



## PIM の設定

---

- 機能情報の確認, 1 ページ
- PIM の前提条件, 2 ページ
- PIM に関する制約事項, 2 ページ
- PIM に関する情報, 6 ページ
- PIM の設定方法, 25 ページ
- PIM の動作の確認, 62 ページ
- PIM のモニタリングとトラブルシューティング, 71 ページ
- PIM の設定例, 74 ページ
- その他の参考資料, 78 ページ
- PIM の機能履歴と情報, 80 ページ

## 機能情報の確認

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

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

## 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せん。
  - 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。
  - スタブルルータと中央のルータの両方に IP マルチキャストルーティングが設定されている必要があります。さらに、スタブルルータのアップリンク インターフェイスに PIM モード（デンス モード、スパース モード、または スパース-デンス モード）が設定されている必要があります。
  - また、デバイスに Enhanced Interior Gateway Routing Protocol (EIGRP) スタブルルーティングか Open Shortest Path First (OSPF) スタブルルーティングのいずれかが設定されている必要があります。
  - PIM スタブルルータは、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) スタブルルーティングではこの動作が強制されます。PIM スタブルルータの動作を支援するためにユニキャスト スタブルルーティングを設定する必要があります。



---

(注) EIGRP または OSPF の設定については、『*Catalyst 3850 Routing Configuration Guide, Release 3SE*』を参照してください。

---

## 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。

- PIM は、LAN Base フィーチャ セットを実行している場合はサポートされません。
- 双方向 PIM はサポートされていません。

## PIMv1 および PIMv2 の相互運用性

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

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

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

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



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

PIMv2 デバイスを PIMv1 デバイスと相互運用させる場合は、自動 RP を事前に導入しておく必要があります。自動 RP マッピングエージェントでもある PIMv2 BSR は、自動 RP で選択された RP を自動的にアダプタイズします。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デバイスごとに 1 つの RP が設定されます。ドメイン内のルータおよびデバイスの中には、複数の RP を選択するために PIMv2 ハッシュ機能を使用しないものもあります。

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

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

- 領域全体で Auto-RP を使用します。
- 領域全体でスパース - デンス モードを設定します。

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

#### 関連トピック

[PIM のバージョン](#), (9 ページ)

## PIM スタブルルーティングの設定に関する制約事項

- IP Services 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。

- 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 トポロジだけがサポートされます。
- IP Base および IP Services の機能セットを実行している場合は、PIM スタブ ルーティングがサポートされます。

#### 関連トピック

[PIM スタブ ルーティングのイネーブル化 \(CLI\) , \(25 ページ\)](#)

[PIM スタブ ルーティング, \(10 ページ\)](#)

## 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)。

- Auto-RP は、LAN Base フィーチャ セットを実行している場合はサポートされません。
- PIM をスパース モードまたはデンス モードに設定し、Auto-RP を設定しない場合は、RP を手動で設定する必要があります。
- ルーテッドインターフェイスが SM に設定されていると、すべてのデバイスが自動 RP グループの手動 RP アドレスによって設定されている場合も、自動 RP を使用できます。
- ルーテッドインターフェイスが SM で設定され、**ip pim autorp listener** グローバル コンフィギュレーション コマンドを入力する場合、すべてのデバイスが Auto-RP グループの手動 RP アドレスを使用して設定されていなくても、Auto-RP は引き続き使用できます。

#### BSR 設定の制約事項

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

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

### Auto-RP および BSR の注意事項と制限事項

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

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



---

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

---

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

#### 関連トピック

[新規インターネットワークでの Auto-RP の設定 \(CLI\) , \(31 ページ\)](#)

[Auto-RP, \(12 ページ\)](#)

[候補 BSR の設定 \(CLI\) , \(48 ページ\)](#)

[PIMv2 ブートストラップルータ, \(16 ページ\)](#)

## 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。

#### 関連トピック

[新規インターネットワークでの Auto-RP の設定 \(CLI\) , \(31 ページ\)](#)

[Auto-RP, \(12 ページ\)](#)

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

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

### PIM デンス モード (PIM-DM)

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

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

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

ルータは、フラッディングとプルーニングのメカニズムを介してデータ ストリームを受信することでステート情報を累積します。これらのデータ ストリームには送信元およびグループの情報が含まれているため、ダウンストリーム ルータがマルチキャスト転送テーブルを構築できます。PIM-DM ではソース ツリー、つまり (S, G) エントリしかサポートしていないため、共有配信ツリーの構築に使用できません。



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

## PIM スパース モード (PIM-SM)

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

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

PIM-SM は、共有ツリー上のデータ パケットを転送することによって、アクティブな送信元に関する情報を配布します。PIM-SM は少なくとも最初は共有ツリーを使用するので、ランデブー ポイント (RP) を使用する必要があります。RP は管理上ネ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 リンクでフラディングするのを防ぎます。

## Multicast Source Discovery Protocol (MSDP)

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

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

## スパース-デンス モード

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

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

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

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



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

- インターフェイス上にメンバまたは DVMRP ネイバーが存在する。
- PIM ネイバーが存在し、グループがブルーニングされていない。

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

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

## PIM のバージョン

PIMv2 は、PIMv1 と比べて次の点が改善されています。

- マルチキャスト グループごとに、複数のバックアップ ランデブー ポイント (RP) を持つアクティブな RP が 1 つ存在します。この単一の RP で、PIMv1 内の同じグループにアクティブな RP が複数ある場合と同様の処理を行います。
- ブートストラップ ルータ (BSP) は耐障害性のある、自動化された RP ディスカバリ メカニズム、および配信機能を提供します。これらの機能により、ルータおよびマルチレイヤ デバイスはグループ/RP マッピングを動的に取得できます。
- スパースモード (SM) およびデンスモード (DM) は、インターフェイスではなく、グループに関するプロパティです。



---

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

---

- PIM の Join メッセージおよびブルーニング 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。

### 関連トピック

[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](#), (73 ページ)

PIMv1 および PIMv2 の相互運用性, (2 ページ)

## PIM スタブルルーティング

PIM スタブル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 スタブルルーティングとして設定するように、分散ルーティングおよびリモートルーティングを設定する必要があります。デバイスは分散ルーティング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、IP Services 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。



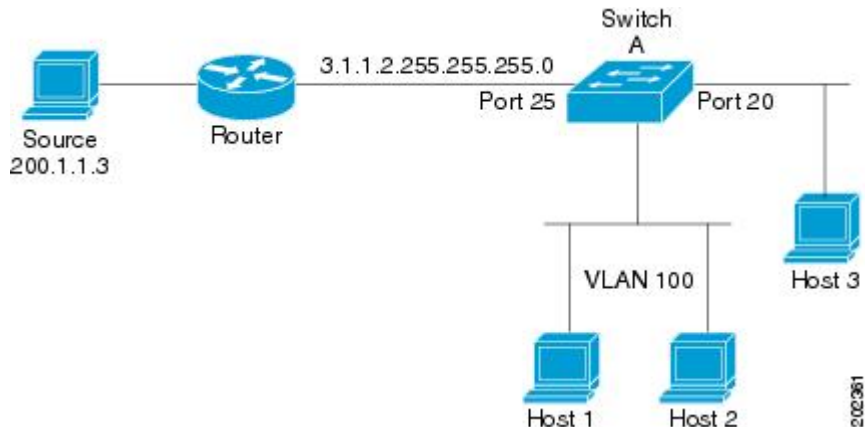
(注) また、PIM スタブルルーティングをデバイスに設定するときは、EIGRP スタブルルーティングも設定する必要があります。

冗長 PIM スタブルルーティング トポロジ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ティング検出メカニズムは、PIM 受動インターフェイスでサポートされません。PIM スタブル機能では、非冗長アクセスルーティング トポロジだけがサポートされます。非冗長 トポロジを使用することで、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ティングであると想定します。

次の図では、デバイス A ルーテッドアップリンク ポート 25 がルーティングに接続され、PIM スタブルルーティングが VLAN 100 インターフェイスとホスト 3 でイネーブルになっています。この設定

により、直接接続されたホストはマルチキャスト発信元 200.1.1.3 からトラフィックを受信できません。

図 1: PIM スタブルータ設定



#### 関連トピック

[PIM スタブルーティングのイネーブル化 \(CLI\) , \(25 ページ\)](#)

[例 : PIM スタブルーティングのイネーブル化, \(74 ページ\)](#)

[例 : PIM スタブルーティングの確認, \(75 ページ\)](#)

[PIM スタブルーティングの設定に関する制約事項, \(3 ページ\)](#)

