CHAPTER 46

IP マルチキャスト ルーティングの設定

この章では、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 マルチキャストは、ネットワークのリソースをより効率的に使用する方法です。特に、音声やビデオのような、帯域幅を消費するサービスに効果があります。IP マルチキャスト ルーティングを使用すると、ホスト（送信元）は IP 「*マルチキャスト グループ アドレス*」と呼ばれる特殊な形式の IP アドレスを使用し、IP ネットワーク内の任意の場所にあるホスト（レシーバー）のグループにパケットを送信できます。送信側ホストは、マルチキャスト グループ アドレスをパケットの IP 宛先アドレス フィールドに挿入します。IP マルチキャスト ルータおよびマルチレイヤ スイッチは、マルチキャスト グループのメンバに接続されたすべてのインターフェイスから着信した IP マルチキャスト パケットを転送します。どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージを受信します。

この機能を使用するには、スイッチまたはスタック マスターで IP サービス フィーチャ セットが稼働している必要があります。PIM スタブ ルーティング機能を使用するには、スイッチまたはスタック マスターを IP Base イメージで稼働します。

特に明記しない限り、*スイッチ*という用語は、スタンドアロン スイッチおよびスイッチ スタックを指します。

この章で説明する内容は、次のとおりです。

Multicast Source Discovery Protocol（MSDP）の設定の詳細については、第 47 章「MSDP の設定」を参照してください。

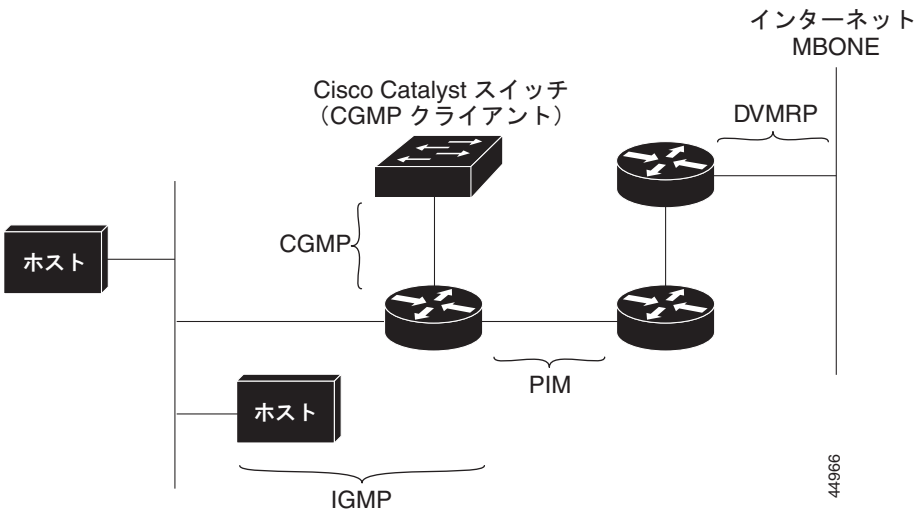
Cisco IP マルチキャスト ルーティングの実装の概要

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、次のプロトコルをサポートしています。

- Internet Group Management Protocol（IGMP）：LAN のホストおよび LAN 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）：ルータおよびマルチレイヤ 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; ディスタンス ベクトル マルチキャスト ルーティング プロトコル）：インターネットの Multicast Backbone（MBONE）に使用されます。ソフトウェアは PIM と DVMRP の相互作用をサポートします。
- Cisco Group Management Protocol（CGMP）：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 46-1 に、これらのプロトコルが動作する IP マルチキャスト環境内の位置を示します。

図 46-1　IP マルチキャスト ルーティング プロトコル



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

IPv4 宛先アドレスと MAC 宛先アドレスが一致しない場合、マルチキャスト パケットは一致しません。スイッチは、一致しないパケットをハードウェア ベースの MAC アドレス テーブルによって転送します。MAC 宛先アドレスが MAC アドレス テーブルにない場合、スイッチは受信したポートと同じ VLAN 内のすべてのポートにパケットをフラッディングします。

ここでは、次の情報について説明します。

- 「IGMP の概要」（P.46-3）
- 「PIM の概要」（P.46-4）
- 「DVMRP の概要」（P.46-9）

- 「CGMP の概要」（P.46-10）

IGMP の概要

IP マルチキャスティングに加入するには、マルチキャスト ホスト、ルータ、およびマルチレイヤ 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 グループに属するネットワーク デバイス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 デバイスです。
- ホストは、クエリアにホスト メンバーシップを通知するためのレポート メッセージ（クエリー メッセージに応答するメッセージ）を送信するレシーバです。

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

どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージを受信します。マルチキャスト グループ内のメンバーシップはダイナミックです。ホストはいつでも加入および脱退できます。マルチキャスト グループ内のメンバの場所または数に制約はありません。ホストは、一度に複数のマルチキャスト グループのメンバにすることができます。マルチキャスト グループのアクティブ状態および所属メンバは、グループや時間によって変化し、マルチキャスト グループを長時間または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 トラフィックには、グループ アドレス（クラス D アドレス）が使用されます。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 アドレスの範囲は 224.0.0.0 ～ 239.255.255.255 です。224.0.0.0 ～ 224.0.0.255 のマルチキャスト アドレスは、ルーティング プロトコルおよびその他のネットワーク制御トラフィックが使用するために予約されています。アドレス 224.0.0.0 は、どのグループにも割り当てられません。

IGMP パケットは、次に示す 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 汎用クエリアは、アドレス 224.0.0.1（サブネット上のすべてのシステム）を宛先とします。
- IGMP グループ固有のクエリーは、クエリー対象グループの IP アドレスを宛先とします。
- IGMP グループ メンバーシップ レポートは、レポート対象グループの IP アドレスを宛先とします。
- IGMPv2（IGMP バージョン 2）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 スタックの中には、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、グループの IP アドレスとなっているものがあります。

IGMPv1

IGMP Version 1（IGMPv1）にはクエリー応答モデルが使用されているため、マルチキャスト ルータおよびマルチレイヤ 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 台または複数存在するか）を判別できます。IGMPv1 では別のプロセスを使用して、ホストをマルチキャスト グループに加入および脱退させることができます。詳細については、RFC 1112 を参照してください。

IGMPv2

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

PIM の概要

PIM は*プロトコルに依存しません*。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、このテーブルの情報を使用してマルチキャスト転送を実行します。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ません。

PIM は、RFC 2362『*Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*』で定義されています。次に示す Internet Engineering Task Force（IETF）インターネット ドラフトを参照してください。

- *『Protocol Independent Multicast (PIM): Motivation and Architecture』*
- *『Protocol Independent Multicast (PIM), Dense Mode Protocol Specification』*
- *『Protocol Independent Multicast (PIM), Sparse Mode Protocol Specification』*
- *『draft-ietf-idmr-igmp-v2-06.txt, Internet Group Management Protocol, Version 2』*
- *『draft-ietf-pim-v2-dm-03.txt, PIM Version 2 Dense Mode』*

PIM のバージョン

PIMv2 は、PIMv1 と比べて次の点が改善されています。

- マルチキャスト グループごとに、複数のバックアップ ランデブー ポイント（RP）を持つアクティブな RP が 1 つ存在します。この単一の RP で、PIMv1 内の同じグループにアクティブな RP が複数ある場合と同様の処理を行います。
- Bootstrap Router（BSR; ブートストラップ ルータ）は耐障害性のある、自動化された RP ディスカバリ メカニズム、および配信メカニズムを提供します。これら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 マッピングを動的に取得できます。
- Sparse Mode（SM; スパース モード）および Dense Mode（DM; デンス 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。SM または DM のいずれか一方だけでなく、SM-DM（sparse-dense モード）を使用してください。
- PIM の Join メッセージおよびプルーニング メッセージを使用すると、複数のアドレス ファミリを柔軟に符号化できます。
- 現在以降の機能オプションを符号化するため、クエリー パケットではなく、より柔軟な hello パケット形式が使用されています。
- RP 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、あるいは指定ルータによって送信されるかは、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、独立したパケットとして処理されます。

PIM のモード

PIM は DM、SM、または PIM SM-DM のいずれかのモードで動作します。PIM DM-SM では、スパース グループとデンス 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配信ツリーが構築されます。DM 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 スイッチで常に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または PIM ネイバーが存在しない場合、PIM DM デバイスがマルチキャスト 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送信され、不要なマルチキャスト トラフィックが停止されます。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。レシーバを含まないブランチが配信ツリーからプルーニングされ、レシーバを含むブランチだけが存続するためです。

プルーニング済みのツリー内ブランチのレシーバがマルチキャスト グループに新規に加入すると、PIM DM デバイスは新しいレシーバを検出し、配信ツリーの送信元方向にすぐに接合メッセージを送信します。アップストリームの PIM DM デバイスが接合メッセージを受信すると、受信したデバイスは接合メッセージが着信したインターフェイスをすぐにフォワーディング ステートにし、マルチキャスト トラフィックのレシーバへの転送を開始します。

PIM-SM

PIM-SM は共有ツリーおよび Shortest-Path-Trees（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 レシーバーに配信します。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）がないかぎり、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と想定します。IGMP を使用してホストがマルチキャスト グループに加入すると、直接接続された PIM-SM デバイスは、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 レシーバを追跡します。また、送信元の先頭ホップ ルータ（*指定ルータ*（DR））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し、これらのトラフィックをすべてのレシーバ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 メッセージが配信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、これらを解除が可能となります。

PIM 対応インターフェイスの数がハードウェアの能力を超え、SPT しきい値が **infinity** に設定された PIM-SM がイネーブルになっている場合、スイッチは一部の直接接続されたインターフェイスに対し、マルチキャスト ルーティング テーブルに（S,G）エントリが存在していなければそのテーブルにエントリを作成しません。スイッチは、これらのインターフェイスからのトラフィックを正しく転送しない場合もあります。

PIM スタブ ルーティング

PIM スタブ ルーティング機能は、すべてのソフトウェア イメージで使用でき、エンド ユーザの近くにルーテッド トラフィックを移動することでリソースの使用状況を低減させます。

（注） IP Base イメージには PIM スタブ ルーティングだけが含まれています。IP サービス イメージには、完全なマルチキャスト ルーティングが含まれます。IP Base イメージを動作させているスイッチ上では、PIM デンス モード、スパース モード、またはデンス - スパース モードで VLAN インターフェイスを設定しようとすると、コンフィギュレーションは許可されません。

PIM スタブ ルーティングを使用するネットワークでは、ユーザに対する IP トラフィックの唯一の許容ルートは、PIM スタブ ルーティングを設定しているスイッチ経由です。PIM 受動インターフェイスは、VLAN などのレイヤ 2 アクセス ドメイン、または他のレイヤ 2 デバイスに接続されているインターフェイスに接続されます。直接接続されたマルチキャスト（IGMP）レシーバおよび送信元だけが、レイヤ 2 アクセス ドメインで許可されます。PIM 受動インターフェイスは、受信した PIM 制御パケットを送信または処理しません。

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

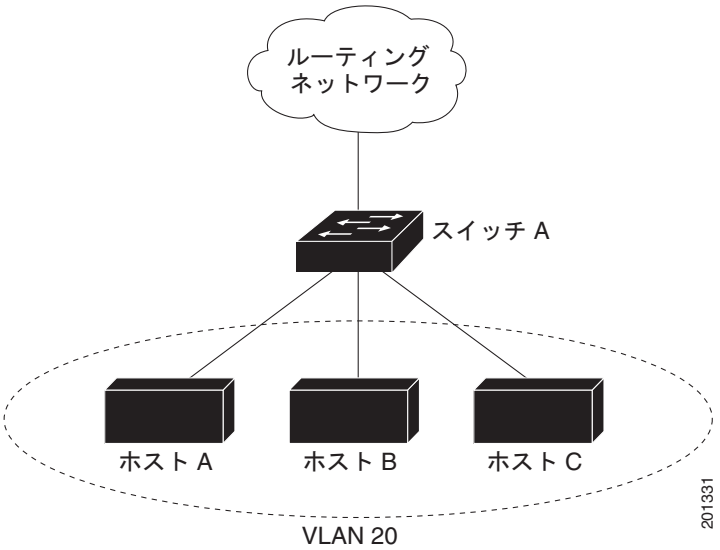
また、PIM スタブ ルーティングをスイッチに設定するときは、EIGRP スタブ ルーティングも設定する必要があります。詳細については、「EIGRP スタブ ルーティング」（P.39-47）を参照してください。

