Cisco IOS XE Everest 16.6.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：2017 年 07 月 31 日

最終更新：2017 年 11 月 03 日

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

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

目 次

第 1 章

IP マルチキャスト ルーティング テクノロジーの概要

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよび Cisco ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、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。

IP マルチキャスト テクノロジーに関する情報

IP マルチキャストについて

（注） 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。
- 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。

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。

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 デンス モード（PIM-DM）

PIM デンス モード（PIM-DM）は、プッシュ モデルを使用してマルチキャスト トラフィックをネットワークの隅々にまでフラッディングします。PIM-DM は、LAN TV や企業情報または財務情報ブロードキャストなど、大部分の LAN でマルチキャストの受信が必要とされるネットワーク

での使用を目的としています。これは、ネットワーク上のすべてのサブネットにアクティブな受信者が存在する場合、効率的な配信メカニズムになります。

PIM デンス モードの詳細については、次の URL を参照してください。 http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_optim/configuration/12-2sx/imc_pim_dense_rfrsh.html

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。

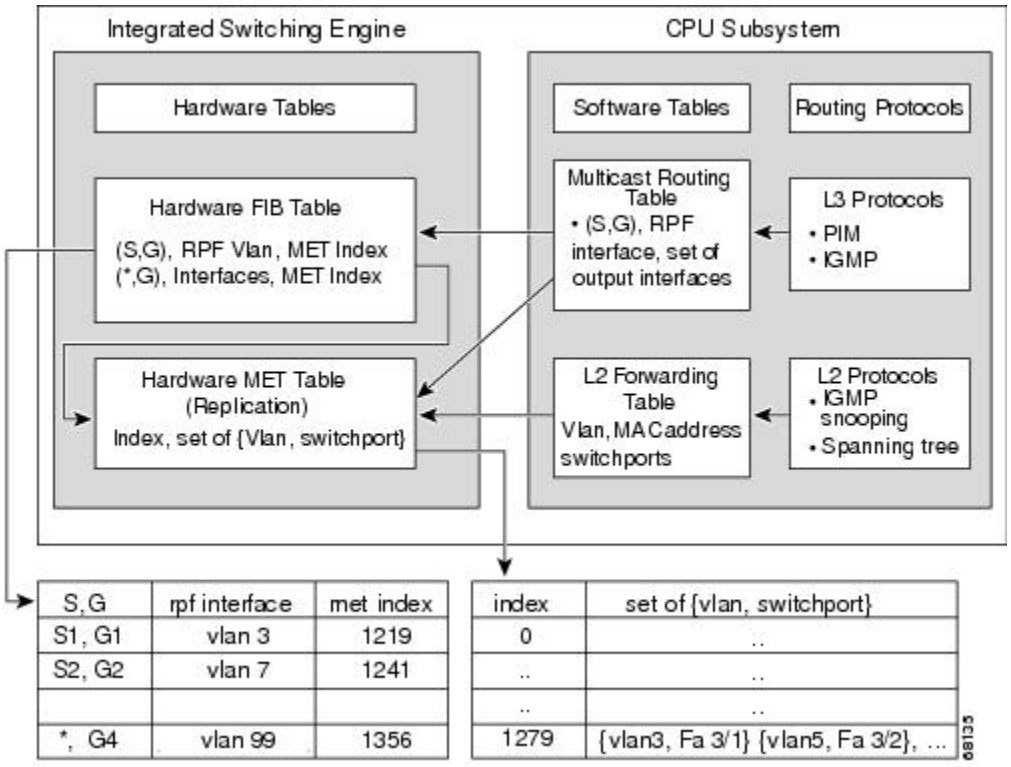
IGMP 制御メッセージはマルチキャスト パケットとして送信されるので、レイヤ 2 ヘッダーだけが検証される場合は、マルチキャスト データと区別できません。IGMP スヌーピングが稼働しているスイッチは、すべてのマルチキャスト データ パケットについて、関連する IGMP 制御情報が含まれているかどうかを調べます。低速の CPU を搭載したローエンドのスイッチに IGMP スヌー

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 *1*：*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

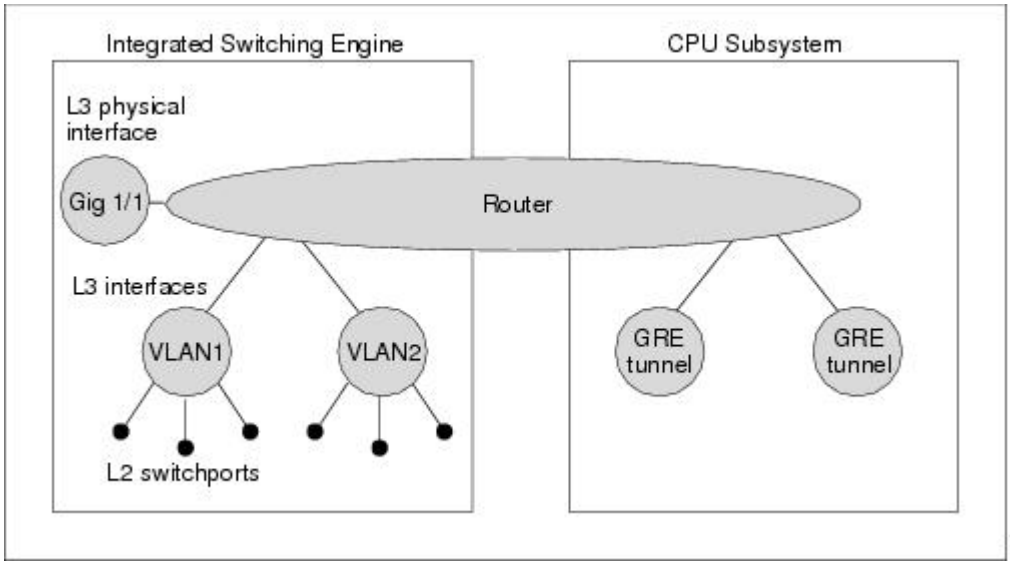
（注） （RET では 102 K エントリまでサポートされます（フラッディング セットに 32K、multicast エントリに 70 K を使用））。

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 *2*：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。

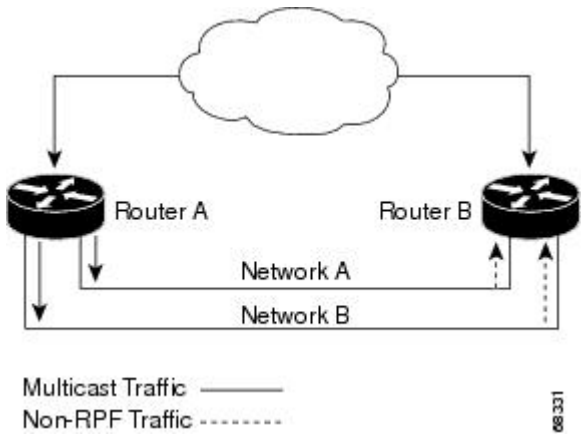
- 224.0.0* の範囲に入るマルチキャスト グループに送信されたパケット。（* は 0 ～ 255 の範囲）。この範囲は、ルーティング プロトコルが使用します。レイヤ 3 スイッチングでは、この範囲以外のすべてのマルチキャスト グループ アドレスがサポートされています。
- IP オプション付きのパケット

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 *3*：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。

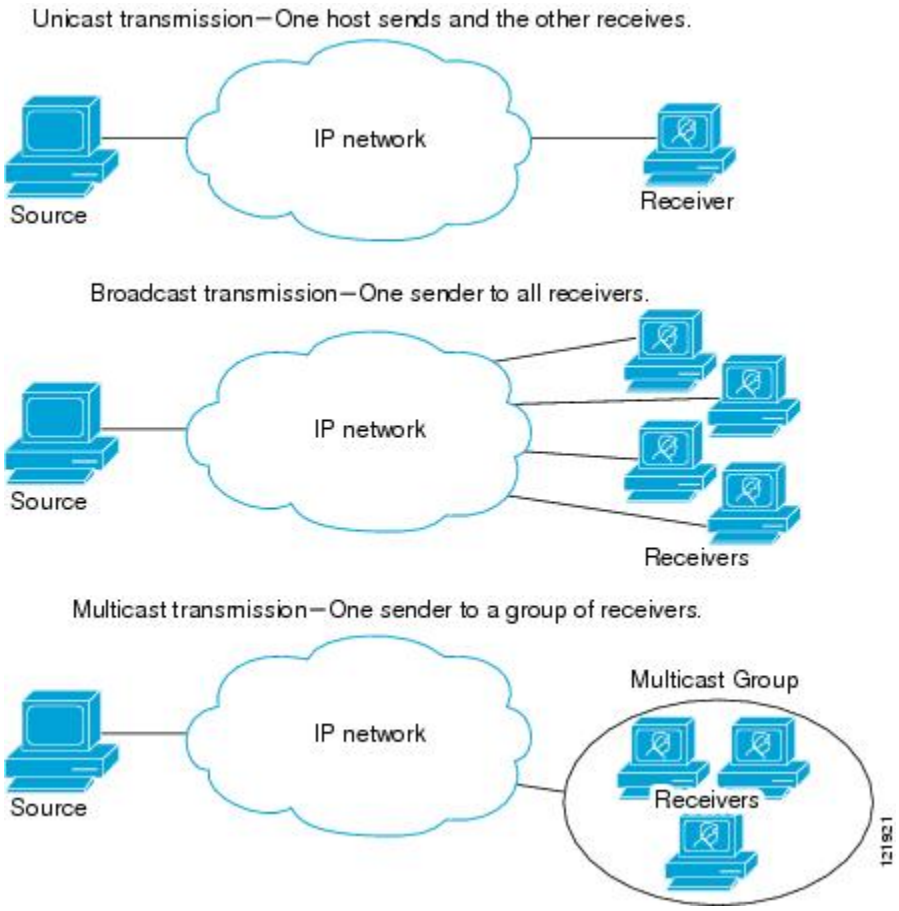
マルチキャスト グループ伝送方式

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。

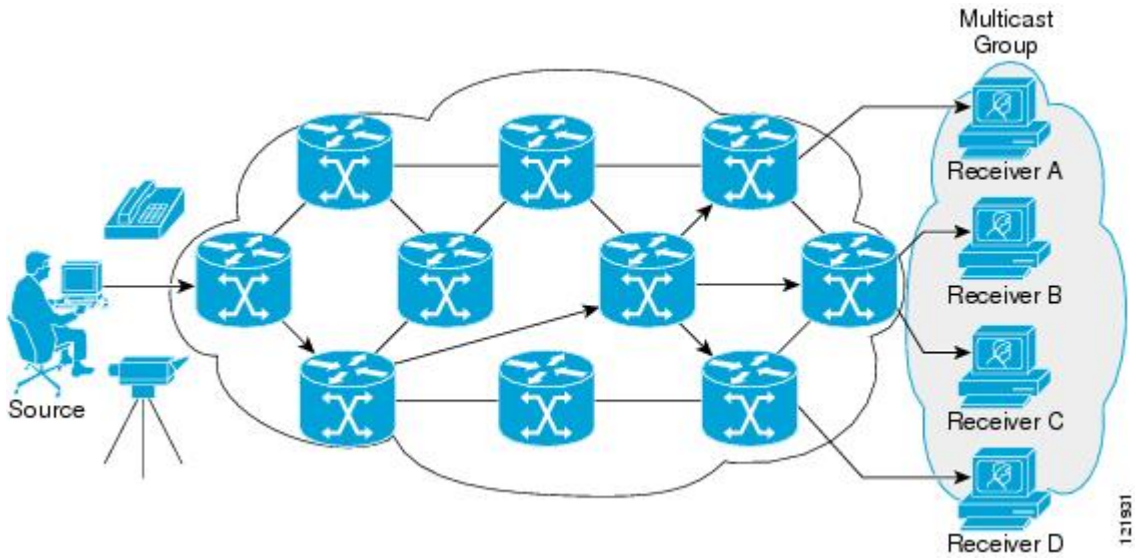
マルチキャストは、このグループの概念に基づいています。マルチキャスト グループは、特定のデータ ストリームを受信するためにグループに加入する任意の数のレシーバです。このマルチキャスト グループには、物理的境界または地理的境界はありません。ホストは、インターネット上または任意のプライベート ネットワーク上のどこにでも配置できます。ソースから特定のグループに対するデータを受信する必要があるホストはそのグループに加入する必要があります。グループに加入するには、ホスト レシーバで Internet Group Management Protocol（IGMP）を使用します。

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

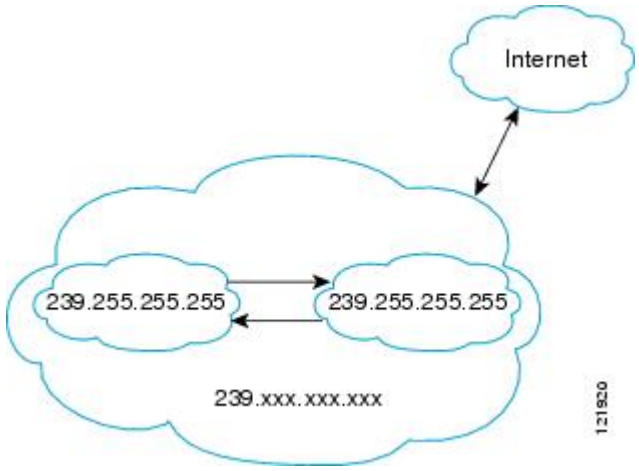
トレポートを送信することによってその意思を示します。この場合、ルータがソースからレシーバへのデータの配信を担います。ルータは、Protocol Independent Multicast（PIM）を使用して、マルチキャスト配信ツリーを動的に作成します。その後、ソースとレシーバ間のパスにあるネットワーク セグメントにのみ、ビデオ データ ストリームが配信されます。



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 *4*：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、**ipmulticastboundary** 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。
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、**ippimssm** 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

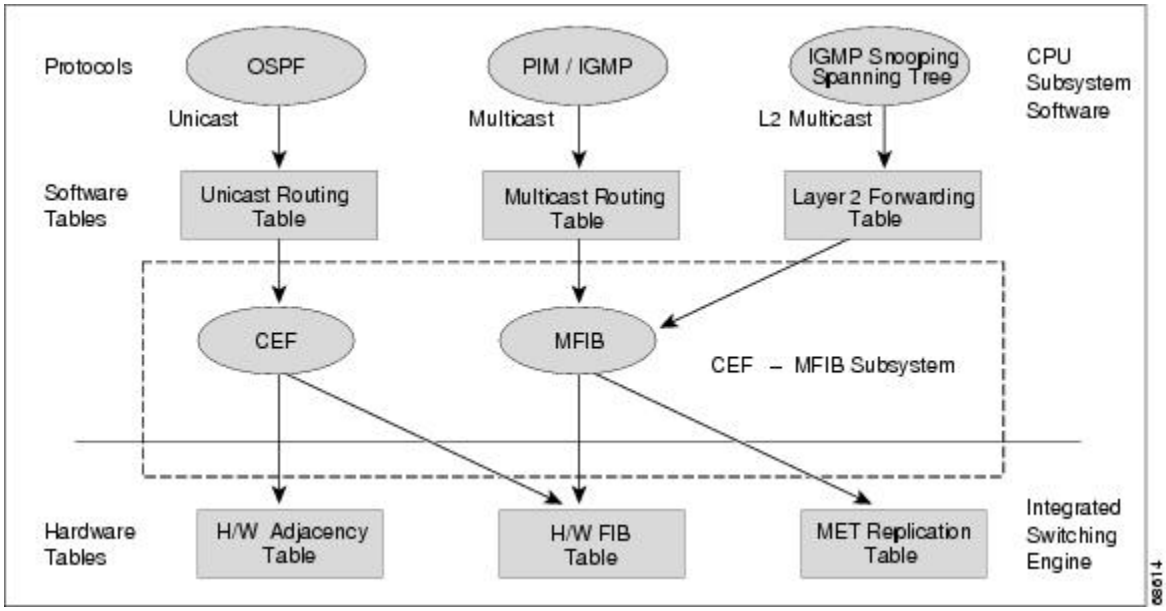
実装された IP マルチキャストは、中央集中型シスコ エクスプレス フォワーディングの拡張機能です。シスコ エクスプレス フォワーディングは、ユニキャスト ルーティング テーブル（BGP、OSPF、EIGRP などのユニキャスト ルーティング プロトコルによって作成される）から情報を抽出し、この情報をハードウェアにロードします。

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 *5*：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 94000 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 のスパース、デンス、Bidir、および SSM モードにサポートされ、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	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

標準および RFC

標準/RFC	役職（Title）
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*』

MIB

MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

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 デバイスは、マルチキャスト グループのメンバー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

デバイス 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ディセーブル
PIM のバージョン	バージョン 2
PIM モード	モードは未定義
PIM スタブ ルーティング	未設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル。
PIM マルチキャスト境界	なし。
候補 BSR	ディセーブル。
候補 RP	ディセーブル。
SPT しきい値レート	0 kb/s
PIM ルータ クエリー メッセージ インターバル	30 秒

基本的な IP マルチキャスト ルーティングの設定方法

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。

はじめる前に

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。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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。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

	コマンドまたはアクション	目的
		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： `Device(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 をディセーブルにするには、**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： `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。

IP マルチキャスト フォワーディングの設定

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** コマンドの **no** 形式を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権EXECモードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。

	コマンドまたはアクション	目的
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 を設定するには、次の手順を実行します。スタティック mroute は、ユニキャスト スタティック ルートに類似していますが、以下の点で異なります。

- 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。

スタティック 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。

スタティック mroute が設定されると、デバイス のスタティック 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、スタティック 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スタティック 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。

複数のスタティック 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip mroute** [**vrf** *vrf-name*] *source-address mask* { **fallback-lookup** {**global** | **vrf** *vrf-name* }[*protocol*] {*rpf-address* | *interface-type interface-number*}} [**distance**] 例： `Device(configure)# 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

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**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。

	コマンドまたはアクション	目的
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。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 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。

	コマンドまたはアクション	目的
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

sdr リスナー サポートのイネーブル化

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。

	コマンドまたはアクション	目的
		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、次を参照してください。 例：ルーテッド ポートとしてのインターフェイス設定, （150ページ） • 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。設定例については、次を参照してください。 例：SVI としてのインターフェイスの設定, （150 ページ） 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`	（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
	running-config **startup-config**	

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sap cache-timeout** 分 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。

	コマンドまたはアクション	目的
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（Command）	目的
clear ip igmp group {**group** [*hostname* | *IP address*] | **vrf** *name***group** [*hostname* | *IP address*] }	IGMP キャッシュのエントリを削除します。
clear ip mroute { ***** | [*hostname* | *IP address*] | **vrf** *name***group** [*hostname* | *IP address*] }	IP マルチキャスト ルーティング テーブルからエントリを削除します。

コマンド（Command）	目的
clear ip sap [*group-address* | **"***session-name***"**]	Session Directory Protocol バージョン 2 キャッシュ（sdr キャッシュ）エントリを削除します。

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（Command）	目的
ping [*group-name* | *group-address*]	マルチキャスト グループ アドレスにインターネット制御メッセージ プロトコル（ICMP）エコー要求を送信します。
show ip igmp groups [*group-name*|*group-address*|*type-number*]	デバイスに直接接続され、IGMP によって取得されたマルチキャスト グループを表示します。
show ip igmp interface [*type number*]	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。
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 テーブルの内容を表示します。
show ip pim interface [*type number*] [**count** | **detail** | **df** | **stats**]	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。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。

コマンド（Command）	目的
show ip pim neighbor [*type number*]	デバイスによって検出された PIM ネイバーのリストを示します。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 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 rpf {*source-address* | *name*}	デバイスのリバース パス転送（RPF）の実行方法（ユニキャスト ルーティング テーブル、DVMRP ルーティング テーブル、またはスタティック マルチキャスト ルーティングのいずれかから）を表示します。 コマンド パラメータは次のとおりです。 • *Host name* または *IP address*：IP 名またはグループ アドレス。 • **Select**：グループ ベースの VRF 選択情報。 • **vrf**：VPN ルーティング/転送インスタンスを選択します。
show ip sap [*group* | "*session-name*" | **detail**]	Session Announcement Protocol（SAP）バージョン 2 キャッシュを表示します。 コマンド パラメータは次のとおりです。 • *A.B.C.D*：IP グループ アドレス。 • *WORD*：セッション名（二重引用符で囲む）。 • **detail**：セッションの詳細。

IP マルチキャスト ルーティングの設定例

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。

```
Device(config)# access-list 1 deny 239.0.0.0 0.255.255.255
Device(config)# access-list 1 permit 224.0.0.0 15.255.255.255
Device(config)# interface gigabitethernet1/0/1
Device(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 デバイス 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 デバイス 自体をクエリすることもできます。

```
Device# 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	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

MIB

MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

基本的な IP マルチキャスト ルーティングの機能情報

次の表に、このモジュールで説明した機能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 リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *5* : 基本的な *IP* マルチキャスト ルーティングの機能情報

機能名（Feature Name）	リリース	機能情報
基本的な IP マルチキャスト ルーティング	Cisco IOS XE Everest 16.5.1a	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。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

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 2000 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 9300 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、ip PIM デンス モード、スパース - デンス モード、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。

（注） Cisco IOS XE Denali 16.3.1 以降では、マルチキャスト ルーティングおよび NHRP が GRE トンネリングでサポートされています。トンネル エンド ポイントのダイナミック検出を促進するために、トンネル インターフェイス上のマルチキャスト設定とともに、NHRP をオプションで設定できます。トンネル インターフェイスに NHRP を設定する方法については、NHRP 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

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

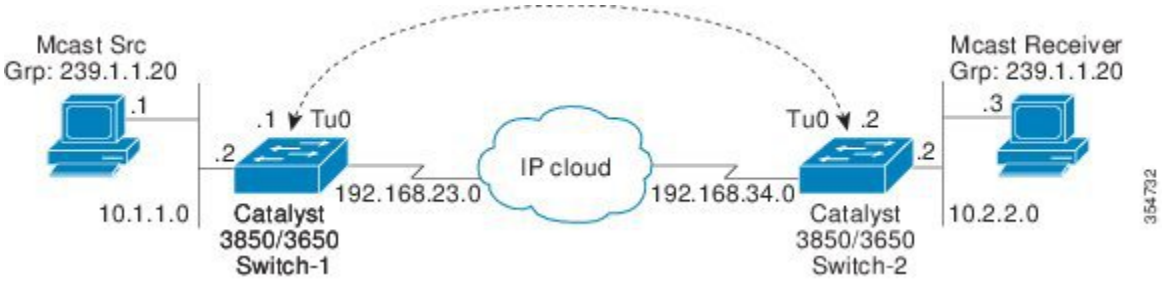
	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip multicast-routing** 例： `Device(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。
ステップ 4	**interfacetunnel** *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。

	コマンドまたはアクション	目的
ステップ 6	**ippim** { **sparse-dense-mode** | **sparse-mode** | **dense-mode** } 例： `Device(config-if)# ip pim sparse-dense-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）を有効にします。 • **sparse-dense-mode** ：マルチキャスト グループの動作モードに応じて、インターフェイスをスパース動作モードまたはデンス動作モードで処理します。 • **sparse-mode** ：スパース動作モードをイネーブルにします。 • **dense-mode** ：デンス動作モードをイネーブルにします。
ステップ 7	**tunnelsource** { *ip-address* | *interface-name* } 例： `Device(config-if)# tunnel source 100.1.1.1`	トンネル送信元を設定します。
ステップ 8	**tunneldestination** { *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 *6*：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 モードまたはデンス モードで PIM をサポートするために、**ip pim sparse-dense-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 sparse-dense-mode 設定により、スパース モード パケットまたはデンス 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-dense-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-dense-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-dense 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-dense-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	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

MIB

MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

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情報

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

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

表 *6*：*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情報

機能名（Feature Name）	リリース	機能情報
GRE トンネルを介するマルチキャスト ルーティング	Cisco IOS XE Everest 16.5.1a	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、GRE トンネルを設定する方法について説明します。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

第 4 章

VRF-Lite の設定

VRF-Lite について

VRF-Lite の機能によって、サービス プロバイダーは、VPN 間で重複した IP アドレスを使用できる複数の VPN をサポートできます。VRF-Lite は入力インターフェイスを使用して異なる VPN のルートを区別し、各 VRF に 1 つまたは複数のレイヤ 3 インターフェイスを対応付けて仮想パケット転送テーブルを形成します。VRF のインターフェイスは、イーサネット ポートなどの物理インターフェイス、または VLAN SVI などの論理インターフェイスにすることができますが、レイヤ 3 インターフェイスは、一度に複数の VRF に属することはできません。

