CHAPTER 49

IP マルチキャスト ルーティングの設定

この章では、IE 3000 スイッチに IP マルチキャスト ルーティングを設定する方法について説明します。IP マルチキャスティングは、ネットワーク リソースをより効率的に使用する方法です。特にオーディオやビデオなどの帯域幅を集中的に使用するサービスに対して効果があります。IP マルチキャスト ルーティングにより、ホスト（送信元）は、IP *マルチキャスト グループ アドレス*と呼ばれる IP アドレスの特殊な形式を使用して、IP ネットワーク内の任意の場所にあるホストのグループ（レシーバー）へのパケットの送信をイネーブルにします。送信ホストは、マルチキャスト グループ アドレスをそのパケットの IP 宛先アドレス フィールドに挿入し、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、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。ホストがグループのメンバーであるかどうかにかかわらず、すべてのホストをグループへ送信できます。ただし、そのメッセージを受信できるのはグループのメンバーだけです。

IP マルチキャスト ルーティング機能を使用するには、スイッチが IP サービス イメージを実行している必要があります。

（注） この章で使用しているコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*』を参照してください。

この章で説明する内容は、次のとおりです。

Multicast Source Discovery Protocol（MSDP）を設定する方法の詳細については、第 50 章「MSDP の設定」を参照してください。

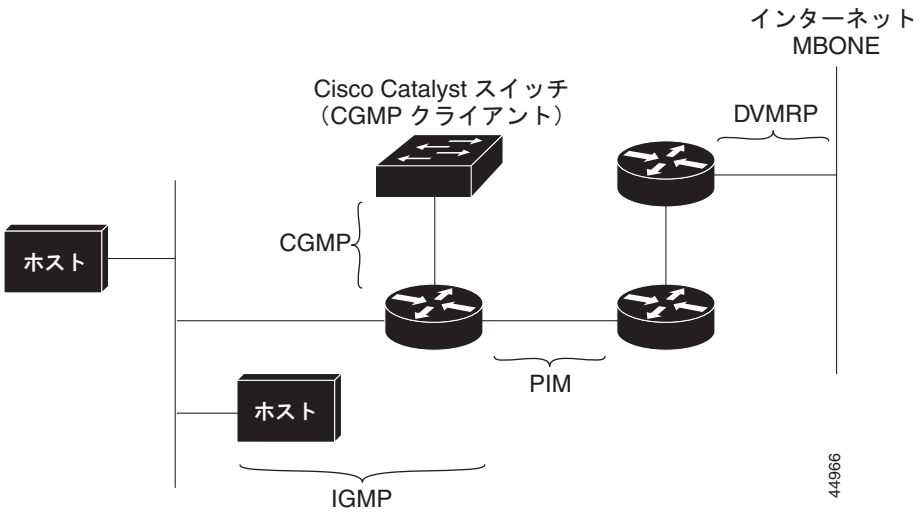
シスコの IP マルチキャスト ルーティング実装の概要

Cisco IOS ソフトウェアは、IP マルチキャスト ルーティングを実装するために次のプロトコルをサポートしています。

- Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）は、LAN 上のホストとその LAN 上のルータ（およびマルチレイヤ スイッチ）間で使用され、ホストがメンバーとして属するマルチキャスト グループを追跡します。
- Protocol-Independent Multicast（PIM）プロトコルは、ルータとマルチレイヤ スイッチ間で使用され、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た LAN に転送されるマルチキャスト パケットを追跡します。
- Distance Vector Multicast Routing Protocol（DVMRP）は、インターネットのマルチキャスト バックボーン（MBONE）で使用されます。PIM と DVMRP の連携がサポートされています。
- Cisco Group Management Protocol（CGMP）は、レイヤ 2 Catalyst スイッチに接続された Cisco ルータおよびマルチレイヤ スイッチで使用され、IGMP で実行される作業と同様の作業を実行します。

図 49-1 に、これらのプロトコルが IP マルチキャスト環境内で動作する場所を示します。

図 49-1　IP マルチキャスト ルーティング プロトコル



IPv4 マルチキャスト標準に従い、MAC 宛先マルチキャスト アドレスは 0100:5e で始まり、IP アドレスの末尾の 23 ビットが追加されます。Catalyst 3560 スイッチでは、スイッチのマルチキャスト アドレスに一致しないマルチキャスト パケットは、次のように処理されます。

- マルチキャスト IP アドレスおよびユニキャスト MAC アドレスを含むパケットである場合は、ソフトウェアで転送されます。これは、レガシー装置上の一部のプロトコルがマルチキャスト IP アドレスとユニキャスト MAC アドレスを併用するために発生することがあります。
- マルチキャスト IP アドレスおよび一致しない MAC アドレスを含むパケットである場合は、廃棄されます。

ここでは、次の内容について説明します。

- 「IGMP の概要」（P.49-3）
- 「PIM の概要」（P.49-4）
- 「DVMRP の概要」（P.49-9）
- 「CGMP の概要」（P.49-10）

IGMP の概要

IP マルチキャスティングに参加するには、マルチキャスト ホスト、ルータ、およびマルチレイヤ スイッチで IGMP が動作している必要があります。このプロトコルは、クエリアおよびホストの役割を定義します。

- クエリアは、指定されたマルチキャスト グループのメンバーであるネットワーク装置を検出するためのクエリー メッセージを送信するネットワーク装置です。
- 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ーです。

同じ送信元からマルチキャスト データ ストリームを受信する一連のクエリアおよびホストは、マルチキャスト グループと呼ばれます。クエリアおよびホストは、IGMP メッセージを使用して、マルチキャスト グループに加入したりそこから脱退したりします。

ホストがグループのメンバーであるかどうかにかかわらず、すべてのホストをグループへ送信できます。ただし、そのメッセージを受信できるのはグループのメンバーだけです。マルチキャスト グループのメンバーシップはダイナミックです。ホストはいつでも加入および脱退できます。マルチキャスト グループの場所またはメンバー数に制限はありません。ホストは一度に複数のマルチキャストのメンバーになることができます。マルチキャスト グループのアクティブ状態および所属メンバーは、グループや時間によって異なります。マルチキャスト グループは、長時間、またはごく短時間アクティブにすることもできます。グループのメンバーシップはいつでも変更可能です。メンバーを含むグループにアクティビティがない場合もあります。

IP マルチキャスト トラフィックは、グループ アドレス（クラス D アドレス）を使用します。クラス D アドレスの上位ビットは 1110 です。したがって、ホスト グループ アドレスは 224.0.0.0 ～ 239.255.255.255 の範囲になります。224.0.0.0 ～ 224.0.0.255 の範囲にあるマルチキャスト 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、次の IP マルチキャスト グループ アドレスを使用して送信されます。

- IGMP の一般的なクエリーは、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、スイッチのクエリー対象となるグループ 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、スイッチのレポート対象となるグループ IP アドレスを宛先とします。
- IGMP バージョン 2（IGMPv2）Leave 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マルチキャスト ルータ）を宛先とします。古いホスト IP スタックでは、Leave メッセージの宛先がすべてのルータのアドレスでなく、グループ IP アドレスである場合があります。

IGMP バージョン 1

IGMP バージョン 1（IGMPv 1）では主に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 スイッチは、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 つ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 グループに加入したりそこから脱退したりできます。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

IGMPv2 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、脱退の待ち時間を短縮し、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、IGMPv2 では、この作業を実行する際に、マルチキャスト プロトコルに依存することなく IGMP クエリアを選定する機能がルータに追加されています。詳細については、RFC 2236 を参照してください。

PIM の概要

PIM は*プロトコル独立型*マルチキャストと呼ばれます。ユニキャスト ルーティング テーブルを読み込むために使用されるユニキャスト ルーティング プロトコルに関係なく、PIM は、マルチキャスト ルーティング テーブルを個別に維持せずに、この情報を使用してマルチキャスト転送を実行します。

PIM は、RFC 2362『*Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*』で定義されています。PIM は次の Internet Engineering Task Force（IETF）インターネット ドラフトに定義されています。

- 『*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*』

PIM のバージョン

PIMv2 では、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 Rendezvous Point（RP; ランデブー ポイント）を持つアクティブな RP が 1 つ存在します。この単一の RP は、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等の処理を行います。
- Bootstrap Router（BSR; ブートストラップ ルータ）は、フォールトトレラントな自動化された RP 検出と配信メカニズムを提供します。このメカニズムにより、ルータおよびマルチレイヤ スイッチは、グループ /RP マッピングをダイナミックに学習できます。
- sparse（疎）モードおよび dense（密）モードは、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。sparse（疎）モードまたは dense（密）モードのいずれか一方だけでなく、sparse-dense モードを使用することを強く推奨します。
- PIM の Join メッセージおよびプルーニング メッセージを使用すると、複数のアドレス ファミリを柔軟に符号化できます。
- 現在は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 への登録メッセージが境界ルータによって送信されるか、指定ルータによって送信されるかどうかは、メッセージ自身によって指定されます。
- PIM パケットは IGMP パケット内に格納されず、スタンドアロンのパケットとして処理されます。

PIM のモード

PIM は Dense Mode（DM; dense（密）モード）、Sparse Mode（SM; sparse（疎）モード）、または sparse-dense モード（PIM SM-DM）のいずれかのモードで動作します。PIM DM-SM では、sparse（疎）グループと dense（密）グループの両方が同時に処理されます。

PIM DM

PIM DM では、送信元ベースのマルチキャスト分散ツリーが構築されます。dense（密）モードの場合、PIM DM のルータまたはマルチレイヤ スイッチは、他のすべてのルータまたはマルチレイヤ スイッチでグループ宛てのマルチキャスト パケットが転送されると想定しています。直接接続されたメンバーまたは PIM ネイバーが存在しない場合、PIM DM 装置がマルチキャスト パケットを受信すると、プルーニング メッセージが送信元に返送され、不要なマルチキャスト トラフィックが停止します。このプルーニング済みブランチ上のこのルータまたはスイッチでは、後続のマルチキャスト パケットがフラッディングしません。レシーバーを含まないブランチが分散ツリーからプルーニングされ、レシーバーを含むブランチだけが残るためです。

事前にプルーニングされたツリー内ブランチのレシーバーがマルチキャスト グループに新規に加入すると、PIM DM 装置は新しいレシーバーを検出し、接合メッセージをただちに送信元に向けて分散ツリーの上方向に送信します。アップストリームの PIM DM 装置が接合メッセージを受信すると、この装置は接合メッセージを受信したインターフェイスをただちにフォワーディング ステートにし、レシーバーへのマルチキャスト トラフィックの転送を開始します。

PIM SM

PIM SM は共有ツリーおよび Shortest-Path-Tree（SPT）を使用し、マルチキャスト トラフィックをネットワーク内のマルチキャスト レシーバーに配布します。PIM SM の場合、ルータまたはマルチレイヤ スイッチは、トラフィックに関する明示的な要求（Join メッセージ）がない限り、他のルータまたはスイッチではグループ宛てのパケットが転送されないことを想定しています。ホストが IGMP を使用してマルチキャスト グループに加入すると、直接接続された PIM SM 装置は、RP と呼ばれるルートに向けて PIM Join メッセージを送信します。この Join メッセージはルートに向かってルータを順次移動しながら、共有ツリーのブランチを作成します。

RP はマルチキャスト レシーバーを追跡します。また、送信元のファーストホップ ルータである *Designated Router*（DR; 指定ルータ）から受信した登録メッセージを使用して送信元を登録し、送信元からレシーバーへの共有ツリー パスを完成させます。共有ツリーを使用する場合、送信元は RP にトラフィックを送信することで、これらのトラフィックをすべてのレシーバーに到達させるようにする必要があります。

マルチキャスト グループ トラフィックをプルーニングする場合は、プルーニング メッセージが分散ツリーの上方向に送信されます。この結果、明示的な Join メッセージによって作成された共有ツリーまたは SPT のブランチが不要になった場合、これらを解除することが可能となります。

PIM スタブ ルーティング

PIM スタブ ルーティング機能は、ルーテッド トラフィックをエンド ユーザにより近い場所に移動することでリソース使用量を削減します。

PIM スタブ ルーティングを使用するネットワークでは、ユーザに対して許容される IP トラフィックのルートは、PIM スタブ ルーティングで設定されたスイッチを介したルートだけです。PIM 受動インターフェイスは、VLAN のようなレイヤ 2 アクセス ドメインに接続したり、その他のレイヤ 2 装置に接続されたインターフェイスに接続しています。レイヤ 2 アクセス ドメインでは、直接接続されたマルチキャスト（IGMP）レシーバーと送信元だけが許可されています。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することはありません。

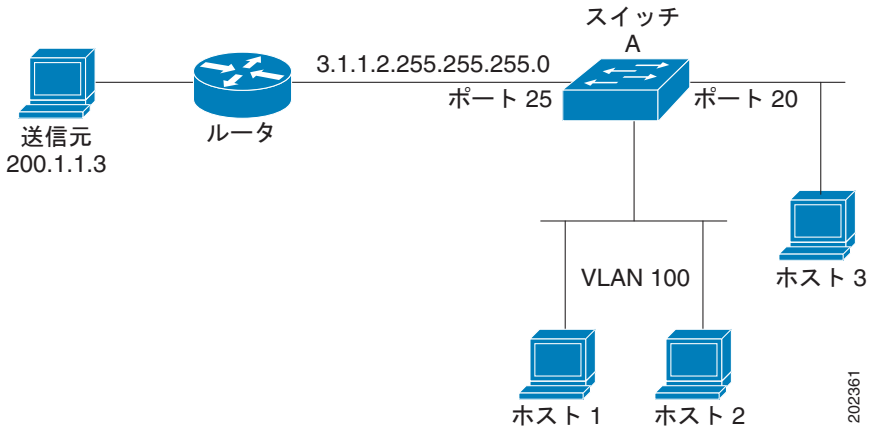
PIM スタブ ルーティングを使用する場合、ディストリビューション ルータとリモート ルータが IP マルチキャスト ルーティングを使用できるように設定し、PIM スタブ ルータとして機能するものがスイッチだけになるように設定する必要があります。スイッチは、ディストリビューション ルータ間の中継トラフィックのルーティングを行いません。また、スイッチにはルーテッド アップリンク ポートを設定する必要があります。スイッチのアップリンク ポートは Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）と併用することができません。SVI アップリンク ポートで PIM が必要な場合は、IP サービス フィーチャ セットにアップグレードする必要があります。

また、スイッチに PIM スタブ ルーティングを設定する場合は、Enhanced Interior Gateway Routing Protocol（EIGRP）スタブ ルーティングを設定する必要もあります。詳細については、「EIGRP スタブ ルーティングの設定」（P.41-41）を参照してください。

冗長 PIM スタブ ルータのトポロジはサポートされません。冗長トポロジは、マルチキャスト トラフィックを 1 つのアクセス ドメインに転送している PIM ルータが複数ある場合に存在します。PIM メッセージはブロックされ、PIM アセットと指定ルータ選定メカニズムは 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 トポロジだけがサポートされます。非冗長トポロジを使用すると、PIM 受動インターフェイスは、非冗長トポロジをそのアクセス ドメイン上の唯一のインターフェイスおよび指定ルータであると想定します。

図 49-2 では、スイッチ A のルーテッド アップリンク ポート 25 がルータに接続し、PIM スタブ ルーティングが VLAN 100 インターフェイスとホスト 3 でイネーブルになっています。このように設定することで、直接接続されているホストがマルチキャストの送信元である 200.1.1.3 からトラフィックを受信できます。詳細については、「PIM スタブ ルーティングの設定」（P.49-23）を参照してください。

図 49-2　PIM スタブ ルータの設定



IGMP ヘルパー

PIM スタブ ルーティングは、ルーテッド トラフィックをエンド ユーザにより近い場所に移動し、ネットワーク トラフィックを削減します。また、IGMP ヘルパー機能を使用してスタブ ルータ（スイッチ）を設定することで、トラフィックを削減することもできます。

