PIM（Protocol Independent Multicast）の設定

PIM の前提条件

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

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

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

- スタブ ルータと中央のルータの両方に IP マルチキャスト ルーティングが設定されている必要があります。スタブルータのアップリンク インターフェイスで、PIM モードの設定も必要です。
- また、デバイスに Enhanced Interior Gateway Routing Protocol（EIGRP）スタブルーティングまたは Open Shortest Path First（OSPF）スタブルーティングが設定されている必要があります。
- PIM スタブ ルータは、ディストリビューション ルータ間の伝送トラフィックのルーティングは行いません。ユニキャスト（EIGRP）スタブ ルーティングではこの動作が強制され

ます。PIM スタブ ルータの動作を支援するためにユニキャスト スタブ ルーティングを設定する必要があります。

PIM に関する制約事項

次に、PIM を設定する際の制約事項を示します。

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

PIMv1 および PIMv2 の相互運用性

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

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

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

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

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

PIMv2 デバイスを PIMv1 デバイスと相互運用させる場合は、自動 RP を事前に導入しておく必要があります。自動 RP マッピング エージェントでもある PIMv2 BSR は、自動 RP で選択された RP を自動的にアドバタイズします。つまり、自動 RP によって、グループ内のルータまた

はマルチレイヤごとに 1 つの RP が設定されます。ドメイン内のルータおよびスイッチの中には、複数の RP を選択するために PIMv2 ハッシュ機能を使用しないものもあります。

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

- 領域全体で Auto-RP を使用します。

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

PIM スタブ ルーティングの設定に関する制約事項

- 直接接続されたマルチキャスト（IGMP）レシーバおよび送信元だけが、レイヤ 2 アクセス ドメインで許可されます。アクセス ドメインでは、PIM プロトコルはサポートされません。
- PIM スタブルーティングを使用するネットワークでは、ユーザに対する IP トラフィックの唯一の許容ルートは、PIM スタブルーティングを設定しているデバイス経由です。
- 冗長 PIM スタブ ルータ トポロジーはサポートされません。PIM スタブ機能では、非冗長アクセス ルータ トポロジーだけがサポートされます。

Auto-RP および BSR の設定に関する制約事項

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

Auto-RP の制約事項

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

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

BSR 設定の制約事項

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

- 候補 BSR を自動 RP 用の RP マッピング エージェントとして設定します。
- グループ プレフィックスが自動 RP によってアドバタイズされた場合は、異なる RP セットによって処理されたこれらのグループ プレフィックスのサブ範囲が、PIMv2 BSR メカニズムによってアドバタイズされないようにする必要があります。PIMv1 および PIMv2

ドメインが混在する環境では、バックアップ RP で同じグループ プレフィックスが処理されるように設定します。このようにすると、RP マッピング データベースの最長一致検索によって、PIMv2 DR はこれらの PIMv1 DR から異なる RP を選択できなくなります。

Auto-RP および BSR の注意事項と制限事項

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

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

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

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

Auto-RP 拡張の制約事項

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

PIM に関する情報

Protocol Independent Multicast の概要

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

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

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

PIM のバージョン

PIMv2 は、PIMv1 と比べて次の点が改善されています。

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

Multicast Source Discovery Protocol（MSDP）

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

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

PIM スパース モード（PIM-SM）

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

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

PIM-SM は、共有ツリー上のデータ パケットを転送することによって、アクティブな送信元に関する情報を配布します。PIM-SM は少なくとも最初は共有ツリーを使用するので、ランデブー ポイント（RP）を使用する必要があります。RP は管理上メットワークで設定されている必要があります。詳細については、ランデブー ポイント （11 ページ）を参照してください。

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

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

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

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

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

双方向 PIM

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

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

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

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

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

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

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

図 *1:* 単方向共有ツリーおよびソース ツリー

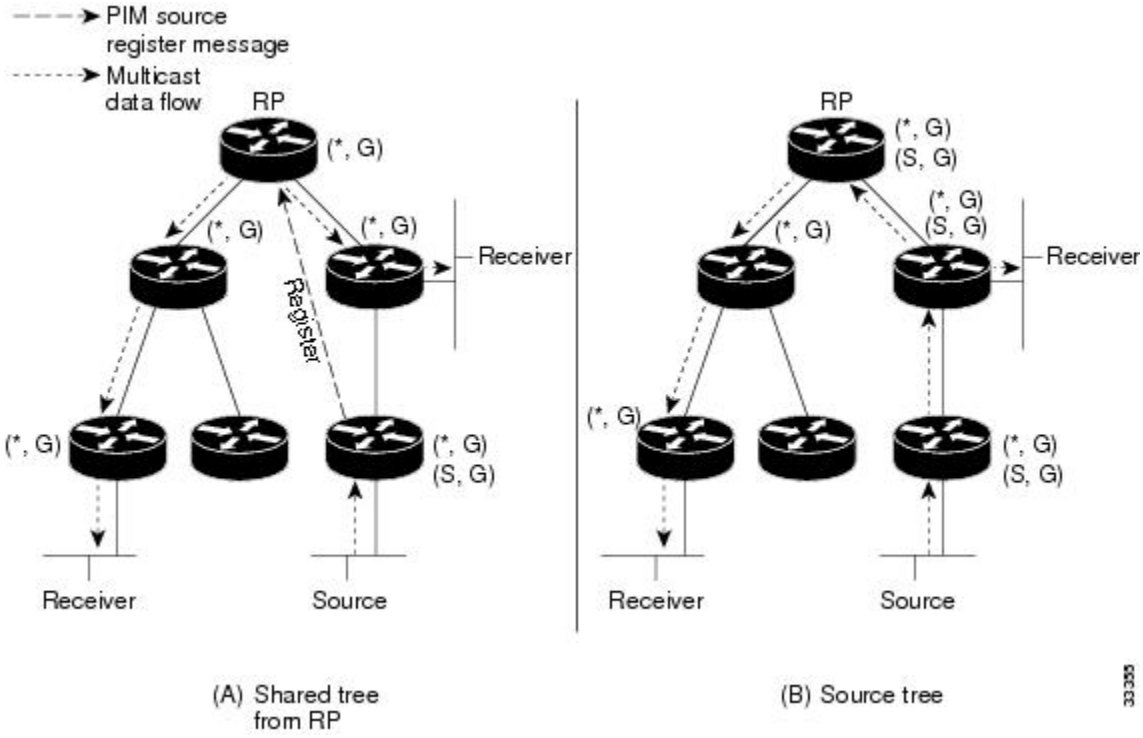
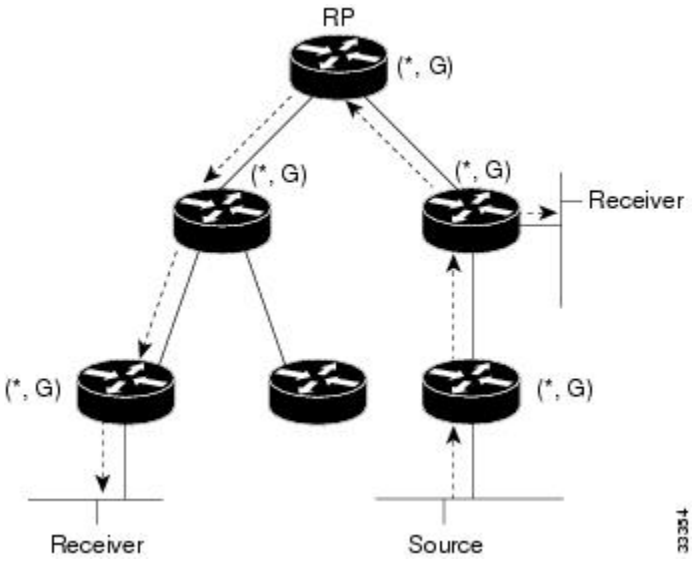


