



IP マルチキャスト ルーティングの設定

この章では、Catalyst 3750 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、音声やビデオなど、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 グループのメンバーに接続されたすべてのインターフェイスから着信した IP マルチキャスト パケットを転送します。グループのメンバーであるかどうかに関係なく、すべてのホストはグループに送信できます。ただし、そのメッセージを受信できるのは、グループのメンバーのみです。

IP マルチキャスト ルーティング機能を使用するには、スタック マスター上で IP サービス イメージが稼動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場合は、スタック マスター上で IP ベース イメージを稼動することができます。

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 スタックを意味します。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2*』を参照してください。このマニュアルは、Cisco.com の [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] を選択すると表示されるページでご利用になれます。

この章で説明する内容は、次のとおりです。

- 「IP マルチキャスト ルーティングの実装の概要」 (P.46-2)
- 「マルチキャスト ルーティングおよびスイッチ スタック」 (P.46-10)
- 「IP マルチキャスト ルーティングの設定」 (P.46-11)
- 「高度な PIM 機能の設定」 (P.46-37)
- 「オプションの IGMP 機能の設定」 (P.46-40)
- 「オプションのマルチキャスト ルーティング機能の設定」 (P.46-46)
- 「基本的な DVMRP 相互運用性機能の設定」 (P.46-50)
- 「高度な DVMRP 相互運用性機能の設定」 (P.46-56)
- 「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」 (P.46-63)

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。

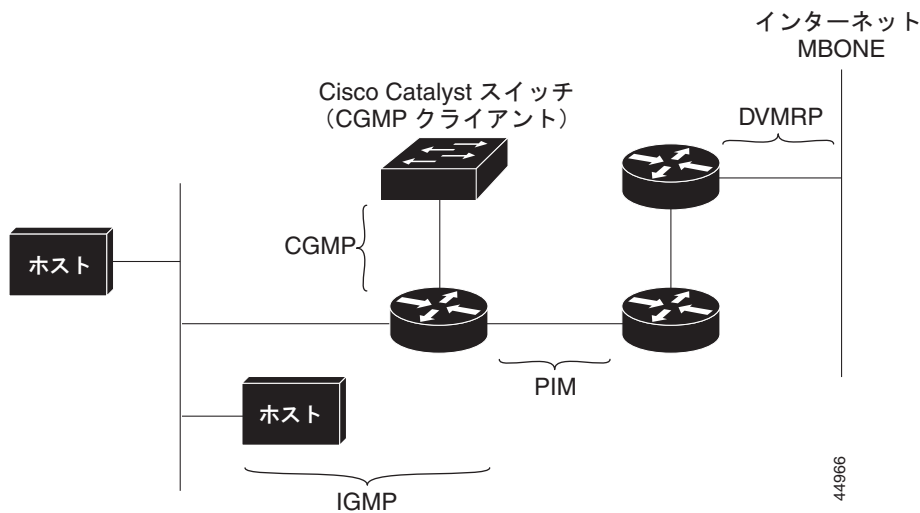
IP マルチキャストルーティングの実装の概要

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)** (インターネットグループ管理プロトコル) : 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、ホストがメンバーとして属するマルチキャストグループをトラッキングします。
- **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トラッキングします。
- **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)** (マルチキャストバックボーン) 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 Cisco 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 マルチキャスト規格に従って、MAC 宛先マルチキャストアドレスは 0100:5e で始まり、IP アドレスの最後の 23 ビットが付加されます。Catalyst 3750 スイッチでは、マルチキャストパケットがスイッチのマルチキャストアドレスと一致しない場合、パケットは次のように取り扱われます。

- パケットにマルチキャスト IP アドレスとユニキャスト MAC アドレスがある場合、パケットはソフトウェアで転送されます。これは、従来型デバイスのプロトコルの中に、マルチキャスト IP アドレスとともにユニキャスト MAC アドレスを使用するものがあるために発生します。
- パケットにマルチキャスト IP アドレスと不一致のマルチキャスト MAC アドレスがある場合、パケットはドロップします。

ここでは、次の内容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 マルチキャストルー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シップを通知するためのレポートメッセージ（クエリーメッセージに応答するメッセージ）を送信するレシーバーです。

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

グループのメンバーであるかどうかに関係なく、すべてのホストはグループに送信できます。ただし、そのメッセージを受信できるのは、グループのメンバーのみです。マルチキャストグループのメンバシップはダイナミックです。ホストはいつでもグループに加入し、また脱退できます。マルチキャストグループの場所またはメンバー数に制限はありません。ホストは一度に複数のマルチキャストのメンバーになることができます。マルチキャストグループのアクティブ状態および所属メンバーは、グループや時間によって変化し、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。グループのメンバシップはいつでも変更可能です。メンバーを含むグループにアクティブ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は 224.0.0.0 ~ 239.255.255.255 の範囲を取ります。224.0.0.0 ~ 224.0.0.255 のマルチキャストアドレスは、ルーティングプロトコルおよびその他のネットワーク制御トラフィックが使用するために確保されています。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 汎用クエリーは、アドレス 224.0.0.1（サブネット上のすべてのシステム）を宛先とします。
- IGMP グループ固有のクエリーは、クエリー対象グループの 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 アドレスであるものがあります。

IGMP バージョン 1

IGMPv1（IGMP バージョン 1）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）を判別できません。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、この作業を行うために、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ない」マルチキャストと呼ばれます。ユニキャストルーティングテーブルを読み込むために使用されるユニキャストルーティングプロトコルに関係なく、PIM は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; インターネット技術特別調査委員会) 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 Rendezvous Point (RP; ランデブーポイント) を持つアクティブな RP が 1 つ存在します。この単一の RP 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) はフォールトトレラントな、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 マッピングをダイナミックに取得できます。
- 希薄モード (SM) および dense (稠密) モード (DM) は、インターフェイスではなく、グループに関するプロパティです。SM または DM のいずれか一方のみでなく、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 Prune メッセージを使用すると、複数のアドレスファミリを柔軟に符号化できます。
- 現在は以降の機能オプションを符号化するため、クエリーパケットではなく、より柔軟な hello パケット形式が使用されています。
- RP への登録メッセージが境界ルータによって送信されるか、あるいは代表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、希薄グループと dense（稠密）グループの両方が同時に処理されます。

PIM DM

PIM DM では、送信元ベースのマルチキャスト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のマルチキャスト パケットが転送されると想定しています。直接接続されたメンバーまたは PIM ネイバーが存在しない場合、PIM DM デバイスがマルチキャスト パケットを受信すると、Prune 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。このプルニング済みブランチ上のこのルータまたはスイッチでは、後続のマルチキャスト パケットがフラッディングしません。レシーバーを含まないブランチが配信ツリーからプルニングされ、レシーバーを含むブランチのみが存続するためです。

プルニング済みのツリー内ブランチのレシーバーがマルチキャスト グループに新規に加入すると、PIM DM デバイスは新しいレシーバーを検出し、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ー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) がない限り、他のルータまたはスイッチではグループ宛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 レシーバーをトラッキングします。また、送信元の先頭ホップ ルータ (Designated Router (DR; 代表ルータ)) から受信した登録メッセージを使用して送信元を登録し、送信元からレシーバーへの共有ツリー パスを完成させます。共有ツリーを使用する場合、送信元は RP にトラフィックを送信し、これらのトラフィックをすべてのレシーバーに到達させるようにする必要があります。

マルチキャスト グループ トラフィックをプルニングする場合は、Prune 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、これらを解除することが可能となります。

PIM スタブルーティング

PIM スタブルーティング機能は、すべてのソフトウェア イメージで使用することができ、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利用率が軽減されます。



(注)

IP ベース イメージには PIM スタブルーティングのみが含まれています。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ています。IP ベース イメージが稼動するスイッチで、VLAN インターフェイスを PIM DM、SM、または SM-DM に設定しようとしても、設定は許可されません。

PIM スタブ ルーティングを使用するネットワークでは、ユーザへの IP トラフィックの許可ルートのみが PIM スタブ ルーティングを設定しているスイッチを通過します。PIM 受動インターフェイスは、VLAN などのレイヤ 2 アクセス ドメインに接続されるか、他のレイヤ 2 デバイスを接続先とするインターフェイスに接続されます。直接接続されるマルチキャスト (IGMP) 受信者と送信元のみが、レイヤ 2 アクセス ドメイン内に許可されます。PIM 受動インターフェイスは、受信した PIM 制御パケットの送信や処理を行いません。

PIM スタブ ルーティングを使用する場合、分散ルータとリモート ルータで IP マルチキャスト ルーティングを使用するように設定し、スイッチのみを PIM スタブ ルータとして設定するようにしてください。スイッチは、分散ルータ間で中継トラフィックをルーティングしません。また、スイッチにルーテッドアップリンク ポートを設定する必要があります。スイッチのアップリンク ポートは SVI と併用できません。SVI アップリンク ポートに 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。

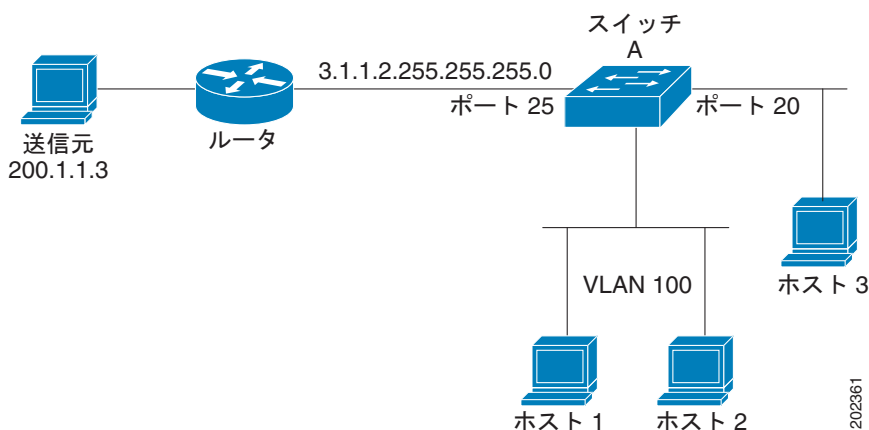
スイッチに PIM スタブ ルーティングを設定する場合は、EIGRP スタブ ルーティングも設定する必要があります。詳細については、「EIGRP スタブ ルーティングの設定」(P.38-45) を参照してください。