スタブ ルータ（スイッチ）を **igmp helper help-address** インターフェイス コンフィギュレーション コマンドで設定することにより、スイッチはネクストホップ インターフェイスにレポートを送信できます。これにより、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 ネットワークを送信元とするマルチキャスト グループに加入できます。この機能が設定されると、マルチキャスト ストリームへの加入を待機しているホストからの IGMP パケットは、アップストリームからネクストホップ装置へ転送されます。アップストリームのセントラル ルータがヘルパー IGMP のレポートを受信した場合または脱退した場合、ルータはそのグループの発信インターフェイスのリストで、インターフェイスの追加または削除を行います。

ip igmp helper-address コマンドの構文と使用方法の詳細については、『*Cisco IOS IP and IP Routing Command Reference, Release 12.1*』を参照してください。

Auto-RP

この独自の機能により、ネットワーク内のルータまたはマルチレイヤ スイッチごとに RP 情報を手動で設定する必要がなくなります。Auto-RP を機能させるには、Cisco ルータまたはマルチレイヤ スイッチをマッピング エージェントとして設定します。マッピング エージェントは IP マルチキャストを使用して、候補 RP アナウンスを受信する候補 RP として設定可能なネットワーク内のルータまたはスイッチを取得します。候補 RP はマルチキャスト RP アナウンス メッセージを特定のグループまたはグループ範囲に定期的に送信し、それらのアベイラビリティをアナウンスします。

マッピング エージェントはこれらの候補 RP アナウンスを待ち受け、この情報を使用して、グループ/RP マッピング キャッシュにエントリを作成します。受信されたグループ/RP 範囲に対して複数の候補 RP が RP アナウンスを送信した場合でも、この範囲にはマッピング キャッシュ エントリが 1 つだけ作成されます。RP アナウンス メッセージ着信時に、マッピング エージェントは最大の IP アドレスを持つルータまたはスイッチをアクティブ RP として選択し、この RP アドレスをグループ/RP マッピング キャッシュ内に保存します。

マッピング エージェントは、グループ/RP マッピング キャッシュの内容を定期的にマルチキャストします。このため、すべてのルータおよびスイッチで、サポート対象のグループに使用される RP が自動的に検出されます。ルータまたはスイッチが RP ディスカバリ メッセージの受信に失敗し、グループ/RP マッピング情報が期限切れになると、ルータまたはスイッチは、**ip pim rp-address** グローバル コンフィギュレーション コマンドによって定義された、スタティックに設定された RP に変更されます。スタティックに設定された RP が存在しない場合、ルータまたはスイッチはグループの動作を dense（密）モードに変更します。

複数の RP がさまざまなグループ範囲として、または相互にホット バックアップとして機能します。

ブートストラップ ルータ

PIMv2 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 スイッチに配信するもう 1 つの方法です。これにより、ネットワーク内のルータまたはスイッチごとに RP 情報を手動で設定する必要がなくなります。ただし、BSR は IP マルチキャストを使用してグループ/RP マッピング情報を配布する代わりに、特殊な BSR メッセージのホップバイホップのフラッディングを使用してマッピング情報を配布します。

BSR は、BSR として機能するように設定されたドメイン内の一連の候補ルータおよびスイッチから選定されます。選定メカニズムは、ブリッジ接続された LAN で使用されるルートブリッジ選定メカニズムと類似しています。BSR の選定は、ネットワークを経由してホップバイホップで送信される BSR メッセージに含まれている装置の BSR プライオリティに基づいて行われます。各 BSR 装置は BSR メッセージを調べ、BSR プライオリティが自身の BSR プライオリティと同等またはそれ以上で、BSR IP アドレスが大きいメッセージだけを、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 が選定されます。

選定された BSR によって、Time to Live（TTL）値が 1 である BSR メッセージが送信されます。ネイバー PIMv2 ルータまたはマルチレイヤ スイッチは 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。このように、BSR メッセージは PIM ドメイン内をホップバイホップで移動します。BSR メッセージには現在の BSR の IP アドレスが含まれているため、候補 RP はフラッディング メカニズムを使用し、どの装置が選定された 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 装置に、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バイホップで移動し、すべてのルータおよびスイッチに送信されます。BSR メッセージ内の RP 情報は、到達したルータおよびスイッチのローカルな RP キャッシュに格納されます。すべてのルータおよびスイッチには一般的な RP ハッシュ アルゴリズムが使用されるため、指定されたグループには同じ RP が選択されます。

マルチキャスト転送およびリバース パス チェック

ユニキャスト ルーティングの場合、ルータおよびマルチレイヤ スイッチは、送信元から IP パケットの宛先アドレス フィールドに IP アドレスが表示されている宛先ホストへ、ネットワーク内の単一のパスに沿ってトラフィックを転送します。パス上の各ルータおよびスイッチは、ユニキャスト ルーティング テーブル内の宛先アドレスを参照し、指定されたインターフェイスを経由して宛先方向のネクストホップへパケットを転送してから、パケット内の宛先 IP アドレスを使用してユニキャスト フォワーディングを判断します。

マルチキャスティングの場合、送信元は IP パケットの宛先アドレス フィールドに表示された、マルチキャスト グループ アドレスで表されるホストの任意のグループにトラフィックを送信します。着信マルチキャスト パケットの転送または廃棄を決定するため、ルータまたはマルチレイヤ スイッチで、パケットに対する Reverse Path Forwarding（RPF）チェックを実行します（図 49-3 を参照）。

1. ルータまたはマルチレイヤ スイッチは着信したマルチキャスト パケットの送信元アドレスを調べ、リバース パス上のインターフェイスに着信したパケットを送信元に戻すかどうかを決定します。
2. パケットが送信元に逆戻りするインターフェイスに着信した場合、RPF チェックは成功し、発信インターフェイス リスト内のすべてのインターフェイス（ルータのすべてのインターフェイスとは限らない）にパケットが転送されます。
3. RPF チェックに失敗した場合、パケットは廃棄されます。

DVMRP などの一部のマルチキャスト ルーティング プロトコルでは、マルチキャスト ルーティング テーブルは個別に維持され、RPF チェックに使用されます。ただし、PIM では RPF チェックを実行するためにユニキャスト ルーティング テーブルが使用されます。

図 49-3 に、送信元 151.10.3.21 からのマルチキャスト パケットを受信するポート 2 を示します。表 49-1 に、送信元へのリバース パス上にあるポートはポート 2 ではなく、ポート 1 であることを示します。RPF チェックに失敗したため、マルチレイヤ スイッチはパケットを廃棄します。送信元 151.10.3.21 からの別のマルチキャスト パケットは、ポート 1 に受信します。ルーティング テーブルには、このポートが送信元へのリバース パス上にあることが示されています。RPF チェックに合格したため、スイッチはパケットを発信ポート リスト内のすべてのポートに転送します。

図 49-3　　RPF チェック

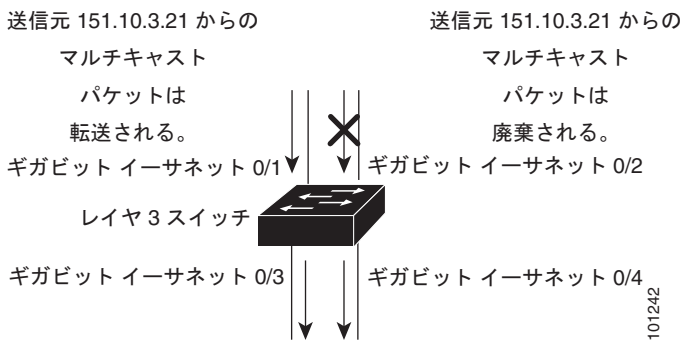


表 49-1　RPF チェックのルーティング テーブル例

ネットワーク	Port
151.10.0.0/16	ギガビット イーサネット 0/1
198.14.32.0/32	ギガビット イーサネット 0/3
204.1.16.0/24	ギガビット イーサネット 0/4

PIM は送信元ツリーと RP でルーティングされた共有ツリーの両方を使用して、データグラムを転送します（「PIM DM」（P.49-5）および「PIM SM」（P.49-5）を参照）。RPF チェックは、それぞれ異なる方法で実行されます。

- PIM ルータまたはマルチレイヤ スイッチが送信元ツリー ステートである場合（つまり（S,G）エントリがマルチキャスト ルーティング テーブル内にある場合）、マルチキャスト パケットの送信元の IP アドレスに対して RPF チェックが実行されます。
- PIM ルータまたはマルチレイヤ スイッチが共有ツリー ステートである場合（および明示的な送信元ツリー ステートがない場合）、（メンバーがグループに加入している場合は既知である）RP アドレスについて RPF チェックが実行されます。

PIM sparse（疎）モードは RPF 検索機能を使用し、加入およびプルーニング メッセージを送信する必要があるかどうかを決定します。

- （S,G）Join メッセージ（送信元ツリー ステート）は送信元に向けて送信されます。
- （*,G）Join メッセージ（共有ツリー ステート）は RP に向けて送信されます。

DVMRP と PIM dense（密）モードでは送信元ツリーだけが使用され、前述の RPF が使用されます。

DVMRP の概要

DVMRP は多くのベンダーの装置に実装されており、パブリック ドメインのマルチキャスト ルーティングされたプログラムに基づいて動作します。このプロトコルは MBONE、およびその他のドメイン内マルチキャスト ネットワークに導入されています。

Cisco ルータおよびマルチレイヤ スイッチでは PIM が実行されているため、DVMRP ネイバーへのマルチキャスト パケットの 転送、および DVMRP ネイバーからのマルチキャスト パケットの受信が可能です。DVMRP ルートを PIM クラウド内に伝播したり、PIM クラウドを経由して伝播することもできます。ソフトウェアは DVMRP ルートを伝播し、ルータやマルチレイヤ スイッチごとにこれらのルートのデータベースを個別に構築します。ただし、PIM はこのルーティング情報をパケット転送の判断に使用します。ソフトウェアに完全な DVMRP は実装されていません。ただし、DVMRP ルータのダイナミック検出をサポートし、従来のメディア（イーサネットや Fiber Distributed Data Interface（FDDI; ファイバ分散データ インターフェイス）など）または DVMRP 固有のトンネルを通して、これらを相互運用します。

DVMRP ネイバーは、ルートレポート メッセージの送信元ネットワーク ルーティング情報を定期的に交換することで、ルート テーブルを構築します。DVMRP ルーティング テーブルに格納されているルーティング情報は、ユニキャスト ルーティング テーブルから独立し、送信元分散ツリーの構築や、RPF を使用したマルチキャスト転送の実行に使用されます。

DVMRP は dense（密）モード プロトコルであり、抑制されたマルチキャスト モデルを使用して親子データベースを構築し、マルチキャスト パケットの送信元でルーティングされた転送ツリーを構築します。マルチキャスト パケットは、最初にこの送信元ツリーの下方向にフラッディングされます。冗長パスが送信元ツリー上にある場合、パケットはこれらのパスに沿って転送されません。これらの親子リンクでプルーニング メッセージが受信されるまで転送が行われ、これによってマルチキャスト パケットのブロードキャストが抑制されます。

CGMP の概要

このソフトウェア リリースは、スイッチで CGMP サーバ サポート機能を提供しています。クライアント側の機能は提供されません。スイッチは、IGMP スヌーピングをサポートしない、CGMP クライアント機能が組み込まれている装置用の CGMP サーバとして機能します。

CGMP は、レイヤ 2 Catalyst スイッチに接続された Cisco ルータおよびマルチレイヤ スイッチで使用されるプロトコルであり、IGMP で実行される作業と同様の作業を実行します。CGMP を使用すると、レイヤ 2 グループ メンバーシップ情報を CGMP サーバからスイッチに通信できます。これにより、スイッチはすべてのスイッチ インターフェイスにマルチキャスト トラフィックをフラッディングせずに、マルチキャスト メンバーが存在するインターフェイスを取得できるようになります（IGMP スヌーピングは、マルチキャスト パケットのフラッディングを抑制するもう 1 つの方法です。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください）。

CGMP が必要となるのは、レイヤ 2 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。

CGMP は HSRPv1 と相互に排他的な関係にあります。CGMP 脱退処理と HSRPv1 を同時にイネーブルにはできません。ただし、CGMP と HSRPv2 を同時にイネーブルにすることはできます。詳細については、「HSRP バージョン」（P.45-3）を参照してください。

IP マルチキャスト ルーティングの設定

ここでは、次の設定情報について説明します。

マルチキャスト ルーティングのデフォルト設定

表 49-2 に、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 49-2　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 バージョン	バージョン 2

表 49-2　マルチキャスト ルーティングのデフォルト設定 （続き）

機能	デフォルト設定
PIM モード	モードは未定義
PIM スタブ ルーティング	設定なし
PIM RP アドレス	設定なし
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
Shortest-Path-Tree スレッシュホールド レート	0 KB/秒
PIM ルータクエリー メッセージ インターバル	30 秒

マルチキャスト ルーティング設定時の注意事項

スイッチ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。

- 「PIMv1 および PIMv2 の相互運用性」（P.49-11）
- 「Auto-RP および BSR 設定時の注意事項」（P.49-12）

PIMv1 および PIMv2 の相互運用性

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移行が可能となりますが、若干の問題が発生する場合もあります。

PIMv2 に付加的にアップグレードできます。PIM バージョン 1 および 2 を、1 つのネットワーク内の異なるルータおよびマルチレイヤ スイッチに設定できます。内部的には、共有メディア ネットワーク上のすべてのルータおよびマルチレイヤ スイッチで同じ PIM バージョンを実行する必要があります。したがって、PIMv2 装置が PIMv1 装置を検出した場合は、バージョン 1 装置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 装置はバージョン 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 プレフィクスの RP 設定情報を検出し、PIM ドメイン内のすべてのルータおよびマルチレイヤ スイッチにアナウンスします。Auto-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、Auto-RP は PIMv1 から独立したシスコ独自のスタンドアロン プロトコルです。PIMv2 は IETF 標準の追跡プロトコルです。そのため、PIMv2 の使用を推奨します。BSR メカニズムは、Cisco ルータおよびマルチレイヤ スイッチ上の Auto-RP と相互運用します。詳細については、「Auto-RP および BSR 設定時の注意事項」（P.49-12）を参照してください。

PIMv2 装置を PIMv1 装置と相互運用させる場合は、Auto-RP を事前に導入しておく必要があります。Auto-RP マッピング エージェントでもある PIMv2 BSR は、Auto-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、Auto-RP によって、グループ内のルータまたはマルチレイヤごとに 1 つの RP が設定されます。ドメイン内のルータおよびスイッチの中には、複数の RP を選択するために PIMv2 ハッシュ機能を使用しないものもあります。

PIMv1 と PIMv2 が混在する領域内の dense（密）モード グループは、特別な設定を行わなくても自動的に相互運用します。

PIMv1 の Auto-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 parse（疎）モード グループを設定できます。すべての PIMv2 装置で 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ための推奨事項を次に示します。

- 領域全体で Auto-RP を使用します。
- 領域全体で sparse-dense モードを設定します。

Auto-RP がまだ PIMv1 領域に設定されていない場合は、Auto-RP を設定してください。詳細については、「Auto-RP の設定」（P.49-27）を参照してください。

Auto-RP および BSR 設定時の注意事項

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導入してバージョン 2 に移行する方法です。

- 使用するネットワークがすべて Cisco ルータおよびマルチレイヤ スイッチである場合は、Auto-RP または BSR を使用します。
- ネットワークに非 Cisco ルータがある場合は、BSR を使用する必要があります。
- シスコ製 PIMv1 ルータと PIMv2 ルータ、マルチレイヤ スイッチ、および非 Cisco ルータがある場合は、Auto-RP と BSR の両方を使用する必要があります。使用する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は、シスコ製 PIMv2 装置上に Auto-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 装置間のパス上に、PIMv1 装置が配置されていないことを確認してください。
- ブートストラップ メッセージはホップバイホップで送信されるため、PIMv1 装置は、これらのメッセージがネットワーク内のすべてのルータおよびマルチレイヤ スイッチに到達することを回避します。したがって、ネットワーク内に PIMv1 装置があり、Cisco ルータおよびマルチレイヤ スイッチだけが存在する場合は、Auto-RP を使用するのが最良です。
- ネットワーク内に非 Cisco ルータがある場合は、シスコ製 PIMv2 ルータまたはマルチレイヤ スイッチに Auto-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 ルータ間のパス上に、PIMv1 装置が配置されていないことを確認してください。
- シスコ製 PIMv1 ルータおよびマルチレイヤ スイッチと他社製の PIMv2 ルータを相互運用させる場合は、Auto-RP と BSR の両方が必要です。シスコ製 PIMv2 装置を、Auto-RP マッピング エージェントと BSR の両方に設定することを推奨します。詳細については、「Auto-RP および BSR の使用」（P.49-35）を参照してください。