図 *2:* 双方向共有ツリー



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

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

指定フォワーダ選択

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

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

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

双方向グループ ツリー ビルディング

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

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

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

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

パケット転送

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

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

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

IPv4 双方向 PIM

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

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

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

PIM スタブ ルーティング

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

PIM スタブ ルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャストルーティングをサポートします。サポート対象の PIM インターフェイスは、アップリンク PIM インターフェイスと PIM パッシブ インターフェイスの 2 種類です。PIM パッシブ モードに設定されているルーテッド インターフェイスは、PIM 制御トラフィックの通過も転送も行いません。通過させたり転送したりするのは IGMP トラフィックだけです。

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

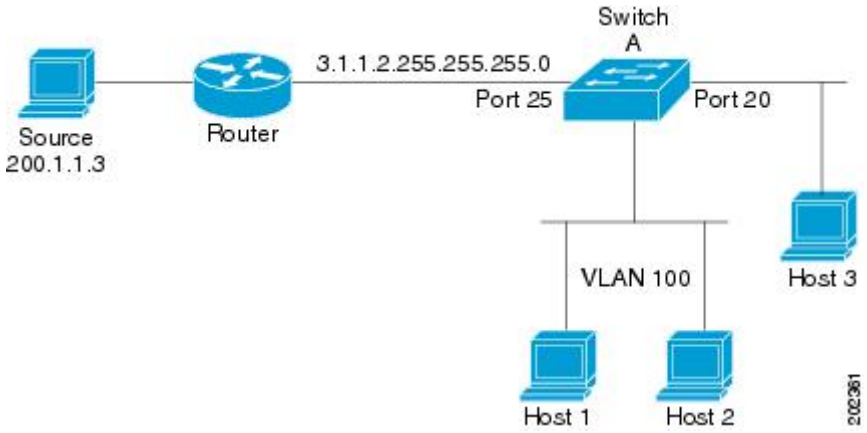
PIM スタブルーティングを使用しているときは、IP マルチキャストルーティングを使用し、デバイスだけを PIM スタブルータとして設定するように、分散ルータおよびリモートルータを設定する必要があります。デバイスは分散ルータ間の伝送トラフィックをルーティングしません。デバイスのルーテッド アップリンク ポートも設定する必要があります。SVI の場合は、デバイスのアップリンクポートを使用できません。SVI アップリンク ポートの PIM が必要な場合は、Network Advantage ライセンスにアップグレードする必要があります。

（注） また、デバイスで PIM スタブルーティングを設定するときは、EIGRP スタブルーティングも設定する必要があります。

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

図 *3 : PIM* スタブ ルータ設定

次の図では、デバイス A のルーテッド アップリンク ポート 25 がルータに接続され、PIM スタブ ルーティングが VLAN 100 インターフェイスとホスト 3 で有効になっています。この設定により、直接接続されたホストはマルチキャスト発信元 200.1.1.3 からトラフィックを受信できます。



ランデブー ポイント

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

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

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

Auto-RP

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

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

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

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

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

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

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

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

PIM ネットワークでの Auto-RP の役割

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

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

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

マルチキャスト境界

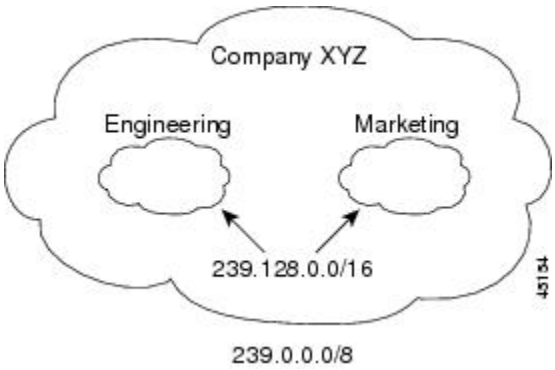
管理用スコープの境界を使用し、ドメインまたはサブドメイン外部へのマルチキャスト トラフィックの転送を制限できます。この方法では、「管理用スコープのアドレス」と呼ばれる特殊なマルチキャストアドレス範囲が境界のメカニズムとして使用されます。管理用スコープの境界をルーテッド インターフェイスに設定すると、マルチキャスト グループ アドレスがこの範囲内にあるマルチキャスト トラフィックは、このインターフェイスに出入りできず、このアドレス範囲内のマルチキャスト トラフィックに対するファイアウォール機能が提供されます。

