアドレスに送信され、そのグループに送信されたトラフィックを受信する意思を示してグループに加入しているすべてのホストによって受信されます。マルチキャスト グループ アドレスは、送信元でグループに割り当てられます。マルチキャスト グループ アドレスを割り当てるネットワーク管理者は、Internet Assigned Numbers Authority（IANA）で予約されるマルチキャスト アドレスの範囲にアドレスが準拠していることを確認する必要があります。

IP クラス D アドレス

IP マルチキャスト アドレスは、IANA によって IPv4 クラス D アドレス空間に割り当てられました。クラス D アドレスの上位 4 ビットは 1110 です。したがって、ホスト グループ アドレスの範囲は 224.0.0.0 ～ 239.255.255.255 であると考えられます。マルチキャスト アドレスは送信元（送信者）でマルチキャスト グループの受信先として選択されます。

（注） クラス D アドレスの範囲は、IP マルチキャスト トラフィックのグループ アドレスまたは宛先アドレスにだけ使用されます。マルチキャストデータグラムの送信元アドレスは常にユニキャスト送信元アドレスになります。

IP マルチキャスト アドレスのスコーピング

さまざまなアドレス範囲の予測可能な動作を提供したり、より小規模なドメイン内でアドレスを再利用したりできるよう、マルチキャストアドレスの範囲はさらに分割されます。表に、マルチキャスト アドレスの範囲を要約します。それに続いて、各範囲について簡単に説明します。

表 *1*：マルチキャスト アドレス範囲の割り当て

名前	範囲	説明
予約済みリンクローカル アドレス	224.0.0.0 ～ 224.0.0.255	ローカル ネットワーク セグメントのネットワーク プロトコルで使用するために予約されています。

名前	範囲	説明
グローバル スコープ アドレス	224.0.1.0 ～ 238.255.255.255	組織間およびインターネット上でマルチキャスト データを送信するために予約されています。
Source Specific Multicast	232.0.0.0 ～ 232.255.255.255	明示的にグループに参加している受信者だけにデータを転送する SSM データグラム配信モデル用に予約されています。
GLOP アドレス	233.0.0.0 ～ 233.255.255.255	割り当て済みの自律システム（AS）ドメイン番号をすでに持つ組織によって静的に定義されるアドレス用に予約されています。
限定スコープ アドレス	239.0.0.0 ～ 239.255.255.255	管理スコープ アドレスまたはプライベート マルチキャスト ドメインで使用するための限定スコープ アドレスとして予約されています。

予約済みリンクローカル アドレス

IANA では、ローカル ネットワーク セグメントのネットワーク プロトコルで使用するために 224.0.0.0 ～ 224.0.0.255 の範囲を予約しています。この範囲のアドレスを持つパケットはスコープ内ローカルであり、IP ルータによって転送されません。通常、リンク ローカル宛先アドレスを持つパケットは存続可能時間（TTL）値 1 を使用して送信されるため、ルータによって転送されません。

この範囲内の予約済みリンクローカル アドレスは、それぞれに予約されたネットワーク プロトコル機能を提供します。ネットワーク プロトコルは、これらのアドレスをルータの自動検出および重要なルーティング情報の伝達用に使用します。たとえば、Open Shortest Path First（OSPF）は、IP アドレスの 224.0.0.5 と 224.0.0.6 を使用してリンクステート情報を交換します。

IANA では、ネットワーク プロトコルやネットワーク アプリケーションに対する単一マルチキャスト アドレス要求を 224.0.1.xxx のアドレス範囲外に割り当てています。マルチキャスト ルータはこれらのマルチキャスト アドレスを転送します。

（注） ASR 903 RSP2 モジュールでは、デフォルトにより、予約済みのリンクローカル アドレスを持つすべてのパケットが CPU にパントされます。

グローバル スコープ アドレス

224.0.1.0 ～ 238.255.255.255 の範囲のアドレスは、グローバル スコープ アドレスと呼ばれます。これらのアドレスは、組織間およびインターネット上でのマルチキャスト データの送信に使用します。これらのアドレスの一部はマルチキャスト アプリケーションで使用するよう IANA によって予約されています。たとえば、IP アドレス 224.0.1.1 は、Network Time Protocol（NTP）用に予約されています。

Source Specific Multicast アドレス

232.0.0.0/8 のアドレス範囲は、Source Specific Multicast（SSM）用に予約されています。Cisco IOS ソフトウェアでは、**ip pim ssm** コマンドを使用して任意の IP マルチキャストアドレス用の SSM も設定できます。SSM は、1 対多通信での効率的なデータ配信メカニズムを可能にする Protocol Independent Multicast（PIM）の拡張版です。SSM については、IP マルチキャスト配信モード （16 ページ）の項を参照してください。

GLOP アドレス

GLOP アドレッシングでは（233/8 の RFC 2770、GLOP アドレッシングで提案されているように）、AS 番号をすでに予約している組織による静的に定義されたアドレス用に 233.0.0.0/8 の範囲を予約することを提案しています。これは、GLOP アドレッシングと呼ばれます。ドメインの AS 番号は 233.0.0.0/8 アドレス範囲の 2 番目と 3 番目のオクテットに組み込まれます。たとえば、AS 62010 は 16 進数形式で F23A と表されます。この 2 つのオクテット F2 および 3A を分割すると、結果は 10 進数でそれぞれ 242 および 58 となります。これらの値は、AS 62010 に使用するようにグローバルに予約される 233.242.58.0/24 のサブネットとなります。

限定スコープ アドレス

239.0.0.0 ～ 239.255.255.255 の範囲は、管理スコープ アドレス、またはプライベート マルチキャスト ドメインで使用する限定スコープ アドレスとして予約されています。これらのアドレスは、ローカル グループまたは組織に使用するように制限されています。会社、大学および他の組織は、限定スコープ アドレスを使用すると、ドメイン外に転送されないローカル マルチキャスト アプリケーションを使用できます。通常、ルータは、このアドレス範囲のマルチキャスト トラフィックが自律システム（AS）またはユーザー定義のドメイン外にフローしないようにするフィルタを使用して設定されます。AS またはドメイン内では、ローカル マルチキャスト境界を定義できるように、限定スコープ アドレス範囲を細分化することもできます。

（注） ネットワーク管理者はこの範囲内のマルチキャスト アドレスを使用できます。これによって、インターネット内の他の場所と競合することはありません。

レイヤ 2 マルチキャスト アドレス

従来、LAN セグメントのネットワーク インターフェイス カード（NIC）が受信できるのは、Burned-In MAC Address またはブロードキャスト MAC アドレスに指定されたパケットだけでした。IP マルチキャストでは、複数のホストが共通の宛先 MAC アドレスを使用した単一のデータ ストリームを受信する必要があります。複数のホストが同じパケットを受信する場合、複数のマルチキャスト グループを区別できるように、何らかの方法を考案する必要があります。そのための 1 つの方法は、IP マルチキャスト クラス D アドレスを MAC アドレスに直接マッピングすることです。この方法を使用すると、NIC は多くの異なる MAC アドレスを宛先とするパケットを受信できます。

Cisco グループ管理プロトコル（CGMP）は、IGMP によって実行される作業と同様の作業を実行するために、Catalyst スイッチに接続されたルータ上で使用されます。IP マルチキャスト

データ パケットと IGMP レポート メッセージ（いずれも MAC レベルで同じグループ アドレスにアドレス指定されます）を区別できない Catalyst スイッチの場合、CGMP が必要になります。

シスコ エクスプレス フォワーディング、MFIB、およびレイヤ 2 転送

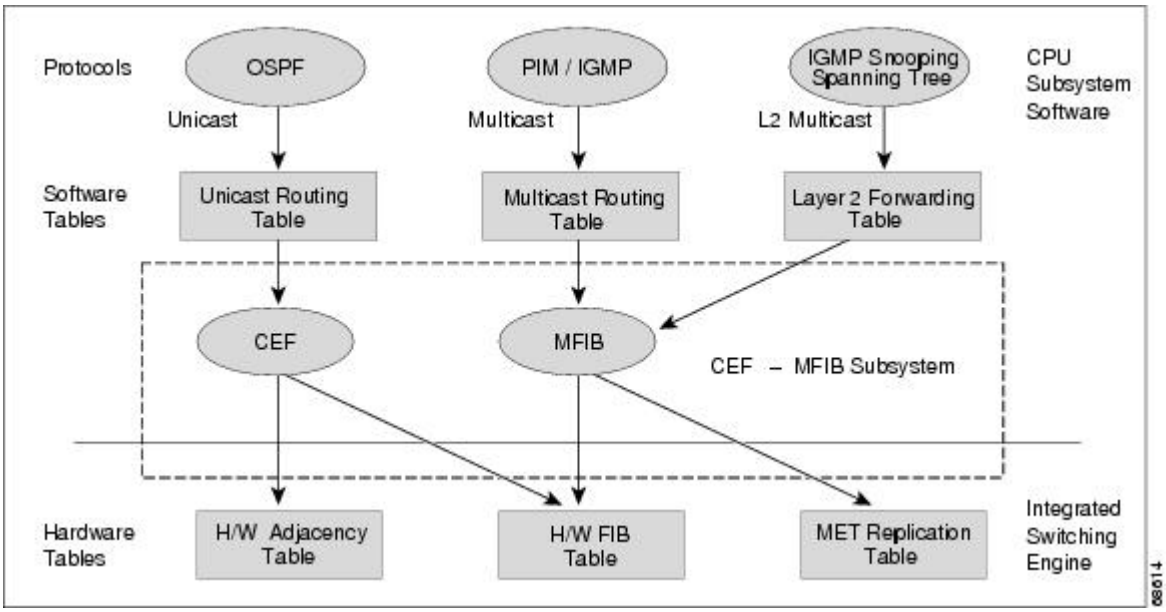
実装された IP マルチキャストは、中央集中型シスコ エクスプレス フォワーディングの拡張機能です。Cisco Express Forwarding は、ユニキャスト ルーティング テーブル（BGP、OSPF、EIGRP などのユニキャスト ルーティング プロトコルによって作成される）から情報を抽出し、この情報をハードウェアにロードします。

転送情報ベース（FIB）FIB のユニキャスト ルートを使用すると、上位層のルーティング テーブルでルートが変更された場合でも、ハードウェア ルーティング ステートの 1 つのルートを変更するだけです。ハードウェアでユニキャスト パケットを転送するために、Integrated Switching Engine は Ternary CAM（TCAM）から送信元および宛先ルートを検索し、ハードウェア FIB から隣接インデックスを取り出して、ハードウェア ネイバー テーブル関係からレイヤ 2 リライト情報およびネクストホップ アドレスを取得します。

マルチキャスト転送情報ベース（MFIB）サブシステムは、ユニキャストシスコ エクスプレス フォワーディングのマルチキャスト版です。この MFIB サブシステムは、PIM および IGMP によって作成されるマルチキャスト ルートを抽出し、ハードウェア転送のためのプロトコル独立フォーマットにします。MFIB サブシステムは、プロトコル固有の情報を削除し、必要なフォワーディング情報だけを残します。MFIB テーブルの各エントリは、（S,G）または（*,G）ルート、入力 RPF VLAN、およびレイヤ 3 出力インターフェイスのリストで構成されます。MFIB サブシステムは、プラットフォーム依存の管理ソフトウェアと連携して、このマルチキャスト ルーティング情報をハードウェア FIB およびハードウェア Replica Expansion Table（RET）にロードします。デバイスは、レイヤ 3 ルーティングとレイヤ 2 ブリッジングを同時に実行します。いずれの VLAN インターフェイスにも複数のレイヤ 2 スイッチ ポートを設定できます。

次の図に、シスコ デバイスがユニキャスト ルーティング、マルチキャスト ルーティング、およびレイヤ 2 ブリッジングの情報を組み合わせてハードウェアで転送を実行する機能の概要を示します。

図 *6 :* ハードウェアでのシスコ エクスプレス フォワーディング、*MFIB*、およびレイヤ *2* 転送情報の組み合わせ



MFIB ルートは、シスコ エクスプレス フォワーディング ユニキャスト ルートと同様にレイヤ 3 であるため、該当するレイヤ 2 情報と結合する必要があります。MFIB ルートの例を示します。

```
(*,203.0.113.1)
RPF interface is Vlan3
Output Interfaces are:
Vlan 1
Vlan 2
```

ルート（*,203.0.113.1）がハードウェア FIB テーブルにロードされ、出力インターフェイスのリストが MET にロードされます。出力インターフェイスのリストへのポインタ、MET インデックス、および RPF インターフェイスも、（*,203.0.113.1）ルートとともにハードウェア FIB にロードされます。ハードウェアにこの情報をロードすることで、レイヤ 2 情報との結合を開始できるようになります。VLAN 1 上の出力インターフェイスについて、Integrated Switching Engine は VLAN 1 上でスパニングツリー フォワーディング ステートにあるすべてのスイッチ ポートにパケットを送信する必要があります。同じプロセスが VLAN 2 に適用されます。VLAN 2 内のスイッチ ポートのセットを決定するために、レイヤ 2 転送テーブルが使用されます。

ハードウェアがパケットをルーティングする場合、すべての出力インターフェイスのすべてのスイッチ ポートにパケットを送信するだけでなく、ハードウェアは入力 VLAN の（パケットが到着したスイッチ ポートを除く）すべてのスイッチ ポートにも、パケットを送信します。たとえば、VLAN 3 に 2 つのスイッチ ポート、GigabitEthernet 3/1 および GigabitEthernet 3/2 があると仮定します。GigabitEthernet 3/1 上のホストがマルチキャスト パケットを送信すると、GigabitEthernet 3/2 上のホストもそのパケットを受信しなければならない場合があります。GigabitEthernet 3/2 上のホストにマルチキャスト パケットを送信するには、MET にロードされるポート セットに入力 VLAN のすべてのスイッチ ポートを追加する必要があります。

VLAN 1 に 1/1 および 1/2、VLAN 2 に 2/1 および 2/2、VLAN 3 に 3/1 および 3/2 が含まれていれば、このルート用の MET チェーンには、スイッチ ポート 1/1、1/2、2/1、2/2、3/1、および 3/2 が含まれることになります。

IGMP スヌーピングがオンの場合、パケットは VLAN 2 のすべての出力スイッチ ポートに転送されるとは限りません。IGMP スヌーピングによって、グループ メンバまたはルータが存在すると判断されたスイッチ ポートだけに、パケットが転送されます。たとえば、VLAN 1 で IGMP スヌーピングがイネーブルで、IGMP スヌーピングによってポート 1/2 だけにグループ メンバが存在すると判断された場合、MET チェーンにはスイッチポート 1/1、1/2、2/1、2/2、3/1、および 3/2 が含まれることになります。

IP マルチキャスト配信モード

IP マルチキャスト配信のモードは、送信元ホストではなく、受信側ホストのみによって異なります。送信元ホストは、パケットの IP 送信元アドレスとしての固有の IP アドレスと、パケットの IP 宛先アドレスとしてのグループ アドレスを使用して、IP マルチキャスト パケットを送信します。

Source Specific Multicast

Source Specific Multicast（SSM）は、ブロードキャスト アプリケーションとしても知られる 1 対多アプリケーションをサポートする最善のデータグラム配信モデルです。SSM は、オーディオおよびビデオのブロードキャスト アプリケーション環境を対象としたシスコの IP マルチキャストのコア ネットワーク テクノロジーです。

SSM 配信モードの場合、IP マルチキャスト レシーバ ホストは IGMP バージョン3（IGMPv3）を使用してチャネル（S, G）を登録する必要があります。このチャネルに登録することによって、ソース ホストがグループ G に送信した IP マルチキャスト トラフィックの受信をレシーバ ホストが要求していることを示します。ネットワークは、ソース ホスト S からグループ G に送信された IP マルチキャスト パケットを、チャネル (S, G) に登録したネットワーク内のすべてのホストに配信します。

SSM では、ネットワーク内でグループ アドレスを割り当てる必要はありません。各ソース ホスト内で割り当てるだけです。同じソース ホストで実行している各アプリケーションはそれぞれ異なる SSM グループを使用する必要があります。異なるソース ホストで実行しているアプリケーションは、SSM グループ アドレスを再利用できます。ネットワークに大量のトラフィックを発生させることはありません。

マルチキャスト高速ドロップ

PIM-SM、PIM-DM などの IP マルチキャスト プロトコルでは、（S,G）または（*,G）ルートごとに、対応する着信インターフェイスがあります。このインターフェイスを、RPF インターフェイスといいます。予測される RPF インターフェイスとは異なるインターフェイスにパケットが到着することもあります。その場合、PIM によってパケットに特殊なプロトコル処理を行うために、そのパケットを CPU サブシステム ソフトウェアに転送する必要があります。PIM が実行する特殊なプロトコル処理の例としては、PIM アサート プロトコルがあります。

デフォルトでは、Integrated Switching Engine ハードウェアは、非 RPF インターフェイスに着信したすべてのパケットを CPU サブシステム ソフトウェアに送信します。ただし、これらの非 RPF パケットはほとんどの場合、マルチキャスト ルーティング プロトコルに必要ではないので、多くの場合、ソフトウェアによる処理は不要です。何の処置も行わなければ、ソフトウェアに送信される非 RPF パケットのため、CPU に負荷がかかるおそれがあります。

高速ドロップエントリをインストールするのではなく、シスコデバイスではダイナミック バッファ制限（DBL）を使用します。このフローベースの輻輳回避メカニズムは、各トラフィック フローのキュー長を追跡することによりアクティブ キュー管理を提供します。フローのキュー長がその設定された制限を超える場合、DBL がパケットをドロップします。CPU が過負荷にならないように、レート DBL は、CPU サブシステムに対する非 RPF トラフィックを制限します。パケットはCPUに対してフローごとにレート制限されます。CAMに高速ドロップエントリをインストールすることは不可能なため、スイッチで処理できる高速ドロップ フローの数を制限する必要はありません。

リンクのダウン、ユニキャストルーティングテーブルの変更などのプロトコルイベントによって、安全に高速ドロップが可能なパケットの集合に影響が出ることがあります。以前は高速ドロップを行っても問題のなかったパケットを、トポロジの変更後、PIM ソフトウェアに処理させるため、CPU サブシステム ソフトウェアに転送する必要があります。CPU サブシステム ソフトウェアは、プロトコル イベントに応答して高速ドロップ エントリのフラッシュを行い、IOS の PIM コードが必要な RPF エラーをすべて処理できるようにします。

RPFエラーが繰り返し発生する可能性があるため、一部の一般的なトポロジでは、ハードウェアにおいて高速ドロップ エントリを使用することが重要です。高速ドロップ エントリがなければ、処理する必要のない RPF エラー パケットによって CPU が過負荷になります。

Multicast Forwarding Information Base（マルチキャスト転送情報ベース）

マルチキャスト転送情報ベース（MFIB）サブシステムは、シスコ デバイス上の Integrated Switching Engine ハードウェアの IP マルチキャスト ルーティングをサポートします。MFIB は、論理的には CPU サブシステムソフトウェアの IP マルチキャスト ルーティング プロトコル（PIM、IGMP、MSDP、MBGP、および DVMRP）と、ハードウェアで IP マルチキャストルーティングを管理するためのプラットフォーム固有のコードとの中間に存在します。MFIB は、マルチキャスト ルーティング プロトコルによって作成されたルーティング テーブル情報を、Integrated Switching Engine ハードウェアが効率的に処理して転送に使用可能な、簡易なフォーマットに変換します。

マルチキャスト ルーティング テーブルの情報を表示するには、**show ip mroute** コマンドを使用します。MFIB テーブルの情報を表示するには、**show ip mfib** コマンドを使用します。

MFIB テーブルには、IP マルチキャスト ルートの集合が含まれます。IP マルチキャスト ルートには（S,G）および（*,G）が含まれます。MFIB テーブルの各ルートに、オプションの 1 つまたは複数のフラグを対応付けることができます。ルート フラグは、ルートに一致するパケットの転送方法を指示します。たとえば、MFIB ルートに付けられた Internal Copy（IC）フラグは、スイッチ上のプロセスがパケットのコピーを受信する必要があることを意味します。MFIB ルートに対応付けできるフラグは、次のとおりです。

- Internal Copy（IC）フラグ：ルータ上のプロセスが、特定のルートに一致するすべてのパケットのコピーを受信する必要がある場合に設定します。
- Signalling（S）フラグ：このルートに一致するパケットを受信したときに、プロセスに通知する必要がある場合に設定します。シグナリングインターフェイス上でのパケット受信に応答して、プロトコルコードがMFIBステートを更新するなどの動作を行うことが考えられます。
- Connected（C）フラグ：このフラグをMFIBルートに設定した場合、直接接続されたホストによってルートに送信されたパケットだけをプロトコルプロセスに通知する必要があるという点を除き、Signalling（S）フラグと同じ意味を持ちます。

ルートには、1つまたは複数のインターフェイスに対応するオプションのフラグを設定することもできます。たとえば、VLAN 1に関するフラグを設定した（S,G）ルートは、VLAN 1に着信するパケットをどのように扱うべきかと、このルートに一致するパケットをVLAN 1に転送すべきかを示します。MFIB でサポートされるインターフェイス単位のフラグは、次のとおりです。

- Accepting（A）：マルチキャスト ルーティングで RPF インターフェイスであることが明らかなインターフェイスに設定します。Accepting（A）をマークされたインターフェイスに着信したパケットは、すべての Forwarding（F）インターフェイスに転送されます。
- Forwarding（F）：上記のように、Accepting（A）フラグと組み合わせて使用します。一連の転送インターフェイスは、マルチキャスト「olist」（出力インターフェイスリスト）と呼ばれるものを形成します。
- Signalling（S）：このインターフェイスにパケットが着信したとき、Cisco IOSの何らかのマルチキャスト ルーティング プロトコル プロセスに通知する必要がある場合に設定します。

（注） PIM-SM ルーティングを使用している場合、MFIB ルートには次の例のようなインターフェイスが含まれる場合があります。

```
PimTunnel [1.2.3.4]
```

これは、パケットが特定の宛先アドレスに対してトンネリングされていることを表すために、MFIB サブシステムが作成する仮想インターフェイスです。PimTunnel インターフェイスは、通常の **show interface** コマンドでは表示できません。

S/M,224/4

MFIBでは、マルチキャスト対応のインターフェイスごとに（S/M,224/4）エントリが作成されます。このエントリによって、直接接続されたネイバーから送信されたすべてのパケットが、PIM-SM RP に Register カプセル化されるようになります。一般に、PIM-SM によって（S,G）ルートが確立されるまでの間、ごく少数のパケットだけが（S/M,224/4）ルートを使用して転送されます。

たとえば、IP アドレス 10.0.0.1 およびネットマスク 255.0.0.0 のインターフェイスで、送信元アドレスがクラス A ネットワーク 10 に所属する IP マルチキャスト パケットにすべて一致するルートが作成されるとします。このルートは、慣例的なサブネット/マスク長の表記では（10/8,224/4）と記述されます。インターフェイスに複数の IP アドレスが割り当てられている場合には、これらの IP アドレスごとに 1 つずつルートが作成されます。

マルチキャスト ハイ アベイラビリティ

Cisco Catalyst 9300 シリーズ スイッチ はマルチキャスト ハイ アベイラビリティをサポートします。これにより、スーパーバイザエンジンに障害が発生してもマルチキャストトラフィックのフローが中断されることはありません。MFIB ステートは、スイッチオーバーの前にスタンバイ スーパーバイザエンジンに同期化され、スーパーバイザエンジンの障害時のスイッチオーバーのときに高速コンバージェンスでの NSF の可用性が確保されます。

マルチキャスト HA（SSO/NSF/ISSU）は、PIM スパースモードと SSM モードでサポートされます。つまり、IGMP および MLD スヌーピング用のレイヤ 2 でサポートされます。

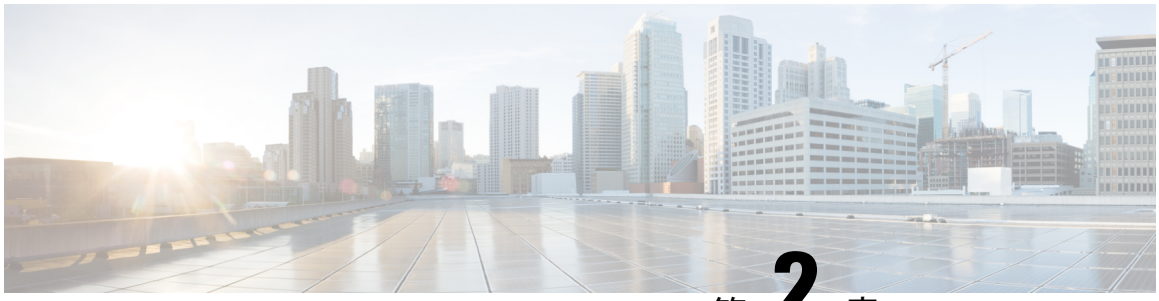
IP マルチキャストに関する追加情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)*

標準および RFC

標準/RFC	タイトル
RFC 1112	『*Host Extensions for IP Multicasting*』
RFC 2236	『*Internet Group Management Protocol, Version 2*』
RFC 4601	『*Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*』



第 2 章

基本的な IP マルチキャスト ルーティングの設定

基本的な IP マルチキャスト ルーティングの前提条件

次に、基本的な IP マルチキャスト ルーティングを設定するための前提条件を示します。

- IP マルチキャスト ルーティングを実行するには、PIM バージョンおよび PIM モードを設定する必要があります。スイッチはモード設定に従って、マルチキャスト ルーティング テーブルを読み込み、直接接続された LAN から受信したマルチキャスト パケットを転送します。インターフェイスはPIMデンス モード、スパース モード、またはSM-DM スパース - デンス モードのいずれかに設定できます。

- インターフェイスで PIM をイネーブルにすると、同じインターフェイス上で IGMP 処理もイネーブルになります。（IPマルチキャスティングに加入するには、マルチキャストホスト、ルータ、およびマルチレイヤデバイスで IGMP が動作している必要があります）

  複数のインターフェイスでPIMをイネーブルにした場合に、そのほとんどのインターフェイスが発信インターフェイス リストに含まれておらず、IGMP スヌーピングがディセーブルになっている場合は、レプリケーションが増加することにより、発信インターフェイスが回線レートを維持できないこともあります。

基本的な IP マルチキャスト ルーティングの制約事項

次に、IP マルチキャスト ルーティングの制約事項を示します。

基本的な IP マルチキャスト ルーティングに関する情報

IP マルチキャストは、ネットワーク リソース（特に、音声やビデオなどの帯域幅集約型サービス）を効率的に使用する方法です。IP マルチキャスト ルーティングにより、ホスト（ソース）は、IP マルチキャスト グループ アドレスと呼ばれる特別な形式の IP アドレスを使用して、IP ネットワーク内の任意の場所にあるホスト（レシーバ）にパケットを送信できます。

送信側ホストは、マルチキャスト グループ アドレスをパケットの IP 宛先アドレスフィールドに挿入します。IPマルチキャストルータおよびマルチレイヤ devicesは、マルチキャストグループのメンバに接続されたすべてのインターフェイスから着信した IP マルチキャストパケットを転送します。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受信します。

マルチキャスト転送情報ベース（MFIB）の概要

device は、IP マルチキャスト用のマルチキャスト転送情報ベース（MFIB）アーキテクチャとマルチキャストルーティング情報ベース（MRIB）を使用します。

MFIB アーキテクチャは、マルチキャスト コントロール プレーン（Protocol Independent Multicast（PIM）および Internet Group Management Protocol（IGMP））とマルチキャスト フォワーディング プレーン（MFIB）の間におけるモジュール性と分離の両方を提供します。このアーキテクチャは、Cisco IOS IPv6 マルチキャスト導入環境において使用します。

MFIB 自体は、マルチキャスト ルーティング プロトコルを選ばないフォワーディング エンジンです。つまり、PIM または他のマルチキャスト ルーティング プロトコルに依存しません。これは次の処理に関与します。

- マルチキャスト パケットの転送
- コントロール プレーンによって設定されたエントリとインターフェイス フラグを学習するための MRIB への登録
- コントロール プレーンに送信する必要があるデータ駆動型のイベントを処理する。
- 受信、ドロップ、および転送されたマルチキャストパケットの数、レート、およびバイトの保守

MRIB は、MRIB クライアント間の通信チャネルです。MRIB クライアントの例としては、PIM、IGMP、マルチキャスト ルーティング（mroute）テーブル、および MFIB があります。

IP マルチキャスト ルーティングのデフォルト設定

次の表に、IP マルチキャスト ルーティングのデフォルト設定を示します。

表 *2 : IP* 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
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

基本的な IP マルチキャスト ルーティングの設定方法

ここでは、基本的な IP マルチキャストルーティングの設定について説明します。

基本的な IP マルチキャスト ルーティングの設定

デフォルトでは、マルチキャストルーティングはディセーブルとなっており、モードは設定されていません。

この手順は必須です。

始める前に

PIM バージョンと PIM モードを設定する必要があります。スイッチはモード設定に従って、マルチキャスト ルーティング テーブルを読み込み、直接接続された LAN から受信したマルチキャスト パケットを転送します。

基本的な IP マルチキャスト ルーティングの設定

マルチキャスト ルーティング テーブルへのパケット読み込みでは、DM インターフェイスは常にテーブルに追加されます。SM インターフェイスがテーブルに追加されるのは、ダウンストリーム デバイスから定期的な Join メッセージを受信した場合、またはインターフェイスに直接接続されたメンバーが存在する場合に限ります。LAN から転送する場合、グループが認識している RP があれば、SM 動作が行われます。その場合、パケットはカプセル化され、その RP に送信されます。認識している RP がなければ、パケットは DM 方式でフラッディングされます。マルチキャスト送信元アドレスは、PIM デンスモードと PIM Any Source マルチキャストモードの両方で、直接接続された着信インターフェイス（同じサブネットの一部）に存在する必要があります。特定の送信元からのマルチキャスト トラフィックが十分であれば、レシーバの先頭ホップ ルータからその送信元に Join メッセージが送信され、送信元を基点とする配信ツリーが構築されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**}
5. **end**
6. **show running-config**
7. **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。 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： `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** *interface-id* 例： `デバイス(config)# interface gigabitethernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ 3 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 コンフィギュレーション コマンドを入力して設定された物理ポー

	コマンドまたはアクション	目的
		トです。また、インターフェイスの IP PIM スパース - デンス 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 IGMP スタティック グループに加入させる必要があります。 • 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 - デンス 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 IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP 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、IP アドレスを割り当てる必要があります。
ステップ 4	**ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**} 例： `デバイス(config-if)# ip pim sparse-dense-mode`	インターフェイスで PIM モードをイネーブルにします。 デフォルトで、モードは設定されていません。 キーワードの意味は次のとおりです。 • **dense-mode**：デンス動作モードをイネーブルにします。 • **sparse-mode**：スパース動作モードをイネーブルにします。SM を設定する場合は、RP も設定する必要があります。 • **sparse-dense-mode**：グループが属するモードでインターフェイスが処理されるようにします。DM-SM 設定を推奨します。 （注） インターフェイスで PIM を無効化するには、**no ip pim** 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。
ステップ 5	**end** 例： `デバイス(config-if)# 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 6	**show running-config** 例： デバイス# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： デバイス# **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。

IP マルチキャスト転送の設定

次の手順を使用して、デバイスに着信パケットまたは発信パケットの IPv4 マルチキャスト転送情報ベース（MFIB）割り込みレベルの IP マルチキャスト転送を設定できます。

（注） **ip multicast-routing** コマンドを使用して IP マルチキャストルーティングを有効にした後、IPv4 マルチキャスト転送が有効になります。IPv4 マルチキャスト転送はデフォルトで有効になっているため、IPv4 マルチキャスト転送を無効にするには、**ip mfib** 形式の **no** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip mfib**
4. **exit**
5. **show running-config**
6. **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： Device> **enable**	特権 EXEC モードを有効にします。 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。

	コマンドまたはアクション	目的
ステップ 3	**ip mfib** 例： `Device(config)# ip mfib`	IP マルチキャスト転送をイネーブルにします。
ステップ 4	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-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。

スタティック マルチキャスト ルート（mroute）の設定

- スタティック mroute は RPF 情報を計算するために使用されますが、トラフィックの転送には使用されません。
- スタティック mroute を再配布することはできません。

静的 mroute は、定義されているデバイスに厳密にローカルなものです。Protocol Independent Multicast（PIM）には独自のルーティング プロトコルがないため、ネットワーク全体にスタティック mroute を配布するメカニズムはありません。その結果、スタティック mroute の管理は、ユニキャスト スタティック ルートの管理よりも複雑になりがちです。

静的 mroute が設定されると、デバイスの静的 mroute テーブルと呼ばれる個別のテーブルに保存されます。設定されると、**ip mroute** コマンドによって、静的 mroute は、source-address および mask 引数に指定された送信元アドレスまたは送信元アドレス範囲の静的 mroute テーブルに入ります。送信元アドレスと一致する送信元、または source-address 引数に指定された送信元アドレス範囲にある送信元は、*rpf-address* 引数に指定された IP アドレスに関連付けられているインターフェイス、または *interface-type* および *interface-number* 引数に指定されたデバイス上のローカルインターフェイスに RPF を行います。IP アドレスが *rpf-address* 引数に指定されている場合、直接接続されたネイバーを検索するために、このアドレスでユニキャスト ルーティング テーブルから再帰ルックアップが実施されます。

複数の静的 mroute が設定されている場合、デバイスは mroute テーブルの最長一致ルックアップを実行します。（発信元アドレスの）最長一致を含む mroute が見つかると、検索が終了し、一致するスタティック mroute の情報が使用されます。スタティック mroute が設定される順序は重要ではありません。

mroute のアドミニストレーティブ ディスタンスは、任意の距離引数に指定することができます。距離引数に値が指定されていない場合、mrouteの距離はデフォルトのゼロになります。スタティック mroute が別の RPF 送信元と同じ距離である場合、スタティック mroute が優先されます。この規則には、2つだけ例外があります。直接接続されたルートとデフォルトのユニキャスト ルートです。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip mroute** [**vrf** *vrf-name*] *source-address mask* { **fallback-lookup** {**global** | **vrf** *vrf-name* }[*protocol*] {*rpf-address* | *interface-type interface-number*}} [**distance**]
4. **exit**
5. **show running-config**
6. **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： `Device> enable`	特権 EXEC モードを有効にします。 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	**ip mroute** [**vrf** *vrf-name*] *source-address mask* { **fallback-lookup** {**global** | **vrf** *vrf-name* }[*protocol*] {*rpf-address* | *interface-type interface-number*}} [**distance**] 例： `Device(config)# ip mroute 10.1.1.1 255.255.255.255 10.2.2.2`	送信元 IP アドレス 10.1.1.1 が、IP アドレス 10.2.2.2 に関連付けられているインターフェイスを介して到達可能であるように設定されます。
ステップ 4	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	（任意）入力を確認します。
ステップ 6	**copy running-config startup-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。

オプションの IP マルチキャスト ルーティングの設定

ここでは、オプションの IP マルチキャストルーティングの設定について説明します。

IP マルチキャスト境界の定義

自動 RP メッセージが PIM ドメインに入らないようにする場合は、マルチキャスト境界を定義します。自動 RP 情報を伝達する 224.0.1.39 および 224.0.1.40 宛てのパケットを拒否するアクセス リストを作成します。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **deny** *source* [*source-wildcard*]
4. **interface** *interface-id*
5. **ip multicast boundary** *access-list-number*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**access-list** *access-list-number* **deny** *source* [*source-wildcard*]
	例：
	`Device(config)#`
	`access-list 12 deny 224.0.1.39`
	`access-list 12 deny 224.0.1.40`
		標準アクセスリストを作成し、コマンドを必要な回数だけ実行します。
		• *access-list-number* の範囲は 1 ～ 99 です。
		• **deny** キーワードは、条件が一致した場合にアクセスを拒否します。
		• *source* には、自動 RP 情報を伝達するマルチキャスト アドレス 224.0.1.39 および 224.0.1.40 を入力します。
		•（任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進

	コマンドまたはアクション	目的
		表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、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。 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。 • 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。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 5	**ip multicast boundary** *access-list-number* 例： `Device(config-if)# ip multicast boundary 12`	ステップ 2 で作成したアクセス リストを指定し、境界を設定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-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。

sdr リスナー サポートの設定

ここでは、sdr リスナーサポートの設定について説明します。

sdr リスナー サポート機能のイネーブル化

デフォルトでは、デバイスでセッションディレクトリのアドバタイズメントは受信されません。この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip sap listen**
5. **end**
6. **show running-config**
7. **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： `Device> enable`	特権 EXEC モードを有効にします。 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	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	sdr 用に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 - デンス 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 IGMP スタティック グループに加入させる必要があります。設定例については、例：ルーテッド ポートとしてのインターフェイス設定（107 ページ）を参照してください。 • 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

	コマンドまたはアクション	目的
		で IP PIM スパース - デンス 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 IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。設定例については、例：SVI としてのインターフェイスの設定 （107 ページ）を参照してください。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip sap listen** 例： `Device(config-if)# ip sap listen`	デバイス ソフトウェアがセッション ディレクトリ アナウンスメントをリッスンできるようにします。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-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。

sdr キャッシュ エントリの存在期間の制限

デフォルトでは、エントリは sdr キャッシュから削除されません。送信元が SAP 情報のアドバタイズを停止した場合に、古いアドバタイズメントが不必要に保持されないようにするため、エントリがアクティブである期間を制限できます。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sap cache-timeout** *minutes*
4. **end**
5. **show running-config**
6. **show ip sap**
7. **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： `Device> enable`	特権 EXEC モードを有効にします。 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	**ip sap cache-timeout** *minutes* 例： `Device(config)# ip sap cache-timeout 30`	Session Announcement Protocol（SAP）キャッシュ エントリがキャッシュ内にアクティブである期間を制限します。 デフォルトでは、エントリはキャッシュから削除されません。 *minutes* に指定できる範囲は 1 ～ 1440 分（24 時間）です。
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	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**show ip sap** 例： `Device# show ip sap`	SAP キャッシュを表示します。
ステップ 7	**copy running-config startup-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。

基本的なIPマルチキャストルーティングのモニタリングおよびメンテナンス

キャッシュ、テーブル、およびデータベースのクリア

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定のキャッシュ、テーブル、またはデータベースの内容が無効である場合、または無効である可能性がある場合は、これらをクリアする必要があります。

次の表に示す特権EXECコマンドのいずれかを使用すると、IPマルチキャストのキャッシュ、テーブル、データベースをクリアできます。

表 *3:* キャッシュ、テーブル、およびデータベースをクリアするコマンド

コマンド	目的
clear ip igmp group {**group** [*hostname* | *IP address*] | **vrf** *name* **group** [*hostname* | *IP address*] }	IGMP キャッシュのエ
clear ip mroute { ***** | [*hostname* | *IP address*] | **vrf** *name* **group** [*hostname* | *IP address*] }	IP マルチキャスト ル除します。
clear ip sap [*group-address* | **"***session-name***"**]	Session Directory Proto シュ）エントリを削

システムおよびネットワーク統計情報の表示

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。

（注） このリリースでは、ルート単位の統計情報がサポートされていません。

また、リソースの使用状況を学習し、ネットワーク問題を解決するための情報を表示することもできます。さらに、ノードの到達可能性に関する情報を表示し、そのパケットが経由するネットワーク内のパスを検出することもできます。

次の表に示す特権EXECコマンドのいずれかを使用すると、さまざまなルーティング統計情報を表示できます。

表 *4:* システムおよびネットワーク統計情報を表示するコマンド

コマンド	目的
ping [*group-name* | *group-address*]	マルチキャスト グループ アドレス求を送信します。
show ip igmp filter	IGMP フィルタ情報を表示します
show ip igmp groups [*group-name*|*group-address*|*type-number*]	デバイスに直接接続され、IGMP
show ip igmp interface [*type number*]	インターフェイスのマルチキャス
show ip igmp profile [profile_number]	IGMP プロファイル情報を表示し
show ip igmp ssm-mapping [*hostname/IP address*]	IGMP SSM マッピング情報を表示
show ip igmp static-group {**class-map** [**interface** [type]]	スタティック グループ情報を表示
show ip igmp membership [*name/group address* | **all** | **tracked**]	転送に関する IGMP メンバーシッ
show ip igmp vrf	選択した VPN ルーティング/転送
show ip mfib [*type number*]	IP マルチキャスト転送情報ベース
show ip mrib { **client** | **route** | **vrf** }	マルチキャスト ルーティング情報
show ip mrm { **interface** | **manager** | **status-report** }	IP マルチキャスト ルーティング
show ip mroute [*group-name* | *group-address*] [*source*] [**count** | **interface** | **proxy** | **pruned** | **summary** | **verbose**]	IP マルチキャスト ルーティング
show ip msdp { **count** | **peer** | **rpf-peer** | **sa-cache** | **summary** | **vrf** }	Multicast Source Discovery Protocol
show ip multicast [**interface** | **limit** | **mpls** | **redundancy** | **vrf**]	グローバル マルチキャスト情報を
show ip pim all-vrfs { **tunnel** }	すべての VRF を表示します。
show ip pim autorp	グローバル Auto-RP 情報を表示し
show ip pim boundary [*type number*]	境界情報を表示します。
show ip pim bsr-router	ブートストラップ ルータ情報（
show ip pim interface [*type number*] [**count** | **detail** | **df** | **stats**]	PIMに対して設定されたインター ソフトウェア イメージで使用でき
show ip pim neighbor [*type number*]	デバイスによって検出されたPIM トウェア イメージで使用できます

コマンド	目的
show ip pim mdt [**bgp**]	マルチキャスト トンネル情報を表示
show ip pim rp [*group-name* | *group-address*]	スパース モードのマルチキャスト グ ドは、すべてのソフトウェア イメー
show ip pim rp-hash [*group-name* | *group-address*]	選択したグループに基づいて選択さ
show ip pim tunnel [*tunnel* | *verbose*]	登録済みのトンネルを表示します。
show ip pim vrf *name*	VPN ルーティングおよび転送のイン
show ip rpf {*source-address* | *name*}	デバイスの RPF の実行方法（ユニキ ル、静的マルチキャストルーティン コマンド パラメータは次のとおりで • *Host name* または *IP address*：IP • **Select**：グループ ベースの VRF • **vrf**：VPN ルーティング/転送イン
show ip sap [*group* | **"***session-name***"** | **detail**]	Session Announcement Protocol（SAP） コマンド パラメータは次のとおりで • *A.B.C.D*：IP グループ アドレス。 • *WORD*：セッション名（二重引用 • **detail**：セッションの詳細。

基本的な IP マルチキャストルーティングの設定例

ここでは、基本的な IP マルチキャストルーティングの設定例を紹介します。

例：IP マルチキャスト境界の設定

次に、すべての管理用スコープのアドレスに対して境界を設定する例を示します。

```
デバイス(config)# access-list 1 deny 239.0.0.0 0.255.255.255
デバイス(config)# access-list 1 permit 224.0.0.0 15.255.255.255
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip multicast boundary 1
```

例：mrinfo 要求への応答

ソフトウェアは、マルチキャストルーティングされたシステム、シスコルータ、およびマルチレイヤdevicesによって送信されたmrinfo要求に応答します。ソフトウェアはネイバーに関する情報を、DVMRPトンネルおよびすべてのルーテッドインターフェイスを通して戻します。この情報にはメトリック（常に1に設定）、設定されたTTLしきい値、インターフェイスのステータス、および各種フラグが含まれます。次の例のように、**mrinfo** 特権 EXEC コマンドを使用し、ルータまたはdevice自体をクエリすることもできます。

```
デバイス# mrinfo
  171.69.214.27 (mm1-7kd.cisco.com) [version cisco 11.1] [flags: PMS]:
  171.69.214.27 -> 171.69.214.26 (mm1-r7kb.cisco.com) [1/0/pim/querier]
  171.69.214.27 -> 171.69.214.25 (mm1-45a.cisco.com) [1/0/pim/querier]
  171.69.214.33 -> 171.69.214.34 (mm1-45c.cisco.com) [1/0/pim]
  171.69.214.137 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
  171.69.214.203 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
  171.69.214.18 -> 171.69.214.20 (mm1-45e.cisco.com) [1/0/pim]
  171.69.214.18 -> 171.69.214.19 (mm1-45c.cisco.com) [1/0/pim]
  171.69.214.18 -> 171.69.214.17 (mm1-45a.cisco.com) [1/0/pim]
```

基本的なIPマルチキャストルーティングに関するその他の関連情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)*

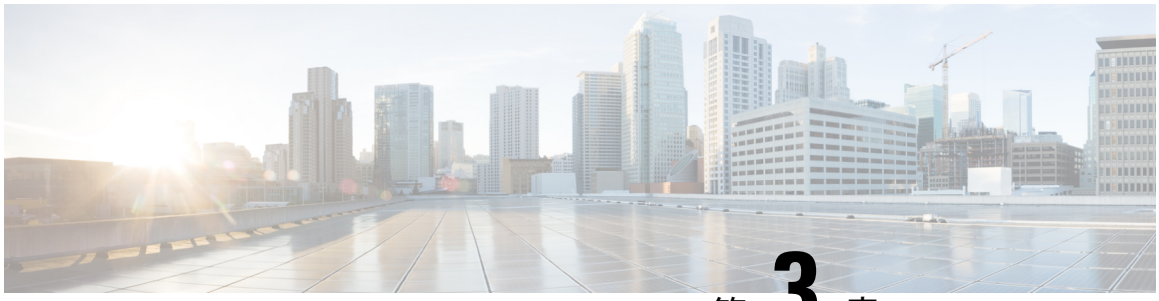
基本的な IP マルチキャストルーティングの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IP マルチキャスト ルーティング	IP マルチキャストは、ネットワーク リソース（特に、音声やビデオなどの帯域幅集約型サービス）を効率的に使用する方法です。IP マルチキャスト ルーティングにより、ホスト（ソース）は、IP マルチキャスト グループ アドレスと呼ばれる特別な形式の IP アドレスを使用して、IP ネットワーク内の任意の場所にあるホスト（レシーバ）にパケットを送信できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。



第 3 章

GRE トンネルを介するマルチキャスト ルーティングの設定

GRE トンネルを介するマルチキャスト ルーティングの設定の前提条件

GRE を介するマルチキャスト ルーティングを設定する前に、IP マルチキャスト ルーティング テクノロジーと GRE トンネリングの概念についてよく理解しておく必要があります。

GRE トンネルを介するマルチキャスト ルーティングの設定の制約事項

次に、GRE トンネルを介するマルチキャスト ルーティングの設定の制約事項を示します。

- GRE トンネルを介する IPv6 マルチキャストはサポートされません。
- サポートされるマルチキャスト ルート（mroute）の総数は、すべてのトンネル全体で32000です。
- 双方向 PIM はサポートされていません。

- GRE トンネルを介するマルチキャストをサポートするには、マルチキャスト ルーティングを最初のホップ ルータ（FHR）、ランデブー ポイント（RP）および最後のホップ ルータ（LHR）で設定する必要があります。
- Catalyst 9000 シリーズ スイッチでは、トンネル送信元をループバック インターフェイス、物理インターフェイス、または L3 EtherChannel インターフェイスにできます。
- IPSec、ACL、トンネル カウンタ、暗号化サポート、フラグメンテーション、Cisco Discovery Protocol（CDP）、QoS、GRE キープアライブ、マルチポイント GRE などの機能の相互作用は、GRE トンネルでサポートされていません。

GRE トンネルを介するマルチキャスト ルーティングについて

この章では、非 IP マルチキャスト エリア間で IP マルチキャスト パケットをトンネリングするために、Generic Route Encapsulation（GRE）トンネルを設定する方法について説明します。その利点は、IP マルチキャストをサポートしないエリアを経由して、IP マルチキャスト トラフィックをソースからマルチキャスト グループに送信できることです。GRE トンネルを介するマルチキャスト ルーティングは、スパース モードおよび pim-ssm モードをサポートしています。また、スタティック RP および Auto-RP もサポートしています。スタティック RP と Auto-RP の設定の詳細については、ランデブー ポイントと Auto-RP を参照してください。

非 IP マルチキャスト エリアを接続するトンネリングの利点

- 送信元とグループ メンバー（宛先）間のパスが IP マルチキャストをサポートしていない場合、それらの間のトンネルは IP マルチキャスト パケットを転送できます。

GRE トンネルを介するマルチキャスト ルーティングの設定方法

ここでは、GRE トンネルを介したマルチキャストルーティングの設定手順について説明します。

非 IP マルチキャスト エリアを接続する GRE トンネルの設定

マルチキャストルーティングをサポートしていないメディアで接続されている送信元と宛先の間の IP マルチキャスト パケットを転送するように GRE トンネルを設定できます。

手順の概要

1. **enable**

2. **configure terminal**
3. **ip multicast-routing**
4. **interface tunnel** *number*
5. **ip address ip_address** *subnet_mask*
6. **ip pim sparse-mode**
7. **tunnel source** { *ip-address* | *interface-name* }
8. **tunnel destination** { *hostname* | *ip-address* }
9. **end**
10. **show interface** *type number*

手順の詳細

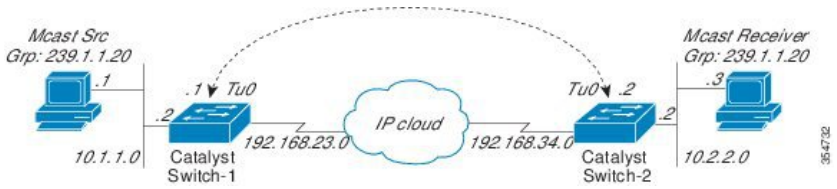
	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip multicast-routing** 例： `Device(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。
ステップ 4	**interface tunnel** *number* 例： `Device(config)# interface tunnel 0`	トンネル 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 5	**ip address ip_address** *subnet_mask* 例： `Device(config-if)# ip address 192.168.24.1 255.255.255.252`	IP アドレスおよび IP サブネットを設定します。
ステップ 6	**ip pim sparse-mode** 例： `Device(config-if)# ip pim sparse-mode`	次の動作モードのいずれかでトンネルインターフェイス上で Protocol Independent Multicast（PIM）の動作のスパース モードをイネーブルにします。
ステップ 7	**tunnel source** { *ip-address* | *interface-name* } 例：	トンネル送信元を設定します。

	コマンドまたはアクション	目的
	`Device(config-if)# tunnel source 100.1.1.1`	
ステップ 8	**tunnel destination** { *hostname* | *ip-address* } 例： `Device(config-if)# tunnel destination 100.1.5.3`	トンネル宛先を設定します。
ステップ 9	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。
ステップ 10	**show interface** *type number* 例： `Device# show interface tunnel 0`	トンネル インターフェイスの情報を表示します。

非 IP マルチキャスト エリアを接続するトンネリングの例

次の例に、GRE トンネルを介した Catalyst スイッチ間のマルチキャストルーティングを示します。

図 7: 非 IP マルチキャスト エリアを接続するトンネル



上の図では、マルチキャスト送信元（10.1.1.1）は、Catalyst スイッチ 1 に接続され、マルチキャストグループ 239.1.1.20 に設定されています。マルチキャスト受信者（10.2.2.3）は、Catalyst スイッチ 2 に接続され、グループ 239.1.1.20 のマルチキャストパケットを受信するように設定されています。スイッチ 1 とスイッチ 2 は、マルチキャスト ルーティング用に設定されていない IP クラウドで分離されています。

GRE トンネルは、ループバック インターフェイスで送信元が特定されたスイッチ 1 とスイッチ 2 の間に設定されています。マルチキャスト ルーティングは、スイッチ 1 とスイッチ 2 で有効になっています。スパースモードで PIM をサポートするために、**ip pim sparse-mode** コマンドがトンネルインターフェイスに設定されています。トンネル インターフェイスのスパース モード設定により、スパース モード パケットをグループのランデブー ポイント（RP）設定に応じてトンネルを経由して転送できます。

スイッチ 1 の設定：

```
Device(config)# ip multicast-routing
Device(config)# interface Loopback0   //Tunnel source interface
Device(config-if)# ip address 2.2.2.2 255.255.255.255

Device(config)# interface Tunnel 10    //Tunnel interface configured for PIM
traffic
Device(config-if)# ip address 192.168.24.1 255.255.255.252
Device(config-if)# ip pim sparse-mode
Device(config-if)# ip nhrp map 192.168.24.3  4.4.4.4  //NHRP may optionally be
configured to dynamically discover tunnel end points.
Device(config-if)# ip nhrp map multicast 4.4.4.4
Device(config-if)# ip nhrp network-id 1
Device(config-if)# ip nhrp nhs 192.168.24.3
Device(config-if)# tunnel source Loopback0
Device(config-if)# tunnel destination 4.4.4.4

Device(config)# interface GigabitEthernet 0/0/0      //Source interface
Device(config-if)# ip address 10.1.1.2 255.255.255.0
Device(config-if)# ip pim sparse-mode
```

スイッチ 2 の設定：

```
Device(config)# ip multicast-routing
Device(config)# interface Loopback0    //Tunnel source interface
Device(config-if)# ip address 4.4.4.4 255.255.255.255

Device(config)# interface Tunnel 10     //Tunnel interface configured for PIM
 traffic
Device(config-if)# ip address 192.168.24.2 255.255.255.252
Device(config-if)# ip nhrp map 192.168.24.4 2.2.2.2  //NHRP may optionally be
configured to dynamically discover tunnel end points.
Device(config-if)# ip nhrp map multicast 2.2.2.2
Device(config-if)# ip nhrp network-id 1
Device(config-if)# ip nhrp nhs 192.168.24.4
Device(config-if)# ip pim sparse-mode
Device(config-if)# tunnel source Loopback0
Device(config-if)# tunnel destination 2.2.2.2

Device(config)# interface GigabitEthernet 0/0/0     //Receiver interface
Device(config-if)# ip address 10.2.2.2 255.255.255.0
Device(config-if)# ip pim sparse-mode
```

GRE トンネルを介するマルチキャスト ルーティングに関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9300 Series Switches)* の「IP マルチキャスト ルーティング コマンド」の項を参照してください。

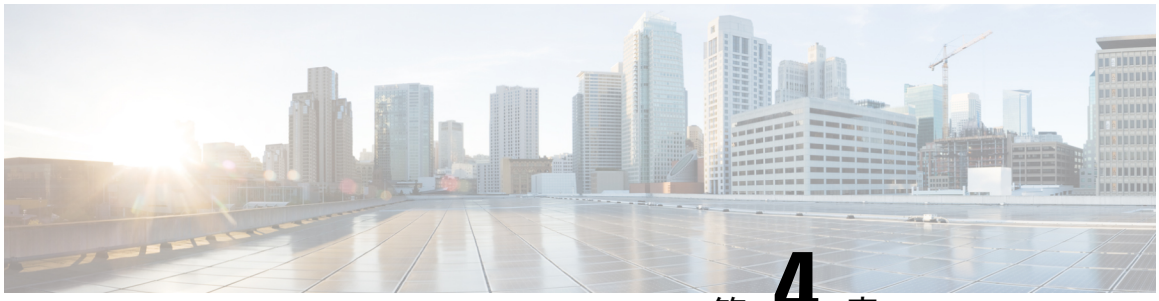
GRE トンネルを介するマルチキャストルーティングの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	GRE トンネルを介するマルチキャスト ルーティング	GRE トンネルを介するマルチキャストルーティングを使用すると、IP マルチキャストをサポートしないエリアを経由して、IP マルチキャストトラフィックを送信元からマルチキャストグループに送信できます。

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。



第 4 章

IGMP の設定

IGMP および IGMP スヌーピングの前提条件

IGMP スヌーピングの前提条件

IGMP スヌーピング クエリアを設定するときには、次の注意事項を順守します。

- VLAN をグローバル コンフィギュレーション モードに設定してください。
- IP アドレスおよび VLAN インターフェイスを設定してください。IGMP スヌーピング クエリアは、イネーブルの場合この IP アドレスをクエリーの送信元アドレスとして使用します。
- VLAN インターフェイス上で IP アドレスが設定されていない場合、IGMP スヌーピング クエリアは IGMP クエリア用に設定されたグローバル IP アドレスを使用しようとします。グローバル IP アドレスが指定されていない場合、IGMP クエリアは VLAN デバイスの仮想インターフェイス（SVI）IP アドレス（存在する場合）を使用しようとします。SVI IP アドレスが存在しない場合、デバイスはデバイス上で設定された利用可能な最初の IP アドレスを使用します。利用可能な最初の IP アドレスは、**show ip interface** 特権 EXEC コマンドの出力に表示されます。IGMP スヌーピング クエリアはデバイス上で利用可能な IP アドレスを検出できない場合、IGMP 一般クエリを生成しません。

- IGMP スヌーピング クエリアは IGMP バージョン 1 および 2 をサポートします。
- 管理上イネーブルである場合、IGMP スヌーピング クエリアはネットワークにマルチキャスト ルータの存在を検出すると、非クエリア ステートになります。
- 管理上イネーブルである場合、IGMP スヌーピング クエリアは操作上、次の状況でディセーブル ステートになります。
  - IGMP スヌーピングが VLAN でディセーブルの場合
  - PIM が、VLAN に対応する SVI でイネーブルの場合

IGMP および IGMP スヌーピングの制約事項

IGMP 設定の制約事項

次に、IGMP を設定する際の制約事項を示します。

- デバイスは IGMP バージョン 1 、2、3 をサポートしています。

（注） IGMP バージョン 3 の場合、IGMP バージョン 3 BISS（基本的な IGMPv3 スヌーピング サポート）のみがサポートされます。

- IGMP バージョン 3 では新しいメンバーシップ レポート メッセージを使用しますが、これらは以前の IGMP スヌーピングデバイスで正しく認識されない可能性があります。
- IGMPv3 は、ISM および SSM と同時に動作可能です。ISM では、exclude と include の両方のモードのレポートを適用できます。SSM では、ラストホップ ルータは include モードのレポートだけを受け入れます。exclude モードのレポートは無視されます。
- ACL により、指定のポートをマルチキャストルータポートではなく、マルチキャストホストポートとしてだけ指定できます。このポートで受信されたマルチキャストルータ制御パケットは、ドロップされます。

IGMP スヌーピングの制約事項

次に、IGMP スヌーピングの制約事項を示します。

- このデバイスは、宛先マルチキャスト IP アドレスのみに基づいて IGMPv3 スヌーピングをサポートします。送信元 IP アドレスやプロキシ レポートに基づいてスヌーピングをサポートすることはありません。
- IGMP フィルタリングまたはマルチキャスト VLAN レジストレーション（MVR）が実行されているデバイスは、IGMPv3 Join および Leave メッセージをサポートしません。

- IGMP レポート抑制は、マルチキャストクエリに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリに IGMPv3 レポートが含まれている場合はサポートされません。
- IGMP の脱退時間の設定は、IGMP バージョン 2 が稼働しているホストでのみサポートされます。IGMP バージョン 2 は、デバイスのデフォルトバージョンです。

  ネットワークで実際の脱退にかかる待ち時間は、通常、設定した脱退時間どおりになります。ただし、脱退時間は、リアルタイムの CPU の負荷の状態、およびネットワークの遅延状態、インターフェイスから送信されたトラフィック量によって、設定された時間を前後することがあります。
- IGMP スロットリング アクションの制約事項は、レイヤ 2 ポートにだけ適用されます。**ip igmp max-groups action replace** インターフェイス コンフィギュレーション コマンドは論理 EtherChannel インターフェイスで使用できますが、EtherChannel ポート グループに属するポートでは使用できません。

  グループの最大数に関する制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups action**{**deny** | **replace**} コマンドを入力しても効果はありません。

  インターフェイスによりマルチキャスト エントリが転送テーブルに追加されてから、スロットリング アクションを設定し、グループの最大数の制限を設定すると、転送テーブルのエントリは、スロットリング アクションに応じて期限切れになるか削除されます。

IGMP に関する情報

Internet Group Management Protocol の役割

IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。インターフェイスで PIM をイネーブルにすると、IGMP もイネーブルになります。IGMP 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。

- 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（ルータなど）です。
- ホストは、クエリアにホスト メンバーシップを通知するためのレポート メッセージ（クエリー メッセージに応答するメッセージ）を送信するレシーバで、ルータも含まれます。ホストでは、IGMP メッセージを使用して、マルチキャスト グループに加入し、マルチキャスト グループを脱退します。

ホストは、そのローカル マルチキャスト デバイスに IGMP メッセージを送信することで、グループ メンバーシップを識別します。IGMP では、デバイスは IGMP メッセージを受信し、定期的にクエリーを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

IGMP マルチキャスト アドレス

IP マルチキャスト トラフィックには、グループ アドレス（クラス D IP アドレス）が使用されます。クラス D アドレスの上位 4 ビットは 1110 です。したがって、ホスト グループ アドレスの範囲は 224.0.0.0 ～ 239.255.255.255 であると考えられます。

224.0.0.0 ～ 224.0.0.255 のマルチキャスト アドレスは、ルーティング プロトコルおよびその他のネットワーク制御トラフィックが使用するために予約されています。アドレス 224.0.0.0 は、どのグループにも割り当てられません。

IGMP パケットは IP マルチキャスト グループ アドレスを使用して次のように送信されます。

- IGMP 汎用クエリーは、アドレス 224.0.0.1（サブネット上のすべてのシステム）を宛先とします。
- IGMP グループ固有のクエリーは、クエリー対象デバイスのグループ IP アドレスを宛先とします。
- IGMP グループ メンバーシップ レポートは、レポート対象デバイスのグループ IP アドレスを宛先とします。
- IGMPv2 グループ脱退メッセージは、アドレス 224.0.0.2（サブネット上のすべてのデバイス）を宛先とします。
- IGMPv3 メンバーシップ レポートはアドレス 224.0.0.22 を宛先とします。すべての IGMPv3 対応マルチキャスト デバイスはこのアドレスをリッスンする必要があります。

IGMP のバージョン

デバイスは、IGMP バージョン 1、IGMP バージョン 2、および IGMP バージョン 3 をサポートしています。これらのバージョンは、デバイス上でそれぞれ相互運用できます。たとえば、IGMP スヌーピングがイネーブルになっていて、クエリアのバージョンが IGMPv2 で、デバイスがホストから IGMPv3 レポートを受信している場合、デバイスは IGMPv3 レポートをマルチキャストルータに転送できます。

IGMPv3 デバイスは、Source Specific Multicast（SSM; 送信元特定マルチキャスト）機能を実行しているデバイスとの間で、メッセージを送受信できます。

IGMP バージョン 1

IGMP バージョン 1（IGMPv1）にはクエリ応答モデルが使用されているため、マルチキャスト ルータおよびマルチレイヤデバイスは、ローカルサブネット上のどのマルチキャストグループがアクティブであるか（マルチキャストグループに関係するホストが 1 台または複数存在するか）を判別できます。IGMPv1 では別のプロセスを使用して、ホストをマルチキャスト グループに加入および脱退させることができます。詳細については、RFC 1112 を参照してください。

IGMPv2

IGMP バージョン 2 は IGMP 機能の拡張版です。IGMP 脱退処理などの機能を提供して、脱退遅延を短縮し、グループ固有のクエリー数を削減し、明示的な最大クエリー応答時間を短縮します。また、この作業を実行するために、マルチキャストプロトコルに依存することなく IGMP クエリアを選択する機能もルータに追加されます。詳細については、RFC 2236 を参照してください。

（注） IGMP バージョン 2 は、デバイスのデフォルトバージョンです。

IGMP バージョン 3

デバイスは IGMP バージョン 3 をサポートしています。

IGMPv3 デバイスは、Basic IGMPv3 Snooping Support（BISS）をサポートしています。BISS は、IGMPv1 および IGMPv2 スイッチでのスヌーピング機能と、IGMPv3 メンバーシップ レポート メッセージをサポートしています。ネットワークに IGMPv3 ホストがある場合、BISS によりマルチキャスト トラフィックのフラッディングは抑制されます。トラフィックは、IGMPv2 または IGMPv1 ホストの IGMP スヌーピング機能の場合とほぼ同じポート セットに抑制されます。

IGMPv3 デバイスは、Source Specific Multicast（SSM; 送信元特定マルチキャスト）機能を実行しているデバイスとの間で、メッセージを送受信できます。

IGMPv3 ホスト シグナリング

IGMPv3 は、ホストがマルチキャスト グループのラスト ホップ デバイスにメンバーシップを伝える IETF 標準トラック プロトコルの第 3 バージョンです。IGMPv3 は、グループ メンバーシップを伝える能力をホストに与えます。これによってソースに関するフィルタリングが可能になります。ホストは、特定のソースを除いて、グループに送信するすべてのソースからトラフィックを受信したい（EXCLUDE と呼ばれるモード）、またはグループに送信する特定のソースからのみトラフィックを受信したい（INCLUDE と呼ばれるモード）と伝えることができます。

IGMPv3 は、ISM および SSM と同時に動作可能です。ISM では、EXCLUDE モードと INCLUDE モードの両方のレポートがラスト ホップ ルータによって受け入れられます。SSM では、INCLUDE モード レポートのみがラスト ホップ ルータによって受け入れられます。

IGMP のバージョンの違い

Internet Engineering Task Force（IETF）の Request for Comments（RFC）ドキュメントで定義されているように、IGMP には 3 種類のバージョンがあります。IGMPv2 は IGMPv1 の強化版で、ホストがマルチキャスト グループからの脱退を通知する機能が追加されていいます。IGMPv3 は IGMPv2 の強化版で、あるソース IP アドレスのセットから送信されたマルチキャストだけをリッスンする機能が追加されています。

表 *5 : IGMP* のバージョン

IGMP のバージョン	説明
IGMPv1	どのマルチキャスト グループがアクティブであるかをマルチキャスト デバイスが判断できる基本的なクエリー応答メカニズムと、ホストがマルチキャスト グループに加入および脱退できるようにするためのその他のプロセスを提供します。RFC 1112 で、IP マルチキャスト用の IGMPv1 ホスト拡張が定義されています。
IGMPv2	IGMP の拡張で、IGMP の脱退処理、グループ固有のクエリーおよび明示的な最大応答時間フィールドなどの機能が可能になっています。また、IGMPv2 ではこの作業を実行するために、マルチキャスト プロトコルに依存することなく IGMP クエリアを選択する機能もデバイスに追加されます。IGMPv2 は RFC 2236 で定義されています。
IGMPv3	ソース フィルタリングを提供します。これにより、マルチキャスト レシーバ ホストは、どのグループからマルチキャスト トラフィックを受信するか、およびこのトラフィックがどのソースからのものと想定されているかをデバイスに知らせることができます。さらに、IGMPv3 は IGMPv3 メンバーシップ レポートの宛先 IP アドレスであるリンク ローカル アドレス 224.0.0.22 をサポートしています。すべての IGMPv3 対応マルチキャスト デバイスは、このアドレスをリッスンする必要があります。IGMPv3 は RFC 3376 で定義されています。

（注） デフォルトでは、インターフェイスで PIM をイネーブルにすると、そのデバイスで IGMPv2 がイネーブルになります。IGMPv2 は、可能な限り IGMPv1 と下位互換性を保つよう設計されました。この下位互換性を実現するために、RFC 2236 は特別な相互運用性ルールを定義しています。ネットワークにレガシー IGMPv1 ホストが含まれている場合は、これらの運用性ルールをよく知っておく必要があります。IGMPv1 と IGMPv2 の相互運用性の詳細については、RFC 2236『Internet Group Management Protocol, Version 2』を参照してください。

IGMPv1 を実行するデバイス

IGMPv1 デバイスは、「全ホスト」へのマルチキャスト アドレスである 224.0.0.1 に IGMP クエリーを送信して、アクティブ マルチキャスト レシーバが存在するマルチキャスト グループを求めます。マルチキャスト レシーバも、デバイスに IGMP レポートを送信して、特定のマルチキャスト ストリームの受信を待機していることを通知できます。ホストは非同期に、またはデバイスによって送信される IGMP クエリーに対応して、レポートを送信できます。同じマルチキャスト グループに複数のマルチキャスト レシーバが存在する場合、これらのホストの 1 つ

のみで、IGMP レポート メッセージが送信されます。他のホストでは、レポート メッセージが抑制されます。

IGMPv1 では、IGMP クエリア選択はありません。セグメント内に複数のデバイスがある場合、すべてのデバイスが定期的に IGMP クエリーを送信します。IGMPv1 には、ホストがグループから脱退できる特別なメカニズムはありません。ホストで、特定のグループに対するマルチキャスト パケットを受信する必要がなくなった場合は、デバイスから送信される IGMP クエリー パケットに対する応答を行わないだけです。デバイスはクエリー パケットを送信し続けます。デバイスが 3 回 IGMP クエリーの応答を受信しないと、グループはタイムアウトし、デバイスはグループのセグメントへのマルチキャスト パケットの送信を停止します。ホストがタイムアウト期間後にマルチキャスト パケットを受信する場合、そのホストは新しい IGMP join をデバイスに送信するだけです。これにより、デバイスはマルチキャスト パケットの転送を再開します。

LAN 上に複数のデバイスが存在する場合は、指定ルータ（DR）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。PIM デバイスは DR を選択する選定プロセスに従います。最も大きい IP アドレスを持つ PIM デバイスが DR になります。

DR は、次のタスクを担当します。

- PIM 登録メッセージ、PIM 加入メッセージ、および PIM プルーニング メッセージをランデブー ポイント（RP）に送信し、ホスト グループ メンバーシップに関する情報を通知する。
- IGMP ホスト クエリー メッセージを送信する。
- IGMP オーバーヘッドをホストおよびネットワークでできるだけ低く維持するために、ホスト クエリー メッセージをデフォルトで 60 秒ごとに送信する。

IGMPv2 を実行するデバイス

IGMPv2 では、IGMPv1 のクエリー メッセージング機能が改善されました。

IGMPv2 のクエリーおよびメンバーシップ レポート メッセージは、次の 2 つの例外を除き、IGMPv1 メッセージと同じです。

- IGMPv2 クエリー メッセージは、一般クエリー（IGMPv1 クエリーと同じ）とグループ固有クエリーの 2 つのカテゴリに分かれる。
- IGMPv1 メンバーシップ レポートと IGMPv2 メンバーシップ レポートの IGMP タイプ コードが異なる。

IGMPv2 では、次の機能に対するサポートを追加することにより、IGMP の機能の強化も行われました。

- クエリア選択プロセス：IGMPv2 デバイスが、プロセスを実行するマルチキャスト ルーティング プロトコルに依存せずに、IGMP クエリアを選択できる機能を提供します。

- [Maximum Response Time] フィールド：IGMP クエリアを使用して最大クエリー応答時間を指定できる、クエリーメッセージの新しいフィールド。このフィールドで、応答のバースト性を制御し、脱退遅延を調整するクエリー応答プロセスの調整ができます。
- グループ固有クエリーメッセージ：すべてのグループではなく特定の 1 つのグループでクエリー操作を実行する目的で、IGMP クエリアを使用することができます。
- グループ脱退メッセージ：グループから脱退することをネットワーク上のデバイスに通知する手段をホストに提供します。

DR と IGMP クエリアが通常同じデバイスである IGMPv1 とは異なり、IGMPv2 では 2 つの機能は分離されます。DR と IGMP クエリアは異なる基準で選択され、同じサブネット上の異なるデバイスである場合があります。DR はサブネットで IP アドレスが最大のデバイスで、IGMP クエリアは最小の IP アドレスを持つデバイスです。

次のように、クエリー メッセージは IGMP クエリアの選択に使用されます。

1. 各 IGMPv2 デバイスは起動時に、そのインターフェイスアドレスを一般クエリーメッセージのソース IP アドレス フィールドに使用して、当該メッセージを全システムのグループアドレス 224.0.0.1 にマルチキャスト送信します。
2. IGMPv2 デバイスが一般クエリー メッセージを受信すると、デバイスは自分のインターフェイス アドレスとメッセージのソース IP アドレスを比較します。サブネット上の最下位 IP アドレスが使用されているデバイスにより、IGMP クエリアが選択されます。
3. すべてのデバイス（クエリアは除く）でクエリー タイマーが開始されます。IGMP クエリアから一般クエリー メッセージを受信するたびに、タイマーはリセットされます。クエリー タイマーが切れると、IGMP クエリアがダウンしたと見なされ、新しい IGMP クエリアを選択するために選択プロセスが再度実行されます。

デフォルトでは、タイマーはクエリー インターバルの 2 倍です。

IGMPv3 を実行するデバイス

IGMPv3 では、ソース フィルタリングのサポートが追加されています。これにより、マルチキャスト レシーバ ホストは、どのグループからマルチキャスト トラフィックを受信するか、およびこのトラフィックがどのソースからのものと想定されているかをデバイスに知らせることができます。このメンバーシップ情報によって、レシーバがトラフィックを要求したソースからのトラフィックだけを転送できます。

IGMPv3 では、トラフィックを受信するソースに明示的に信号を送信するアプリケーションがサポートされます。IGMPv3 では、次の 2 つのモードで、レシーバにより、マルチキャスト グループにメンバーシップの信号が送信されます。

- INCLUDE モード：このモードでは、レシーバはグループにメンバーシップをアナウンスし、トラフィックを受信する IP アドレスのリスト（INCLUDE リスト）を提供します。
- EXCLUDE モード：このモードでは、レシーバはグループにメンバーシップをアナウンスし、トラフィックを受信しない IP アドレスのリスト（EXCLUDE リスト）を提供します。つまり、ホストは IP アドレスが EXCLUDE リストに記載されていないソースからのトラ

フィックだけを受信します。インターネット標準マルチキャスト（ISM）サービスモデルの場合など、すべてのソースからトラフィックを受信するには、空のEXCLUDEリストを使用してEXCLUDEモードのメンバーシップを通知します。

IGMPv3はSSMネットワーク環境でホストがチャネル加入者に信号を送信する業界指定の標準プロトコルです。IGMPv3に依存するSSMでは、ラストホップデバイスおよびホストで実行されているオペレーティングシステムのネットワークスタック部分でIGMPv3が使用でき、そのホスト上で動作しているアプリケーションで使用されている必要があります。

IGMPv3では、ホストは224.0.0.22にメンバーシップレポートを送信します。そのため、すべてのIGMPv3デバイスでこのアドレスをリッスンする必要があります。ただし、ホストは224.0.0.22をリッスンせず、応答しません。ホストはこのアドレスにレポートを送信するだけです。さらに、IGMPv3ではIGMPv3ホストが他のホストによって送信されたレポートをリッスンしないため、メンバーシップレポートの抑制はありません。したがって、一般クエリーが送信されると、ネットワークのすべてのホストが応答します。

IGMP の加入および脱退処理

IGMP の加入処理

ホストがマルチキャストグループに加入するとき、ホストは、加入するマルチキャストグループに1つ以上の送信要求されていないメンバーシップレポートを送信します。IGMP加入処理は、IGMPv1ホストとIGMPv2ホストで同じです。

IGMPv3では、ホストの加入処理は次のように処理されます。

- ホストがグループに加入する場合は、空のEXCLUDEリストを使用して、224.0.0.22にIGMPv3メンバーシップレポートを送信します。
- ホストが特定のチャネルに加入する場合は、特定のソースアドレスを含むINCLUDEリストを使用して、224.0.0.22にIGMPv3メンバーシップレポートを送信します。
- ホストが特定のソースを除くグループに加入する場合は、これらのソースをEXCLUDEリストで除外して、224.0.0.22にIGMPv3メンバーシップレポートを送信します。

（注） LAN上にある一部のIGMPv3ホストでソースが除外され、その他のホストで同じソースが含まれている場合、デバイスはLAN上でそのソースのトラフィックを送信します（つまり、この場合、包含が除外より優先されます）。

IGMP の脱退処理

ホストがグループから脱退するために使用する方法は、動作中のIGMPのバージョンによって異なります。

IGMPv1 の脱退処理

IGMPv1には、ホストがあるグループからのマルチキャストトラフィックを受信しないことをそのサブネットのデバイスに通知するグループ脱退メッセージはありません。ホストでは、マルチキャストグループに対するトラフィックの処理が停止するだけで、そのグループに対するIGMP メンバーシップ レポートを使用したIGMP クエリーへの応答が終了します。その結果、IGMPv1デバイスがサブネットの特定のマルチキャストグループにアクティブなレシーバがなくなったことを認識する唯一の方法は、デバイスがメンバーシップ レポートを受信しなくなったときになります。このプロセスを容易にするために、IGMPv1 デバイスは、サブネットのIGMP グループとカウントダウンタイマーを関連付けます。サブネットのグループがメンバーシップ レポートを受信すると、タイマーがリセットされます。IGMPv1デバイスでは、このタイムアウト間隔は通常クエリー間隔の3倍（3分）です。このタイムアウト間隔は、すべてのホストがマルチキャストグループから脱退した後最大3分間、デバイスがサブネットにマルチキャスト トラフィックを転送し続ける可能性があることを意味します。

IGMPv2 の脱退処理

IGMPv2には、特定のグループのマルチキャストトラフィックの受信を停止することをホストが提示する手段を提供するグループ脱退メッセージが組み込まれています。IGMPv2 ホストがマルチキャスト グループから脱退するとき、そのホストがそのグループのメンバーシップ レポートでクエリーに応答する最後のホストである場合、デバイス全体のマルチキャストグループ（224.0.0.2）にグループ脱退メッセージを送信します。

IGMPv3 の脱退処理

IGMPv3 は、IGMPv3 メンバーシップ レポートにソース、グループ、またはチャネルを含めるか除外することによって、ホストが特定のグループ、ソース、またはチャネルからのトラフィックの受信を停止できる機能を導入することで、脱退処理を拡張しています。

IGMP スヌーピング

レイヤ2はIGMP スヌーピングを使用して、レイヤ2インターフェイスを動的に設定し、マルチキャストトラフィックがIP マルチキャストデバイスと対応付けられたインターフェイスにのみ転送されるようにすることによって、マルチキャストトラフィックのフラッディングを制限できます。名称が示すとおり、IGMPスヌーピングの場合は、LANデバイスでホストとルータ間のIGMP伝送をスヌーピングし、マルチキャストグループとメンバポートを追跡する必要があります。デバイスがホストから特定のマルチキャストグループについてのIGMP レポートを受信した場合、デバイスはホストのポート番号を転送テーブルエントリに追加します。ホストから IGMP Leave Group メッセージを受信した場合は、テーブルエントリからホストポートを削除します。マルチキャスト クライアントから IGMP メンバーシップ レポートを受信しなかった場合にも、スイッチはエントリを定期的に削除します。

（注） IP マルチキャストおよびIGMP の詳細については、RFC 1112 およびRFC 2236 を参照してください。

アクティブデバイスに設定されたマルチキャストルータは、すべての VLAN に対して定期的に一般クエリを送信します。このマルチキャスト トラフィックに関心のあるホストはすべて Join 要求を送信し、転送テーブルのエントリに追加されます。デバイスは、IGMP Join 要求の送信元となる各グループの IGMP スヌーピング IP マルチキャスト転送テーブルで、VLAN ごとに 1 つずつエントリを作成します。

デバイスは、MAC アドレスに基づくグループではなく、IP マルチキャストグループに基づくブリッジングをサポートしています。マルチキャスト MAC アドレスに基づくグループの場合、設定されている IP アドレスを設定済みの MAC アドレス（エイリアス）または予約済みのマルチキャスト MAC アドレス（224.0.0.xxx の範囲内）に変換すると、コマンドがエラーになります。デバイスでは IP マルチキャストグループを使用するので、アドレスエイリアスの問題は発生しません。

IGMP スヌーピングによって、IP マルチキャスト グループは動的に学習されます。ただし、**ip igmp snooping vlan** *vlan-id* **static** *ip_address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを使用すると、マルチキャストグループを静的に設定できます。グループ メンバーシップをマルチキャスト グループ アドレスに静的に指定すると、その設定値は IGMP スヌーピングによる自動操作より優先されます。マルチキャスト グループ メンバーシップのリストは、ユーザが定義した設定値および IGMP スヌーピングによって学習された設定値の両方で構成できます。

マルチキャストトラフィックはルーティングする必要がないのでマルチキャストインターフェイスを使用せずに、サブネットの IGMP スヌーピングをサポートするよう IGMP スヌーピング クエリーを設定できます。

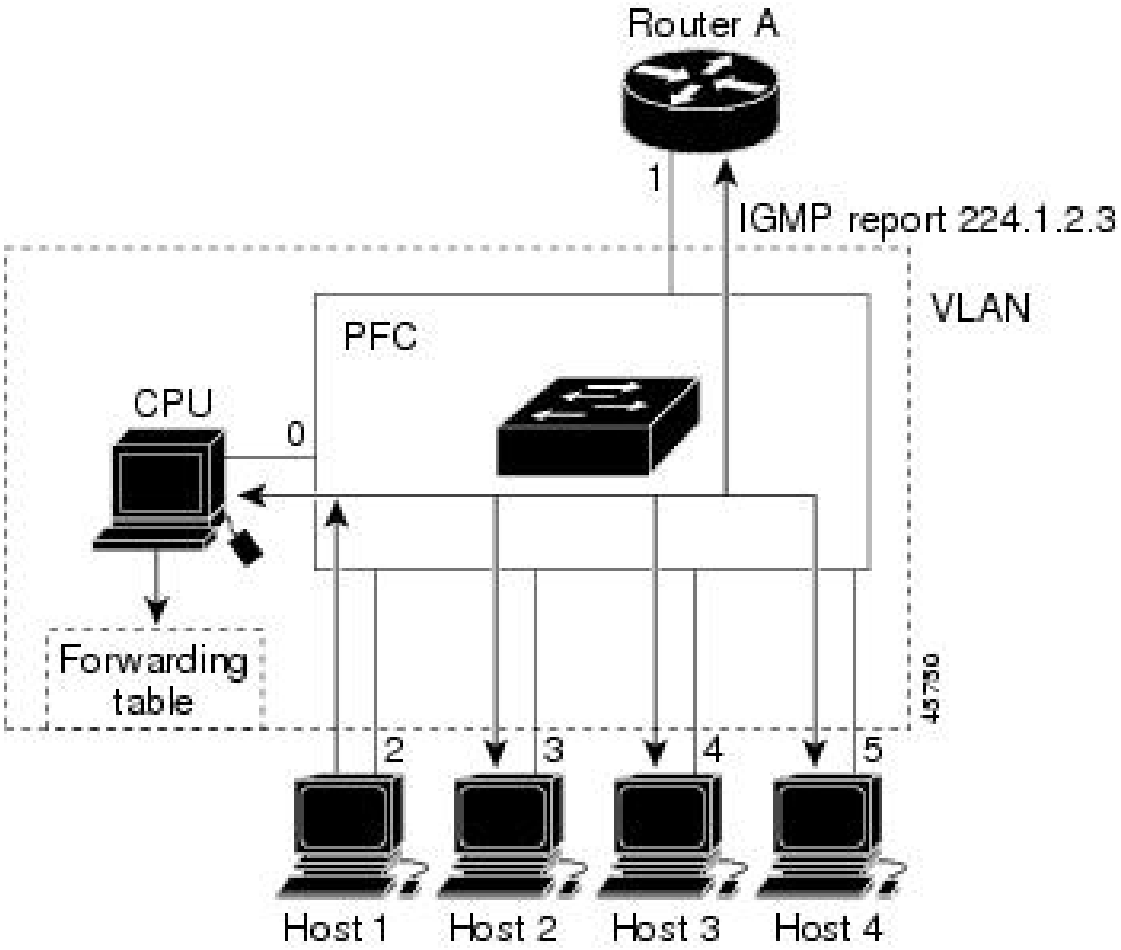
ポート スパニングツリー、ポート グループ、または VLAN ID が変更された場合、VLAN 上のこのポートから IGMP スヌーピングで学習されたマルチキャスト グループは削除されます。

ここでは、IGMP スヌーピングの特性について説明します。

マルチキャスト グループへの加入

図 *8 :* 最初の *IGMP Join* メッセージ

デバイスに接続したホストが IP マルチキャストグループに加入し、なおかつそのホストが IGMP バージョン 2 クライアントの場合、ホストは加入する IP マルチキャストグループを指定した非送信請求 IGMP Join メッセージを送信します。別の方法として、ルータから一般クエリを受信したデバイスは、そのクエリを VLAN 内のすべてのポートに転送します。IGMP バージョン 1 またはバージョン 2 のホストがマルチキャストグループに加入する場合、ホストはデバイスに Join メッセージを送信することによって応答します。デバイスの CPU は、そのグループのマルチキャスト転送テーブルエントリがまだ存在していないのであれば、エントリを作成します。CPU はさらに、Join メッセージを受信したインターフェイスを転送テーブル エントリに追加します。そのインターフェイスと対応付けられたホストが、そのマルチキャスト グループ用のマルチキャスト トラフィックを受信します。



ルータ A がデバイスに一般クエリを送信し、そこでそのクエリは同じ VLAN のすべてのメンバであるポート 2 ～ 5 に転送されます。ホスト 1 はマルチキャスト グループ 224.1.2.3 に加入するために、グループに IGMP メンバーシップ レポート（IGMP Join メッセージ）をマルチキャストします。デバイスの CPU は IGMP レポートの情報を使用して、転送テーブルのエントリを設定します。転送テーブルにはホスト 1 およびルータに接続しているポート番号が含まれます。

表 *6 : IGMP* スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1、2

デバイスのハードウェアは、IGMP 情報パケットをマルチキャストグループの他のパケットと区別できます。テーブルの情報は、224.1.2.3 マルチキャスト IP アドレス宛ての、IGMP パケットではないフレームを、ルータおよびグループに加入したホストに対して送信するように、スイッチング エンジンに指示します。

図 *9 : 2* 番目のホストのマルチキャスト グループへの加入

別のホスト（たとえば、ホスト 4）が、同じグループ用に非送信請求 IGMP Join メッセージを送信する場合、CPUがそのメッセージを受け取り、ホスト4のポート番号を転送テーブルに追加します。転送テーブルは CPU 宛てだけに IGMP メッセージを送るので、メッセージはデバイスの他のポートにフラッディングされません。認識されているマルチキャスト トラフィックは、CPU 宛てではなくグループ宛てに転送されます。

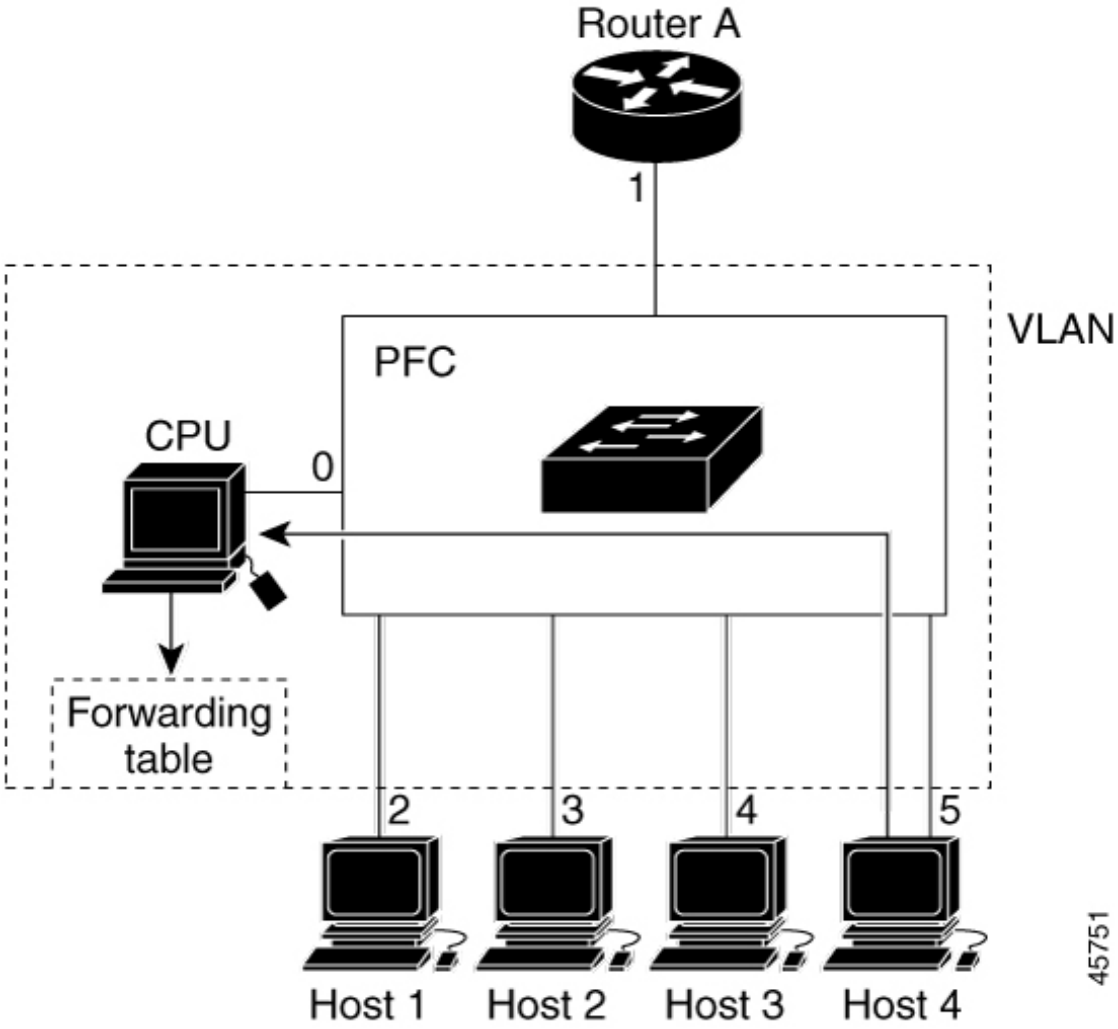


表 *7 :* 更新された *IGMP* スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1, 2, 5

マルチキャスト グループからの脱退

ルータはマルチキャスト一般クエリを定期的に送信し、デバイスはそれらのクエリを VLAN のすべてのポートを通じて転送します。関心のあるホストがクエリーに応答します。VLAN内

の少なくとも 1 つのホストがマルチキャスト トラフィックを受信するようなら、ルータは、その VLAN へのマルチキャスト トラフィックの転送を続行します。デバイスは、その IGMP スヌーピングによって維持された IP マルチキャストグループの転送テーブルで指定されたホストに対してだけ、マルチキャスト グループ トラフィックを転送します。

ホストがマルチキャスト グループから脱退する場合、何も通知せずに脱退することも、Leave メッセージを送信することもできます。ホストから Leave メッセージを受信したデバイスは、グループ固有のクエリを送信して、そのインターフェイスに接続された他のデバイスが所定のマルチキャストグループのトラフィックに関与しているかどうかを学習します。デバイスはさらに、転送テーブルでその MAC グループの情報を更新し、そのグループのマルチキャスト トラフィックの受信に関心のあるホストだけが、転送テーブルに指定されるようにします。ルータが VLAN からレポートを受信しなかった場合、その VLAN 用のグループは IGMP キャッシュから削除されます。

即時脱退

デバイスは IGMP スヌーピングの即時脱退を使用して、先にデバイスからインターフェイスにグループ固有のクエリを送信しなくても、Leave メッセージを送信するインターフェイスを転送テーブルから削除できるようにします。VLAN インターフェイスは、最初の Leave メッセージで指定されたマルチキャスト グループのマルチキャスト ツリーからプルーニングされます。即時脱退によって、複数のマルチキャスト グループが同時に使用されている場合でも、スイッチド ネットワークのすべてのホストに最適な帯域幅管理が保証されます。

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。IGMP バージョン 2 は、デバイスのデフォルトバージョンです。

（注） 即時脱退機能を使用するのは、各ポートに接続されているホストが 1 つだけの VLAN に限定してください。ポートに複数のホストが接続されている VLAN 上で即時脱退をイネーブルにすると、一部のホストが誤ってドロップされる可能性があります。

IGMP 脱退タイマーの設定

まだ指定のマルチキャストグループに関心があるかどうかを確認するために、グループ固有のクエリを送信した後のデバイスの待機時間を設定できます。IGMP 脱退応答時間は、100 ～ 32767 ミリ秒の間で設定できます。

IGMP レポート抑制

IGMP レポート抑制は、マルチキャストクエリに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリに IGMPv3 レポートが含まれている場合はサポートされません。

デバイスは IGMP レポート抑制を使用して、マルチキャストルータクエリごとに 1 つの IGMP レポートのみをマルチキャストデバイスに転送します。IGMP レポート抑制がイネーブル（デフォルト）である場合、デバイスは最初の IGMP レポートをグループのすべてのホストからすべてのマルチキャストルータに送信します。デバイスは、グループの残りの IGMP レポートを

マルチキャストルータに送信しません。この機能により、マルチキャストデバイスにレポートが重複して送信されることを防ぎます。

マルチキャストルータクエリに IGMPv1 および IGMPv2 レポートに対する要求のみが含まれている場合、デバイスは最初の IGMPv1 レポートまたは IGMPv2 レポートのみを、グループのすべてのホストからすべてのマルチキャストルータに転送します。

マルチキャストルータクエリに IGMPv3 レポートに対する要求も含まれる場合、デバイスはグループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャストデバイスに転送します。

IGMP レポート抑制をディセーブルにすると、すべての IGMP レポートはマルチキャスト ルータに転送されます。

IGMP スヌーピングとデバイススタック

IGMP スヌーピング機能はデバイススタック間で機能します。つまり、1 つのデバイスからの IGMP 制御情報は、スタックにあるすべてのデバイスに配信されます。スタック メンバが、どの IGMP マルチキャスト データ経由でスタックに入ったかに関係なく、データは、そのグループで登録されたホストに到達します。

スタック内のデバイスで障害が発生した場合、またはデバイスがスタックから削除された場合、そのデバイス上にあるマルチキャストグループのメンバのみが、マルチキャストデータを受信しません。スタック内にあるその他のデバイスでは、マルチキャストグループの他のすべてのメンバが、マルチキャスト データ ストリームを継続して受信します。ただし、アクティブなデバイスが削除された場合、レイヤ 2 およびレイヤ 3（IP マルチキャストルーティング）の両方に共通のマルチキャストグループでは、コンバージェンスに時間がかかる場合があります。

IGMP フィルタリングおよびスロットリング

都市部や Multiple-Dwelling Unit（MDU）などの環境では、スイッチ ポート上のユーザが属する一連のマルチキャスト グループを制御する必要があります。この機能を使用することにより、IP/TV などのマルチキャスト サービスの配信を、特定タイプの契約またはサービス計画に基づいて制御できます。また、マルチキャスト グループの数を、スイッチ ポート上でユーザが所属できる数に制限することもできます。

IGMP フィルタリング機能を使用すると、IP マルチキャスト プロファイルを設定し、それらを各スイッチ ポートに関連付けて、ポート単位でマルチキャスト加入をフィルタリングできます。IGMP プロファイルにはマルチキャスト グループを 1 つまたは複数格納して、グループへのアクセスを許可するか拒否するかを指定できます。マルチキャストグループへのアクセスを拒否する IGMP プロファイルがスイッチ ポートに適用されると、IP マルチキャスト トラフィックのストリームを要求する IGMP Join レポートが廃棄され、ポートはそのグループからの IP マルチキャスト トラフィックを受信できなくなります。マルチキャスト グループへのアクセスがフィルタリング アクションで許可されている場合は、ポートからの IGMP レポートが転送されて、通常の処理が行われます。レイヤ 2 インターフェイスが加入できる IGMP グループの最大数も設定できます。

IGMP フィルタリングで制御されるのは、グループ固有のクエリーおよびメンバーシップ レポート（Join および Leave レポートを含む）だけです。一般 IGMP クエリーは制御されません。IGMP フィルタリングは、IP マルチキャスト トラフィックの転送を指示する機能とは無関係です。フィルタリング機能は、マルチキャスト トラフィックの転送に CGMP が使用されているか、または MVR が使用されているかに関係なく、同じように動作します。

IGMP フィルタリングが適用されるのは、IP マルチキャスト グループ アドレスを動的に学習する場合だけです。静的な設定には適用されません。

IGMP スロットリング機能を使用すると、レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定できます。IGMP グループの最大数が設定され、IGMP スヌーピング転送テーブルに最大数のエントリが登録されていて、インターフェイスで IGMP Join レポートを受信する場合、インターフェイスを設定することにより、IGMP レポートを廃棄するか、あるいは受信した IGMP レポートでランダムに選択されたマルチキャスト エントリを上書きします。

（注） IGMP フィルタリングが実行されているデバイスは、IGMPv3 Join および Leave メッセージをサポートしていません。

IGMP のデフォルト設定

次の表に、デバイスの IGMP デフォルト設定を示します。

表 *8 : IGMP* のデフォルト設定

機能	デフォルト設定
マルチキャストグループのメンバとしてのマルチレイヤデバイス	グループ メンバーシップは未定義
マルチキャスト グループへのアクセス	インターフェイスのすべてのグループを
IGMP のバージョン	すべてのインターフェイスでバージョン
IGMP ホストクエリー メッセージ インターバル	すべてのインターフェイスで 60 秒
IGMP クエリー タイムアウト	すべてのインターフェイスで 60 秒
IGMP 最大クエリー応答時間	すべてのインターフェイスで 10 秒
静的に接続されたメンバーとしてのマルチレイヤ デバイス	ディセーブル

IGMP スヌーピングのデフォルト設定

次の表に、デバイスの IGMP スヌーピングのデフォルト設定を示します。

表 *9 : IGMP* スヌーピングのデフォルト設定

機能	デフォルト設定
IGMP スヌーピング	グローバルおよび VLAN 単位でイネーブ
マルチキャスト ルータ	未設定
IGMP スヌーピング即時脱退	ディセーブル
スタティック グループ	未設定
TCN[1]フラッド クエリ カウント	2
TCN クエリー送信要求	ディセーブル
IGMP スヌーピング クエリア	ディセーブル
IGMP レポート抑制	有効

[1] (1) TCN = トポロジ変更通知

IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定

次の表に、デバイスの IGMP フィルタリングおよびスロットリングのデフォルト設定を示します。

表 *10 : IGMP* フィルタリングのデフォルト設定

機能	デフォルト設定
IGMP フィルタ	適用なし
IGMP グループの最大数	最大数の設定なし （注） 転送テーブルに登録されているグループ していると、デフォルトの IGMP スロッ ションは IGMP レポートを拒否します。
IGMP プロファイル	未定義
IGMP プロファイル アクション	範囲で示されたアドレスを拒否

IGMP の設定方法

グループのメンバとしてデバイスを設定

デバイスをマルチキャストグループのメンバとして設定し、マルチキャストがネットワークに到達可能かどうかを検出できます。管理対象のすべてのマルチキャスト対応ルータおよびマルチレイヤデバイスがマルチキャストグループのメンバーである場合、グループに ping を送信すると、これらのすべてのデバイスが応答します。デバイスは、所属グループにアドレス指定された ICMP エコー要求パケットに応答します。もう 1 つの例は、ソフトウェア付属のマルチキャスト トレースルート ツールです。

⚠

注意 この手順を実行すると、グループ アドレス用のデータ トラフィックがすべて CPU に送られるため、CPU のパフォーマンスが低下する場合があります。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp join-group** *group-address*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **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： `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	**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	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ 3 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。 • 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。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip igmp join-group** *group-address* 例： `Device(config-if)# ip igmp join-group 225.2.2.2`	デバイスをマルチキャストグループに加入するように設定します。デフォルトで、グループのメンバーシップは定義されていません。 *group-address* には、マルチキャスト IP アドレスをドット付き 10 進表記で指定します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface GigabitEthernet 1/0/1`	入力を確認します。
ステップ 7	**copy running-config startup-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。

IGMP バージョンの変更

スイッチでは、IGMP クエリー タイムアウトや最大クエリー応答時間などの機能を使用できる IGMP バージョン 2 がデフォルトで使用されます。

サブネット上のすべてのシステムで、同じバージョンをサポートする必要があります。スイッチは自動的にバージョン 1 のシステムを検出せず、バージョン 1 へのスイッチングも行いません。バージョン 2 のルータまたはスイッチは、常に IGMPv1 ホストと正しく連動しているため、バージョン 1 とバージョン 2 のホストはサブネット上で混在できます。

使用しているホストでバージョン 2 がサポートされていない場合は、スイッチをバージョン 1 に設定してください。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp version** {**1** | **2** | **3** }
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **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： `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	**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	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定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。
ステップ 4	**ip igmp version** {**1**	**2**	**3** } 例： `Device(config-if)# ip igmp version 2`	スイッチで使用する IGMP バージョンを指定します。 （注） バージョン 1 に変更すると、 **ip igmp query-interval** および **ip igmp query-max-response-time** インターフェイス コンフィギュレーション コマンドを設定できません。

	コマンドまたはアクション	目的
		デフォルトの設定に戻す場合は、 **no ip igmp version** 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。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-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。