基本的なマルチキャスト ルーティングの設定

IP マルチキャスト ルーティングをイネーブルにし、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。これにより、ソフトウェアはマルチキャスト パケットを転送し、スイッチがそのマルチキャスト ルーティング テーブルを読み込むことができます。

インターフェイスは PIM dense（密）モード、sparse（疎）モード、または sparse-dense モードのいずれかに設定できます。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。IP マルチキャスト ルーティングを実行するには、インターフェイスに対して、これらの PIM モードのいずれかをイネーブルにする必要があります。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 動作もイネーブルになります。

（注）　複数のインターフェイスで PIM がイネーブルに設定されており、これらのインターフェイスのほとんどが発信インターフェイス リストに存在せず、IGMP スヌーピングがディセーブルになっている場合、発信インターフェイスは、余分なレプリケーションが作成されるためにマルチキャスト トラフィックのラインレートを維持できない可能性があります。

マルチキャスト ルーティング テーブルの読み込みでは、dense（密）モード インターフェイスは常にテーブルに追加されます。sparse（疎）モード インターフェイスがテーブルに追加されるのは、ダウンストリーム装置から定期的な 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だけです。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、sparse（疎）モード動作が行われます。その場合、パケットはカプセル化され、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 dense（密）モード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る場合、レシーバーのファーストホップ ルータから送信元に向けて Join メッセージが送信され、送信元ベースの分散ツリーが構築されます。

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になっており、モードは設定されていません。この手順は必須です。

IP マルチキャスティングをイネーブルにし、PIM バージョンおよび PIM モードを設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip multicast-routing distributed**	IP 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 3	**interface** *interface-id*	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：**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、レイヤ 3 ポートとして設定された物理ポートです。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。詳細については、「レイヤ 3 インターフェイスの設定」（P.14-21）を参照してください。
ステップ 4	**ip pim version** [**1** | **2**]	インターフェイスに PIM バージョンを設定します。 デフォルトでは、バージョン 2 はイネーブルになっています（推奨設定）。 PIMv2 モードのインターフェイスに PIMv1 ネイバーがある場合、インターフェイスは自動的に PIMv1 モードにダウングレードされます。バージョン 1 のすべてのネイバーがシャットダウンするかアップグレードされると、インターフェイスはバージョン 2 モードに戻ります。 詳細については、「PIMv1 および PIMv2 の相互運用性」（P.49-11）を参照してください。

	コマンド	目的
ステップ 5	**ip pim** {**dense-mode** | **sparse-mode** | **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。 デフォルトでは、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**：動作の dense（密）モードをイネーブルにします。 • **sparse-mode**：動作の sparse（疎）モードをイネーブルにします。sparse（疎）モードを設定する場合は、RP を設定する必要もあります。詳細については、「ランデブー ポイントの設定」（P.49-25）を参照してください。 • **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ます。sparse-dense モード設定を推奨します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

マルチキャスティングをディセーブルにするには、**no ip multicast-routing distributed** 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。デフォルトの PIM バージョンに戻すには、**no ip pim 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。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。

Source-Specific Multicast の設定

ここでは、Source-Specific Multicast（SSM; 送信元固有マルチキャスト）を設定する方法を説明します。この項で使用している SSM コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*』の「IP Multicast Routing Commands」を参照してください。この章で扱うその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 インデックスを使用するか、オンライン検索を実行して該当するドキュメントを検索してください。

SSM は、IP マルチキャストの拡張機能です。この機能を使用すると、レシーバーに転送されるデータグラム トラフィックは、そのレシーバー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 用に設定されたマルチキャスト グループでは、共有ツリーではなく、SSM 分散ツリーだけが作成されます。

SSM コンポーネントの概要

1 対多アプリケーションを最大限にサポートするデータグラム デリバリ モデルである SSM は、ブロードキャスト アプリケーションとも呼ばれます。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 ソリューション実装のコア ネットワーキング テクノロジーです。スイッチは 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 プロトコルであり、Protocol-Independent Multicast Sparse-Mode（PIM-SM; Protocol-Independent Multicast sparse（疎）モード）から派生したものです。

- Internet Group Management Protocol version 3（IGMPv3）

  IGMPv3 を使用して SSM を実行するには、Cisco IOS ルータ、アプリケーションを実行しているホスト、およびアプリケーション自体で SSM がサポートされている必要があります。

SSM と Internet Standard Multicast の違い

インターネットの現在の 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 モデルの制限があります。たとえば、ISM では、ネットワークは、ネットワーク内のどのホストがマルチキャスト トラフィックをアクティブに送信しているか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構成されます。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必要なのは、IGMP バージョン 1、2、または 3 によるホスト グループへのシグナリングだけです。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 のいずれにおいても、送信元になるための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定するために、(S, G）チャネルへの加入またはそこからの脱退を行う必要があります。つまり、レシーバーは加入した（S, G）チャネルからのトラフィックだけを受信できます。一方、ISM では、レシーバーは受信するトラフィックの送信元の IP アドレスを認識す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手法として、IGMP include モード メンバーシップ レポートの使用が提案されますが、この手法をサポートしているのは IGMP バージョン 3 だけです。

SSM IP アドレス範囲

IP マルチキャスト グループ アドレス範囲の設定済みサブセットに SSM デリバリ モデルを適用することにより、SSM と ISM サービスは共存できます。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 設定ができます。SSM 範囲が定義されている場合、既存の IP マルチキャスト レシーバー アプリケーションが SSM 範囲のアドレスの使用しようとしても、(アプリケーションが明示的な（S, G）チャネル加入を使用するように修正されない限り）トラフィックを受信できません。

SSM の動作

SSM サービスは、IP マルチキャスト サービスが PIM SM に基づいている確立されたネットワークでサポートされます。SSM サービスだけが必要な場合は、ドメイン間の PIM-SM に必要なすべてのプロトコル範囲（たとえば、MSDP、Auto-RP、またはブートストラップ ルータ（BSR）など）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 用に設定されたネットワークに 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、これらのラストホップ ルータ以外のルータでは、SSM 範囲内の PIM-SM だけを実行する必要があります。このようなルータは SSM 範囲内での MSDP シグナリング、登録、または PIM-SM 共有ツリー動作を抑制するために、追加のアクセス制御設定が必要になる場合もあります。

SSM 範囲を設定して 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。この設定が及ぼす影響を次に示します。

- SSM 範囲内のグループの場合、(S, G）チャネルへの加入は、IGMPv3 include モード メンバーシップ レポートを通して受け入れられます。

- SSM 範囲内のアドレスの 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 およびプルーニング メッセージだけであり、（S, G）の Rendezvous Point Tree（RPT; ランデブー ポイント ツリー）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ただちに 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 には PIM-SM との下位互換性があります。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 MSDP Source-Active（SA）メッセージの受け入れ、生成、転送は行われません。

IGMPv3 ホスト シグナリング

IGMPv3 では、ホストはマルチキャスト グループのラストホップ ルータにメンバーシップ シグナルを送信します。ホストは、グループ メンバーシップ シグナルの送信に、送信元に関するフィルタリング機能を使用できます。ホストは、いくつかの特定の送信元を除いてすべての送信元からグループへのトラフィックを受信する（exclude モードと呼ばれる）シグナルか、または、いくつかの特定の送信元からグループへのトラフィックだけを受信する（include モードと呼ばれる）シグナルを送信できます。

IGMPv3 は、ISM および SSM と連携して動作できます。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。

設定時の注意事項

ここでは、SSM の設定時の注意事項について説明します。

SSM 範囲のレガシー アプリケーションに関する制約事項

ネットワーク内の SSM 未対応の既存のアプリケーションは、（S, G）チャネル加入をサポートするように変更しない限り SSM 範囲内で機能しません。したがって、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を引き起こす可能性があります。

アドレス管理に関する制約事項

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、同じグループを共有している異なる（S, G）チャネルを要求する場合、レシーバーはこれらの既存メカニズムの利点を活用できません。代わりに、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時にフィルタリングします。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ため、この状況では、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最小限にすることが重要です。たとえば、テレビ チャネル セットを提供するアプリケーション サービスでは、SSM を使用する場合でも、各テレビ（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。この設定により、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ーが接続されていても、レイヤ 2 スイッチ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。

IGMP スヌーピングおよび CGMP の制限事項

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、古い IGMP スヌーピング スイッチでは正しく認識されない場合があります。

IGMP（特に CGMP）に関連したスイッチング問題に関する詳細については、「IGMP の概要」（P.49-3）を参照してください。

ステート維持の制限事項

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。そのため、レシーバーが（S, G）加入メッセージを送信する限り、送信元から長時間（またはまったく）トラフィックが送信されなくても、レシーバーから送信元への Shortest Path Tree（SPT）ステートは維持されます。

これは、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 とは対照的です。PIM-SM では、（S, G）ステートは送信元がトラフィックの送信を 3 分以上停止すると削除され、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だけ再確立されます。PIM-SSM では、送信元がアクティブであることをレシーバーに通知するメカニズムがないため、レシーバーが（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。

SSM の設定

SSM を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**ip pim ssm** [**default** | **range** *access-list*]	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 2	**interface** type number	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、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip pim** {**sparse-mode** | **sparse-dense-mode**}	インターフェイスで PIM をイネーブルにします。**sparse（疎）モード**と **sparse-dense モード**のいずれかを使用する必要があります。
ステップ 4	**ip igmp version 3**	このインターフェイスで 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 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SSM のモニタ

SSM をモニタするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
show ip igmp groups detail	IGMPv3 による（S, G）チャネル加入登録を表示します。
show ip mroute	マルチキャスト グループが SSM サービスをサポートしているかどうか、または送信元固有のホスト レポートが受信されたかどうかを表示します。

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 をサポートすることができない場合、またはサポートすることが望ましくない場合に、SSM 移行をサポートします。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 Set-Top Box（STB; セットトップ ボックス）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。

ここでは、次の内容について説明します。

設定時の注意事項

SSM マッピング設定時の注意事項を次に示します。

- SSM マッピングを設定する前に、IP マルチキャスト ルーティングをイネーブルにし、PIM sparse（疎）モードをイネーブルにして、SSM を設定します。IP マルチキャスト ルーティングおよび PIM sparse（疎）モードのイネーブル化については、「マルチキャスト ルーティングのデフォルト設定」（P.49-10）を参照してください。
- スタティック SSM マッピングを設定する前に、Access Control List（ACL; アクセス制御リスト）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。ACL の設定手順については、第 38 章「ACL によるネットワーク セキュリティの設定」を参照してください。
- SSM マッピングと DNS ルックアップを設定して使用する前に、実行している DNS サーバにレコードを追加できるようにする必要があります。実行している 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。

  Cisco ネットワーク レジストラなどの製品を使用できます。詳細については、次の URL を参照してください。

  http://www.cisco.com/warp/public/cc/pd/nemnsw/nerr/index.shtml

SSM マッピングには次のような制約があります。

- SSM マッピング機能には、SSM のすべての利点はありません。SSM マッピング機能では、ホストからグループ加入を得て、このグループを 1 つまたは複数の送信元に関連付けられた 1 つのアプリケーションで識別するため、サポートできるアプリケーションは各グループに 1 つだけとなります。すべての SSM アプリケーションが SSM マッピング内の同じグループを共有することは可能です。
- すべての SSM 用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な注意が必要です。SSM マッピングと IGMPv3 を両方イネーブルにした場合、すでに IGMPv3 をサポートしている（SSM はサポートしていない）ホストは IGMPv3 グループ レポートを送信します。SSM マッピングは、このような IGMPv3 グループ レポートをサポートしないため、ルータは送信元をこれらのレポートと正しく関連付けることができません。

SSM マッピングの概要

一般的な 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 チャネルを送信するアクティブなサーバ ホストは 1 つです。単一のサーバから複数の TV チャネルを送信できますが、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 チャネルの既知の 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ルータは、このレポートを、このグループに関連付けられている既知の送信元の 1 つまたは複数のチャネル メンバーシップに変換します。

ルータは、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、SSM マッピングを使用して、そのグループに対する 1 つまたは複数の送信元 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 のメンバーシップ 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、これらの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 サーバを使用し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。

SSM マッピングの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

スタティック SSM マッピング

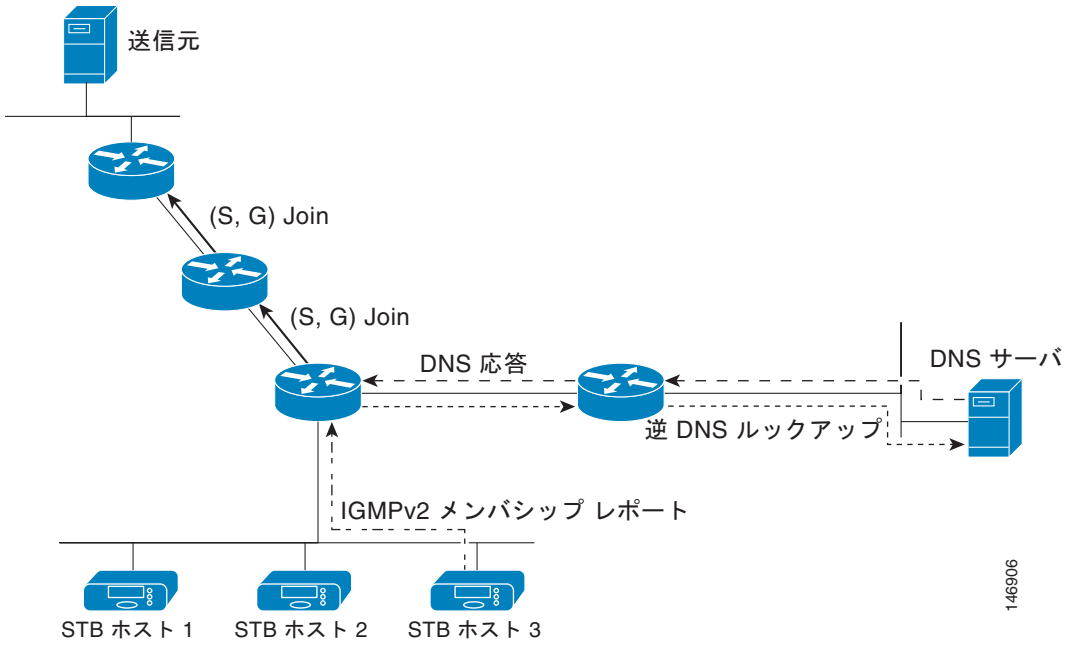
スタティック SSM マッピングでは、ラストホップ ルータが、グループに送信する送信元をスタティック マップを使用して決定するように設定できます。スタティック SSM マッピングを使用するには、グループ範囲を定義した ACL を設定する必要があります。次に、**ip igmp static ssm-map** グローバル コンフィギュレーション コマンドを使用して、ACL で許可されたグループを送信元にマッピングします。

DNS が必要とされない場合やローカルで DNS マッピングが上書きされる場合、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。設定された場合、スタティック SSM マッピングは DNS マッピングより優先されます。

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 ルータが逆 DNS ルックアップを実行し、グループの送信元を決定するように設定できます。DNS ベースの SSM マッピングが設定された場合、ルータはグループ アドレス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 レコードを検索し、それらをこの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 マッピングは、グループごとに最大 20 の送信元をサポートします。ルータは各グループに設定されているすべての送信元に加入します（図 49-4 を参照）。

図 49-4　DNS ベースの SSM マッピング



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 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て、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冗長性を持たせます。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、TV チャネルのビデオ トラフィックを送信する前に、アクティブな送信元の障害が検出されるまで待機します。このため、サーバ側のスイッチオーバー メカニズムにより、TV チャネルのビデオ トラフィックをアクティブに送信するサーバは 1 つだけになります。