冗長 PIM スタブ ルータ トポロジはサポートされません。マルチキャスト トラフィックをシングル アクセス ドメインにフォワーディングする PIM ルータが複数存在すると、冗長トポロジになります。PIM メッセージはブロックされ、PIM アセットおよび代表ルータ選出メカニズムは PIM 受動インターフェイスではサポートされません。PIM スタブ機能は、非冗長アクセス ルータ トポロジのみをサポートします。非冗長トポロジを使用することで、PIM 受動インターフェイスは自己がアクセス ドメイン上の唯一のインターフェイスで代表ルータであると想定します。

PIM スタブ機能は、IP ベース イメージに実装されています。上位のソフトウェア バージョンにアップグレードした場合、インターフェイスを再設定するまで PIM スタブ設定は残ります。

図 46-2 で、スイッチ A のルーテッドアップリンク ポート 25 はルータに接続されており、VLAN 100 インターフェイスおよびホスト 3 で PIM スタブ ルーティングがイネーブルになっています。この設定により、直接接続されているホストはマルチキャスト送信元 200.1.1.3 からのトラフィックを受信できます。詳細については、「PIM スタブ ルーティングの設定」(P.46-24) 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 ルーティングはルーティングされたトラフィックをエンドユーザの近くに移動させ、ネットワーク トラフィックを軽減します。また、スタブ ルータ (スイッチ) に IGMP ヘルパー機能を設定してトラフィックを軽減させることもできます。

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) を設定し、スイッチからネクスト ホップ インターフェイスにレポートを送信できます。このようにすると、ダウンストリーム ルータに直接接続していないホストはアップストリーム ネットワークからのマルチキャスト グループに参加できます。この機能を設定すると、マルチキャスト ストリームへの参加を待機しているホストの IGMP パケットが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。アップストリーム中央ルータがヘルパー IGMP レポートを受信した場合や脱退した場合、ルータはそのグループの発信インターフェイス リストにインターフェイスを追加または削除します。

ip igmp helper-address コマンドの詳しい構文と使い方については、『*Cisco IOS IP and IP Routing Command Reference, Release 12.1*』を参照してください。

自動 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 Cisco 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リスニングし、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 エントリのみが作成されます。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、スタティックに設定された RP に切り替わります。スタティックに設定された RP が存在しない場合、ルータまたはスイッチはグループの動作を 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バイホップでフラッド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バイホップで送信される 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のみを、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。ネイバー PIMv2 ルータまたはマルチレイヤ スイッチは BSR メッセージを受信し、TTL 値が 1 である他のすべてのインターフェイス (BSR メッセージの着信インターフェイスを除く) にマルチキャストします。この方法で、BSR メッセージは PIM ドメイン内をホップバイホップで移動します。BSR メッセージには現在の BSR の IP アドレスが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バイホップで移動し、すべてのルータおよびスイッチに送信されます。BSR メッセージ内の RP 情報は、到達したルータおよびスイッチのローカルな RP キャッシュに格納されます。すべてのルータおよびスイッチには一般的な RP ハッシュ アルゴリズムが使用されるため、指定されたグループには同じ RP が選択されます。

マルチキャスト転送およびリバース パス チェック

ユニキャストルーティングの場合、ルータおよびマルチレイヤ スイッチは、送信元から IP パケットの宛先アドレス フィールドに IP アドレスが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。その後、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。

マルチキャストルーティングの場合、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 パケットを転送するかドロップするかを決定するため、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 RPF チェックを実行します (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、リバース パス上のインターフェイスに着信したパケットを送信元に戻すかどうかを決定します。
2. パケットが送信元に逆戻りするインターフェイスに着信した場合、RPF チェックは成功し、発信インターフェイス リスト内のすべてのインターフェイス (ルータのすべてのインターフェイスとは限りません) 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、送信元へのリバース パス上にあるポートはポート 2 ではなく、ポート 1 であることがわかります。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リバース パス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

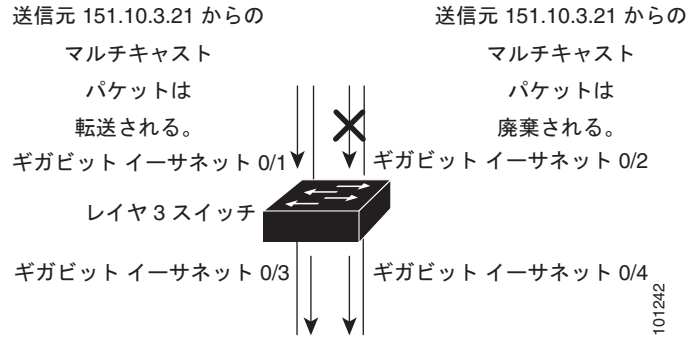


表 46-1 RPF チェックのルーティング テーブル例

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] エントリーがマルチキャスト 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 Prune 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 では送信元ツリーのみが使用され、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 Cisco 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 ディスカバリーをサポートし、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 Prune 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 Cisco 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 アドレスにアドレッシングされます。

CGMP は HSRPv1 と相互に排他的です。CGMP 脱退処理と HSRPv1 を同時にイネーブルにすることはできません。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 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。

Catalyst 3750 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、スタック メンバーに配信します。



(注) IP サービス イメージを実行しているスタック 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 イメージ (以前の標準マルチレイヤ イメージ [SMI]) が稼動している場合、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 5 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、次の設定情報について説明します。

- 「マルチキャスト ルーティングのデフォルト設定」(P.46-11)
- 「マルチキャスト ルーティング設定時の注意事項」(P.46-12)
- 「基本的なマルチキャスト ルーティングの設定」(P.46-13) (必須)
- 「SSM の設定」(P.46-15)
- 「SSM マッピングの設定」(P.46-18)
- 「PIM スタブ ルーティングの設定」(P.46-24) (任意)
- 「RP の設定」(P.46-26) (インターフェイスが SM モードで、グループを希薄グループとして扱う場合に必須)
- 「自動 RP および BSR の使用」(P.46-36) (他社製の PIMv2 デバイスをシスコ製 PIMv1 デバイスと相互運用する場合に必須)
- 「RP マッピング情報のモニタ」(P.46-36) (任意)
- 「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」(P.46-37) (任意)

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

表 46-2 マルチキャストルーティングのデフォルト設定 (続き)

機能	デフォルト設定
SPT しきい値レート	0 kbps
PIM ルータ クエリー メッセージ インターバル	30 秒

マルチキャストルーティング設定時の注意事項

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

- 「PIMv1 および PIMv2 の相互運用性」(P.46-12)
- 「自動 RP および BSR 設定時の注意事項」(P.46-13)

PIMv1 および PIMv2 の相互運用性

シスコの PIMv2 実装機能を使用すると、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 に付加的にアップグレードできます。PIM バージョン 1 および 2 を、1 つのネットワーク内の異なるルータおよびマルチレイヤスイッチに設定できます。内部的には、共有メディアネットワーク上のすべてのルータおよびマルチレイヤスイッチで同じ PIM バージョンを実行する必要があります。したがって、PIMv2 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、スタンダードアロンのシスコ独自のプロトコルで、PIMv2 は IETF 標準のトラッキングプロトコルです。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 Cisco 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 を自動的にアダプタイズします。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、「自動 RP の設定」(P.46-28) 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 Cisco 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。
- ネットワークに非 Cisco 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 Cisco マルチレイヤ スイッチ、および非 Cisco 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バイホップで送信されるため、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 Cisco マルチレイヤ スイッチのみが存在する場合は、自動 RP を使用してください。
- ネットワーク内に非 Cisco ルータが存在する場合は、Cisco PIMv2 ルータまたは Cisco 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](#)」(P.46-36) 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、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 リストになく、IGMP スヌーピングがディセーブルであると、余分なレプリケーションのために発信インターフェイスでマルチキャスト トラフィックのラインレートを維持することができません。

マルチキャスト ルーティング テーブルへのパケット読み込みでは、DM インターフェイスは常にテーブルに追加されます。SM インターフェイスがテーブルに追加されるのは、ダウンストリーム デバイスから定期的な Join メッセージを受信した場合、またはインターフェイスに直接接続されたメンバーが存在する場合に限ります。LAN から転送する場合、グループが認識している RP があれば、SM 動作が行われます。その場合、パケットはカプセル化され、その RP に送信されます。認識している RP がなければ、パケットは DM 方式でフラッドングされます。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、レシーバーの先頭ホップ 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。

■ IP マルチキャストルーティングの設定

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

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	<code>configure terminal</code>	グローバル 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	<code>ip multicast-routing distributed</code>	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。
ステップ 3	<code>interface interface-id</code>	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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 (仮想 LAN) インターフェイスです。 <p>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.12-27) を参照してください。</p>
ステップ 4	<code>ip pim version [1 2]</code>	<p>インターフェイスに PIM バージョンを設定します。</p> <p>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)。</p> <p>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。</p> <p>詳細については、「PIMv1 および PIMv2 の相互運用性」(P.46-12) を参照してください。</p>
ステップ 5	<code>ip pim {dense-mode sparse-mode sparse-dense-mode}</code>	<p>インターフェイスで PIM モードをイネーブルにします。</p> <p>デフォルトで、モードは設定されていません。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • 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.46-26) 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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show running-config</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

マルチキャストルー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。

SSM の設定

ここでは、Source-Specific Multicast (SSM) の設定方法について説明します。ここに記載されている SSM コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*』の「IP Multicast Routing Commands」の章を参照してください。この章に記載されている他のコマンドのマニュアルについては、コマンドリファレンス マスター インデックスを使用するか、オンラインで検索してください。