冗長 PIM スタブ ルータ トポロジーはサポートされません。単一のアクセス ドメインにマルチキャスト トラフィックを転送している複数の PIM ルータがある場合、冗長トポロジーが存在します。PIM メッセージはブロックされ、PIM 資産および指定ルータ検出メカニズムは、PIM 受動インターフェイスでサポートされません。PIM スタブ機能では、非冗長アクセス ルータ トポロジーだけがサポートされます。非冗長トポロジーを使用することで、PIM 受動インターフェイスはそのアクセス ドメインで唯一のインターフェイスおよび指定ルータであると想定します。

PIM スタブ機能は、IP Base イメージで実行されます。より新しいソフトウェア バージョンにアップグレードする場合、PIM スタブ コンフィギュレーションはインターフェイスを再設定するまでそのままとなります。

図 46-2 では、スイッチ A ルーテッド アップリンク ポート 25 がルータに接続され、PIM スタブ ルーティングが VLAN 100 インターフェイスとホスト 3 でイネーブルになっています。この設定により、直接接続されたホストはマルチキャスト発信元 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 ルーティングのイネーブル化」（P.46-28）を参照してください。

図 46-2　PIM スタブ ルータ設定



IGMP ヘルパー

PIM スタブ ルーティングによって、ルーテッド トラフィックがエンド ユーザの近くに移動し、ネットワーク トラフィックが軽減されます。スタブ ルータ（スイッチ）に IGMP ヘルパー機能を設定する方法でもトラフィックを軽減できます。

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

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。自動 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 アナウンスメントを受信する候補 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、それらが使用可能であること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 アナウンスメントを受信し、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 アナウンスメントを送信した場合でも、この範囲には 1 つのマッピング キャッシュ エントリだけが作成されます。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 IP が最大である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、静的に設定された RP に変更されます。静的に設定された 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 DM 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、または互いのホット バックアップとして機能します。

BSR

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別の方法です。これにより、ネットワーク内のルータまたはスイッチごとに RP 情報を手動で設定する必要がなくなります。ただし、BSR は IP マルチキャストを使用してグループ /RP マッピング情報を配信する代わりに、特殊な BSR メッセージをホップ単位でフラッディングしてマッピング情報を配信します。

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

選択された BSR によって、Time to Live（TTL; 存続可能時間）値が 1 である BSR メッセージが送信されます。隣接する PIMv2 ルータまたはマルチレイヤ 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。この方法で、BSR メッセージは PIM ドメイン内をホップ単位で移動します。BSR メッセージには現在の BSR の IP アドレスが格納されているため、候補 RP はフラッディング メカニズムを使用し、どのデバイスが選択された BSR であるかを自動的に学習します。

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

マルチキャスト転送および逆経路チェック

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 アドレスが格納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送信します。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ます。そのあと、パケット内の宛先 IP アドレスを使用して、ユニキャスト転送判断を行います。

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 フィールドに格納された、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、ドロップを決定するため、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）チェックを使用します（図 46-3 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、逆経路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りません）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 46-3 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 46-1 により、送信元への逆経路上にあるポートはポート 2 ではなく、ポート 1 であることがわかります。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 に着信します。ルーティング テーブルにより、このポートは送信元への逆経路上にあることがわかります。RPF チェックに合格したため、パケットは発信ポート リスト内のすべてのポートに転送されます。

図 46-3　RPF チェック

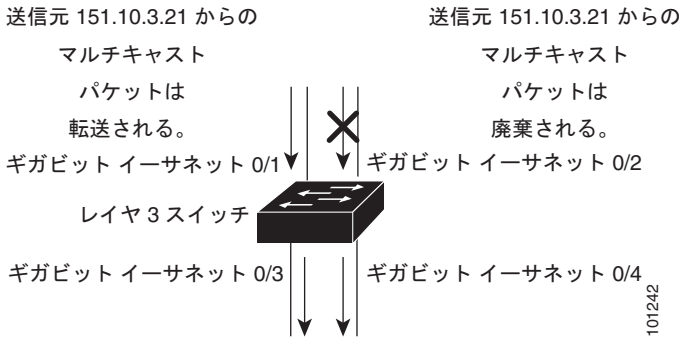


表 46-1　RPF チェックのルーティング テーブル例

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

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を使用して、データグラムを転送します（「PIM DM」（P.46-5）および「PIM-SM」（P.46-5）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（および送信元ツリー ステートが明示されていない場合）、（メンバーがグループに加入している場合は既知である）RP アドレスについて RPF チェックが実行されます。

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

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

DVMRP および PIM DM では送信元ツリーだけが使用され、上記のように RPF が使用されます。

DVMRP の概要

DVMRP は多くのベンダーのデバイスに実装されており、パブリック ドメインでマルチキャスト ルーティング（mroute）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 ネットワークに採用されています。

Cisco ルータおよびマルチレイヤ スイッチでは PIM が動作し、マルチキャスト パケットの DVMRP ネイバーへの転送および、DVMRP ネイバーからの受信を可能にします。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。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 ディスカバリをサポートし、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、送信元ネットワーク ルーティング情報をルートレポート メッセージに格納して定期的に交換し、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、送信元配信ツリーの構築および、RPF によるマルチキャスト転送の実行に使用されます。

DVMRP は DM プロトコルです。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 パケットはまず、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、スイッチ上で CGMP サーバ サポート機能を提供します。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デバイス用の 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、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しないで、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ためのもう 1 つの方法です）。詳細については、第 24 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 と HSRPv1 は両立できません。CGMP 脱退処理と HSRPv1 を同時にイネーブルにできません。ただし、CGMP と HSRPv2 は同時にイネーブルにできます。詳細については、「HSRP のバージョン」（P.42-3）を参照してください。

マルチキャスト ルーティングおよびスイッチ スタック

すべてのマルチキャスト ルーティング プロトコルでは、スタック全体が単一ルータとしてネットワークに認識され、単一のマルチキャスト ルータとして動作します。

スイッチ スタックでは、ルーティング マスター（スタック マスター）は次の機能を実行します。

- スタックの IP マルチキャスト ルーティング機能を実行します。IP マルチキャスト ルーティング プロトコルを完全に初期化して、実行します。
- スタック全体のマルチキャスト ルーティング テーブルを構築して、保持します。
- マルチキャスト ルーティング テーブルをすべてのスタック メンバーに配信します。

スタック メンバーは、次に示す機能を実行します。

- マルチキャスト ルーティング スタンバイ デバイスとして機能し、スタック マスターに障害が発生した場合に処理を引き継ぎます。

スタック マスターに障害が発生すると、すべてのスタック メンバーは自身のマルチキャスト ルーティング テーブルを削除します。新規に選択されたスタック マスターはルーティング テーブルの構築を開始して、そのテーブルをスタック メンバーに配信します。

（注） IP サービス フィーチャ セットが稼働しているスタック マスターで障害が発生し、新しく選択されたスタック マスターで IP ベース フィーチャ セットが稼働している場合、そのスイッチ スタックのマルチキャスト ルーティング機能は失われます。

スタック マスターの選択プロセスについては、第 7 章「スイッチ スタックの管理」を参照してください。

- マルチキャスト ルーティング テーブルを構築しないで、スタック マスターから配信されたマルチキャスト ルーティング テーブルを使用します。

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 46-2 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 46-2　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 のバージョン	バージョン 2
PIM モード	モードは未定義
PIM スタブ ルーティング	未設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル
PIM マルチキャスト境界	なし。
候補 BSR	ディセーブル
候補 RP	ディセーブル
SPT しきい値レート	0 kb/s
PIM ルータ クエリー メッセージ インターバル	30 秒

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

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

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

PIMv2 は BSR を使用して各グループ プレフィックスの RP 設定情報を検出し、PIM ドメイン内のすべてのルータおよびマルチレイヤ スイッチにアナウンスします。自動 RP 機能を組み合わせることにより、PIMv2 BSR と同じ作業を PIMv1 で実行できます。ただし、自動 RP は PIMv1 から独立している、スタンドアロンのシスコ独自のプロトコルで、PIMv2 は IETF 標準の追跡プロトコルです。したがって、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 スイッチ上の自動 RP と相互運用します。詳細については、「自動 RP および BSR 設定時の注意事項」（P.46-13）を参照してください。

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

PIMv1 と PIMv2 が混在する領域内の DM グループは、特殊な設定を行わなくても自動的に相互運用します。

PIMv1 の自動 RP 機能は PIMv2 RP 機能と相互運用するため、PIMv1 と PIMv2 が混在する領域内に SM グループを設定できます。すべての PIMv2 デバイスで PIMv1 を使用できますが、RP を PIMv2 にアップグレードすることを推奨します。PIMv2 への変換を簡単に行うための推奨事項は次のとおりです。

- 領域全体で自動 RP を使用します。
- 領域全体で SM-DM を設定します。

自動 RP がまだ PIMv1 領域に設定されていない場合は、自動 RP を設定してください。詳細については、「Auto-RP の設定」（P.46-31）を参照してください。

自動 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採用してバージョン 2 に移行する方法です。

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

- ブートストラップ メッセージはホップ単位で送信されるため、PIMv1 デバイスの場合、これらのメッセージはネットワーク内の一部のルータおよびマルチレイヤ スイッチに到達しません。このため、ネットワーク内に PIMv1 デバイスがあり、Cisco ルータおよびマルチレイヤ スイッチだけが存在する場合は、自動 RP を使用してください。
- ネットワーク内に他社製のルータが存在する場合は、Cisco PIMv2 ルータまたはマルチレイヤ スイッチに自動 RP マッピング エージェントおよび BSR を設定します。BSR と他社製の PIMv2 ルータ間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。
- シスコ PIMv1 ルータおよびマルチレイヤ スイッチと他社製の PIMv2 ルータを相互運用させる場合は、自動 RP と BSR の両方が必要です。シスコ PIMv2 デバイスを、自動 RP マッピング エージェントと BSR の両方に設定してください。詳細については、「自動 RP および BSR の使用法」（P.46-40）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 DM、SM、または SM-DM 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 処理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 をイネーブルにした場合に、そのほとんどのインターフェイスが発信インターフェイス リストに含まれておらず、IGMP スヌーピングがディセーブルになっている場合は、レプリケーションが増加することにより、発信インターフェイスが回線レートを維持できないこともあります。

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

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

IP マルチキャストをイネーブルにし、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 マルチキャストによる分散スイッチングをイネーブルにします。

	コマンド	目的
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.11-26）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 がイネーブルです（推奨設定）。 PIMv2 モードのインターフェイスに PIMv1 ネイバーが存在する場合、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.46-13）を参照してください。
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、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**：DM 動作をイネーブルにします。 • **sparse-mode**：SM 動作をイネーブルにします。SM を設定する場合は、RP も設定する必要があります。詳細については、「RP の設定」（P.46-29）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。DM-SM 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）コンフィギュレーション ファイルに設定を保存します。

マルチキャス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（SSM）の設定

ここでは、Source-Specific Multicast（SSM）の設定方法を説明します。ここで説明する 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」の章を参照してください。この章で言及する他のコマンドについては、コマンド リファレンス マスター インデックス（オンライン検索）を使用して、該当するマニュアルを参照してください。

SSM 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 用にマルチキャスト グループを設定する場合、SSM 配信ツリー（共有ツリーはない）だけが作成されます。

SSM コンポーネントの概要

SSM は、1 対多のアプリケーション（ブロードキャスト アプリケーション）に最適なデータグラム配信モデルです。SSM は、オーディオおよびビデオのブロードキャスト アプリケーション環境を対象としたシスコの IP マルチキャスト ソリューションの中核的なネットワーキング テクノロジーです。このスイッチは次の SSM 対応コンポーネントをサポートしています。