## IGMP ヘルパー

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

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

## ランデブーポイント

ランデブーポイント (RP) は、デバイスが PIM (Protocol Independent Multicast) スパースモード (SM) で動作している場合にデバイスが実行するロールです。RPが必要になるのは、PIM-SM を実行しているネットワークだけです。PIM-SM モデルでは、マルチキャストデータを明示的に要

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

RP は、マルチキャストデータのソースとレシーバの接点として機能します。PIM-SM 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。

### 関連トピック

[候補 RP の設定 \(CLI\) , \(49 ページ\)](#)

[ランデブーポイントの設定, \(28 ページ\)](#)

[例: 候補 RP の設定, \(78 ページ\)](#)

## Auto-RP

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

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

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

複数の RP を使用して、異なるグループ範囲にサービスを提供したり、互いにバックアップとしての役割を果たしたりできます。Auto-RP が機能するためには、RP 通知メッセージを RP から受信して競合を解決する RP マッピング エージェントとしてルータが指定されている必要があります。その場合、RP マッピング エージェントは、グループから RP への一貫したマッピングを他の

すべてのルータに送信します。これにより、すべてのルータは、サポート対象のグループに使用する RP を自動的に検出します。



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



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

Auto-RP が機能するためには、RP 通知メッセージを RP から受信して競合を解決する RP マッピング エージェントとしてルータが指定されている必要があります。その後、RP マッピング エージェントは、デンス モードフラッドイングにより、グループから RP への一貫したマッピングを他のすべてのルータに送信するようになります。これにより、すべてのルータは、サポート対象のグループに使用する RP を自動的に検出します。インターネット割り当て番号局 (IANA) は、224.0.1.39 と 224.0.1.40 という2つのグループアドレスを Auto-RP 用に割り当てています。Auto-RP の利点の1つは、指定した RP に対するすべての変更は、RP であるルータ上で設定するだけで、リーフルータ上で設定する必要がないことです。Auto-RP のもう1つの利点は、ドメイン内で RP アドレスの範囲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。代替の方法として、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。

#### 関連トピック

[新規インターネットワークでの Auto-RP の設定 \(CLI\) , \(31 ページ\)](#)

[例 : Auto-RP の設定, \(75 ページ\)](#)

[例 : Auto-RP でのスパース モード, \(76 ページ\)](#)

[Auto-RP および BSR の設定に関する制約事項, \(4 ページ\)](#)

[Auto-RP 拡張の制約事項, \(5 ページ\)](#)

## PIM ネットワークでの Auto-RP の役割

Auto-RP は、PIM ネットワークにおけるグループからランデブーポイント (RP) へのマッピングの配信を自動化します。Auto-RP が機能するためには、RP アナウンスメントメッセージを RP から受信して競合を解決する RP マッピング エージェントとしてデバイスが指定されている必要があります。その後、RP マッピング エージェントは、デンス モードフラッドイングにより、一貫した group-to-RP マッピングを他のすべてのデバイスに送信します。

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

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

## マルチキャスト境界

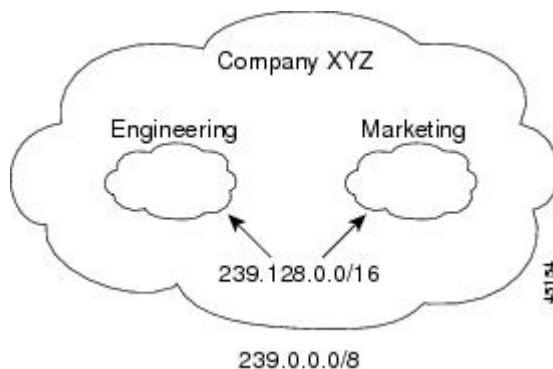
管理用スコープの境界を使用し、ドメインまたはサブドメイン外部へのマルチキャストトラフィックの転送を制限できます。この方法では、「管理用スコープのアドレス」と呼ばれる特殊なマルチキャストアドレス範囲が境界のメカニズムとして使用されます。管理用スコープの境界をルーテッドインターフェイスに設定すると、マルチキャストグループアドレスがこの範囲内にあるマルチキャストトラフィックは、このインターフェイスに出入りできず、このアドレス範囲内のマルチキャストトラフィックに対するファイアウォール機能が提供されます。



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

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

図 2：管理用スコープの境界



マルチキャスト グループ アドレスに対して、ルーテッド インターフェイス上に管理用スコープの境界を定義できます。影響を受けるアドレス範囲は、標準アクセスリストによって定義されません。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見なされます。

**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。

#### 関連トピック

[IP マルチキャスト境界の定義 \(CLI\) , \(45 ページ\)](#)

[例 : Auto-RP 情報を拒否する IP マルチキャスト境界の定義, \(76 ページ\)](#)

## 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ドされます (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 がいない場合は、グループがデンスモードに戻り、データがフラッドされる可能性があります。

#### 関連トピック

[既存のスパースモードクラウドへの Auto-RP の追加 \(CLI\) , \(35 ページ\)](#)

## Auto-RP の利点

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

- ネットワーク内で複数の RP を使用し、複数のグループ範囲を処理する作業が簡単になります。
- 複数の RP 間で負荷を分散し、グループに加入するホストの場所に従って RP を配置できます。
- PIM ネットワーク内のすべてのルータおよびマルチレイヤ デバイスで矛盾が発生しなくなり、手動による RP 設定が不要になります。この結果、接続問題を引き起こす要因が取り除かれます。

## PIM ネットワークでの Auto-RP の利点

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

## PIMv2 ブートストラップ ルータ

PIMv2 ブートストラップ ルータ (BSR) は、グループ/RP マッピング情報をネットワーク内のすべての PIM ルータおよびマルチレイヤデバイスに配信する別の方法です。これにより、ネットワーク内のルータまたはデバイスごとに RP 情報を手動で設定する必要がなくなります。ただし、BSR は IP マルチキャストを使用してグループ/RP マッピング情報を配信する代わりに、特殊な BSR メッセージをホップ単位でフラッ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デバイスから選択されます。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 はフラッドメカニズムを使用し、どのデバイスが選択された BSR であるかを自動的に学習します。



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

#### 関連トピック

[候補 BSR の設定 \(CLI\) , \(48 ページ\)](#)

[PIMv2 BSR の設定, \(43 ページ\)](#)

[例: 候補 BSR の設定, \(77 ページ\)](#)

[Auto-RP および BSR の設定に関する制約事項, \(4 ページ\)](#)

## 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。

#### 関連トピック

[PIM ドメイン境界の定義 \(CLI\) , \(43 ページ\)](#)

## マルチキャスト転送

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

マルチキャストトラフィックは、すべてのソースをグループ内のすべてのレシーバに接続する配信ツリー上で、ソースからマルチキャストグループに流れます。このツリーは、すべてのソースで共有できます (共有ツリー)。または、各ソースに個別の配信ツリーを作成することもできます (ソース ツリー)。共有ツリーは一方または双方向です。

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

• (S, G) = (マルチキャストグループ G のユニキャストソース, マルチキャストグループ G)

• (\*, G) = (マルチキャストグループ G のすべてのソース, マルチキャストグループ G)

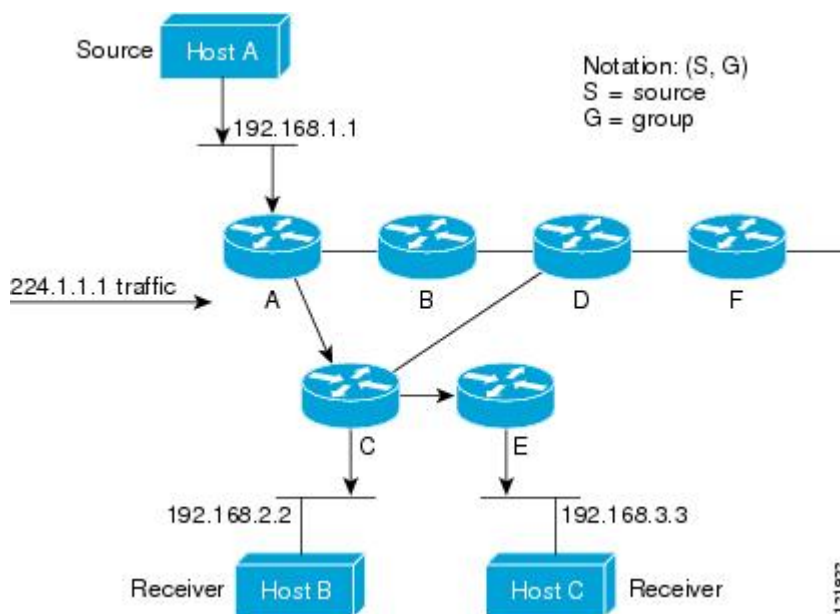
(S, G) という表記 (「S カンマ G」と読みます) は、最短パスツリーの列挙です。S はソースの IP アドレス、G はマルチキャストグループアドレスを表します。