（注） VRF-Lite インターフェイスは、レイヤ 3 インターフェイスである必要があります。

VRF-Lite には次のデバイスが含まれます。

- CE デバイスにおいて、カスタマーは、1 つまたは複数の プロバイダー エッジ（PE）ルータへのデータ リンクを介してサービス プロバイダー ネットワークにアクセスできます。CE デバイスは、サイトのローカル ルートをプロバイダー エッジ ルータにアドバタイズし、そこ

からリモート VPN ルートを学習します。Cisco Catalyst スイッチは、CE にすることができます。

- プロバイダー エッジ（PE）ルータは、スタティック ルーティングまたはルーティング プロトコル（BGP、RIPv1、RIPv2 など）を使用して、CE デバイスとルーティング情報を交換します。

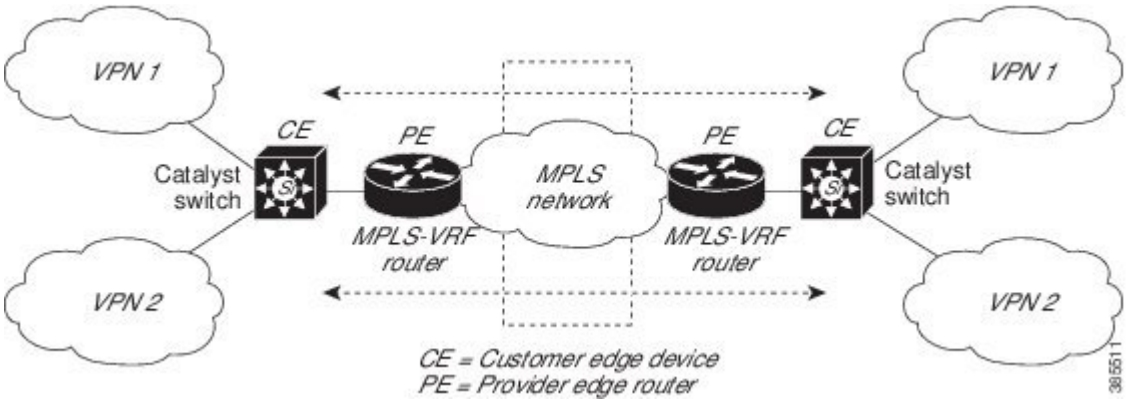
  PE は、直接接続している VPN に対する VPN ルートのみを保守する必要があります。そのため、すべてのサービス プロバイダー VPN ルートを PE が保守する必要はありません。各 PE ルータは、直接接続しているサイトごとに VRF を維持します。すべてのサイトが同じ VPN に存在する場合は、PE ルータの複数のインターフェイスを 1 つの VRF に関連付けることができます。各 VPN は、指定された VRF にマッピングされます。PE ルータは、ローカル VPN ルートを CE から学習したあとで、IBGP を使用して別の PE ルータと VPN ルーティング情報を交換します。

- プロバイダー ルータ（またはコア ルータ）とは、サービス プロバイダー ネットワーク内にあり、CE デバイスに接続していないすべてのルータです。

VRF-lite を使用すると、複数の顧客が 1 つの CE を共有できます。また、1 つの物理リンクのみが CE と PE 間に使用されます。共有 CE は、お客様ごとに別々の VRF テーブルを維持し、独自のルーティング テーブルに基づいて、お客様ごとにパケットをスイッチングまたはルーティングします。VRF-lite は限定された PE の機能を CE デバイスに拡張して、個別の VRF テーブルを保守する機能を付与し、VPN のプライバシーおよびセキュリティをブランチ オフィスまで拡張します。

次の図に、各 Cisco Catalyst スイッチが複数の仮想 CE として機能する設定を示します。VRF-Lite はレイヤ 3 機能であるため、VRF の各インターフェイスはレイヤ 3 インターフェイスである必要があります。

図 *7*：複数の仮想 *CE* として機能する *Cisco Catalyst* スイッチ



次の図に、VRF-Lite の CE 対応ネットワークでのパケット転送プロセスを示します。

- CE が VPN からパケットを受信すると、CE は入力インターフェイスに基づいたルーティング テーブルを検索します。ルートが見つかると、CE はパケットを PE に転送します。

- 入力 PE は、CE からパケットを受信すると、VRF 検索を実行します。ルートが見つかると、ルータは対応する MPLS ラベルをパケットに追加し、MPLS ネットワークに送信します。

- 出力 PE は、ネットワークからパケットを受信すると、ラベルを除去してそのラベルを使用し、正しい VPN ルーティング テーブルを識別します。次に、出力 PE が通常のルート検索を行います。ルートが見つかると、パケットを正しい隣接デバイスに転送します。
- CE が出力 PE からパケットを受信すると、CE は入力インターフェイスを使用して正しい VPN ルーティング テーブルを検索します。ルートが見つかると、CE はパケットを VPN 内に転送します。

VRF を設定するには、VRF テーブルを作成し、VRF に対応付けられたレイヤ 3 インターフェイスを指定します。次に、VPN および CE と PE 間でルーティング プロトコルを設定します。プロバイダーのバックボーンで VPN ルーティング情報を配信する場合は、BGP が優先ルーティング プロトコルです。VRF-Lite ネットワークには、次の 3 つの主要なコンポーネントがあります。

- VPN ルート ターゲット コミュニティ：VPN コミュニティの他のすべてのメンバをリストします。VPN コミュニティ メンバーごとに VPN ルート ターゲットを設定する必要があります。
- VPN コミュニティ PE ルータのマルチプロトコル BGP ピアリング： VPN コミュニティのすべてのメンバに VRF の到着可能性情報を伝播します。VPN コミュニティのすべての PE ルータで BGP ピアリングを設定する必要があります。
- VPN 転送：VPN サービスプロバイダー ネットワークのすべての VPN コミュニティ メンバ間のすべてのトラフィックを転送します。

VRF-Lite の設定に関するガイドライン

IPv4 と IPv6

- VRF-Lite が設定されたスイッチは複数のカスタマーで共有され、すべてのカスタマーが独自のルーティング テーブルを持ちます。
- カスタマーは別々の VRF テーブルを使用するので、同じ IP アドレスを再利用できます。別々の VPN では IP アドレスの重複が許可されます。
- VRF-Lite では、複数のカスタマーが PE と CE の間で同一の物理リンクを共有できます。複数の VLAN を持つトランク ポートでは、パケットがお客様間で分離されます。すべてのカスタマーが独自の VLAN を持ちます。
- PE ルータでは、VRF-Lite の使用と複数の CE の使用には違いがありません。#unique_93 では、複数の仮想レイヤ 3 インターフェイスが VRF-Lite デバイスに接続されています。
- Cisco Catalyst スイッチでは、物理ポートか VLAN SVI、またはその両方の組み合わせを使用して、VRF を設定できます。アクセス ポートまたはトランク ポート経由で SVI を接続できます。
- お客様は、別のお客様と重複しないかぎり、複数の VLAN を使用できます。お客様の VLAN は、スイッチに保存されている適切なルーティング テーブルの識別に使用される特定のルーティング テーブル ID にマッピングされます。

- レイヤ 3 TCAM リソースは、すべての VRF 間で共有されます。各 VRF が十分な CAM 領域を持つようにするには、**maximum routes** コマンドを使用します。
- VRF を使用した Cisco Catalyst スイッチは、1 つのグローバル ネットワークと複数の VRF をサポートできます。サポートされるルートの総数は、TCAM のサイズに制限されます。
- 1 つの VRF を IPv4 と IPv6 の両方に設定できます。
- 着信パケットの宛先アドレスが VRF テーブルにない場合、そのパケットはドロップされます。また、VRF ルートに TCAM 領域が十分にない場合、その VRF のハードウェア切り替えは無効になり、対応するデータ パケットがソフトウェアに送信されて処理されます。

IPv4 固有

- CE と PE 間のほとんどのルーティング プロトコル（BGP、OSPF、EIGRP、RIP、およびスタティック ルーティング）を使用できます。ただし、次の理由から External BGP（EBGP）を使用することを推奨します。
  - BGP では、複数の CE とのやり取りに複数のアルゴリズムを必要としません。
  - BGP は、さまざまな管理者によって稼働するシステム間でルーティング情報を渡すように設計されています。
  - BGP は、ルートの属性の CE への引き渡しを単純化します。
- Cisco Catalyst スイッチでは、すべての PIM プロトコル（PIM-SM、PIM-DM、PIM-SSM）がサポートされます。
- **router ospf** の **capability vrf-lite** サブコマンドは、PE と CE 間のルーティング プロトコルとして OSPF が設定されている場合に使用する必要があります。

IPv6 固有

- VRF 認識 OSPFv3、BGPv6、EIGRPv6、および IPv6 スタティック ルーティングがサポートされます。
- VRF 認識 IPv6 ルート アプリケーションには、ping、telnet、ssh、tftp、ftp、およびトレースルートが含まれています（このリストには Mgt インターフェイスは含まれていません。これは、その下に IPv4 も IPv6 も設定できますが、別々に処理されます）。

トピック 2.1

VRF-Lite の設定方法

IPv4 用の VRF-Lite の設定

VRF 認識サービスの設定

IP サービスは、グローバルなインターフェイス上と、グローバルなルーティング インスタンス内で設定できます。IP サービスは複数のルーティング インスタンス上で稼働するように拡張されます。これが、VRF 認識です。システム内の任意の設定済み VRF であればいずれも、VRF 認識サービス用に指定できます。

VRF 認識サービスは、プラットフォームから独立したモジュールに実装されています。VRF は、Cisco IOS 内の複数のルーティング インスタンスを提供します。各プラットフォームには、サポートする VRF 数に関して独自の制限があります。

VRF 認識サービスには、次の特性があります。

- ユーザは、ユーザ指定の VRF 内のホストに ping を実行できます。
- ARP エントリは、個別の VRF で学習されます。ユーザは、特定の VRF の ARP エントリを表示できます。

ARP のユーザ インターフェイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**show ip arp vrf** *vrf-name* 例： `Switch# show ip arp vrf vrf-name`	指定された VRF で、ARP テーブル（スタティック エントリおよびダイナミック エントリ）を表示します。
ステップ 2	**arp vrf** *vrf-name ip-address mac-address ARPA* 例： `Switch(config)# arp vrf vrf-name ip-address mac-address ARPA`	指定された VRF でスタティック ARP エントリを作成します。

TACACS+ サーバ用の Per-VRF の設定

TACACS+ サーバ機能の per-VRF は TACACS+ サーバの per- 仮想単位ルート転送（per-VRF）の認証、認可、アカウンティング（AAA）を設定することができます。

VRF ルーティング テーブル（ステップ 3 および 4 で示すように）を作成し、インターフェイスを設定する（ステップ 6、7、および 8）ことができます。TACACS+ サーバの per-VRF 単位の実際の設定は、ステップ 10～13 で行われます。

はじめる前に

TACACS+ サーバの per-VRF を設定する前に、AAA およびサーバ グループを設定しておく必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip vrf** *vrf-name* 例： `Switch(config)# ip vrf vrf-name`	VRF テーブルを設定し、VRF 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	**rd** *route-distinguisher* 例： `Switch (config-vrf)# rd route-distinguisher`	VRF インスタンスに対するルーティングおよびフォワーディング テーブルを作成します。
ステップ 5	**exit** 例： `Switch (config-vrf)# exit`	VRF コンフィギュレーション モードを終了します。
ステップ 6	**interface** *interface-name* 例： `Switch (config)# interface interface-name`	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。

	コマンドまたはアクション	目的
ステップ 7	**vrf forwarding** *vrf-name* 例： `Switch (config-if)# vrf forwarding vrf-name`	インターフェイスに VRF を設定します。
ステップ 8	**ip address** *ip-address mask* [**secondary**] 例： `Switch (config-if)# ip address ip-address mask [secondary]`	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 9	**exit** 例： `Switch (config-vrf)# 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 10	**aaa group server tacacs+** *group-name* 例： `Switch (config)# aaa group server tacacs+ tacacs1`	異なる TACACS+ サーバ ホストを別々のリストと方式にグループ化し、server-group コンフィギュレーション モードを開始します。
ステップ 11	**server-private** {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*] 例： `Switch (config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco`	グループ サーバに対するプライベート TACACS+ サーバの IP アドレスを設定します。
ステップ 12	**vrf forwarding** *vrf-name* 例： `Switch (config-sg-tacacs+)# vrf forwarding vrf-name`	AAA TACACS+ サーバ グループの VRF リファレンスを設定します。
ステップ 13	**ip tacacs source-interface** *subinterface-name* 例： `Switch (config-sg-tacacs+)# ip tacacs source-interface subinterface-name`	すべての発信 TACACS+ パケットに対して、指定されたインターフェイスの IP アドレスを使用します。
ステップ 14	**exit** 例： `Switch (config-sg-tacacs)# exit`	server-group コンフィギュレーション モードを終了します。

次の例で、per-VRF TACACS+ の設定に必要なすべての手順をリストします。

```
Switch> enable
Switch# configure terminal
Switch (config)# ip vrf cisco
Switch (config-vrf)# rd 100:1
Switch (config-vrf)# exit
Switch (config)# interface Loopback0
Switch (config-if)# vrf forwarding cisco
Switch (config-if)# ip address 10.0.0.2 255.0.0.0
Switch (config-if)# exit
Switch (config-sg-tacacs+)# vrf forwarding cisco
Switch (config-sg-tacacs+)# ip tacacs source-interface Loopback0
Switch (config-sg-tacacs)# exit
```

マルチキャスト VRF の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing** 例： `Switch(config)# ip routing`	IP ルーティングをイネーブルにします。
ステップ 3	**ip vrf** *vrf-name* 例： `Switch(config)# ip vrf vrf-name`	VRF テーブルを設定し、VRF 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 multicast-routing vrf** *vrf-name* 例： `Switch(config-vrf)# ip multicast-routing vrf vrf-name`	（任意）VRF テーブルでグローバル 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 5	**rd** *route-distinguisher* 例： `Switch (config-vrf)# rd route-distinguisher`	ルート識別子を指定して VRF テーブルを作成します。自律システム（AS）番号および任意の数（xxx:y）または IP アドレスおよび任意の数（A.B.C.D:y）のどちらかを入力します。
ステップ 6	**route-target** {**export** | **import** | **both**} *route-target-ext-community* 例： `Switch(config-vrf)# route-target {export | import | both} route-target-ext-community`	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。

	コマンドまたはアクション	目的
		ルート ターゲット ext コミュニティ値は、ステップ 4 で入力した route-distinguisher 値と同じです。
ステップ 7	**import map** ルート マップ 例： `Switch(config-vrf)# import map route-map`	（任意）VRF にルート マップを対応付けます。
ステップ 8	**interface** *interface-id* 例： `Switch (config)# interface interface-id`	インターフェイス コンフィギュレーション モードを開始して、VRF に対応付けるレイヤ 3 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、ルーテッド ポートまたは SVI です。
ステップ 9	**vrf forwarding** *vrf-name* 例： `Switch (config-sg-tacacs+)# vrf forwarding vrf-name`	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 10	**ip address** *ip-address* **mask** 例： `Switch (config-if)# ip address ip-address mask`	レイヤ 3 インターフェイスの IP アドレスを設定します。
ステップ 11	**ip pim** [**sparse-dense mode** | **dense-mode** | **sparse-mode**] 例： `Switch(config-if)# ip pim [sparse-dense mode | dense-mode | sparse-mode]`	VRF に関連付けられているレイヤ 3 インターフェイス上で、PIM をイネーブルにします。
ステップ 12	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 13	show ip vrf [brief | detail | interfaces] [vrf-name] 例： **show ip vrf** ［**brief** | **detail** | **interfaces**］［*vrf-name*］	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 14	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、VRF テーブル内にマルチキャストを設定する例を示します。

```
Switch(config)# ip routing
Switch(config)# ip vrf multiVrfA
Switch(config-vrf)# ip multicast-routing vrf multiVrfA
Switch(config-vrf)# interface GigabitEthernet3/1/0
Switch(config-if)# vrf forwarding multiVrfA
Switch(config-if)# ip address 172.21.200.203 255.255.255.0
Switch(config-if)# ip pim sparse-mode
```

VPN ルーティング セッションの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospf** *process-id***vrf vrf-name** 例： `Switch(config)# router ospf process-id vrf vrf-name`	OSPF ルーティングをイネーブルにし、VPN 転送テーブルを指定して、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**log-adjacency-changes** 例： `Switch(config-router)# log-adjacency-changes`	（任意）隣接状態（デフォルト）の変更を記録します。
ステップ 4	**redistribute bgp** *autonomous-system-number subnets* 例： `Switch(config-router)# redistribute bgp autonomous-system-number subnets`	BGP ネットワークから OSPF ネットワークに情報を再配布するようにスイッチを設定します。
ステップ 5	**network** *network-number***area** *area-id* 例： `Switch(config-router)# network network-number area area-id`	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	**end** 例： `Switch(config-router)# 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 7	**show ip ospf** *process-id* 例： `Switch# show ip ospf process-id`	OSPF ネットワークの設定を確認します。
ステップ 8	copy running-config startup-config 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。 **no router ospf** *process-id* **vrf** *vrf-name* 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、OSPF ルーティング プロセスから VPN転送テーブルの関連付けを解除します。

```
Switch(config)# ip vrf VRF-RED
Switch(config-vrf)# rd 1:1
Switch(config-vrf)# exit
Switch(config)# router eigrp virtual-name
Switch(config-router)# address-family ipv4 vrf VRF-RED autonomous-system 1
Switch(config-router-af)# network 10.0.0.0 0.0.0.255
Switch(config-router-af)# topology base
Switch(config-router-topology)# default-metric 10000 100 255 1 1500
Switch(config-router-topology)# exit-af-topology
Switch(config-router-af)# exit-address-family
```

BGP PE/CE ルーティング セッションの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number* 例： `Switch(config)# router bgp autonomous-system-number`	その他の BGP ルータに渡された AS 番号で BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**network** *network-number***mask** *network-mask* 例： `Switch(config-router)# network network-number mask network-mask`	BGP を使用してアナウンスするネットワークおよびマスクを指定します。

	コマンドまたはアクション	目的
ステップ 4	**redistribute ospf** *process-id match internal* 例： `Switch(config-router)# redistribute ospf process-id match internal`	OSPF内部ルートを再配布するようにスイッチを設定します。
ステップ 5	**network** *network-number***area** *area-id* 例： `Switch(config-router)# network network-number area area-id`	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	**address-family ipv4 vrf** *vrf-name* 例： `Switch(config-router-af)# address-family ipv4 vrf vrf-name`	PE から CE のルーティング セッションの BGP パラメータを定義し、VRF アドレス ファミリ モードを開始します。
ステップ 7	**neighbor** *address***remote-as** *as-number* 例： `Switch(config-router-af)# neighbor address remote-as as-number`	PE と CE ルータの間の BGP セッションを定義します。
ステップ 8	**neighbor** *address***activate** 例： `Switch(config-router-af)# neighbor address activate`	IPv4 アドレス ファミリのアドバタイズメントをアクティブ化します。
ステップ 9	**end** 例： `Switch(config-router-af)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show ip bgp** [**ipv4**] [**neighbors**] 例： `Switch# show ip bgp [ipv4] [neighbors]`	BGP 設定を確認します。 **no router bgp** *autonomous-system-number* グローバル コンフィギュレーション コマンドを使用して、BGP ルーティング プロセスを削除します。ルーティング特性を削除するには、コマンドにキーワードを指定してこのコマンドを使用します。

IPv4 VRF の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip routing** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip vrf** *vrf-name* 例： `Switch(config)# ip vrf vrf-name`	VRF 名を指定し、VRF 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	**rd** *route-distinguisher* 例： `Switch(config-vrf)# rd route-distinguisher`	ルート識別子を指定して VRF テーブルを作成します。自律システム番号と任意の数値（xxx:y）、または IP アドレスと任意の数値（A.B.C.D:y）のいずれかを入力します。
ステップ 5	**route-target** {**export** | **import** | **both**} *route-target-ext-community* 例： `Switch(config-vrf)# route-target {export | import | both} route-target-ext-community`	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。 （注） このコマンドは、BGP が動作している場合にのみ有効です。
ステップ 6	**import map** ルート マップ 例： `Switch(config-vrf)# import map route-map`	（任意）VRF にルート マップを対応付けます。
ステップ 7	**interface** *interface-id* 例： `Switch(config-vrf)# interface interface-id`	インターフェイス コンフィギュレーション モードを開始して、VRF に対応付けるレイヤ 3 インターフェイスを指定します。インターフェイスにはルーテッド ポートまたは SVI を設定できます。
ステップ 8	**vrf forwarding** *vrf-name* 例： `Switch(config-if)# vrf forwarding vrf-name`	VRF をレイヤ 3 インターフェイスに対応付けます。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*] 例： `Switch# show ip vrf [brief | detail | interfaces] [vrf-name]`	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 11	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。 （注） 次のコマンドの完全な構文と使用方法については、このリリースに対応するスイッチ コマンド リファレンスおよび『Cisco IOS Switching Services Command Reference』を参照してください。 VRF を削除してすべてのインターフェイスを削除するには、**no ip vrf** *vrf-name* 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。VRF からインターフェイスを削除するには、**no vrf forwarding** インターフェイス コンフィギュレーション コマンドを使用します。

IPv6 用の VRF-Lite の設定

VRF 認識サービスの設定

IPv6 サービスは、グローバルなインターフェイス上と、グローバルなルーティング インスタンス内で設定できます。IPv6 サービスは複数のルーティング インスタンス上で稼働するように拡張されます。これが、VRF 認識です。システム内の任意の設定済み VRF であればいずれも、VRF 認識サービス用に指定できます。

VRF 認識サービスは、プラットフォームから独立したモジュールに実装されています。VRF は、Cisco IOS 内の複数のルーティング インスタンスを提供します。各プラットフォームには、サポートする VRF 数に関して独自の制限があります。

VRF 認識サービスには、次の特性があります。

- ユーザは、ユーザ指定の VRF 内のホストに ping を実行できます。

- ネイバー探索エントリは、個別の VRF で学習されます。ユーザは、特定の VRF のネイバー探索（ND）エントリを表示できます。

次のサービスは VRF 認識です。

- Ping
- ユニキャスト RPF（uRPF）
- Traceroute
- FTP および TFTP
- [Telnet および SSH（Telnet and SSH）]
- NTP

PING のユーザ インターフェイスの設定

VRF 認識 ping を設定するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**ping vrf** *vrf-name***ipv6-host** 例： `Switch# ping vrf vrf-name ipv6-host`	指定された VRF で、IPv6 ホストまたはアドレスに対して ping を実行します。

uRPF のユーザ インターフェイスの設定

VRF に割り当てられているインターフェイス上で、uRPF を設定できます。送信元の検索が VRF テーブルで実行されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id* 例： `Switch (config)# interface interface-id`	インターフェイス コンフィギュレーション モードを開始し、設定するレイヤ 3 インターフェイスを指定します。

	コマンドまたはアクション	目的
ステップ 3	**no switchport** 例： `Switch (config-if)# no switchport`	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 4	**vrf forwarding** *vrf-name* 例： `Switch (config-if)# vrf forwarding vrf-name`	インターフェイス上で VRF を設定します。
ステップ 5	**ipv6 address** *ip-address* **subnet-mask** 例： `Switch (config-if)# ip address ip-address mask`	インターフェイスの IPv6 アドレスを入力します。
ステップ 6	**ipv6 verify unicast source reachable-via rx allow-default** 例： `Switch(config-if)# ipv6 verify unicast source reachable-via rx allow-default`	インターフェイス上で uRPF をイネーブルにします。
ステップ 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

Traceroute のユーザ インターフェイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**traceroute vrf** *vrf-name ipv6address* 例： `Switch# traceroute vrf vrf-name ipv6address`	宛先アドレスを取得する VPN VRF の名前を指定します。