IGMP ホストクエリー メッセージ インターバルの変更

デバイスは、IGMP ホストクエリメッセージを定期的に送信し、接続されたネットワーク上にあるマルチキャストグループを検出します。これらのメッセージは、TTL が 1 の全ホスト マルチキャスト グループ（224.0.0.1）に送信されます。デバイスはホストクエリメッセージを送信し、ネットワーク上に存在するメンバーシップに関する情報をリフレッシュします。クエリーをいくつか実行したあとで、マルチキャスト グループのメンバーであるローカルホストが存在しないことをソフトウェアが検出した場合、そのグループのリモート送信元からローカル ネットワークへのマルチキャスト パケット転送が停止され、プルーニング メッセージが送信元のアップストリーム方向へ送信されます。

デバイスは LAN（サブネット）用の PIM DR を選択します。DR は、LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。SM の場合、DR は PIM 登録メッセージおよび PIM Join メッセージも RP ルータに向けて送信します。IGMPv2 では、DR は IP アドレスが最大である、ルータまたはマルチレイヤデバイスです。IGMPv1 では、DR は LAN 上で動作するマルチキャスト ルーティング プロトコルに従って選択されます。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*

4. **ip igmp query-interval** *seconds*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **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： `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	**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	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ 3 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 コンフィギュレーション コマンドを入力して設定された物理ポートです。 • 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。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip igmp query-interval** *seconds* 例： `Device(config-if)# ip igmp query-interval 75`	DR が IGMP ホストクエリー メッセージを送信する頻度を設定します。 デフォルトでは、DR は IGMP ホストクエリー メッセージを 60 秒ごとに送信し、ホストおよびネットワークでの IGMP オーバーヘッドを抑制します。 指定できる範囲は 1 ～ 65535 です。

	コマンドまたはアクション	目的
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	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	Displays
ステップ 7	**copy running-config startup-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。

IGMPv2 の最大クエリー応答時間の変更

IGMPv2 を使用している場合は、IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更できます。デバイスは最大クエリ応答時間を使用し、LAN 上に直接接続されたグループメンバが存在しないことを短時間で検出します。値を小さくすると、デバイスによるグループのプルーニング速度が向上します。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp query-max-response-time** *seconds*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **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： `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）。

	コマンドまたはアクション	目的
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	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ 3 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 コンフィギュレーション コマンドを入力して設定された物理ポートです。 • 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。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip igmp query-max-response-time** *seconds* 例： `Device(config-if)# ip igmp query-max-response-time 15`	IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更します。 デフォルトは 10 秒です。指定できる範囲は 1 ～ 25 です。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-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。

静的に接続されたメンバとしてデバイスを設定

ネットワーク セグメント上にグループ メンバが存在しなかったり、ホストで IGMP を使用してグループ メンバーシップを報告できないことがあります。しかし、そのネットワーク セグメントに対して、マルチキャスト トラフィックの送信が必要な場合もあります。マルチキャスト トラフィックをネットワーク セグメントに送り込むには、次のコマンドを使用します。

- **ip igmp join-group**：デバイスはマルチキャストパケットの転送だけでなく、マルチキャストパケットを受け入れます。マルチキャストパケットを受信する場合は、高速スイッチングを実行できません。
- **ip igmp static-group**： デバイスは、パケットを転送するだけで、パケット自体は受け入れません。この方法を使用すると、高速スイッチングが可能です。発信インターフェイスが IGMP キャッシュに格納されますが、マルチキャスト ルート エントリに「L」（ローカル）フラグが付かないことからも明らかなように、デバイス自体はメンバではありません。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp static-group** *group-address*
5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **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： `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	**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	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ 3 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。

	コマンドまたはアクション	目的
		• 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。 • 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。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip igmp static-group** *group-address* 例： `Device(config-if)# ip igmp static-group 239.100.100.101`	デバイスを静的に接続されたグループのメンバとして設定します。デフォルトでは、この機能はディセーブルになっています。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface GigabitEthernet 1/0/1`	入力を確認します。
ステップ 7	**copy running-config startup-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。

IGMP プロファイルの設定

IGMP プロファイルを作成するには、次の手順を実行します。

このタスクはオプションです。

手順の概要

1. **enable**

2. **configure terminal**
3. **ip igmp profile** *profile number*
4. **permit** | **deny**
5. **range** *ip multicast address*
6. **end**
7. **show ip igmp profile** *profile number*
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip igmp profile** *profile number* 例： `Device(config)# ip igmp profile 3`	設定するプロファイルに番号を割り当て、IGMP プロファイル コンフィギュレーション モードを開始します。指定できるプロファイル番号の範囲は 1 ～ 4294967295 です。IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。 • **deny**：一致するアドレスを拒否します。デフォルトで設定されています。 • **exit**：IGMP プロファイル コンフィギュレーション モードを終了します。 • **no**：コマンドを否定するか、または設定をデフォルトに戻します。 • **permit**：一致するアドレスを許可するように指定します。 • **range**：プロファイルの IP アドレスの範囲を指定します。単一の IP アドレス、または開始アドレスと終了アドレスで指定された IP アドレス範囲を入力できます。 デバイスのデフォルトでは、 IGMP プロファイルが設定されていません。

	コマンドまたはアクション	目的
		（注） プロファイルを削除するには、**no ip igmp profile** *profile number* 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。
ステップ 4	**permit** | **deny** 例： `Device(config-igmp-profile)# permit`	（任意）IP マルチキャスト アドレスへのアクセスを許可または拒否するアクションを設定します。アクションを設定しないと、プロファイルのデフォルト設定はアクセス拒否になります。
ステップ 5	**range** *ip multicast address* 例： `Device(config-igmp-profile)# range 229.9.9.0`	アクセスを制御する IP マルチキャスト アドレスまたは IP マルチキャスト アドレスの範囲を入力します。範囲を入力する場合は、IP マルチキャスト アドレスの下限値、スペースを 1 つ、IP マルチキャスト アドレスの上限値を入力します。 **range** コマンドを複数回入力し、複数のアドレスまたはアドレス範囲を入力できます。 （注） IP マルチキャスト アドレスまたは IP マルチキャスト アドレス範囲を削除するには、**no range** *ip multicast address* IGMP プロファイル コンフィギュレーション コマンドを使用します。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip igmp profile** *profile number* 例： `Device# show ip igmp profile 3`	プロファイルの設定を確認します。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例：	（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
	`Device# copy running-config startup-config`	

IGMP プロファイルの適用

IGMP プロファイルで定義されているとおりにアクセスを制御するには、プロファイルを該当するインターフェイスに適用する必要があります。IGMP プロファイルを適用できるのは、レイヤ 2 アクセス ポートだけです。ルーテッド ポートや SVI には適用できません。EtherChannel ポート グループに所属するポートに、プロファイルを適用することはできません。1 つのプロファイルを複数のインターフェイスに適用できますが、1 つのインターフェイスに適用できるプロファイルは 1 つだけです。

スイッチ ポートに IGMP プロファイルを適用するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp filter** *profile number*
5. **end**
6. **show running-config**
7. **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： `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	**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	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet 1/0/1`	物理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。インターフェイスは、EtherChannel ポート グループに所属していないレイヤ 2 ポートでなければなりません。

	コマンドまたはアクション	目的
ステップ 4	**ip igmp filter** *profile number* 例： `Device(config-if)# ip igmp filter 321`	インターフェイスに指定された IGMP プロファイルを適用します。指定できる範囲は 1 ～ 4294967295 です。 （注） インターフェイスからプロファイルを削除するには、 **no ip igmp filter***profile number* 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。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-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。

IGMP グループの最大数の設定

レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定するには、次の手順を実行します。

始める前に

この制限が適用されるのはレイヤ 2 ポートだけです。ルーテッド ポートや SVI には IGMP グループの最大数を設定できません。このコマンドは、論理 EtherChannel インターフェイスでも使用できますが、EtherChannel ポート グループに属するポートでは使用できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp max-groups** *number*
5. **end**
6. **show running-config interface** *interface-id*
7. **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： `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	**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	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	設定するインターフェイスを指定して、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。インターフェイスは、EtherChannel ポート グループに所属しないレイヤ 2 ポート、または EtherChannel インターフェイスのいずれかにできます。
ステップ 4	**ip igmp max-groups** *number* 例： `Device(config-if)# ip igmp max-groups 20`	インターフェイスが加入できる IGMP グループの最大数を設定します。指定できる範囲は 0 ～ 4294967294 です。デフォルトでは最大数は設定されません。
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	**show running-config interface** *interface-id* 例： `Device# show running-config interface gigabitethernet1/0/1`	入力を確認します。
ステップ 7	**copy running-config startup-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。

IGMP スロットリング アクションの設定

レイヤ2インターフェイスが加入できるIGMPグループの最大数を設定した後、受信したIGMPレポートの新しいグループで、既存のグループを上書きするようにインターフェイスを設定できます。

転送テーブルに最大数のエントリが登録されているときにスロットリングアクションを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp max-groups action** {**deny** | **replace**}
5. **end**
6. **show running-config interface** *interface-id*
7. **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： `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	**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	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定する物理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。インターフェイスは、EtherChannel ポート グループに所属しないレイヤ 2 ポート、または EtherChannel インターフェイスのいずれかにできます。トランク ポートをインターフェイスにすることはできません。
ステップ 4	**ip igmp max-groups action** {**deny**	**replace**} 例： `Device(config-if)# ip igmp max-groups action replace`	インターフェイスが IGMP レポートを受信したときに、転送テーブルに最大数のエントリが登録されている場合は、次のいずれかのアクションをインターフェイスに指定します。 • **deny**：レポートを破棄します。このスロットリング アクションを設定すると、すでに転送テーブルに登録されていたエントリは、削除されることはありませんが期限切れになります。エン

	コマンドまたはアクション	目的
		トリが期限切れになり、最大数のエントリが転送テーブルに登録されていると、デバイスは、インターフェイスで受信した次の IGMP レポートを廃棄します。 • **replace**：既存のグループを、IGMP レポートを受信した新しいグループで上書きします。このスロットリング アクションを設定すると、すでに転送テーブルに登録されていたエントリは削除されます。転送テーブルのエントリが最大数まで達したら、デバイスはランダムに選択したエントリを受信した IGMP レポートで上書きします。 デバイスが転送テーブルのエントリを削除しないようにするには、インターフェイスにより転送テーブルにエントリが追加される前に、IGMP スロットリングアクションを設定します。 （注） レポートの廃棄というデフォルトのアクションに戻すには、**no ip igmp max-groups action** 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。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id* 例： `Device# show running-config interface gigabitethernet1/0/1`	入力を確認します。
ステップ 7	**copy running-config startup-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。

直接接続の IGMP ホストがない場合にマルチキャスト トラフィックが転送されるようにデバイスを設定する方法

直接接続されたIGMPホストがない場合に、マルチキャストトラフィックを転送するようにデバイスを設定するには、次のオプション作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. 次のいずれかを実行します。
   - **ip igmp join-group** *group-address*
   - **ip igmp static-group** {***** | *group-address* [**source** *source-address*]}
5. **end**
6. **show ip igmp interface** [*interface-type interface-number*]

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	**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	**interface** *type number* 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 モードを開始します。 • *type* 引数および *number* 引数に、ホストに接続されているインターフェイスを指定します。
ステップ 4	次のいずれかを実行します。 • **ip igmp join-group** *group-address* • **ip igmp static-group** {***** | *group-address* [**source** *source-address*]} 例： `Device(config-if)# ip igmp join-group 225.2.2.2` 例：	最初の例では、指定したグループに加入するデバイスのインターフェイスを設定する例を示します。 この方法では、デバイスは、マルチキャストパケットの転送に加えて、マルチキャストパケットを受信します。マルチキャスト パケットを受信する場合は、高速スイッチングを実行できません。 2 番目の例では、インターフェイスでスタティック グループ メンバーシップ エントリを設定する例を

	コマンドまたはアクション	目的
	`Device(config-if)# ip igmp static-group 225.2.2.2`	示します。この方法の場合、デバイスはパケットそのものを受信せず、転送だけを実行します。したがって、この方法では、高速スイッチングを実行できます。発信インターフェイスが IGMP キャッシュに格納されますが、マルチキャスト ルート エントリに「L」（ローカル）フラグが付かないことからも明らかなように、デバイス自体はメンバではありません。
ステップ 5	**end** 例： `Device#(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp interface** [*interface-type interface-number*] 例： `Device# show ip igmp interface`	（任意）インターフェイスに関するマルチキャスト関連情報を表示します。

IGMP 拡張アクセス リストを使用して SSM ネットワークへのアクセスを制御する方法

ソース アドレス、グループ アドレス、またはその両方に基づいて SSM トラフィックをフィルタする IGMP 拡張アクセス リストを使用して SSM ネットワークへのアクセスを制御するには、次のオプション作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **ip pim ssm** {**default** | **range** *access-list*}
5. **ip access-list extended** *access-list* -name
6. **deny igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]
7. **permit igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]
8. **exit**
9. interface type number
10. **ip igmp access-group** *access-list*
11. **ip pim sparse-mode**
12. SSM チャネル メンバーシップのアクセス コントロールを必要とするすべてのインターフェイスでステップ 1 ～ 11 を繰り返します。

13. **ip igmp version 3**
14. ホスト方向のインターフェイスすべてでステップ 13 を繰り返します。
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip multicast-routing** [**distributed**] 例： `Device(config)# ip multicast-routing distributed`	IP マルチキャスト ルーティングを有効にします。 • **distributed** キーワードは、IPv4 マルチキャストの場合に必要です。
ステップ 4	**ip pim ssm** {**default** | **range** *access-list*} 例： `Device(config)# ip pim ssm default`	SSM サービスを設定します。 • **default** キーワードは SSM 範囲のアクセスリストを 232/8 と定義します。 • **range** キーワードは標準の IP アクセスリスト番号または SSM 範囲を定義する名前を指定します。
ステップ 5	**ip access-list extended** *access-list* -name 例： `Device(config)# ip access-list extended mygroup`	名前付き拡張 IP アクセス リストを指定します。
ステップ 6	**deny igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# deny igmp host 10.1.2.3 any`	（任意）IGMP レポートから指定したソース アドレスまたはグループ アドレスをフィルタリングすることで、サブネットのホストをメンバーシップから (S, G) チャネルに制限します。 • サブネット メンバーシップから他の (S, G) チャネルにホストを制限するには、この手順を繰り返します。（特に許可されない送信元またはグループは拒否されるため、これらの送信元は後続の **permit** ステートメントより限定的になります）。

	コマンドまたはアクション	目的
		• アクセスリストは、暗黙の **deny** ステートメントで終了することに注意してください。 • 次に、ソース 10.1.2.3 に対してすべてのグループをフィルタリングして、効果的にソースを拒否する deny ステートメントを作成する例を示します。
ステップ 7	**permit igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# permit igmp any any`	IGMP レポートのソース アドレスまたはグループ アドレスが IP アクセス リストを渡すことができます。 • アクセスリストには少なくとも 1 つの **permit** ステートメントが必要です。 • 他のソースが IP アクセス リストを渡せるようにする場合は、この手順を繰り返します。 • この例では、前の **deny** ステートメントによって拒否されていない送信元およびグループに対するメンバーシップを許可する方法を示します。
ステップ 8	**exit** 例： `Device(config-ext-nacl)# exit`	現在のコンフィギュレーション セッションを終了し、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 type number 例： `Device(config)# interface ethernet 0`	IGMPv3 をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 10	**ip igmp access-group** *access-list* 例： `Device(config-if)# ip igmp access-group mygroup`	IGMP レポートに指定されたアクセス リストが適用されます。
ステップ 11	**ip pim sparse-mode** 例： `Device(config-if)# ip pim sparse-mode`	インターフェイスで PIM-SM をイネーブルにします。 （注） スパース モードを使用する必要があります。

	コマンドまたはアクション	目的
ステップ 12	SSM チャネル メンバーシップのアクセス コントロールを必要とするすべてのインターフェイスでステップ 1 ～ 11 を繰り返します。	--
ステップ 13	**ip igmp version 3** 例： `Device(config-if)# ip igmp version 3`	このインターフェイス上で IGMPv3 をイネーブルにします。デフォルトの IGMP バージョンは IGMP バージョン 2 です。SSM にはバージョン 3 が必要です。
ステップ 14	ホスト方向のインターフェイスすべてでステップ 13 を繰り返します。	--
ステップ 15	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

IGMP スヌーピングを設定する方法

IGMP スヌーピングのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping**
4. **bridge-domain** *bridge-id*
5. **ip igmp snooping**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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 3	**ip igmp snooping** 例： `Device(config)# ip igmp snooping`	ディセーブルにした後で、IGMP スヌーピングをグローバルにイネーブルにします。
ステップ 4	**bridge-domain** *bridge-id* 例： `Device(config)# bridge-domain 100`	（任意）ブリッジ ドメイン コンフィギュレーション モードを開始します。
ステップ 5	**ip igmp snooping** 例： `Device(config-bdomain)# ip igmp snooping`	（任意）設定されたブリッジドメインインターフェイス上で IGMP スヌーピングをイネーブルにします。 • 指定されたブリッジドメインで IGMP スヌーピングが明示的にディセーブルにされた場合にだけ必要です。
ステップ 6	**end** 例： `Device(config-bdomain)# end`	特権 EXEC モードに戻ります。

VLAN インターフェイスでの IGMP スヌーピングのイネーブル化またはディセーブル化

VLAN インターフェイス上で IGMP スヌーピングを有効にするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping vlan** *vlan-id*
4. **end**
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： `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）。

	コマンドまたはアクション	目的
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	**ip igmp snooping vlan** *vlan-id* 例： `Device(config)# ip igmp snooping vlan 7`	VLAN インターフェイス上で IGMP 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。 VLAN スヌーピングをイネーブルにするには、IGMP スヌーピングをグローバルにイネーブルに設定しておく必要があります。 （注） 特定の VLAN インターフェイス上で IGMP スヌーピングをディセーブルにするには、**no ip igmp snooping vlan** *vlan-id* グローバル コンフィギュレーション コマンドを、指定した VLAN 番号に対して使用します。
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	**copy running-config startup-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。

スヌーピング方法の設定

マルチキャスト対応のルータ ポートは、レイヤ 2 マルチキャスト エントリごとに転送テーブルに追加されます。デバイスは、次のいずれかの方法でポートを学習します。

- IGMP クエリおよび Protocol Independent Multicast（PIM）パケットのスヌーピング
- **ip igmp snooping mrouter** グローバル コンフィギュレーション コマンドによるマルチキャストルータポートへの静的な接続

VLAN インターフェイスがマルチキャストルータにアクセスする方法を変更するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping vlan** *vlan-id* **mrouter interface** {**GigabitEthernet** | **Port-Channel** | **TenGigabitEthernet**}
4. **end**
5. **show ip igmp snooping**
6. **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： `Device> enable`	特権 EXEC モードを有効にします。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	**ip igmp snooping vlan** *vlan-id* **mrouter interface** {**GigabitEthernet** | **Port-Channel** | **TenGigabitEthernet**} 例： `Device(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet1/0/3`	VLAN 上で IGMP 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。
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	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	設定を確認します。
ステップ 6	**copy running-config startup-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。

マルチキャスト ルータ ポートの設定

デバイスにマルチキャストルータポートを追加する（マルチキャストルータへのスタティック接続を有効にする）には、次の手順を実行します。

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

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id*
4. **end**
5. **show ip igmp snooping mrouter** [**vlan** *vlan-id*]
6. **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： `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	**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	**ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id* 例： `Device(config)# ip igmp snooping vlan 5 mrouter interface GigabitEthernet 1/0/1`	マルチキャストルータのVLAN IDおよびマルチキャスト ルータに対するインターフェイスを指定します。 • 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポート チャネル範囲は 1 ～ 128 です。 （注） VLANからマルチキャストルータポートを削除するには、**no ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping mrouter** [**vlan** *vlan-id*] 例： `Device# show ip igmp snooping mrouter vlan 5`	VLAN インターフェイス上で IGMP スヌーピングが有効になっていることを確認します。
ステップ 6	**copy running-config startup-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。

グループに加入するホストの静的な設定

ホストまたはレイヤ 2 ポートは通常、マルチキャスト グループに動的に加入しますが、インターフェイス上にホストを静的に設定することもできます。

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

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping vlan** *vlan-id* **static** *ip_address* **interface** *interface-id*
4. **end**
5. **show ip igmp snooping groups**
6. **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： `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	**configure terminal** 例：	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
	`Device# configure terminal`	
ステップ 3	**ip igmp snooping vlan** *vlan-id* **static** *ip_address* **interface** *interface-id* 例： `Device(config)# ip igmp snooping vlan 105 static 230.0.0.1 interface gigabitethernet1/0/1`	マルチキャスト グループのメンバとしてレイヤ 2 ポートを静的に設定します。 • *vlan-id* は、マルチキャスト グループの VLAN ID です。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。 • *ip-address* は、グループの IP アドレスです。 • *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（1～128）に設定できます。 （注） マルチキャストグループからレイヤ 2 ポートを削除するには、 **no ip igmp snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping groups** 例： `Device# show ip igmp snooping groups`	メンバ ポートおよび IP アドレスを確認します。
ステップ 6	**copy running-config startup-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。

IGMP 即時脱退のイネーブル化

IGMP 即時脱退をイネーブルに設定すると、デバイスはポート上で IGMP バージョン 2 の Leave メッセージを検出した場合、ただちにそのポートを削除します。即時脱退機能は、VLAN の各ポートにレシーバが 1 つ存在する場合にだけ使用してください。

（注） 即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。IGMP バージョン 2 は、デバイスのデフォルトバージョンです。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping vlan** *vlan-id* **immediate-leave**
4. **end**
5. **show ip igmp snooping vlan** *vlan-id*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip igmp snooping vlan** *vlan-id* **immediate-leave** 例： `Device(config)# ip igmp snooping vlan 21 immediate-leave`	VLAN インターフェイス上で、IGMP 即時脱退をイネーブルにします。 （注） VLAN 上で IGMP 即時脱退をディセーブルにするには、 **no ip igmp snooping vlan** *vlan-id* **immediate-leave** 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。
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	**show ip igmp snooping vlan** *vlan-id* 例：	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。

	コマンドまたはアクション	目的
	`Device# show ip igmp snooping vlan 21`	
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

IGMP 脱退タイマーの設定

脱退時間はグローバルまたはVLAN単位で設定できます。IGMP脱退タイマーの設定をイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping last-member-query-interval** *time*
4. **ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *time*
5. **end**
6. **show ip igmp snooping**
7. **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： `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	**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	**ip igmp snooping last-member-query-interval** *time* 例： `Device(config)# ip igmp snooping`	IGMP 脱退タイマーをグローバルに設定します。指定できる範囲は 100 ～ 32767 ミリ秒です。 デフォルトの脱退時間は 1000 ミリ秒です。

	コマンドまたはアクション	目的
	`last-member-query-interval 1000`	（注） IGMP 脱退タイマーをグローバルにリセットしてデフォルト設定に戻すには、**no ip igmp snooping last-member-query-interval** 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。
ステップ 4	**ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *time* 例： `Device(config)# ip igmp snooping vlan 210 last-member-query-interval 1000`	（任意）VLAN インターフェイス上で IGMP 脱退時間を設定します。有効値は 100 ～ 32767 ミリ秒です。 （注） VLAN 上に脱退時間を設定すると、グローバルに設定された内容は上書きされます。 （注） 特定の VLAN から IGMP 脱退タイマーの設定を削除するには、**no ip igmp snooping vlan** *vlan-id* **last-member-query-interval** 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。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	（任意）設定された IGMP 脱退時間を表示します。
ステップ 7	**copy running-config startup-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。

IGMP 堅牢性変数の設定

このデバイスで IGMP 堅牢性変数を設定するには、次の手順を使用します。

堅牢性変数は、IGMP メッセージの計算時に IGMP スヌーピングで使用される整数です。堅牢性変数により、想定されるパケット損失を考慮した微調整を実施できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping robustness-variable** *count*
4. **ip igmp snooping vlan** *vlan-id* **robustness-variable** *count*
5. **end**
6. **show ip igmp snooping**
7. **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： `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	**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	**ip igmp snooping robustness-variable** *count* 例： `Device(config)# ip igmp snooping robustness-variable 3`	IGMP 堅牢性変数を設定します。範囲は、1 ～ 3 回です。 堅牢性変数の推奨値は 2 です。IGMP スヌーピングの堅牢性変数の値をデフォルトの 2 から指定した値に変更するには、このコマンドを使用します。
ステップ 4	**ip igmp snooping vlan** *vlan-id* **robustness-variable** *count* 例： `Device(config)#ip igmp snooping vlan 100 robustness-variable 3`	（任意）VLAN インターフェイス上で IGMP 堅牢性変数を設定します。範囲は、1 ～ 3 回です。堅牢性変数の推奨値は 2 です。 （注） VLAN で堅牢性変数カウントを設定すると、グローバルに設定された値が上書きされます。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp snooping** 例：	（任意）設定された IGMP 堅牢性変数カウントを表示します。

	コマンドまたはアクション	目的
	`Device# show ip igmp snooping`	
ステップ 7	**copy running-config startup-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。

IGMP 最終メンバー クエリ回数の設定

グループ固有またはグループソース固有の leave メッセージの受信に応答して、IGMP グループ固有またはグループソース固有の（IGMP バージョン 3 で）クエリメッセージをデバイスが送信する回数を設定するには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping last-member-query-count** *count*
4. **ip igmp snooping vlan** *vlan-id* **last-member-query-count** *count*
5. **end**
6. **show ip igmp snooping**
7. **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： `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	**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	**ip igmp snooping last-member-query-count** *count* 例： `Device(config)# ip igmp snooping last-member-query-count 3`	IGMP 最終メンバー クエリ回数を設定します。指定できる範囲は 1 ～ 7 です。デフォルト値は 2 メッセージです。

	コマンドまたはアクション	目的
ステップ 4	**ip igmp snooping vlan** *vlan-id* **last-member-query-count** *count* 例： `Device(config)#ip igmp snooping vlan 100 last-member-query-count 3`	（任意）VLAN インターフェイス上で IGMP 最終メンバー クエリ回数を設定します。指定できる範囲は 1 ～ 7 です。 （注） VLAN で最終メンバー クエリ回数を設定すると、グローバルに設定されたタイマーが上書きされます。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	（任意）設定された IGMP 最終メンバー クエリ回数を表示します。
ステップ 7	**copy running-config startup-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。

TCN 関連コマンドの設定

TCN イベント後のマルチキャスト フラッディング時間の制御

トポロジ変更通知（TCN）イベント後にフラッディングするマルチキャストデータのトラフィックに対し、一般クエリー数を設定できます。TCN フラッド クエリ カウントを 1 に設定した場合は、1 つの一般クエリーを受信した後にフラッディングが停止します。カウントを 7 に設定した場合、一般クエリーを 7 つ受信するまでフラッディングが続きます。グループは、TCN イベント中に受信した一般的クエリーに基づいて学習されます。

クライアント ロケーションが変更され、ブロックされていた後に現在は転送中の受信者が同じポートに存在する場合や、ポートが脱退メッセージを送信せずにダウンした場合などに TCN イベントが発生します。

TCN フラッド クエリー カウントを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**

3. **ip igmp snooping tcn flood query count** *count*
4. **end**
5. **show ip igmp snooping**
6. **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： `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	**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	**ip igmp snooping tcn flood query count** *count* 例： `Device(config)# ip igmp snooping tcn flood query count 3`	マルチキャスト トラフィックがフラッディングする IGMP の一般クエリー数を指定します。 指定できる範囲は1～10です。デフォルトのフラッディング クエリー カウントは 2 です。 （注） デフォルトのフラッディング クエリ カウントに戻すには、**no ip igmp snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	TCN の設定を確認します。
ステップ 6	**copy running-config startup-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。

フラッディング モードからの回復

トポロジの変更が発生した場合、スパニングツリーのルートは特別な IGMP Leave メッセージ（グローバル Leave メッセージ）をグループ マルチキャスト アドレス 0.0.0.0. に送信します。ただし、スパニングツリープロトコルのルートであるかどうかにかかわらず、グローバルな Leave メッセージを送信するようにデバイスを設定できます。ルータはこの特別な Leave メッセージを受信した場合、即座に一般クエリーを送信して、TCN 中のフラッディング モードからできるだけ早く回復するようにします。デバイスがスパニングツリープロトコルのルートであれば、このコンフィギュレーションに関係なく、Leave メッセージが常に送信されます。

Leave メッセージを送信できるようにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping tcn query solicit**
4. **end**
5. **show ip igmp snooping**
6. **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： `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	**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	**ip igmp snooping tcn query solicit** 例： `Device(config)# ip igmp snooping tcn query solicit`	TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げるために、IGMP Leave メッセージ（グローバル脱退）を送信します。デフォルトでは、クエリー送信要求はディセーブルに設定されています。 （注） デフォルトのクエリソリューションに戻すには、 **no ip igmp snooping tcn query solicit** グローバル コンフィギュレーション コマンドを使用します。

	コマンドまたはアクション	目的
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	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	TCN の設定を確認します。
ステップ 6	**copy running-config startup-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。

TCN イベント中のマルチキャスト フラッディングのディセーブル化

デバイスは TCN を受信すると、一般クエリを 2 つ受信するまで、すべてのポートに対してマルチキャストトラフィックをフラッディングします。異なるマルチキャストグループのホストに接続されているポートが複数ある場合、リンク範囲を超えてにデバイスよるフラッディングが行われ、パケット損失が発生する可能性があります。TCN フラッディングを制御するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **no ip igmp snooping tcn flood**
5. **end**
6. **show ip igmp snooping**
7. **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： `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	**configure terminal** 例：	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
	`Device# configure terminal`	
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet 1/0/1`	設定するインターフェイスを指定して、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 4	**no ip igmp snooping tcn flood** 例： `Device(config-if)# no ip igmp snooping tcn flood`	スパニングツリーの TCN イベント中に発生するマルチキャスト トラフィックのフラッディングをディセーブルにします。 デフォルトでは、インターフェイス上のマルチキャスト フラッディングはイネーブルです。 （注） インターフェイス上でマルチキャストフラッディングを再度イネーブルにするには、 **ip igmp snooping tcn flood** 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。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	TCN の設定を確認します。
ステップ 7	**copy running-config startup-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。

IGMP スヌーピング クエリアの設定

特定の VLAN で IGMP スヌーピング クエリア機能をイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**

2. **configure terminal**
3. **ip igmp snooping querier**
4. **ip igmp snooping querier address** *ip_address*
5. **ip igmp snooping querier query-interval** *interval-count*
6. **ip igmp snooping querier tcn query** [**count** *count* | **interval** *interval*]
7. **ip igmp snooping querier timer expiry** *timeout*
8. **ip igmp snooping querier version** *version*
9. **end**
10. **show ip igmp snooping vlan** *vlan-id*
11. **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： `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	**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	**ip igmp snooping querier** 例： `Device(config)# ip igmp snooping querier`	IGMP スヌーピング クエリアをイネーブルにします。
ステップ 4	**ip igmp snooping querier address** *ip_address* 例： `Device(config)# ip igmp snooping querier address 172.16.24.1`	（任意）IGMP スヌーピング クエリアの IP アドレスを指定します。IP アドレスを指定しない場合、クエリアはIGMPクエリアに設定されたグローバル IP アドレスを使用します。 （注） IGMP スヌーピングクエリアがデバイス上で IP アドレスを検出できない場合、IGMP一般クエリを生成しません。
ステップ 5	**ip igmp snooping querier query-interval** *interval-count* 例： `Device(config)# ip igmp snooping querier query-interval 30`	（任意）IGMPクエリアの間隔を設定します。指定できる範囲は 1 ～ 18000 秒です。

	コマンドまたはアクション	目的
ステップ 6	**ip igmp snooping querier tcn query** [**count** *count* | **interval** *interval*] 例： `Device(config)# ip igmp snooping querier tcn query interval 20`	（任意）トポロジ変更通知（TCN）クエリーの間隔を設定します。指定できる count の範囲は 1 ～ 10 です。指定できる interval の範囲は 1 ～ 255 秒です。
ステップ 7	**ip igmp snooping querier timer expiry** *timeout* 例： `Device(config)# ip igmp snooping querier timer expiry 180`	（任意）IGMP クエリアが期限切れになる時間を設定します。指定できる範囲は 60 ～ 300 秒です。
ステップ 8	**ip igmp snooping querier version** *version* 例： `Device(config)# ip igmp snooping querier version 2`	（任意）クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。
ステップ 9	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show ip igmp snooping vlan** *vlan-id* 例： `Device# show ip igmp snooping vlan 30`	（任意）VLAN インターフェイス上で IGMP スヌーピング クエリアがイネーブルになっていることを確認します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
ステップ 11	**copy running-config startup-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。

IGMP レポート抑制のディセーブル化

IGMP レポート抑制をディセーブルにするには、次の手順を実行します。

手順の概要

1. **enable**

2. **configure terminal**
3. **no ip igmp snooping report-suppression**
4. **end**
5. **show ip igmp snooping**
6. **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： `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	**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	**no ip igmp snooping report-suppression** 例： `Device(config)# no ip igmp snooping report-suppression`	IGMP レポート抑制をディセーブルにします。IGMP レポート抑制がディセーブルの場合、すべての IGMP レポートがマルチキャスト ルータに転送されます。 IGMP レポート抑制はデフォルトでイネーブルです。 IGMP レポート抑制がイネーブルの場合、デバイスはマルチキャスト ルータ クエリごとに IGMP レポートを 1 つだけ転送します。 （注） IGMP レポート抑制を再びイネーブルにするには、 **ip igmp snooping report-suppression** 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。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	IGMP レポート抑制がディセーブルになっていることを確認します。
ステップ 6	**copy running-config startup-config** 例：	（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
	`Device# copy running-config startup-config`	

IGMP のモニタリング

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。

（注） このリリースでは、ルート単位の統計情報がサポートされていません。

また、リソースの使用状況を学習し、ネットワーク問題を解決するための情報を表示することもできます。さらに、ノードの到達可能性に関する情報を表示し、そのパケットが経由するネットワーク内のパスを検出することもできます。

次の表に示す特権EXECコマンドのいずれかを使用すると、さまざまなルーティング統計情報を表示できます。

表 *11 :* システムおよびネットワーク統計情報を表示するコマンド

コマンド	目的
show ip igmp filter	IGMP フィルタ情報を表示します。
show ip igmp groups [*type-number* | *detail*]	デバイスに直接接続され、IGMP す。
show ip igmp interface [*type number*]	インターフェイスのマルチキャス
show ip igmp membership [*name/group address* | **all** | **tracked**]	転送に関する IGMP メンバーシッ
show ip igmp profile [*profile_number*]	IGMP プロファイル情報を表示し
show ip igmp ssm-mapping [*hostname/IP address*]	IGMP SSM マッピング情報を表示
show ip igmp static-group {**class-map** [**interface** [*type*]]	スタティック グループ情報を表示
show ip igmp vrf	選択した VPN ルーティング/転送

IGMP スヌーピング情報の監視

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 IGMP スヌーピング情報を表示できます。また、IGMP スヌーピング用に設定された VLAN の IP 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 *12 : IGMP* スヌーピング情報を表示するためのコマンド

コマンド	目的
show ip igmp snooping detail	動作状態情報を表示します。
show ip igmp snooping groups [**count** |**dynamic** [**count**] | **user** [**count**]]	デバイスまたは特定のパラメ • **count**：実エントリの代わ す。 • **dynamic**：IGMP スヌー • **user**：ユーザーによって
show ip igmp snooping groups [**count** | [**vlan** *vlan-id* [*A.B.C.D* | **count**]]	デバイスまたは特定のパラメ • **count**：グループの合計数 • **vlan**：VLAN ID によるク
show ip igmp snooping igmpv2-tracking	IGMP スヌーピング トラッキ （注） このコマンドでは プおよびIPアドレ ません。このコマ にしておく必要が
show ip igmp snooping groups vlan *vlan-id* [*ip_address* | **count** | **dynamic** [**count**] | **user**[**count**]]	マルチキャスト VLAN または テーブル情報を表示します。 • *vlan-id*：VLAN ID の範囲 • **count**：実エントリの代わ す。 • **dynamic**：IGMP スヌー • *ip_address*：指定したグル ます。 • **user**：ユーザーによって
show ip igmp snooping mrouter [**vlan** *vlan-id*]	ダイナミックに学習され、手 報を表示します。 （注） IGMP スヌーピン 先インターフェイ に学習されます。 （任意）個々の VLAN に関す

コマンド	目的
show ip igmp snooping querier [**detail** | **vlan** *vlan-id*]	IP アドレス、および VLAN で受 る情報を表示します。 （任意）VLAN の詳細な IGMP （任意）個々の VLAN に関する
show ip igmp snooping querier [**vlan** *vlan-id*] **detail**	IP アドレスおよび VLAN で受信 る情報、VLAN の IGMP スヌー 表示します。
show ip igmp snooping [**vlan** *vlan-id* [**detail**]]	デバイス上のすべての VLAN ま （任意）個々の VLAN に関する る VLAN ID の範囲は 1 ～ 1001

IGMP フィルタリングおよび IGMP スロットリングの設定のモニタリング

IGMP プロファイルの特性を表示したり、デバイス上のすべてのインターフェイスまたは指定されたインターフェイスの IGMP プロファイルや最大グループ設定を表示したりできます。また、デバイス上のすべてのインターフェイスまたは指定したインターフェイスに関する IGMP スロットリング設定を表示することもできます。

表 *13 : IGMP* フィルタリングおよび *IGMP* スロットリング設定を表示するためのコマンド

コマンド	目的
show ip igmp profile [*profile number*]	特定の IGMP プロファイルまたはデバイ れているすべての IGMP プロファイルを表
show running-config [**interface** *interface-id*]	インターフェイスが所属できる IGMP グ 数（設定されている場合）や、インター 用される IGMP プロファイルを含む、特定 フェイスまたはデバイス上のすべてのイン スの設定を表示します。

IGMP の設定例

例：マルチキャストグループのメンバとしてデバイスを設定

次に、マルチキャストグループ 255.2.2.2 へのデバイス加入を許可する例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip igmp join-group 255.2.2.2
Device(config-if)#
```

例：マルチキャスト グループへのアクセスの制御

インターフェイスで参加数を制限するには、IGMPプロファイルと関連付けるフィルタ用のポートを設定します。

```
Device# configure terminal
Device(config)# ip igmp profile 10
Device(config-igmp-profile)# ?

IGMP profile configuration commands:
deny matching addresses are denied
exit Exit from igmp profile configuration mode
no Negate a command or set its defaults
permit matching addresses are permitted
range add a range to the set

Device(config-igmp-profile)# range 172.16.5.1
Device(config-igmp-profile)# exit
Device(config)# interface gigabitEthernet 2/0/10
Device(config-if)# ip igmp filter 10
```

例：IGMP スヌーピングの設定

次に、マルチキャスト ルータへの静的な接続をイネーブルにする例を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet1/0/2
Device(config)# end
```

次に、ポート上のホストを静的に設定する例を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet1/0/1
Device(config)# end
```

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

```
Device# configure terminal
Device(config)# ip igmp snooping vlan 130 immediate-leave
Device(config)# end
```

次に、IGMP スヌーピング クエリアの送信元アドレスを 10.0.0.64 に設定する例を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping querier 10.0.0.64
Device(config)# end
```

次の例では、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する方法を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping querier query-interval 25
Device(config)# end
```

次の例では、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する方法を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping querier timer expiry 60
Device(config)# end
```

次に、IGMP スヌーピング クエリア機能をバージョン 2 に設定する例を示します。

```
Device# configure terminal
Device(config)# no ip igmp snooping querier version 2
Device(config)# end
```

例：IGMP プロファイルの設定

次に、単一の IP マルチキャスト アドレスへのアクセスを許可する IGMP プロファイル 4 を作成して、設定を確認する例を示します。アクションが拒否（デフォルト）である場合は、**show ip igmp profile** の出力には表示されません。

```
Device(config)# ip igmp profile 4
Device(config-igmp-profile)# permit
Device(config-igmp-profile)# range 229.9.9.0
Device(config-igmp-profile)# end
Device# show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

例：IGMP プロファイルの適用

次に、ポートに IGMP プロファイル 4 を適用する例を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip igmp filter 4
Device(config-if)# end
```

例：IGMP グループの最大数の設定

次の例では、ポートが加入できる IGMP グループ数を 25 に制限する方法を示します。

```
Device(config)# interface Gigabitethernet1/0/2
Device(config-if)# ip igmp max-groups 25
Device(config-if)# end
```

例：ルーテッド ポートとしてのインターフェイス設定

次に、デバイスのインターフェイスをルーテッドポートとして設定する例を示します。**no switchport** コマンドを実行して複数の IP マルチキャストルーティングを設定する必要がある場合、インターフェイスでこの設定を行う必要があります。

```
Device# configure terminal
Device(config)#  interface GigabitEthernet1/0/9
Device(config-if)# description interface to be use as routed port
Device(config-if)# no switchport
Device(config-if)# ip address 10.20.20.1 255.255.255.0
Device(config-if)# ip pim sparse-mode
Device(config-if)# ip igmp join-group 224.1.2.3 source 15.15.15.2
Device(config-if)# end
Device# configure terminal
Device# show run interface gigabitEthernet 1/0/9

Current configuration : 166 bytes
!
interface GigabitEthernet1/0/9
 no switchport
 ip address 10.20.20.1 255.255.255.0
 ip pim sparse-mode
 ip igmp static-group 224.1.2.3 source 15.15.15.2
end
```

例：SVI としてのインターフェイスの設定

次に、デバイスのインターフェイスを SVI として設定する例を示します。**no switchport** コマンドを実行して複数の IP マルチキャストルーティングを設定する必要がある場合、インターフェイスでこの設定を行う必要があります。

```
Device(config)# interface vlan 150
Device(config-if)# ip address 10.20.20.1 255.255.255.0
Device(config-if)# ip pim sparse-mode
Device(config-if)#  ip igmp join-group 224.1.2.3 source 15.15.15.2
Device(config-if)# end
Device# configure terminal
Device(config)# ip igmp snooping vlan 20 static 224.1.2.3 interface gigabitEthernet 1/0/9
Device# show run interface vlan 150

Current configuration : 137 bytes
!
interface vlan 150
 ip address 10.20.20.1 255.255.255.0
 ip pim sparse-mode
 ip igmp static-group 224.1.2.3 source 15.15.15.2
end
```

例：直接接続された IGMP ホストがない場合に、マルチキャスト トラフィックを転送するようにデバイスを設定

ip igmp join-group コマンドを使用して、直接接続された IGMP ホストがない場合に、マルチキャストトラフィックを転送するようデバイスを設定する例を以下に示します。この方法では、デバイスは、マルチキャスト パケットの転送に加えて、マルチキャスト パケットを受信します。マルチキャスト パケットを受信する場合は、高速スイッチングを実行できません。

この例では、デバイスでギガビットイーサネットインターフェイス 1/0/1 が、グループ 225.2.2.2 に加入するように設定されています。

```
interface GigabitEthernet1/0/1
 ip igmp join-group 225.2.2.2
```

ip igmp static-group コマンドを使用して、直接接続された IGMP ホストがない場合に、マルチキャストトラフィックを転送するようデバイスを設定する例を以下に示します。この方法の場合、デバイスはパケットそのものを受信せず、転送だけを実行します。したがって、この方法では、高速スイッチングを実行できます。発信インターフェイスが IGMP キャッシュに格納されますが、マルチキャストルートエントリに「L」（ローカル）フラグが付かないことからも明らかなように、デバイス自体はメンバではありません。

この例では、グループ 225.2.2.2 のスタティック グループ メンバーシップ エントリがファストイーサネット インターフェイス 0/1/0 で設定されます。

```
interface GigabitEthernet1/0/1
 ip igmp static-group 225.2.2.2
```

IGMP 拡張アクセス リストを使用して SSM ネットワークへのアクセスを制御する方法

ここでは、IGMP 拡張アクセス リストを使用して SSM ネットワーク上でアクセスを制御する、次の設定例について説明します。

（注） アクセス リストは非常に柔軟が高いことに留意してください。マルチキャスト トラフィックのフィルタリングに使用できる permit ステートメントと deny ステートメントの組み合わせは多数あります。この項では、少しの例を示します。

例：グループ G のすべての状態を拒否

次に、グループ G のすべての状態を拒否する方法の例を示します。この例では、IGMPv3 レポートの SSM グループ 232.2.2.2 のすべての送信元がフィルタリングされるよう、ファストイーサネット インターフェイス 0/0/0 が設定されます。これにより、このグループが効率的に拒否されます。

```
ip access-list extended test1
 deny igmp any host 232.2.2.2
 permit igmp any any
!
interface GigabitEthernet 1/0/1
 ip igmp access-group test1
```

例：ソース S のすべての状態を拒否

次に、ソース S ですべての状態を拒否する方法の例を示します。この例では、IGMPv3 レポートの送信元の 10.2.1.32 のグループがフィルタリングされるよう、ギガビット イーサネット インターフェイス 1/1/0 が設定されます。これにより、このソースが効果的に拒否されます。

```
ip access-list extended test2
 deny igmp host 10.2.1.32 any
 permit igmp any any
!
interface GigabitEthernet1/0/1
 ip igmp access-group test2
```

例：グループ G のすべての状態を許可

次に、グループ G ですべての状態を許可する例を示します。この例では、IGMPv3 レポートの SSM グループ 232.1.1.10 に対するすべてのソースが受け付けられるよう、ギガビット イーサネット インターフェイス 1/2/0 が設定されます。これにより、このグループ全体が効果的に受け付けられます。

```
ip access-list extended test3
 permit igmp any host 232.1.1.10
!
interface GigabitEthernet 1/2/0
 ip igmp access-group test3
```

例：ソース S のすべての状態を許可

次に、ソース S ですべての状態を許可する例を示します。この例では、IGMPv3 レポートのソース 10.6.23.32 に対するすべてのグループが受け付けられるよう、ギガビット イーサネット インターフェイス 1/2 が設定されます。これにより、このソース全体が効果的に受け付けられます。

```
ip access-list extended test4
 permit igmp host 10.6.23.32 any
!
interface GigabitEthernet1/2/0
 ip igmp access-group test4
```

例：グループ G のソース S をフィルタリング

次に、グループ G の特定のソース S のフィルタリング例を示します。この例では、IGMPv3 レポートの SSM グループ 232.2.30.30 のソース 232.2.2.2 をフィルタリングするよう、ギガビット イーサネット インターフェイス 0/3/0 が設定されます。

```
ip access-list extended test5
 deny igmp host 10.4.4.4 host 232.2.30.30
 permit igmp any any
!
interface GigabitEthernet0/3/0
 ip igmp access-group test5
```

IGMP に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)*

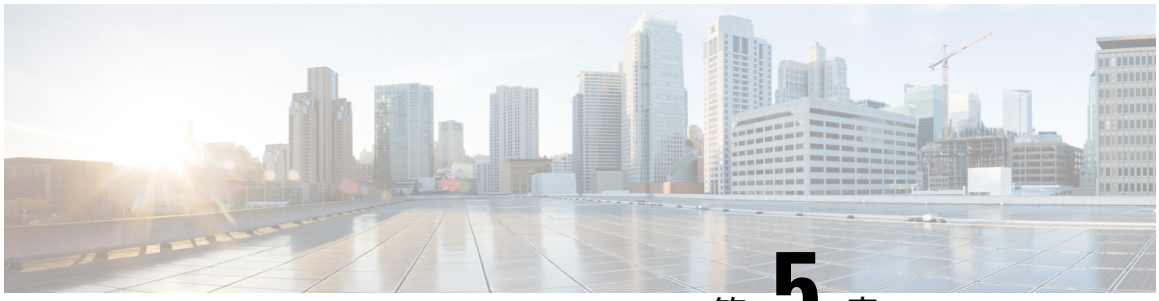
IGMP の機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IGMP	IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。インターフェイスで PIM をイネーブルにすると、IGMP もイネーブルになります。IGMP 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。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。



第 5 章

IGMP プロキシの設定

IGMP プロキシの前提条件

- IGMP UDL 上のすべてのデバイスに、同じサブネット アドレスがあること。UDL 上のすべてのデバイスで、同じサブネットアドレスを持つことができない場合、アップストリーム デバイスは、ダウンストリーム デバイスが接続されているすべてのサブネットに一致するセカンダリ アドレスで設定される必要があります。
- IP マルチキャストがイネーブルになり、PIM インターフェイスが設定されます。IGMP プロキシ用の PIM インターフェイスを設定する際、インターフェイスがスパースモード領域で稼働中で、静的RP、ブートストラップ（BSR）、またはリスナー機能付きの Auto-RP を実行している場合は、PIM スパースモード（PIM-SM）を使用します。

IGMP プロキシについて

IGMP プロキシ

IGMPプロキシは、アップストリーム ネットワークがソースのマルチキャスト グループに、ダウンストリーム ルータに直接接続されていない単方向リンク ルーティング（UDLR）環境のホストが加入できるようにします。

IGMPプロキシを実装するには、次の 2 つの方法があります。

- 単一のアップストリーム インターフェイス用の IGMP プロキシ

- 複数のアップストリーム インターフェイス用の IGMP プロキシ

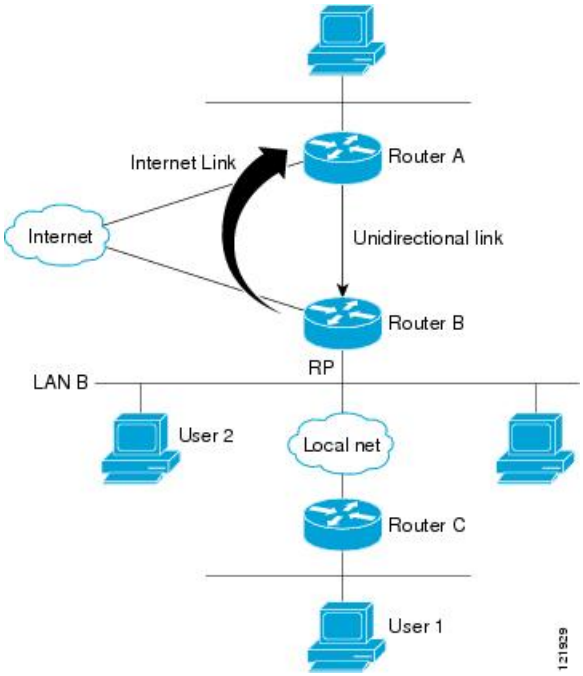
単一のアップストリーム インターフェイス用の IGMP プロキシ

次の図は、2 つの UDLR シナリオを示すトポロジ例です。

- 従来型の UDL ルーティングのシナリオ：直接接続されたレシーバがある UDL デバイス。
- IGMP プロキシのシナリオ：直接接続されたレシーバのない UDL デバイス。

IGMP UDL は、アップストリームおよびダウンストリーム デバイス上にある必要はありません。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。



シナリオ 1：従来型の UDLR のシナリオ（受信先が直接接続されている UDL デバイス）

シナリオ 1 では、IGMP プロキシ メカニズムは必要ありません。このシナリオでは、次の一連のイベントが発生します。

1. ユーザー 2 がグループ G の対象を要求する IGMP メンバーシップ レポートを送信します。
2. ルータ B は、IGMP メンバーシップ レポートを受信し、LAN B のグループ G の転送エントリを追加し、UDLR アップストリーム デバイスであるルータ A に IGMP レポートをプロキシします。

3. IGMP レポートは、インターネット リンク間でプロキシされます。
4. ルータ A は IGMP プロキシを受信し、単方向リンクの転送エントリを保持します。

シナリオ 2：IGMP プロキシのシナリオ（受信先が直接接続されていない UDL デバイス）

シナリオ 2 の場合、アップストリーム ネットワークがソースのマルチキャスト グループに、ダウンストリーム デバイスに直接接続されていないホストが加入できるように、IGMP プロキシ メカニズムが必要です。このシナリオでは、次の一連のイベントが発生します。

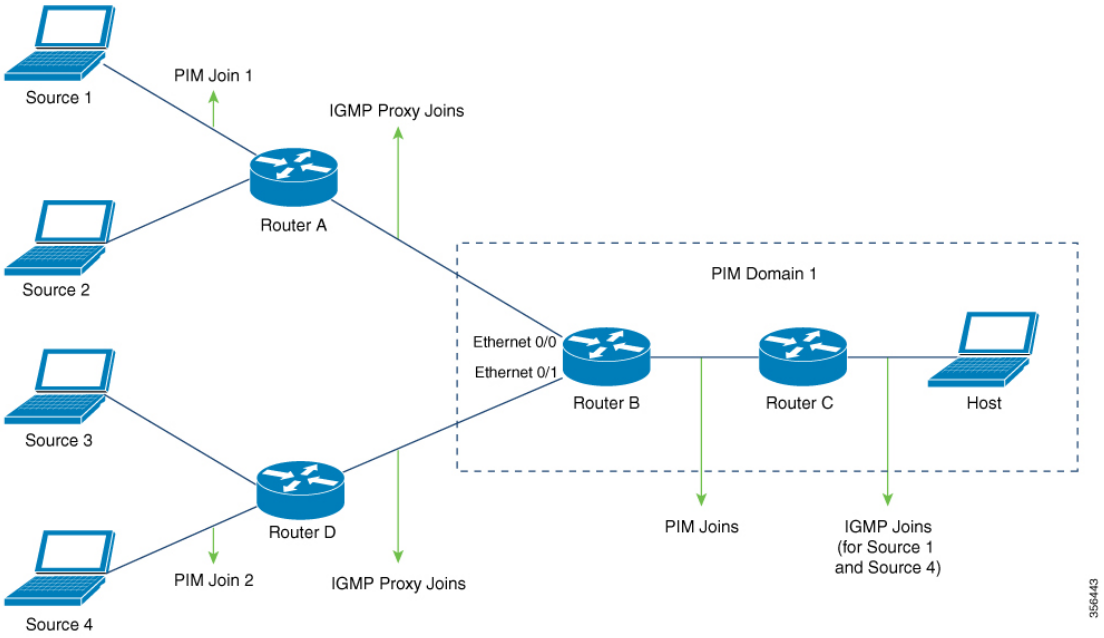
1. ユーザー 1 がグループ G の対象を要求する IGMP メンバーシップ レポートを送信します。
2. ルータ C が RP（ルータ B）に PIM Join メッセージをホップバイホップで送信します。
3. ルータ B で PIM 加入メッセージを受信し、LAN B 上のグループ G に対する転送エントリが追加されます。
4. ルータ B では、その mroute テーブルが定期的にチェックされ、インターネット リンクを介してアップストリーム UDL デバイスに IGMP メンバーシップ レポートがプロキシされます。
5. ルータ A は単方向リンク（UDL）転送エントリを作成し、維持します。

エンタープライズ ネットワークでは、サテライトを介して IP マルチキャスト トラフィックを受信し、ネットワーク中にトラフィックを転送することができる必要があります。シナリオ 2 は、受信ホストがダウンストリーム デバイスのルータ B に直接接続する必要があるため、単方向リンク ルーティング（UDLR）だけでは不可能です。IGMP プロキシ メカニズムを使用すると、マルチキャスト転送テーブル内の (*, G) エントリに対し IGMP レポートを作成することで、この制限が取り除かれます。そのため、このシナリオを機能させるには、インターフェイスでプロキシされた (*, G) 静的マルチキャストルート（mroute）エントリの IGMP レポートの転送をイネーブルにして（**ip igmp mroute-proxy** コマンドを使用）、mroute プロキシサービスをイネーブルにし（**ip igmp proxy-service** コマンドを使用）、PIM 対応ネットワークと可能性があるメンバに導く必要があります。

（注） PIM メッセージはアップストリームに転送されないため、各ダウンストリーム ネットワークとアップストリーム ネットワークのドメインは別になります。

複数のアップストリーム インターフェイス用の IGMP プロキシ

IGMP プロキシを使用すると、複数のアップストリーム インターフェイスからデータを要求することもできます。ネットワーク内のアップストリームデバイス数が多い場合は、この方法で IGMP プロキシを実装できます。この方法を使用する場合、前のセクションで説明した 3 つのシナリオのいずれかのように、単一のアップストリームデバイスに IGMP プロキシを実装することもできます。



この方法では、IGMP プロキシを使用して、複数のアップストリームデバイスからトラフィックを受信できます。次の一連のイベントが発生します。

1. ホストは PIM ドメイン 1 にあり、複数の IGMP メンバーシップレポートを**ルータ C** に送信して（加入要求）、異なるグループへの関心を要求します。**ルータ C** は IGMP 加入を PIM 加入に変換し、**ルータ B** に送信します。これらの要求は、**ルータ B** から**ルータ A** にアップストリームで送信する必要があります。ルータは 2 つの異なる PIM ドメイン内にあります（PIM ネイバーではありません）。
2. **ルータ B** は PIM 加入メッセージを IGMP プロキシ加入メッセージに変換して、上位のインターフェイスに転送できるようにします。
3. クラスマップはグローバルに設定されます。このクラスマップには、マルチキャストグループに関する情報を記述します。次の条件が満たされると、異なるマルチキャストグループの IGMP プロキシ加入が送信されます。
   - グループに (*, G) または (S, G) エントリがある。
   - (*, G) または (S, G) エントリに NULL ではない OIF リストがある。
4. IGMP プロキシのインターバルで、異なるグループの IGMP プロキシ加入がそれぞれのアップストリーム インターフェイスを介して送信されます。
5. IGMP プロキシ加入メッセージが**ルータ A** に到達すると、PIM 加入メッセージとしてそれぞれの送信元デバイスに転送されます。

IGMP プロキシの設定方法

IGMP UDLR に対するアップストリーム UDL デバイスの設定

IGMP UDLR に対するアップストリーム UDL デバイスを設定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip igmp unidirectional-link**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/0`	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。 • *type* および *number* 引数に、アップストリーム デバイスの UDL として使用するインターフェイスを指定します。
ステップ 4	**ip igmp unidirectional-link** 例： `Device(config-if)# ip igmp unidirectional-link`	インターフェイス上の IGMP を、IGMP UDLR に対して単方向になるよう設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。

IGMP プロキシ サポート付きの IGMP UDLR に対するダウンストリーム UDL デバイスの設定

IGMP プロキシ サポート付きの IGMP UDLR に対するダウンストリーム UDL デバイスを設定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip igmp unidirectional-link**
5. **exit**
6. **interface** *type number*
7. **ip igmp mroute-proxy** *type number*
8. **exit**
9. **interface** *type number*
10. **ip igmp helper-address udl** *interface-type interface-number*
11. **ip igmp proxy-service**
12. **end**
13. **show ip igmp interface**
14. **show ip igmp udlr**

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	**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	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	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。 • *type* および *number* 引数に、IGMP UDLR に対するダウンストリーム デバイスの UDL として使用するインターフェイスを指定します。
ステップ 4	**ip igmp unidirectional-link** 例：	インターフェイス上の IGMP を、IGMP UDLR に対して単方向になるよう設定します。

	コマンドまたはアクション	目的
	`Device(config-if)# ip igmp unidirectional-link`	
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 6	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/0`	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。 • *type* および *number* 引数で、間接的に接続されているホストの方向に向いているインターフェイスを選択します。
ステップ 7	**ip igmp mroute-proxy** *type number* 例： `Device(config-if)# ip igmp mroute-proxy loopback 0`	プロキシされた (*, G) マルチキャスト スタティック ルート（mroute）エントリの IGMP レポートの転送をイネーブルにします。 • この手順は、マルチキャスト転送テーブルにあるすべての (*, G) 転送エントリに対するプロキシ サービス インターフェイスへの、IGMP レポートの転送をイネーブルにするために実行されます。 • この例では、ギガビットイーサネットインターフェイス 1/0/0 で、ギガビット イーサネット インターフェイス 1/0/0 に転送される mroute テーブルのすべてのグループのループバック インターフェイス 0 に IGMP レポートを送信するように要求する **ip igmp mroute-proxy** コマンドが設定されます。
ステップ 8	**exit** 例： `Device(config-if)# exit`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 9	**interface** *type number* 例： `Device(config)# interface loopback 0`	指定したインターフェイスに対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。 • この例では、ループバック インターフェイス 0 が指定されます。
ステップ 10	**ip igmp helper-address udl** *interface-type interface-number*	UDLR で IGMP ヘルパーを設定します。

	コマンドまたはアクション	目的
	例： `Device(config-if)# ip igmp helper-address udl gigabitethernet 0/0/0`	• このステップで、ダウンストリーム デバイスが受信したホストから *interface-type* および *interface-number* 引数で指定されたインターフェイスに関連付けられた UDL に接続されているアップストリーム デバイスへの IGMP レポートをヘルパー処理できるようになります。 • トポロジ例では、IGMPヘルパーはダウンストリーム デバイスのループバック インターフェイス0に設定されます。そのため、ループバックインターフェイス0が、ホストからギガビット イーサネット インターフェイス 0/0/0 に接続されているアップストリーム デバイスへの IGMP レポートをヘルパー処理するように設定されます。
ステップ 11	**ip igmp proxy-service** 例： `Device(config-if)# ip igmp proxy-service`	mroute プロキシ サービスをイネーブルにします。 • mroute プロキシサービスがイネーブルのときに、IGMP クエリインターバルに基づいて **ip igmp mroute-proxy** コマンド（ステップ 7 を参照）で設定されたインターフェイスに一致する、(*, G) 転送エントリの静的 mroute テーブルが、デバイスによって定期的にチェックされます。一致が存在する場合、1 つの IGMP レポートがこのインターフェイスで作成され、受信されます。 （注） **ip igmp proxy-service** コマンドは、**ip igmp helper-address**（UDL）コマンドとともに使用することを目的としています。 • この例では、**ip igmp mroute-proxy** コマンドで登録されているインターフェイスに対するすべてのグループのインターフェイスに対して IGMP レポートの転送をイネーブルにするように、ループバック インターフェイス 0 で **ip igmp proxy-service** コマンドが設定されます（ステップ 7 を参照してください）。
ステップ 12	**end** 例：	現在のコンフィギュレーション セッションを終了して、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
	`Device(config-if)# end`	
ステップ 13	**show ip igmp interface** 例： `Device# show ip igmp interface`	（任意）インターフェイスに関するマルチキャスト関連情報を表示します。
ステップ 14	**show ip igmp udlr** 例： `Device# show ip igmp udlr`	（任意）設定された UDL ヘルパー アドレスがあるインターフェイス上で、マルチキャスト グループに直接接続されている UDLR 情報を表示します。

複数のアップストリーム インターフェイスの IGMP プロキシ向けダウンストリームデバイスの設定

複数のアップストリームインターフェイス向けIGMPプロキシのダウンストリームデバイスを設定するには、次の作業を実行します

（前の図を参照して、アップストリーム デバイスに接続されているルータ *B* のインターフェイスですべての手順を実行してください）。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type multicast-flows** *name*
4. **interface** *type number*
5. **ip igmp upstream-proxy** *class-map-name*
6. **ip igmp iif-starg**
7. **ip igmp proxy-report-interval** *time*
8. **end**
9. **show ip igmp interface**

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	**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 3	**class-map type multicast-flows** *name* 例： `Device(config-if)# class-map type multicast-flows proxymap`	異なるマルチキャストグループのアップリンク インターフェイスが定義されているクラスマップを使用して、インターフェイスを設定します。 マルチキャストグループの範囲は、225.0.0.1 ー 225.0.0.10 です。
ステップ 4	**interface** *type number* 例： `Device(config)# interface ethernet 0/0`	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。 *type* 引数および *number* 引数では、ホストに接続されているインターフェイスを指定します。
ステップ 5	**ip igmp upstream-proxy** *class-map-name* 例： `Device(config-if)# ip igmp upstream-proxy proxymap`	IGMP プロキシとのインターフェイスをイネーブルにします。次の条件が満たされると、クラスマップ内にあるこれらのグループの IGMP プロキシ参加が送信されます。 • (*,G) または (S,G) mroute が、インターフェイスと同じ mvrf のグループに対して存在する。 • (*,G) または (S,G) mroute に NULL ではない OIF リストがある。
ステップ 6	**ip igmp iif-starg** 例： `Device(config-if)# ip igmp iif-starg`	クラスマップで指定したグループの mroute の RPF インターフェイスをイーサネット 0/0 に変更します。
ステップ 7	**ip igmp proxy-report-interval** *time* 例： `Device(config-if)# ip igmp proxy-report-interval 130`	プロキシレポートの送信間隔（秒単位）を設定します。デフォルト値は 60 秒です。
ステップ 8	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 9	**show ip igmp interface** 例： `Device# show ip igmp interface`	（任意）インターフェイスに関するマルチキャスト関連情報を表示します。

IGMP プロキシの設定例

例：IGMP UDLR 向けアップストリーム UDL デバイスの設定

IGMP UDLR 向けアップストリーム UDL の設定例を以下に示します。

```
interface gigabitethernet 0/0/0
ip address 10.1.1.1 255.255.255.0
ip pim sparse-mode
!
interface gigabitethernet 1/0/0
ip address 10.2.1.1 255.255.255.0
ip pim sparse-mode
ip igmp unidirectional-link
!
interface gigabitethernet 2/0/0
ip address 10.3.1.1 255.255.255.0
```

例：IGMP プロキシサポートによる IGMP UDLR 向けダウンストリーム UDL デバイスの設定

IGMP プロキシサポートを使用して、IGMP UDLR 向けのダウンストリーム UDL デバイスを設定する例を以下に示します。

```
ip pim rp-address 10.5.1.1 5
access-list 5 permit 239.0.0.0 0.255.255.255
!
interface loopback 0
ip address 10.7.1.1 255.255.255.0
ip pim sparse-mode
ip igmp helper-address udl ethernet 0
ip igmp proxy-service
!
interface gigabitethernet 0/0/0
ip address 10.2.1.2 255.255.255.0
ip pim sparse-mode
ip igmp unidirectional-link
!
interface gigabitethernet 1/0/0
ip address 10.5.1.1 255.255.255.0
ip pim sparse-mode
ip igmp mroute-proxy loopback 0
!
interface gigabitethernet 2/0/0
ip address 10.6.1.1 255.255.255.0
```

例：複数のアップストリーム インターフェイスの IGMP プロキシ向けダウンストリームデバイスの設定

複数のアップストリームインターフェイスのIGMPプロキシ向けダウンストリームデバイスを設定する例を次に示します。

```
interface gigabitethernet0/0
ip address 99.99.99.1 255.255.255.0
ip pim passive
ip igmp upstream-proxy l2
ip igmp iif-starg
ip igmp proxy-report-interval 100
end

class-map type multicast-flows l2
group 229.0.0.1
group 228.0.0.1 to 228.0.0.10
```

IGMP プロキシに関するその他の関連資料

ここでは、IGMP のカスタマイズに関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)*

標準および RFC

標準/RFC	タイトル
RFC 1112	『*Host extensions for IP multicasting*』
RFC 2236	『*Internet Group Management Protocol, Version 2*』
RFC 3376	『*Internet Group Management Protocol, Version 3*』

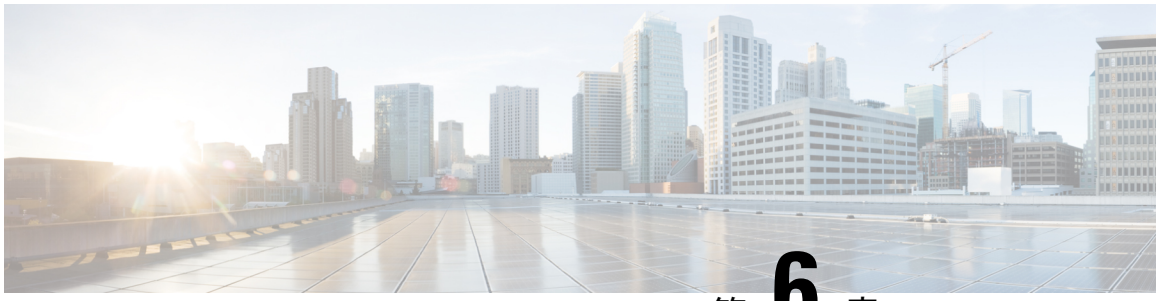
IGMP プロキシの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IGMP プロキシ	IGMP プロキシは、アップストリーム ネットワークがソースのマルチキャスト グループに、ダウンストリーム ルータに直接接続されていない単方向リンク ルーティング（UDLR）環境のホストが加入できるようにします。
Cisco IOS XE Amsterdam 17.1.1	複数のアップストリーム インターフェイス用の IGMP プロキシ	IGMPプロキシを使用すると、ユーザーは複数のアップストリームデバイスからトラフィックを受信できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。



第 6 章

IGMP の明示的なトラッキング

このモジュールでは、インターネット グループ管理プロトコル（IGMP）のホスト、グループ、およびチャンネルの明示的なトラッキングについて説明します。

IGMP の明示的なトラッキングの制約事項

次の制約事項がこの機能に適用されます。

- ネットワーク上に IGMP バージョン 1 または IGMP バージョン 2 のみがサポートされている 1 つまたは複数のホストがある場合、ホストが加入しているマルチキャスト グループに対する脱退遅延は、ホストの IGMP バージョンの脱退遅延に戻されます。これは、IGMP バージョン 2 では約 3 秒間で、IGMP バージョン 1 では最大 180 秒間（3 分間）です。この条件は、これらのレガシー ホストが実際に何らかの時点で実際に加入しているマルチキャスト グループのみに影響します。さらに、IGMPv3 ホストが送信したこれらのマルチキャスト グループのメンバーシップ レポートは、IGMP バージョン 1 やバージョン 2 のメンバーシップ レポートに戻り、これらのホスト メンバーシップの明示的なトラッキングが無効になる場合があります。

- IGMP バージョン 3 Lite（IGMP v3lite）または URL ランデブー ディレクトリ（URD）のチャネル メンバーシップ レポートの明示的なトラッキングはサポートされていません。そのため、IGMPv3 Lite または URD を使用したホストにトラフィックを送信するマルチキャスト グループの脱退遅延は、ホスト上で設定されている IGMP のバージョンの脱退遅延によって決定されます（IGMPv3 の場合、明示的トラッキングが設定されていないときの脱退遅延は通常、3 秒です）。

IGMP の明示的トラッキングについて

IGMP の明示的なトラッキング

インターネット グループ管理プロトコル（IGMP）は、隣接するマルチキャスト デバイスにマルチキャスト グループ メンバーシップを報告するために IP ホストによって使用されます。IGMP の明示的トラッキング機能は、特定のマルチアクセス ネットワーク内のすべてのマルチキャスト ホストのメンバーシップをマルチキャスト デバイスで明示的に追跡できるようにします。IGMP の明示的なトラッキングはグローバルに有効にしたり、レイヤ 3 インターフェイスで有効にすることができます。

ホスト、グループ、およびチャネルの明示的トラッキングでは、特定のグループまたはチャネルに参加している各個別ホストをデバイスが追跡できるようにします。この機能の主なメリットは、IGMP の脱退遅延を最小にし、チャネル変更を高速化し、診断機能を向上させることです。

最小脱退遅延

IGMP でのホスト、グループ、およびチャネルの明示的トラッキングの主なメリットは、ホストがマルチキャスト グループまたはチャネルを脱退するときに脱退遅延を最小にできることです。ホストの脱退とデバイスのトラフィック転送の停止との間の時間を IGMP 脱退遅延と呼びます。IGMP バージョン 3（IGMPv3）と明示的なトラッキングで設定したデバイスは、デバイスからのトラフィックの受信を要求する最後のホストがトラフィックの受信をそれ以上必要としていないことを示している場合、トラフィックの転送を即時に停止できます。したがって、脱退遅延はマルチアクセス ネットワークのパケット伝送遅延とデバイスでの処理時間によってのみバウンドされます。

IGMP バージョン 2 では、ホストからの IGMP 脱退メッセージをデバイスで受信するときに、そのデバイスでは、まず、IGMP グループ固有クエリを送信して、同じマルチアクセス ネットワーク上にある他のホストで、依然、トラフィックの受信が要求されているかどうかを認識する必要があります。特定の時間（デフォルト値は約 3 秒）経過後にクエリに応答するホストがない場合、デバイスはトラフィックの転送を停止します。IGMP バージョン 1 と 2 では、ネットワーク内の別のホストによって同じレポートがすでに送信されている場合、IGMP メンバーシップ レポートが抑制されるため、このクエリ プロセスが必要です。そのため、トラフィックの受信を要求しているホストがマルチアクセス ネットワーク上にいくつあるかをデバイスが正確に把握するのは不可能です。

高速チャネル変更

マルチキャスト デバイスとホスト間で帯域幅が制約されるネットワークでは（xDSL 導入環境の場合など）、デバイスとホスト間の帯域幅は一般に N のマルチキャスト ストリームを並行して受信するよう維持するには十分です。これらの導入環境では、通常は各ホストが 1 つのマルチキャスト ストリームにのみ参加し、許容されるホストの全体数は N に限定されます。こ

れらの環境での効果的な脱退遅延が受信アプリケーションのチャネル変更時間を定義します。つまり、1 つの単一ホストでは、前のストリームの転送が停止するまでは、新しいマルチキャスト ストリームを受信できません。アプリケーションが脱退遅延よりも速くチャネルを変更しようとすると、そのアプリケーションはアクセス ネットワークの帯域幅に過負荷をかけ、すべてのホストのトラフィック フローを一時的に低下させることになります。IGMP でのホスト、グループ、およびチャネルの明示的トラッキングでは、脱退遅延を最小化できるため、高速チャネル変更機能が可能になります。

診断機能の向上

IGMP でのホスト、グループ、およびチャネルの明示的トラッキングでは、ネットワーク管理者が他のマルチキャスト グループまたはチャネルに参加しているマルチキャスト ホストを簡単に特定できます。

IGMP の明示的トラッキングの設定方法

明示的なトラッキングのグローバルな有効化

明示的なトラッキングをグローバルおよびレイヤ 3 インターフェイスで有効にできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping vlan** *vlan-id***explicit-tracking**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip igmp snooping vlan** *vlan-id***explicit-tracking** 例： `Device(config)# ip igmp snooping vlan 1 explicit-tracking`	IGMP の明示的なホスト トラッキングを有効にします。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

レイヤ 3 インターフェイス上での明示的なトラッキングの有効化

明示的なトラッキングをグローバルおよびレイヤ 3 インターフェイスで有効にできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **ip pim sparse-mode**
6. **ip igmp version 3**
7. **ip igmp explicit-tracking**
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**interface** *type number* 例： `Device(config)# interface vlan 77`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.254`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 5	**ip pim sparse-mode** 例： `Device(config-if)# ip pim sparse-mode`	Protocol Independent Multicast（PIM）スパース モードをインターフェイス上で有効にします。

	コマンドまたはアクション	目的
ステップ 6	**ip igmp version 3** 例： `Device(config-if)# ip igmp version 3`	デバイス上で Internet Group Management Protocol（IGMP）バージョン3（IGMPv3）を有効にします。
ステップ 7	**ip igmp explicit-tracking** 例： `Device(config-if)# ip igmp explicit-tracking`	IGMP の明示的なホスト トラッキングを有効にします。
ステップ 8	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

IGMP の明示的トラッキングの設定例

例：明示的なトラッキングの有効化

次に、IGMP の明示的トラッキングをグローバルに有効にする基本設定の例を示します。

```
Device# configure terminal
Device(config)# ip multicast routing
Device(config)# ip igmp snooping vlan 1 explicit-tracking
Device(config)# end
```

次に、IGMP の明示的トラッキングをレイヤ 3 インターフェイス上で有効にする基本設定の例を示します。

```
Device# configure terminal
Device(config)# interface vlan 77
Device(config-if)# ip address 10.1.1.1 255.255.255.254
Device(config-if)# ip pim sparse-mode
Device(config-if)# ip igmp version 3
Device(config-if)# ip igmp explicit-tracking
Device(config-if)# end
```

IGMP の明示的なトラッキングの確認

手順の概要

1. **enable**
2. **show ip igmp snooping vlan** *vlan-ID*
3. **show ip igmp groups** *interface-type interface-number*
4. **show ip igmp membership tracked**
5. **show ip igmp snooping vlan** *vlan-ID*

手順の詳細

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 show ip igmp snooping vlan *vlan-ID*

例：

```
Device# show ip igmp snooping vlan 77
```

Catalyst VLAN のスヌーピング情報を表示します。

```
Device# show  ip igmp  snooping vlan  77

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping              : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 77:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Explicit host tracking               : Enabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
Device#
```

ステップ 3 **show ip igmp groups** *interface-type interface-number*

例：

```
Device# show ip igmp groups GigabitEthernet 1/0/24
```

デバイスに直接接続されていて、IGMP を介して学習するマルチキャスト グループを表示します。

```
show ip igmp groups GigabitEthernet 1/0/24

IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter   Group Accounted
203.0.113.245    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.244    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.247    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.246    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.241    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.240    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.243    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.242    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.253    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.252    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.221    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.254    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.249    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.248    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.251    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.250    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.228    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.229    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.230    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.231    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
203.0.113.224    GigabitEthernet1/0/24    00:00:35  stopped   10.34.34.2
```

ステップ 4 **show ip igmp membership tracked**

例：

```
Device# show ip igmp membership tracked
```

有効にした明示的なトラッキング機能を使用してマルチキャスト グループを表示します。

```
Device# show ip igmp  membership tracked

Flags: A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, U - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP, the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (G))
Reporter:
       <mac-or-ip-address> - last reporter if group is not explicitly tracked
       <n>/<m>      - <n> reporter in include mode, <m> reporter in exclude

 Channel/Group                 Reporter        Uptime   Exp.  Flags  Interface
 *,203.0.113.10                 1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.10       10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.11                 1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.11       10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.14                 1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.14       10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.15                 1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.15       10.34.34.2      00:20:46 02:59 T      Gi1/0/24
```

```
 *,203.0.113.12                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.12        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.13                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.13        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.19                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.19        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.18                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.18        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.17                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.17        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.16                  1/0             00:20:46 stop  3AT    Gi1/0/24
 192.168.0.2,203.0.113.16        10.34.34.2      00:20:46 02:59 T      Gi1/0/24
 *,203.0.113.40                  0/1             00:20:48 02:16 3LAT   Gi1/0/24
 *,209.165.201.1                 10.34.34.1      00:20:48 02:16 3LT    Gi1/0/24
Device#
```

ステップ 5 show ip igmp snooping vlan *vlan-ID*

例：

```
Device# show ip igmp snooping vlan 77
```

VLAN 上の IGMP スヌーピング設定を表示します。

```
Device# show  ip igmp  snooping vlan  77

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping              : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 77:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Explicit host tracking               : Enabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
Device#
```

IGMP の明示的追跡に関するその他の関連情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)*

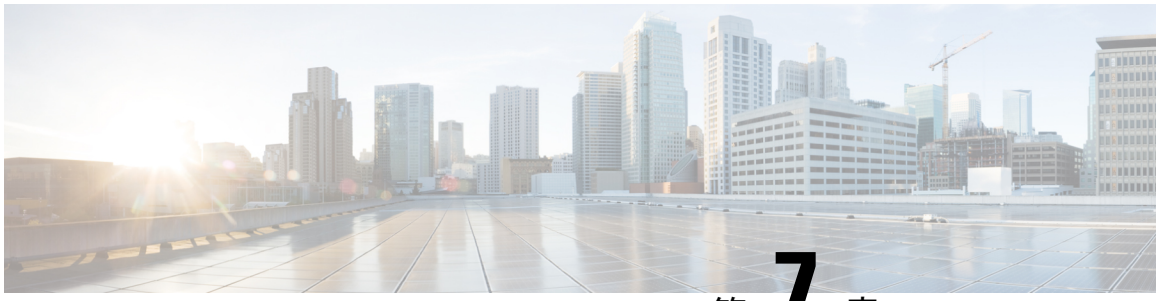
IGMP の明示的トラッキングの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	IGMP の明示的なトラッキング	IGMP の明示的なトラッキング機能を使用すると、特定のマルチアクセスネットワーク内のすべてのマルチキャストホストのメンバーシップをマルチキャストデバイスで明示的に追跡できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。



第 7 章

スイッチドイーサネットでの IP マルチキャストの抑制

スイッチドイーサネット ネットワークで IP マルチキャストを抑制するための前提条件

このモジュールの作業を実行する前に、IP マルチキャスト ルーティング テクノロジーの概要（1 ページ） モジュールで説明している概念をよく理解しておく必要があります。

スイッチドイーサネットネットワークでのIPマルチキャストについての情報

IP マルチキャスト トラフィックとレイヤ 2 スイッチ

レイヤ 2 スイッチのデフォルト動作では、スイッチ上の宛先 LAN に属する各ポートに、すべてのマルチキャスト トラフィックが転送されます。この動作では、スイッチの効率が低下します。その目的は、データを受信する必要があるポートへのトラフィックを制限することです。

この動作では、不要なマルチキャスト トラフィックを減らす抑制メカニズムが必要です。これによって、スイッチのパフォーマンスが改善されます。

Cisco Group Management Protocol（CGMP）、Router Group Management Protocol（RGMP）、および IGMP スヌーピングは、レイヤ 2 スイッチング環境で IP マルチキャストを効果的に抑制します。

- CGMP および IGMP スヌーピングは、エンド ユーザーまたはレシーバ クライアントが含まれているサブネットで使用されます。
- RGMP は、コラプスト バックボーンなどのルータのみに含まれているルーティング対象セグメントで使用されます。
- RGMP と CGMP は相互運用できません。ただし、インターネット グループ管理プロトコル（IGMP）は、CGMP および RGMP スヌーピングと相互運用できます。

IP マルチキャスト用の Catalyst スイッチの CGMP

CGMP は、IGMP によって実行される作業と同様の作業を実行するために、Catalyst スイッチに接続されたデバイスで使用される、シスコが開発したプロトコルです。IP マルチキャスト データ パケットと IGMP レポート メッセージ（いずれも MAC レベルで同じグループ アドレスにアドレス指定されます）を区別しない Catalyst スイッチの場合、CGMP が必要になります。スイッチは IGMP パケットを区別できますが、スイッチ上でソフトウェアを使用する必要があり、これがパフォーマンスに大きな影響を与えます。

マルチキャスト デバイスとレイヤ 2 スイッチで CGMP を設定する必要があります。結果的に CGMP では、該当するレシーバに接続されている Catalyst スイッチのポートにだけ IP マルチキャスト トラフィックが提供されます。トラフィックを明示的に要求していない他のすべてのポートは、これらのポートがマルチキャスト ルータに接続されていない限り、トラフィックを受信しません。マルチキャスト ルータ ポートは、すべての IP マルチキャスト データ パケットを受信する必要があります。

マルチキャスト グループに加入するとき、ホストは CGMP を使用して、送信要求されなくてもターゲット グループへの IGMP メンバーシップ レポート メッセージをマルチキャストします。通常の IGMP 処理では、IGMP レポートが、スイッチを介してルータに渡されます。ルータ（このインターフェイス上で CGMP がイネーブルにされている必要がある）では、IGMP レポートを受信し、通常どおりに処理されますが、CGMP 加入メッセージも作成され、スイッチに送信されます。Join メッセージには、エンド ステーションの MAC アドレスと加入したグループの MAC アドレスが含まれます。

スイッチは、CGMP Join メッセージを受信し、そのマルチキャスト グループ用の連想メモリ（CAM）テーブルにポートを追加します。以後、このマルチキャスト グループに対するすべての後続のトラフィックは、そのホストのポートに転送されます。

レイヤ 2 スイッチは、いくつかの宛先 MAC アドレスを 1 つの物理ポートに割り当てることができるよう、設計されています。この設計により、スイッチを階層構造で接続できるようになります。また、多数のマルチキャスト宛先アドレスを単一ポートに転送できます。

デバイス ポートは、マルチキャスト グループのエントリにも追加されます。IGMP コントロール メッセージもマルチキャスト トラフィックとして送信されるため、マルチキャスト デバイスは、各グループに対するすべてのマルチキャスト トラフィックをリッスンします。その他のマルチキャスト トラフィックは、CGMP で作成された新しいエントリを含む CAM テーブルを使用して転送されます。

IGMP スヌーピング

IGMP スヌーピングは、レイヤ 2 LAN スイッチで実行される IP マルチキャスト抑制メカニズムです。IGMP スヌーピングでは、ホストとルータとの間で送信される IGMP パケットで、一部のレイヤ 3 情報（IGMP Join/Leave メッセージ）を調査、すなわち「スヌープ」します。スイッチでは、特定のマルチキャスト グループに対するホストから IGMP ホスト レポートを受信するときに、関連付けられているマルチキャスト テーブル エントリにホストのポート番号が追加されます。スイッチがホストから IGMP グループ脱退メッセージを受信すると、スイッチはホストのテーブル エントリを削除します。

IGMP 制御メッセージはマルチキャスト パケットとして送信されるので、レイヤ 2 ではマルチキャスト データと区別できません。IGMP スヌーピングを実行しているスイッチでは、各マルチキャスト データ パケットを検査し、永続的な IGMP コントロール情報が含まれているかどうかを特定できます。低速の CPU を搭載したローエンドのスイッチに IGMP スヌーピングを実装すると、データが高速で送信される場合に、パフォーマンスに重大な影響を与える可能性があります。解決策として、ハードウェアで IGMP チェックを実行できる特別な ASIC（特定用途向け集積回路）を備えたハイエンドのスイッチに IGMP スヌーピングを実装します。CGMP は特別なハードウェアを使用しない、ローエンドのスイッチのための新しいオプションです。

Router-Port Group Management Protocol（RGMP）

CGMP および IGMP スヌーピングは、アクティブなレシーバがあるルーティング対象ネットワーク セグメントで動作するように設計されている、IP マルチキャスト抑制メカニズムです。両方とも、ホストとルータとの間で送信される IGMP コントロール メッセージに依存して、該当する受信先に接続されているスイッチ ポートが特定されます。

スイッチド イーサネット バックボーン ネットワーク セグメントは、通常、そのセグメント上にホストなしでスイッチに接続されているいくつかのルータで構成されています。ルータでは IGMP ホスト レポートが生成されないため、CGMP および IGMP スヌーピングによって、マルチキャスト トラフィックを抑制することができず、VLAN 上の各ポートにフラッディングされます。ルータでは、代わりに、Protocol Independent Multicast（PIM）メッセージが生成され、レイヤ 3 レベルで、マルチキャスト トラフィック フローに加入またはマルチキャスト トラフィック フローがプルーニングされます。

Router-Port Group Management Protocol（RGMP）は、ルータのみのネットワーク セグメントに対する、IP マルチキャスト抑制メカニズムです。RGMP は、ルータ上およびレイヤ 2 スイッチ上でイネーブルにする必要があります。マルチキャスト ルータは、特定のグループに RGMP Join メッセージを送信することによって、データ フローを受信したいことを示します。次に、CGMP Join メッセージの処理方法と同様に、スイッチによって、そのマルチキャスト グループに対する転送テーブルに、適切なポートが追加されます。IP マルチキャスト データ フローは、

関連するルータ ポートにのみ転送されます。ルータがそのデータ フローを必要としなくなった場合、RGMP Leave メッセージを送信し、スイッチは転送エントリを削除します。

RGMP 対応されていないルータがある場合は、すべてのマルチキャスト データを受信し続けます。

スイッチドイーサネットネットワークでマルチキャストを抑制する例

IP マルチキャスト用のスイッチの設定

マルチキャスト ネットワークにスイッチングがある場合、IP マルチキャストの設定方法の詳細について、使用しているスイッチのマニュアルを参照してください。

IGMP スヌーピングの設定

ルータ上での設定は不要です。使用しているスイッチで IGMP スヌーピングをイネーブルにする方法についてはドキュメントを参照し、提示された手順に従ってください。

CGMP のイネーブル化

CGMP は、IGMP によって実行される作業と同様の作業を実行するために、Catalyst スイッチに接続されたデバイス上で使用されるプロトコルです。CGMP が必要となるのは、Catalyst スイッチで IP マルチキャスト データ パケットと IGMP レポート メッセージを区別できないためです。これらはともに MAC レベルで、同じグループ アドレスにアドレス指定されます。

（注）
- CGMP は 802 または ATM メディア、または ATM 経由の LAN エミュレーション（LANE）でのみイネーブルにする必要があります。
- CGMP は、Catalyst スイッチに接続されているデバイス上でのみ、イネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip cgmp** [**proxy** | **router-only**]
5. **end**
6. **clear ip cgmp** [*interface-type interface-number*]

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	**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	**interface** *type number* 例： `Device(config)# interface ethernet 1`	IGMPv3 をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 4	**ip cgmp** [**proxy** | **router-only**] 例： `Device(config-if)# ip cgmp proxy`	Cisco Catalyst 5000 ファミリ スイッチに接続されているデバイスのインターフェイス上で CGMP をイネーブルにします。 • **proxy** キーワードは、CGMP プロキシ機能をイネーブルにします。イネーブルにすると、CGMP 対応でないデバイスがプロキシルータによってアドバタイズされます。プロキシルータでは、非 CGMP 対応デバイスの MAC アドレスおよびグループ アドレス 0000.0000.0000 が使用されている CGMP Join メッセージを送信することによって、他の非CGMP 対応デバイスの存在がアドバタイズされます。
ステップ 5	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーションセッションを終了して、EXEC モードに戻ります。
ステップ 6	**clear ip cgmp** [*interface-type interface-number*] 例： `Device# clear ip cgmp`	（任意）Catalyst スイッチのキャッシュからすべてのグループ エントリをクリアします。

レイヤ 2 スイッチド イーサネット ネットワークでの IP マルチキャストの設定

RGMP を使用してレイヤ 2 スイッチド イーサネット ネットワークで IP マルチキャストを設定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip rgmp**
5. **end**
6. **debug ip rgmp**
7. **show ip igmp interface**

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	**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	**interface** *type number* 例： `Device(config)# interface ethernet 1`	ホストに接続されているインターフェイスを選択します。
ステップ 4	**ip rgmp** 例： `Device(config-if)# ip rgmp`	イーサネット インターフェイス、ファスト イーサネット インターフェイス、およびギガビット イーサネットインターフェイスで、RGMP をイネーブルにします。
ステップ 5	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーションセッションを終了して、EXEC モードに戻ります。
ステップ 6	**debug ip rgmp** 例：	（任意）RGMP 対応デバイスによって送信されたデバッグ メッセージを記録します。

	コマンドまたはアクション	目的
	`Device# debug ip rgmp`	
ステップ 7	**show ip igmp interface** 例： `Device# show ip igmp interface`	（任意）インターフェイスに関するマルチキャスト関連情報を表示します。

スイッチド イーサネット ネットワークで IP マルチキャストを抑制する設定例

RGMP の設定例

次に、ルータ上で RGMP を設定する方法の例を示します。

```
ip multicast-routing
ip pim sparse-mode
interface ethernet 0
 ip rgmp
```

スイッチドイーサネットネットワークでのIPマルチキャスト抑制に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)*

MIB

MIB	MIB のリンク
これらの機能によってサポートされる新しい MIB または変更された MIB はありません。またこれらの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB を検索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

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

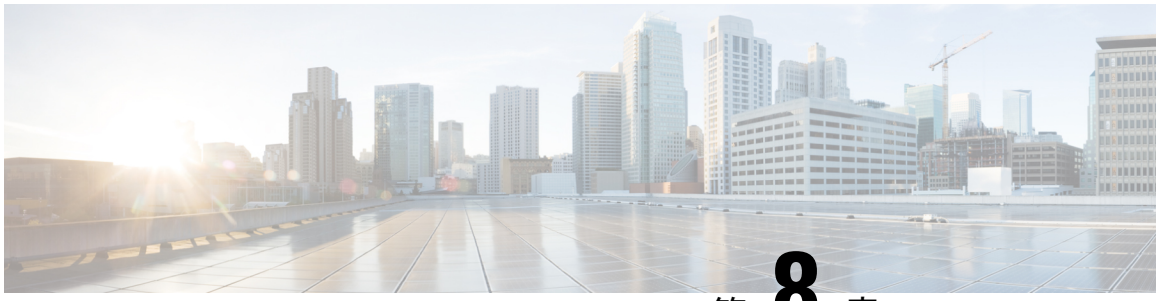
スイッチドイーサネットでのIPマルチキャスト抑制の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	スイッチドイーサネットでの IP マルチキャストの抑制	スイッチドイーサネットでの IP マルチキャストでは、不要なマルチキャストトラフィックを減らす抑制メカニズムが提供され、スイッチのパフォーマンスが向上します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。



第 8 章

PIM（Protocol Independent Multicast）の設定

PIM の前提条件

PIM 設定プロセスを開始する前に、使用する PIM モードを決定します。この決定は、ネットワーク上でサポートするアプリケーションに基づきます。次の注意事項に従ってください。

- 一般に、本質的に 1 対多または多対多アプリケーションでは PIM-SM を正常に使用できます。
- 1 対多アプリケーションで最適なパフォーマンスを得るには、SSM が適しています。ただし、IGMP バージョン 3 サポートが必要です。

PIM スタブ ルーティングを設定する前に、次の条件を満たしていることを確認します。

- スタブ ルータと中央のルータの両方に IP 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。スタブルータのアップリンク インターフェイスで、PIM モードの設定も必要です。
- また、デバイスに Enhanced Interior Gateway Routing Protocol（EIGRP）スタブルーティングまたは Open Shortest Path First（OSPF）スタブルーティング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。

PIM に関する制約事項

次に、PIM を設定する際の制約事項を示します。

- ACLにより、指定のポートをマルチキャストルータポートではなく、マルチキャストホストポートとしてだけ指定できます。このポートで受信されたマルチキャストルータ制御パケットは、ドロップされます。
- PIM非ブロードキャストマルチアクセス（NBMA）モードは、イーサネットインターフェイスではサポートされません。
- Hot Standby Router Protocol（HSRP）対応の PIM がサポートされます。

PIMv1 および PIMv2 の相互運用性

デバイス上でのマルチキャストルーティングの設定ミスを回避するには、ここに記載する情報を確認してください。

シスコの PIMv2 実装を使用すると、バージョン 1 とバージョン 2 間での相互運用性および変換が可能となります。ただし、若干の問題が発生する場合もあります。

PIMv2 に差分的にアップグレードできます。PIM バージョン 1 および 2 を、1 つのネットワーク内の異なるルータおよびマルチレイヤ スイッチに設定できます。内部的には、共有メディア ネットワーク上のすべてのルータおよびマルチレイヤ スイッチで同じ PIM バージョンを実行する必要があります。したがって、PIMv2デバイスがPIMv1デバイスを検出した場合は、バージョン1デバイスがシャットダウンするかアップグレードされるまで、バージョン2デバイスはバージョン 1 にダウングレードされます。

PIMv2 は BSR を使用して各グループ プレフィックスの RP 設定情報を検出し、PIM ドメイン内のすべてのルータおよびマルチレイヤ スイッチにアナウンスします。自動 RP 機能を組み合わせることにより、PIMv2 BSR と同じ作業を PIMv1 で実行できます。ただし、自動 RP は PIMv1 から独立している、スタンドアロンのシスコ独自のプロトコルで、PIMv2 は IETF 標準の追跡プロトコルです。

（注） したがって、PIMv2の使用を推奨します。BSR機能は、Ciscoルータおよびマルチレイヤスイッチ上の Auto-RP と相互運用します。

PIMv2デバイスをPIMv1デバイスと相互運用させる場合は、自動RPを事前に導入しておく必要があります。自動 RP マッピング エージェントでもある PIMv2 BSR は、自動 RP で選択され

た RP を自動的にアドバタイズします。つまり、自動 RP によって、グループ内のルータまたはマルチレイヤごとに 1 つの RP が設定されます。ドメイン内のルータおよびスイッチの中には、複数の RP を選択するために PIMv2 ハッシュ機能を使用しないものもあります。

PIMv1 の自動 RP 機能は PIMv2 RP 機能と相互運用するため、PIMv1 と PIMv2 が混在する領域内に SM グループを設定できます。すべての PIMv2 デバイスで PIMv1 を使用できますが、RP を PIMv2 にアップグレードすることを推奨します。PIMv2 への移行を簡単に行うには、以下を推奨します。

- 領域全体で Auto-RP を使用します。

自動 RP がまだ PIMv1 領域に設定されていない場合は、自動 RP を設定してください。

双方向 PIM に関する制約事項

ファントム ランデブー ポイント（RP）はサポートされていません。

PIM スタブ ルーティングの設定に関する制約事項

- 直接接続されたマルチキャスト（IGMP）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。
- PIM スタブルーティングを使用するネットワークでは、ユーザーに対する IP 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デバイス経由です。
- 冗長 PIM スタブ ルータ トポロジーはサポートされません。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。

Auto-RP および BSR の設定に関する制約事項

Auto-RP および BSR を設定する場合は、ネットワーク設定と次の制約事項を考慮してください。

Auto-RP の制約事項

次に、Auto-RP の設定に関する制約事項を示します（ネットワーク設定で使用する場合）。

- ルーテッド インターフェイスが SM に設定されていると、すべてのデバイスが自動 RP グループの手動 RP アドレスによって設定されている場合も、自動 RP を使用できます。
- ルーテッドインターフェイスが SM で設定され、**ip pim autorp listener** グローバル コンフィギュレーション コマンドを入力する場合、すべてのデバイスが Auto-RP グループの手動 RP アドレスを使用して設定されていなくても、Auto-RP は引き続き使用できます。

BSR 設定の制約事項

次に、BSR の設定に関する制約事項を示します（ネットワーク設定で使用する場合）。

- 候補 BSR を自動 RP 用の RP マッピング エージェントとして設定します。
- グループ プレフィックスが自動 RP によってアドバタイズされた場合は、異なる RP セットによって処理されたこれらのグループ プレフィックスのサブ範囲が、PIMv2 BSR メカニズムによってアドバタイズされないようにする必要があります。PIMv1 および PIMv2 ドメインが混在する環境では、バックアップ RP で同じグループ プレフィックスが処理されるように設定します。このようにすると、RP マッピング データベースの最長一致検索によって、PIMv2 DR はこれらの PIMv1 DR から異なる RP を選択できなくなります。

Auto-RP および BSR の注意事項と制限事項

次に、Auto-RP および BSR の設定に関する制約事項を示します（ネットワーク設定で使用する場合）。

- 使用しているネットワークがすべて Cisco ルータおよびマルチレイヤ スイッチである場合は、自動 RP または BSR のいずれかを使用できます。
- ネットワークに他社製のルータがある場合は、BSR を使用する必要があります。
- Cisco PIMv1 および PIMv2 ルータとマルチレイヤ スイッチ、および他社製のルータがある場合は、自動 RP と BSR の両方を使用する必要があります。ネットワークに他のベンダー製のルータが含まれる場合には、シスコの PIMv2 デバイス上に自動 RP マッピング エージェントと BSR を設定します。BSR と他社製の PIMv2 デバイス間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。

（注） PIMv2 は 2 つの方法で使用できます。1 つはバージョン 2 をネットワーク内で排他的に使用する方法、もう 1 つは PIM バージョンの混在環境を採用してバージョン 2 に移行する方法です。

- ブートストラップ メッセージはホップ単位で送信されるため、PIMv1 デバイスの場合、これらのメッセージはネットワーク内の一部のルータおよびマルチレイヤ スイッチに到達しません。このため、ネットワーク内に PIMv1 デバイスがあり、Cisco ルータおよびマルチレイヤ スイッチだけが存在する場合は、自動 RP を使用してください。
- ネットワーク内に他社製のルータが存在する場合は、Cisco PIMv2 ルータまたはマルチレイヤ スイッチに自動 RP マッピング エージェントおよび BSR を設定します。BSR と他社製の PIMv2 ルータ間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。
- シスコ PIMv1 ルータおよびマルチレイヤ スイッチと他社製の PIMv2 ルータを相互運用させる場合は、自動 RP と BSR の両方が必要です。シスコ PIMv2 デバイスを、自動 RP マッピング エージェントと BSR の両方に設定してください。

Auto-RP 拡張の制約事項

Auto-RP とブートストラップ ルータ（BSP）の同時配備はサポートされていません。

PIM に関する情報

Protocol Independent Multicast の概要

PIM（Protocol Independent Multicast）プロトコルは、受信側が開始したメンバーシップの現在の IP マルチキャスト サービス モードを維持します。PIM は、特定のユニキャスト ルーティング プロトコルに依存しません。つまり、IP ルーティング プロトコルに依存せず、ユニキャスト ルーティング テーブルへの入力に使用されるユニキャスト ルーティング プロトコル（Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、Border Gateway Protocol（BGP）、および スタティック ルート）のいずれも利用できます。PIM は、ユニキャスト ルーティング情報を使用してマルチキャスト転送機能を実行します。

PIM はマルチキャスト ルーティング テーブルと呼ばれていますが、実際には完全に独立したマルチキャスト ルーティング テーブルを作成する代わりに、ユニキャスト ルーティング テーブルを使用してリバース パス フォワーディング（RPF）チェック機能を実行します。他のルーティング プロトコルとは異なり、PIM はルータ間のルーティング アップデートを送受信しません。