G1、G2、G3、G4 を含むグループの 1 つまたは複数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 マッピングの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

SSM マッピングの設定

- 「スタティック SSM マッピングの設定」（P.49-21）（必須）
- 「DNS ベースの SSM マッピングの設定」（P.49-21）（必須）
- 「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」（P.49-22）（任意）

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、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp ssm-map enable**	設定されている SSM 範囲のグループに対する SSM マッピングをイネーブルにします。 **（注）** デフォルトでは、このコマンドを使用すると DNS ベースの SSM マッピングがイネーブルになります。
ステップ 3	**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** 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 DNS ベースの SSM マッピングがイネーブルになります。
ステップ 4	**ip igmp ssm-map static** *access-list source-address*	スタティック SSM マッピングを設定します。 *access-list* に入力した ACL によって、*source-address* に入力した送信元 IP アドレスにマッピングされるグループが定義されます。 **（注）** 追加のスタティック SSM マッピングを設定できます。追加の SSM マッピングを設定した場合、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、スイッチは、設定済みの各 **ip igmp ssm-map static** コマンドを使用して、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。スイッチは、グループごとに最大 20 の送信元を関連付けます。
ステップ 5	必要に応じて、ステップ 4 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**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SSM マッピングの設定例については、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

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、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のためにも 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。DNS ベースの SSM マッピングだけがそのルータで使用されている DNS 実装である場合、空のルート ゾーン、またはそれ自体を示すルート ゾーンで false の DNS セットアップを設定できます。

DNS ベースの SSM マッピングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp ssm-map enable**	設定されている SSM 範囲のグループに対する SSM マッピングをイネーブルにします。
ステップ 3	**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** コマンドを使用すると DNS ベースの SSM マッピングがイネーブルになります。実行コンフィギュレーションに保存されるのは、このコマンドの **no** 形式だけです。 **（注）** DNS ベースの SSM マッピングがディセーブルの場合に DNS ベースの SSM マッピングを再びイネーブルにするには、このコマンドを使用します。
ステップ 4	**ip domain multicast** *domain-prefix*	（任意）スイッチが DNS ベースの SSM マッピングに使用するドメイン プレフィクスを変更します。 デフォルトでは、スイッチは *ip-addr.arpa* ドメイン プレフィクスを使用します。
ステップ 5	**ip name-server** *server-address1* [*server-address2... server-address6*]	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。
ステップ 6	必要に応じて、ステップ 5 を繰り返して追加の DNS サーバを設定して冗長性を確保します。	—
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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

SSM マッピングを使用したスタティック トラフィック転送によって、特定のグループに SSM トラフィックをスタティックに転送できます。

SSM マッピングを使用したスタティック トラフィック転送を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number*	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。 **（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 マッピングか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。

	コマンド	目的
ステップ 3	**ip igmp static-group** *group-address* **source ssm-map**	インターフェイスから（S, G）チャネルをスタティックに転送するには、SSM マッピングを設定します。 このコマンドは、特定のグループに SSM トラフィックをスタティックに転送する場合に使用します。チャネルの送信元アドレスを決定するには、DNS ベースの SSM マッピングを使用します。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SSM マッピングのモニタ

SSM マッピングをモニタするには、表 49-3 に示す各特権 EXEC コマンドを使用します。

表 49-3　SSM マッピング モニタ コマンド

コマンド	目的
show ip igmp ssm-mapping	SSM マッピングに関する情報を表示します。
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。
show ip igmp groups [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]	ルータに直接接続され、IGMP を通じて学習されたレシーバーのマルチキャスト グループを表示します。
show host	デフォルトのドメイン名、名前検索サービスの方式、ネームサーバ ホストのリスト、およびキャッシュされたホスト名とアドレスのリストを表示します。
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 マッピングのモニタリングの例については、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html#wp1047772

PIM スタブ ルーティングの設定

PIM スタブ ルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャスト ルーティングをサポートします。サポート対象の PIM インターフェイスは、アップリンク PIM インターフェイスと PIM 受動インターフェイスの 2 種類です。PIM passive 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。通過と転送を行うのは IGMP トラフィックだけです。

PIM スタブ ルーティング設定時の注意事項

インターフェイスで PIM スタブ ルーティングをイネーブルにする場合には、次の注意事項に従ってください。

- PIM スタブ ルーティングを設定する前に、スタブ ルータとセントラル 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（dense（密）モード、sparse（疎）モード、または dense-sparse モード）が設定されている必要があります。
- PIM スタブ ルータは、ディストリビューション ルータ間の中継トラフィックのルーティングを行いません。ユニキャスト（EIGRP）スタブ ルーティングではこの動作が強制されます。PIM スタブ ルータの動作を支援するためにユニキャスト スタブ ルーティングを設定する必要があります。詳細については、「EIGRP スタブ ルーティングの設定」（P.41-41）を参照してください。
- レイヤ 2 アクセス ドメインでは、直接接続されたマルチキャスト（IGMP）レシーバーと送信元だけが許可されています。PIM プロトコルはアクセス ドメインではサポートされません。
- 冗長 PIM スタブ ルータのトポロジはサポートされません。

PIM スタブ ルーティングのイネーブル化

インターフェイス上で PIM スタブ ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	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。
ステップ 3	**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 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip pim interface**	各インターフェイスでイネーブルになっている PIM スタブを表示します。
ステップ 6	show running-config	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスで PIM スタブ ルーティングをディセーブルにするには、**no ip pim passive** 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。

次の例では、IP マルチキャスト ルーティングをイネーブルに設定し、スイッチ A の PIM アップリンク ポート 25 を **spare-dense-mode enabled** を使用するルーテッド アップリンク ポートとして設定しています。図 49-2 では、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なっています。

```
Switch(config)# ip multicast-routing distributed
Switch(config)# interface GigabitEthernet1/25
Switch(config-if)# no switchport
Switch(config-if)# ip address 3.1.1.2 255.255.255.0
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/20
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip address 100.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet1/20
```

```
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.1.1.1 255.255.255.0
Switch(config-if)# ip pim passive
Switch(config-if)# end
```

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 interface** 特権 EXEC コマンドを使用します。

```
Switch# show ip pim interface
Address Interface Ver/ Nbr Query DR DR
Mode Count Intvl Prior
3.1.1.2 GigabitEthernet1/25 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 GigabitEthernet1/20 v2/P 0 30 1 10.1.1.1
```

PIM スタブの設定とステータスの情報を表示するには、次の特権 EXEC コマンドを使用します。

- **show ip pim interface** は、各インターフェイスでイネーブルになっている PIM スタブを表示します。
- **show ip igmp detail** は、特定のマルチキャスト送信元グループに参加した対象クライアントを表示します。
- **show ip igmp mroute** は、送信元から対象クライアントへマルチキャスト ストリームが転送されていることを確認します。

ランデブー ポイントの設定

インターフェイスが sparse-dense モードで、グループを sparse（疎）グループとして扱う場合には、RP を設定する必要があります。いくつかの方法を使用できます。

- 「手動でのマルチキャスト グループへの RP の割り当て」（P.49-25）
- 「Auto-RP の設定」（P.49-27）（PIMv1 から独立したシスコ独自のスタンドアロン プロトコル）
- 「PIMv2 BSR の設定」（P.49-31）（Internet Engineering Task Force（IETF）標準の追跡プロトコル）

実行している 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、Auto-RP、BSR、またはこれらを組み合わせて使用できます。詳細については、「PIMv1 および PIMv2 の相互運用性」（P.49-11）および「Auto-RP および BSR 設定時の注意事項」（P.49-12）を参照してください。

手動でのマルチキャスト グループへの RP の割り当て

ここでは、RP を手動で設定する方法を説明します。ダイナミック メカニズム（Auto-RP や BSR など）を通じてグループの RP を学習する場合、その RP に対してこの作業を実行す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、送信元のファーストホップ 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て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 を使用してマルチキャスト 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。RP はマルチキャスト グループのメンバーではなく、マルチキャスト送信元およびグループ メンバーの「合流地点」として機能します。

アクセス リストで定義される複数のグループに、単一の RP を設定できます。グループに RP が設定されていない場合、マルチレイヤ スイッチは PIM dense（密）モード技術を使用して、グループを dense（密）として処理します。

手動で RP のアドレスを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip pim rp-address** *ip-address* [*access-list-number*] [**override**]	PIM RP のアドレスを設定します。 デフォルトでは、PIM RP アドレスは設定されていません。すべてのルータおよびマルチレイヤ スイッチ（RP を含む）で、RP の IP アドレスを設定する必要があります。グループに RP が設定されていない場合、スイッチは PIM dense（密）モード技術を使用して、グループを dense（密）として処理します。 PIM 装置を、複数のグループの RP にできます。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、装置がどのグループの 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* には、1 ～ 99 までの標準 IP アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • （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、Auto-RP または BSR で学習された 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 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、RP が使用されるマルチキャスト グループ アドレスを入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード 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 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

RP アドレスを削除するには、**no ip pim rp-address** *ip-address* [*access-list-number*] [**override**] 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。

次に、RP のアドレスを、マルチキャスト グループ 225.2.2.2 の場合だけ 147.106.6.22 に設定する例を示します。

```
Switch(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Switch(config)# ip pim rp-address 147.106.6.22 1
```

Auto-RP の設定

Auto-RP は IP マルチキャストを使用して、グループ/RP マッピングを PIM ネットワーク内のすべての Cisco ルータおよびマルチレイヤ スイッチに自動配布します。Auto-RP には、次のような利点があります。

- さまざまなグループ範囲として機能するネットワーク内の複数の RP を使用するのが簡単になります。
- 異なる RP 間で負荷を分散し、グループに加入する場所に従って 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 スイッチ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、接続の問題を引き起こす原因が取り除かれます。

Auto-RP を設定する場合、次の注意事項に従ってください。

- PIM を sparse（疎）モードまたは sparse-dense 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（「手動でのマルチキャスト グループへの RP の割り当て」（P.49-25）を参照）。
- ルーテッド インターフェイスが sparse（疎）モードに設定されていると、すべての装置が Auto-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でも、Auto-RP を使用できます。
- ルーテッド インターフェイスが sparse（疎）モードに設定され、**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と、すべての装置が 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い場合でも、Auto-RP を使用できます。

ここでは、Auto-RP の設定手順について説明します。

- 「新規インターネットワークでの Auto-RP の設定」（P.49-27）（任意）
- 「既存の sparse（疎）モード クラウドへの Auto-RP の追加」（P.49-27）（任意）
- 「問題のある RP への Join メッセージ送信の防止」（P.49-29）（任意）
- 「着信 RP アナウンス メッセージのフィルタリング」（P.49-30）（任意）

概要については、「Auto-RP」（P.49-7）を参照してください。

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 Auto-RP を設定している場合は、すべてのインターフェイスが sparse-dense モードに設定されるため、デフォルトの RP は不要です。「既存の sparse（疎）モード クラウドへの Auto-RP の追加」（P.49-27）のプロセスに従ってください。ただし、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、ステップ 3 を省略してください。

既存の sparse（疎）モード クラウドへの Auto-RP の追加

ここでは、Auto-RP を既存の sparse（疎）モード クラウドに最初に導入する際に、既存のマルチキャスト インフラストラクチャの破壊を最小限に抑える方法について説明します。

既存の sparse（疎）モード クラウドに Auto-RP を導入するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**show running-config**	すべての PIM 装置上でデフォルトの RP がすでに設定されていること、および RP が sparse（疎）モード 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 コマンドによって事前に設定されています。 spare-dense モード環境の場合、このステップは不要です。 選択された RP は接続が良好で、ネットワーク全体で使用可能である必要があります。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）に対して使用します。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。Auto-RP によってダイナミックに検出された RP は、スタティックに設定された 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 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim send-rp-announce** *interface-id* **scope** *ttl* **group-list** *access-list-number* **interval** *seconds*	別の PIM 装置をローカル 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のタイプと番号を入力します。有効なインターフェイスとしては、物理ポート、ポート チャネル、および VLAN があります。 • **scope** *ttl* には、ホップの Time to Live 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できるように、十分なホップ カウントを入力します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。 • **group-list** *access-list-number* には、1 ～ 99 までの標準 IP アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • **interval** *seconds* には、アナウンス メッセージを送信する頻度を指定します。デフォルト値は 60 秒です。指定できる範囲は 1 ～ 16383 です。
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、必要な回数だけコマンドを繰り返します。 • *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 アドレス範囲を入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード 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 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。

	コマンド	目的
ステップ 5	**ip pim send-rp-discovery scope** *ttl*	接続が中断される可能性がないスイッチを検索し、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 Time to Live 値を指定し、RP 検出パケットを制限します。ホップ カウント内にあるすべての装置は、送信元装置から Auto-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装置に対し、矛盾（グループ/RP 範囲の重複など）を回避するために使用されるグループ/RP マッピングを通知します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
	show ip pim rp mapping **show ip pim rp**	関連付けられたマルチキャスト ルーティング エントリとともにキャッシュされたアクティブ RP を表示します。 ルーティング テーブルにキャッシュされた情報を表示します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

候補 RP として設定された PIM 装置を解除するには、**no ip pim send-rp-announce** *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。RP マッピング エージェントとして設定されたスイッチを解除するには、**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。

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、このスイッチが RP として機能するグループが記述されています。

```
Switch(config)# ip pim send-rp-announce gigabitethernet1/1 scope 31 group-list 5
Switch(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```

問題のある RP への Join メッセージ送信の防止

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装置がある場合は、あとでこの問題に対処できます。ルータまたはマルチレイヤ スイッチが **ip pim accept-rp** コマンドによってすでに設定されている場合は、このコマンドを再入力し、新しくアドバタイズされた RP を許可する必要があります。

Auto-RP でアドバタイズされたすべての 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。

すべてのインターフェイスが sparse（疎）モードの場合はデフォルト設定の RP を使用し、224.0.1.39 および 224.0.1.40 の 2 つの既知のグループをサポートします。Auto-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および配布します。このように **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する必要があります。

```
Switch(config)# ip pim accept-rp 172.10.20.1 1
Switch(config)# access-list 1 permit 224.0.1.39
Switch(config)# access-list 1 permit 224.0.1.40
```

着信 RP アナウンス 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、不正に設定されたルータが候補 RP になりすまして問題を引き起こすことを回避できます。

着信 RP アナウンス メッセージをフィルタリングするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip pim rp-announce-filter rp-list** *access-list-number* **group-list** *access-list-number*	着信 RP アナウンス メッセージをフィルタリングします。 このコマンドは、ネットワーク内のマッピング エージェントごとに入力します。このコマンドを使用しなければ、すべての着信 RP アナウンス メッセージがデフォルトで受け入れられます。 **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。この変数を省略した場合は、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発生しないように、すべてのマッピング エージェント間でフィルタが一貫している必要があります。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *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。 • マッピング エージェントが、どのルータおよびマルチレイヤ スイッチからの候補 RP アナウンス（rp-list ACL）を許可す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（group-list 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 アドレス範囲を入力します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード 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 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

着信 RP アナウンス メッセージに関するフィルタを削除するには、**no ip pim rp-announce-filter rp-list** *access-list-number* [**group-list** *access-list-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。

次に、不正な候補 RP が候補 RP アナウンスを許可することを防ぐために使用される Auto-RP マッピング エージェントを設定する例を示します。