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

## マルチキャスト配信のソース ツリー

マルチキャスト配信ツリーの最も単純な形式は、ソース ツリーです。ソース ツリーは、ソース ホストをルートとし、ネットワークを介してレシーバに接続するスパニングツリーを形成するブランチを持ちます。このツリーはネットワーク上での最短パスを使用するため、最短パスツリー (SPT) とも呼ばれます。

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



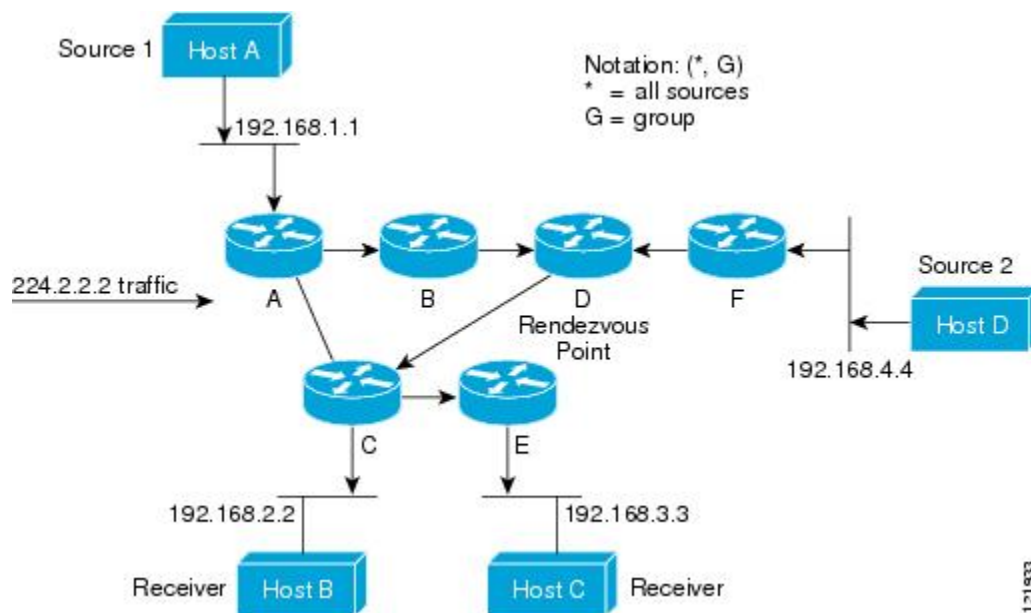
標準表記を使用すると、図の例の SPT は (192.168.1.1, 224.1.1.1) となります。

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

## マルチキャスト配信の共有ツリー

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

**マルチキャスト配信の共有ツリー** 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方向に転送され、すべてのレシーバに到達します (レシーバがソースと RP の間に配置されていない場合は、直接サービスが提供されます)。



この例では、ソース（ホスト A およびホスト D）からのマルチキャストトラフィックがルート（ルータ D）に移動した後に共有ツリーから 2 つのレシーバ（ホスト B およびホスト C）へと到達します。マルチキャストグループ内のすべての送信元が一般的な共有ツリーを使用するため、(\*,G) というワイルドカード表記（「アスタリスク、カンマ、G」と読みます）でそのツリーを表します。この場合、\* はすべてのソースを意味し、G はマルチキャストグループを表します。したがって、**マルチキャスト配信の共有ツリー**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ります。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、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方向へユニキャストパケットのコピーを転送します。

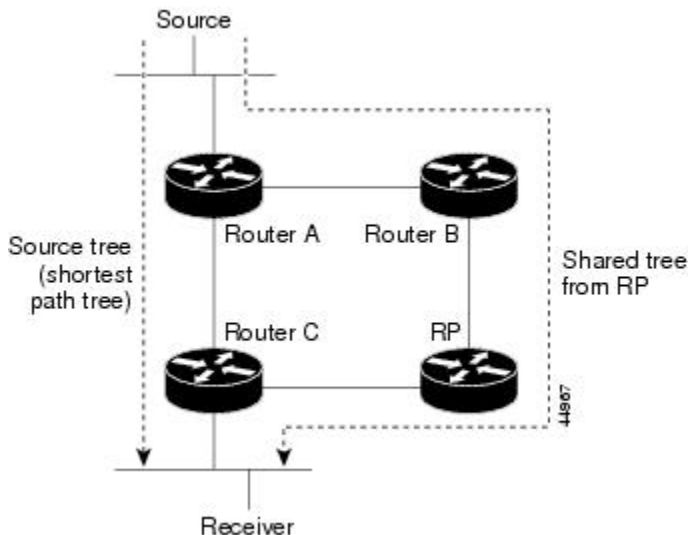
マルチキャスト転送では、ソースは、マルチキャストグループアドレスによって表される任意のホストグループにトラフィックを送信します。マルチキャストルータは、どの方向が（ソースへ向かう）アップストリーム方向で、どの方向（1方向または複数の方向）が（レシーバへ向かう）ダウンストリーム方向であるかを決定する必要があります。複数のダウンストリームパスがある場合、ルータはパケットを複製し、それを適切なダウンストリームパス（最善のユニキャストルートメトリック）で下方向に転送します。これらのパスがすべてであるとは限りません。レシーバの方向ではなく、ソースから遠ざかる方向へのマルチキャストトラフィック転送は、Reverse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

## PIM 共有ツリーおよびソース ツリー

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

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

図 3: 共有ツリーおよびソース ツリー（最短パスツリー）



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

共有ツリーから送信元ツリーへの移動プロセスは、次のとおりです。

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

## 関連トピック

[PIM 最短パス ツリーの使用の延期 \(CLI\) , \(58 ページ\)](#)

## 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

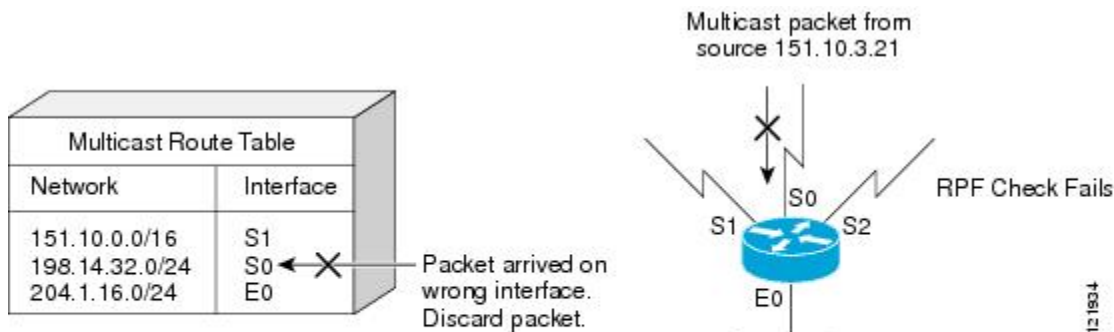
マルチキャストパケットがルータに到達すると、ルータはそのパケットに対してRPFチェックを実行します。RPFチェックが成功すると、パケットが転送されます。そうでない場合、パケットはドロップされます。

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。

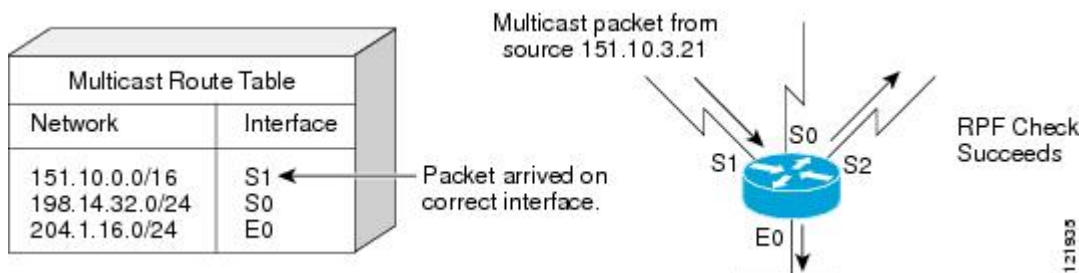
図 4: RPFチェックの失敗



図に示すように、ソース 151.10.3.21 から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 5: 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 デバイスがソース ツリー ステートである場合（つまり (S, G) エントリがマルチキャストルーティング テーブル内にある場合）、マルチキャスト パケットの送信元の IP アドレスに対して RPF チェックが実行されます。
- PIM ルータまたはマルチレイヤ デバイスが共有ツリー ステートである場合（およびソース ツリー ステートが明示されていない場合）、（メンバ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。