- Protocol Independent Multicast Source-Specific Mode（PIM-SSM）

  PIM-SSM は、SSM の実装をサポートするルーティング プロトコルで、PIM Sparse Mode（PIM-SM）に基づいています。

- Internet Group Management Protocol version 3（IGMPv3）

  IGMPv3 で SSM を使用するには、Cisco IOS ルータ、アプリケーションが稼働しているホスト、そしてアプリケーション自体が SSM をサポートしている必要があります。

Internet Standard Multicast と SSM の違い

インターネットの現行の IP マルチキャスト インフラストラクチャや多くの企業のイントラネットは、PIM-SM プロトコルと Multicast Source Discovery Protocol（MSDP）に基づいています。これらのプロトコルには、Internet Standard Multicast（ISM）サービス モデルの限界があります。たとえば、ISM では、ネットワークは、実際にマルチキャスト トラフィックを送信しているホストについての情報を維持する必要があります。

ISM サービスは、任意の送信元からマルチキャスト ホスト グループと呼ばれるレシーバー グループへの IP データグラムの配信でなりたっています。マルチキャスト ホスト グループのデータグラム トラフィックは、任意の IP ユニキャスト送信元アドレス S と IP 宛先アドレスとしてのマルチキャスト グループ アドレス G のデータグラムで構成されます。システムは、ホスト グループのメンバーになることによって、このトラフィックを受信します。

ホスト グループのメンバーシップに必要なのは、IGMP version 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 のいずれも、送信元になるのにシグナリングは必要ありません。ただし、SSM では、レシーバーは特定の送信元からのトラフィックの受信または非受信を決めるために（S, G）への加入または脱退を行う必要があります。つまり、レシーバーは加入した（S, G）チャネルからだけトラフィックを受信できます。一方、ISM では、レシーバーは受信するトラフィックの送信元の IP アドレスを知る必要はありません。チャネル加入シグナリングの標準的な方法として、IGMP include モード メンバーシップ レポートの使用が提案されていますが、この手法をサポートしているのは IGMP version 3 だけです。

SSM IP アドレスの範囲

IP マルチキャスト グループ アドレス範囲の設定済みのサブセットに SSM 配信モデルを適用することにより、SSM と ISM サービスを一緒に使用できます。Cisco IOS ソフトウェアでは、224.0.0.0 ～ 239.255.255.255 の IP マルチキャスト アドレス範囲の SSM 設定が可能です。SSM 範囲が定義されている場合、既存の IP マルチキャスト受信アプリケーションが SSM 範囲のアドレスの使用を試行しても、トラフィックを受信できません。

SSM の動作

確立されているネットワークは、IP マルチキャスト サービスが PIM SM に基づいているので、SSM サービスをサポートできます。SSM サービスだけが必要な場合は、ドメイン間の PIM-SM に必要なプロトコル（MSDP、自動 RP、Bootstrap Router（BSR; ブートストラップ ルータ）など）がすべて揃っていないネットワークでも、SSM を単独で導入できます。

PIM-SM 用に設定されているネットワークに SSM を配置する場合、SSM をサポートするのはラストホップ ルータだけです。レシーバーに直接接続されていないルータは SSM をサポートする必要はありません。一般的に、ラストホップ以外のルータに必要なのは、SSM 範囲内の PIM-SM だけです。このようなルータは SSM 範囲内での MSDP シグナリング、登録、PIM-SM 共有ツリー操作を抑制するために、ほかのアクセス コントロール設定が必要になる場合もあります。

SSM を設定しイネーブルにするには、**ip pim ssm** グローバル コンフィギュレーション コマンドを使用します。この設定による影響は次のとおりです。

- SSM 範囲内のグループは、IGMPv3 include モード メンバーシップ レポートを通じて、（S, G）チャネルに加入できます。
- SSM 範囲のアドレスの PIM 動作は、PIM-SM の派生モードである PIM-SSM に変更されます。このモードでは、ルータで生成されるのは PIM（S, G）の join と prune のメッセージだけであり、（S, G）の Rendezvous Point Tree（RPT）や（*, G）の RPT メッセージは生成されません。RPT 動作に関連する着信メッセージは無視されるか拒否されます。着信 PIM 登録メッセージに対しては即座に register-stop メッセージで応答が行われます。ラストホップ ルータ以外のルータでは、PIM-SSM は PIM-SM と下位互換性を保ちます。したがって、ラストホップ ルータ以外のルータは SSM グループに PIM-SM を使用できます（SSM をサポートしていない場合など）。
- SSM 範囲内の Source-Active（SA）メッセージは、受け入れ、生成、転送のいずれも実行されません。

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く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）というシグナルか、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）というシグナルを送信できます。

IGMPv3 は、ISM および SSM と同時に動作可能です。ISM では、exclude 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 を設定する際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

SSM にまだ対応していない、ネットワーク内の既存のアプリケーションは、（S, G）チャネル加入をサポートするように変更されないと、SSM 範囲内では機能しません。そのため、既存のアプリケーションが指定の SSM 範囲内のアドレスを使用する場合、ネットワークで SSM をイネーブルにすると問題が発生することがあります。

アドレス管理に関する制約

SSM をレイヤ 2 スイッチング メカニズムとともに使用する場合は、ある程度のアドレス管理が必要となります。Cisco Group Management Protocol（CGMP）、IGMP スヌーピング、または Router-Port Group Management Protocol（RGMP）でサポートされるのはグループ固有のフィルタリングだけであり、（S, G）チャネル固有のフィルタリングはサポートされていません。同じスイッチド ネットワーク内の異なるレシーバーが異なる（S, G）チャネルを要求し、これらのチャネルが同じグループを共有している場合、レシーバーは上記のような既存メカニズムの利点を活用できません。どちらのレシーバーも、すべての（S, G）チャネル トラフィックを受信し、不要なトラフィックを入力から除外します。SSM は、独立した多くのアプリケーションに SSM 範囲のグループ アドレスを再利用できるので、このような状況では、スイッチド ネットワークのトラフィック フィルタリング機能が低下する可能性があります。そのため、アプリケーションに対して SSM 範囲の IP アドレスをランダムに使用し、SSM 範囲内の 1 つのアドレスがさまざまなアプリケーションに再利用される可能性を小さくすることが重要です。たとえば、TV チャネル セットを提供するアプリケーション サービスで、SSM を使用する場合は、各 TV（S, G）チャネルに異なるグループを使用する必要があります。このようにすれば、同じアプリケーション サービス内の異なるチャネルに複数のレシーバ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

IGMPv3 で使用される新しいメンバーシップ レポート メッセージは、旧型の IGMP スヌーピング 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の詳細については、「IGMP の概要」（P.46-3）を参照してください。

ステート管理の制限事項

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; 最短パスツリー）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、送信元がトラフィックの送信を 3 分間停止すると、（S, G）ステートは削除され、再確立されるのは、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です。PI-SSM では、送信元がアクティブであることをレシーバに通知するメカニズムがないので、レシーバが（S, G）チャネルの受信を要求している限り、（S, G）ステートを維持する必要があります。

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 をイネーブルに設定可能なホストに接続されているインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip pim** {**sparse-mode** | **sparse-dense-mode**}	インターフェイスの PIM をイネーブルにします。**sparse mode** と **sparse-dense mode** のどちら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に対して 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**	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SSM のモニタリング

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
Router# **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。
Router# **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 マッピングの設定

Source Specific Multicast（SSM）マッピング機能は、管理上または技術上の理由からエンド システムで SSM をサポートできないかまたはサポートが望ましくない場合に SSM 移行手段として使用できます。SSM マッピングを使用すると、IGMPv3 をサポートしないレガシー STB へのビデオ配信や、IGMPv3 ホスト スタックを使用しないアプリケーションに SSM を活用できます。

ここで説明する内容は次のとおりです。

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 スパース 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 スパース 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.46-12）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場合は、事前にアクセス コントロール リスト（ACL）を設定して、送信元アドレスにマッピングされるグループ範囲を定義する必要があります。ACL の設定の詳細については、第 35 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使用するには、稼働中の DNS サーバにレコードを追加できなければなりません。稼働中の DNS サーバがない場合は、DNS サーバをインストールする必要があります。

  Cisco Network Registra（CNR; Cisco ネットワーク レジストラ）などの製品が使用できます。詳細については、次の URL にアクセスしてください。

  http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/index.html

SSM マッピングには次のような制約があります。

- SSM マッピング機能では、SSM の利点をすべて得られるわけではありません。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 つ以上の送信元に関連付けられたアプリケーションと関連づけるので、サポートできるアプリケーションは各グループに 1 つだけです。複数の完全な 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できます。
- 完全な SSM への移行ソリューションとして SSM マッピングだけを使用する場合は、ラストホップ ルータの IGMPv3 をイネーブルにする際に十分に注意してください。SSM マッピングと IGMPv3 を両方イネーブルにした場合、すでに IGMPv3 をサポートしている（SSM はサポートしていない）ホストは IGMPv3 グループ レポートを送信します。SSM マッピングは、このような IGMPv3 グループ レポートをサポートしていないので、ルータは送信元をこれらのレポートと正しく関連付けることができません。

SSM マッピングの概要

典型的な 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 チャネルの送信を行うアクティブなサーバは 1 つです。1 つのサーバから複数の TV チャネルへの送信は可能ですが、各チャネルのグループはそれぞれ異なります。このようなネットワーク環境で、ルータが特定のグループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信した場合、レポートの宛先は、そのマルチキャスト グループに関連付けられている TV チャネルの well-known TV サーバになります。

SSM マッピングが設定されている場合、特定グループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信したルータは、レポートを、このグループに関連付けられている well-known 送信元の 1 つ以上のチャネル メンバーシップに変換します。

ルータは、IGMPv1 または IGMPv2 のメンバーシップ レポートを受信すると、SSM マッピングを使用して、そのグループ に 1 つ以上の送信元 IP アドレスを決定します。その後、SSM マッピングによって、そのメンバーシップ レポートが IGMPv3 レポートに変換され、IGMPv3 レポートを受信した場合と同様に処理が続行されます。IGMPv1 または IGMPv2 メンバーシップ レポートの受信が続き、そのグループの SSM マッピングが同じである限り、ルータは PIM join を送信し、グループに加入し続けます。

SSM マッピング機能を使用すると、ラストホップ ルータはスタティックに設定されたルータ上のテーブルまたは DNS サーバを通じて、送信元アドレスを決定できます。スタティックに設定されたテーブルまたは DNS マッピングが変更された場合、ルータは加入しているグループに関連付けられている現在の送信元から脱退します。

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/docs/ios/12_3t/12_3t2/feature/guide/gtssmma.html

スタティック SSM マッピング

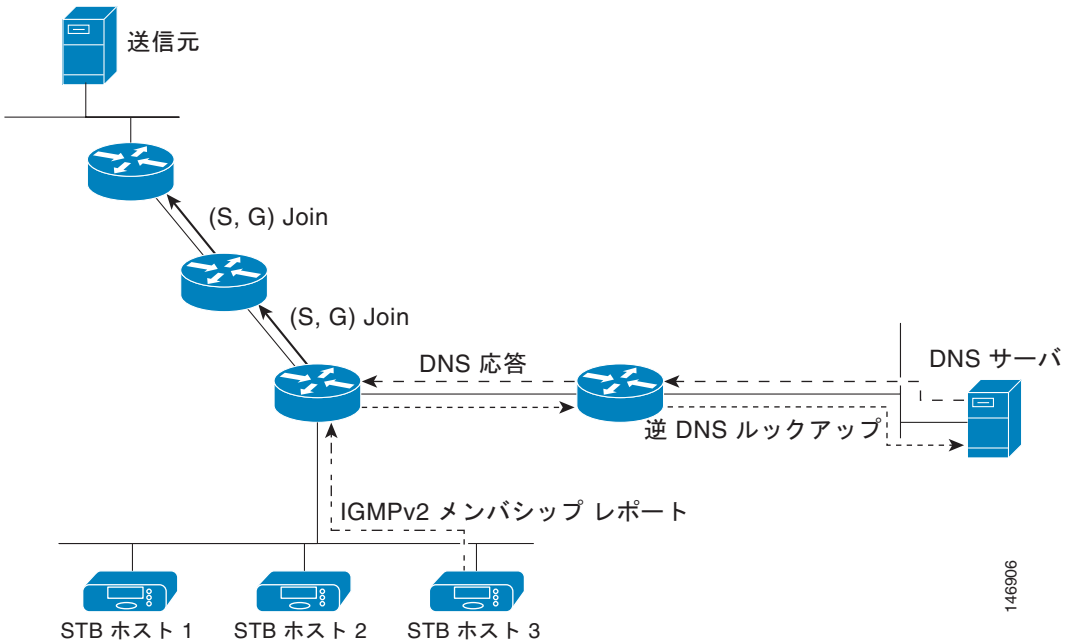
スタティック SSM マッピングでは、ラストホップ ルータは、グループへの送信を行う送信元を決定するために、継続的にスタティック マップを使用します。スタティック SSM マッピングを使用するには、グループ範囲を定義した ACL を設定する必要があります。その後、**ip igmp static ssm-map** グローバル コンフィギュレーション コマンドを使用して、ACL で許可されたグループを送信元にマッピングできます。