SSM 機能は IP マルチキャストの拡張版で、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だけからのデータグラム トラフィックをレシーバーに転送します。SSM 用に設定されるマルチキャスト グループには、SSM 配信ツリーのみ（共有ツリーなし）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）を最適なデータグラム デリバリティ モデルです。SSM は、音声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にしたシスコの IP マルチキャスト ソリューションのコア ネットワーキング テクノロジーです。スイッチは、SSM の導入をサポートする次のコンポーネントをサポートします。

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

PIM-SSM は SSM の導入をサポートするルーティング プロトコルであり、PIM Sparse Mode (PIM-SM; PIM 希薄モード) から派生しています。

- IGMP バージョン 3 (IGMPv3)

SSM と IGMPv3 を稼動するには、SSM が Cisco IOS ルータ、アプリケーションの稼動するホスト、およびアプリケーション自身でサポートされている必要があります。

SSM とインターネット標準マルチキャストとの違い

インターネットおよび多くの企業イントラネットの IP マルチキャスト インフラストラクチャは、PIM-SM プロトコルおよび Multicast Source Discovery Protocol (MSDP) に基づいています。これらのプロトコルには、Internet Standard Multicast (ISM) サービス モデルの制限があります。たとえば、ISM を使用する場合、ネットワークはネットワーク内でマルチキャスト トラフィックをアクティブに送信しているホストを把握している必要があります。

ISM サービスは、任意の送信元からレシーバー グループ（マルチキャスト ホスト グループ）への IP データグラムの配信です。マルチキャスト ホスト グループに対するデータグラム 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 宛先アドレスであるマルチキャスト グループ アドレス G で構成されています。システムは、ホスト グループのメンバーになることでこのトラフィックを受信します。

ホスト グループのメンバシップに必要なのは、IGMP バージョン 1、2、または 3 を使用してホスト グループにシグナリングすることだけです。SSM では、データグラムの配信は (S, G) チャネルに基づいています。SSM および ISM のどちらでも、送信元になるためにシグナリングは必要ありません。ただし SSM の場合、レシーバーは、特定の送信元からのトラフィックを受信するには (S,G) チャネルに加入し、受信しないようにするには (S,G) チャネルから脱退する必要があります。つまりレシーバーは、加入先の (S,G) チャネルからのみトラフィックを受信できます。これに対し ISM の場合、

受信トラフィックの送信元 IP アドレスを知る必要はありません。チャンネル加入シグナリングに関する提案標準方式では、IGMP の INCLUDE モードメンバシップレポートを使用しますが、これは IGMP バージョン 3 でのみサポートされます。

SSM の IP アドレスの範囲

SSM は、SSM デリバリ モデルを IP マルチキャスト グループ アドレス範囲の既定サブセットに適用することで、ISM サービスと共存できます。Cisco IOS ソフトウェアでは、224.0.0.0 ~ 239.255.255.255 の IP マルチキャスト アドレス範囲に対して SSM を設定できます。SSM 範囲が定義されると、既存の IP マルチキャスト レシーバー アプリケーションがその SSM 範囲のアドレスを使用しようとしても、トラフィックをまったく受信しません（アプリケーションが明示的な [S, G] チャンネル加入を使用するように変更されている場合を除きます）。

SSM の動作

PIM-SM に基づいて IP マルチキャスト サービスを実装しているネットワークでは、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 がすでに設定されているネットワークに SSM を導入する場合、SSM がサポートされるのは最終ホップ 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がありません。一般に、最終ホップを除いたこれらのルータは、SSM 範囲で PIM-SM だけを実行する必要があり、アクセス コントロールを追加設定して SSM 範囲内で MSDP シグナリング、登録動作、または PIM-SM 共有ツリー動作が起こらないようにすることが必要になる場合があります。

SSM 範囲を設定し、SSM をイネーブルにするには、`ip pim ssm` グローバル コンフィギュレーション コマンドを使用します。この設定は、次のような影響があります。

- SSM 範囲内のグループについては、(S,G) チャンネル加入は IGMPv3 の INCLUDE モードメンバシップレポートを使用して受け入れられます。
- SSM 範囲内にあるアドレスの PIM 動作は、PIM-SM から派生したモードである PIM-SSM に切り替わります。このモードでは、PIM (S,G) Join および Prune メッセージだけがルータによって生成され、(S,G) Rendezvous Point Tree (RPT) および (*, G) 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、無視または廃棄されます。着信 PIM 登録メッセージには、登録停止メッセージがただちに返されます。ルータが最終ホップ ルータである場合を除いて、PIM-SSM は PIM-SM と下位互換性があります。したがって、最終ホップ以外のルータは SSM グループに対し PIM-SM を実行できます（ルータが SSM をまだサポートしていない場合など）。
- SSM 範囲内の MSDP Source-Active (SA) メッセージは、受け入れ、生成、転送ができません。

IGMPv3 ホスト シグナリング

IGMPv3 では、ホストがマルチキャスト グループの最終ホップ ルータにメンバシップを伝えます。ホストは、送信元を基準にしたフィルタリング機能を使用してグループメンバシップを伝えることができます。具体的には、ホストは、グループに送信するすべての送信元のうち、特定送信元からのトラフィックの受信を希望しない (EXCLUDE モード) こと、またはそのグループに送信する特定送信元だけからのトラフィックの受信を希望する (INCLUDE モード) ことを伝えることができます。

IGMPv3 は ISM および SSM の両方と連動できます。ISM では、EXCLUDE および INCLUDE モードレポートの両方を使用できます。SSM では、INCLUDE モードレポートのみが最終ホップ ルータで受け入れられます。EXCLUDE モード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 範囲の制約事項に該当するレガシー アプリケーション

SSM より古いネットワークの既存アプリケーションは、(S,G) チャネル加入をサポートするように変更しない限り、SSM 範囲内では動作しません。そのため、ネットワークで SSM をイネーブルにした場合、既存アプリケーションが SSM の指定範囲内のアドレスを使用していると問題が生じます。

アドレス管理の制約事項

SSM をレイヤ 2 スイッチング メカニズムで使用すると、アドレス管理がある程度は必要になります。CGMP、IGMP スヌーピング、または Router-Port Group Management Protocol (RGMP) は、グループ別フィルタリングだけをサポートし、(S,G) チャネル別フィルタリングをサポートしていません。スイッチド ネットワーク内の異なるレシーバーが、同じグループを共有している異なる (S,G) チャネルを要求した場合、レシーバーは既存メカニズムの恩恵を受けられません。代わりに、両方のレシーバーは全 (S,G) チャネルのトラフィックを受信し、入力時に不要なトラフィックをフィルタリングします。SSM は、多くの個別アプリケーションに対し SSM 範囲のグループ アドレスを再利用できるので、この状況はスイッチド ネットワークのトラフィック フィルタリング機能の低下につながります。この理由から、SSM 範囲からランダムな IP アドレスをアプリケーションに使用するようにして、異なるアプリケーション間で SSM 範囲内の単一アドレスが再利用される可能性を最小限にすることが重要です。たとえば、TV チャネルセットを提供するアプリケーション サービスは、SSM を使用する場合でも、TV (S,G) チャネルごとに異なるグループを使用するようにしてください。このようにすることで、レイヤ 2 スイッチを含むネットワークにおいて、同じアプリケーション サービス内の異なるチャネルを利用する複数のレシーバーでトラフィック エイリアシングが発生しないようにできます。

IGMP スヌーピングおよび CGMP の制限事項

IGMPv3 には新しいメンバシップ レポート メッセージが採用されており、このメッセージが従来の IGMP スヌーピング スイッチで正しく認識されない場合があります。

IGMP (特に CGMP) に関連するスイッチングの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、インターフェイス上に適切な (S,G) 加入が存在している場合、最終ホップ ルータは (S,G) Join メッセージの定期的な送信を継続します。したがって、レシーバーが (S,G) 加入を送信している限り、レシーバーから送信元への Shortest Path Tree (SPT) ステートが維持されます。これは送信元が長期間 (あるいはまったく) トラフィックを送信しない場合も同様です。

PIM-SM は、この反対の動作になります。つまり、送信元がトラフィックの送信を続けていて、レシーバーがグループに加入している場合に限り、(S,G) ステートが維持されます。PIM-SM では、送信元が 3 分間を超えて送信を停止した場合、(S,G) ステートは削除され、送信元からのパケットが再び RPT を介して到着した後に再確立されます。PIM-SSM には送信元がアクティブであることをレシーバーに通知するメカニズムが存在しないため、ネットワークはレシーバーがそのチャネルの受信を要求している限り、PIM-SSM の (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 <code>ip pim ssm [default range access-list]</code>	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 <code>interface type number</code>	IGMPv3 をイネーブルにできるホストに接続されているインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 <code>ip pim {sparse-mode sparse-dense-mode}</code>	インターフェイス上で PIM をイネーブルにします。 sparse mode または 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 <code>ip igmp version 3</code>	このインターフェイス上で IGMPv3 をイネーブルにします。IGMP のデフォルト バージョンはバージョン 2 に設定されています。
ステップ 5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6 <code>show running-config</code>	設定を確認します。
ステップ 7 <code>copy running-config startup-config</code>	(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
<code>show ip igmp groups detail</code>	IGMPv3 を介した (S,G) チャンネル加入を表示します。
<code>show ip mroute</code>	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 レポートを受信したかどうかを表示します。

SSM マッピングの設定

SSM マッピング機能は、エンドシステムでの SSM のサポートが管理上または技術的な理由で不可能であるか、または望ましくない場合に SSM の変換をサポートします。SSM マッピングを使用すると、IGMPv3 がサポートされないレガシー STB にビデオを配信したり、IGMPv3 ホスト スタックを使用しないアプリケーションで、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」 (P.46-19)
- 「SSM マッピングの概要」 (P.46-19)
- 「SSM マッピングの設定」 (P.46-21)
- 「SSM マッピングのモニタリング」 (P.46-23)

設定時の注意事項

SSM マッピングの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-SM 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-SM をイネーブルにする方法については、「マルチキャスト ルーティングのデフォルト設定」(P.46-11) を参照してください。
- スタティック SSM マッピングを設定する前に、Access Control List (ACL; アクセス コントロール リスト) を設定して、送信元アドレスにマッピングするグループ範囲を定義しておく必要があります。ACL の設定方法については、第 34 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 マッピングを設定し DNS lookup を使用して SSM マッピングを行う前に、稼働中の DNS サーバにレコードを追加できるようになっている必要があります。DNS サーバが稼働していない場合は、インストールする必要があります。