DVMRP およびデンス モードの PIM ではソース ツリーだけが使用され、RPF が使用されます。



(注) デバイスでは 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

次の表に、デバイスの PIM ルーティングのデフォルト設定を示します。



表 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
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 (CLI)

この手順は任意です。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例: Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	<b>configureterminal</b>  例 :  Device# <b>configure terminal</b>	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	<b>interfaceinterface-id</b>  例 :  Device(config)# <b>interface</b> <b>gigabitethernet 1/0/1</b>	PIM スタブルーティングをイネーブルにするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。  次のいずれかのインターフェイスを指定する必要があります。 <ul style="list-style-type: none"> <li>• ルーテッド ポート : レイヤ 3 ポートとして <b>no switchport</b> インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。</li> <li>• SVI : <b>interface vlanvlan-id</b> グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。</li> </ul> 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	<b>ip pim passive</b>  例 :  Device(config-if)# <b>ip pim</b> <b>passive</b>	インターフェイスに PIM スタブ機能を設定します。

	コマンドまたはアクション	目的
ステップ 5	<b>end</b>  例 : Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show ip pim interface</b>  例 : Device# <b>show ip pim interface</b>	(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	<b>show ip igmp groups detail</b>  例 : Device# <b>show ip igmp groups detail</b>	(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。
ステップ 8	<b>show ip mroute</b>  例 : Device# <b>show ip mroute</b>	(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	<b>show running-config</b>  例 : Device# <b>show running-config</b>	入力を確認します。
ステップ 10	<b>copy running-config startup-config</b>  例 : Device# <b>copy running-config startup-config</b>	(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。

#### 関連トピック

[PIM スタブルルーティング, \(10 ページ\)](#)

例 : [PIM スタブルルーティングのイネーブル化, \(74 ページ\)](#)

例 : [PIM スタブルルーティングの確認, \(75 ページ\)](#)

[PIM スタブ ルーティングの設定に関する制約事項, \(3 ページ\)](#)

## ランデブーポイントの設定

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

- RP をマルチキャストグループに手動で割り当てる
- PIMv1 から独立した、以下を含むスタンドアロンとしてのシスコ独自のプロトコル
  - 新規インターネットワークでの自動 RP の設定
  - 既存のスパースモードクラウドへの自動 RP の追加
  - 問題のある RP への Join メッセージの送信禁止
  - 着信 RP アナウンスメントメッセージのフィルタリング
- Internet Engineering Task Force (IETF) の標準追跡プロトコルの使用 (PIMv2 BSR の設定を含む)



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

### 関連トピック

[候補 RP の設定 \(CLI\), \(49 ページ\)](#)

[ランデブーポイント, \(11 ページ\)](#)

## マルチキャストグループへの RP の手動割り当て (CLI)

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

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



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

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

この手順は任意です。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例： Device# <b>configure terminal</b>	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	<b>ip pim rp-address ip-address [access-list-number] [override]</b>  例： Device(config)# <b>ip pim rp-address 10.1.1.1 20 override</b>	<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デバイス（RP を含む）で、RP の IP アドレスを設定する必要があります。</p> <p>（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。</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"> <li>• <i>ip-address</i> 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。</li> <li>• （任意） <i>access-list-number</i> 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。</li> <li>• （任意） <b>override</b> 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。</li> </ul>

	コマンドまたはアクション	目的
ステップ 4	<p><b>access-list</b><i>access-list-number</i> {<b>deny</b>   <b>permit</b>} <i>source</i> [<i>source-wildcard</i>]</p> <p>例 :</p> <pre>Device(config)# access-list 25 permit 10.5.0.1 255.224.0.0</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• <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。</li> <li>• <b>deny</b> 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。</li> <li>• <b>permit</b> 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。</li> <li>• <i>source</i> 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。</li> <li>• (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 を設定します。</li> </ul> <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します。</p>
ステップ 5	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 6	<p><b>show running-config</b></p> <p>例 :</p> <pre>Device# show running-config</pre>	<p>入力を確認します。</p>
ステップ 7	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	<p>(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。</p>

#### 関連トピック

例 : マルチキャストグループへの RP の手動割り当て, (75 ページ)

## 新規インターネットワークでの Auto-RP の設定 (CLI)

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



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

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードをインターフェイスにします。パスワードを入力します (設定された場合)。
ステップ 2	<b>show running-config</b> 例： Device# <b>show running-config</b>	すべての PIM デバイスでデフォルトの RP が設定されていること、および RP が SM ネットワークにあることを確認します。RP は、 <b>ip pim rp-address</b> 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) 以外の他のグローバルグループ (224.x.x.x) に対して設定されます。この RP で設定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 によって自動的に検出された RP は、自動的に設定された RP よ

	コマンドまたはアクション	目的
		優先されます。ローカルグループ用に 2 番目の RP を使用することもできます。
ステップ 3	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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	<b>ip pim</b> <b>send-rp-announce interface-id scope ttl group-list access-list-number interval seconds</b> 例 : Device (config)# <b>ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120</b>	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。 <ul style="list-style-type: none"> <li>• <b>interface-id</b> 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、ポートチャンネル、VLAN などです。</li> <li>• <b>scope ttl</b> 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。</li> <li>• <b>group-list access-list-number</b> 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</li> </ul>



	コマンドまたはアクション	目的
		<p>てのグループにR 使用されます。</p> <ul style="list-style-type: none"> <li>• <b>intervalseconds</b> に アナウンスメント メッセージを送信 る頻度を指定しま す。デフォルトは 秒です。指定でき 範囲は 1 ~ 16383 す。</li> </ul>
<p>ス テッ プ 5</p>	<p><b>access-list</b><i>access-list-number</i> {<b>deny</b>   <b>permit</b>} <i>source</i> [<i>source-wildcard</i>]</p> <p>例 :</p> <pre>Device(config)# <b>access-list 10 permit 10.10.0.0</b></pre>	<p>標準アクセス リストを 成し、コマンドを必要 数だけ実行します。</p> <ul style="list-style-type: none"> <li>• <b>access-list-number</b> は、ステップ 3 で 定したアクセス ト番号を入力しま す。</li> <li>• <b>deny</b> キーワードは 条件が一致した場 にアクセスを拒否 ます。</li> <li>• <b>permit</b> キーワー は、条件が一致し 場合にアクセスを 可します。</li> <li>• <b>source</b> には、RP 用されるマルチキ ストグループの レス範囲を入力し す。</li> <li>• (任意) <i>source-wildcard</i> に は、<b>source</b> に適用 れるワイルドカー ビットをドット付 10 進表記で入力 す。無視するビッ</li> </ul>

	コマンドまたはアクション	目的
		<p>位置には 1 を設定します。</p> <p>(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。</p>
ステップ 6	<p><b>ip pim send-rp-discovery scopettl</b></p> <p>例 :</p> <pre>Device(config)# ip pim send-rp-discovery scope 50</pre>	<p>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。</p> <p><b>scopettl</b> 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。</p>
ステップ 7	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 8	<p><b>show running-config</b></p> <p>例 :</p> <pre>Device# show running-config</pre>	<p>入力を確認します。</p>

	コマンドまたはアクション	目的
ステップ 9	<b>show ip pim rp mapping</b> 例： Device# <b>show ip pim rp mapping</b>	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タイプな RP を表示します。
ステップ 10	<b>show ip pim rp</b> 例： Device# <b>show ip pim rp</b>	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	<b>copy running-config startup-config</b> 例： Device# <b>copy running-config startup-config</b>	(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。

#### 関連トピック

[Auto-RP, \(12 ページ\)](#)

例：[Auto-RP の設定, \(75 ページ\)](#)

例：[Auto-RP でのスパス モード, \(76 ページ\)](#)

[Auto-RP および BSR の設定に関する制約事項, \(4 ページ\)](#)

[Auto-RP 拡張の制約事項, \(5 ページ\)](#)