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

図 *4：* 管理用スコープの境界

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

それぞれのネットワークに入ったり、外部に出ることができません。



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

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

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

Auto-RP のスパース - デンス モード

Auto-RP の前提条件として、**ip pim sparse-dense-mode** インターフェイス コンフィギュレーション コマンドを使用してすべてのインターフェイスをスパース-デンスモードで設定する必要があります。スパース-デンス モードで設定されたインターフェイスは、マルチキャスト グループの動作モードに応じてスパース モードまたはデンス モードで処理されます。マルチキャスト グループ内に既知の RP が存在する場合、インターフェイスはスパース モードで処理されます。グループ内に既知の RP が存在しない場合、デフォルトでは、インターフェイスはデンス モードで処理され、このインターフェイス上にデータがフラッディングされます（デンス モード フォールバックを回避することもできます。「Configuring Basic IP Multicast」モジュールを参照してください）。

Auto-RP を正常に実装し、224.0.1.39 および 224.0.1.40 以外のグループがデンス モードで動作することを回避するには、「シンク RP」（「ラスト リゾート RP」とも呼ばれます）を設定することを推奨します。シンク RP は、ネットワーク内に実際に存在するかどうかわからない静的に設定された RP です。デフォルトでは、Auto-RP メッセージはスタティック RP 設定よりも優先されるため、シンク RP の設定は Auto-RP の動作と干渉しません。未知のソースや予期し

ないソースをアクティブにできるため、ネットワーク内の可能なすべてのマルチキャスト グループにシンク RP を設定することを推奨します。ソースの登録を制限するように設定された RP がない場合は、グループがデンス モードに戻り、データがフラッディングされる可能性があります。

Auto-RP のメリット

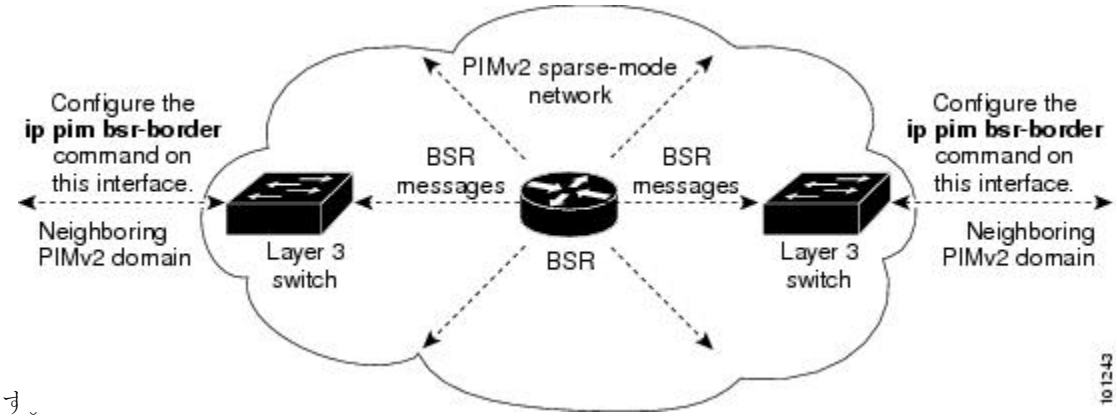
PIM ネットワークでの Auto-RP の利点

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

PIM ドメイン境界

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

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



PIMv2 ブートストラップ ルータ

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

BSR は、BSR として機能するように設定されたドメイン内の一連の候補ルータおよびスイッチから選択されます。選択メカニズムは、ブリッジングされた LAN で使用されるルートブリッジ選択メカニズムと類似しています。BSR の選択メカニズムの基準は、ネットワークを経由し

てホップ単位で送信される BSR メッセージに格納されている、デバイスの BSR プライオリティです。各 BSR デバイスは BSR メッセージを調べ、自身の BSR プライオリティよりも BSR プライオリティが同等以上で、BSR IP アドレスが大きなメッセージだけを、すべてのインターフェイスから転送します。この方法によって、BSR が選択されます。

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

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

マルチキャスト転送

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

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

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

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

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

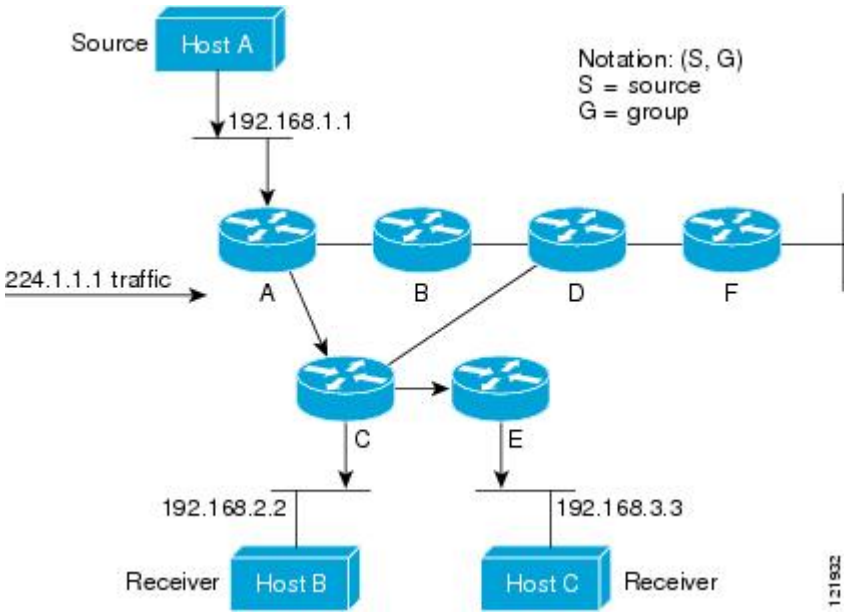
共有ツリーは (*, G) で表されます。ソース ツリーは (S, G) で表され、常にソースでルーティングされます。