Telnet および SSH のユーザ インターフェイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**telnet** *ipv6-address*/**vrf** *vrf-name* 例： `Switch# telnet ipv6-address/vrf vrf-name`	指定された VRF で、IPv6 ホストまたはアドレスに Telnet 経由で接続します。
ステップ 2	**ssh -l** *username*-**vrf** *vrf-name***ipv6-host** 例： `Switch# ssh -l username -vrf vrf-name ipv6-host`	指定された VRF で、IPv6 ホストまたはアドレスに SSH 経由で接続します。

NTP のユーザ インターフェイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ntp server vrf** *vrf-name***ipv6-host** 例： `Device(config)# ntp server vrf vrf-name ipv6-host`	指定された VRF で NTP サーバを設定します。
ステップ 3	**ntp peer vrf** *vrf-name***ipv6-host** 例： `Device(config)# ntp peer vrf vrf-name ipv6-host`	指定された VRF で NTP ピアを設定します。

IPv6 VRF の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vrf definition** *vrf-name* 例： `Switch(config)# vrf definition vrf-name`	VRF名を指定し、VRF 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	**rd** *route-distinguisher* 例： `Switch(config-vrf)# rd route-distinguisher`	（任意）ルート識別子を指定して VRF テーブルを作成します。自律システム番号および任意の数（xxx:y）、または IP アドレスおよび任意の数（A.B.C.D:y）のいずれかを入力します。
ステップ 4	**address-family** *ipv4* | *ipv6* 例： `Switch(config-vrf)# address-family ipv4 | ipv6`	（任意）デフォルトは IPv4 です。IPv6 の必須設定。
ステップ 5	**route-target** {**export** | **import** | **both**} *route-target-ext-community* 例： `Switch(config-vrf)# route-target {export | import | both} route-target-ext-community`	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。 （注） このコマンドは、BGP が動作している場合にのみ有効です。
ステップ 6	**exit-address-family** 例： `Switch(config-vrf)# exit-address-family`	VRF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、VRF コンフィギュレーション モードに戻ります。
ステップ 7	**vrf definition** *vrf-name* 例： `Switch(config)# vrf definition vrf-name`	VRF 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 8	**ipv6 multicast multitopology** 例： `Switch(config-vrf-af)# ipv6 multicast multitopology`	マルチキャスト固有の RPF トポロジを有効にします。
ステップ 9	**address-family ipv6 multicast** 例： `Switch(config-vrf)# address-family ipv6 multicast`	マルチキャスト IPv6 アドレス ファミリを入力します。
ステップ 10	**end** 例： `Switch(config-vrf-af)# end`	特権 EXEC モードに戻ります。

次に、VRF を設定する例を示します。

```
Switch(config)#  vrf definition red
Switch(config-vrf)# rd 100:1
Switch(config-vrf)# address family ipv6
Switch(config-vrf-af)# route-target both 200:1
Switch(config-vrf)# exit-address-family
Switch(config-vrf)# vrf definition red
Switch(config-if)# ipv6 multicast multitopology
Switch(config-if)# address-family ipv6 multicast
Switch(config-vrf-af)# end
Switch#
```

定義済み VRF へのインターフェイスの関連付け

手順

	コマンドまたはアクション	目的
ステップ 1	**interface** *interface-id* 例： `Switch(config-vrf)# interface interface-id`	インターフェイス コンフィギュレーション モードを開始して、VRF に対応付けるレイヤ 3 インターフェイスを指定します。インターフェイスにはルーテッド ポートまたは SVI を設定できます。
ステップ 2	**no switchport** 例： `Switch(config-if)# no switchport`	コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。

	コマンドまたはアクション	目的
ステップ 3	**vrf forwarding** *vrf-name* 例： `Switch(config-if)# vrf forwarding vrf-name`	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 4	**ipv6 enable** 例： `Switch(config-if)# ipv6 enable`	インターフェイスで IPv6 をイネーブルにします。
ステップ 5	**ipv6 address** *ip-address subnet-mask* 例： `Switch(config-if)# ipv6 address ip-address subnet-mask`	インターフェイスの IPv6 アドレスを入力します。
ステップ 6	**show ipv6 vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*] 例： `Switch# show ipv6 vrf [brief | detail | interfaces] [vrf-name]`	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイスを VRF に関連付ける例を示します。

```
Switch(config-vrf)# interface ethernet0/1
Switch(config-if)# vrf forwarding red
Switch(config-if)# ipv6 enable
Switch(config-if)# ipv6 address 5000::72B/64
```

ルーティング プロトコル経由での VRF へのルートの入力

VRF スタティック ルートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ipv6 route** [**vrf** *vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | **interface-type** *interface-number* [*ipv6-address*]} 例： `Switch(config)# ipv6 route [vrf vrf-name] ipv6-prefix/prefix-length {ipv6-address | interface-type interface-number [ipv6-address]}`	VRF に固有のスタティック ルートを設定します。

```
Switch(config)# ipv6 route vrf v6a 7000::/64 TenGigabitEthernet32 4000::2
```

OSPFv3 ルータ プロセスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router ospfv3** *process-id* 例： `Switch(config)# router ospfv3 process-id`	IPv6 アドレス ファミリの OSPFv3 ルータ コンフィギュレーション モードを有効にします。
ステップ 3	**area** *area-ID* [**default-cot** | **nssa** | **stub**] 例： `Switch(config-router)# area area-ID [default-cot | nssa | stub]`	OSPFv3 エリアを設定します。
ステップ 4	**router-id** *router-id* 例： `Switch(config-router)# router-id router-id`	固定ルータ ID を使用します。
ステップ 5	**address-family ipv6 unicast vrf** *vrf-name* 例： `Switch(config-router)# address-family ipv6 unicast vrf vrf-name`	vrf vrf-name の OSPFv3 の IPv6 アドレス ファミリ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**redistribute source-protocol** [*process-id*] **options** 例： `Switch(config-router)# redistribute source-protocol [process-id] options`	あるルーティング ドメインから別のルーティング ドメインへ IPv6 ルートを再配布します。
ステップ 7	**end** 例： `Switch(config-router)# end`	特権 EXEC モードに戻ります。

次に、OSPFv3 ルータ プロセスを設定する例を示します。

```
Switch(config-router)# router ospfv3 1
Switch(config-router)# router-id 1.1.1.1
Switch(config-router)# address-family ipv6 unicast
Switch(config-router-af)# exit-address-family
```

インターフェイス上での OSPFv3 のイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type-number* 例： `Switch(config-vrf)# interface type-number`	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 3	**ospfv3** *process-id***area** *area-ID***ipv6** [**instance** *instance-id*] 例： `Switch(config-if)# ospfv3 process-id area area-ID ipv6 [instance instance-id]`	IPv6 AF を設定したインターフェイスで OSPFv3 を有効にします。
ステップ 4	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。

次に、インターフェイス上で OSPFv3 を有効にする例を示します。

```
Switch(config)# interface GigabitEthernet2/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 4000::2/64
Switch(config-if)# ipv6 enable
Switch(config-if)# ipv6 ospf 1 area 0
Switch(config-if)# end
```

EIGRPv6 ルーティング プロセスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp** *virtual-instance-name* 例： `Switch(config)# router eigrp virtual-instance-name`	EIGRP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	**address-family ipv6 vrf** *vrf-name***autonomous-system** *autonomous-system-number* 例： `Switch(config-router)# address-family ipv6 vrf vrf-name autonomous-system autonomous-system-number`	EIGRP IPv6 VRF-Lite を有効にし、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 4	**topology** {**base** | **topology-nametidnumber** 例： `Switch(config-router-af)# topology {base | topology-name tid number`	指定されたトポロジ インスタンスで IP トラフィックをルーティングするよう EIGRP プロセスを設定し、アドレス ファミリ トポロジ 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	**exit-aftopology** 例： `Switch(config-router-af-topology)# exit-aftopology`	アドレス ファミリ トポロジ コンフィギュレーション モードを終了します。
ステップ 6	**eigrp router-id** *ip-address* 例： `Switch(config-router)# eigrp router-id ip-address`	固定ルータ ID の使用を有効にします。

	コマンドまたはアクション	目的
ステップ 7	終了 例： `Switch(config-router)# end`	ルータ コンフィギュレーション モードを終了します。

次に、EIGRP ルーティング プロセスを設定する例を示します。

```
Switch(config)# router eigrp test
Switch(config-router)# address-family ipv6 unicast vrf b1 autonomous-system 10
Switch(config-router-af)# topology base
Switch(config-router-af-topology)# exit-af-topology
Switch(config-router)# eigrp router-id 2.3.4.5
Switch(config-router)# exit-address-family
```

EBGPv6 ルーティング プロセスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *as-number* 例： `Switch(config)# router bgp as-number`	指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。
ステップ 3	**neighbor** *peer-group-name peer-group* 例： `Switch(config-router)# neighbor peer-group-name peer-group`	マルチプロトコル BGP ピア グループを作成します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address*[*%*] | *peer-group-name*}**remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number* ...] 例： `Switch(config-router)# neighbor {ip-address | ipv6-address[%] | peer-group-name}remote-as autonomous-system-number [alternate-as autonomous-system-number ...]`	指定した自律システム内のネイバーの IPv6 アドレスを、ローカル ルータの IPv6 マルチプロトコル BGP ネイバーテーブルに追加します。

	コマンドまたはアクション	目的
ステップ 5	**address-family ipv6** [**vrf** *vrf-name*] [**unicast** | **multicast** | **vpnv6**] 例： `Switch(config-router)# address-family ipv6 [vrf vrf-name] [unicast | multicast | vpnv6]`	IPv6 アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。 • unicast キーワードは、IPv6 ユニキャスト アドレス ファミリを指定します。デフォルトでは、address-family ipv6 コマンドでユニキャスト キーワードが指定されていない場合、スイッチは IPv6 ユニキャスト アドレス ファミリのコンフィギュレーション モードになります。 • multicast キーワードは、IPv6 マルチキャスト アドレス プレフィックスを指定します。
ステップ 6	**neighbor** *ipv6-address***peer-group** *peer-group-name* 例： `Switch(config-router-af)# neighbor ipv6-address peer-group peer-group-name`	BGP ネイバーの IPv6 アドレスをピア グループに割り当てます。
ステップ 7	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*[*%*]}**route-map** *map-name* {**in** | **out**} 例： `Switch(config-router-af)# neighbor {ip-address | peer-group-name | ipv6-address[%]}route-map map-name {in | out}`	着信ルートまたは発信ルートにルート マップを適用します。ルート マップへの変更は、ピアリングがリセットされるまで、またはソフト リセットが実行されるまで、現在のピアでは有効になりません。soft キーワードと in キーワードを指定して clear bgp ipv6 コマンドを使用すると、ソフト リセットが実行されます。
ステップ 8	[終了(exit)] 例： `Switch(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、ルータをルータ コンフィギュレーション モードに戻します。

次に、EBRPv6 を設定する例を示します。

```
Switch(config)# router bgp 2
Switch(config-router)# bgp router-id 2.2.2.2
Switch(config-router)# bgp log-neighbor-changes
Switch(config-router)# no bgp default ipv4-unicast
Switch(config-router)# neighbor 2500::1 remote-as 1
Switch(config-router)# neighbor 4000::2 remote-as 3
Switch(config-router)# address-family ipv6 vrf b1
Switch(config-router-af)# network 2500::/64
Switch(config-router-af)# network 4000::/64
Switch(config-router-af)# neighbor 2500::1 remote-as 1
Switch(config-router-af)# neighbor 2500::1 activate
```

```
Switch(config-router-af)# neighbor 4000::2 remote-as 3
Switch(config-router-af)# neighbor 4000::2 activate
Switch(config-router-af)# exit-address-family
```

VRF-Lite に関する追加情報

IPv4 と IPv6 間での VPN の共存

IPv4 を設定するための「以前の」CLI と、IPv6 用の「新しい」CLI 間には下位互換性があります。つまり、設定に両方の CLI を含めることができます。IPv4 CLI は、同じインターフェイス上で、VRF 内で定義されている IP アドレスとともにグローバル ルーティング テーブルで定義されている IPv6 アドレスも備える機能を保持しています。

次に例を示します。

```
vrf definition red
 rd 100:1
 address family ipv6
 route-target both 200:1
 exit-address-family
!
ip vrf blue
 rd 200:1
 route-target both 200:1
!
interface Ethernet0/0
 vrf forwarding red
 ip address 50.1.1.2 255.255.255.0
 ipv6 address 4000::72B/64
!
interface Ethernet0/1
 vrf forwarding blue
 ip address 60.1.1.2 255.255.255.0
 ipv6 address 5000::72B/64
```

この例では、Ethernet0/0 用に定義されたすべてのアドレス（v4 と v6）が VRF red を参照します。Ethernet0/1 については、IP アドレスは VRF blue を参照しますが、ipv6 アドレスはグローバル IPv6 アドレス ルーティング テーブルを参照します。

VRF-Lite 設定の確認

IPv4 VRF-Lite ステータスの表示

VRF-Liteの設定およびステータスに関する情報を表示するには、次の作業のいずれかを行います。

コマンド（Command）	目的
`Switch#` **show ip protocols vrf** *vrf-name*	VRF に対応付けられたルーティング プロトコル情報を表示します。
`Switch#` **show ip route vrf** *vrf-name* [**connected**] [*protocol* [*as-number*]] [**list**] [**mobile**] [**odr**] [**profile**] [**static**] [**summary**] [**supernets-only**]	VRF に対応付けられた IP ルーティング テーブル情報を表示します。
`Switch#` **show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*]	定義された VRF インスタンスに関する情報を表示します。
`Switch#` **bidir vrf** *instance-name a.b.c.d* | **active** | **bidriectional**| **count** | **dense**| **interface** | **proxy** | **pruned** | **sparse** | **ssm** | **static** | **summary**	定義された VRF インスタンスに関する情報を表示します。

次に、VRF インスタンス内のマルチキャスト ルート テーブル情報を表示する例を示します。

```
Switch# show ip mroute 226.0.0.2
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
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 226.0.0.2), 00:01:17/stopped, RP 1.11.1.1, flags: SJCF
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan100, Forward/Sparse-Dense, 00:01:17/00:02:36

(5.0.0.11, 226.0.0.2), 00:01:17/00:01:42, flags: FT
  Incoming interface: Vlan5, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan100, Forward/Sparse-Dense, 00:01:17/00:02:36
```

IPv6 VRF-Lite ステータスの表示

VRF-Liteの設定およびステータスに関する情報を表示するには、次の作業のいずれかを行います。

コマンド（Command）	目的
Switch# **show ipv6 mroute vrf** *instance-name* [*X:X:X:X::X/<0-128>*] [**bgp**] [**connected**] [**eigrp**] [**interface**] [**isis**] [**local**] [**nd**] [**nsf**] [**ospf**] [**repair**] [**rip**] [**shortcut**] [**static**] [**summary**] [**tag**] [**updated**] [**watch**]	VRF に対応付けられたルーティング プロトコル情報を表示します。
Switch# **show ipv6 mfib vrf** *instance-name a.b.c.d* | **active** | **all** | **count** | **linkscope**| **route** | **summary** | **update-sets** | **verbose**	定義された VRF インスタンスに関する情報を表示します。

次に、VRF インスタンス内のマルチキャスト ルート テーブル情報を表示する例を示します。

show ipv6 mroute vrf *vrf1 FF05:ABCD:0:0:0:0:0:1*

```
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
C - Connected, L - Local, I - Received Source Specific Host Report,
P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
J - Join SPT, Y - Joined MDT-data group,
y - Sending to MDT-data group

g - BGP signal originated, G - BGP Signal received,
N - BGP Shared-Tree Prune received, n - BGP C-Mroute suppressed,
q - BGP Src-Active originated, Q - BGP Src-Active received
E - Extranet
Timers: Uptime/Expires
Interface state: Interface, State

(*, FF05:ABCD::1), 00:06:22/never, RP 1010:ABCD::10, flags: SCJ
Incoming interface: Port-channel33
RPF nbr: FE80::2E31:24FF:FE06:134A
Immediate Outgoing interface list:
TenGigabitEthernet4/0/18, Forward, 00:06:22/never

(3232:ABCD::2, FF05:ABCD::1), 00:04:54/00:02:16, flags: SJT
Incoming interface: Port-channel33
RPF nbr: FE80::2E31:24FF:FE06:134A
Inherited Outgoing interface list:
TenGigabitEthernet4/0/18, Forward, 00:06:22/never
```

次に、**show ipv6 mfib** コマンドの出力例を示します。

Switch# **show ipv6 mfib vrf** *vrf1 FF05:ABCD:0:0:0:0:0:1*

```
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
                ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
                MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
                MS  - MoFRR  Entry in Sync, MC - MoFRR entry in MoFRR Client.
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, A2 - Accept backup,
                RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

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 testvrf1
```

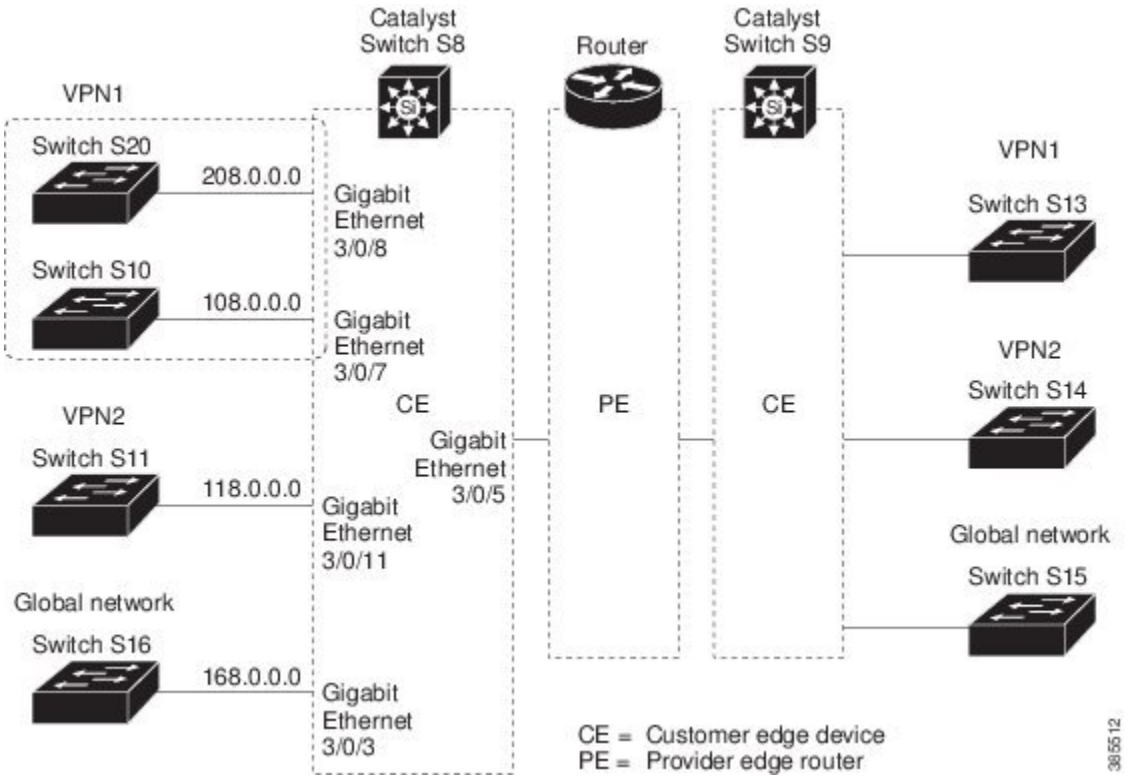
```
 (*,FF05:ABCD::1) Flags: C HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   295/0/512/0, Other: 0/0/0
   Port-channel33 Flags: A NS
   TenGigabitEthernet4/0/18 Flags: F NS
     Pkts: 0/0
 (3232:ABCD::2,FF05:ABCD::1) Flags: HW
   SW Forwarding: 50/0/512/0, Other: 111/0/111
   HW Forwarding:   4387686/14849/512/59398, Other: 0/0/0
   Port-channel33 Flags: A
   TenGigabitEthernet4/0/18 Flags: F NS
     Pkts: 0/50

Switch#
```

VRF-Lite の設定例

IPv4 VRF-Lite の設定例

VPN1、VPN2、およびグローバル ネットワークで使用されるプロトコルは OSPF です。CE/PE 接続には BGP が使用されます。次の例のコマンドは、CE スイッチ S8 を設定する方法を示し、スイッチ S20 および S11 の VRF 設定、およびスイッチ S8 のトラフィックに関連する PE ルータ コマンドが含まれます。その他のスイッチの設定のコマンドは含まれていませんが、類似したものになります。

図 *8*：*VRF-Lite* の設定例



スイッチ S8 の設定

スイッチ S8 上のルーティングをイネーブルにし、VRF を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# ip vrf v11
Switch(config-vrf)# rd 800:1
Switch(config-vrf)# route-target export 800:1
Switch(config-vrf)# route-target import 800:1
Switch(config-vrf)# exit
Switch(config)# ip vrf v12
Switch(config-vrf)# rd 800:2
Switch(config-vrf)# route-target export 800:2
Switch(config-vrf)# route-target import 800:2
Switch(config-vrf)# exit
```

スイッチ S8 上でループバックおよび物理インターフェイスを設定します。ファスト イーサネット インターフェイス 3/5 は、PE へのトランク接続です。インターフェイス 3/7 および 3/11 は、VPN に接続します。

```
Switch(config)# interface loopback1
Switch(config-if)# vrf forwarding v11
Switch(config-if)# ip address 8.8.1.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface loopback2
Switch(config-if)# vrf forwarding v12
Switch(config-if)# ip address 8.8.2.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface FastEthernet3/5
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface FastEthernet3/8
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface FastEthernet3/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit
```

スイッチ S8 上で使用される VLAN を設定します。VLAN 10 は、CE と PE 間の VRF 11 によって使用されます。VLAN 20 は、CE と PE 間の VRF 12 によって使用されます。VLAN 118 および 208 は、それぞれスイッチ S11 およびスイッチ S20 を含む VPN の VRF に使用されます。

```
Switch(config)# interface Vlan10
Switch(config-if)# vrf forwarding v11
Switch(config-if)# ip address 38.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface Vlan20
Switch(config-if)# vrf forwarding v12
Switch(config-if)# ip address 83.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface Vlan118
Switch(config-if)# vrf forwarding v12
Switch(config-if)# ip address 118.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface Vlan208
Switch(config-if)# vrf forwarding v11
Switch(config-if)# ip address 208.0.0.8 255.255.255.0
Switch(config-if)# exit
```

VPN1 および VPN2 に OSPF ルーティングを設定します。

```
Switch(config)# router ospf 1 vrf vl1
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
Switch(config)# router ospf 2 vrf vl2
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
```

CE から PE のルーティングに BGP を設定します。

```
Switch(config)# router bgp 800
Switch(config-router)# address-family ipv4 vrf vl2
Switch(config-router-af)# redistribute ospf 2 match internal
Switch(config-router-af)# neighbor 83.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 83.0.0.3 activate
Switch(config-router-af)# network 8.8.2.0 mask 255.255.255.0
Switch(config-router-af)# exit

Switch(config-router)# address-family ipv4 vrf vl1
Switch(config-router-af)# redistribute ospf 1 match internal
Switch(config-router-af)# neighbor 38.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 38.0.0.3 activate
Switch(config-router-af)# network 8.8.1.0 mask 255.255.255.0
Switch(config-router-af)# end
```

スイッチ S20 の設定

CE に接続するように S20 を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface Fast Ethernet 0/7
Switch(config-if)# no switchport
Switch(config-if)# ip address 208.0.0.20 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

スイッチ S11 の設定

CE に接続するように S11 を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface Gigabit Ethernet 0/3
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface Vlan118
Switch(config-if)# ip address 118.0.0.11 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

PE スイッチ S3 の設定

スイッチ S3（ルータ）上では、次のコマンドはスイッチ S8 への接続だけを設定します。

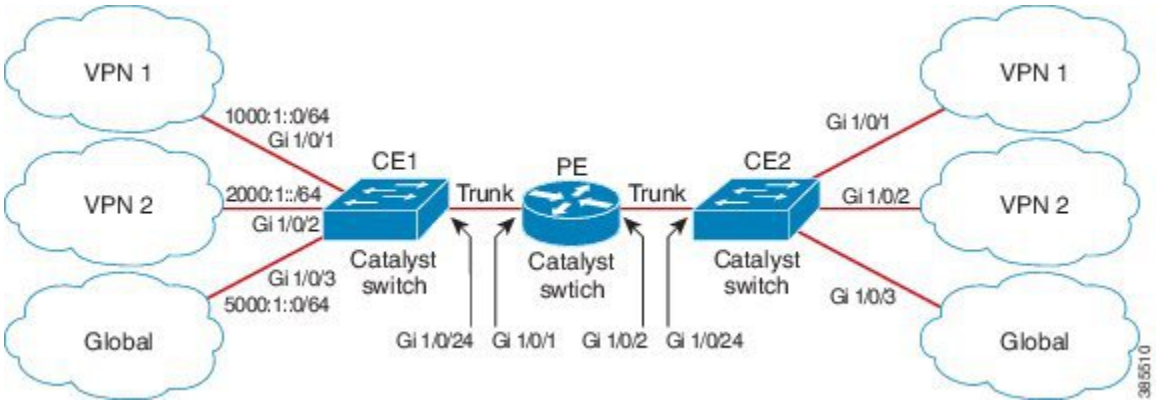
```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip vrf v1
```