## 既存のスパス モード クラウドへの Auto-RP の追加 (CLI)

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

この手順は任意です。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します (設定された場合)。

	コマンドまたはアクション	目的
ステップ 2	<p><b>show running-config</b></p> <p>例 :</p> <pre>Device# show running-config</pre>	<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。</p> <p>RP は、<b>ip pim rp-address</b> 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>(注) 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 番目の RP を使用することもできます。</p>
ステップ 3	<p><b>configure terminal</b></p> <p>例 :</p> <pre>Device# configure terminal</pre>	<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 4	<p><b>ip pim</b></p> <p><b>send-rp-announce interface-id scope ttl group-list access-list-number interval seconds</b></p> <p>例 :</p> <pre>Device(config)# ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120</pre>	<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"> <li><b>interface-id</b> には、RP アドレスを識別するインターフェイス</li> </ul>

	コマンドまたはアクション	目的
		<p>IP および番号を力します。有効なインターフェイスは物理ポート、ポートチャンネル、VLAN などです。</p> <ul style="list-style-type: none"> <li>• <b>scopetl</b>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ランデブーポイントに到達するまでに、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 ～ です。</li> <li>• <b>group-listaccess-list-number</b>を指定する場合は、1 ～ 99 の IP 標準アクセスリスト番号を力します。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 R 使用されます。</li> <li>• <b>intervalseconds</b>に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。デフォルトは秒です。指定できる範囲は 1 ～ 16383 です。</li> </ul>
ステップ 5	<p><b>access-list</b><i>access-list-number</i> {deny   permit} <i>source</i> [<i>source-wildcard</i>]</p> <p>例 :</p> <pre>Device(config)# access-list 10</pre>	<p>標準アクセスリストを作成し、コマンドを必要数だけ実行します。</p>

	コマンドまたはアクション	目的
	<pre>permit 224.0.0.0 15.255.255.255</pre>	<ul style="list-style-type: none"> <li>• <i>access-list-number</i> 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。</li> <li>• <b>deny</b> 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。</li> <li>• <b>permit</b> 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。</li> <li>• <i>source</i> 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。</li> <li>• (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 を設定します。</li> </ul> <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 6	<pre>ip pim send-rp-discovery scopettl</pre> <p>例 :</p> <pre>Device(config)# ip pim send-rp-discovery scope 50</pre>	<p>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。</p> <p><b>scopettl</b> には、ホップの TTL 値を指定し、RP デイスクバリ パケットを制限</p>

	コマンドまたはアクション	目的
		<p>します。ホップ数内にすべてのデバイスは、元デバイスから自動 R 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 範囲の重なりなを回避するために使用するグループ/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。指定する範囲は 1～255 で</p> <p>(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、<b>n</b> <b>pim</b> <b>send-rp-discovery</b> グローバル フィギュレーション コマンドを使用します</p>
ステップ 7	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 8	<p><b>show running-config</b></p> <p>例 :</p> <pre>Device# show running-config</pre>	入力を確認します。
ステップ 9	<p><b>show ip pim rp mapping</b></p> <p>例 :</p> <pre>Device# show ip pim rp mapping</pre>	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タイプな RP を表示します。

	コマンドまたはアクション	目的
ステップ 10	<b>show ip pim rp</b> 例 : Device# <b>show ip pim rp</b>	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	<b>copy running-config startup-config</b> 例 : Device# <b>copy running-config startup-config</b>	(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。

#### 関連トピック

[Auto-RP のスパス - デンス モード, \(15 ページ\)](#)

## 問題のある RP への Join メッセージの送信禁止 (CLI)

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

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

この手順は任意です。

#### 関連トピック

[例 : 問題のある RP への Join メッセージの送信禁止, \(77 ページ\)](#)

## 着信 RP アナウンスメント メッセージのフィルタリング (CLI)

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

この手順は任意です。



## 手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例 :</p> <pre>Device&gt; enable</pre>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<p><b>configure terminal</b></p> <p>例 :</p> <pre>Device# configure terminal</pre>	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	<p><b>ip pim rp-announce-filter rp-list access-list-number group-list access-list-number</b></p> <p>例 :</p> <pre>Device(config)# ip pim rp-announce-filter rp-list 10 group-list 14</pre>	<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><b>rp-list access-list-number</b> 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、<b>group-list access-list-number</b> 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せん。</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 4	<p><b>access-list access-list-number {deny   permit} source [source-wildcard]</b></p> <p>例 :</p> <pre>Device(config)# access-list 10 permit 10.8.1.0 255.255.224.0</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>access-list-number</b> 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。</li> <li>• <b>deny</b> 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。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>permit</b> 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。</li> <li>• どのルータおよびマルチレイヤデバイスからの候補 RP アナウンスメント (<b>rp-list</b> 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。</li> <li>• 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。</li> <li>• <b>source</b> 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。</li> <li>• (任意) <b>source-wildcard</b> には、<b>source</b> 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。</li> </ul> <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します。</p>
ステップ 5	<b>end</b>  例 :  Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b>  例 :  Device# <b>show running-config</b>	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	<b>copy running-config startup-config</b> 例： Device# <b>copy running-config startup-config</b>	(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。

#### 関連トピック

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、(76 ページ)

## 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

#### 関連トピック

候補 BSR の設定 (CLI) , (48 ページ)

PIMv2 ブートストラップルータ、(16 ページ)

### PIM ドメイン境界の定義 (CLI)

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

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	<b>configureterminal</b>  例 :  Device# <b>configure terminal</b>	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	<b>interfaceinterface-id</b>  例 :  Device (config) # <b>interface gigabitethernet 1/0/1</b>	<p>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。</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"> <li>• ルーテッドポート：レイヤ3ポートとして <b>no switchport</b> インターフェイスコンフィギュレーションコマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース-デンスモードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティックグループに加入させる必要があります。</li> <li>• SVI： <b>interface vlanvlan-id</b> グローバルコンフィギュレーションコマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース-デンスモードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティックグループに加入させ、VLAN、IGMP スタティックグループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。</li> </ul> <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。</p>
ステップ 4	<b>ip pim bsr-border</b>  例 :  Device (config-if) # <b>ip pim bsr-border</b>	<p>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。</p> <p>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。</p> <p>(注) PIM 境界を削除するには、<b>no ip pim bsr-border</b> 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。</p>

	コマンドまたはアクション	目的
ステップ 5	<b>end</b>  例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b>  例： Device# <b>show running-config</b>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b>  例： Device# <b>copy running-config startup-config</b>	(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。

#### 関連トピック

[PIM ドメイン境界, \(17 ページ\)](#)

## IP マルチキャスト境界の定義 (CLI)

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 packets を拒否するアクセスリストを作成します。

この手順は任意です。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	<b>configureterminal</b>  例 :  Device# <b>configure terminal</b>	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	<b>access-listaccess-list-numberdeny</b> source [source-wildcard]  例 : Device(config)# <b>access-list 12 deny 224.0.1.39</b> <b>access-list 12 deny 224.0.1.40</b>	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。 <ul style="list-style-type: none"> <li>• <i>access-list-number</i> の範囲は 1 ~ 99 です。</li> <li>• <b>deny</b> 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。</li> <li>• <i>source</i> 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。</li> <li>• (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 を設定します。</li> </ul> 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	<b>interfaceinterface-id</b>  例 :  Device(config)# <b>interface</b> <b>gigabitethernet 1/0/1</b>	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。 <ul style="list-style-type: none"> <li>• ルーテッド ポート : レイヤ 3 ポートとして <b>no switchport</b> インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース-デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。</li> <li>• SVI : <b>interface vlanvlan-id</b> グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース-デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタ</li> </ul>

	コマンドまたはアクション	目的
		<p>ティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理 インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。</p> <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。</p>
ステップ 5	<p><b>ip multicast boundary</b><i>access-list-number</i></p> <p>例 :</p> <pre>Device(config-if)# ip multicast boundary 12</pre>	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	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 7	<p><b>show running-config</b></p> <p>例 :</p> <pre>Device# show running-config</pre>	入力を確認します。
ステップ 8	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	(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。

#### 関連トピック

[マルチキャスト境界, \(14 ページ\)](#)

例 : [Auto-RP 情報を拒否する IP マルチキャスト境界の定義, \(76 ページ\)](#)

[IP マルチキャスト境界](#)

[マルチキャスト グループ伝送方式](#)

例 : [IP マルチキャスト境界の設定](#)

## 候補 BSR の設定 (CLI)

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

この手順は任意です。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例： Device# <b>configure terminal</b>	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	<b>ip pim</b> <b>bsr-candidate</b> <i>interface-id</i> <i>hash-mask-length</i> [ <i>priority</i> ]  例： Device(config)# <b>ip pim</b> <b>bsr-candidate</b> <b>gigabitethernet 1/0/3 28</b> <b>100</b>	候補 BSR となるようにデバイスを設定します。 <ul style="list-style-type: none"> <li>• <i>interface-id</i> には、スイッチを候補 BSR に設定するとき BSR アドレスの取得元となるデバイス上のインターフェイスを入力します。このインターフェイスは PIM を使用して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。</li> <li>• <i>hash-mask-length</i> 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 ビットだけが使用されます。</li> <li>• (任意) <i>priority</i> 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。</li> </ul>