マルチキャスト配信のソース ツリー

マルチキャスト配信ツリーの最も単純な形式は、ソース ツリーです。ソース ツリーは、ソース ホストをルートとし、ネットワークを介してレシーバに接続するスパニングツリーを形成す

るブランチを持ちます。このツリーはネットワーク上での最短パスを使用するため、最短パスツリー（SPT）とも呼ばれます。

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



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

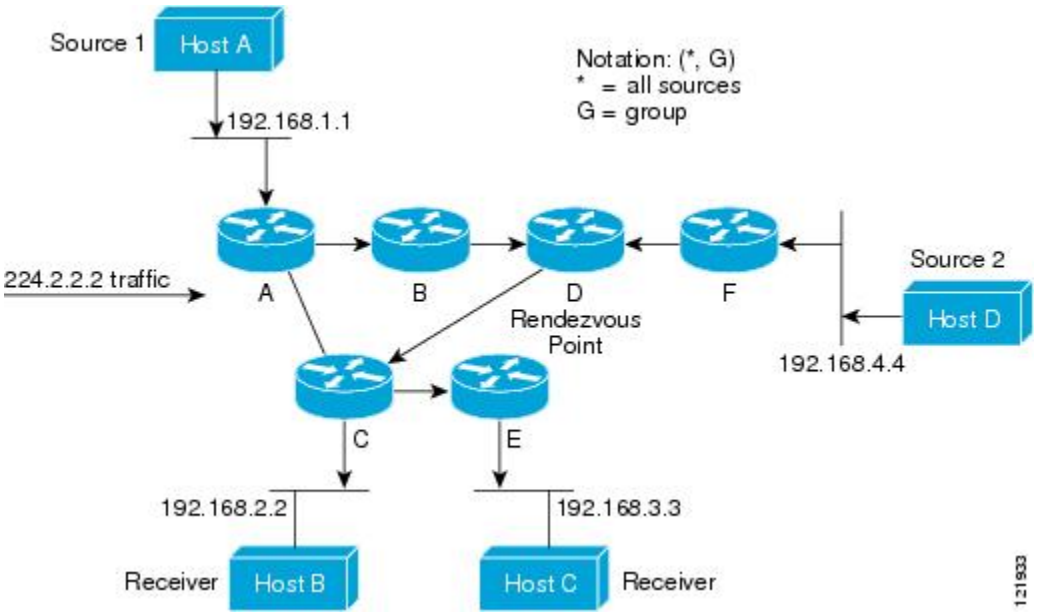
(S, G) という表記は、各グループに送信する個々のソースに個別の SPT が存在することを意味します。

マルチキャスト配信の共有ツリー

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

次の図に、ルータ D にルートが配置されたグループ 224.2.2.2 の共有ツリーを示します。この共有ツリーは単方向です。ソーストラフィックは、ソースツリー上の RP に向けて送信されます。このトラフィックは、次に RP から共有ツリーを下方向に転送され、すべてのレシーバに到達します（レシーバがソースと RP の間に配置されていない場合は、直接サービスが提供されます）。

図 *5:* 共有ツリー



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

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

ソース ツリーの利点

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

共有ツリーの利点

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

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

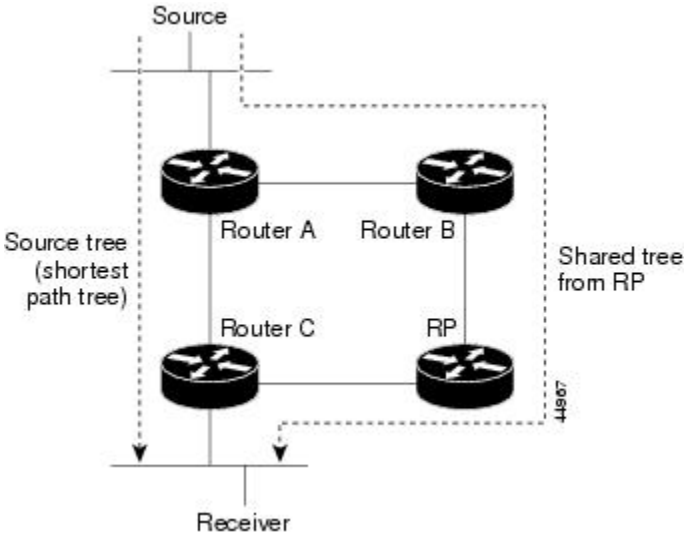
マルチキャスト転送では、ソースは、マルチキャスト グループ アドレスによって表される任意のホスト グループにトラフィックを送信します。マルチキャスト ルータは、どの方向が（ソースへ向かう）アップストリーム方向で、どの方向（1方向または複数の方向）が（レシーバへ向かう）ダウンストリーム方向であるかを決定する必要があります。複数のダウンストリームパスがある場合、ルータはパケットを複製し、それを適切なダウンストリームパス（最善のユニキャスト ルート メトリック）で下方向に転送します。これらのパスがすべてであるとは限りません。レシーバの方向ではなく、ソースから遠ざかる方向へのマルチキャスト トラフィッ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

PIM 共有ツリーおよびソース ツリー

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

図 *6:* 共有ツリーおよびソース ツリー（最短パスツリー）

次の図に、このタイプの共有配信ツリーを示します。送信側からのデータは、RP に配信され、その共有ツリーに加入しているグループ メンバに配布されます。



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

共有ツリーから送信元ツリーへの移動プロセスは、次のとおりです。

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

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

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

最初のデータ パケットがラスト ホップ ルータに着信すると、共有ツリーからソース ツリーへと変更されます。この変更は、**ip pim spt-threshold** グローバル コンフィギュレーション コマンドを使用して設定したしきい値によって異なります。