PIMは、RFC 4601 の Protocol Independent Multicast - Sparse Mode（PIM-SM）で定義されています。

PIM のバージョン

PIMv2 は、PIMv1 と比べて次の点が改善されています。

- マルチキャスト グループごとに、複数のバックアップ ランデブー ポイント（RP）を持つアクティブな RP が 1 つ存在します。この単一の RP で、PIMv1 内の同じグループにアクティブな RP が複数ある場合と同様の処理を行います。
- ブートストラップルータ（BSP）は耐障害性のある、自動化された RP ディスカバリメカニズム、および配信機能を提供します。これらの機能により、ルータおよびマルチレイヤスイッチはグループ/RP マッピングを動的に取得できます。
- PIM の Join メッセージおよびプルーニング メッセージを使用すると、複数のアドレス ファミリを柔軟に符号化できます。
- 現在以降の機能オプションを符号化するため、クエリー パケットではなく、より柔軟な hello パケット形式が使用されています。
- RPに送信される登録メッセージが、境界ルータによって送信されるか、あるいは指定ルータによって送信されるかを指定します。
- PIM パケットは IGMP パケット内に格納されず、独立したパケットとして処理されます。

Multicast Source Discovery Protocol（MSDP）

Multicast Source Discovery Protocol（MSDP）は、PIM SM を使用する場合のドメイン間送信元検出に使用されます。各 PIM 管理ドメインには独自の RP があります。あるドメイン内の RP が他のドメイン内の RP に新しい送信元を信号で伝えるために、MSDP が使用されます。

MSDP が設定されている状態で、あるドメイン内の RP が新しい送信元の PIM 登録メッセージを受信すると、その RP は、新しい Source-Active（SA）メッセージを他のドメイン内のすべての MSDP ピアに送信します。それぞれの中間 MSDP ピアは、この SA メッセージを発信側の RP から離してフラッディングします。MSDP ピアは、この SA メッセージを自身の MSDP sa-cache にインストールします。他のドメイン内の RP が SA メッセージに記述されているグループへの加入要求を持っている場合（空でない発信インターフェイス リストで (*,G) エントリが存在することで示される）、そのグループはドメインの対象となり、RP から送信元方向に (S,G) Join メッセージが送信されます。

PIM スパース モード（PIM-SM）

PIM スパース モード（PIM-SM）は、プル モデルを使用してマルチキャスト トラフィックを配信します。明示的にデータを要求したアクティブなレシーバを含むネットワーク セグメントだけがトラフィックを受信します。

スパース モードのインターフェイスは、ダウンストリームのルータから定期的に加入メッセージを受信する場合またはインターフェイスに直接接続のメンバがある場合のみマルチキャスト ルーティング テーブルに追加されます。LAN から転送する場合、グループが認識している RP があれば、SM 動作が行われます。その場合、パケットはカプセル化され、その RP に送信されます。特定のソースからのマルチキャスト トラフィックが十分である場合、レシーバのファースト ホップ ルータは、ソース ベースのマルチキャスト配信ツリーを構築するために加入メッセージをソースに向けて送信できます。

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 は少なくとも最初は共有ツリーを使用するので、ランデブー ポイント（RP）を使用する必要があります。RP は管理上メットワークで設定されている必要があります。詳細については、ランデブー ポイント（153 ページ）を参照してください。

スパース モードでは、ルータは、トラフィックに対する明示的な要求がない限り、他のルータはグループのマルチキャスト パケットを転送しないと見なします。ホストがマルチキャスト グループに加入すると、直接接続されたルータは RP に PIM 加入メッセージを送信します。RP はマルチキャスト グループを追跡します。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 ルータによって RP に登録されます。その後、RP は、ソースに加入メッセージを送信します。この時点で、パケットが共有配信ツリー上で転送されます。特定のソースからのマルチキャスト トラフィックが十分である場合、ホストのファースト ホップ ルータは、ソース ベースのマルチキャスト配信ツリーを構築するために加入メッセージをソースに向けて送信できます。

送信元が RP に登録され、データは共有ツリーを下ってレシーバに転送されます。エッジ ルータは、RP を介してソースから共有ツリーでデータ パケットを受信するときに、そのソースについて学習します。次に、エッジ ルータは、そのソースに向けて PIM (S, G)加入メッセージを送信します。リバース パスに沿った各ルータは、RP アドレスのユニキャスト ルーティング メ

トリックをソースアドレスのメトリックと比較します。送信元アドレスのメトリックの方が良い場合は、ソースに向けて PIM（S, G）加入メッセージを転送します。RP のメトリックと同じ、または RP のメトリックの方が良い場合は、RP と同じ方向に PIM (S, G)加入メッセージが送信されます。この場合、共有ツリーとソース ツリーは一致すると見なされます。

共有ツリーがソースとレシーバの間の最適なパスでない場合、ルータは動的にソース ツリーを作成し、共有ツリーの下方向へのトラフィック フローを停止します。この動作は、ソフトウェアのデフォルトの動作です。ネットワーク管理者は、**ip pim spt-threshold infinity** コマンドを使用して、トラフィックを強制的に共有ツリー上で保持することができます。

PIM-SM は、WAN リンク付きのネットワークを含む、任意のサイズのネットワークに合わせて拡大または縮小します。明示的な加入メカニズムによって、不要なトラフィックが WAN リンクでフラッディングするのを防ぎます。

双方向 PIM

双方向 PIM は、IP マルチキャスト用ルーティングプロトコルの PIM スイートのバリアントです。PIM では、マルチキャスト グループのパケット トラフィックは、そのマルチキャスト グループのために設定されたモードのルールに従ってルーティングされます。

双方向モードでは、トラフィックは、グループのランデブー ポイント（RP）をルートとする双方向共有ツリーに沿ってのみ、ルーティングされます。Bidir-PIM では、RP の IP アドレスは、すべてのルータがその IP アドレスをルートとするループフリーのスパニングツリー トポロジを確立するうえで重要な役割を果たします。この IP アドレスはルータである必要はなく、PIM ドメイン内のどこからでも到達可能なネットワーク上の任意の未割り当て IP アドレスを使用できます。この技術は、Bidir-PIM の冗長 RP 設定を確立するための優先設定方式です。

双方向グループに対するメンバーシップは、明示的な加入メッセージを通じて伝えられます。ソースからのトラフィックは、無条件で、共有ツリーの上方向にある RP に向けて送信され、ツリーの下方向にある各ブランチ上のレシーバに渡されます。

Bidir-PIM は、各 PM ドメイン内の多対多のアプリケーションで使用するよう設計されています。双方向モードのマルチキャスト グループは、ソースの数によるオーバーヘッドを引き起こすことなく、任意の数のソースに拡張できます。

PIM-SM は、トラフィックを 1 つのリバース パス フォワーディング（RPF）インターフェイスからのみ受け入れるため、ツリーのアップストリーム方向にトラフィックを転送できません。（共有ツリーの）このインターフェイスは RP 方向を指し、そのため、ダウンストリーム トラフィック フローのみを許可します。この場合、アップストリーム トラフィックはまずユニキャスト登録メッセージにカプセル化され、これが送信元の指定ルータ（DR）から RP に渡されます。次に、RP が送信元をルートとする SPT に加入します。したがって、PIM-SM では、RP に宛てられた送信元からのトラフィックは、共有ツリー内でアップストリームにはフローしませんが、送信元の SPT に沿って RP に到達するまでダウンストリームでフローします。RP から、トラフィックは共有ツリーに沿ってすべてのレシーバに向けてフローします。

Bidir-PIM は PIM SM のメカニズムから派生しており、多くの最短パスツリー（SPT）動作を共有しています。Bidir-PIM にも、共有ツリー上で送信元から RP に向けてアップストリーム トラフィックを無条件に転送する機能がありますが、PIM-SM のような送信元の登録プロセスはありません。これらの変更は、すべてのルータで (*, G) マルチキャスト ルーティング エント

リだけに基づいてトラフィックを転送できるようにするには、必要にして十分なものです。この機能では、ソース固有のステートは不要であり、スケーリング機能を使用して任意の数のソースに対応できます。下の図は、単方向共有ツリーや送信元ツリーの場合と双方向共有ツリーの場合とを比較し、ルータごとの状態の違いを示しています。

図 *10* : 単方向共有ツリーおよびソース ツリー

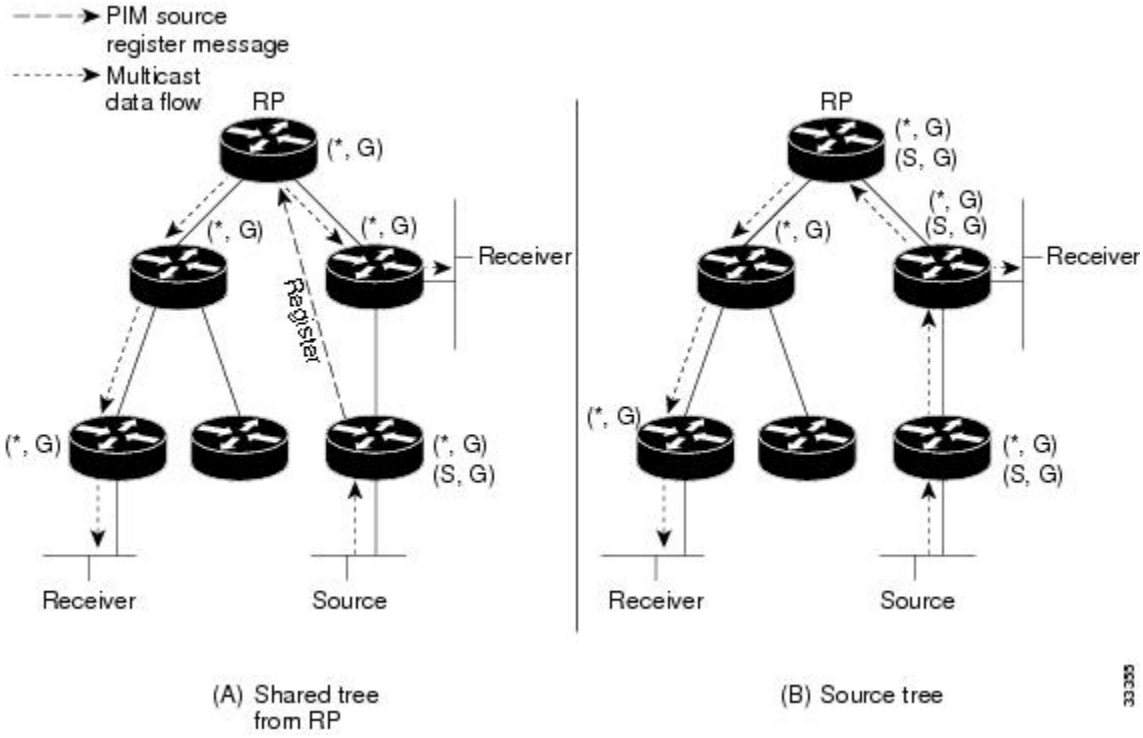
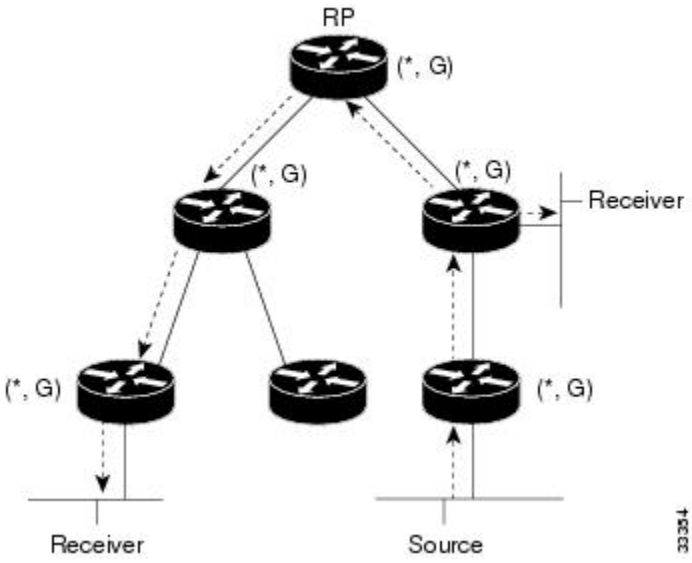


図 *11* : 双方向共有ツリー



バケットがRPから受信側方向へダウンストリームで転送される場合、Bidir-PIMとPIM-SMの間で基本的な違いはありません。送信元からアップストリームでRP方向に送られるトラフィックの場合、Bidir-PIMはPIM-SMと大きく異なります。

Bidir-PIMでは、パケット転送ルールがPIM-SMから改善され、トラフィックを、共有ツリーを通ってRP方向にアップストリームに送れるようになりました。マルチキャストパケットループィングを避けるために、Bidir-PIMは指定フォワーダ（DF）選定と呼ばれる新しいメカニズムを導入します。これは、RPをルートとするループフリーSPTを確立します。

指定フォワーダ選択

すべてのネットワークセグメントとポイントツーポイントリンクで、PIMルータはすべて指定フォワーダ（DF）選定と呼ばれる手順に参加します。この手順では、双方向グループのすべてのRPでDFとしてルータを1つ選定します。このルータは、そのネットワークで受信されたマルチキャストパケットをRPにアップストリームで転送します。

DF選定は、ユニキャストルーティングメトリックに基づいており、PIMアサートプロセスで採用されているものと同じタイブレークルールを使用します。RPへの最も望ましいユニキャストルーティングメトリックを持つルータがDFになります。この方法を使用することによって、RPへのパラレル等コストパスがある場合にも、すべてのパケットのコピー1つだけがRPに送信されます。

DFは双方向グループのすべてのRPに対して選定されます。結果として、ネットワークセグメント上で各RPに1つずつ複数のルータがDFとして選定されます。また、複数のインターフェイスで特定のルータがDFとして選定される場合があります。

双方向グループ ツリー ビルディング

双方向グループの共有ツリーへの加入手順は、PIM SMでの手順とほとんど同じです。1つ大きな違いは、双方向グループの場合、DRのロールがRPのDFによって仮定される点です。

ローカル受信先のあるネットワークでは、DFとして選定されたルータのみがInternet Group Management Protocol（IGMP）加入メッセージの受信時に発信インターフェイスリスト（olist）を読み込み、(*, G) 加入および脱退メッセージをRP方向にアップストリームに送信します。ダウンストリームルータが共有ツリーに参加したい場合、PIM加入および脱退メッセージのRPFネイバーが常にRPに向かうインターフェイスのDFに選定されます。

ルータが加入または脱退メッセージを受け取り、ルータが受信インターフェイスのDFでない場合、メッセージは無視されます。そうでない場合、ルータは共有ツリーをスパースモードと同じように更新します。

ルータがすべて双方向共有ツリーをサポートしているネットワークでは、(S, G) 加入および脱退メッセージは無視されます。DF選定手順はRPからパラレルダウンストリームパスをなくすため、PIMアサートメッセージを送信する必要もありません。また、RPは送信元へのパスに参加することなく、登録停止も送信しません。

パケット転送

ルータは双方向グループに対して (*, G) エントリのみを作成します。(*, G) エントリのolistには、ルータが選定されたDFであり、IGMPまたはPIM加入メッセージを受信したインター

フェイスがすべて含まれます。ルータが送信者専用ブランチにある場合、(*, G) ステートも作成されますが、olist にはいずれのインターフェイスも含まれません。

パケットを RP 方向の RPF インターフェイスから受信した場合、(*, G) エントリの olist に従って、パケットはダウンストリームに転送されます。それ以外の場合、受信インターフェイスの DF であるルータのみがパケットを RP 方向にアップストリームに転送します。その他のルータはすべてパケットを廃棄する必要があります。

IPv4 双方向 PIM

双方向 PIM の動作には、指定フォワーダが必要です。DF は、IPv4 双方向 PIM グループのセグメントへ、またセグメントからパケットを転送するよう選定されたルータです。DF モードでは、スイッチは RPF および DF インターフェイスからパケットを受け入れます。

スイッチが IPv4 双方向 PIM グループを転送するとき、RPF インターフェイスは常に（*,G）エントリの発信インターフェイス リストに含まれ、DF インターフェイスが含まれるエントリは IGMP/PIM Join に応じて決まります。

RP へのルートが使用できない場合、グループは dense モードに変更されます。RP への RPF リンクが使用できなくなると、IPv4 双方向 PIM フローはハードウェア FIB から削除されます。

PIM スタブ ルーティング

PIM スタブルーティング機能は、すべてのデバイス ソフトウェア イメージで使用でき、エンドユーザー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使用状況を低減させます。

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 IGMP トラフィックだけです。

PIM スタブルーティングを使用するネットワークでは、ユーザーに対する IP 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デバイス経由です。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（IGMP）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。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。

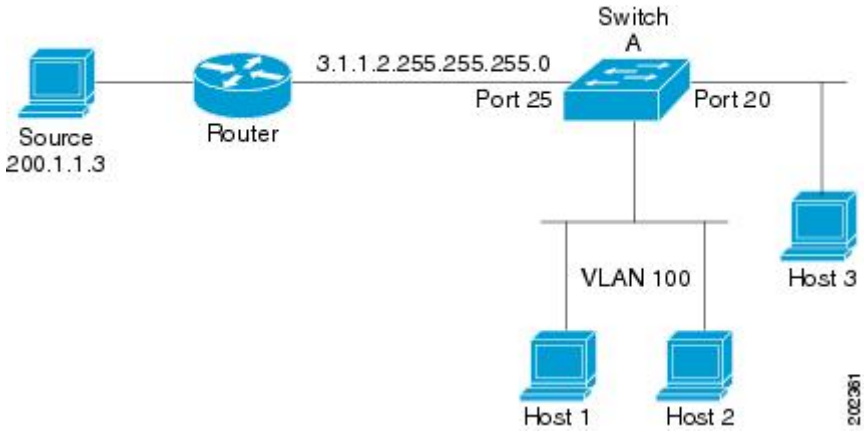
PIM スタブルーティングを使用しているときは、IP マルチキャストルーティングを使用し、デバイスだけを PIM スタブルータとして設定するように、分散ルータおよびリモートルータを設定する必要があります。デバイスは分散ルータ間の伝送トラフィックをルーティングしません。デバイスのルーテッド アップリンク ポートも設定する必要があります。SVI の場合は、デバイスのアップリンクポートを使用できません。SVI アップリンク ポートの PIM が必要な場合は、Network Advantage ライセンスにアップグレードする必要があります。

（注） また、デバイスで PIM スタブルーティングを設定するときは、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 資産および指定ルータ検出メカニズムは、PIM 受動インターフェイスで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。

図 *12 : PIM* スタブ ルータ設定

次の図では、デバイス A のルーテッド 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 で有効になっています。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 200.1.1.3 からトラフィックを受信できます。



ランデブー ポイント

ランデブー ポイント（RP）は、デバイスが PIM（Protocol Independent Multicast）スパース モード（SM）で動作している場合にデバイスが実行するロールです。RP が必要になるのは、PIM SM を実行しているネットワークだけです。PIM-SM モデルでは、マルチキャスト データを明示的に要求したアクティブなレシーバを含むネットワーク セグメントだけにトラフィックが転送されます。

RP は、マルチキャスト データのソースとレシーバの接点として機能します。PIM SIM ネットワークでは、ソースが RP にトラフィックを送信する必要があります。このトラフィックは、それから共有配信ツリーを下ってレシーバに転送されます。デフォルトでは、レシーバのファースト ホップ デバイスがソースを認識すると、ソースに Join メッセージを直接送信し、ソースからレシーバへのソース ベースの配信ツリーを作成します。ソースとレシーバ間の最短パス内に RP が配置されていない限り、このソース ツリーに RP は含まれません。

ほとんどの場合、ネットワークにおける RP の配置は複雑な判断を必要としません。デフォルトでは、RP が必要になるのは、ソースおよびレシーバとの新しいセッションを開始する場合だけです。その結果、RP では、トラフィックのフローまたは処理によるオーバーヘッドはほとんど発生しません。PIM バージョン 2 で実行される処理は PIM バージョン 1 よりも少なくなっています。これは、ソースを定期的に RP に登録するだけでステートを作成できるためです。

Auto-RP

PIM-SMの最初のバージョンでは、すべてのリーフルータ（ソースまたはレシーバに直接接続されたルータ）は、RP の IP アドレスを使用して手動で設定する必要がありました。このような設定は、スタティック RP 設定とも呼ばれます。スタティック RP の設定は、小規模のネットワークでは比較的容易ですが、大規模で複雑なネットワークでは困難を伴う可能性があります。

PIM-SM バージョン 1 の導入に続き、シスコは、Auto-RP 機能を備えた PIM-SM のバージョンを実装しました。Auto-RP は、PIM ネットワークにおけるグループから RP へのマッピングの配信を自動化します。Auto-RP には、次の利点があります。

- さまざまなグループにサービスを提供するために、ネットワーク内で複数の RP を設定することが比較的容易です。
- Auto-RP では、複数の RP 間で負荷を分散し、グループに加入するホストの場所に従って RP を配置できます。
- Auto-RP により、接続の問題の原因となる、矛盾した手動 RP 設定を回避できます。

複数の RP を使用して、異なるグループ範囲にサービスを提供したり、互いにバックアップとしての役割を果たしたりできます。Auto-RP が機能するためには、RP 通知メッセージを RP から受信して競合を解決する RP マッピング エージェントとしてルータが指定されている必要があります。その場合、RP マッピング エージェントは、グループから RP への一貫したマッピングを他のすべてのルータに送信します。これにより、すべてのルータは、サポート対象のグループに使用する RP を自動的に検出します。

（注） ルータ インターフェイスがスパース モードに設定されている場合、Auto-RP グループに対してすべてのルータが 1 つのスタティック アドレスで設定されているときは、引き続き Auto-RP グループを使用できます。

Auto-RP が機能するためには、RP 通知メッセージを RP から受信して競合を解決する RP マッピング エージェントとしてルータが指定されている必要があります。これにより、すべてのルータは、サポート対象のグループに使用する RP を自動的に検出します。インターネット割り当て番号局（IANA）は、224.0.1.39 と 224.0.1.40 という 2 つのグループ アドレスを Auto-RP 用に割り当てています。Auto-RP の利点の 1 つは、指定した RP に対するすべての変更は、RP であるルータ上で設定するだけで、リーフ ルータ上で設定する必要がないことです。Auto-RP のもう 1 つの利点は、ドメイン内で RP アドレスのスコープを設定する機能を提供することで

す。スコーピングを設定するには、Auto-RP アドバタイズメントに許容されている存続可能時間（TTL）値を定義します。

RP の各設定方式には、それぞれの長所、短所、および複雑度のレベルがあります。従来の IP マルチキャスト ネットワーク シナリオにおいては、Auto-RP を使用して RP を設定することを推奨します。Auto-RP は、設定が容易で、十分にテストされており、安定しているためです。代わりの方法として、スタティック RP、Auto-RP、およびブートストラップ ルータを使用して RP を設定することもできます。

PIM ネットワークでの Auto-RP の役割

Auto-RP は、PIM ネットワークにおけるグループからランデブー ポイント（RP）へのマッピングの配信を自動化します。Auto-RP が機能するためには、RP アナウンスメント メッセージを RP から受信して競合を解決する RP マッピング エージェントとしてデバイスが指定されている必要があります。

これにより、すべてのルータは、サポート対象のグループに使用する RP を自動的に検出します。インターネット割り当て番号局（IANA）は、224.0.1.39 と 224.0.1.40 という 2 つのグループ アドレスを Auto-RP 用に割り当てています。

マッピング エージェントは、Candidate-RP から RP になる意図の通知を受信します。その後、マッピング エージェントが RP 選定の結果を通知します。この通知は、他のマッピング エージェントによる決定とは別に行われます。

マルチキャスト境界

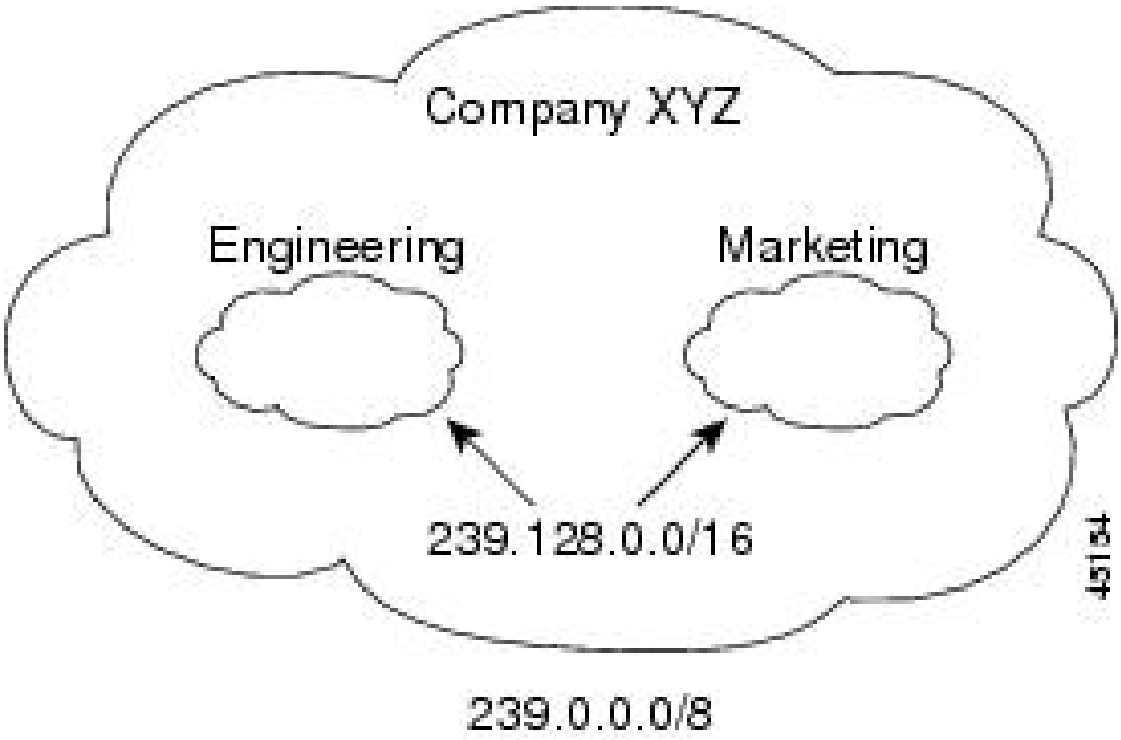
管理用スコープの境界を使用し、ドメインまたはサブドメイン外部へのマルチキャスト トラフィックの転送を制限できます。この方法では、「管理用スコープのアドレス」と呼ばれる特殊なマルチキャストアドレス範囲が境界のメカニズムとして使用されます。管理用スコープの境界をルーテッド インターフェイスに設定すると、マルチキャスト グループ アドレスがこの範囲内にあるマルチキャスト トラフィックは、このインターフェイスに出入りできず、このアドレス範囲内のマルチキャスト トラフィックに対するファイアウォール機能が提供されます。

（注） マルチキャスト境界および TTL しきい値は、マルチキャスドメインの有効範囲を制御しますが、TTL しきい値はこのデバイスではサポートされていません。ドメインまたはサブドメイン外部へのマルチキャスト トラフィックの転送を制限するには、TTL しきい値でなくマルチキャスト境界を使用する必要があります。

図 *13：* 管理用スコープの境界

次の図に、XYZ社が自社ネットワーク周辺にあるすべてのルーテッドインターフェイス上で、管理用スコープの境界をマルチキャスト アドレス範囲 239.0.0.0/8 に設定した例を示します。この境界では、239.0.0.0 ～ 239.255.255.255 の範囲のマルチキャスト トラフィックはネットワークに入ったり、外へ出ることができません。同様に、エンジニアリング部およびマーケティング部では、各自のネットワークの周辺で、管理用スコープの境界を 239.128.0.0/16 に設定しました。この境界では、239.128.0.0 ～ 239.128.255.255 の範囲のマルチキャスト トラフィックは、

それぞれのネットワークに入ったり、外部に出ることができません。



マルチキャスト グループ アドレスに対して、ルーテッド インターフェイス上に管理用スコープの境界を定義できます。影響を受けるアドレス範囲は、標準アクセスリストによって定義されます。この境界が定義されている場合、マルチキャスト データ パケットはいずれの方向であっても境界を通過できません。境界を定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

IANA は、マルチキャスト アドレス範囲 239.0.0.0 ～ 239.255.255.255 を管理用スコープのアドレスとして指定しました。このアドレス範囲は、異なる組織によって管理されたドメイン内で再利用できます。このアドレスはグローバルではなく、ローカルで一意であるとみなされます。

filter-autorp キーワードを設定して、管理用スコープの境界で Auto-RP 検出と通知メッセージを検査し、フィルタできます。境界のアクセス コントロール リスト（ACL）に拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

Auto-RP のスパース - デンス モード

Auto-RP の前提条件として、**ip pim sparse-dense-mode** 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すべてのインターフェイスをスパース-デンスモードで設定する必要があります。スパース-デンス モードで設定されたインターフェイスは、マルチキャスト グループの動作モードに応じてスパース モードまたはデンス モードで処理されます。マルチキャスト グループ内に既知の RP が存在する場合、インターフェイスはスパース モードで処理されま

す。グループ内に既知の RP が存在しない場合、デフォルトでは、インターフェイスはデンス モードで処理され、このインターフェイス上にデータがフラッディングされます（デンス モード フォールバックを回避することもできます。「Configuring Basic IP Multicast」モジュールを参照してください）。

Auto-RP を正常に実装し、224.0.1.39 および 224.0.1.40 以外のグループがデンス モードで動作することを回避するには、「シンク RP」（「ラストリゾート RP」とも呼ばれます）を設定することを推奨します。シンク RP は、ネットワーク内に実際に存在するかどうかわからない静的に設定された RP です。デフォルトでは、Auto-RP メッセージはスタティック RP 設定よりも優先されるため、シンク RP の設定は Auto-RP の動作と干渉しません。未知のソースや予期しないソースをアクティブにできるため、ネットワーク内の可能なすべてのマルチキャスト グループにシンク RP を設定することを推奨します。ソースの登録を制限するように設定された RP がない場合は、グループがデンス モードに戻り、データがフラッディングされる可能性があります。

Auto-RP のメリット

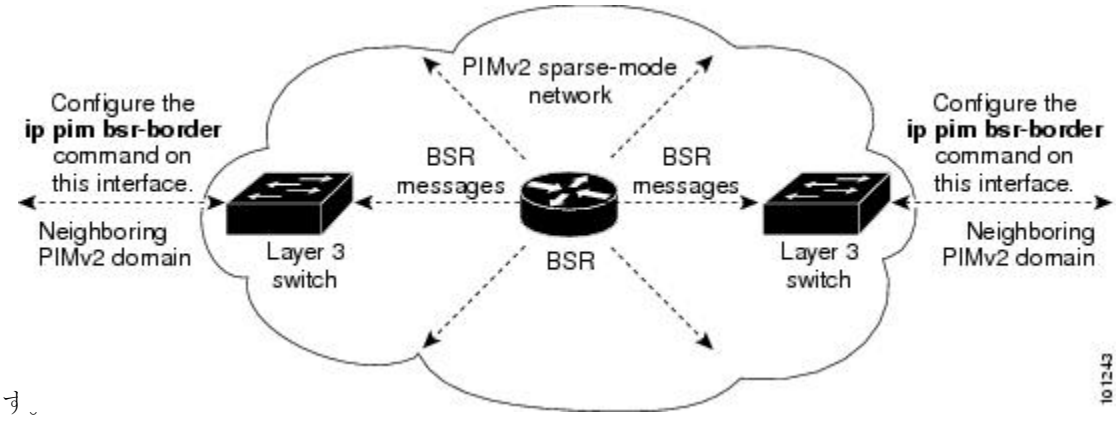
PIM ネットワークでの Auto-RP の利点

- Auto-RP では、RP 指定に対するすべての変更を、RP であるデバイス上でのみ設定されるようにし、リーフ ルータ上では設定されないようにすることができます。
- Auto-RP には、ドメイン内の RP アドレスのスコープを設定する機能があります。

PIM ドメイン境界

IP マルチキャストの普及に伴い、PIMv2 ドメインと別の PIMv2 ドメインが境界を挟んで隣接する場合が増えています。2 つのドメインは同じ RP、BSR、候補 RP、候補 BSR のセットを共有していないことが多いため、PIMv2 BSR メッセージがドメインの内外に流れないようにする必要があります。メッセージのドメイン境界通過を許可すると、通常の BSR 選択メカニズムに悪影響が及んだり、境界に位置するすべてのドメインで単一の BSR が選択されたり、候補 RP アドバタイズメントが混在し、間違ったドメイン内で RP が選択されたりします。

ip pim bsr-border コマンドを使用して PIM ドメインの境界を設定する方法を次の図に示します。



PIMv2 ブートストラップ ルータ

PIMv2 ブートストラップルータ（BSR）は、グループ/RP マッピング情報をネットワーク内のすべての PIM ルータおよびマルチレイヤデバイスに配信する別の方法です。これにより、ネットワーク内のルータまたはスイッチごとに RP 情報を手動で設定する必要がなくなります。ただし、BSR は IP マルチキャストを使用してグループ/RP マッピング情報を配信する代わりに、特殊な BSR メッセージをホップ単位でフラッディングしてマッピング情報を配信します。

BSR は、BSR として機能するように設定されたドメイン内の一連の候補ルータおよびスイッチから選択されます。選択メカニズムは、ブリッジングされた LAN で使用されるルートブリッジ選択メカニズムと類似しています。BSR の選択メカニズムの基準は、ネットワークを経由してホップ単位で送信される BSR メッセージに格納されている、デバイスの BSR プライオリティです。各 BSR デバイスは BSR メッセージを調べ、自身の BSR プライオリティよりも BSR プライオリティが同等以上で、BSR IP アドレスが大きなメッセージだけを、すべてのインターフェイスから転送します。この方法によって、BSR が選択されます。

選択された BSR によって、TTL 値が 1 である BSR メッセージが送信されます。隣接する PIMv2 ルータまたはマルチレイヤデバイス は BSR メッセージを受信し、TTL 値が 1 である他のすべてのインターフェイス（BSR メッセージの着信インターフェイスを除く）にマルチキャストします。この方法で、BSR メッセージは PIM ドメイン内をホップ単位で移動します。BSR メッセージには現在の BSR の IP アドレスが格納されているため、候補 RP はフラッディング メカニズムを使用し、どのデバイスが選択された BSR であるかを自動的に学習します。

候補 RP は候補 RP アドバタイズメントを送信し、対象となるグループ範囲を BSR に指示します。この情報は、ローカルな候補 RP キャッシュに格納されます。BSR はドメイン内の他のすべての PIM デバイスに、BSR メッセージ内のこのキャッシュの内容を定期的にアドバタイズします。これらのメッセージはネットワークをホップ単位で移動し、すべてのルータおよびスイッチに送信されます。BSR メッセージ内の RP 情報は、到達したルータおよびスイッチのローカルな RP キャッシュに格納されます。すべてのルータおよびスイッチには一般的な RP ハッシュ アルゴリズムが使用されるため、指定されたグループには同じ RP が選択されます。

マルチキャスト転送

マルチキャスト トラフィックの転送は、マルチキャスト対応ルータによって行われます。このようなルータは、すべてのレシーバにトラフィックを配信するために、IP マルチキャストがネットワーク上でたどるパスを制御する配信ツリーを作成します。

マルチキャスト トラフィックは、すべてのソースをグループ内のすべてのレシーバに接続する配信ツリー上で、ソースからマルチキャスト グループに流れます。このツリーは、すべてのソースで共有できます（共有ツリー）。または、各ソースに個別の配信ツリーを作成することもできます（ソース ツリー）。共有ツリーは一方向または双方向です。

ソース ツリーと共有ツリーの構造を説明する前に、マルチキャスト ルーティング テーブルで使用する表記について触れておきます。これらの表記には次のものが含まれます。

- (S, G) = (マルチキャスト グループ G のユニキャスト ソース, マルチキャスト グループ G)
- (*, G) = (マルチキャスト グループ G のすべてのソース, マルチキャスト グループ G)

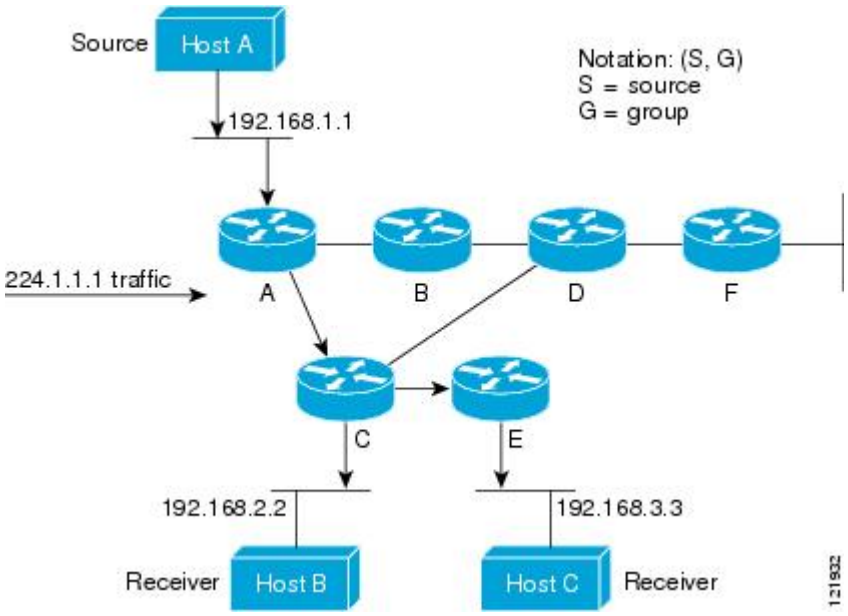
(S, G) という表記（「S カンマ G」と読みます）は、最短パス ツリーの列挙です。S はソースの IP アドレス、G はマルチキャスト グループ アドレスを表します。

共有ツリーは (*, G) で表されます。ソース ツリーは (S, G) で表され、常にソースでルーティングされます。

マルチキャスト配信のソース ツリー

マルチキャスト配信ツリーの最も単純な形式は、ソース ツリーです。ソース ツリーは、ソース ホストをルートとし、ネットワークを介してレシーバに接続するスパニングツリーを形成するブランチを持ちます。このツリーはネットワーク上での最短パスを使用するため、最短パス ツリー（SPT）とも呼ばれます。

次の図に、ソース（ホスト A）をルートとし、2 つのレシーバ（ホスト B およびホスト C）に接続するグループ 224.1.1.1 の SPT の例を示します。



標準表記を使用すると、図の例の SPT は（192.168.1.1, 224.1.1.1）となります。

(S, G) という表記は、各グループに送信する個々のソースに個別の SPT が存在することを意味します。

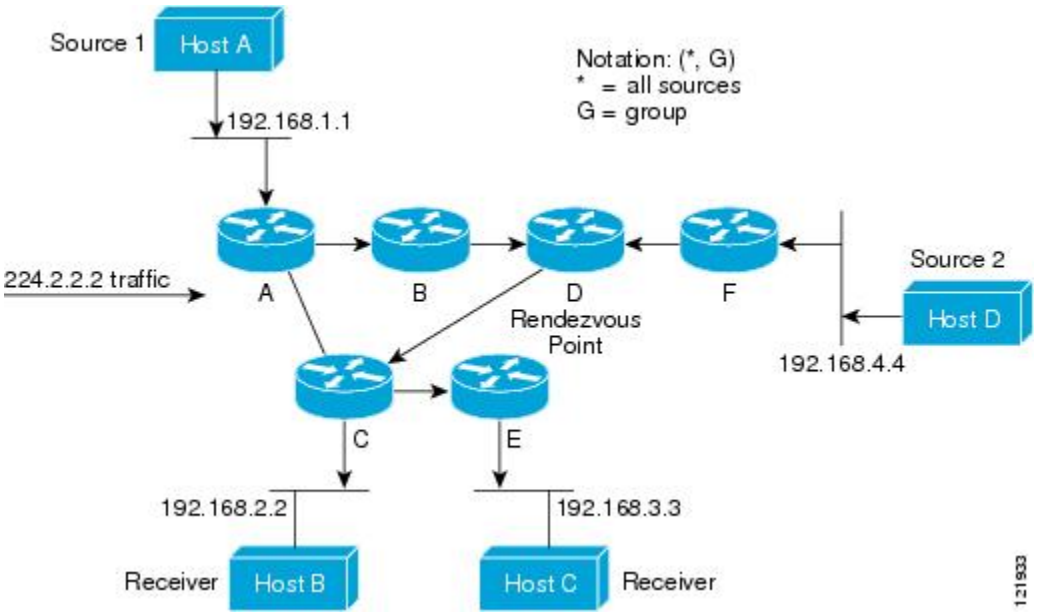
マルチキャスト配信の共有ツリー

ソースをルートとするソース ツリーとは異なり、共有ツリーはネットワーク内の選択されたポイントに配置された単一の共通ルートを使用します。この共有されたルートは、ランデブー ポイント（RP）と呼ばれます。

次の図に、ルータ D にルートが配置されたグループ 224.2.2.2 の共有ツリーを示します。この共有ツリーは単方向です。ソース トラフィックは、ソース ツリー上の RP に向けて送信されます。このトラフィックは、次に RP から共有ツリーを下方向に転送され、すべてのレシーバに

到達します（レシーバがソースと RP の間に配置されていない場合は、直接サービスが提供されます）。

図 *14 :* 共有ツリー



この例では、送信元（ホストAおよびホストD）からのマルチキャストトラフィックがルート（ルータ D）に移動した後に共有ツリーから 2 つの受信先（ホスト B およびホスト C）へと到達します。マルチキャストグループ内のすべての送信元が一般的な共有ツリーを使用するため、(*, G) というワイルドカード表記（「アスタリスク、カンマ、G」と読みます）でそのツリーを表します。この場合、* はすべてのソースを意味し、G はマルチキャスト グループを表します。したがって、図の共有ツリーは (*, 224.2.2.2) と表記します。

ソース ツリーと共有ツリーは、どちらもループフリーです。ツリーが分岐する場所でのみ、メッセージが複製されます。マルチキャスト グループのメンバは常に加入または脱退する可能性があるため、配信ツリーを動的に更新する必要があります。特定のブランチに存在するすべてのアクティブ レシーバが特定のマルチキャスト グループに対してトラフィックを要求しなくなると、ルータは配信ツリーからそのブランチをプルーニングし、そのブランチから下方向へのトラフィック転送を停止します。そのブランチの特定のレシーバがアクティブになり、マルチキャストトラフィックを要求すると、ルータは配信ツリーを動的に変更し、トラフィック転送を再開します。

ソース ツリーの利点

ソース ツリーには、ソースとレシーバの間に最適なパスを作成するという利点があります。この利点により、マルチキャストトラフィックの転送におけるネットワーク遅延を最小限に抑えることができます。ただし、この最適化は代償を伴います。ルータがソースごとにパス情報を維持する必要があるのです。何千ものソース、何千ものグループが存在するネットワークでは、このオーバーヘッドがすぐにルータ上でのリソースの問題につながる可能性があります。ネットワーク設計者は、マルチキャスト ルーティング テーブルのサイズによるメモリ消費について考慮する必要があります。

共有ツリーの利点

共有ツリーには、各ルータにおいて要求されるステートの量が最小限に抑えられるという利点があります。この利点により、共有ツリーだけが許容されるネットワークの全体的なメモリ要件が緩和されます。共有ツリーの欠点は、特定の状況でソースとレシーバの間のパスが最適パスではなくなり、パケット配信に遅延を生じる可能性があることです。たとえば、上の図のホストA（ソース1）とホスト 2（レシーバ）間の最短パスはルータ A とルータ B です。共有ツリーのルートとしてルータ D を使用するため、トラフィックはルータ A、B、D、そして次にCを通過する必要があります。ネットワーク設計者は、共有ツリー専用環境を実装する際にランデブー ポイント（RP）の配置を慎重に考慮する必要があります。

ユニキャストルーティングでは、トラフィックは、ネットワーク上でソースから宛先ホストまでの単一パスに沿ってルーティングされます。ユニキャスト ルータは、ソース アドレスを考慮せず、宛先アドレスおよびその宛先へのトラフィックの転送方法だけを考慮します。ルータは、ルーティングテーブル全体をスキャンして宛先アドレスを取得し、適正なインターフェイスから宛先の方向へユニキャスト パケットのコピーを転送します。

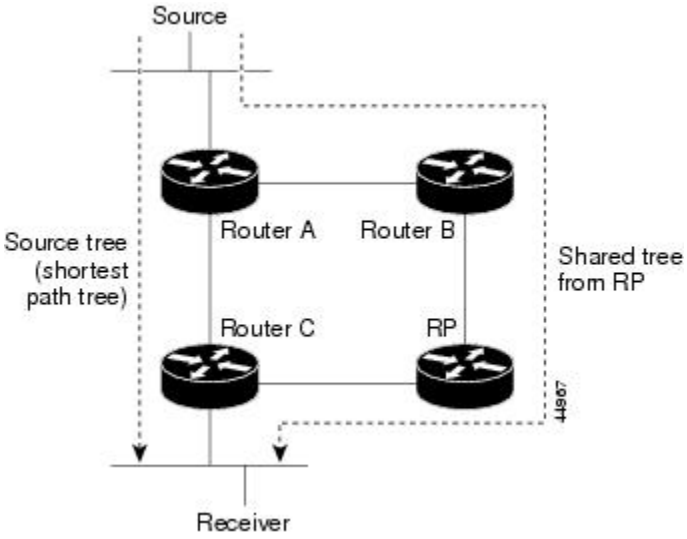
マルチキャスト転送では、ソースは、マルチキャスト グループ アドレスによって表される任意のホスト グループにトラフィックを送信します。マルチキャスト ルータは、どの方向が（ソースへ向かう）アップストリーム方向で、どの方向（1方向または複数の方向）が（レシーバへ向かう）ダウンストリーム方向であるかを決定する必要があります。複数のダウンストリームパスがある場合、ルータはパケットを複製し、それを適切なダウンストリームパス（最善のユニキャスト ルート メトリック）で下方向に転送します。これらのパスがすべてであるとは限りません。レシーバの方向ではなく、ソースから遠ざかる方向へのマルチキャスト トラフィック転送は、Reverse Path Forwarding（RPF）と呼ばれます。RPF については、次の項を参照してください。

PIM 共有ツリーおよびソース ツリー

デフォルトでは、グループのメンバーで受信されるデータは、RP でルーティングされた単一のデータ配信ツリーを経由して、送信側からグループに送られます。

図 *15 :* 共有ツリーおよびソース ツリー（最短パスツリー）

次の図に、このタイプの共有配信ツリーを示します。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 レートによって保証されている場合は、送信元でルーティングされるデータ配信ツリーを、共有ツリーのリーフ ルータ（ダウンストリーム接続がないルータ）で使用できます。このタイプの配信ツリーは、SPT または送信元ツリーと呼ばれます。デフォルトでは、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すると、送信元ツリーに切り替わります。

共有ツリーから送信元ツリーへの移動プロセスは、次のとおりです。

1. レシーバがグループに加入します。リーフ ルータ C は Join メッセージを RP に向けて送信します。
2. RP はルータ C とのリンクを発信インターフェイス リストに格納します。
3. 送信元がデータを送信します。ルータ A はデータをカプセル化して登録メッセージに格納し、RP に送信します。
4. RP はデータをルータ C に向けて共有ツリーの下方向に転送し、送信元に向けて Join メッセージを送信します。この時点で、データはルータ C に 2 回着信する可能性があります（カプセル化されたデータ、およびネイティブ状態のデータ）。
5. データがネイティブ状態（カプセル化されていない状態）で着信すると、RP は登録停止メッセージをルータ A に送信します。
6. デフォルトでは、最初のデータ パケット受信時に、ルータ 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. ルータ C が（S, G）でデータを受信すると、ルータ C は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ルータ C へのリンクを削除します。RP は送信元に向けてプルーニング メッセージを送信します。

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単位で送信され、送信元または RP へのパス上にある各 PIM デバイスで処理されます。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ルータによって送信され、グループの RP によって受信されます。

グループへ送信する複数の送信元で、共有ツリーが使用されます。共有ツリー上に存在するように、PIM デバイスを設定できます。

最初のデータ パケットがラスト ホップ ルータに着信すると、共有ツリーからソース ツリーへと変更されます。この変更は、**ip pim spt-threshold** 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たしきい値によって異なります。

SPT には共有ツリーよりも多くのメモリが必要ですが、遅延が短縮されます。SPT の使用を延期することもできます。リーフ ルータを SPT にすぐ移動せず、トラフィックがしきい値に最初に到達したあとで移動するように指定できます。

PIM リーフ ルータが、指定グループの SPT に加入する時期を設定できます。送信元の送信速度が指定速度（キロビット/秒）以上の場合、マルチレイヤ スイッチは PIM Join メッセージを送信元に向けて送信し、送信元ツリー（SPT）を構築します。送信元からのトラフィック速度がしきい値を下回ると、リーフ ルータは共有ツリーに再び切り替わり、プルーニング メッセージを送信元に送信します。

SPT しきい値を適用するグループを指定するには、グループ リスト（標準アクセス リスト）を使用します。値 0 を指定する場合、またはグループ リストを使用しない場合、しきい値はすべてのグループに適用されます。

Reverse Path Forwarding

ユニキャスト ルーティングでは、トラフィックは、ネットワーク上でソースから宛先ホストまでの単一パスに沿ってルーティングされます。ユニキャスト ルータは、ソース アドレスを考慮せず、宛先アドレスおよびその宛先へのトラフィックの転送方法だけを考慮します。ルータは、ルーティング テーブル全体をスキャンして宛先ネットワークを取得し、適正なインターフェイスから宛先の方向へユニキャスト パケットのコピーを転送します。

マルチキャスト転送では、ソースは、マルチキャスト グループ アドレスによって表される任意のホスト グループにトラフィックを送信します。マルチキャスト ルータは、どの方向が（ソースへ向かう）アップストリーム方向で、どの方向（1 方向または複数の方向）が（レシーバへ向かう）ダウンストリーム方向であるかを決定する必要があります。複数のダウンストリーム パスがある場合、ルータはパケットを複製し、それを適切なダウンストリーム パス（最善のユニキャスト ルート メトリック）で下方向に転送します。これらのパスがすべてであるとは限りません。レシーバの方向ではなく、ソースから遠ざかる方向へのマルチキャスト トラフィック転送は、Reverse Path Forwarding（RPF）と呼ばれます。RPF は、マルチキャスト データグラムの転送に使用されるアルゴリズムです。

Protocol Independent Multicast（PIM）は、ユニキャスト ルーティング情報を使用して、レシーバからソースへ向かうリバース パスに沿って配信ツリーを作成します。その後、マルチキャスト ルータは、その配信ツリーに沿ってソースからレシーバにパケットを転送します。RPF は、マルチキャスト転送における重要な概念です。RPF により、ルータは、配信ツリーの下方向へ

正しくマルチキャスト トラフィックを転送できます。RPF は、既存のユニキャスト ルーティング テーブルを使用して、アップストリーム ネイバーとダウンストリーム ネイバーを決定します。ルータは、アップストリームインターフェイスで受信した場合にのみ、マルチキャスト パケットを転送します。この RPF チェックにより、配信ツリーがループフリーであることを保証できます。

RPF チェック

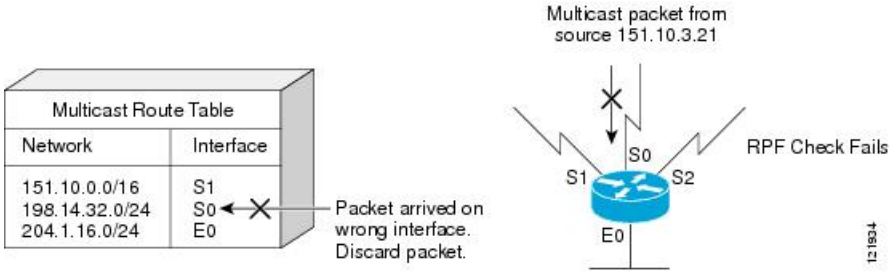
マルチキャスト パケットがルータに到達すると、ルータはそのパケットに対して RPF チェックを実行します。RPFチェックが成功すると、パケットが転送されます。そうでない場合、パケットはドロップされます。

ソース ツリーを下方向へ流れるトラフィックに対する RPF チェック手順は次のとおりです。

1. ルータは、ユニキャスト ルーティング テーブルでソース アドレスを検索して、ソースへのリバースパス上にあるインターフェイスにパケットが到達したかどうかを判定します。
2. ソースに戻すインターフェイスにパケットが到達した場合、RPF チェックは成功し、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 リストに示されているインターフェイスからパケットが転送されます。
3. ステップ 2 で RPF チェックに失敗した場合は、パケットがドロップされます。

図に、RPF チェックの失敗例を示します。

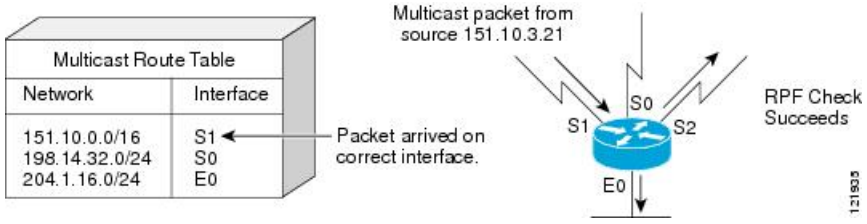
図 *16 : RPF* チェックの失敗



図に示すように、ソース 151.10.3.21 からのマルチキャスト パケットはシリアル インターフェイス 0（S0）上で受信されています。ユニキャスト ルート テーブルのチェック結果は、このルータが 151.10.3.21 にユニキャスト データを転送するために使用するインターフェイスは S1 であることを示しています。パケットはインターフェイス S0 に到達しているため、このパケットは廃棄されます。

図に RPF チェックの成功例を示します。

図 *17 : RPF* チェックの成功



この例では、マルチキャスト パケットはインターフェイス S1 に到達しています。ルータはユニキャスト ルーティング テーブルを参照し、S1 が適正なインターフェイスであることを知ります。RPF チェックが成功し、パケットが転送されます。

PIM はソース ツリーと RP でルーティングされた共有ツリーを使用して、データグラムを転送します。RPF チェックは、それぞれ異なる方法で実行されます。

- PIM ルータまたはマルチレイヤスイッチが送信元ツリーの状態である場合（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 IP アドレスに対して RPF チェックが実行されます。
- PIM ルータまたはマルチレイヤ 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）、（メンバーがグループに加入している場合は既知である）RP アドレスについて RPF チェックが実行されます。

（注） このスイッチでは DVMRP はサポートされません。

PIM SM は RPF 参照機能を使用し、加入およびプルーニング メッセージを送信する必要があるかどうかを決定します。

- （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 メッセージ（共有ツリー ステート）は RP に向け送信されます。

PIM ルーティングのデフォルト設定

デバイス用の PIM ルーティングのデフォルト設定を次の表に示します。

表 *14 :* 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
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

機能	デフォルト設定
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

PIM の設定方法

PIM スタブ ルーティングのイネーブル化

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip pim passive**
5. **end**
6. **show ip pim interface**
7. **show ip igmp groups detail**
8. **show ip mroute**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `# 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** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	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。 指定するインターフェイスは、次のいずれかである必要があります。これらのインターフェイスには、IP アドレスが割り当てられている必要があります。 • 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。 • 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。
ステップ 4	**ip pim passive** 例： `Device(config-if)# ip pim passive`	インターフェイスに PIM スタブ機能を設定します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip pim interface** 例： `Device# show ip pim interface`	（任意）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。
ステップ 7	**show ip igmp groups detail** 例： `Device# show ip igmp groups detail`	（任意）特定のマルチキャスト送信元グループに参加した対象クライアントを表示します。

	コマンドまたはアクション	目的
ステップ 8	**show ip mroute** 例： `Device# show ip mroute`	（任意）IP マルチキャスト ルーティング テーブルを表示します。
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-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。

ランデブー ポイントの設定

インターフェイスがスパース - デンス モードで、グループをスパース グループとして扱う場合には、ランデブー ポイント（RP）を設定する必要があります。次の方法を使用できます。

- RP をマルチキャスト グループに手動で割り当てる
- PIMv1 から独立した、以下を含むスタンドアロンとしてのシスコ独自のプロトコル
- Internet Engineering Task Force（IETF）の標準追跡プロトコルの使用（PIMv2 BSR の設定を含む）

（注） 動作中の PIM バージョン、およびネットワーク内のルータ タイプに応じて、自動 RP、BSR、またはこれらを組み合わせて使用できます。ネットワーク内の異なるバージョンの PIM を利用する方法については、PIMv1 および PIMv2 の相互運用性 （144 ページ）を参照してください。

マルチキャスト グループへの RP の手動割り当て

ダイナミック メカニズム（自動 RP や BSR など）を使用してグループのランデブー ポイント（RP）を取得する場合、RP を手動で割り当てる必要はありません。

マルチキャスト トラフィックの送信側は、送信元の先頭ホップ ルータ（指定ルータ）から受信して RP に転送される登録メッセージを通し、自身の存在をアナウンスします。マルチキャスト パケットの受信側は RP を使用し、マルチキャスト グループに加入します。この場合は、明示的な Join メッセージが使用されます。

（注） RP はマルチキャスト グループのメンバーではなく、マルチキャスト送信元およびグループ メンバーの合流地点として機能します。

アクセス リストで定義される複数のグループに、単一の RP を設定できます。グループに RP が設定されていない場合、マルチレイヤスイッチはデンスとしてグループに応答し、デンス モードの PIM 技術を使用します。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip pim rp-address** *ip-address* [*access-list-number*] [**override**]
4. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
5. **end**
6. **show running-config**
7. **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： `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	**configure terminal** 例： `# 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	**ip pim rp-address** *ip-address* [*access-list-number*] [**override**] 例： `Device(config)# ip pim rp-address 10.1.1.1 20 override`	PIM RP のアドレスを設定します。 デフォルトで、PIM RP アドレスは設定されていません。すべてのルータおよびマルチレイヤスイッチ（RP を含む）で、RP の IP アドレスを設定する必要があります。 （注） グループに RP が設定されていない場合、デバイスは PIM DM 技術を使用し、グループをデンスとして処理します。 1 台の PIM デバイスを、複数のグループの RP にできます。1 つの PIM ドメイン内で一度に使用できる

	コマンドまたはアクション	目的
		RP アドレスは、1 つだけです。アクセス リスト条件により、デバイスがどのグループの RP であるかを指定します。 • *ip-address* には、RP のユニキャスト アドレスをドット付き 10 進表記で入力します。 •（任意）*access-list-number* を指定する場合は、1 ～ 99 の IP 標準アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 •（任意）**override** キーワードを指定すると、このコマンドによって設定された RP と、自動 RP または BSR で取得された RP との間に矛盾が生じた場合に、このコマンドによって設定された RP が優先されます。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 25 permit 10.5.0.1 255.224.0.0`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、RP が使用されるマルチキャスト グループのアドレスを入力します。 •（任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 5	**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 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-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。

新規ネットワークでの Auto-RP の設定

（注） PIM ルータをローカル グループの RP として設定する場合は、次の手順のステップ 3 を省略します。

手順の概要

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **ip pim send-rp-announce** *interface-id* **scope** *ttl* **group-list** *access-list-number* **interval** *seconds*
5. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
6. **ip pim send-rp-discovery scope** *ttl*
7. **end**
8. **show running-config**
9. **show ip pim rp mapping**
10. **show ip pim rp**
11. **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： `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	**show running-config** 例：	すべての PIM デバイス上でデフォルトの RP が設定されていること、および RP が SM ネットワーク内

	コマンドまたはアクション	目的
	`Device# show running-config`	にあることを確認します。RP は、**ip pim rp-address** グローバル コンフィギュレーション コマンドによって設定済みです。 （注） SM-DM 環境の場合、このステップは不要です。 選択された RP は接続が良好で、ネットワークで使用可能となる必要があります。この RP は、グローバル グループ（224.x.x.x やその他のグローバル グループなど）に対して使用されます。この RP で処理されるグループ アドレス範囲は再設定しないでください。自動 RP によって動的に検出された RP は、静的に設定された RP よりも優先されます。ローカル グループ用に 2 番めの RP を使用することもできます。
ステップ 3	**configure terminal** 例： `# 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	**ip pim send-rp-announce** *interface-id* **scope** *ttl* **group-list** *access-list-number* **interval** *seconds* 例： `Device(config)# ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120`	別の PIM デバイスをローカル グループの候補 RP として設定します。 • *interface-id* には、RP アドレスを識別するインターフェイス タイプおよび番号を入力します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • **scope** *ttl* には、ホップの存続可能時間の値を指定します。RP アナウンス メッセージがネットワーク内のすべてのマッピング エージェントに到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。 • **group-list** *access-list-number* には、1 ～ 99 の範囲で標準の IP アクセスリスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • **interval** *seconds* には、アナウンスメントメッセージを送信する頻度を指定します。デフォルトは 60 秒です。指定できる範囲は 1 ～ 16383 です。

	コマンドまたはアクション	目的
ステップ 5	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 10 permit 10.10.0.0`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 3 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 （注） アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 6	**ip pim send-rp-discovery scope** *ttl* 例： `Device(config)# ip pim send-rp-discovery scope 50`	接続が中断される可能性がないデバイスを検索し、RP マッピング エージェントの役割を割り当てます。 **scope** *ttl* には、ホップの存続可能時間の値を指定し、RP ディスカバリ パケットを制限します。ホップ数内にあるすべてのデバイスは、送信元デバイスから自動 RP ディスカバリ メッセージを受信します。これらのメッセージは他のデバイスに対し、矛盾（グループ/RP 範囲の重なりなど）を回避するために使用されるグループ/RP マッピングを通知します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例：	入力を確認します。

	コマンドまたはアクション	目的
	`Device# show running-config`	
ステップ 9	**show ip pim rp mapping** 例： `Device# show ip pim rp mapping`	関連するマルチキャスト ルーティング エントリとともに保管されているアクティブな RP を表示します。
ステップ 10	**show ip pim rp** 例： `Device# show ip pim rp`	ルーティング テーブルに保管されている情報を表示します。
ステップ 11	**copy running-config startup-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。

既存の SM クラウドへの Auto-RP の追加

ここでは、最初に自動 RP を既存の SM クラウドに導入し、既存のマルチキャスト インフラストラクチャができるだけ破壊されないようにする方法について説明します。

この手順は任意です。

手順の概要

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **ip pim send-rp-announce** *interface-id* **scope** *ttl* **group-list** *access-list-number* **interval** *seconds*
5. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
6. **ip pim send-rp-discovery scope** *ttl*
7. **end**
8. **show running-config**
9. **show ip pim rp mapping**
10. **show ip pim rp**
11. **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： `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	**show running-config** 例： `Device# show running-config`	すべての PIM デバイス上でデフォルトの RP が設定されていること、および RP が SM ネットワーク内にあることを確認します。RP は、**ip pim rp-address** グローバル コンフィギュレーション コマンドによって設定済みです。 （注） SM-DM 環境の場合、このステップは不要です。 選択された RP は接続が良好で、ネットワークで使用可能となる必要があります。この RP は、グローバル グループ（224.x.x.x やその他のグローバル グループなど）に対して使用されます。この RP で処理されるグループ アドレス範囲は再設定しないでください。自動 RP によって動的に検出された RP は、静的に設定された RP よりも優先されます。ローカル グループ用に 2 番めの RP を使用することもできます。
ステップ 3	**configure terminal** 例： `# 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	**ip pim send-rp-announce** *interface-id* **scope** *ttl* **group-list** *access-list-number* **interval** *seconds* 例： `Device(config)# ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120`	別の PIM デバイスをローカル グループの候補 RP として設定します。 • *interface-id* には、RP アドレスを識別するインターフェイス タイプおよび番号を入力します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • **scope** *ttl* には、ホップの存続可能時間の値を指定します。RP アナウンス メッセージがネットワーク内のすべてのマッピング エージェントに到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。

	コマンドまたはアクション	目的
		• **group-list** *access-list-number* には、1 ～ 99 の範囲で標準の IP アクセスリスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • **interval** *seconds* には、アナウンスメントメッセージを送信する頻度を指定します。デフォルトは 60 秒です。指定できる範囲は 1 ～ 16383 です。
ステップ 5	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 10 permit  224.0.0.0 15.255.255.255`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 3 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 6	**ip pim send-rp-discovery scope** *ttl* 例： `Device(config)# ip pim send-rp-discovery scope 50`	接続が中断される可能性がないデバイスを検索し、RP マッピング エージェントの役割を割り当てます。 **scope** *ttl* には、ホップの存続可能時間の値を指定し、RP ディスカバリ パケットを制限します。ホップ数内にあるすべてのデバイスは、送信元デバイスから自動 RP ディスカバリ メッセージを受信します。これらのメッセージは他のデバイスに対し、矛盾（グループ/RP 範囲の重なりなど）を回避するために使用されるグループ/RP マッピングを通知します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。

	コマンドまたはアクション	目的
		（注） RPマッピングエージェントとして設定されたデバイスを削除するには、**no ip pim send-rp-discovery** 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。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**show ip pim rp mapping** 例： `Device# show ip pim rp mapping`	関連するマルチキャスト ルーティング エントリとともに保管されているアクティブなRPを表示します。
ステップ 10	**show ip pim rp** 例： `Device# show ip pim rp`	ルーティング テーブルに保管されている情報を表示します。
ステップ 11	**copy running-config startup-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。

問題のある RP への Join メッセージの送信禁止

ip pim accept-rp コマンドがネットワーク全体に設定されているかどうかを判別するには、**show running-config** 特権 EXEC コマンドを使用します。**ip pim accept-rp** コマンドが設定されていないデバイスがある場合は、後でこの問題を解決できます。ルータまたはマルチレイヤスイッチが **ip pim accept-rp** コマンドによってすでに設定されている場合は、このコマンドを再入力し、新規にアドバタイズされる RP を許可する必要があります。

着信 RP アナウンスメント メッセージのフィルタリング

マッピング エージェントにコンフィギュレーション コマンドを追加すると、故意に不正設定されたルータが候補 RP として動作し問題を引き起こさないようにできます。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip pim rp-announce-filter rp-list** *access-list-number* **group-list** *access-list-number*
4. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
5. **end**
6. **show running-config**
7. **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： `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	**configure terminal** 例： `# 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	**ip pim rp-announce-filter rp-list** *access-list-number* **group-list** *access-list-number* 例： `Device(config)# ip pim rp-announce-filter rp-list 10 group-list 14`	着信 RP アナウンスメント メッセージをフィルタリングします。 ネットワーク内のマッピングエージェントごとに、このコマンドを入力します。このコマンドを使用しないと、すべての着信 RP アナウンスメント メッセージがデフォルトで許可されます。 **rp-list** *access-list-number* には、候補 RP アドレスのアクセスリストを設定します。アクセスリストが許可されている場合は、**group-list** *access-list-number* 変数で指定されたグループ範囲に対してアクセスリストを使用できます。この変数を省略すると、すべてのマルチキャスト グループにフィルタが適用されます。

	コマンドまたはアクション	目的
		複数のマッピングエージェントを使用する場合は、グループ/RP マッピング情報に矛盾が生じないようにするため、すべてのマッピングエージェント間でフィルタを統一する必要があります。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 10 permit 10.8.1.0 255.255.224.0`	標準アクセスリストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • どのルータおよびマルチレイヤ スイッチからの候補 RP アナウンスメント（rp-list アクセス コントロール リスト（ACL））がマッピングエージェントによって許可されるかを指定するアクセス リストを作成します。 • 許可または拒否するマルチキャスト グループの範囲を指定するアクセスリスト（グループリスト ACL）を作成します。 • *source* には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
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	**show running-config** 例：	入力を確認します。

	コマンドまたはアクション	目的
	`Device# show running-config`	
ステップ 7	**copy running-config startup-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。

PIMv2 BSR の設定

PIMv2 BSR を設定するプロセスには、次のオプションの作業が含まれることがあります。

- PIM ドメイン境界の定義
- IP マルチキャスト境界の定義
- 候補 BSR の設定
- 候補 RP の設定

PIM ドメイン境界の定義

PIM ドメイン境界を設定するには、次の手順を実行します。この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip pim bsr-border**
5. **end**
6. **show running-config**
7. **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： `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	**configure terminal** 例：	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
	`Device# configure terminal`	
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、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。 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。 • 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。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip pim bsr-border** 例： `Device(config-if)# ip pim bsr-border`	PIM ドメイン用の PIM ブートストラップ メッセージ境界を定義します。 境界に位置する他の PIM ドメインに接続されているインターフェイスごとに、このコマンドを入力します。このコマンドを実行すると、デバイスは、このインターフェイス上で PIMv2 BSR メッセージを送受信しないように指示されます。 （注） PIM 境界を削除するには、 **no ip pim bsr-border** 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。
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	**show running-config** 例： `Device# show running-config`	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 7	**copy running-config startup-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。

IP マルチキャスト境界の定義

自動 RP メッセージが PIM ドメインに入らないようにする場合は、マルチキャスト境界を定義します。自動 RP 情報を伝達する 224.0.1.39 および 224.0.1.40 宛てのパケットを拒否するアクセス リストを作成します。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **deny** *source* [*source-wildcard*]
4. **interface** *interface-id*
5. **ip multicast boundary** *access-list-number*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**configure terminal** 例： `# 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	**access-list** *access-list-number* **deny** *source* [*source-wildcard*] 例： `Device(config)# access-list 12 deny 224.0.1.39`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* の範囲は 1 ～ 99 です。

	コマンドまたはアクション	目的
	`access-list 12 deny 224.0.1.40`	• **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • *source* には、自動RP情報を伝達するマルチキャスト アドレス 224.0.1.39 および 224.0.1.40 を入力します。 •（任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、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。 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。 • 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。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 5	**ip multicast boundary** *access-list-number* 例： `Device(config-if)# ip multicast boundary 12`	ステップ 2 で作成したアクセス リストを指定し、境界を設定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例：	入力を確認します。

	コマンドまたはアクション	目的
	`Device# show running-config`	
ステップ 8	**copy running-config startup-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。

候補 BSR の設定

候補 BSR を、1 つまたは複数設定できます。候補 BSR として機能するデバイスは、他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip pim bsr-candidate** *interface-id hash-mask-length* [*priority*]
4. **end**
5. **show running-config**
6. **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： `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	**configure terminal** 例： `# 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	**ip pim bsr-candidate** *interface-id hash-mask-length* [*priority*] 例： `Device(config)# ip pim bsr-candidate gigabitethernet 1/0/3 28 100`	候補 BSR となるようにデバイスを設定します。 • *interface-id* には、デバイスを候補 BSR に設定するときに BSR アドレスの取得元となる 上のインターフェイスを入力します。このインターフェイスは PIM を使用してイネーブルにする必

	コマンドまたはアクション	目的
		要があります。有効なインターフェイスは、物理ポート、ポートチャネル、VLANなどです。 • *hash-mask-length* には、ハッシュ機能を呼び出す前にグループ アドレスとの AND 条件となるマスク長（最大 32 ビット）を指定します。ハッシュ元が同じであるすべてのグループは、同じ RP に対応します。たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。 •（任意）*priority* を指定する場合は、0 ～ 255 の番号を入力します。プライオリティが大きな BSR が優先されます。このプライオリティ値が同じである場合は、大きなIPアドレスを持つデバイスがBSRとして選択されます。デフォルトは 0 です。
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	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-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。

候補 RP の設定

候補 RP を、1 つまたは複数設定できます。BSR と同様、RP は他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。RP は IP マルチキャスト アドレス空間全体、またはその一部を処理します。候補 RP は候補 RP アドバタイズを BSR に送信します。

この手順は任意です。

始める前に

RP となるデバイスを決定するときは、次の可能性を考慮してください。

- 自動 RP だけが使用されている Cisco ルータおよびマルチレイヤ スイッチで構成されるネットワークでは、すべてのデバイスを RP として設定できます。
- シスコの PIMv2 ルータおよびマルチレイヤ スイッチと、他のベンダーのルータだけで構成されるネットワークでは、すべてのデバイスを RP として使用できます。
- シスコの PIMv1 ルータ、PIMv2 ルータ、および他のベンダーのルータで構成されるネットワークでは、シスコ PIMv2 ルータおよびマルチレイヤ スイッチを RP として設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip pim rp-candidate** *interface-id* [**group-list** *access-list-number*]
4. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
5. **end**
6. **show running-config**
7. **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： `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	**configure terminal** 例： `# 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	**ip pim rp-candidate** *interface-id* [**group-list** *access-list-number*] 例： `Device(config)# ip pim rp-candidate gigabitethernet 1/0/5 group-list 10`	候補 RP となるようにデバイスを設定します。 • *interface-id* には、対応する IP アドレスが候補 RP アドレスとしてアドバタイズされるインターフェイスを指定します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 •（任意）**group-list** *access-list-number* を指定する場合は、1 ～ 99 の IP 標準アクセス リスト番号

	コマンドまたはアクション	目的
		を入力します。group-list を指定しない場合は、このデバイスがすべてのグループの候補 RP となります。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 10 permit 239.0.0.0 0.255.255.255`	標準アクセスリストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 •（任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
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	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-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。

Auto-RP によるスパース モードの設定

始める前に

- Auto-RPを設定するときに必要なすべてのアクセスリストは、設定作業を開始する前に設定しておく必要があります。

（注）

- グループ内に既知の RP がなく、インターフェイスがスパース - デンス モードに設定されている場合、インターフェイスはデンス モードであるように扱われ、データはインターフェイスを介してフラッディングされます。このデータのフラッディングを避けるために、Auto-RPリスナーを設定してから、インターフェイスをスパースモードとして設定します。
- Auto-RP を設定するには、Auto-RP リスナー機能を設定するか（ステップ 5）、スパースモードを指定する（ステップ 7）必要があります。
- スパース-デンス モードを指定する場合、デンス モードのフェールオーバーがネットワークのデンスモードのフラッディングを引き起こす可能性があります。この状況を避けるため、Auto-RP リスナー機能で PIM スパース モードを使用します。

自動ランデブー ポイント（Auto-RP）を設定するには、次の手順に従います。Auto-RP は任意でエニーキャスト RP でも使用できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast-routing**
4. ステップ 5 ～ 7 を実行するか、またはステップ 6 および 8 を実行します。
5. **interface** *type number*
6. **ip pim sparse-mode**
7. **exit**
8. すべての PIM インターフェイス上でステップ 1 ～ 9 を繰り返します。
9. **ip pim send-rp-announce** {*interface-type interface-number* | *ip-address*} **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**]
10. **ip pim send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value* [**interval** *seconds*]
11. **ip pim rp-announce-filter rp-list** *access-list* **group-list** *access-list*
12. **interface** *type number*
13. **ip multicast boundary** *access-list* [**filter-autorp**]
14. **end**
15. **show ip pim autorp**
16. **show ip pim rp** [**mapping**] [*rp-address*]
17. **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]

18. **show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*]

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	**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	**ip multicast-routing** 例： `Device(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。
ステップ 4	ステップ 5 ～ 7 を実行するか、またはステップ 6 および 8 を実行します。	--
ステップ 5	**interface** *type number* 例： `Device(config)# interface Gigabitethernet 1/0/0`	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 6	**ip pim sparse-mode** 例： `Device(config-if)# ip pim sparse-mode`	インターフェイスで PIM スパース モードをイネーブルにします。スパース モードで Auto-RP を設定している場合、次のステップで Auto-RP リスナーも設定する必要があります。 • ステップ 8 でスパース-デンス モードを設定している場合、このステップはスキップします。
ステップ 7	**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、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 8	すべての PIM インターフェイス上でステップ 1 ～ 9 を繰り返します。	--
ステップ 9	**ip pim send-rp-announce** {*interface-type interface-number* | *ip-address*} **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**]	RP アナウンスメントをすべての PIM 対応インターフェイスに送信します。 • RPデバイスでのみこのステップを実行します。

	コマンドまたはアクション	目的
	例： `Device(config)# ip pim send-rp-announce loopback0 scope 31 group-list 5`	• RP アドレスとして使用する IP アドレスを定義するには、*interface-type* 引数と *interface-number* 引数を使用します。 • 直接接続されている IP アドレスを RP アドレスとして指定するには、*ip-address* 引数を使用します。 （注） このコマンドに *ip-address* 引数が設定されている場合、RP 通知メッセージがこのアドレスが接続されているインターフェイスによって送信されます（つまり、RP 通知メッセージの IP ヘッダーのソース アドレスがそのインターフェイスの IP アドレスです）。 • 次の例は、最大ホップ数が 31 でインターフェイスがイネーブルであることを示します。デバイスは、ループバック インターフェイス 0 に関連付けられた IP アドレスによって RP として識別されることを望みます。アクセス リスト 5 はこのデバイスが RP として機能しているグループを示しています。
ステップ 10	**ip pim send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value* [**interval** *seconds*] 例： `Device(config)# ip pim send-rp-discovery loopback 1 scope 31`	デバイスを RP マッピング エージェントとして設定します。 • RP マッピング エージェント デバイス上、または RP/RP マッピング エージェント複合デバイス上で、このステップを実行します。 （注） Auto-RP によって、RP 機能は 1 台のデバイス上で単独で実行でき、RP マッピング エージェントは 1 台または複数のデバイス上で実行できます。RP/RP マッピング エージェント複合デバイス上で、RP および RP マッピング エージェントを展開することができます。 • RP マッピング エージェントのソース アドレスとして使用する IP アドレスを定義するには、オプションの *interface-type* 引数と *interface-number* 引数を使用します。

	コマンドまたはアクション	目的
		• Auto-RP 検出メッセージの IP ヘッダーで存続可能時間（TTL）値を指定するには、**scope** キーワードと *ttl-value* 引数を使用します。 • Auto-RP 検出メッセージが送信される間隔を指定するには、オプションの **interval** キーワードと *seconds* 引数を使用します。 （注） Auto-RP 検出メッセージが送信される間隔をデフォルト値の 60 秒から減らすと、group-to-RP マッピングのより頻繁なフラッディングが発生します。一部のネットワーク環境では、間隔を短縮する欠点（コントロールパケット オーバーヘッドの増加）が利点（グループと RP のマッピングのより頻繁な更新）を上回る場合があります。 • 例では、ループバック インターフェイス 1 で Auto-RP 検出メッセージを 31 ホップに制限していることを示しています。
ステップ 11	**ip pim rp-announce-filter rp-list** *access-list* **group-list** *access-list* 例： `Device(config)# ip pim rp-announce-filter rp-list 1 group-list 2`	候補 RP（C-RP）から RP マッピング エージェントに送信された着信 RP アナウンスメント メッセージをフィルタリングします。 • このステップは、RP マッピング エージェントでのみ実行します。
ステップ 12	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/0`	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 13	**ip multicast boundary** *access-list* [**filter-autorp**] 例： `Device(config-if)# ip multicast boundary 10 filter-autorp`	管理用スコープの境界を設定します。 • このステップは、他のデバイスとの境界であるインターフェイス上で実行します。 • この作業ではアクセス リストは表示されません。 • アクセスリストエントリで **deny** キーワードを使用すると、そのエントリに一致するパケットのマルチキャスト境界が作成されます。

	コマンドまたはアクション	目的
ステップ 14	**end** 例： `Device(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 15	**show ip pim autorp** 例： `Device# show ip pim autorp`	（任意）Auto-RP 情報を表示します。
ステップ 16	**show ip pim rp** [**mapping**] [*rp-address*] 例： `Device# show ip pim rp mapping`	（任意）ネットワークで既知の RP を表示し、デバイスが各 RP について学習する方法を示します。
ステップ 17	**show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**] 例： `Device# show ip igmp groups`	（任意）デバイスに直接接続されている、インターネット グループ管理プロトコル（IGMP）を通じて学習されたレシーバを持つマルチキャスト グループを表示します。 • レシーバ情報が結果の画面に表示されるには、レシーバがこのコマンドが発行された時点でネットワーク上でアクティブである必要があります。
ステップ 18	**show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*] 例： `Device# show ip mroute cbone-audio`	（任意）IP マルチキャスト ルーティング（mroute）テーブルの内容を表示します。

IPv4 双方向 PIM の設定

ここでは、双方向 PIM の設定について説明します。

IPv4 双方向 PIM のグローバルなイネーブル化

IPv4 双方向 PIM をイネーブルにするには、次の作業を行います。

始める前に

双方向 PIM を設定する前に、そのドメイン内のすべての IP マルチキャスト対応ルータでこの機能がサポートされていることを確認します。部分的にアップグレードされたネットワークでは、双方向 PIM の一連の動作を有効にすることはできません。双方向 PIM をサポートするた

めに部分的にしかアップグレードされていないネットワークでは、パケットループがただちに発生します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip pim bidir-enable**

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	**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	**ip pim bidir-enable** 例： `Device(config)# ip pim bidir-enable`	デバイスで IPv4 双方向 PIM をグローバルにイネーブルにします。

IPv4 双方向 PIM グループのランデブー ポイントの設定

IPv4 双方向 PIM グループのランデブー ポイントをスタティックに設定するには、次の作業を行います。

始める前に

IPv4 双方向 PIM グループのランデブーポイントを設定する前に、双方向 PIM がグローバルにイネーブルになっていることを確認します。

手順の概要

1. **ip pim** ［**vrf** *vrf-name*］ **rp-address** *ip-address* ［*access-list*］［**override**］ **bidir**
2. **access-list** *access-list* ［ **permit** | **deny** ］ *ip-address*
3. **ip pim** ［**vrf** *vrf-name*］ **send-rp-announce** *interface-type interface-number* **scope** *ttl-value* ［**group-list** *access-list*］［**interval** *seconds*］［**bidir**］
4. **ip access-list standard** *access-list-name* ［**permit** | **deny**］ *ip-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ip pim**［**vrf** *vrf-name*］**rp-address** *ip-address*［*access-list*］［**override**］**bidir** 例： `Device(config)# ip pim rp-address 10.0.0.1 10 override bidir`	グループのランデブー ポイントの IP アドレスをスタティックに設定します。override オプションを指定する場合、スタティック ランデブー ポイントを使用します。
ステップ 2	**access-list** *access-list*［ **permit** | **deny** ］*ip-address* 例： `Device(config)# access-list 10 permit 224.1.0.0 0.0.255.255`	アクセス リストを設定します。
ステップ 3	**ip pim**［**vrf** *vrf-name*］**send-rp-announce** *interface-type interface-number* **scope** *ttl-value*［**group-list** *access-list*］［**interval** *seconds*］［**bidir**］ 例： `Device(config)# ip pim send-rp-announce Loopback0 scope 16 group-list c21-rp-list-0 bidir`	自動 RP を使用してルータがランデブー ポイント（RP）として動作するグループを設定するように、システムを設定します。
ステップ 4	**ip access-list standard** *access-list-name*［**permit** | **deny**］*ip-address* 例： `Device(config)# ip access-list standard c21-rp-list-0 permit 230.31.31.1 0.0.255.255`	標準 IP アクセス リストを設定します。

PIM 最短パス ツリーの使用の延期

マルチキャスト ルーティングが送信元ツリーから最短パスツリーに切り替わる前に到達する必要があるトラフィック レートしきい値を設定するには、次の手順を実行します。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
4. **ip pim spt-threshold** {*kbps* | **infinity**} [**group-list** *access-list-number*]
5. **end**
6. **show running-config**
7. **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： `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	**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	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 16 permit 225.0.0.0 0.255.255.255`	標準アクセス リストを作成します。 • *access-list-number* の範囲は 1 ～ 99 です。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、しきい値が適用されるマルチキャスト グループを指定します。 •（任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 4	**ip pim spt-threshold** {*kbps* | **infinity**} [**group-list** *access-list-number*] 例： `Device(config)# ip pim spt-threshold infinity group-list 16`	最短パスツリー（SPT）に移行するまでに到達する必要があるしきい値を指定します。 • *kbps* を指定する場合は、トラフィック レートをキロビット/秒で指定します。デフォルト値は 0 キロビット/秒です。 （注） 有効範囲は 0 ～ 4294967 ですが、デバイス ハードウェアの制限により、0 キロビット/秒以外は無効です。 • **infinity** を指定すると、指定されたグループのすべての送信元で共有ツリーが使用され、送信元ツリーに切り替わらなくなります。

	コマンドまたはアクション	目的
		• （任意）**group-list** *access-list-number* には、ステップ 2 で作成したアクセスリストを指定します。値 0 を指定する場合、またはグループ リストを使用しない場合、しきい値はすべてのグループに適用されます。
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	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-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。

PIM ルータクエリー メッセージ間隔の変更

PIM ルータおよびマルチレイヤスイッチでは、各 LAN セグメント（サブネット）の代表ルータ（DR）になるデバイスを検出するため、PIM ルータクエリメッセージが送信されます。DR は、直接接続された LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。

PIM DM 動作では、IGMPv1 が使用中の場合だけ、DR は意味を持ちます。IGMPv1 には IGMP クエリア選択プロセスがないため、選択された DR は IGMP クエリアとして機能します。PIM-SM 動作では、マルチキャスト送信元に直接接続されたデバイスが DR になります。DR は PIM 登録メッセージを送信し、送信元からのマルチキャスト トラフィックを共有ツリーの下方向へ転送する必要があることを RP に通知します。この場合、DR は最大の IP アドレスを持つデバイスです。

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip pim query-interval** *seconds*

5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **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： `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	**configure terminal** 例： `# 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** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、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。 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。 • 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。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip pim query-interval** *seconds* 例： `Device(config-if)# ip pim query-interval 45`	デバイスが PIM ルータクエリ メッセージを送信する頻度を設定します。 デフォルトは 30 秒です。指定できる範囲は 1 ～ 65535 です。
ステップ 5	**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 6	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-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。

PIM の動作の確認

PIM-SM ネットワークまたは PIM-SSM ネットワークでの IP マルチキャスト動作の確認

PIM-SM ネットワーク環境または PIM-SSM ネットワーク環境で IP マルチキャストの動作を確認する際、まずラストホップルータから検証を開始し、SPTに沿って次々にルータの検証を続け、最後にファースト ホップ ルータの検証を行う方法が効果的です。この確認の目的は、IP マルチキャスト ネットワークを介して IP マルチキャスト トラフィックが適切にルーティングされていることを確認することです。

PIM-SM ネットワークまたは PIM-SSM ネットワークでの IP マルチキャスト動作を確認するには、次の作業を実行します。これらの作業は、ソースとレシーバが想定どおりに動作しない場合に障害のあるホップを検出するのに役立ちます。

（注） パケットが想定された宛先に到達しない場合は、IP マルチキャストのファスト スイッチングをディセーブルにすることを検討してください。ディセーブルにすると、ルータがプロセス スイッチング モードになります。IP マルチキャストのファスト スイッチングをディセーブルにした後、パケットが正しい宛先に到達するようになった場合、問題はIPマルチキャストのファスト スイッチングに関連している可能性があります。

ファースト ホップ ルータでの IP マルチキャストの確認

ファーストホップルータでのIPマルチキャスト動作を確認するには、ファーストホップルータに次のコマンドを入力します。

手順の概要

1. **enable**

2. **show ip mroute** [*group-address*]
3. **show ip mroute active** [*kb/s*]

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	**show ip mroute** [*group-address*]
	例：
	`Device# show ip mroute 239.1.2.3`
	`(*, 239.1.2.3), 00:18:10/stopped, RP 172.16.0.1, flags: SPF`
	`Incoming interface: Serial1/0, RPF nbr 172.31.200.2`
	`Outgoing interface list: Null`
	`(10.0.0.1, 239.1.2.3), 00:18:10/00:03:22, flags: FT`
	`Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0`
	`Outgoing interface list:`
	`Serial1/0, Forward/Sparse, 00:18:10/00:03:19`
		ファースト ホップ ルータの mroute に F フラグが設定されていることを確認します。

ステップ 3	**show ip mroute active** [*kb/s*]
	例：
	`Device# show ip mroute active`
	`Active IP Multicast Sources - sending >= 4 kbps`
	`Group: 239.1.2.3, (?)`
	`Source: 10.0.0.1 (?)`
	`Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)`
		グループに送信しているアクティブなマルチキャスト送信元に関する情報を表示します。このコマンドの出力では、アクティブなソースのマルチキャスト パケット レートに関する情報が示されます。
		（注） デフォルトでは、**show ip mroute** コマンドと **active** キーワードによる出力では、4 kb/s 以上のレートでグループにトラフィックを送信するアクティブなソースの情報が表示されます。より低いレートのトラフィック（4 kb/s 未満のトラフィック）をグループに送信しているアクティブなソースに関する情報を表示する場合は、*kb/s* 引数に 1 の値を指定します。この引数に 1 の値を指定すると、1 kb/s 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソース トラフィックに関する情報が効果的に表示されます。

SPT 上のルータでの IP マルチキャストの確認

PIM-SM または PIM-SSM ネットワーク内の SPT 上のルータでの IP マルチキャスト動作を確認するには、SPT 上のルータに次のコマンドを入力します。

手順の概要

1. **enable**
2. **show ip mroute** [*group-address*]
3. **show ip mroute active**

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	**show ip mroute** [*group-address*]
	例：
	`Device# show ip mroute 239.1.2.3`
	`(*, 239.1.2.3), 00:17:56/00:03:02, RP 172.16.0.1, flags: S`
	`Incoming interface: Null, RPF nbr 0.0.0.0`
	`Outgoing interface list:`
	`GigabitEthernet0/0/0, Forward/Sparse, 00:17:56/00:03:02`
	`(10.0.0.1, 239.1.2.3), 00:15:34/00:03:28, flags: T`
	`Incoming interface: Serial1/0, RPF nbr 172.31.200.1`
	`Outgoing interface list:`
	`GigabitEthernet0/0/0, Forward/Sparse, 00:15:34/00:03:02`
		特定のグループの送信元に対する RPF ネイバーを確認します。

ステップ 3	**show ip mroute active**
	例：
	`Device# show ip mroute active`
	`Active IP Multicast Sources - sending >= 4 kbps`
		グループに送信しているアクティブなマルチキャスト送信元に関する情報を表示します。このコマンドの出力では、アクティブなソースのマルチキャスト パケット レートに関する情報が示されます。

	コマンドまたはアクション	目的

	`Group: 239.1.2.3, (?)`
	`  Source: 10.0.0.1 (?)`
	`  Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)`
		（注） デフォルトでは、**show ip mroute** コマンドと **active** キーワードによる出力では、4 kb/s 以上のレートでグループにトラフィックを送信するアクティブなソースの情報が表示されます。より低いレートのトラフィック（4 kb/s 未満のトラフィック）をグループに送信しているアクティブなソースに関する情報を表示する場合は、*kb/s* 引数に 1 の値を指定します。この引数に 1 の値を指定すると、1 kb/s 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソース トラフィックに関する情報が効果的に表示されます。

ラスト ホップ ルータでの IP マルチキャスト動作の確認

ラスト ホップ ルータでの IP マルチキャスト動作を確認するには、ラスト ホップ ルータで次のコマンドを入力します。

手順の概要

1. **enable**
2. **show ip igmp groups**
3. **show ip pim rp mapping**
4. **show ip mroute**
5. **show ip interface** [*type number*]
6. **show ip mfib**
7. **show ip pim interface count**
8. **show ip mroute count**
9. **show ip mroute active** [*kb/s*]

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）。

	コマンドまたはアクション	目的

ステップ 2	**show ip igmp groups**
	例：
	`Device# show ip igmp groups`
	`IGMP Connected Group Membership`
	`Group Address Interface Uptime Expires Last Reporter`
	`239.1.2.3 GigabitEthernet1/0/0 00:05:14 00:02:14 10.1.0.6`
	`224.0.1.39 GigabitEthernet0/0/0 00:09:11 00:02:08 172.31.100.1`
		ラスト ホップ ルータの IGMP メンバーシップを確認します。この情報によって、ラスト ホップ ルータに直接接続され、IGMP を介して認識されるレシーバが使用されているマルチキャスト グループが確認されます。

ステップ 3	**show ip pim rp mapping**
	例：
	`Device# show ip pim rp mapping`
	`PIM Group-to-RP Mappings`
	
	`Group(s) 224.0.0.0/4`
	`RP 172.16.0.1 (?), v2v1`
	`Info source: 172.16.0.1 (?), elected via Auto-RP`
	`Uptime: 00:09:11, expires: 00:02:47`
		グループと RP 間のマッピングがラスト ホップ ルータで正しく生成されていることを確認します。
		（注） PIM/SSM ネットワークでラスト ホップ ルータを確認する場合は、この手順を無視してください。PIM-SSM ではランデブーポイント（RP）が使用されないため、**show ip pim rp mapping** コマンドは PIM/SSM ネットワーク内のルータでは動作しません。さらに、正しく設定されている場合は、PIM/SSM グループは **show ip pim rp mapping** コマンドの出力には表示されません。

ステップ 4	**show ip mroute**
	例：
	`Device# show ip mroute`
	`(*, 239.1.2.3), 00:05:14/00:03:04, RP 172.16.0.1, flags: SJC`
	`Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1`
	`Outgoing interface list:`
	`GigabitEthernet1/0, Forward/Sparse, 00:05:10/00:03:04`
	
	`(10.0.0.1, 239.1.2.3), 00:02:49/00:03:29, flags: T`
	`Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1`
	`Outgoing interface list:`
	`GigabitEthernet1/0, Forward/Sparse, 00:02:49/00:03:04`
	
	`(*, 224.0.1.39), 00:10:05/stopped, RP 0.0.0.0, flags: DC`
	`Incoming interface: Null, RPF nbr 0.0.0.0`
	`Outgoing interface list:`
	`GigabitEthernet1/0, Forward/Sparse, 00:05:15/00:00:00`
	`GigabitEthernet0/0, Forward/Sparse, 00:10:05/00:00:00`
		mroute テーブルがラスト ホップ ルータに正しく入力されていることを確認します。

	コマンドまたはアクション	目的
	(172.16.0.1, 224.0.1.39), 00:02:00/00:01:33, flags: PTX Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1	

ステップ 5	**show ip interface** [*type number*]
	例：
	Device# **show ip interface GigabitEthernet 0/0/0**
	GigabitEthernet0/0/0 is up, line protocol is up
	  Internet address is 172.31.100.2/24
	  Broadcast address is 255.255.255.255
	  Address determined by setup command
	  MTU is 1500 bytes
	  Helper address is not set
	  Directed broadcast forwarding is disabled
	  Multicast reserved groups joined: 224.0.0.1 224.0.0.22 224.0.0.13
	  224.0.0.5 224.0.0.6
	  Outgoing access list is not set
	  Inbound access list is not set
	  Proxy ARP is enabled
	  Local Proxy ARP is disabled
	  Security level is default
	  Split horizon is enabled
	  ICMP redirects are always sent
	  ICMP unreachables are always sent
	  ICMP mask replies are never sent
	  IP fast switching is enabled
	  IP fast switching on the same interface is disabled
	  IP Flow switching is disabled
	  IP CEF switching is disabled
	  IP Fast switching turbo vector
	  IP multicast fast switching is enabled
	  IP route-cache flags are Fast
	  Router Discovery is disabled
	  IP output packet accounting is disabled
	  IP access violation accounting is disabled
	  TCP/IP header compression is disabled
	  RTP/IP header compression is disabled
	  Policy routing is disabled
	  Network address translation is disabled
	  WCCP Redirect outbound is disabled
	  WCCP Redirect inbound is disabled
	  WCCP Redirect exclude is disabled
	  BGP Policy Mapping is disabled
		マルチキャスト高速スイッチングがイネーブルになっており、ラスト ホップ ルータの発信インターフェイスでのパフォーマンスが最適化されていることを確認します。
		（注） **no ip mroute-cache** インターフェイスコマンドを使用すると、IPマルチキャスト高速スイッチングがディセーブルになります。IPマルチキャスト高速スイッチングがディセーブルになると、プロセススイッチド パスを介してパケットが転送されます。

ステップ 6	**show ip mfib** 例： Device# **show ip mfib**	IP マルチキャスト転送情報ベース（MFIB）の転送エントリとインターフェイスが表示されます。
ステップ 7	**show ip pim interface count** 例： Device# **show ip pim interface count** State: * - Fast Switched, H - Hardware Switching Enabled	マルチキャスト トラフィックがラスト ホップ ルータに転送されることを確認します。

	コマンドまたはアクション	目的
	Address Interface FS Mpackets In/Out 172.31.100.2 GigabitEthernet0/0/0 * 4122/0 10.1.0.1 GigabitEthernet1/0/0 * 0/3193	
ステップ 8	**show ip mroute count** 例： Device# **show ip mroute count** IP Multicast Statistics 6 routes using 4008 bytes of memory 3 groups, 1.00 average sources per group Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc) Group: 239.1.2.3, Source count: 1, Packets forwarded: 3165, Packets received: 3165 RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0 Source: 10.0.0.1/32, Forwarding: 3165/20/28/4, Other: 0/0/0 Group: 224.0.1.39, Source count: 1, Packets forwarded: 21, Packets received: 120 Source: 172.16.0.1/32, Forwarding: 21/1/48/0, Other: 120/0/99 Group: 224.0.1.40, Source count: 1, Packets forwarded: 10, Packets received: 10 Source: 172.16.0.1/32, Forwarding: 10/1/48/0, Other: 10/0/0	マルチキャスト トラフィックがラスト ホップ ルータに転送されることを確認します。
ステップ 9	**show ip mroute active** [*kb/s*] 例： Device# **show ip mroute active** Active IP Multicast Sources - sending >= 4 kbps Group: 239.1.2.3, (?) Source: 10.0.0.1 (?)	ラスト ホップ ルータ上のグループにトラフィックを送信しているアクティブなマルチキャスト ソースに関する情報を表示します。このコマンドの出力では、アクティブなソースのマルチキャスト パケット レートに関する情報が示されます。

	コマンドまたはアクション	目的
	`Rate: 20 pps/4 kbps(1sec), 4 kbps(last 50 secs), 4 kbps(life avg)`	（注） デフォルトでは、**show ip mroute** コマンドと **active** キーワードによる出力では、4 kb/s 以上のレートでグループにトラフィックを送信するアクティブなソースの情報が表示されます。より低いレートのトラフィック（4 kb/s 未満のトラフィック）をグループに送信しているアクティブなソースに関する情報を表示する場合は、*kb/s* 引数に 1 の値を指定します。この引数に 1 の値を指定すると、1 kb/s 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソース トラフィックに関する情報が効果的に表示されます。

PIM 対応ルータを使用した IP マルチキャストの到達可能性のテスト

管理しているすべての PIM 対応ルータおよびアクセス サーバーが、マルチキャスト グループのメンバで、すべてのルータが応答する原因となる ping が送信されます。これは、効果的な管理およびデバッグのツールです。

PIM 対応ルータを使用して IP マルチキャストの到達可能性をテストするには、次の作業を実行します。

マルチキャスト ping に応答するルータの設定

ルータがマルチキャスト ping に応答するように設定するには、次の手順を実行します。1 つのルータ上のすべてのインターフェイスと、マルチキャスト ネットワーク内のすべてのルータ上のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip igmp join-group** *group-address*
5. マルチキャスト ネットワークに加入しているルータ上のインターフェイスで、ステップ 3 とステップ 4 を繰り返します。
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/0`	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。 *type* 引数および *number* 引数には、ホストに直接接続されているインターフェイス、またはホストに対応しているインターフェイスを指定します。
ステップ 4	**ip igmp join-group** *group-address* 例： `Device(config-if)# ip igmp join-group 225.2.2.2`	（任意）指定したグループに加入するようにルータ上のインターフェイスを設定します。 この作業の目的として、マルチキャスト ネットワークに加入しているルータ上のすべてのインターフェイス上で、*group-address* 引数に同じグループ アドレスを設定します。 （注） この方法では、ルータは、マルチキャスト パケットの転送に加えて、マルチキャスト パケットを受信します。マルチキャスト パケットを受信することにより、ルータの高速スイッチングは行われません。
ステップ 5	マルチキャスト ネットワークに加入しているルータ上のインターフェイスで、ステップ 3 とステップ 4 を繰り返します。	--
ステップ 6	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。

マルチキャスト ping に応答するように設定されたルータへの ping

マルチキャスト ping に応答するように設定されているルータに対して ping テストを開始するには、ルータで次の手順を実行します。このタスクは、ネットワーク内の IP マルチキャストの到達可能性のテストに使用します。

手順の概要

1. **enable**
2. **ping** *group-address*

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	**ping** *group-address* 例： `Device# ping 225.2.2.2`	IP マルチキャスト グループ アドレスを ping します。 正常な応答は、グループ アドレスが機能していることを示します。

PIM のモニタリングとトラブルシューティング

PIM 情報のモニタリング

PIM 設定をモニターするには、次の表に記載された特権 EXEC コマンドを使用します。

表 *15 : PIM* モニタリング コマンド

コマンド	目的
show ip pim all-vrfs tunnel [**tunnel** *tunnel_number* | **verbose**]	すべての VRF を表示します。
show ip pim autorp	グローバル Auto-RP 情報を表示します。
show ip pim boundary	インターフェイスに設定された、管理スコープ IPv4 マルチキャスト境界によってフィルタリングされた mroute に関する情報を表示します。