	コマンドまたはアクション	目的
ステップ 4	<b>end</b>  例 : Device (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>  例 : Device# <b>show running-config</b>	入力を確認します。
ステップ 6	<b>copy running-config startup-config</b>  例 : Device# <b>copy running-config startup-config</b>	(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。

#### 関連トピック

- [PIMv2 ブートストラップ ルータ, \(16 ページ\)](#)
- [PIMv2 BSR の設定, \(43 ページ\)](#)
- [例 : 候補 BSR の設定, \(77 ページ\)](#)
- [Auto-RP および BSR の設定に関する制約事項, \(4 ページ\)](#)

## 候補 RP の設定 (CLI)

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

この手順は任意です。

#### はじめる前に

RP となるデバイスを決定するときは、次の可能性を考慮してください。

- 自動 RP だけが使用されている Cisco ルータおよびマルチレイヤ デバイスで構成されるネットワークでは、すべてのデバイスを RP として設定できます。

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

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例： Device# <b>configure terminal</b>	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	<b>ip pim rp-candidateinterface-id [group-listaccess-list-number]</b>  例： Device(config)# <b>ip pim rp-candidate gigabitethernet 1/0/5 group-list 10</b>	候補 RP となるようにデバイスを設定します。 <ul style="list-style-type: none"> <li>• <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。</li> <li>• (任意) <b>group-listaccess-list-number</b> 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。<b>group-list</b> を指定しない場合は、デバイスがすべてのグループの候補 RP となります。</li> </ul>
ステップ 4	<b>access-listaccess-list-number {deny   permit} source [source-wildcard]</b>  例： Device(config)# <b>access-list 10 permit 239.0.0.0 0.255.255.255</b>	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。 <ul style="list-style-type: none"> <li>• <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。</li> <li>• <b>deny</b> 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。<b>permit</b> 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。</li> <li>• <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。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• (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を設定します。</li> </ul> <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します。</p>
ステップ5	<b>end</b>  例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ6	<b>show running-config</b>  例： Device# <b>show running-config</b>	入力を確認します。
ステップ7	<b>copy running-config startup-config</b>  例： Device# <b>copy running-config startup-config</b>	(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。

#### 関連トピック

- [ランデブー ポイント, \(11 ページ\)](#)
- [ランデブー ポイントの設定, \(28 ページ\)](#)
- [例: 候補 RP の設定, \(78 ページ\)](#)

## Auto-RP によるスパス モードの設定 (CLI)

### はじめる前に

- スパス-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ス モードまたはデンス モードで処理されます。インターフェイスを設定する方法を決定する必要があります。
- Auto-RP を設定するときに必要なすべてのアクセスリストは、設定作業を開始する前に設定しておく必要があります。



(注)

- グループ内に既知の RP がなく、インターフェイスがスパース-デンス モードに設定されている場合、インターフェイスはデンス モードであるように扱われ、データはインターフェイスを介してフラッディングされます。このデータのフラッディングを避けるために、Auto-RP リスナーを設定してから、インターフェイスをスパース モードとして設定します。
- Auto-RP を設定するには、Auto-RP リスナーの機能を設定し (ステップ 5)、スパース モードを指定するか (ステップ 7)、またはスパース-デンス モードを指定する (ステップ 8) 必要があります。
- スパース-デンス モードを指定する場合、デンス モードのフェールオーバーがネットワークのデンス モードのフラッディングを引き起こす可能性があります。この状況を避けるため、Auto-RP リスナー機能で PIM スパース モードを使用します。

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

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> enable	特権 EXEC モードをイネーブルにします。  • パスワードを入力します (要求された場合)。
ステップ 2	<b>configureterminal</b> 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	<b>ipmulticast-routing [distributed]</b> 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。  • <b>distributed</b> キーワードを使用して、マルチキャスト分散スイッチングをイネーブルにします。
ステップ 4	ステップ 5 ~ 7 を実行するか、またはステップ 6 および 8 を実行します。	--

	コマンドまたはアクション	目的
ステップ 5	<b>ippimautorplistener</b> 例 : <pre>Device(config)# ip pim autorp listener</pre>	2 つの Auto-RP グループ 224.0.1.39 と 224.0.1.40 の IP マルチキャストトラフィックを PIM スパースモードで動作しているインターフェイスでフラグディングされる PIM デンスモードにします。 <ul style="list-style-type: none"> <li>• 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。</li> </ul>
ステップ 6	<b>interfacetypenumber</b> 例 : <pre>Device(config)# interface GigabitEthernet 1/0/0</pre>	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 7	<b>ippimsparse-mode</b> 例 : <pre>Device(config-if)# ip pim sparse-mode</pre>	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。 <ul style="list-style-type: none"> <li>• 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。</li> </ul>
ステップ 8	<b>ippimsparse-dense-mode</b> 例 : <pre>Device(config-if)# ip pim sparse-dense-mode</pre>	インターフェイスで PIM スパース-デンスモードをイネーブルにします。 <ul style="list-style-type: none"> <li>• ステップ 7 でスパースモードを設定している場合は、このステップをスキップします。</li> </ul>
ステップ 9	<b>exit</b> 例 : <pre>Device(config-if)# exit</pre>	インターフェイスコンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	すべての PIM インターフェイス上でステップ 1 ~ 9 を繰り返します。	--
ステップ 11	<p><b>ippimsend-rp-announce</b> {<i>interface-type</i><i>interface-number</i>   <i>ip-address</i>} <i>scope</i> <i>ttl-value</i> [<i>group-list</i> <i>access-list</i>] [<i>intervalseconds</i>] [<i>bidir</i>]</p> <p>例 :</p> <pre>Device(config)# ip pim send-rp-announce loopback0 scope 31 group-list 5</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• RP デバイスでのみこのステップを実行します。</li> <li>• RP アドレスとして使用する IP アドレスを定義するには、<i>interface-type</i> 引数と <i>interface-number</i> 引数を使用します。</li> <li>• 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、<i>ip-address</i> 引数を使用します。</li> </ul> <p>(注) このコマンドに <i>ip-address</i> 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)。</p> <ul style="list-style-type: none"> <li>• 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</li> </ul>

	コマンドまたはアクション	目的
		<p>ているグループを示しています。</p>
<p>ステップ 12</p>	<p><b>ip pim send-rp-discovery</b> [<i>interface-type</i><i>interface-number</i>] <b>scope</b><i>ttl-value</i> [<i>intervalseconds</i>]</p> <p>例 :</p> <pre>Device(config)# ip pim send-rp-discovery loopback 1 scope 31</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> </ul> <p>(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。</p> <ul style="list-style-type: none"> <li>• 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 <i>interface-type</i> 引数と <i>interface-number</i> 引数を使用します。</li> <li>• 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、<b>scope</b> キーワードと <i>ttl-value</i> 引数を使用します。</li> <li>• 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 <b>interval</b> キーワードと</li> </ul>

	コマンドまたはアクション	目的
		<p><i>seconds</i> 引数を使用します。</p> <p>(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、<b>group-to-RP</b> マッピングのより頻繁なフラッシュが発生します。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。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
ステップ 13	<p><b>ippimrp-announce-filter rp-list access-list group-list access-list</b></p> <p>例 :</p> <pre>Device(config)# ip pim rp-announce-filter rp-list 1 group-list 2</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
ステップ 14	<p><b>noippimdm-fallback</b></p> <p>例 :</p> <pre>Device(config)# no ip pim dm-fallback</pre>	<p>(任意) PIM デンス モード フォールバックを防ぎます。</p> <ul style="list-style-type: none"> <li>すべてのインターフェイスが PIM スパス モードで動作するように設定されている場合、このステップはスキップします。</li> </ul>