DNS が必要とされないか、またはローカルで DNS マッピングが変更される場合、小規模なネットワークではスタティック SSM マッピングを設定できます。設定されたスタティック SSM マッピングは、DNS マッピングよりも優先されます。

DNS ベースの SSM マッピング

DNS ベースの SSM マッピングを使用して、ラストホップ ルータが継続的に逆 DNS ルックアップを実行し、グループに送信する送信元を決定するようにすることも可能です。DNS ベースの SSM マッピングが設定されると、ルータはグループ名を含むドメイン名を構築し、DNS への逆ルックアップを実行します。ルータは IP アドレス リソースを検索し、それらをグループに関連付けられた送信元アドレスとして使用します。SSM マッピングでサポートできる送信元の数は、グループごとに最大 20 です。ルータは各グループに設定されているすべての送信元に加入します（図 46-4 を参照）。

図 46-4　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ようにする SSM マッピング メカニズムによって、TV ブロードキャストの送信元に冗長性を持たせることができます。この場合、ラストホップ ルータは、SSM マッピングを使用し、同じ TV チャネルに対して 2 つのビデオ送信元に同時に加入することにより冗長性を提供します。ただし、ラストホップ ルータでのビデオ トラフィックの重複を防ぐため、ビデオ送信元がサーバ側でスイッチオーバー メカニズムを使用する必要があります。一方のビデオ送信元はアクティブ、もう一方のバックアップ ビデオ送信元はパッシブになります。パッシブの送信元は待機状態になり、アクティブな送信元の障害が検出された場合に、その TV チャネルにビデオ トラフィックを送信します。サーバ側のスイッチオーバー メカニズムによって、実際にその TV チャネルにビデオ トラフィックを送信するサーバは 1 つだけになります。

G1、G2、G3、G4 を含むグループの 1 つ以上の送信元アドレスを検索するには、DNS サーバに次のような DNS レコードを設定する必要があります。

```
G4.G3.G2.G1 [multicast-domain] [timeout]IN A source-address-1
    IN A source-address-2
    IN A source-address-n
```

DNS リソース レコードの詳細については、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/docs/ios/12_3t/12_3t2/feature/guide/gtssmma.html

SSM マッピングの設定

ここで説明する内容は次のとおりです。

- 「スタティック SSM マッピングの設定」（P.46-22）（必須）
- 「DNS ベースの SSM マッピングの設定」（P.46-23）（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.46-24）（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、このコマンドによって DNS ベースの SSM マッピングがイネーブルになります。
ステップ 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 コマンドによって DNS ベースの SSM マッピングがイネーブルになります。

	コマンド	目的
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決まります。 **（注）** 追加のスタティック SSM マッピングを設定することもできます。SSM マッピングを追加設定した場合、ルータが SSM 範囲のグループの IGMPv1 または IGMPv2 のメンバーシップ レポートを受信すると、スイッチは、設定されている各 **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。スイッチは各グループに最大 20 の送信元を関連付けます。
ステップ 5	必要な場合は、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**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

DNS ベースの SSM マッピングの設定

DNS ベースの SSM マッピングを設定するには、DNS サーバ ゾーンを作成するか、または既存のゾーンにレコードを追加する必要があります。DNS ベースの SSM マッピングを使用するルータが他の目的にも DNS を使用している場合は、通常の設定の DNS サーバを使用する必要があります。そのルータで使用されている DNS 実装が DNS ベースの SSM マッピングだけの場合は、ルート ゾーンが空であるか、またはそれ自身を指すようなフォールス DNS セットアップが可能です。

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** コマンドによって DNS ベースの SSM マッピングがイネーブルになります。実行コンフィギュレーションに保存されるのは、このコマンドを **no** 形式で使用した場合だけです。 **（注）** DNS ベースの SSM マッピングがディセーブルになっている場合、このコマンドを使用すると、DNS ベースの SSM マッピングが再度イネーブルになります。
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 プレフィックスを変更します。 デフォルトでは、スイッチは *ip-addr.arpa* ドメイン プレフィックスを使用します。
ステップ 5	**ip name-server** *server-address1* [*server-address2... server-address6*]	1 つまたは複数のネーム サーバのアドレスを指定して、名前およびアドレスの解決に使用します。

	コマンド	目的
ステップ 6	必要な場合は、ステップ 5 を反復し、追加の DNS サーバを設定して冗長構成にします。	—
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**	入力内容を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SSM マッピングを使用したスタティック トラフィック転送の設定

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 マッピングによるスタティック 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 マッピングとスタティックに設定された SSM マッピングのいずれかで機能します。
ステップ 3	**ip igmp static-group** *group-address* **source ssm-map**	そのインターフェイスから（S, G）チャネルへのスタティック転送用の SSM マッピングを設定します。 このコマンドは、特定グループに SSM トラフィックをスタティックに転送する場合に使用します。チャネルの送信元アドレスを決定するには DNS ベースの SSM マッピングを使用します。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SSM マッピングのモニタリング

SSM マッピングを監視するには、表 46-3 の特権 ECEC コマンドを使用します。

表 46-3　SSM マッピングのモニタリングに使用するコマンド

コマンド	目的
show ip igmp ssm-mapping	SSM マッピングについての情報を表示します。
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ているレシーバーおよび IGMP によって取得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。

表 46-3　SSM マッピングのモニタリングに使用するコマンド （続き）

コマンド	目的
show host	デフォルトのドメイン名、名前検索サービスの方式、サーバ ホスト名のリスト、およびキャッシュに格納されている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。

Source-Specific Multicast（SSM）の設定

ここでは、Source-Specific Multicast（SSM）の設定方法を説明します。

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 用にマルチキャスト グループを設定する場合、SSM 配信ツリー（共有ツリーはない）だけが作成されます。

SSM コンポーネントの概要

SSM は、1 対多のアプリケーション（ブロードキャスト アプリケーション）に最適なデータグラム配信モデルです。SSM は、オーディオおよびビデオのブロードキャスト アプリケーション環境を対象としたシスコの IP マルチキャスト ソリューションの中核的なネットワーキング テクノロジーです。このスイッチは次の SSM 対応コンポーネントをサポートしています。

- Protocol Independent Multicast Source-Specific Mode（PIM-SSM）

  PIM-SSM は、SSM の実装をサポートするルーティング プロトコルで、PIM Sparse Mode（PIM-SM）に基づいています。

- Internet Group Management Protocol version 3（IGMPv3）

  IGMPv3 で SSM を使用するには、Cisco IOS ルータ、アプリケーションが稼働しているホスト、そしてアプリケーション自体が SSM をサポートしている必要があります。

Internet Standard Multicast と SSM の違い

インターネットの現行の IP マルチキャスト インフラストラクチャや多くの企業のイントラネットは、PIM-SM プロトコルと Multicast Source Discovery Protocol（MSDP）に基づいています。これらのプロトコルには、Internet Standard Multicast（ISM）サービス モデルの限界があります。たとえば、ISM では、ネットワークは、実際にマルチキャスト トラフィックを送信しているホストについての情報を維持する必要があります。

ISM サービスは、任意の送信元からマルチキャスト ホスト グループと呼ばれるレシーバー グループへの IP データグラムの配信でなりたっています。マルチキャスト ホスト グループのデータグラム トラフィックは、任意の IP ユニキャスト送信元アドレス S と IP 宛先アドレスとしてのマルチキャスト グループ アドレス G のデータグラムで構成されます。システムは、ホスト グループのメンバーになることによって、このトラフィックを受信します。

ホスト グループのメンバーシップに必要なのは、IGMP version 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 のいずれも、送信元になるのにシグナリングは必要ありません。ただし、SSM では、レシーバーは特定の送信元からのトラフィックの受信または非受信を決めるために（S, G）への加入または脱退を行う必要があります。つまり、レシーバーは加入した（S, G）チャネルからだけトラフィック

を受信できます。一方、ISM では、レシーバーは受信するトラフィックの送信元の IP アドレスを知る必要はありません。チャネル加入シグナリングの標準的な方法として、IGMP include モード メンバーシップ レポートの使用が提案されていますが、この手法をサポートしているのは IGMP version 3 だけです。

SSM IP アドレスの範囲

IP マルチキャスト グループ アドレス範囲の設定済みのサブセットに SSM 配信モデルを適用することにより、SSM と ISM サービスを一緒に使用できます。Cisco IOS ソフトウェアでは、224.0.0.0 ～ 239.255.255.255 の IP マルチキャスト アドレス範囲の SSM 設定が可能です。SSM 範囲が定義されている場合、既存の IP マルチキャスト受信アプリケーションが SSM 範囲のアドレスの使用を試行しても、トラフィックを受信できません。

SSM の動作

確立されているネットワークは、IP マルチキャスト サービスが PIM SM に基づいているので、SSM サービスをサポートできます。SSM サービスだけが必要な場合は、ドメイン間の PIM-SM に必要なプロトコル（MSDP、自動 RP、Bootstrap Router（BSR; ブートストラップ ルータ）など）がすべて揃っていないネットワークでも、SSM を単独で導入できます。

PIM-SM 用に設定されているネットワークに SSM を配置する場合、SSM をサポートするのはラストホップ ルータだけです。レシーバーに直接接続されていないルータは SSM をサポートする必要はありません。一般的に、ラストホップ以外のルータに必要なのは、SSM 範囲内の PIM-SM だけです。このようなルータは SSM 範囲内での MSDP シグナリング、登録、PIM-SM 共有ツリー操作を抑制するために、ほかのアクセス コントロール設定が必要になる場合もあります。

SSM を設定しイネーブルにするには、**ip pim ssm** グローバル コンフィギュレーション コマンドを使用します。この設定による影響は次のとおりです。

- SSM 範囲内のグループは、IGMPv3 include モード メンバーシップ レポートを通じて、（S, G）チャネルに加入できます。
- SSM 範囲のアドレスの PIM 動作は、PIM-SM の派生モードである PIM-SSM に変更されます。このモードでは、ルータで生成されるのは PIM（S, G）の join と prune のメッセージだけであり、（S, G）の Rendezvous Point Tree（RPT）や（*, G）の RPT メッセージは生成されません。RPT 動作に関連する着信メッセージは無視されるか拒否されます。着信 PIM 登録メッセージに対しては即座に register-stop メッセージで応答が行われます。ラストホップ ルータ以外のルータでは、PIM-SSM は PIM-SM と下位互換性を保ちます。したがって、ラストホップ ルータ以外のルータは SSM グループに PIM-SM を使用できます（SSM をサポートしていない場合など）。
- SSM 範囲内の Source-Active（SA）メッセージは、受け入れ、生成、転送のいずれも実行されません。

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く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）というシグナルか、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）というシグナルを送信できます。

IGMPv3 は、ISM および SSM と同時に動作可能です。ISM では、exclude 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 を設定する際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

SSM にまだ対応していない、ネットワーク内の既存のアプリケーションは、（S, G）チャネル加入をサポートするように変更されないと、SSM 範囲内では機能しません。そのため、既存のアプリケーションが指定の SSM 範囲内のアドレスを使用する場合、ネットワークで SSM をイネーブルにすると問題が発生することがあります。