```
Switch(config)# ip pim rp-announce-filter rp-list 10 group-list 20
Switch(config)# access-list 10 permit host 172.16.5.1
Switch(config)# access-list 10 permit host 172.16.2.1
Switch(config)# access-list 20 deny 239.0.0.0 0.0.255.255
Switch(config)# access-list 20 permit 224.0.0.0 15.255.255.255
```

この例では、マッピング エージェントは、172.16.5.1 および 172.16.2.1 の 2 つの装置からの候補 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 つの装置からの候補 RP アナウンスのうち、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装置からの候補 RP アナウンスを許可しません。さらに、候補 RP アナウンスが 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 アナウンスを許可しません。この範囲は、管理用スコープのアドレス範囲です。

PIMv2 BSR の設定

ここでは、PIMv2 ネットワークでの BSR の設定手順について説明します。

- 「PIM ドメイン境界の定義」（P.49-31）（任意）
- 「IP マルチキャスト境界の定義」（P.49-32）（任意）
- 「候補 BSR の設定」（P.49-33）（任意）
- 「候補 RP の設定」（P.49-33）（任意）

概要については、「ブートストラップ ルータ」（P.49-7）を参照してください。

PIM ドメイン境界の定義

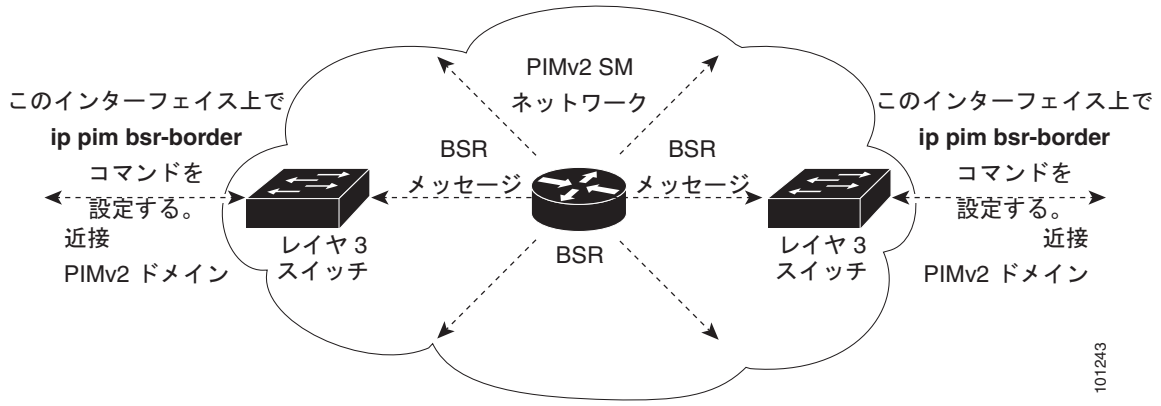
IP マルチキャストの普及に伴い、1 つの PIMv2 ドメインと別の PIMv2 ドメインが境界を挟んで隣接する機会が増えています。これらの 2 つのドメインは同じ RP、BSR、候補 RP、候補 BSR のセットを共有していない可能性があるため、PIMv2 BSR メッセージがドメインの内外に流れないように抑制する必要があります。これらメッセージのドメイン境界通過を許可すると、通常の BSR 選定メカニズムに悪影響を与えたり、境界に位置するすべてのドメインで単一の BSR が選択されたり、候補 RP アドバタイズが共存し、誤ったドメイン内で RP が選択されたりすることがあります。

PIM ドメイン境界を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**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。 このコマンドは、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入力します。このコマンドを実行すると、スイッチは、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定されます（図 49-5 を参照）。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。

図 49-5　PIMv2 BSR メッセージの抑制



IP マルチキャスト境界の定義

Auto-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。Auto-RP 情報を伝送する 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。

マルチキャスト境界を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* **deny** *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *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、Auto-RP 情報を伝送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、送信元に適用するワイルドカード 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 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 3	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip multicast boundary** *access-list-number*	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 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

境界を削除するには、**no ip multicast boundary** 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。

次に、Auto-RP 情報を拒否する IP マルチキャスト境界を設定する例の一部を示します。

```
Switch(config)# access-list 1 deny 224.0.1.39
Switch(config)# access-list 1 deny 224.0.1.40
Switch(config)# access-list 1 permit all
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip multicast boundary 1
```

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 として機能する装置は、他の装置との接続が良好で、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。

スイッチを候補 BSR として設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip pim bsr-candidate** *interface-id hash-mask-length* [*priority*]	スイッチが候補 BSR になるように設定します。 • *interface-id* には、スイッチを候補 BSR に設定するときに BSR アドレスが取得される、スイッチのインターフェイスを入力します。このインターフェイスは PIM を使用してイネーブルにする必要があります。有効なインターフェイスとしては、物理ポート、ポート チャネル、および VLAN があります。 • *hash-mask-length* には、ハッシュ機能をコールする前の、グループ アドレスと 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、この値が 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* には、0 ～ 255 までの番号を入力します。プライオリティの高い BSR が優先されます。プライオリティ値が同じである場合は、最大の IP アドレスを持つ装置が BSR として選択されます。デフォルト値は 0 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

候補 BSR として設定されたこの装置を解除するには、**no ip pim bsr-candidate** 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。

次に、候補 BSR を設定する例を示します。この例では、アドバタイズされる BSR アドレスとしてポートの IP アドレス 172.21.24.18 を使用し、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。

```
Switch(config)# interface gigabitethernet1/2
```

候補 RP の設定

候補 RP を 1 つまたは複数設定できます。BSR と同様に RP は、他の装置との接続が良好で、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。RP となる装置を決定するときには、次のオプションを考慮してください。

- Cisco ルータおよびマルチレイヤ スイッチで構成される、Auto-RP だけが使用されているネットワークでは、すべての装置を RP として設定できます。
- シスコ製 PIMv2 ルータおよびマルチレイヤ スイッチと、他のベンダー製のルータだけで構成されるネットワークでは、すべての装置を RP として使用できます。
- シスコ製 PIMv1 ルータ、PIMv2 ルータ、および他のベンダー製のルータで構成されるネットワークでは、シスコ製 PIMv2 ルータおよびマルチレイヤ スイッチだけを RP として設定します。

スイッチが自身を PIMv2 候補 RP として BSR にアドバタイズするように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip pim rp-candidate** *interface-id* [**group-list** *access-list-number*]	スイッチが候補 RP になるように設定します。 • *interface-id* には、関連付けられた 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としては、物理ポート、ポート チャネル、および VLAN があります。 • （任意）**group-list** *access-list-number* には、1 ～ 99 までの標準 IP アクセス リスト番号を入力します。group-list が指定されていない場合は、スイッチがすべてのグループの候補 RP となります。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *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、パケットの送信元とな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、送信元に適用するワイルドカード 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 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

候補 RP として設定されたこの装置を解除するには、**no ip pim rp-candidate** *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。

次に、スイッチが自身を候補 RP として PIM ドメイン内の BSR にアドバタイズするように設定する例を示します。標準アクセス リスト番号 4 は、ポートによって識別されるアドレスを持つ RP に関連付けられたグループ プレフィクスを指定します。この RP は、プレフィクスが 239 であるグループを処理します。

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

Auto-RP および BSR の使用

ネットワーク上のルータがすべてシスコ デバイスである（他のベンダー製のルータが存在しない）場合には、BSR を設定する必要はありません。PIMv1 と PIMv2 が両方とも動作しているネットワークに、Auto-RP を設定します。

シスコ製 PIMv1 ルータおよびマルチレイヤ スイッチと他社製の PIMv2 ルータを相互運用させる場合は、Auto-RP と BSR の両方が必要です。シスコ製 PIMv2 ルータまたはマルチレイヤ スイッチを、Auto-RP マッピング エージェントと BSR の両方に設定することを推奨します。

BSR を 1 つまたは複数使用する必要がある場合の推奨事項を次に示します。

- 候補 BSR を Auto-RP 用の RP マッピング エージェントとして設定します。詳細については、「Auto-RP の設定」（P.49-27）および「候補 BSR の設定」（P.49-33）を参照してください。
- グループ プレフィクスが Auto-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 と 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 プレフィクスが処理されるように設定します。この設定により、PIMv2 DR は、RP マッピング データベースでの最長一致検索のために、これらの PIMv1 DR から異なる RP を選択できなくなります。

グループ/RP マッピングの整合性を確認するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**show ip pim rp** [[*group-name* | *group-address*] | **mapping**]	任意のシスコ デバイスについて、使用可能な RP マッピングを表示します。 • （任意）*group-name* には、RP を表示するグループの名前を指定します。 • （任意）*group-address* には、RP を表示するグループのアドレスを指定します。 • （任意）シスコ デバイスが認識する（設定または Auto-RP から学習された）すべてのグループ/RP マッピングを表示するには、**mapping** キーワードを使用します。
ステップ 2	**show ip pim rp-hash** *group*	PIMv2 ルータまたはマルチレイヤ スイッチで、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。

RP マッピング情報のモニタ

RP マッピング情報をモニタするには、特権 EXEC モードで次のコマンドを使用します。

- **show ip pim bsr** は、選定された BSR の情報を表示します。
- **show ip pim rp-hash** *group* は、指定グループに選択された RP を表示します。
- **show ip pim rp** [*group-name* | *group-address* | **mapping**] は、スイッチが（BSR 経由で、または Auto-RPRP メカニズムによって）RP を学習する方法を表示します。

PIMv1 および PIMv2 相互運用性の問題のトラブルシューティング

PIMv1 および PIMv2 間の相互運用性の問題をデバッグする場合、次の点を順に確認します。

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ます。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、register-stop メッセージに応答し、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）。

高度な PIM 機能の設定

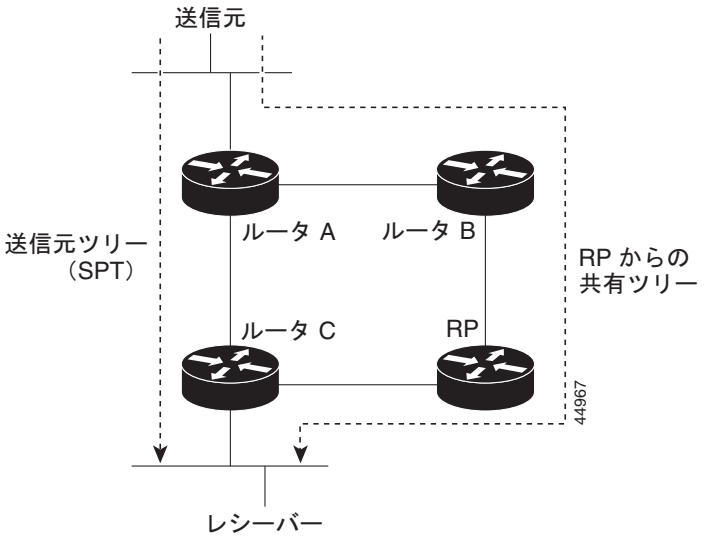
ここでは、オプションの高度な PIM 機能について説明します。

- 「PIM 共有ツリーおよび送信元ツリーの概要」（P.49-36）
- 「PIM Shortest-Path Tree 使用の延期」（P.49-37）（任意）
- 「PIM ルータクエリー メッセージ インターバルの変更」（P.49-39）（任意）

PIM 共有ツリーおよび送信元ツリーの概要

デフォルトでは、グループのメンバーが受信するデータは、RP でルーティングされた単一のデータ分散ツリーを経由して、送信側からグループに送信されます。図 49-6 に、このタイプの共有分散ツリーを示します。送信側からのデータは RP に配信され、共有ツリーに加入しているグループ メンバーへ配布されます。

図 49-6　共有ツリーおよび送信元ツリー（Shortest-Path Tree）



データ レートが保証されている場合は、送信元でルーティングされたデータ分散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。このタイプの分散ツリーは、Shortest-Path Tree 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、送信元ツリーに切り替わります。

共有ツリーから送信元ツリーへの移動プロセスを次に示します。

1. レシーバー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 はデータを登録メッセージにカプセル化して 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。1 つはカプセル化されたデータ、もう 1 つはネイティブ状態のデータです。
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 register-stop 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 パケットを受信すると、ルータ C が送信元に Join メッセージを送信するように求められます。
7. （S,G）に関するデータを受信すると、ルータ C は送信元宛のプルーニング メッセージを共有ツリーの上方向に送信します。
8. RP は（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 メッセージをトリガーします。

Join メッセージとプルーニング メッセージが送信元および 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 へのパス上にある各 PIM 装置で処理されます。登録メッセージと 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た指定ルータで送信され、グループの RP で受信されます。

グループへ送信する複数の送信元は、共有ツリーを使用します。

PIM 装置を共有ツリー上に存在するように設定できます。詳細については、「PIM Shortest-Path Tree 使用の延期」（P.49-37）を参照してください。

PIM Shortest-Path Tree 使用の延期

共有ツリーから送信元ツリーへの変更は、最初のデータ パケットがラストホップ ルータ（図 49-6 のルータ C）に着信すると発生します。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 コマンドによってタイミングが制御されるために発生します。

Shortest-Path Tree では共有ツリーよりも多くのメモリが必要となりますが、遅延が短縮されます。Shortest-Path Tree の使用を延期することも可能です。リーフ ルータを Shortest-Path Tree にすぐ移動する代わりに、トラフィックがスレッシュホールドに先に到達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 Shortest-Path Tree 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（KB/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トリガーし、送信元ツリー（Shortest-Path Tree）を構築します。送信元からのトラフィック レートがスレッシュホールド値を下回ると、リーフ ルータは共有ツリーに再び切り替わり、送信元にプルーニング メッセージを送信します。

Shortest-Path Tree スレッシュホールド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、スレッシュホールドはすべてのグループに適用されます。

マルチキャスト ルーティングが送信元ツリーから Shortest-Path Tree に切り替わる前の上限値となるトラフィック レートのスレッショルドを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	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、スレッショルドを適用するマルチキャスト グループを指定します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード 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 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 3	**ip pim spt-threshold** {*kbps* | **infinity**} [**group-list** *access-list-number*]	Shortest-Path Tree（SPT）に移動する前の上限値となるスレッショルドを指定します。 • *kbps* には、トラフィック レートを Kbps で指定します。デフォルト値は 0 KB/ 秒です。 **（注）** 指定できる範囲は 0 ～ 4294967 ですが、スイッチ ハードウェアの制限により、0 KB/ 秒だけが有効となります。 • 指定グループのすべての送信元で共有ツリーを使用し、送信元ツリーに切り替わらないようにするには、**infinity** を指定します。 • （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 が 0 の場合、または group-list を使用しない場合、スレッショルドはすべてのグループに適用されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip pim spt-threshold** {*kbps* | **infinity**} 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。

PIM ルータクエリー メッセージ インターバルの変更

PIM ルータおよびマルチレイヤ スイッチでは、各 LAN セグメント（サブネット）の DR になる装置を判別するために、PIM ルータクエリー メッセージが送信されます。DR は、直接接続されている 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、DR は IGMPv1 を使用している場合だけ意味があります。IGMPv1 には IGMP クエリア選定プロセスがないため、選定された 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ている装置が 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、最大の IP アドレスを持つ装置が DR となります。

ルータクエリー メッセージ インターバルを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip pim query-interval** *seconds*	スイッチが 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。 デフォルト値は 30 秒です。指定できる範囲は 1 ～ 65535 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip pim query-interval** [*seconds*] 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。

オプションの IGMP 機能の設定

ここでは、次の設定情報について説明します。

- 「IGMP のデフォルト設定」（P.49-40）
- 「グループのメンバーとしてのスイッチの設定」（P.49-40）（任意）
- 「IP マルチキャスト グループへのアクセスの制御」（P.49-41）（任意）
- 「IGMP バージョンの変更」（P.49-42）（任意）
- 「IGMP ホストクエリー メッセージ インターバルの変更」（P.49-42）（任意）
- 「IGMPv2 の IGMP クエリー タイムアウトの変更」（P.49-43）（任意）
- 「IGMPv2 の最大クエリー応答時間の変更」（P.49-44）（任意）
- 「スタティックに接続されたメンバーとしてのスイッチの設定」（P.49-44）（任意）

IGMP のデフォルト設定

表 49-4 に、IGMP のデフォルト設定を示します。

表 49-4　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 グループのメンバーとしてのマルチレイヤ スイッチ	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 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
スタティックに接続されたメンバーとしてのマルチレイヤ スイッチ	ディセーブル

グループのメンバーとしてのスイッチの設定

スイッチをマルチキャスト グループのメンバーとして設定し、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 スイッチがマルチキャスト グループのメンバーである場合、グループに ping を使用すると、これらのすべての装置が応答します。装置は、属する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、CPU がグループ アドレスのデータ トラフィックをすべて受信するため、CPU のパフォーマンスに影響を与える場合があります。

スイッチがグループのメンバーになるように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp join-group** *group-address*	マルチキャスト グループに加入するスイッチを設定します。 デフォルトでは、グループ 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 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

グループのメンバーシップをキャンセルするには、**no ip igmp join-group** *group-address* インターフェイス コンフィギュレーション コマンドを使用します。

次に、スイッチをマルチキャスト グループ 255.2.2.2 の加入をイネーブルにする例を示します。

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

IP マルチキャスト グループへのアクセスの制御

スイッチは IGMP ホストクエリー 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、スイッチはマルチキャスト 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。各インターフェイスにフィルタを適用することで、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できるマルチキャスト グループを制限できます。

インターフェイスで許可されるマルチキャスト グループをフィルタリングするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp access-group** *access-list-number*	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できるマルチキャスト グループを指定します。 デフォルトでは、インターフェイスのすべてのグループが許可されています。 *access-list-number* には、標準 IP アクセス リスト番号を指定します。指定できる範囲は 1 ～ 99 です。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成します。 • *access-list-number* には、ステップ 3 で作成したアクセス リストを指定します。 • **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、サブネット上のホストが加入できるマルチキャスト グループを指定します。 • （任意）*source-wildcard* には、送信元に適用するワイルドカード 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 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

インターフェイスでグループをディセーブルにするには、**no ip igmp access-group** 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。

次に、ポートに接続されたホストが、グループ 255.2.2.2 だけに加入できるように設定する例を示します。