コマンド	目的
show ip pim interface	Protocol Independent Multicast（PIM）のために設定されているインターフェイスに関する情報を表示します。
show ip pim neighbor	PIM ネイバー情報を表示します。
show ip pim rp[*group-name* | *group-address*]	スパース モードのマルチキャスト グループに関連付けられた RP ルータを表示します。このコマンドは、すべてのソフトウェア イメージで使用できます。
show ip pim tunnel [**tunnel** | **verbose**]	Protocol Independent Multicast（PIM）トンネル インターフェイスに関する情報を表示します。
show ip pim vrf { **word** { **all-vrfs** | **autorp** | **boundary** | **bsr-router** | **interface** | **mdt** | **neighbor** | **rp** | **rp-hash** | **tunnel** } }	VPN ルーティング/転送インスタンスを表示します。
show ip igmp groups detail	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。

RP マッピングおよび BSR 情報のモニタリング

次の表に示す特権 EXEC モードを使用して、グループ/RP マッピングの一貫性を確認します。

表 *16 : RP* マッピングのモニタリング コマンド

コマンド	目的
show ip pim rp [*hostname* または *IP address* | **mapping** [*hostname* または *IP address* | **elected** | **in-use**] | **metric** [*hostname* または *IP address*]]	使用可能なすべての RP マッピングおよびメトリックを表示します。これにより、（BSR または Auto-RP メカニズムを通じて）デバイスがどのように RP を学習するかがわかります。 • （任意）*hostname* を指定する場合は、RP を表示するグループの IP 名を指定します。 • （任意）*IP address* を指定する場合は、RP を表示するグループの IP アドレスを指定します。 • （任意）シスコ デバイスによって認識されている（設定されている、または Auto-RP によって取得されている）すべてのグループ/RP マッピングを表示するには、**mapping** キーワードを使用します。 • （任意）**metric** キーワードを使用して、RP RPF メトリックを表示します。
show ip pim rp-hash *group*	指定したグループに選択されている RP を表示します。つまり、PIMv2 ルータまたはマルチレイヤスイッチ上で、PIMv1 システムで選択されている RP と同じ RP が使用されていることを確認します。*group* には、RP 情報を表示するグループ アドレスを入力します。

BSR の情報をモニターするには、次の表に示す特権 EXEC コマンドを使用します。

表 *17 : VTP* モニタリング コマンド

コマンド	目的
show ip pim bsr	選択された BSR に関する情報を表示します。
show ip pim bsr-router	BSRv2 に関する情報を表示します。

PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング

PIMv1 および PIMv2 間の相互運用性に関する問題をデバッグするには、次の点を順にチェックします。

1. **show ip pim rp-hash** 特権 EXEC コマンドを使用して RP マッピングを確認し、すべてのシステムが同じグループの同じ RP に同意していることを確認します。
2. DR と RP の各バージョン間の相互運用性を確認し、RP が DR と適切に相互作用していることを確認します（この場合は、登録停止に応答し、カプセル化が解除されたデータ パケットをレジスタから転送します）。

IPv4 双方向 PIM 情報のモニタリング

双方向の PIM 設定をモニターするには、次の表に記載された特権 EXEC コマンドを使用します。

コマンド	目的
show ip mfib	双方向 PIM の MFIB 情報を表示します。
show platform software fed switch {*switch-number* | **active** | **standby** } **ip multicast groups**	プラットフォーム依存IPマルチキャストテーブルおよびその他の情報を表示します。
show ip pim [**vrf** *vrf-name*] **interface** *interface-type interface-number* **df** [*rp-address*]	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。
show ip pim [**vrf** *vrf-name*] **rp** [**mapping** | **metric**] [*rp-address*]	関連マルチキャスト ルーティング エントリとともにキャッシュされているアクティブ ランデブー ポイントを表示します。
show platform software fed switch {*switch-number* | **active** | **standby** }**ip multicast df** [**vrf-id** *vrf-id* | **vrf-name** *vrf-name*] [*df-index*]	IPマルチキャスト指定フォワーダ（DF）に関する情報を表示します。

PIM の設定例

例：PIM スタブ ルーティングのイネーブル化

次の例では、IP マルチキャスト ルーティングがイネーブルになっており、スイッチ A の PIM アップリンク ポート 25 はルーテッド アップリンク ポートとして設定されています（**spare-dense-mode** がイネーブル）。VLAN 100 インターフェイスとギガビット イーサネット ポート 20 で PIM スタブ ルーティングがイネーブルに設定されています。

```
Device(config)# ip multicast-routing
Device(config)# interface GigabitEthernet3/0/25
Device(config-if)# no switchport
Device(config-if)# ip address 3.1.1.2 255.255.255.0
Device(config-if)# ip pim sparse-dense-mode
Device(config-if)# exit
```

```
Device(config)# interface vlan100
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface GigabitEthernet3/0/20
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface vlan100
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface GigabitEthernet3/0/20
Device(config-if)# no switchport
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# ip pim passive
Device(config-if)# end
```

例：PIM スタブ ルーティングの確認

各インターフェイスのPIMスタブがイネーブルになっていることを確認するには、**show ip pim interfac** 特権 EXEC コマンドを使用します。

```
デバイス# show ip pim interface
Address Interface Ver/ Nbr Query DR DR
Mode Count Intvl Prior
3.1.1.2 GigabitEthernet3/0/25 v2/SD 1 30 1 3.1.1.2
100.1.1.1 Vlan100 v2/P 0 30 1 100.1.1.1
10.1.1.1 GigabitEthernet3/0/20 v2/P 0 30 1 10.1.1.1
```

例：マルチキャスト グループへの RP の手動割り当て

次に、マルチキャスト グループ 225.2.2.2 の場合だけ、RP のアドレスを 147.106.6.22 に設定する例を示します。

```
デバイス(config)# access-list 1 permit 225.2.2.2 0.0.0.0
デバイス(config)# ip pim rp-address 147.106.6.22 1
```

例：Auto-RP の設定

次に、最大ホップ数が 31 であるすべての PIM 対応インターフェイスから RP アナウンスメントを送信する例を示します。ポート 1 の IP アドレスが RP です。アクセス リスト 5 には、この deviceが RP として機能するグループが記述されています。

```
デバイス(config)# ip pim send-rp-announce gigabitethernet1/0/1 scope 31 group-list 5
デバイス(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```

例：Auto-RP でのスパース モード

次の例では、Auto-RP でスパース モードを設定しています。

```
ip multicast-routing
ip pim autorp listener
ip pim send-rp-announce Loopback0 scope 16 group-list 1
ip pim send-rp-discovery Loopback1 scope 16
no ip pim dm-fallback
access-list 1 permit 239.254.2.0 0.0.0.255
access-list 1 permit 239.254.3.0 0.0.0.255
.
.
.
access-list 10 permit 224.0.1.39
access-list 10 permit 224.0.1.40
access-list 10 permit 239.254.2.0 0.0.0.255
access-list 10 permit 239.254.3.0 0.0.0.255
```

例：Auto-RP 情報を拒否する IP マルチキャスト境界の定義

次に、自動 RP 情報を拒否する IP マルチキャスト境界のコンフィギュレーション例の一部を示します。

```
デバイス(config)# access-list 1 deny 224.0.1.39
デバイス(config)# access-list 1 deny 224.0.1.40
デバイス(config)# access-list 1 permit all
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip multicast boundary 1
```

例：着信 RP アナウンスメント メッセージのフィルタリング

次に、候補 RP アナウンスメントが不正な候補 RP から許可されないようにするために使用される自動 RP マッピング エージェントの設定例を示します。

```
デバイス(config)# ip pim rp-announce-filter rp-list 10 group-list 20
デバイス(config)# access-list 10 permit host 172.16.5.1
デバイス(config)# access-list 10 permit host 172.16.2.1
デバイス(config)# access-list 20 deny 239.0.0.0 0.0.255.255
デバイス(config)# access-list 20 permit 224.0.0.0 15.255.255.255
```

マッピング エージェントは 2 つのデバイス（172.16.5.1 および 172.16.2.1）からの候補 RP アナウンスだけを許可します。マッピング エージェントは 2 つのデバイスからの候補 RP アナウンスメントのうち、グループ範囲が 224.0.0.0 ～ 239.255.255.255 であるマルチキャスト グループ宛てのアナウンスメントだけを許可します。マッピングエージェントは、ネットワーク内の他のデバイスからの候補 RP アナウンスメントを許可しません。さらに、候補 RP アナウンスメントが 239.0.0.0 ～ 239.255.255.255 の範囲のグループに宛てたものである場合、マッピング エージェントは 172.16.5.1 または 172.16.2.1 からの候補 RP アナウンスメントを許可しません。この範囲は、管理の有効範囲付きアドレス範囲です。

例：問題のある RP への Join メッセージの送信禁止

すべてのインターフェイスが SM の場合はデフォルト設定の RP を使用し、既知のグループ 224.0.1.39 および 224.0.1.40 をサポートします。自動 RP はこれら 2 つの既知のグループを使用し、RP マッピング情報を収集、配信します。**ip pim accept-rp auto-rp** コマンドが設定されている場合は、RP を許可する別の **ip pim accept-rp** コマンドを次のように設定してください。

```
デバイス(config)# ip pim accept-rp 172.10.20.1 1
デバイス(config)# access-list 1 permit 224.0.1.39
デバイス(config)# access-list 1 permit 224.0.1.40
```

例：候補 BSR の設定

次に、候補 BSR の設定例を示します。この例では、アドバタイズ済み BSR アドレスとしてポートの IP アドレス 172.21.24.18 を、hash-mask-length として 30 ビットを使用します。プライオリティは 10 です。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# ip address 172.21.24.18 255.255.255.0
デバイス(config-if)# ip pim sparse-mode
デバイス(config-if)# ip pim bsr-candidate gigabitethernet1/0/2 30 10
```

例：候補 RP の設定

次に、device が自身を候補 RP として PIM ドメイン内の BSR にアドバタイズするよう設定する例を示します。標準アクセス リスト番号 4 により、ポートで識別されるアドレスを持つ RP に対応するグループ プレフィックスが指定されます。この RP は、プレフィックスが 239 であるグループを処理します。

```
デバイス(config)# ip pim rp-candidate gigabitethernet1/0/2 group-list 4
デバイス(config)# access-list 4 permit 239.0.0.0 0.255.255.255
```

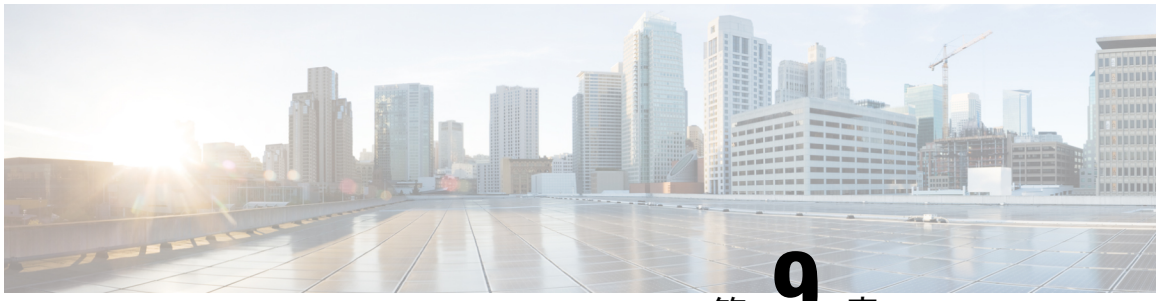
PIM 機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	PIM	PIM（Protocol Independent Multicast）プロトコルは、受信側が開始したメンバーシップの現在の IP マルチキャスト サービス モードを維持します。PIM は、特定のユニキャスト ルーティング プロトコルに依存しません。つまり、IP ルーティング プロトコルに依存せず、ユニキャスト ルーティング テーブルへの入力に使用されるユニキャスト ルーティング プロトコル（Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、Border Gateway Protocol（BGP）、およびスタティック ルート）のいずれも利用できます。PIM は、ユニキャスト ルーティング情報を使用してマルチキャスト転送機能を実行します。
Cisco IOS XE Gibraltar 16.12.1	双方向 PIM	双方向 PIM は、IP マルチキャスト用ルーティングプロトコルの PIM スイートのバリアントです。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。



第 9 章

IP マルチキャストに対する PIM MIB 拡張の設定

IP マルチキャストに対する PIM MIB 拡張について

IP マルチキャストに対する SNMP トラップの PIM MIB 拡張

Protocol Independent Multicast（PIM）は、マルチキャスト データ パケットをマルチキャスト グループにルーティングするために使用される IP マルチキャスト ルーティング プロトコルです。RFC 2934 は、IPv4 用の PIM MIB を定義します。PIM MIB は、Simple Network Management Protocol（SNMP）を使用してユーザーがリモートに PIM を監視および設定できるようにする管理対象オブジェクトを記述したものです。

PIM MIB 拡張では、次の新しいクラスの PIM 通知を導入しています。

- neighbor-change：この通知は、次の条件により発生します。
  - ルータの PIM インターフェイスが（インターフェイス コンフィギュレーション モードで **ip pim** コマンドを使用して）無効化、または有効化されている。
  - ルータの PIM ネイバーの隣接関係が失効している（RFC 2934 の定義による）。
- rp-mapping-change：この通知は、自動RPメッセージまたはブートストラップ ルータ（BSP）メッセージのいずれかが原因で、ランデブー ポイント（RP）マッピング情報が変更された場合に、発生します。
- invalid-pim-message：この通知は、次の条件により発生します。

- 無効な (*, G) Join または Prune メッセージがデバイスで受信された（たとえば、パケットで指定された RP がマルチキャスト グループの RP でない Join または Prune メッセージをルータが受信した場合）
- 無効な PIM 登録メッセージがデバイスで受信された（たとえば、RP ではないマルチキャスト グループから登録メッセージをルータが受信した場合）

PIM MIB 拡張の利点

PIM MIB 拡張：

- ユーザーは、RP マッピングの変更を検出することで、ネットワークのマルチキャスト トポロジの変更を確認できます。
- PIM 対応インターフェイスで PIM プロトコルをモニターするトラップが提供されます。
- マルチキャストの隣接関係がマルチキャスト インターフェイスで期限切れになったときに、ユーザーがルーティングの問題を特定するのを支援します。
- ユーザーが RP 設定エラー（たとえば、Auto-RP などのダイナミック RP 割り当てプロトコルのフラッピングによるエラーなど）をモニターできるようにします。

IP マルチキャストに対する PIM MIB 拡張の設定方法

IP マルチキャストに対する PIM MIB 拡張のイネーブル化

IP マルチキャストに対する PIM MIB 拡張を有効にするには、次のタスクを実行します。

（注）
- pimInterfaceVersion オブジェクトは RFC 2934 から削除されたので、ソフトウェアではサポートされていません。
- 次の MIB テーブルは、シスコ ソフトウェアでサポートされていません。
  - pimIpMRouteTable
  - pimIpMRouteNextHopTable

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pim** [**neighbor-change** | **rp-mapping-change** | **invalid-pim-message**]
4. **snmp-server host** *host-address* [**traps** | **informs**] *community-string* **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	**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	**snmp-server enable traps pim** [**neighbor-change** | **rp-mapping-change** | **invalid-pim-message**] 例： `Device(config)# snmp-server enable traps pim neighbor-change`	デバイスが PIM 通知を送信できるようにします。 • **neighbor-change** ：このキーワードは、デバイスの PIM インターフェイスがディセーブル、またはイネーブルである、あるいはデバイスの PIM 隣接関係が失効していることを示す通知をイネーブル化します。 • **rp-mapping-change** ：このキーワードは、Auto-RP メッセージまたは BSR メッセージによる RP マッピング情報の変更を示す通知をイネーブル化します。 • **invalid-pim-message** ：このキーワードは、無効な PIM プロトコル操作のモニタリングに関する通知をイネーブル化します（たとえば、パケットに指定された RP がマルチキャスト グループの RP ではない Join または Prune メッセージをデバイスが受信する場合、または RP ではないマルチキャスト グループから登録メッセージをデバイスが受信する場合）。
ステップ 4	**snmp-server host** *host-address* [**traps** | **informs**] *community-string* **pim** 例： `Device(config)# snmp-server host 10.10.10.10 traps public pim`	PIM SNMP 通知操作の受信者を指定します。

PIM MIB 拡張の設定例

IP マルチキャストに対する PIM MIB 拡張のイネーブル化の例

次の例に、ルータの PIM インターフェイスが有効になっていることを示す通知を生成するようにルータを設定する方法を示します。最初の行では、IP アドレスが 10.0.0.1 のホストに SNMP v2c トラップとして送信されるよう、PIM トラップが設定されます。2 行目では、トラップ通知の neighbor-change クラスをホストに送信するよう、ルータが設定されます。

```
snmp-server host 10.0.0.1 traps version 2c public pim
snmp-server enable traps pim neighbor-change
interface ethernet0/0
 ip pim sparse-mode
```

IP マルチキャストに対する PIM MIB 拡張に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)*

標準および RFC

標準/RFC	タイトル
draft-kouvelas-pim-bidir-new-00.txt	『A New Proposal for Bi-directional PIM』
RFC 1112	『Host Extensions for IP Multicasting』
RFC 1918	『Address Allocation for Private Internets』
RFC 2770	『GLOP Addressing in 233/8』
RFC 3569	『An Overview of Source-Specific Multicast (SSM)』

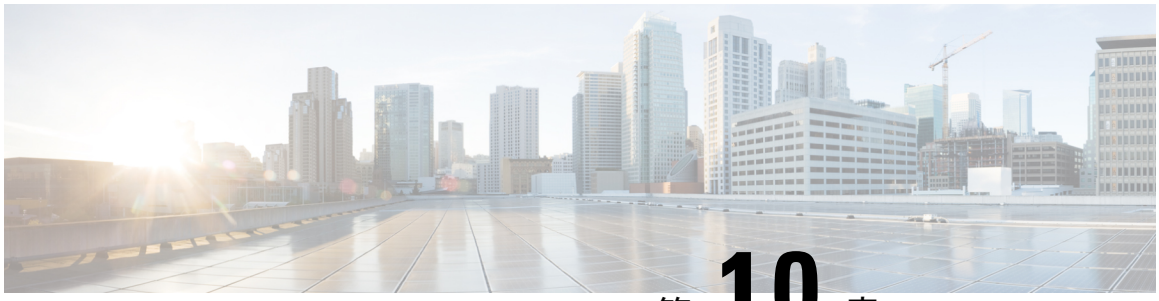
IP マルチキャストに対する PIM MIB 拡張の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IP マルチキャストに対する PIM MIB 拡張	Protocol Independent Multicast（PIM）は、マルチキャスト データ パケットをマルチキャスト グループにルーティングするために使用される IP マルチキャスト ルーティング プロトコルです。RFC 2934 は、IPv4 用の PIM MIB を定義します。PIM MIB は、Simple Network Management Protocol（SNMP）を使用してユーザーがリモートに PIM を監視および設定できるようにする管理対象オブジェクトを記述したものです。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。



第 10 章

MSDP の設定

MSDP を使用した複数の PIM-SM ドメインの相互接続の前提条件

MSDP を設定する前に、すべての MSDP ピアのアドレスが Border Gateway Protocol（BGP）で認識されている必要があります。

MSDP を使用して複数の PIM-SM ドメインを相互接続するための情報

ここでは、MSDP を使用した複数の PIM-SM ドメインの相互接続について説明します。

MSDP を使用した複数の PIM-SM ドメインの相互接続の利点

- ランデブー ポイント(RP)が動的にドメイン外のアクティブな送信元を検出できます。
- 複数のドメイン間でマルチキャスト配信ツリーを構築するための、より管理しやすいアプローチが導入されます。

複数の PIM-SM ドメインを相互接続するための MSDP の使用

MSDP は複数の PIM-SM ドメインを接続するメカニズムです。MSDP は、他の PIM ドメイン内のマルチキャスト送信元を検出することを目的としています。MSDP の主な利点は、（一般的な共有ツリーではなく）ドメイン間ソース ツリーを PIM-SM ドメインで使用できるようにし、複数の PIM-SM ドメインを相互接続する複雑性を軽減することです。MSDP がネットワークで設定されている場合、RP は他のドメイン内の RP と送信元情報を交換します。RP は、レシーバがいるグループに送信するソースのドメイン間ソース ツリーに参加できます。RP は、そのドメイン内の共有ツリーのルートであり、アクティブ レシーバが存在するドメイン内のすべてのポイントへのブランチがあるため、これを行うことができます。PIM-SM ドメイン外の新しい送信元を（共有ツリーの送信元からのマルチキャストパケットの到着によって）ラスト ホップ デバイスが認識すると、その送信元に加入要求を送信してドメイン間ソース ツリーに参加できます。

（注） RP に特定グループの共有ツリーがないか、発信インターフェイス リストがヌルの共有ツリーがある場合は、別のドメインの発信元に加入要求を送信しません。

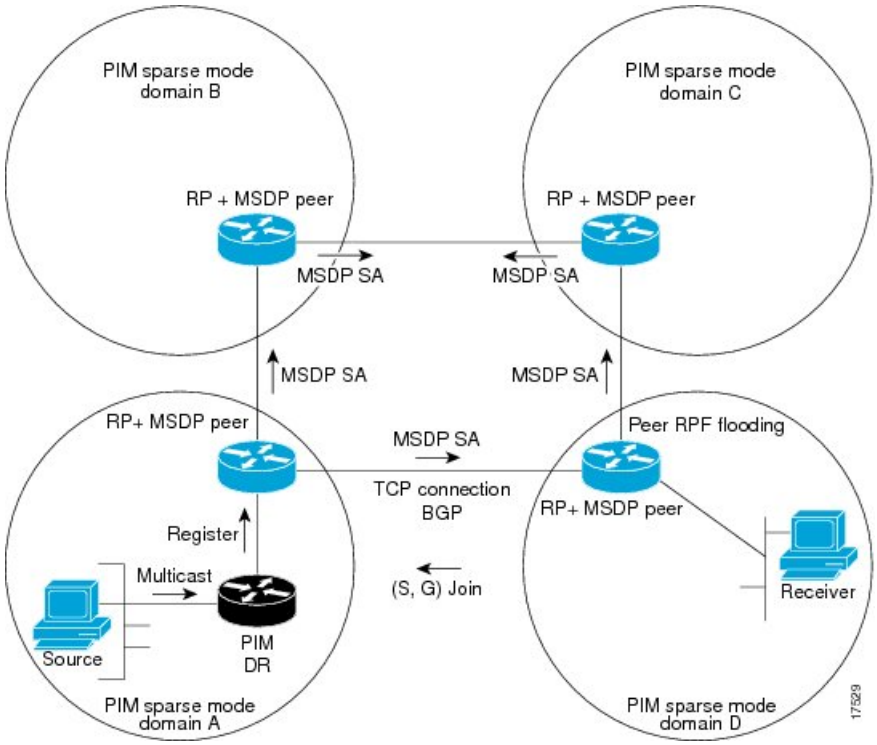
MSDP がイネーブルになっている場合、PIM-SM ドメインの RP は、他のドメインの MSDP 対応デバイスとの MSDP ピアリング関係を維持します。このピアリング関係は TCP 接続を通じて発生します。交換されるのは主にマルチキャスト グループを送信する送信元のリストです。MSDP はピアリング接続に TCP（ポート 639）を使用します。BGP と同様に、ポイントツーポイント TCP ピアリングを使用する場合は、各ピアを明示的に設定する必要があります。さらに、RP 間の TCP 接続は基本的なルーティング システムによって実現されます。受信側の RP では、送信元リストを使用して送信元のパスが確立されます。マルチキャスト ソースがレシーバがいるドメインの対象である場合、マルチキャスト データは PIM-SM で提供される通常のソース ツリー構築メカニズムを使用して配信されます。MSDP は、グループを送信する送信元のアナウンスにも使用されます。これらのアナウンスは、ドメインの RP で発信する必要があります。

（注） MSDP は、ドメイン間動作を行うための BGP または Multiprotocol BGP（MBGP）によって異なります。グローバル マルチキャスト グループに送信する RP で MSDP を実行することを推奨します。

図に、2 つの MSDP ピア間の MSDP の動作を示します。PIM では、ドメインの RP に送信元を登録するための標準メカニズムとして、MSDP が使用されます。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *18 : RP* ピア間で動作する *MSDP*



MSDP が実装されている場合、次のイベント シーケンスが発生します。

1. 図に示すように、PIM 指定デバイス（DR）が送信元を RP に登録すると、その RP が Source-Active（SA）メッセージをすべての MSDP ピアに送信します。

（注） DR は、（ソースがアクティブになると）カプセル化されたデータをソースごとに 1 回だけ RP に送信します。ソースがタイムアウトした場合、ソースが再度アクティブになるとこのプロセスが実行されます。これは、発信元 RP に登録されているすべての発信元を含んでいる定期的な SA メッセージの場合とは異なります。これらの SA メッセージは MSDP 制御パケットであるため、アクティブな送信元からのカプセル化されたデータを含んでいません。

1. SA メッセージでは、ソース アドレス、ソースの送信先グループ、および RP のアドレスまたは発信者 ID が識別されます（設定されている場合）。

2. SA メッセージを受信する各 MSDP ピアは、発信者からのダウンストリームのすべてのピアに SA メッセージをフラッディングします。場合によっては（図の PIM-SM ドメイン B および C 内の RP の場合など）、RP は複数の MSDP ピアからの SA メッセージのコピーを受信することがあります。ループが作成されないように、RP は BGP ネクスト ホップ データベースに問い合わせて、SA メッセージの発信者へのネクスト ホップを識別します。MBGP とユニキャスト BGP の両方が設定されている場合、MBGP が最初に確認されてからユニキャスト BGP が確認されます。そのネクストホップ ネイバーが発信元の RPF ピアです。RPF ピアへのインターフェイス以外のインターフェイスにある発信元から受信した

SA メッセージはドロップされます。そのため、SA メッセージ フラッディング プロセスはピア RPF フラッディングと呼ばれます。ピア RPF フラッディング メカニズムにより、BGP または MBGP は MSDP とともに実行する必要があります。

（注）

- (M)BGP は MSDP メッシュ グループのシナリオでは必須ではありません。MSDP メッシュ グループの詳細については、「MSDP メッシュ グループの設定（247 ページ）」を参照してください。
- （M）BGP は、デフォルト MSDP ピアのシナリオまたは MSDP ピアが 1 つだけ設定されているシナリオでは必要ありません。詳細については、デフォルトの MSDP ピアの設定（246 ページ）の項を参照してください。

1. SA メッセージを受信した RP は、グループの (*, G) 送信インターフェイス リストにインターフェイスが存在するかどうかを確認することによって、そのドメイン内にアドバタイズされたグループのメンバが存在するかどうかを確認します。グループ メンバが存在しない場合、RP は何も実行しません。グループ メンバが存在する場合、RP は（S, G）加入要求を送信元に送信します。その結果、ドメイン間ソース ツリーのブランチが自律システムの RP との境界に構築されます。マルチキャスト パケットは、RP に着信すると、その共有ツリーを経由して RP のドメイン内のグループ メンバに転送されます。メンバの DR は、標準的な PIM-SM 手順を使用してソースへのランデブー ポイント ツリー（RPT）に加入することもできます。
2. 発信元 RP は、送信元がグループにパケットを送信し続ける限り、60 秒ごとに（S, G）ステートに関する SA メッセージを定期的に送信し続けます。RP は SA メッセージを受信すると、SA メッセージをキャッシュします。たとえば、発信元 RP 10.5.4.3 から (172.16.5.4, 228.1.2.3) に対する SA メッセージを受信したとします。RP は mroute テーブルを確認し、グループ 228.1.2.3 にアクティブなメンバが存在しないことを検出すると、SA メッセージを 10.5.4.3 のダウンストリームにあるピアに渡します。次に、ドメイン内のホストが加入要求をグループ 228.1.2.3 の RP に送信した場合、その RP はホストへのインターフェイスを (*, 224.1.2.3) エントリの発信インターフェイス リストに追加します。RP は SA メッセージをキャッシュするため、デバイスは (172.16.5.4, 228.1.2.3) のエントリを持ち、ホストが加入を要求するとすぐにソース ツリーに加入できます。

（注） 現行のすべてのサポート対象のソフトウェア リリースでは、MSDP SA メッセージのキャッシュは必須であり、手動でイネーブルまたはディセーブルにすることはできません。デフォルトでは、MSDP ピアが設定されると、**ip multicast cache-sa-state** コマンドが自動的に実行コンフィギュレーションに追加されます。

MSDP メッセージ タイプ

MSDP メッセージには4つの基本タイプがあり、それぞれが固有の Type、Length、および Value（TLV）データ フォーマットでエンコードされています。

SA メッセージ

SA メッセージを使用して、ドメイン内のアクティブなソースをアドバタイズします。また、これらの SA メッセージには送信元によって送信された最初のマルチキャスト データ パケットが含まれていることがあります。

SA メッセージには、発信元 RP の IPアドレスと、アドバタイズされる 1 つ以上の（S, G）ペアが含まれています。また、SA メッセージにカプセル化されたデータ パケットが含まれていることがあります。

（注） SA メッセージの詳細については、SA メッセージの発信、受信および処理 （226 ページ）を参照してください。

SA 要求メッセージ

SA要求メッセージを使用して、特定のグループにアクティブなソースのリストを要求します。これらのメッセージは、SA キャッシュにアクティブな（S,G）ペアのリストを保持する MSDP SA キャッシュに送信されます。グループ内のすべてのアクティブなソースが発信元の RP によって再アドバタイズされるまで待つ代わりに、SA 要求メッセージを使用してアクティブなソースのリストを要求すると、加入遅延を短縮できます。

（注） SA 要求メッセージの詳細については、MSDP ピアへの送信元情報の要求 （252 ページ）を参照してください。

SA 応答メッセージ

SA 応答メッセージは SA 要求メッセージに応答する MSDP ピアによって送信されます。SA 応答メッセージには、発信元の RP の IP アドレスと、キャッシュに保存されている発信元 RP のドメイン内のアクティブなソースの 1 つ以上の（S, G）ペアが含まれています。

（注） SA 応答メッセージの詳細については、SA 要求フィルタを使用した MSDP ピアからの発信 SA 要求メッセージに対する応答の制御 （253 ページ）を参照してください。

キープアライブ メッセージ

キープアライブ メッセージは 60 秒ごとに送信され、MSDP セッションをアクティブに保ちます。キープアライブ メッセージまたは SA メッセージを 75 秒間受信しなかった場合、MSDP セッションがリセットされます。

（注） キープアライブ メッセージの詳細については、MSDP キープアライブ インターバルおよび保留時間インターバルの調整 （244 ページ）を参照してください。

SA メッセージの発信、受信および処理

ここでは、SA メッセージの発信、受信、および処理について詳しく説明します。

SA メッセージの発信

SA メッセージは、ローカル PIM-SM ドメイン内で新しいソースがアクティブになると、RP によってトリガーされます（MSDP が設定されている場合）。ローカル送信元は、RP に直接接続された送信元であるか、または RP に登録済みのファーストホップ DR です。RP は、PIM-SM ドメイン内のローカル送信元（つまり、RP に登録しているローカル送信元）に対してのみ SA メッセージを発信します。

（注） ローカル送信元は、RP の (S, G) mroute エントリに設定されている A フラグによって示されます（**show ip mroute** コマンドの出力で確認できます）。このフラグは、送信元が他の MSDP ピアに対する RP によるアドバタイズメントの候補であることを示します。

送信元がローカルの PIM-SM ドメインにある場合、RP で (S, G) ステートが作成されます。登録メッセージを受信するか、または直接接続された送信元から最初の (S, G) パケットが到着することによって、新しい送信元は RP によって検出されます。ソースから送信された最初のマルチキャスト パケット（登録メッセージにカプセル化されるか、直接接続されているソースから受信します）は、最初の SA メッセージにカプセル化されます。

SA メッセージの受信

SA メッセージは、送信元に戻るベスト パスにある MSDP RPF ピアからのみ受け入れられます。他の MSDP ピアから到着する同じ SA メッセージは無視する必要があり、そうしないと SA ループが発生する可能性があります。到着した SA メッセージの MSDP RPF ピアを確定的に選択するには、MSDP トポロジの知識が必要です。ただし、MSDP はルーティング アップデートの形式でトポロジ情報を配信しません。MSDP は、SA RPF チェック機能に関する MSDP トポロジの最良近似として (M)BGP ルーティング データを使用することで、この情報を推測します。したがって、MSDP トポロジは BGP ピア トポロジと同じ汎用トポロジに従う必要があります。わずかな例外（MSDP メッシュ グループ内のデフォルトの MSDP ピアおよび MSDP ピア）を除き、MSDP ピアは一般的に (M)BGP ピアでもあります。

RPF チェック ルールが SA メッセージに適用される仕組み

SA メッセージの RPF チェックに適用されるルールは、MSDP ピア間の BGP ピアリングに依存します。

- ルール 1：送信側の MSDP ピアが Interior (M)BGP（i（M）BGP）ピアでもある場合に適用されます。
- ルール 2：送信側の MSDP ピアが exterior (M)BGP ピアでもある場合に適用されます。
- ルール 3：送信側の MSDP ピアが (M)BGP ピアでない場合に適用されます。

RPF チェックは、次の場合は実行されません。

- 送信側の MSDP ピアが唯一の MSDP ピアであり、唯一の単一の MSDP ピアまたはデフォルトの MSDP ピアが設定されている状況の場合。
- 送信側の MSDP ピアがメッシュ グループのメンバーである場合。
- 送信側の MSDP ピアのアドレスが SA メッセージに含まれる RP アドレスである場合

RPF チェックに適用するルールをソフトウェアが決定する仕組み

ソフトウェアは、次のロジックを使用して、RPF チェックに適用される RPF ルールを決定します。

- 送信側の MSDP ピアと同じ IP アドレスを持つ (M)BGP ネイバーを見つけます。
  - 一致した (M)BGP ネイバーが Internal BGP（iBGP）ピアである場合、ルール 1 を適用します。
  - 一致した（M）BGP ネイバーが External BGP（eBGP）ピアである場合、ルール 2 を適用します。
  - 一致するネイバーが見つからなかった場合、ルール 3 を適用します。

RPF チェック ルール選択の影響は次のとおりです。デバイスで MSDP ピアの設定に使用される IP アドレスは、同じデバイスで (M)BGP ピアの設定に使用される IP アドレスと一致する必要があります。

MSDP における SA メッセージの RPF チェックのルール 1

送信側の MSDP ピアが i(M)BGP ピアでもある場合、MSDP における RPF チェックのルール 1 が適用されます。ルール 1 が適用されると、RPF チェックは次のように行われます。

1. ピアは、BGP マルチキャスト ルーティング情報ベース（MRIB）を検索して SA メッセージを発信した RP への最適パスを探します。MRIB でパスが検出されなかった場合、ピアはユニキャスト ルーティング情報ベース（URIB）を検索します。それでもパスが検出されなかった場合は、RPF チェックは失敗します。

2. 前の検索が成功した（つまり、ベスト パスが見つかった）場合、ピアは、このベスト パスに対する BGP ネイバーのアドレスを判別します。このアドレスは、BGP 更新メッセージでピアにパスを送信した BGP ネイバーのアドレスです。

（注） BGP ネイバーアドレスは、パス内のネクストホップアドレスと同じではありません。i(M)BGP ピアはパスのネクストホップ属性を更新しないので、ネクストホップアドレスは通常、シスコにパスを送信した BGP ピアのアドレスと同じではありません。

BGP ネイバーアドレスは、ピアにパスを送信したピアの BGP ID と必ずしも同じとは限りません。

1. 送信側の MSDP ピアの IP アドレスが BGP ネイバーアドレス（ピアにパスを送信した BGP ピアのアドレス）と同じである場合、RPF チェックは正常に終了します。同じでない場合は、RPF チェックは失敗します。

MSDP に対する RPF チェック ルール 1 の影響

MSDP トポロジでは、（M）BGP トポロジをミラーリングする必要があります。通常、2 つのデバイス間に i(M)BGP ピア接続がある場合は、MSDP ピア接続を設定する必要があります。つまり、遠端 MSDP ピア接続の IP アドレスは、遠端 i（M）BGP ピア接続と同じにする必要があります。自律システム内の i(M)BGP ピア間の BGP トポロジは AS パスによって記述されないため、アドレスは同じである必要があります。別の i（M）BGP ピアへのアップデートの送信時に i（M）BGP ピアがパス内のネクスト ホップ アドレスをアップデートした場合、ピアはネクスト ホップ アドレスを使用して i（M）BGP トポロジ（したがって MSDP トポロジ）を表すことができます。ただし、i(M)BGP ピアのデフォルトの動作ではネクストホップ アドレスがアップデートされないため、ピアは (M)BGP トポロジ（MSDP トポロジ）の記述にネクスト ホップ アドレスを当てにすることができません。その代わりに、i（M）BGP ピアは、パスを送信した i（M）BGP ピアのアドレスを使用して、自律システム内の i（M）BGP トポロジ（MSDP トポロジ）を表します。

ヒント i(M)BGP と MSDP の両方のピア アドレスに同じアドレスが使用されるように、MSDP ピア アドレスの設定時は注意を払う必要があります。

MSDP における SA メッセージの RPF チェックのルール 2

送信側の MSDP ピアが e(M)BGP ピアでもある場合、MSDP における RPF チェックのルール 2 が適用されます。ルール 2 が適用されると、RPF チェックは次のように行われます。

1. ピアは、BGP MRIB を検索して SA メッセージを発信した RP への最適パスを探します。MRIB でパスが検出されなかった場合、ピアは URIB を検索します。それでもパスが検出されなかった場合は、RPF チェックは失敗します。

2. 前の検索が成功した（つまり、ベストパスが見つかった）場合、ピアはパスを調べます。RP へのベスト パス内の最初の自律システムが e(M)BGP ピア（送信側の MSDP ピアでもあ

る）の自律システムと同じである場合、RPF チェックは正常に終了します。同じでない場合は失敗します。

MSDP に対する RPF チェック ルール 2 の影響

MSDP トポロジでは、（M）BGP トポロジをミラーリングする必要があります。通常、2 つのデバイス間に e(M)BGP ピア接続がある場合は、MSDP ピア接続を設定する必要があります。ルール 1 とは対照的に、遠端 MSDP ピア接続の IP アドレスは遠端 e（M）BGP ピア接続と同じである必要はありません。その理由は、2 つの e（M）BGP ピア間の BGP トポロジが AS パスで記述されないためです。

MSDP における SA メッセージの RPF チェックのルール 3

送信側の MSDP ピアが (M)BGP ピアではない場合、RPF チェックのルール 3 が適用されます。ルール 3 が適用されると、RPF チェックは次のように行われます。

1. ピアは、BGP MRIB を検索して SA メッセージを発信した RP への最適パスを探します。MRIB でパスが検出されなかった場合、ピアは URIB を検索します。それでもパスが検出されなかった場合は、RPF チェックは失敗します。
2. 前の検索が成功した（つまり、SA メッセージを発信した RP へのベスト パスが見つかった）場合、ピアは、SA メッセージを送信した MSDP ピアへのベスト パスの BGP MRIB を検索します。MRIB でパスが検出されなかった場合、ピアは URIB を検索します。それでもパスが検出されなかった場合は、RPF チェックは失敗します。

（注） SA メッセージを送信した MSDP ピアの自律システムは発信元自律システムで、これは MSDP ピアへの AS パス内にある最後の自律システムです。

1. RP への最適パス内の最初の自律システムが送信側の MSDP ピアの自律システムと同じである場合、RPF チェックは正常に終了します。同じでない場合は、RPF チェックは失敗します。

SA メッセージの処理

次の手順は、MSDP ピアが SA メッセージを処理するときに実行されます。

1. ピアは SA メッセージの (S, G) ペアのグループ アドレス G を使用して、mroute テーブル内の関連する (*, G) エントリを見つけます。(*, G) エントリが見つかり、その発信インターフェイスのリストがヌルでない場合は、SA メッセージでアドバタイズされる送信元用の PIM-SM ドメインにアクティブな受信者がいます。
2. その後、MSDP ピアは、アドバタイズされた送信元用に (S, G) エントリを作成します。
3. (S, G) エントリがない場合、MSDP ピアはソース ツリーに加入するためにソースへの (S, G) 加入をただちにトリガーします。

4. ピアは SA メッセージをその他のすべての MSDP ピアにフラッディングします。ただし、次を除きます。
   - SA メッセージが受信された MSDP ピア。
   - このデバイスと同じ MSDP メッシュ グループにある MSDP ピア（ピアがメッシュ グループのメンバーである場合）。

（注） SA メッセージは、デバイスの SA キャッシュにローカルに保存されます。

MSDP ピア

BGP と同様に、MSDP は他の MSDP ピアとのネイバー関係を確立します。MSDP ピアは、TCP ポート 639 を使用して接続します。下位の IP アドレス ピアは、TCP 接続のオープンにおいてアクティブな役割を果たします。上位の IP アドレス ピアは、もう一方が接続を行うまで LISTEN ステートで待機します。MSDP ピアは、60 秒ごとにキープアライブ メッセージを送信します。データが着信すると、キープアライブ メッセージと同じ機能が実行され、セッションがタイムアウトにならないようにします。キープアライブ メッセージまたはデータを 75 秒間受信しなかった場合、TCP 接続がリセットされます。

MSDP MD5 パスワード認証

MSDP MD5 パスワード認証機能は、2 つの MSDP ピア間の TCP 接続上で Message Digest 5（MD5）シグネチャの保護を提供するための拡張です。この機能は、TCP 接続ストリームに導入されるスプーフィングされた TCP セグメントの脅威に対して MSDP を保護することにより、追加のセキュリティを提供します。

MSDP MD5 パスワード認証の動作

RFC 2385 に従って開発された、MSDP MD5 パスワード認証機能は、MSDP ピア間の TCP 接続上で送信された各セグメントを検証するために使用されます。**ip msdp password peer** コマンドは、2 つの MSDP ピア間で TCP 接続の MD5 認証をイネーブルにするために使用されます。2 つの MSDP ピア間で MD5 認証がイネーブルになると、ピア間の TCP 接続で送信された各セグメントが確認されます。どちらの MSDP ピアでも同じパスワードを使用して MD5 認証を設定する必要があります。そうしない場合は、これらの間の接続が確立されません。MD5 認証を設定すると、Cisco IOS ソフトウェアにより、TCP 接続上で送信される各セグメントについて MD5 ダイジェストが生成され、検証されるようになります。

MSDP MD5 パスワード認証の利点

- TCP 接続ストリームに導入されるスプーフィングされた TCP セグメントの脅威に対して MSDP を保護します。
- 業界標準の MD5 アルゴリズムを使用して信頼性およびセキュリティを向上させます。

SA メッセージの制限

デバイスが特定の MSDP ピアから受け入れることができる SA メッセージの総数を制限するには、**ip msdp sa-limit** コマンドを使用します。 **ip msdp sa-limit** コマンドが設定されている場合、デバイスは SA キャッシュに保存された SA メッセージの数をピアごとに維持し、そのピアに設定された SA メッセージの制限に達した場合は、ピアからの新しいメッセージを無視します。

MSDP 対応デバイスをサービス妨害（DoS）攻撃から保護する手段として、**ip msdp sa-limit** コマンドが導入されました。デバイスですべての MSDP ピアリングに対する SA メッセージの制限を設定することを推奨します。適度に低い SA 制限をスタブ MSDP リージョンとのピアリングに設定する必要があります（たとえば、さらにダウンストリーム ピアを持つが、インターネットの残りの部分で SA メッセージの中継として動作しないピアなど）。インターネット上の SA メッセージの中継として動作するすべての MSDP ピアリングに高い SA 制限を設定する必要があります。

MSDP キープアライブ インターバルおよび保留時間インターバル

ip msdp keepalive コマンドは、MSDP ピアがキープアライブメッセージを送信する間隔、および MSDP ピアが他のピアがダウンしたと宣言するまでに他のピアからのキープアライブメッセージを待機する間隔を調整するために使用します。

MSDP のピアリング セッションが確立されると、接続の各サイドでキープアライブ メッセージを送信し、キープアライブ タイマーを設定します。キープアライブ タイマーの期限が切れると、ローカル MSDP ピアはキープアライブ メッセージを送信し、キープアライブ タイマーを再開します。この間隔をキープアライブ インターバルといいます。*keepalive-interval* 引数は、キープアライブ メッセージの送信間隔を調整するために使用されます。キープアライブ タイマーは、ピアがアップ状態のときに *keepalive-interval* 引数に指定された値に設定されます。MSDP キープアライブ メッセージがピアに送信され、タイマーが期限切れになったときにリセットされると、キープアライブ タイマーは *keepalive-interval* 引数の値にリセットされます。キープアライブ タイマーは、MSDP ピアリング セッションがクローズすると削除されます。デフォルトでは、keepalive タイマーは 60 秒に設定されます。

（注） *keepalive-interval* 引数に指定される値は、*holdtime-interval* 引数に指定される値未満にしなければならず、また、1 秒以上に設定する必要があります。

保留時間タイマーは、MSDP ピアリング接続が確立されると *hold-time-interval* 引数の値に初期化され、MSDP キープアライブ メッセージが受信されると *hold-time-interval* 引数の値にリセットされます。保留時間タイマーは、MSDP ピアリング接続がクローズすると削除されます。デフォルトでは、保留時間インターバルは 75 秒に設定されています。

MSDP ピアが他のピアがダウンしたと宣言するまで他のピアからのキープアライブ メッセージを待機する間隔を調整するには、*hold-time-interval* 引数を使用します。

MSDP 接続再試行インターバル

ピアリング セッションがリセットされてからピアリング セッションの再確立が試行されるまですべてのMSDPピアが待機する間隔を調整できます。この間隔は、接続再試行間隔と呼ばれます。デフォルトでは、ピアリングセッションがリセットされてから他のピアとのピアリングセッションの再確立が試行されるまで MSDP ピアは 30 秒間待機します。変更設定された接続再試行間隔は、デバイス上のすべての MSDP ピアリング セッションに適用されます。

デフォルト MSDP ピア

ほとんどのシナリオでは、MSDP ピアは BGP ピアでもあります。自律システムがスタブまたは非推移的な自律システムの場合で、特に自律システムがマルチホームでないときは、中継自律システムに BGP を実行する理由はほとんど、またはまったくありません。一般に、スタブ自律システムのスタティックなデフォルト ルート、および中継自律システムのスタブ プレフィックスに接続するスタティックなルートで十分です。ただし、スタブ自律システムがマルチキャスト ドメインでもあり、RP が隣接ドメイン内の RP とピアリングする必要がある場合は、MSDP は BGP ネクスト ホップ データベースを使用してピア RPF チェックを行います。ピア RPF チェックを実行せずにすべての SA メッセージを受け入れるデフォルトのピアを定義することで、BGP でのこの依存関係をディセーブルにできます。デフォルトの MSDP ピアは、事前に設定しておく必要があります。

スイッチが BGP や MBGP をサポートしていない場合は、**ip msdp peer** 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、ローカルスイッチに MSDP ピアを設定できません。その代わり、このスイッチのすべての SA メッセージを受け入れることができるデフォルトの MSDP ピアを（ip msdp default-peer 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）定義します。デフォルトの MSDP ピアは、事前に設定しておく必要があります。スイッチで MSDP ピアによる BGP または MBGP ピアリングが行われない場合は、デフォルトの MSDP ピアを設定します。単一の MSDP ピアが設定されている場合、スイッチでは常にそのピアからのすべての SA メッセージが受信されます。

スタブ自律システムには、冗長性を実現するために複数の RP との MSDP ピアリングが必要な場合もあります。たとえば、RPF チェック メカニズムがないため、SA メッセージは複数のデフォルト ピアから受け入れられません。その代わりに、SA メッセージは 1 つのピアからだけ受け入れられます。そのピアに障害が発生した場合、SA メッセージは別のピアから受け入れられます。もちろん、デフォルトのピアが両方とも同じ SAメッセージを送信することがこの基本的な前提となっています。

下の図に、デフォルトの MSDP ピアが使用されるシナリオを示します。この図では、デバイス B を所有するカスタマーが 2 つのインターネット サービス プロバイダ（ISP）を介してインターネットに接続されています。一方の ISP はデバイス A を所有し、もう一方の ISP はデバイス C を所有しています。どちらもそれらの間で BGP も MBGP も実行していません。カスタマーが ISP ドメインまたは他のドメイン内のソースについて学習するために、デバイス B はデバイス A をデフォルト MSDP ピアとして識別します。デバイス B はデバイス A とデバイス C の両方に SA メッセージをアドバタイズしますが、デバイス A だけまたはデバイス C だけから SA メッセージを受け入れます。デバイス A が設定内の最初のデフォルト ピアである場合、デ

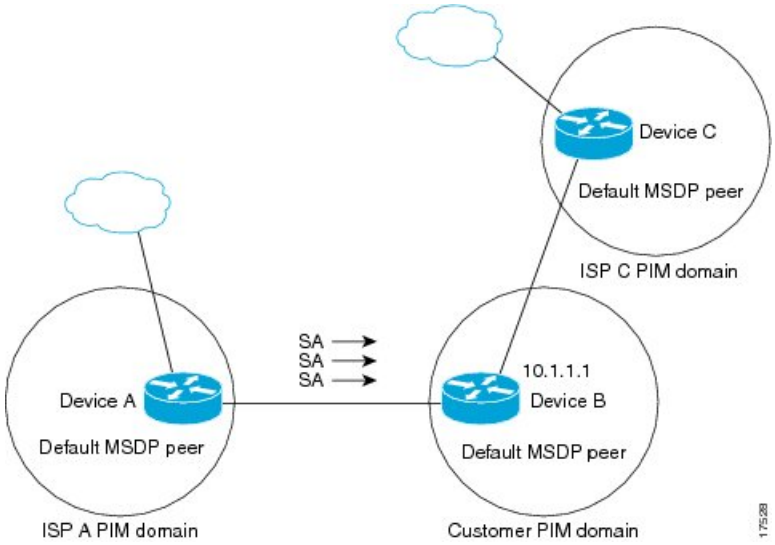
バイス A が稼働していればデバイス A が使用されます。デバイス A が稼働していない場合に限り、デバイス B がデバイス C からの SA メッセージを受け入れます。

ISP は、プレフィックス リストを使用して、カスタマーのデバイスから受け入れるプレフィックスを定義する場合もあります。カスタマーは、複数のデフォルト ピアを定義します。各ピアには関連するプレフィックスを 1 つまたは複数設定します。

カスタマーは 2 つの ISP を使用しています。カスタマーはこの 2 つの ISP をデフォルト ピアとして定義します。設定内で最初のデフォルト ピアとして特定されているピアが稼働している限り、このピアがデフォルト ピアになり、カスタマーはそのピアから受信するすべての SA メッセージを受け入れます。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *19* : デフォルト *MSDP* ピアのシナリオ



デバイス B はデバイス A およびデバイス C に SA をアドバタイズしますが、デバイス A またはデバイス C だけを使用して SA メッセージを受け入れます。デバイス A が設定内の最初のデバイスである場合、デバイス A が稼働していればデバイス A が使用されます。デバイス A が稼働していない場合に限り、デバイス B がデバイス C から SA メッセージを受け入れます。これは、プレフィックス リストを使用しない動作です。

プレフィックス リストを指定すると、リスト内のプレフィックスに対してだけピアはデフォルト ピアになります。プレフィックス リストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。プレフィックス リストがない場合も、複数のデフォルト ピアを設定できますが、アクティブなデフォルト ピアになるのは最初のピアだけです（このピアにデバイスが接続されていて、ピアがアクティブの場合に限ります）。最初に設定されたピアがダウンするか、このピアとの接続がダウンした場合、2 番目に設定されたピアがアクティブなデフォルト ピアになります。以下同様です。

MSDP メッシュ グループ

MSDP メッシュ グループは、MSDP によってフル メッシュ型に相互接続された MSDP スピーカーのグループです。つまり、グループの各 MSDP ピアには、グループ内の他のすべての MSDP ピアとの MSDP ピアリング関係（MSDP 接続）が必要です。MSDP メッシュ グループが MSDP ピアのグループ間に設定されている場合、SA メッセージのフラッディングが削減されます。グループ内の MSDP ピアがグループ内の別の MSDP ピアから SA メッセージを受信すると、この SA メッセージはグループ内のその他のすべての MSDP ピアに送信されたとみなされるためです。その結果、受信側の MSDP ピアがグループ内の他の MSDP ピアに SA メッセージをフラッディングする必要はありません。

MSDP メッシュ グループの利点

- SA フラッディングの最適化：グループ内に複数のピアがある場合、SA フラッディングを最適化するために MSDP メッシュ グループは特に有用です。
- インターネットを通過する SA トラフィック量の削減：MSDP メッシュ グループを使用すると、SA メッセージは他のメッシュ グループ ピアにフラッディングされません。
- 着信 SA メッセージの RPF チェックの省略：MSDP メッシュ グループが設定されていると、メッシュ グループ ピアからの SA メッセージは常に受け入れられます。

SA 発信フィルタ

デフォルトでは、MSDP を実行するように設定されている RP は、それが RP であるすべてのローカル ソースの SA メッセージを発信します。そのため、RP に登録されているローカル ソースは SA メッセージでアドバタイズされますが、これが望ましくない場合もあります。たとえば、PIM-SM ドメイン内のソースがプライベート アドレス（たとえば、ネットワーク 10.0.0.0/8）を使用している場合、SA 発信フィルタを設定してこれらのアドレスがインターネット上の他の MSDP ピアにアドバタイズされないようにする必要があります。

SA メッセージでアドバタイズされるソースを制御するには、RP に SA 発信フィルタを設定します。SA 発信フィルタを作成すると、SA メッセージでアドバタイズされるソースを次のように制御できます。

- デバイスが SA メッセージでローカル ソースをアドバタイズしないように RP を設定できます。この場合もデバイスは通常の方法で他の MSDP ピアからの SA メッセージを転送します。ローカル ソースの SA メッセージは発信しません。
- 拡張アクセス リストで定義されている（S,G）ペアと一致する、特定のグループに送信するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。
- AS パス アクセス リストで定義されている AS パスと一致する、特定のグループに送信するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。

- ルート マップで定義されている基準と一致するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。
- 拡張アクセス リスト、AS パス アクセス リスト、およびルート マップ（またはそれらのその組み合わせ）を含む SA 発信フィルタを設定します。この場合、ローカル ソースが SA メッセージでアドバタイズされる前に、すべての条件を満たしている必要があります。

MSDP での発信フィルタ リストの使用

デフォルトでは、MSDP 対応デバイスは、受信したすべての SA メッセージをその MSDP ピアすべてに転送します。ただし、発信フィルタ リストを作成することで、SA メッセージが MSDP ピアに転送されないようにできます。発信フィルタ リストは、ローカルに発信されたか別の MSDP ピアから受信したかに関係なくすべての SA メッセージに適用されますが、SA 発信フィルタはローカルに発信された SA メッセージだけに適用されます。ローカル デバイスから発信される MSDP SA メッセージのフィルタをイネーブルにする方法の詳細については、ローカル ソースの RP によって発信された SA メッセージの制御 （248 ページ）を参照してください。

発信フィルタ リストを作成すると、デバイスがピアへ転送する SA メッセージを次のように制御できます。

- 指定した MSDP ピアへ転送したすべての発信 SAメッセージをフィルタリングするには、MSDP ピアへの SA メッセージの転送を停止するようにデバイスを設定します。
- 指定した MSDP ピアへ転送した発信 SA メッセージのサブセットを拡張アクセス リストに定義された（S, G）ペアに基づいてフィルタリングするには、拡張アクセス リストで許可されている（S, G）ペアに一致する MSDP ピアへの SA メッセージだけを転送するようにデバイスを設定します。その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。
- 指定した MSDP へ転送した発信 SA メッセージのサブセットをルート マップに定義された一致基準に基づいてフィルタリングするには、ルート マップに定義された基準に一致する SA メッセージだけを転送するようにデバイスを設定します。その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。
- 指定したピアからの発信 SA メッセージのサブセットを SA メッセージに含まれているアナウンス側 RP アドレスに基づいてフィルタリングするには、SA メッセージが1 つ以上の MSDP ピアに送信されていても、それらの発信元に基づいて発信 SA メッセージをフィルタリングするようにデバイスを設定します。その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。
- 拡張アクセス リスト、ルート マップ、および RP アクセス リストまたは RP ルート マップのいずれかを含む発信フィルタ リストを設定できます。この場合、MSDP ピアで発信 SA メッセージを転送するにはすべての条件を満たしている必要があります。

⚠

注意 SA メッセージの任意のフィルタリングを実行すると、ダウンストリーム MSDP ピアで正当なアクティブソースの SA メッセージを受信できなくなることがあります。そのため、このタイプのフィルタを使用する場合は注意が必要です。通常、発信フィルタ リストは、プライベート アドレスを使用するソースなど、望ましくないソースを拒否するためだけに使用します。

MSDP での着信フィルタ リストの使用

デフォルトでは、MSDP 対応デバイスは MSDP ピアからそのデバイスに送信されたすべての SA メッセージを受信します。ただし、着信フィルタ リストを作成することによって、MSDP ピアからデバイスが受信する送信元情報を制御できます。

着信フィルタ リストを作成すると、デバイスがピアから受信する着信 SA メッセージを次のように制御できます。

- 指定した MSDP ピアからのすべての着信 SAメッセージをフィルタリングするには、指定した MSDP ピアから送信されたすべての SAメッセージを無視するようにデバイスを設定します。
- 指定したピアからの着信 SA メッセージのサブセットを拡張アクセス リストに定義された（S, G）ペアに基づいてフィルタリングするには、拡張アクセス リストに定義された（S, G）ペアに一致する MSDP ピアからの SA メッセージだけを受信するようにデバイスを設定します。MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- 指定したピアからの着信 SA 要求メッセージのサブセットをルート マップに定義された一致基準に基づいてフィルタリングするには、ルート マップに指定された基準に一致する SA メッセージだけを受信するようにデバイスを設定します。MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- 指定したピアからの着信 SA メッセージのサブセットを拡張アクセス リストに定義された（S, G）ペアと、ルートマップに定義された基準の両方に基づいてフィルタリングするには、拡張アクセス リストに定義された（S, G）ペアと、ルート マップに定義された基準の両方に一致する着信 SA メッセージだけを受信するようにデバイスを設定します。MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- 指定したピアからの着信 SA メッセージのサブセットを SA メッセージに含まれているアナウンス側 RP アドレスに基づいてフィルタリングするには、SA メッセージがすでに1 つ以上の MSDP ピア全体に送信されている可能性がある場合でも、それらの発信元に基づいて着信 SA メッセージをフィルタリングするようにデバイスを設定します。
- 拡張アクセス リスト、ルート マップ、および RP アクセス リストまたは RP ルート マップのいずれかを含む着信フィルタ リストを設定できます。この場合、MSDP ピアで着信 SA メッセージを受信するにはすべての条件を満たしている必要があります。

注意 SA メッセージの任意のフィルタリングを実行すると、ダウンストリーム MSDP ピアで正当なアクティブソースの SA メッセージを受信できなくなることがあります。そのため、このタイプのフィルタを使用する場合は注意が必要です。通常、着信フィルタ リストは、プライベート アドレスを使用するソースなど、望ましくないソースを拒否するためだけに使用されます。

MSDP の TTL しきい値

存続可能時間（TTL）値を使用して、ドロップされる前にパケットが取得できるホップの数を制限できます。特定の MSDP ピアに送信された、データがカプセル化された SA メッセージの TTL を指定するには、**ip multicast ttl-threshold** コマンドを使用します。デフォルトでは、パケットの TTL 値が 0（標準 TTL 動作）より大きい場合は、SA メッセージのマルチキャスト データ パケットは MSDP ピアに送信されます。

一般に、TTL しきい値の問題は、SA メッセージ内でソースの初期マルチキャスト パケットがカプセル化されることによって発生することがあります。マルチキャスト パケットはユニキャスト SA メッセージ内部でカプセル化されるため（TTL は 255）、SA メッセージが MSDP ピアに送信されるときに TTL は減少しません。さらに、マルチキャスト トラフィックおよびユニキャスト トラフィックは MSDP ピア、したがってリモート PIM-SM ドメインへのまったく異なるパスに従うため、SA メッセージが通過するホップの総数は、通常のマルチキャスト パケットとは大きく異なります。その結果、カプセル化されたパケットは TTL しきい値に違反することになります。この問題を解決するには、**ip multicast ttl-threshold** コマンドを使用して、特定の MSDP ピアに送信された SA メッセージにカプセル化されているマルチキャスト パケットに関連付けられた TTL しきい値を設定します。**ip msdp ttl-threshold** コマンドを使用すると、IP ヘッダーの TTL が *ttl-value* 引数に指定されている TTL 値未満であるマルチキャスト パケットが、ピアに送信される SA メッセージにカプセル化されないようにすることができます。

SA 要求メッセージ

1 つ以上の指定した MSDP ピアに SA 要求メッセージを送信するように非キャッシュ デバイスを設定できます。非キャッシュ RP に SA をキャッシュする MSDP ピアがある場合、非キャッシュ ピアが SA 要求メッセージを送信できるようにすると非キャッシュ ピアの参加遅延を低減できます。ホストが特定のグループに対して加入を要求すると、非キャッシュ RP は SA 要求メッセージをキャッシュ ピアに送信します。ピアがこの特定のグループのソース情報をキャッシュしている場合、SA 応答メッセージで要求側の RP に情報を送信します。要求側の RP は SA 応答内の情報を使用しますが、他のピアにメッセージを転送しません。非キャッシュ RP が SA 要求を受信すると、要求者にエラー メッセージを返します。

（注） 現行のすべてのサポート対象のソフトウェア リリースでは、MSDP SA メッセージのキャッシュは必須であり、手動でイネーブルまたはディセーブルにすることはできません。デフォルトでは、MSDP ピアが設定されると、設定コマンドが自動的に実行コンフィギュレーションに追加されます。

SA 要求フィルタ

デフォルトでは、デバイスはその MSDP ピアからのすべての発信 SA 要求メッセージを受け入れます。つまり、デバイスはキャッシュされたソース情報を要求側の MSDP ピアに SA 応答メッセージで送信します。デバイスが特定のピアから受け入れる発信 SA 要求メッセージを制御するには、SA 要求フィルタを作成します。SA 要求フィルタは、デバイスが MSDP ピアから受け入れる発信 SA 要求を次のように制御します。

- 指定したピアからのすべての SA 要求メッセージをフィルタリングするには、指定した MSDP ピアからのすべての SA 要求を無視するようにデバイスを設定します。
- 指定したピアからの SA 要求メッセージのサブセットを標準アクセス リストに定義されたグループに基づいてフィルタリングするには、標準アクセス リストに定義されたグループに一致する MSDP ピアからの SA 要求メッセージだけを受け入れるようにデバイスを設定します。その他のグループの指定されたピアからの SA 要求メッセージは無視されます。

MSDP を使用して複数の PIM-SM ドメインを相互接続する方法

最初の作業は必須で、他の作業はすべて任意です。

MSDP ピアの設定

（注） MSDP ピアをイネーブルにすることで、MSDP は暗黙的にイネーブルになります。

始める前に

- IP マルチキャスト ルーティングをイネーブルにし、PIM-SM を設定する必要があります。
- 単一の MSDP ピア、デフォルトの MSDP ピア、および MSDP メッシュ グループの場合を除き、すべての MSDP ピアは MSDP に設定される前に BGP を実行するように設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp peer** {*peer-name*| *peer-address*} [*connect-source type number*] [**remote-as** *as-number*]
4. **ip msdp description** {*peer-name*| *peer-address*} *text*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip msdp peer** {*peer-name*| *peer-address*} [*connect-source type number*] [**remote-as** *as-number*] 例： `Device(config)# ip msdp peer 192.168.1.2 connect-source loopback0`	MSDP をイネーブルにし、DNS 名または IP アドレスで指定される MSDP ピアを設定します。 （注） MSDP ピアとして設定するように選択されたデバイスは、通常は BGP ネイバーでもあります。そうでない場合は、デフォルトの MSDP ピアの設定（246 ページ）または MSDP メッシュ グループの設定（247 ページ）を参照してください。 • **connect-source** キーワードを指定した場合、指定されたローカルインターフェイスの *type* と *number* の値で示されるプライマリアドレスは TCP 接続の送信元 IP アドレスとして使用されます。リモートドメイン内のデバイスとのピアを確立している境界上の MSDP ピアの場合は特に、**connect-source** キーワードを推奨します。
ステップ 4	**ip msdp description** {*peer-name*| *peer-address*} *text* 例： `Device(config)# ip msdp description 192.168.1.2 router at customer a`	（任意）設定内で、または **show** コマンド出力内で簡単に識別できるように、指定されたピアの説明を設定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	グローバル 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。

MSDP ピアのシャットダウン

MSDP ピアをシャットダウンするには、次の任意の作業を実行します。

複数の MSDP ピアを設定し、そのすべての設定が終了するまではどのピアもアクティブにしない場合は、それぞれのピアをシャットダウンし、ピアごとに設定して、後からそれぞれのピアを起動することができます。その MSDP ピアの設定を失うことなく、MSDP セッションをシャットダウンすることもできます。

（注） MSDP ピアをシャットダウンすると、TCP 接続が終了します。**no ip msdp shutdown** コマンドを（指定したピアに対して）使用し、ピアを起動するまではこの接続は再開されません。

始める前に

MSDP が動作していて、MSDP ピアを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp shutdown** {*peer-name* | *peer-address*}
4. 別の MSDP ピアをシャットダウンするには、ステップ 3 を繰り返します。
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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 3	**ip msdp shutdown** {*peer-name* | *peer-address*} 例： `Device(config)# ip msdp shutdown 192.168.1.3`	指定された MSDP ピアを管理シャットダウンします。
ステップ 4	別の MSDP ピアをシャットダウンするには、ステップ 3 を繰り返します。	--
ステップ 5	**end** 例： `Device(config)# end`	グローバル 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。

MSDP ピア間の MSDP MD5 パスワード認証の設定

MSDP ピア間の MSDP Message Digest 5（MD5）パスワード認証を設定するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string*
4. **exit**
5. **show ip msdp peer** [peer-address | peer-name]

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	**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	**ip msdp password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string* 例： `Device(config)# ip msdp password peer 10.32.43.144 0 test`	2 つの MSDP ピア間の TCP 接続の MD5 パスワード暗号化をイネーブルにします。 （注） どちらの MSDP ピアでも同じパスワードを使用して MD5 認証を設定する必要があります。そうしない場合は、これらの間の接続が確立されません。

	コマンドまたはアクション	目的
		• 2 つの MSDP ピアの間で MD5 認証に使用されるパスワードやキーを設定または変更した場合、パスワードの設定後にローカルデバイスの既存のセッションは切断されません。新しいパスワードまたは変更されたパスワードをアクティブにするには、手動でセッションを切断する必要があります。
ステップ 4	**exit** 例： `Device(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、特権 EXEC モードに戻ります。
ステップ 5	**show ip msdp peer** [peer-address | peer-name] 例： `Device# show ip msdp peer`	（任意）MSDP ピアに関する詳細情報を表示します。 （注） このコマンドを使用して、MSDP ピアで MD5 パスワード認証がイネーブルになっているかどうかを確認します。

トラブルシューティングのヒント

デバイスにMSDPピア用のパスワードが設定されているが、MSDPピアには設定されていない場合、デバイスがそれらの間でMSDPセッションを確立しようとすると、次のようなメッセージがコンソールに表示されます。

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's
IP address]:179
```

同様に、2 台のデバイスに異なるパスワードが設定されている場合、次のようなメッセージがコンソールに表示されます。

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's
IP address]:179
```

debug ip tcp transactions コマンドを使用すると、ステートの変更、再送、重複するパケットなどの重要な TCP トランザクションに関する情報が表示されます。MSDP MD5 パスワード認証のモニタリングまたはトラブルシューティングでは、**debug ip tcp transactions** コマンドを使用して、MD5 パスワードが有効かどうか、およびキープアライブメッセージが MSDP ピアで受信されるかどうかを確認します。

SA キャッシュ内で許可される特定の MSDP ピアからの SA メッセージ数の制限によるサービス拒絶（DoS）攻撃の防止

デバイスが指定された MSDP ピアから受け入れることができる SA メッセージの総数を制限するには、このオプションの（しかし強く推奨されます）タスクを実行します。この作業を実行することで、MSDP 対応デバイスを分散型サービス妨害（DoS）攻撃から保護します。

（注） デバイス上のすべての MSDP ピアリングに対してこの作業を実行することを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp sa-limit** {*peer-address* | *peer-name*} *sa-limit*
4. 別の MSDP ピアの SA 制限を設定するには、ステップ 3 を繰り返します。
5. **exit**
6. **show ip msdp count** [*as-number*]
7. **show ip msdp peer** [*peer-address* | *peer-name*]
8. **show ip msdp summary**

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	**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	**ip msdp sa-limit** {*peer-address* | *peer-name*} *sa-limit* 例： `Device(config)# ip msdp sa-limit 192.168.10.1 100`	SA キャッシュ内で許可される特定の MSDP ピアからの SA メッセージの数を制限します。
ステップ 4	別の MSDP ピアの SA 制限を設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例：	グローバル 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。

	コマンドまたはアクション	目的
	`Device(config)# exit`	
ステップ 6	**show ip msdp count** [*as-number*] 例： `Device# show ip msdp count`	（任意）MSDP SA メッセージ内で発信されたソースおよびグループの数、および SA キャッシュ内の MSDP ピアからの SA メッセージの数を表示します。
ステップ 7	**show ip msdp peer** [*peer-address* | *peer-name*] 例： `Device# show ip msdp peer`	（任意）MSDP ピアに関する詳細情報を表示します。 （注） このコマンドの出力には、キャッシュに格納されている MSDP ピアから受信した SA メッセージの数が表示されます。
ステップ 8	**show ip msdp summary** 例： `Device# show ip msdp summary`	（任意）MSDP ピアのステータスを表示します。 （注） このコマンドの出力には、キャッシュに格納されている SA の数を表示するピアごとの「SA Count」フィールドが表示されます。

MSDP キープアライブ インターバルおよび保留時間インターバルの調整

MSDP ピアがキープアライブ メッセージを送信する間隔、および MSDP ピアが他のピアがダウンしたと宣言するまでに他のピアからのキープアライブ メッセージを待機する間隔を調整するには、次の任意の作業を実行します。デフォルトでは、MSDP ピアが別の MSDP ピアとのピアリング セッションのダウンを検出するまでに 75 秒かかる場合があります。冗長 MSDP ピアが設定されたネットワーク環境では、保持時間間隔を短縮すると、MSDP ピアの障害発生時に MSDP ピアの再コンバージェンス時間を短縮できます。

（注） コマンドのデフォルトは RFC 3618、*Multicast Source Discovery Protocol* に従うため、**ip msdp keepalive** コマンドのデフォルトを変更しないことを推奨します。デフォルトの変更が必要なネットワーク環境の場合は、MSDP ピアリングセッションの終了時の *keepalive-interval* と *hold-time-interval*の両方の引数に同じ時刻値を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp keepalive** {*peer-address* | *peer-name*} *keepalive-interval hold-time-interval*

4. 別の MSDP ピアのキープアライブ メッセージの間隔を調整するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip msdp keepalive** {*peer-address* | *peer-name*} *keepalive-interval hold-time-interval* 例： `Device(config)# ip msdp keepalive 10.1.1.3 40 55`	MSDP ピアがキープアライブ メッセージを送信する間隔、およびMSDP ピアが他のピアがダウンとしたと宣言するまでに他のピアからのキープアライブ メッセージを待機する間隔を設定します。
ステップ 4	別の MSDP ピアのキープアライブ メッセージの間隔を調整するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

MSDP 接続再試行インターバルの調整

ピアリング セッションがリセットされてからピアリング セッションの再確立が試行されるまで MSDP ピアが待機する間隔を調整するには、次のオプション タスクを実行します。取引フロアのネットワーク環境など、SA メッセージの高速リカバリが必要なネットワーク環境では、接続再試行間隔をデフォルト値の 30 秒未満の時間値に減らすことができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp timer** *connection-retry-interval*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip msdp timer** *connection-retry-interval* 例： `Device# ip msdp timer 45`	ピアリング セッションがリセットされてからピアリング セッションの再確立が試行されるまで MSDP ピアが待機する間隔を設定します。
ステップ 4	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

デフォルトの MSDP ピアの設定

デフォルト MSDP ピアを設定するには、次の任意の作業を実行します。

始める前に

デフォルト MSDP ピアは、事前に設定されている MSDP ピアでなければなりません。デフォルト MSDP ピアを設定する前に、まず MSDP ピアを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp default-peer** {*peer-address* | *peer-name*} [**prefix-list** *list*]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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）。

	コマンドまたはアクション	目的
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	**ip msdp default-peer** {*peer-address* | *peer-name*} [**prefix-list** *list*] 例： `Device(config)# ip msdp default-peer 192.168.1.3`	すべての MSDP SA メッセージの受信元となるデフォルト ピアを設定します。
ステップ 4	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

MSDP メッシュ グループの設定

MSDP メッシュ グループを設定するには、次の任意の作業を実行します。

（注） デバイスごとに複数のメッシュ グループを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp mesh-group** *mesh-name* {*peer-address* | *peer-name*}
4. MSDP ピアをメッシュ グループのメンバとして追加するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**configure terminal** 例：	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
	`Device# configure terminal`	
ステップ 3	**ip msdp mesh-group** *mesh-name* {*peer-address* | *peer-name*} 例： `Device(config)# ip msdp mesh-group peermesh`	MSDP メッシュ グループを設定し、MSDP ピアがそのメッシュ グループに属することを指定します。 （注） メッシュ グループに参加しているデバイス上のすべての MSDP ピアは、そのグループ内の他のすべての MSDP ピアと完全にメッシュ構造になっている必要があります。各デバイスの各 MSDP ピアは、**ip msdp peer** コマンドを使用して、ピアとして設定する必要があります、また、**ip msdp mesh-group** コマンドを使用して、そのメッシュグループのメンバとしても設定する必要があります。
ステップ 4	MSDP ピアをメッシュ グループのメンバとして追加するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

ローカル ソースの RP によって発信された SA メッセージの制御

SA メッセージでアドバタイズされる登録ソースを制限するフィルタをイネーブルにして、RP によって発信された SA メッセージを制御するには、次の作業を実行します。

（注） MSDP SA メッセージ フィルタの設定に関するベスト プラクティス情報については、テクニカル ノート『Multicast Source Discovery Protocol SA Filter Recommendations』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp redistribute** [**list** *access-list*] [**asn** *as-access-list*] [**route-map** *map-name*]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip msdp redistribute** [**list** *access-list*] [**asn** *as-access-list*] [**route-map** *map-name*] 例： `Device(config)# ip msdp redistribute route-map customer-sources`	ローカル デバイスによって発信される MSDP SA メッセージのフィルタをイネーブルにします。 （注） **ip msdp redistribute** コマンドは、RP で認識されているが登録されていない送信元をアドバタイズするために使用することもできます。ただし、RP に登録されていないソースのアドバタイズメントは発信しないことを強く推奨します。
ステップ 4	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

発信フィルタ リストを使用した SA メッセージの MSDP ピアへの転送の制御

発信フィルタ リストを設定して SA メッセージの MSDP ピアへの転送を制御するには、次の任意の作業を実行します。

（注） MSDP SA メッセージ フィルタの設定に関するベスト プラクティス情報については、テクニカル ノート『Multicast Source Discovery Protocol SA Filter Recommendations』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*]

4. 別の MSDP ピアの発信フィルタ リストを設定するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip msdp sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*] 例： `Device(config)# ip msdp sa-filter out 192.168.1.5 peerone`	発信 MSDP メッセージのフィルタをイネーブルにします。
ステップ 4	別の MSDP ピアの発信フィルタ リストを設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

着信フィルタ リストを使用した MSDP ピアからの SA メッセージの受信の制御

MSDP ピアからの着信 SA メッセージの受信を制御するには、次の任意の作業を実行します。

（注） MSDP SA メッセージ フィルタの設定に関するベスト プラクティス情報については、テクニカル ノート『Multicast Source Discovery Protocol SA Filter Recommendations』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**

3. **ip msdp sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*]
4. 別の MSDP ピアの着信フィルタ リストを設定するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip msdp sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*] 例： `Device(config)# ip msdp sa-filter in 192.168.1.3`	着信 MSDP SA メッセージのフィルタをイネーブルにします。
ステップ 4	別の MSDP ピアの着信フィルタ リストを設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

TTL しきい値を使用した SA メッセージで送信されたマルチキャスト データの制限

SA メッセージで送信されるマルチキャスト データを制限するために存続可能時間（TTL）しきい値を確立するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp ttl-threshold** {*peer-address* | *peer-name*} *ttl-value*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip msdp ttl-threshold** {*peer-address* | *peer-name*} *ttl-value* 例： 例： `Device(config)# ip msdp ttl-threshold 192.168.1.5 8`	ローカルデバイスにより発信される MSDP メッセージの TTL 値を設定します。 • デフォルトでは、パケットの TTL 値が 0（標準 TTL 動作）より大きい場合は、SA メッセージのマルチキャスト データ パケットは MSDP ピアに送信されます。
ステップ 4	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

MSDP ピアへの送信元情報の要求

デバイスが MSDP ピアから送信元情報を要求できるようにするには、次の任意の作業を実行します。

（注） シスコの以前のソフトウェア リリースでは SA キャッシングはデフォルトでイネーブルになっており、明示的にイネーブルまたはディセーブルにすることはできないため、この作業はほとんど必要ありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp sa-request** {*peer-address* | *peer-name*}
4. デバイスが別の MSDP キャッシュ ピアに SA 要求メッセージを送信するように指定するには、ステップ 3 を繰り返します。

5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip msdp sa-request** {*peer-address* | *peer-name*} 例： `Device(config)# ip msdp sa-request 192.168.10.1`	デバイスが指定された MSDP ピアに SA 要求メッセージを送信するように指定します。
ステップ 4	デバイスが別の MSDP キャッシュ ピアに SA 要求メッセージを送信するように指定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

SA 要求フィルタを使用した MSDP ピアからの発信 SA 要求メッセージに対する応答の制御

デバイスが MSDP ピアから受け入れる発信 SA 要求メッセージを制御するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp filter-sa-request** {*peer-address* | *peer-name*} [**list** *access-list*]
4. 別の MSDP ピアの SA 要求フィルタを設定するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip msdp filter-sa-request** {*peer-address* | *peer-name*} [**list** *access-list*] 例： `Device(config)# ip msdp filter sa-request 172.31.2.2 list 1`	発信 SA 要求メッセージのフィルタをイネーブルにします。 （注） MSDP ピアには SA 要求フィルタを 1 つだけ設定できます。
ステップ 4	別の MSDP ピアの SA 要求フィルタを設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

RP アドレス以外の発信元アドレスの設定

SA メッセージを発信する MSDP スピーカーがそのインターフェイスの IP アドレスを SA メッセージ内の RP アドレスとして使用できるようにするには、次の任意の作業を実行します。

また、次のいずれかの理由により、発信元 ID を変更できます。

- Anycast RP の MSDP メッシュ グループに複数のデバイスを設定する場合。
- デバイスが PIM-SM ドメインと PIM-DM ドメインの境界にある場合。デバイスが PIM-SM ドメインと PIM-DM ドメインの境界にあり、PIM-DM ドメイン内のアクティブなソースをアドバタイズする場合は、SA メッセージ内の RP アドレスが発信元デバイスのインターフェイスのアドレスになるように設定します。

始める前に

MSDP がイネーブルになり、MSDP ピアが設定されます。MSDP ピアの設定の詳細については、MSDP ピアの設定 （238 ページ）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp originator-id** *type number*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip msdp originator-id** *type number* 例： `Device(config)# ip msdp originator-id ethernet 1`	発信元デバイスのインターフェイスのアドレスとなるように、SA メッセージ内の RP アドレスを設定します。
ステップ 4	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

MSDP のモニタリング

MSDP の SA メッセージ、ピア、ステート、およびピアのステータスをモニタリングするには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **debug ip msdp** [*peer-address* | *peer-name*] [**detail**] [**routes**]
3. **debug ip msdp resets**
4. **show ip msdp count** [*as-number*]
5. **show ip msdp peer** [*peer-address* | *peer-name*]
6. **show ip msdp sa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*]
7. **show ip msdp summary**

手順の詳細

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 **debug ip msdp** [*peer-address* | *peer-name*] [**detail**] [**routes**]

このコマンドを使用して、MSDP アクティビティをデバッグします。

オプションの *peer-address* または *peer-name* 引数を使用して、デバッグ イベントをログに記録するピアを指定します。

次に、**debug ip msdp** コマンドの出力例を示します。

例：

```
Device# debug ip msdp
MSDP debugging is on
Device#
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.254: Received 1028-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1028, ec: 85, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1028-byte SA to peer
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.250: Received 56-byte message from peer
MSDP: 224.150.44.250: SA TLV, len: 56, ec: 4, RP: 192.168.76.241
MSDP: 224.150.44.250: Peer RPF check passed for 192.168.76.241, used EMBGP peer
MSDP: 224.150.44.254: Forward 56-byte SA to peer
MSDP: 224.150.44.254: Received 116-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 116, ec: 9, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.250: Forward 116-byte SA to peer
MSDP: 224.150.44.254: Received 32-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 32, ec: 2, RP: 172.31.3.78
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.78, used EMBGP peer
MSDP: 224.150.44.250: Forward 32-byte SA to peer
```

ステップ 3 **debug ip msdp resets**

このコマンドを使用して、MSDP ピアのリセット理由をデバッグします。

例：

```
Device# debug ip msdp resets
```

ステップ 4 **show ip msdp count** [*as-number*]

このコマンドを使用して、MSDP SA メッセージ内で発信したソースおよびグループの数、および SA キャッシュ内の MSDP ピアからの SA メッセージの数を表示します。**ip msdp cache-sa-state** コマンドは、このコマンドによって出力が生成されるように設定する必要があります。

次に、**show ip msdp count** コマンドの出力例を示します。

例：

```
Device# show ip msdp count
SA State per Peer Counters, <Peer>: <# SA learned>
    192.168.4.4: 8
SA State per ASN Counters, <asn>: <# sources>/<# groups>
    Total entries: 8
    ?: 8/8
```

ステップ 5 **show ip msdp peer** [*peer-address* | *peer-name*]

このコマンドを使用して、MSDP ピアに関する詳細情報を表示します。

オプションの *peer-address* 引数または *peer-name* 引数を使用して、特定のピアに関する情報を表示します。

次に、**show ip msdp peer** コマンドの出力例を示します。

例：

```
Device# show ip msdp peer 192.168.4.4
MSDP Peer 192.168.4.4 (?), AS 64512 (configured AS)
  Connection status:
    State: Up, Resets: 0, Connection source: Loopback0 (2.2.2.2)
    Uptime(Downtime): 00:07:55, Messages sent/received: 8/18
    Output messages discarded: 0
    Connection and counters cleared 00:08:55 ago
  SA Filtering:
    Input (S,G) filter: none, route-map: none
    Input RP filter: none, route-map: none
    Output (S,G) filter: none, route-map: none
    Output RP filter: none, route-map: none
  SA-Requests:
    Input filter: none
  Peer ttl threshold: 0
  SAs learned from this peer: 8
  Input queue size: 0, Output queue size: 0
  MD5 signature protection on MSDP TCP connection: not enabled
```

ステップ 6 **show ip msdp sa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*]

このコマンドを使用して、MSDP ピアから学習した (S, G) ステートを表示します。

次に、**show ip msdp sa-cache** コマンドの出力例を示します。

例：

```
Device# show ip msdp sa-cache
MSDP Source-Active Cache - 8 entries
(10.44.44.5, 239.232.1.0), RP 192.168.4.4, BGP/AS 64512, 00:01:20/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.1), RP 192.168.4.4, BGP/AS 64512, 00:01:20/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.2), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.3), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.4), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
```

```
(10.44.44.5, 239.232.1.5), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.6), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.7), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
```

ステップ 7 **show ip msdp summary**

このコマンドを使用して、MSDP ピアのステータスを表示します。

次に、**show ip msdp summary** コマンドの出力例を示します。

例：

```
Device# show ip msdp summary
MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
                                Downtime Count Count
192.168.4.4      4     Up       00:08:05 0     8     ?
```

MSDP 接続統計情報および SA キャッシュ エントリの消去

MSDP 接続、統計情報または SA キャッシュ エントリを消去するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **clear ip msdp peer** [*peer-address* | *peer-name*]
3. **clear ip msdp statistics** [*peer-address* | peer-name]
4. **clear ip msdp sa-cache** [*group-address*]

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	**clear ip msdp peer** [*peer-address*	*peer-name*] **例**： `Device# clear ip msdp peer`	指定された MSDP ピアへの TCP 接続をクリアし、すべての MSDP メッセージ カウンタをリセットします。
ステップ 3	**clear ip msdp statistics** [*peer-address*	peer-name] **例**： `Device# clear ip msdp statistics`	指定された MSDP ピアの統計カウンタをクリアし、すべての MSDP メッセージ カウンタをリセットします。

	コマンドまたはアクション	目的
ステップ 4	**clear ip msdp sa-cache** [*group-address*] 例： `Device# clear ip msdp sa-cache`	SA キャッシュ エントリを消去します。 • **clear ip msdp sa-cache** コマンドにオプションの *group-address* 引数または *source-address* 引数を指定した場合、すべての SA キャッシュエントリが消去されます。 • 特定のグループに関連付けられたすべての SA キャッシュ エントリを消去するには、オプションの *group-address* 引数を使用します。

MSDPの簡易ネットワーク管理プロトコル（SNMP）モニタリングのイネーブル化

MSDP の簡易ネットワーク管理プロトコル（SNMP）モニタリングをイネーブルにするには、次の任意の作業を実行します。

始める前に

- SNMP および MSDP はデバイスに設定されています。
- 各 PIM-SM ドメインには、MSDP スピーカーとして設定されているデバイスが必要です。このデバイスは、SNMP と MSDP MIB がイネーブルに設定されている必要があります。

（注）
- すべての MSDP-MIB オブジェクトは読み取り専用として実装されます。
- 要求テーブルは、シスコの MSDP MIB の実装ではサポートされていません。
- MSDP 確立の通知は、シスコの MSDP MIB の実装ではサポートされていません。

手順の概要

1. **enable**
2. **snmp-server enable traps msdp**
3. **snmp-server host** *host* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth**| **priv** | **noauth**]}] *community-string* [**udp-port** *port-number*] **msdp**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**snmp-server enable traps msdp** 例： `Device# snmp-server enable traps msdp`	SNMP で使用される MSDP 通知の送信をイネーブルにします。 （注） **snmp-server enable traps msdp** コマンドは、トラップと通知の両方をイネーブルにします。
ステップ 3	**snmp-server host** *host* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth**| **priv** | **noauth**]}] *community-string* [**udp-port** *port-number*] **msdp** 例： `Device# snmp-server host examplehost msdp`	MSDP トラップまたは応答要求の受信者（ホスト）を指定します。
ステップ 4	**exit** 例： `Device(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、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

MSDP MIB 通知の結果とソフトウェアの出力を比較するには、適切なデバイスで **show ip msdp summary** コマンドおよび **show ip msdp peer** コマンドを使用します。また、これらのコマンドの結果と SNMP GET 操作の結果を比較することもできます。SA キャッシュテーブルエントリを確認するには、**show ip msdp sa-cache** コマンドを使用します。接続のローカルアドレス、ローカルポート、リモートポートなどのその他のトラブルシューティング情報は、**debug ip msdp** コマンドの出力を使用して取得できます。

MSDP を使用して複数の PIM-SM ドメインを相互接続する設定例

ここでは、MSDP を使用して複数の PIM-SM ドメインを相互接続するための設定例を紹介します。

例：MSDP ピアの設定

次に、3 つの MSDP ピア間で MSDP ピアリング接続を確立する例を示します。

デバイス A

```
!
interface Loopback 0
 ip address 10.220.8.1 255.255.255.255
!
ip msdp peer 10.220.16.1 connect-source Loopback0
ip msdp peer 10.220.32.1 connect-source Loopback0
!
```

デバイス B

```
!
interface Loopback 0
 ip address 10.220.16.1 255.255.255.255
!
ip msdp peer 10.220.8.1 connect connect-source Loopback0
ip msdp peer 10.220.32.1 connect connect-source Loopback0
!
```

デバイス C

```
!
interface Loopback 0
 ip address 10.220.32.1 255.255.255.255
!
ip msdp peer 10.220.8.1 connect 10.220.8.1 connect-source Loopback0
ip msdp peer 10.220.16.1 connect 10.220.16.1 connect-source Loopback0
!
```

例：MSDP MD5 パスワード認証の設定

次に、2 つの MSDP ピア間の TCP 接続の MD5 パスワード認証をイネーブルにする例を示します。

デバイス A

```
!
ip msdp peer 10.3.32.154
ip msdp password peer 10.3.32.154 0 test
!
```

デバイス B

```
!
ip msdp peer 10.3.32.153
ip msdp password peer 10.3.32.153 0 test
!
```

例：デフォルト MSDP ピアの設定

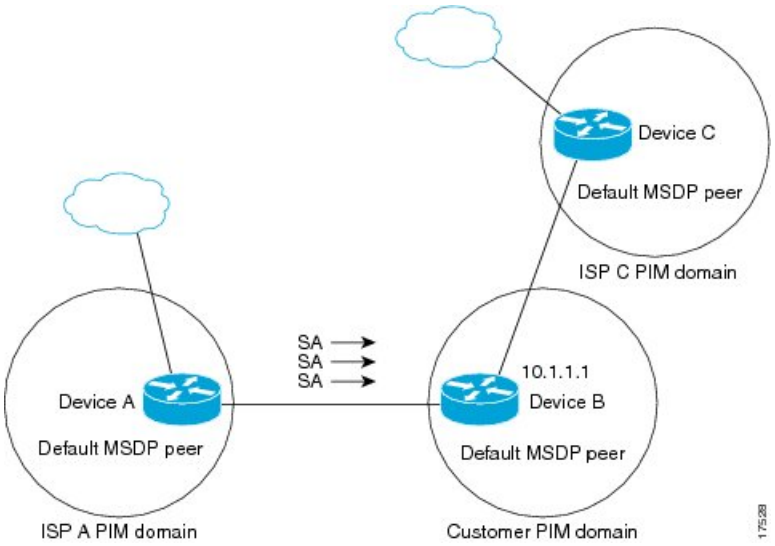
下の図に、デフォルトの MSDP ピアが使用されるシナリオを示します。この図では、デバイス B を所有するカスタマーが 2 つの ISP を介してインターネットに接続されています。一方の ISP はデバイス A を所有し、もう一方の ISP はデバイス C を所有しています。どちらもそれらの間で (M)BGP を実行していません。カスタマーが ISP ドメインまたは他のドメイン内のソースについて学習するために、デバイス B はデバイス A をデフォルト MSDP ピアとして識別します。デバイス B はデバイス A とデバイス C の両方に SA メッセージをアドバタイズしますが、デバイス A だけまたはデバイス C だけから SA メッセージを受け入れます。デバイス A が設定内の最初のデフォルト ピアである場合、デバイス A が稼働していればデバイス A が使用されます。デバイス A が稼働していない場合に限り、デバイス B がデバイス C からの SA メッセージを受け入れます。

ISP は、プレフィックス リストを使用して、カスタマーのデバイスから受け入れるプレフィックスを定義する場合もあります。カスタマーは、複数のデフォルト ピアを定義します。各ピアには関連するプレフィックスを 1 つまたは複数設定します。

カスタマーは 2 つの ISP を使用しています。カスタマーはこの 2 つの ISP をデフォルト ピアとして定義します。設定内で最初のデフォルト ピアとして特定されているピアが稼働している限り、このピアがデフォルト ピアになり、カスタマーはそのピアから受信するすべての SA メッセージを受け入れます。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *20 :* デフォルト *MSDP* ピアのシナリオ



デバイス B はデバイス A およびデバイス C に SA をアドバタイズしますが、デバイス A またはデバイス C だけを使用して SA メッセージを受け入れます。デバイス A が設定ファイル内の最初のデバイスである場合、デバイス A が稼働していればデバイス A が使用されます。デバ

イス A が稼働していない場合に限り、デバイス B がデバイス C から SA メッセージを受け入れます。これは、プレフィックス リストを使用しない動作です。

プレフィックス リストを指定すると、リスト内のプレフィックスに対してだけピアはデフォルト ピアになります。プレフィックス リストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。プレフィックス リストがない場合も、複数のデフォルト ピアを設定できますが、アクティブなデフォルト ピアになるのは最初のピアだけです（このピアにデバイスが接続されていて、ピアがアクティブの場合に限ります）。最初に設定されたピアがダウンするか、このピアとの接続がダウンした場合、2 番目に設定されたピアがアクティブなデフォルト ピアになります。以下同様です。

次に、図に示されているデバイス A およびデバイス C の部分的な設定例を示します。これらの ISP にはそれぞれ、図に示すカスタマーのような、デフォルト ピアリングを使用している複数のカスタマーがいる可能性があります。そのようなカスタマーの設定は類似しています。つまり、SA が対応するプレフィックス リストによって許可される場合、デフォルト ピアからの SA だけを受け入れます。

デバイス A の設定

```
ip msdp default-peer 10.1.1.1
ip msdp default-peer 10.1.1.1 prefix-list site-b ge 32
ip prefix-list site-b permit 10.0.0.0/8
```

デバイス C の設定

```
ip msdp default-peer 10.1.1.1 prefix-list site-b ge 32
ip prefix-list site-b permit 10.0.0.0/8
```

例：MSDP メッシュ グループの設定

次に、3 台のデバイスを MSDP メッシュ グループのフル メッシュ メンバになるように設定する例を示します。

デバイス A の設定

```
ip msdp peer 10.2.2.2
ip msdp peer 10.3.3.3
ip msdp mesh-group test-mesh-group 10.2.2.2
ip msdp mesh-group test-mesh-group 10.3.3.3
```

デバイス B の設定

```
ip msdp peer 10.1.1.1
ip msdp peer 10.3.3.3
ip msdp mesh-group test-mesh-group 10.1.1.1
ip msdp mesh-group test-mesh-group 10.3.3.3
```

デバイス C の設定

```
ip msdp peer 10.1.1.1
ip msdp peer 10.2.2.2
ip msdp mesh-group test-mesh-group 10.1.1.1
ip msdp mesh-group test-mesh-group 10.2.2.2
```

マルチキャスト送信元検出プロトコルに関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9300 Series Switches)* の「IP マルチキャスト ルーティング コマンド」の項を参照してください。

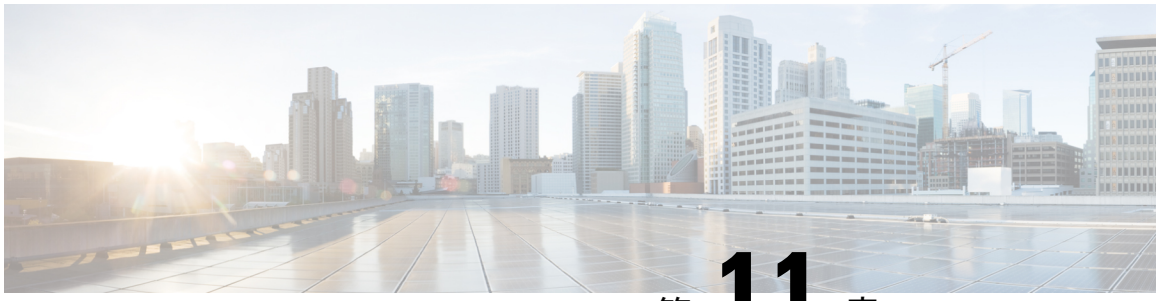
Multicast Source Discovery Protocol の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	Multicast Source Discovery Protocol	MSDP は複数の PIM-SM ドメインを接続するメカニズムです。MSDP は、他の PIM ドメイン内のマルチキャスト送信元を検出することを目的としています。MSDP の主な利点は、（一般的な共有ツリーではなく）ドメイン間ソース ツリーを PIM-SM ドメインで使用できるようにし、複数の PIM-SM ドメインを相互接続する複雑性を軽減することです。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。



第 11 章

SSM の設定

SSM の設定の前提条件

次に、Source-Specific Multicast （SSM）およびSSMマッピングを設定するための前提条件を示します。

- SSM マッピングを設定する前に、次の作業を実行する必要があります。
  - IP マルチキャスト ルーティングをイネーブルにします。
  - PIM スパース モードをイネーブルにします。
  - SSM を設定します。
- スタティック SSM マッピングを設定する場合は、事前にアクセス コントロール リスト（ACL）を設定して、送信元アドレスにマッピングされるグループ範囲を定義する必要があります。
- SSMマッピングを設定し、DNSルックアップで使用できるようにするには、稼動中のDNSサーバーにレコードを追加する必要があります。稼働中の DNS サーバーがない場合は、DNS サーバーをインストールする必要があります。

（注） 実行中のDNSサーバーにレコードを追加するには、*Cisco Network Registrar* などの製品を使用できます。

SSM 設定の制約事項

次に、SSM を設定する際の制約事項を示します。

- IGMPv3 で SSM を使用するには、Cisco IOS ルータ、アプリケーションが稼働しているホスト、そしてアプリケーション自体が SSM をサポートしている必要があります。
- SSM にまだ対応していない、ネットワーク内の既存のアプリケーションは、(S, G) チャネル加入をサポートするように変更されないと、SSM 範囲内では機能しません。そのため、既存のアプリケーションが指定の SSM 範囲内のアドレスを使用する場合、ネットワークで SSM をイネーブルにすると問題が発生することがあります。
- IGMP スヌーピング：IGMPv3 で使用される新しいメンバーシップ レポート メッセージは、旧型の IGMP スヌーピングデバイスでは正しく認識されない場合があります。
- SSM をレイヤ 2 スイッチング メカニズムとともに使用する場合は、ある程度のアドレス管理が必要となります。Cisco Group Management Protocol（CGMP）、IGMP スヌーピング、または Router-Port Group Management Protocol（RGMP）でサポートされるのはグループ固有のフィルタリングだけであり、（S, G）チャネル固有のフィルタリングはサポートされていません。同じスイッチドネットワーク内の異なるレシーバーが異なる（S, G）チャネルを要求し、これらのチャネルが同じグループを共有している場合、レシーバーは上記のような既存メカニズムの利点を活用できません。どちらのレシーバーも、すべての（S, G）チャネル トラフィックを受信し、不要なトラフィックを入力から除外します。SSM は、独立した多くのアプリケーションに SSM 範囲のグループ アドレスを再利用できるので、このような状況では、スイッチド ネットワークのトラフィック フィルタリング機能が低下する可能性があります。そのため、アプリケーションに対して SSM 範囲の IP アドレスをランダムに使用し、SSM 範囲内の 1 つのアドレスがさまざまなアプリケーションに再利用される可能性を小さくすることが重要です。たとえば、TV チャネル セットを提供するアプリケーション サービスで、SSM を使用する場合は、各 TV（S, G）チャネルに異なるグループを使用する必要があります。このようにすれば、同じアプリケーション サービス内の異なるチャネルに複数のレシーバが接続されていても、レイヤ 2 デバイスを含むネットワークでトラフィック エイリアシングが発生しなくなります。
- PIM-SSM では、ラストホップ ルータは、そのインターフェイス上に適切な（S, G）加入登録があると、定期的に（S, G）Join メッセージを送信し続けます。このため、レシーバが（S, G）加入を送信する限り、ソースが長時間（または二度と）トラフィックを送信しなくてもレシーバからソースへの最短パス ツリー（SPT）状態が維持されます。

  送信元がトラフィックを送信し、レシーバーがグループに加入している場合にだけ（S, G）ステートが維持される PIM-SM では、これとは対照的な状況が発生します。PIM-SM では、送信元がトラフィックの送信を 3 分以上停止すると、（S, G）ステートは削除され、その送信元からのパケットが RPT を通じて再度到達した場合のみに再確立されます。PI-SSM では、送信元がアクティブであることをレシーバに通知するメカニズムがないので、レシーバが（S, G）チャネルの受信を要求している限り、（S, G）ステートを維持する必要があります。

次に、SSM マッピングを設定する際の制約事項を示します。

- SSM マッピング機能で、SSM の利点をすべて共有できるわけではありません。SSM マッピングでは、ホストからグループ G の加入が取得され、1 つまたは複数のソースに関連付けられているアプリケーションでこのグループを指定できるため、グループ G ごとにこのようなアプリケーション 1 つのみをサポートできます。それにもかかわらず、完全な SSM アプリケーションは、SSM マッピングにも使用される同じグループを共有することができます。
- 完全な SSM への移行ソリューションとして SSM マッピングだけを使用する場合は、ラストホップ ルータの IGMPv3 をイネーブルにする際に十分に注意してください。SSM マッピングと IGMPv3 を両方イネーブルにした場合、すでに IGMPv3 をサポートしている（SSM はサポートしていない）ホストは IGMPv3 グループ レポートを送信します。SSM マッピングは、このような IGMPv3 グループ レポートをサポートしていないので、ルータは送信元をこれらのレポートと正しく関連付けることができません。