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

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

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

Reverse Path Forwarding

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

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

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

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

RPF チェック

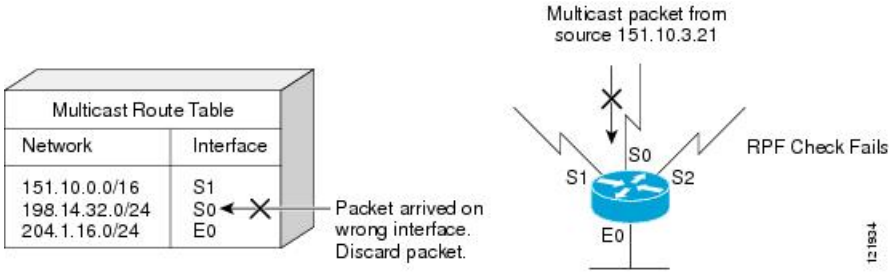
マルチキャスト パケットがルータに到達すると、ルータはそのパケットに対して RPF チェックを実行します。RPFチェックが成功すると、パケットが転送されます。そうでない場合、パケットはドロップされます。

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

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

図に、RPF チェックの失敗例を示します。

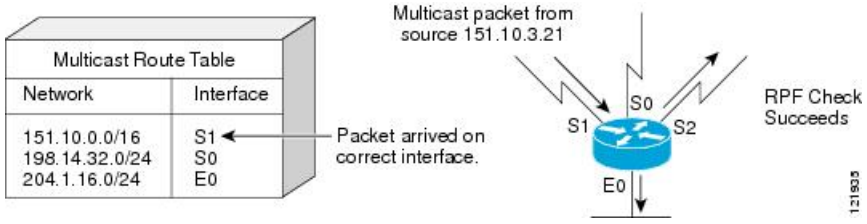
図 *7: RPF* チェックの失敗



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

図に RPF チェックの成功例を示します。

図 *8 : RPF* チェックの成功



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

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

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

（注） このスイッチでは DVMRP はサポートされません。

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

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

PIM ルーティングのデフォルト設定

デバイス用の PIM ルーティングのデフォルト設定を次の表に示します。

表 *1 :* 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

機能	デフォルト設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル
PIM マルチキャスト境界	なし
候補 BSR	ディセーブル
候補 RP	ディセーブル
SPT しきい値レート	0 kb/s
PIM ルータ クエリー メッセージ インターバル	30 秒

PIM の設定方法

PIM スタブ ルーティングのイネーブル化

この手順は任意です。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	PIM スタブ ルーティングをイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定するインターフェイスは、次のいずれかである必要があります。これらのインターフェイスには、IP アドレスが割り当てられている必要があります。 • ルーテッドポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。
ステップ 4	**ip pim passive** 例： `Device(config-if)# ip pim passive`	インターフェイスに PIM スタブ機能を設定します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ip pim interface** 例： `Device# show ip pim interface`	（任意）各インターフェイスで有効になっている PIM スタブを表示します。
ステップ 7	**show ip igmp groups detail** 例： `Device# show ip igmp groups detail`	（任意）特定のマルチキャスト送信元グループに参加した対象クライアントを表示します。

	コマンドまたはアクション	目的
ステップ 8	**show ip mroute** 例： `Device# show ip mroute`	（任意）IP マルチキャスト ルーティング テーブルを表示します。
ステップ 9	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

ランデブー ポイントの設定

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

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

（注） 動作中の PIM バージョン、およびネットワーク内のルータ タイプに応じて、自動 RP、BSR、またはこれらを組み合わせて使用できます。ネットワーク内の異なるバージョンの PIM を利用する方法については、PIMv1 および PIMv2 の相互運用性 （2 ページ）を参照してください。

マルチキャスト グループへの RP の手動割り当て

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

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

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

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

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip pim rp-address** *ip-address* [*access-list-number*] [**override**]
4. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim rp-address** *ip-address* [*access-list-number*] [**override**] 例： `Device(config)# ip pim rp-address 10.1.1.1 20 override`	PIM RP のアドレスを設定します。 デフォルトで、PIM RP アドレスは設定されていません。すべてのルータおよびマルチレイヤスイッチ（RP を含む）で、RP の IP アドレスを設定する必要があります。 （注） グループに RP が設定されていない場合、デバイスは PIM DM 技術を使用し、グループをデンスとして処理します。 1 台の PIM デバイスを、複数のグループの RP にできます。1 つの PIM ドメイン内で一度に使用できる

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

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

新規ネットワークでの Auto-RP の設定

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

手順の概要

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **ip pim send-rp-announce** *interface-id* **scope** *ttl* **group-list** *access-list-number* **interval** *seconds*
5. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
6. **ip pim send-rp-discovery scope** *ttl*
7. **end**
8. **show running-config**
9. **show ip pim rp mapping**
10. **show ip pim rp**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show running-config** 例：	すべての PIM デバイス上でデフォルトの RP が設定されていること、および RP が SM ネットワーク内

	コマンドまたはアクション	目的
	`Device# show running-config`	にあることを確認します。RP は、**ip pim rp-address** グローバル コンフィギュレーション コマンドによって設定済みです。 （注） SM-DM 環境の場合、このステップは不要です。 選択された RP は接続が良好で、ネットワークで使用可能となる必要があります。この RP は、グローバル グループ（224.x.x.x やその他のグローバル グループなど）に対して使用されます。この RP で処理されるグループ アドレス範囲は再設定しないでください。自動 RP によって動的に検出された RP は、静的に設定された RP よりも優先されます。ローカル グループ用に 2 番めの RP を使用することもできます。
ステップ 3	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**ip pim send-rp-announce** *interface-id* **scope** *ttl* **group-list** *access-list-number* **interval** *seconds* 例： `Device(config)# ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120`	別の PIM デバイスをローカル グループの候補 RP として設定します。 • *interface-id* には、RP アドレスを識別するインターフェイス タイプおよび番号を入力します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • **scope** *ttl* には、ホップの存続可能時間の値を指定します。RP アナウンス メッセージがネットワーク内のすべてのマッピング エージェントに到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。指定できる範囲は 1 ～ 255 です。 • **group-list** *access-list-number* には、1 ～ 99 の範囲で標準の IP アクセスリスト番号を入力します。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。 • **interval** *seconds* には、アナウンスメントメッセージを送信する頻度を指定します。デフォルトは 60 秒です。指定できる範囲は 1 ～ 16383 です。