```
Switch(config)# access-list 1 255.2.2.2 0.0.0.0
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip igmp access-group 1
```

IGMP バージョンの変更

デフォルトでは、スイッチは 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提供する IGMP バージョン 2 を使用します。

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、バージョン 1 システムを自動的に検出せず、バージョン 1 への切り替えも行いません。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、サブネット上でバージョン 1 とバージョン 2 のホストを混在できます。

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。

IGMP バージョンを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp version** {**1** | **2**}	スイッチが使用する IGMP バージョンを指定します。 **（注）** バージョン 1 に変更する場合、**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。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**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。

IGMP ホストクエリー メッセージ インターバルの変更

スイッチは 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存在するマルチキャスト グループを検出します。これらのメッセージは、Time to Live（TTL）が 1 であるすべてのホスト マルチキャスト グループ（224.0.0.1）に送信されます。スイッチはホストクエリー 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ついての情報を更新します。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、ソフトウェアは、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 パケット転送を停止し、送信元のアップストリーム方向へプルーニング メッセージを送信します。

スイッチはLAN（サブネット）用の PIM 指定ルータ（DR）を選定します。DR は、最大の IP アドレスを持つ、IGMPv2 用のルータまたはマルチレイヤ スイッチです。IGMPv1 の場合、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定されます。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。sparse（疎）モードの場合、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。

ホストクエリー インターバルを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp query-interval** *seconds*	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 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip igmp query-interval** インターフェイス コンフィギュレーション コマンドを使用します。

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、スイッチがインターフェイスのクエリアとして処理を引き継ぐまでの時間を指定できます。デフォルトでは、スイッチは **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間隔の 2 倍の時間待機します。この時間を経過してもスイッチ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。

クエリー間隔を設定するには、**show ip igmp interface** *interface-id* 特権 EXEC コマンドを入力します。

IGMP クエリー タイムアウトを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp querier-timeout** *seconds*	IGMP クエリー タイムアウトを指定します。 デフォルト値は 60 秒です（クエリー間隔の 2 倍）。指定できる範囲は 60 ～ 300 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip igmp querier-timeout** 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。

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、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。最大クエリー応答時間により、LAN 上に直接接続されているグループ メンバーが存在しないことを短時間で検出するようにスイッチをイネーブルにします。値を小さくすると、グループのプルーニング速度が向上します。

最大クエリー応答時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp query-max-response-time** *seconds*	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。 デフォルト値は 10 秒です。指定できる範囲は 1 ～ 25 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no 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 コマンドを使用します。

スタティックに接続されたメンバーとしてのスイッチの設定

ネットワーク セグメント上にグループ メンバーが存在しない場合や、ホストが IGMP を使用してグループ メンバーシップをレポートできない場合があります。ただし、そのネットワーク セグメントにマルチキャスト トラフィックを送り込むことが必要な場合があります。次に、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方法を示します。

- **ip igmp join-group** 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。この方法の場合、スイッチはマルチキャスト パケットの受け入れに加えて転送もします。マルチキャスト パケットを受け入れる場合は、高速スイッチングを実行できません。
- **ip igmp static-group** 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。この方法の場合、スイッチはパケットそのものを受け入れず、転送だけを実行します。この方法の場合は高速スイッチングをイネーブルにします。発信インターフェイスは 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）フラグがないことからわかるように、スイッチ自体はメンバーではありません。

スタティックに接続されたグループのメンバーになるように（および高速スイッチングをイネーブルにできるように）スイッチを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp static-group** *group-address*	スイッチをスタティックに接続されたグループのメンバーとして設定します。 デフォルトでは、この機能はディセーブルです。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp interface** [*interface-id*]	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

グループのメンバーとして設定されたスイッチを解除するには、**no ip igmp static-group** *group-address* インターフェイス コンフィギュレーション コマンドを使用します。

オプションのマルチキャスト ルーティング機能の設定

ここでは、オプションのマルチキャスト ルーティング機能の設定手順について説明します。

- レイヤ 2 接続と MBONE マルチメディア会議セッションに関する機能と設定
  - 「CGMP サーバ サポートのイネーブル化」（P.49-45）（任意）
  - 「sdr リスナー サポートの設定」（P.49-47）（任意）
- 帯域利用率を制御する機能
  - 「IP マルチキャスト境界の設定」（P.49-48）（任意）
- Virtual Private Network（VPN; 仮想私設網）Routing/Forwarding（VRF; VPN ルーティング / 転送）テーブル内のマルチキャストの設定手順
  - 「マルチキャスト VRF の設定」（P.41-79）

CGMP サーバ サポートのイネーブル化

スイッチは、IGMP スヌーピングをサポートしない、CGMP クライアント機能が組み込まれている装置用の CGMP サーバとして機能します。CGMP は、レイヤ 2 Catalyst スイッチに接続された Cisco ルータおよびマルチレイヤ スイッチで使用されるプロトコルであり、IGMP で実行される作業と同様の作業を実行します。CGMP が必要となるのは、レイヤ 2 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。

スイッチインターフェイスで CGMP サーバをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	レイヤ 2 Catalyst スイッチに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip cgmp** [**proxy**]	インターフェイスで CGMP をイネーブルにします。 デフォルトでは、CGMP はすべてのインターフェイスでディセーブルになっています。 CGMP をイネーブルにすると、CGMP Join メッセージがトリガーされます。CGMP は、レイヤ 2 Catalyst スイッチに接続されたレイヤ 3 インターフェイスでだけイネーブルにします。 （任意）**proxy** キーワードを入力すると、CGMP プロキシ機能がイネーブルになります。プロキシ ルータは、CGMP 非対応ルータの MAC アドレスおよびグループ アドレス 0000.0000.0000 が格納された CGMP Join メッセージを送信することで、CGMP 非対応ルータの存在をアドバタイズします。 **（注）** CGMP プロキシを実行するには、スイッチを IGMP クエリアに設定する必要があります。**ip cgmp proxy** コマンドを設定する場合は、ネットワークで動作中の IGMP のバージョンに応じて、最大または最小の IP アドレスのスイッチが IGMP クエリアになるように、IP アドレスを処理する必要があります。IGMP バージョン 2 クエリアは、インターフェイスの最小の IP アドレスに基づいて選択されます。IGMP バージョン 1 クエリアは、インターフェイスで使用されるマルチキャスト ルーティング プロトコルに基づいて選択されます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。
ステップ 7		レイヤ 2 Catalyst スイッチ CGMP クライアントの設定を確認します。詳細については、製品に付属のマニュアルを参照してください。

インターフェイスで CGMP をディセーブルにするには、**no ip cgmp** 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。

複数のシスコ製 CGMP 対応装置がスイッチド ネットワークに接続されている状態で **ip cgmp proxy** コマンドを使用する必要がある場合は、すべての装置を同じ CGMP オプションで設定し、IGMP クエリアを非 Cisco ルータよりも優先させることを推奨します。

sdr リスナー サポートの設定

MBONE は、相互接続され、IP マルチキャスト トラフィックの転送が可能なインターネット ルータおよびホストの小さなサブセットです。その他のマルチメディア コンテンツも、多くの場合、MBONE を通してブロードキャストされます。マルチメディア セッションに加入する前に、このセッションで使用されているマルチキャスト グループ アドレスとポート、セッションがアクティブになる時期、およびワークステーションで必要とされるアプリケーションの種類（オーディオやビデオなど）を把握する必要があります。この情報は、MBONE Session Directory バージョン 2（sdr）ツールによって提供されます。このフリーウェア アプリケーションは WWW 上の複数のサイト（http://www.video.ja.net/mice/index.html など）からダウンロードできます。

SDR は、Session Announcement Protocol（SAP; セッション通知プロトコル）マルチキャスト パケット用の既知のマルチキャスト グループ アドレスとポートを、会議セッションをアナウンスする SAP クライアントから待ち受けるマルチキャスト アプリケーションです。これらの SAP パケットには、セッションの説明、セッションがアクティブな期間、IP マルチキャスト グループ アドレス、メディア形式、担当者、およびアドバタイズされたマルチメディア セッションに関するその他の情報が含まれています。SAP パケットの情報は、[SDR Session Announcement] ウィンドウに表示されます。

sdr リスナー サポートのイネーブル化

デフォルトでは、スイッチはセッション ディレクトリのアドバタイズを待ち受けません。

スイッチがインターフェイスのデフォルトのセッション ディレクトリ グループ（224.2.127.254）に加入し、セッション ディレクトリ アドバタイズを待ち受けられるようにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	sdr に対して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。
ステップ 3	**ip sdr listen**	sdr リスナー サポートをイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

sdr サポートをディセーブルにするには、**no ip sdr listen** 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。

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、古いアドバタイズが不必要に保持されることを防ぐために、エントリがアクティブである期間を制限できます。

sdr キャッシュ エントリがキャッシュ内でアクティブである期間を制限するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip sdr cache-timeout** *minutes*	sdr キャッシュ エントリがキャッシュ内で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 sdr 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 ～ 4294967295 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip sdr cache-timeout** 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。キャッシュ全体を削除するには、**clear ip sdr** 特権 EXEC コマンドを使用します。

セッション ディレクトリ キャッシュを表示するには、**show ip sdr** 特権 EXEC コマンドを使用します。

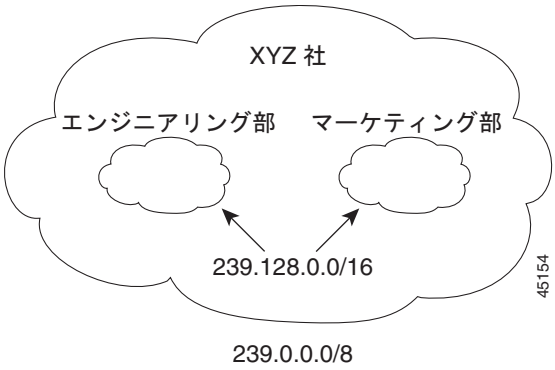
IP マルチキャスト境界の設定

管理用スコープの境界を使用して、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することができません。したがって、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が提供されます。

（注）　マルチキャスト境界および TTL スレッシュホールドは、マルチキャスト ドメインのスコープを制御しますが、TTL スレッシュホールドはこのスイッチでサポートされません。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 スレッシュホールドではなくマルチキャスト境界を使用する必要があります。

図 49-7 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、ネットワークに入ることやそこから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が、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ることやそこから出ることができません。

図 49-7　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、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。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することができません。境界を使用することにより、異なる管理ドメイン内で同じマルチキャスト グループ アドレスを再利用できます。

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、異なる組織が管理する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見なされます。

管理用スコープの境界を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *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、パケットの送信元とな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、送信元に適用するワイルドカード 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 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 3	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip multicast boundary** *access-list-number*	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 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

境界を削除するには、**no ip multicast boundary** 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。

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。

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

基本的な DVMRP 相互運用性機能の設定

ここでは、次の設定情報について説明します。

- 「DVMRP 相互運用性の設定」（P.49-50）（任意）
- 「DVMRP トンネルの設定」（P.49-52）（任意）
- 「DVMRP ネイバーへのネットワーク 0.0.0.0 のアドバタイズ」（P.49-54）（任意）
- 「mrinfo 要求への応答」（P.49-55）（任意）

高度な DVMRP 機能の詳細については、「高度な DVMRP 相互運用性機能の設定」（P.49-55）を参照してください。

DVMRP 相互運用性の設定

PIM を使用するシスコ製マルチキャスト ルータおよびマルチレイヤ スイッチは、DVMRP を使用する他社製のマルチキャスト ルータとの相互運用が可能になります。

PIM 装置は、DVMR プローブ メッセージを待ち受け、接続されたネットワーク上にある DVMRP マルチキャスト ルータをダイナミックに検出します。DVMRP ネイバーが検出されると、PIM 装置は、PIM ドメイン内の到達可能なユニキャスト送信元をアドバタイズする DVMRP レポート メッセージを定期的に送信します。デフォルトでは、直接接続されたサブネットおよびネットワークがアドバタイズされます。装置は DVMRP ルータによって転送されたマルチキャスト パケットを転送し、次に、DVMRP ルータにマルチキャスト パケットを転送します。

MBONE に接続された PIM ルーテッド インターフェイスにアクセス リストを設定することで、DVMRP ルート レポート内でアドバタイズされるユニキャスト ルート数を制限できます。設定していない場合、ユニキャスト ルーティング テーブル内のすべてのルートがアドバタイズされます。

（注） マルチキャスト ルーティングされたプロトコルは、DVMRP のパブリック ドメインの実装です。Cisco ルータおよびマルチレイヤ スイッチを DVMRP ルータに直接接続する場合、または MBONE トンネルを通して DVMRP ルータと相互運用する場合は、マルチキャスト ルーティングされたバージョン 3.8 を使用する必要があります（バージョン 3.8 には、DVMRP の非プルーニング バージョンが実装されています）。Cisco IOS ソフトウェアで作成された DVMRP アドバタイズを使用すると、古いバージョンのマルチキャスト ルーティングされたプロトコルにより、ルーティング テーブルやネイバーのルーティング テーブルが破壊されることがあります。

ip dvmrp metric インターフェイス コンフィギュレーション コマンドを設定することで、アドバタイズされる送信元、および使用されるメトリックを設定できます。特定のユニキャスト ルーティング プロセスによって学習されたすべての送信元を、DVMRP にアドバタイズするように指示することもできます。

DVMRP ルートレポート メッセージが送信されるときに、アドバタイズされる送信元と使用されるメトリックを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *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、パケットの送信元とな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、送信元に適用するワイルドカード 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 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 3	**interface** *interface-id*	MBONE に接続されている、マルチキャスト ルーティングがイネーブルであるインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip dvmrp metric** *metric* [**list** *access-list-number*] [[*protocol process-id*] | [**dvmrp**]]	DVMRP レポートの一連の宛先に関連付けられているメトリックを設定します。 • *metric* に指定できる範囲は 0 ～ 32 です。0 の値は、ルートがアドバタイズされないことを意味します。32 の値は、無限（到達不能）を意味します。 • （任意）**list** *access-list-number* には、ステップ 2 で作成したアクセス リストを入力します。指定されている場合は、アクセス リストと一致するマルチキャスト宛先だけが、設定されたメトリックとともにレポートされます。 • （任意）*protocol process-id* には、**eigrp**、**igrp**、**ospf**、**rip**、**static**、または **dvmrp** などのユニキャスト ルーティング プロトコルの名前と、ルーティング プロトコルのプロセス ID 番号を入力します。指定されている場合は、指定されたルーティング プロトコルによって学習されたルートだけが、DVMRP レポート メッセージでアドバタイズされます。 • （任意）指定されている場合は、**dvmrp** キーワードにより、設定された *metric* を使用して DVMRP ルーティング テーブルのルートをアドバタイズしたり、フィルタリングできます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

メトリックまたはルート マップをディセーブルにするには、**no ip dvmrp metric** *metric* [**list** *access-list-number*] [[*protocol process-id*] | [**dvmrp**]] または **no ip dvmrp metric** *metric* **route-map** *map-name* 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。

より詳細な方法で上記コマンドと同じ結果を得るには、アクセス リストの代わりに、ルート マップ（**ip dvmrp metric** *metric* **route-map** *map-name* 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。ユニキャスト ルートが DVMRP に入る前に、ルート マップ条件にユニキャスト ルートを適用します。

次に、PIM 装置および DVMRP ルータが同じネットワーク セグメントにある場合に、DVMRP 相互運用性を設定する例を示します。この例では、アクセス リスト 1 はネットワーク（198.92.35.0、198.92.36.0、198.92.37.0、131.108.0.0、および 150.136.0.0）を DVMRP ルータにアドバタイズし、アクセス リスト 2 は他のすべてのネットワークのアドバタイズを禁止します（**ip dvmrp metric 0** インターフェイス コンフィギュレーション コマンド）。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip address 131.119.244.244 255.255.255.0
Switch(config-if)# ip pim dense-mode
Switch(config-if)# ip dvmrp metric 1 list 1
Switch(config-if)# ip dvmrp metric 0 list 2
Switch(config-if)# exit
Switch(config)# access-list 1 permit 198.92.35.0 0.0.0.255
Switch(config)# access-list 1 permit 198.92.36.0 0.0.0.255
Switch(config)# access-list 1 permit 198.92.37.0 0.0.0.255
Switch(config)# access-list 1 permit 131.108.0.0 0.0.255.255
Switch(config)# access-list 1 permit 150.136.0.0 0.0.255.255
Switch(config)# access-list 1 deny   0.0.0.0 255.255.255.255
Switch(config)# access-list 2 permit 0.0.0.0 255.255.255.255
```