```
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit

Router(config)# ip vrf v2
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit

Router(config)# ip cef
Router(config)# interface Loopback1
Router(config-if)# vrf forwarding v1
Router(config-if)# ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Loopback2
Router(config-if)# vrf forwarding v2
Router(config-if)# ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Fast Ethernet3/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# vrf forwarding v1
Router(config-if)# ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Fast Ethernet3/0.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf v2
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
Router(config-router)# address-family ipv4 vrf vl
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.1.0 mask 255.255.255.0
Router(config-router-af)# end
```

IPv6 VRF-Lite の設定例

次に、CE-PE ルーティングに OSPFv3 を使用するトポロジを示します。

図 *9*：*VRF-Lite* の設定例



CE1 スイッチの設定

```
ipv6 unicast-routing
vrf definition v1
 rd 100:1
 !
address-family ipv6
 exit-address-family
!

vrf definition v2
 rd 200:1
 !
address-family ipv6
 exit-address-family
!

interface Vlan100
 vrf forwarding v1
 ipv6 address 1000:1::1/64
 ospfv3 100 ipv6 area 0
!

interface Vlan200
 vrf forwarding v2
 ipv6 address 2000:1::1/64
 ospfv3 200 ipv6 area 0
!

interface GigabitEthernet 1/0/1
switchport access vlan 100
end

interface GigabitEthernet 1/0/2
switchport access vlan 200
end

interface GigabitEthernet 1/0/24
 switchport trunk encapsulation dot1q

switchport mode trunk
end
```

```
router ospfv3 100
 router-id 10.10.10.10
 !
 address-family ipv6 unicast vrf v1
  redistribute connected
  area 0 normal
 exit-address-family
!

router ospfv3 200
 router-id 20.20.20.20
 !
 address-family ipv6 unicast vrf v2
  redistribute connected
  area 0 normal
 exit-address-family
!
```

PE スイッチの設定

```
ipv6 unicast-routing

vrf definition v1
 rd 100:1
 !
address-family ipv6
 exit-address-family
!

vrf definition v2
 rd 200:1
 !
address-family ipv6
 exit-address-family
!
interface Vlan600
 vrf forwarding v1
 no ipv6 address
 ipv6 address 1000:1::2/64
 ospfv3 100 ipv6 area 0
!

interface Vlan700
 vrf forwarding v2
 no ipv6 address
 ipv6 address 2000:1::2/64
 ospfv3 200 ipv6 area 0
!

interface Vlan800
 vrf forwarding v1
 ipv6 address 3000:1::7/64
 ospfv3 100 ipv6 area 0
!
interface Vlan900
 vrf forwarding v2
 ipv6 address 4000:1::7/64
 ospfv3 200 ipv6 area 0
!

interface GigabitEthernet 1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 exit

interface GigabitEthernet 1/0/2
 switchport trunk encapsulation dot1q

switchport mode trunk
 exit
```

```
router ospfv3 100
 router-id 30.30.30.30
 !
 address-family ipv6 unicast vrf v1
  redistribute connected
  area 0 normal
 exit-address-family
 !
address-family ipv6 unicast vrf v2
  redistribute connected
  area 0 normal
 exit-address-family
 !
```

CE2 スイッチの設定

```
ipv6 unicast-routing

vrf definition v1
 rd 100:1
 !
address-family ipv6
 exit-address-family
!

vrf definition v2
 rd 200:1
 !
address-family ipv6
 exit-address-family
!

interface Vlan100
 vrf forwarding v1

ipv6 address 1000:1::3/64
 ospfv3 100 ipv6 area 0
!

interface Vlan200
 vrf forwarding v2
 ipv6 address 2000:1::3/64
 ospfv3 200 ipv6 area 0
!

interface GigabitEthernet 1/0/1
switchport access vlan 100
end

interface GigabitEthernet 1/0/2
switchport access vlan 200
end

interface GigabitEthernet 1/0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
 end

router ospfv3 100
 router-id 40.40.40.40
 !
 address-family ipv6 unicast vrf v1
  redistribute connected
  area 0 normal
 exit-address-family
!

router ospfv3 200
 router-id 50.50.50.50
 !
 address-family ipv6 unicast vrf v2
  redistribute connected
```

```
area 0 normal
 exit-address-family
!
```

マルチキャスト VRF-Lite の機能履歴と情報

機能名（Feature Name）	リリース	機能情報
VRF-Lite を使用した IPv6 マルチキャストのサポート		IPv6 VRF-Lite によって、サービスプロバイダーは 1 つのインターフェイスを使用して、重複する IP アドレスを持つ複数の VPN をサポートできます。 この機能が導入されました。

第 5 章

IGMP の設定

IGMP および IGMP スヌーピングの前提条件

IGMP のの前提条件

- このモジュールの作業を実行する前に、『IP Multicast Routing Technology Overview』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。
- このモジュールの作業では、IP マルチキャストがイネーブルに設定され、「Configuring Multicast Routing」モジュールで説明されている作業を使用して、Protocol Independent Multicast（PIM）インターフェイスが設定されていることを前提とします。

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 デバイス仮想インターフェイス（SVI）IP アドレス（存在する場合）の使用を試みます。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 一般クエリーを生成しません。
- 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、および 3 をサポートします。

（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 デバイスが正しく認識し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。

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。

- 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 クエリーに 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、クエリーに 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おり、クエリーのバージョンが 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）機能を実行しているデバイスとメッセージの送受信を行うことができます。

IGMP バージョン 1

IGMP バージョン 1（IGMPv1）にはクエリー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。

IGMP バージョン 2

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）機能を実行しているデバイスとメッセージの送受信を行うことができます。

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 *7*：*IGMP* のバージョン

IGMP Version	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。

（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。

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 デバイスは 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。特定のマルチキャスト グループについて、デバイスがホストから IGMP レポートを受信すると、その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。

マルチキャスト ルータは、すべての VLAN に一般的なクエリーを定期的に送信します。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。

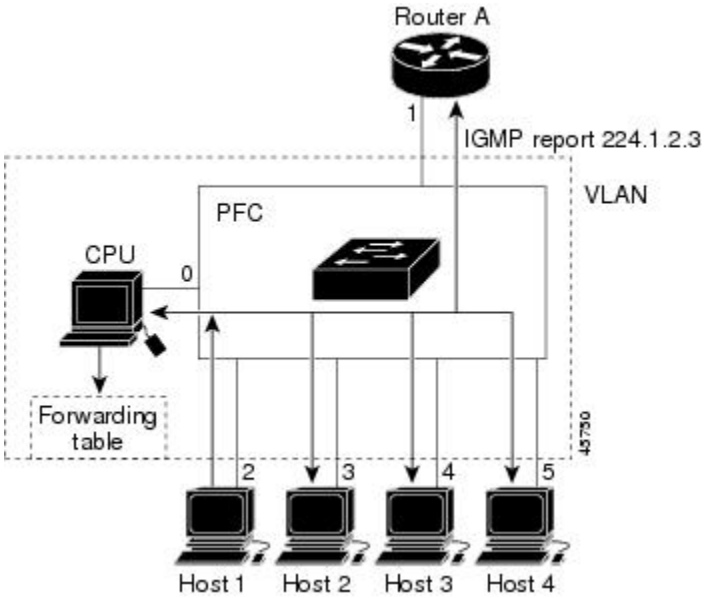
ここでは、IGMP スヌーピングの特性について説明します。

マルチキャスト グループへの加入

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ーを受信したデバイスは、そのクエリーを 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。

図 *10*：最初の *IGMP Join* メッセージ



ルータ A がデバイスに一般クエリーを送信し、スイッチがそのクエリーを同じ VLAN のすべてのメンバであるポート 2 ～ 5 に転送します。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 *8*：*IGMP* スヌーピング転送テーブル

[宛先アドレス（Destination Address）]	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。

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へ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。

図 *11*：*2*番目のホストのマルチキャスト グループへの加入

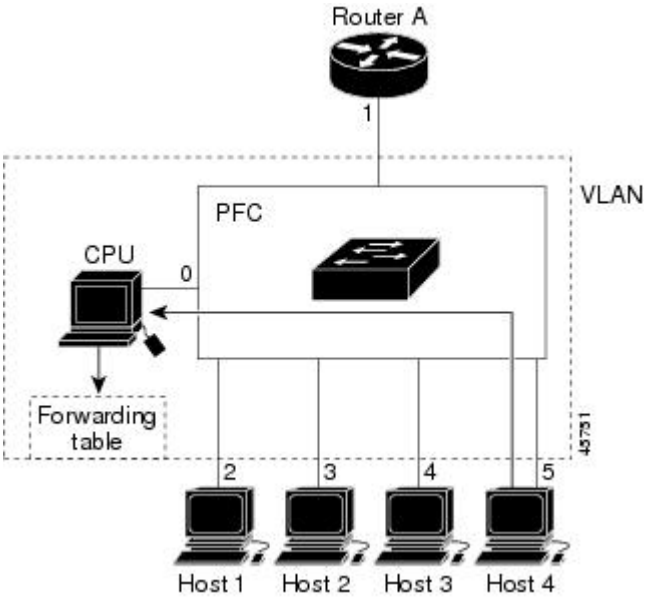


表 *9*：更新された *IGMP* スヌーピング転送テーブル

[宛先アドレス（Destination Address）]	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

ルータは定期的にマルチキャスト一般クエリーを送信し、デバイスはそれらのクエリーをVLAN内のすべてのポート経由で転送します。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ーを送信して、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ーを送信しなくても、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 設定可能脱退タイマー

特定のマルチキャスト グループへの参加がまだ必要かどうかを確認するために、グループ固有のクエリー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

（注） IGMP レポート抑制は、マルチキャスト クエリーに 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、クエリーに 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、1 つのマルチキャスト 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だけ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 レポートだけを、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。

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、スタック内の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に障害が発生した、または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。スタック内のその他のデバイス上のマルチキャスト グループの他のすべてのメンバでは、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、収束するために、より長い時間を要する場合があります。

IGMP フィルタリングおよびスロットリング

都市部や集合住宅（MDU）などの環境では、デバイス 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、デバイス 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、それらを各デバイス 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 プロファイルがデバイス 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 のデフォルト設定を示します。

表 *10*：*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許可
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 2
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 *11* : *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 単位でイネーブル
マルチキャスト ルータ	未設定
IGMP スヌーピング即時脱退	無効
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	無効
IGMP スヌーピング クエリア	無効
IGMP レポート抑制	[有効（Enabled）]

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 *12* : *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が最大数に達していると、デフォルトのIGMPスロットリング アクションは 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のデバイスの設定

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。管理している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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。また、インターフェイスの IP PIM スパース - デン

	コマンドまたはアクション	目的
		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 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 グループに参加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)# 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`	（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
	`startup-config`	

IP マルチキャスト グループへのアクセスの制御

デバイス は IGMP ホストクエリ メッセージを送信し、接続されたローカル ネットワーク上のメンバーが属しているマルチキャスト グループを判別します。次に、デバイスは、マルチキャスト グループにアドレス指定されたすべてのパケットをこれらのグループ メンバーに転送します。インターフェイスごとにフィルタを適用し、インターフェイスで処理されるサブネット上のホストが加入可能なマルチキャスト グループを制限できます。

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。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**ip igmp profile**
	例：
	`Device(config)# ip igmp profile 10`
	`Device(config-igmp-profile)# ?`
		1 ～ 4294967295 の範囲で、IGMP フィルタ プロファイル番号を入力します。
		IGMP フィルタ プロファイルの設定の詳細については、IGMP プロファイルの設定，（114 ページ）を参照してください。

ステップ 4	**permit** 例： `Device(config-igmp-profile)#`	IGMP プロファイル設定操作を開始します。次の IGMP プロファイル設定操作がサポートされています。 • **deny**：一致する IP アドレスが拒否されます。

	コマンドまたはアクション	目的
	`permit 229.9.9.0`	• **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**：コマンドを無効にするか、そのデフォルトに設定します。 • **permit**：一致するアドレスが許可されます。 • **range**：設定に範囲を追加します。
ステップ 5	**exit** 例： `Device(config-igmp-profile)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**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 7	**ip igmp filter** *filter_number* 例： `Device(config-if)# ip igmp filter 10`	IGMP フィルタ プロファイル番号を指定します。 IGMP フィルタ プロファイルの適用の詳細については、IGMP プロファイルの適用，（117 ページ）を参照してください。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 10	**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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。

	コマンドまたはアクション	目的
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** または **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。 デフォルトの設定に戻すには、 **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)# 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 ホストクエリー 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ー 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。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。

	コマンドまたはアクション	目的
		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** 秒 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。
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`	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。

IGMPv2 の IGMP クエリー タイムアウトの変更

IGMPv2 を使用している場合、デバイスがインターフェイスのクエリアとして引き継ぐまでの時間を指定できます。デフォルトでは、デバイスは **ip igmp query-interval** インターフェイス コンフィギュレーション コマンドによって制御されるクエリー インターバルの 2 倍の時間だけ待機します。この時間を経過しても、デバイスがクエリーを受信しない場合は、スイッチがクエリアになります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。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 igmp querier-timeout** 秒	IGMP クエリー タイムアウトを指定します。

	コマンドまたはアクション	目的
	例： `Device(config-if)# ip igmp querier-timeout 120`	デフォルトは 60 秒です（クエリー インターバルの 2 倍）。指定できる範囲は 60 ～ 300 です。
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 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。

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ー応答時間を使用し、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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。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。

	コマンドまたはアクション	目的
ステップ 4	**ip igmp query-max-response-time** 秒 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)# 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のデバイスの設定

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と、デバイス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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。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。

	コマンドまたはアクション	目的
		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、この機能は無効になっています。
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 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。 デフォルトでは、デバイスには IGMP プロファイルが設定されていません。 （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。

	コマンドまたはアクション	目的
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すると、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)# 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： `Device# copy running-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	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。
ステップ 4	**ip igmp filter** *profile number* 例： `Device(config-if)# ip igmp`	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。

	コマンドまたはアクション	目的
	`filter 321`	
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。

はじめる前に

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

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	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。

	コマンドまたはアクション	目的
		• **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)# 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 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。
	• **ipigmpjoin-group** *group-address*
	• **ipigmpstatic-group** {***** | *group-address* [**source** *source-address*]}
	
	例：
	`Device(config-if)# ip igmp join-group 225.2.2.2`
	
	例：
	`Device(config-if)# ip igmp static-group 225.2.2.2`
		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

	コマンドまたはアクション	目的
		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	**showipigmpinterface** [*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。
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。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmulticast-routing** [**distributed**] 例： `Device(config)# ip multicast-routing distributed`	IP マルチキャスト ルーティングをイネーブルにします。 • **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	**ippimssm** {**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	**ipaccess-listextended** *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	**denyigmp** *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。（特に許可されないソースまたはグループは拒否されるため、これらのソースは後続の **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	**permitigmp** *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ソース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	**ipigmpaccess-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。

	コマンドまたはアクション	目的
ステップ 11	**ippimsparse-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。
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	**ipigmpversion3** 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

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

	コマンドまたはアクション	目的
ステップ 2	**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** 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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、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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**ip igmp snooping vlan** *vlan-id* **mrouterinterface** {**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`	（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
	startup-config	

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権EXECモードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping vlan** *vlan-id***mrouter interface** *interface-id* 例： `Device(config)# ip igmp snooping vlan 5 mrouter interface gigabitethernet1/0/1`	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)# 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
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)# 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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： `Device# show ip igmp snooping vlan 21`	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
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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権EXECモードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping last-member-query-interval** 時刻 例： `Device(config)# ip igmp snooping last-member-query-interval 1000`	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。 （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`	（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。

	コマンドまたはアクション	目的
	snooping vlan 210 last-member-query-interval 1000	（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)# 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

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

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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)# 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 堅牢性変数カウントを表示します。
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 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。
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)# 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。

	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。

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping tcn flood query count** *count* 例： `Device(config)# ip igmp`	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。

	コマンドまたはアクション	目的
	snooping tcn flood query count 3	（注） デフォルトのフラッディングクエリー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)# 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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ー送信要求に戻すには、 **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。
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、一般クエリーを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しているポートが複数ある場合、リンク範囲を超えてデバイスに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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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)# 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 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。

	コマンドまたはアクション	目的
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 クエリアはデバイス上で IP アドレスを検出できない場合、IGMP 一般クエリーを生成しません。
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。範囲は 1 ～ 18000 秒です。
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** タイムアウト 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。範囲は 60 ～ 300 秒です。
ステップ 8	**ip igmp snooping querier version** バージョン 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)# 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 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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 クエリーごとに IGMP レポートを 1 つだけ転送します。

	コマンドまたはアクション	目的
		（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)# 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： `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 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 *13*：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（Command）	目的
show ip igmp groups [*type-number* | *detail*]	デバイスに直接接続され、IGMP によって取得されたマルチキャスト グループを表示します。
show ip igmp interface [*type number*]	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。
show ip igmp profile [*profile_number*]	IGMP プロファイル情報を表示します。
show ip igmp ssm-mapping [*hostname/IP address*]	IGMP SSM マッピング情報を表示します。
show ip igmp static-group {**class-map** [**interface** [*type*]]	スタティック グループ情報を表示します。
show ip igmp vrf	選択した VPN ルーティング/転送インスタンスを名前別に表示します。

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 *14*：*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（Command）	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** | [**vlan** *vlan-id* [*A.B.C.D* | **count**]]	デバイスまたは特定のパラメータに関して、マルチキャスト テーブル情報を表示します。 • **count**：グループの合計数を表示します。 • **vlan**：VLAN ID によるグループ情報を表示します。

コマンド（Command）	目的
show ip igmp 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。 （注） IGMP スヌーピングを有効にすると、デバイスはマルチキャスト ルータの接続先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。
show ip igmp snooping querier [**detail** | **vlan** *vlan-id*]	IP アドレス、および VLAN で受信した最新の IGMP クエリ メッセージの受信ポートに関する情報を表示します。 （任意）VLAN の詳細な IGMP クエリア情報を表示するには、**detail** を入力します。 （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。
show ip igmp snooping [**vlan** *vlan-id* [**detail**]]	デバイス上のすべての VLAN または特定の VLAN の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。

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 *15* : *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（**Command**）	目的
show ip igmp profile [*profile number*]	特定の IGMP プロファイルまたはデバイス上で定義されているすべての IGMP プロファイルを表示します。
show running-config [**interface** *interface-id*]	インターフェイスが所属できる IGMP グループの最大数（設定されている場合）や、インターフェイスに適用される IGMP プロファイルを含む、特定のインターフェイスまたはデバイス上のすべてのインターフェイ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のデバイスの設定

次に、マルチキャスト グループ 255.2.2.2 へのデバイスの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)#
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** コマンドを実行する必要がある複数の IP マルチキャスト ルーティングの設定手順の場合に、この設定をインターフェイスで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 20.20.20.1 255.255.255.0
Device(config-if)# ip pim sparse-dense-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 20.20.20.1 255.255.255.0
 ip pim sparse-dense-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** コマンドを実行する必要がある複数の IP マルチキャスト ルーティングの設定手順の場合に、この設定をインターフェイスで行う必要があります。

```
Device(config)# interface vlan 150
```

```
Device(config-if)# ip address 20.20.20.1 255.255.255.0
Device(config-if)# ip pim sparse-dense-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 Vlan150
 ip address 20.20.20.1 255.255.255.0
 ip pim sparse-dense-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

次に、**ipigmpjoin-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、グループ 225.2.2.2 に加入するように、デバイスでファスト イーサネット インターフェイス 0/0/0 が設定されています。

```
interface FastEthernet0/0/0
 ip igmp join-group 225.2.2.2
```

次に、 **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 FastEthernet0/1/0
 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 FastEthernet0/0/0
 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 GigabitEthernet1/1/0
 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 GigabitEthernet1/2/0
 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	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

標準および RFC

標準/RFC	役職（Title）
RFC 1112	『Host Extensions for IP Multicasting』
RFC 2236	『Internet Group Management Protocol, Version 2』
RFC 3376	『*Internet Group Management Protocol, Version 3*』

MIB

MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IGMP の機能情報

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

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

表 *16* : *IGMP* の機能情報

機能名（Feature Name）	リリース	機能情報
IGMP	Cisco IOS XE Everest 16.5.1a	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。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

第 6 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。

（注） IGMP プロキシの PIM インターフェイスを設定する際は、次のガイドラインに従ってください。

- インターフェイスがスパース モード領域で実行中で、スタティック RP、ブートストラップ（BSR）、または自動 RP リスナー機能ありで自動 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。
- インターフェイスがスパース-デンス モード領域で実行中で、自動 RP リスナー機能なしで自動 RP を実行している場合は、PIM スパース-デンス モードを使用します。
- インターフェイスがデンス モードで実行されているときに、デンス モード領域に加入する場合は、PIM デンス モード（PIM-DM）を使用します。
- インターフェイスが、スパース モード領域のレシーバに到達する必要があるトラフィックをデンス モード領域から受信する場合は、プロキシ登録機能ありの PIM-DM を使用します。

IGMP プロキシの情報

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。

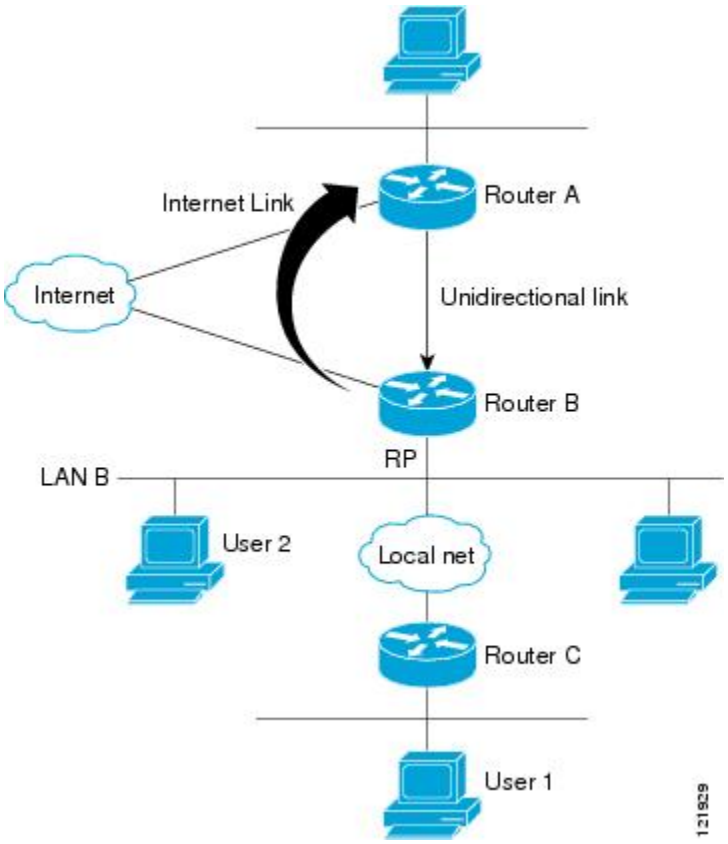
次の図に、2 つの UDLR シナリオを示すトポロジ例を図示します。

- 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。

（注） 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（ルータやコントローラ）を使用できます。

（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。



シナリオ 1：**従来型の UDLR のシナリオ（直接接続されたレシーバがある 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 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（直接接続されたレシーバのない 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 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) 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て（**ipigmpmroute-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、（**ipigmpproxy-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ー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。

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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	**ipigmpunidirectional-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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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	**ipigmpunidirectional-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	**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 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	**ipigmpmroute-proxy** *type number* 例： `Device(config-if)# ip`	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