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

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

既存の SM クラウドへの Auto-RP の追加

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

この手順は任意です。

手順の概要

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **ip pim send-rp-announce** *interface-id* **scope** *ttl* **group-list** *access-list-number* **interval** *seconds*
5. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
6. **ip pim send-rp-discovery scope** *ttl*
7. **end**
8. **show running-config**
9. **show ip pim rp mapping**
10. **show ip pim rp**
11. **copy running-config startup-config**

手順の詳細

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

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

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

問題のある RP への Join メッセージの送信禁止

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

着信 RP アナウンスメント メッセージのフィルタリング

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

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip pim rp-announce-filter rp-list** *access-list-number* **group-list** *access-list-number*
4. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim rp-announce-filter rp-list** *access-list-number* **group-list** *access-list-number* 例： `Device(config)# ip pim rp-announce-filter rp-list 10 group-list 14`	着信 RP アナウンスメント メッセージをフィルタリングします。 ネットワーク内のマッピングエージェントごとに、このコマンドを入力します。このコマンドを使用しないと、すべての着信 RP アナウンスメント メッセージがデフォルトで許可されます。 **rp-list** *access-list-number* には、候補 RP アドレスのアクセスリストを設定します。アクセスリストが許可されている場合は、**group-list** *access-list-number* 変数で指定されたグループ範囲に対してアクセスリストを使用できます。この変数を省略すると、すべてのマルチキャスト グループにフィルタが適用されます。 複数のマッピングエージェントを使用する場合は、グループ/RP マッピング情報に矛盾が生じないようにするため、すべてのマッピングエージェント間でフィルタを統一する必要があります。

	コマンドまたはアクション	目的
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 10 permit 10.8.1.0 255.255.224.0`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 • **permit** キーワードは、条件が一致した場合にアクセスを許可します。 • どのルータおよびマルチレイヤ スイッチからの候補 RP アナウンスメント（rp-list アクセス コントロール リスト（ACL））がマッピング エージェントによって許可されるかを指定するアクセス リストを作成します。 • 許可または拒否するマルチキャスト グループの範囲を指定するアクセス リスト（グループリスト ACL）を作成します。 • *source* には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 •（任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例：	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`Device# copy running-config startup-config`	

PIMv2 BSR の設定

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

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

PIM ドメイン境界の定義

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

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip pim bsr-border**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッドポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip pim bsr-border** 例： `Device(config-if)# ip pim bsr-border`	PIM ドメイン用の PIM ブートストラップ メッセージ境界を定義します。 境界に位置する他の PIM ドメインに接続されているインターフェイスごとに、このコマンドを入力します。このコマンドを実行すると、デバイスは、このインターフェイス上で PIMv2 BSR メッセージを送受信しないように指示されます。 （注） PIM 境界を削除するには、 **no ip pim bsr-border** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例：	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	`Device# copy running-config startup-config`	

IP マルチキャスト境界の定義

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

この手順は任意です。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**access-list** *access-list-number* **deny** *source* [*source-wildcard*]
	例：
	`Device(config)#`
	`access-list 12 deny 224.0.1.39`
	`access-list 12 deny 224.0.1.40`
		標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。
		• *access-list-number* の範囲は 1 ～ 99 です。
		• **deny** キーワードは、条件が一致した場合にアクセスを拒否します。

	コマンドまたはアクション	目的
		• *source* には、自動RP情報を伝達するマルチキャスト アドレス 224.0.1.39 および 224.0.1.40 を入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッドポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 5	**ip multicast boundary** *access-list-number* 例： `Device(config-if)# ip multicast boundary 12`	ステップ 2 で作成したアクセス リストを指定し、境界を設定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

候補 BSR の設定

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

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip pim bsr-candidate** *interface-id hash-mask-length* [*priority*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim bsr-candidate** *interface-id hash-mask-length* [*priority*] 例： `Device(config)# ip pim bsr-candidate gigabitethernet 1/0/3 28 100`	候補 BSR となるようにデバイスを設定します。 • *interface-id* には、デバイスを候補 BSR に設定するときに BSR アドレスの取得元となる 上のインターフェイスを入力します。このインターフェイスは PIM を使用してイネーブルにする必要があります。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。

	コマンドまたはアクション	目的
		• *hash-mask-length* には、ハッシュ機能を呼び出す前にグループ アドレスとの AND 条件となるマスク長（最大 32 ビット）を指定します。ハッシュ元が同じであるすべてのグループは、同じ RP に対応します。たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。 • （任意）*priority* を指定する場合は、0 ～ 255 の番号を入力します。プライオリティが大きな BSR が優先されます。このプライオリティ値が同じである場合は、大きな IP アドレスを持つデバイスが BSR として選択されます。デフォルトは 0 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

候補 RP の設定

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

この手順は任意です。

始める前に

RP となるデバイスを決定するときは、次の可能性を考慮してください。

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

手順の概要

1. **enable**
2. **configure terminal**
3. **ip pim rp-candidate** *interface-id* [**group-list** *access-list-number*]
4. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim rp-candidate** *interface-id* [**group-list** *access-list-number*] 例： `Device(config)# ip pim rp-candidate gigabitethernet 1/0/5 group-list 10`	候補 RP となるようにデバイスを設定します。 • *interface-id* には、対応する IP アドレスが候補 RP アドレスとしてアドバタイズされるインターフェイスを指定します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • （任意）**group-list** *access-list-number* を指定する場合は、1 ～ 99 の IP 標準アクセス リスト番号を入力します。group-list を指定しない場合は、このデバイスがすべてのグループの候補 RP となります。