SSM に関する情報

Source-Specific Multicast（SSM; 送信元特定マルチキャスト）機能は、IP マルチキャストの拡張機能であり、この機能を使用すると、受信者に転送されるデータグラム トラフィックは、その受信者が明示的に加入しているマルチキャスト送信元からのトラフィックだけになります。SSM 用にマルチキャスト グループを設定する場合、SSM 配信ツリー（共有ツリーはない）だけが作成されます。

ここでは、Source-Specific Multicast（SSM）の設定方法を説明します。この項の SSM コマンドの詳細な説明については、『*IP Multicast Command Reference*』を参照してください。

SSM コンポーネントの概要

SSM は、1 対多のアプリケーション（ブロードキャスト アプリケーション）に最適なデータグラム配信モデルです。SSM は、オーディオおよびビデオのブロードキャスト アプリケーション環境を対象としたシスコの IP マルチキャスト ソリューションの中核的なネットワーキング テクノロジーです。このデバイスは、次のコンポーネントをサポートしているため、SSM の実装が可能です。

- Protocol Independent Multicast Source-Specific Mode（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、PIM Sparse Mode（PIM-SM）に基づいています。

- Internet Group Management Protocol version 3（IGMPv3）

SSM および Internet Standard Multicast（ISM）

インターネットの現行の IP マルチキャスト インフラストラクチャや多くの企業のイントラネットは、PIM-SM プロトコルと Multicast Source Discovery Protocol（MSDP）に基づいています。これらのプロトコルには、Internet Standard Multicast（ISM）サービス モデルの限界がありま

す。たとえば、ISM では、ネットワークは、実際にマルチキャスト トラフィックを送信しているホストについての情報を維持する必要があります。

ISM サービスは、任意の送信元からマルチキャスト ホスト グループと呼ばれるレシーバー グループへの IP データグラムの配信でなりたっています。マルチキャスト ホスト グループのデータグラム トラフィックは、任意の IP ユニキャスト送信元アドレス（S）と IP 宛先アドレスとしてのマルチキャスト グループ アドレス（G）のデータグラムで構成されます。システムは、ホスト グループのメンバーになることによって、このトラフィックを受信します。ホスト グループのメンバーシップには IGMP バージョン 1、2、または 3 によるホスト グループのシグナリングが必要です。

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。SSM と ISM のどちらでも、ソースになるためにシグナリングは必要ありません。ただし、SSM では、レシーバーは特定の送信元からのトラフィックの受信または非受信を決めるために（S, G）への加入または脱退を行う必要があります。つまり、レシーバは加入した（S,G）チャネルからだけトラフィックを受信できます。一方、 ISM では、レシーバは受信するトラフィックの送信元の IP アドレスを知る必要はありません。チャネル加入シグナリングの標準的な方法として、IGMP を使用してモードメンバーシップ レポートを包含することが提案されていますが、この手法をサポートしているのは IGMP version 3 だけです。

SSM IP アドレスの範囲

IP マルチキャスト グループ アドレス範囲の設定済みのサブセットに SSM 配信モデルを適用することにより、SSM と ISM サービスを一緒に使用できます。Cisco IOS ソフトウェアでは、224.0.0.0 ～ 239.255.255.255 の IP マルチキャスト アドレス範囲の SSM 設定が可能です。SSM 範囲が定義されている場合、既存の IP マルチキャスト受信アプリケーションが SSM 範囲のアドレスの使用を試行しても、トラフィックを受信できません。

SSM の動作

確立されているネットワークは、IP マルチキャスト サービスが PIM SM に基づいているので、SSM サービスをサポートできます。SSM サービスだけが必要な場合は、ドメイン間の PIM-SM に必要な全プロトコル範囲（MSDP、Auto-RP、またはブートストラップ ルータ（BSR））ではなく、SSM を単独でネットワークに配置することもできます。

PIM-SM 用に設定されているネットワークに SSM を配置する場合、SSM をサポートするのはラストホップ ルータだけです。レシーバーに直接接続されていないルータは SSM をサポートする必要はありません。一般的に、ラストホップ以外のルータに必要なのは、SSM 範囲内の PIM-SM だけです。このようなルータは SSM 範囲内での MSDP シグナリング、登録、PIM-SM 共有ツリー操作を抑制するために、ほかのアクセス コントロール設定が必要になる場合もあります。

SSM の範囲を設定し SSM をイネーブルにするには、**ip pim ssm** 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。この設定による影響は次のとおりです。

- SSM 範囲内のグループは、IGMPv3 include モード メンバーシップ レポートを通じて、（S, G）チャネルに加入できます。

- SSM 範囲のアドレスの PIM 動作は、PIM-SM の派生モードである PIM-SSM に変更されます。このモードでは、ルータで生成されるのは PIM（S, G）の join と prune のメッセージだけであり、（S, G）の Rendezvous Point Tree（RPT）や（*, G）の RPT メッセージは生成されません。RPT 動作に関連する着信メッセージは無視されるか拒否されます。着信 PIM 登録メッセージに対しては即座に register-stop メッセージで応答が行われます。ラストホップ ルータ以外のルータでは、PIM-SSM は PIM-SM と下位互換性を保ちます。したがって、ラストホップ ルータ以外のルータは SSM グループに PIM-SM を使用できます（SSM をサポートしていない場合など）。
- SSM 範囲内の Source-Active（SA）メッセージは、受け入れ、生成、転送のいずれも実行されません。

SSM マッピング

典型的なセットトップ ボックス（STB）配置では、各 TV チャネルは独立した 1 つの IP マルチキャスト グループを使用し、その TV チャネルの送信を行うアクティブなサーバーは 1 つです。1 つのサーバーから複数の TV チャネルへの送信は可能ですが、各チャネルのグループはそれぞれ異なります。このようなネットワーク環境で、ルータが特定のグループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信した場合、レポートの宛先は、そのマルチキャスト グループに関連付けられている TV チャネルの well-known TV サーバーになります。

SSM マッピングが設定されている場合、特定グループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信したルータは、レポートを、このグループに関連付けられている well-known 送信元の 1 つ以上のチャネル メンバーシップに変換します。

ルータは、IGMPv1 または IGMPv2 のメンバーシップ レポートを受信すると、SSM マッピングを使用して、そのグループ に 1 つ以上の送信元 IP アドレスを決定します。その後、SSM マッピングによって、そのメンバーシップ レポートが IGMPv3 レポートに変換され、IGMPv3 レポートを受信した場合と同様に処理が続行されます。IGMPv1 または IGMPv2 メンバーシップ レポートの受信が続き、そのグループの SSM マッピングが同じである限り、ルータは PIM join を送信し、グループに加入し続けます。

SSM マッピング機能を使用すると、ラストホップ ルータはスタティックに設定されたルータ上のテーブルまたは DNS サーバーを通じて、送信元アドレスを決定できます。スタティックに設定されたテーブルまたは DNS マッピングが変更された場合、ルータは加入しているグループに関連付けられている現在の送信元から脱退します。

スタティック SSM マッピング

スタティック SSM マッピングでは、ラストホップ ルータは、グループへの送信を行う送信元を決定するために、継続的にスタティック マップを使用します。スタティック SSM マッピングを使用するには、グループ範囲を定義した ACL を設定する必要があります。グループ範囲を定義する ACL を設定した後、**ip igmp ssm-map static** 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、ACL で許可されたグループを送信元にマッピングできます。

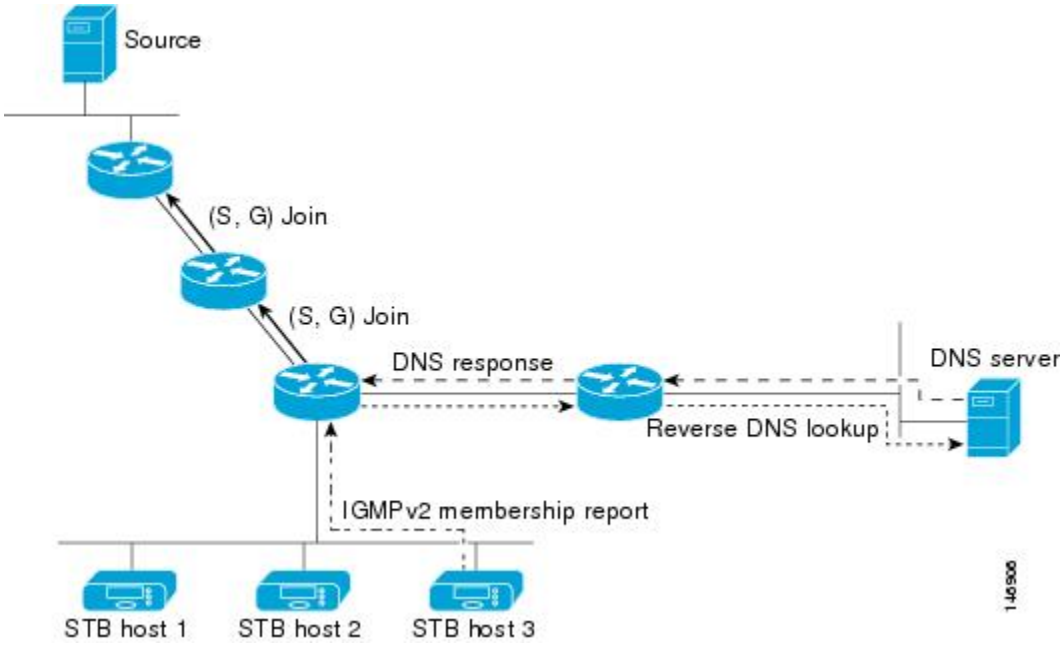
DNSが必要とされないか、またはローカルでDNSマッピングが変更される場合、小規模なネットワークではスタティック SSM マッピングを設定できます。設定されたスタティック SSM マッピングは、DNS マッピングよりも優先されます。

DNS ベースの SSM マッピング

DNSベースのSSMマッピングを使用して、ラストホップルータが継続的に逆DNSルックアップを実行し、グループに送信する送信元を決定するようにすることも可能です。DNSベースのSSM マッピングが設定されると、ルータはグループ名を含むドメイン名を構築し、DNS への逆ルックアップを実行します。ルータは IP アドレス リソースを検索し、それらをグループに関連付けられた送信元アドレスとして使用します。SSMマッピングでサポートできる送信元の数は、グループごとに最大 20 です。ルータは各グループに設定されているすべてのソースに加入します。

図 *21 : DNS* ベースの *SSM* マッピング

次の図は、DNS ベースの SSM マッピングを示します。



ラスト ホップ ルータが 1 つのグループの複数の送信元に加入できるようにする SSM マッピング メカニズムによって、TV ブロードキャストの送信元に冗長性を持たせることができます。この場合、ラストホップ ルータは、SSM マッピングを使用し、同じ TV チャネルに対して 2 つのビデオ送信元に同時に加入することにより冗長性を提供します。ただし、ラストホップ ルータでのビデオ トラフィックの重複を防ぐため、ビデオ送信元がサーバー側でスイッチオーバー メカニズムを使用する必要があります。一方のビデオ送信元はアクティブ、もう一方のバックアップ ビデオ送信元はパッシブになります。パッシブの送信元は待機状態になり、アクティブな送信元の障害が検出された場合に、そのTVチャネルにビデオ トラフィックを送信します。サーバー側のスイッチオーバー メカニズムによって、実際にそのTVチャネルにビデオ トラフィックを送信するサーバーは 1 つだけになります。

G1、G2、G3、G4 を含むグループの 1 つ以上の送信元アドレスを検索するには、DNS サーバーに次のような DNS レコードを設定する必要があります。

```
G4.G3.G2.G1 [multicast-domain] [timeout] IN A source-address-1
 IN A source-address-2
 IN A source-address-n
```

DNS リソース レコードの設定の詳細については、DNS サーバーのマニュアルを参照してください。

SSM の設定方法

SSM の設定

SSM を設定するには、次の手順を実行します。

この手順は任意です。

始める前に

Source Specific Multicast（SSM）範囲の定義にアクセスリストを使用する場合、**ip pim ssm** コマンドでアクセスリストを参照する前にアクセスリストを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip pim ssm** [**default** | **range** *access-list*]
4. **interface** *type number*
5. **ip pim** {**sparse-mode** }
6. **ip igmp version 3**
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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）。

	コマンドまたはアクション	目的
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	**ip pim ssm** [**default** | **range** *access-list*] 例： `Device(config)# ip pim ssm range 20`	IP マルチキャスト アドレスの SSM 範囲を定義します。
ステップ 4	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/1`	IGMPv3 をイネーブルに設定可能なホストに接続されているインターフェイスを選択し、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 コンフィギュレーション コマンドを入力して設定された物理ポートです。 • 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。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 5	**ip pim** {**sparse-mode** } 例： `Device(config-if)# ip pim sparse-mode`	インターフェイスに対して PIM をイネーブルにします。
ステップ 6	**ip igmp version 3** 例： `Device(config-if)# ip igmp version 3`	このインターフェイス上で IGMPv3 をイネーブルにします。デフォルトでは、IGMP のバージョン 2 が設定されます。
ステップ 7	**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 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-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。

Source-Specific Multicast（SSM）マッピングの設定

Source Specific Multicast（SSM）マッピング機能は、管理上または技術上の理由からエンド システムで SSM をサポートできないかまたはサポートが望ましくない場合に SSM 移行手段として使用できます。SSM マッピングを使用すると、IGMPv3 をサポートしないレガシー STB へのビデオ配信や、IGMPv3 ホスト スタックを使用しないアプリケーションに SSM を活用できます。

スタティック SSM マッピングの設定

スタティック SSM マッピングを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp ssm-map enable**
4. **no ip igmp ssm-map query dns**
5. **ip igmp ssm-map static** *access-list source-address*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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）。

	コマンドまたはアクション	目的
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	**ip igmp ssm-map enable** 例： `Device(config)# ip igmp ssm-map enable`	設定されている SSM 範囲で、グループの SSM マッピングをイネーブルにします。 （注） このコマンドでは、デフォルトで、DNS ベースの SSM マッピングがイネーブルにされます。
ステップ 4	**no ip igmp ssm-map query dns** 例： `Device(config)# no ip igmp ssm-map query dns`	（任意）DNS ベースの SSM マッピングをディセーブルにします。 （注） スタティック SSM マッピングだけを使用する場合は、DNS ベースの SSM マッピングをディセーブルにします。デフォルトでは、**ip igmp ssm-map** コマンドによって DNS ベースの SSM マッピングがイネーブルになります。
ステップ 5	**ip igmp ssm-map static** *access-list source-address* 例： `Device(config)# ip igmp ssm-map static 11 172.16.8.11`	スタティック SSM マッピングを設定します。 • *access-list* 引数に入力した ACL によって、*source-address* 引数に入力したソース IP アドレスにマッピングされるグループが決まります。 （注） 追加のスタティック SSM マッピングを設定することもできます。SSM マッピングを追加設定した場合、ルータが SSM 範囲のグループの IGMPv1 または IGMPv2 のメンバーシップレポートを受信すると、デバイスは、設定されている各 **ip igmp ssm-map static** コマンドに基づいて、そのグループに関連付けられている送信元アドレスを特定します。デバイスは各グループに最大 20 の送信元を関連付けます。 必要な場合は、ステップを繰り返して、追加のスタティック SSM マッピングを設定します。
ステップ 6	**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
	`Device(config)# end`	
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-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。

DNS ベースの SSM マッピングの設定

DNS ベースの SSM マッピングを設定するには、DNS サーバー ゾーンを作成するか、または既存のゾーンにレコードを追加する必要があります。DNS ベースの SSM マッピングを使用するルータが他の目的にも DNS を使用している場合は、通常の設定の DNS サーバーを使用する必要があります。そのルータで使用されている DNS 実装が DNS ベースの SSM マッピングだけの場合は、ルート ゾーンが空であるか、またはそれ自身を指すようなフォールス DNS セットアップが可能です。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp ssm-map enable**
4. **ip igmp ssm-map query dns**
5. **ip domain multicast** *domain-prefix*
6. **ip name-server** *server-address1* [*server-address2...server-address6*]
7. 冗長性のために追加の DNS サーバーを設定する場合は、必要に応じて、ステップ 6 を繰り返します。
8. **end**
9. **show running-config**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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
	`Device> enable`	
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	**ip igmp ssm-map enable** 例： `Device(config)# ip igmp ssm-map enable`	設定されている SSM 範囲で、グループの SSM マッピングをイネーブルにします。
ステップ 4	**ip igmp ssm-map query dns** 例： `Device(config)# ip igmp ssm-map query dns`	（任意）DNS ベースの SSM マッピングをイネーブルにします。 • デフォルトでは、**ip igmp ssm-map** コマンドによって DNS ベースの SSM マッピングがイネーブルになります。実行コンフィギュレーションに保存されるのは、このコマンドを **no** 形式で使用した場合だけです。 （注） DNS ベースの SSM マッピングがディセーブルの場合、このコマンドを使用して DNS ベースの SSM マッピングを再度イネーブルにします。
ステップ 5	**ip domain multicast** *domain-prefix* 例： `Device(config)# ip domain multicast ssm-map.cisco.com`	（任意）DNS ベースの SSM マッピングに使用するドメイン プレフィックスを変更します。 • デフォルトでは、ip-addr.arpa ドメイン プレフィックスが使用されます。
ステップ 6	**ip name-server** *server-address1* [*server-address2...server-address6*] 例： `Device(config)# ip name-server 10.48.81.21`	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバーのアドレスを指定します。
ステップ 7	冗長性のために追加の DNS サーバーを設定する場合は、必要に応じて、ステップ 6 を繰り返します。	
ステップ 8	**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
	`Device(config)# end`	
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-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。

SSM マッピングを使用したスタティック トラフィック転送の設定

ラスト ホップ ルータ上の SSM マッピングでスタティック トラフィック転送を設定する場合は、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip igmp static-group** *group-address* **source ssm-map**
5. **end**
6. **show running-config**
7. **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： `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	**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 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	SSM マッピングを使用してマルチキャスト グループにスタティックにトラフィックを転送するインターフェイスを選択し、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 コンフィギュレーション コマンドを入力して設定された物理ポートです。 • 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。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。 （注） SSM マッピングを使用したトラフィックのスタティック転送は、DNS ベースの SSM マッピングとスタティックに設定された SSM マッピングのいずれかで機能します。
ステップ 4	**ip igmp static-group** *group-address* **source ssm-map** 例： `Device(config-if)# ip igmp static-group 239.1.2.1 source ssm-map`	そのインターフェイスから（S, G）チャネルへのスタティック転送用の SSM マッピングを設定します。 このコマンドは、特定グループに SSM トラフィックをスタティックに転送する場合に使用します。チャネルの送信元アドレスを決定するには DNS ベースの SSM マッピングを使用します。
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	**show running-config** 例： `Device# show running-config`	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 7	**copy running-config startup-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。

SSM のモニタリング

SSM をモニターするには、次の表の特権 EXEC コマンドを使用します。

表 *18 : SSM* のモニタリング コマンド

コマンド	目的
show ip igmp groups detail	IGMPv3 による (S, G) チャネル加入登録を表示します。
show ip mroute	マルチキャスト グループが SSM サービスをサポートしているかどうか、または送信元固有のホスト レポートが受信されたかどうかを表示します。

SSM マッピングのモニタリング

SSM マッピングをモニターするには、次の表の特権 EXEC コマンドを使用します。

表 *19 : SSM* マッピングをモニターするコマンド

コマンド	目的
show ip igmp ssm-mapping	SSM マッピングについての情報を表示
show ip igmp ssm-mapping *group-address*	SSM マッピングが特定のグループに使 示します。
show ip igmp groups [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]	ルータに直接接続されているレシーバ 学習されたレシーバを持つマルチキャ 示します。
show host	デフォルトのドメイン名、名前ルック ネーム サーバー ホストのリスト、およ レスのキャッシュされたリストを表示

コマンド	目的
debug ip igmp *group-address*	送受信された IGMP パケットと IGMP ホトを表示します。

SSM の次の作業

次の設定を行えます。

- IGMP
- PIM
- IP マルチキャスト ルーティング
- サービス検出ゲートウェイ

SSM に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)*

標準および RFC

標準/RFC	タイトル
RFC 4601	『*Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*』

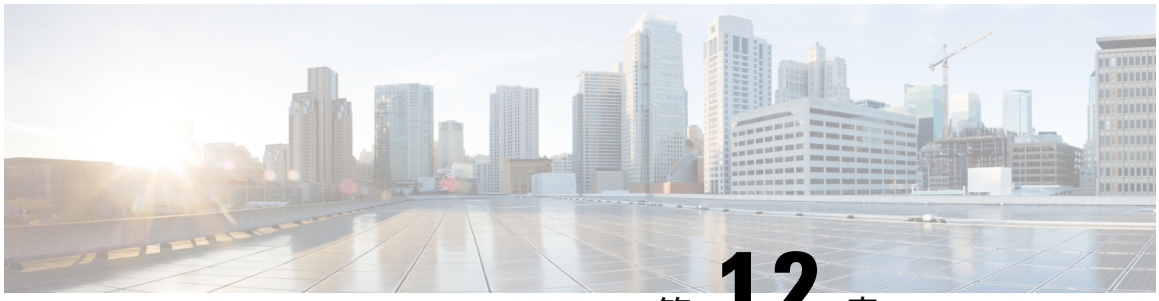
SSM の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	SSM	SSM は、受信者が明示的に参加したマルチキャストソースからのみデータグラムトラフィックが受信者に転送される IP マルチキャストの拡張機能です。SSM 用にマルチキャスト グループを設定する場合、SSM 配信ツリー（共有ツリーはない）だけが作成されます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。



第 12 章

Local Area Bonjour および Wide Area Bonjour ドメインの設定

Bonjour ソリューション向け Cisco DNA サービスの概要

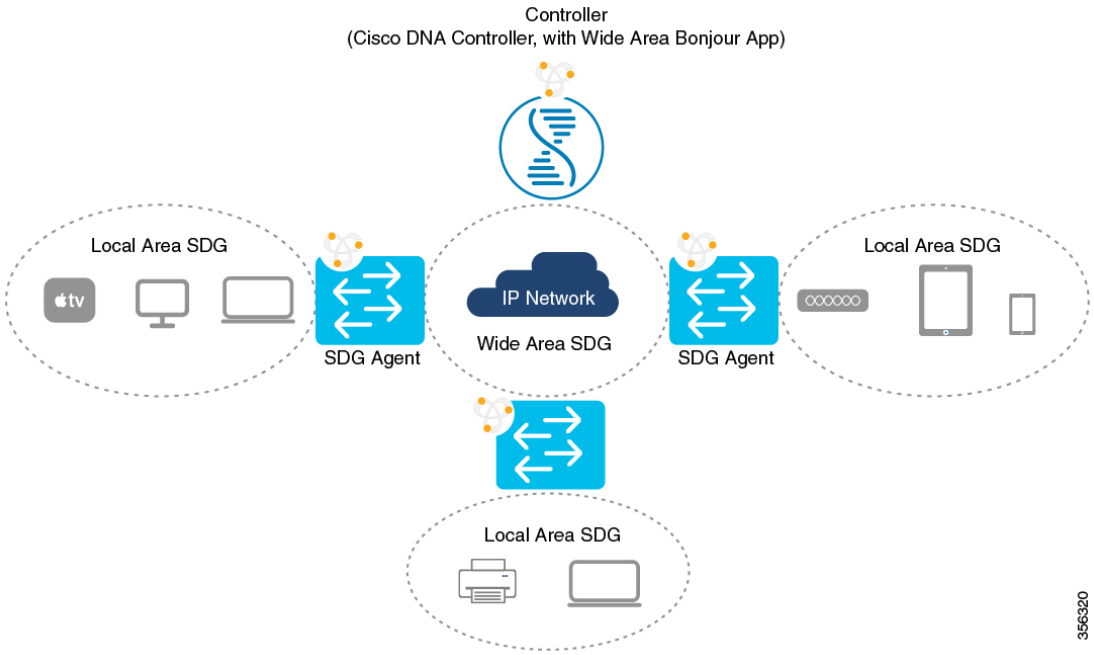
Cisco DNA Center 上の Cisco Wide Area Bonjour アプリケーションの概要

Apple Bonjour プロトコルは、ネットワーク設定をシンプル化する設定不要のソリューションであり、接続デバイス、サービス、およびアプリケーション間の通信を確立します。Bonjour を使用すると、最小限の操作と設定で共有サービスを検出して使用できます。Bonjour は単一のレイヤ 2 ドメイン用に設計されており、ホームネットワークなどの小規模でフラットな単一ドメイン構成に最適です。Cisco Wide Area Bonjour ソリューションは、単一のレイヤ 2 ドメインの制約を排除し、Cisco Software-Defined Access（SD-Access）や VXLAN を備えた業界標準の BGP EVPN といったオーバーレイネットワークを含む、エンタープライズグレードの従来型有線およびワイヤレスネットワークまで対応範囲を拡張します。

Wide Area Bonjour アプリケーションは、コントローラベースのソフトウェアデファインド ソリューションです。デバイスがレイヤ 2 ドメイン全体で Bonjour サービスをアドバタイズおよび検出できるようにし、それらのサービスをさまざまな有線およびワイヤレスのエンタープライズ ネットワークに適用できるようにします。Wide Area Bonjour アプリケーションは、大規模なセキュリティ、ポリシーの適用、サービス管理に関連する問題にも対処します。この新しい分散型アーキテクチャは、マルチキャスト DNS（mDNS）フラッド境界を排除して、ユニキャストベースのサービスルーティングに移行するように設計されており、ポリシー適用ポイントを提供し、Bonjour サービスの管理を可能にします。Wide Area Bonjour アプリケーションを使用すると、既存のネットワーク設計や設定を変更することなく、既存の企業環境に新しいサービスをシームレスに導入できます。

強化された直感的な GUI により、アクセス制御とモニタリングの機能を一元化できるとともに、サポートされるさまざまなタイプのエンタープライズ ネットワークへの大規模な Bonjour サービスの展開に必要な拡張性とパフォーマンスを実現できます。

Wide Area Bonjour アプリケーションは、2 つの統合ドメインネットワークで稼働します。



- ローカルエリア SDG ドメイン - マルチキャスト DNS モード：mDNS フラッドを使用した従来型の展開モードで、レイヤ 3 境界にある Cisco Catalyst スイッチは、ローカル VLAN 間のローカルキャッシュ検出および分散型機能のサービス ディスカバリ ゲートウェイ（SDG）として機能します。Cisco DNA Center コントローラが不要のこの Bonjour ソリューション（コントローラ）では、SDG ゲートウェイスイッチが LAN およびワイヤレス ディストリビューション ブロックで単一のゲートウェイソリューションを提供します。SDG スイッチは、ローカルの Bonjour エンドポイントと通信して、サービス情報を構築および管理します。Bonjour ゲートウェイ機能は、これらのエンドポイントが標準ベースのフラッドアンドラーニング ルールに従うため、同じレイヤ 2 の有線およびワイヤレスネットワーク内の Bonjour エンドポイント間では無効です。

- ローカルエリア SDG ドメイン - ユニキャストモード：レイヤ 2 の Cisco Catalyst スイッチおよび Cisco Catalyst 9800 シリーズ ワイヤレス LAN コントローラ（WLC）では、ネットワークでの新しいユニキャストベースのサービスルーティングをサポートするために、従来の flood-n-learn に代わるサービスピアロールが導入されます。また、サービスピアスイッチと WLC は、mDNS flood-n-learn を、RFC 6762 マルチキャスト DNS 互換の有線およびワイヤレスエンドポイントとのユニキャストベースの通信に置き換えます。サービスピア ネットワーク デバイスは、Bonjour サービス情報をレイヤ 3 境界のアップストリーム IP ゲートウェイにエクスポートし、ローカル キャッシュ検出および分散型機能のサービス ディスカバリ ゲートウェイ（SDG）として機能します。Cisco DNA Center コントローラが不要のこの Bonjour ソリューション（コントローラ）では、SDG ゲートウェイスイッチが

LAN およびワイヤレス ディストリビューション ブロックで単一のゲートウェイソリューションを提供します。

- ワイドエリア SDG ドメイン：Wide Area Bonjour ドメインは、コントローラベースのソリューションです。Cisco Catalyst スイッチの Bonjour ゲートウェイの役割と責任は、SDG から SDG エージェントに拡大されています。ネットワーク全体に分散される SDG エージェントデバイスは、Wide Area Bonjour アプリケーションを実行する中央集中型 Cisco DNA Center コントローラとの軽量かつステートフルで信頼性の高い通信チャネルを確立します。SDGエージェントとコントローラ間のサービスルーティングは、TCP ポート 9991 を使用して通常の IP ネットワーク上で実行されます。SDG エージェントは、エクスポートポリシーに基づいて、ローカルで検出されたサービスをルーティングします。

機能制限

- シスコのサービス検出ゲートウェイ（SDG）と Wide Area Bonjour ゲートウェイ機能は、Cisco Catalyst スイッチおよび Cisco ISR 4000 シリーズ ルータでサポートされています。サポート対象のプラットフォーム、ソフトウェアバージョン、およびライセンスレベルの完全なリストについては、ソリューションのコンポーネント（286 ページ）を参照してください。
- Cisco IOS では、従来の方法と新しい方法でローカルの Bonjour 設定ポリシーを構築できます。従来の方法は **service-list mdns-sd** CLI に基づきますが、新しい方法は **mdns-sd gateway** に基づきます。従来の設定サポートは近い将来のリリースで廃止されるため、新しい **mdns-sd gateway** の方法を使用することを推奨します。
- 従来の方法から新しい方法の CLI に移行するには、手動で設定を変換します。
- Cisco SDG ゲートウェイの Bonjour サービスポリシーは、ローカル VLAN 間で有効です。それに加えて、特定の出力ポリシーは、コントローラにエクスポートされるサービスのタイプを制御します。同じブロードキャストドメイン上にある 2 つのエンドポイント間のレイヤ 2 マルチキャスト DNS Bonjour 通信は、ゲートウェイに対して透過的です。
- ワイヤレスネットワークでエンドツーエンドの Wide Area Bonjour ソリューションを有効にするには、Cisco WLC コントローラで mDNS スヌーピング機能を有効にしないでください。専用 Cisco Catalyst スイッチのアップストリーム IP ゲートウェイでは、ワイヤレスクライアントに対して Bonjour ゲートウェイ機能を有効にする必要があります。
- Cisco ワイヤレス LAN コントローラでは、一意のマルチキャストグループで AP マルチキャストを有効にする必要があります。AP が WLC マルチキャストグループに参加していない場合、mDNS メッセージはクライアントとゲートウェイスイッチ間で処理されません。クライアント SSID または VLAN のマルチキャストは、他のマルチキャスト アプリケーションではオプションであるため、Bonjour ソリューションでは必須ではありません。
- Cisco Catalyst 9800 WLC は、mDNS ゲートウェイとして設定できます。このモードでは、Cisco Catalyst 9800 WLC は、ワイヤレス専用ネットワーク限定の Local-Area Bonjour ゲートウェイソリューションをサポートします。Cisco Catalyst 9800 は、Wide Area Bonjour をサポートしていません。エンドツーエンドの有線およびワイヤレス Bonjour をサポートす

るには、アップストリーム Cisco Catalyst スイッチを IP および Bonjour ゲートウェイとして使用することを推奨します。

ソリューションのコンポーネント

Bonjour 向け Cisco DNA サービスソリューションは、次の主要コンポーネントから構成されるエンドツーエンド ソリューションです。

- **Cisco SDG エージェント**：Cisco Catalyst スイッチや ISR 4000 シリーズ ルータは、サービス検出ゲートウェイ（SDG）エージェントとして機能し、レイヤ2 ドメインおよび中央の Cisco DNA Center コントローラ内の Bonjour サービスエンドポイントと通信します。
- **Cisco DNA コントローラ**：Cisco DNA コントローラは、信頼できる SDG エージェントとのセキュアなチャネルを提供し、サービス管理の一元化とサービスルーティングの制御を実現します。
- **Cisco ワイヤレス LAN コントローラ**：Cisco ワイヤレス LAN コントローラ（WLC）は、ディストリビューション層ネットワークのワイヤレスクライアントとアップストリーム Bonjour ゲートウェイスイッチ間で mDNS メッセージを透過的に切り替えます。
- **エンドポイント**：Bonjour エンドポイントは、RFC 6762 に準拠する Bonjour サービスをアドバタイズまたは照会する任意のデバイスです。Bonjour エンドポイントは、LAN または WLAN に配置できます。Wide Area Bonjour アプリケーションは、RFC 6762 準拠の Bonjour サービス（Apple、Microsoft、Google、HP など）と統合できるように設計されています。

Cisco Wide Area Bonjour サービスのワークフロー

Cisco Wide Area Bonjour ソリューションは、クライアント/サーバーモデルに従います。SDG エージェントはクライアントとして機能し、Cisco DNA Center の Cisco Wide Area Bonjour アプリケーションはサーバーとして機能します。

ここでは、IP ネットワークでのサービスのアナウンスと検出のワークフローについて説明します。

ネットワークへのサービスのアナウンス

- Local Area Bonjour ドメインのエンドポイントデバイス（送信元）は、サービスのアナウンスを SDG エージェントに送信し、提供するサービスを指定します。たとえば、_airplay._tcp.local、_raop._tcp.local、_ipp._tcp.local などです。
- SDG エージェントはこれらのアナウンスをリッスンすると、設定されたローカルエリア SDG エージェントポリシーと照合します。アナウンスが設定されたポリシーと一致すると、SDG エージェントはサービスのアナウンスを受け入れ、コントローラにサービスをルーティングします。

ネットワークで使用可能なサービスの検出

- ローカルエリア SDG エージェントに接続されているエンドポイントデバイス（受信先）は、mDNS プロトコルを使用して Bonjour クエリを送信し、使用可能なサービスを検出します。
- クエリが設定されたポリシーに準拠している場合、SDG エージェントは Wide Area Bonjour コントローラを介して適切なサービスルーティングから取得したサービスで応答します。

Wide Area Bonjour 多層ポリシー

Bonjour のアナウンスとクエリを制御するためのさまざまなポリシーは、次のように分類されます。

- **ローカルエリア SDG エージェントフィルタ**：レイヤ 2 ネットワークドメインの SDG エージェントに適用されます。この双方向ポリシーは、SDG エージェントと Bonjour エンドポイント間の Bonjour アナウンスやクエリを制御します。
- **ワイドエリア SDG エージェントフィルタ**：コントローラへのエクスポート制御用に SDG エージェントに適用されます。この出力単方向ポリシーは、SDG エージェントからコントローラへのサービスルーティングを制御します。
- **Cisco Wide Area Bonjour ポリシー**：グローバルサービスの検出と配信用にコントローラに適用されます。コントローラと IP ネットワーク間のポリシーの適用は双方向です。

サポートされるプラットフォーム

サポートされるコントローラのハードウェアとソフトウェアバージョンを次の表に示します。

サポートされるコントローラ	ハードウェア	ソフトウェア バージョン
Cisco DNA Center アプライアンス	DN2-HW-APL DN2-HW-APL-L DN2-HW-APL-XL	1.3.1.0
Cisco Wide Area Bonjour アプリケーション	Cisco DNA Center アプライアンス	2.4.0.10062

サポートされる SDG エージェントのライセンスとソフトウェア要件を次の表に示します。

サポートされる **SDG** エージェント	ローカルエリア **SDG**	ワイドエリア **SDG**	最小ソフトウェア
Cisco Catalyst 9200 シリーズ スイッチ	DNA Essentials	Unsupported	17.1.1
Cisco Catalyst 9200L シリーズ スイッチ	Unsupported	Unsupported	-

サポートされる SDG エージェント	ローカルエリア SDG	ワイドエリア SDG	最小ソフトウェア
Cisco Catalyst 9300 シリーズ スイッチ	DNA Essentials	DNA Advantage	16.11.1
Cisco Catalyst 9400 シリーズ スイッチ	DNA Essentials	DNA Advantage	16.11.1
Cisco Catalyst 9500 シリーズ スイッチ	DNA Essentials	DNA Advantage	16.11.1
Cisco Catalyst 9500 シリーズ スイッチ - ハイパフォーマンス	DNA Essentials	DNA Advantage	16.11.1
Cisco Catalyst 9600 シリーズ スイッチ	DNA Essentials	DNA Advantage	16.11.1
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	DNA Essentials	Unsupported	16.11.1
Cisco 5500 シリーズ ワイヤレス コントローラ	Unsupported	Unsupported	パススルー
Cisco 8540 ワイヤレス コントローラ	Unsupported	Unsupported	パススルー
Cisco Catalyst 6800 シリーズ スイッチ	IP Base	IP サービス + DNA アドオン	15.5(1)SY4
Cisco Catalyst 4500-E シリーズ スイッチ	IP Base	IP サービス + DNA アドオン	3.11.0
Cisco Catalyst 4500-X シリーズ スイッチ	IP Base	IP サービス + DNA アドオン	3.11.0
Cisco Catalyst 3650 シリーズ スイッチ	DNA Essentials	DNA Advantage	16.11.1
Cisco Catalyst 3850 シリーズ スイッチ	DNA Essentials	DNA Advantage	16.11.1
Cisco Catalyst 2960-X シリーズ スイッチ	LAN ベース	Unsupported	15.2.6E2
Cisco Catalyst 2960-XR シリーズ スイッチ	IP Lite	Unsupported	15.2.6E2

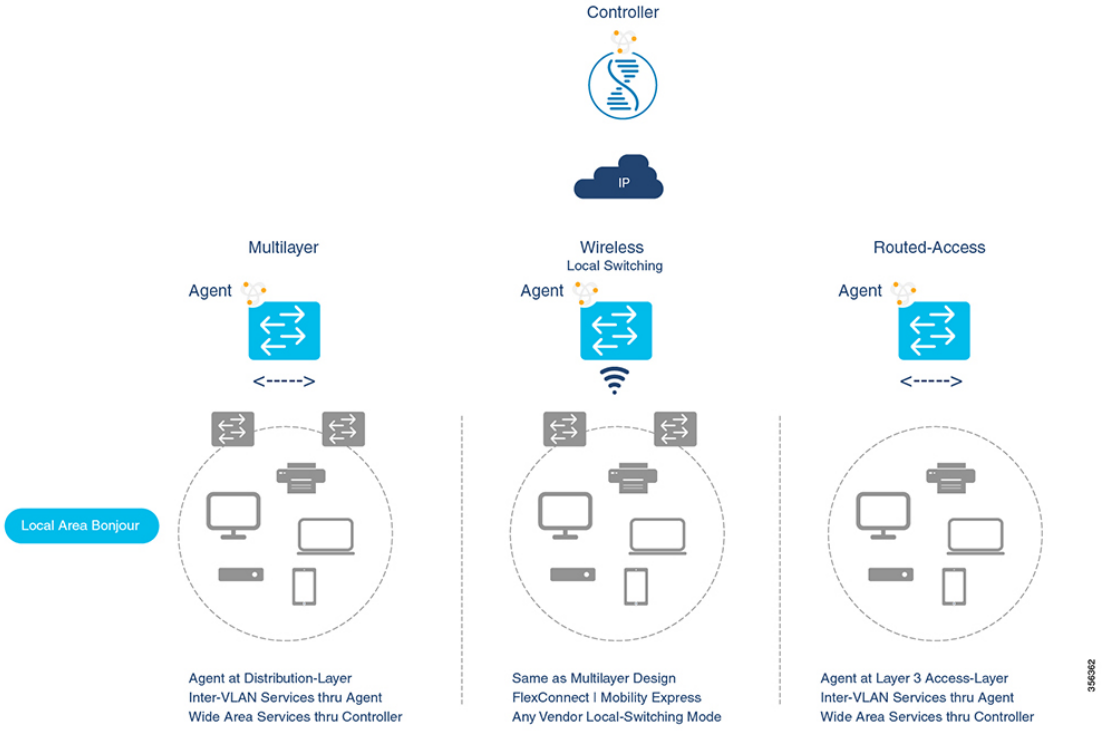
サポートされる SDG エージェント	ローカルエリア SDG	ワイドエリア SDG	最小ソフトウェア
Cisco 4000 シリーズサービス統合型ルータ（ISR）	IP Base	AppX	16.11.1

Cisco Wide Area Bonjour 対応のネットワーク設計

従来の有線およびワイヤレスネットワーク

Bonjour 向け Cisco DNA サービスは、企業で一般的に導入されているさまざまな LAN ネットワーク設計をサポートします。Bonjour ゲートウェイ機能を提供する SDG エージェントは通常、マルチレイヤネットワーク設計のディストリビューション層またはルーテッド アクセス ネットワーク設計のアクセス層に配置される可能性がある有線エンドポイントの IP ゲートウェイです。

この項で詳しく説明するトポロジを次の図に示します。



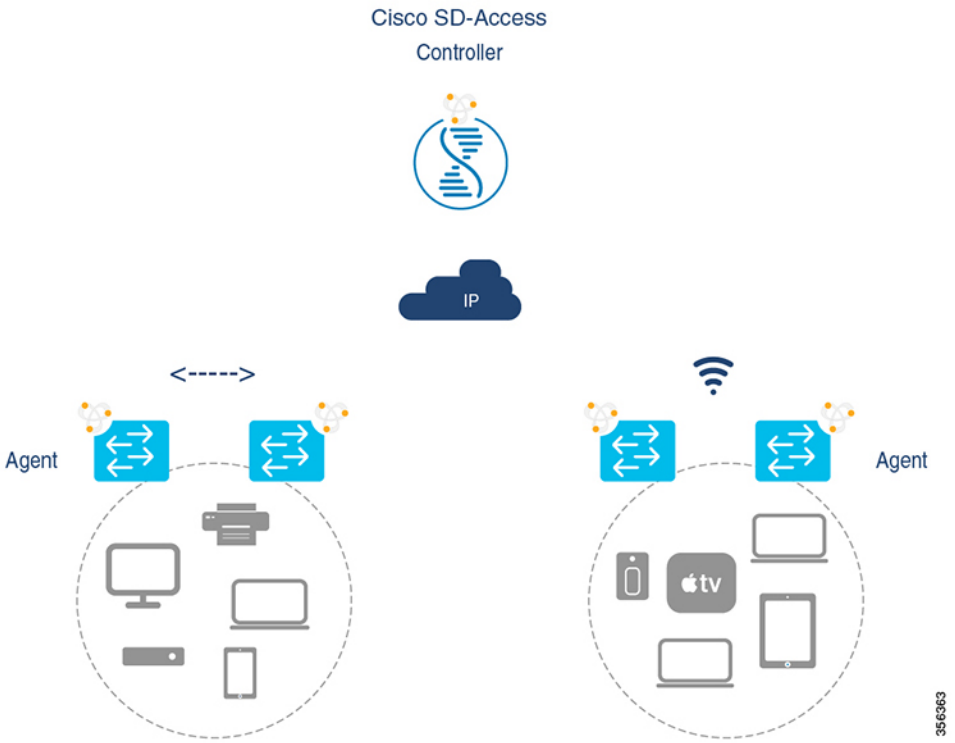
- **マルチレイヤ LAN**：この導入モードでは、レイヤ 2 アクセススイッチは、IP ゲートウェイおよび SDG エージェントとして機能するディストリビューション層システムに Bonjour サービスのトランスペアレントブリッジング機能を提供します。アクセス層とディストリビューション層の Cisco Catalyst スイッチ間にある既存のレイヤ 2 トランク設定を変更する際、追加の設定や新しい要件はありません。

- **ルーテッドアクセス**：この導入モードでは、ファーストホップスイッチは IP ゲートウェイ境界であるため、SDG エージェントのロールと組み合わせる必要があります。

Bonjour 向け Cisco DNA Service は、企業で一般的に導入されているさまざまなワイヤレス LAN ネットワーク設計もサポートします。SDG エージェントは、有線ネットワークの場合と同様に、ワイヤレスエンドポイントに一貫した Bonjour ゲートウェイ機能を提供します。一般に、ワイヤレスクライアントの IP ゲートウェイは Bonjour ゲートウェイでもあります。ただし、SDG エージェントの配置は、ワイヤレス LAN の展開モードによって異なる場合があります。

Cisco SD Access 有線および無線ネットワーク

Cisco SD-Access ネットワークでは、ファブリックエッジスイッチは、ファブリック対応の有線およびワイヤレスネットワーク向けの SDG エージェントとして設定します。仮想ネットワークや SGT ポリシーに関係する SD-Access ネットワークポリシーがある場合は、Wide Area Bonjour ポリシーと整合させる必要があります。



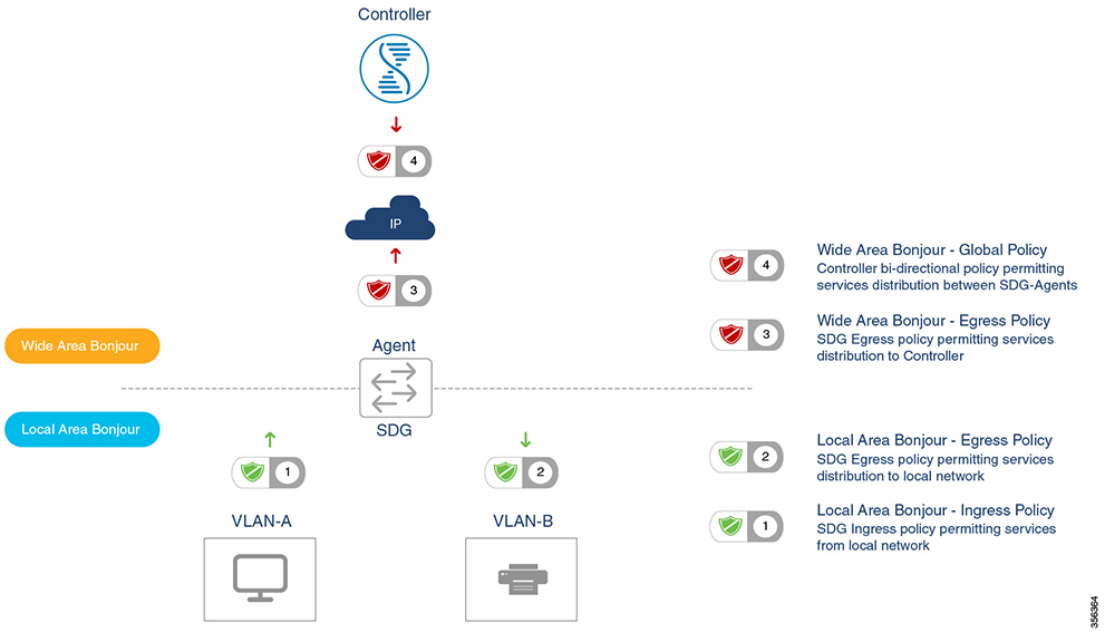
Wide Area Bonjour では、ネットワーク内の 2 つの論理コンポーネントが使用されます。

- SDG エージェント：ファブリックエッジスイッチは SDG エージェントとして設定されます。この設定は SD-Access が設定された後にのみ追加されます。
- Wide Area Bonjour コントローラ：Cisco DNA Center の Wide Area Bonjour アプリケーションはコントローラとして機能します。

SDG エージェントとコントローラ間の Wide Area Bonjour 通信は、ネットワークアンダーレイを介して確立されます。SDGエージェントは、ファブリックアンダーレイを介してエンドポイントのアナウンスやクエリをコントローラに転送します。Bonjour対応アプリケーションがサービスを検出すると、検出されたデバイスとの間で、ファブリックオーバーレイを介して直接ユニキャスト通信を確立します。この通信は、設定されたルーティングポリシーおよび SDG ポリシーに従います。

Local および Wide Area Bonjour ポリシー

Cisco Wide Area Bonjour ポリシーは、ポリシーベースの Bonjour サービスの検出と配信を 2 層ドメインで実行できるように、4 つの固有機能に分割されています。ネットワーク管理者は、有効にする必要がある Bonjour サービスのリストを特定し、要件に基づいてディスカバリ境界を設定する必要があります。境界はローカルまたはグローバルに制限できます。次の図は、SDG エージェントレベルおよび Cisco DNA-Center Wide Area Bonjour アプリケーションにおける 4 種類すべての Bonjour ポリシーの適用ポイントと方向を示しています。

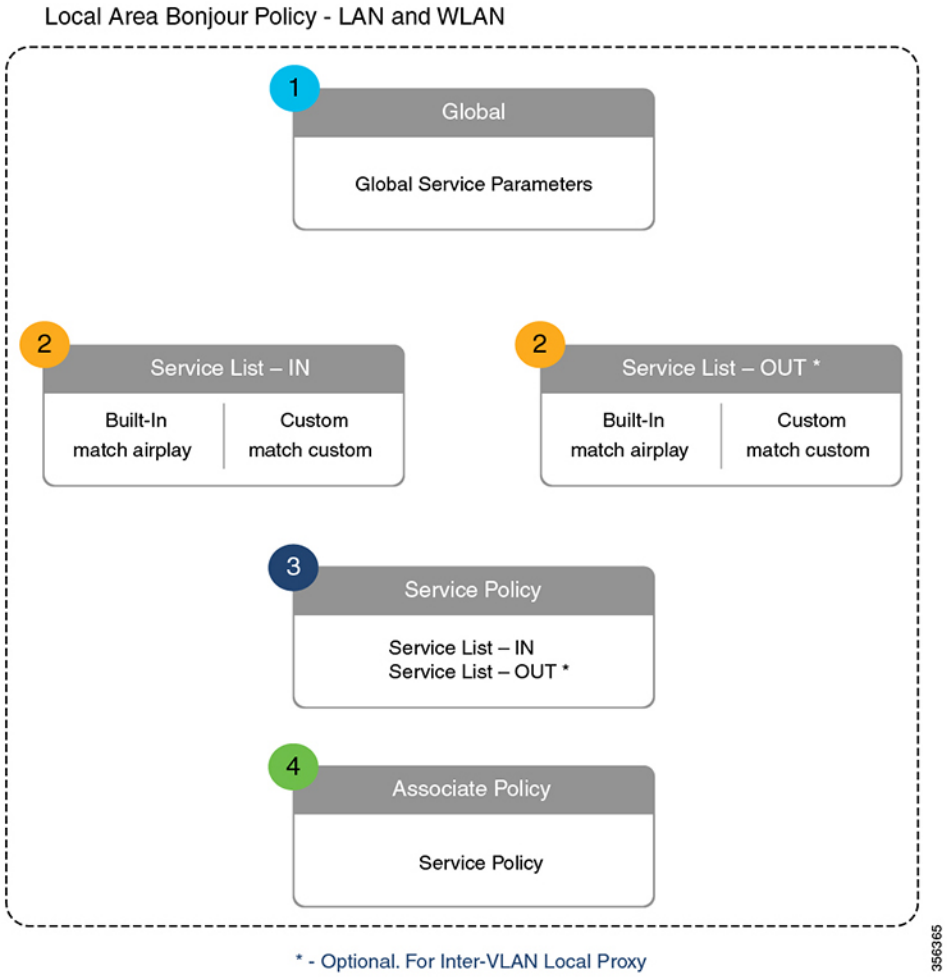


Local Area Bonjour ポリシー

Cisco IOS Bonjour ポリシー構造は、新しいコンフィギュレーション モードで大幅にシンプル化され、拡張性も備えています。サービスは、個別の mDNS PoinTeR（PTR）レコードドタイプではなく、直感的で使いやすいサービスタイプを指定して有効にできます。たとえば AirPlay を選択すると、Apple TV や同等の対応デバイスのビデオやオーディオサービスが自動的に有効になります。企業で一般的に使用されるサービスタイプの一部は、組み込みサービスタイプを使用して有効にできます。組み込みサービスタイプが制限されている場合、ネットワーク管理者はカスタムサービスタイプを作成し、ネットワークでサービス配信を有効にできます。

Local Area Bonjour ドメインのポリシー設定は必須であり、3 ステップのプロセスです。次の図は、Local Area Bonjour ポリシーを構築し、選択したローカルネットワークでゲートウェイ機能を有効にするための詳細手順を示しています。

図 *22 : Local Area Bonjour* ポリシーの階層



Local Area Bonjour ポリシーを設定するには、mDNS をグローバルに有効にします。デバイスがインターフェイスで mDNS パケットを受信できるように、インターフェイスで mDNS ゲートウェイを設定します。フィルタオプションを使用してサービスリストを作成し、そのリスト内でデバイスやインターフェイスとの間で送受信を許可するサービスを指定します。mDNS ゲートウェイをグローバルにインターフェイス上で有効にした後、**service-policy** コマンドを使用して、サービス検出情報にフィルタ（インバウンドフィルタリングまたはアウトバウンドフィルタリング）を適用できます。

組み込みサービスリスト

Cisco IOS ソフトウェアに組み込まれているサービスリストは、複数の Bonjour サービスタイプで構成できます。単一のサービスリストには、サービスプロバイダーからのサービスアナウン

スや受信側のエンドポイントからのサービスクエリを受け入れる際のデフォルトルールを設定し、複数のサービスタイプエントリを含めることができます。選択したサービスタイプに複数の Bonjour サービスタイプ（PTR）を含めると、それらの組み込み Bonjour サービスタイプのいずれかに対するアナウンスまたはクエリであれば受け入れられます。たとえば、Apple Time Capsule Data サービスタイプは、_adisk と _afpovertcp の 2 つの組み込み PTR で構成されますが、エンドポイントが _afpovertcp サービスに対してのみアナウンスまたは要求しても、SDG エージェントがアナウンスや要求を適切に分類して処理します。サービスリストは、すべての未定義の組み込みエントリやカスタムサービスエントリに対して暗黙的拒否します。

Local Area Bonjour でポリシーを作成する際に使用できる組み込み Bonjour サービスの完全なリストを次の表に示します。

表 *20 : Cisco IOS* 組み込み *Bonjour* サービスデータベース

サービス	サービス名	mDNS PTR
Apple TV	airplay	_airplay._tcp.local
AirServer ミラーリングサービス	airserver	_airserver._tcp.local _airplay._tcp.local
Apple AirTunes	airtunes	_raop._tcp.local
Amazon Fire TV	amazon-fire-tv	_amzn-wplay._tcp.local
Apple AirPrint	apple-airprint	_ipp._tcp.local _universal._sub._ipp._tcp.local
Apple TV 2	apple-continuity	_companion-link._tcp.local
Apple ファイル共有	apple-file-share	_afpovertcp._tcp.local
Apple HomeKit	apple-homekit	_hap._tcp.local _homekit._ipp.local
Apple iTunes Library	apple-itunes-library	_atc._tcp.local
Apple iTunes Music	apple-itunes-music	_daap._tcp.local
Apple iTunes Photo	apple-itunes-photo	_dpap._tcp.local
Apple KeyNote Remote Control	apple-keynote	_keynotepair._tcp.local _keynotecontrol._tcp.local
Apple Remote Desktop	apple-rdp	_net-assistant._tcp.local _afpovertcp._tcp.local
Apple Remote Event	apple-remote-events	_eppc._tcp.local

サービス	サービス名	mDNS PTR
Apple Remote Login	apple-remote-login	_sftp-ssh._tcp.local _ssh._tcp.local
Apple Screen Share	apple-screen-share	_rfb._tcp.local
Apple Time Capsule Data	apple-timecapsule	_adisk._tcp.local _afpovertcp._tcp.local
Apple Time Capsule Management	apple-timecapsule-mgmt	_airport._tcp.local
Apple MS Window ファイル共有	apple-windows-fileshare	_smb._tcp.local
Fax	fax	_fax-ipp._tcp.local
Google ChromeCast	google-chromecast	_googlecast._tcp.local
Apple HomeSharing	homesharing	_home-sharing._tcp.local
Apple iTunes データ同期	itune-wireless-devicesharing2	_apple-mobdev2._tcp.local
多機能プリンタ	multifunction-printer	_ipp._tcp.local _scanner._tcp.local _fax-ipp._tcp.local
Phillips Hue Lights	phillips-hue-lights	_hap._tcp.local
プリンタ：インターネット印刷プロトコル	printer-ipp	_ipp._tcp.local
プリンタ：SSL による IPP	printer-ipps	_ipps._tcp.local
Linux プリンタ–ラインプリンタデーモン	printer-lpd	_printer._tcp.local
プリンタソケット	printer-socket	_pdl-datastream._tcp.local
Roku メディアプレイヤー	roku	_rsp._tcp.local
Scanner	scanner	_scanner._tcp.local
Spotify 音楽サービス	spotify	_spotify-connect._tcp.local
Web サーバー	web-server	_http._tcp.local
WorkStation	workstation	_workstation._tcp.local

カスタムサービスリスト

組み込みの Bonjour データベースが特定のサービスやバンドルされたサービスタイプをサポートしていない場合、ネットワーク管理者はカスタムサービスリストを使用してサービスを設定できます。たとえば、ファイル共有の要件で、MacOS ユーザー間の Apple Filing Protocol（AFP）のサポートと、MacOS デバイスと Microsoft Windows デバイス間のサーバーメッセージブロック（SMB）ファイル転送機能のサポートが必要だとします。このような要件の場合、ネットワーク管理者は AFP（_afpovertcp._tcp.local）と SMB（_smb._tcp.local）を組み合わせたカスタムサービスリストを作成できます。

サービスリストを使用することで、単一のリストで組み込みサービス定義とカスタムサービス定義を柔軟に組み合わせることができます。カスタムサービス定義リストの数および単一サービスリストへの関連付けについての制限はありません。

ポリシーの方向

Cisco IOS の Local Area Bonjour ポリシーにより、ネットワーク管理者は同一または異なるローカルネットワークにおいて、サービスアナウンスとクエリ管理を柔軟に調整できます。サービスポリシーを入力方向または出力方向に関連付けて、両方向のサービス制御を適用できます。次のサブセクションでは、サービスポリシー設定の詳細について説明します。

入力サービスポリシー

入力サービスポリシーは必須の設定要素であり、着信 mDNS サービスアナウンスやクエリ要求の処理を許可するために使用します。入力サービスポリシーが設定されていない場合、対象の有線またはワイヤレスネットワークで Bonjour ゲートウェイ機能は有効になりません。入力サービスポリシーを使用すると、ユーザー定義のサービスタイプごとにサービスアナウンスやクエリを柔軟に許可できます。つまり、AirPlay サービスではアナウンスとクエリ要求を許可し、プリンタサービスではクエリ要求のみを有効にできます。

出力サービスポリシー

出力サービスポリシーはオプション設定であり、次の 2 つの条件下では必要ありません。

- 出力サービスポリシーは、想定される Bonjour エンドポイントがサービスプロバイダーのみのローカル VLAN には適用されません。つまり、サービス VLAN ネットワークには、IT マネージド サービス プロバイダー エンドポイント（Apple TV、プリンタなど）のみ含まれます。これらのポイントは、ネットワーク内の他のサービスタイプを照会しません。
- 有線またはワイヤレスのユーザーは Cisco DNA-Center で Wide Area Bonjour サービスからのサービスのみを受信する必要があります。同じ SDG エージェントに接続されている他の Bonjour エンドポイントからのサービスは受信しません。出力サービスポリシーの設定は、SDG エージェントが、ローカルに検出された Bonjour サービス情報をある VLAN から別の VLAN に配信する必要がある場合にのみ必要です。たとえば、VLAN-B の受信側エンドポイントで VLAN-A からのプリンタ情報を検出する場合、SDG エージェントは入力サービスポリシーに基づいて、VLAN-A から AirPrint 対応プリンタを検出してキャッシュに保存します。このとき、SDG エージェントには、両方の VLAN で AirPrint サービスを許可する入出力サービスポリシーが必要です。

条件付き出力サービスポリシー

ネットワーク管理者は、オプションで出力サービスポリシーをカスタマイズして、特定のVLANネットワークからの条件付きサービス応答を有効にできます。たとえば、SDGエージェントは入力サービスポリシーに基づいて、 VLAN-A および VLAN-C ネットワークから AirPrint 対応プリンタを検出できます。条件付き Local Area Bonjour の出力サービスポリシールールを使用すると、ネットワーク管理者は VLAN-A から検出されたプリンタ情報を VLAN-B ネットワーク内の受信者に配信することを制限したり、VLAN-Cプリンタを自動的にフィルタリングしたりできます。条件付き出力サービスポリシーのサポートはオプション設定です。また、出力方向サービスポリシーにのみ適用できます。

サービスステータスタイマーの管理

Bonjour サービス プロバイダー エンドポイントは、mDNS レコードと各レコードの存続可能時間（TTL）サービスタイマーを組み合わせて、ネットワーク内の 1 つ以上のサービスをアナウンスできます。TTL 値は、ネットワーク内のエンドポイントの可用性と有用性を保証します。SDG エージェントは、Local Area Bonjour ドメイン内の TTL などのイベントに基づいて、ローカルの最新情報を取り込み、コントローラのグローバルサービスを更新します。ネットワーク管理者は、サービスプロバイダー エンドポイントの検出を許可するサービスステータスタイマーを設定する必要があります。

Wide Area Bonjour ポリシー

ローカルサービスのルーティングを制御し、Cisco DNA-Center からのリモートサービスを検出するためには、コントローラにバインドされた Wide Area Bonjour サービスのエクスポートポリシーが SDG エージェントで必須になります。Cisco DNA-Center および SDG エージェントによって信頼できる通信チャネルが確立されるため、Wide Area Bonjour アプリケーションからのリモートサービス応答は SDG エージェントで暗黙的に許可されます。したがって、Wide Area Bonjour ポリシーは単方向であり、コントローラへの出力サービスポリシーのみが必要です。

Wide Area Bonjour ポリシーの階層と構造については、「Local Area Bonjour ポリシーの階層」で説明されているとおりです。次のサブセクションでは、Cisco DNA-Center の Wide Area Bonjour アプリケーションとの正常な通信を実現するためのポリシーを構築して適用する際に参考となる設定方法を順を追って説明します。

サービスリスト：組み込みおよびカスタム

ネットワーク管理者は Wide Area Bonjour ドメインに対応して、新しいコントローラにバインドする出力サービスリストを作成する必要があります。最も一般的なネットワーク展開モデルでは、Wide Area Bonjour サービスリストに Local Area Bonjour と同じサービスタイプを含めて、両方のドメイン間で共通のサービスを実装します。要件に基づいて、特定のサービスをローカルエリアに制限し、ワイドエリアドメインにルーティングされないようにできます。デフォルトでは、サービス許可リストのエントリのみが許可され、残りは暗黙的な拒否ルールでドロップされます。

入力方向ポリシー

Wide Area Bonjour ドメインの入力サービスポリシーは必須ではなく、コントローラに関連付けることはできません。

出力方向ポリシー

説明したように、ローカルエリアとワイドエリアの間で Bonjour ポリシーの構造に一貫性はありますが、エンフォースメントポイントは異なります。Wide Area Bonjour ドメインに個別のサービスリストとサービスポリシーを設定することを推奨します。各ドメインに固有のポリシーセットを作成するのに役立ちます。

条件付き出力サービスリスト

Wide Area Bonjour 出力サービスリストの設定をカスタマイズすると、Cisco DNA-Center にサービスまたはクエリ要求を条件付きでルーティングできます。この代替コンフィギュレーションを使用すると、ネットワーク管理者はシステム全体からではなく、特定のローカル送信元VLANネットワークからサービスのルーティングや Wide Area Bonjour ドメイン内の要求照会を実行できます。

Wide Area Bonjour サービスステータスタイマーの管理

Cisco DNA-Center では、ネットワーク全体に広く分散された SDG エージェントからのサービス情報が一元管理されます。コントローラの拡張性とパフォーマンスを維持するために、サービスルーティング情報が各 SDG エージェント ネットワーク デバイスから定期的に送信され、同期されます。システムとネットワークのパフォーマンスを保護するために、スケジューラベースでサービス情報が交換され、信頼性が高く洗練された方法で Wide Area Bonjour ドメイン全体で Bonjour サービスを検出および配信できます。

ほとんどの大規模ネットワーク環境で SDG エージェントのデフォルト Bonjour サービスタイマーはあらかじめ微調整されており、これ以上の調整は必要ありません。インターバルタイマーの値をデフォルトのままにして、ユーザーエクスペリエンスの問題が発生した場合にのみ調整することを推奨します。また、パラメータを変更する場合には、拡張性やパフォーマンスに影響を与えないかを考慮してください。

Local Area Bonjour および Wide Area Bonjour ドメインの設定

有線ネットワーク向け Local Area Bonjour ドメインの設定

デバイスでの mDNS ゲートウェイの有効化

デバイスで mDNS を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mdns-sd gateway**

4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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	**mdns-sd gateway** 例： `Device(config)# mdns-sd gateway`	デバイスで mDNS を有効にし、mDNS ゲートウェイ コンフィギュレーション モードを開始します。 mDNSゲートウェイ コンフィギュレーション モードで次のコマンドを入力して、それぞれの機能を有効にします。 • **air-print-helper** ：iPAD などの IOS デバイスが Bonjour 対応の旧式のプリンタを検出して使用できるようにします。 • **cache-memory-max** ：キャッシュのメモリの割合を設定します • **ingress-client** ：入力クライアントのパケット チューナーを設定します • **rate-limit** ：着信 mDNS パケットのレート制限を有効にします • **service-announcement-count** ：最大アドバタイズメント数を設定します • **service-announcement-timer** ：アドバタイズメント アナウンス タイマーの周期を設定します。 • **service-query-count** ：最大クエリ数を設定します • **service-query-timer** ：クエリ転送タイマーの周期を設定します • **service-type-enumeration** ：サービスの列挙数を設定します

	コマンドまたはアクション	目的
		（注） 一般的な展開の場合は、**cache-memory-max**、**ingress-client**、**rate-limit**、**service-announcement-count**、**service-announcement-timer**、**service-query-count**、**service-query-timer**、および **service-type-enumeration** コマンドのパラメータのデフォルト値それぞれを保持できます。必要に応じて、特定の展開の場合は異なる値を設定します。
ステップ 4	**exit** 例： `Device(config-mdns-sd)# exit`	mDNS ゲートウェイ コンフィギュレーション モードを終了します。

カスタムサービス定義の作成

サービス定義は、1 つ以上の mDNS サービスタイプまたは PTR リソースレコード名に管理者フレンドリ名を提供する構造体です。デフォルトでは、いくつかの組み込みサービス定義が事前に定義されており、管理者が使用できるようになっています。組み込みのサービス定義に加えて、管理者はカスタムサービス定義を定義することもできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **mdns-sd service-definition** *service-definition-name*
4. **service-type** *string*
5. カスタムサービス定義で複数のサービスタイプを設定するには、ステップ 4 を繰り返します。
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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。

	コマンドまたはアクション	目的
ステップ 3	**mdns-sd service-definition** *service-definition-name* 例： `Device(config)# mdns-sd service-definition CUSTOM1`	mDNS サービス定義を設定します。 （注） 作成されたカスタムサービス定義はすべて、プライマリサービスリストに追加されます。プライマリサービスリストは、カスタムおよび組み込みのサービス定義のリストで構成されます。
ステップ 4	**service-type** *string* 例： `Device(config-mdns-ser-def)# service-type _custom1._tcp.local`	mDNS サービスタイプを設定します。
ステップ 5	カスタムサービス定義で複数のサービスタイプを設定するには、ステップ 4 を繰り返します。	
ステップ 6	**exit** 例： `Device(config-mdns-ser-def)# exit`	mDNS サービス定義コンフィギュレーション モードを終了します。

サービスリストの作成

mDNS サービスリストは、サービス定義の集合です。サービスリストを作成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mdns-sd service-list** *service-list-name* {**in** | **out**}
4. **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}]
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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。

	コマンドまたはアクション	目的
ステップ 3	**mdns-sd service-list** *service-list-name* {**in** | **out**} 例： `Device(config)# mdns-sd service-list VLAN100-list in`	mDNS サービスリストを設定します。
ステップ 4	**match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] 例： `Device(config-mdns-sl-in)# match PRINTER message-type announcement`	サービスをメッセージタイプと照合します。ここで、service-definition-name は、airplay、airserver、airtunes などのサービスの名前を指します。 （注） サービスを追加するには、サービス名がプライマリサービスリストに含まれている必要があります。 mDNS サービスリストが IN に設定されている場合、適用可能なコマンド構文は **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] です。 mDNS サービスリストが OFF に設定されている場合、適用可能なコマンド構文は **match** *service-definition-name* です。
ステップ 5	**exit** 例： `Device(config-mdns-sl-in)# exit`	mDNS サービスリストコンフィギュレーションモードを終了します。

サービスポリシーの作成

インターフェイスに適用するサービスポリシーでは、許可する Bonjour サービスアナウンスメント、あるいは入力方向や出力方向で処理する特定のサービスタイプのクエリを指定します。このため、サービスポリシーでは2つのサービスリストを定義します。入力方向と出力方向に 1 つずつです。Local Area Bonjour ドメインでは、同じサービスポリシーを 1 つ以上の Bonjour クライアント VLAN に割り当てることができます。ただし、VLAN ごとにサービスポリシーが異なる場合があります。

サービスリストを使用してサービスポリシーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mdns-sd service-policy** *service-policy-name*
4. **service-list** *service-list-name* {**in** | **out**}
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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	**mdns-sd service-policy** *service-policy-name* 例： `Device(config)# mdns-sd service-policy mdns-policy1`	mDNS サービスポリシーを設定します。

ステップ 4	**service-list** *service-list-name* {**in** | **out**}
	例：
	`Device(config-mdns-ser-pol)# service-list VLAN100-list in`
	`Device(config-mdns-ser-pol)# service-list VLAN300-list out`
		入力方向と出力方向のサービスリストを設定します。

ステップ 5	**exit** 例： `Device(config-mdns-ser-pol)# exit`	mDNS サービス ポリシー コンフィギュレーション モードを終了します。

インターフェイスへのサービスポリシーの関連付け

デバイスで mDNS を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-name*
4. **mdns-sd gateway**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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	**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	**interface** *interface-name* 例： `Device(config)# interface Vlan 601`	インターフェイスDNSコンフィギュレーションモードを開始し、インターフェイス コンフィギュレーションをイネーブルにします。
ステップ 4	**mdns-sd gateway** 例： `Device(config-if)# mdns-sd gateway`	インターフェイスでmDNSゲートウェイを設定します。 インターフェイスの mDNSゲートウェイ コンフィギュレーションモードで次のコマンドを入力して、それぞれの機能を有効にします。 • **active-query** ：SDG エージェントが、接続中の Bonjour クライアントサービスのアクティブステータスを更新する時間間隔を設定します。タイマー値の範囲は 60 ー 120 秒です。 （注） 接続中の Bonjour クライアントから Bonjour サービスのアナウンスメントを受け入れるように VLAN の Bonjour ポリシーが設定されている場合に限り、この設定は必須です。Bonjour クエリのみを受け入れ、Bonjour サービスのアナウンスメントを受け入れないように VLAN が設定されている場合、この設定は任意です。 • **service-instance-suffix**（任意）：コントローラに転送されるアナウンス済みサービス名にサービスインスタンスのサフィックスを追加します。 • **service-mdns-query**［**ptr** | **all**］：指定したクエリタイプのmDNSクエリ要求メッセージ処理を設定します。 キーワードを指定せずに **service-mdns-query** コマンドを使用すると、すべての Bonjour クエリタイプ（PTR、SRV、TXT）がデフォルトで処理されます。**service-mdns-query ptr** コマンドを使用することを推奨します。

	コマンドまたはアクション	目的
		• **service-policy** *policy-name*：指定したサービスポリシーを VLAN に割り当てます。VLAN で送受信される Bonjour アナウンスとクエリは、サービスポリシーの設定に従って制御されます。すべての VLAN でこの設定は必須です。 （注） サービスポリシーは、インターフェイスレベルでのみ割り当てることができます。 • **transport**［**all** | **ipv4** | **ipv6**］（任意）：BCP パラメータを設定します。 ネットワークで Bonjour クライアントが IPv6 アナウンスとクエリのみを送信する場合を除き、**transport ipv4** コマンドを使用することを推奨します。
ステップ 5	**exit** 例： `Device(config-if-mdns-sd)# exit`	mDNS ゲートウェイ コンフィギュレーション モードを終了します。

ワイヤレスネットワーク向け Local Area Bonjour ドメインの設定

ワイヤレスネットワークの SDG エージェントとして機能するスイッチで、Local Area Bonjour を設定するには、有線ネットワークの SDG エージェントとして機能するスイッチで Local Area Bonjour を設定する場合と同じ一連の手順を実行します。

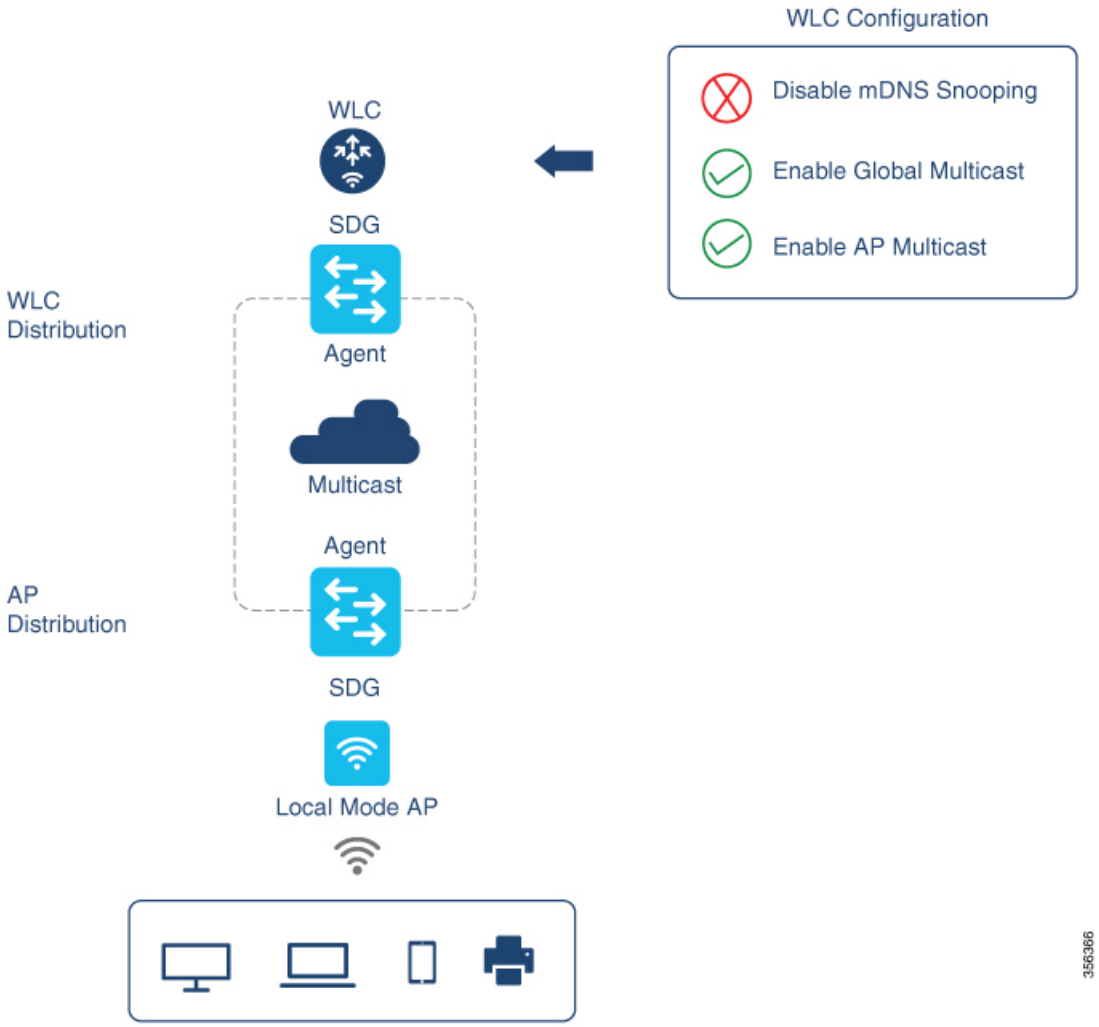
Bonjour プロトコルは、サービスアナウンスメントおよびクエリで動作します。各クエリやアドバタイズメントは、Bonjour マルチキャスト アドレス ipv4 224.0.0.251（ipv6 FF02::FB）に送信されます。このプロトコルは、UDP ポート 5353 で mDNS を使用します。

Bonjour プロトコルが使用するアドレスはリンクローカル マルチキャスト アドレスであるため、ローカル L2 ネットワークにのみ転送されます。マルチキャスト DNS は、クライアントが同じ L2 ドメインに属している必要があるサービスを検出できるように、L2 ドメインに制限されますが、大規模な導入や企業では常にこのことが可能になるとは限りません。

この問題に対処するため、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは Bonjour ゲートウェイとして動作します。これにより、コントローラは Bonjour サービスをリッスンし、ソースまたはホストからの Bonjour アドバタイズメント（AirPlay、AirPrint など）をキャッシュします。たとえば Apple TV は、Bonjour クライアントがサービスを依頼または要求したときに、それらに応答します。このようにして、異なるサブネットのソースとクライアントを使用できます。

デフォルトでは、mDNS ゲートウェイはコントローラで無効になっています。mDNS ゲートウェイ機能を有効にするには、CLI または Web UI を使用して mDNS ゲートウェイを明示的に設定する必要があります。

次の図は、SDG エージェントスイッチとワイヤレスエンドポイント間でシームレスな通信を確立するための前提条件となるワイヤレスネットワークの設定を示しています。



Cisco WLC およびアクセスポイントは、デフォルトで、ワイヤレス ネットワーク インフラストラクチャと有線ネットワーク インフラストラクチャ間でレイヤ 2 とレイヤ 3 のマルチキャストフレームを転送しません。AP マルチキャストを使用してステートフル機能を有効にすると、転送が実行されます。ネットワーク管理者は、マルチキャストをグローバルに有効にし、ネットワークでアドバタイズする一意のマルチキャストグループを設定する必要があります。このマルチキャストグループは、Cisco アクセスポイントにおいてマルチキャスト オーバー マルチキャスト（MCMC）機能を LAN ネットワーク全体で有効にする場合にのみ必要です。Bonjour ソリューションでは、ワイヤレスクライアント VLAN のマルチキャスト要件はありません。したがって、これはオプションであり、他のレイヤ 3 マルチキャストアプリケーションにのみ適用されます。

コアネットワークではマルチキャストルーティングを適切に設定し、APがWLCマルチキャストグループに加入できるようにする必要があります。マルチキャスト設定は、CiscoWLC管理VLANおよびそれぞれのディストリビューション層スイッチのCiscoアクセスポイントで有効にする必要があります。

デバイスでの mDNS ゲートウェイの有効化

デバイスで mDNS を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mdns-sd gateway**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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	**mdns-sd gateway** 例： `Device(config)# mdns-sd gateway`	デバイスでmDNSを有効にし、mDNSゲートウェイコンフィギュレーション モードを開始します。 mDNSゲートウェイ コンフィギュレーションモードで次のコマンドを入力して、それぞれの機能を有効にします。 • **air-print-helper** ：iPAD などの IOS デバイスが Bonjour 対応の旧式のプリンタを検出して使用できるようにします。 • **cache-memory-max** ：キャッシュのメモリの割合を設定します • **ingress-client** ：入力クライアントのパケットチューナーを設定します • **rate-limit** ：着信 mDNS パケットのレート制限を有効にします

	コマンドまたはアクション	目的
		• **service-announcement-count** ：最大アドバタイズメント数を設定します • **service-announcement-timer** ：アドバタイズメント アナウンス タイマーの周期を設定します。 • **service-query-count** ：最大クエリ数を設定します • **service-query-timer** ：クエリ転送タイマーの周期を設定します • **service-type-enumeration** ：サービスの列挙数を設定します （注） 一般的な展開の場合は、**cache-memory-max**、**ingress-client**、**rate-limit**、**service-announcement-count**、**service-announcement-timer**、**service-query-count**、**service-query-timer**、および **service-type-enumeration** コマンドのパラメータのデフォルト値それぞれを保持できます。必要に応じて、特定の展開の場合は異なる値を設定します。
ステップ 4	**exit** 例： `Device(config-mdns-sd)# exit`	mDNS ゲートウェイ コンフィギュレーション モードを終了します。

カスタムサービス定義の作成

サービス定義は、1 つ以上の mDNS サービスタイプまたは PTR リソースレコード名に管理者フレンドリ名を提供する構造体です。デフォルトでは、いくつかの組み込みサービス定義が事前に定義されており、管理者が使用できるようになっています。組み込みのサービス定義に加えて、管理者はカスタムサービス定義を定義することもできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **mdns-sd service-definition** *service-definition-name*
4. **service-type** *string*
5. カスタムサービス定義で複数のサービスタイプを設定するには、ステップ 4 を繰り返します。

6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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	**mdns-sd service-definition** *service-definition-name* 例： `Device(config)# mdns-sd service-definition CUSTOM1`	mDNS サービス定義を設定します。 （注） 作成されたカスタムサービス定義はすべて、プライマリサービスリストに追加されます。プライマリサービスリストは、カスタムおよび組み込みのサービス定義のリストで構成されます。
ステップ 4	**service-type** *string* 例： `Device(config-mdns-ser-def)# service-type _custom1._tcp.local`	mDNS サービスタイプを設定します。
ステップ 5	カスタムサービス定義で複数のサービスタイプを設定するには、ステップ 4 を繰り返します。	
ステップ 6	**exit** 例： `Device(config-mdns-ser-def)# exit`	mDNS サービス定義コンフィギュレーション モードを終了します。

サービスリストの作成

mDNS サービスリストは、サービス定義の集合です。サービスリストを作成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mdns-sd service-list** *service-list-name* {**in** | **out**}
4. **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}]
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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	**mdns-sd service-list** *service-list-name* {**in** | **out**} 例： `Device(config)# mdns-sd service-list VLAN100-list in`	mDNS サービスリストを設定します。
ステップ 4	**match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] 例： `Device(config-mdns-sl-in)# match PRINTER message-type announcement`	サービスをメッセージタイプと照合します。ここで、service-definition-name は、airplay、airserver、airtunes などのサービスの名前を指します。 （注） サービスを追加するには、サービス名がプライマリサービスリストに含まれている必要があります。 mDNS サービスリストが IN に設定されている場合、適用可能なコマンド構文は **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] です。 mDNS サービスリストが OFF に設定されている場合、適用可能なコマンド構文は **match** *service-definition-name* です。
ステップ 5	**exit** 例： `Device(config-mdns-sl-in)# exit`	mDNS サービスリストコンフィギュレーションモードを終了します。

サービスポリシーの作成

インターフェイスに適用するサービスポリシーでは、許可する Bonjour サービスアナウンスメント、あるいは入力方向や出力方向で処理する特定のサービスタイプのクエリを指定します。このため、サービスポリシーでは2つのサービスリストを定義します。入力方向と出力方向に 1 つずつです。Local Area Bonjour ドメインでは、同じサービスポリシーを 1 つ以上の Bonjour クライアント VLAN に割り当てることができます。ただし、VLAN ごとにサービスポリシーが異なる場合があります。

サービスリストを使用してサービスポリシーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mdns-sd service-policy** *service-policy-name*
4. **service-list** *service-list-name* {**in** | **out**}
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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	**mdns-sd service-policy** *service-policy-name* 例： `Device(config)# mdns-sd service-policy mdns-policy1`	mDNS サービスポリシーを設定します。

ステップ 4	**service-list** *service-list-name* {**in**	**out**}
		例：
		`Device(config-mdns-ser-pol)# service-list VLAN100-list in`
		`Device(config-mdns-ser-pol)# service-list VLAN300-list out`
			入力方向と出力方向のサービスリストを設定します。

ステップ 5	**exit** 例： `Device(config-mdns-ser-pol)# exit`	mDNS サービス ポリシー コンフィギュレーション モードを終了します。

サービスポリシーとワイヤレス プロファイル ポリシーの関連付け

デフォルトの mDNS サービスポリシーは、ワイヤレス プロファイル ポリシーが作成された時点ですでに接続されています。次の手順を使用して、デフォルトの mDNS サービスポリシーを目的のサービスポリシーに上書きできます。

手順の概要

1. **enable**

2. **configure terminal**
3. **wireless profile policy** *profile-policy-name*
4. **mdns-sd service-policy** *custom-mdns-service-policy*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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	**wireless profile policy** *profile-policy-name* 例： `Device(config)# wireless profile policy default-policy-profile`	ワイヤレス プロファイル ポリシーを設定します。
ステップ 4	**mdns-sd service-policy** *custom-mdns-service-policy* 例： `Device(config-wireless-policy)# mdns-sd service-policy custom-mdns-service-policy`	mDNS サービスポリシーをワイヤレスプロファイルポリシーに関連付けます。 デフォルトの mDNS サービスポリシー名は **default-mdns-service-policy** です。
ステップ 5	**exit** 例： `Device(config-wireless-policy)# exit`	ワイヤレスプロファイルポリシーコンフィギュレーション モードを終了します。

Wide Area Bonjour ドメインの設定

Wide Area Bonjour ドメインの設定では、Cisco DNA Center で実行されている Wide Area Bonjour アプリケーションであるコントローラのパラメータと、SDGエージェントからコントローラにエクスポートする必要があるサービスタイプを指定します。Wide Area Bonjour ドメインの設定では、Local Area Bonjourの場合と同様に、サービスリストとサービスポリシーを作成します。ただし、SDG エージェントからコントローラへの出力ポリシーのみが適用されます。

デバイスでの mDNS ゲートウェイの有効化

デバイスで mDNS を設定するには、次の手順を実行します。

手順の概要

1. **enable**

2. **configure terminal**
3. **mdns-sd gateway**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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	**mdns-sd gateway** 例： `Device(config)# mdns-sd gateway`	デバイスで mDNS を有効にし、mDNS ゲートウェイ コンフィギュレーション モードを開始します。 mDNSゲートウェイ コンフィギュレーション モードで次のコマンドを入力して、それぞれの機能を有効にします。 • **air-print-helper** ：iPAD などの IOS デバイスが Bonjour 対応の旧式のプリンタを検出して使用できるようにします。 • **cache-memory-max** ：キャッシュのメモリの割合を設定します • **ingress-client** ：入力クライアントのパケット チューナーを設定します • **rate-limit** ：着信 mDNS パケットのレート制限を有効にします • **service-announcement-count** ：最大アドバタイズメント数を設定します • **service-announcement-timer** ：アドバタイズメント アナウンス タイマーの周期を設定します。 • **service-query-count** ：最大クエリ数を設定します • **service-query-timer** ：クエリ転送タイマーの周期を設定します • **service-type-enumeration** ：サービスの列挙数を設定します

	コマンドまたはアクション	目的
		（注） 一般的な展開の場合は、**cache-memory-max**、**ingress-client**、**rate-limit**、**service-announcement-count**、**service-announcement-timer**、**service-query-count**、**service-query-timer**、および **service-type-enumeration** コマンドのパラメータのデフォルト値それぞれを保持できます。必要に応じて、特定の展開の場合は異なる値を設定します。
ステップ 4	**exit** 例： `Device(config-mdns-sd)# exit`	mDNS ゲートウェイ コンフィギュレーション モードを終了します。

カスタムサービス定義の作成

サービス定義は、1 つ以上の mDNS サービスタイプまたは PTR リソースレコード名に管理者フレンドリ名を提供する構造体です。デフォルトでは、いくつかの組み込みサービス定義が事前に定義されており、管理者が使用できるようになっています。組み込みのサービス定義に加えて、管理者はカスタムサービス定義を定義することもできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **mdns-sd service-definition** *service-definition-name*
4. **service-type** *string*
5. カスタムサービス定義で複数のサービスタイプを設定するには、ステップ 4 を繰り返します。
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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。

	コマンドまたはアクション	目的
ステップ 3	**mdns-sd service-definition** *service-definition-name* 例： `Device(config)# mdns-sd service-definition CUSTOM1`	mDNS サービス定義を設定します。 （注） 作成されたカスタムサービス定義はすべて、プライマリサービスリストに追加されます。プライマリサービスリストは、カスタムおよび組み込みのサービス定義のリストで構成されます。
ステップ 4	**service-type** *string* 例： `Device(config-mdns-ser-def)# service-type _custom1._tcp.local`	mDNS サービスタイプを設定します。
ステップ 5	カスタムサービス定義で複数のサービスタイプを設定するには、ステップ 4 を繰り返します。	
ステップ 6	**exit** 例： `Device(config-mdns-ser-def)# exit`	mDNS サービス定義コンフィギュレーション モードを終了します。

サービスリストの作成

mDNS サービスリストは、サービス定義の集合です。サービスリストを作成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mdns-sd service-list** *service-list-name* {**in** | **out**}
4. **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}]
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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。

	コマンドまたはアクション	目的
ステップ 3	**mdns-sd service-list** *service-list-name* {**in** | **out**} 例： `Device(config)# mdns-sd service-list VLAN100-list in`	mDNS サービスリストを設定します。
ステップ 4	**match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] 例： `Device(config-mdns-sl-in)# match PRINTER message-type announcement`	サービスをメッセージタイプと照合します。ここで、service-definition-name は、airplay、airserver、airtunes などのサービスの名前を指します。 （注） サービスを追加するには、サービス名がプライマリサービスリストに含まれている必要があります。 mDNS サービスリストが IN に設定されている場合、適用可能なコマンド構文は **match** *service-definition-name* [**message-type** {**any** | **announcement** | **query**}] です。 mDNS サービスリストが OFF に設定されている場合、適用可能なコマンド構文は **match** *service-definition-name* です。
ステップ 5	**exit** 例： `Device(config-mdns-sl-in)# exit`	mDNS サービスリストコンフィギュレーションモードを終了します。

サービスポリシーの作成

インターフェイスに適用するサービスポリシーでは、許可する Bonjour サービスアナウンスメント、あるいは入力方向や出力方向で処理する特定のサービスタイプのクエリを指定します。このため、サービスポリシーでは2つのサービスリストを定義します。入力方向と出力方向に 1 つずつです。Local Area Bonjour ドメインでは、同じサービスポリシーを 1 つ以上の Bonjour クライアント VLAN に割り当てることができます。ただし、VLAN ごとにサービスポリシーが異なる場合があります。

サービスリストを使用してサービスポリシーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mdns-sd service-policy** *service-policy-name*
4. **service-list** *service-list-name* {**in** | **out**}
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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	**mdns-sd service-policy** *service-policy-name* 例： `Device(config)# mdns-sd service-policy mdns-policy1`	mDNS サービスポリシーを設定します。

ステップ 4	**service-list** *service-list-name* {**in** | **out**}
	例：
	`Device(config-mdns-ser-pol)# service-list VLAN100-list in`
	`Device(config-mdns-ser-pol)# service-list VLAN300-list out`
		入力方向と出力方向のサービスリストを設定します。

ステップ 5	**exit** 例： `Device(config-mdns-ser-pol)# exit`	mDNS サービス ポリシー コンフィギュレーション モードを終了します。

サービスポリシーと Wide Area Bonjour ドメインの関連付け

Wide Area Bonjour では、サービスポリシーはグローバルに設定します。Local Area Bonjour の場合のように、VLAN には関連付けません。

サービスポリシーをグローバルに設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **service-export mdns-sd controller** *controller name*
4. **controller-address** *ipv4-address*
5. **controller-port** *port-number*
6. **controller-source-interface** *interface-name*
7. **controller-service-policy** *service-policy-name* **out**
8. **exit**
9. **mdns-sd gateway**
10. **ingress-client query-suppression enable**

11. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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	**service-export mdns-sd controller** *controller name* 例： `Device(config)# service-export mdns-sd controller DNAC-BONJOUR-CONTROLLER`	コントローラ名を指定し、サービスエクスポート モードを開始します。
ステップ 4	**controller-address** *ipv4-address* 例： `Device(config-mdns-sd-se)# controller-address 199.245.1.7`	コントローラのアドレスを指定します。
ステップ 5	**controller-port** *port-number* 例： `Device(config-mdns-sd-se)# controller-port 9991`	コントローラが待機しているポート番号を指定します。
ステップ 6	**controller-source-interface** *interface-name* 例： `Device(config-mdns-sd-se)# controller-source-interface Loopback0`	コントローラの送信元インターフェイスを指定します。
ステップ 7	**controller-service-policy** *service-policy-name* **out** 例： `Device(config-mdns-sd-se)# controller-service-policy policy1 OUT`	コントローラで使用するサービスポリシーを指定します。 （注） Wide Area Bonjour には、出力方向のポリシーのみが適用されます。
ステップ 8	**exit** 例： `Device(config-mdns-sd)# exit`	コントローラサービスのエクスポート コンフィギュレーション モードを終了します。
ステップ 9	**mdns-sd gateway** 例： `Device(config)# mdns-sd gateway`	mDNS ゲートウェイ 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 10	**ingress-client query-suppression enable** 例： `Device(config-mdns-sd)# ingress-client query-suppression enable`	拡張性とパフォーマンスを向上させるため、入力クエリの抑制を有効にします。
ステップ 11	**exit** 例： `Device(config-mdns-sd)# exit`	mDNS ゲートウェイ コンフィギュレーション モードを終了します。

Local Area Bonjour および Wide Area Bonjour ドメインの確認

サービス検出ゲートウェイの確認

次に、**show mdns-sd service-list** *service-list-name* {**in** | **out**} コマンドの出力例を示します。

```
Name   Direction  Service  Message-Type    Source
================================================================================
VLAN100-list        In        Printer      Announcement       -
         In        Airplay  Query       -
         In        CUSTOM1        Any    -
VLAN300-list  Out  Printer      Announcement     Vl200
```

次に、**show mdns-sd service-definition***service-definition-name* **service-type** {*custom* | *built-in*} コマンドの出力例を示します。

```
Service    PTR       Type
================================================================================
apple-tv        _airplay._tcp.local  Built-In
                          _raop._tcp.local
apple-file-share     _afpovertcp._tcp.local          Built-In
CUSTOM1         _custom1._tcp.local       Custom
CUSTOM2         _customA._tcp.local             Custom
                          _customA._tcp.local
```

次に、**show mdns-sd** *service-policy-name* **interface** *interface-name* コマンドの出力例を示します。

```
Name   Service-List-In   Service-List-Out
================================================
mdns-policy-1  VLAN100-list   VLAN300-list
mdns-policy-2  VLAN400-list   VLAN400-list
```

次に、**show mdns-sd summary** [**interface** *interface-name*] コマンドの出力例を示します。

```
Global mDNS Gateway
=========================================
mDNS Gateway           : Enabled
Rate Limit                    : 60 PPS (default)
AirPrint Helper            : Disabled

Interface  :  Vlan601
=========================================
mDNS Gateway             : Enabled
mDNS Service Policy      : policy1
Active Query                   : Enabled
                                          : Periodicity 60 Seconds
Transport Type               : Both IPv4 & IPv6
Service Instance Suffix  : ghalwasi
mDNS Query Type          : ALL

Interface  :  Vlan602
=========================================
mDNS Gateway             : Enabled
mDNS Service Policy      : int602
Active Query                   : Enabled
                                          : Periodicity 100 Seconds
Transport Type               : Both IPv4 & IPv6
Service Instance Suffix  : 602
mDNS Query Type          : ALL
```

コントローラの確認

次に、**show mdns controller summary** コマンドの出力例を示します。

```
Device# show mdns controller summary

Controller Summary
===================================
 Controller Name  :   DNAC-BONJOUR-CONTROLLER
 Controller IP    :   10.104.52.241
 State            :   UP
 Port             :   9991
 Interface        :   Loopback0
 Filter List      :   policy1
 Dead Time        :   00:01:00
```

次に、**show mdns controller export-summary** コマンドの出力例を示します。

```
Device# show mdns controller export-summary

Controller Export Summary
=========================
 Controller IP    :   10.104.52.241
 State            :   UP
 Filter List      :   policy1
```

```
 Count            :   100
 Delay Timer      :   30 seconds
 Export           :   300
 Drop             :   0
 Next Export      :   00:00:01
```

次に、**show mdns controller statistics** コマンドの出力例を示します。

```
Device# show mdns controller statistics

Total BCP message sent           : 47589
  Total BCP message received       : 3
  Interface WITHDRAW messages sent : 0
  Clear cache messages sent        : 0
  Total RESYNC state count         : 0
  Last successful RESYNC           : Not-Applicable

  Service Advertisements:
   IPv6 advertised                 : 0
   IPv4 advertised                 : 300
   Withdraws sent                  : 0
   Advertisements Filtered         : 0
   Total service resynced          : 0

  Service Queries:
   IPv6 queries sent               : 0
   IPv6 query responses received   : 0
   IPv4 queries sent               : 0
   IPv4 query responses received   : 0
```

次に、**show mdns controller detail** コマンドの出力例を示します。

```
Device# show mdns controller detail

Controller : DNAC-BONJOUR-CONTROLLER
 IP : 10.104.52.241, Dest Port : 9991, Src Port : 0, State : UP
 Source Interface : Loopback0, MD5 Disabled
 Hello Timer 0 sec, Dead Timer 0 sec, Next Hello 00:00:00
 Uptime 00:00:00
Service Announcement :
 Filter : policy1
 Count 100, Delay Timer 30 sec, Pending Announcement 0, Pending Withdraw
 0
 Total Export Count 300, Next Export in 00:00:16
Service Query :
 Query Suppression Disabled
 Query Count 50, Query Delay Timer 15 sec, Pending 0
 Total Query Count 0, Next Query in 00:00:01
```

有線およびワイヤレスネットワーク向け Local Area Bonjour の確認

次に、**show run** コマンドの出力例を示します。

```
mdns-sd gateway
 rate-limit 100
 service-query-count 100
 service-announcement-count 100


mdns-sd service-definition custom1
 service-type _airplay._tcp.local
 service-type _raop._tcp.local
 service-type _ipp._tcp.local
 service-type _afpovertcp._tcp.local
 service-type _nfs._tcp.local
 service-type _ssh._tcp.local
 service-type _dpap._tcp.local
 service-type _daap._tcp.local
 service-type _ichat._tcp.local
 service-type _presence._tcp.local
 service-type _http._tcp.local
 service-type _ipps._tcp.local
 service-type _printer._tcp.local
 service-type _smb._tcp.local
 service-type _ftp._tcp.local


mdns-sd service-list list1 IN
 match custom1
mdns-sd service-list list2 OUT
match custom1


mdns-sd service-policy policy1
service-list list1 IN
service-list list2 OUT


service-export mdns-sd controller APIC-EM
controller-address 99.99.99.10
controller-port 9991
controller-service-policy policy1 OUT
controller-source-interface Loopback0
```

Bonjour 向け DNAサービスに関する追加情報

関連項目	マニュアル タイトル
Cisco DNA Center Cisco Wide Area Bonjour アプリケーション ユーザー ガイド	Cisco DNA Center Cisco Wide Area Bonjour アプリケーション ユーザー ガイド リリース 1.3.1.0

MIB

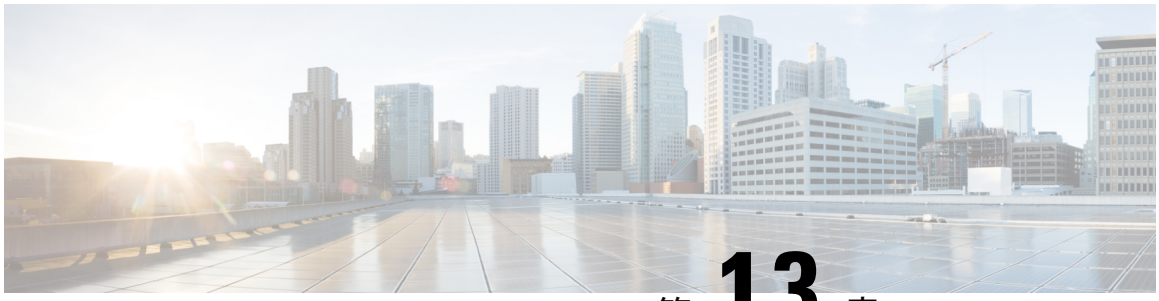
MIB	MIB のリンク
CISCO-SDG-MDNS-MIB	この MIB モジュールでは、63 のローカルエリアおよびワイドエリア mDNS SDG エージェントの統計情報を記述するオブジェクトを定義します。統計情報は、グローバルまたはインターフェイスごとに 64 です。

Bonjour 向け DNA サービスの機能履歴

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。

リリース	変更内容
Cisco IOS 15.2(6) E2	Local Area Bonjour および Wide Area Bonjour 向けの Cisco DNA サービスが次のプラットフォームに導入されました。 • Cisco Catalyst 2960-X シリーズ スイッチ • Cisco Catalyst 2960-XR シリーズ スイッチ
Cisco IOS 15.5(1)SY4	Local Area Bonjour および Wide Area Bonjour 向けの Cisco DNA サービスが Cisco Catalyst 6800 シリーズ スイッチに導入されました。
Cisco IOS XE 3.11.0 E	Local Area Bonjour および Wide Area Bonjour 向けの Cisco DNA サービスが次のプラットフォームに導入されました。 • Cisco Catalyst 4500-E シリーズ スイッチ • Cisco Catalyst 4500-X シリーズ スイッチ