アドレス管理に関する制約

SSM をレイヤ 2 スイッチング メカニズムとともに使用する場合は、ある程度のアドレス管理が必要となります。Cisco Group Management Protocol（CGMP）、IGMP スヌーピング、または Router-Port Group Management Protocol（RGMP）でサポートされるのはグループ固有のフィルタリングだけであり、（S, G）チャネル固有のフィルタリングはサポートされていません。同じスイッチド ネットワーク内の異なるレシーバーが異なる（S, G）チャネルを要求し、これらのチャネルが同じグループを共有している場合、レシーバーは上記のような既存メカニズムの利点を活用できません。どちらのレシーバーも、すべての（S, G）チャネル トラフィックを受信し、不要なトラフィックを入力から除外します。SSM は、独立した多くのアプリケーションに SSM 範囲のグループ アドレスを再利用できるので、このような状況では、スイッチド ネットワークのトラフィック フィルタリング機能が低下する可能性があります。そのため、アプリケーションに対して SSM 範囲の IP アドレスをランダムに使用し、SSM 範囲内の 1 つのアドレスがさまざまなアプリケーションに再利用される可能性を小さくすることが重要です。たとえば、TV チャネル セットを提供するアプリケーション サービスで、SSM を使用する場合は、各 TV（S, G）チャネルに異なるグループを使用する必要があります。このようにすれば、同じアプリケーション サービス内の異なるチャネルに複数のレシーバ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

IGMPv3 で使用される新しいメンバーシップ レポート メッセージは、旧型の IGMP スヌーピング 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、「Configuring IP Multicast Routing」の章の「Configuring IGMP Version 3」の項を参照してください。

ステート管理の制限事項

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; 最短パスツリー）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、送信元がトラフィックの送信を 3 分間停止すると、（S, G）ステートは削除され、再確立されるのは、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です。PI-SSM では、送信元がアクティブであることをレシーバに通知するメカニズムがないので、レシーバが（S, G）チャネルの受信を要求している限り、（S, G）ステートを維持する必要があります。

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。この手順は任意です。

	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 をイネーブルに設定可能なホストに接続されているインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip pim** {**sparse-mode** | **sparse-dense-mode**}	インターフェイスの PIM をイネーブルにします。**sparse mode** と **sparse-dense mode** のどちら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に対して 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。

SSM のモニタリング

SSM を監視するには、特権 EXEC モードで次のコマンドを使用します。

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。

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。 IP ベース イメージを実行しているスイッチでは、指定されたインターフェイスが、**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る VLAN インターフェイスである SVI である必要があります。他のすべてのソフトウェアでは、指定されたインターフェイスは任意のルーテッド インターフェイスに設定できます。
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 running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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 ルーティングがイネーブルになっており、スイッチ A の PIM アップリンク ポート 25 はルーテッド アップリンク ポートとして設定されています（**spare-dense-mode** がイネーブル）。図 46-2 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設定されています。

```
Switch(config)# ip multicast-routing distributed
Switch(config)# interface GigabitEthernet3/0/25
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 GigabitEthernet3/0/20
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 GigabitEthernet3/0/20
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 GigabitEthernet3/0/25 v2/SD 1 30 1 3.1.1.2
100.1.1.1 Vlan100 v2/P 0 30 1 100.1.1.1
10.1.1.1 GigabitEthernet3/0/20 v2/P 0 30 1 10.1.1.1
```

これらの特権 EXEC コマンドを使用すると、PIM スタブの設定およびステータスについての情報が表示されます。

- **show ip pim interface** では、各インターフェイスでイネーブルになっている PIM スタブが表示されます。
- **show ip igmp detail** では、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が表示されます。
- **show ip igmp mroute** では、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ることを確認できます。

RP の設定

インターフェイスが SM-DM で、グループをスパース 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。ここに記載するいくつかの方法を使用できます。

- 「マルチキャスト グループへの RP の手動割り当て」（P.46-30）
- 「Auto-RP の設定」（P.46-31）（PIMv1 から独立した、スタンドアロンのシスコ独自のプロトコル）
- 「PIMv2 BSR の設定」（P.46-36）（IETF 標準の追跡プロトコル）

動作中の PIM バージョン、およびネットワーク内のルータ タイプに応じて、自動 RP、BSR、またはこれらを組み合わせて使用できます。詳細については、「PIMv1 および PIMv2 の相互運用性」（P.46-13）および「自動 RP および BSR 設定時の注意事項」（P.46-13）を参照してください。

マルチキャスト グループへの RP の手動割り当て

ここでは、RP を手動で割り当てる方法について説明します。ダイナミック メカニズム（自動 RP や BSR など）を使用してグループの RP を取得する場合、RP を手動で割り当てる必要はありません。

マルチキャスト トラフィックの送信側は、送信元の先頭ホップ ルータ（指定ルータ）から受信して RP に転送される登録メッセージを通し、自身の存在をアナウンスします。マルチキャスト パケットの受信側は RP を使用し、マルチキャスト グループに加入します。この場合は、明示的な Join メッセージが使用されます。RP はマルチキャスト グループのメンバではなく、マルチキャスト送信元およびグループ メンバの「*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 DM 技術を使用し、グループをデンスとして処理します。

RP のアドレスを手動で設定するには、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、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 DM 技術を使用し、グループをデンスとして処理します。 1 台の PIM デバイスを、複数のグループの RP にできます。1 つの PIM ドメイン内で一度に使用できる RP アドレスは、1 つだけです。アクセス リスト条件により、デバイスがどのグループの RP であるかを指定します。 • *ip-address* には、RP のユニキャスト アドレスをドット付き 10 進表記で入力します。 • （任意）*access-list-number* を指定する場合は、1 ～ 99 の IP 標準アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • （任意）**override** キーワードを指定すると、このコマンドによって設定された RP と、自動 RP または BSR で取得された RP との間に矛盾が生じた場合に、このコマンドによって設定された RP が優先されます。

	コマンド	目的
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 グループのアドレスを入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在す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）コンフィギュレーション ファイルに設定を保存します。

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

```
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

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

- ネットワーク内で複数の RP を使用し、複数のグループ範囲を処理する作業が簡単になります。
- 複数の RP 間で負荷を分散し、グループに加入するホストの場所に従って RP を配置できます。
- PIM ネットワーク内のすべてのルータおよびマルチレイヤ 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、接続問題を引き起こす要因が取り除かれます。

自動 RP を設定するときには、次の注意事項に従ってください。

- PIM を SM または SM-DM に設定し、自動 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（「マルチキャスト グループへの RP の手動割り当て」（P.46-30）を参照）。
- ルーテッド インターフェイスが SM に設定されていると、すべてのデバイスが自動 RP グループの手動 RP アドレスによって設定されている場合も、自動 RP を使用できます。
- ルーテッド インターフェイスが SM で設定され、**ip pim autorp listener** グローバル コンフィギュレーション コマンドを入力する場合、すべてのデバイスが自動 RP グループの手動 RP アドレスを使用して設定されていなくても、自動 RP は引き続き使用できます。

ここでは、自動 RP を設定する方法について説明します。

- 「新規インターネットワークでの自動 RP の設定」（P.46-32）（任意）

- 「既存の SM クラウドへの自動 RP の追加」（P.46-32）（任意）
- 「問題のある RP への Join メッセージの送信禁止」（P.46-33）（任意）
- 「着信 RP アナウンスメント メッセージのフィルタリング」（P.46-34）（任意）

概要については、「Auto-RP」（P.46-7）を参照してください。

新規インターネットワークでの自動 RP の設定

新規インターネットワーク内に自動 RP を設定している場合は、すべてのインターフェイスが SM-DM に設定されるため、デフォルトの RP は不要です。「既存の SM クラウドへの自動 RP の追加」（P.46-32）に記載された手順に従ってください。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 SM クラウドへの自動 RP の追加

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

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

	コマンド	目的
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 グループのアドレス範囲を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 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 TTL 値を指定し、RP ディスカバリ パケットを制限します。ホップ数内にあるすべてのデバイスは、送信元デバイスから自動 RP ディスカバリ メッセージを受信します。これらのメッセージは他のデバイスに対し、矛盾（グループ /RP 範囲の重なりなど）を回避するために使用されるグループ /RP マッピングを通知します。デフォルト設定はありません。有効値は 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** **show ip pim rp mapping** **show ip pim rp**	設定を確認します。 関連するマルチキャスト ルーティング エントリとともに保管されているアクティブな RP を表示します。 ルーティング テーブルに保管されている情報を表示します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

候補 RP として設定された PIM デバイスを解除するには、**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 アナウンスメントを送信する例を示します。ポート 1 の IP アドレスが RP です。アクセス リスト 5 には、このスイッチが 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 gigabitethernet0/1 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 メッセージの送信禁止

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

自動 RP によってアドバタイズされるすべての RP を許可し、他のすべての RP をデフォルトで拒否するには、**ip pim accept-rp auto-rp** グローバル コンフィギュレーション コマンドを使用します。この手順は任意です。

すべてのインターフェイスが SM の場合はデフォルト設定の RP を使用し、既知のグループ 224.0.1.39 および 224.0.1.40 をサポートします。自動 RP はこれら 2 つの既知のグループを使用し、RP マッピング情報を収集、配信します。**ip pim accept-rp auto-rp** コマンドが設定されている場合は、RP を許可する別の **ip pim accept-rp** コマンドを次のように設定してください。

```
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 アナウンスメント メッセージのフィルタリング

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

着信 RP アナウンスメント 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 アナウンスメント メッセージをフィルタリングします。 ネットワーク内のマッピング エージェントごとに、このコマンドを入力します。このコマンドを使用しないと、すべての着信 RP アナウンスメント メッセージがデフォルトで許可されます。 **rp-list** *access-list-number* を指定する場合は、候補 RP アドレスのアクセス リストを設定します。アクセス リストが許可されている場合は、**group-list** *access-list-number* 変数で指定されたグループ範囲に対してアクセス リストを使用できます。この変数を省略すると、すべてのマルチキャスト グループにフィルタが適用されます。 複数のマッピング エージェントを使用する場合は、グループ /RP マッピング情報に矛盾が生じないようにするため、すべてのマッピング エージェント間でフィルタを統一する必要があります。

	コマンド	目的
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。 • どのルータおよびマルチレイヤ スイッチからの候補 RP アナウンスメント（rp-list Access Control List（ACL; アクセス コントロール リスト））がマッピング エージェントによって許可されるかを指定するアクセス リストを作成します。 • 許可または拒否するマルチキャスト グループの範囲を指定するアクセス リスト（グループリスト ACL）を作成します。 • *source* には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在す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）コンフィギュレーション ファイルに設定を保存します。