	コマンドまたはアクション	目的
	`igmp mroute-proxy loopback 0`	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 **ipigmpmroute-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 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 9	**interface** *type number* 例： `Device(config)# interface loopback 0`	指定したインターフェイスのインターフェイス 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	**ipigmphelper-addressudl** *interface-type interface-number* 例： `Device(config-if)# ip igmp helper-address udl gigabitethernet 0/0/0`	UDLR で IGMP ヘルパーを設定します。 • 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	**ipigmpproxy-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 **ipigmpmroute-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

	コマンドまたはアクション	目的
		送エントリのスタティック 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） **ipigmpproxy-service** コマンドは、**ipigmphelper-address**（UDL）コマンドと共に使用するように意図されています。 • この例では、**ipigmpmroute-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 **ipigmpproxy-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： `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 13	**showipigmpinterface** 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	**showipigmpudlr** 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。

IGMP プロキシの設定例

例：IGMP プロキシ設定

次に、IGMP UDLR に対してアップストリーム UDL デバイスを設定し、IGMP プロキシ サポート付きの IGMP UDLR に対してダウンストリーム UDL デバイスを設定する例を示します。

アップストリーム デバイスの設定

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

ダウンストリーム デバイスの設定

```
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 dense-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 dense-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
```

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	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト テクノロジー分野の概要	「IPマルチキャストルーティングテクノロジーの概要」モジュール
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

標準および RFC

標準/RFC	役職（Title）
RFC 1112	『*Host extensions for IP multicasting*』
RFC 2236	『*Internet Group Management Protocol, Version 2*』
RFC 3376	『*Internet Group Management Protocol, Version 3*』

MIB

MIB	MIB 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 Release、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

テクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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

IGMP プロキシの機能情報

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

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

表 *17* : *IGMP* プロキシの機能情報

機能名（Feature Name）	リリース	機能情報
IGMP プロキシ	Cisco IOS XE Everest 16.5.1a	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。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

第 7 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
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。
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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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

ステップ 1 **enable**

例：
```
Device> enable
```
特権 EXEC モードをイネーブルにします。

- プロンプトが表示されたら、パスワードを入力します。

ステップ 2 **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 リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *18* : *IGMP* の明示的トラッキングの機能情報

機能名（Feature Name）	リリース	機能情報
IGMP の明示的なトラッキング	Cisco IOS XE Everest 16.6.1	このモジュールでは、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。 Cisco IOS XE Everest 16.6.1 では、この機能は次のプラットフォームに実装されていました。

第 8 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 Multicast Technology Overview」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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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	**ipcgmp** [**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。

	コマンドまたはアクション	目的
ステップ 6	**clearipcgmp** [*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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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	**iprgmp** 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。

	コマンドまたはアクション	目的
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	**debugiprgmp** 例： `Device# debug ip rgmp`	（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。
ステップ 7	**showipigmpinterface** 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

例：CGMP の設定

次の例は、マルチキャスト ソースとマルチキャスト レシーバが同じ VLAN にある基本的なネットワーク環境向けです。目的とする動作は、スイッチ上でのマルチキャストの転送を、そのマルチキャスト ストリームを要求しているポート宛てに限定することです。

4908G-L3 ルータは、VLAN 50 のポート 3/1 で Catalyst 4003 に接続されます。次の設定は、GigabitEthernet1 インターフェイスに適用されます。ルータがインターフェイスでマルチキャストトラフィックをルーティングしないため、**ipmulticast-routing** コマンドが設定されないことに注意してください。

```
interface GigabitEthernet1
 ip address 192.168.50.11 255.255.255.0
 ip pim dense-mode
 ip cgmp
```

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	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

MIB

MIB	MIB 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 Release、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

テクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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情報

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

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

表 *19* : 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情報

機能名（Feature Name）	リリース	機能情報
スイッチド イーサネットでの IP マルチキャストの抑制	Cisco IOS XE Everest 16.5.1a	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。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

第 9 章

PIM（ProtocolIndependentMulticast）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。さらに、スタブ ルータのアップリンク インターフェイスに PIM モード（デンス モード、スパース モード、または スパース - デンス モード）が設定されている必要があります。

- また、デバイスに Enhanced Interior Gateway Routing Protocol（EIGRP）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。

- 双方向 PIM はサポートされていません。

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 デバイスに設定できます。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 デバイスで同じ 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 デバイス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 デバイス上の 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 デバイスごとに 1 つの RP が設定されます。ドメイン内のルータおよびデバイスの中には、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 と PIMv2 が混在する領域内の DM グループは、特殊な設定を行わなくても自動的に相互運用します。

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。
- 領域全体でスパース - デンス モードを設定します。

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。

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）。

- PIM をスパース モードまたはデンス モードに設定し、Auto-RP を設定しない場合は、RP を手動で設定する必要があります。
- 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 デバイスである場合は、Auto-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 デバイス、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デバイスに到達しません。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 デバイスだけが存在する場合は、Auto-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 デバイスに Auto-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 デバイスと他社製の PIMv2 ルータを相互運用させる場合は、Auto-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

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、デンス モードまたはスパース モードで動作します。ルータは、スパース グループとデンス グループの両方を同時に処理できます。これらのモードは、ルータによるマルチキャスト ルーティング テーブルの書き込み方法と、ルータが直接接続された LAN から受信したマルチキャスト パケットの転送方法を決定します。

PIM 転送（インターフェイス）モードについては、次の項を参照してください。

PIM デンス モード（PIM-DM）

PIM デンス モード（PIM-DM）は、プッシュ モデルを使用してマルチキャスト トラフィックをネットワークの隅々にまでフラッディングします。このプッシュ モデルは、データを要求するレシーバを使用せずにデータをレシーバに配信するための方式です。この方式は、ネットワークのあらゆるサブネットにアクティブなレシーバが存在する特定の配置には効率的です。

デンス モードでは、ルータは、他のすべてのルータが特定のグループのマルチキャスト パケットの転送を求めていると想定します。あるルータがマルチキャスト パケットを受信した場合、直接接続されたメンバまたは PIM ネイバーが存在しないときは、ソースにプルーニング メッセージが返送されます。後続のマルチキャスト パケットは、このプルーニング済みのブランチのこのルータにはフラッディングされません。PIM は、ソース ベースのマルチキャスト配信ツリーを構築します。

PIM-DM は最初に、ネットワーク全体にマルチキャスト トラフィックをフラッディングします。ダウンストリーム ネイバーを持たないルータは、不要なトラフィックをプルーニングします。このプロセスは 3 分ごとに繰り返されます。

ルータは、フラッディングとプルーニングのメカニズムを介してデータ ストリームを受信することでステート情報を累積します。これらのデータ ストリームには送信元およびグループの情報が含まれているため、ダウンストリーム ルータがマルチキャスト転送テーブルを構築できます。

PIM-DM ではソース ツリー、つまり（S, G）エントリしかサポートしていないため、共有配信ツリーの構築に使用できません。

（注） デンス モードはほとんど使用されておらず、また、その使用もお勧めしません。このため、関連モジュールの設定作業では指定しません。

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。

デンスモードのインターフェイスと異なり、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。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。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，（198 ページ）」の項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。

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。

スパース-デンス モード

インターフェイス上でスパース モードまたはデンス モードを設定すると、そのインターフェイス全体にスパース性またはデンス性が適用されます。ただし、環境によっては、単一リージョン内の一部のグループについては PIM をスパース モードで実行し、残りのグループについてはデンス モードで実行しなければならない場合があります。

デンス モードだけ、またはスパース モードだけをイネーブルにする代わりに、スパース-デンス モードをイネーブルにできます。この場合、グループがデンス モードであればインターフェイスはデンス モードとして処理され、グループがスパース モードであればインターフェイスはスパース モードとして処理されます。インターフェイスがスパース-デンス モードである場合にグループをスパース グループとして処理するには、RP が必要です。

スパース-デンス モードを設定すると、ルータがメンバになっているグループにスパース性またはデンス性の概念が適用されます。

スパース - デンス モードのもう 1 つの利点は、Auto-RP 情報をデンス モードで配信しながら、ユーザ グループのマルチキャスト グループをスパース モード方式で使用できることです。したがって、リーフ ルータ上にデフォルト RP を設定する必要はありません。

インターフェイスがデンス モードで処理される場合、次のいずれかの条件が満たされると、そのインターフェイスはマルチキャスト ルーティング テーブルの発信インターフェイス リストに追加されます。

- インターフェイス上にメンバまたは DVMRP ネイバーが存在する。

- PIM ネイバーが存在し、グループがプルーニングされていない。

インターフェイスがスパース モードで処理される場合、次のいずれかの条件が満たされると、そのインターフェイスはマルチキャスト ルーティング テーブルの発信インターフェイス リストに追加されます。

- インターフェイス上にメンバまたは DVMRP ネイバーが存在する。
- インターフェイス上の PIM ネイバーが明示的な加入メッセージを受信した。

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デバイスはグループ/RP マッピングを動的に取得できます。
- スパース モード（SM）およびデンス モード（DM）は、インターフェイスではなく、グループに関するプロパティです。

（注） SM または DM のいずれか一方だけでなく、SM-DM（スパース/デンス モード）を使用してください。

- 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。

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。

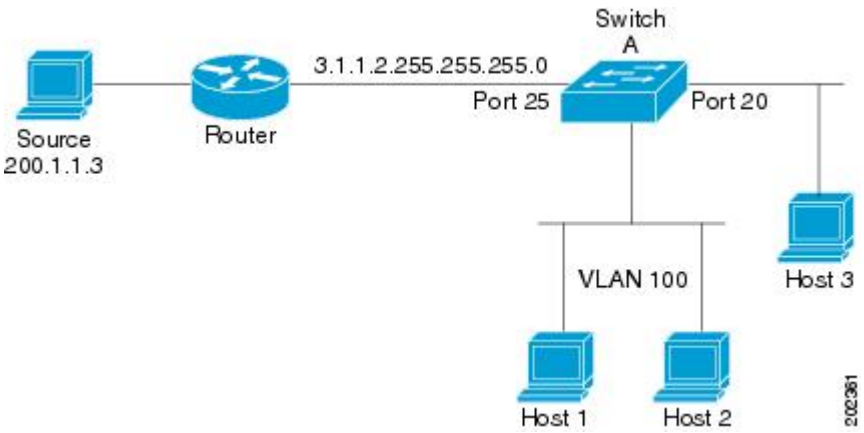
PIM スタブ ルーティングを使用しているときは、IP マルチキャスト ルーティングを使用し、デバイスだけを PIM スタブ ルータとして設定するように、分散ルータおよびリモート ルータを設定する必要があります。デバイスは分散ルータ間の伝送トラフィックをルーティングしません。デバイスのルーテッド アップリンク ポートも設定する必要があります。SVI の場合は、デバイスのアップリンク ポートを使用できません。SVI アップリンク ポートの PIM が必要な場合は、Network Advantage ライセンスにアップグレードする必要があります。

（注） また、PIM スタブ ルーティングをデバイスに設定するときは、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 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。

次の図では、デバイス 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。

図 *12*：*PIM* スタブ ルータ設定



IGMP ヘルパー

PIM スタブ ルーティングはルーティングされたトラフィックをエンドユーザの近くに移動させ、ネットワーク トラフィックを軽減します。スタブ ルータ（スイッチ）に IGMP ヘルパー機能を設定する方法でもトラフィックを軽減できます。

ip igmp helper-address *ip-address* インターフェイス コンフィギュレーション コマンドを使用してスタブルータ（スイッチ）を設定すると、スイッチによるネクストホップインターフェイスへのレポート送信をイネーブルにできます。ダウンストリーム ルータに直接接続されていないホストはアップストリーム ネットワークの送信元マルチキャスト グループに加入できます。この機能が設定されていると、マルチキャスト ストリームへの加入を求めるホストからの IGMP パケットはアップストリームのネクストホップ デバイスに転送されます。アップストリームのセントラル ルータは、ヘルパー IGMP レポートまたは leave を受信すると、そのグループの発信インターフェイス リストからインターフェイスの追加または削除を行います。

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。マルチキャスト データの配信方法は、PIM デンス モード（PIM DM）とは対照的です。PIM DM では、マルチキャスト トラフィックが最初にネットワークのすべてのセグメントにフラッディングされます。ダウンストリーム ネイバーを持たないルータ、または直接レシーバに接続されているルータは、不要なトラフィックをプルーニングします。

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） PIM をスパース モードまたはデンス モードに設定し、Auto-RP を設定しない場合は、RP を静的に設定する必要があります。

（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。その後、RP マッピング エージェントは、デンス モード フラッディングにより、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するようになります。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。その後、RP マッピング エージェントは、デンス モード フラッディングにより、一貫した group-to-RP マッピングを他のすべてのデバイスに送信します。

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。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

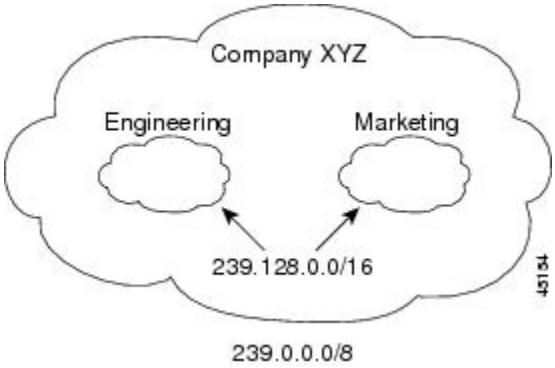
管理用スコープの境界を使用し、ドメインまたはサブドメイン外部へのマルチキャスト トラフィックの転送を制限できます。この方法では、「管理用スコープのアドレス」と呼ばれる特殊なマルチキャスト アドレス範囲が境界のメカニズムとして使用されます。管理用スコープの境界をルーテッド インターフェイスに設定すると、マルチキャスト グループ アドレスがこの範囲内にあるマルチキャスト トラフィックは、このインターフェイスに出入りできず、このアドレス範囲内のマルチキャスト トラフィックに対するファイアウォール機能が提供されます。

（注） マルチキャスト境界および TTL しきい値は、マルチキャスト 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。

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。

図 *13*：管理用スコープの境界



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 の利点

Auto-RP は IP マルチキャストを使用し、グループ/RP マッピングを PIM ネットワーク内のすべてのシスコ ルータおよびマルチレイヤ デバイス に自動配信します。Auto-RP には次の利点があります。

- ネットワーク内で複数の RP を使用し、複数のグループ範囲を処理する作業が簡単になります。
- 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。
- PIM ネットワーク内のすべてのルータおよびマルチレイヤ デバイス で矛盾が発生しなくなり、手動による RP 設定が不要になります。この結果、接続問題を引き起こす要因が取り除かれます。

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。

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 デバイス 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 デバイス 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デバイスに送信されます。BSR メッセージ内の RP 情報は、ローカルの RP キャッシュに格納されます。すべてのルータおよびデバイス 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。

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。

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)

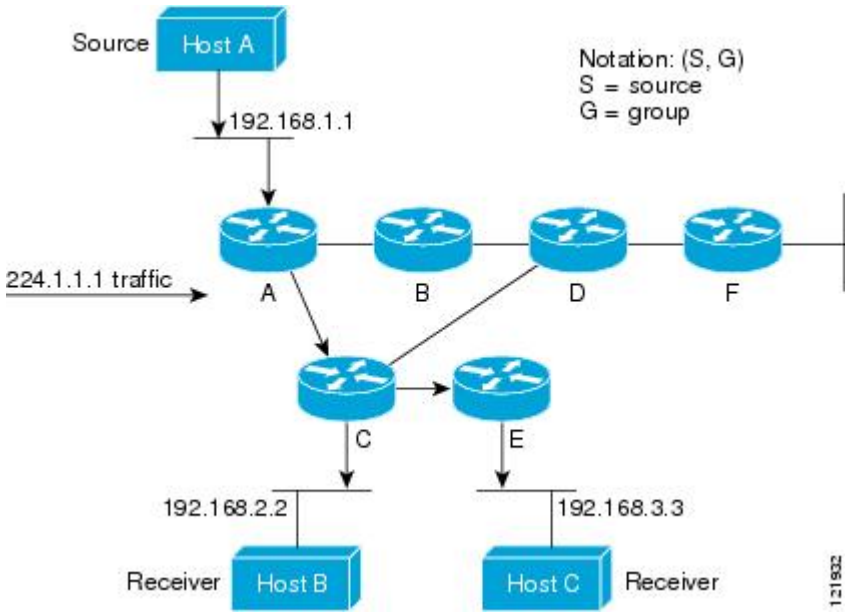
(S, G) という表記（「S カンマ G」と読みます）は、最短パス ツリーの列挙です。S はソースの IP アドレス、G はマルチキャスト グループ アドレスを表します。

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。



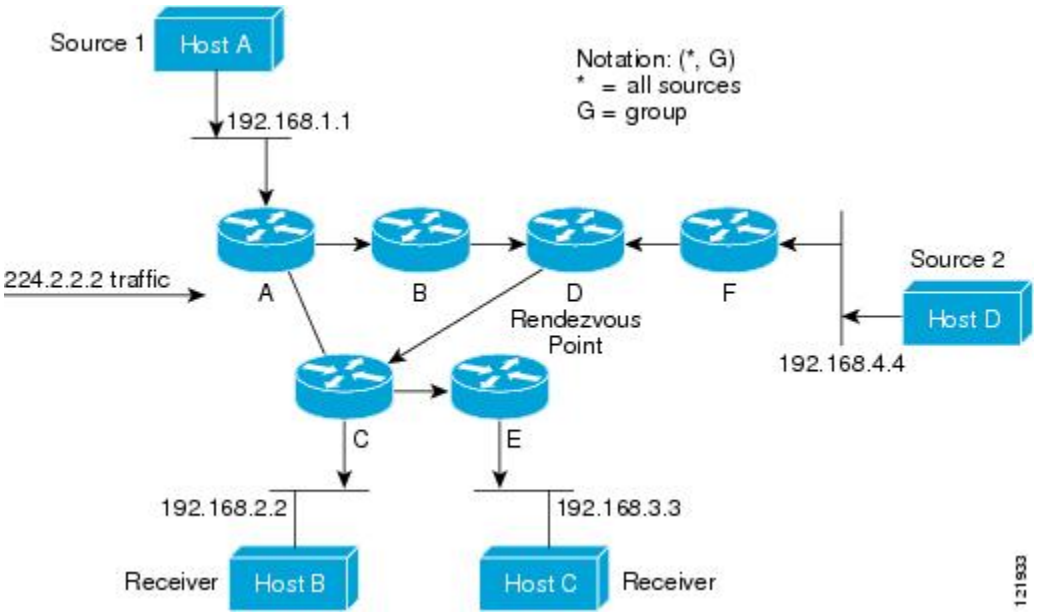
標準表記を使用すると、図の例の SPT は（192.168.1.1, 224.1.1.1）となります。

(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。

図 5 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）。



この例では、ソース（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 つのレシーバ（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 5 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。

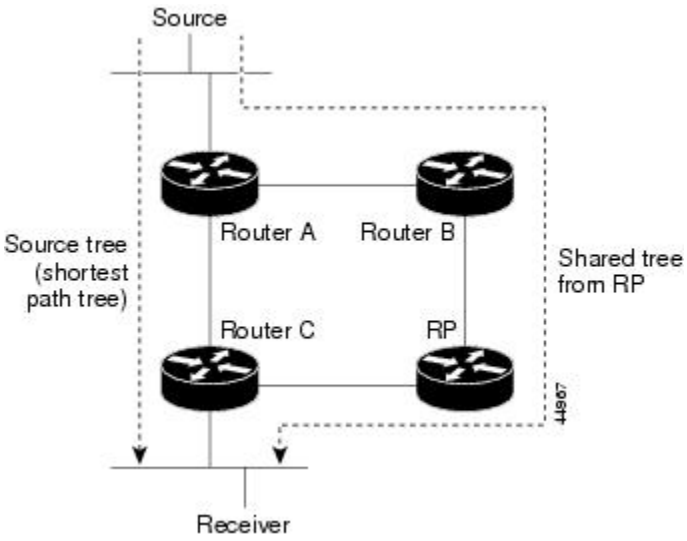
マルチキャスト転送では、ソースは、マルチキャスト グループ アドレスによって表される任意のホスト グループにトラフィックを送信します。マルチキャスト ルータは、どの方向が（ソースへ向かう）アップストリーム方向で、どの方向（1 方向または複数の方向）が（レシーバへ向かう）ダウンストリーム方向であるかを決定する必要があります。複数のダウンストリーム パスがある場合、ルータはパケットを複製し、それを適切なダウンストリーム パス（最善のユニキャスト ルート メトリック）で下方向に転送します。これらのパスがすべてであるとは限りません。レシーバの方向ではなく、ソースから遠ざかる方向へのマルチキャスト トラ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

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。

図 *14*：共有ツリーおよびソース ツリー（最短パスツリー）



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、ソフトウェアが送信元から最初のデータ パケットを受信すると、ソース ツリーにデバイスします。

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

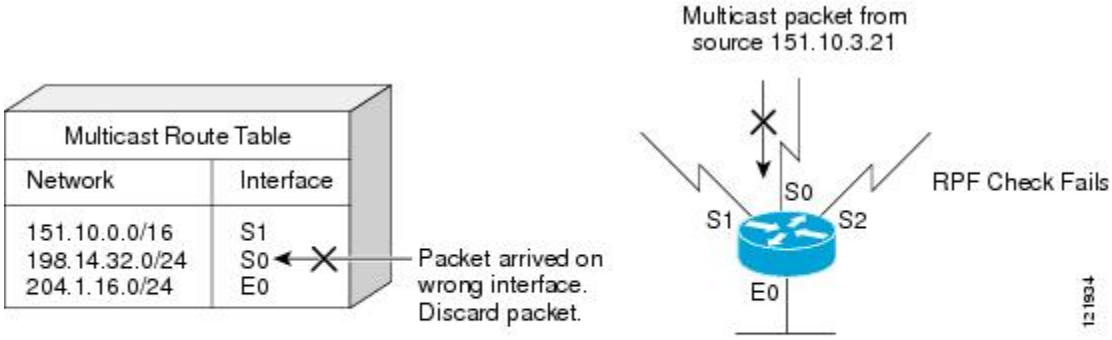
マルチキャスト パケットがルータに到達すると、ルータはそのパケットに対して RPF チェックを実行します。RPF チェックが成功すると、パケットが転送されます。そうでない場合、パケットはドロップされます。

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。

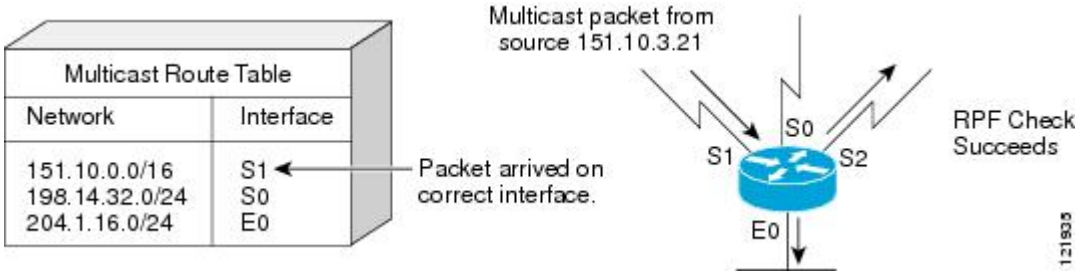
図 *15*：*RPF* チェックの失敗



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 *16*：*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 ルーティングのデフォルト設定

次の表に、デバイスの PIM ルーティングのデフォルト設定を示します。

表 *20*：マルチキャスト ルーティングのデフォルト設定

機能	デフォルト設定
マルチキャスト ルーティング	すべてのインターフェイスでディセーブル
PIM のバージョン	バージョン 2
PIM モード	モードは未定義
PIM スタブ ルーティング	未設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル。
PIM マルチキャスト境界	なし。
候補 BSR	ディセーブル。
候補 RP	ディセーブル。
SPT しきい値レート	0 kb/s
PIM ルータ クエリー メッセージ インターバル	30 秒

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。 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。 • 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、

	コマンドまたはアクション	目的
		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 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 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。