Cisco Network Registrar (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/warp/public/cc/pd/nemnsw/nerr/index.shtml>

SSM マッピングの制約事項を次に示します。

- SSM マッピング機能では、完全な SSM の利点のすべてが提供されるわけではありません。SSM マッピングでは、ホストのグループ加入を用いて、1 つまたは複数の送信元に関連付けられたアプリケーションとそのグループを結び付けるため、グループあたり 1 つのアプリケーションしかサポートできません。完全な SSM のアプリケーションでも、SSM マッピングに見られるような同じグループを共有できます。
- 完全な SSM の変換ソリューションとして SSM マッピングに全面的に依存している場合は、注意して最終ホップ ルータで IGMPv3 をイネーブルにしてください。SSM マッピングおよび IGMPv3 の両方をイネーブルにするときに、各ホストがすでに IGMPv3 をサポートしている場合 (ただし 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、これらの IGMPv3 グループ レポートをサポートしていません。またルータは、送信元とこれらのレポートを正しく関連付けることができません。

SSM マッピングの概要

一般的な STB 構成の場合、各 TV チャンネルは、1 つの独立した IP マルチキャスト グループを使用し、TV チャンネルを送信する 1 つのアクティブ サーバ ホストを持っています。1 つのサーバで複数の TV チャンネルを送信できますが、各チャンネルは異なるグループに送信されます。このネットワーク環境では、特定グループに対する IGMPv1 または IGMPv2 メンバシップ レポートをルータが受信する場合、レポートはマルチキャスト グループに関連付けられた TV チャンネルの well-known TV サーバに宛てられます。

SSM マッピングが設定されている場合、特定のグループに対する IGMPv1 または IGMPv2 メンバシップ レポートをルータが受信すると、ルータはこのレポートをそのグループに関連付けられている well-known 送信元の 1 つまたは複数のチャンネル メンバシップに変換します。

ルータがグループに対する IGMPv1 または IGMPv2 メンバシップ レポートを受信すると、ルータは SSM マッピングを使用して、そのグループの 1 つまたは複数の送信元 IP アドレスを特定します。SSM マッピングは次に、メンバシップ レポートを IGMPv3 レポートとして変換し、IGMPv3 レポートを受信したのものとして動作を続けます。ルータは次に、PIM Join を送信し、IGMPv1 または IGMPv2 メンバシップ レポートを受信し続ける限り、グループに加入され続けます。グループの SSM マッピングも同じ状態のままです。

SSM マッピングにより、最終ホップ ルータは、ルータ上のスタティックに設定されたテーブルまたは DNS サーバを使用して送信元アドレスを特定することができます。スタティックに設定されたテーブルまたは DNS マッピングの変更があると、ルータは加入グループに関連付けられた現在の送信元から脱退します。

SSM マッピングについては、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

スタティック SSM マッピング

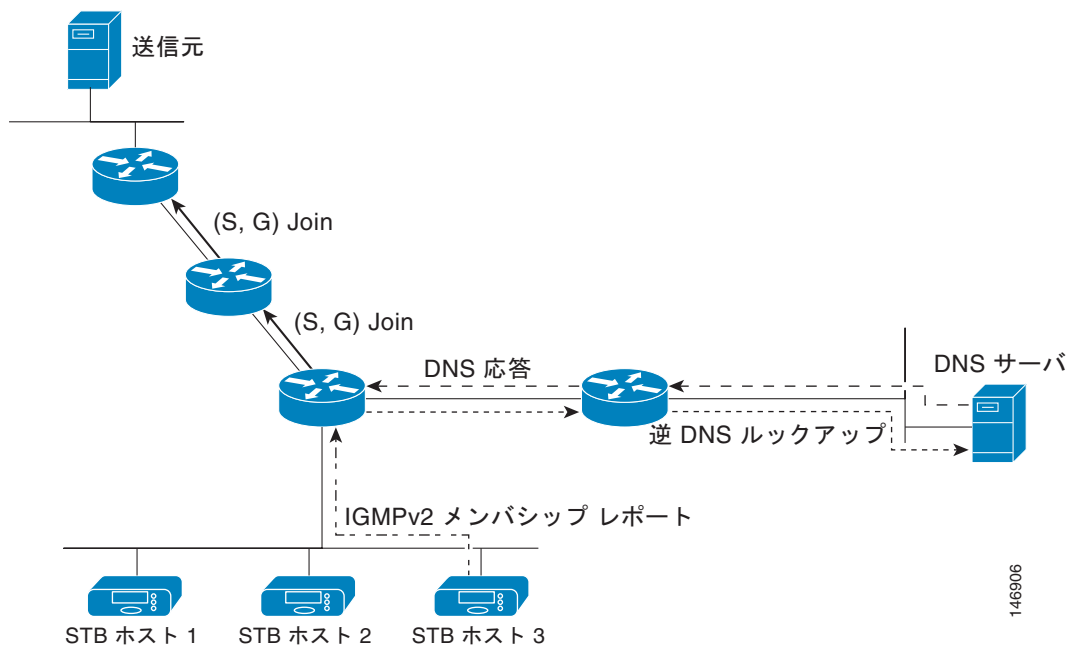
スタティック SSM マッピングを使用すると、グループに送信する送信元の特定にスタティック マップを使用するよう最終ホップ ルータを設定できます。スタティック SSM マッピングを使用するには、ACL を設定してグループ範囲を定義する必要があります。次に、**ip igmp static ssm-map** グローバル コンフィギュレーション コマンドを使用して、ACL で許可したグループを送信元にマッピングします。

DNS が必要ない小規模ネットワークや、DNS マッピングをローカルで無効にする場合、スタティック SSM マッピングを設定できます。スタティック SSM マッピングが設定されると、DNS マッピングに優先します。

DNS ベースの SSM マッピング

DNS ベースの SSM マッピングを使用すると、グループに送信する送信元の特定に逆 DNS ルックアップを実行するよう最終ホップ ルータを設定できます。DNS ベースの SSM マッピングが設定されている場合、ルータはグループアドレスを含んだドメイン名を作成し、DNS の逆ルックアップを実行します。ルータは IP アドレス リソース レコードを検索し、それ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 マッピングは、グループあたり最大 20 の送信元をサポートしています。ルータは、1 つの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



SSM マッピングのメカニズムにより、最終ホップ ルータがグループの複数の送信元に加入できるため、TV ブロードキャストの送信元冗長性を提供できます。この状況では、最終ホップ ルータが SSM マッピングの使用により冗長性を提供して、同じ TV チャンネルの 2 つのビデオ送信元に同時に加入しま

す。ただし、最終ホップ ルータでビデオトラフィックが重複しないように、ビデオの送信元はサーバ側のスイッチオーバー メカニズムを使用する必要があります。つまり、一方のビデオ送信元をアクティブに、他方のバックアップビデオ送信元をパッシブにします。パッシブな送信元はアクティブな送信元の障害が検出されるのを待って、TV チャンネルのビデオトラフィックを送信します。このように、サーバ側のスイッチオーバー メカニズムにより、1 台のサーバだけが TV チャンネルのビデオトラフィックをアクティブに送信できるようになります。

G1、G2、G3、および G4 を含むグループの 1 つまたは複数の送信元アドレスを検索するには、DNS サーバ上に次の DNS レコードを設定する必要があります。

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

DNS リソース レコードの設定の詳細については、DNS サーバのマニュアルを参照してください。SSM マッピングについては、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

SSM マッピングの設定

- 「スタティック SSM マッピングの設定」(P.46-21) (必須)
- 「DNS ベースの SSM マッピングの設定」(P.46-22) (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 フォワーディングの設定」(P.46-23) (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	<code>configure terminal</code>	グローバル 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	<code>ip igmp ssm-map enable</code>	設定した SSM 範囲内のグループの SSM マッピングをイネーブルにします。 (注) デフォルトでは、このコマンドは DNS ベースの SSM マッピングをイネーブルにします。
ステップ 3	<code>no ip igmp ssm-map query dns</code>	(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 マッピングのみを使用する場合、DNS ベースの SSM マッピングをディセーブルにしてください。デフォルトでは、 <code>ip igmp ssm-map</code> グローバル コンフィギュレーション コマンドは DNS ベースの SSM マッピングをイネーブルにします。

■ IP マルチキャストルーティングの設定

コマンド	目的
ステップ 4 ip igmp ssm-map static access-list source-address	<p>スタティック SSM マッピングを設定します。</p> <p><i>access-list</i> の ACL には、<i>source-address</i> 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を定義します。</p> <p>(注) スタティック SSM マッピングの設定は追加できます。SSM マッピングの設定が追加されている場合、ルータが SSM 範囲内のグループの IGMPv1 または IGMPv2 メンバシップ レポートを受信すると、スイッチは設定された各 ip igmp ssm-map static コマンドを使用して、グループに関連付けられた送信元アドレスを特定します。スイッチはグループあたり 20 までの送信元を関連付けます。</p>
ステップ 5 必要な場合は、ステップ 4 を繰り返してスタティック SSM マッピングの設定を追加します。	—
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。

SSM マッピングの設定例については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html

DNS ベースの SSM マッピングの設定

DNS ベースの SSM マッピングを設定するには、DNS サーバゾーンを作成するか、既存のゾーンにレコードを追加する必要があります。DNS ベースの SSM マッピングを使用しているルータが他の目的にも DNS を使用している場合は、通常設定されている DNS サーバを使用するようにしてください。DNS ベースの SSM マッピングがルータ上で使用されている唯一の DNS の運用である場合は、空のルートゾーンを使用するか、自身を指定するルートゾーンを使用して疑似的な DNS セットアップを設定できます。