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	Local Area Bonjour および Wide Area Bonjour 向けの Cisco DNA サービスが次のプラットフォームに導入されました。 • Cisco Catalyst 3650 シリーズ スイッチ • Cisco Catalyst 3850 シリーズ スイッチ • Cisco Catalyst 9300 シリーズ スイッチ • Cisco Catalyst 9400 シリーズ スイッチ • Cisco Catalyst 9500 シリーズ スイッチ • Cisco Catalyst 9500 シリーズ スイッチ - ハイ パフォーマンス • Cisco Catalyst 9600 シリーズ スイッチ • Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ • Cisco 5500 シリーズ ワイヤレス コントローラ • Cisco 8540 ワイヤレスコントローラ • Cisco 4000 シリーズ サービス統合型ルータ（ISR）
Cisco IOS XE Amsterdam 17.1.1	Local Area Bonjour 向けの Cisco DNA サービスが Cisco Catalyst 9200 シリーズ スイッチに導入されました。



第 13 章

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 9300 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、ユーザーは最初に、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 ユーザー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、ユーザーに対する 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。

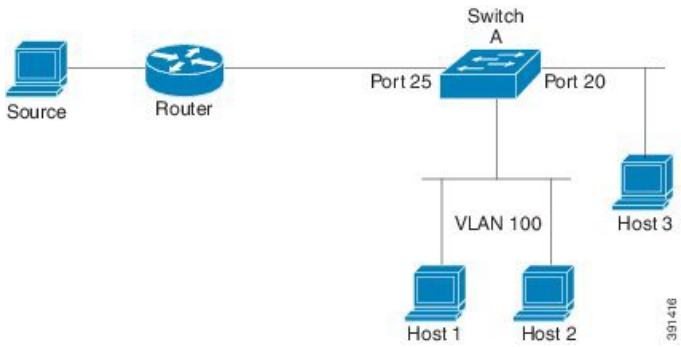
PIM スタブ ルーティングを使用しているときは、IPv6 マルチキャスト ルーティングを使用し、スイッチだけを PIM スタブ ルータとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。スイッチは分散ルータ間の伝送トラフィックをルーティングしません。スイッチのルーテッドアップリンク ポートも設定する必要があります。SVI の場合は、スイッチのアップリンク ポートを使用できません。

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 *23 : 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。ユーザーは、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、ユーザーは、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

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：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	デバイス> **enable**	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。
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。

	コマンドまたはアクション	目的
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`	ユーザーに 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： `デバイス# 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：	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。

	コマンドまたはアクション	目的
	デバイス# **debug ipv6 mld**	
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。ユーザー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）。
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：	MLD ステートの数をグローバルに制限します。

	コマンドまたはアクション	目的
	デバイス(config)# **ipv6 mld state-limit 300**	
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。
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：	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
	デバイス# **configure terminal**	
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。
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： デバイス# **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 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。

	コマンドまたはアクション	目的
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： 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	**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。
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。

	コマンドまたはアクション	目的
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、ユーザーは 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、ユーザーは 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： `デバイス# 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 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、ユーザーは 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。
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。

	コマンドまたはアクション	目的
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 *21 :* 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
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

	コマンドまたはアクション	目的
		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： `デバイス(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ー

表 *22 : 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。

コマンド	目的
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。

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。

	コマンドまたはアクション	目的
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。

	コマンドまたはアクション	目的
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）。
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：	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
	デバイス(config)# **ipv6 pim bsr candidate rp 2001:DB8:1:1:1 group-list list scope 6**	
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。ユーザーは、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。

	コマンドまたはアクション	目的
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 サーバー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 サーバーを少なくとも 1 つ見つける必要があります。スイッチは、その DNS サーバー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。

	コマンドまたはアクション	目的
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：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	デバイス> **enable**	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。
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。
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。

	コマンドまたはアクション	目的
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)*』

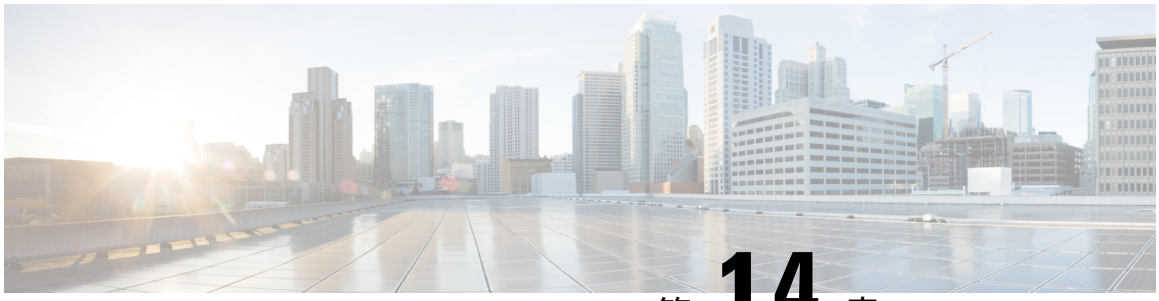
IPv6 マルチキャストの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IPv6 マルチキャスト	IPv6 マルチキャストでは、ホストから単一データストリームをすべてのホストのサブネットに同時に送信（グループ伝送）できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。



第 14 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。

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。

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。

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

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

MLD メッセージ

MLDv1 は、次の 3 種類のメッセージをサポートします。

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

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

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

MLD クエリー

スイッチは MLD クエリーを送信し、IPv6 マルチキャスト アドレス データベースを構築し、MLD グループ固有クエリー、MLD グループおよび送信元固有クエリーを生成して、MLD Done

メッセージに応答します。また、スイッチはレポート抑制、レポートプロキシング、即時脱退機能、およびスタティックな IPv6 マルチキャスト グループ アドレス設定もサポートします。

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

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

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

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

マルチキャスト クライアント エージングの堅牢性

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

マルチキャスト ルータ検出

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

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

- 受信された IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネーブルかどうかにかかわらず、常に入力 VLAN にフラッディングされます。
- 最初の IPv6 マルチキャスト ルータ ポートが検出された後は、不明の IPv6 マルチキャスト データは、検出されたルータ ポートに対してのみ転送されます（それまでは、すべての IPv6 マルチキャスト データは入力 VLAN にフラッディングされます）。

MLD レポート

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

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

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

MLD Done メッセージおよび即時脱退

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

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

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

MASQ は、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信されます。スイッチの最大応答時間内に MASQ で指定された IPv6 マルチキャスト アドレスにレポートが送信されなければ、MASQ が送信されたポートは IPv6 マルチキャスト アドレス データベースか

ら削除されます。最大応答時間は、 **ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュレーション コマンドにより設定します。削除されたポートがマルチキャスト アドレスの最後のメンバである場合は、マルチキャストアドレスも削除され、スイッチは検出されたマルチキャスト ルータすべてにアドレス脱退情報を送信します。

TCN 処理

ipv6 mld snooping tcn query solicit グローバル コンフィギュレーション コマンドを使用して、トポロジ変更通知（TCN）送信要求を有効にすると、MLDv1 スヌーピングは、設定された数の MLDv1 クエリによりすべての 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

Table 23: MLD **スヌーピングのデフォルト設定**

機能	デフォルト設定
MLD スヌーピング（グローバル）	ディセーブル。
MLD スヌーピング（VLAN 単位）	イネーブルVLAN MLD スヌーピングが実行されるためには、MLD スヌーピングがグローバルにイネーブルである必要があります。
IPv6 マルチキャスト アドレス	未設定
IPv6 マルチキャスト ルータ ポート	未設定
MLD スヌーピング即時脱退	ディセーブル。
MLD スヌーピングの堅牢性変数	グローバル：2、VLAN 単位：0 **Note** 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 **Note** 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 **Note** 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。
- MLD スヌーピングと IGMP スヌーピングは相互に独立して動作します。スイッチで両方の機能を同時にイネーブルにできます。
- スイッチまたはスイッチ スタックに保持可能なアドレス エントリの最大数は 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

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。

スイッチでグローバルにMLDスヌーピングをイネーブルにするには、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： `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	**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	**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 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**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。
ステップ 6	**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 に対する MLD スヌーピングのイネーブル化またはディセーブル化

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

Procedure

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `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	**configure terminal** **Example:** `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 snooping** **Example:** `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 4	**ipv6 mld snooping vlan** *vlan-id* **Example:** `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。 **Note** 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 5	**end** **Example:** `Device(config)# ipv6 mld snooping vlan 1`	特権 EXEC モードに戻ります。

スタティックなマルチキャスト グループの設定

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

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

Procedure

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `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	**configure terminal** **Example:** `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 snooping vlan** *vlan-id* **static** *ipv6_multicast_address* **interface** *interface-id* **Example:** `Device(config)# ipv6 mld snooping vlan 1 static 3333.0000.1111 interface gigabitethernet 1/1/0/1`	マルチキャスト グループのメンバとしてレイヤ 2 ポートにマルチキャスト グループを設定します。 • *vlan-id* は、マルチキャスト グループの VLAN ID です。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • *ipv6_multicast_address* は、128 ビットのグループ IPv6 アドレスです。このアドレスは RFC 2373 で指定された形式でなければなりません。 • *interface-id* は、メンバ ポートです。物理インターフェイスまたはポート チャネル（1 ～ 48）に設定できます。
ステップ 4	**end** **Example:** `Device(config)# end`	特権 EXEC モードに戻ります。

ステップ 5	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*
	Example:
	`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

Note 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、次の手順を実行します。

Procedure

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `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	**configure terminal** **Example:** `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 snooping vlan** *vlan-id* **mrouter interface** *interface-id* **Example:** `Device(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet 1/0/2`	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 4	**end** **Example:** `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 mld snooping mrouter** [**vlan** *vlan-id*] **Example:** `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

MLDv1 即時脱退をイネーブルにするには、次の手順を実行します。

Procedure

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `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	**configure terminal** **Example:** `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 snooping vlan** *vlan-id* **immediate-leave** **Example:** `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。
ステップ 4	**end** **Example:** `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 mld snooping vlan** *vlan-id* **Example:** `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

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

Procedure

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `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	**configure terminal** **Example:** `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。

	Command or Action	Purpose
ステップ 3	**ipv6 mld snooping robustness-variable** *value* **Example:** `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 4	**ipv6 mld snooping vlan** *vlan-id* **robustness-variable** *value* **Example:** `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。
ステップ 5	**ipv6 mld snooping last-listener-query-count** *count* **Example:** `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 6	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-count** *count* **Example:** `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 7	**ipv6 mld snooping last-listener-query-interval** *interval* **Example:** `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 8	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-interval** *interval* **Example:** `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 9	**ipv6 mld snooping tcn query solicit** **Example:** `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

	Command or Action	Purpose
		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 10	**ipv6 mld snooping tcn flood query count** *count* **Example:** `Device(config)# ipv6 mld snooping tcn flood query count 5`	（任意）TCNがイネーブルの場合、送信されるTCNクエリー数を指定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show ipv6 mld snooping querier** [**vlan** *vlan-id*] **Example:** `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

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、次の手順を実行します。

Procedure

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `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	**configure terminal** **Example:** `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	**no ipv6 mld snooping listener-message-suppression** **Example:** `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。

	Command or Action	Purpose
ステップ 4	**end** **Example:** `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 mld snooping** **Example:** `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。

***Table 24: MLD* スヌーピング情報表示用のコマンド**

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

コマンド	目的
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 3333.0000.1111 interface
gigabitethernet1/0/1
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
        1/0/2
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
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9300 Series Switches)*

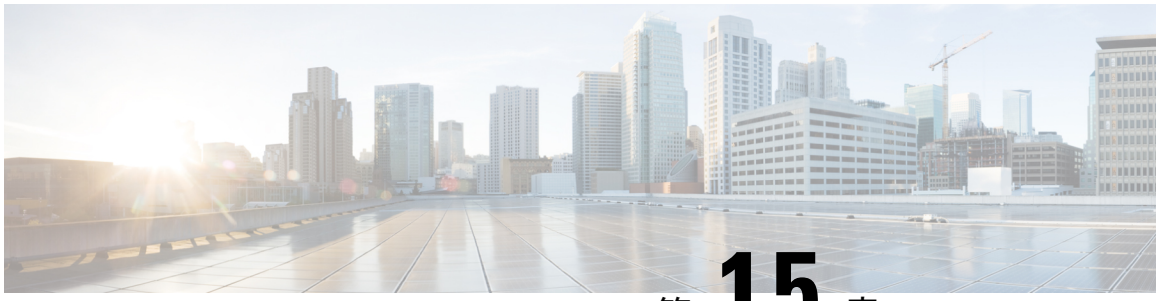
MLD スヌーピングの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能名	機能情報
Cisco IOS XE Everest 16.5.1a	MLD スヌーピング	MLD スヌーピングにより、スイッチで MLD パケットを調べ、パケットの内容に基づいて転送先を決定できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/にアクセスします。



第 15 章

マルチキャスト バーチャル プライベート ネットワークの設定

マルチキャスト VPN の設定に関する前提条件

「Configuring Basic IP Multicast」モジュールに記載されているタスクを使用して、IP マルチキャストを有効にして PIM インターフェイスを設定します。

マルチキャスト VPN の設定の制限

- ボーダー ゲートウェイ プロトコル（BGP）ピアリングのアップデート ソース インターフェイスは、デフォルト マルチキャスト配信ツリー（MDT）を適切に設定するために、デバイス上に設定されたすべての BGP ピアリングで同じにする必要があります。BGP ピアリングにループバック アドレスを使用する場合は、ループバック アドレスで PIM スパース モードをイネーブルにする必要があります。
- MVPN では、複数の BGP ピアリング更新送信元をサポートしていません。
- 複数の BGP 更新送信元はサポートされていません。これらを設定すると、リバース パス フォワーディング（RPF）のチェックが中断される可能性があります。MVPN トンネルの送信元 IP アドレスは、BGP ピアリング更新送信元に使用される最高の IP アドレスによって決まります。この IP アドレスが、リモートのプロバイダ エッジ（PE）デバイスを含む BGP ピアリング アドレスとして使用される IP アドレスでない場合、MVPN は適切に機能しません。

- エクストラネットでのマルチキャスト VPN はサポートされていません。

マルチキャスト VPN の設定について

ここでは、マルチキャスト VPN の設定について説明します。

マルチキャスト VPN の操作

MVPN IP を使用すると、サービス プロバイダは MPLS VPN 環境でマルチキャスト トラフィックを設定およびサポートできます。この機能は、個々の VRF インスタンスでのマルチキャスト パケットのルーティングおよび転送をサポートし、サービス プロバイダのバックボーンに VPN マルチキャスト パケットを転送するメカニズムも提供します。

VPN は、ISP などの共有インフラストラクチャを介するネットワークの接続性です。その役割は、プライベート ネットワークとして、同じポリシーとパフォーマンスを低い所有コストで提供することによって、業務とインフラストラクチャを通して、多くのコスト削減の機会を作り出すことです。

MVPN により、企業はサービス プロバイダのネットワーク バックボーンでプライベート ネットワークをトランスペアレントに相互接続することができます。このように MVPN を使用して企業ネットワークを相互接続しても、企業ネットワークの管理方法や、企業の全体的な接続性は変更されません。

マルチキャスト VPN の利点

- 複数の場所に情報を動的に送信するスケーラブルなメソッドを提供します。
- 高速な情報伝送を提供します。
- 共有インフラストラクチャを介して接続性を提供します。

マルチキャスト VPN ルーティングおよび転送とマルチキャスト ドメイン

MVPN は、VPN ルーティングおよび転送テーブルにマルチキャスト ルーティング情報を導入します。プロバイダ エッジ（PE）デバイスがマルチキャスト データまたは制御パケットをカスタマー エッジ（CE）ルータから受信すると、マルチキャスト VPN ルーティングおよび転送インスタンス（MVRF）の情報に従って転送が実行されます。MVPN は、ラベル スイッチングを使用しません。

マルチキャスト トラフィックを相互に送信できる MVRF のセットは、マルチキャスト ドメインの構成要素です。たとえば、特定タイプのマルチキャスト トラフィックをすべてのグローバルな従業員に送信するカスタマーのマルチキャスト ドメインは、そのエンタープライズと関連するすべての CE ルータから構成されます。

マルチキャスト配信ツリー

MVPN は、各マルチキャスト ドメインにスタティック デフォルト マルチキャスト配信ツリー（MDT）を確立します。デフォルト MDT は、PE ルータが使用するパスを定義し、マルチキャスト ドメインにある他のすべての PE ルータに、マルチキャスト データとコントロール メッセージを送信します。

Source Specific Multicast（SSM; 送信元特定マルチキャスト）がコア マルチキャスト ルーティング プロトコルとして使用される場合、デフォルト MDT およびデータ MDT に使用されるマルチキャスト IP アドレスは、すべての PE ルータの SSM 範囲内に設定する必要があります。

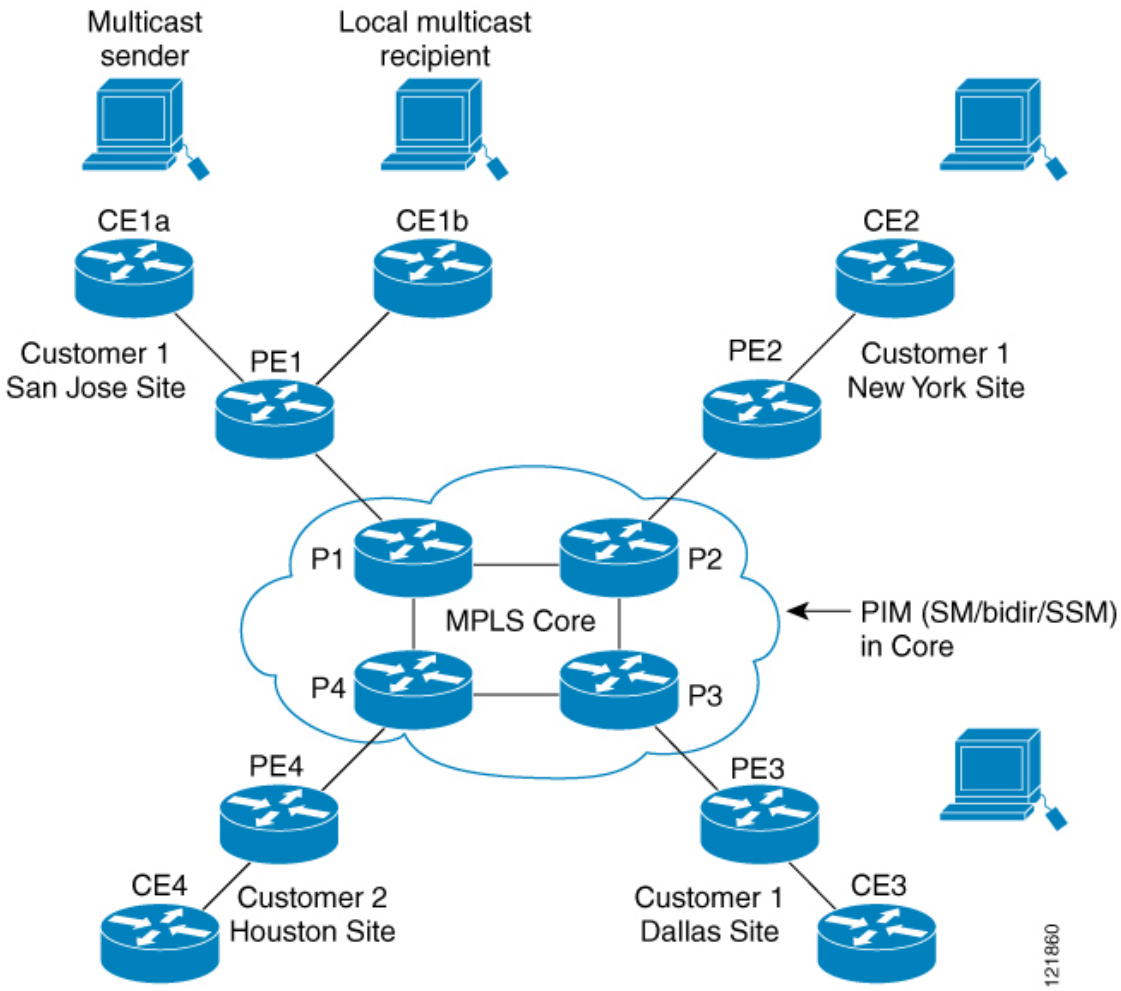
また、MVPN は、高帯域幅伝送用の MDT のダイナミックな作成もサポートします。データ MDT は、Cisco IOS ソフトウェアに一意な機能です。データ MDT は、VPN 内のフルモーション ビデオなどの高帯域幅の送信元向けであり、MPLS VPN コアの最適なトラフィック転送を確保することを目的としています。データ MDT が作成されるしきい値は、ルータ単位または VRF 単位で設定できます。マルチキャスト伝送が定義されたしきい値を超えると、送信側の PE ルータがデータ MDT を作成し、データ MDT に関する情報を含む UDP メッセージをデフォルト MDT のすべてのルータに送信します。マルチキャスト ストリームがデータ MDT のしきい値を超えたかどうかを判断する統計情報は、1 秒に 1 回確認されます。PE ルータは UDP メッセージを送信した後、切り替わるまでに 3 秒以上待機します。最も長くかかる場合は 13 秒、最良の場合は 3 秒です。

データ MDT は、VRF マルチキャスト ルーティング テーブル内で、（S,G）マルチキャスト ルート エントリ専用に作成されます。個々のソースデータ レートの値に関係なく、(*, G) エントリ用には作成されません。

次の例のサービス プロバイダには、San Jose、New York、Dallas にオフィスがあるマルチキャスト カスタマーがいます。San Jose では、一方向のマルチキャスト プレゼンテーションが行われています。サービス プロバイダ ネットワークでは、このカスタマーと関連する 3 つすべてのサイト、および別のエンタープライズ カスタマーの Houston サイトがサポートされます。

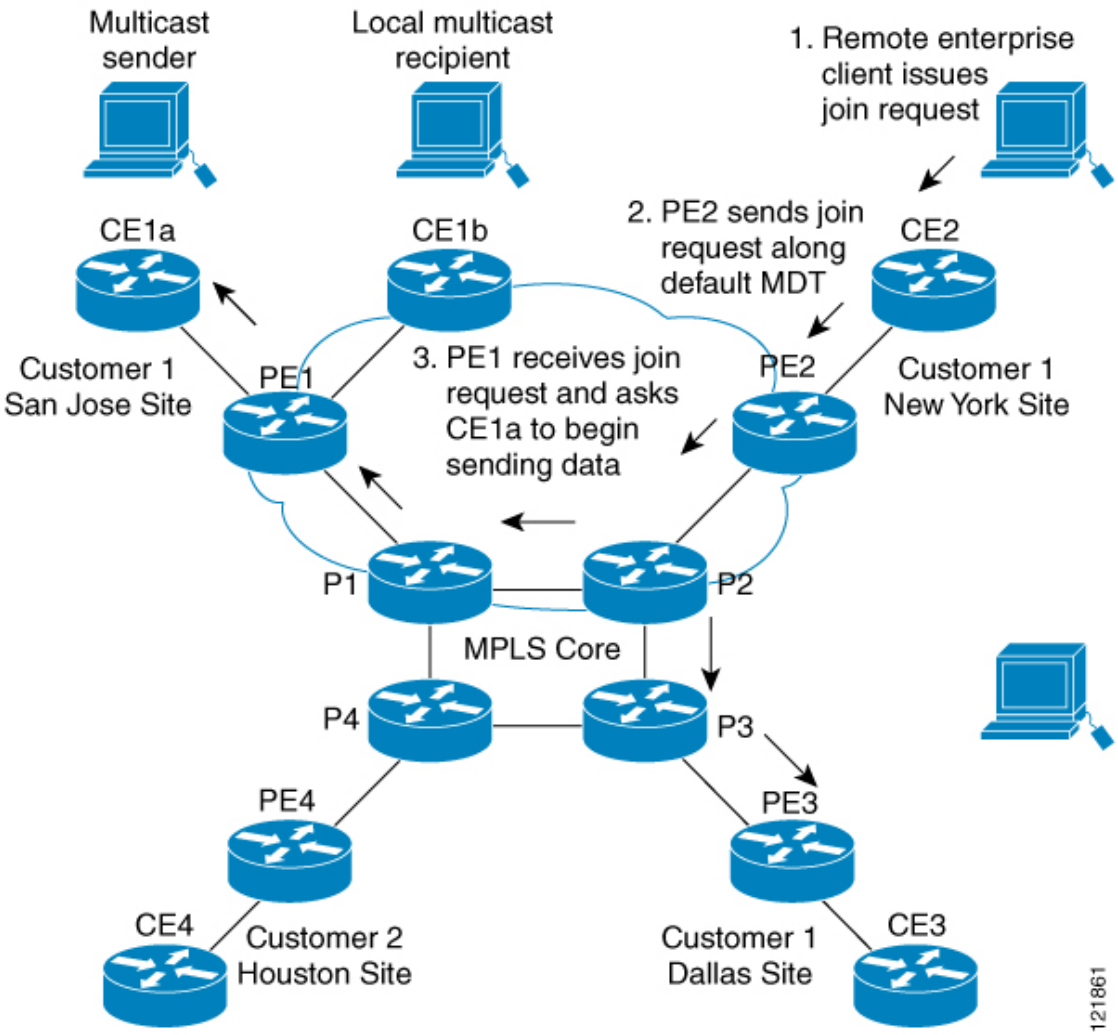
エンタープライズ カスタマーのデフォルト MDT は、プロバイダのルータ P1、P2、P3、およびその関連 PE ルータから構成されています。PE4 は別のカスタマーに関連付けられているため、デフォルト MDT の一部ではありません。次の図からは、San Jose 以外はマルチキャストに加入していないため、データがデフォルト MDT に沿って転送されていないことがわかります。

図 *24 :* デフォルト マルチキャスト配信ツリーの概要



New York の従業員がマルチキャスト セッションに加入します。New York のサイトに関連付けられている PE ルータは、カスタマーのマルチキャスト ドメインのデフォルト MDT を介して転送される加入要求を送信します。PE1 は、マルチキャスト セッションの送信元に関連付けられている PE ルータであり、この要求を受信します。次の図は、PE ルータが、マルチキャスト送信元（CE1a）と関連する CE ルータに要求を転送する方法を示しています。

図 *25* : データ *MDT* の初期化



CE ルータ（CE1a）が関連する PE ルータ（PE1）へマルチキャスト データの送信を開始すると、PE ルータ（PE1）は、デフォルト MDT に沿ってマルチキャスト データを送信します。PE1 は、マルチキャスト データを送信すると、マルチキャスト データがデータ MDT を作成する対象の帯域幅のしきい値を超えていることを認識します。したがって、PE1 はデータ MDT を作成し、データ MDT に関する情報を含むデフォルト MDT を使用して、すべてのルータにメッセージを送信し、3 秒後、データ MDT を使用して、その特定のストリームのマルチキャスト データを送信し始めます。このソースに関係する受信先は PE2 だけにあるので、PE2 だけがデータ MDT に加入し、データ MDT でトラフィックを受信します。

PE ルータは、デフォルト MDT を介して他の PE ルータと PIM 関係を維持するとともに、直接接続された PE ルータとの PIM 関係をも維持します。

マルチキャスト トンネル インターフェイス

マルチキャスト ドメインごとに作成される MVRF では、デバイスは、すべての MVRF トラフィックが発信されるトンネルインターフェイスを作成する必要があります。マルチキャスト トンネル インターフェイスは、MVRF がマルチキャスト ドメインにアクセスするために使用するインターフェイスです。これは MVRF とグローバル MVRF をつなぐコンジットと見なすことができます。MVRF ごとに 1 つのトンネル インターフェイスが作成されます。

マルチキャスト VPN での BGP の MDT アドレス ファミリ

MDT アドレスファミリセッションを設定するために、**mdt** キーワードが **address-family ipv4** コマンドに追加されました。MDT アドレス ファミリ セッションは、Border Gateway Protocol（BGP）MDT Subaddress Family Identifier（SAFI）のアップデートを使用して PIM に送信元 PE アドレスと MDT グループ アドレスを渡すために使用されます。

マルチキャスト VPN サポートの BGP アドバタイズメント方式

1 つの自律システムで、MVPN のデフォルト MDT がランデブー ポイント（RP）のあるスパース モード（PIM-SM）を使用している場合、ソース PE とレシーバ PE は RP を通して互いを検出するため、PIM は、マルチキャスト トンネル インターフェイス（MTI）に隣接を確立できます。このシナリオでは、ローカル PE（送信元 PE）が RP に登録メッセージを送信し、次に RP が送信元 PE に向けて最短パスツリーを構築します。次にリモート PE（MDT マルチキャスト グループの受信者として機能します）が RP に向けて (*, G) 加入メッセージを送信し、そのグループの配信ツリーに参加します。

しかし、デフォルト MDT グループが PIM-SM 環境ではなく PIM Source Specific Multicast（PIM-SSM）環境で設定されている場合、受信側 PE は送信元 PE とデフォルト MDT グループに関する情報を必要とします。この情報は、送信元 PE に向けて (S, G) 加入メッセージを送信し、送信元PEからの配信ツリーを構築するために使用されます。（RPは必要ありません）。送信元 PE アドレスとデフォルト MDT グループ アドレスは、BGP を使用して送信されます。

BGP 拡張コミュニティ

BGP拡張コミュニティを使用すると、PEループバック（発信元アドレス）情報はVPNv4プレフィックスとしてルート識別子（RD）タイプ2を使用して送信されます（ユニキャストVPNv4プレフィックスと区別するため）。MDT グループ アドレスは、BGP 拡張コミュニティに伝えられます。VPNv4アドレスに組み込まれた送信元と拡張コミュニティ内のグループの組み合わせを使用すると、同じ MVRF インスタンス内の PE ルータは相互に SSM ツリーを確立できます。

（注） MDT SAFI サポートが導入される前、BGP 拡張コミュニティの属性は、IETF によって標準化される前のソース PE およびデフォルト MDT グループの IP アドレスをアドバタイズするための暫定的ソリューションとして使用されていました。しかし、MVPN 環境の BGP 拡張コミュニティ属性には一定の制限があります。AS 間シナリオでは使用できず（属性が非推移的であるため）、RD タイプ 2 が使用されます（これはサポートされる標準ではありません）。

マルチキャスト VPN の設定方法

ここでは、マルチキャスト VPN を設定する際の手順を説明します。

データ マルチキャスト グループの設定

データ MDT グループには、VPN、VRF、PE デバイスごとに最大 256 のマルチキャスト グループを含むことができます。データ MDT グループの作成に使用されるマルチキャスト グループは、設定済み IP アドレスのプールからダイナミックに選択されます。デバイスでデータ マルチキャスト グループを設定するには、次の手順を使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target both** *ASN:nn* または *IP-address:nn*
6. **address family ipv4 unicast** *value*
7. **mdt default** *group-address*
8. **mdt data** *group number*
9. **mdt data threshold** *kbps*
10. **mdt log-reuse**
11. **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： `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	**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	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition vrf1`	VRF コンフィギュレーション モードを開始し、VRF 名を割り当てることにより VPN ルーティング インスタンスを定義します。

	コマンドまたはアクション	目的
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 1:1`	VRF のルーティング テーブルと転送テーブルを作成します。 • *route-distinguisher* 引数では、8 バイトの値を IPv4 プレフィックスに追加して VPN IPv4 プレフィックスを作成することを指定します。*route-distinguisher* は、次のいずれかの形式で入力できます。 • 16 ビット ASN：32 ビット数値。たとえば、101:3 と指定します。 • 32 ビット IP アドレス：16 ビット数値。たとえば、192.168.122.15:1 と指定します。
ステップ 5	**route-target both** *ASN:nn* または *IP-address:nn* 例： `Device(config-vrf)# route-target both 1:1`	VRF 用にルート ターゲット拡張コミュニティを作成します。**both** キーワードを使用すると、ルーティング情報のターゲット VPN 拡張コミュニティからのインポート、およびターゲット VPN 拡張コミュニティへのエクスポートの両方が行われます。
ステップ 6	**address family ipv4 unicast** *value* 例： `Device(config-vrf)# address family ipv4 unicast`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、VRF のアドレス ファミリを指定します。 • **ipv4** キーワードは、VRF の IPv4 アドレス ファミリを指定します。
ステップ 7	**mdt default** *group-address* 例： `Device(config-vrf-af)# mdt default 226.10.10.10`	VRF に、データ MDT グループのマルチキャスト グループ アドレスの範囲を設定します。 • このコマンドによって、トンネルインターフェイスが作成されます。 • デフォルト MDT グループアドレス設定は、同じ VRF 内のすべての PE で同一にする必要があります。
ステップ 8	**mdt data** *group number* 例： `Device(config-vrf-af)# mdt data 232.0.1.0 0.0.0.31`	データ MDT プールで使用されるアドレスの範囲を指定します。
ステップ 9	**mdt data threshold** *kbps* 例：	しきい値を *kbps* 単位で指定します。範囲は 1 ～ 4294967 です。

	コマンドまたはアクション	目的
	`Device(config-vrf-af)# mdt data threshold 50`	
ステップ 10	**mdt log-reuse** 例： `Device(config-vrf-af)# mdt log-reuse`	（任意）データ MDT 再使用の記録をイネーブルにし、データ MDT が再使用された場合に、syslog メッセージを生成します。
ステップ 11	**end** 例： `Device(config-vrf-af)# end`	特権 EXEC モードに戻ります。

VRF のデフォルト MDT グループの設定

VRF にデフォルト MDT グループを設定するには、次の作業を実行します。

デフォルト MDT グループは、同じ VPN に属するすべてのデバイスに設定された同じグループである必要があります。送信元 IP アドレスは、BGP セッションの送信元を特定するために使用するアドレスです。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast-routing**
4. **ip multicast-routing vrf** *vrf-name*
5. **vrf definition** *vrf-name*
6. **rd** *route-distinguisher*
7. **route-target both** *ASN:nn* または *IP-address:nn*
8. **address family ipv4 unicast** *value*
9. **mdt default** *group-address*
10. **end**
11. **configure terminal**
12. **ip pim vrf** *vrf-name***rp-address** *value*

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）。

	コマンドまたはアクション	目的
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	**ip multicast-routing** 例： `Device(config)# ip multicast-routing`	マルチキャスト ルーティングをイネーブルにします。
ステップ 4	**ip multicast-routing vrf** *vrf-name* 例： `Device(config)# ip multicast-routing vrf vrf1`	MVPN VRF インスタンスをサポートします。
ステップ 5	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition vrf1`	VRF コンフィギュレーション モードを開始し、VRF 名を割り当てることにより VPN ルーティング インスタンスを定義します。
ステップ 6	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 1:1`	VRF のルーティング テーブルと転送テーブルを作成します。 • *route-distinguisher* 引数では、8 バイトの値を IPv4 プレフィックスに追加して VPN IPv4 プレフィックスを作成することを指定します。*route-distinguisher* は、次のいずれかの形式で入力できます。 • 16 ビット ASN：32 ビット数値。たとえば、101:3 と指定します。 • 32 ビット IP アドレス：16 ビット数値。たとえば、192.168.122.15:1 と指定します。
ステップ 7	**route-target both** *ASN:nn* または *IP-address:nn* 例： `Device(config-vrf)# route-target both 1:1`	VRF 用にルート ターゲット拡張コミュニティを作成します。**both** キーワードを使用すると、ルーティング情報のターゲット VPN 拡張コミュニティからのインポート、およびターゲット VPN 拡張コミュニティへのエクスポートの両方が行われます。
ステップ 8	**address family ipv4 unicast** *value* 例： `Device(config-vrf)# address family ipv4 unicast`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、VRF のアドレス ファミリを指定します。 • **ipv4** キーワードは、VRF の IPv4 アドレス ファミリを指定します。

	コマンドまたはアクション	目的
ステップ 9	**mdt default** *group-address* 例： `Device(config-vrf-af)# mdt default 226.10.10.10`	VRF に、データ MDT グループのマルチキャスト グループ アドレスの範囲を設定します。 • このコマンドによって、トンネルインターフェイスが作成されます。 • デフォルト MDT グループ アドレス設定は、同じ VRF 内のすべての PE で同一にする必要があります。
ステップ 10	**end** 例： `Device(config-vrf-af)# end`	特権 EXEC モードに戻ります。
ステップ 11	**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 12	**ip pim vrf** *vrf-name***rp-address** *value* 例： `Device(config-vrf-af)# ip pim vrf vrf1 rp-address 1.1.1.1`	RP コンフィギュレーション モードを開始します。

マルチキャスト VPN での BGP の MDT アドレス ファミリの設定

PE デバイスに MDT アドレス ファミリ セッションを設定し、MVPN の MDT ピアリング セッションを確立するには、次の作業を実行します。

始める前に

MDT アドレス ファミリを通して MVPN ピアリングを確立する前に、CE デバイスに VPN サービスを提供する PE デバイス上の BGP ネットワークおよびマルチプロトコル BGP に、MPLS およびシスコ エクスプレス フォワーディング（CEF）を設定する必要があります。

（注） 次のポリシー設定パラメータは、サポートされていません。

- ルートオリジネータ属性
- ネットワーク層到着可能性情報（NLRI）プレフィックス フィルタリング（プレフィックス リスト、配信リスト）
- 拡張コミュニティ属性（ルート ターゲットおよび発信元サイト）

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4 mdt**
5. **neighbor** *neighbor-address* **activate**
6. **neighbor** *neighbor-address* **send-community** [**both** | **extended** | **standard**]
7. **exit**
8. **address-family vpnv4**
9. **neighbor** *neighbor-address* **activate**
10. **neighbor** *neighbor-address* **send-community** [**both** | **extended** | **standard**]
11. **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： `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	**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	**router bgp** *as-number* 例： `Device(config)# router bgp 65535`	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。
ステップ 4	**address-family ipv4 mdt** 例： `Device(config-router)# address-family ipv4 mdt`	アドレス ファミリ コンフィギュレーションを開始し、IP MDT アドレス ファミリ セッションを作成します。
ステップ 5	**neighbor** *neighbor-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.1.1 activate`	このネイバーの MDT アドレス ファミリをイネーブルにします。
ステップ 6	**neighbor** *neighbor-address* **send-community** [**both** | **extended** | **standard**] 例：	指定されたネイバーとのコミュニティおよび（または）拡張コミュニティの交換をイネーブルにします。

	コマンドまたはアクション	目的
	`Device(config-router-af)# neighbor 192.168.1.1 send-community extended`	
ステップ 7	**exit** 例： `Device(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。
ステップ 8	**address-family vpnv4** 例： `Device(config-router)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始し、VPNv4 アドレス ファミリ セッションを作成します。
ステップ 9	**neighbor** *neighbor-address* **activate** 例： `Device(config-router-af)# neighbor 192.168.1.1 activate`	このネイバーの VPNv4 アドレス ファミリをイネーブルにします。
ステップ 10	**neighbor** *neighbor-address* **send-community** [**both** | **extended** | **standard**] 例： `Device(config-router-af)# neighbor 192.168.1.1 send-community extended`	指定されたネイバーとのコミュニティおよび（または）拡張コミュニティの交換をイネーブルにします。
ステップ 11	**end** 例： `Device(config-router-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

MDT デフォルト グループの情報の確認

手順の概要

1. **enable**
2. **show ip pim** [**vrf** *vrf-name*] **mdt bgp**
3. **show ip pim** [**vrf** *vrf-name*] **mdt send**
4. **show ip pim vrf** *vrf-name* **mdt history interval** *minutes*

手順の詳細

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 **show ip pim** [**vrf** *vrf-name*] **mdt bgp**

例：

```
Device# show ip pim mdt bgp

MDT-default group 232.2.1.4
rid:1.1.1.1 next_hop:1.1.1.1
```

MDT デフォルト グループの RD の BGP アドバタイズメントに関する情報を表示します。

ステップ 3 **show ip pim** [**vrf** *vrf-name*] **mdt send**

例：

```
Device# show ip pim mdt send

MDT-data send list for VRF:vpn8
  (source, group)                    MDT-data group      ref_count
  (10.100.8.10, 225.1.8.1)           232.2.8.0           1
  (10.100.8.10, 225.1.8.2)           232.2.8.1           1
  (10.100.8.10, 225.1.8.3)           232.2.8.2           1
  (10.100.8.10, 225.1.8.4)           232.2.8.3           1
  (10.100.8.10, 225.1.8.5)           232.2.8.4           1
  (10.100.8.10, 225.1.8.6)           232.2.8.5           1
  (10.100.8.10, 225.1.8.7)           232.2.8.6           1
  (10.100.8.10, 225.1.8.8)           232.2.8.7           1
  (10.100.8.10, 225.1.8.9)           232.2.8.8           1
  (10.100.8.10, 225.1.8.10)          232.2.8.9           1
```

指定されたデバイスが行った MDT アドバタイズメントを含む MDT データ グループに関する詳細情報を表示します。

ステップ 4 **show ip pim vrf** *vrf-name* **mdt history interval** *minutes*

例：

```
Device# show ip pim vrf vrf1 mdt history interval 20

   MDT-data send history for VRF - vrf1 for the past 20 minutes
MDT-data group        Number of reuse
     10.9.9.8           3
     10.9.9.9           2
```

過去に設定されたインターバル中に再利用されたデータ MDT を表示します。

マルチキャスト VPN の設定例

マルチキャスト VPN の設定例を次に紹介します。

例：MVPN および SSM の設定

次の例では、PIM-SSM がバックボーンに設定されています。そのため、デフォルト グループとデータ MDT グループは、IP アドレスの SSM 範囲内に設定されています。VPN の内部では、PIM-SM が設定され、Auto-RP アナウンスのみが受け入れられます。

```
ip vrf vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 mdt default 232.0.0.1
 mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
!
ip pim ssm default
ip pim vrf vrf1 accept-rp auto-rp
```

例：マルチキャスト ルーティングの VPN のイネーブル化

次の例では、マルチキャスト ルーティングは、vrf1 という VPN ルーティング インスタンスを使用してイネーブル化されます。

```
ip multicast-routing vrf1
```

例：データ MDT グループ用のマルチキャスト グループ アドレス範囲の設定

次の例では、VPN ルーティング インスタンスは、blue という VRF が割り当てられます。VPN VRF の MDT デフォルト グループは 239.1.1.1、MDT グループのマルチキャスト グループ アドレスの範囲は 239.1.2.0（ワイルドカード ビットが 0.0.0.3）です。

```
ip vrf blue
 rd 55:1111
 route-target both 55:1111
 mdt default 239.1.1.1
 mdt data 239.1.2.0 0.0.0.3
 end
```

例：マルチキャスト ルートの数の制限

次の例では、マルチキャスト ルーティング テーブルに追加できるマルチキャスト ルートの数が 200,000 に設定され、警告メッセージが発生する原因となる mroute の数のしきい値が 20,000 に設定されています。

```
!
ip multicast-routing
ip multicast-routing vrf cisco
ip multicast cache-headers
ip multicast route-limit 200000 20000
ip multicast vrf cisco route-limit 200000 20000
```

```
no mpls traffic-eng auto-bw timers frequency 0
!
```

マルチキャスト VPN の設定に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「Multicast VPN Commands」の項を参照してください*Command Reference (Catalyst 9300 Series Switches)*

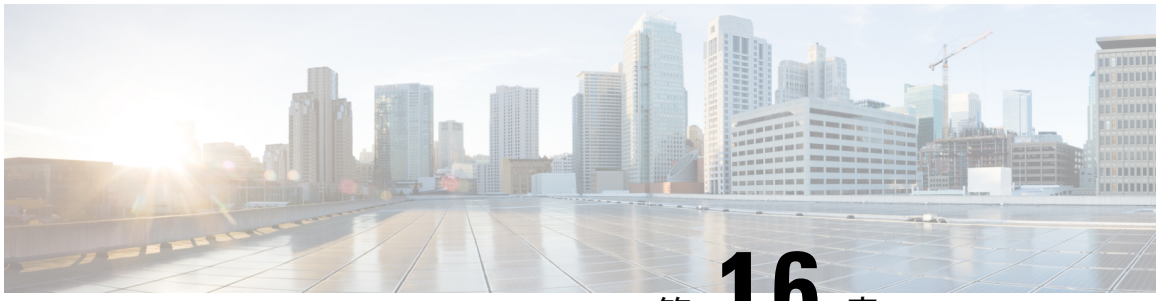
マルチキャスト VPN の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能名	機能情報
Cisco IOS XE Everest 16.5.1a	マルチキャスト VPN	マルチキャスト VPN により、企業はサービスプロバイダのネットワークバックボーンでプライベートネットワークを透過的に相互接続できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/にアクセスします。



第 16 章

MVPNv6 の設定

MVPNv6 の前提条件

- マルチキャストトラフィックを送受信するすべてのデバイスでは、BGP を設定して稼働させる必要があります。
- ネットワークでマルチキャスト配信ツリー（MDT）を使用できるようにするには、BGP 拡張コミュニティを有効にする必要があります。BGP 拡張コミュニティを有効にするには、**neighbor send-community both** または **neighbor send-community extended** コマンドを使用します。
- MVPNv6 に使用する VPN ルーティングおよび転送（MVRF）インスタンスは、PE デバイスで設定する必要があります。

MVPNv6 についての制限事項

- ポイントツーポイント GRE トンネルは、MVPNv6 向け VRF の出力インターフェイスとしてサポートされていません。

MVPNv6 について

サービスプロバイダーが複数の分散したサイトを持つカスタマーにレイヤ 3 マルチキャストサービスを提供する場合は、サービス プロバイダー ネットワーク経由でマルチキャストトラ

フィックを伝送するセキュアかつスケーラブルなメカニズムが必要です。IPv4マルチキャストVPN（MVPN）は、共有サービスプロバイダーのバックボーンを通して、このようなIPv4マルチキャストトラフィック向けサービスを提供します。

IPv6マルチキャスト バーチャル プライベート ネットワーク（MVPNv6）は、IPv6トラフィック向けに同様のサービスを提供し、サービスプロバイダーが既存のIPv4バックボーンを使用してカスタマーにマルチキャスト対応のプライベートIPv6ネットワークを提供できるようにします。IPv4とIPv6のVPNトラフィックは、同じトンネル上で同時に伝送されます。

MVPNv6 の設定方法

マルチキャスト ルーティングの設定

MVPNv6で使用するマルチキャストVPNルーティングおよび転送（MVRF）インスタンスのIPv4および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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip routing**
4. **ip routing vrf** *vrf-name*
5. **ipv6 routing**
6. **ipv6 routing vrf** *vrf-name*
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip routing** 例： `Device(config)# ip routing`	IPv4マルチキャストルーティングをイネーブルにします。
ステップ 4	**ip routing vrf** *vrf-name* 例： `Device(config)# ip routing vrf blue`	指定したMVRFインスタンスのIPv4マルチキャストルーティング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 5	**ipv6 routing** 例： `Device(config)# ipv6 routing`	IPv6 マルチキャストルーティングをイネーブルにします。
ステップ 6	**ipv6 routing vrf** *vrf-name* 例： `Device(config)# ipv6 routing vrf blue`	指定した MVRF インスタンスの IPv6 マルチキャストルーティングをイネーブルにします。
ステップ 7	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

PE デバイスでの MVRF の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask*
6. **ip pim sparse-mode**
7. **delay** *tens-of-seconds*
8. **ipv6 address** *ipv6-address* **link-local**
9. **ipv6 address** *ipv6-address-prefix*
10. **ipv6 pim**
11. **exit**
12. **ip pim rp-address** *ip-address*
13. **ip pim vrf** *vrf-name* **rp-address** *address*
14. **ipv6 pim vrf** *vrf-name* **rp-address** *ipv6-address*
15. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 3/0/3`	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 4	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding blue`	VRF をインターフェイスに関連付けます。
ステップ 5	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.1.0.1 255.255.0.0`	インターフェイスに IPv4 アドレスを設定します。
ステップ 6	**ip pim sparse-mode** 例： `Device(config-if)# ip pim sparse-mode`	インターフェイスでプロトコル独立マルチキャスト（PIM）をイネーブルにします。
ステップ 7	**delay** *tens-of-seconds* 例： `Device(config-if)# delay 1000`	インターフェイスの遅延値を設定します。
ステップ 8	**ipv6 address** *ipv6-address* **link-local** 例： `Device(config-if)# ipv6 address FE80::20:1:1 link-local`	リンクローカル IPv6 アドレスを指定します。 インターフェイスで IPv6 をイネーブルにした際に自動設定されたリンクローカルアドレスでなく、このアドレスが使用されます。
ステップ 9	**ipv6 address** *ipv6-address-prefix* 例： `Device(config-if)# ipv6 address FC00::/7`	インターフェイスに IPv6 アドレスを設定します。
ステップ 10	**ipv6 pim** 例： `Device(config-if)# ipv6 pim`	IPv6 プロトコル独立マルチキャスト（PIM）をイネーブルにします。
ステップ 11	**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。
ステップ 12	**ip pim rp-address** *ip-address* 例： `Device(config)# ip pim rp-address 10.10.10.10`	マルチキャストグループの PIM ランデブーポイント（RP）の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 13	**ip pim vrf** *vrf-name* **rp-address** *address* 例： `Device(config)# ip pim vrf blue rp-address 10.10.0.10`	PIM RP の IPv4 アドレスを設定し、指定した MVRF インスタンスに RP を関連付けます。
ステップ 14	**ipv6 pim vrf** *vrf-name* **rp-address** *ipv6-address* 例： `Device(config)# ipv6 pim vrf blue rp-address FC00::1:1:1`	PIM RP の IPv6 アドレスを設定し、指定した MVRF インスタンスに RP を関連付けます。
ステップ 15	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。

PE デバイスと CE デバイス間でのルーティング プロトコルの設定

始める前に

PE デバイスと CE デバイスでは、同じルーティングプロトコルを使用するように設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv6 vrf** *vrf-name*
5. **redistribute connected**
6. **redistribute eigrp** *as-number*
7. **redistribute static**
8. **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： `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	**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 3	**router bgp** *as-number* 例： `Device(config)# router bgp 55`	別の BGP デバイスに接続されるデバイスを識別する自律システムの番号を指定します。
ステップ 4	**address-family ipv6 vrf** *vrf-name* 例： `Device(config-router)# address-family ipv6 vrf blue`	後続のアドレス ファミリ コンフィギュレーション モードコマンドと関連付ける VRF 名を指定します。
ステップ 5	**redistribute connected** 例： `Device(config-router-af)# redistibute connected`	直接接続されたネットワークを BGP に再配布します。
ステップ 6	**redistribute eigrp** *as-number* 例： `Device(config-router-af)# redistribute eigrp 11`	EIGRP ルートを BGP に再配布します。
ステップ 7	**redistribute static** 例： `Device(config-router-af)# redistribute static`	静的ルートを BGP に再配布します。
ステップ 8	**end** 例： `Device(config-router-af)# end`	特権 EXEC モードに戻ります。

MVPNv6 の設定例

MVPNv6 の設定例を以下に示します。

```
mls ipv6 vrf
!
vrf definition blue
 rd 55:1111
 route-target export 55:1111
 route-target import 55:1111
 !
 address-family ipv4
  mdt default 232.1.1.1
 exit-address-family
 !
 address-family ipv6
  mdt default 232.1.1.1
 exit-address-family
!

ip multicast-routing
ip multicast-routing vrf blue
```

```
!
!
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 multicast-routing vrf blue
!

interface GigabitEthernet3/0/3
 vrf forwarding blue
 ip address 10.1.0.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip pim sparse-dense-mode
 delay 100
 ipv6 address FE80::20:1:1 link-local
 ipv6 address FC00::/7
 no mls qos trust
!
router bgp 55
address-family ipv6 vrf blue
  redistribute connected
  redistribute eigrp 11
  redistribute static
 exit-address-family
!

ip pim vrf blue rp-address 10.10.0.10
!
ipv6 pim vrf blue rp-address FC00::1:1:1
!
!
```

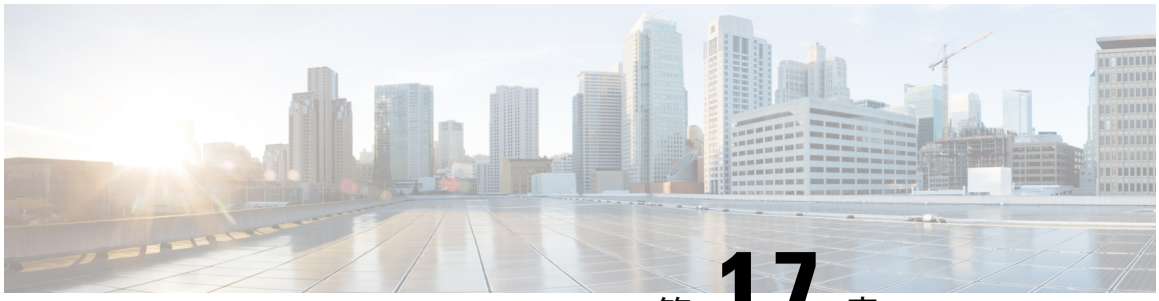
MVPNv6 の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.11.1	MVPNv6	この機能により、サービスプロバイダは既存の IPv4 バックボーンを使用して、マルチキャスト対応のプライベート IPv6 ネットワークをカスタマーに提供できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。



第 17 章

マルチキャスト VPN エクストラネットサポートの設定

mVPN エクストラネットサポートの設定に関する制限事項

- マルチネット VPN（MVPNv6）エクストラネットサポート機能は、Protocol Independent Multicast（PIM）スパースモード（PIM-SM）と Source Specific Multicast（SSM）トラフィックをサポートします。PIM デンスモード（PIM-DM）および双方向 PIM（Bidir-PIM）トラフィックはサポートされません。
- PIM-SM 環境で mVPN エクストラネットを設定する場合、送信元とランデブーポイント（RP）は、同じプロバイダエッジ（PE）ルータの背後にある mVPN の同じサイトに存在する必要があります。
- IPV6 ベースの mVPN エクストラネットはサポートされていません。

mVPN エクストラネットサポートについて

mVPNエクストラネットサポート機能は、ある企業サイトから他の企業サイトに送信されたIPマルチキャストコンテンツをサービスプロバイダーが配信できるようにします。この機能により、サービスプロバイダーは、次世代の柔軟なエクストラネットサービスを提供でき、異なるエンタープライズVPNカスタマー間でのビジネスパートナーシップの実現を支援します。サー

ビスプロバイダーは、短期契約、年次契約、ローリング契約など、さまざまなビジネスパートナーシップ要件を満たすマルチキャスト エクストラネット契約を提供できます。

エクストラネットは、企業外部のユーザーに拡張された企業イントラネットの一部と見なすことができます。この機能では、カスタマーおよび企業に製品やコンテンツを販売する手段、また他の企業とビジネスを行う手段として VPN が使用されます。エクストラネットは、企業などのサイトを外部のビジネスパートナーやサプライヤに繋げて、ビジネス情報や業務の一部を安全に共有するための VPN です。 mVPN エクストラネットサポート機能により、企業間およびサービスプロバイダーやコンテンツプロバイダーから別の企業 VPN カスタマーへの効率的なコンテンツ配信が可能になります。

マルチプロトコル ラベル スイッチング（MPLS）VPN は、本質的なセキュリティを提供し、ユーザーが適切な情報にのみアクセスできるようにします。MPLS VPN エクストラネットサービスは企業データの完全性に妥協することなく、エクストラネットユーザーに対してユニキャスト接続を提供します。mVPN エクストラネットサポート機能では、このユニキャスト接続が拡張され、興味に基づくコミュニティへのマルチキャスト接続も追加されます。

mVPN エクストラネットサポートの概要

ユニキャストの場合、ルーティングの観点からイントラネットとエクストラネットに違いはありません。つまり、VRF がプレフィックスをインポートすると、そのプレフィックスはラベルスイッチドパス（LSP）を介して到達可能になります。企業がプレフィックスを所有している場合、プレフィックスは企業イントラネットの一部と見なされます。プレフィックスを所有していない場合は、はエクストラネットの一部と見なされます。ただし、マルチキャストの場合、プレフィックスの到達可能性（特に LSP を介した）は、マルチキャスト配信ツリー（MDT）を構築するには不十分です。

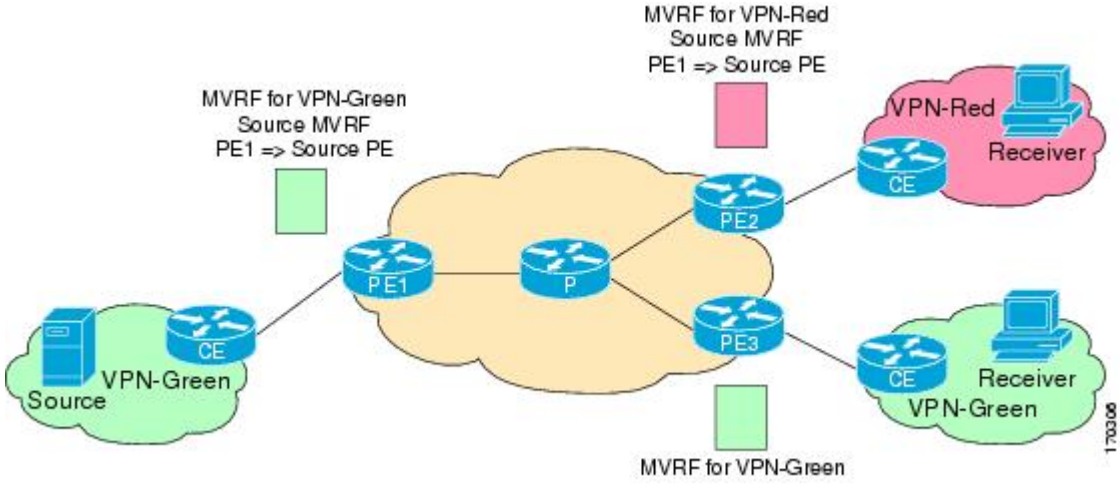
mVPN エクストラネットサービスのサポートを提供するには、送信元および受信先のマルチキャスト VPN ルーティングおよび転送（MVRF）で同じデフォルト MDT グループを設定する必要があります。

mVPN エクストラネットサポート機能では、受信先および送信元の MVRF マルチキャストルート（mroute）エントリがリンクされています。リバースパスフォワーディング（RPF）チェック機能は、ユニキャストルーティング情報に基づいて、送信元に到達可能なインターフェイスを決定します。このインターフェイスは、RPF インターフェイスとして使用されます。

mVPN エクストラネットのコンポーネント

次の図に、mVPN エクストラネットを構成するコンポーネントを示します。

図 *26 : mVPN* エクストラネットのコンポーネント



- MVRF：MVRF はマルチキャスト対応の VRF です。VRF は、IP ルーティング テーブル、取得されたルーティング テーブル、そのルーティング テーブルを使用する一連のインターフェイス、ルーティング テーブルに登録されるものを決定する一連のルールおよびルーティング プロトコルで構成されています。一般に、VRF には、プロバイダ エッジ（PE）ルータに付加されるカスタマー VPN サイトが定義されたルーティング情報が格納されています。
- 送信元 MVRF：直接接続されたカスタマーエッジ（CE）ルータを使用して送信元に到達できる MVRF。
- 受信 MVRF：受信先が 1 つまたは複数の CE デバイスを介して接続される MVRF。
- 送信元 PE：直接接続された CE ルータの背後にマルチキャスト送信元が存在する PE ルータ。
- 受信 PE：直接接続された CE ルータの背後に 1 つ以上の該当する受信先を持つ PE ルータ。

mVPN エクストラネットサポートの設定

次の mVPN エクストラネットサービス設定オプションを使用できます。

- オプション 1：受信 PE ルータでの送信元 MVRF の設定。
- オプション 2：送信元 PE ルータでの受信側 MVRF の設定。

mVPN エクストラネットサポート設定（オプション 1）

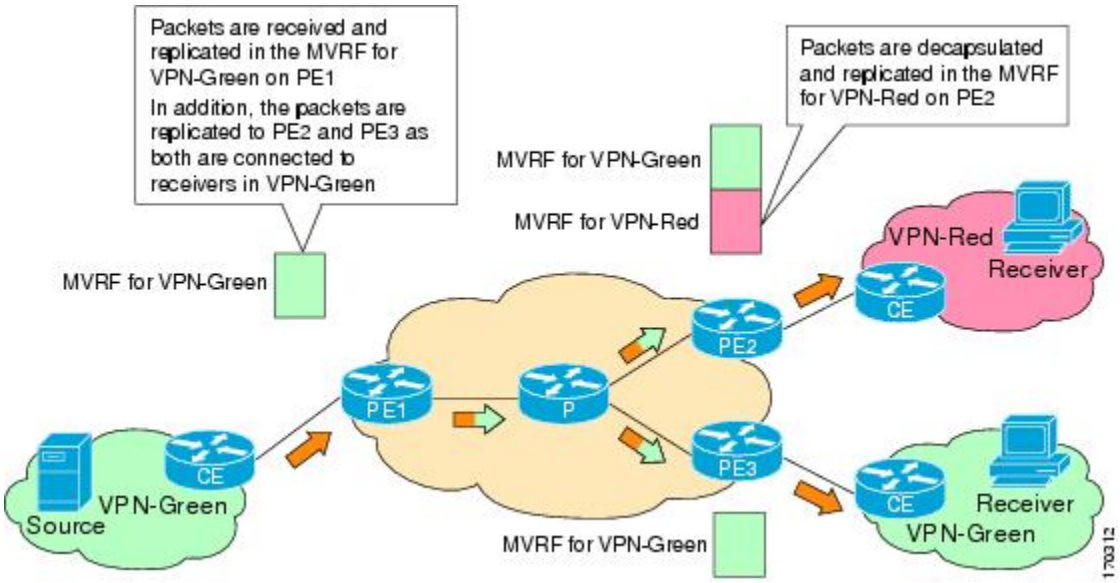
受信側 PE ルータで送信元 MVRF を設定すると、エンタープライズ VPN カスタマーに mVPN エクストラネットサービスを提供できます。

- MVRF が設定されていない場合、直接接続された CE ルータの背後のエクストラネットサイトに 1 つ以上の受信先が存在する受信側 PE ルータで、マルチキャスト送信元に接続されたサイトと同じデフォルト MDT グループを持つ MVRF を追加設定します。
- 送信元 MVRF から受信側 MVRF へのルートをインポートするために同じユニキャスト ルーティング ポリシーを設定します。

エクストラネット MVPN トポロジのマルチキャストトラフィックのフローを次の図に示します。送信元 MVRF は受信側 PE ルータで設定されています（オプション 1）。このトポロジでは、MVRF は、PE2（受信側 PE ルータ）上で VPN-Green および VPN-Red 用に設定されています。PE1 の背後にあるマルチキャスト送信元（送信元 PE ルータ）は、VPN-Green の MVRF にマルチキャストストリームを送信しています。該当する受信先は、PE2（VPN-Red の 受信側 PE ルータ）の背後および PE3（VPN-Green の受信側 PE ルータ）の背後に存在します。PE1 は VPN-Green の MVRF の送信元からパケットを受信すると、パケットを複製して PE2 と PE3 に転送します。両方のルータが VPN-Green の受信先に接続されているためです。VPN-Green から発信されたパケットは、PE2 で複製され、VPN-Red の該当する受信先に転送されます。また、PE3 で複製され、VPN-Green の該当する受信先に転送されます。

受信側 PE ルータで送信元 MVRF を設定する際、送信元 MVRF の MDT グループ設定は、送信元と受信側 PE ルータの両方で同じにする必要があります。また、送信元 MVRF（VPN-Green の MVRF）から受信側 MVRF（VPN-Red の MVRF）にルートをインポートするためには、同じユニキャスト ルーティング ポリシーを設定する必要があります。

図 *27 : mVPN* エクストラネットサポート設定オプション *1* のパケットフロー



mVPN エクストラネットサポート設定（オプション 2）

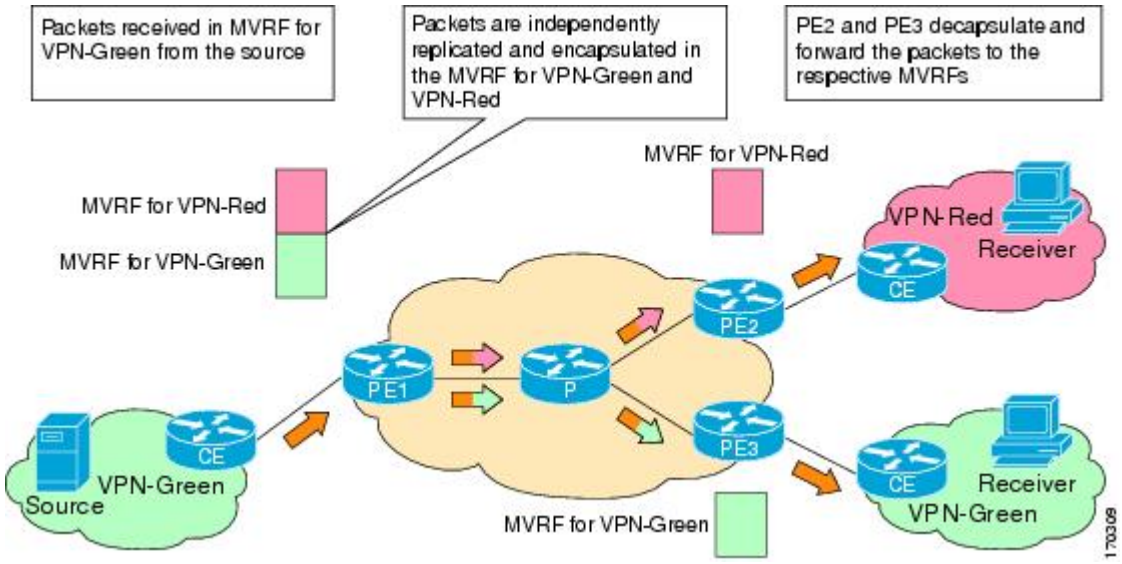
送信元 PE ルータで受信側 MVRF を設定すると、エンタープライズ VPN カスタマーに mVPN エクストラネットサービスを提供できます。

- 各エクストラネットサイトでは、MVRF が送信元 PE で設定されていない場合、受信側 MVRF と同じデフォルト MDT グループが割り当てられている送信元 PE ルータで、追加の MVRF を設定する必要があります。
- 送信元 MVRF から受信側 MVRF にルートをインポートするためには、受信側 MVRF の設定で送信元と受信側 PE ルータに同じユニキャスト ルーティング ポリシーを設定する必要があります。

受信側 MVRF が送信元 PE ルータ上で設定されている（オプション 2）mVPN エクストラネットトポロジのマルチキャストトラフィックのフローを次の図に示します。このトポロジでは、MVRF は、PE1（送信元 PE ルータ）上で VPN-Green および VPN-Red 用に設定されています。PE1 の背後のマルチキャスト送信元は、PN-Green の MVRF にマルチキャストストリームを送信し、PE2 と PE3（それぞれ VPN-Red と VPN-Green の受信側 PE ルータ）の背後に対象となる受信先があります。PE1 は、VPN-Green の MVRF の送信元からパケットを受信すると、VPN-Green および VPN-Red の MVRF でパケットを個別に複製およびカプセル化してから転送します。この送信元からのパケットを受信すると、PE2 と PE3 はパケットのカプセル化を解除し、それぞれの MVRF に転送します。

送信元 PE ルータで受信側 MVRF を設定する際、受信側 MVRF の設定では、送信元と受信側 PE ルータの両方で、デフォルトの MDT グループを同じにする必要があります。また、送信元 MVRF（VPN-Green の MVRF）から受信側 MVRF（VPN-Red の MVRF）にルートをインポートするためには、同じユニキャスト ルーティング ポリシーを設定する必要があります。

図 *28 : mVPN* エクストラネットサポート設定オプション *2* のパケットフロー



インポートされたルートを使用した mVPN エクストラネットサポート向けの RPF

エクストラネットリンクを作成するには、送信元 PE ルータで受信 MVRF を設定するか（オプション 1）、受信 PE ルータで送信元 MVRF を設定する（オプション 2）必要があります。設

定が完了すると、RPFはユニキャストルーティング情報に基づいて、送信元に到達可能なインターフェイスを決定します。このインターフェイスは、RPFインターフェイスとして使用されます。RPF解決には追加設定は必要ありません。mVPNエクストラネットサポート機能は、任意のVRFから別のVRF、VRFからグローバルルーティングテーブル、およびグローバルルーティングテーブルからVRFへのRPFをサポートします。

静的 mroutes を使用した mVPN エクストラネットサポート向けの RPF

デフォルトでは、mVPNエクストラネットはRPFインターフェイスを決定する際にユニキャストルーティングポリシーに依存します。RPFルックアップが受信先のMVRFで開始され、RPFインターフェイスが同じMVRFにないことが判明した場合、ルータはボーダーゲートウェイプロトコル（BGP）のインポートルートの情報を使用して送信元MVRFを決定します。RPFルックアップは、引き続きソースMVRFで解決します。マルチキャストトポロジとユニキャストトポロジが一致しない場合、受信先MVRFに静的mrouteを設定してデフォルトの動作を無効にし、**fallback-lookup**キーワードおよび**vrf** *vrf-name*のキーワードと引数とともに**ip mroute**コマンドを使用して、ソースMVRFを明示的に指定します。

送信元がMVRFにあり、受信先がグローバルテーブルにある場合、静的mrouteを設定して、mVPNエクストラネットのRPFをサポートすることもできます。この場合、BGPはVPNv4ルートのIPv4ルーティングテーブルへのインポートを許可しないので、ユニキャストは、RPFルックアップを解決するために必要なソースMVRFの情報を取得できません。このような場合にRPFルックアップを解決できるようにするには、**fallback-lookup**キーワードと**global**キーワードを指定した **ip mroute** コマンドを使用して、送信元MVRFを明示的に指定するように静的mrouteを設定します。

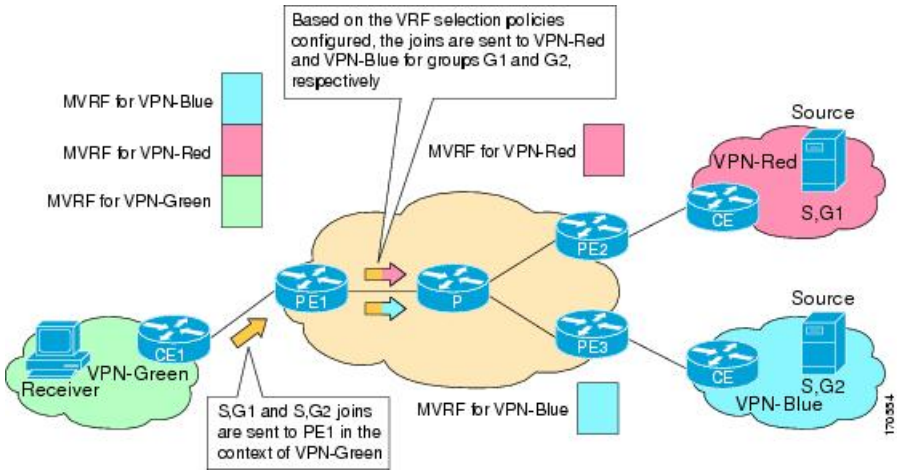
mVPN エクストラネットの VRF の選択

mVPNエクストラネットのVRF選択機能は、VRFセレクタとしてグループアドレスを使用して、異なるVRFで同じソースアドレスに対してRPFルックアップを実行するための機能を提供します。この機能は、異なるmVPNから入ってきたコンテンツストリームをサービスプロバイダーが再配布できるようにすることによってmVPNエクストラネットを強化します。

mVPNのVRF選択機能は、グループベースのVRF選択ポリシーを作成して設定します。グループベースのVRF選択ポリシーは、**ip multicast rpf select**コマンドを使用して設定します。**ip multicast rpf select**コマンドを使用すると、受信側MVRFまたはグローバルルーティングテーブルでRPFルックアップが開始された場合、グループアドレスに基づいて、送信元MVRFまたはグローバルルーティングテーブルで解決されるように設定できます。アクセスコントロールリスト（ACL）は、グループベースのVRF選択ポリシーに適用するグループを定義するために使用します。

次の図は、mVPN VRF選択機能が設定されたmVPNエクストラネットトポロジを示しています。このトポロジでは、VPN-Green（受信側VRF）から発信される(S, G1)および(S, G2) PIM加入は、PE1（受信側PE）に転送されます。設定されたグループベースのVRF選択ポリシーに基づいて、PE1は、PIM加入をG1およびG2の各グループのVPN-RedとVPN-Blueに送信します。

図 *29* : グループベースの *VRF* 選択ポリシーを使用した *RPF* ルックアップ



mVPN エクストラネットサポートの設定方法

mVPN サポートの設定

IPv4 コアネットワークで mVPN エクストラネット機能を提供するには、次の作業のいずれかを実行します。

受信側 PE での送信元 MVRF の設定（オプション 1）

受信側 PE ルータで送信元 MVRF を設定し（オプション 1）、mVPN エクストラネットサービスのサポートを提供するには、次の手順を行います。

始める前に

このタスクを実行する前に、送信元および受信側 VPN でイントラネット VPN を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target import** *route-target-ext-community*
6. **mdt default** *group-address*
7. **end**
8. **show ip mroute** [**vrf** *vrf-name*] *group-address*
9. **show platform software fed switch** {*switch-number* | **active** | **standby** } **ip multicast groups** [**vrf-id** *vrf-id* | **vrf-name** *vrf-name*] [*group-address* | **count** | **summary**]

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	**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	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition VPN-Red`	VRF 名を割り当て、VRF コンフィギュレーション モードを開始することにより、VPN ルーティング インスタンスを定義します。 • *vrf-name* 引数は、VRF に割り当てる名前です。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 55:1111`	ルーティング テーブルと転送テーブルを作成します。 • *route-distinguisher* 引数によって、8 バイトの値が IPv4 プレフィックスに追加され、VPN IPv4 プレフィックスが作成されます。RD は、次のいずれかの形式で入力できます。 • 16 ビット自律システム番号：101:3 などの 32 ビット数値 • 32 ビットの IP アドレス:16 ビットの番号。192.168.122.15:1 など。
ステップ 5	**route-target import** *route-target-ext-community* 例： `Device(config-vrf)# route-target import 55:1111`	VRF 用にルート ターゲット拡張コミュニティを作成します。 • **import** キーワードを使用すると、ルーティング情報がターゲット VPN 拡張コミュニティにエクスポートされます。 • *route-target-ext-community* 引数により、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。

	コマンドまたはアクション	目的
		（注） ソース MVRF からレシーバ MVRF に配信するコンテンツの場合、ソースおよびレシーバ PE ルータに同じユニキャストルーティング ポリシーを設定し、ソース VRF からレシーバ VRF へのルートをインポートする必要があります。
ステップ 6	**mdt default** *group-address* 例： `Device(config-vrf)# mdt default 232.1.1.1`	VRF に、データ MDT グループのマルチキャスト グループ アドレスの範囲を設定します。 • このコマンドによって、トンネルインターフェイスが作成されます。 • デフォルトでは、トンネルヘッダーの宛先アドレスは、*group-address* 引数です。
ステップ 7	**end** 例： `Device(config-vrf)# end`	VRF 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。
ステップ 8	**show ip mroute** [**vrf** *vrf-name*] *group-address* 例： `Device# show ip mroute 232.1.1.1`	（任意）特定のグループ アドレスの IP マルチキャスト mroute テーブルの内容を表示します。
ステップ 9	**show platform software fed switch** {*switch-number* | **active** | **standby** } **ip multicast groups** [**vrf-id** *vrf-id* | **vrf-name** *vrf-name*] [*group-address* | **count** | **summary**] 例： `Device# show platform software fed switch active ip multicast groups 232.3.3.3/32`	（任意）特定のマルチキャストグループに関連する情報を表示します。

送信元 PE での受信側 MVRF の設定（オプション 2）

送信元 PE ルータで受信側 MVRF を設定し（オプション 2）、mVPN エクストラネットサービスのサポートを提供するには、次の手順を行います。

始める前に

このタスクを実行する前に、送信元および受信側 VPN でイントラネット VPN を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target import** *route-target-ext-community*
6. **mdt default** *group-address*
7. **end**
8. **show ip mroute** [**vrf** *vrf-name*] *group-address*

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	**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	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition VPN-Red`	VRF 名を割り当て、VRF コンフィギュレーション モードを開始することにより、VPN ルーティング インスタンスを定義します。 • *vrf-name* 引数は、VRF に割り当てる名前です。

ステップ 4	**rd** *route-distinguisher*
	例：
	`Device(config-vrf)# rd 55:2222`
		ルーティング テーブルと転送テーブルを作成します。
		• VPN IPv4 プレフィックスを作成するために、*route-distinguisher* 引数を指定して、IPv4 プレフィックスに 8 バイト値を追加します。RD は、次のいずれかの形式で入力できます。
		  • 16 ビット自律システム番号：101:3 などの 32 ビット数値
		  • 32 ビットの IP アドレス:16 ビットの番号。192.168.122.15:1 など。

ステップ 5	**route-target import** *route-target-ext-community* 例：	VRF 用にルート ターゲット拡張コミュニティを作成します。

	コマンドまたはアクション	目的
	`Device(config-vrf)# route-target import 55:1111`	• **import** キーワードを使用すると、ターゲット VPN 拡張コミュニティからルーティング情報がインポートされます。 • *route-target-ext-community* 引数により、route-target 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の route-target 拡張コミュニティの VRF リストに追加されます。 （注） ソース MVRF からレシーバ MVRF に配信するコンテンツの場合、ソースおよびレシーバ PE ルータに同じユニキャストルーティング ポリシーを設定し、ソース VRF からレシーバ VRF へのルートをインポートする必要があります。
ステップ 6	**mdt default** *group-address* 例： `Device(config-vrf)# mdt default 232.3.3.3`	VRF に、データ MDT グループのマルチキャスト グループ アドレスの範囲を設定します。 • このコマンドによって、トンネルインターフェイスが作成されます。 • デフォルトでは、トンネルヘッダーの宛先アドレスは、*group-address* 引数です。
ステップ 7	**end** 例： `Device(config-vrf)# end`	VRF 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。
ステップ 8	**show ip mroute** [**vrf** *vrf-name*] *group-address* 例： `Device# show ip mroute 232.3.3.3`	（任意）特定のグループ アドレスの IP マルチキャスト mroute テーブルの内容を表示します。

静的 Mroute を使用した MVPN エクストラネットサポート向けの RPF の設定

始める前に

このタスクを実行する前に、mVPNエクストラネットサービスのサポートを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip mroute vrf** *vrf-name source-address mask* **fallback-lookup** {**global** | **vrf** *vrf-name*} [*distance*]
4. **end**
5. **show ip mroute** [**vrf** *vrf-name*] *group-address*

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	**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	**ip mroute vrf** *vrf-name source-address mask* **fallback-lookup** {**global** | **vrf** *vrf-name*} [*distance*] 例： `Device(config)# ip mroute vrf VPN-Red 224.100.0.5 255.255.255.255 fallback-lookup vrf VPN-Green`	スタティック mroute を使用して、レシーバ MVRF で発生する RPF ルックアップがソース MVRF またはグローバル ルーティング テーブルで継続され、解決されるように設定します。 • **global** キーワードを使用すると、送信元 MVRF がグローバル ルーティング テーブルにあることを定義できます。 • VRF を送信元 MVRF として明示的に定義するには、**vrf** キーワード と *vrf-name* 引数を使用します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル 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 5	**show ip mroute** [**vrf** *vrf-name*] *group-address* 例： `Device# show ip mroute 224.100.0.5`	（任意）特定のグループ アドレスの IP マルチキャスト mroute テーブルの内容を表示します。

mVPN エクストラネットにおけるグループベースの VRF 選択ポリシーの設定

mVPN でグループベースの VRF 選択ポリシーを設定するには、次の作業を実行します。

この作業を実行すると、VRF セレクタとしてグループ アドレスを使用して、異なる VRF にある同じソース アドレスに対して、RPF ルックアップを実行できます。

始める前に

- このタスクを実行する前に、mVPNエクストラネットサービスのサポートを設定する必要があります。
- グループベースの VRF 選択ポリシーに適用する ACL を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast** [**vrf** *receiver-vrf-name*] **rpf select** {**global** | **vrf** *source-vrf-name*} **group-list** *access-list*
4. 追加のグループベースの VRF 選択ポリシーを作成するには、ステップ 3 を繰り返します。
5. **end**
6. **show ip**} **rpf** [**vrf** *vrf-name*] **select**
7. **show ip rpf** [**vrf** *vrf-name*] *source-address* [*group-address*]

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	**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	**ip multicast** [**vrf** *receiver-vrf-name*] **rpf select** {**global** | **vrf** *source-vrf-name*} **group-list** *access-list* 例： `Device(config)# ip multicast vrf VPN-Green rpf select vrf VPN-Red group-list 1`	• レシーバ MVRF またはグローバル ルーティング テーブルで発生する RPF ルックアップが、ソース MVRF またはグループ アドレス ベースのグローバル ルーティング テーブルで解決されるように設定します。
ステップ 4	追加のグループベースの VRF 選択ポリシーを作成するには、ステップ 3 を繰り返します。	--

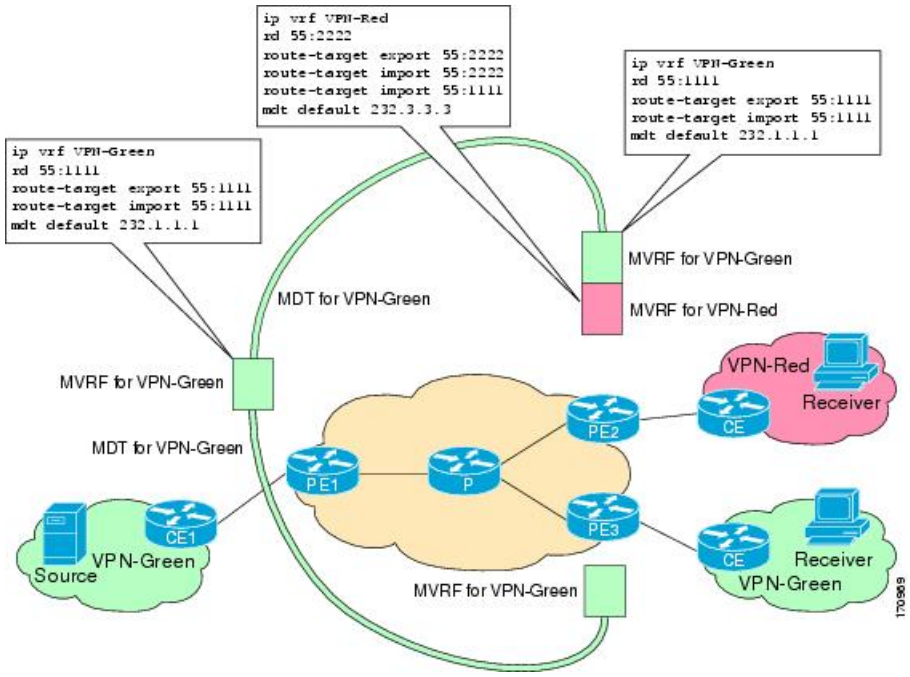
	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 6	**show ip} rpf** [**vrf** *vrf-name*] **select** 例： `Device# show ip rpf select`	グループから VRF へのマッピング情報を表示します。
ステップ 7	**show ip rpf** [**vrf** *vrf-name*] *source-address* [*group-address*] 例： `Device# show ip rpf 172.16.10.13`	IP マルチキャスト ルーティングで RPF を行う方法に関する情報を表示します。 • グループアドレスに基づいて RPF ルックアップが実行されていることを確認し、RPF ルックアップが実行されている VRF を表示するには、グループベースの VRF 選択ポリシーを設定した後に、このコマンドを使用します。

mVPN エクストラネットサポートの設定例

例：受信側 PE ルータでの送信元 VRF の設定（オプション 1）

次の設定例は、図に示す mVPN エクストラネットトポロジに基づいています。この例は、PE2（受信側 PE ルータ）および PE1（送信元 PE ルータ）の設定を示します。この例では、mVPN エクストラネットサービスは、PE2 の VPN-Green に送信元 MVRF を設定することによって、VPN-Green と VPN-Red の間でサポートされます。同じユニキャスト ルーティング ポリシーは、VPN-Green から VPN-Red へのルートをインポートするように設定されます。

図 *30 : mVPN* エクストラネット サポート オプション *1* 設定例のトポロジ



PE2 の設定

```
ip cef
!
vrf definition VPN-Red
 rd 55:2222
 route-target export 55:2222
 route-target import 55:2222
 route-target import 55:1111
 mdt default 232.3.3.3
!
vrf definition VPN-Green
 rd 55:1111
 route-target export 55:1111
 route-target import 55:1111
 mdt default 232.1.1.1
!
ip multicast-routing
ip multicast-routing vrf VPN-Red
ip multicast-routing vrf VPN-Green
!
interface Loopback0
 ip address 10.2.0.2 255.255.255.0
 ip pim sparse-dense-mode
!
.
.
.
!
router bgp 55
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.1.0.1 remote-as 55
```

```
 neighbor 10.1.0.1 update-source Loopback0
 !
 address-family ipv4 mdt
 neighbor 10.1.0.1 activate
 neighbor 10.1.0.1 send-community extended
 !
 address-family vpnv4
 neighbor 10.1.0.1 activate
 neighbor 10.1.0.1 send-community extended
 !
```

PE1 の設定

```
ip cef
!
vrf definition VPN-Green
 rd 55:1111
 route-target export 55:1111
 route-target import 55:1111
 mdt default 232.1.1.1
!
ip multicast-routing
ip multicast-routing vrf VPN-Green
!
interface Loopback0
 ip address 10.1.0.1 255.255.255.0
 ip pim sparse-dense-mode
!
.
.
.
!
router bgp 55
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.2.0.2 remote-as 55
 neighbor 10.2.0.2 update-source Loopback0
 !
 address-family ipv4 mdt
 neighbor 10.2.0.2 activate
 neighbor 10.2.0.2 send-community extended
 !
 address-family vpnv4
 neighbor 10.2.0.2 activate
 neighbor 10.2.0.2 send-community extended
 !
```

MDT デフォルト グループ 232.1.1.1 の PE1 および PE2 のグローバル テーブルでの状態

PE1 および PE2 で **show ip mroute** コマンドを実行した場合の出力例を以下に示します。サンプル出力は、PE1 と PE2 での MDT デフォルト グループ 232.1.1.1 のグローバル テーブルを示しています。

```
Device# show ip mroute 232.1.1.1
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
```

```
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(10.2.0.2, 232.1.1.1), 00:01:19/00:02:42, flags: sTIZ
  Incoming interface: Ethernet0/0, RPF nbr 10.0.1.4
  Outgoing interface list:
    MVRF VPN-Green, Forward/Sparse-Dense, 00:01:19/00:02:07
(10.1.0.1, 232.1.1.1), 00:02:19/00:03:11, flags: sT
  Incoming interface: Loopback0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0/0, Forward/Sparse-Dense, 00:02:00/00:02:36
Device# show ip mroute 232.1.1.1
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(10.1.0.1, 232.1.1.1), 00:02:04/00:02:38, flags: sTIZ
  Incoming interface: Ethernet1/0, RPF nbr 10.0.2.4
  Outgoing interface list:
    MVRF VPN-Green, Forward/Sparse-Dense, 00:02:04/00:02:09
(10.2.0.2, 232.1.1.1), 00:02:04/00:03:09, flags: sT
  Incoming interface: Loopback0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet1/0, Forward/Sparse-Dense, 00:01:22/00:03:09
```

PE1 および PE2 が mVPN エクストラネットサポート用に設定されている場合の MDT デフォルトグループ 232.1.1.1 の PE1 および PE2 のグローバルテーブルの状態

```
Device# show ip mroute 232.1.1.1
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(10.2.0.2, 232.1.1.1), 00:01:19/00:02:42, flags: sTIZ
  Incoming interface: GigabitEthernet2/16, RPF nbr 10.0.1.4, RPF-MFD
  Outgoing interface list:
    MVRF VPN-Green, Forward/Sparse-Dense, 00:01:19/00:02:07, H
(10.1.0.1, 232.1.1.1), 00:02:19/00:03:11, flags: sT
  Incoming interface: Loopback0, RPF nbr 0.0.0.0, RPF-MFD
  Outgoing interface list:
    GigabitEthernet2/16, Forward/Sparse-Dense, 00:02:00/00:02:36, H
Device# show ip mroute 232.1.1.1
IP Multicast Routing Table
```

```
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(10.1.0.1, 232.1.1.1), 00:02:04/00:02:38, flags: sTIZ
  Incoming interface: GigabitEthernet4/1, RPF nbr 10.0.2.4, RPF-MFD
  Outgoing interface list:
    MVRF VPN-Green, Forward/Sparse-Dense, 00:02:04/00:02:09, H
(10.2.0.2, 232.1.1.1), 00:02:04/00:03:09, flags: sT
  Incoming interface: Loopback0, RPF nbr 0.0.0.0, RPF-MFD
  Outgoing interface list:
    GigabitEthernet4/1, Forward/Sparse-Dense, 00:01:22/00:03:09, H
```

VPN-Red の受信先がマルチキャストグループ 228.8.8.8 に加入した後の PE1 の VPN-Green に設定された VRF テーブルの状態

PE 1 で **show ip mroute** コマンドを実行した場合の出力例を以下に示します。サンプル出力は、レシーバがマルチキャスト グループ 228.8.8.8 に加入したときの PE1 の VPN-Green の VRF テーブルの状態を示しています。

```
Device# show ip mroute vrf VPN-Green 228.8.8.8
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.8.8.8), 00:01:43/00:02:52, RP 10.100.0.5, flags: S
  Incoming interface: Ethernet3/0, RPF nbr 10.1.1.5
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 00:01:43/00:02:52
(10.1.1.200, 228.8.8.8), 00:01:15/00:03:26, flags: T
  Incoming interface: Ethernet3/0, RPF nbr 10.1.1.5
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 00:01:15/00:03:19
```

VPN-Red の受信先がマルチキャストグループ 228.8.8.8 に加入した後の PE1 の VPN-Green に設定された VRF テーブルの状態（PE1 が mVPN エクストラネットサポート向けに設定されたスイッチの場合）

```
Device# show ip mroute vrf VPN-Green 228.8.8.8
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
```

```
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.8.8.8), 00:01:43/00:02:52, RP 10.100.0.5, flags: S
  Incoming interface: GigabitEthernet3/1, RPF nbr 10.1.1.5, RPF-MFD
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 00:01:43/00:02:52, H
(10.1.1.200, 228.8.8.8), 00:01:15/00:03:26, flags: T
  Incoming interface: GigabitEthernet3/1, RPF nbr 10.1.1.5, RPF-MFD
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 00:01:15/00:03:19, H
```

VPN-Red のレシーバのマルチキャスト グループ 228.8.8.8 への加入後の PE2 の VPN-Green の VRF テーブルにおける状態

PE 2 で **show ip mroute** コマンドを実行した場合の出力例を以下に示します。この出力は、受信先がマルチキャストグループ 228.8.8.8 に加入したときの PE1 上にある VPN-Green の VRF テーブルの状態を示しています。この出力は、VPN-Red のエクストラネット受信先が、VPN-Green の送信元からコンテンツを受信していることを示しています。VPN-Green がマルチキャストグループ 228.8.8.8 にコンテンツを送信 しています。「E」フラグは、VRF ルーティングテーブル内の (*, G) や (S, G) エントリが送信元 VRF エントリで、エクストラネット受信先 MVRF mroute エントリがリンクされていることを示しています。

```
Device# show ip mroute vrf VPN-Green 228.8.8.8
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.8.8.8), 00:01:59/stopped, RP 10.100.0.5, flags: SE
  Incoming interface: Tunnel0, RPF nbr 10.1.0.1
  Outgoing interface list: Null
  Extranet receivers in vrf VPN-Red:
(*, 228.8.8.8), 00:01:59/stopped, RP 10.100.0.5, OIF count: 1, flags: S
(10.1.1.200, 228.8.8.8), 00:01:31/00:02:59, flags: TE
  Incoming interface: Tunnel0, RPF nbr 10.1.0.1
  Outgoing interface list: Null
  Extranet receivers in vrf VPN-Red:
  (10.1.1.200, 228.8.8.8), 00:01:31/00:03:29, OIF count: 1, flags:
```

VPN-Red の受信先がマルチキャストグループ 228.8.8.8 に加入した後の PE2 の VPN-Green に設定された VRF テーブルの状態（PE2 が mVPN エクストラネットサポート向けに設定されたスイッチの場合）

```
Device# show ip mroute vrf VPN-Green 228.8.8.8
IP Multicast Routing Table
```

```
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.8.8.8), 00:01:59/stopped, RP 10.100.0.5, flags: SE
  Incoming interface: Tunnel0, RPF nbr 10.1.0.1, RPF-MFD
  Outgoing interface list: Null
  Extranet receivers in vrf VPN-Red:
(*, 228.8.8.8), 00:01:59/stopped, RP 10.100.0.5, OIF count: 1, flags: S
(10.1.1.200, 228.8.8.8), 00:01:31/00:02:59, flags: TE
  Incoming interface: Tunnel0, RPF nbr 10.1.0.1, RPF-MFD
  Outgoing interface list: Null
  Extranet receivers in vrf VPN-Red:
  (10.1.1.200, 228.8.8.8), 00:01:31/00:03:29, OIF count: 1, flags:
```

VPN-Red の受信先がマルチキャストグループ 228.8.8.8 に加入した後の PE2 の VPN-Red に設定された VRF テーブルの状態

PE 2 で **show ip mroute** コマンドを実行した場合の出力例を以下に示します。この出力例は、受信先がマルチキャストグループ 228.8.8.8 に加入したときの PE2 上にある VPN-Red の VRF テーブルの状態を示しています。「using vrf VPN-Green」フィールドは、送信元が到達可能な RPF インターフェイスを決定するために、VPN-Red が VPN-Green からのユニキャストルーティング情報を使用していることを示しています。

```
Device# show ip mroute vrf VPN-Red 228.8.8.8

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.8.8.8), 00:02:00/stopped, RP 10.100.0.5, flags: S
  Incoming interface: Tunnel0, RPF nbr 10.1.0.1, using vrf VPN-Green
  Outgoing interface list:
    Ethernet9/0, Forward/Sparse-Dense, 00:02:00/00:02:34
(10.1.1.200, 228.8.8.8), 00:01:32/00:03:28, flags:
  Incoming interface: Tunnel0, RPF nbr 10.1.0.1, using vrf VPN-Green
  Outgoing interface list:
    Ethernet9/0, Forward/Sparse-Dense, 00:01:32/00:03:01
```

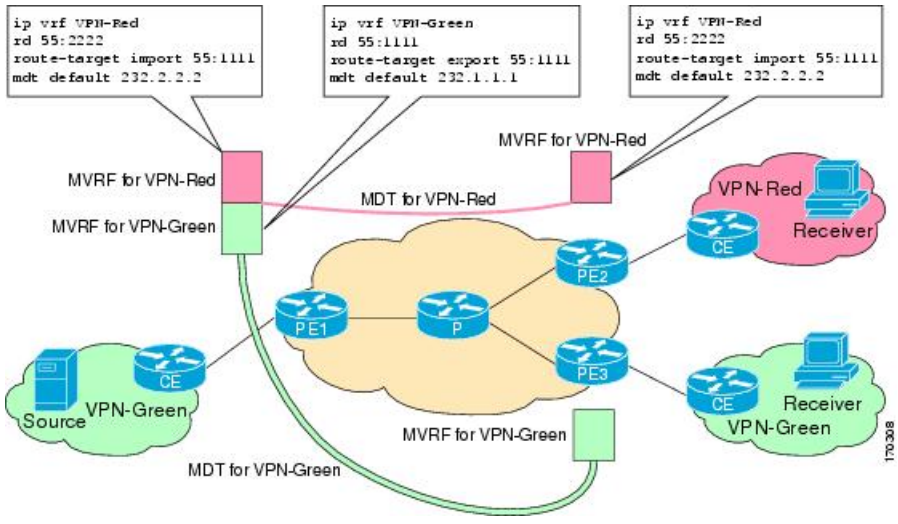
VPN-Red の受信先がマルチキャストグループ **228.8.8.8** に加入した後の **PE2** の **VPN-Red** に設定された **VRF** テーブルの状態（**PE2** が **mVPN** エクストラネットサポート向けに設定されたスイッチの場合）

```
Device# show ip mroute vrf VPN-Red 228.8.8.8
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.8.8.8), 00:02:00/stopped, RP 10.100.0.5, flags: S
  Incoming interface: Tunnel0, RPF nbr 10.1.0.1, using vrf VPN-Green, RPF-MFD
  Outgoing interface list:
    GigabitEthernet9/1, Forward/Sparse-Dense, 00:02:00/00:02:34, H
(10.1.1.200, 228.8.8.8), 00:01:32/00:03:28, flags:
  Incoming interface: Tunnel0, RPF nbr 10.1.0.1, using vrf VPN-Green, RPF-MFD
  Outgoing interface list:
    GigabitEthernet9/1, Forward/Sparse-Dense, 00:01:32/00:03:01, H
```

例：送信元 PE ルータでの受信側 VRF の設定（オプション 2）

次の図は、PE1（送信元 PE ルータ）と PE2（受信側 PE ルータ）の設定例を示しています。この例では、mVPN エクストラネットサービスは、送信元 PE ルータである PE1 の VPN-Red に受信側 MVRF を設定することによって、VPN-Green と VPN-Red の間でサポートされます。VPN-Red の MVRF を設定すると、VPN-Green の MVRF から VPN-Red の MVRF にルートをインポートするように設定されます。

図 *31 : mVPN* エクストラネット サポート オプション *2* 設定例のトポロジ



PE1 の設定

```
ip cef
!
vrf definition VPN-Green
 rd 55:1111
 route-target export 55:1111
 route-target import 55:1111
 mdt default 232.1.1.1
!
vrf definition VPN-Red
 rd 55:2222
 route-target export 55:2222
 route-target import 55:2222
 route-target import 55:1111
 mdt default 232.3.3.3
!
ip multicast-routing
ip multicast-routing vrf VPN-Green
ip multicast-routing vrf VPN-Red
!
interface Loopback0
 ip address 10.1.0.1 255.255.255.0
 ip pim sparse-dense-mode
!
.
.
.
!
router bgp 55
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.2.0.2 remote-as 55
 neighbor 10.2.0.2 update-source Loopback0
 !
 address-family ipv4 mdt
 neighbor 10.2.0.2 activate
 neighbor 10.2.0.2 send-community extended
 !
 address-family vpnv4
 neighbor 10.2.0.2 activate
 neighbor 10.2.0.2 send-community extended
 !
```

PE2 の設定

```
!
vrf definition VPN-Red
 rd 55:2222
 route-target export 55:2222
 route-target import 55:2222
 route-target import 55:1111
 mdt default 232.3.3.3
!
ip multicast-routing
ip multicast-routing vrf VPN-Red
!
interface Loopback0
 ip address 10.2.0.2 255.255.255.0
 ip pim sparse-dense-mode
!
.
```

```
.
.
!
router bgp 55
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.1.0.1 remote-as 55
 neighbor 10.1.0.1 update-source Loopback0
 !
 address-family ipv4 mdt
 neighbor 10.1.0.1 activate
 neighbor 10.1.0.1 send-community extended
 !
 address-family vpnv4
 neighbor 10.1.0.1 activate
 neighbor 10.1.0.1 send-community extended
 !
```

MDT デフォルトグループ 232.3.3.3 の PE1 および PE2 のグローバルテーブルでの状態

PE1 および PE2 で **show ip mroute** コマンドを実行した場合の出力例を以下に示します。サンプル出力は、PE1 と PE2 での MDT デフォルト グループ 232.3.3.3 のグローバル テーブルを示しています。

```
PE1# show ip mroute 232.3.3.3
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(10.1.0.1, 232.3.3.3), 00:46:27/00:03:27, flags: sT
  Incoming interface: Loopback0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0/0, Forward/Sparse-Dense, 00:45:17/00:02:44
(10.2.0.2, 232.3.3.3), 00:45:17/00:02:57, flags: sTIZ
  Incoming interface: Ethernet0/0, RPF nbr 224.0.1.4
  Outgoing interface list:
    MVRF VPN-Red, Forward/Sparse-Dense, 00:45:17/00:01:09
PE2# show ip mroute 232.3.3.3
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(10.1.0.1, 232.3.3.3), 00:45:08/00:02:37, flags: sTIZ
  Incoming interface: Ethernet1/0, RPF nbr 224.0.2.4
  Outgoing interface list:
```

```
    MVRF VPN-Red, Forward/Sparse-Dense, 00:45:08/00:01:27
(10.2.0.2, 232.3.3.3), 00:46:19/00:03:07, flags: sT
  Incoming interface: Loopback0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet1/0, Forward/Sparse-Dense, 00:45:08/00:02:49
```