着信 RP アナウンスメント 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、候補 RP アナウンスメントが不正な候補 RP から許可されないようにするために使用される自動 RP マッピング エージェントの設定例を示します。

```
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 2 つのデバイス（172.16.5.1 および 172.16.2.1）からの候補 RP アナウンスだけを許可します。マッピング エージェントは 2 つのデバイスからの候補 RP アナウンスメントのうち、グループ範囲が 224.0.0.0 ～ 239.255.255.255 であるマルチキャスト グループ宛てのアナウンスメントだけを許可します。マッピング エージェントは、ネットワーク内の他のデバイスからの候補 RP アナウンスメントを許可しません。さらに、候補 RP アナウンスメントが 239.0.0.0 ～ 239.255.255.255 の範囲のグループに宛てたものである場合、マッピング エージェントは 172.16.5.1 または 172.16.2.1 からの候補 RP アナウンスメントを許可しません。この範囲は、管理の有効範囲付きアドレス範囲です。

PIMv2 BSR の設定

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

- 「PIM ドメイン境界の定義」（P.46-36）（任意）
- 「IP マルチキャスト境界の定義」（P.46-37）（任意）
- 「候補 BSR の設定」（P.46-38）（任意）
- 「候補 RP の設定」（P.46-39）（任意）

概要については、「BSR」（P.46-7）を参照してください。

PIM ドメイン境界の定義

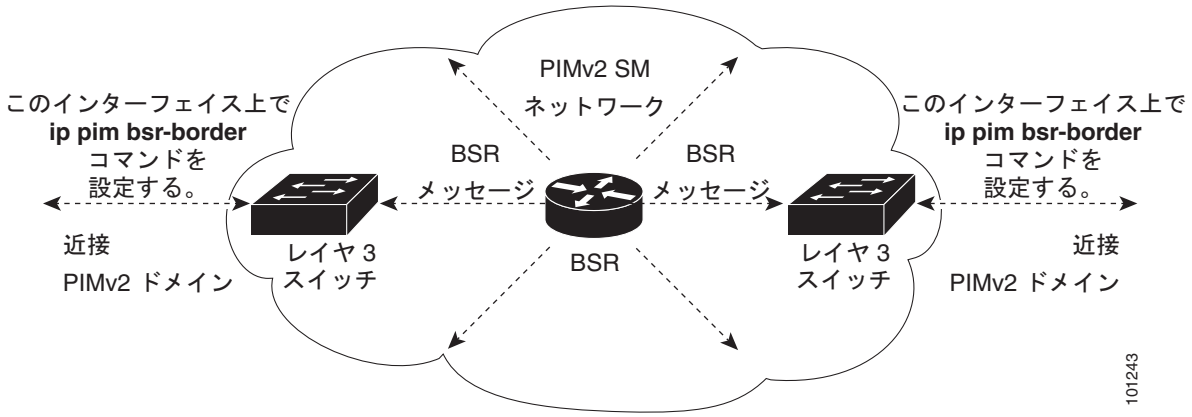
IP マルチキャストの普及に伴い、PIMv2 ドメインと別の PIMv2 ドメインが境界を挟んで隣接する場合が増えています。これらの 2 つのドメインは同じ RP、BSR、候補 RP、候補 BSR のセットを共有していないことが多いため、PIMv2 BSR メッセージがドメインの内外に流れないようにする必要があります。これらメッセージのドメイン境界通過を許可すると、通常の BSR 選択メカニズムに悪影響が及んだり、境界に位置するすべてのドメインで単一の BSR が選択されたり、候補 RP アドバタイズメントが共存し、間違ったドメイン内で RP が選択されたりします。

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。 境界に位置する他の PIM ドメインに接続されているインターフェイスごとに、このコマンドを入力します。このコマンドを実行すると、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示されます（図 46-5 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）コンフィギュレーション ファイルに設定を保存します。

PIM 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 46-5　PIMv2 BSR メッセージの抑制



IP マルチキャスト境界の定義

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

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、自動 RP 情報を伝達するマルチキャスト アドレス 224.0.1.39 および 224.0.1.40 を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在す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）コンフィギュレーション ファイルに設定を保存します。

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、自動 RP 情報を拒否する IP マルチキャスト境界のコンフィギュレーション例の一部を示します。

```
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 gigabitethernet1/0/1
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 として機能するデバイスは、他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。

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*]	候補 BSR となるようにスイッチを設定します。 • *interface-id* には、スイッチを候補 BSR に設定するときに BSR アドレスの取得元となる、スイッチ上のインターフェイスを入力します。このインターフェイスは PIM を使用してイネーブルにする必要があります。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • *hash-mask-length* には、ハッシュ機能を呼び出す前に、グループ アドレスとの AND 条件となるマスク長（最大 32 ビット）を指定します。ハッシュ元が同じであるすべてのグループは、同じ RP に対応します。たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。 • （任意）*priority* を指定する場合は、0 ～ 255 の番号を入力します。プライオリティが大きな BSR が優先されます。このプライオリティ値が同じである場合は、大きな IP アドレスを持つデバイスが BSR として選択されます。デフォルトは 0 です。
ステップ 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）コンフィギュレーション ファイルに設定を保存します。

候補 BSR として設定されたデバイスを解除するには、**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 の設定例を示します。この例では、アドバタイズ済み BSR アドレスとしてポートの IP アドレス 172.21.24.18 を、hash-mask-length として 30 ビットを使用します。プライオリティは 10 です。

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

候補 RP の設定

候補 RP を、1 つまたは複数設定できます。BSR と同様、RP は他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。RP は IP マルチキャスト アドレス スペース全体、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 となるデバイスを決定するときは、次の可能性を考慮してください。

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

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*]	候補 RP となるようにスイッチを設定します。 • *interface-id* には、対応する IP アドレスが候補 RP アドレスとしてアドバタイズされるインターフェイスを指定します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • （任意）**group-list** *access-list-numbe*r を指定する場合は、1 ～ 99 の IP 標準アクセス リスト番号を入力します。group-list を指定しない場合は、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、パケットの送信元であるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在す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）コンフィギュレーション ファイルに設定を保存します。

候補 RP として設定されたデバイスを解除するには、**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設定する例を示します。標準アクセス リスト番号 4 により、ポートで識別されるアドレスを持つ RP に対応するグループ プレフィックスが指定されます。この RP は、プレフィックスが 239 であるグループを処理します。

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

自動 RP および BSR の使用法

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、自動 RP を設定します。

シスコ PIMv1 ルータおよびマルチレイヤ スイッチと他社製の PIMv2 ルータを相互運用させる場合は、自動 RP と BSR の両方が必要です。シスコ PIMv2 ルータまたはマルチレイヤ スイッチを、自動 RP マッピング エージェントと BSR の両方に設定してください。

BSR を 1 つまたは複数使用する必要がある場合は、次の推奨事項に従ってください。

- 候補 BSR を自動 RP 用の RP マッピング エージェントとして設定します。詳細については、「Auto-RP の設定」（P.46-31）および「候補 BSR の設定」（P.46-38）を参照してください。
- グループ プレフィックスが自動 RP によってアドバタイズされた場合は、異なる RP セットによって処理されたこれらのグループ プレフィックスのサブ範囲が、PIMv2 BSR メカニズムによってアドバタイズされないようにする必要があります。PIMv1 および PIMv2 ドメインが混在する環境では、バックアップ RP で同じグループ プレフィックスが処理されるように設定します。このようにすると、RP マッピング データベースの最長一致検索によって、PIMv2 DR はこれらの PIMv1 DR から異なる RP を選択できなくなります。

グループ /RP マッピングの一貫性を確認するには、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 デバイスに関して、使用可能な RP マッピングを表示します。 • （任意）*group-name* を指定する場合は、RP を表示するグループの名前を指定します。 • （任意）*group-address* を指定する場合は、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 デバイスによって認識されている（設定されている、または自動 RP によって取得されている）すべてのグループ /RP マッピングを表示するには、**mapping** キーワードを使用します。
ステップ 2	**show ip pim rp-hash** *group*	PIMv2 ルータまたはマルチレイヤ スイッチ上で、PIMv1 システムで選択されている RP と同じ RP が使用されていることを確認します。 *group* には、RP 情報を表示するグループ アドレスを入力します。

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**：現在選択されている BSR の情報を表示します。
- **show ip pim rp-hash** *group*：指定グループに選択されている RP を表示します。
- **show ip pim rp** [*group-name* | *group-address* | **mapping**]：スイッチが RP を学習する方法（BSR 経由か、または自動 RP メカニズムによるか）を表示します。

PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング

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

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

高度な PIM 機能の設定

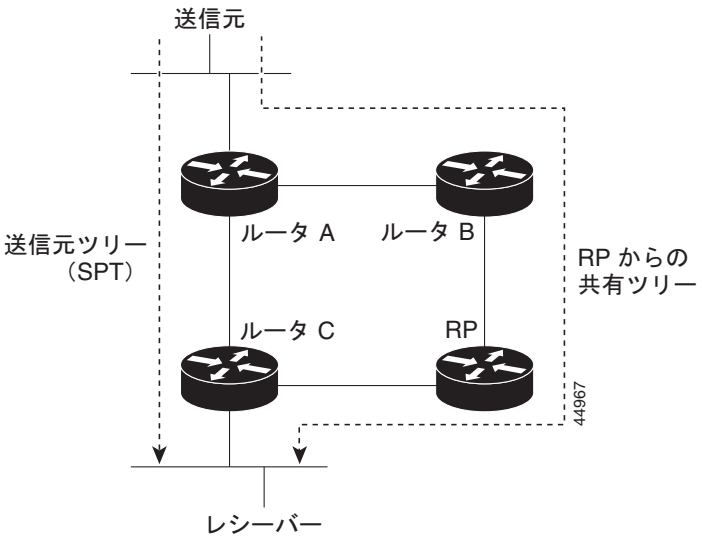
ここでは、高度なオプションの PIM 機能について説明します。

- 「PIM 共有ツリーおよび送信元ツリーの概要」（P.46-42）
- 「PIM SPT 使用の延期」（P.46-43）（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.46-44）（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、グループのメンバで受信されるデータは、RP でルーティングされた単一のデータ配信ツリーを経由して、送信側からグループに送られます。図 46-6 に、このタイプの共有配信ツリーを示します。送信側からのデータは、RP に配信され、その共有ツリーに加入しているグループ メンバに配布されます。

図 46-6　　共有ツリーおよび送信元ツリー（SPT）



データ レートによって保証されている場合は、送信元でルーティングされるデータ配信ツリーを、共有ツリーのリーフ ルータ（ダウンストリーム接続がないルータ）で使用できます。このタイプの配信ツリーは、SPT または送信元ツリーと呼ばれます。デフォルトでは、ソフトウェアが送信元から最初のデータ パケットを受信すると、送信元ツリーに切り替わります。

共有ツリーから送信元ツリーへの移動プロセスは、次のとおりです。

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

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

グループへ送信する複数の送信元で、共有ツリーが使用されます。

共有ツリー上に存在するように、PIM デバイスを設定できます。詳細については、「PIM SPT 使用の延期」（P.46-43）を参照してください。

PIM SPT 使用の延期

最初のデータ パケットが最終ホップ ルータ（図 46-6 のルータ C）に着信すると、共有ツリーから送信元ツリーへと変更されます。この変更が生じるのは、**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です。

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

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

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

マルチキャスト ルーティングが送信元ツリーから SPT に切り替わる上限値となるトラフィック速度のしきい値を設定するには、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、しきい値が適用されるマルチキャスト グループを指定します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。

	コマンド	目的
ステップ 3	**ip pim spt-threshold** {*kbps* | **infinity**} [**group-list** *access-list-number*]	SPT に移行する上限値となるしきい値を指定します。 • *kbps* を指定する場合は、トラフィック速度をキロビット/秒で指定します。デフォルト値は 0 キロビット/秒です。 （注）　有効範囲は 0 ～ 4294967 ですが、スイッチ ハードウェアの制限により、0 キロビット/秒以外は無効です。 • **infinity** を指定すると、指定されたグループのすべての送信元で共有ツリーが使用され、送信元ツリーに切り替わらなくなります。 • （任意）**group-list** *access-list-number* を指定する場合は、ステップ 2 で作成したアクセス リストを指定します。値 0 を指定する場合、または group-list を使用しない場合、しきい値はすべてのグループに適用されます。
ステップ 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）コンフィギュレーション ファイルに設定を保存します。

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 になるデバイスを判別するため、PIM ルータクエリー メッセージが送信されます。DR は、直接接続された LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。

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

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）コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**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、次の設定について説明します。

- 「IGMP のデフォルト設定」（P.46-45）
- 「グループのメンバーとしてのスイッチの設定」（P.46-45）（任意）
- 「IP マルチキャスト グループへのアクセスの制御」（P.46-46）（任意）
- 「IGMP バージョンの変更」（P.46-47）（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.46-48）（任意）
- 「IGMPv2 の IGMP クエリー タイムアウトの変更」（P.46-49）（任意）
- 「IGMPv2 の最大クエリー応答時間の変更」（P.46-49）（任意）
- 「静的に接続されたメンバーとしてのスイッチの設定」（P.46-50）（任意）

IGMP のデフォルト設定

表 46-4 に、IGMP のデフォルト設定を示します。

表 46-4　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 のバージョン	すべてのインターフェイスでバージョン 2
IGMP ホストクエリー メッセージ インターバル	すべてのインターフェイスで 60 秒
IGMP クエリー タイムアウト	すべてのインターフェイスで 60 秒
IGMP 最大クエリー応答時間	すべてのインターフェイスで 10 秒
静的に接続されたメンバとしてのマルチレイヤ 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 グループのメンバである場合、グループに ping を送信すると、これらのすべてのデバイスが応答します。デバイスは、所属グループにアドレス指定された ICMP エコー要求パケットに応答します。もう 1 つの例は、ソフトウェア付属のマルチキャスト トレースルート ツールです。