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

コマンド	目的
ステップ 1 configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2 ip igmp ssm-map enable	設定した SSM 範囲内のグループの SSM マッピングをイネーブルにします。
ステップ 3 ip igmp ssm-map query dns	<p>(任意) DNS ベースの SSM マッピングをイネーブルにします。</p> <p>デフォルトでは、ip igmp ssm-map コマンドは DNS ベースの SSM マッピングをイネーブルにします。この no 形式のコマンドだけが実行コンフィギュレーションに保存されます。</p> <p>(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に、DNS ベースの SSM マッピングを再度イネーブルにするためにこのコマンドを使用します。</p>

コマンド	目的
ステップ 4 ip domain multicast <i>domain-prefix</i>	(任意) DNS ベースの SSM マッピングにスイッチが使用しているドメインプレフィクスを変更します。 デフォルトでは、スイッチは <i>ip-addr.arpa</i> ドメインプレフィクスを使用します。
ステップ 5 ip name-server <i>server-address1</i> [<i>server-address2</i>... <i>server-address6</i>]	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。
ステップ 6 必要な場合は、ステップ 5 を繰り返して冗長性のための DNS サーバの設定を追加します。	—
ステップ 7 end	特権 EXEC モードに戻ります。
ステップ 8 show running-config	設定を確認します。
ステップ 9 copy running-config startup-config	(任意) 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 フォワーディングの設定

特定のグループの SSM トラフィックをスタティックに転送するには、SSM マッピングによるスタティック トラフィック フォワーディングを使用します。

SSM マッピングを使用したスタティック トラフィック フォワーディ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 interface <i>type number</i>	マルチキャスト グループのトラフィックを SSM マッピングを使用してスタティックに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 マッピングによるトラフィックのスタティック フォワーディングは、DNS ベースの SSM マッピングまたはスタティックに設定された SSM マッピングと連動します。
ステップ 3 ip igmp static-group <i>group-address</i> source <i>ssm-map</i>	インターフェイスからの (S,G) チャンネルをスタティックに転送するように SSM マッピングを設定します。 特定のグループの SSM トラフィックをスタティックに転送する場合には、このコマンドを使用します。DNS ベースの SSM マッピングは、チャンネルの送信元アドレスの特定に使用します。
ステップ 4 show running-config	設定を確認します。
ステップ 5 copy running-config startup-config	(任意) 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 マッピングをモニタするには、表 46-3 に示す特権 EXEC 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 コマンド

コマンド	目的
show ip igmp ssm-mapping	SSM マッピングに関する情報を表示します。
show ip igmp ssm-mapping group-address	SSM マッピングが使用する、特定のグループの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で IGMP によって学習されたレシーバーを持ったマルチキャスト グループを表示します。
show host	デフォルトのドメイン名、名前検索サービスの方式、ネームサーバホストのリスト、およびキャッシュ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	送受信した IGMP パケットおよび IGMP ホスト関連のイベントを表示します。

SSM マッピングのモニタリング例については、次の URL にアクセスしてください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a6d6f.html#wp1047772

PIM スタブ ルーティングの設定

PIM スタブ ルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャストルーティングをサポートします。また、アップリンク PIM インターフェイスと PIM パッシブ インターフェイスの 2 種類の PIM インターフェイスをサポートします。PIM パッシブ モードで設定されたルーテッド インターフェイスは、PIM コントロール トラフィックの通過または転送を行いません。IGMP トラフィックの通過または転送のみを行います。

PIM スタブ ルーティングの設定時の注意事項

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

- PIM スタブ ルーティングを設定する前に、スタブ ルータおよび中央ルータの両方に IP マルチキャストルーティングを設定しておく必要があります。また、スタブ ルータのアップリンク インターフェイスに PIM モード (DM、SM、または DM-SM) も設定しておく必要があります。
- PIM スタブ ルータは、ディストリビューション ルータ間で中継トラフィックのルーティングを行いません。ユニキャスト (EIGRP) スタブ ルーティングではこの動作が適用されます。ユニキャスト スタブ ルーティングを設定して PIM スタブ ルータの動作を補助する必要があります。詳細については、「EIGRP スタブ ルーティングの設定」(P.38-45) を参照してください。
- 直接接続されるマルチキャスト (IGMP) 受信者と送信元のみが、レイヤ 2 アクセス ドメイン内に許可されます。PIM プロトコルは、アクセス ドメインではサポートされません。
- 冗長 PIM スタブ ルータ トポロジはサポートされません。

PIM スタブルーティングのイネーブル化

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル 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	<code>interface interface-id</code>	PIM スタブルーティングをイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>ip pim passive</code>	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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip pim interface</code>	各インターフェイスでイネーブルになっている PIM スタブを表示します。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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 (`sparse-dense-mode` がイネーブル)。PIM スタブルーティングは、図 46-2 に示すように、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 でイネーブルになっています。

```
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で 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 コマンドを使用してください。

```
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
```

PIM スタブの設定およびステータスに関する情報を表示するには、次の特権 EXEC コマンドを使用します。

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

RP の設定

インターフェイスが SM-DM で、グループを希薄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。複数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.46-26)
- 「自動 RP の設定」(P.46-28) (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.46-32) (IETF 標準のトラッキング 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.46-12) 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 (代表ルータ) から受信して RP に転送される Register 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せん。RP はマルチキャスト グループのメンバーではなく、マルチキャスト送信元およびグループ メンバーの「合流地点」として機能します。

アクセス リストで定義される複数のグループに、単一の RP を設定できます。グループに RP が設定されていない場合、マルチレイヤ スイッチは PIM DM 技術を使用し、グループを dense (稠密) 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	<code>configure terminal</code>	グローバル 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	<code>ip pim rp-address ip-address [access-list-number] [override]</code>	<p>PIM RP のアドレスを設定します。</p> <p>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 dense (稠密) として処理します。</p> <p>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。</p> <ul style="list-style-type: none"> <code>ip-address</code> 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) <code>access-list-number</code> を指定する場合は、1 ~ 99 の IP 標準アクセス リスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 (任意) override キーワードを指定すると、このコマンドによって設定された RP と、自動 RP または BSR で取得された RP との間に矛盾が生じた場合に、このコマンドによって設定された RP が優先されます。
ステップ 3	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	<p>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。</p> <ul style="list-style-type: none"> <code>access-list-number</code> 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。 <code>source</code> 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) <code>source-wildcard</code> には、<code>source</code> 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 を入れます。 <p>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。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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 の場合のみ、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
```

自動 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 Cisco 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 を設定する場合は、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.46-26) 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 に設定されていて、**ip pim autorp listener** グローバル コンフィギュレーション コマンドを入力した場合は、自動 RP グループの手動 RP アドレスですべてのデバイスが設定されていない場合でも、自動 RP を使用できます。

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ネットワークでの自動 RP の設定](#)」(P.46-28) (任意)
- 「[既存の SM クラウドへの自動 RP の追加](#)」(P.46-28) (任意)
- 「[問題のある RP への Join メッセージの送信禁止](#)」(P.46-30) (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.46-31) (任意)

概要については、「[自動 RP](#)」(P.46-7) を参照してください。

新規インターネットネットワークでの自動 RP の設定

新規インターネット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.46-28) 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 <code>show running-config</code>	<p>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。</p> <p>SM-DM 環境の場合、このステップは不要です。</p> <p>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 によってダイナミックに検出された RP は、スタティックに設定された RP よりも優先されます。ローカル グループ用に別の RP を使用することもできます。</p>
ステップ 2 <code>configure terminal</code>	<p>グローバル コンフィギュレーション モードを開始します。</p>
ステップ 3 <code>ip pim send-rp-announce interface-id scope ttl group-list access-list-number interval seconds</code>	<p>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。</p> <ul style="list-style-type: none"> 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。指定できる範囲は 1 ~ 255 です。 group-list access-list-number には、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。デフォルト値は 60 ミリ秒です。指定できる範囲は 1 ~ 16383 です。
ステップ 4 <code>access-list access-list-number {deny permit} source [source-wildcard]</code>	<p>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。</p> <ul style="list-style-type: none"> 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 を入れます。 <p>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。</p>

コマンド	目的
ステップ 5 <code>ip pim send-rp-discovery scope ttl</code>	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。指定できる範囲は 1 ~ 255 です。
ステップ 6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 7 <code>show running-config</code> <code>show ip pim rp mapping</code> <code>show ip pim rp</code>	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 <code>copy running-config startup-config</code>	(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 gigabitethernet1/0/1 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、後でこの問題を解決できます。ルータまたはマルチレイヤ スイッチが `ip pim accept-rp` コマンドによってすでに設定されている場合は、このコマンドを再入力し、新規にアドバタイズされる RP を許可する必要があります。

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	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
ステップ 3 access-list access-list-number {deny permit} source [source-wildcard]	<p>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。</p> <ul style="list-style-type: none"> 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 を入れます。 <p>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。</p>
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 アナウンスのみを許可します。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 グループ宛のアナウンスメントのみを許可します。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.46-32) (任意)
- 「IP マルチキャスト境界の定義」(P.46-33) (任意)
- 「候補 BSR の設定」(P.46-34) (任意)
- 「候補 RP の設定」(P.46-35) (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きます。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、間違っただメイン内で RP が選択されたりすることがあります。

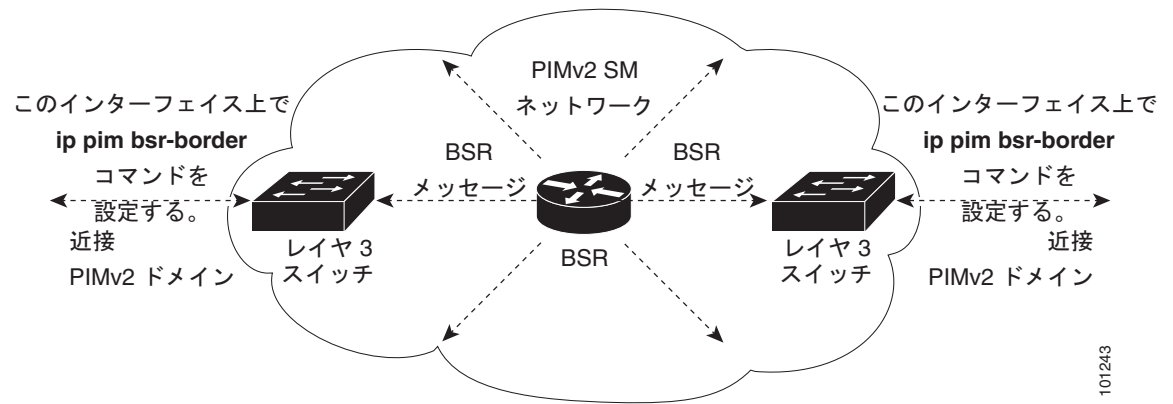
PIM ドメイン境界を定義するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip pim bsr-border	PIM ドメイン用の PIM ブートストラップ メッセージ境界を定義します。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)。