PE1 および PE2 が mVPN エクストラネットサポート用に設定されている場合の MDT デフォルトグループ 232.3.3.3 の PE1 および PE2 のグローバルテーブルの状態

PE1 と PE2 が mVPN エクストラネットサービスをサポートするように設定されているスイッチの場合に、PE1 および PE2 で **show ip mroute** を実行したときの出力例を以下に示します。**show ip mroute** コマンドからの出力例は、PE1 と PE2 における MDT デフォルトグループ 232.3.3.3 のグローバルテーブルを示しています。この出力で、「RPF-MFD」フラグはマルチキャストフローが完全にハードウェアでスイッチングされることを示し、「H」フラグはフローが発信インターフェイスのハードウェアでスイッチングされることを示しています。

```
Device# show ip mroute 232.3.3.3
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(10.1.0.1, 232.3.3.3), 00:46:27/00:03:27, flags: sT
  Incoming interface: Loopback0, RPF nbr 0.0.0.0, RPF-MFD
  Outgoing interface list:
    GigabitEthernet2/16, Forward/Sparse-Dense, 00:45:17/00:02:44, H
(10.2.0.2, 232.3.3.3), 00:45:17/00:02:57, flags: sTIZ
  Incoming interface: GigabitEthernet2/16, RPF nbr 224.0.1.4, RPF-MFD
  Outgoing interface list:
    MVRF VPN-Red, Forward/Sparse-Dense, 00:45:17/00:01:09, H


Device# show ip mroute 232.3.3.3
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(10.1.0.1, 232.3.3.3), 00:45:08/00:02:37, flags: sTIZ
  Incoming interface: GigabitEthernet4/1, RPF nbr 224.0.2.4, RPF-MFD
  Outgoing interface list:
    MVRF VPN-Red, Forward/Sparse-Dense, 00:45:08/00:01:27, H
(10.2.0.2, 232.3.3.3), 00:46:19/00:03:07, flags: sT
  Incoming interface: Loopback0, RPF nbr 0.0.0.0, RPF-MFD
  Outgoing interface list:
    GigabitEthernet4/1, Forward/Sparse-Dense, 00:45:08/00:02:49, H
```

VPN-Red の受信先がマルチキャストグループ 228.8.8.8 に加入した後の PE1 の VPN-Green に設定された VRF テーブルの状態

PE 1 で **show ip mroute** コマンドを実行した場合の出力例を以下に示します。サンプル出力は、レシーバがマルチキャスト グループ 228.8.8.8 に加入したときの PE1 の VPN-Green の VRF テーブルの状態を示しています。この出力は、VPN-Red のエクストラネット受信先が、VPN-Green の送信元からコンテンツを受信していることを示しています。VPN-Green がマルチキャストグループ 228.8.8.8 にコンテンツを送信 しています。出力の「E」フラグは、VRF ルーティングテーブル内の (*, G) や (S, G) エントリが送信元 VRF エントリで、エクストラネット受信先 MVRF mroute エントリがリンクされていることを示しています。

```
Device# show ip mroute vrf VPN-Green 228.8.8.8
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.8.8.8), 00:01:38/stopped, RP 10.100.0.5, flags: SE
  Incoming interface: Ethernet3/0, RPF nbr 10.1.1.5
  Outgoing interface list: Null
  Extranet receivers in vrf VPN-Red:
(*, 228.8.8.8), 00:01:38/stopped, RP 10.100.0.5, OIF count: 1, flags: S
(10.1.1.200, 228.8.8.8), 00:00:05/00:02:54, flags: TE
  Incoming interface: Ethernet3/0, RPF nbr 10.1.1.5
  Outgoing interface list: Null
  Extranet receivers in vrf VPN-Red:
  (10.1.1.200, 228.8.8.8), 00:00:05/stopped, OIF count: 1, flags:
```

VPN-Red の受信先がマルチキャストグループ 228.8.8.8 に加入した後の PE1 の VPN-Green に設定された VRF テーブルの状態（PE1 が mVPN エクストラネットサポート向けに設定されたスイッチの場合）

PE1 がエクストラネット MVPN サービスをサポートするように設定された Catalyst 6500 シリーズ スイッチである場合に、PE1 で **show ip mroute** コマンドを実行したときの出力例を以下に示します。**show ip mroute** コマンドの出力例は、受信先がマルチキャストグループ 228.8.8.8 に加入したときの PE1 上にある VPN-Green の VRF テーブルの状態を示しています。この出力例は、VPN-Red のエクストラネット受信先が、VPN-Green の送信元からコンテンツを受信していることを示しています。VPN-Green がマルチキャストグループ 228.8.8.8 にコンテンツを送信しています。

```
Device# show ip mroute vrf VPN-Green 228.8.8.8
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
```

```
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.8.8.8), 00:01:38/stopped, RP 10.100.0.5, flags: SE
  Incoming interface: GigabitEthernet3/1, RPF nbr 10.1.1.5, RPF-MFD
  Outgoing interface list: Null
  Extranet receivers in vrf VPN-Red:
(*, 228.8.8.8), 00:01:38/stopped, RP 10.100.0.5, OIF count: 1, flags: S
(10.1.1.200, 228.8.8.8), 00:00:05/00:02:54, flags: TE
  Incoming interface: GigabitEthernet3/1, RPF nbr 10.1.1.5, RPF-MFD
  Outgoing interface list: Null
  Extranet receivers in vrf VPN-Red:
  (10.1.1.200, 228.8.8.8), 00:00:05/stopped, OIF count: 1, flags:
```

VPN-Red の受信先がマルチキャストグループ 228.8.8.8 に加入後の PE1 上にある VPN-Red の VRF テーブルの状態

PE 1 で **show ip mroute** コマンドを実行した場合の出力例を以下に示します。この出力例は、受信先がマルチキャストグループ 228.8.8.8 に加入したときの PE1 上にある VPN-Red の VRF テーブルの状態を示しています。「using vrf VPN-Green」フィールドは、送信元が到達可能な RPF インターフェイスを決定するために、VPN-Red が VPN-Green からのユニキャストルーティング情報を使用していることを示しています。

```
Device# show ip mroute vrf VPN-Red 228.8.8.8
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.8.8.8), 00:01:45/stopped, RP 10.100.0.5, flags: S
  Incoming interface: Ethernet3/0, RPF nbr 10.1.1.5, using vrf VPN-Green
  Outgoing interface list:
    Tunnel2, Forward/Sparse-Dense, 00:01:45/00:02:49
(10.1.1.200, 228.8.8.8), 00:00:12/00:03:27, flags:
  Incoming interface: Ethernet3/0, RPF nbr 10.1.1.5, using vrf VPN-Green
  Outgoing interface list:
    Tunnel2, Forward/Sparse-Dense, 00:00:12/00:03:18
```

VPN-Red の受信先がマルチキャストグループ 228.8.8.8 に加入した後の PE1 の VPN-Red に設定された VRF テーブルの状態（PE1 が mVPN エクストラネットサポート向けに設定されたスイッチの場合）

```
Device# show ip mroute vrf VPN-Red 228.8.8.8
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
```

```
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.8.8.8), 00:01:45/stopped, RP 10.100.0.5, flags: S
  Incoming interface: GigabitEthernet3/1, RPF nbr 10.1.1.5, using vrf VPN-Green, RPF-MFD

  Outgoing interface list:
    Tunnel2, Forward/Sparse-Dense, 00:01:45/00:02:49, H
(10.1.1.200, 228.8.8.8), 00:00:12/00:03:27, flags:
  Incoming interface: GigabitEthernet3/1, RPF nbr 10.1.1.5, using vrf VPN-Green, RPF-MFD

  Outgoing interface list:
    Tunnel2, Forward/Sparse-Dense, 00:00:12/00:03:18, H
```

VPN-Red の受信先がマルチキャストグループ 228.8.8.8 に加入した後の PE2 の VPN-Red に設定された VRF テーブルの状態

PE 2 で **show ip mroute** コマンドを実行した場合の出力例を以下に示します。この出力例は、受信先がマルチキャストグループ 228.8.8.8 に加入したときの PE2 上にある VPN-Red の VRF テーブルを示しています。

```
PE2# show ip mroute vrf VPN-Red 228.8.8.8
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.8.8.8), 00:00:28/stopped, RP 10.100.0.5, flags: S
  Incoming interface: Tunnel1, RPF nbr 10.1.0.1
  Outgoing interface list:
    Ethernet9/0, Forward/Sparse-Dense, 00:00:28/00:03:02
(10.1.1.200, 228.8.8.8), 00:00:00/00:03:29, flags:
  Incoming interface: Tunnel1, RPF nbr 10.1.0.1
  Outgoing interface list:
    Ethernet9/0, Forward/Sparse-Dense, 00:00:00/00:03:29
```

VPN-Red の受信先がマルチキャストグループ 228.8.8.8 に加入した後の PE2 の VPN-Red に設定された VRF テーブルの状態（PE2 が mVPN エクストラネットサポート向けに設定されたスイッチの場合）

```
PE2# show ip mroute vrf VPN-Red 228.8.8.8
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
```

```
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.8.8.8), 00:00:28/stopped, RP 10.100.0.5, flags: S
  Incoming interface: Tunnel1, RPF nbr 10.1.0.1, RPF-MFD
  Outgoing interface list:
    GigabitEthernet9/1, Forward/Sparse-Dense, 00:00:28/00:03:02, H
(10.1.1.200, 228.8.8.8), 00:00:00/00:03:29, flags:
  Incoming interface: Tunnel1, RPF nbr 10.1.0.1, RPF-MFD
  Outgoing interface list:
    GigabitEthernet9/1, Forward/Sparse-Dense, 00:00:00/00:03:29, H
```

例：mVPN エクストラネットサポートの統計情報の表示

この例はスタンドアロンの場合の例であり、他のテクノロジーにはふれていません。

MFIB ベースの IP マルチキャストを実装すると、mVPN エクストラネットの送信元 MVRF mroute エントリのカウンタが更新されます。送信元 MVRF のカウンタは、Cisco IOS コマンドを使用して表示できます。受信側の MVRF mroute エントリのカウンタはゼロのままです。

送信元と受信側の MVRF を特定するには、**show ip mroute** コマンドを使用します。次の出力例は、VRF blue が送信元 MVRF であり、VRF redが 受信側 MVRF であることを示しています。

```
Device# show ip mroute vrf blue 228.1.1.1

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.1.1.1), 00:05:48/stopped, RP 202.100.0.5, flags: SE
  Incoming interface: Ethernet3/0, RPF nbr 200.1.1.5
  Outgoing interface list: Null
  Extranet receivers in vrf red:
(*, 228.1.1.1), 00:05:48/stopped, RP 202.100.0.5, OIF count: 1, flags: S
(220.1.1.200, 228.1.1.1), 00:02:42/00:02:09, flags: TE
  Incoming interface: Ethernet3/0, RPF nbr 200.1.1.5
  Outgoing interface list: Null
  Extranet receivers in vrf red:
  (220.1.1.200, 228.1.1.1), 00:02:42/stopped, OIF count: 1, flags: T


Device# show ip mroute vrf red 228.1.1.1

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
```

```
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 228.1.1.1), 00:05:55/stopped, RP 202.100.0.5, flags: S
  Incoming interface: Ethernet3/0, RPF nbr 200.1.1.5, using vrf blue
  Outgoing interface list:
    Tunnel16, Forward/Sparse-Dense, 00:05:55/00:03:26
(220.1.1.200, 228.1.1.1), 00:02:49/stopped, flags: T
  Incoming interface: Ethernet3/0, RPF nbr 200.1.1.5, using vrf blue
  Outgoing interface list:
    Tunnel16, Forward/Sparse-Dense, 00:02:49/00:03:26
```

vrf-name 引数に送信元 MVRF を指定して **show ip mfib vrf** *vrf-name* コマンドを使用すると、統計情報が表示されます。

送信元 MVRF blue の統計情報の例を以下に示します。出力を精査して、送信元 MVRF MFIB の転送統計情報が正しく、送信元 MVRF で A および F フラグが設定されていることを確認します。MFIB にエクストラネット転送の痕跡がないか注意してください。

```
Device# show ip mfib vrf blue 228.1.1.1

Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A
flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB
Forward,
                MA - MFIB Accept
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per
second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
VRF blue
(*,228.1.1.1) Flags: C
  SW Forwarding: 1/0/100/0, Other: 0/0/0
  Ethernet3/0 Flags: A
  Tunnel16, MDT/239.3.3.3 Flags: F
    Pkts: 1/0
(220.1.1.200,228.1.1.1) Flags:
  SW Forwarding: 37/0/100/0, Other: 0/0/0
  Ethernet3/0 Flags: A NS
  Tunnel16, MDT/239.3.3.3 Flags: F
    Pkts: 37/0
```

以下の例は、受信先 MVRF red に関する次の情報を示します。

- これらの統計情報は送信元 MVRF で収集されるため、受信側 MVRF MFIB に転送統計情報はありません。
- A および F フラグは設定されていません。これらのフラグは、mVPN エクストラネットの送信元 MVRF でのみ設定されます。
- MFIB にエクストラネット転送の痕跡はありません。

（注） 出力の NS フラグは、受信側 MVRF で PIM 制御トラフィックを受信するために存在します。

```
Device# show ip mfib vrf red 228.1.1.1

Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A
flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB
Forward,
                MA - MFIB Accept
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per
second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
VRF red
(*,228.1.1.1) Flags: C
  SW Forwarding: 0/0/0/0, Other: 0/0/0
  Tunnel16, MDT/239.3.3.3 Flags: NS
(220.1.1.200,228.1.1.1) Flags:
  SW Forwarding: 0/0/0/0, Other: 0/0/0
Tunnel16, MDT/239.3.3.3 Flags: NS
```

また、**show ip mroute count** コマンドを使用して、mVPN エクストラネットの統計情報を表示することもできます。ただし、**show ip mfib** コマンドを代わりに使用することを推奨します。**show ip mroute count** コマンドを使用して統計情報を表示する場合は、出力を精査して、送信元 MVRF の転送統計情報が正しいこと、および受信側 MVRF に転送統計情報がないことを確認します。

次の **show ip mroute count** コマンドの出力例は、送信元 MVRF blue の統計情報を示しています。

```
Device# show ip mroute vrf blue 228.1.1.1 count

Use "show ip mfib count" to get better response time for a large number of
mroutes.

IP Multicast Statistics
3 routes using 1354 bytes of memory
2 groups, 0.50 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: 228.1.1.1, Source count: 1, Packets forwarded: 38, Packets received: 38
  RP-tree: Forwarding: 1/0/100/0, Other: 1/0/0
  Source: 220.1.1.200/32, Forwarding: 37/0/100/0, Other: 37/0/0
```

次の **show ip mroute count** コマンドの出力例は、受信側 MVRF red を対象にしています。

```
Device# show ip mroute vrf red 228.1.1.1 count

Use "show ip mfib count" to get better response time for a large number of
mroutes.
```

```
IP Multicast Statistics
3 routes using 1672 bytes of memory
2 groups, 0.50 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Group: 228.1.1.1, Source count: 1, Packets forwarded: 0, Packets received: 0
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
  Source: 220.1.1.200/32, Forwarding: 0/0/0/0, Other: 0/0/0
```

例：静的 Mroute を使用した mVPN エクストラネットサポート向けの RPF の設定

次の例は、スタティック mroute 192.168.1.1 を使用して、VPN-Red で発生する RPF ルックアップが VPN-Green で解決されるように設定する方法を示します。

```
ip mroute vrf VPN-Red 192.168.1.1 255.255.255.255 fallback-lookup vrf VPN-Green
```

例：mVPN エクストラネットサポートにおけるグループベースの VRF 選択ポリシーの設定

グループベースの VRF 選択ポリシーを使用した例を以下に示します。VPN-Green で RPF ルックアップが発信された場合、グループアドレスが ACL 1 に一致する場合は VPN-Red で実行し、ACL 2 に一致する場合は VPN-Blue で実行するように設定します。

```
ip multicast vrf VPN-Green rpf select vrf VPN-Red group-list 1
ip multicast vrf VPN-Green rpf select vrf VPN-Blue group-list 2
!
.
.
.
!
access-list 1 permit 239.0.0.0 0.255.255.255
access-list 2 permit 238.0.0.0 0.255.255.255
!
```

その他の参考資料

関連資料

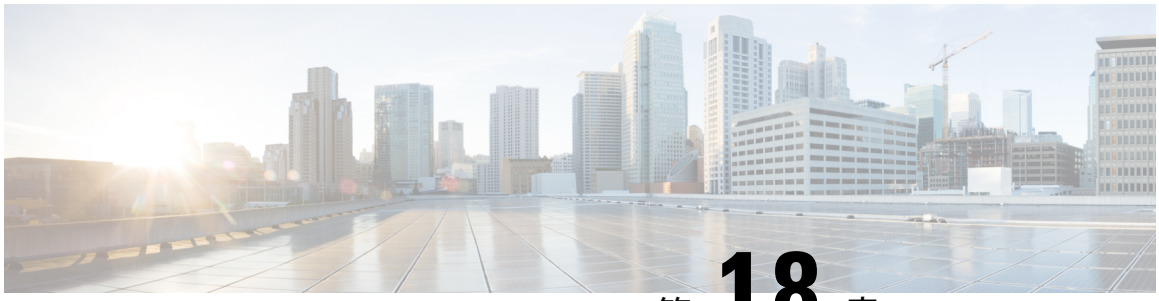
関連項目	マニュアル タイトル
基本的なIPマルチキャストの概念、設定作業、および例	「基本的な IP マルチキャストルーティングの設定」モジュール
IP マルチキャストの概要	「IP マルチキャスト ルーティング テクノロジー」モジュール

関連項目	マニュアル タイトル
MPLS レイヤ 3 VPN の概念および設定作業	「MPLS レイヤ 3 VPN の設定」モジュール
マルチキャスト VPN の概念、設定作業、および例	「マルチキャスト VPN の設定」モジュール

mVPN エクストラネットサポートの設定に関する機能履歴と情報

表 *25 : mVPN* エクストラネットサポートの設定に関する機能情報

機能名	リリース	機能情報
mVPN エクストラネットサポート	Cisco IOS XE Amsterdam 17.1.1	mVPN エクストラネットサポート機能は、ある企業サイトから他の企業サイトに送信された IP マルチキャストコンテンツをサービスプロバイダが配信できるようにします。この機能により、サービス プロバイダは、次世代の柔軟なエクストラネット サービスを提供でき、異なるエンタープライズ VPN カスタマー間でのビジネスパートナーシップの実現を支援します。



第 18 章

MLDP-Based MVPN

MLDP-Based MVPN

MLDP ベースの MVPN 機能は、マルチキャスト仮想プライベートネットワーク（MVPN）コアネットワークでの転送用に、ポイントツーマルチポイント（P2MP）およびマルチポイントツーマルチポイント（MP2MP）ラベルスイッチドパス（LSP）を設定するためのラベル配布プロトコル（LDP）の拡張機能を提供します。

MLDP ベースの MVPN の前提条件

- IPv4 マルチキャスト ルーティングの設定作業と概要に関する知識が必要です。
- Cisco Express Forwarding（CEF）が、ラベルスイッチング用のルータで有効になっている必要があります。
- ユニキャスト ルーティングは動作可能でなければなりません。
- MLDP ベースのマルチキャスト VPN を有効にするには、VPN ルーティングおよび転送（VRF）インスタンスを設定する必要があります。

MLDP ベースの VPN の制約事項

- MLDP プロファイル 1、13、および 14 のみがサポートされています。
- MLDP エクストラネットはサポートされていません。
- コアの GRE トンネルは MLDP ではサポートされていません。
- MLDP FRR はサポートされていません。
- サポートされているコンテンツグループモードは、Protocol Independent Multicast（PIM）スパースモード（PIM-SM）および Source Specific Multicast（SSM; 送信元特定マルチキャスト）です。双方向 PIM（PIM-Bidir）トラフィックは、プロファイル 1 でのみサポートされています。
- PIM デンスモード（PIM-DM）はサポートされていません。
- RSVP-TE ベースの LSM はサポートされていません。
- PIM スパース コンテンツ グループ モードは、PE ルータの裏側（CE 上）または送信元 PE ルータで RP が設定されている場合にサポートされます。
- IGP MLDP ECMP はサポートされていません。MLDP マルチパスを使用するように **no mpls mldp forwarding recursive** を設定する必要があります。
- L2 PE のデュアルホーミングは、MVPN プロファイルではサポートされていません。
- シームレス MPLS アーキテクチャでは MLDP はサポートされていません。

MLDP ベースの MVPN に関する情報

MLDP ベースの MVPN の概要

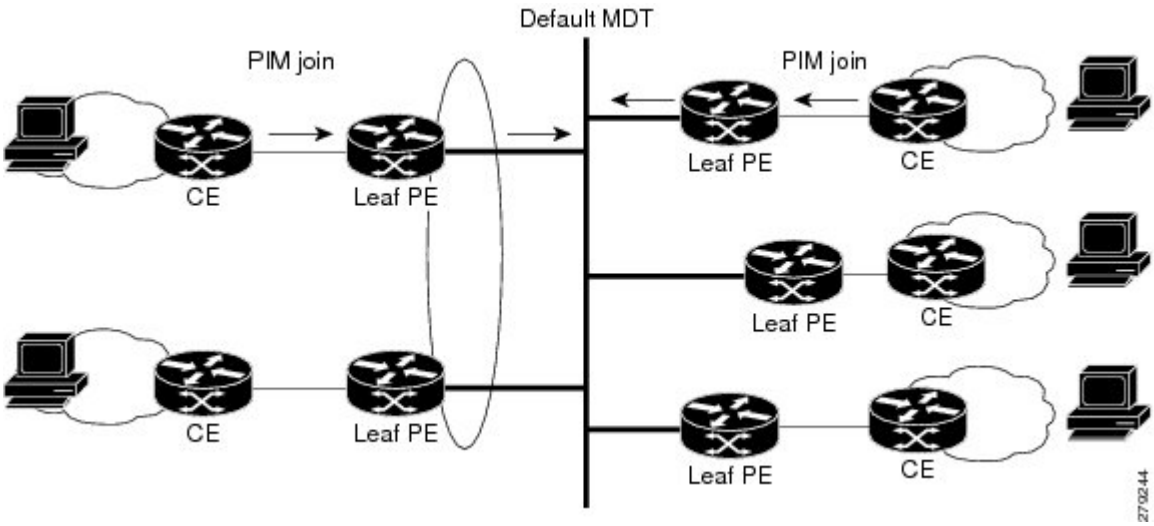
MVPN を使用すると、サービスプロバイダーは MPLS VPN 環境でマルチキャストトラフィックを設定およびサポートできます。この機能は、個々の VRF インスタンスでのマルチキャスト パケットのルーティングおよび転送をサポートし、サービス プロバイダーのバックボーンに VPN マルチキャスト パケットを転送するメカニズムも提供します。

VPNは、インターネットサービスプロバイダー（ISP）のような共有インフラストラクチャを介するネットワーク接続です。その役割は、プライベートネットワークとして、同じポリシーとパフォーマンスを低い所有コストで提供することによって、業務とインフラストラクチャを通して、多くのコスト削減の機会を作り出すことです。

MVPN により、企業はサービス プロバイダのネットワーク バックボーンでプライベート ネットワークをトランスペアレントに相互接続することができます。このように MVPN を使用してエンタープライズ ネットワークを相互接続しても、エンタープライズ ネットワークの管理方法や、企業の全体的な接続性は変わりません。

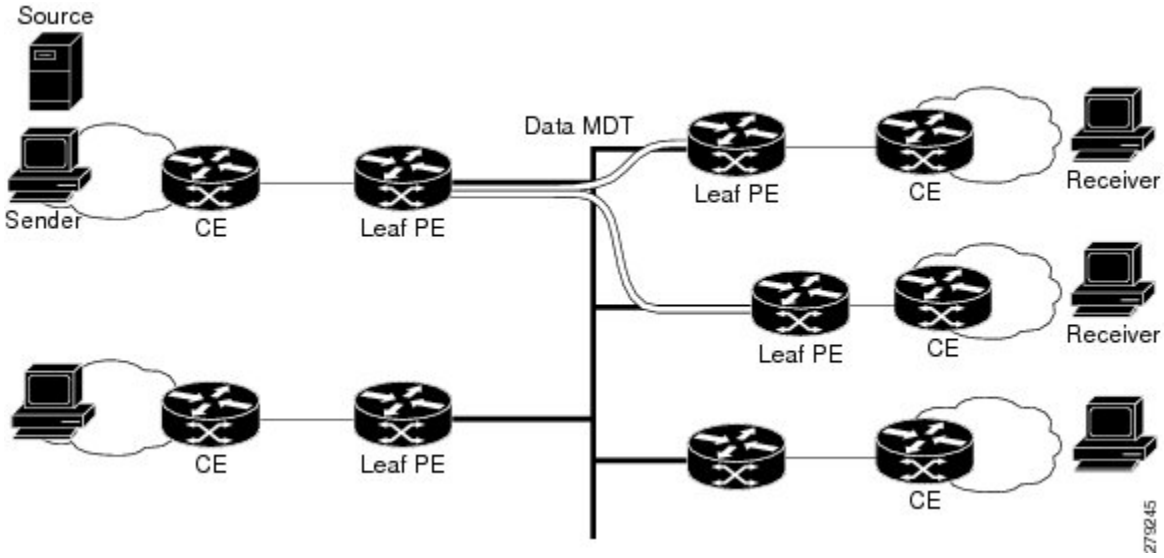
図に示されているように、MLDP ベースの MVPN は、各マルチキャストドメインに対して静的なデフォルトのマルチキャスト配信ツリー（MDT）を確立します。デフォルト MDT により、プロバイダーエッジ（PE）デバイスが使用するパスが定義され、マルチキャストドメインにある他のすべての PE デバイスに、マルチキャストデータと制御メッセージが送信されます。デフォルト MDT は、単一の MP2MP LSP を使用してコア ネットワークに作成されます。デフォルト MDT は仮想 LAN のように動作します。

図 *32*：デフォルト *MDT* のシナリオを使用した *MLDP*



図に示されているように、MLDP ベースの MVPN は、高帯域幅の送信用にデータ MDT の動的な作成もサポートします。レートの高いデータソースの場合、ストリームに参加しない PE への帯域幅を浪費しないよう、デフォルト MDT からのトラフィックをオフロードするために、P2MP LSP を使用してデータ MDT が構築されます。データ MDT の構築は、MDT Join TLV メッセージを使用して動的に通知されます。データ MDT は、Cisco IOS ソフトウェアに一意な機能です。データ MDT は、VPN 内のフルモーション ビデオなどの高帯域幅の送信元向けであり、MPLS VPN コアの最適なトラフィック転送を確保することを目的としています。データ MDT が構築されるしきい値は、デバイス単位または VRF 単位で設定できます。マルチキャスト伝送量が定義されたしきい値を超えると、送信側の PE デバイスがデータ MDT を構築し、データ MDT に関する情報を含むユーザー データグラム プロトコル（UDP）メッセージをデフォルト MDT のすべてのデバイスに送信します。

図 *33 :* データ *MDT* のシナリオを使用した *MLDP*



データ MDT は、VRF マルチキャスト ルーティング テーブル内で、（S,G）マルチキャスト ルートエントリ専用に作成されます。個々のソースデータ レートの値に関係なく、(*, G) エントリ用には作成されません。

以前はトランスポートメカニズムとして、IP コアネットワーク上で Multipoint Generic Routing Encapsulation（mGRE）を使用する Protocol Independent Multicast（PIM）のみ使用できました。マルチキャストラベル配布プロトコル（MLDP）の導入により、MPLS コアネットワーク上でラベルのプセル化とともに MLDP を使用した伝送が可能です。

MLDP により、次のように MDT が作成されます。

- デフォルト MDT は MP2MP LSP を使用します。
  - VRF 間の低帯域幅と制御トラフィックをサポートします。
- データ MDT は P2MP LSP を使用します。
  - VRF からの単一の高帯域幅ソースストリームをサポートします。

MVPN の他のすべての動作は、トンネリングメカニズムに関係なく同じです。

- VRF の PIM ネイバーは、ラベルスイッチパス仮想インターフェイス（LSP-VIF）を介して認識されます。
- VPN マルチキャストステートは PIM によって通知されます。

MLDP を使用する場合の唯一の違いは、mGRE ソリューションで使用される MDT グループアドレスが VPN ID に置き換えられることです。

MLDP ベースの MVPN には、次の利点があります。

- ユニキャストトラフィックとマルチキャストトラフィックの両方に単一の MPLS 転送プレーンを使用できます。
- 既存の MPLS 保護（MPLS トラフィックエンジニアリング/Resource Reservation Protocol（TE/RSVP リンク保護）および MPLS 運用、管理、保守（OAM）メカニズムなど）をマルチキャストトラフィックに使用できます。
- MPLS コアネットワークで PIM が不要になるため、運用上の複雑さが軽減されます。

MLDP ベースの MVPN の初期展開

MLDP ベースの MVPN の初期展開では、デフォルトの MDT と 1 つ以上のデータ MDT の設定を行います。

各マルチキャスト ドメインに対してデフォルトのスタティック MDT が確立されます。デフォルト MDT により、PE デバイスが使用するパスが定義され、マルチキャストドメインにある他のすべての PE デバイスに、マルチキャストデータと制御メッセージが送信されます。デフォルト MDT は、単一の MP2MP LSP を使用してコア ネットワークに作成されます。

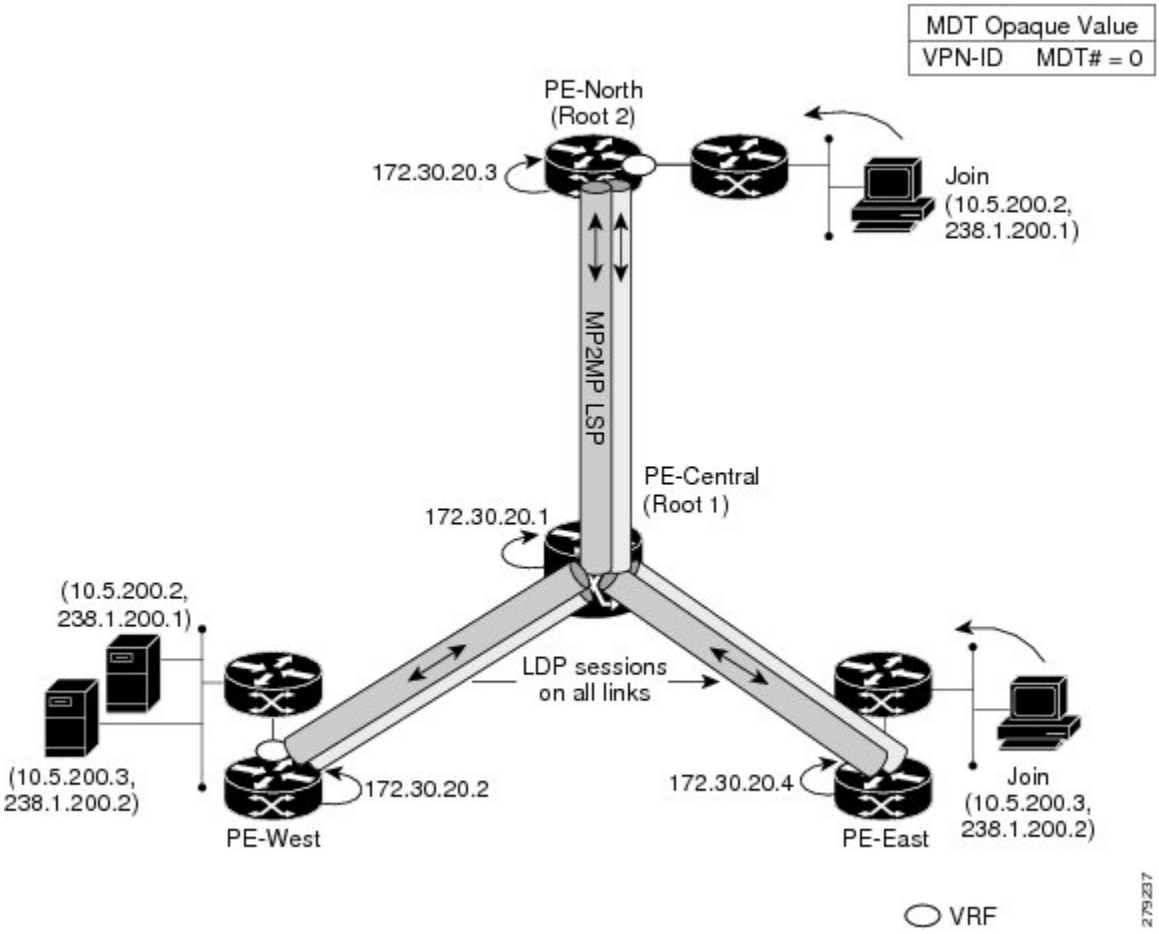
MLDP ベースの MVPN では、高帯域幅の送信用にデータ MDT の動的な作成もサポートされます。

デフォルト MDT の構築

図は、デフォルト MDT のシナリオを示しています。デフォルト MDT のシグナリングに使用される Opaque 値は、VPN ID と VPN の MDT 番号の 2 つのパラメータで構成されます。形式は（vpn-id、0）で、vpn-id は VPN を一意に識別する手動で設定された 7 バイトの番号です。デフォルト MDT はゼロに設定されています。

このシナリオでは、3 つの PE デバイスはそれぞれ VRF と呼ばれる VRF に属し、同じ VPN ID を持ちます。同じ VPN ID を持つ各 PE デバイスは、同じ MP2MP ツリーに参加します。PE デバイスには、P-Central（ルート 1）をルートとするプライマリ MP2MP ツリーと、PE-North（ルート 2）をルートとするバックアップ MP2MP ツリーが作成されています。PE-West には 2 つの送信元があり、PE-North と PE-East の両方に該当する受信者がいます。PE-West では MP2MP ツリーの 1 つを選択してカスタマー VPN トラフィックが送信されますが、すべての PE デバイスがいずれかの MP2MP ツリーでトラフィックを受信できます。

図 *34 :* デフォルト *MDT* のシナリオ



LSP ダウンストリームのデフォルト MDT の構築

図は、各ルートのダウンストリームツリーの構築内容を示しています。VPN ID 100:2 で設定された各 PE デバイスでは、同じ転送等価クラス（FEC）のタイプ、長さ、および値（TLV）が作成されますが、MP2MP ツリーごとに異なるルートとダウンストリームラベルが使用されます。FEC タイプは MP2MP Down になり、アップストリーム ラベル マッピング メッセージで応答してアップストリームパスを作成するように受信側の Label Switched Route（LSR）に指示します。

図 *35 :* デフォルト *MDT* ダウンストリーム：ルート *1*

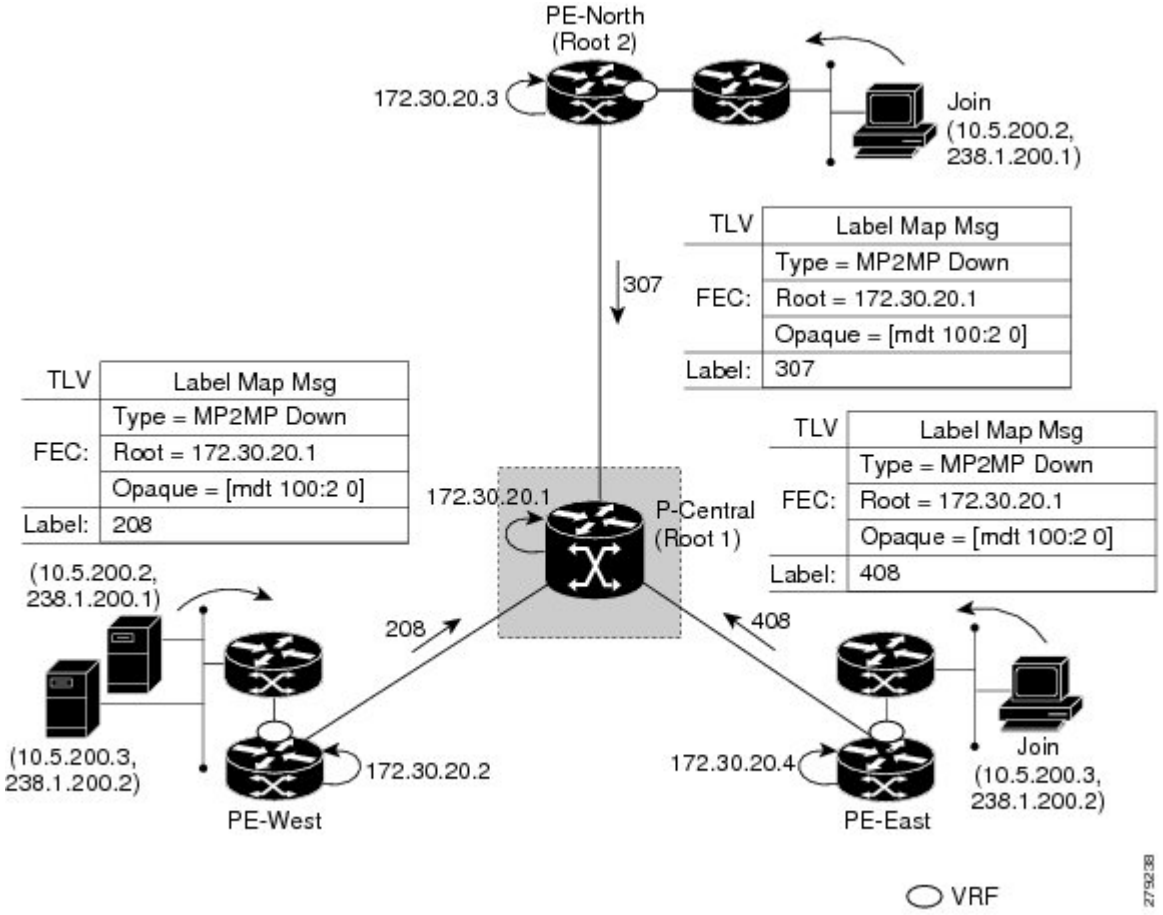
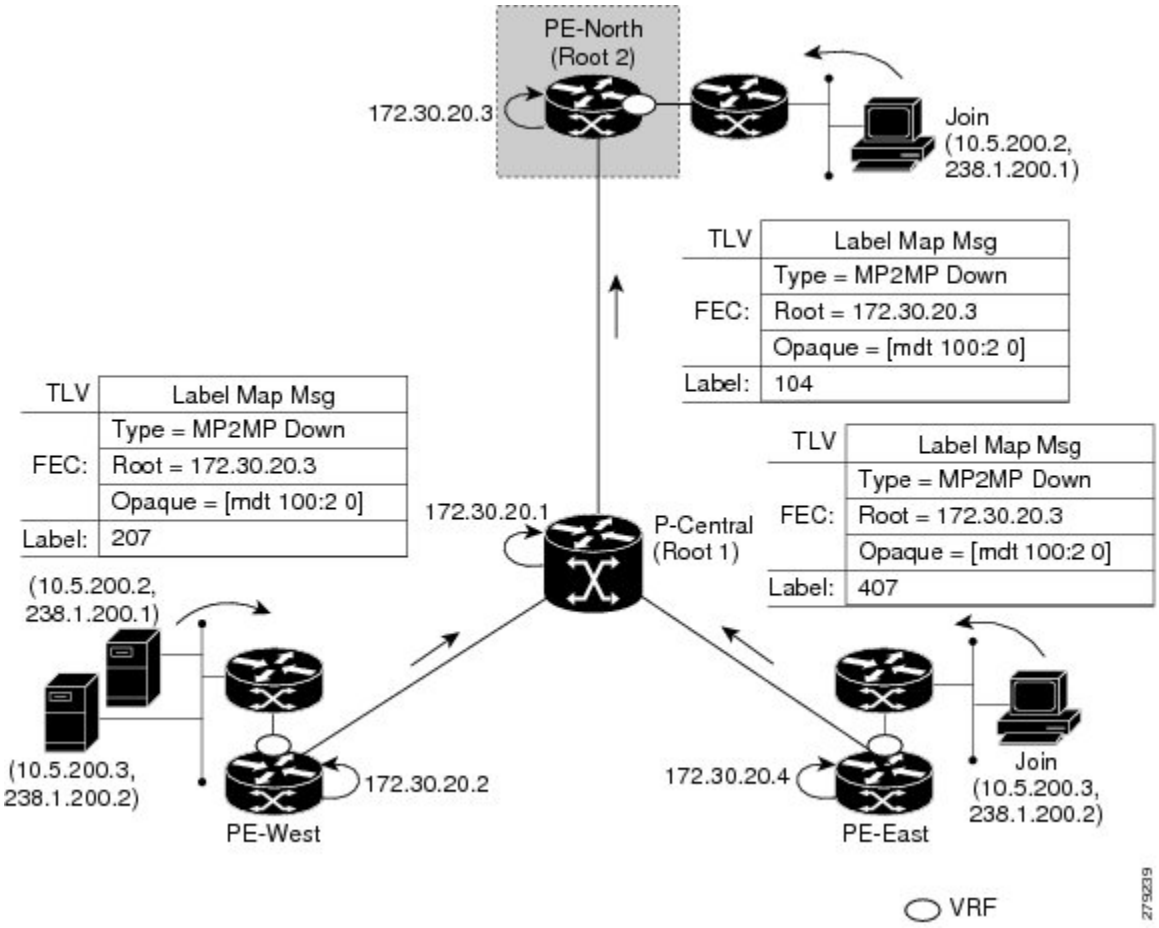


図 *36 :* デフォルト *MDT* ダウンストリーム：ルート *2*



LSP アップストリームのデフォルト MDT の構築

図は、デフォルト MDT のアップストリーム LSP の構築内容を示しています。受信したダウンストリームラベルごとに、対応するアップストリームラベルが送信されます。最初の図では、P-Central は 3 つのアップストリームラベル（111、109、および 105）を各ダウンストリームの直接接続されたネイバーに送信します（ダウンストリームはルートから離れています）。2 番目の図に示されているように、直接接続されたダウンストリームネイバーは 1 つしかないため、PE-North のプロセスは単一のアップストリームラベル（313）のみを送信することを除いて同じです。

図 *37 :* デフォルト *MDT* アップストリーム：ルート *1*

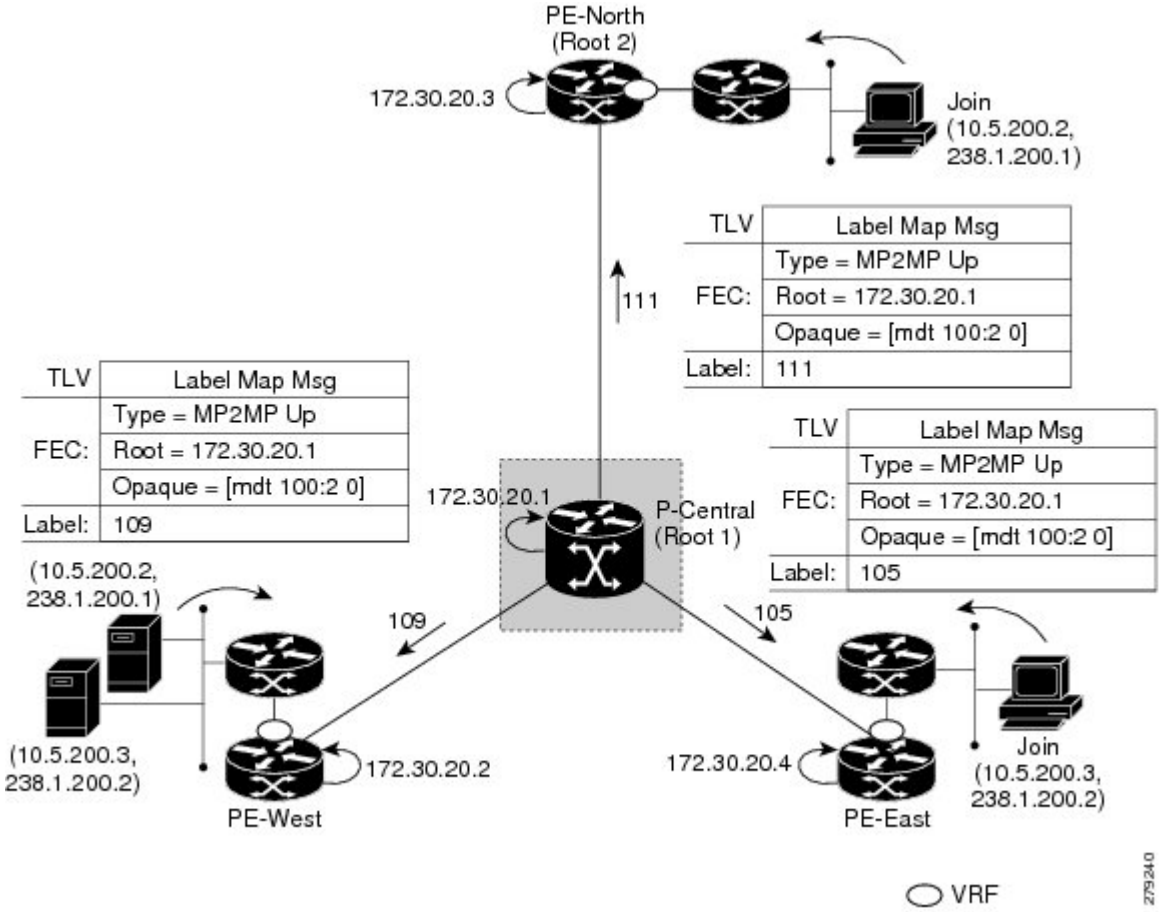
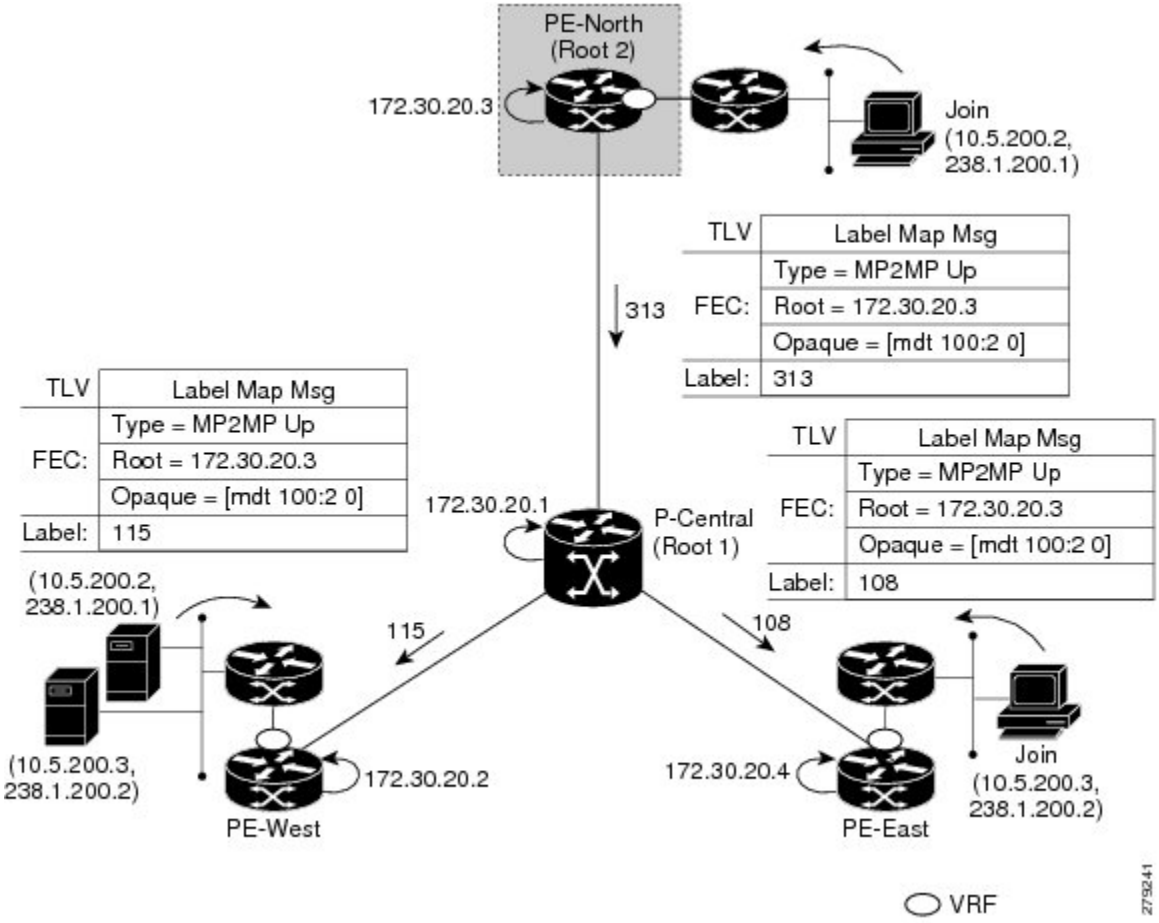


図 *38 :* デフォルト *MDT* アップストリーム：ルート *2*

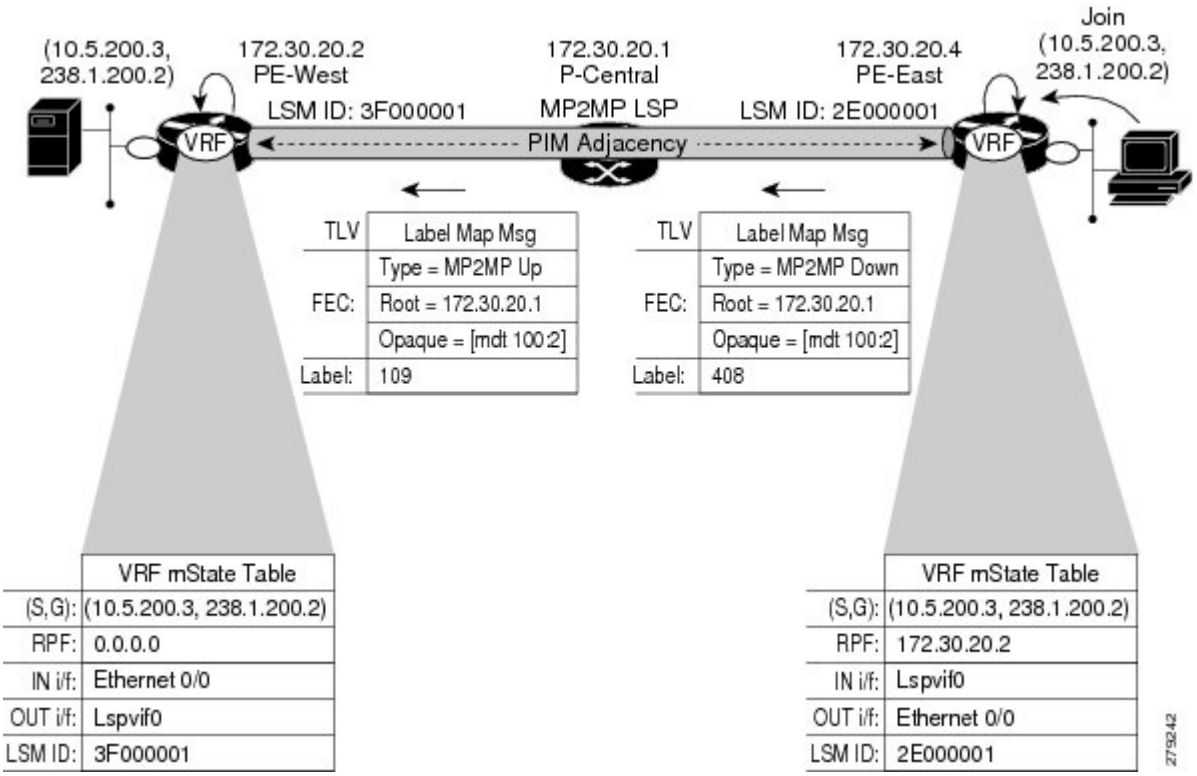


VPN マルチキャストステートの PIM オーバーレイシグナリング

VPN 内のマルチキャストステートのシグナリングは、PIM 経由で行われます。PIM セッションはマルチポイント LSP 上で動作し、VPN マルチキャストフローが LSP にマッピングされるため、オーバーレイシグナリングと呼ばれます。MVPN では、PIM の動作は、基盤となるトンネルテクノロジーに依存しません。MVPN ソリューションでは、PE デバイス間で PIM 隣接関係が作成され、VRF 内のマルチキャストステートが PIM セッションを介して入力されます。MLDP を使用する場合、PIM セッションは LSP-VIF インターフェイス上で実行されます。図は、デフォルト MDT MP2MP LSP 上で実行される PIM シグナリングを示しています。MP2MP LSP へのアクセスは LSP-VIF を介して行われます。LSP-VIF を使用すると、LAN インターフェイスと同様に、ブランチの終端にあるすべてのリーフ PE デバイスを確認できます。図では、PE-East はダウンストリーム ラベル マッピング メッセージをルートである P-Central に送信し、P-Central はアップストリーム ラベル マッピング メッセージを PE-West に送信しています。これらのメッセージにより、2 つのリーフ PE デバイス間に LSP が作成されます。その後、PIM セッションを LSP の上部でアクティブにして、（S、G）ステートと制御メッセージを PE-West と PE-East 間でシグナリングできます。この場合、PE-East が VRF 内の（10.5.200.3、238.1.200.2）の Join TLV メッセージを受信し、mroute テーブルに挿入します。Join TLV メッセージは、PIM

セッションを介して PE-West（BGP ネクストホップ 10.5.200.3）に送信され、VRF mroute テーブルに入力されます。この手順は、mGRE トンネルを使用する場合の手順と同じです。

図 *39 : LSP* を介した *PIM* シグナリング



データ MDT のシナリオ

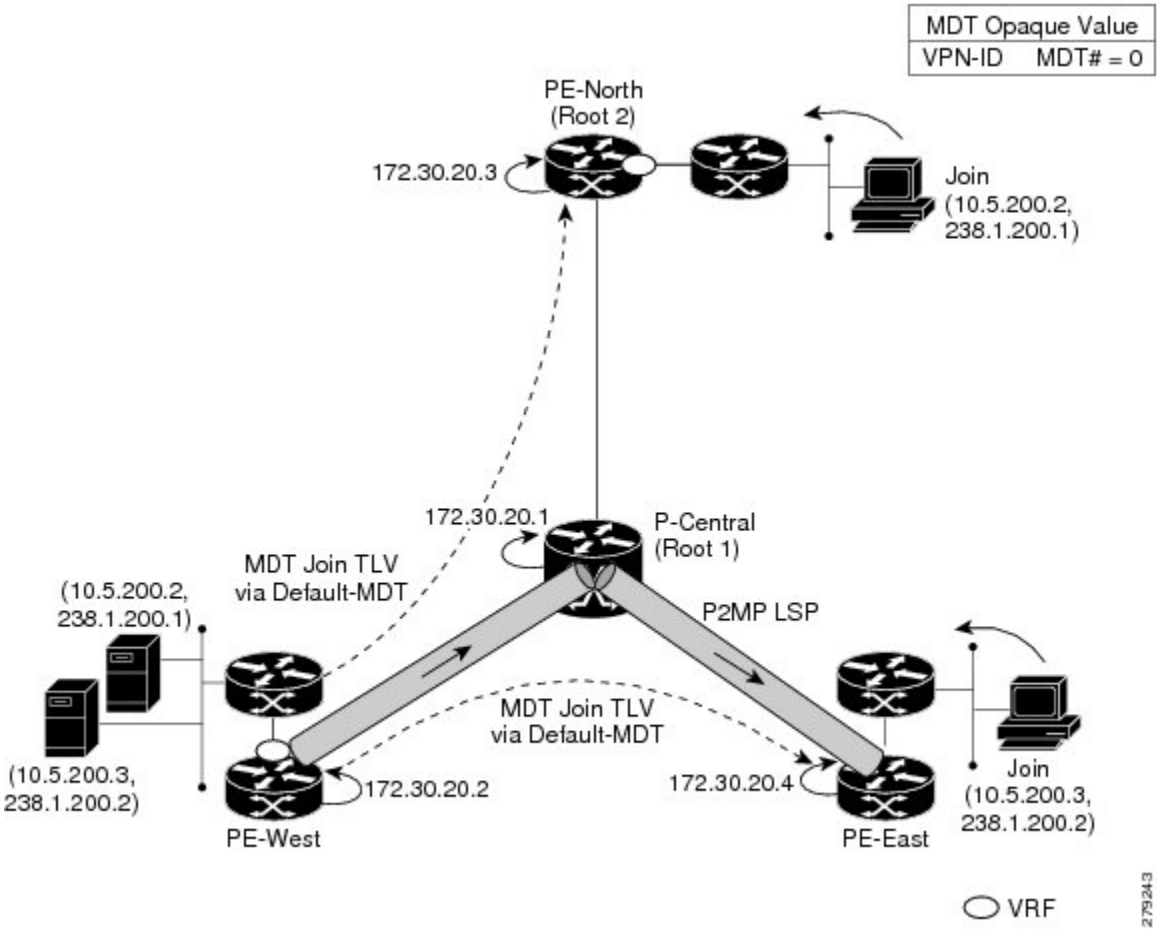
MVPN では、特定のしきい値を超えるトラフィックは、デフォルト MDT からデータ MDT に移動できます。

図は、データ MDT のシナリオを示しています。データ MDT のシグナリングに使用される Opaque 値は、VPN ID と MDT 番号の 2 つのパラメータで構成されます。形式は（vpn-id、MDT# > 0）で、vpn-id は VPN を一意に識別する手動で設定された 7 バイトの番号です。2 番目のパラメータは、この VPN の一意のデータ MDT 番号で、ゼロより大きい数値です。

このシナリオでは、PE-North と PE-East の 2 つの受信者が PE-West の 2 つの送信元に関心を持っています。送信元（10.5.200.3）がデフォルト MDT のしきい値を超えると、PE-West は、新しいデータ MDT が作成されていることをすべての PE デバイスに通知する MDT Join TLV メッセージをデフォルト MDT MP2MP LSP 経由で発行します。

PE-East には VRF に該当する受信者がいるため、P2MP を使用してマルチポイント LSP を構築し、ツリーのルートとなる PE-West に戻します。PE-North には 10.5.200.3 の受信者がいないため、Join TLV メッセージをキャッシュするだけです。

図 *40 :* データ *MDT* のシナリオ



P2MP および MP2MP ラベル スイッチド パス

MLDP は、MPLS コアにマルチキャスト ルーティング プロトコルが存在しなくても、MPLS ネットワーク内にマルチポイント ラベル スイッチ パス（MP LSP）を設定できるアプリケーションです。MLDP では、他のマルチキャストツリー構築プロトコルと相互に作用したり、それらのプロトコルに依存したりすることなく、P2MP または MP2MP LSP を構築できます。MP LSP およびユニキャスト IP ルーティングに LDP 拡張を使用すると、MLDP で MP LSP を設定できます。設定できる MP LSP のタイプには、ポイントツーマルチポイント（P2MP）とマルチポイントツーマルチポイント（MP2MP）のタイプの LSP の 2 つがあります。

P2MP LSP を使用すると、1 つのルート（入力ノード）からのトラフィックを複数のリーフ（出力ノード）に配信できます。ここで、各 P2MP ツリーは 2 タプル（ルート ノード アドレス、P2MP LSP 識別子）で一意に識別されます。P2MP LSP は、1 つのルート ノード、0 個以上の中継ノード、および 1 つ以上のリーフ ノードで構成されます。ここで通常、ルート ノードとリーフ ノードは PE であり、中継ノードは P ルータです。P2MP LSP の設定はレシーバから起動され、MLDP P2MP FEC を使用してシグナリングされます。ここで、LSP 識別子は MP Opaque Value 要素で表されます。MP Opaque Value は、入力 LSR とリーフ LSR が認識している情報を

伝送しますが、中継 LSR で解釈する必要はありません。特定の入力ノードをルートとする、それぞれ独自の識別子を持つ MP LSP が複数存在する可能性があります。

MP2MP LSP を使用すると、複数の入力ノードからのトラフィックを複数の出力ノードに配信できます。ここで、MP2MP ツリーは 2 タプル（ルート ノードアドレス、MP2MP LSP 識別子）で一意に識別されます。MP2MP LSP の場合は、入力ノードから送信されたパケットを、送信ノードを除くすべての出力ノードが受信します。

MP2MP LSP は P2MP LSP と同様ですが、各リーフ ノードが入力ノードと出力ノードの両方として機能します。MP2MP LSP を構築するには、ダウンストリーム パスとアップストリーム パスを次のように設定できます。

- ダウンストリームパスは、通常の P2MP LSP のように設定します。
- アップストリーム パスは、アップストリーム ルータに向けられた P2P LSP のように設定しますが、ダウンストリーム ラベルをダウンストリーム P2MP LSP から継承するようにします。

（注） プレフィックスごとに 1 つの P2MP MDT ツリーを設定することを推奨します。たとえば、500 のマルチキャストルートが必要な場合は、少なくとも 500 の P2MP MDT ツリーを設定する必要があります。

MLDP ベースの MVPN のパケットフロー

着信するパケットごとに、MPLS は複数の外側ラベルを作成します。ソース ネットワークからのパケットは、レシーバ ネットワークへのパス上で複製されます。CE1 ルータは、ネイティブの IP マルチキャスト トラフィックを送信します。PE1 ルータは着信マルチキャスト パケットにラベルを付加し、MPLS コア ネットワークへのラベル付きパケットを複製します。パケットは、コア ルータ（P）に到達すると、MP2MP のデフォルト MDT または P2MP のデータ MDT に対応する適切なラベル付きで複製され、すべての出力 PE に送信されます。パケットが出力 PE に到達すると、ラベルが削除され、IP マルチキャスト パケットは VRF インターフェイスに複製されます。

MLDP ベースの MVPN の実現

MLDP によって構築されたラベルスイッチパス（LSP）は、アプリケーションの要件や性質に応じて、次のように使用できます。

- インバンド シグナリングを使用したグローバル テーブル中継マルチキャスト用の P2MP LSP。
- MI-PMSI（Multidirectional Inclusive Provider Multicast Service Instance）に基づいた MVPN 用の P2MP/MP2MP LSP（Rosen ドラフト）。
- MS-PMSI（Multidirectional Selective Provider Multicast Service Instance）に基づいた MVPN 用の P2MP/MP2MP LSP（パーティション化 E-LAN）。

デバイスでは、MLDP の実装のための次の重要な機能が実行されます。

1. VRF マルチキャスト IP パケットの GRE/ラベルによるカプセル化、およびコアインターフェイスへの複製（インポジションノード）。
2. マルチキャストラベルパケットの異なるラベルによる別のインターフェイスへの複製（中間ノード）。
3. ラベル パケットのカプセル化解除、および VRF インターフェイスへの複製（ディスポジション ノード）。

MVPN MLDP パーティション MDT の概要

MVPN を使用すると、サービスプロバイダは MPLS VPN 環境でマルチキャストトラフィックを設定およびサポートできます。このタイプでは、個々のVPNルーティングおよび転送（VRF）インスタンスでのマルチキャストパケットのルーティングおよび転送がサポートされ、サービス プロバイダーのバックボーン全体にわたって VPN マルチキャスト パケットを転送するためのメカニズムも提供されます。MLDP の場合は、通常のラベル スイッチ パス転送が使用されるため、コアが PIM プロトコルを実行する必要はありません。このシナリオでは、c パケットは MPLS ラベル内にカプセル化され、MPLS ラベルスイッチパス（LSP）に基づいて転送されます。

MVPN MLDP サービスにより、送信元と受信側が異なるサイトに配置された Protocol Independent Multicast（PIM）ドメインを構築できます。

複数の分散したサイトがあるカスタマーにレイヤ 3 マルチキャスト サービスを提供する場合は、サービス プロバイダーはプロバイダー ネットワーク経由でカスタマーのマルチキャストトラフィックを伝送するセキュアかつスケーラブルなメカニズムを求めます。マルチキャスト VPN（MVPN）は、BGP/MPLS VPN のようなネイティブ マルチキャスト テクノロジーを使用して共有サービス プロバイダー バックボーンを介して、このようなサービスを提供します。

MVPN は、マルチキャストドメイン（MD）の概念を採用するときに MPLS VPN テクノロジーをエミュレートします。その際、プロバイダー エッジ（PE）ルータは、同一カスタマー VPN に接続している他の PE ルータとの仮想 PIM ネイバー接続を確立します。これらの PE ルータはプロバイダー ネットワーク上のセキュアな仮想マルチキャスト ドメインを形成します。マルチキャスト トラフィックは、専用プロバイダー ネットワークを通過しているかのように、サイト間をコア ネットワーク上で伝送されます。

VPN ルーティングおよび転送（VRF）インスタンスごとに個別のマルチキャスト ルーティングおよび転送テーブルが保持され、トラフィックは、サービスプロバイダーのバックボーン全体にわたって VPN トンネル経由で送信されます。

Rosen MVPN MLDP ソリューションでは、コントロールプレーンとデータトラフィックを伝送するために、マルチポイントツーマルチポイント（MP2MP）のデフォルト MDT が設定されます。このソリューションの欠点は、MVPN の一部であるすべての PE ルータがこのデフォルト MDT ツリーに参加する必要があることです。MVPN のすべての PE ルータ間に MP2MP ツリーを設定することは、各 PE をルートとする N 個の P2MP ツリーを作成することと同じです（N は PE ルータの数）。Inter-AS（オプション A）ソリューションでは、全 AS 上のすべての PE

ルータがデフォルト MDT に参加する必要があるため、この問題は悪化します。このソリューションのもう 1 つの欠点は、デフォルト MDT を介して送信されたパケットが、必要ない場合でもすべての PE ルータに到達することです。

パーティション MDT アプローチでは、特定の入力 PE からのトラフィック要求を受信する出力 PE ルータだけが、その入力 PEで設定された PMSI に参加します。これにより、ネットワーク内の入力 PE ルータの数が少なくなり、コア内のツリーの数が制限されます。

サポートされる MLDP プロファイル

プロファイル名	MLDP でサポート可
プロファイル 1 デフォルト MDT - MLDP MP2MP - PIM C-mcast シグナリング	対応
プロファイル 2 パーティション MDT - MLDP MP2MP - PIM C-mcast シグナリング	非対応
プロファイル 4 パーティション MDT - MLDP MP2MP - BGP-AD - PIM C-mcast シグナリング	非対応
プロファイル 5 パーティション MDT - MLDP P2MP - BGP-AD - PIM C-mcast シグナリング	非対応
プロファイル 6 VRF MLDP - インバンドシグナリング	非対応
プロファイル 7 グローバル MLDP - インバンドシグナリング	非対応
プロファイル 9 デフォルト MDT - MLDP - MP2MP - BGP-AD - PIM C-mcast シグナリング	非対応
プロファイル 12 デフォルト MDT - MLDP - P2MP - BGP-AD - BGP C-mcast シグナリング	非対応
プロファイル 13 デフォルト MDT - MLDP - MP2MP - BGP-AD - BGP C-mcast シグナリング	対応
プロファイル 14 パーティション MDT - MLDP P2MP - BGP-AD - BGP C-mast シグナリング	対応
プロファイル 15 パーティション MDT - MLDP MP2MP - BGP-AD - BGP C-mast シグナリング	非対応
プロファイル 17 デフォルト MDT - MLDP - P2MP - BGP-AD - PIM C-mcast シグナリング	なし

MLDP ベースの MVPN の設定方法

MLDP の初期設定の設定

MLDP の初期設定を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mpls mldp logging notifications**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**mpls mldp logging notifications** 例： `Device(config)# mpls mldp logging notifications`	MLDP ロギング通知を有効にします。
ステップ 4	**end** 例： `Device(config)# end`	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。

MLDP ベースの MVPN の設定

MLDP ベースの MVPN を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**

3. **ip multicast-routing**
4. **ip multicast-routing vrf** *vrf-name*
5. **vrf definition** *vrf-name*
6. **rd** *route-distinguisher*
7. **vpn id** *oui* **:** *vpn-index*
8. **address family ipv4**
9. **mdt preference** { **mldp** | **pim** }
10. **mdt default mpls mldp** *group-address*
11. **mdt data mpls mldp** *number-of-data-mdt*
12. **mdt data threshold** *kb/s* **list** *access-list*
13. **route target export** *route-target-ext-community*
14. **route target import** *route-target-ext-community*
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**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	**ip multicast-routing** 例： `Device(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。
ステップ 4	**ip multicast-routing vrf** *vrf-name* 例： `Device(config)# ip multicast-routing vrf VRF`	*vrf-name* 引数に指定された MVPN VRF の IP マルチキャストルーティングを有効にします。
ステップ 5	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition VRF`	VRF コンフィギュレーションモードを開始し、VRF 名を割り当てることにより VPN ルーティング インスタンスを定義します。
ステップ 6	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 50:11`	ルート識別子（RD）が作成されます（VRF を機能させるため）。ルーティングテーブルと転送テーブルを作成し、RD と VRF インスタンスを関連付けて、VPN のデフォルト RD を指定します。

	コマンドまたはアクション	目的
ステップ 7	**vpn id** *oui* **:** *vpn-index* 例： `Device(config-vrf)# vpn id 50:10`	VRF インスタンスの VPN ID を設定または更新します。
ステップ 8	**address family ipv4** 例： `Device(config-vrf)# address family ipv4`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、VRF のアドレス ファミリを指定します。 • **ipv4** キーワードは、VRF の IPv4 アドレスファミリを指定します。
ステップ 9	**mdt preference** { **mldp** | **pim** } 例： `Device(config-vrf-af)# mdt preference mldp`	特定の MDT タイプ（MLDP または PIM）の設定を指定します。
ステップ 10	**mdt default mpls mldp** *group-address* 例： `Device(config-vrf-af)# mdt default mpls mldp 172.30.20.1`	VPN VRF インスタンスのデフォルト MDT グループを設定します。
ステップ 11	**mdt data mpls mldp** *number-of-data-mdt* 例： `Device(config-vrf-af)# mdt data mpls mldp 255`	データ MDT プールで使用されるアドレスの範囲を指定します。
ステップ 12	**mdt data threshold** *kb/s* **list** *access-list* 例： `Device(config-vrf-af)# mdt data threshold 40 list 1`	帯域幅しきい値をキロビット/秒単位で定義します。
ステップ 13	**route target export** *route-target-ext-community* 例： `Device(config-vrf-af)# route target export 100:100`	指定した VRF のエクスポート ルート ターゲット拡張コミュニティを作成します。
ステップ 14	**route target import** *route-target-ext-community* 例： `Device(config-vrf-af)# route target import 100:100`	指定した VRF のインポートルートターゲット拡張コミュニティを作成します。

	コマンドまたはアクション	目的
ステップ 15	**end** 例： `Device(config-vrf-af)# end`	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。

MLDP ベースの MVPN に関する設定の確認

MLDP ベースの MVPN の設定を確認するには、特権 EXEC モードで次の作業を実行します。

手順の概要

1. show mpls mldp database
2. **show ip pim neighbor** [**vrf** *vrf-name*] **neighbor** [*interface-type interface-number*]
3. **show ip mroute** [**vrf** *vrf-name*] [[**active** [*kbps*] [**interface** *type number*] | **bidirectional** | **count** [**terse**] | **dense** | **interface** *type number* | **proxy** | **pruned** | **sparse** | **ssm** | **static** | **summary**] | [*group-address* [*source-address*]] [**count** [**terse**] | **interface** *type number* | **proxy** | **pruned** | **summary**] | [*source-address group-address*] [**count** [**terse**] | **interface** *type number* | **proxy** | **pruned** | **summary**] | [*group-address*] **active** [*kbps*] [**interface** *type number* | **verbose**]]
4. **show mpls forwarding-table** [*network* {*mask* | *length*} | **labels** *label* [**-** *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vrf-name*] [**detail**]

手順の詳細

ステップ 1 show mpls mldp database

MLDP データベースの情報を表示するには、**show mpls mldp database** コマンドを入力します。FEC 復号された FEC の Opaque 値、および関連付けられたレプリケーション クライアントが表示されます。

例：

```
Device# show mpls mldp database
  * For interface indicates MLDP recursive forwarding is enabled
  * For RPF-ID indicates wildcard value
  > Indicates it is a Primary MLDP MDT Branch

LSM ID : CB (RNR LSM ID: CC)   Type: MP2MP   Uptime : 00:01:38
  FEC Root           : 2.2.2.2 (we are the root)
  Opaque decoded     : [mdt 3001:1 0]
  Opaque length      : 11 bytes
  Opaque value       : 02 000B 003001000000100000000
  RNR active LSP     : (this entry)
  Upstream client(s) :
    None
      Expires        : N/A           Path Set ID  : D5
  Replication client(s):
>   MDT  (VRF vrf3001)
      Uptime         : 00:01:38      Path Set ID  : D6
      Interface      : Lspvif101     RPF-ID       : *
    33.33.33.33:0
      Uptime         : 00:01:22      Path Set ID  : D7
```

```
      Out label (D)  : 2343          Interface    : Vlan2222*
      Local label (U): 466           Next Hop     : 26.1.3.2
```

ステップ 2 **show ip pim neighbor** [**vrf** *vrf-name*] **neighbor** [*interface-type interface-number*]

show ip pim neighbor コマンドを入力して、PIM 隣接関係の情報を表示します。

例：

```
Device# show ip pim vrf vrf3001 neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable,
      L - DR Load-balancing Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
192.168.1.2       Port-channel122.3001     3d19h/00:01:30    v2    1 / DR B S P G
5.5.5.5           Lspvif101                00:01:48/00:01:25 v2    1 / B S P G
7.7.7.7           Lspvif101                00:01:48/00:01:25 v2    1 / DR S P G
```

ステップ 3 **show ip mroute** [**vrf** *vrf-name*] [[**active** [*kbps*] [**interface** *type number*] | **bidirectional** | **count** [**terse**] | **dense** | **interface** *type number* | **proxy** | **pruned** | **sparse** | **ssm** | **static** | **summary**] | [*group-address* [*source-address*]] [**count** [**terse**] | **interface** *type number* | **proxy** | **pruned** | **summary**] | [*source-address group-address*] [**count** [**terse**] | **interface** *type number* | **proxy** | **pruned** | **summary**] | [*group-address*] **active** [*kbps*] [**interface** *type number* | **verbose**]]

show ip mroute コマンドを入力して、マルチキャストルーティング（mroute）テーブルの内容を表示します。

例：

```
Device# show ip mroute vrf vrf3001 225.1.1.1 30.22.1.10
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group, c - PFP-SA cache created entry,
       * - determined by Assert, # - iif-starg configured on rpf intf,
       e - encap-helper tunnel flag
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(30.22.1.10, 225.1.1.1), 00:31:08/00:02:14, flags: JTY
  Incoming interface: Lspvif101, RPF nbr 2.2.2.2, MDT: [2, 2.2.2.2]/00:02:51
  Outgoing interface list:
    Vlan3001, Forward/Sparse, 00:31:08/00:02:35
```

ステップ 4 **show mpls forwarding-table** [*network* {*mask* | *length*} | **labels** *label* [**-** *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vrf-name*] [**detail**]

show mpls forwarding-table コマンドを入力して、MPLS ラベル転送情報ベース（LFIB）の内容を表示します。

例：

```
Device# show mpls forwarding-table vrf vrf3001
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
150        No Label   192.168.1.0/24[V]   \
                                       0             aggregate/vrf3001
356        No Label   30.1.30.2/32[V]  0             Po122.3001  192.168.1.2
357        No Label   30.1.30.1/32[V]  0             Po122.3001  192.168.1.2
358        No Label   30.22.1.0/24[V]  0             Po122.3001  192.168.1.2
466   [T]  No Label   [mdt 3001:1 0][V]   \
                                       65660         aggregate/vrf3001

[T]     Forwarding through a LSP tunnel.
        View additional labelling info with the 'detail' option
```

MLDP ベースの MVPN の設定例

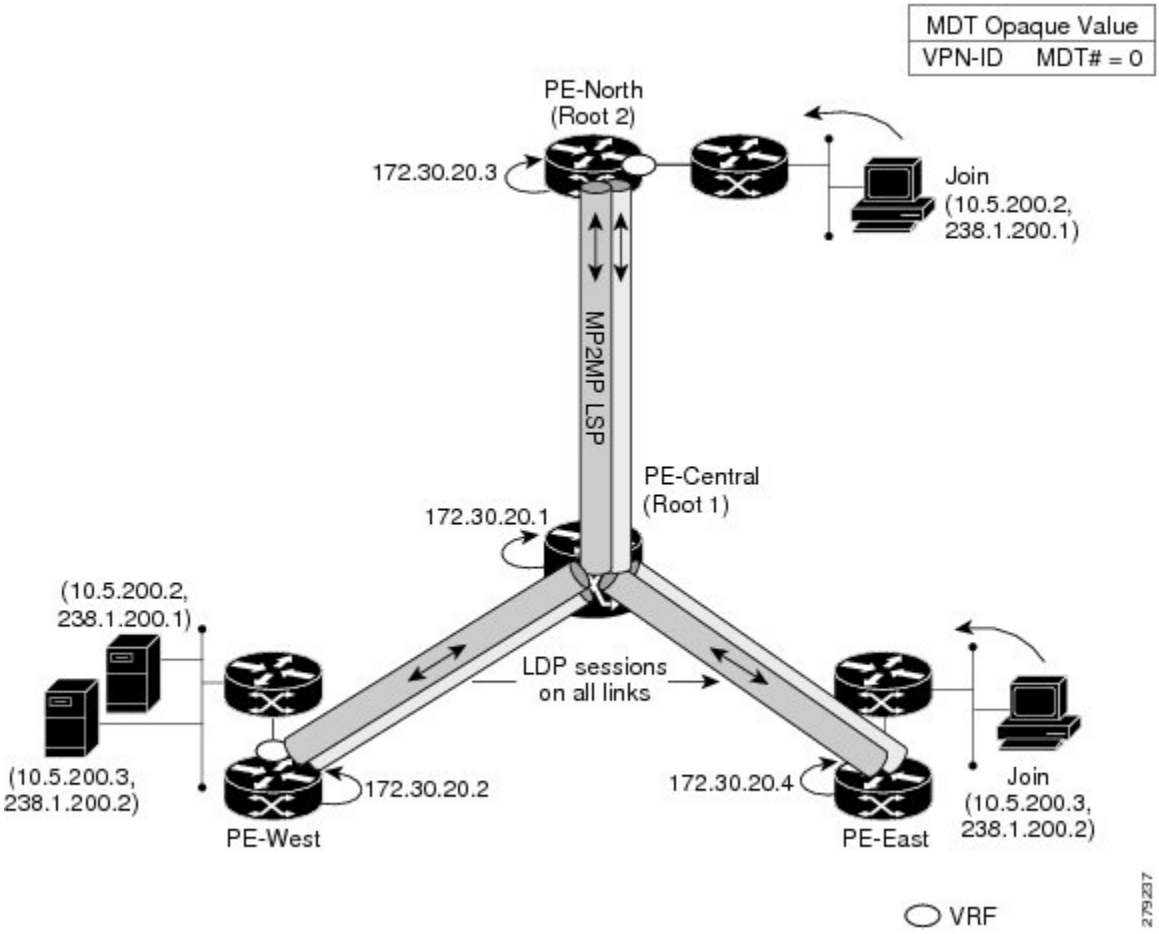
例：MLDP ベースの MVPN の初期展開

MLDP ベースの MVPN の初期展開では、デフォルトの MDT と 1 つ以上のデータ MDT の設定を行います。

デフォルト MDT の設定

次に、MLDP ベースの MVPN のデフォルト MDT を設定する例を示します。この設定は、図に示されているトポロジ例に基づいています。

図 *41* : デフォルト *MDT* の例



この設定は、同じ VPN ID に参加するすべての PE デバイスで一貫しています。**vpn id 100:2** コマンドは、mGRE トランスポート方式で使用される MDT グループアドレスを置き換えます。冗長性を提供するために、P-Central と PE-North をルートとする 2 つのデフォルト MDT ツリーが静的に設定されます。デフォルト MDT が特定の PE デバイスで使用する MP2MP ツリーの選択は、内部ゲートウェイプロトコル（IGP）メトリックによって決まります。MP2MP LSP は、デフォルト MDT に対して暗黙的です。

```
ip pim mpls source Loopback0
ip multicast-routing
ip multicast-routing vrf VRF
!
ip vrf VRF
 rd 100:2
 vpn id 100:2
 route-target export 200:2
 route-target import 200:2
 mdt default mpls mldp 172.30.20.1 (P-Central)
 mdt default mpls mldp 172.30.20.3 (PE-North)
```

PIM 隣接関係

PIM は、通常のトンネルインターフェイスであるかのように LSP-VIF 上で動作します。つまり、PIM hello メッセージが LSP-VIF を介して交換され、デフォルト MDT を介して PIM 隣接関係が確立されます。このセクションの出力例には、PE-East の VRF にある 3 つの PIM 隣接関係が表示されています。ここに記載されているのは、LSP-VIF インターフェイス 101 経由で MP2MP LSP を介した PE-West および PE-North への隣接関係です。

```
PE-East# show ip pim vrf vrf3001 neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable,
      L - DR Load-balancing Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
5.5.5.5           Lspvif0                  00:18:54/00:01:33 v2    1 / S P G
2.2.2.2           Lspvif0                  1d00h/00:01:34    v2    1 / S P G
22.22.22.22       Lspvif0                  1d00h/00:01:34    v2    1 / DR S P G
```

show ip mroute コマンドの出力には、VRF の（S、G）エントリも表示されます。ストリーム 225.1.1.1 には、LSP-VIF インターフェイス 101 のリバース パス フォワーディング（RPF）インターフェイスと、ネイバー 2.2.2.2（PE-West）があります。

```
PE-East# show ip mroute vrf vrf3001 225.1.1.1 30.22.1.10
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group, c - PFP-SA cache created entry,
       * - determined by Assert, # - iif-starg configured on rpf intf,
       e - encap-helper tunnel flag
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(30.22.1.10, 225.1.1.1), 00:31:08/00:02:14, flags: JTY
  Incoming interface: Lspvif101, RPF nbr 2.2.2.2, MDT: [2, 2.2.2.2]/00:02:51
  Outgoing interface list:
    Vlan3001, Forward/Sparse, 00:31:08/00:02:35
```

MLDP データベースエントリ：PE-East

このセクションの出力例には、PE-East のデフォルト MDT をサポートする MP2MP ツリーのデータベースエントリが表示されています。データベースは Opaque 値 MDT 3001:1 で検索され、2 つの MP2MP ツリー（ルートごとに 1 つ）の情報が返されます。両方のツリーのシステム ID は異なり、同じ Opaque 値（[[mdt 3001:1 1]）が使用されますが、ルートが異なります。エントリ 3E0 は、それがプライマリ MP2MP ツリーであることを示しているため、PE-East は

このLSP上のすべての送信元マルチキャストトラフィックを送信し、21Cがバックアップルートになります。インターフェイス LSP-VIF インターフェイス 101 は、両方の MP2MP LSP を表します。ローカルラベル（D）は、PE-East によってこのツリーに割り当てられたダウンストリームラベルです。つまり、ルートからのトラフィックは、プライマリツリーまたはバックアップツリーのいずれかで受信されます。アウトラベル（U）は、PE-Eastがトラフィックをツリー、ルートへのアップストリームに送信するために使用するラベルです（プライマリツリーの場合は 361、バックアップツリーの場合は 363）。ラベルはどちらも P-Central から受信しています。

```
PE-East# show mpls mldp database opaque_type mdt 3001:1
LSM ID : 3E0   Type: P2MP   Uptime : 00:34:24
  FEC Root           : 2.2.2.2
  Opaque decoded     : [mdt 3001:1 1]
  Opaque length      : 11 bytes
  Opaque value       : 02 000B 003001000000100000001
  Upstream client(s) :
    33.33.33.33:0    [Active]
      Expires        : Never         Path Set ID  : 1C0
      Out Label (U)  : None          Interface    : Port-channel23*
      Local Label (D): 361           Next Hop     : 104.2.3.2
  Replication client(s):
    MDT  (VRF vrf3001)
      Uptime         : 00:34:24      Path Set ID  : None
      Interface      : Lspvif101     RPF-ID       : *

LSM ID : 21C   Type: P2MP   Uptime : 00:34:16
  FEC Root           : 2.2.2.2
  Opaque decoded     : [mdt 3001:1 2]
  Opaque length      : 11 bytes
  Opaque value       : 02 000B 003001000000100000002
  Upstream client(s) :
    33.33.33.33:0    [Active]
      Expires        : Never         Path Set ID  : 17D
      Out Label (U)  : None          Interface    : Port-channel23*
      Local Label (D): 363           Next Hop     : 104.2.3.2
  Replication client(s):
    MDT  (VRF vrf3001)
      Uptime         : 00:34:16      Path Set ID  : None
      Interface      : Lspvif101     RPF-ID       : *
```

ラベル転送エントリ：P-Central（ルート 1）

このセクションの出力例には、P-Centralであるプライマリ MP2MP LSP の VRF（MDT 3001:1）MLDP データベースエントリ 7035A が表示されています。ローカルデバイス P-Central がルートであるため、アップストリームピア ID はなく、ローカルに割り当てられているラベルはありません。ただし、3 つの PE デバイス（PE-North、PE-West、および PE-East）を表す 3 つのレプリケーションクライアントがあります。これらのレプリケーションクライアントは、P2MP LSPのダウンストリームノードです。これらのクライアントは、マルチポイント複製トラフィックを受信します。

ルートの観点から見たレプリケーションエントリには、次の 2 つのタイプのラベルがあります。

- アウトラベル（D）：これらは、ルートへのダウンストリームであるリモートピアから受信したラベルです（トラフィックフローはルートからダウンストリームになります）。

- ローカルラベル（U）：これらは、P-Central からネイバーに提供されるラベルで、アップストリームラベル（ルートにトラフィックを送信）として使用されます。ローカルラベルはすべて、P-Central で使用するように設定した 100 の範囲内で始まるため簡単に識別できます。P-Central は、タイプが MP2MP Down の FEC を受信すると、ローカルラベルを送信します。

レプリケーションエントリで送受信されたラベルから、ラベル転送情報ベース（LFIB）が作成されます。LFIB には、アップストリームパスごとに 1 つのエントリと、ダウンストリームパスごとに 1 つのエントリがあります。この場合、P-Central がルートであるため、対応するダウンストリームラベルとマージされたアップストリームエントリのみが LFIB にあります。たとえば、ラベル 105 は、送信元トラフィックをアップストリームに送信するために PE-East に送信されるラベル P-Central です。PE-East から受信したトラフィックは、ダウンストリームラベル 307 を使用して PE-West に、ラベル 208 を使用して PE-North に複製されます。

```
P-Central# show mpls mldp database opaque_type mdt 3001:1
LSM ID : 7035A   Type: P2MP   Uptime : 00:01:13
  FEC Root           : 2.2.2.2
  Opaque decoded     : [mdt 3001:1 1]
  Opaque length      : 11 bytes
  Opaque value       : 02 000B 003001000000100000001
  Upstream client(s) :
    33.33.33.33:0    [Active]
      Expires        : Never         Path Set ID  : 501A2
      Out Label (U)  : None          Interface    : Vlan31*
      Local Label (D): 997           Next Hop     : 104.3.1.2
  Replication client(s):
    MDT  (VRF vrf3001)
      Uptime         : 00:01:13      Path Set ID  : None
      Interface      : Lspvif1       RPF-ID       : *
```

このセクションの出力例には、PE-North（バックアップルート）をルートとする P2MP LSP の P-Central のエントリが表示されています。このツリーでは、P-Central はツリーのブランチであり、ルートではありません。そのため、注意すべき点がいくつかあります。

- アップストリームピア ID は PE-North であるため、P-Central は PE-North へのダウンストリーム方向にラベル 915 を割り当てています。PE-North はその後アップストリームラベルで応答しています。
- PE-East と PE-West を表す 2 つのレプリケーションエントリが表示されます。
- マージされた LFIB には次の 3 つのエントリが表示されます。
  - ルート 2（PE-North）からトラフィックを受信する 1 つのダウンストリームエントリ（ラベル 915）。トラフィックは、PE-West および PE-East のアウトラベルを使用してさらにダウンストリームに転送されます。
  - リーフからトラフィックを受信し、アウトラベルを使用してダウンストリームまたはアップストリームに転送する 2 つのアップストリームエントリ。

```
Central_P# show mpls mldp database opaque_type mdt 3001:1
LSM ID : 3024C (RNR LSM ID: 1026F)   Type: MP2MP   Uptime : 2w3d
FEC Root               : 2.2.2.2
```

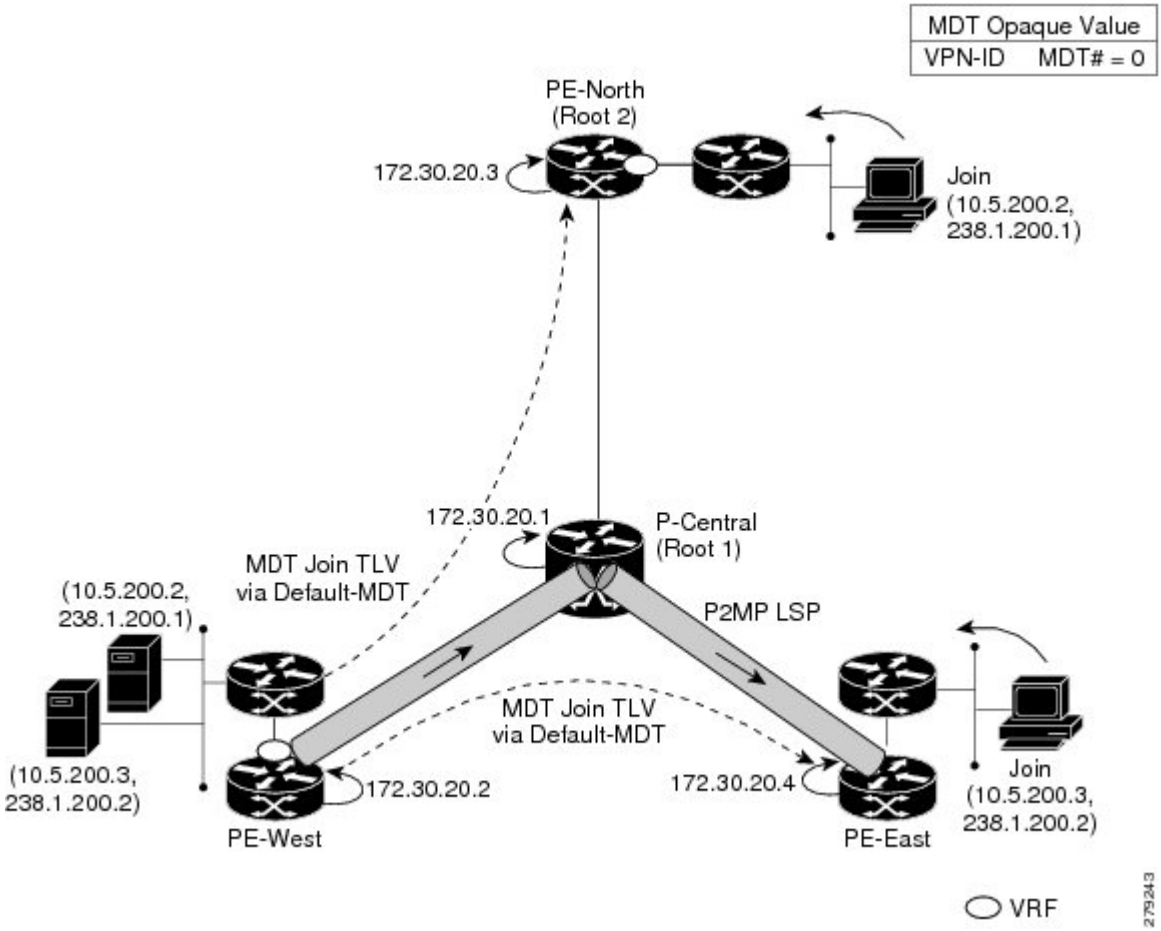
```
Opaque decoded          : [mdt 3001:1 0]
Opaque length           : 11 bytes
Opaque value            : 02 000B 003001000000100000000
RNR active LSP          : 101F6 (root: 22.22.22.22)
Upstream client(s)      :
33.33.33.33:0 [Active]
Expires                 : Never         Path Set ID   : D0157
Out Label (U)           : 4069          Interface     : Port-channel31*
Local Label (D)         : 915           Next Hop      : 104.3.1.2
Replication client(s)   :
> MDT (VRF vrf3001)
Uptime                  : 2w3d          Path Set ID   : F0036
Interface               : Lspvif1       RPF-ID        : *
7.7.7.7:0
Uptime                  : 1d20h         Path Set ID   : B01ED
Out label (D)           : 25            Interface     : Port-channel71.1*
Local label (U)         : 941           Next Hop      : 104.71.1.1

LSM ID : 101F6 (RNR LSM ID: 1026F)   Type: MP2MP   Uptime : 21:17:45
FEC Root                : 22.22.22.22 (we are the root)
Opaque decoded          : [mdt 3001:1 0]
Opaque length           : 11 bytes
Opaque value            : 02 000B 003001000000100000000
RNR active LSP          : (this entry)
Candidate RNR ID(s)     : 3024C
Upstream client(s)      :
None
Expires                 : N/A           Path Set ID   : F007B
Replication client(s)   :
> MDT (VRF vrf3001)
Uptime                  : 20:51:46      Path Set ID   : C001F
Interface               : Lspvif1       RPF-ID        : *
7.7.7.7:0
Uptime                  : 20:51:43      Path Set ID   : C0020
Out label (D)           : 44            Interface     : Port-channel71.1*
Local label (U)         : 1191          Next Hop      : 104.71.1.1
33.33.33.33:0
Uptime                  : 00:00:34      Path Set ID   : 100049
Out label (D)           : 3109          Interface     : Port-channel31*
Local label (U)         : 1340          Next Hop      : 104.3.1.2
```

データ MDT の設定

次に、MLDP ベースの MVPN のデータ MDT を設定する例を示します。この設定は、図に示されているトポロジ例に基づいています。

図 *42* : データ *MDT* の例



このセクションの出力例には、すべての PE デバイスのデータ MDT の設定が表示されています。必要な追加コマンドは **mdt data** コマンドだけです。最初の **mdt data** コマンドでは最大 60 個のデータ MDT を作成でき、2 番目の **mdt data** コマンドではしきい値を設定できます。データ MDT の数が 60 を超えると、データ MDT は mGRE トンネル方式（参照カウントが最も低い方式）の場合と同じ方法で再利用されます。

```
ip pim vrf VRF mpls source Loopback0
!
ip vrf VRF
 rd 100:2
 vpn id 100:2
 route-target export 200:2
 route-target import 200:2
 mdt default mpls mldp 172.30.20.1 (P-Central)
 mdt default mpls mldp 172.30.20.3 (PE-North)
 mdt data mpls mldp 60
 mdt data threshold 1
```

VRF mroute テーブル：PE-West

このセクションの出力例には、高帯域幅の送信元がしきい値を超える前の PE-West の VRF mrouteテーブルが表示されています。この時点で、単一のMP2MP LSP（システムID 2）上に、PE-West の 2 つの VPN 送信元を表す 2 つのストリームがあります。LSP は、LSP-VIF インターフェイス 0 を介してアクセスされるデフォルト MDT を表します。

```
PE-West# show ip mroute vrf vrf3001 verbose.
.
.

(30.0.5.10, 228.1.1.1), 16:08:00/00:02:21, flags: FTAp
Incoming interface: Vlan3001, RPF nbr 0.0.0.0
Outgoing interface list:
Lspvif0, LSM MDT: 2 (default), Forward/Sparse, 16:08:00/00:03:25, Pkts:0, p

.
.
.

(30.0.5.10, 228.1.1.3), 15:55:20/00:01:38, flags: FTAp
Incoming interface: Vlan3001, RPF nbr 0.0.0.0
Outgoing interface list:
Lspvif0, LSM MDT: 2 (default), Forward/Sparse, 15:55:13/00:02:44, Pkts:0, p
```

このセクションの出力例には、送信元の送信料がしきい値を超えた後の出力が表示されています。PE-West は MDT Join TLV メッセージを送信して、データ MDT の構築を通知します。この場合、データ MDT 番号は 8 であるため、PE-East は、ルート = PE-West、Opaque 値 =（mdt vpn-id 8）を含む FEC TLV を使用して、ラベルマッピングメッセージを PE-West に返送します。システム ID は D に変更され、別の LSP をシグナリングします。ただし、LSP-VIF は引き続き LSP-VIF インターフェイス 0です。（S、G）エントリには、このストリームがデータ MDT に切り替わったことを示す「y」フラグも設定されます。

```
PE-West# show ip mroute vrf vrf3001 228.1.1.3 30.0.5.10 verbose
.
.
.
(30.0.5.10, 228.1.1.3), 16:00:17/00:02:49, flags: FTAyp
Incoming interface: Vlan3001, RPF nbr 0.0.0.0
MDT TX nr: 8 LSM-ID: 0xD
Outgoing interface list:
Lspvif0, LSM MDT: D (data), Forward/Sparse, 16:00:10/00:02:43, Pkts:0, p
```

MLDP データベースエントリ

このセクションの出力例には、入力デバイス PE-West のデータ MDT（F）の MLDP エントリが表示されています。このエントリに関する次の点に注意してください。

- ツリータイプは P2MP で、ルートは PE-West（5.5.5.5）です。
- Opaque 値は [mdt 3001:1 10] で、最初のデータ MDT を示しています。
- ルートであるため、ラベルは割り当てられていません。
- このツリーには 1 つのレプリケーション クライアント エントリがあります。

• MDT エントリは内部構造です。

```
PE-West# show mpls mldp database id F
LSM ID : F   Type: P2MP   Uptime : 00:02:37
  FEC Root           : 5.5.5.5 (we are the root)
  Opaque decoded     : [mdt 3001:1 10]
  Opaque length      : 11 bytes
  Opaque value       : 02 000B 003001000000010000000A
  Upstream client(s) :
    None
      Expires        : N/A           Path Set ID  : 10
  Replication client(s):
>   MDT  (VRF vrf3001)
      Uptime         : 00:02:37      Path Set ID  : None
      Interface      : Lspvif0       RPF-ID       : *
    33.33.33.33:0
      Uptime         : 00:02:37      Path Set ID  : None
      Out label (D)  : 3326          Interface    : Port-channel23*
      Local label (U): None          Next Hop     : 104.2.3.2
```

このセクションの出力例には、出力デバイスである PE-East のデータ MDT のデータベースエントリが表示されています。また、デフォルト MDT を介して PE-West から送信された MDT Join TLV メッセージも表示されます。MDT Join TLV メッセージには、PE-East がラベルマッピングメッセージ P2MP LSP を作成して PE-West のルートに戻すために必要なすべての情報が含まれています。

```
PE-East# show mpls mldp database opaque_type mdt 3001:1
LSM ID : CD   Type: P2MP   Uptime : 00:33:46
  FEC Root           : 2.2.2.2 (we are the root)
  Opaque decoded     : [mdt 3001:1 1]
  Opaque length      : 11 bytes
  Opaque value       : 02 000B 003001000000010000000001
  Upstream client(s) :
    None
      Expires        : N/A           Path Set ID  : D8
  Replication client(s):
>   MDT  (VRF vrf3001)
      Uptime         : 00:33:46      Path Set ID  : None
      Interface      : Lspvif101     RPF-ID       : *
    33.33.33.33:0
      Uptime         : 00:33:46      Path Set ID  : None
      Out label (D)  : 348           Interface    : Vlan2222*
      Local label (U): None          Next Hop     : 26.1.3.2

LSM ID : CE   Type: P2MP   Uptime : 00:33:38
  FEC Root           : 2.2.2.2 (we are the root)
  Opaque decoded     : [mdt 3001:1 2]
  Opaque length      : 11 bytes
  Opaque value       : 02 000B 003001000000010000000002
  Upstream client(s) :
    None
      Expires        : N/A           Path Set ID  : D9
  Replication client(s):
>   MDT  (VRF vrf3001)
      Uptime         : 00:33:38      Path Set ID  : None
      Interface      : Lspvif101     RPF-ID       : *
    33.33.33.33:0
      Uptime         : 00:33:38      Path Set ID  : None
      Out label (D)  : 2399          Interface    : Vlan2222*
```

```
      Local label (U): None          Next Hop     : 26.1.3.2
```