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
  - 新規インターネットワークでの自動 RP の設定
  - 既存のスパースモード クラウドへの自動 RP の追加
  - 問題のある RP への Join メッセージの送信禁止
  - 着信 RP アナウンスメント メッセージのフィルタリング
- 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, （190 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、マルチレイヤデバイス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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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 デバイス（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 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*]	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。

	コマンドまたはアクション	目的
	例： `Device(config)# access-list 25 permit 10.5.0.1 255.224.0.0`	• *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。
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。

新規インターネットワークでの Auto-RP の設定

新規インターネットワーク内に自動 RP を設定している場合は、すべてのインターフェイスが SM-DM に設定されるため、デフォルトの RP は不要です。

（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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権EXECモードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**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	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 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`	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

	コマンドまたはアクション	目的
	`1/0/5 scope 20 group-list 10 interval 120`	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* 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。 • **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 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。

	コマンドまたはアクション	目的
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。

既存のスパース モード 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

	コマンドまたはアクション	目的
ステップ1	**enable** 例： `Device> enable`	特権EXECモードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ2	**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	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ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* 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。 • **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。 （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。

	コマンドまたはアクション	目的
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 デバイスが **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。

自動 RP によってアドバタイズされるすべての RP を許可し、他のすべての RP をデフォルトで拒否するには、**ip pim accept-rp auto-rp** 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。

この手順は任意です。

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。 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*]	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。

	コマンドまたはアクション	目的
	例： `Device(config)# access-list 10 permit 10.8.1.0 255.255.224.0`	• *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 デバイスからの候補 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： `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`	（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
	`running-config` `startup-config`	

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権EXECモードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface`	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。

	コマンドまたはアクション	目的
	gigabitethernet 1/0/1	• 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。 • 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 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**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。

	コマンドまたはアクション	目的
		• （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。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 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。

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

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
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、スイッチを候補 BSR に設定するときに BSR アドレスの取得元となるデバイス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 を使用して有効化する必要があります。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。

はじめる前に

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 デバイス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 デバイスと、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 デバイスを RP として設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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 リスト番号を入力します。group-list を指定しない場合は、

	コマンドまたはアクション	目的
		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

はじめる前に

- 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。インターフェイスを設定する方法を決定する必要があります。
- 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 リスナーの機能を設定し（ステップ 5）、スパース モードを指定するか（ステップ 7）、またはスパース - デンス モードを指定する（ステップ 8）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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipmulticast-routing** [**distributed**] 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。 • **distributed** キーワードを使用して、マルチキャスト分散スイッチ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	**ippimautorplistener** 例： `Device(config)# ip pim autorp listener`	2 つの Auto-RP グループ 209.165.201.1 と 209.165.201.22 の IP マルチキャスト トラフィックを PIM スパース モードで動作しているインターフェイスでフラッディングされる PIM デンス モードにします。 • 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 6	**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 7	**ippimsparse-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 8	**ippimsparse-dense-mode** 例： `Device(config-if)# ip pim sparse-dense-mode`	インターフェイスで PIM スパース-デンス モードをイネーブルにします。 • ステップ 7 でスパース モードを設定している場合は、このステップをスキップします。
ステップ 9	**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。

	コマンドまたはアクション	目的
ステップ 10	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 11	**ippimsend-rp-announce** {*interface-type interface-number* | *ip-address*} **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**] 例： `Device(config)# ip pim send-rp-announce loopback0 scope 31 group-list 5`	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。 • 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 12	**ippimsend-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value* [**interval** *seconds*] 例： `Device(config)# ip pim`	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。

	コマンドまたはアクション	目的
	`send-rp-discovery loopback 1 scope 31`	• 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。 • 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 13	**ippimrp-announce-filterrp-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 14	**noippimdm-fallback** 例： `Device(config)# no ip pim dm-fallback`	（任意）PIM デンス モード フォールバックを防ぎます。 • すべてのインターフェイスが PIM スパース モードで動作するよう設定されている場合、このステップはスキップします。 （注） （**ippimsparse-mode** コマンドを使用して）すべてのインターフェイスが PIM スパース モードで動作するよう設定されている場合、**noippimdm-fallback** コマンド動作がデフォルトでイネーブルになります。

	コマンドまたはアクション	目的
ステップ 15	**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 16	**ipmulticastboundary** *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。 • **deny** キーワードを使用するアクセス リスト エントリは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を作成します。
ステップ 17	**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 18	**showippimautorp** 例： `Device# show ip pim autorp`	（任意）Auto-RP 情報を表示します。
ステップ 19	**showippimrp** [**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 20	**showipigmpgroups** [*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。

	コマンドまたはアクション	目的
ステップ 21	**showipmroute**[*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。

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。

	コマンドまたはアクション	目的
		• （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。 • （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`	（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
	`startup-config`	

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 デバイスでは、各 LAN セグメント（サブネット）の指定ルータ（DR）になるデバイスを検出するため、PIM ルータクエリー 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。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

	コマンドまたはアクション	目的
		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 query-interval** 秒 例： `Device(config-if)# ip pim query-interval 45`	デバイスが 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。 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。
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

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

ステップ 2	**showipmroute** [*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:`
		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。

	コマンドまたはアクション	目的
	Serial1/0, Forward/Sparse-Dense, 00:18:10/00:03:19	

ステップ 3	**showipmrouteactive**[*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、**showipmroute** 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送信元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

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

	コマンドまたはアクション	目的

ステップ 2	**showipmroute** [*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-Dense, 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-Dense, 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	**showipmrouteactive**
	
	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、**showipmroute** 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送信元の情報が表示されます。より低いレートのトラフィック（4kb/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

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

ステップ 2	**showipigmpgroups**
	
	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	**showippimrpmapping**
	
	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、**showippimrpmapping** 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 **showippimrpmapping** コマンドの出力には表示されません。

ステップ 4	**showipmroute**
	
	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-Dense, 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:`
		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
	GigabitEthernet1/0, Forward/Sparse-Dense, 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-Dense, 00:05:15/00:00:00 GigabitEthernet0/0, Forward/Sparse-Dense, 00:10:05/00:00:00 (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	**showipinterface** [*type number*] 例： Device# **show ip interface GigabitEthernet 0/0/0** GigabitEthernet0/0 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 multicast distributed fast switching is disabled 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） **noipmroute-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。

	コマンドまたはアクション	目的

ステップ 6	**showippiminterfacecount**
	
	例：
	`Device# show ip pim interface count`
	
	`State: * - Fast Switched, D - Distributed Fast Switched`
	`H - Hardware Switching Enabled`
	`Address Interface FS Mpackets In/Out`
	`172.31.100.2 GigabitEthernet0/0/0 * 4122/0`
	`10.1.0.1 GigabitEthernet1/0/0 * 0/3193`
		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 7	**showipmroutecount**
	
	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 8	**showipmrouteactive**[*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、**showipmroute** コマンドと **active** キーワードによる出力では、4kb/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送信元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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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	**ipigmpjoin-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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**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 *21*：*PIM* モニタリング コマンド

コマンド（Command）	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。

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 *22*：*RP* マッピングのモニタリング コマンド

コマンド（Command）	目的
show ip pim rp-hash グループ	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 デバイス上で、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 の情報をモニタするには、次の表に示す特権 EXEC コマンドを使用します。

表 *23*：*VTP* モニタリング コマンド

コマンド（Command）	目的
show ip pim bsr	選択された BSR 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）。

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 distributed
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。

```
Device# 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。

```
Device(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Device(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、このデバイスが RP として機能するグループが記述されています。

```
Device(config)# ip pim send-rp-announce gigabitethernet1/0/1 scope 31 group-list 5
```

```
Device(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。

```
Device(config)# access-list 1 deny 224.0.1.39
Device(config)# access-list 1 deny 224.0.1.40
Device(config)# access-list 1 permit all
Device(config)# interface gigabitethernet1/0/1
Device(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。

```
Device(config)# ip pim rp-announce-filter rp-list 10 group-list 20
Device(config)# access-list 10 permit host 172.16.5.1
Device(config)# access-list 10 permit host 172.16.2.1
Device(config)# access-list 20 deny 239.0.0.0 0.0.255.255
Device(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。

```
Device(config)# ip pim accept-rp 172.10.20.1 1
Device(config)# access-list 1 permit 224.0.1.39
Device(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。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip address 172.21.24.18 255.255.255.0
Device(config-if)# ip pim sparse-dense-mode
Device(config-if)# ip pim bsr-candidate gigabitethernet1/0/2 30 10
```

例：候補 RP の設定

次に、デバイスが自身を候補 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。

```
Device(config)# ip pim rp-candidate gigabitethernet1/0/2 group-list 4
Device(config)# access-list 4 permit 239.0.0.0 0.255.255.255
```

PIM に関する追加情報

関連資料

関連項目	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

標準および RFC

標準/RFC	役職（Title）
PIM については、RFC 4601 および次に示す Internet Engineering Task Force（IETF）インターネット ドラフトを参照してください。	• 『*Protocol Independent Multicast (PIM): Motivation and Architecture*』 • 『*Protocol Independent Multicast (PIM), Dense Mode Protocol Specification*』 • 『*Protocol Independent Multicast (PIM), Sparse Mode Protocol Specification*』 • 『*draft-ietf-idmr-igmp-v2-06.txt, Internet Group Management Protocol, Version 2*』 • 『*draft-ietf-pim-v2-dm-03.txt, PIM Version 2 Dense Mode*』

MIB

MIB	MIB 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 リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

PIM の機能情報

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

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

表 *24*：*PIM* の機能情報

機能名（Feature Name）	リリース	機能情報
PIM	Cisco IOS XE Everest 16.5.1a	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。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

第 10 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-serverenabletrapspim** [**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-serverhost** *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-dense-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	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

標準および RFC

標準/RFC	役職（Title）
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)』

MIB

MIB	MIB リンク
こ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 ソフトウェア 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場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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

IP マルチキャストに対する PIM MIB 拡張の機能情報

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

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

表 *25* : *IP* マルチキャストに対する *PIM MIB* 拡張の機能情報

機能名（Feature Name）	リリース	機能情報
IP マルチキャストに対する PIM MIB 拡張	Cisco IOS XE Everest 16.5.1a	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。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

第 11 章

MSDP の設定

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

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。

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。

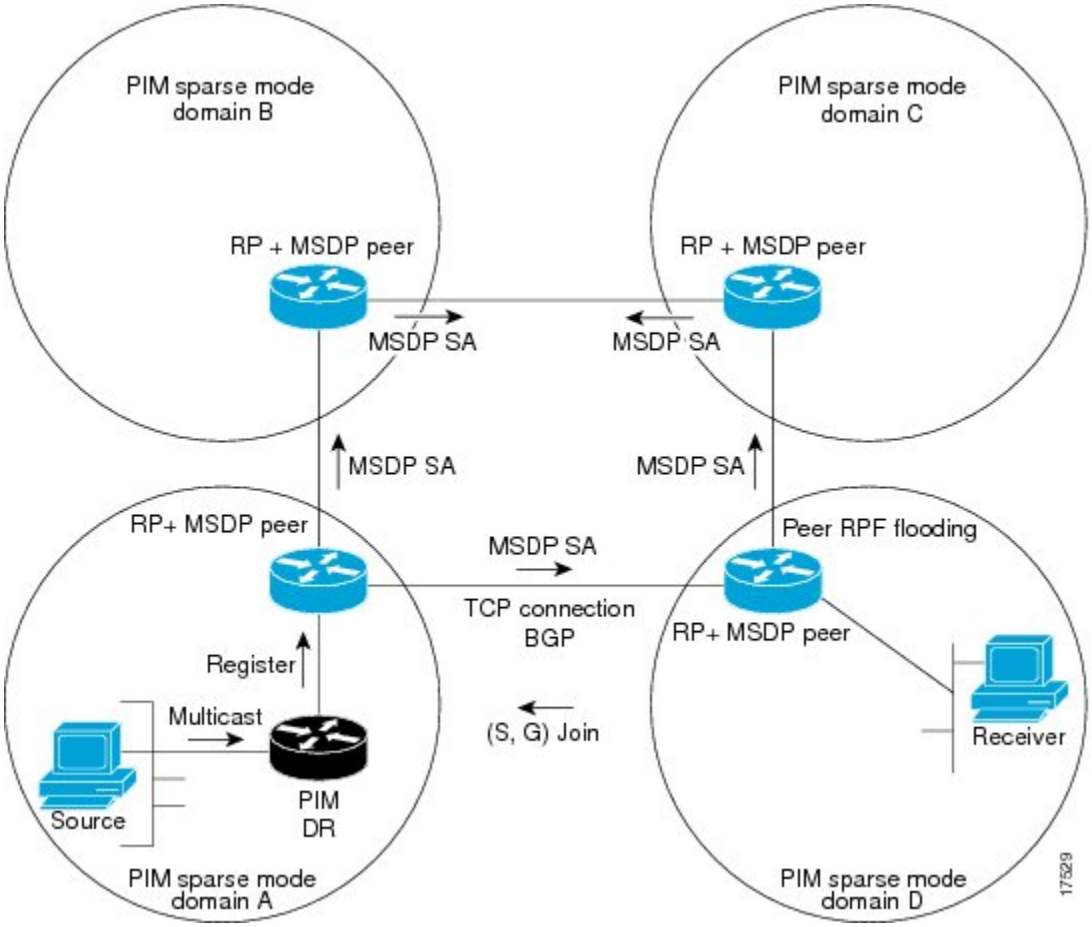
MSDP がイネーブルになっている場合、PIM-SM ドメインの RP は、他のドメインの MSDP 対応デバイスとの MSDP ピアリング関係を維持します。このピアリング関係は TCP 接続を通じて発生します。交換されるのは主にマルチキャスト グループを送信する送信元のリストです。MSDP はピアリング接続に TCP（ポート 639）を使用します。BGP と同様に、ポイントツーポイント TCP ピアリングを使用する場合は、各ピアを明示的に設定する必要があります。さらに、RP 間の TCP 接続は基本的なルーティング システムによって実現されます。受信側の RP では、送信元リストを使用して送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。

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（ルータやコントローラ）を使用できます。

（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 *17* : ***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。

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、**ipmulticastcache-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, （268 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。

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。

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。

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。

（注） 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 ピア間の 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、**ipmsdpsa-limit** コマンドを使用します。**ipmsdpsa-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、**ipmsdpsa-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

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 プロバイダー（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。

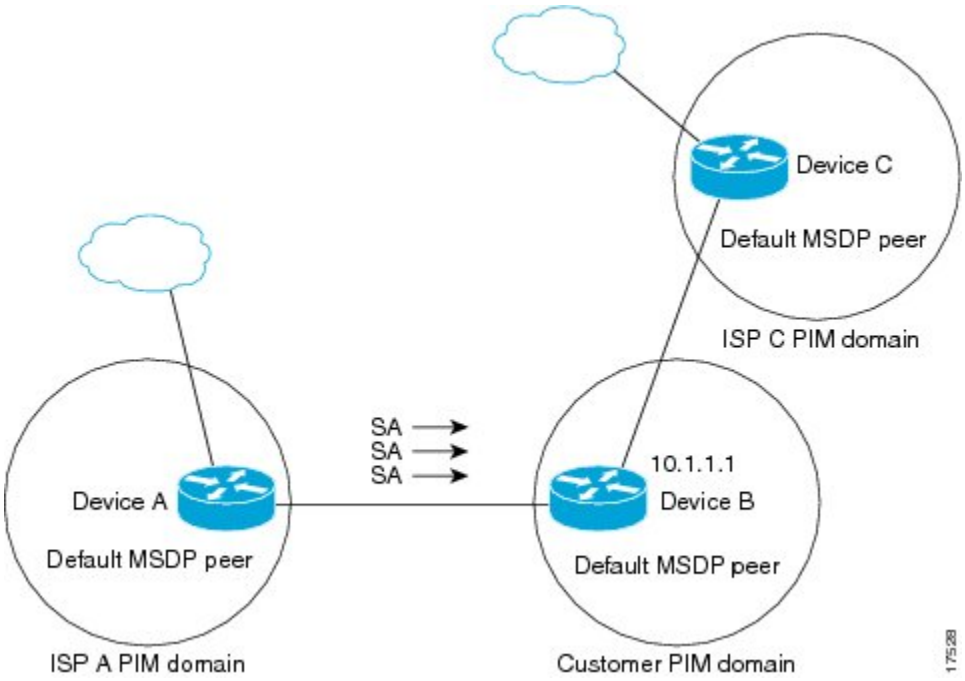
ISP は、プレフィックス リストを使用して、カスタマーのデバイスから受け入れるプレフィックスを定義する場合もあります。カスタマーは、複数のデフォルト ピアを定義します。各ピアには関連するプレフィックスを 1 つまたは複数設定します。

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（ルータやコントローラ）を使用できます。

（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*：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」の項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。

はじめる前に

- 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdppeer** {*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，（288 ページ）またはMSDP メッシュ グループの設定，（289 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	**ipmsdpdescription** {*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。
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。

はじめる前に

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpshutdown** {*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。	--

	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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdppassword 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。 • 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。

	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。
ステップ 5	**showipmsdppeer**[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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpsa-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： `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	**showipmsdpcount** [*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	**showipmsdppeer** [*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	**showipmsdpsummary** 例： `Device# show ip msdp summary`	（任意）MSDP ピアのステータスを表示します。

	コマンドまたはアクション	目的
		（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、**ipmsdpkeepalive** 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpkeepalive**{*peer-address* | *peer-name*} *keepalive-interval hold-time-interval*	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

	コマンドまたはアクション	目的
	例： `Device(config)# ip msdp keepalive 10.1.1.3 40 55`	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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdptimer** *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。

	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。

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。

はじめる前に

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpdefault-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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします • 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 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、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されている必要があります。
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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpredistribute**[**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） **ipmsdpredistribute** コマンドは、RP で認識されているが登録されていないソース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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpsa-filterout** {*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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpsa-filterin** {*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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpttl-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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpsa-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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpfilter-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。

境界 PIM デンス モード領域の MSDP への包含

PIM デンス モード（PIM-DM）リージョンでアクティブなソースの SA メッセージを送信するように境界デバイスを設定するには、次の任意の作業を実行します。

PIM-SM リージョンと PIM-DM リージョンの境界にデバイスを設定できます。デフォルトでは、PIM-DM ドメインのソースは MSDP に含まれません。PIM-DM ドメインでアクティブなソースの SA メッセージを送信するようにこの境界デバイスを設定できます。その場合、**ipmsdpredistribute** コマンドを設定してアドバタイズする PIM-DM ドメインのローカル ソースを制御することも非常に重要です。このコマンドを設定しないと、PIM-DM ドメインのソースが送信を停止した後も長時間 (S, G) ステートのままになります。設定の詳細については、「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, （290 ページ）」の項を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdpbordersa-address** *type number* 例： `Device(config)# ip msdp border sa-address gigabitethernet0/0/0`	PIM-DM ドメインでアクティブなソースの SA メッセージを発信するように、PIM-SM および PIM-DM ドメイン間の境界にデバイスを設定します。 • インターフェイスの IP アドレスは、SA メッセージの RP フィールドに示されるソース ID として使用されます。
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。

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。

はじめる前に

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, （280 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmsdporiginator-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

ステップ 1 **enable**

例：

```
Device# enable
```

特権 EXEC モードをイネーブルにします。

- プロンプトが表示されたら、パスワードを入力します。

ステップ 2 **debugipmsdp** [*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、**debugipmsdp** 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 **debugipmsdpresets**

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 **showipmsdpcount** [*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。**ipmsdpcache-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、**showipmsdpcount** 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 **showipmsdppeer** [*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、**showipmsdppeer** 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 **showipmsdpsa-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、**showipmsdpsa-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 **showipmsdpsummary**

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、**showipmsdp 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**clearipmsdppeer** [*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	**clearipmsdpstatistics** [*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。
ステップ 4	**clearipmsdpsa-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。 • **clearipmsdpsa-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。

はじめる前に

- 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。
- msdpEstablished 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**snmp-serverenabletrapsmsdp** 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-serverenabletraps msdp** コマンドは、トラップと応答要求の両方をイネーブルにします。
ステップ 3	**snmp-serverhost** *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。

	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。

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 **showipmsdpsummary** コマンドおよび **showipmsdppeer** 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、**showipmsdpsa-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、**debugipmsdp** 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

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。

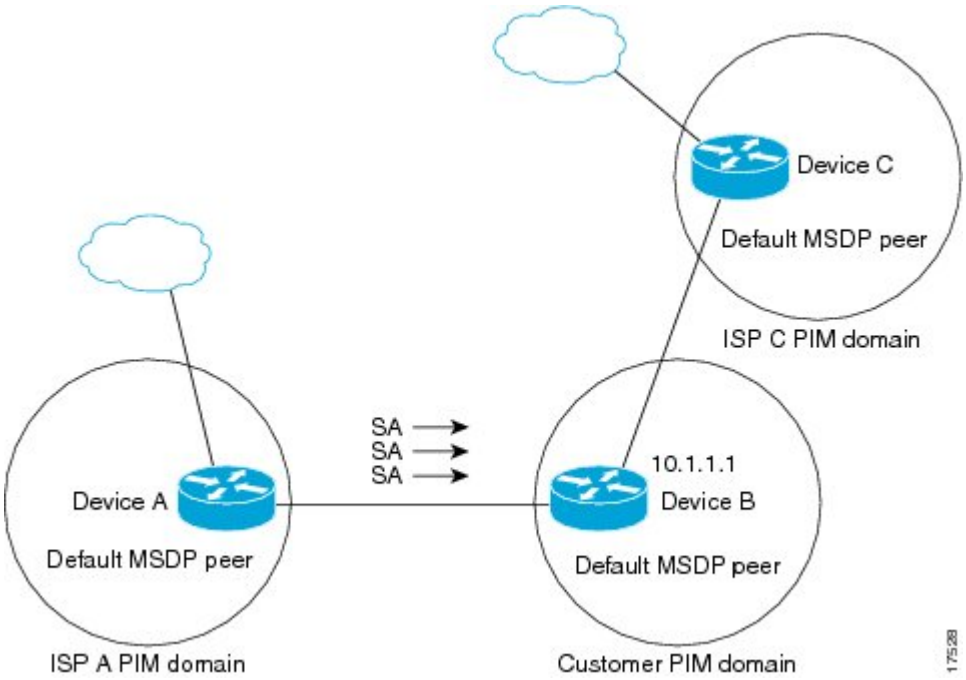
ISP は、プレフィックス リストを使用して、カスタマーのデバイスから受け入れるプレフィックスを定義する場合もあります。カスタマーは、複数のデフォルト ピアを定義します。各ピアには関連するプレフィックスを 1 つまたは複数設定します。

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（ルータやコントローラ）を使用できます。

（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
```

その他の参考資料

関連資料

関連項目	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
IPv6 コマンド	*IPv6* コマンドの参考資料

標準および RFC

標準/RFC	役職（Title）
IPv6 に関する RFC	*IPv6* の *RFC*

MIB

MIB	MIB リンク
こ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 リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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

Multicast Source Discovery Protocol の機能情報

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

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

表 *26*：*Multicast Source Discovery Protocol* の機能情報

機能名（Feature Name）	リリース	機能情報
Multicast Source Discovery Protocol	Cisco IOS XE Everest 16.5.1a	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。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

第 12 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 サーバがない場合は、DNS サーバ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）チャネルの加入登録をサポートするように変更していない限り、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 マッピング機能は、完全な SSM の利点を共有しません。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 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。この章で言及する他のコマンドについては、コマンド リファレンス マスター インデックス（オンライン検索）を使用して、該当するマニュアル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。デバイスは、SSMの実装をサポートする次のコンポーネントをサポートしています。

- 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は 1 つです。1 つのサーバから複数の 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。

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 サーバのマニュアルを参照してください。

SSM の設定方法

この項の Source-Specific Multicast（SSM; 送信元特定マルチキャスト）コマンドの詳細な説明については、『*IP Multicast Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』を参照してください。この章で言及する他のコマンドについては、コマンド リファレンス マスター インデックス（オンライン検索）を使用して、該当するマニュアルを参照してください。

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。

はじめる前に

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。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

	コマンドまたはアクション	目的
		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 5	**ip pim** {**sparse-mode** | **sparse-dense-mode**} 例： `Device(config-if)# ip pim sparse-dense-mode`	インターフェイスに対して PIM をイネーブルにします。スパース モードまたはスパース ― デンス モードのどちらかを使用する必要があります。
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。
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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipigmpssm-mapenable** 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	**noipigmpssm-mapquerydns** 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** コマンドは DNS ベースの SSM マッピングをイネーブルにします。
ステップ 5	**ipigmpssm-mapstatic** *access-list source-address*	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。