	コマンドまたはアクション	目的
		(注) <b>(ippimsparse-mode</b> コマンドを使用して) すべてのインターフェイスが PIM スパース モードで動作するように設定されている場合、 <b>noippimdm-fallback</b> コマンド動作がデフォルトでイネーブルになります。
ステップ 15	<b>interfacetypenumber</b>  例：  Device(config)# interface gigabitethernet 1/0/0	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 16	<b>ipmulticastboundaryaccess-list [filter-autorp]</b>  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。  <ul style="list-style-type: none"> <li>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。</li> <li>この作業ではアクセスリストは表示されません。</li> <li><b>deny</b> キーワードを使用するアクセスリストエントリはそのエントリに一致するパケットのマルチキャスト境界を作成します。</li> </ul>
ステップ 17	<b>end</b>  例：  Device(config-if)# end	グローバル コンフィギュレーション モードに戻ります。
ステップ 18	<b>showippimautorp</b>  例：  Device# show ip pim autorp	(任意) Auto-RP 情報を表示します。

	コマンドまたはアクション	目的
ステップ 19	<b>show ip pim rp [mapping] [rp-address]</b> 例： Device# show ip pim rp mapping	(任意) ネットワークで既知の RP を表示し、デバイスが各 RP について学習する方法を示します。
ステップ 20	<b>show ip igmp groups [group-name   group-address [interface-type interface-number] [detail]</b> 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。 <ul style="list-style-type: none"> <li>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。</li> </ul>
ステップ 21	<b>show ip mroute [group-address   group-name] [source-address   source-name] [interface-type interface-number] [summary] [count] [active kbps]</b> 例： Device# show ip mroute cbone-audio	(任意) IP マルチキャストルーティング (mroute) テーブルの内容を表示します。

## PIM 最短パス ツリーの使用の延期 (CLI)

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

この手順は任意です。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例 : Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configureterminal</b>  例 : Device# <b>configure terminal</b>	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	<b>access-listaccess-list-number {deny   permit} source [source-wildcard]</b>  例 : Device(config)# <b>access-list 16 permit 225.0.0.0 0.255.255.255</b>	標準アクセス リストを作成します。 <ul style="list-style-type: none"> <li>• <i>access-list-number</i> の範囲は 1 ~ 99 です。</li> <li>• <b>deny</b> 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。</li> <li>• <b>permit</b> 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。</li> <li>• <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。</li> <li>• (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 を設定します。</li> </ul> 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	<b>ip pim spt-threshold {kbps   infinity} [group-listaccess-list-number]</b>  例 : Device(config)# <b>ip pim spt-threshold infinity group-list 16</b>	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。 <ul style="list-style-type: none"> <li>• <i>kbps</i> 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。</li> <li>• <b>infinity</b> 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。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>(任意) <b>group-listaccess-list-number</b> 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。</li> </ul>
ステップ 5	<b>end</b>  例： Device (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b>  例： Device# <b>show running-config</b>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b>  例： Device# <b>copy running-config startup-config</b>	(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。

#### 関連トピック

[PIM 共有ツリーおよびソース ツリー, \(20 ページ\)](#)

## PIM ルータクエリーメッセージ間隔の変更 (CLI)

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

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

この手順は任意です。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例 : Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configureterminal</b>  例 : Device# <b>configure terminal</b>	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	<b>interfaceinterface-id</b>  例 : Device(config)# <b>interface gigabitethernet 1/0/1</b>	<p>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。</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"> <li>• ルーテッド ポート : レイヤ 3 ポートとして <b>no switchport</b> インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース-デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。</li> <li>• SVI : <b>interface vlanvlan-id</b> グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース-デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。</li> </ul> <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。</p>
ステップ 4	<b>ip pim query-intervalseconds</b>  例 : Device(config-if)# <b>ip pim</b>	デバイスが PIM ルータクエリー メッセージを送信する頻度を設定します。

	コマンドまたはアクション	目的
	<code>query-interval 45</code>	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	<code>end</code>  例： Device(config)# <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show ip igmp interface [interface-id]</code>  例： Device# <code>show ip igmp interface</code>	入力を確認します。
ステップ 7	<code>copy running-config startup-config</code>  例： Device# <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。

## 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

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例 :  Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。
ステップ 2	<b>showipmroute [group-address]</b>  例 : Device# <b>show ip mroute 239.1.2.3</b> (*, 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-Dense, 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	<b>showipmrouteactive[kb/s]</b>  例 : Device# <b>show ip mroute active</b> 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
	<pre>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)</pre>	<p>(注) デフォルトでは、<b>showipmroute</b> コマンドと <b>active</b> キーワードによる出力では、4 kb/s以上のレートでグループにトラフィックを送信するアクティブな送信元の情報が表示されます。より低いレートのトラフィック（4 kb/s未満のトラフィック）をグループに送信しているアクティブなソースに関する情報を表示する場合は、<i>kb/s</i> 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。</p>

## SPT 上のルータでの IP マルチキャストの確認

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

### 手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例 :</p> <pre>Device&gt; enable</pre>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<p><b>showipmroute [group-address]</b></p> <p>例 :</p> <pre>Device# show ip mroute 239.1.2.3 (*, 239.1.2.3), 00:17:56/00:03:02, RP 172.16.0.1, flags: S Incoming interface: Null, RPF nbr 0.0.0.0 Outgoing interface list: GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:17:56/00:03:02 (10.0.0.1, 239.1.2.3),</pre>	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。



	コマンドまたはアクション	目的
	00:15:34/00:03:28, flags: T Incoming interface: Serial1/0, RPF nbr 172.31.200.1 Outgoing interface list: GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:15:34/00:03:02	
ステップ 3	<b>showipmrouteactive</b>  例 : Device# <b>show ip mroute active</b> 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、 <b>showipmroute</b> コマンドと <b>active</b> キーワードによる出力では、 <b>4 kb/s</b> 以上のレートでグループにトラフィックを送信するアクティブな送信元の情報が表示されます。より低いレートのトラフィック ( <b>4kb/s</b> 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、 <i>kb/s</i> 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、 <b>1 kb/s</b> 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソーストラフィックに関する情報が効果的に表示されます。

## ラストホップルータでの IP マルチキャスト動作の確認

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

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例 :  Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	<p><b>showipigmgroups</b></p> <p>例 :</p> <pre>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</pre>	<p>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。</p>
ステップ 3	<p><b>showippimrpmapping</b></p> <p>例 :</p> <pre>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</pre>	<p>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。</p> <p>(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、<b>showippimrpmapping</b> 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 <b>showippimrpmapping</b> コマンドの出力には表示されません。</p>
ステップ 4	<p><b>showipmroute</b></p> <p>例 :</p> <pre>Device# show ip mroute (*, 239.1.2.3), 00:05:14/00:03:04, RP 172.16.0.1, flags: SJC   Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1   Outgoing interface list:   GigabitEthernet1/0, Forward/Sparse-Dense, 00:05:10/00:03:04  (10.0.0.1, 239.1.2.3), 00:02:49/00:03:29, flags: T   Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1   Outgoing interface list:   GigabitEthernet1/0, Forward/Sparse-Dense, 00:02:49/00:03:04  (*, 224.0.1.39), 00:10:05/stopped, RP 0.0.0.0, flags: DC   Incoming interface: Null, RPF nbr 0.0.0.0    Outgoing interface list:   GigabitEthernet1/0, Forward/Sparse-Dense, 00:05:15/00:00:00   GigabitEthernet0/0,</pre>	<p>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。</p>

	コマンドまたはアクション	目的
	Forward/Sparse-Dense, 00:10:05/00:00:00  (172.16.0.1, 224.0.1.39), 00:02:00/00:01:33, flags: PTX Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1	
ステップ 5	<b>showipinterface [typenumber]</b>  例 : Device# <b>show ip interface GigabitEthernet 0/0/0</b> GigabitEthernet0/0 is up, line protocol is up Internet address is 172.31.100.2/24 Broadcast address is 255.255.255.255 Address determined by setup command MTU is 1500 bytes Helper address is not set Directed broadcast forwarding is disabled  Multicast reserved groups joined: 224.0.0.1 224.0.0.22 224.0.0.13 224.0.0.5 224.0.0.6 Outgoing access list is not set Inbound access list is not set Proxy ARP is enabled Local Proxy ARP is disabled Security level is default Split horizon is enabled ICMP redirects are always sent ICMP unreachable are always sent ICMP mask replies are never sent IP fast switching is enabled IP fast switching on the same interface is disabled IP Flow switching is disabled IP CEF switching is disabled IP Fast switching turbo vector IP multicast fast switching is enabled IP multicast distributed fast switching is disabled IP route-cache flags are Fast Router Discovery is disabled IP output packet accounting is disabled IP access violation accounting is disabled TCP/IP header compression is disabled RTP/IP header compression is disabled Policy routing is disabled Network address translation is disabled WCCP Redirect outbound is disabled WCCP Redirect inbound is disabled WCCP Redirect exclude is disabled BGP Policy Mapping is disabled	マルチキャスト高速スイッチングがイネーブルになっており、ラストホップルータの発信インターフェイスでのパフォーマンスが最適化されていることを確認します。  (注) <b>noiproute-cache</b> 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	<b>showipmfib</b>  例 : Device# <b>show ip mfib</b>	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。