データ MDT の LFIB エントリ

このセクションの出力例には、P-Central および PE-East を通過するデータ MDT の LFIB エントリが表示されています。LSP に使用されるトンネル ID は Opaque 値 [mdt 3001:1 0] です。

```
P-Central# show mpls forwarding-table labels 1191
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
1191       2602       [mdt 3001:1 0][V]   \
                                       156663076     Po31       104.3.1.2
      [T]  No Label   [mdt 3001:1 0][V]   \
                                       45279264      aggregate/vrf3001

[T]     Forwarding through a LSP tunnel.
        View additional labelling info with the 'detail' option

PE-East# show mpls forwarding-table vrf vrf3001
 Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
132        No Label   30.0.1.0/24[V]   0             drop
133        Pop Label  30.30.1.1/32[V]  0             aggregate/vrf3001
137        Pop Label  30.1.30.1/32[V]  0             aggregate/vrf3001
138        No Label   30.0.5.0/24[V]   0             aggregate/vrf3001
142   [T]  No Label   [mdt 3001:1 0][V]   \
                                       905056        aggregate/vrf3001
145   [T]  No Label   [mdt 3001:1 0][V]   \
                                       7448          aggregate/vrf3001

[T]     Forwarding through a LSP tunnel.
        View additional labelling info with the 'detail' option
```

例：MVPN プロファイル 1 - デフォルト MDT - MLDP MP2MP - PIM C-mcast シグナリングの設定

次に、MVPN プロファイル 1 を設定する例を示します。

```
vrf definition one
 rd 1:2
 vpn id 1000:2000
!
 address-family ipv4
  mdt default mpls mldp 10.100.1.1
  route-target export 1:1
  route-target import 1:1
 exit-address-family
!

ip multicast-routing vrf one

mpls mldp logging notifications

router bgp 1
 bgp log-neighbor-changes
 neighbor 10.100.1.7 remote-as 1
 neighbor 10.100.1.7 update-source Loopback0
 !
```

```
 address-family vpnv4
  neighbor 10.100.1.7 activate
  neighbor 10.100.1.7 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf one
  redistribute connected
  neighbor 10.2.2.9 remote-as 65002
  neighbor 10.2.2.9 activate
 exit-address-family
```

例：MVPN プロファイル 13 - デフォルト MDT - MLDP - MP2MP - BGP-AD - BGP C-mcast シグナリングの設定

次に、MVPN プロファイル 13 を設定する例を示します。

```
vrf definition one
 rd 1:1
 vpn id 1000:2000
 !
 address-family ipv4
  mdt auto-discovery mldp
  mdt default mpls mldp 10.100.1.3
  mdt overlay use-bgp
  route-target export 1:1
  route-target import 1:1
 exit-address-family
!

interface Ethernet2/0
 vrf forwarding one
 ip address 10.2.1.1 255.255.255.0
 ip pim sparse-mode

router bgp 1
 neighbor 10.100.1.7 remote-as 1
 neighbor 10.100.1.7 update-source Loopback0
 !
 address-family ipv4 mvpn
  neighbor 10.100.1.7 activate
  neighbor 10.100.1.7 send-community extended
 exit-address-family
 !
 address-family vpnv4
  neighbor 10.100.1.7 activate
  neighbor 10.100.1.7 send-community extended
 exit-address-family
!
```

例：MVPN プロファイル 14 - パーティション MDT - MLDP P2MP - BGP-AD - BGP C-mast シグナリングの設定

次に、MVPN プロファイル 14 を設定する例を示します。

```
vrf definition one
 rd 1:1
```

```
 !
 address-family ipv4
  mdt auto-discovery mldp
  mdt strict-rpf interface
  mdt partitioned mldp p2mp
  mdt overlay use-bgp
  route-target export 1:1
  route-target import 1:1
 exit-address-family

!
interface Ethernet2/0
 vrf forwarding one
 ip address 10.2.1.1 255.255.255.0
 ip pim sparse-mode
!

router bgp 1
 neighbor 10.100.1.7 remote-as 1
 neighbor 10.100.1.7 update-source Loopback0
 !
 address-family ipv4 mvpn
  neighbor 10.100.1.7 activate
  neighbor 10.100.1.7 send-community extended
 exit-address-family
 !
 address-family vpnv4
  neighbor 10.100.1.7 activate
  neighbor 10.100.1.7 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf one
  redistribute connected
  neighbor 10.2.1.8 remote-as 65001
  neighbor 10.2.1.8 activate
 exit-address-family
!
```

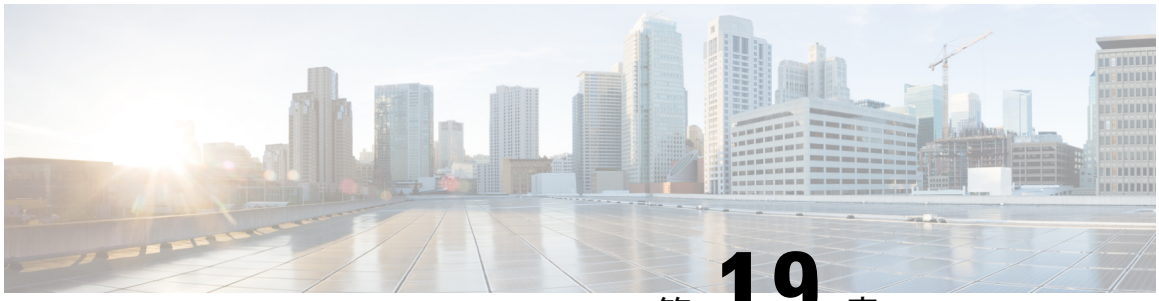
MLDP ベースの MVPN の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Amsterdam 17.3.3	MLDP-Based MVPN	MLDP ベースの MVPN 機能は、マルチキャスト仮想プライベートネットワーク（MVPN）コアネットワークでの転送用に、ポイントツーマルチポイント（P2MP）およびマルチポイントツーマルチポイント（MP2MP）ラベルスイッチドパス（LSP）を設定するためのラベル配布プロトコル（LDP）の拡張機能を提供します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。



第 19 章

IP マルチキャストの最適化：大規模な IP マルチキャスト展開での PIM スパース モードの最適化

大規模な IP マルチキャスト展開での PIM スパース モードの最適化の前提条件

- PIM スパース モードがネットワークで実行されている必要があります。
- どのグループに最短パス ツリー（SPT）しきい値を適用するかを制御するのにグループ リストを使用することを計画している場合は、この作業を実行する前にアクセス リストを設定する必要があります。

大規模な IP マルチキャスト展開での PIM スパース モードの最適化について

PIM 登録プロセス

IP マルチキャスト ソースは、その存在をアナウンスするのにシグナリング メカニズムを使用しません。送信元は接続ネットワークにデータを送信するだけなのに対し、受信者は Internet Group Management Protocol（IGMP）を使用して、自身の在席状態を示します。ソースが PIM スパースモード（PIM-SM）で設定されているマルチキャストグループにトラフィックを送信すると、ソースにつながる指定ルータ（DR）は、このソースの存在についてランデブー ポイント（RP）に知らせなければなりません。この送信元からマルチキャストトラフィックを（ネイティブに）受信するダウンストリーム受信者がRPにいて、RPが送信元につながる最短パスに加入していない場合、DRはトラフィックを送信元からRPに送信する必要があります。PIM 登録プロセスは、各 (S, G) エントリに対し個別に実行されますが、DR と RP 間のこれらのタスクを実行します。

登録プロセスは、DR が新しい (S, G) ステートを作成すると開始されます。DR は、(S, G) ステートに一致するすべてのデータ パケットを PIM 登録メッセージにカプセル化し、それらの登録メッセージを RP にユニキャストします。

RP が新しいソースからの登録メッセージを受信したいダウンストリーム レシーバを持っている場合は、RP は、登録メッセージを DR を通じて受信し続けることも、ソースにつながる最短パスに加入することもできます。デフォルトでは、ネイティブ マルチキャスト トラフィックの配信が最も高いスループットを実現するため、RP は最短パスに加入します。最短パス経由でネイティブに到着した最初のパケットを受信後、RP は DR に登録停止メッセージを送り返します。DRは、この登録停止メッセージを受信したら、RPへの登録メッセージの送信を停止します。

RP に新しい送信元からの登録メッセージを受信するダウンストリーム受信者がいない場合、RP は最短パスに加入しません。その代わり、RP は、ただちに DR に登録停止メッセージを送り返します。DRは、この登録停止メッセージを受信したら、RPへの登録メッセージの送信を停止します。

いったんソースへのルーティング エントリが確立されたら、DR と RP の間で定期的な再登録が発生します。DR が RP から登録停止メッセージを受信するまでは、ソースがアクティブであれば、マルチキャスト ルーティング テーブル ステートがタイムアウトする 1 分前に DR が1つのデータのない登録メッセージをRPに送信します。このアクションがマルチキャストルーティングテーブルエントリのタイムアウト時間をリスタートさせ、通常は、2分ごとに1つの登録交換が行われることになります。登録は、ステートを維持するため、ステート損失から回復するため、およびRP上でソースを追跡するために必要です。これは、RPの最短パスへの加入からは独立して発生します。

PIM バージョン 1 の互換性

RP が PIM バージョン 1 を実行している場合、それはデータのない登録メッセージは理解しません。この場合、DR は RP にデータのない登録メッセージを送信しません。代わりに、RP から登録停止メッセージを受信後約 3 分おきに、DR は送信元からの着信データ パケットを登録メッセージにカプセル化し、それを RP に送信します。DR は RP から別の登録停止メッセージを受信するまで、登録メッセージを送信し続けます。DR が PIM バージョン 1 を実行している場合、同じ動作が起こります。

PIM バージョン 1 を実行している DR が特定の (S, G) エントリ向けの登録メッセージにデータ パケットをカプセル化すると、エントリではプロセス スイッチングが行われます（高速スイッチングやハードウェア スイッチングではない）。これらの高速パスをサポートしているプラットフォームでは、PIM バージョン 1 を実行している RP または DR の PIM 登録プロセスが、定期的で不適切なパケット配信の原因となる可能性があります。そのため、ネットワークを PIM バージョン 1 から PIM バージョン 2 にアップグレードすることを推奨しています。

PIM 指定ルータ

IP マルチキャスト用に設定されているデバイスは、PIM ハロー メッセージを送信して、どのデバイスが各 LAN セグメント（サブネット）の指定ルータ（DR）であるかを調べます。ハロー メッセージにはデバイスの IP アドレスが含まれており、最も大きい IP アドレスを持つデバイスが DR になります。

DR は、直接接続された LAN 上のすべてのホストに Internet Group Management Protocol（IGMP）ホスト クエリ メッセージを送信します。スパース モードで稼働している場合は、DR は、ソース登録メッセージをランデブー ポイント（RP）に送信します。

デフォルトでは、マルチキャスト デバイスは、30 秒ごとに PIM ルータ クエリ メッセージを送信します。デバイスがより頻繁に PIM ハロー メッセージを送信できるようにすることにより、デバイスは、応答しないネイバーをより迅速に検出できるようになります。その結果、デバイスは、より効率的なフェールオーバー手順または回復手順を実装できます。この変更は、ネットワークのエッジ上の冗長デバイスに対してのみ行うことが推奨されます。

PIM スパース モード登録メッセージ

データのない登録メッセージは、1 秒に 1 メッセージのレートで送信されます。DR が集中的なソース（データ レートの高いソース）を登録しており、RP が PIM バージョン 2 を実行していない場合は、連続的に高いレートの登録メッセージが発生する可能性があります。

デフォルトでは、PIM スパース モード登録メッセージは、レート制限なしで送信されます。登録メッセージのレートを制限すると、設定された制限を超えた登録メッセージはドロップされるという代償を伴いますが、DR および RP にかかる負荷が制限されます。レシーバは、パケットが集中的なソースから送信されてから最初の 1 秒間に、データ パケット損失を経験する可能性があります。

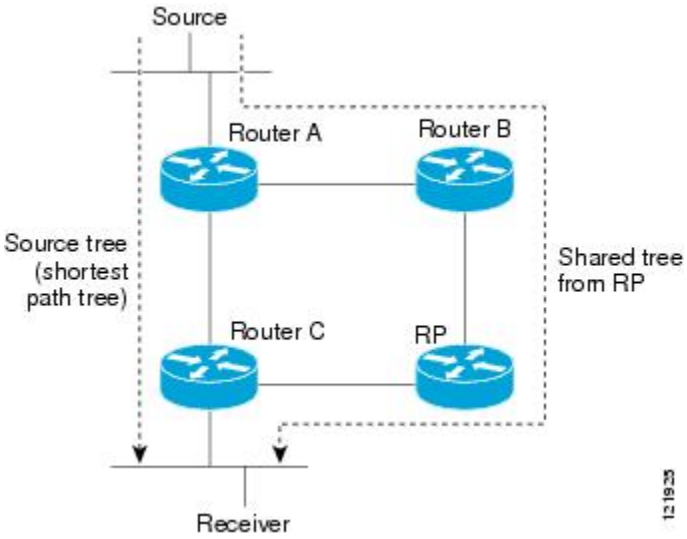
メモリ要件を減らすために最短パス ツリーの使用を回避する

PIM 共有ツリーとソース ツリーを理解しておくと、最短パス ツリーの使用を回避することでどのようにメモリ要件を減らせるかについて理解しやすくなります。

PIM 共有ツリーおよびソース ツリー（最短パス ツリー）

デフォルトでは、ランデブー ポイント（RP）がルートになる単一のデータ配信ツリー全体にわたって、マルチキャスト グループのメンバが送信者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、図に示すように、共有ツリーと呼ばれます。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。

図 *43*：共有ツリーとソース ツリー（最短パス ツリー）



データ レートで保証される場合、共有ツリー上のリーフ ルータは、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。このタイプの配信ツリーは、最短パス ツリー（SPT）またはソース ツリーと呼ばれます。デフォルトでは、ソフトウェアが送信元から最初のデータ パケットを受信すると、送信元ツリーに切り替わります。

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. レシーバがグループに加入します。リーフ ルータであるルータ C が、RP に向けて加入メッセージを送信します。
2. RP がルータ 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。ルータ A はデータをカプセル化して登録メッセージに格納し、RP に送信します。
4. RP が、データを共有ツリーの下流に向けて、ルータ C に転送し、ソースに向けて加入メッセージを送信します。この時点で、データはルータ 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に（マルチキャストを通じて）RP に到着すると、RP は、ルータ A に登録停止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の受信で、ルータ C のソースへの加入メッセージ送信が促されます。
7. ルータ C は、(S, G) でデータを受信すると、共有ツリーの上流に向けて、ソースのプルーニング 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ルータ C へのリンクを削除します。RP は、ソースに向けてプルーニング メッセージをトリガーします。

加入メッセージとプルーニング メッセージが、ソースと RP に送信されます。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 に向かうパス上の各 PIM ルータによって処理されます。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ルータによって送信され、グループの RP によって受信されます。

グループへ送信する複数の送信元で、共有ツリーが使用されます。

最短パスツリーの使用を回避または延期する利点

共有ツリーからソース ツリーへのスイッチは、最初のデータ パケットのラスト ホップ デバイス（PIM 共有ツリーおよびソース ツリー（最短パス ツリー） （472 ページ） でのルータ C）への到着によって発生します。このスイッチが発生するのは、**ip pim spt-threshold** コマンドがタイミングを制御しているためで、そのデフォルト設定は 0 kbps です。

最短パスツリーは共有ツリーより多くのメモリを必要としますが、遅延は低減します。この使用を回避または延期して、メモリの要件を減らすことができます。リーフデバイスがただちに最短パスツリーに移動できるようにする代わりに、SPT の使用を防止したり、まずトラフィックがしきい値に到達しなければならないように指定したりできます。

PIM リーフ デバイスが、指定グループの SPT に加入する時期を設定できます。送信元の送信速度が指定速度（キロビット/秒）以上の場合、デバイスは PIM Join メッセージを送信元に向けて送信し、ソース ツリー（SPT）を構築します。**infinity** キーワードを指定すると、指定されたグループのすべての送信元で共有ツリーが使用され、送信元ツリーに切り替わらなくなります。

大規模な IP マルチキャスト展開で PIM スパース モードを最適化する方法

大規模な展開での PIM スパース モードの最適化

IP マルチキャストの展開が大規模な場合には、この作業を行うことを検討してください。

このタスクのステップ3、5、および6は相互に依存せず、オプションと見なされます。これらの手順はいずれも、PIM スパース モードの最適化に役立ちます。ステップ 5 または 6 を実行する場合は、ステップ 4 を実行する必要があります。ステップ 6 は、指定ルータにしか適用されません。PIM クエリーの間隔の変更は、PIM ドメインのエッジにある冗長ルータに対してしか適切ではありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip pim register-rate-limit** *rate*
4. **ip pim spt-threshold** {*kbps*| **infinity**}[**group-list** *access-list*]
5. **interface** *type number*
6. **ip pim query-interval** *period* [**msec**]

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： `Router> 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： `Router# 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	**ip pim register-rate-limit** *rate* 例： `Router(config)# ip pim register-rate-limit 10`	（任意）各 (S, G) ルーティング エントリについて、1 秒当たりに送信される PIM スパース モード登録メッセージの最大数の制限を設定します。 • このコマンドは、指定ルータ（DR）が各 (S, G) エントリに許可する登録メッセージ数を制限する場合に使用します。 • デフォルトでは、最大レートは設定されていません。 • このコマンドを設定すると、設定された制限を超えた登録メッセージはドロップされるという代償を伴いますが、DRおよびRPへの負荷は制限されます。 • レシーバは、登録メッセージが集中的なソースから送信されてから最初の1秒間に、データ パケット損失を経験する可能性があります。

	コマンドまたはアクション	目的
ステップ 4	**ip pim spt-threshold** {*kbps*| **infinity**}[**group-list** *access-list*] 例： `Router(config)# ip pim spt-threshold infinity group-list 5`	（任意）最短パスツリーに移行するには超えなければならないしきい値を指定します。 • デフォルト値は **0** です。この場合、ルータは、最初のデータパケットを受信するとただちに SPT に加入します。 • **infinity** キーワードを指定すると、最短パスツリーへの移行は一切行われなくなり、共有ツリーのままとなります。このキーワードは、「多対多」通信のマルチキャスト環境に適用されます。 • グループ リストは、SPT のしきい値がどのグループに適用されるかを制御する標準アクセスリストです。0の値を指定するか、またはグループ リストを指定しなかった場合、しきい値はすべてのグループに適用されます。 • この例では、グループ リスト 5 は、すでにマルチキャスト グループ 239.254.2.0 および 239.254.3.0 を許可するように設定されています（access-list 5 permit 239.254.2.0 0.0.0.255 access-list 5 permit 239.254.3.0 0.0.0.255）。
ステップ 5	**interface** *type number* 例： `Router(config)# interface Gigabitethernet 1/0/1`	インターフェイスを設定します。 • PIM SPT しきい値または PIM クエリー間隔のデフォルト値を変更したくない場合は、このステップは実行しないでください。このステップで変更が行われます。
ステップ 6	**ip pim query-interval** *period* [**msec**] 例： `Router(config-if)# ip pim query-interval 1`	（任意）マルチキャスト ルータが PIM ルータ クエリー メッセージを送信する頻度を設定します。 • この手順は、PIM ドメインのエッジにある冗長ルータに対してだけ実行してください。 • デフォルトのクエリー間隔は 30 秒です。 • **msec** キーワードを指定しない限り、*period* 引数の単位は秒です。 • クエリー間隔を少ない秒数に設定するとコンバージェンスを高速化できますが、コンバージェンスの高速化と引き換えに CPU と帯域幅の使用量が大きくなります。

大規模なマルチキャスト展開での PIM スパース モードの最適化の設定例

大規模な IP マルチキャスト展開での PIM スパース モードの最適化の例

次の例は、下記のことを行う方法を示します。

- クエリー間隔を 1 秒に設定して、コンバージェンスを高速化する。
- ルータが一切 SPT に移行せず、共有ツリーに留まるように設定する。
- 各 (S, G) ルーティング エントリについて、1 秒当たりに送信される PIM スパース モード登録メッセージの制限を 10 個に設定する。

```
interface Gigabitethernet 1/0/1
 ip pim query-interval 1
.
.
.
!
ip pim spt-threshold infinity
ip pim register-rate-limit 10
!
```

IP マルチキャストの最適化：大規模な IP マルチキャスト展開での PIM スパース モードの最適化に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)*

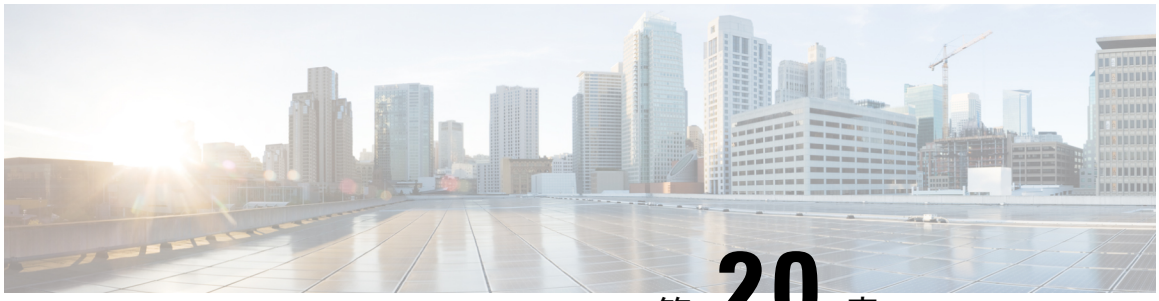
IP マルチキャストの最適化の機能履歴：大規模な IP マルチキャスト展開での PIM スパースモードの最適化

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IP マルチキャストの最適化：大規模な IP マルチキャスト展開での PIM スパース モードの最適化	Protocol Independent Multicast（PIM）には、スパースモードとデンスモードの 2 つの基本的な動作モードがあり、多様なリンクやデバイスが混在する大規模なネットワークに適しています。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/にアクセスします。



第 20 章

IPマルチキャストの最適化：マルチキャスト サブセカンド コンバージェンス

マルチキャストサブセカンドコンバージェンスの前提条件

サービス プロバイダは、シスコ マルチキャスト サブセカンド コンバージェンス機能を使用するには、マルチキャスト対応コアが必要です。

マルチキャストサブセカンドコンバージェンスの制約事項

サブセカンド指定ルータ（DR）フェールオーバー拡張機能を使用するデバイスは、到着したHello インターバル情報をミリ秒単位で処理できる必要があります。輻輳しているデバイス、またはHello インターバルを処理するための十分なCPU サイクルがないデバイスは、それが事実でない可能性があっても、Protocol Independent Multicast（PIM）ネイバーが切断されていると見なす可能性があります。

マルチキャストサブセカンドコンバージェンスについて

マルチキャスト サブセカンド コンバージェンスの利点

- スケーラビリティ コンポーネントは、サービス ユーザー（レシーバ）とサービス負荷（ソースまたはコンテンツ）の増加（または減少）を処理する際の効率を向上させます。
- 新しいアルゴリズムとプロセス（最大 1000 個の個別メッセージを 1 つのパケットに入れて配信する、集約された加入メッセージなど）が、コンバージェンスに達するまでの時間を 10 分の 1 にも低減します。
- マルチキャスト サブセカンド コンバージェンスが、大規模なマルチキャスト ネットワークのサービス可用性を向上させます。
- マルチキャスト機能は以前に必要とした何分の1かの時間で元に戻せるため、金融サービス会社や証券会社などのマルチキャスト ユーザーは、Quality of Service（QoS）の向上が得られます。

マルチキャスト サブセカンド コンバージェンス スケーラビリティ拡張機能

マルチキャストサブセカンドコンバージェンス機能は、サービスユーザー（レシーバ）とサービス負荷（ソースまたはコンテンツ）の増加（または減少）を処理する際の効率を向上させるスケーラビリティ拡張機能を提供します。このリリースのスケーラビリティ拡張機能に含まれているものは次のとおりです。

- 新しいタイマー管理テクニックによる、インターネット グループ管理プロトコル（IGMP）と PIM ステート メンテナンスの向上
- Multicast Source Discovery Protocol（MSDP）Source-Active（SA）キャッシュの規模拡張の向上

スケーラビリティ拡張機能には、以下のメリットがあります。

- 可能な PIM マルチキャスト ルート（mroute）、IGMP、および MSDP SA キャッシュ ステート容量の増加
- CPU 使用率の減少

PIM ルータ クエリ メッセージ

マルチキャストサブセカンドコンバージェンスによって、PIMルータ クエリ メッセージ（PIM hello）を数ミリ秒ごとに送信できます。PIM hello メッセージは、隣接する PIM デバイスを探すために使用されます。この機能の導入前は、デバイスは PIM hello を数秒単位でしか送信で

きませんでした。デバイスがより頻繁に PIM ハロー メッセージを送信できるようにすることにより、デバイスは、この機能を使用して応答しないネイバーをより迅速に検出できるようになります。その結果、デバイスは、より効率的なフェールオーバー手順または回復手順を実装できます。

Reverse Path Forwarding

ユニキャスト リバース パス転送（RPF）機能は、裏付けのない IP ソース アドレスを持つ IP パケットを廃棄することにより、ネットワークに変形または偽造（スプーフィング）された IP ソース アドレスが注入されて引き起こされる問題の緩和に役立ちます。変形または偽造（スプーフィング）された送信元アドレスは、送信元 IP アドレスのスプーフィングに基づいたサービス拒絶（DoS）攻撃を示す場合があります。

RPF はアクセス コントロール リスト（ACL）を使用して、不正なまたは偽造の IP 送信元アドレスを持つデータ パケットをドロップまたは転送するかどうかを判断します。ACL コマンドのオプションを使用して、システム管理者は、ドロップまたは転送されたパケットに関する情報をログに記録できます。偽装パケットに関する情報をログに記録しておくと、可能性のあるネットワーク攻撃に関する情報の発見に役立てることができます。

インターフェイスごとの統計情報を使用して、システム管理者は、ネットワーク攻撃のエントリ ポイントとなっているインターフェイスを迅速に検出できます。

トポロジの変更とマルチキャスト ルーティングのリカバリ

マルチキャスト サブセカンド コンバージェンス フィーチャ セットは、ユニキャスト ルーティングのリカバリの後にほぼ瞬時に完了するマルチキャスト パス リカバリを提供することにより、企業とサービス プロバイダ両方のネットワーク バックボーンを強化します。

ネットワーク トポロジの変更が発生すると、PIM は RPF の計算をユニキャスト ルーティング テーブルに依存するため、ユニキャスト プロトコルは最初にトラフィックのベスト パスのオプションを計算する必要があり、その後、マルチキャストはベストパスを決定できるようになります。

マルチキャスト サブセカンド コンバージェンスは、ユニキャストの計算が完了した後の、ほぼ瞬時のマルチキャスト プロトコル計算完了を可能にします。その結果、トポロジの変更後、マルチキャスト トラフィックの転送は大幅に速く復元されます。

マルチキャスト サブセカンド コンバージェンスの設定方法

PIM ルータ クエリ メッセージ間隔の変更

PIM ルータ クエリ メッセージ間隔を変更するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port*
4. **ip pim query-interval** *period* [**msec**]

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	**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	**interface** *type slot* / *subslot* / *port* 例： `Device(config)# interface gigabitethernet 1/0/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip pim query-interval** *period* [**msec**] 例： `Device(config-if)# ip pim query-interval 45`	マルチキャスト ルータが PIM ルータ クエリー メッセージを送信する頻度を設定します。

マルチキャスト サブセカンド コンバージェンス設定の確認

マルチキャスト サブセカンド コンバージェンス機能に関する詳細情報を表示し、確認するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **show ip pim interface** *type number*
3. **show ip pim neighbor**

手順の詳細

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 **show ip pim interface** *type number*

このコマンドを使用して、PIM に設定されているインターフェイスに関する情報を表示します。

次に、**show ip pim interface** コマンドの出力例を示します。

例：

```
Device# show ip pim interface GigabitEthernet 1/0/0
Address          Interface                Ver/   Nbr    Query  DR     DR
                                          Mode   Count  Intvl  Prior
172.16.1.4       GigabitEthernet1/0/0     v2/S   1      100 ms 1      172.16.1.4
```

ステップ 3 **show ip pim neighbor**

Cisco IOS XE ソフトウェアによって検出された PIM ネイバーを表示するには、このコマンドを使用します。

次に、**show ip pim neighbor** コマンドの出力例を示します。

例：

```
Device# show ip pim neighbor
PIM Neighbor Table
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
172.16.1.3        GigabitEthernet1/0/0     00:03:41/250 msec v2    1 / S
```

マルチキャストサブセカンドコンバージェンスの設定例

PIM ルータ クエリ メッセージ インターバルの変更例

次の例では、 **ip pim query-interval** コマンドが 100 ミリ秒に設定されています。このコマンドは、間隔値がデフォルト以外の値になるように設定されていない限り、**show running-config** コマンド出力に表示されません。

```
!
interface gigabitethernet 1/0/1
 ip address 172.16.2.1 255.255.255.0
ip pim query-interval 100 msec
ip pim sparse-mode
```

IPマルチキャストの最適化：マルチキャストサブセカンドコンバージェンスに関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)*

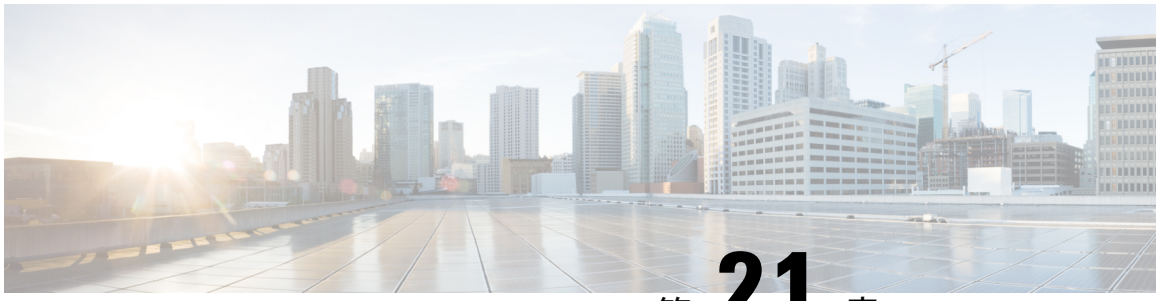
IPマルチキャストの最適化：マルチキャストサブセカンドコンバージェンスの機能情報

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IPマルチキャストの最適化：マルチキャストサブセカンドコンバージェンス	マルチキャスト サブセカンド コンバージェンス機能は、サービス ユーザー（レシーバ）とサービス負荷（ソースまたはコンテンツ）の増加（または減少）を処理する際の効率を向上させるスケーラビリティ拡張機能を提供します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/にアクセスします。



第 21 章

IP マルチキャストの最適化：等コスト パス間での IP マルチキャスト ロード スプリッティング

等コスト パス間での IP マルチキャスト ロード スプリットの前提条件

IP マルチキャストをデバイスで有効にするには、『*IP Multicast Routing Configuration Guide*』の「Configuring Basic IP Multicast」モジュールに記載されているタスクを使用します。

等コスト パス間での IP マルチキャスト ロード スプリッティングについて

ロード スプリットとロード バランシング

ロード スプリットとロード バランシングは同じではありません。ロード スプリットでは、複数の等コスト リバース パス フォワーディング（RPF）パスを介して (*, G) および (S, G) トラフィック ストリームをランダムに分散する手段が提供され、必ずしもそれらの等コスト RPF パス上で平衡のとれた IP マルチキャスト トラフィック負荷が得られるわけではありません。IP マルチキャスト トラフィックのロード スプリットに使用される方法は、(*, G) および (S, G) トラフィック ストリームをランダムに分散させることによって、フローをカウントしてではなく、むしろ疑似乱数判定を作成して、使用可能な各 RPF パスに等価な量のトラフィック フローを分散させようとします。これらの方法は総称して等コスト マルチパス（ECMP）マルチキャスト ロード スプリットと呼ばれ、ほぼ同量の帯域幅を使用する多くのトラフィック ストリームがあるネットワークでのロード シェアリングを向上させます。

一連の等コスト リンクにわたってわずか 2、3 の (S, G) または (*, G) ステート フローしかない場合は、それらの良好なバランスが得られる可能性は非常に低くなります。この制限を克服するため、(S, G) ステートの場合は事前に計算された発信元アドレス、または (*, G) ステートの場合はランデブー ポイント（RP）アドレスを使用して、合理的な形式のロード バランシングを実現できます。この制限は、Cisco Express Forwarding（CEF）または EtherChannel でのフロー単位のロード スプリットに同様に適用されます。わずかなフローがある限り、それらの方法でロード スプリットを行っても、何らかの形式の手動によるエンジニアリングなしでは良好なロード分散は得られません。

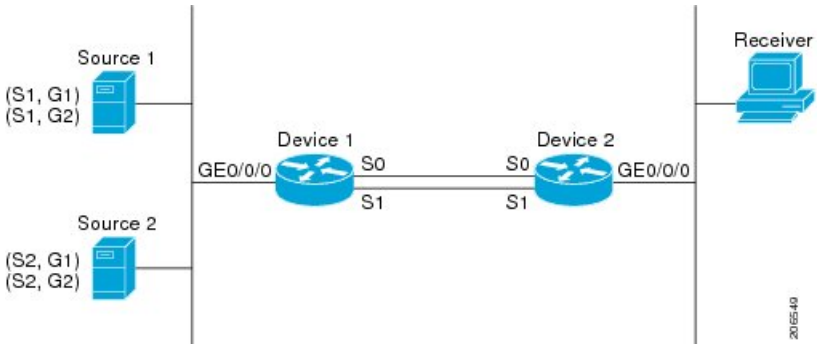
複数の等コスト パスが存在する場合の IP マルチキャストのデフォルト動作

デフォルトでは、Protocol Independent Multicast スパースモード（PIM-SM）、Source Specific Multicast（PIM-SSM）、双方向 PIM（Bidir-PIM）、グループについては、複数の等コストパスが使用可能な場合、IPv4 マルチキャストトラフィック向けのリバースパスフォワーディング（RPF）は、最も大きい IP アドレスを持つ PIM ネイバーに基づきます。この方法は、最高 PIM ネイバー動作と呼ばれます。この動作は、PIM-SM の RFC 2362 に基づいていますが、PIM-SSM、および Bidir-PIM にも適用されます。

次の図に、複数の等コスト パスが存在する場合の IP マルチキャストのデフォルト動作を説明するためにここで使用するサンプル トポロジを示します。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやコントローラ）を使用できます。

図 *44 :* 複数の等コスト パスが存在する場合の *IP* マルチキャストのデフォルト動作



この図では、2 つの送信元 S1 および S2 が、トラフックを IPv4 マルチキャスト グループ G1 および G2 に送信しています。PIM-SM、PIM-SSM、PIM-DM のいずれかをこのトポロジに使用できます。PIM-SM を使用する場合は、**ip pim spt-threshold** コマンドのデフォルト 0 がデバイス 2 で使用中であること、内部ゲートウェイプロトコル（IGP）が実行中であること、S1 および S2 （デバイス 2 で入力した場合）で **show ip route** コマンドの出力に、デバイス 1 のシリアルインターフェイス 0 とシリアルインターフェイス 1 が、デバイス 2 の等コストネクストホップ PIM ネイバーとして表示されることを前提としています。

追加の設定を行うことなく、図に示すトポロジ内の IPv4 マルチキャスト トラフィックは、どちらのインターフェイスがより高い IP アドレスを持っているかに応じて、常に 1 つのシリアル インターフェイス（シリアル インターフェイス 0 またはシリアル インターフェイス 1）を経由して移動します。たとえば、デバイス 1 上のシリアル インターフェイス 0 とシリアル インターフェイス 1 で設定されている IP アドレスが、それぞれ 10.1.1.1 と 10.1.2.1 であるものとします。このシナリオが与えられているとして、PIM-SM と PIM-SSM の場合、デバイス 2 は、図に示されるすべてのソースおよびグループについて、常に PIM 加入メッセージを 10.1.2.1 に送信し、常にシリアル インターフェイス 1 上で IPv4 マルチキャスト トラフィックを受信します。

IPv4 RPF ルックアップが中継マルチキャスト デバイスによって実行され、IPv4 (*,G) および (S, G) マルチキャスト ルート（ツリー）のための RPF インターフェイスと RPF ネイバーが決定されます。RPF ルックアップは、RPF ルート選択とルートパス選択によって構成されます。RPF ルート選択は、マルチキャスト ツリーのルートを特定するために、IP ユニキャスト アドレスだけで動作します。(*, G) ルート（PIM-SM および Bidir-PIM）の場合、マルチキャストツリーのルートはグループ G の RP アドレスです。(S, G) ツリー（PIM-SM、PIM-SSM）の場合、マルチキャストツリーのルートは送信元 S です。RPF ルート選択では、ルーティング情報ベース（RIB）で、また設定済みの場合（または使用可能な場合）は、ディスタンス ベクター マルチキャスト ルーティング プロトコル（DVMRP）ルーティング テーブル、マルチプロトコル ボーダー ゲートウェイ プロトコル（MBGP）ルーティング テーブルまたは設定済みの静的マルチキャストルータで、RP または送信元に対する最適なルートが検索されます。得られたルートが使用可能な 1 つのパスだけだった場合は、RPF ルックアップが完了し、ルートのネクストホップ デバイスおよびインターフェイスが、このマルチキャスト ツリーの RPF ネイバーと RPF インターフェイスになります。そのルートに使用可能な複数のパスがある場合は、ルートパス選択を使用して、どのパスを選択するかが決定されます。

IP マルチキャストでは、ルート パス選択に次の方法が使用できます。

（注） IP マルチキャストで使用可能なルート パス選択のデフォルトの方法以外のすべての方法で、いくつかの形式の ECMP マルチキャスト ロード スプリッティングが可能です。

- 最も高い PIM ネイバー：これはデフォルトの方法です。したがって、設定は不要です。複数の等コスト パスが使用できる場合は、RPF for IPv4 マルチキャスト トラフィックは、最も大きい IP アドレスを持つ PIM ネイバーに基づき、その結果、設定しなければ、ECMP マルチキャスト ロード スプリットはデフォルトでディセーブルになります。
- ECMP マルチキャスト ロード スプリットの送信元アドレスに基づいた方法：**ip multicast multipath** コマンドを使用して、ECMP マルチキャスト ロード スプリットを設定できます。この形式の **ip multicast multipath** コマンドを入力すると、S ハッシュアルゴリズムを使用した送信元アドレスに基づく ECMP マルチキャスト ロード スプリットがイネーブルになります。詳細については、「*S* ハッシュアルゴリズムを使用した、送信元アドレスに基づく *ECMP* マルチキャスト ロード スプリット」の項を参照してください。
- ECMP マルチキャスト ロード スプリットの送信元アドレスとグループアドレスに基づいた方法：**ip multicast multipath** コマンドに **s-g-hash** キーワードと **basic** キーワードを指定して、ECMP マルチキャスト ロード スプリットを設定できます。この形式の **ip multicast multipath** コマンドを入力すると、基本 S-G ハッシュアルゴリズムを使用した送信元アドレスとグループアドレスに基づく ECMP マルチキャスト ロード スプリットがイネーブルになります。詳細については、「基本*S-G*ハッシュアルゴリズムを使用した、送信元アドレスとグループアドレスに基づく *ECMP* マルチキャスト ロード スプリット」の項を参照してください。
- ECMP マルチキャスト ロード スプリットの送信元アドレス、グループアドレス、ネクストホップアドレスに基づいた方法：**ip multicast multipath** コマンドに **s-g-hash** キーワードと **next-hop-based** キーワードを指定して、ECMP マルチキャスト ロード スプリットを設定できます。この形式のコマンドを入力すると、ネクストホップ ベースの S-G ハッシュアルゴリズムを使用した、ソース アドレス、グループ アドレス、およびネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリットが可能になります。詳細については、「送信元アドレス、グループアドレス、およびネクストホップアドレスに基づく *ECMP* マルチキャスト ロード スプリットのイネーブル化」の項を参照してください。

デフォルト動作（最高 PIM ネイバー動作）は、IP マルチキャストでのどのような形の ECMP ロード スプリットにもならず、使用可能なパスのネクスト ホップ PIM ネイバーの中から最も大きい IP アドレスを持つ PIM ネイバーを選択します。ネクストホップが **show ip pim neighbor** コマンドの出力に表示された場合、PIM ネイバーとみなされます。これは、PIM Hello メッセージがネクストホップから受信され、タイムアウトしていない場合です。使用可能なネクストホップのいずれも PIM ネイバーでない場合は、そのまま最も高い IP アドレスを持つネクストホップが選択されます。

IP マルチキャスト トラフィックをロード スプリットする方法

一般に、IP マルチキャスト トラフィックのロード スプリットには、次の方法が使用できます。

- ソース アドレス、ソース アドレスとグループ アドレス、またはソース アドレスとグループ アドレスとネクスト ホップ アドレスに基づいて、ECMP マルチキャスト ロード スプリッティングをイネーブルにできます。等コスト パスが認識された後、ECMP マルチキャスト ロード スプリットは、ユニキャスト トラフィックと同様に、パケットごとではなく、(S, G) ごとに動作します。
- IP マルチキャストをロード スプリットする別の方法としては、2 つ以上の等コスト パスを Generic Routing Encapsulation（GRE）トンネルに統合して、ユニキャスト ルーティング プロトコルがロード スプリットを実行できるようにするか、または Fast または Gigabit EtherChannel インターフェイス、マルチリンク PPP（MLPPP）リンク バンドル、またはマルチリンク フレーム リレー（FR.16）リンク バンドルなどのバンドル インターフェイスを介してロード スプリットできるようにします。

ECMP マルチキャスト ロード スプリットの概要

デフォルトでは、IPv4 マルチキャスト トラフィックの ECMP マルチキャスト ロード スプリットはディセーブルになっています。ECMP マルチキャスト ロード スプリットは、**ip multicast multipath** コマンドを使用してイネーブルにできます。

S ハッシュ アルゴリズムを使用した、ソース アドレスに基づく ECMP マルチキャスト ロード スプリット

発信元アドレスに基づく ECMP マルチキャスト ロード スプリットのトラフィックは、S ハッシュ アルゴリズムを使用して、各 (*, G) または (S, G) ステートの RPF インターフェイスが、ステートの解決される RPF アドレスに応じて、使用可能な等コスト パスの中から選択されるようにします。(S, G) ステートの場合、RPF アドレスはステートの発信元アドレスです。(*, G) ステートの場合、RPF アドレスはステートのグループ アドレスに関連付けられた RP のアドレスです。

発信元アドレスに基づいて ECMP マルチキャスト ロード スプリットを設定すると、さまざまなステートのマルチキャスト トラフィックを等コスト インターフェイスのうち複数を介して受信できます。原則として、IPv4 マルチキャストによって適用される方法は、IPv4 CEF でのデフォルトのフロー単位のロード スプリットまたは Fast および Gigabit EtherChannel で使用されるロード スプリットとかなり似ています。しかし、ECMP マルチキャスト ロード スプリットのこの方法は、局在化の影響を受けます。

基本 S-G ハッシュ アルゴリズムを使用した、ソース アドレスとグループ アドレスに基づく ECMP マルチキャスト ロード スプリット

送信元アドレスとグループ アドレスに基づく ECMP マルチキャスト ロード スプリットでは、送信元アドレスとグループ アドレスに基づいた基本 S-G ハッシュ アルゴリズムと呼ばれる、単純なハッシュが使用されます。基本 S-G ハッシュ アルゴリズムは、ハッシュ値を出すためにランダム化を一切使用しないため、予測可能です。ただし、S-G ハッシュ アルゴリズムは、特定のソースとグループについて、どのデバイス上でそのハッシュが計算されたかに関係なく常に同じハッシュが得られるため、局在化する傾向があります。

（注） 基本の S-G ハッシュ アルゴリズムでは、Bidir-PIM グループは無視されます。

S ハッシュおよび基本 S-G ハッシュ アルゴリズムを使用した場合の副産物としての予測可能性

IPv4 マルチキャストの ECMP マルチキャスト ロード スプリットで使用される方法では、同じ数の等コストパスがトポロジ内の複数の場所に存在するネットワークにおいて、一貫したロードスプリットが可能です。フローを N パスを通過して分割させるために RP アドレスまたは送信元アドレスが計算されると、フローはトポロジ内のすべての場所で同じようにそれらの N パスを通過して分割されます。一貫したロードスプリットによって予測可能性を考慮でき、それにより、IPv4 マルチキャスト トラフィックのロード スプリットを手動で操作できるようになります。

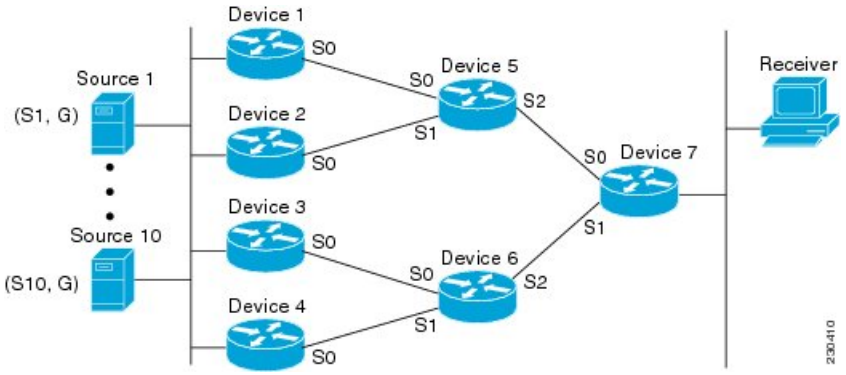
S ハッシュおよび基本 S-G ハッシュ アルゴリズムを使用した場合の副産物としての局在化

ソース アドレスまたはソースおよびグループ アドレスによってマルチキャスト トラフィックをロード スプリットするために IPv4 マルチキャストで使用されるハッシュ機能には通常、局在化と呼ばれる問題があります。ソース アドレスまたはソースおよびグループ アドレスに基づく ECMP マルチキャスト ロード スプリットの副産物として、局在化は、一部のトポロジ内のルータがロードスプリットに使用可能なすべてのパスを効果的に使用できないという問題です。

次の図に、ソース アドレスに基づく、またはソース アドレスとグループ アドレスに基づく ECMP マルチキャスト ロード スプリットを設定した場合の局在化の問題を説明するために、ここで使用するトポロジを示します。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *45 :* 局在化トポロジ



図に示すトポロジでは、ルータ 7 がルータ 5 およびルータ 6 を経由してソース S1 ～ S10 に向かう 2 つの等コスト パスがあることに注目してください。このトポロジでは、トポロジ内のすべてのルータで ECMP マルチキャスト ロード スプリッティングが **ip multicast multipath** コマンドを使用して有効になっていると仮定します。このシナリオでは、ルータ 7 は、10 個の (S, G) ステートに等コスト ロード スプリットを適用します。このシナリオにおける局在化の問題は、ルータ 7 に影響します。そのルータがソース S1 ～ S5 についてはルータ 5 でシリアル インターフェイス 0 を選択し、ソース S6 ～ S10 についてはルータ 6 でシリアル インターフェイス 1 を選択することになるからです。さらに、このトポロジでは、局在化の問題による影響はルータ 5 とルータ 6 にも及びます。ルータ 5 には、ルータ 1 上のシリアル インターフェイス 0 およびルータ 2 上のシリアル インターフェイス 1 を経由する S1 ～ S5 への 2 つの等コスト パスがあります。ルータ 5 は、2 つのパスのどちらを使用するかの選択に同じハッシュ アルゴリズムを適用するため、ソース S1 ～ S5 には 2 つのアップストリーム パスのうちの片方だけを使用することになります。つまり、すべてのトラフィックがルータ 1 とルータ 5 を流れるか、またはルータ 2 とルータ 5 を流れるかのいずれかになります。このトポロジでは、ロード スプリットにルータ 1 とルータ 5 およびルータ 2 とルータ 5 を使用することはできません。同様に、局在化問題は、ルータ 3 とルータ 6 およびルータ 4 とルータ 6 に当てはまります。つまり、このトポロジでは、ロード スプリットにルータ 3 とルータ 6 およびルータ 4 とルータ 6 の両方を使用することはできません。

ソース グループとネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリッティング

ソース、グループ、およびネクストホップ アドレスに基づいて ECMP マルチキャスト ロード スプリットを設定すると、ソース、グループ、およびネクストホップ アドレスに基づくより複雑なハッシュ、ネクストホップ ベースの S-G ハッシュ アルゴリズムが有効になります。ネクスト ホップ ベースの S-G ハッシュ アルゴリズムは、ハッシュ値の計算にランダム化を一切使用しないため、予測可能です。S ハッシュ アルゴリズムや基本 S-G ハッシュ アルゴリズムと違って、ネクスト ホップ ベースの S-G ハッシュ アルゴリズムに使用されるハッシュ メカニズムは、局在化の傾向がありません。

（注） IPv4 マルチキャストにおけるネクストホップ ベースの S-G ハッシュ アルゴリズムは、IPv6 ECMP マルチキャスト ロード スプリットで使用されるものと同じアルゴリズムであり、PIM-SM ブートストラップ デバイス（BSR）に使用されるものと同じハッシュ機能を活用できます。

ネクストホップ ベースのハッシュ機能では局在化は生成されず、パスで障害が発生した場合により良い RPF の安定性が維持されます。これらの利点には、ソース アドレスまたは RP IP アドレスを使用して信頼性を持って予測したり、ネクスト ホップ ベースの S-G ハッシュ アルゴリズムを使用した場合にロード スプリットの成果をエンジニアリングしたりすることができないという代償が伴います。多くのカスタマー ネットワークは等コスト マルチパス トポロジを実装しているため、ロード スプリットの手動操作は多くの場合必須ではありません。むしろ、IP マルチキャストのデフォルトの動作が IP ユニキャストと類似している必要があります。つまり、IP マルチキャストはベストエフォート ベースで複数の等コスト パスを使用すると期待されます。そのため、局在化の異常により、IPv4 マルチキャストのロード スプリットはデフォルトで有効にできません。

（注） また、CEF ユニキャストのロード スプリットは局在化を示さない方法を使用し、同様にロード スプリットの結果を予測したりロード スプリットの結果を操作するために使用することはできません。

ネクストホップ ベースのハッシュ機能では、PIM ネイバーの実際のネクストホップ IP アドレスが計算に取り込まれるため、局在化を回避できます。そのため、ハッシュの結果は各デバイスで異なり、実質的に局在化の問題はありません。局在化の回避に加えて、このハッシュ機能は、パスの障害に直面して選択された RPF パスの安定性も向上させます。4 つの等コスト パスを持つデバイスと、これらのパス間でロードスプリットされる多数のステートを考えます。これらのパスの 1 つに障害が発生し、残りの 3 つのパスが使用可能な状態になったとします。ハッシュ機能の二極化によって使用されるハッシュ機能（S ハッシュおよび基本の S-G ハッシュ アルゴリズムによって使用されるハッシュ機能）を使用して、すべてのステートの RPF パスは再コンバージェンスされるため、それら 3 つのパスの間（特にそれら 3 つのパスのいずれかをすでに使用していたパス）で変更される可能性があります。したがって、これらのステートは、その RPF インターフェイスとネクスト ホップ ネイバーが不必要に変更されることになります。この問題が発生するのは、このアルゴリズムでは、選択されるパスが、考慮できるすべてのパスの総数を取ることにより決定されるためです。このため、いったんパスが変わると、すべてのステートの RPF 選択も変更の対象となります。ネクスト ホップ ベースのハッシュ アルゴリズムでは、RPF の変更されたパスを使用していたステートだけが、残る 3 つのパスのいずれかへと再コンバージェンスする必要があります。すでにこれらのパスのいずれかを使用しているステートは、変更されません。4 つ目のパスが再び稼働し始めると、最初はそれを使用していたステートが、ただちに再コンバージェンスしてそのパスに戻ります。他のステートは、一切影響を受けません。

（注） ネクスト ホップ ベースの S-G ハッシュ アルゴリズムでは、Bidir-PIM グループは無視されます。

RPF パス選択のための PIM ネイバー クエリおよびハロー メッセージへの ECMP マルチキャスト ロード スプリットの影響

ECMP を介する IP マルチキャスト トラフィックのロード スプリットがイネーブルになっておらず、RP またはソースに向けて複数の等コスト パスが存在する場合、IPv4 マルチキャストは、まず最も大きい IP アドレスの PIM ネイバーを選択します。PIM ネイバーとは、受信した PIM ハロー（または PIMv1 クエリ）メッセージのソース デバイスです。たとえば、IGP で学習された、または 2 つのスタティック ルート経由で設定された 2 つの等コスト パスを持つデバイスを考えてみます。これら 2 つのパスのネクスト ホップは、10.1.1.1 と 10.1.2.1 です。これらのネクスト ホップ デバイスの両方が PIM ハロー メッセージを送信した場合、10.1.2.1 が最も IP アドレスの大きい PIM ネイバーとして選択されます。10.1.1.1 だけが PIM ハロー メッセージを送信した場合は、10.1.1.1 が選択されます。これらのデバイスのどちらも PIM ハロー メッセージを送信しない場合は、10.1.2.1 が選択されます。PIM ハロー メッセージへのこの違いが、スタティック マルチキャスト ルート（mroute）しか持たない特定のタイプのダイナミッ

ク フェールオーバー シナリオの構築を可能にします。それ以外では、これはあまり有用ではありません。

（注） スタティック mroute の設定の詳細については、ftp://ftpeng.cisco.com/ipmulticast/config-notes/static-mroutes.txt で Cisco IOS IP マルチキャスト FTP サイトにある『*Configuring Multiple Static Mroutes in Cisco IOS*』設定ノートを参照してください。

ECMP を介する IP マルチキャスト トラフィックのロード スプリットがイネーブルになっている場合、ネイバーからの PIM ハロー メッセージの存在は考慮されません。つまり、選択される RPF ネイバーは、そのネイバーからの PIM ハロー メッセージを受信したかどうかに左右されません。選択は、等コスト ルート エントリの有無にだけ依存します。

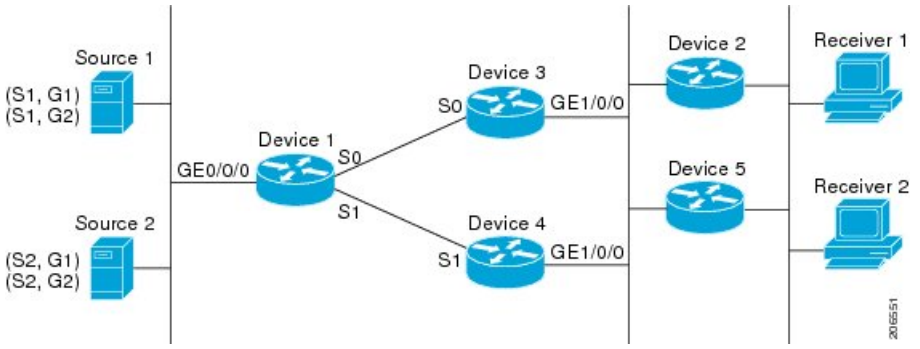
PIM-SM および PIM-SSM での PIM アサート処理に対する ECMP マルチキャスト ロード スプリットの影響

PIM-SM を (*, G) または (S, G) 転送で使用していた場合、または PIM-SSM を (S, G) 転送で使用していた場合でも、PIM アサート処理が発生したことが原因で **ip multicast multipath** コマンドでの ECMP マルチキャスト ロード スプリットが有効でなくなる場合もあります。

次の図に、PIM-SM および PIM-SSM での ECMP マルチキャスト ロード スプリットの PIM アサート処理への影響を説明するためにここで使用するサンプル トポロジを示します。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやコントローラ）を使用できます。

図 *46 : PIM-SM* および *PIM-SSM* での *ECMP* マルチキャスト ロード スプリットと *PIM* アサート処理



図に示すトポロジでは、デバイス 2 とデバイス 5 の両方がシスコデバイスで、**ip multicast multipath** コマンドを使用して ECMP マルチキャスト ロード スプリット用に一貫性を持って設定されており、ロードスプリットが期待どおりに動作し続けるようになっています。つまり、両方のデバイスがデバイス 3 とデバイス 4 を等コストネクストホップとして持ち、等コストパスのリストを同じ方法で（IP アドレスにより）ソートします。各 (S, G) ステートまたは (*, G) ステートに対してマルチパス ハッシュ関数を適用すると、それらは同じ RPF ネイバー（デバ

イス 3 またはデバイス 4）を選択し、その PIM 加入をこのネイバーに送信するようになります。

デバイス 5 とデバイス 2 が **ip multicast multipath** コマンドで一貫性のないように設定されている場合、またはデバイス 5 がサードパーティ製デバイスの場合は、デバイス 2 とデバイス 5 が、一部の (*, G) ステートまたは (S, G) ステートに対して異なる RPF ネイバーを選択する可能性があります。たとえば、デバイス 2 は、特定の (S, G) ステートに対してデバイス 3 を選択し、デバイス 5 は特定の (S, G) ステートに対してデバイス 4 を選択したりします。このシナリオでは、デバイス 3 とデバイス 4 が両方ともそのステートのトラフィックのギガビット イーサネット インターフェイス 1/0/0 への転送を開始し、お互いの転送したトラフィックを見て、トラフィックの重複を回避するためにアサート処理を開始します。その結果、その (S, G) ステートについては、ギガビット イーサネット インターフェイス 1/0/0 に最も大きい IP アドレスを持つデバイスがトラフィックを転送します。ところが、デバイス 2 とデバイス 5 は両方ともアサート選定での選択結果を追跡し、このアサートで選択されたデバイスが自分がその RPF 選択で計算して得たデバイスと同じでなくても、そのステートのための PIM 加入をこのアサートで選択されたデバイスに送信します。このため、PIM-SM と PIM-SSM では、ECMP マルチキャスト ロード スプリットの動作が保証されるのは、LAN 上のすべてのダウンストリーム デバイスが一貫性を持って設定されたシスコ デバイスである場合だけです。

ユニキャスト ルーティングが変わった場合の ECMP マルチキャスト ロード スプリットと再コンバージェンス

ユニキャスト ルーティングが変わると、すべての IP マルチキャスト ルーティング ステートが、利用可能なユニキャスト ルーティング情報を元にしてただちに再コンバージェンスされます。特に、1 つのパスが停止した場合、残りのパスがただちに再コンバージェンスされ、そのパスが再び稼働し始めた場合、それ以降は、マルチキャスト転送は、そのパスが停止する前に使用されていた同じ RPF パスに再コンバージェンスされます。再コンバージェンスは、ECMP 上の IP マルチキャスト トラフィックのロード スプリットが設定されているかどうかにかかわらず発生します。

ECMP マルチキャスト ロード スプリットでの BGP の使用

ECMP マルチキャスト ロード スプリットは、BGP を通じて学習した RPF 情報とも、その他のプロトコルから学習した RPF 情報と同じ方法で一緒に動作します。このプロトコルによりインストールされた複数のパスの中から 1 つのパスを選択します。BGP での主な違いは、デフォルトでは単一のパスしかインストールされないことです。たとえば、BGP スピーカーがプレフィックスに 2 つの同一外部 BGP（eBGP）パスを学習した場合、最も小さいデバイス ID を持つパスが最良パスとして選択されます。この最良パスが IP ルーティング テーブルにインストールされます。BGP マルチパス サポートがイネーブルになっており、隣接する同一の AS から複数の eBGP パスが学習された場合、単一の最良パスが選ばれるのではなく、複数のパスが IP ルーティング テーブルにインストールされます。デフォルトでは、BGP は IP ルーティング テーブルに 1 つのパスしかインストールしません。

BGP に学習されるプレフィックスに ECMP マルチキャスト ロード スプリットを使用するには、BGP マルチパスをイネーブルにする必要があります。一度設定されると、BGP によりリモート ネクスト ホップ情報がインストールされた場合、その BGP ネクスト ホップに対して（ユニキャストとして）最良のネクスト ホップを検出するため、RPF ルックアップが再帰的

に実行されます。たとえば、与えられたプレフィックスに対して単一の BGP パスしかないのに、その BGP ネクスト ホップに到達する IGP パスが 2 つあった場合、マルチキャスト RPF は、この異なる 2 つの IGP パス間で正しくロード スプリットします。

スタティック mroute での ECMP マルチキャスト ロード スプリットの使用

特定のソースまたは RP に対して IGP を使用して等コスト ルートをインストールすることが可能でない場合、スタティック ルートを設定して、ロード スプリットのための等コスト パスを指定することができます。ソフトウェアは、プレフィックスに対し 1 つのスタティック mroute という設定をサポートしていないため、等コスト パスの設定にスタティック mroute は使用できません。再帰的なルート ルックアップを使用した場合のこの制限にはいくつかの回避策がありますが、その回避策は等コスト マルチパス ルーティングには適用できません。

（注） スタティック mroute の設定の詳細については、ftp://ftpeng.cisco.com/ipmulticast/config-notes/static-mroutes.txt で Cisco IOS IP マルチキャスト FTP サイトにある『*Configuring Multiple Static Mroutes in Cisco IOS*』設定ノートを参照してください。

IPv4 マルチキャストでは等コスト マルチパスにスタティック mroute のみを指定できます。しかし、それらのスタティック mroute はマルチキャストにのみ適用できます。または、等コスト マルチパスがユニキャストおよびマルチキャスト ルーティングの両方に適用されるように指定できます。IPv6 マルチキャストでは、このような制限はありません。等コスト マルチパス mroute を、ユニキャスト ルーティングのみ、マルチキャスト ルーティングのみ、またはこの双方に適用するスタティック IPv6 mroute に設定することができます。

IP マルチキャスト トラフィックのロード スプリッティングの代替方法

IP マルチキャスト トラフィックのロード スプリットは、複数のパラレル リンクを単一のトンネルに統合し、マルチキャスト トラフィックがそのトンネルを介してルーティングされるようにすることによっても達成できます。ロード スプリッティングのこの方法は、ECMP マルチキャスト ロード スプリッティングよりも設定が複雑です。GRE リンクを使用した等コスト パスを介したロード スプリットを設定するのが有利である例として、(S, G) ステートまたは (*, G) ステートの合計数が非常に小さく、各ステートによって伝送される帯域幅の変動が大きいため、ソースまたは RP アドレスの手動でのエンジニアリングでさえトラフィックの適切なロード スプリットを保証できない場合が挙げられます。

（注） ECMP マルチキャスト ロード スプリットの可用性があるため、通常は、パケットごとのロード シェアリングが必要な場合にしかトンネルを使用する必要はありません。

IP マルチキャスト トラフィックは、ファストまたはギガビット EtherChannel インターフェイス、MLPPP リンク バンドル、マルチリンク フレーム リレー（FRF.16）バンドルなどのバンドル インターフェイスを介したロード スプリットにも使用できます。GRE またはその他のタイプのトンネルも、このような形態のレイヤ 2 リンク バンドルを構成できます。このようなレイ

ヤ2メカニズムを使用する場合は、ユニキャストとマルチキャストのトラフィックがどのようにロード スプリットされるかを理解しておく必要があります。

トンネルを介した等コスト パス間で IP マルチキャスト トラフィックをロード スプリットするには、その前に CEF のパケットごとのロード バランシングを設定しておく必要があります。これをしなければ、GRE パケットにパケットごとのロード バランシングが行われません。

ECMP を介して IP マルチキャスト トラフィックをロード スプリットする方法

ECMP マルチキャスト ロード スプリットのイネーブル化

発信元アドレスに基づいて複数の等コスト パス間で IP マルチキャスト トラフィックの負荷を分割するには、次のタスクを実行します。

ソースから 2 つ以上の等コスト パスが使用できる場合は、ユニキャスト トラフィックはそれらのパスの間でロード スプリットされます。一方、マルチキャスト トラフィックは、デフォルトでは、複数の等コスト パスの間でロード スプリットすることはありません。一般に、マルチキャスト トラフィックは、RPF ネイバーから下流に流れます。PIM 仕様によると、複数のネイバーが同じメトリックを持つ場合、このネイバーは最も大きい IP アドレスを持っていなければなりません。

ip multicast multipath コマンドでロードスプリットを設定すると、システムは送信元アドレスに基づき、S ハッシュアルゴリズムを使用して複数の等コストパスの間でマルチキャストトラフィックをロードスプリットします。**ip multicast multipath** コマンドを設定していて、複数の等コストパスが存在する場合、マルチキャストトラフィックを伝送するパスは、送信元 IP アドレスに基づいて選択されます。異なる複数のソースからのマルチキャスト トラフィックが、異なる複数の等コスト パスの間でロード スプリットされます。同一ソースから異なる複数のマルチキャスト グループに送信されたマルチキャスト トラフィックについては、複数の等コスト パスの間でロード スプリットは行われません。

（注） **ip multicast multipath** コマンドは、トラフィックのロードバランシングではなくロードスプリットを行います。ソースからのトラフィックは、そのトラフィックがその他のソースからのトラフィックよりはるかに多い場合でも、1 つのパスしか使用しません。

IP マルチキャスト ロード スプリットの前提条件：ECMP

- 発信元アドレスに基づいて ECMP マルチキャスト ロード スプリットを有効にするには、十分な数の送信元（少なくとも 3 つの送信元）が必要です。
- ECMP マルチキャスト ロード スプリットを設定するには、RP が使用できる複数のパスが必要です。

（注） 送信元または RP がそれぞれ使用できるパスが複数あることを確認するには、*ip-address* 引数に送信元の IP アドレスまたは RP の IP アドレスを指定して、**show ip route** コマンドを使用します。コマンドの出力に複数のパスが表示されない場合は、ECMP マルチキャスト ロード スプリットを設定することはできません。

- 最短パス ツリー（SPT）フォワーディングで PIM-SM を使用する場合は、すべての (S, G) ステートのフォワーディングに T ビットを設定する必要があります。
- ECMP マルチキャスト ロード スプリットを設定する前に、**show ip rpf** コマンドを使用して、送信元が IP マルチキャストマルチパス機能を利用できるかどうかを確認しておくことをベストプラクティスとして推奨します。
- BGP は、デフォルトでは複数の等コスト パスをインストールしません。**maximum-paths** コマンドを使用して（たとえば BGP での）マルチパスを設定してください。詳細は、ECMP マルチキャスト ロード スプリットでの BGP の使用 （494 ページ）のセクションを参照してください。

IP マルチキャスト ロード スプリッティング ECMP の制約事項

- ソースから 2 つ以上の等コスト パスが使用できる場合は、ユニキャスト トラフィックはそれらのパスの間でロードスプリットされます。一方、マルチキャスト トラフィックは、デフォルトでは、複数の等コスト パスの間でロード スプリットすることはありません。一般に、マルチキャスト トラフィックは、RPF ネイバーから下流に流れます。PIM 仕様によると、複数のネイバーが同じメトリックを持つ場合、このネイバーは最も大きい IP アドレスを持っていなければなりません。
- **ip multicast multipath** コマンドは、同一の PIM ネイバー IP アドレスに複数の等コストパスを介して到達できるような設定はサポートしていません。この状況は、通常、番号付けされていないインターフェイスを使用している場合に発生します。**ip multicast multipath** コマンドを設定する際は、すべてのインターフェイスに異なる IP アドレスを使用します。
- **ip multicast multipath** コマンドは、トラフィックのロードバランシングではなくロードスプリットを行います。ソースからのトラフィックは、そのトラフィックがその他のソースからのトラフィックよりはるかに多い場合でも、1 つのパスしか使用しません。

ソース アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化

ソース アドレスに基づいたマルチキャスト トラフィックの ECMP マルチキャスト ロード スプリット（S ハッシュ アルゴリズムを使用）をイネーブルにして、ネットワーク上にある複数のパスの利点を活かすには、次の作業を実行します。S ハッシュ アルゴリズムは、ハッシュ値の計算にランダム化を一切使用しないため、予測可能です。ただし、S ハッシュ アルゴリズムは、特定のソースについて、ハッシュが計算されたデバイスに関係なく常に同じハッシュが得られるため、局在化する傾向があります。

（注） 複数の着信インターフェイスからのトラフィックのレシーバになるデバイスで ECMP マルチキャスト ロート スプリットをイネーブルにします。これは、ユニキャスト ルーティングと反対です。ユニキャストの視点からすると、複数の発信インターフェイスに接続されている送信デバイス上でマルチキャストがアクティブになっています。

始める前に

- 発信元アドレスに基づいて ECMP マルチキャスト ロード スプリットを有効にするには、十分な数の送信元（少なくとも 3 つの送信元）が必要です。
- ECMP マルチキャスト ロード スプリットを設定するには、RP が使用できる複数のパスが必要です。

（注） 送信元または RP がそれぞれ使用できるパスが複数あることを確認するには、*ip-address* 引数に送信元の IP アドレスまたは RP の IP アドレスを指定して、**show ip route** コマンドを使用します。コマンドの出力に複数のパスが表示されない場合は、ECMP マルチキャスト ロード スプリットを設定することはできません。

- 最短パス ツリー（SPT）フォワーディングで PIM-SM を使用する場合は、すべての (S, G) ステートのフォワーディングに T ビットを設定する必要があります。
- ECMP マルチキャスト ロード スプリットを設定する前に、**show ip rpf** コマンドを使用して、送信元が IP マルチキャストマルチパス機能を利用できるかどうかを確認しておくことをベストプラクティスとして推奨します。
- BGP は、デフォルトでは複数の等コスト パスをインストールしません。**maximum-paths** コマンドを使用して（たとえば BGP での）マルチパスを設定してください。詳細については、「*ECMP* マルチキャスト ロード スプリットでの *BGP* の使用」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast multipath**
4. 冗長トポロジ内のすべてのデバイスで、ステップ 3 を繰り返します。
5. **exit**
6. **show ip rpf** *source-address* [*group-address*]
7. **show ip route** *ip-address*

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	**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	**ip multicast multipath** 例： `Device(config)# ip multicast multipath`	S ハッシュ アルゴリズムを使用した、ソース アドレスに基づく ECMP マルチキャスト ロード スプリットをイネーブルにします。 • このコマンドはRPF ネイバーが選択される方法を変更するため、ループを回避するために、冗長トポロジ内のすべてのデバイスに一貫性を持たせて設定しなければなりません。 • このコマンドは、同一の PIM ネイバー IP アドレスに複数の等コストパスを介して到達できるような設定はサポートしていません。この状況は、通常、番号付けされていないインターフェイスを使用している場合に発生します。このコマンドが設定されるデバイスでは、各インターフェイスに異なる IP アドレスを使用します。 • このコマンドは、トラフィックのロードバランシングではなくロードスプリットを行います。ソースからのトラフィックは、そのトラフィックがその他のソースからのトラフィックよりはるかに多い場合でも、1 つのパスしか使用しません。
ステップ 4	冗長トポロジ内のすべてのデバイスで、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(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、特権 EXEC モードに戻ります。
ステップ 6	**show ip rpf** *source-address* [*group-address*] 例：	（任意）IP マルチキャスト ルーティングが RPF チェックの実行に使用する情報を表示します。

	コマンドまたはアクション	目的
	`Device# show ip rpf 10.1.1.2`	• IP マルチキャスト トラフィックが正常にロード スプリットされるようにするために、このコマンドを使用して RPF 選択を確認します。
ステップ 7	**show ip route** *ip-address* 例： `Device# show ip route 10.1.1.2`	（任意）IP ルーティング テーブルの現在のステータスを表示します。 • このコマンドを使用して、ECMP マルチキャスト ロード スプリットのために、ソースまたは RP までに複数のパスが使用できることを確認します。 • *ip-address* 引数については、ソースまでに複数のパスが使用できることを確認するにはソースの IP アドレスを入力し（最短パス ツリーの場合）、RP までに複数のパスが使用できることを確認するには RP の IP アドレスを入力します（共有ツリーの場合）。

ソースアドレスおよびグループアドレスに基づくECMPマルチキャストロードスプリットのイネーブル化

ソース アドレスとグループ アドレスに基づいたマルチキャスト トラフィックの ECMP マルチキャスト ロード スプリット（基本 S-G ハッシュ アルゴリズムを使用）をイネーブルにして、ネットワーク上にある複数のパスの利点を活かすには、次の作業を実行します。基本S-Gハッシュ アルゴリズムは、ハッシュ値の計算にランダム化を一切しようしないため、予測可能です。ただし、基本S-Gハッシュ アルゴリズムは、特定のソースとグループについて、ハッシュが計算されているデバイスに関係なく常に同じハッシュが得られるため、局在化する傾向があります。

基本S-Gハッシュ アルゴリズムは、ECMPマルチキャスト ロード スプリットに対して、Sハッシュ アルゴリズムよりも柔軟なサポートを提供します。ロード スプリットに基本S-Gハッシュ アルゴリズムを使用すると、特に、グループに多数のストリームを送信するデバイスや、IPTV サーバーや MPEG ビデオ サーバーのように多くのチャネルをブロードキャストするデバイスからのマルチキャスト トラフィックを、複数の等コスト パスの間でより効果的にロード スプリットすることが可能になります。

（注） 複数の着信インターフェイスからのトラフィックのレシーバになるデバイスで ECMP マルチキャスト ロート スプリットをイネーブルにします。これは、ユニキャスト ルーティングと反対です。ユニキャストの視点からすると、複数の発信インターフェイスに接続されている送信デバイス上でマルチキャストがアクティブになっています。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast multipath s-g-hash basic**
4. 冗長トポロジ内のすべてのデバイスで、ステップ 3 を繰り返します。
5. **exit**
6. **show ip rpf** *source-address* [*group-address*]
7. **show ip route** *ip-address*

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	**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	**ip multicast multipath s-g-hash basic** 例： `Device(config)# ip multicast multipath s-g-hash basic`	基本S-Gハッシュ アルゴリズムを使用した、ソース アドレスとグループ アドレスに基づく ECMP マルチキャスト ロード スプリットをイネーブルにします。 • このコマンドはRPF ネイバーが選択される方法を変更するため、ループを回避するために、冗長トポロジ内のすべてのデバイスに一貫性を持たせて設定しなければなりません。
ステップ 4	冗長トポロジ内のすべてのデバイスで、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(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、特権 EXEC モードに戻ります。
ステップ 6	**show ip rpf** *source-address* [*group-address*] 例： `Device# show ip rpf 10.1.1.2`	（任意）IP マルチキャスト ルーティングが RPF チェックの実行に使用する情報を表示します。 • IPマルチキャストトラフィックが正常にロードスプリットされるようにするために、このコマンドを使用して RPF 選択を確認します。

	コマンドまたはアクション	目的
ステップ 7	**show ip route** *ip-address* 例： `Device# show ip route 10.1.1.2`	（任意）IP ルーティング テーブルの現在のステータスを表示します。 • このコマンドを使用して、ECMP マルチキャスト ロード スプリットのために、ソースまたは RP までに複数のパスが使用できることを確認します。 • *ip-address* 引数については、ソースまでに複数のパスが使用できることを確認するにはソースの IP アドレスを入力し（最短パス ツリーの場合）、RP までに複数のパスが使用できることを確認するには RP の IP アドレスを入力します（共有ツリーの場合）。

ソース グループおよびネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化

ソース アドレス、グループ アドレス、およびネクスト ホップ アドレスに基づいたマルチキャスト トラフィックの ECMP マルチキャスト ロード スプリット（ネクスト ホップ ベースの S-G ハッシュ アルゴリズムを使用）をイネーブルにして、ネットワーク上にある複数のパスの利点を活かすには、次の作業を実行します。ネクスト ホップ ベースの S-G ハッシュ アルゴリズムは、ハッシュ値の計算にランダム化を一切使用しないため、予測可能です。S ハッシュ アルゴリズムや基本 S-G ハッシュ アルゴリズムと違って、ネクスト ホップ ベースの S-G ハッシュ アルゴリズムに使用されるハッシュ メカニズムは、局在化の傾向がありません。

ネクスト ホップ ベースの S-G ハッシュ アルゴリズムは、ECMP マルチキャスト ロード スプリットに対して、S ハッシュ アルゴリズムよりも柔軟なサポートを提供し、局在化の問題をなくします。ECMP マルチキャスト ロード スプリットにネクスト ホップ ベースの S-G ハッシュ アルゴリズムを使用すると、グループに多数のストリームを送信するデバイスや、IPTV サーバーや MPEG ビデオ サーバーのように多くのチャネルをブロードキャストするデバイスからのマルチキャスト トラフィックを、複数の等コスト パスの間でより効果的にロード スプリットすることが可能になります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast multipath s-g-hash next-hop-based**
4. 冗長トポロジ内のすべてのルータについて、ステップ 1 ～ 3 を繰り返します。
5. **end**
6. **show ip rpf** *source-address* [*group-address*]
7. **show ip route** *ip-address*

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	**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	**ip multicast multipath s-g-hash next-hop-based** 例： `Device(config)# ip multicast multipath s-g-hash next-hop-based`	ネクスト ホップ ベースの S-G ハッシュ アルゴリズムを使用した、ソース アドレス、グループ アドレス、およびネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリットをイネーブル化します。 • このコマンドはRPF ネイバーが選択される方法を変更するため、ループを回避するために、冗長トポロジ内のすべてのルータに一貫性を持たせて設定しなければなりません。 （注） 複数の着信インターフェイスからのトラフィックの受信先になると想定されるルータ上で、**ip multicast multipath** コマンドをイネーブルにします。これは、ユニキャストルーティングと反対です。ユニキャストの視点からすると、複数の発信インターフェイスに接続されている送信ルータ上でマルチキャストがアクティブになっています。
ステップ 4	冗長トポロジ内のすべてのルータについて、ステップ 1 ～ 3 を繰り返します。	--
ステップ 5	**end** 例： `Device(config)# end`	グローバル 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。
ステップ 6	**show ip rpf** *source-address* [*group-address*] 例：	（任意）IP マルチキャスト ルーティングが RPF チェックの実行に使用する情報を表示します。

	コマンドまたはアクション	目的
	`Device# show ip rpf 10.1.1.2`	• IP マルチキャスト トラフィックが正常にロード スプリットされるようにするために、このコマンドを使用して RPF 選択を確認します。
ステップ 7	**show ip route** *ip-address* 例： `Device# show ip route 10.1.1.2`	（任意）IP ルーティング テーブルの現在のステータスを表示します。 • このコマンドを使用して、ECMP マルチキャスト ロード スプリットのために、ソースまたは RP までに複数のパスが使用できることを確認します。 • *ip-address* 引数については、ソースまでに複数のパスが使用できることを確認するにはソースの IP アドレスを入力し（最短パス ツリーの場合）、RP までに複数のパスが使用できることを確認するには RP の IP アドレスを入力します（共有ツリーの場合）。

ECMP を介した IP マルチキャスト トラフィックのロード スプリットの設定例

例：ソース アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化

次の例は、S ハッシュ アルゴリズムを使用した、ソース アドレスに基づく ECMP マルチキャスト ロード スプリットをルータ上でイネーブルにする方法を示します。

```
ip multicast multipath
```

ソース アドレスおよびグループ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化の例

次の例は、基本 S-G ハッシュ アルゴリズムを使用した、ソース アドレスとグループ アドレスに基づく ECMP マルチキャスト ロード スプリットをルータ上でイネーブルにする方法を示します。

```
ip multicast multipath s-g-hash basic
```

ソース グループおよびネクストホップ アドレスに基づく ECMP マルチキャスト ロード スプリットのイネーブル化の例

次の例は、ネクスト ホップ ベースの S-G ハッシュ アルゴリズムを使用した、ソース アドレス、グループ アドレス、およびネクスト ホップ アドレスに基づく ECMP マルチキャスト ロード スプリットをルータ上でイネーブルにする方法を示します。

```
ip multicast multipath s-g-hash next-hop-based
```

IP マルチキャストの最適化に関するその他の関連情報：等コストパス間での IP マルチキャスト ロード スプリッティング

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)* の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)*

標準および RFC

標準/RFC	タイトル
RFC 4601	『Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification』

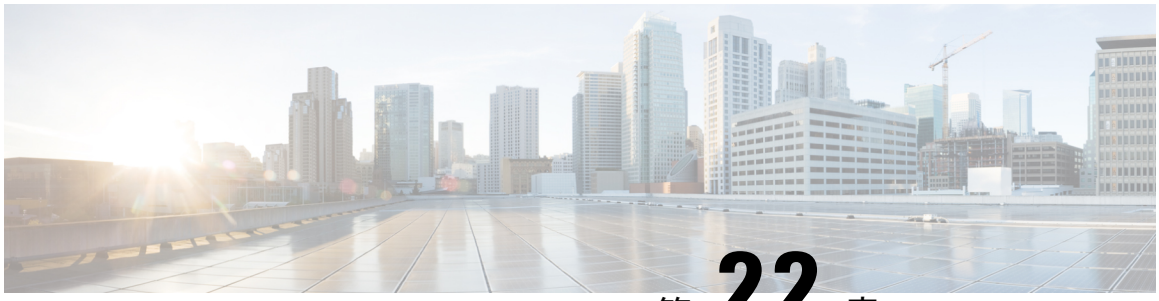
IP マルチキャストの最適化の機能履歴：等コストパス間での IP マルチキャスト ロード スプリッティング

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IP マルチキャストの最適化：ECMP を介した IP マルチキャストトラフィックのロードスプリット	ロード スプリットとロード バランシングは同じではありません。ロード スプリットでは、複数の等コスト リバース パス フォワーディング（RPF）パスを介して (*, G) および (S, G) トラフィック ストリームをランダムに分散する手段が提供され、必ずしもそれらの等コスト RPF パス上で平衡のとれた IP マルチキャスト トラフィック負荷が得られるわけではありません。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/にアクセスします。



第 22 章

IPマルチキャストの最適化：マルチキャスト向けSSMチャネル ベース フィルタリング

マルチキャスト境界向け SSM チャネル ベース フィルタリングの前提条件

IP マルチキャストをデバイスで有効にするには、『*IP Multicast: PIM Configuration Guide*』の「Configuring Basic IP Multicast」モジュールに記載されているタスクを使用します。

マルチキャスト境界向け SSM チャネル ベース フィルタリングについて

ここでは、マルチキャスト境界向けの SSM チャネル ベース フィルタリング機能について説明します。

マルチキャスト境界のルール

マルチキャスト境界向けのSSMチャネルベースフィルタリング機能は、**ip multicast boundary** コマンドを拡張して、コントロール プレーン フィルタリングをサポートします。1 つのインターフェイスに複数の **ip multicast boundary** コマンドを適用できます。

次のルールで **ip multicast boundary** コマンドは制御されます。

- 1 つのインターフェイスに設定できるのは、**in** および **out** キーワードの一方のインスタンスです。
- **in** および **out** キーワードは、標準アクセスリストまたは拡張アクセスリストに使用できます。
- **filter-autorp** キーワードまたは no キーワードを使用する場合、標準のアクセスリストだけが許可されます。
- コマンドの最大 3 つのインスタンスが 1 つのインターフェイスで許可されます。**in** の 1 つのインスタンス、**out** の 1 つのインスタンス、および **filter-autorp** または no キーワードの 1 つのインスタンスです。
- コマンドの複数のインスタンスを使用すると、フィルタリングは累積的になります。キーワードなしの境界ステートメントが、**in** キーワードが含まれる境界ステートメントと存在する場合、両方のアクセスリストが入力方向に適用され、どちらか一方での一致で十分です。
- コマンドのすべてのインスタンスは、制御トラフィックおよびデータ プレーン トラフィックの両方に適用されます。
- 拡張アクセスリストのプロトコル情報は解析され、一貫性の再利用とフィルタリングが許可されます。アクセス リストがすべてのプロトコルの（S,G）トラフィックをフィルタリングする場合、（S,G）オペレーションは、キーワードについて記述されたすべての条件で拡張アクセス リストによってフィルタリングされます。

マルチキャスト境界向け SSM チャネル ベース フィルタリングの利点

- この機能によって、送信元インターフェイスでの入力が可能になります。
- アクセス制御機能は、SSM および Any Source Multicast（ASM）の場合と同じです。

マルチキャスト境界向け SSM チャネル ベース フィルタリングの設定方法

ここでは、マルチキャスト境界に SSM チャネルベースのフィルタリングを設定する手順について説明します。

マルチキャスト境界の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list** {**standard**| **extended**} *access-list-name*
4. **permit** *protocol* **host** *address* **host** *address*
5. **deny** *protocol* **host** *address* **host** *address*
6. 必要に応じて、ステップ 4 またはステップ 5 を繰り返します。
7. **interface** *type* **interface-number** *port -number*
8. **ip multicast boundary** *access-list-name* [**in**| **out** | **filter-autorp**]

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。
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	**ip access-list** {**standard**| **extended**} *access-list-name* 例： `Device(config)# ip access-list 101`	標準または拡張のアクセス リストを設定します。
ステップ 4	**permit** *protocol* **host** *address* **host** *address* 例： `Device(config-ext-nacl)# permit ip host 181.1.2.201 host 232.1.1.11`	指定された ip ホスト トラフィックを許可します。
ステップ 5	**deny** *protocol* **host** *address* **host** *address* 例： `Device(config-acl-nacl)# deny ip host 181.1.2.203 host 232.1.1.1`	指定されたマルチキャスト ip グループおよび送信元トラフィックを拒否します。
ステップ 6	必要に応じて、ステップ 4 またはステップ 5 を繰り返します。	指定されたホストおよび送信元トラフィックを許可および拒否します。

	コマンドまたはアクション	目的
ステップ 7	**interface** *type* **interface-number** *port -number* 例： `Device(config)# interface gigabitethernet 2/3/0`	インターフェイス コンフィギュレーション モードをイネーブルにします。
ステップ 8	**ip multicast boundary** *access-list-name* [**in**| **out** | **filter-autorp**] 例： `Device(config-if)# ip multicast boundary acc_grp1 out`	マルチキャスト境界を設定します。 （注） **filter-autorp** キーワードは、拡張アクセスリストをサポートしていません。

マルチキャスト境界向け SSM チャネル ベース フィルタリングの設定例

ここでは、マルチキャスト境界向け SSM チャネル ベースフィルタリング機能の設定例を紹介します。

トラフィックを許可および拒否するマルチキャスト境界の設定例

次の例では、(181.1.2.201, 232.1.1.1) および (181.1.2.202, 232.1.1.1) への発信トラフィックを許可し、他のすべての (S,G) を拒否します。

```
configure terminal
 ip access-list extended acc_grp1
 permit ip host 0.0.0.0 232.1.1.1 0.0.0.255
 permit ip host 181.1.2.201 host 232.1.1.1
 permit udp host 181.1.2.202 host 232.1.1.1
 permit ip host 181.1.2.202 host 232.1.1.1
 deny igmp host 181.2.3.303 host 232.1.1.1
 interface gigabitethernet 1/0/1
 ip multicast boundary acc_grp1 out
```

トラフィックを許可するマルチキャスト境界の設定例

次の例では、(192.168.2.201, 232.1.1.5) および (192.168.2.202, 232.1.1.5) への発信トラフィックを許可します。

```
configure terminal
ip access-list extended acc_grp6
 permit ip host 0.0.0.0 232.1.1.1 5.0.0.255
 deny udp host 192.168.2.201 host 232.1.1.5
 permit ip host 192.168.2.201 host 232.1.1.5
 deny pim host 192.168.2.201 host 232.1.1.5
 permit ip host 192.168.2.202 host 232.1.1.5
```

```
 deny igmp host 192.2.3.303 host 232.1.1.1
interface gigabitethernet 1/0/1
 ip multicast boundary acc_grp6 out
```

トラフィックを拒否するマルチキャスト境界の設定例

次に、候補 RP でアナウンスされるグループ範囲を拒否する例を示します。グループ範囲が拒否されるため、pim auto-rp マッピングは作成されません。

```
configure terminal
ip access-list standard acc_grp10
 deny 225.0.0.0 0.255.255.255
 permit any
 access-list extended acc_grp12
 permit pim host 181.1.2.201 host 232.1.1.8
 deny udp host 181.1.2.201 host 232.1.1.8
 permit pim host 181.1.2.203 0.0.0.255 host 227.7.7.7
 permit ip host 0.0.0.0 host 227.7.7.7
 permit ip 181.1.2.203 0.0.0.255 host 227.7.7.7
 permit ip host 181.1.2.201 host 232.1.1.7
ip access-list extended acc_grp13
 deny ip host 181.1.2.201 host 232.1.1.8
 permit ip any any
interface gigabitethernet 1/0/1
 ip multicast boundary acc_grp10 filter-autorp
 ip multicast boundary acc_grp12 out
 ip multicast boundary acc_grp13 in
```

IP マルチキャストの最適化：マルチキャスト向け SSM チャネルベースフィルタリングに関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9300 Series Switches)* の「IP マルチキャスト ルーティング コマンド」の項を参照してください。

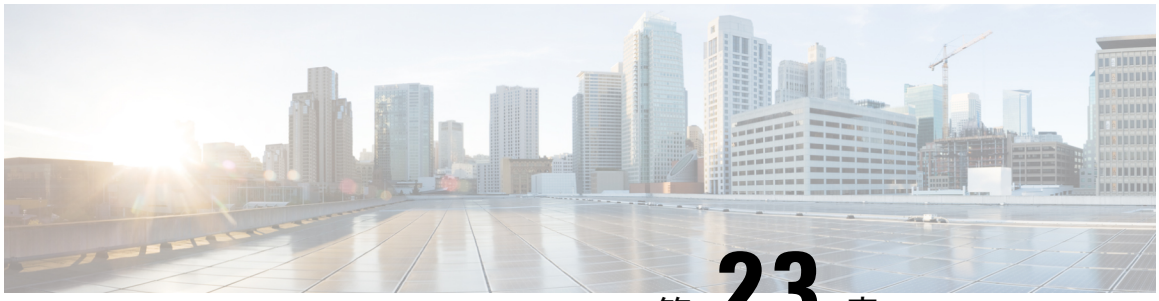
IP マルチキャストの最適化の機能履歴：マルチキャスト向け SSM チャネル ベース フィルタリング

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IPマルチキャストの最適化：マルチキャスト向け SSM チャネル ベース フィルタリング	マルチキャスト境界のための SSM チャネル ベース フィルタリング機能は、ip multicast boundary コマンドを拡張して、コントロール プレーン フィルタリングをサポートします。複数のip multicast boundary コマンドをインターフェイスに適用できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/にアクセスします。



第 23 章

IP マルチキャストの最適化：IGMP ステート制限

IGMP ステート制限の前提条件

- IP マルチキャストを有効にして、Protocol Independent Multicast（PIM）インターフェイスを設定するには、『*IP Multicast: PIM Configuration Guide*』の「Configuring Basic IP Multicast」モジュールに記載されているタスクを使用します。
- すべての ACL を設定する必要があります。詳細については、『*Security Configuration Guide: Access Control Lists*』ガイドの「Creating an IP Access List and Applying It to an Interface」モジュールを参照してください。

IGMP ステート制限の制約事項

デバイスごとに 1 つのグローバル制限と、インターフェイスごとに 1 つの制限を設定できます。

IGMP ステート制限に関する情報

ここでは、IGMP ステート制限について説明します。

IGMP ステート制限

IGMP ステート制限機能を使用すると、IGMP ステート リミッタの設定が可能になり、この設定により、IGMP メンバーシップ レポート（IGMP 加入）により生成される mroute ステートの数がグローバルに、またはインターフェイスごとに制限されます。設定されている制限を超えたメンバーシップ レポートは、IGMP キャッシュに入れられません。この機能により、DoS（サービス拒絶）攻撃を防止したり、すべてのマルチキャスト フローがほぼ同量の帯域幅を使用するネットワーク環境でマルチキャスト CAC メカニズムを提供したりできます。

（注） IGMP ステート リミッタは、IGMP、IGMP v3lite、および URL Rendezvous Directory（URD）メンバーシップ レポートから生じる route ステートの数に、グローバルまたはインターフェイスごとに制限をかけます。

IGMP ステート制限機能の設計

- グローバル コンフィギュレーション モードで IGMP ステート リミッタを設定すると、キャッシュに格納できる IGMP メンバーシップ レポートの数に対してグローバルな制限を指定できます。
- インターフェイス コンフィギュレーション モードで IGMP ステート リミッタを設定すると、IGMP メンバーシップ レポートの数に対してインターフェイスごとの制限を指定できます。
- ACL を使用すれば、グループまたはチャネルがインターフェイス制限に対してカウントされることがなくなります。標準 ACL または拡張 ACL を指定できます。標準 ACL は、(*, G) ステートがインターフェイスへの制限から除外されるように定義するのに使用できます。拡張 ACL は、(S, G) ステートがインターフェイスへの制限から除外されるように定義するのに使用できます。拡張 ACL は、拡張アクセス リストを構成する許可文または拒否文の中でソース アドレスとソース ワイルドカードに 0.0.0.0 を指定することにより（(0, G) とみなされます）インターフェイスへの制限から除外される (*, G) ステートを定義するのにも使用できます。
- デバイスごとに 1 つのグローバル制限と、インターフェイスごとに 1 つの制限を設定できます。

IGMP ステート リミッタのメカニズム

IGMP ステート リミッタのメカニズムは、次のとおりです。

- ルータが特定のグループまたはチャネルに関する IGMP メンバーシップ レポートを受信するたびに、Cisco IOS ソフトウェアは、グローバル IGMP ステート リミッタまたはインターフェイスごとの IGMP ステート リミッタが制限に達したかどうかを確認します。
- グローバル IGMP ステート リミッタだけが設定されていて、その制限に達していない場合は、IGMP メンバーシップ レポートは受け入れられます。設定されている制限に達した場

合は、以降の IGMP メンバーシップ レポートは無視され（ドロップされ）、次のいずれかの形式の警告メッセージが生成されます。

- ```
  %IGMP-6-IGMP_GROUP_LIMIT: IGMP limit exceeded for <group (*, group address)> on
   <interface type number> by host <ip address>
  ```
- ```
  %IGMP-6-IGMP_CHANNEL_LIMIT: IGMP limit exceeded for <channel (source address,
  group address)> on <interface type number> by host <ip address>
  ```

- インターフェイスごとの IGMP ステート リミッタだけに達した場合、各制限はそれが設定されているインターフェイスに対してだけカウントされます。
- グローバル IGMP ステート リミッタとインターフェイスごとの IGMP ステート リミッタの両方が設定されている場合、インターフェイスごとの IGMP ステート リミッタに設定されている制限も実施されますが、グローバル制限により制約されます。

IGMP ステート制限の設定方法

ここでは、IGMP ステート制限を設定する方法について説明します。

IGMP ステート リミッタの設定

IGMP ステート リミッタは、IGMP、IGMP v3lite、および URD メンバーシップ レポートから生じる route ステートの数に、グローバルにかまたはインターフェイスごとに制限をかけます。

グローバルな IGMP ステート リミッタの設定

デバイスごとに 1 つのグローバルな IGMP ステート リミッタを設定するには、次の任意作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp limit** *number*
4. **end**
5. **show ip igmp groups**

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）。

	コマンドまたはアクション	目的
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	**ip igmp limit** *number* 例： `Device(config)# ip igmp limit 150`	IGMP メンバーシップ レポート（IGMP 加入）から生じる mroute ステートの数に対するグローバルな制限を設定します。
ステップ 4	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp groups** 例： `Device# show ip igmp groups`	（任意）デバイスに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャスト グループを表示します。

インターフェイスごとの IGMP ステート リミッタの設定

インターフェイスごとの IGMP ステート リミッタを設定するには、次の任意作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip igmp limit** *number* [**except** *access-list*]
5. 次のいずれかを実行します。
   - **exit**
   - **end**
6. **show ip igmp interface** [*type number*]
7. **show ip igmp groups**

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）。

	コマンドまたはアクション	目的
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	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/0`	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。 • ホストに接続されているインターフェイスを指定します。
ステップ 4	**ip igmp limit** *number* [**except** *access-list*] 例： `Device(config-if)# ip igmp limit 100`	IGMP メンバーシップ レポート（IGMP 加入）の結果として作成される mroute ステートの数に対するインターフェイスごとの制限を設定します。

ステップ 5	次のいずれかを実行します。
	• **exit**
	• **end**
	例：
	`Device(config-if)# exit`
	`Device(config-if)# end`
		• （任意）現在のコンフィギュレーション セッションを終了して、グローバル コンフィギュレーション モードに戻ります。別のインターフェイスでインターフェイスごとのリミッタを設定するには、ステップ 3 および 4 を繰り返します。
		• 現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。

ステップ 6	**show ip igmp interface** [*type number*] 例： `Device# show ip igmp interface`	（任意）インターフェイス上の IGMP のステータスと設定およびマルチキャスト ルーティングに関する情報を表示します。
ステップ 7	**show ip igmp groups** 例： `Device# show ip igmp groups`	（任意）デバイスに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャスト グループを表示します。

IGMP ステート制限の設定例

ここでは、IGMP ステート制限の設定例を紹介します。

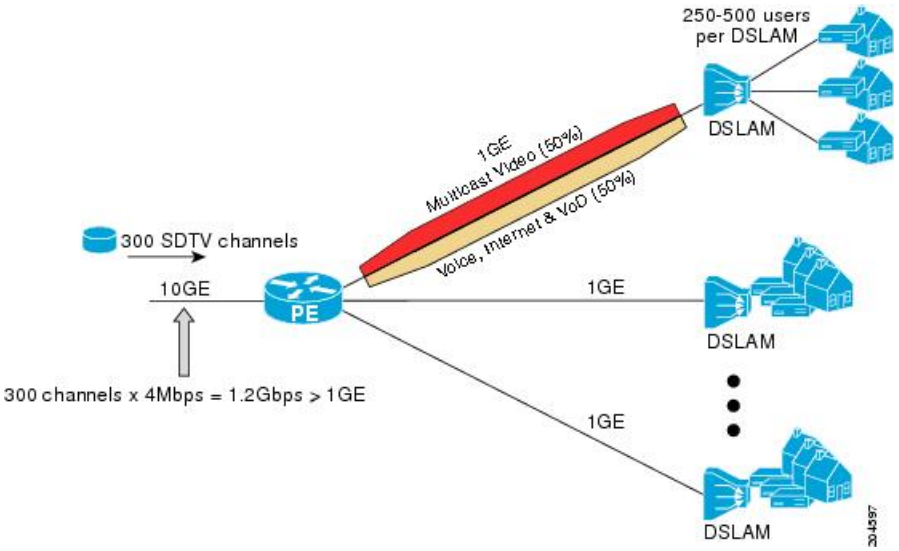
IGMP ステート リミッタの設定例

次の例は、すべてのマルチキャスト フローがほぼ同量の帯域幅を使用するネットワーク環境でマルチキャスト CAC を提供するために、IGMP ステート リミッタを設定する方法を示します。

この例では、図に示すトポロジを使用します。

（注） 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 *47 : IGMP* ステート制限のサンプル トポロジ



この例では、サービス プロバイダーは、300 の標準画質（SD）TV チャネルを提供しています。各 SD チャネルが、約 4 Mbps を使用します。

このサービス プロバイダーは、デジタル加入者回線アクセス マルチプレクサ（DSLAM）に接続されている PE ルータ上のギガビット イーサネット インターフェイスを、リンクの帯域幅の 50%（500 Mbps）をインターネット、音声、およびビデオ オン デマンド（VoD）サービス提供の加入者が利用できるようにしたうえで、リンクの帯域幅の残りの 50%（500 Mbps）は SD チャネル提供の加入者が利用できるようにプロビジョニングしなければなりません。

各 SD チャネルが同量の帯域幅（4 Mbps）を使用するため、このサービス プロバイダーが提供するサービスのプロビジョニングに必要な CAC は、インターフェイスごとの IGMP ステート リミッタを使用して提供できます。インターフェイスごとに必要な必須 CAC を調べるために、チャネルの総数を 4 で割ります（各チャネルが 4 Mbps の帯域幅を使用するため）。したがって、インターフェイスごとに必要な必須 CAC は、次のようになります。

500Mbps / 4Mbps = 125 mroute

必須 CAC がわかったら、サービス プロバイダーは、その結果を使用して、PE ルータ上でギガビット イーサネット インターフェイスをプロビジョニングするのに必要な IGMP ごとのステー

トリミッタを設定します。このサービス プロバイダーは、ネットワークの CAC 要件に基づいて、ギガビット イーサネット インターフェイスから外部へ転送できる SD チャネルを（常時）125 に制限しなければなりません。SD チャネルのプロビジョンのためのインターフェイスごとの IGMP ステート制限を 125 に設定すると、リンクの帯域幅の 50% は常に SD チャネルの提供に確保しなければならない（しかし使用が 50% を超えてはならない）500 Mbps の帯域幅にインターフェイスをプロビジョニングできます。

次の設定は、サービス プロバイダーがインターフェイスごとの mroute ステート リミッタを使用して、加入者に提供する SD チャネルとインターネット、音声、および VoD サービス用にインターフェイス ギガビット イーサネット 0/0 をプロビジョニングする方法を示します。

```
interface GigabitEthernet0/0/0
description --- Interface towards the DSLAM ---
.
.
.
ip igmp limit 125
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)*

IP マルチキャストの最適化の機能履歴：IGMP ステート制限

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IPマルチキャストの最適化：IGMP ステート制限	IGMP ステート制限機能を使用すると、IGMP ステートリミッタの設定が可能になり、この設定により、IGMP メンバーシップ レポート（IGMP 加入）により生成される mroute ステートの数がグローバルに、またはインターフェイスごとに制限されます。設定されている制限を超えたメンバーシップ レポートは、IGMP キャッシュに入れられません。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/にアクセスします。

翻訳について
このドキュメントは、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。