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 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。 <ul style="list-style-type: none"> 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 を入れます。 <p>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。</p>
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。

■ IP マルチキャストルーティングの設定

	コマンド	目的
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。 <ul style="list-style-type: none"> 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 ビットのみが使用されます。 (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
Switch(config-if)# ip pim bsr-candidate gigabitethernet0/2 30 10
Switch(config-if)# ip pim bsr-candidate gigabitethernet1/2 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 アドバタイズメントを 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 のみが使用されている Cisco ルータおよび Cisco 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のみ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。 <ul style="list-style-type: none"> • <i>interface-id</i> には、対応する IP アドレスが候補 RP アドレスとしてアドバタイズされるインターフェイスを指定します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • (任意) group-list access-list-number には、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。 <ul style="list-style-type: none"> • <i>access-list-number</i> 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。 • <i>source</i> 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) <i>source-wildcard</i> には、<i>source</i> 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 を入れます。 <p>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。</p>
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クスが指定されます。この RP は、プレフィクスが 239 であるグループを処理します。

```
Switch(config)# ip pim rp-candidate gigabitethernet1/0/2 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

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、「[自動 RP の設定](#)」(P.46-28) および「[候補 BSR の設定](#)」(P.46-34) を参照してください。
- グループプレフィクスが自動 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	<code>show ip pim rp [[group-name group-address] mapping]</code>	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。 <ul style="list-style-type: none"> • (任意) <code>group-name</code> 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) <code>group-address</code> 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（設定されているか、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、<code>mapping</code> キーワードを使用します。
ステップ 2	<code>show ip pim rp-hash group</code>	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。 <code>group</code> 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 を取得する方法 (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解決するには、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

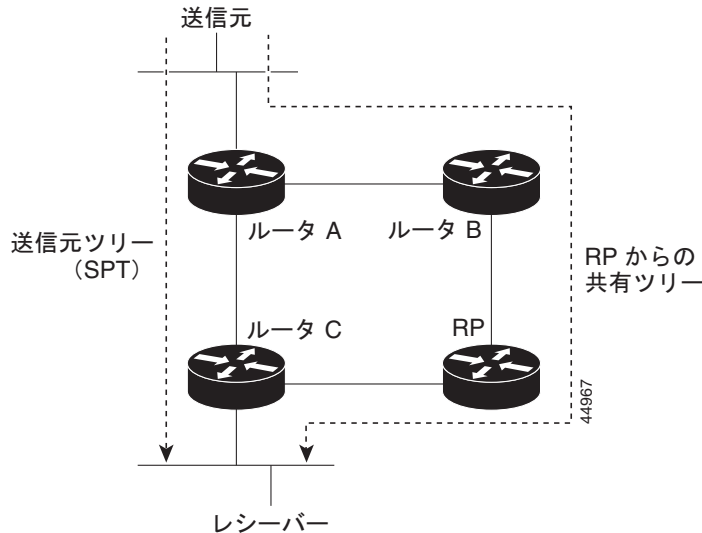
ここでは、高度なオプションの PIM 機能について説明します。

- 「PIM 共有ツリーおよび送信元ツリーの概要」 (P.46-37)
- 「PIM SPT 使用の延期」 (P.46-39) (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.46-40) (任意)

PIM 共有ツリーおよび送信元ツリーの概要

デフォルトでは、グループのメンバー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、共有ツリーに加入しているグループ メンバーに配信するため、RP にアドバタイズされます。

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. レシーバーがグループに加入します。リーフ ルータ C は Join メッセージを RP に向けて送信します。
2. RP はルータ C とのリンクを発信インターフェイス リストに格納します。
3. 送信元がデータを送信します。ルータ A はデータをカプセル化して Register 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 Register 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 は送信元宛の Prune 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 Prune メッセージを送信します。

Join および Prune メッセージが送信元および RP に送信されます。これらのメッセージはホップバイホップで送信され、送信元または RP へのパス上にある各 PIM デバイスで処理されます。Register メッセージおよび Register 停止メッセージはホップバイホップで送信されません。これらのメッセージは、送信元に直接接続された代表ルータで送信され、グループの RP で受信されます。

グループへ送信する複数の送信元で、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.46-39) 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後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、**Prune** 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。 <ul style="list-style-type: none"> <i>access-list-number</i> 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。 <i>source</i> 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) <i>source-wildcard</i> には、<i>source</i> 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 を入れます。 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	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。 <ul style="list-style-type: none"> <i>kbps</i> 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。デフォルトは 0 kbps 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 kbps 以外は無効です。 <ul style="list-style-type: none"> infinity を指定すると、指定されたグループのすべての送信元で共有ツリーが使用され、送信元ツリーに切り替わらなくなります。 (任意) group-list access-list-number には、ステップ 2 で作成したアクセス リストを指定します。値 0 を指定する場合、またはグループ リストを使用しない場合、しきい値はすべてのグループに適用されます。
ステップ 4	end	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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 {kpbs | 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 が使用中の場合のみ、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 Register 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	<code>configure terminal</code>	グローバル 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	<code>interface interface-id</code>	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	<code>ip pim query-interval seconds</code>	スイッチが PIM ルータクエリー メッセージを送信する頻度を設定します。 デフォルト値は 30 秒です。指定できる範囲は 1 ~ 65535 です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip igmp interface [interface-id]</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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、次の設定情報について説明します。

- 「IGMP のデフォルト設定」 (P.46-41)
- 「グループのメンバーとしてのスイッチの設定」 (P.46-41) (任意)
- 「IP マルチキャスト グループへのアクセスの制御」 (P.46-42) (任意)
- 「IGMP バージョンの変更」 (P.46-43) (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.46-43) (任意)
- 「IGMPv2 の IGMP クエリー タイムアウトの変更」 (P.46-44) (任意)

- 「IGMPv2 の最大クエリー応答時間の変更」(P.46-45) (任意)
- 「スタティックに接続されたメンバーとしてのスイッチの設定」(P.46-45) (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 グループのメンバーとしてのマルチレイヤ スイッチ	グループ メンバシップは未定義
マルチキャスト グループへのアクセス	インターフェイスのすべてのグループを許可
IGMP バージョン	すべてのインターフェイスでバージョン 2
IGMP ホストクエリー メッセージ インターバル	すべてのインターフェイスで 60 秒
IGMP クエリー タイムアウト	すべてのインターフェイスで 60 秒
IGMP 最大クエリー応答時間	すべてのインターフェイスで 10 秒
スタティックに接続されたメンバーとしてのマルチレイヤ スイッチ	ディセーブル

グループのメンバーとしてのスイッチの設定

スイッチをマルチキャスト グループのメンバーとして設定し、マルチキャストがネットワークに到達可能かどうかを検出できます。管理しているすべてのマルチキャスト対応ルータおよびマルチレイヤ スイッチがマルチキャスト グループのメンバーである場合、グループに ping を送信すると、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ッシングされた 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ーになるように設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル 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 <code>interface interface-id</code>	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 <code>ip igmp join-group group-address</code>	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、グループのメンバシップは定義されていません。 <code>group-address</code> 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 <code>end</code>	特権 EXEC モードに戻ります。

■ オプションの IGMP 機能の設定

	コマンド	目的
ステップ 5	<code>show ip igmp interface [interface-id]</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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ーが属しているマルチキャスト グループを判別します。次に、スイッチは、マルチキャスト グループにアドレッシングされたすべてのパケットをこれらのグループ メンバーに転送します。インターフェイスごとにフィルタを適用し、インターフェイスで処理されるサブネット上のホストが加入可能なマルチキャスト グループを制限できます。

インターフェイスで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	<code>configure terminal</code>	グローバル 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	<code>interface interface-id</code>	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	<code>ip igmp access-group access-list-number</code>	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。 <i>access-list-number</i> 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	<code>exit</code>	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	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	標準アクセス リストを作成します。 <ul style="list-style-type: none"> <i>access-list-number</i> 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。 <i>source</i> 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) <i>source-wildcard</i> には、<i>source</i> 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 を入れます。 <p>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。</p>

	コマンド	目的
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show ip igmp interface [interface-id]</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(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 にのみ加入できるように設定する例を示します。

```
Switch(config)# access-list 1 255.2.2.2 0.0.0.0
Switch(config)# interface gigabitethernet1/0/1
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	<code>configure terminal</code>	グローバル 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	<code>interface interface-id</code>	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	<code>ip igmp version {1 2}</code>	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 コマンドを設定することができません。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip igmp interface [interface-id]</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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後で、マルチキャスト グループのメンバーであるローカルホストが存在しないことをソフトウェアが検出した場合、そのグループのリモート送信元からローカル ネットワークへのマルチキャスト パケット転送が停止され、Prune 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	<code>configure terminal</code>	グローバル 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	<code>interface interface-id</code>	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	<code>ip igmp query-interval seconds</code>	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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show ip igmp interface [interface-id]</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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	<code>configure terminal</code>	グローバル 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	<code>interface interface-id</code>	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 <code>ip igmp querier-timeout seconds</code>	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 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 5 <code>show ip igmp interface [interface-id]</code>	設定を確認します。
ステップ 6 <code>copy running-config startup-config</code>	(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 メンバー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 <code>configure terminal</code>	グローバル 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 <code>interface interface-id</code>	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 <code>ip igmp query-max-response-time seconds</code>	IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更します。 デフォルト値は 10 秒です。指定できる範囲は 1 ~ 25 です。
ステップ 4 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 5 <code>show ip igmp interface [interface-id]</code>	設定を確認します。
ステップ 6 <code>copy running-config startup-config</code>	(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。