DVMRP トンネルの設定

ソフトウェアは MBONE への DVMRP トンネルをサポートしています。一端で DVMRP が動作しているルータまたはマルチレイヤ スイッチには、DVMRP トンネルを設定できます。これにより、ソフトウェアはトンネルを介してマルチキャスト パケットを送受信します。この方法によって、パス上のすべてのルータでマルチキャスト ルーティングがサポートされていない場合でも、PIM ドメインを DVMRP ルータに接続できます。2 つのルータ間で DVMRP トンネルを設定できません。

Cisco ルータまたはマルチレイヤ スイッチがトンネルを介して DVMRP を実行している場合は、DVMRP レポート メッセージ内の送信元が、実際のネットワークと同様にアドバタイズされます。また、受信した DVMRP レポート メッセージはキャッシュに格納され、RPF 計算に使用されます。この動作により、トンネルを介して受信されたマルチキャスト パケットの転送をイネーブルにします。

次の場合は、DVMRP トンネルの設定時に IP アドレスをトンネルに割り当てる必要があります。

- トンネルを介して IP パケットを送信する場合
- DVMRP サマライズを実行するようにソフトウェアを設定する場合

トンネルとサブネットのネットワーク番号が異なる場合、サブネットはトンネルを介してアドバタイズされません。この場合は、ネットワーク番号だけがトンネルを介してアドバタイズされます。

DVMRP トンネルを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	標準アクセス リストを作成し、必要な回数だけコマンドを繰り返します。 • *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、パケットの送信元とな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、送信元に適用するワイルドカード 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 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 3	**interface tunnel** *number*	トンネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**tunnel source** *ip-address*	トンネル インターフェイスの送信元アドレスを指定します。スイッチのインターフェイスの IP アドレスを入力します。
ステップ 5	**tunnel destination** *ip-address*	トンネル インターフェイスの宛先アドレスを指定します。マルチキャスト ルーティングされたルータの IP アドレスを入力します。
ステップ 6	**tunnel mode dvmrp**	DVMRP へのトンネルに対してカプセル化モードを設定します。
ステップ 7	**ip address** *address mask* または **ip unnumbered** *type number*	インターフェイスに IP アドレスを割り当てます。 または インターフェイスを番号付けせずに設定します。
ステップ 8	**ip pim** [**dense-mode** | **sparse-mode**]	インターフェイスに PIM モードを設定します。
ステップ 9	**ip dvmrp accept-filter** *access-list-number* [*distance*] **neighbor-list** *access-list-number*	着信 DVMRP レポートに対して許可フィルタを設定します。 デフォルトでは、距離が 0 のすべての宛先レポートが許可されます。すべてのネイバーからのレポートが許可されます。 • *access-list-number* には、ステップ 2 で作成したアクセス リスト番号を指定します。アクセス リストに一致するすべての送信元は、距離とともに DVMRP ルーティング テーブルに格納されます。 • （任意）*distance* には、宛先への管理ディスタンスを入力します。デフォルトでは、DVMRP ルートへの管理ディスタンスは 0 で、ユニキャスト ルーティング テーブル ルートよりも優先されます。送信元へのパスが、1 つはユニキャスト ルーティングによるパス（マルチキャスト ルーティング プロトコルとして PIM を使用）、もう 1 つは DVMRP を使用するパスの 2 つのパスである場合、PIM パスを使用するときは、DVMRP ルートの管理ディスタンスを増加させます。指定できる範囲は 1 ～ 255 です。 • **neighbor-list** *access-list-number* には、ステップ 2 で作成したネイバー リストの番号を入力します。DVMRP レポートは、リスト内のネイバーでだけ許可されます。
ステップ 10	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 11	**show running-config**	設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

フィルタをディセーブルにするには、**no ip dvmrp accept-filter** *access-list-number* [*distance*] **neighbor-list** *access-list-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。

次に、DVMRP トンネルを設定する例を示します。この設定では、Cisco スイッチ上のトンネルの IP アドレスに *unnumbered* が割り当てられます。これにより、トンネルにはポート 1 と同じ IP アドレスが設定されます。トンネルのエンドポイント送信元アドレスは 172.16.2.1 になり、トンネルの接続先であるリモート DVMRP ルータのトンネルのエンドポイント アドレスは 192.168.1.10 になります。トンネルを介して送信されるすべてのパケットは、外部 IP ヘッダーにカプセル化されます。Cisco スイッチは 198.92.37.0 ～ 198.92.37.255 への距離が 100 である着信 DVMRP レポートを受信するように設定されます。

```
Switch(config)# ip multicast-routing
Switch(config)# interface tunnel 0
Switch(config-if)# ip unnumbered gigabitethernet1/1
Switch(config-if)# ip pim dense-mode
Switch(config-if)# tunnel source gigabitethernet1/1
Switch(config-if)# tunnel destination 192.168.1.10
Switch(config-if)# tunnel mode dvmrp
Switch(config-if)# ip dvmrp accept-filter 1 100
Switch(config-if)# interface gigabitethernet1/1
Switch(config-if)# ip address 172.16.2.1 255.255.255.0
Switch(config-if)# ip pim dense-mode
Switch(config)# exit
Switch(config)# access-list 1 permit 198.92.37.0 0.0.0.255
```

DVMRP ネイバーへのネットワーク 0.0.0.0 のアドバタイズ

使用しているスイッチがマルチキャスト ルーティング バージョン 3.6 の装置のネイバーである場合は、ネットワーク 0.0.0.0（デフォルト ルート）を DVMRP ネイバーにアドバタイズするように、ソフトウェアを設定できます。DVMRP デフォルト ルートでは、具体的なルートと一致しないマルチキャスト送信元の RPF 情報が計算されます。

DVMRP のデフォルト ルートを MBONE にアドバタイズしないでください。

インターフェイスの DVMRP ネイバーにネットワーク 0.0.0.0 をアドバタイズするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	DVMRP ルータに接続された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	目的
ステップ 3	**ip dvmrp default-information** {**originate** | **only**}	DVMRP ネイバーにネットワーク 0.0.0.0 をアドバタイズします。 このコマンドは、スイッチがマルチキャスト ルーティング バージョン 3.6 マシンのネイバーである場合に限り使用します。 キーワードの意味は次のとおりです。 • **originate**：0.0.0.0 以外の具体的なルートもアドバタイズできるように指定します。 • **only**：0.0.0.0 以外の DVMRP ルートがアドバタイズされないように指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト ルートのアドバタイズを禁止するには、**no ip dvmrp default-information** 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。

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、Cisco ルータ、およびマルチレイヤ スイッチ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、DVMRP トンネルとすべてのルーテッド インターフェイスを介してネイバーに関する情報を戻します。この情報には、メトリック（常に 1 に設定）、設定された TTL スレッショルド、インターフェイスのステータス、およびさまざまなフラグが含まれます。次の例に示すように、**mrinfo** 特権 EXEC コマンドを使用して、ルータまたはスイッチ自体をクエリーすることもできます。

```
Switch# 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]
```

高度な DVMRP 相互運用性機能の設定

Cisco ルータおよびマルチレイヤ スイッチは PIM を実行し、マルチキャスト パケットをレシーバーに転送し、送信元から受信します。DVMRP ルートを PIM クラウド内に伝播したり、PIM クラウドを経由して伝播することもできます。PIM はこの情報を使用しますが、Cisco ルータおよびマルチレイヤ スイッチでは、DVMRP を実装してマルチキャスト パケットを転送することはありません。

ここでは、次の設定情報について説明します。

- 「DVMRP ユニキャスト ルーティングのイネーブル化」（P.49-56）（任意）
- 「DVMRP の非プルーニング ネイバーの拒否」（P.49-57）（任意）
- 「ルート交換の制御」（P.49-59）（任意）

基本的な DVMRP 機能の詳細については、「基本的な DVMRP 相互運用性機能の設定」（P.49-50）を参照してください。

DVMRP ユニキャスト ルーティングのイネーブル化

マルチキャスト ルーティングおよびユニキャスト ルーティングには個別のトポロジが必要となるため、PIM はマルチキャスト トポロジに従って、ループのない分散ツリーを構築する必要があります。Cisco ルータ、マルチレイヤ スイッチ、およびマルチキャスト ルーティング ベースのマシンは、DVMRP ユニキャスト ルーティングを使用して、DVMRP ユニキャスト ルートを交換します。PIM はこれらのルートにリバースパスを転送できます。

シスコ デバイスは DVMRP マルチキャスト ルーティングを相互に実行しませんが、DVMRP ルートを交換できます。DVMRP ルートは、ユニキャスト トポロジと異なるマルチキャスト トポロジを提供します。これにより、マルチキャスト トポロジを通して PIM を実行し、この結果 MBONE トポロジを通した PIM sparse（疎）モードがイネーブルになります。

DVMRP ユニキャスト ルーティングがイネーブルの場合、ルータまたはスイッチは、DVMRP ルーティング テーブル内の DVMRP レポート メッセージで学習されたルートをキャッシュに格納します。PIM を実行中の場合、これらのルートはユニキャスト ルーティング テーブル内のルートよりも優先される場合があります。そのため、MBONE トポロジがユニキャスト トポロジと異なる場合、PIM を MBONE トポロジで実行することが可能になります。

DVMRP ユニキャスト ルーティングは、すべてのインターフェイスで実行できます。DVMRP トンネルの場合は、DVMRP マルチキャスト ルーティングが使用されます。この機能を使用しても、Cisco ルータおよびマルチレイヤ スイッチ間で DVMRP マルチキャスト ルーティングはイネーブルになりません。ただし、DVMRP 対応マルチキャスト ルータがある場合は、シスコ デバイスで PIM/DVMRP マルチキャスト ルーティングを実行できます。

DVMRP ユニキャスト ルーティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

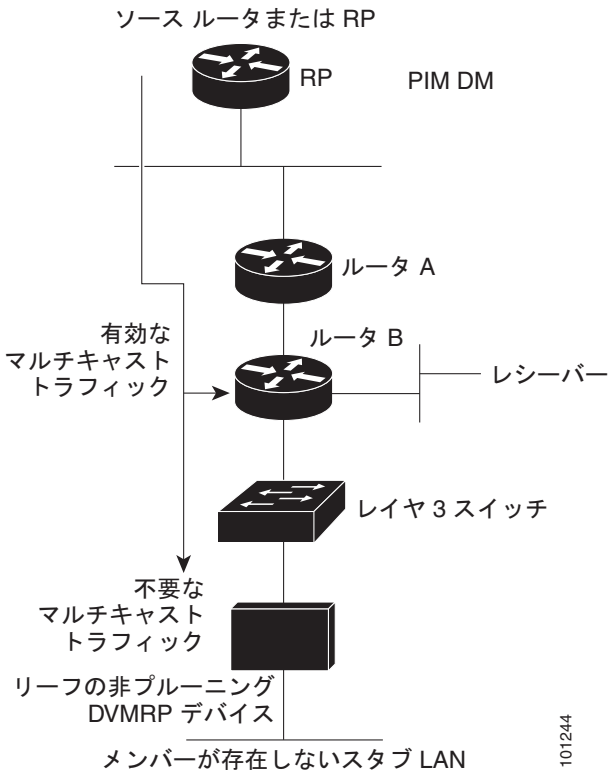
	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip dvmrp unicast-routing**	DVMRP ユニキャスト ルーティングをイネーブルにします（DVMRP ルートを送受信します）。デフォルトでは、この機能はディセーブルになっています。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

この機能をディセーブルにするには、**no ip dvmrp unicast-routing** 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。

DVMRP の非プルーニング ネイバーの拒否

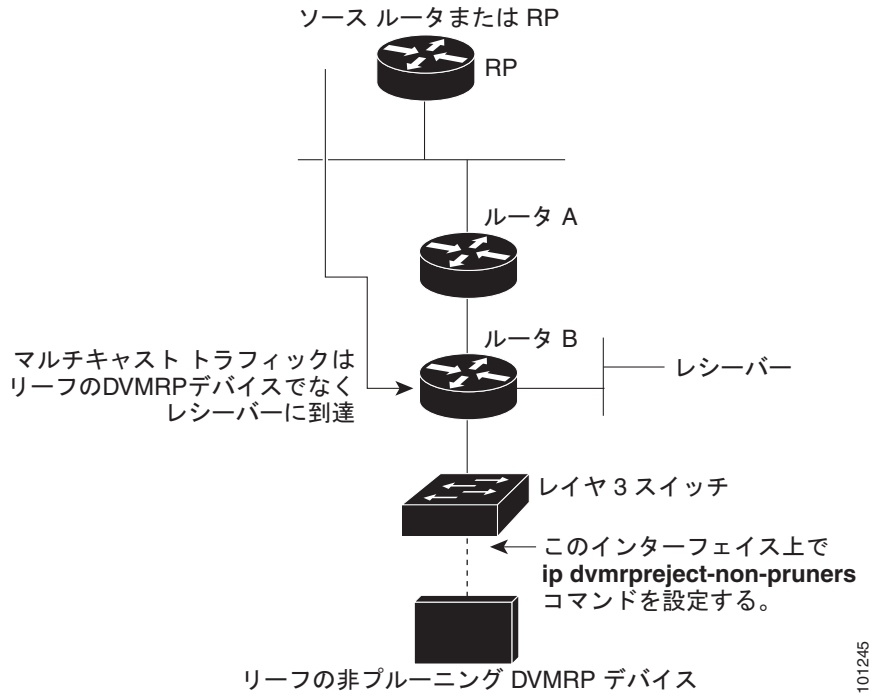
デフォルトでは、DVMRP 機能にかかわらず、シスコ デバイスはすべての DVMRP ネイバーをピアとして受け入れます。ただし、一部の非シスコ デバイスでは、プルーニングできない古いバージョンの DVMRP が実行されているため、転送パケットを常時受信し、帯域幅を浪費します。図 49-8 に、このシナリオを示します。

図 49-8　リーフの非プルーニング DVMRP ネイバー



DVMRP ネイバーで DVMRP プルーニングまたは接合がサポートされていない場合、スイッチとこのネイバーとのピアリング（通信）を防止できます。これを行うには、非プルーニング マシンに接続されたインターフェイスで **ip dvmrp reject-non-pruners** 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、スイッチ（リーフの非プルーニング DVMRP マシンのネイバー）を設定します（図 49-9 を参照）。この場合、スイッチがプルーニング対応フラグの設定されていない DVMRP プローブまたはレポート メッセージを受信すると、Syslog メッセージが記録され、メッセージが廃棄されます。