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

スイッチがグループのメンバ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、グループのメンバーシップは定義されていません。 *group-address* には、マルチキャスト IP アドレスをドット付き 10 進表記で指定します。
ステップ 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）コンフィギュレーション ファイルに設定を保存します。

グループ内のメンバーシップを取り消すには、**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、マルチキャスト グループ 255.2.2.2 へのスイッチの加入を許可する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
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 メンバに転送します。インターフェイスごとにフィルタを適用し、インターフェイスで処理されるサブネット上のホストが加入可能なマルチキャスト グループを制限できます。

インターフェイスで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。

	コマンド	目的
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、IP 標準アドレス 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、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 6	**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）コンフィギュレーション ファイルに設定を保存します。

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 にだけ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-if)# interface gigabitethernet1/0/1
Switch(config-if)# ip igmp access-group 1
```

IGMP バージョンの変更

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

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

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

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**}	スイッチで使用する IGMP バージョンを指定します。 （注）　バージョン 1 に変更すると、**ip igmp query-interval** または **ip igmp query-max-response-time** インターフェイス コンフィギュレーション コマンドを設定できません。
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）コンフィギュレーション ファイルに設定を保存します。

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

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

スイッチは LAN（サブネット）用の PIM DR を選択します。DR は、IP アドレスが最大である、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択されます。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。SM の場合、DR は PIM 登録メッセージおよび PIM Join メッセージも RP ルータに向けて送信します。

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）コンフィギュレーション ファイルに設定を保存します。

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 インターバルの 2 倍の時間だけ待機します。この時間を経過しても、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 インターバルを設定するには、**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。 デフォルトは 60 秒です（クエリー インターバルの 2 倍）。指定できる範囲は 60 ～ 300 です。
ステップ 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）コンフィギュレーション ファイルに設定を保存します。

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は、IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更できます。スイッチは最大クエリー応答時間を使用し、LAN 上に直接接続されたグループ メンバが存在しないことを短時間で検出します。値を小さくすると、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。 デフォルトは 10 秒です。指定できる範囲は 1 ～ 25 秒です。

	コマンド	目的
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）コンフィギュレーション ファイルに設定を保存します。

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。

静的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 メンバが存在しなかったり、ホストで IGMP を使用してグループ メンバーシップを報告できないにもかかわらず、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もあります。マルチキャスト トラフィックをネットワーク セグメントに送り込む方法は次のとおりです。

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

静的に接続されたグループのメンバになるように（および高速スイッチングできるように）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*	スイッチを静的に接続されたグループのメンバとして設定します。 デフォルトでは、この機能はディセーブルになっています。
ステップ 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）コンフィギュレーション ファイルに設定を保存します。

グループ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方法について説明します。

- レイヤ 2 接続および 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 サポート機能のイネーブル化」（P.46-51）（任意）

– 「sdr リスナー サポート機能の設定」（P.46-52）（任意）

- 帯域幅の利用率を制御する機能：
  – 「IP マルチキャスト境界の設定」（P.46-53）（任意）
- VPN ルーティング/転送（VRF）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.39-90）（任意）

CGMP サーバ サポート機能のイネーブル化

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デバイス用の 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、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**]	インターフェイス上で 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上でディセーブルです。 CGMP をイネーブルにすると、CGMP Join メッセージが送信されます。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、CGMP を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 メッセージを送信し、CGMP 非対応ルータが存在すること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、IP アドレスが最大または最小のスイッチが IGMP クエリアになるように IP アドレスを手動で操作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。

	コマンド	目的
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 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。

インターフェイス上で 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 CGMP 対応デバイスがスイッチド ネットワークに接続されていて、**ip cgmp proxy** コマンドを使用する必要がある場合は、すべてのデバイスを同じ CGMP オプションを使用して設定し、他社製のルータよりも IGMP クエリアになる優先順位を上げてください。

sdr リスナー サポート機能の設定

MBONE は、相互接続された、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、通常は 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メディア グループ アドレス、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なるアプリケーションの種類（音声、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ワールドワイド ウェブ上の複数のサイトからダウンロードできます。

SDR は、Session Announcement Protocol（SAP）マルチキャスト パケット用の Well-known マルチキャスト グループ アドレスおよびポートを、SAP クライアントから傍受するマルチキャスト アプリケーションです（SAP クライアントは、会議セッションをアナウンスします）。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格納されます。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 サポート機能のイネーブル化

デフォルトでは、スイッチでセッション ディレクトリのアドバタイズメントは受信されません。

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 アドバタイズメントを受信できるようにするには、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 サポート機能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）コンフィギュレーション ファイルに設定を保存します。

sdr サポート機能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、古いアドバタイズメントが無駄に保持されないようにするため、エントリがアクティブである期間を制限できます。

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）コンフィギュレーション ファイルに設定を保存します。

デフォルトの設定に戻すには、**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。

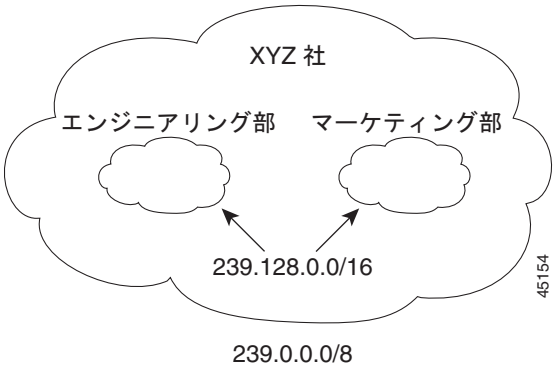
IP マルチキャスト境界の設定

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

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

図 46-7 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ったり、外へ出ることができません。同様に、エンジニアリング部およびマーケティング部では、各自のネットワークの周辺で、管理用スコープの境界を 239.128.0.0/16 に設定しました。この境界では、239.128.0.0 ～ 239.128.255.255 の範囲のマルチキャスト トラフィックは、それぞれのネットワークに入ったり、外部に出ることができません。

図 46-7　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、ルーテッド インターフェイス上に管理用スコープの境界を定義できます。影響を受けるアドレス範囲は、標準アクセス リストによって定義されます。この境界が定義されている場合、マルチキャスト データ パケットはいずれの方向であっても境界を通過できません。この境界を使用すると、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、異なる組織によって管理されたドメイン内で再利用できます。このアドレスはグローバルではなく、ローカルで一意であると見なされます。

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、パケットの送信元であるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在す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。

	コマンド	目的
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）コンフィギュレーション ファイルに設定を保存します。

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 gigabitethernet1/0/1
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、次の設定について説明します。

- 「DVMRP 相互運用性の設定」（P.46-55）（任意）
- 「DVMRP トンネルの設定」（P.46-57）（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.46-59）（任意）
- 「mrinfo 要求への応答」（P.46-60）（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.46-60）を参照してください。

DVMRP 相互運用性の設定

PIM を使用するシスコのマルチキャスト 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 ルータと相互運用させることができます。

PIM デバイスは、DVMR プローブ メッセージを受信し、接続されているネットワーク上にある DVMRP マルチキャスト ルータを動的に検出します。DVMRP ネイバーが検出された場合、PIM デバイスは、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。デバイスは 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、次にマルチキャスト パケットを DVMRP ルータに転送します。

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 ルート数を制限するには、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 リストを設定できます。この設定を行わないと、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 ルーティングされるプロトコルは、DVMRP のパブリック ドメイン実装バージョンです。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 ルーティングのバージョン 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 ソフトウェアによって作成される DVMRP アドバタイズメントを使用すると、マルチキャスト ルーティングされた古いバージョンのプロトコルによってルーティング 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もあります。

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する場合は、**ip dvmrp metric** インターフェイス コンフィギュレーション コマンドを設定します。特定のユニキャスト ルーティング プロセスによって取得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、パケットの送信元であるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在す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 ルーティングが可能な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るメトリックを設定します。 • *metric* の範囲は、0 ～ 32 です。値が 0 の場合、ルートはアドバタイズされません。値 32 は無限大（到達不能）を意味します。 • （任意）**list** *access-list-number* を指定する場合は、ステップ 2 で作成したアクセス リスト番号を入力します。これらが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* を指定する場合は、**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、およびルーティング プロトコルのプロセス ID 番号を入力します。これらが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取得されたルートだけが、DVMRP レポート メッセージに格納されてアドバタイズされます。 • （任意）**dvmrp** キーワードが指定されている場合は、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）コンフィギュレーション ファイルに設定を保存します。

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 デバイスおよび DVMRP ルータが同じネットワーク セグメント上にある場合に、DVMRP 相互運用性を設定する例を示します。次の例では、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ます。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-if)# interface gigabitethernet1/0/1
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ます。一方の端で 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、トンネルを通してマルチキャスト パケットが送受信されます。この方法で、パス上の一部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に、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通して 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、受信された DVMRP レポート メッセージはキャッシュに格納され、RPF 計算にも使用されます。この動作により、トンネルを通して受信されたマルチキャスト パケットの転送が可能になります。

次の場合は、DVMRP トンネルを設定するときに、IP アドレスをトンネルに割り当てる必要があります。

- トンネルを通して 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通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通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、パケットの送信元であるネットワークまたはホストの番号を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在す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なしとして設定します。