	コマンドまたはアクション	目的
	例： `Device(config)# ip igmp ssm-map static 11 172.16.8.11`	（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 **ipigmpssm-mapstatic** 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決定します。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： `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。

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 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipigmpssm-mapenable** 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	**ipigmpssm-mapquerydns** 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** コマンドは DNS ベースの SSM マッピングをイネーブルにします。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	**ipdomainmulticast** *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	**ipname-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のアドレスを指定します。

	コマンドまたはアクション	目的
ステップ 7	冗長性のために追加の DNS サーバを設定する場合は、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： `Device(config)# end`	特権 EXEC モードに戻ります。
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。

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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権EXECモードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	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。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。 （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。

	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 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。

SSM のモニタリング

SSM をモニタするには、次の表の特権 EXEC コマンドを使用します。

表 *27*：***SSM*** のモニタリング コマンド

コマンド（Command）	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するには、次の表の特権 EXEC コマンドを使用します。

表 *28* : *SSM* マッピングをモニタするコマンド

コマンド（Command）	目的
Device# **show ip igmp ssm-mapping**	SSM マッピングについての情報を表示します。
Device#**show ip igmp ssm-mapping** *group-address*	SSMマッピングが特定のグループに使用する送信元を表示します。
Device#**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。
Device#**show host**	デフォルトのドメイン名、名前ルックアップサービス、ネーム サーバ ホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。
Device#**debug ip igmp** *group-address*	送受信された IGMP パケットと IGMP ホスト関連イベントを表示します。

SSM の次の作業

次の設定を行えます。

- IGMP
- ワイヤレス マルチキャスト
- 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	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

標準および RFC

標準/RFC	役職（Title）
RFC 4601	『*Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*』

MIB

MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

SSM の機能情報

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

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

表 *29* : *SSM* の機能情報

機能名（Feature Name）	リリース	機能情報
SSM	Cisco IOS XE Everest 16.5.1a	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。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

第 13 章

サービス検出ゲートウェイの設定

サービス検出ゲートウェイの設定に関する制約事項

サービス検出ゲートウェイの設定に関する制約事項は次のとおりです。

- サービス検出ゲートウェイは、複数のホップによるトポロジをサポートしていません。すべてのネットワーク セグメントを直接接続する必要があります。サービス検出ゲートウェイは、接続されているすべてのセグメントからサービスを学習して、キャッシュを構築し、プロキシとして動作する要求に応答できます。
- サードパーティ mDNS サーバまたはアプリケーションの使用は、この機能ではサポートされていません。

サービス検出ゲートウェイおよび mDNS に関する情報

mDNS

mDNS は設定不要を実現するために定義され、設定不要は次の機能を提供するものとして定義されています。

- アドレッシング：ホストへの IP アドレスの割り当て
- ネーミング：IP アドレスの代わりに名前を使用したホストの参照
- サービス検出：ネットワークでの自動的なサービスの検索

mDNS を使用すると、ネットワーク ユーザは、ネットワーク上のサービスにアクセスするために IPアドレスを割り当てたり、ホスト名を割り当てたり、名前を入力する必要がなくなります。ユーザが行うことは、利用可能なネットワーク サービスの表示を要求し、リストから選択することだけです。

mDNS では、DHCP/DHCPv6 または IPv4 および IPv6 リンク ローカル スコープ アドレスの使用を通じてアドレッシングが実行されます。設定不要の利点が生じるのは、DHCP や DNS のようなインフラストラクチャ サービスが存在せず、自分で割り当てたリンクローカルアドレッシングを使用できる場合です。その結果、クライアントは、リンクローカル範囲（169.254.0.0/24）内でランダムな IPv4 アドレスを選択するか、またはその IPv6 リンクローカル アドレス（FE80::/10）を使用して通信を行うことができます。

mDNS では、ネーミング（mDNS を使用したローカル ネットワークでの名前/アドレス変換）クエリはリンクローカル スコープ IP マルチキャストを使用してローカル ネットワークを介して送信されます。これらの DNS クエリはマルチキャスト アドレス（IPv4 アドレス 224.0.0.251 または IPv6 アドレス FF02::FB）に送信されるため、クエリへの応答にグローバルな知識を持つ単一の DNS サーバは必要ありません。サービスまたはデバイスは、認識しているサービスに関するクエリを確認すると、キャッシュからの情報が含まれた DNS 応答を提供します。

mDNS では、サービス検出はブラウジングによって実行されます。mDNS クエリは、特定のサービス タイプとドメインに応じて送信され、一致するサービスを認識しているデバイスがサービス情報を返します。その結果は利用可能なサービスのリストからなり、ユーザはそのリストから選択できます。

mDNS プロトコル（mDNS-RFC）を DNS サービス検出（DNS-SD-RFC）とともに使用すると、アドレッシング、ネーミング、およびサービス検出の設定が不要になります。

mDNS-SD

マルチキャスト DNS サービス検出（mDNS-SD）は、DNS プロトコル セマンティックおよびウェルノウンマルチキャストアドレス経由のマルチキャストを使用して、設定不要のサービス検出を実現します。DNS パケットは、マルチキャスト アドレス 224.0.0.251 とその IPv6 相当の FF02::FB を使用してポート 5353 上で送受信されます。

mDNS はリンクローカル マルチキャスト アドレスを使用するため、その範囲は 1 つの物理 LAN または論理的LANに制限されます。ネットワーキングの範囲を分散したキャンパス、またはさまざまな多数のネットワーク テクノロジーで構成される広域環境に拡張する必要がある場合は、mDNS ゲートウェイが実装されます。mDNS ゲートウェイでは、1 つのレイヤ 3 ドメインから別のドメインへのサービスのフィルタリング、キャッシング、および再配布を行うことで、レイヤ 3 境界間での mDNS パケットの転送を行うことができます。

サービス検出ゲートウェイ

サービス検出ゲートウェイ機能により、マルチキャスト ドメイン ネーム システム（mDNS）は、レイヤ3の境界を越えて（異なるサブネットで）動作します。mDNS ゲートウェイでは、1 つのレイヤ3 ドメイン（サブネット）から別のドメインへのサービスのフィルタリング、キャッシング、および再配布を行うことで、レイヤ 3 境界間でのサービス検出の転送を行うことができます。この機能が実装される前は、リンクローカル スコープのマルチキャスト アドレスを使用していたため、mDNS は 1 サブネット内に範囲が制限されていました。この機能により、Bring Your Own Device（BYOD）が強化されます。

mDNS ゲートウェイとサブネット

サービス検出をサブネット間で動作させるには、mDNS ゲートウェイを有効にする必要があります。mDNS ゲートウェイは、デバイスまたはインターフェイスに対してイネーブルにできます。

（注） インターフェイス レベルで設定する前に、グローバルにサービスを設定する必要があります。

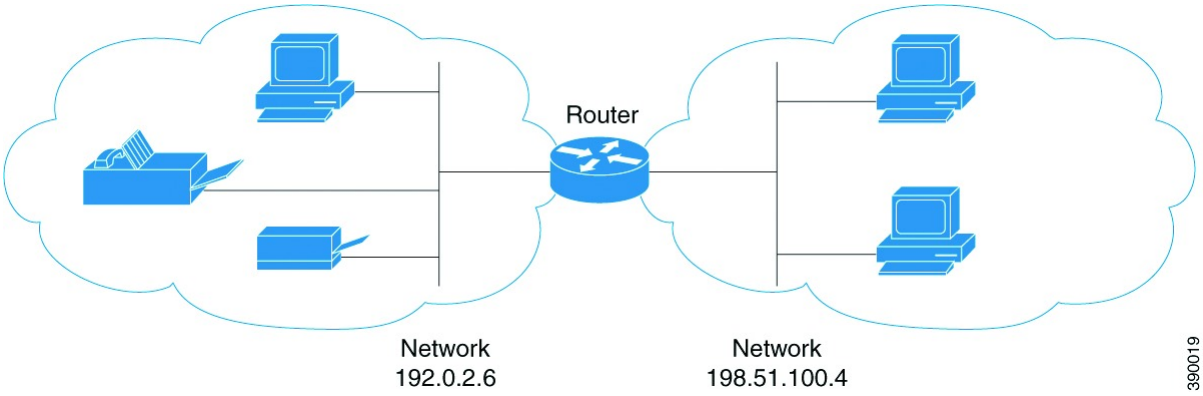
デバイスまたはインターフェイスを有効にした後、サブネット間にサービス検出情報を再配布できます。サービス ポリシーを作成し、着信サービス検出情報（インバウンド（IN）フィルタリングと呼ぶ）または発信サービス検出情報（アウトバウンド（OUT）フィルタリングと呼ぶ）に対してフィルタを適用できます。

（注） 再配布がグローバルに有効になっている場合は、グローバル コンフィギュレーションがインターフェイス コンフィギュレーションよりも優先順位が高くなります。

たとえば、mDNS ゲートウェイ機能がこの図のルータで有効になっている場合は、サービス情報を 1 つのサブネットから別のサブネットに送信することができ、その逆も同様です。たとえば、IP アドレス 192.0.2.6 のネットワークでアドバタイズされているプリンタとファクスのサービス情報は、IP アドレス 198.51.100.4 のネットワークに再配布されます。IP アドレス 192.0.2.6 のネット

ワーク内のプリンタとファクスのサービス情報は、他のネットワーク内の mDNS 対応ホストとデバイスによって学習されます。

図 *20*：サンプルのネットワーク シナリオ



フィルタリング

mDNS ゲートウェイとサブネットを設定した後、再配布するサービスをフィルタリングできます。サービス リストを作成するときは、**permit** または **deny** コマンド オプションが使用されます。

- **permit** コマンド オプションを使用すると、特定のサービス リスト情報を許可したり転送したりできます。
- **deny** オプションを使用すると、他のサブネットに転送可能なサービス リスト情報を拒否することができます。

permit または **deny** コマンド オプションを使用する場合は、シーケンス番号を含める必要があります。同じサービス リスト名を複数のシーケンス番号に関連付けることができ、各シーケンス番号はルールにマッピングされます。

（注） フィルタが設定されていない場合、デフォルトのアクションは、デバイスまたはインターフェイスを通して転送されるサービス リスト情報を拒否することです。

クエリは、サービスリストを作成する際に提供される別のオプションです。サービスリストを使用してクエリを作成できます。サービスについて参照する場合は、アクティブなクエリを使用できます。この機能は、キャッシュ内で更新されたレコードを保持するのに役立ちます。

（注） アクティブなクエリはグローバルでのみ使用でき、インターフェイス レベルでは使用できません。

サービスが起動すると、サービス エンドポイント（プリンタ、ファックスなど）は非請求アナウンスメントを送信します。その後、ネットワーク変更イベント（インターフェイスの表示や消去

など）が発生するたびに、非請求アナウンスメントを送信します。デバイスは必ずクエリに応答します。

サービス リストを作成し、**permit** または **deny** コマンド オプションを使用した後、*service-instance*、*service-type* または *message-type* に基づいて、match ステートメント（コマンド）を使用してフィルタリングできます（アナウンスメントまたはクエリ）。

サービス検出ゲートウェイの設定方法

サービス リストの設定

次の手順では、サービス リストを作成し、サービス リストにフィルタを適用して、サービス リスト名のパラメータを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**service-list mdns-sd** *service-list-name* {**deny** *sequence-number* | **permit** *sequence-number* | **query**}
	
	例：
	`Device(config)# service-list mdns-sd sl1 permit 3`
	
	`Device(config)#`
		mDNS サービス検出サービス リスト モードを開始します。このモードでは、次の操作を実行できます。
		• サービス リストを作成し、シーケンス番号に適用された **permit** または **deny** オプションに従って、サービス リストにフィルタを適用します。
		• **query** オプションを使用している場合は、サービス リストを作成し、サービス リスト名のクエリを関連付けます。
		
		（注） シーケンス番号は、ルールの優先順位を設定するものです。低いシーケンス番号を持つルールが最初に選択され、サービスアナウンスメントまたはクエリがそれに応じて許可または拒否されます。ネットワーク要件によってシーケンス番号を定義します。

	コマンドまたはアクション	目的
	service-list mdns-sd sl4 query	
ステップ 4	**match message-type** {**announcement** | **any** | **query**} 例： `Device(config-mdns-sd-sl)# match message-type announcement`	（任意）照合するメッセージ タイプを設定します。次のメッセージ タイプを照合できます。 • アナウンスメント • 任意 • クエリ これらのコマンドでは、ステップ 2 で作成されたサービス リスト名に対するパラメータが設定されます。 **match message-type** がアナウンスメントの場合、サービス リストのルールでは、デバイスに対するサービス アドバタイズメントまたはアナウンスメントのみが許可されます。**match message-type** がクエリの場合は、ネットワーク内の特定のサービスに対するクライアントからのクエリのみが許可されます。 異なるシーケンス番号を持つ同じ名前の複数のサービス マップを作成することができ、フィルタの評価順序はシーケンス番号に基づきます。サービス リストは、それぞれが許可または拒否の結果を持つ個々の文を一定の順序で並べたものです。サービス リストの評価は、事前に定義された順序でのリストのスキャンと、一致する各文の基準の評価で構成されています。リストのスキャンは、文の一致が初めて見つかり、その文に関連付けられたアクション permit または deny が実行されると停止します。リスト全体をスキャンした後のデフォルトのアクションは deny です。 （注） 前のステップで **query** オプションを使用していた場合は、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションでのみ使用できます。
ステップ 5	**match service-instance** { *LINE* } 例： `Device(config-mdns-sd-sl)## match service-instance servInst 1`	（任意）照合するサービス インスタンスを設定します。 このコマンドでは、ステップ 2 で作成されたサービス リスト名に対するパラメータが設定されます。 （注） 前のステップで **query** オプションを使用していた場合は、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションでのみ使用できます。

	コマンドまたはアクション	目的
ステップ 6	**match service-type** {*LINE* } 例： `Device(config-mdns-sd-sl)# match service-type _ipp._tcp`	（任意）照合する mDNS サービス タイプ文字列の値を設定します。 このコマンドでは、ステップ 2 で作成されたサービス リスト名に対するパラメータが設定されます。 （注） 前のステップで **query** オプションを使用していた場合は、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションでのみ使用できます。
ステップ 7	**end** 例： `Device(config-mdns-sd-sl)# end`	特権 EXEC モードに戻ります。

次の作業

mDNS ゲートウェイを有効にして、サービスの再配布に進みます。

mDNS ゲートウェイの有効化とサービスの再配布

デバイスに対して mDNS ゲートウェイをイネーブルにしたら、フィルタ（インバウンド（IN）フィルタリングまたはアウトバウンド（OUT）フィルタリングを適用）およびアクティブなクエリを、それぞれ **service-policy** コマンドと **service-policy-query** コマンドを使用して適用できます。**redistribute mdns-sd** コマンドを使用して、サービスおよびサービス アナウンスメントを再配布でき、**cache-memory-max** コマンドを使用して、システム メモリの一部をキャッシュ用に設定できます。

（注） デフォルトでは、mDNS ゲートウェイはすべてのインターフェイスでディセーブルです。

手順

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**service-routing mdns-sd** 例： `Device (config)# service-routing mdns-sd`	デバイスに対して mDNS ゲートウェイ機能をイネーブルにし、マルチキャスト DNS コンフィギュレーション（config-mdns）モードを開始します。 （注） このコマンドは、mDNS機能をグローバルに有効にします。 （注） 発信インターフェイスに何も設定されていない場合にそのIPアドレスを使用できるように、発信 mDNS パケットに代替送信元インターフェイスを指定するには、グローバル コンフィギュレーション モードまたはインターフェイス コンフィギュレーション モードで **service-routing mdns-sd source-interface** *if-name* コマンドを入力します。
ステップ 4	**service-policy** *service-policy-name* {**IN** | **OUT**} 例： `Device (config-mdns)# service-policy serv-pol1 IN`	（任意）サービス リストで、フィルタを着信サービス検出情報（インバウンド（IN）フィルタリング）または発信サービス ディスカバリ情報（アウトバウンド（OUT）フィルタリング）に対して適用します。
ステップ 5	**redistribute mdns-sd** 例： `Device (config-mdns)# redistribute mdns-sd`	（任意）サブネット全体にサービスやサービス アナウンスメントを再配布します。 （注） 再配布がグローバルに有効になっている場合は、グローバル コンフィギュレーションがインターフェイス コンフィギュレーションよりも優先順位が高くなります。
ステップ 6	**cache-memory-max** *cache-config-percentage* 例： `Device (config-mdns)# cache-memory-max 20`	（任意）システム メモリの一部を（パーセンテージ単位で）キャッシュ用に設定します。 （注） デフォルトでは、システム メモリの 10% がキャッシュ用に取り分けられます。デフォルト値は、次のコマンドを使用してオーバーライドできます。

	コマンドまたはアクション	目的
ステップ 7	**service-policy-query** *service-list-query-name service-list-query-periodicity* 例： `Device (config-mdns)# service-policy-query sl-query1 100`	（任意）サービス リスト クエリの周期性を設定します。
ステップ 8	**exit** 例： `Device (config-mdns)#exit`	（任意）グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

サービス検出ゲートウェイのモニタリング

表 *30*：サービス検出ゲートウェイのモニタリング

コマンド（Command）	目的
show mdns requests [**detail** | **name** *record-name*| **type** *record-type* [**name** *record-name*]]	このコマンドは、レコード名とレコードタイプ情報を含む、未処理の mDNS 要求についての情報を表示します。
show mdns cache [**interface** *type number* | **name** *record-name* [**type** *record-type*]| **type** *record-type*]	このコマンドにより、mDNS キャッシュ情報が表示されます。
show mdns statistics {**all** | **service-list** *list-name* | **service-policy** {**all** | **interface** *type number* }}	次のコマンドでは、mDNS の統計情報が表示されます。

設定例

例：発信 mDNS パケットに対する代替送信元インターフェイスの指定

次の例に、発信インターフェイスに何も設定されていない場合にその IP アドレスを使用できるように、発信 mDNS パケットに代替送信元インターフェイスを指定する方法を示します。

```
Device(config)# service-routing mdns-sd
Device(config-mdns)# source-interface if-name
```

例：サービス アナウンスメントの再配布

次の例に、1 つのインターフェイスで受信されたサービス アナウンスメントをすべてのインターフェイスまたは特定のインターフェイスに再配布する方法を示します。

```
Device(config)# service-routing mdns-sd
Device(config-mdns)# Redistribute mdns-sd if-name
```

例：サービスリストの作成、フィルタの適用およびパラメータの設定

以下の例は、サービス リスト sl1 の作成を示しています。**permit** コマンド オプションはシーケンス番号 3 で適用され、メッセージ タイプがアナウンスメントであるすべてのサービスがフィルタ処理され、デバイスに関連するさまざまなサブネット間で転送できるようになります。

```
Device# configure terminal
Device(config)# service-list mdns-sd sl1 permit 3
Device(config-mdns-sd-sl)#match message-type announcement
Device(config-mdns)# exit
```

例：mDNS ゲートウェイの有効化とサービスの再配布

次の例に、デバイスの mDNS ゲートウェイを有効にして、サブネット間のサービスの再配布を有効にする方法を示します。インバウンド フィルタリングは、サービス リスト serv-pol1 に適用されます。システム メモリの 20% をキャッシュに使用でき、サービス リスト クエリの周期性は 100 秒に設定されています。

```
Device# configure terminal
Device# service-routing mdns-sd
Device(config-mdns)# service-policy serv-pol1 IN
Device(config-mdns)# redistribute mdns-sd
Device(config-mdns)# cache-memory-max 20
Device(config-mdns)# service-policy-query sl-query1 100
Device(config-mdns)# exit
```

例：グローバル mDNS 設定

次に、mDNS をグローバルに設定する例を示します。

```
Device# configure terminal
Device(config)# service-list mdns-sd mypermit-all permit 10
Device(config-mdns-sd-s1)# exit
Device(config)# service-list mdns-sd querier query
Device(config-mdns-sd-s1)# service-type _dns._udp
Device(config-mdns-sd-s1)# end
Device# configure terminal
Device(config)# service-routing mdns-sd
Device(config-mdns)# service-policy mypermit-all IN
Device(config-mdns)# service-policy mypermit-all OUT
```

例：インターフェイス mDNS 設定

次に、インターフェイスに mDNS を設定する例を示します。

```
Device(config)#interface Vlan136
Device(config-if)# description *** Mgmt VLAN ***
Device(config-if)# ip address 9.7.136.10 255.255.255.0
Device(config-if)# ip helper-address 9.1.0.100
Device(config-if)# service-routing mdns-sd
Device(config-if-mdns-sd)#  service-policy mypermit-all IN
Device(config-if-mdns-sd)# service-policy mypermit-all OUT
Device(config-if-mdns-sd)#  service-policy-query querier 60
```

サービス検出ゲートウェイの設定の次の作業

次の設定を行えます。

サービス検出ゲートウェイに関する追加情報

関連資料

関連項目	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

標準および RFC

標準/RFC	役職（Title）
RFC 6763	『*DNS-Based Service Discovery*』
マルチキャストDNSインターネット（ドラフト）	マルチキャスト（Multicast）

MIB

MIB	MIB リンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

サービス検出ゲートウェイに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを

示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *31*：サービス検出ゲートウェイに関する機能情報

機能名（Feature Name）	リリース	機能情報
サービス検出ゲートウェイ	Cisco IOS XE Everest 16.5.1a	サービス検出ゲートウェイ機能により、マルチキャスト ドメイン ネーム システム（mDNS）は、レイヤ3の境界を越えて（異なるサブネットで）動作します。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

第 14 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。

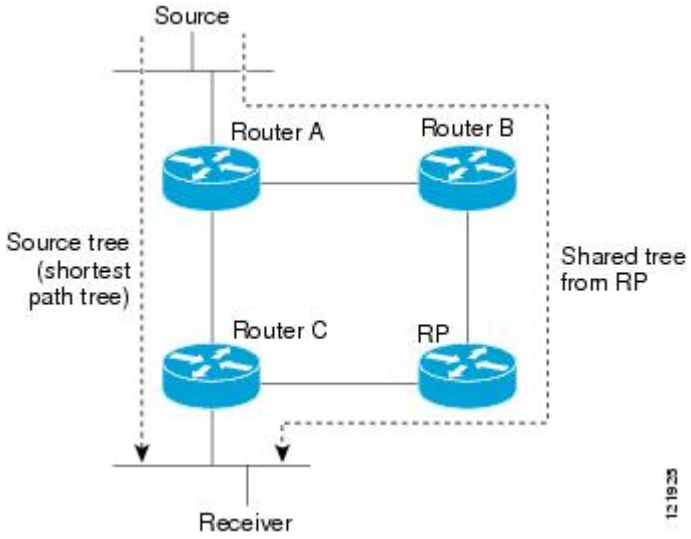
メモリ要件を減らすために最短パス ツリーの使用を回避する

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 *21*：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（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、**ippimspt-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

	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 モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `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	**ippimregister-rate-limit** レート 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。
ステップ 4	**ippimspt-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 パケットを受信したらただちに 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

	コマンドまたはアクション	目的
		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 ethernet 0`	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	**ippimquery-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** キーワードが指定されないかぎり、*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 ethernet 0
 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	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

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 モードの最適化の機能履歴と情報

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

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

表 *32*：*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 モードの最適化の機能情報

機能名（Feature Name）	リリース	機能情報
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	Cisco IOS XE Everest 16.5.1a	この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

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 モードの最適化の機能履歴と情報

第 15 章

IP マルチキャストの最適化：PIM デンス モード ステート リフレッシュ

PIM デンス モード ステート リフレッシュの前提条件

- PIM デンス モード ステート リフレッシュ機能を設定するには、その前にインターフェイス上で PIM デンス モードをイネーブルにしておく必要があります。

PIM デンス モード ステート リフレッシュの制約事項

- PIM デンス モード ネットワーク内のすべてのルータは、ステート リフレッシュ制御メッセージを処理して転送するためには、PIM デンス モード ステート リフレッシュ機能をサポートしているソフトウェア リリースを実行する必要があります。
- ステート リフレッシュ制御メッセージの発信間隔は、同じ LAN 上のすべての PIM ルータで同じである必要があります。具体的には、LAN に直接接続されている各ルータ インターフェイスに同じ発信間隔を設定する必要があります。