スタティックに接続されたメンバーとしてのスイッチの設定

ネットワーク セグメント上にグループ メンバーが存在しなかったり、ホストで IGMP を使用してグループ メンバシップを報告することが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。

■ オプションのマルチキャストルーティング機能の設定

- **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、転送のみを実行します。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明らかなように、スイッチ自体はメンバーではありません。

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

	コマンド	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-id	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	ip igmp static-group group-address	スイッチをスタティックに接続されたグループのメンバーとして設定します。 デフォルトでは、この機能はディセーブルです。
ステップ 4	end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp interface [interface-id]	設定を確認します。
ステップ 6	copy running-config startup-config	(任意) 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.46-46) (任意)
 - 「[sdr リスナー サポート機能の設定](#)」 (P.46-47) (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.46-49) (任意)
- VPN Routing/Forwarding Table (VRF; VPN ルーティング/転送テーブル) にマルチキャストを設定する手順：
 - 「[マルチキャスト VRF の設定](#)」 (P.38-84)

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 Cisco 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 アドレスにアドレッシングされます。

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	<code>configure terminal</code>	グローバル 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	<code>interface interface-id</code>	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	<code>ip cgmp [proxy]</code>	<p>インターフェイス上で CGMP をイネーブルにします。</p> <p>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。</p> <p>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のみ、CGMP をイネーブルにします。</p> <p>(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。</p> <p>(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。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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、非 Cisco ルータよりも IGMP クエリアを優先させてください。

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 を通じ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。

■ オプションのマルチキャストルーティング機能の設定

ます。この情報は、MBONE Session Directory バージョン 2 (sdr) ツールによって提供されます。このフリーウェアアプリケーションは WWW 上の複数のサイト (<http://www.video.ja.net/mice/index.html> など) からダウンロードできます。

SDR は、Session Announcement Protocol (SAP) マルチキャスト パケット用の既知のマルチキャストグループ アドレスおよびポートを、SAP クライアントからリスニング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、およびアダプ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 ディレクトリのアダプタイズメントはリスニングされません。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 アダプタイズメントをリスニング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	<code>configure terminal</code>	グローバル 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	<code>interface interface-id</code>	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	<code>ip sdr listen</code>	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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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 情報のアダプタイズを停止した場合に、古いアダプ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	<code>configure terminal</code>	グローバル 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	<code>ip sdr cache-timeout minutes</code>	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。 <code>minutes</code> に指定できる範囲は 1 ~ 4294967295 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(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

管理の有効範囲付き境界を使用し、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、「管理の有効範囲付きアドレス」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。管理の有効範囲付き境界をルーテッドインターフェイスに設定すると、マルチキャストグループアドレスがこの範囲内にあるマルチキャストトラフィックは、このインターフェイスに出入りすることができません。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。

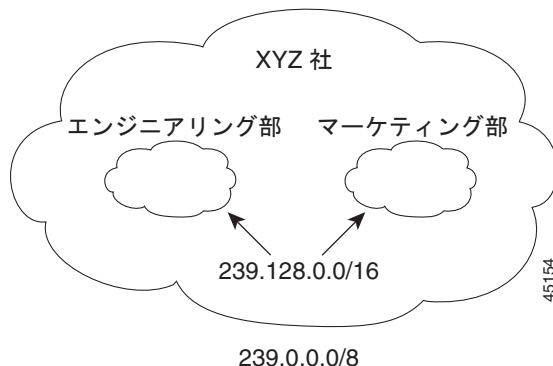


(注)

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、管理の有効範囲付き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、管理の有効範囲付き境界を 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 管理の有効範囲付き境界



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の有効範囲付き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することができません。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。

■ 基本的な DVMRP 相互運用性機能の設定

IANA は、マルチキャスト アドレス範囲 239.0.0.0 ~ 239.255.255.255 を管理の有効範囲付き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せん。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。

管理の有効範囲付き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	<code>configure terminal</code>	グローバル 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	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	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。 <ul style="list-style-type: none"> <code>access-list-number</code> の範囲は 1 ~ 99 です。 <code>deny</code> 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。 <code>permit</code> 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。 <code>source</code> 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) <code>source-wildcard</code> には、<code>source</code> 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 を入れます。 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	<code>interface interface-id</code>	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	<code>ip multicast boundary access-list-number</code>	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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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、すべての管理の有効範囲付き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、次の設定情報について説明します。

- 「DVMRP 相互運用性の設定」(P.46-51) (任意)
- 「DVMRP トンネルの設定」(P.46-53) (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.46-55) (任意)
- 「mrinfo 要求への応答」(P.46-55) (任意)

高度な DVMRP 機能の詳細については、「高度な DVMRP 相互運用性機能の設定」(P.46-56) 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、DVMRP プローブ メッセージをリスニングし、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 Cisco 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 <code>configure terminal</code>	グローバル 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 <code>access-list access-list-number {deny permit} source [source-wildcard]</code>	<p>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。</p> <ul style="list-style-type: none"> <code>access-list-number</code> の範囲は 1 ~ 99 です。 <code>deny</code> 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。<code>permit</code> 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。 <code>source</code> 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) <code>source-wildcard</code> には、<code>source</code> 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 を入れます。 <p>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。</p>

	コマンド	目的
ステップ 3	<code>interface interface-id</code>	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	<code>ip dvmrp metric metric [list access-list-number] [[protocol process-id] [dvmrp]]</code>	<p>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。</p> <ul style="list-style-type: none"> <code>metric</code> 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) <code>list access-list-number</code> に、ステップ 2 で作成されたアクセスリスト番号を入力します。この指定をすると、このアクセスリストに一致するマルチキャストの宛先だけが設定済みの基準に従ってレポートされます。 (任意) <code>protocol process-id</code> を指定する場合は、<code>eigrp</code>、<code>igrp</code>、<code>ospf</code>、<code>rip</code>、<code>static</code>、または <code>dvmrp</code> 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) <code>dvmrp</code> キーワードが指定されている場合は、設定された <code>metric</code> 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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(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)# 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 トンネルを設定することはできません。

Cisco ルータまたは Cisco 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、ネットワーク番号のみ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	<code>configure terminal</code>	グローバル 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	<code>access-list access-list-number {deny permit} source [source-wildcard]</code>	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。 <ul style="list-style-type: none"> • <code>access-list-number</code> の範囲は 1 ~ 99 です。 • <code>deny</code> 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。 <code>permit</code> 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。 • <code>source</code> 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) <code>source-wildcard</code> には、<code>source</code> 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 を入れます。 <p>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。</p>
ステップ 3	<code>interface tunnel number</code>	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	<code>tunnel source ip-address</code>	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	<code>tunnel destination ip-address</code>	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	<code>tunnel mode dvmrp</code>	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	<code>ip address address mask</code> または <code>ip unnumbered type number</code>	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非番号として設定します。
ステップ 8	<code>ip pim [dense-mode sparse-mode]</code>	インターフェイスに PIM モードを設定します。

	コマンド	目的
ステップ 9	ip dvmrp accept-filter <i>access-list-number</i> [<i>distance</i>] neighbor-list <i>access-list-number</i>	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。 <ul style="list-style-type: none"> • <i>access-list-number</i> 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) <i>distance</i> 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。指定できる範囲は 1 ~ 255 です。 • neighbor-list <i>access-list-number</i> 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のみ許可されます。
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 のデバイスと近接している場合は、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	<code>configure terminal</code>	グローバル 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	<code>interface interface-id</code>	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	<code>ip dvmrp default-information {originate only}</code>	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 のデバイスのネイバーのみ使用します。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • originate - 0.0.0.0 以外の具体的なルートもアドバタイズできるように指定します。 • only - 0.0.0.0 以外の DVMRP ルートはアドバタイズされません。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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 Cisco 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 Cisco マルチレイヤ スイッチは PIM を実行し、マルチキャスト パケットをレシーバーに転送したり、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 Cisco 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、次の設定情報について説明します。

- 「DVMRP ユニキャスト ルーティングのイネーブル化」(P.46-56) (任意)
- 「DVMRP の非プルーニング ネイバーの拒否」(P.46-57) (任意)
- 「ルート交換の制御」(P.46-59) (任意)

基本的な DVMRP 機能の詳細については、「基本的な DVMRP 相互運用性機能の設定」(P.46-50) を参照してください。

DVMRP ユニキャスト ルーティングのイネーブル化

マルチキャスト ルーティングおよびユニキャスト ルーティングには個別のトポロジが必要となるため、PIM はマルチキャスト トポロジに従って、ループのない配信ツリーを構築する必要があります。Cisco ルータ、Cisco 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リバース パスを転送します。

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 Cisco 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	<code>configure terminal</code>	グローバル 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	<code>interface interface-id</code>	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	<code>ip dvmrp unicast-routing</code>	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設定されています。

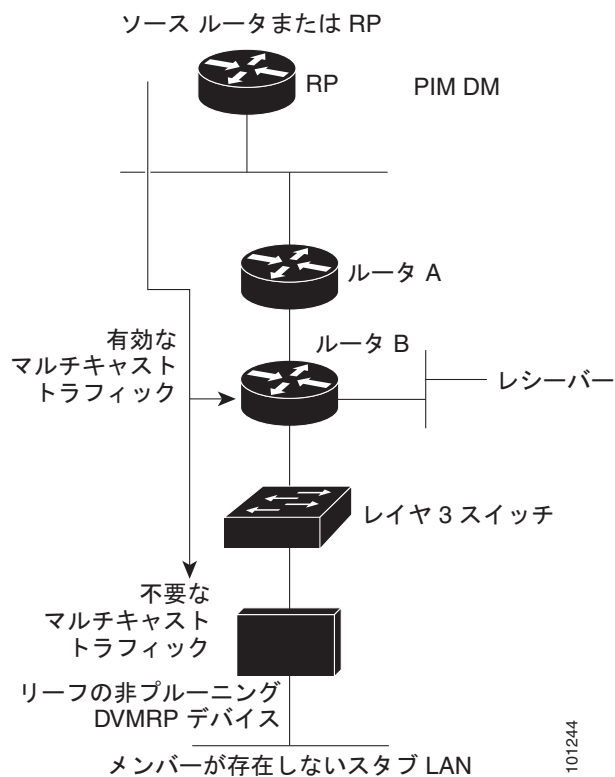
	コマンド	目的
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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