	コマンドまたはアクション	目的
ステップ 7	<b>showip pim interface count</b>  例 : Device# <b>show ip pim interface count</b>  State: * - Fast Switched, D - Distributed Fast Switched H - Hardware Switching Enabled Address          Interface FS Mpackets In/Out 172.31.100.2      GigabitEthernet0/0/0 *      4122/0 10.1.0.1          GigabitEthernet1/0/0 *      0/3193	マルチキャストトラフィックがラストホップルータに転送されることを確認します。
ステップ 8	<b>show ip mroute count</b>  例 : Device# <b>show ip mroute count</b> 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	<b>show ip mroute active [kb/s]</b>  例 : Device# <b>show ip mroute active</b> 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、 <b>showipmroute</b> コマンドと <b>active</b> キーワードによる出力では、4kb/s 以上のレートでグループにトラフィックを送信するアクティブな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、 <i>kb/s</i> 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せん。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ーで、すべてのルータが応答する原因となる ping が送信されます。これは、効果的な管理およびデバッグのツールです。

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

### マルチキャスト ping に応答するルータの設定

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

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b>  例： Device# <b>configure terminal</b>	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	<b>interface type number</b>  例： Device(config)# <b>interface gigabitethernet 1/0/0</b>	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。  <i>type</i> 引数および <i>number</i> 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	<b>ip igmp join-group group-address</b>  例： Device(config-if)# <b>ip igmp join-group 225.2.2.2</b>	（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、 <i>group-address</i> 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	<b>end</b>  例： Device(config-if)# <b>end</b>	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。

## マルチキャスト ping に応答するように設定されたルータへの ping

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

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>pinggroup-address</b>  例： Device# <b>ping 225.2.2.2</b>	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
<b>show ip pim all-vrfs tunnel</b> [ <i>tunnel tunnel_number</i>   <i>verbose</i> ]	すべての VRF を表示します。
<b>show ip pim autorp</b>	グローバル Auto-RP 情報を表示します。
<b>show ip pim boundary</b>	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。

コマンド	目的
<b>show ip pim interface</b>	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。
<b>show ip pim neighbor</b>	PIM ネイバー情報を表示します。
<b>show ip pim rp</b> [ <i>group-name</i>   <i>group-address</i> ]	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。
<b>show ip pim tunnel</b> [ <i>tunnel</i>   <i>verbose</i> ]	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。
<b>show ip pim vrf</b> { <i>word</i> { <i>all-vrfs</i>   <i>autorp</i>   <i>boundary</i>   <i>bsr-router</i>   <i>interface</i>   <i>mdt</i>   <i>neighbor</i>   <i>rp</i>   <i>rp-hash</i>   <i>tunnel</i> } }	VPN ルーティング/転送インスタンスを表示します。
<b>show ip igmp groups detail</b>	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
<code>show ip pim rp [ hostname or IP address   mapping [ hostname or IP address   elected   in-use ]   metric [ hostname or IP address ] ]</code>	<p>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。</p> <ul style="list-style-type: none"> <li>• (任意) <i>hostname</i> 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。</li> <li>• (任意) <i>IP address</i> 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。</li> <li>• (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、<b>mapping</b> キーワードを使用します。</li> <li>• (任意) <b>metric</b> キーワードを使用して、RPRPF メトリックを表示します。</li> </ul>
<code>show ip pim rp-hashgroup</code>	<p>指定したグループに選択されている RP を表示します。つまり、PIMv2 ルータまたはマルチレイヤデバイス上で、PIMv1 システムで選択されている RP と同じ RP が使用されていることを確認します。<i>group</i> には、RP 情報を表示するグループアドレスを入力します。</p>

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
<code>show ip pim bsr</code>	選択された BSR に関する情報を表示します。
<code>show ip pim bsr-router</code>	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ตอบสนอง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）。

#### 関連トピック

[PIM のバージョン](#), (9 ページ)

## PIM の設定例

### 例 : PIM スタブル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 スタブルルーティングがイネーブルに設定されています。

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

#### 関連トピック

[PIM スタブルルーティングのイネーブル化 \(CLI\)](#), (25 ページ)

[PIM スタブルルーティング](#), (10 ページ)

## 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 interface** 特権 EXEC コマンドを使用します。

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

### 関連トピック

[PIM スタブルーティングのイネーブル化 \(CLI\) , \(25 ページ\)](#)

[PIM スタブルーティング, \(10 ページ\)](#)

## 例：マルチキャストグループへの RP の手動割り当て

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

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

### 関連トピック

[マルチキャストグループへの RP の手動割り当て \(CLI\) , \(28 ページ\)](#)

## 例：Auto-RP の設定

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

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

### 関連トピック

[新規インターネットワークでの Auto-RP の設定 \(CLI\) , \(31 ページ\)](#)

[Auto-RP, \(12 ページ\)](#)

## 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
```

### 関連トピック

[新規インターネットワークでの Auto-RP の設定 \(CLI\) , \(31 ページ\)](#)

[Auto-RP, \(12 ページ\)](#)

## 例 : Auto-RP 情報を拒否する IP マルチキャスト境界の定義

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

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

### 関連トピック

[IP マルチキャスト境界の定義 \(CLI\) , \(45 ページ\)](#)

[マルチキャスト境界, \(14 ページ\)](#)

## 例 : 着信 RP アナウンスメント メッセージのフィルタリング

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

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

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

#### 関連トピック

[着信 RP アナウンスメント メッセージのフィルタリング \(CLI\) , \(40 ページ\)](#)

## 例：問題のある RP への Join メッセージの送信禁止

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

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

#### 関連トピック

[問題のある RP への Join メッセージの送信禁止 \(CLI\) , \(40 ページ\)](#)

## 例：候補 BSR の設定

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

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

#### 関連トピック

[候補 BSR の設定 \(CLI\) , \(48 ページ\)](#)

[PIMv2 ブートストラップ ルータ, \(16 ページ\)](#)

## 例：候補 RP の設定

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

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

### 関連トピック

[候補 RP の設定 \(CLI\)](#) , (49 ページ)

[ランデブー ポイント](#) , (11 ページ)

## その他の参考資料

### 関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	『 <a href="#">IP Multicast Routing Command Reference (Catalyst 3850 Switches)</a> 』
IGMP ヘルパー コマンドの構文および使用方法の詳細。	『 <a href="#">IP Multicast Routing Command Reference (Catalyst 3850 Switches)</a> 』
Multicast Source Discovery Protocol (MSDP)	『 <a href="#">IP Routing: Protocol-Independent Configuration Guide, Cisco IOS XE Release 3E (Catalyst 3850 Switches)</a> 』
Enhanced Interior Gateway Routing Protocol (EIGRP) スタブ ルーティング	『 <a href="#">IP Routing: EIGRP Configuration Guide, Cisco IOS XE Release 3E (Catalyst 3850 Switches)</a> 』
Open Shortest Path First (OSPF) スタブ ルーティング	『 <a href="#">IP Routing: OSPF Configuration Guide, Cisco IOS XE 3E (Catalyst 3850 Switches)</a> 』
Cisco IOS コマンド	『 <a href="#">Cisco IOS Master Commands List, All Releases</a> 』
Cisco IOS IP SLA コマンド	『 <a href="#">Cisco IOS IP Multicast Command Reference</a> 』

## エラー メッセージ デコーダ

説明	リンク
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	<a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a>

## 標準および RFC

標準/RFC	タイトル
PIM については、 <a href="#">RFC 4601</a> および次に示す Internet Engineering Task Force (IETF) インターネット ドラフトを参照してください。	<ul style="list-style-type: none"> <li>『<i>Protocol Independent Multicast (PIM): Motivation and Architecture</i>』</li> <li>『<i>Protocol Independent Multicast (PIM), Dense Mode Protocol Specification</i>』</li> <li>『<i>Protocol Independent Multicast (PIM), Sparse Mode Protocol Specification</i>』</li> <li>『<i>draft-ietf-idmr-igmp-v2-06.txt, Internet Group Management Protocol, Version 2</i>』</li> <li>『<i>draft-ietf-pim-v2-dm-03.txt, PIM Version 2 Dense Mode</i>』</li> </ul>

## MIB

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

## シスコのテクニカル サポート

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

## PIM の機能履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。