	コマンドまたはアクション	目的
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Device(config)# access-list 10 permit 239.0.0.0 0.255.255.255`	標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、パケットの送信元であるネットワークまたはホストの番号を入力します。 •（任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

Auto-RP によるスパース モードの設定

始める前に

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

（注）

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip multicast-routing** 例： `Device(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。
ステップ 4	ステップ 5 ～ 7 を実行するか、またはステップ 6 および 8 を実行します。	--
ステップ 5	**interface** *type number* 例： `Device(config)# interface Gigabitethernet 1/0/0`	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 6	**ip pim sparse-mode** 例： `Device(config-if)# ip pim sparse-mode`	インターフェイスで PIM スパース モードをイネーブルにします。スパース モードで Auto-RP を設定している場合、次のステップで Auto-RP リスナーも設定する必要があります。 • ステップ 8 でスパース-デンス モードを設定している場合、このステップはスキップします。
ステップ 7	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 8	すべての PIM インターフェイス上でステップ 1 ～ 9 を繰り返します。	--
ステップ 9	**ip pim send-rp-announce** {*interface-type interface-number* | *ip-address*} **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] 例：	RP アナウンスメントをすべての PIM 対応インターフェイスに送信します。 • RPデバイスでのみこのステップを実行します。

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

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

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

IPv4 双方向 PIM の設定

ここでは、双方向 PIM の設定について説明します。

IPv4 双方向 PIM のグローバルなイネーブル化

IPv4 双方向 PIM をイネーブルにするには、次の作業を行います。

始める前に

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip pim bidir-enable** 例： `Device(config)# ip pim bidir-enable`	デバイスで IPv4 双方向 PIM をグローバルにイネーブルにします。

IPv4 双方向 PIM グループのランデブー ポイントの設定

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

始める前に

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

手順の概要

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

手順の詳細

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

PIM 最短パス ツリーの使用の延期

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

この手順は任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]
4. **ip pim spt-threshold** {*kbps* | **infinity**} [**group-list** *access-list-number*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
		• （任意）**group-list** *access-list-number* には、ステップ 2 で作成したアクセスリストを指定します。値 0 を指定する場合、またはグループ リストを使用しない場合、しきい値はすべてのグループに適用されます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM ルータクエリー メッセージ間隔の変更

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

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

この手順は任意です。

手順の概要

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

5. **end**
6. **show ip igmp interface** [*interface-id*]
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッドポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip pim query-interval** *seconds* 例： `Device(config-if)# ip pim query-interval 45`	デバイスが PIM ルータクエリ メッセージを送信する頻度を設定します。 デフォルトは 30 秒です。指定できる範囲は 1 ～ 65535 です。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM の動作の確認

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

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

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

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

ファースト ホップ ルータでの IP マルチキャストの確認

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

手順の概要

1. **enable**

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

ステップ 2	**show ip mroute** [*group-address*]
	例：
	`Device# show ip mroute 239.1.2.3`
	`(*, 239.1.2.3), 00:18:10/stopped, RP 172.16.0.1, flags: SPF`
	`Incoming interface: Serial1/0, RPF nbr 172.31.200.2`
	`Outgoing interface list: Null`
	`(10.0.0.1, 239.1.2.3), 00:18:10/00:03:22, flags: FT`
	`Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0`
	`Outgoing interface list:`
	`Serial1/0, Forward/Sparse, 00:18:10/00:03:19`
		ファースト ホップ ルータの mroute に F フラグが設定されていることを確認します。

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

SPT 上のルータでの IP マルチキャストの確認

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

ステップ 2	**show ip mroute** [*group-address*]
	例：
	`Device# show ip mroute 239.1.2.3`
	`(*, 239.1.2.3), 00:17:56/00:03:02, RP 172.16.0.1, flags: S`
	`Incoming interface: Null, RPF nbr 0.0.0.0`
	`Outgoing interface list:`
	`GigabitEthernet0/0/0, Forward/Sparse, 00:17:56/00:03:02`
	`(10.0.0.1, 239.1.2.3), 00:15:34/00:03:28, flags: T`
	`Incoming interface: Serial1/0, RPF nbr 172.31.200.1`
	`Outgoing interface list:`
	`GigabitEthernet0/0/0, Forward/Sparse, 00:15:34/00:03:02`
		特定のグループの送信元に対する RPF ネイバーを確認します。

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

	コマンドまたはアクション	目的

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

ラスト ホップ ルータでの IP マルチキャスト動作の確認

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的

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

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

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

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

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

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

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

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

PIM 対応ルータを使用した IP マルチキャストの到達可能性のテスト

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

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

マルチキャスト ping に応答するルータの設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/0`	インターフェイス コンフィギュレーション モードを開始します。 *type* 引数および *number* 引数には、ホストに直接接続されているインターフェイス、またはホストに対応しているインターフェイスを指定します。
ステップ 4	**ip igmp join-group** *group-address* 例： `Device(config-if)# ip igmp join-group 225.2.2.2`	（任意）指定したグループに加入するようにルータ上のインターフェイスを設定します。 この作業の目的として、マルチキャスト ネットワークに加入しているルータ上のすべてのインターフェイス上で、*group-address* 引数に同じグループ アドレスを設定します。 （注） この方法では、ルータは、マルチキャスト パケットの転送に加えて、マルチキャスト パケットを受信します。マルチキャスト パケットを受信することにより、ルータの高速スイッチングは行われません。
ステップ 5	マルチキャスト ネットワークに加入しているルータ上のインターフェイスで、ステップ 3 とステップ 4 を繰り返します。	--
ステップ 6	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。

マルチキャスト ping に応答するように設定されたルータへの ping

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**ping** *group-address* 例： `Device# ping 225.2.2.2`	IP マルチキャスト グループ アドレスを ping します。 正常な応答は、グループ アドレスが機能していることを示します。