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。したがって、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* を指定する場合は、宛先への管理上の距離を入力します。デフォルトでは、DVMRP ルートへの管理上の距離は 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。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）と DVMRP を使用するパスという、送信元への 2 つのパスがある場合に PIM パスを使用するときは、DVMRP ルートの管理上の距離を増加させます。有効値は 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。

	コマンド	目的
ステップ 10	**end**	特権 EXEC モードに戻ります。
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）コンフィギュレーション ファイルに設定を保存します。

フ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 IP アドレスは 172.16.2.1 です。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 です。トンネルを通して送信されるパケットは、外部 IP ヘッダー内にカプセル化されます。Cisco スイッチは、198.92.37.0 から 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 gigabitethernet1/0/1
Switch(config-if)# ip pim dense-mode
Switch(config-if)# tunnel source gigabitethernet1/0/1
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 gigabitethernet1/0/1
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 のデバイスと隣接している場合は、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 ネイバーへのネットワーク 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 のデバイスと近接してい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ます。 • **only**：0.0.0.0 以外の DVMRP ルートはアドバタイズされません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルト ルートのアドバタイズメントを禁止するには、**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。ソフトウェアはネイバーに関する情報を、DVMRP トンネルおよびすべてのルーテッド インターフェイスを通して戻します。この情報にはメトリック（常に 1 に設定）、設定された TTL しきい値、インターフェイスのステータス、および各種フラグが含まれます。次の例のように、**mrinfo** 特権 EXEC コマンドを使用し、ルータまたは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に転送したり、送信側から受信したりします。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、マルチキャスト パケットを転送するために DVMRP を実行しません。

ここでは、次の設定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.46-61）（任意）
- 「DVMRP の非プルーニング ネイバーの拒否」（P.46-62）（任意）
- 「ルート交換の制御」（P.46-64）（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.46-55）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、ループのない配信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 ベースのデバイスは、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逆経路を転送できます。

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 ルートを交換します。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。このため、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 トポロジを通しての PIM SM が可能になります。

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 メッセージで取得されたルートをキャッシュに格納します。PIM が動作中の場合、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ます。したがって、MBONE トポロジがユニキャスト トポロジと異なる場合、PIM による MBONE トポロジが可能となります。

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。

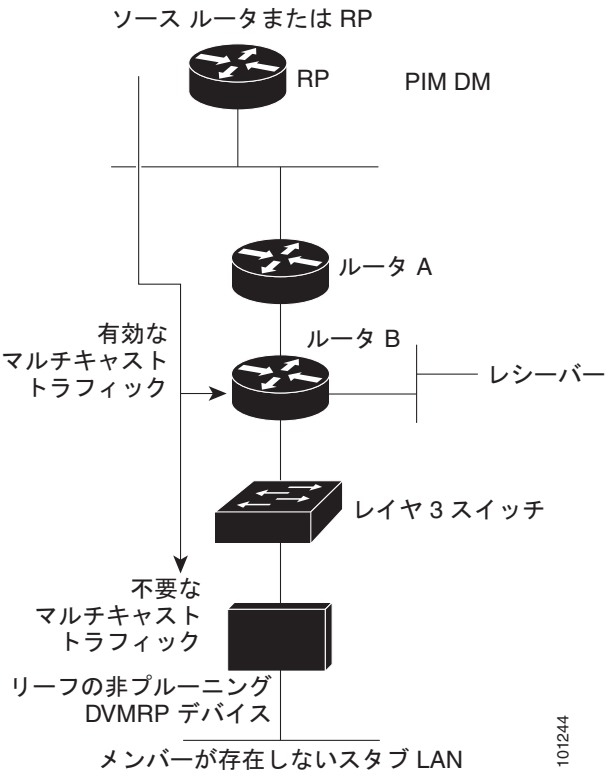
	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	DVMRP ルータに接続されたインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ip dvmrp unicast-routing**	DVMRP ユニキャスト ルーティングをイネーブルにします（DVMRP ルートを送受信します）。 この機能は、デフォルトではディセーブルになっています。
ステップ 4	**end**	特権 EXEC モ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

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

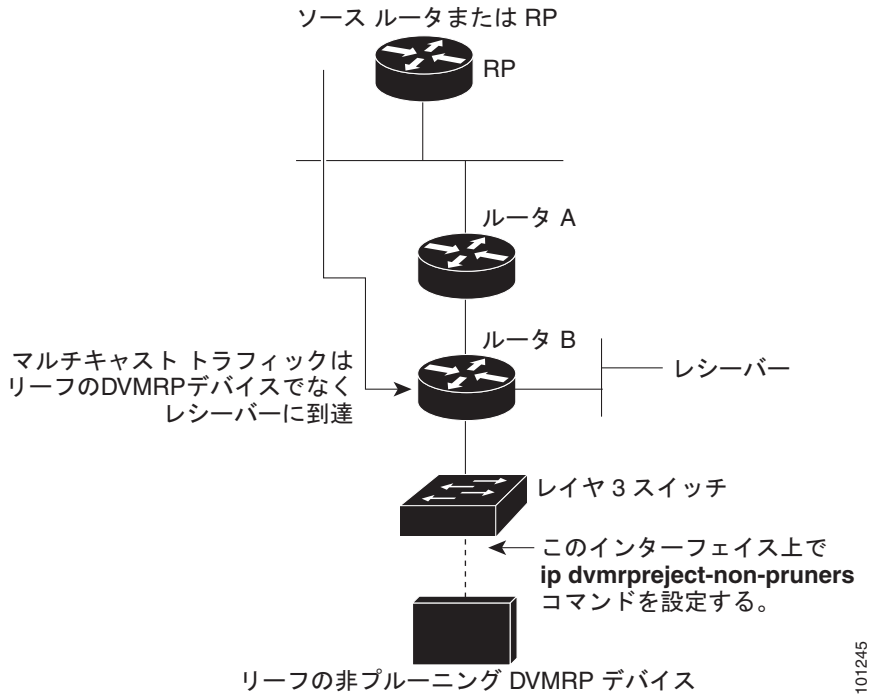
デフォルトでは、DVMRP 機能に関係なく、シスコ デバイスはすべての DVMRP ネイバーをピアとして受け入れます。ただし、一部の他社製のデバイスでは、プルーニング機能を持たない古いバージョンの DVMRP が動作するため、常時転送パケットが受信されて帯域幅が消費されます。図 46-8 にこの事例を示します。

図 46-8　　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）を禁止できます。これを行うには、非プルーニング デバイス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 デバイスのネイバー）を設定します（図 46-9 を参照）。この場合、プルーニング対応フラグが設定されていない DVMRP プローブまたはレポート メッセージをスイッチが受信すると、Syslog メッセージがロギングされ、メッセージが廃棄されます。

図 46-9　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禁止されます。拒否されていない非プルーニング ルータが（レシーバ候補のダウンストリーム方向に）2 ホップ以上離れている場合、非プルーニング DVMRP ネットワークが存在する場合もあります。

非プルーニング DVMRP ネイバーとのピアリングを禁止するには、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禁止します。
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）コンフィギュレーション ファイルに設定を保存します。

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メント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.46-64）（任意）
- 「DVMRP ルートしきい値の変更」（P.46-64）（任意）
- 「DVMRP サマリー アドレスの設定」（P.46-65）（任意）
- 「DVMRP 自動サマライズのディセーブル化」（P.46-67）（任意）
- 「DVMRP ルートへのメトリック オフセットの追加」（P.46-67）（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）を通して、7000 の 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通してアドバタイズされる DVMRP 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る MBONE への大量のルート注入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）コンフィギュレーション ファイルに設定を保存します。

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 ルートしきい値の変更

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。通常この警告は、デバイスの設定ミスにより大量のルートが MBONE に入った場合、迅速な検出を行うために使用されます。

警告送信の基準となるルート数のしきい値を変更するには、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 メッセージの送信基準となるルート数を設定します。 デフォルト値は 10,000 ルートで、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）コンフィギュレーション ファイルに設定を保存します。

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* *** が表示行に表示されます。

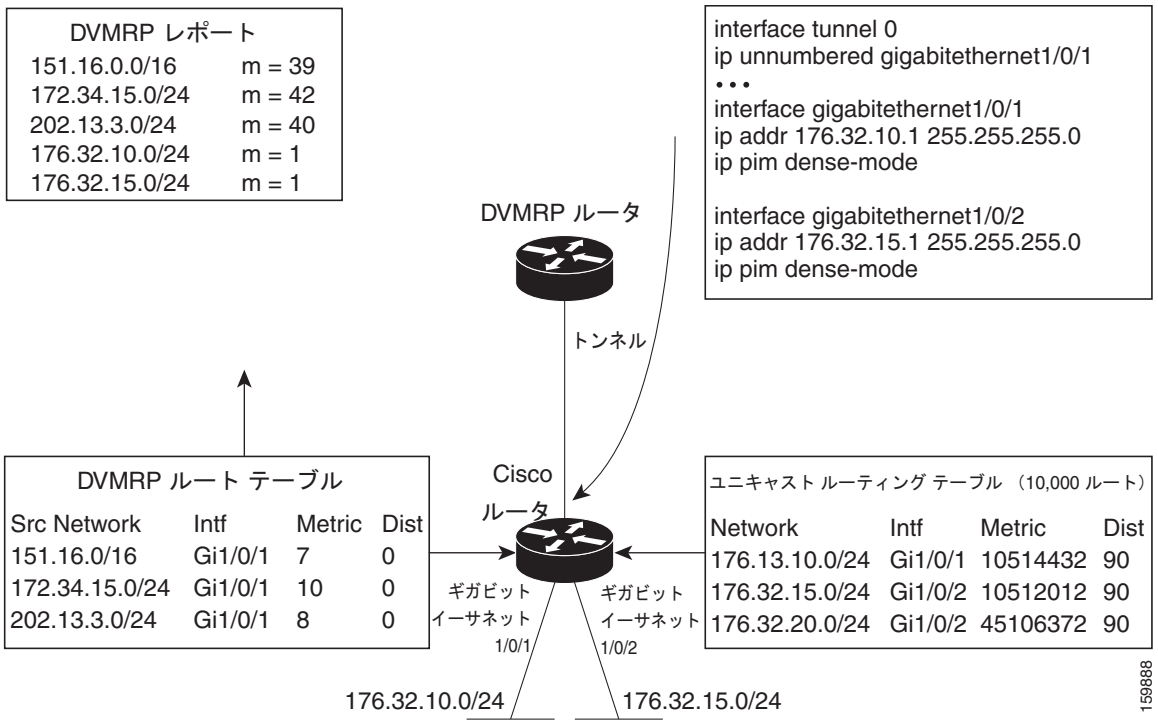
DVMRP サマリー アドレスの設定

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 メッセージに格納してアドバタイズします。これらのルートは、通常の DVMRP のクラス指定されたルート サマライズによって処理されます。このプロセスは、アドバタイズされているルートとアドバタイズ中に経由するインターフェイスが、クラス指定された同じネットワーク内にあるかどうかに応じて異なります。

図 46-10 に、デフォルトの動作例を示します。この例で、Cisco ルータによって送信される DVMRP レポートに記述されているのは、DVMRP メトリックに 32 を追加してポイズンリバースされた DVMRP ルータから受信した 3 つの元のルートです。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、直接接続されている 2 つのネットワーク（176.32.10.0/24 および 176.32.15.0/24）にアドバタイズされる 2 つのルートが記述されています。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してクラス指定サマライズは実行されません。その結果、DVMRP ルータは、直接接続されたサブネットへ向かうこれらの 2 つのルートだけをポイズン リバースします。また、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 だけを適切に実行します。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 ルータに関する 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。ユニキャスト ルーティング テーブルにサマリー アドレス範囲内のルートが 1 つまたは複数格納されている場合は、サマリー アドレスが DVMRP ルート レポートに格納されて送信されます。それ以外の場合、サマリー アドレスはアドバタイズされません。図 46-10 では、Cisco ルータ 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。その結果、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、サマライズされた単一のクラス B アドバタイズを送信します。

図 46-10　接続されたユニキャスト ルートに限りアドバタイズ（デフォルト）する例



デフォルトのクラス指定サマライズが要求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 1 つまたは複数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* を指定する場合は、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）コンフィギュレーション ファイルに設定を保存します。

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

ソフトウェアでは、デフォルトで一部のレベルの DVMRP サマライズが自動実行されます。サマリーだけで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隣接する DVMRP ルータを使用し、DVMRP ネットワーク内のマルチキャスト トラフィックの流れを詳細に制御できます。この例としては、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いるとき、具体的な（サマライズされていない）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へ向かう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が得られます。

DVMRP 自動サマリー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）コンフィギュレーション ファイルに設定を保存します。

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、着信 DVMRP レポートに格納されてアドバタイズされた DVMRP ルートのメトリック（ホップ数）は、スイッチによって 1 だけ増加されます。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 からルートが取得され、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ため、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できます。この結果、スイッチ B を経由するパスを選択できます。

デフォルトの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。

	コマンド	目的
ステップ 3	**ip dvmrp metric-offset** [**in** | **out**] *increment*	着信レポートに格納されてアドバタイズされる DVMRP ルートに追加される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 応答内で報告されます。 • （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ます。 **in** と **out** のどちらも指定しない場合は、**in** がデフォルトになります。 *increment* には、レポート メッセージに格納されてアドバタイズされる DVMRP ルータのメトリックの増分値を指定します。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 です。発信ルートのデフォルト値は 0 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）コンフィギュレーション ファイルに設定を保存します。

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 ルーティングのモニタ方法およびメンテナンス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クリア」（P.46-68）
- 「システムおよびネットワーク統計情報の表示」（P.46-69）
- 「IP マルチキャスト ルーティングのモニタ」（P.46-70）

キャッシュ、テーブル、およびデータベースのクリア

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

表 46-5 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、データベースをクリアできます。

表 46-5　キャッシュ、テーブル、およびデータベースをクリアするコマンド

コマンド	目的
clear ip cgmp	Catalyst スイッチによってキャッシュに格納されたすべてのグループ エントリをクリアします。
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 キャッシュの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 テーブルのエントリを削除します。
clear ip pim auto-rp *rp-address*	自動 RP キャッシュをクリアします。
clear ip sdr [*group-address* | "*session-name*"]	Session Directory Protocol バージョン 2 キャッシュ（sdr キャッシュ エントリ）を削除します。

システムおよびネットワーク統計情報の表示

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

（注）　このリリースでは、ルート単位の統計情報がサポートされていません。

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

表 46-6 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 46-6　システムおよびネットワーク統計情報を表示するコマンド

コマンド	目的
ping [*group-name* | *group-address*]	マルチキャスト グループ アドレスに 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ている、IGMP によって取得されたマルチキャスト グループを表示します。
show ip igmp interface [*type number*]	インターフェイスのマルチキャスト関連情報を表示します。
show ip 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。

表 46-6　システムおよびネットワーク統計情報を表示するコマンド （続き）

コマンド	目的
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*]	SM 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*}	スイッチの RPF の実行方法（ユニキャスト ルーティング テーブル、DVMRP ルーティング テーブル、またはスタティック マルチキャスト ルーティングのいずれか）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 46-7 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 46-7　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する隣接マルチキャスト デバイスに関して、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 パケット速度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配信ツリーに対して、送信元から宛先ブランチへのパスをトレースします。