PIM デンス モード ステート リフレッシュについて

PIM デンス モード ステート リフレッシュの概要

PIM デンス モード ステート リフレッシュ機能は、PIM バージョン 2 マルチキャスト ルーティング アーキテクチャの拡張機能です。

PIM デンス モードは、フラッディング/プルーニング原則で動作するソース ベースのマルチキャスト配信ツリーを構築します。ソースからのマルチキャストパケットは、PIMデンスモードネットワークのすべてのエリアにフラッディングされます。マルチキャスト グループ メンバまたは PIM ネイバーに直接接続されていない PIM ルータは、マルチキャスト パケットを受信すると、ソースベースの配信ツリーをバックアップするプルーニング メッセージをパケットのソースに向けて送信します。その結果、後続のマルチキャスト パケットは、配信ツリーのプルーニング済みブランチにはフラッディングされません。ところが、PIM デンス モードでのプルーニングされたステートは、およそ 3 分間ごとにタイムアウトし、PIM デンス モード ネットワーク全体が、マルチキャスト パケットとプルーニング メッセージで再フラッディングされます。PIM デンス モード ネットワーク全体の望ましくないトラフィックの再フラッディングは、ネットワーク帯域幅を消費します。

PIM デンス モード ステート リフレッシュ機能は、定期的に制御メッセージをソース ベースの配信ツリーの下流へと転送することにより、PIM デンス モードのプルーニングされたステートをタイムアウトしないように維持します。制御メッセージによって、配信ツリー内の各ルータの発信インターフェイスのプルーニング状態が更新されます。

PIM デンス モード ステート リフレッシュの利点

PIM デンス モード ステート リフレッシュ機能は、PIM デンス モードでのプルーニングされたステートをタイムアウトしないようにします。これは、PIM デンス モード ネットワークのプルーニングされたブランチへの不要なマルチキャスト トラフィックの再フラッディングを大幅に低減することにより、ネットワーク帯域幅を節約します。また、この機能によって、PIM デンス モード マルチキャスト ネットワーク内の PIM ルータは、デフォルトの 3 分間のステート リフレッシュ タイムアウト期間の前に、トポロジの変更（マルチキャスト グループに参加する送信元またはマルチキャスト グループから脱退した送信元）を認証することができます。

PIM デンス モード ステート リフレッシュの設定方法

PIM デンス モード ステート リフレッシュの設定

PIMデンスモードステートリフレッシュ機能を有効にするための設定作業はありません。デフォルトでは、PIM デンス モード ステート リフレッシュ機能をサポートする Cisco IOS XE ソフトウェ

ア リリースを実行するすべての PIM ルータが、ステート リフレッシュ制御メッセージを自動的に処理し、転送します。

PIM ルータ上でのステート リフレッシュ制御メッセージの処理と転送をディセーブルにするには、**ip pim state-refresh disable** 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。無効になっているステート リフレッシュを再度有効にするには、**no ip pim state-refresh disable** 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。

ステート リフレッシュ制御メッセージの発生はデフォルトで無効になっています。PIM ルータ上の制御メッセージの発生を設定するには、グローバル コンフィギュレーション モードで始めて、次のコマンドを使用します。

コマンド（Command）	目的
`Router(config)#` **interface** *type number*	インターフェイスを指定し、ルータをインターフェイス コンフィギュレーション モードにします。
`Router(config-if)#` **ip pim state-refresh origination-interval** [*interval*]	PIM デンス モード ステート リフレッシュ制御メッセージの発生を設定します。必要に応じて、*interval* 引数を使用して、制御メッセージ間の秒数を設定できます。デフォルト インターバルは 60 秒です。指定できる間隔の範囲は 1 ～ 100 秒です。

PIM デンス モード ステート リフレッシュの設定

PIM デンス モード ステート リフレッシュ機能が正しく設定されているかを確認するには、**show ip pim interface** [*type number*] **detail** および **show ip pim neighbor** [*interface*] コマンドを使用します。次の **show ip pim interface** [*type number*] **detail** コマンドの出力は、ステート リフレッシュ制御メッセージの処理、転送、および発信が有効になっていることを示します。

```
Router# show ip pim interface fastethernet 0/1/0 detail
FastEthernet0/1/0 is up, line protocol is up
  Internet address is 172.16.8.1/24
  Multicast switching:process
  Multicast packets in/out:0/0
  Multicast boundary:not set
  Multicast TTL threshold:0
  PIM:enabled
    PIM version:2, mode:dense
    PIM DR:172.16.8.1 (this system)
    PIM neighbor count:0
    PIM Hello/Query interval:30 seconds
 PIM State-Refresh processing:enabled
 PIM State-Refresh origination:enabled, interval:60 seconds
    PIM NBMA mode:disabled
    PIM ATM multipoint signalling:disabled
    PIM domain border:disabled
  Multicast Tagswitching:disabled
```

次の **show ip pim neighbor** [*interface*] コマンド出力の Mode フィールドに表示されている S は、ネイバーの PIM デンス モード ステート リフレッシュ機能が設定されていることを示します。

```
Router# show ip pim neighbor
PIM Neighbor Table
Neighbor          Interface          Uptime/Expires    Ver   DR
Address                                                    Priority/Mode
172.16.5.1        Ethernet1/1        00:09:03/00:01:41 v2    1 / B S
```

PIM DM ステート リフレッシュのモニタリングと維持

以下に、**debug ip pim** 特権 EXEC コマンドをマルチキャスト グループ 239.0.0.1 に設定した後に PIM ルータで送受信される PIM デンス モード ステート リフレッシュ制御メッセージを示します。

```
Router# debug ip pim 239.0.0.1
*Mar  1 00:25:10.416:PIM:Originating refresh message for
(172.16.8.3,239.0.0.1)
*Mar  1 00:25:10.416:PIM:Send SR on GigabitEthernet1/1/0 for (172.16.8.3,239.0.0.1)
TTL=9
```

show ip mroute コマンドが表示する次の出力は、GigabitEthernet インターフェイス 1/0/0 およびマルチキャスト グループ 239.0.0.1 に得られたプルーニング タイマーの変更です。（次の出力は、**debug ip pim** 特権 EXEC コマンドがルータにすでに設定されていると仮定しています）。**show ip mroute** コマンドからの最初の出力では、プルーニング タイマーは 00:02:06 と示しています。このデバッグ メッセージは、PIM デンス モード ステート リフレッシュ制御メッセージがイーサネット インターフェイス 1/0 で送受信され、他の PIM デンス モード ステート リフレッシュ ルータが検出されたことを示します。**show ip mroute** コマンドからの 2 番目の出力では、プルーニング タイマーが 00:02:55 にリセットされています。

```
Router# show ip mroute 239.0.0.1
(172.16.8.3, 239.0.0.1), 00:09:50/00:02:06, flags:PT
  Incoming interface:GigabitEthernet1/1/0, RPF nbr 172.16.5.2
  Outgoing interface list:
 GigabitEthernet1/0/0, Prune/Dense, 00:09:43/00:02:06
Router#
*Mar  1 00:32:06.657:PIM:SR on iif from 172.16.5.2 orig 172.16.8.1 for
(172.16.8.3,239.0.0.1)
*Mar  1 00:32:06.661:     flags:prune-indicator
*Mar  1 00:32:06.661:PIM:Cached metric is [0/0]
*Mar  1 00:32:06.661:PIM:Keep RPF nbr 172.16.5.2
*Mar  1 00:32:06.661:PIM:Send SR on Ethernet1/0 for (172.16.8.3,239.0.0.1)
TTL=8
*Mar  1 00:32:06.661:     flags:prune-indicator
Router# show ip mroute 239.0.0.1
(172.16.8.3, 239.0.0.1), 00:10:01/00:02:55, flags:PT
  Incoming interface:GigabitEthernet1/1/0, RPF nbr 172.16.5.2
  Outgoing interface list:
 GigabitEthernet1/0/0, Prune/Dense, 00:09:55/00:02:55
```

PIM デンス モード ステート リフレッシュの設定例

PIM デンス モード ステート リフレッシュ制御メッセージの発信、処理、および転送の例

次に、ファストイーサネットインターフェイス 0/1/0 で PIM デンス モード ステート リフレッシュ制御メッセージを 60 秒ごとに発信、処理および転送している PIM ルータの例を示します。

```
ip multicast-routing distributed
interface FastEthernet0/1/0
 ip address 172.16.8.1 255.255.255.0
 ip pim state-refresh origination-interval 60
 ip pim dense-mode
```

PIM デンス モード ステート リフレッシュ制御メッセージの処理および転送の例

次に、ファストイーサネットインターフェイス 1/1/0 で PIM デンス モード ステート リフレッシュ制御メッセージを処理および転送しているだけの PIM ルータの例を示します。

```
ip multicast-routing
interface FastEthernet1/1/0
 ip address 172.16.7.3 255.255.255.0
 ip pim dense-mode
```

IP マルチキャストの最適化：PIM デンス モード ステート リフレッシュに関するその他の関連資料

関連資料

関連項目	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IP マルチキャストの最適化：PIM デンス モード ステート リフレッシュの機能情報

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

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

表 *33*：*IP* マルチキャストの最適化：*PIM* デンス モード ステート リフレッシュの機能情報

機能名（Feature Name）	リリース	機能情報
IP マルチキャストの最適化：PIM デンス モード ステート リフレッシュ	Cisco IOS XE Everest 16.5.1a	PIM デンス モード ステート リフレッシュ機能は、PIM バージョン2マルチキャスト ルーティング アーキテクチャの拡張機能です。PIM デンス モードは、フラッディング/プルーニング原則で動作するソース ベースのマルチキャスト配信ツリーを構築します。ソースからのマルチキャスト パケットは、PIM デンス モード ネットワークのすべてのエリアにフラッディングされます。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

第 16 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

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

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 プロバイダーは、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（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（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 プロバイダー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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**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。

	コマンドまたはアクション	目的
ステップ 4	**ippimquery-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

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードをイネーブルにします。

- プロンプトが表示されたら、パスワードを入力します。

ステップ 2 **showippiminterface** *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、**showippiminterface** 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 **showippimneighbor**

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、**showippimneighbor** 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 gigabitethernet0/0/1
 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	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

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 リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *34*：*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

機能名（Feature Name）	リリース	機能情報
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	Cisco IOS XE Everest 16.5.1a	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（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。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

第 17 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: 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。

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

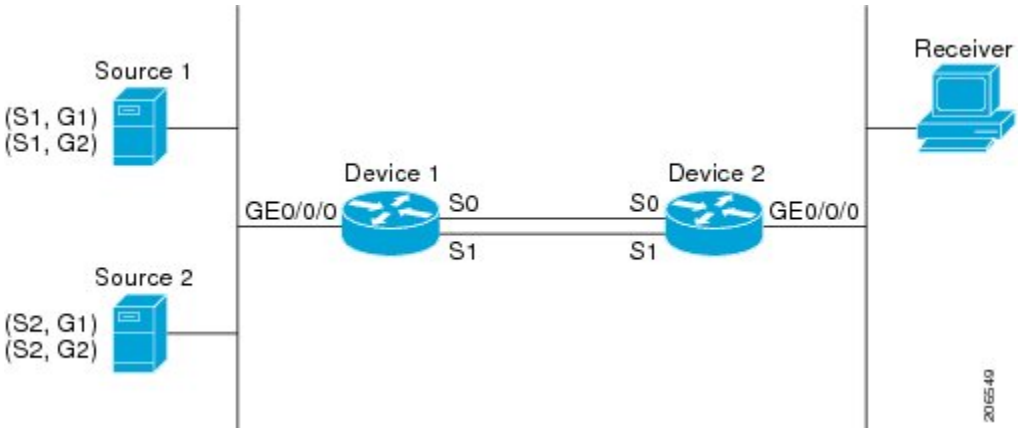
デフォルトでは、Protocol Independent Multicast スパース モード（PIM-SM）、Source Specific Multicast（PIM-SSM）、双方向 PIM（Bidir-PIM）、および PIM デンス モード（PIM-DM）グループについては、複数の等コスト パスが使用可能な場合、リバース パス転送（RPF）for IPv4 マルチキャスト トラフィックは、最も大きい IP アドレスを持つ PIM ネイバーに基づきます。この方法は、最高 PIM ネイバー動作と呼ばれます。この動作は、PIM-SM の RFC 2362 に基づいていますが、PIM-SSM、PIM-DM、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。

（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 *22*：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 のいずれかが、このトポロジに使用できます。PIM-SM が使用される場合は、**ippimspt-threshold** コマンドのデフォルト 0 がデバイス 2 で使用中で、内部ゲートウェイ プロトコル（IGP）が実行中で、S1 および S2 向け（デバイス 2 で入力された場合）の **showiproute** コマンドの出力に、デバイス 1 でのシリアル インターフェイス 0 およびシリアル 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と仮定します。

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。PIM-DM の場合は、デバイス 2 は、常に IP マルチキャスト トラフィックをシリアル インターフェイス 1 上で受信し、その場合にだけ、PIM 加入メッセージが PIM-DM で使用されず、代わりにデバイス 2 はシリアル インターフェイス 0 を通る IP マルチキャスト トラフィックをプルーニングし、それをシリアル インターフェイス 1 を通じて受信します。これは、デバイス 1 上ではシリアル インターフェイス 1 が最も大きい IP アドレスを持つためです。

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 および PIM-DM）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 スプリットの発信元アドレスに基づいた方法：**ipmulticastmultipath** コマンドにを使用して、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 **ipmulticastmultipath** コマンドを入力すると、S ハッシュ アルゴリズムを使用する、発信元アドレスに基づいた 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、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，（371 ページ）」の項を参照してください。
- ECMP マルチキャスト ロード スプリットのソースおよびグループ アドレスに基づいた方法：**ipmulticastmultipath** 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 **ipmulticastmultipath** 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する、ソースとグループ アドレスに基づいた ECMP マルチキャスト ロード ス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、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，（372 ページ）」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 アドレスに基づいた方法：**ipmulticastmultipath** 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、「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，（374 ページ）」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 ホップは **showippimneighbor** コマンドの出力に表示された場合に PIM ネイバーとみなされます。これは、それからの PIM のハロー メッセージが受信され、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

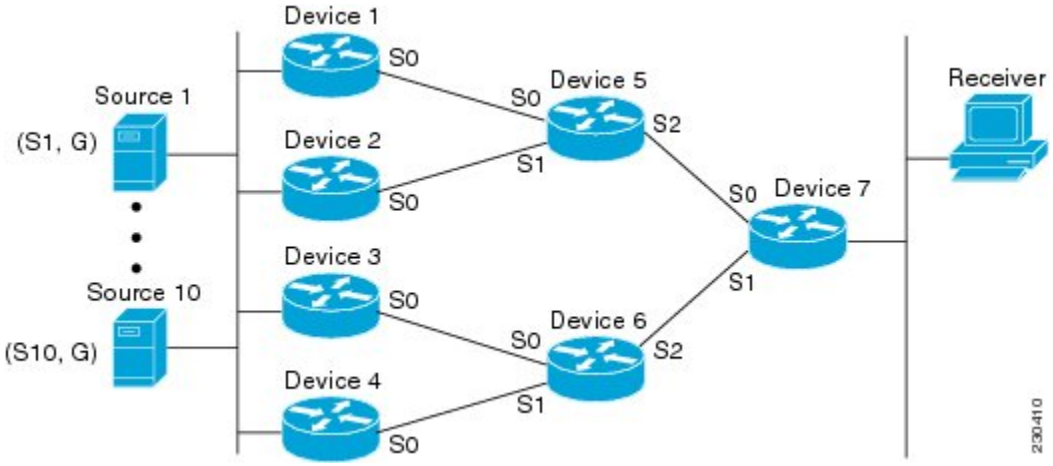
ソース アドレスまたはソースおよびグループ アドレスによってマルチキャスト トラフィックをロード スプリットするために IPv4 マルチキャストで使用されるハッシュ機能には通常、局在化と呼ばれる問題があります。ソース アドレスまたはソースおよびグループ アドレスに基づく ECMP マルチキャスト ロード スプリットの副産物として、局在化は、一部のトポロジ内のルータがロード スプリットに使用可能なすべてのパスを効果的に使用できないという問題です。

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（ルータやコントローラ）を使用できます。

（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 *23*：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、ECMP マルチキャスト ロード スプリッティングが **ipmulticastmultipath** コマンドを使用してトポロジ内のすべてのルータで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

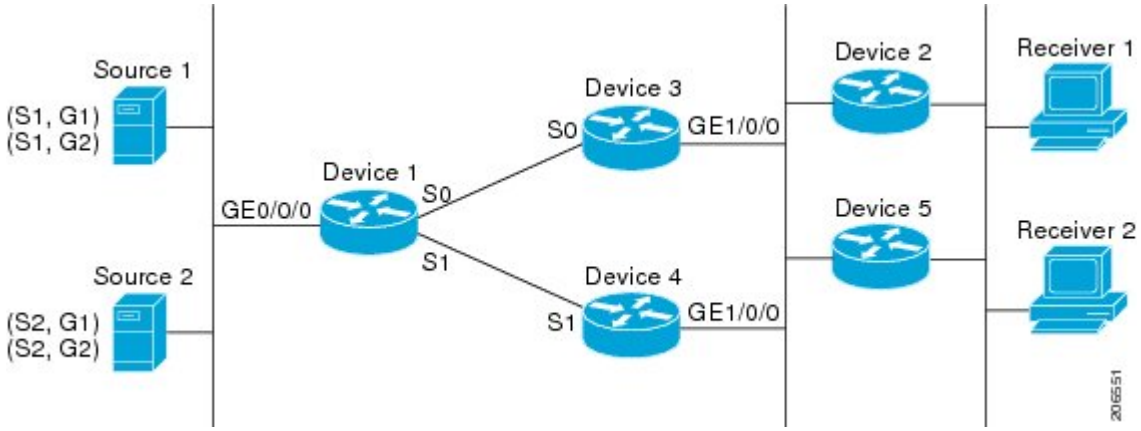
PIM-SM を (*, G) または (S, G) 転送で使用していた場合、または PIM-SSM を (S, G) 転送で使用していた場合でも、PIM アサート処理が発生したことが原因で **ipmulticastmultipath** コマンドでの ECMP マルチキャスト ロード スプリットが有効でなくなる場合もあります。

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。

（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 *24*：*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、**ipmulticastmultipath** 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 **ipmulticastmultipath** 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。

ipmulticastmultipath コマンドでロード スプリッティングを設定すると、システムは、S ハッシュ アルゴリズムを使用して、ソースアドレスに基づいて、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。**ipmulticastmultipath** 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、ソース 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） **ipmulticastmultipath** 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、**showiproute** 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、**showiprpf** コマンドを使用して、ソースが 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, （377 ページ）」の項を参照してください。

制限事項

- 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。
- **ipmulticastmultipath** 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。**ipmulticastmultipath** コマンドを設定する場合は、すべてのインターフェイスに異なる IP アドレスを使用してください。
- **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。

はじめる前に

- 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、**showiproute** 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、**showiprpf** コマンドを使用して、ソースが 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, （377 ページ）」の項を参照してください。

手順

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

	コマンドまたはアクション	目的
ステップ 2	**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	**ipmulticastmultipath** 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	**showiprpf** *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	**showiproute** *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 サーバや MPEG ビデオ サーバ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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipmulticastmultipath 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	**showiprpf** *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。
ステップ 7	**showiproute** *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。

	コマンドまたはアクション	目的
		• *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 サーバや MPEG ビデオサーバ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

	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 モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `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。

	コマンドまたはアクション	目的
ステップ 3	**ipmulticastmultipath s-g-hashnext-hop-based** 例： `Router(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レシーバ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： `Router(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	**showiprpf** *source-address* [*group-address*] 例： `Router# 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。
ステップ 7	**showiproute** *ip-address* 例： `Router# 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

	コマンドまたはアクション	目的
		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
```

その他の参考資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』

標準および RFC

標準/RFC	役職（Title）
RFC 4601	『Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification』

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS XE Release、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

テクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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

ECMP を介した IP マルチキャスト トラフィックのロード スプリットの機能履歴と情報

リリース	変更箇所
Cisco IOS XE Everest 16.5.1a	この機能が導入されました。

第 18 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 フィルタリング機能について

マルチキャスト境界のルール

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。

次のルールで、**ipmulticastboundary** 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 in 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

マルチキャスト境界の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。
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	**ipaccess-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	**ipmulticastboundary** *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

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 181.1.2.3.303 host 232.1.1.1
 interface gigabitethernet 2/3/0
 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 2/3/0
 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 2/3/0
 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	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Product Alert Tool（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

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 フィルタリングの機能情報

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

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

表 *35*：*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 フィルタリングの機能情報

機能名（Feature Name）	リリース	機能情報
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	Cisco IOS XE Everest 16.5.1a	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。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

第 19 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

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

IGMP ステート リミッタの設定

（注） 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

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

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipigmplimit** *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	**showipigmpgroups** 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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	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 GigabitEthernet0/0`	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	**ipigmplimit** *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	**showipigmpinterface** [*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	**showipigmpgroups** 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

IGMP ステート リミッタの設定例

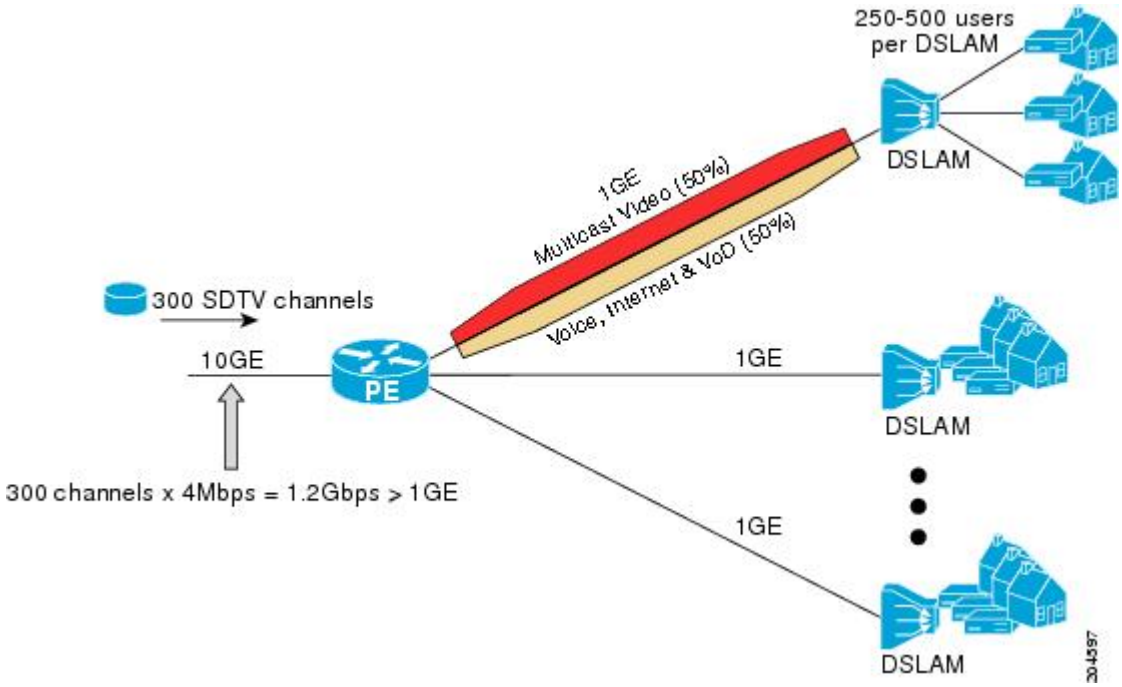
次の例は、すべてのマルチキャスト フローがほぼ同量の帯域幅を使用するネットワーク環境でマルチキャスト CAC を提供するために、IGMP ステート リミッタを設定する方法を示します。

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（ルータやコントローラ）を使用できます。

（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 *25*：*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	参照先
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 ルーティングのコマンド」の項を参照してください。
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS XE Release、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

テクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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

IP マルチキャストの最適化：IGMP ステート制限の機能情報

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

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

表 *36*：*IP* マルチキャストの最適化：*IGMP* ステート制限の機能情報

機能名（Feature Name）	リリース	機能情報
IP マルチキャストの最適化：IGMP ステート制限	Cisco IOS XE Everest 16.5.1a	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。 この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 9300 シリーズ スイッチ

通告

Trademarks