PIM のモニタリングとトラブルシューティング

PIM 情報のモニタリング

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

表 *2 : PIM* モニタリング コマンド

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

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

RP マッピングおよび BSR 情報のモニタリング

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

表 *3 : RP* マッピングのモニタリング コマンド

コマンド	目的
show ip pim rp [*hostname* または *IP address* | **mapping** [*hostname* または *IP address* | **elected** | **in-use**] | **metric** [*hostname* または *IP address*]]	使用可能なすべての RP マッピングおよびメトリックを表示します。これにより、（BSR または Auto-RP メカニズムを通じて）デバイスがどのように RP を学習するかがわかります。 • （任意）*hostname* を指定する場合は、RP を表示するグループの IP 名を指定します。 • （任意）*IP address* を指定する場合は、RP を表示するグループの IP アドレスを指定します。 • （任意）シスコ デバイスによって認識されている（設定されている、または Auto-RP によって取得されている）すべてのグループ/RP マッピングを表示するには、**mapping** キーワードを使用します。 • （任意）**metric** キーワードを使用して、RP RPF メトリックを表示します。

コマンド	目的
show ip pim rp-hash *group*	指定したグループに選択されている RP を表示します。つまり、PIMv2 ルータまたはマルチレイヤスイッチ上で、PIMv1 システムで選択されている RP と同じ RP が使用されていることを確認します。*group* には、RP 情報を表示するグループ アドレスを入力します。

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

表 *4 : VTP* モニタリング コマンド

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

PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング

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

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

IPv4 双方向 PIM 情報のモニタリング

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

コマンド	目的
show ip mfib	双方向 PIM の MFIB 情報を表示します。
show platform software fed {**active** | **standby** } **ip multicast groups**	プラットフォーム依存 IP マルチキャスト テーブルおよびその他の情報を表示します。
show ip pim [**vrf** *vrf-name*] **interface** *interface-type interface-number* **df** [*rp-address*]	PIM に対して設定されたインターフェイスに関する情報を表示します。
show ip pim [**vrf** *vrf-name*] **rp** [**mapping** | **metric**] [*rp-address*]	関連マルチキャスト ルーティング エントリとともにキャッシュされているアクティブ ランデブー ポイントを表示します。

コマンド	目的
show platform software fed ip multicast df ［**vrf-id** *vrf-id*	**vrf-name** *vrf-name*］［*df-index*］	IPマルチキャスト指定フォワーダ（DF）に関する情報を表示します。

PIM の設定例

例：PIM スタブ ルーティングのイネーブル化

次の例では、IP マルチキャスト ルーティングがイネーブルになっており、スイッチ A の PIM アップリンク ポート 25 はルーテッド アップリンク ポートとして設定されています（**spare-dense-mode** がイネーブル）。VLAN 100 インターフェイスとギガビット イーサネット ポート 20 で PIM スタブ ルーティングがイネーブルに設定されています。

```
Device(config)# ip multicast-routing
Device(config)# interface GigabitEthernet3/0/25
Device(config-if)# no switchport
Device(config-if)# ip address 3.1.1.2 255.255.255.0
Device(config-if)# ip pim sparse-dense-mode
Device(config-if)# exit
Device(config)# interface vlan100
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface GigabitEthernet3/0/20
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface vlan100
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface GigabitEthernet3/0/20
Device(config-if)# no switchport
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# ip pim passive
Device(config-if)# end
```

例：PIM スタブ ルーティングの確認

各インターフェイスの PIM スタブがイネーブルになっていることを確認するには、**show ip pim interfac** 特権 EXEC コマンドを使用します。

```
デバイス# show ip pim interface
Address Interface Ver/ Nbr Query DR DR
Mode Count Intvl Prior
3.1.1.2 GigabitEthernet3/0/25 v2/SD 1 30 1 3.1.1.2
100.1.1.1 Vlan100 v2/P 0 30 1 100.1.1.1
10.1.1.1 GigabitEthernet3/0/20 v2/P 0 30 1 10.1.1.1
```

例：マルチキャスト グループへの RP の手動割り当て

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

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

例：Auto-RP の設定

次に、最大ホップ数が 31 であるすべての PIM 対応インターフェイスから RP アナウンスメントを送信する例を示します。ポート 1 の IP アドレスが RP です。アクセス リスト 5 には、この deviceが RP として機能するグループが記述されています。

```
デバイス(config)# ip pim send-rp-announce gigabitethernet1/0/1 scope 31 group-list 5
デバイス(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```

例：Auto-RP でのスパース モード

次の例では、Auto-RP でスパース モードを設定しています。

```
ip multicast-routing
ip pim autorp listener
ip pim send-rp-announce Loopback0 scope 16 group-list 1
ip pim send-rp-discovery Loopback1 scope 16
no ip pim dm-fallback
access-list 1 permit 239.254.2.0 0.0.0.255
access-list 1 permit 239.254.3.0 0.0.0.255
.
.
.
access-list 10 permit 224.0.1.39
access-list 10 permit 224.0.1.40
access-list 10 permit 239.254.2.0 0.0.0.255
access-list 10 permit 239.254.3.0 0.0.0.255
```

例：Auto-RP 情報を拒否する IP マルチキャスト境界の定義

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

```
デバイス(config)# access-list 1 deny 224.0.1.39
デバイス(config)# access-list 1 deny 224.0.1.40
デバイス(config)# access-list 1 permit all
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip multicast boundary 1
```

例：着信 RP アナウンスメント メッセージのフィルタリング

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

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

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

例：問題のある RP への Join メッセージの送信禁止

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

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

例：候補 BSR の設定

次に、候補 BSR の設定例を示します。この例では、アドバタイズ済み BSR アドレスとしてポートの IP アドレス 172.21.24.18 を、hash-mask-length として 30 ビットを使用します。プライオリティは 10 です。

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

例：候補 RP の設定

次に、device が自身を候補 RP として PIM ドメイン内の BSR にアドバタイズするよう設定する例を示します。標準アクセス リスト番号 4 により、ポートで識別されるアドレスを持つ RP に対応するグループ プレフィックスが指定されます。この RP は、プレフィックスが 239 であるグループを処理します。

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