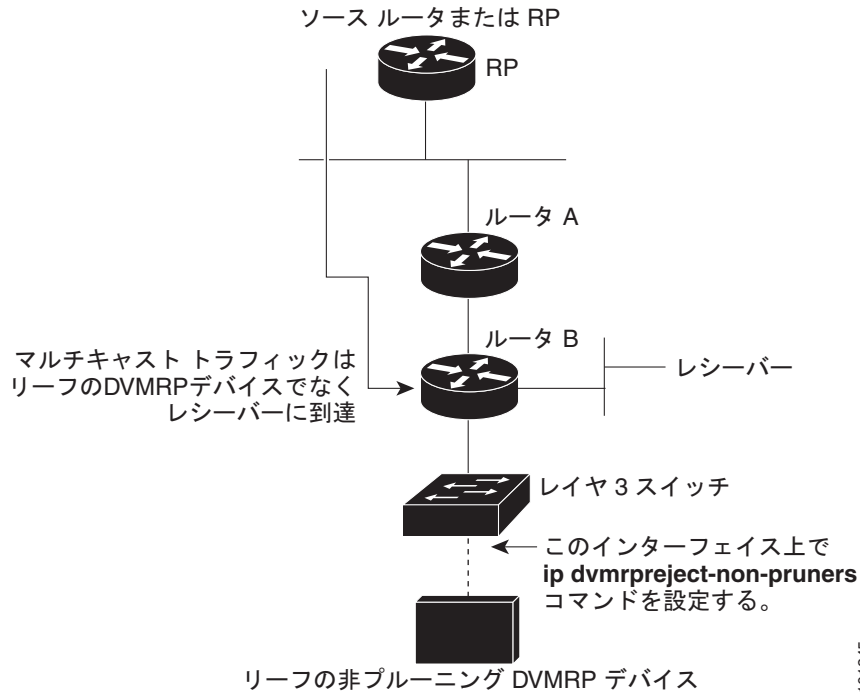
デフォルトでは、DVMRP 機能に関係なく、シスコ デバイスはすべての DVMRP ネイバーをピアとして受け入れます。ただし、一部の非シスコ デバイスでは、プルーニング機能を持たない古いバージョンの DVMRP が動作するため、常時転送パケットが受信されて帯域幅が消費されます。図 46-8 にこの事例を示します。

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 ルータが非プルーンング 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のみが禁止されます。拒否されていない非プルーンング ルータが（レシーバー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、非プルーンング DVMRP ネットワークが存在する場合があります。

非プルーンング 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 <code>configure terminal</code>	グローバル 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 <code>interface interface-id</code>	非プルーンング 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 <code>ip dvmrp reject-non-pruners</code>	非プルーンング DVMRP ネイバーとのピアリングを禁止します。
ステップ 4 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 5 <code>show running-config</code>	設定を確認します。
ステップ 6 <code>copy running-config startup-config</code>	(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.46-59) (任意)
- 「DVMRP ルートしきい値の変更」(P.46-59) (任意)
- 「DVMRP サマリーアドレスの設定」(P.46-60) (任意)
- 「DVMRP 自動サマライズのディセーブル化」(P.46-62) (任意)
- 「DVMRP ルートへのメトリック オフセットの追加」(P.46-62) (任意)

アドバタイズされる DVMRP ルート数の制限

デフォルトでは、DVMRP を実行するためにイネーブル化されたインターフェイス（つまり、DVMRP トンネル、DVMRP ネイバーが検出されたインターフェイス、または **ip dvmrp unicast-routing** インターフェイス コンフィギュレーション コマンドを実行するように設定されたインターフェイス）を通して、7000 の DVMRP ルートのみ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って大量のルートが MBONE に入るのを防ぐことができます。 デフォルトでは、7000 のルートがアドバタイズされます。指定できる範囲は 0 ～ 4294967295 です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show running-config	設定を確認します。
ステップ 5	copy running-config startup-config	(任意) 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 10000 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	<code>configure terminal</code>	グローバル 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	<code>ip dvmrp routehog-notification route-count</code>	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 10000 ルートで、指定できる範囲は 1 ~ 4294967295 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(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。

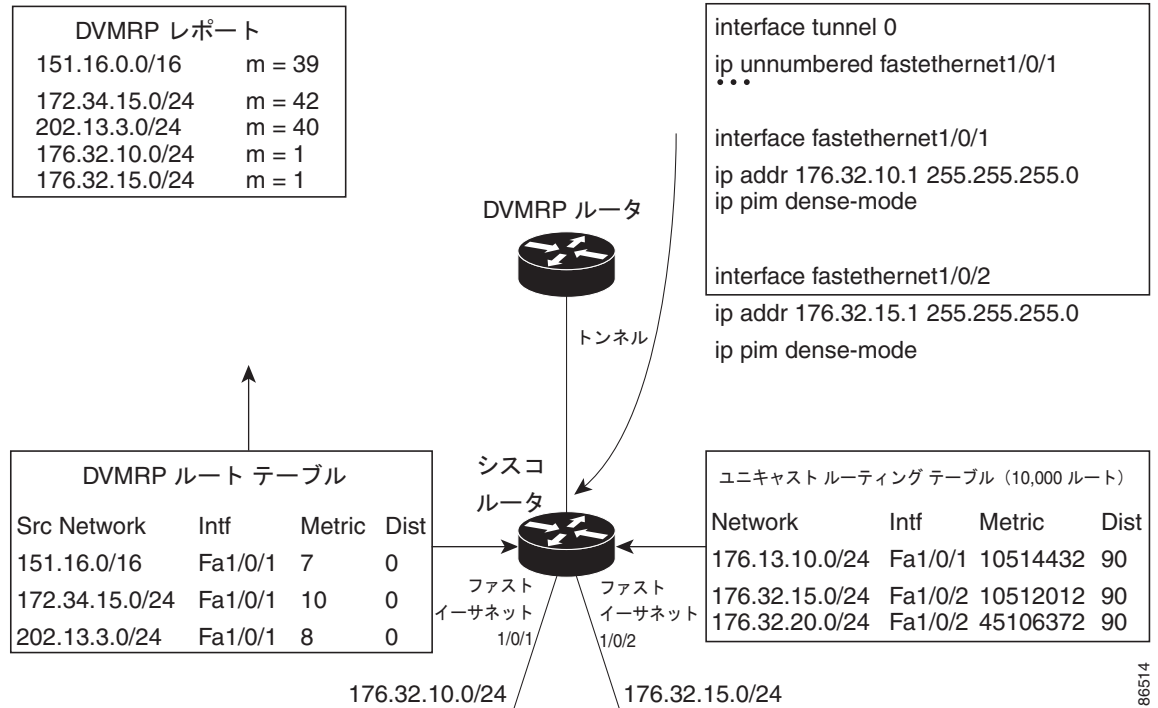
DVMRP サマリー アドレスの設定

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 ルートのみ（つまり、ルータに直接接続されたサブネットへのルートのみ）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。この例では、Cisco ルータによって送信される DVMRP レポートに、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 つの元のルートが記述されています。これらのルートの後に、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）にアドバタイズメントされる 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 つのルートのみ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 のみ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 アドバタイズメントを送信します。

図 46-10 接続されたユニキャスト ルートにのみアドバタイズ (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。 <ul style="list-style-type: none"> 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。デフォルト値は 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ネイバー 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 から取得されたとします。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 によって取得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 によって取得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	<code>configure terminal</code>	グローバル 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	<code>interface interface-id</code>	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	<code>ip dvmrp metric-offset [in out] increment</code>	<p>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。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> （任意） in : 増分値が着信 DVMRP レポートに追加され、mrinfo 応答内で報告されるように指定します。 （任意） out : 増分値が、DVMRP ルーティング テーブルのルートに対する発信 DVMRP レポートに追加されるように指定します。 <p>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。</p> <p><i>increment</i> 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。</p> <p><code>ip dvmrp metric-offset</code> 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。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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.46-64)
- 「システムおよびネットワーク統計情報の表示」 (P.46-64)
- 「IP マルチキャストルーティングのモニタ」 (P.46-65)

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
<code>clear ip cgmp</code>	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。
<code>clear ip dvmrp route {* route}</code>	DVMRP ルーティング テーブルからルートを削除します。
<code>clear ip igmp group [group-name group-address interface]</code>	IGMP キャッシュのエントリを削除します。
<code>clear ip mroute {* group [source]}</code>	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。
<code>clear ip pim auto-rp rp-address</code>	自動 RP キャッシュをクリアします。
<code>clear ip sdr [group-address "session-name"]</code>	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、デバイス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
<code>ping [group-name group-address]</code>	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。
<code>show ip dvmrp route [ip-address]</code>	DVMRP ルーティング テーブルのエントリを表示します。
<code>show ip igmp groups [group-name group-address type number]</code>	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。
<code>show ip igmp interface [type number]</code>	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。

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
<code>show ip mcache [group [source]]</code>	IP 高速スイッチング キャッシュの内容を表示します。
<code>show ip mpacket [source-address name] [group-address name] [detail]</code>	回覧用キャッシュヘッダー バッファの内容を表示します。
<code>show ip mroute [group-name group-address] [source] [summary] [count] [active kbps]</code>	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。
<code>show ip pim interface [type number] [count] [detail]</code>	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。
<code>show ip pim neighbor [type number]</code>	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。
<code>show ip pim rp [group-name group-address]</code>	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。
<code>show ip rpf {source-address name}</code>	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。
<code>show ip sdr [group "session-name" detail]</code>	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
<code>mrinfo [hostname address] [source-address interface]</code>	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ネイバー 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。
<code>mstat source [destination] [group]</code>	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。
<code>mtrace source [destination] [group]</code>	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。