図 49-9　ルータが非プルーニング DVMRP ネイバーを拒否する例



ip dvmrp reject-non-pruners インターフェイス コンフィギュレーション コマンドを使用すると、ネイバーとのピアリングだけが防止されます。（レシーバー候補へのダウンストリーム方向に）数ホップ離れた拒否されていない非プルーニング ルータが存在する場合、非プルーニング DVMRP ネットワークが存在する場合があります。

非プルーニング DVMRP ネイバーとのピアリングを防止するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	非プルーニング DVMRP ネイバーに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip dvmrp reject-non-pruners**	非プルーニング DVMRP ネイバーとのピアリングを防止します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

この機能をディセーブルにするには、**no ip dvmrp reject-non-pruners** 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。

ルート交換の制御

ここでは、DVMRP ルートに関するシスコ デバイスのアドバタイズを調整する方法について説明します。

- 「アドバタイズされる DVMRP ルート数の制限」（P.49-59）（任意）
- 「DVMRP ルート スレッシュホールドの変更」（P.49-59）（任意）
- 「DVMRP サマリー アドレスの設定」（P.49-60）（任意）
- 「DVMRP 自動サマライズのディセーブル化」（P.49-62）（任意）
- 「DVMRP ルートへのメトリック オフセットの追加」（P.49-62）（任意）

アドバタイズされる DVMRP ルート数の制限

デフォルトでは、DVMRP を実行するためにイネーブル化されたインターフェイス（つまり、DVMRP トンネル、DVMRP ネイバーが検出されたインターフェイス、または **ip dvmrp unicast-routing** インターフェイス コンフィギュレーション コマンドを実行するように設定されたインターフェイス）を介して、7000 DVMRP ルートだけがアドバタイズされます。

DVMRP ルートの制限を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dvmrp route-limit** *count*	DVMRP に対してイネーブル化されたインターフェイスを介してアドバタイズされる DVMRP ルート数を変更します。 このコマンドを使用すると、**ip dvmrp metric** インターフェイス コンフィギュレーション コマンドの設定ミスによって大量のルートが MBONE に入るのを防ぐことができます。 デフォルトでは、7000 のルートがアドバタイズされます。指定できる範囲は 0 ～ 4294967295 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ルート数が制限されないように設定するには、**no ip dvmrp route-limit** 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。

DVMRP ルート スレッシュホールドの変更

デフォルトでは、1 つのインターフェイスにつき、1 分間に 10,000 の DVMRP ルートを受信できます。この速度を超えると、ルート サージが発生した可能性を警告する Syslog メッセージが発行されます。この警告は、通常、装置の設定ミスによって大量のルートが MBONE に入った場合に、短時間で検出を行うために使用されます。

警告をトリガーするルート数のスレッシュホールドを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dvmrp routehog-notification** *route-count*	Syslog メッセージをトリガーするルート数を設定します。 デフォルト値は 10,000 ルートです。指定できる範囲は 1 ～ 4294967295 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip dvmrp routehog-notification** 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。

動作中のルート数を表示するには、**show ip igmp interface** 特権 EXEC コマンドを使用します。このルート数を超えると、*** *ALERT* *** が行に追加されます。

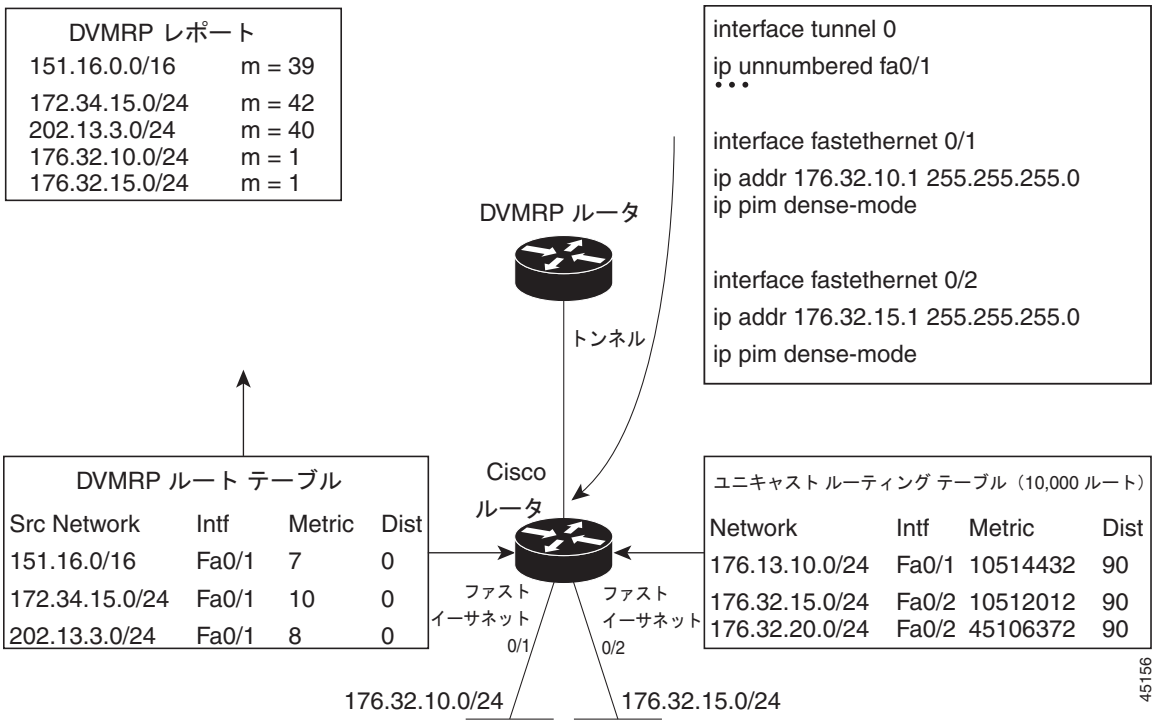
DVMRP サマリー アドレスの設定

デフォルトでは、シスコ デバイスは、ユニキャスト ルーティング テーブル内の接続されたユニキャスト ルートだけ（つまり、ルータに直接接続されたサブネットへのルートだけ）を DVMRP ルート レポート メッセージでアドバタイズします。これらのルートでは、通常の DVMRP のクラスフル ルート サマライズが行われます。このプロセスは、アドバタイズされているルートと、ルートがアドバタイズで経由するインターフェイスが、同じクラスフル ネットワーク内にあるかどうかによって異なります。

図 49-10 に、デフォルト動作の例を示します。この例では、Cisco ルータによって送信される DVMRP レポートに、DVMRP ルータから受信した 3 つの元のルートが含まれています。この DVMRP ルータは、DVMRP メトリックに 32 を追加してポイズンリバースされたものです。これらのルートのあとに、ユニキャスト ルーティング テーブルから取得した、直接接続された 2 つのネットワーク（176.32.10.0/24 および 176.32.15.0/24）のアドバタイズである 2 つのルートがリストされています。DVMRP トンネルはファスト イーサネット ポート 1 と同じ IP アドレスを共有し、直接接続された 2 つのサブネットと同じクラス B ネットワークに分類されるため、これらのルートに対するクラスフル サマライズは実行されません。そのため、DVMRP ルータは、直接接続されたサブネットにこれらの 2 つのルートだけをポイズンリバースし、これらの 2 つのイーサネット セグメント上の送信元によって送信されたマルチキャスト トラフィックに対しては、RPF だけを適切に実行できます。これら 2 つのイーサネット セグメント上にはない、Cisco ルータ背後のネットワーク内の他のマルチキャスト送信元では、DVMRP ルータで RPF チェックは適切に行われず、廃棄されます。

サマリー アドレス（**ip dvmrp summary-address** *address mask* インターフェイス コンフィギュレーション コマンドのアドレスおよびマスクのペアで指定）の範囲内にあるルートの代わりに、サマリー アドレスをアドバタイズするように Cisco ルータを設定できます。この範囲内にあるルートがユニキャスト ルーティング テーブルに少なくとも 1 つ含まれている場合は、サマリー アドレスが DVMRP ルート レポートで送信されます。それ以外の場合は、サマリー アドレスはアドバタイズされません。図 49-10 では、Cisco ルータのトンネル インターフェイスに **ip dvmrp summary-address** コマンドを設定します。そのため、Cisco ルータは、ユニキャスト ルーティング テーブルのネットワーク 176.32.0.0/16 に対し、サマライズされた単一のクラス B アドバタイズだけを送信します。

図 49-10　接続されたユニキャスト ルートだけアドバタイズ（デフォルト）する例



デフォルトのクラスフル自動サマライズがニーズを満たさない場合に DVMRP ルートのサマライズをカスタマイズするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

（注）　設定されたサマリー アドレスをアドバタイズする前に、ユニキャスト ルーティング テーブルに具体的なルートを少なくとも 1 つ設定する必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	DVMRP ルータに接続された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 コマンドを入力します。
ステップ 3	**ip dvmrp summary-address** *address mask* [**metric** *value*]	DVMRP サマリー アドレスを指定します。 • **summary-address** *address mask* には、サマリー IP アドレス、および具体的なルートの代わりにアドバタイズされるマスクを指定します。 • （任意）**metric** *value* には、サマリー アドレスとともにアドバタイズされるメトリックを指定します。デフォルトは 1 です。指定できる範囲は 1 ～ 32 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

サマリー アドレスを削除するには、**no ip dvmrp summary-address** *address mask* [**metric** *value*] 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。

DVMRP 自動サマライズのディセーブル化

デフォルトでは、一部のレベルの DVMRP サマライズがソフトウェアで自動的に実行されます。サマリーだけではなくすべてのルートをアドバタイズする場合は、この機能をディセーブルにします。特別な場合には、すべてのサブネット情報が格納されたネイバー DVMRP ルータを使用して、DVMRP ネットワーク内のマルチキャスト トラフィック フローを詳細に制御できます。一例としては、PIM ネットワークが DVMRP クラウドに複数のポイントで接続されており、具体的な（集約されていない）ルートが DVMRP ネットワークに送信され、PIM クラウド内の各サブネットに対するさらに適切なパスがアドバタイズされる場合などがあります。

ip dvmrp summary-address インターフェイス コンフィギュレーション コマンドを設定し、**no ip dvmrp auto-summary** を設定しなかった場合は、カスタムと自動サマリーの両方を取得します。

DVMRP 自動サマライズをディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no ip dvmrp auto-summary**	DVMRP 自動サマライズをディセーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

自動サマライズを再びイネーブルにするには、**ip dvmrp auto-summary** 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。

DVMRP ルートへのメトリック オフセットの追加

デフォルトでは、スイッチは着信 DVMRP レポートでアドバタイズされた DVMRP ルートのメトリック（ホップ カウント）を 1 つ増加させます。特定のルートの優先度を上下させる場合は、メトリックを変更できます。

たとえば、マルチレイヤ スイッチ A からルートが学習され、より大きなメトリックを持つ同じルートがマルチレイヤ スイッチ B から学習されたとします。スイッチ B を経由するパスの方が高速であるという理由でこのパスを使用する場合は、スイッチ A によって学習されたルートにメトリック オフセットを適用し、スイッチ B によって学習されたメトリックよりもメトリックを大きくすることで、スイッチ B を経由するパスを選択できます。

デフォルト メトリックを変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip dvmrp metric-offset** [**in** | **out**] *increment*	着信レポートでアドバタイズされる DVMRP ルートに追加されたメトリックを変更します。 キーワードの意味は次のとおりです。 • （任意）**in**：増分値が着信 DVMRP レポートに追加され、mrinfo 応答で報告されるように指定します。 • （任意）**out**：増分値が DVMRP ルーティング テーブルのルートに対する発信 DVMRP レポートに追加されるように指定します。 **in** と **out** のどちらも指定されていない場合、**in** がデフォルトになります。 *increment* には、レポート メッセージでアドバタイズされる DVMRP ルータのメトリックに追加する値を指定します。指定できる範囲は 1 ～ 31 です。 **ip dvmrp metric-offset** コマンドがインターフェイス上で設定されていない場合、着信ルートのデフォルトの増分値は 1 となり、発信ルートのデフォルト値は 0 になります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルト設定に戻すには、**no ip dvmrp metric-offset** 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。

IP マルチキャスト ルーティングのモニタおよびメンテナンス

ここでは、IP マルチキャスト ルーティングをモニタする方法およびメンテナンスする方法について説明します。

- 「キャッシュ、テーブル、およびデータベースの消去」（P.49-64）
- 「システムおよびネットワーク統計情報の表示」（P.49-64）
- 「IP マルチキャスト ルーティングのモニタ」（P.49-65）

キャッシュ、テーブル、およびデータベースの消去

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。特定の構造の内容が無効になる場合、または無効である疑いがある場合に、キャッシュ、テーブル、またはデータベースを消去する必要があります。

表 49-5 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、データベースを消去できます。

表 49-5　キャッシュ、テーブル、およびデータベースを消去するためのコマンド

コマンド	目的
clear ip cgmp	Catalyst スイッチによってキャッシュされたすべてのグループ エントリを消去します。
clear ip dvmrp route {* | *route*}	DVMRP ルーティング テーブルからルートを削除します。
clear ip igmp group [*group-name* | *group-address* | *interface*]	IGMP キャッシュからエントリを削除します。
clear ip mroute {* | *group* [*source*]}	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。
clear ip pim auto-rp *rp-address*	Auto-RP キャッシュを消去します。
clear ip sdr [*group-address* | "*session-name*"]	Session Directory Protocol バージョン 2 キャッシュまたは 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） このリリースは、ルート単位の統計情報をサポートしません。

また、リソース使用量を学習したり、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、装置のパケットがネットワーク上で通過するルーティング パスを検出することもできます。

表 49-6 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 49-6　システムおよびネットワーク統計情報を表示するためのコマンド

コマンド	目的
ping [*group-name* | *group-address*]	マルチキャスト グループ アドレスに ICMP エコー要求を送信します。
show ip dvmrp route [*ip-address*]	DVMRP ルーティング テーブルのエントリを表示します。
show ip igmp groups [*group-name* | *group-address* | *type number*]	スイッチに直接接続され、IGMP を通じて学習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*]	インターフェイスについてのマルチキャスト関連情報を表示します。

表 49-6　システムおよびネットワーク統計情報を表示するためのコマンド （続き）

コマンド	目的
show ip mcache [*group* [*source*]]	IP 高速スイッチング キャッシュの内容を表示します。
show ip mpacket [*source-address* | *name*] [*group-address* | *name*] [**detail**]	循環キャッシュヘッダー バッファの内容を表示します。
show ip mroute [*group-name* | *group-address*] [*source*] [**summary**] [**count**] [**active** *kbps*]	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**]	PIM 用に設定されたインターフェイスの情報を表示します。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。
show ip pim neighbor [*type number*]	スイッチ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*]	sparse（疎）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*}	スイッチが Reverse Path Forwarding（RPF）を実行する方法（つまり、ユニキャスト ルーティング テーブルから、DVMRP ルーティング テーブルから、またはスタティック マルチキャスト ルーティングからのいずれか）を表示します。
show ip sdr [*group* | **“***session-name***”** | **detail**]	Session Directory Protocol バージョン 2 のキャッシュを表示します。

IP マルチキャスト ルーティングのモニタ

表 49-7 に示す特権 EXEC コマンドを使用すると、IP マルチキャスト ルータ、パケット、パスをモニタできます。

表 49-7　IP マルチキャスト ルーティングをモニタするためのコマンド

コマンド	目的
mrinfo [*hostname* | *address*] [*source-address* | *interface*]	マルチキャスト ルータまたはマルチレイヤ スイッチとピアリングしているネイバー マルチキャスト装置を特定するために、そのマルチキャスト ルータまたはマルチレイヤ スイッチをクエリーします。
mstat *source* [*destination*] [*group*]	IP マルチキャスト パケットのレートおよび損失情報を表示します。
mtrace *source* [*destination*] [*group*]	指定されたグループのマルチキャスト分散ツリーに対して、送信元から宛先ブランチへのパスを追跡します。