



## PIM の構成

この章では、IPv4 ネットワークの Cisco Nexus 3600 プラットフォーム スイッチに Protocol Independent Multicast (PIM) 機能を構成する方法を説明します。

この章は、次の項で構成されています。

- [PIM に関する情報 \(1 ページ\)](#)
- [PIM の前提条件 \(9 ページ\)](#)
- [PIM の注意事項と制約事項 \(10 ページ\)](#)
- [PIM のデフォルト設定 \(10 ページ\)](#)
- [PIM の構成 \(11 ページ\)](#)
- [PIM 設定の確認 \(35 ページ\)](#)
- [統計の表示 \(36 ページ\)](#)
- [PIM の設定例 \(37 ページ\)](#)
- [次の作業 \(44 ページ\)](#)
- [その他の参考資料 \(44 ページ\)](#)

## PIM に関する情報

マルチキャスト対応ルータ間で使用される PIM は、マルチキャスト配信ツリーを構築して、ルーティング ドメイン内にグループ メンバーシップをアドバタイズします。PIM は、複数の送信元からのパケットが転送される共有配信ツリーと、単一の送信元からのパケットが転送される送信元配信ツリーを構築します。マルチキャストの詳細については、「[マルチキャストに関する詳細](#)」セクションを参照してください。

Cisco NX-OS は、IPv4 ネットワーク (PIM) 対応の PIM スペース モードをサポートします。(PIM スペース モードでは、ネットワーク上の要求元だけにマルチキャスト トラフィックが伝送されます。) ルータ上で同時に実行するように PIM を構成できます。PIM グローバル パラメータを使用すると、ランデブー ポイント (RP)、メッセージ パケット フィルタリング、および統計情報を設定できます。PIM インターフェイス パラメータを使用すると、マルチキャスト機能のイネーブル化、PIM の境界の識別、PIM hello メッセージ インターバルの設定、および指定ルータ (DR) のプライオリティ 設定を実行できます。詳細については、「[PIM スペース モードの構成](#)」セクションを参照してください。

## vPC を使用した PIM SSM



(注) Cisco Nexus 3600 プラットフォーム スイッチは、PIM デンス モードをサポートしていません。

Cisco NX-OS でマルチキャスト機能を有効化するには、各ルータで PIM 機能を有効化してから、マルチキャストに参加する各インターフェイスで、PIM スパース モードを有効化する必要があります。PIM は IPv4 ネットワーク用に設定できます。IPv4 ネットワーク上のルータで IGMP がイネーブルになっていない場合は、PIM によって自動的にイネーブルにされます。IGMP の構成に関する詳細は、「[IGMP の設定](#)」を参照してください。



(注) Cisco Nexus 3600 プラットフォーム スイッチは、PIM6 をサポートしていません。

PIM グローバル コンフィギュレーション パラメータを使用すると、マルチキャスト グループ アドレスの範囲を設定して、次に示す 2 つのツリー 配信モードで利用できます。

- Any Source Multicast (ASM) : マルチキャスト送信元の検出機能を提供します。ASM では、マルチキャスト グループの送信元と受信者間に共有ツリーを構築し、新しい受信者が グループに追加された場合は、送信元ツリーに切り替えることができます。ASM モード を利用するには、RP を設定する必要があります。
- 送信元 固有 マルチキャスト (SSM) は、マルチキャスト送信元への加入要求を受信する LAN セグメント上の代表ルータを起点として、送信元ツリーを構築します。SSM モード では、RP を設定する必要がありません。送信元の検出は、その他の方法で実行する必要があります。

モードを組み合わせて、さまざまな範囲の グループ アドレスに対応することができます。詳細 については、「[PIM の構成](#)」セクションを参照してください。

ASM モードで使用される PIM スパース モードと共有配信ツリーの詳細については、「[RFC 4601](#)」を参照してください。

SSM モードの PIM の詳細については、「[RFC 3569](#)」を参照してください。



(注) Cisco Nexus 3548 シリーズ デバイス対応の Cisco NX-OS では、マルチキャストの等コスト マルチパス (ECMP) がデフォルトでオフになっています。ECMP をオフにすることはできません。プレフィックスに対し複数のパスが存在する場合は、PIM がルーティング テーブル内で最も低いアドミニストレー ティブ ディスタンスを持つパスを選択します。Cisco NX-OS は、宛先までの 16 のパスをサポートします。

## vPC を使用した PIM SSM

vPC 機能とともにアップストリーム レイヤ 3 クラウドを備えた Cisco Nexus 3600 プラットフォーム スイッチで PIM SSM を有効にできます。ダウンストリーム PIM ネイバーがない場合は、

vPC ピア リンクを介して vPC VLAN 上の 2 つのスイッチ間に PIM ネイバー関係を形成できます。

## Hello メッセージ

ルータは、マルチキャスト アドレス 224.0.0.13 に PIM hello メッセージを送信して、PIM ネイバー ルータとの隣接関係を確立します。hello メッセージは 30 秒間隔で定期的に送信されます。PIM ソフトウェアはすべてのネイバーからの応答を確認すると、各 LAN セグメント内で優先順位が最大のルータを代表ルータ (DR) として選択します。DR 優先順位は、PIM hello メッセージの DR 優先順位値に基づいて決まります。全ルータの DR プライオリティ値が不明、またはプライオリティが等しい場合は、IP アドレスが最上位のルータが DR として選定されます。



**注意** PIM hello 間隔を低い値に変更する場合は、ネットワーク環境に適した値に変更することを推奨します。

hello メッセージには保持時間の値も含まれています。通常、この値は hello インターバルの 3.5 倍です。ネイバーから後続の hello メッセージがないまま保持時間を経過すると、スイッチはそのリンクで PIM エラーを検出します。

PIM ソフトウェアで、PIM ネイバーとの PIM hello メッセージの認証に MD5 ハッシュ値を使用するよう設定すると、セキュリティを高めることができます。IGMP スヌーピングソフトウェアは、PIM hello メッセージも処理します。

hello メッセージ認証の構成に関する詳細は、「[PIM スペース モードの構成](#)」セクションを参照してください。

## Join-Prune メッセージ

DR が新しいグループの受信者または送信元から IGMP メンバーシップ レポート メッセージを受信すると、DR は、ランデブー ポイント (ASM モード) または送信元 (SSM モード) に面しているインターフェイスから PIM Join メッセージを送信することにより、受信者を送信元に接続するためのツリーを作成します。ランデブー ポイント (RP) とは、ASM モードで PIM ドメイン内のすべての送信元およびホストにより使用される、共有ツリーのルートです。SSM では RP を使用せず、送信元と受信者間の最小コスト パスである最短パスツリー (SPT) を構築します。

DR はグループまたは送信元から最後のホストが脱退したことを認識すると、PIM Prune メッセージを送信して、配信ツリーから該当するパスを削除します。

各ルータは、マルチキャスト配信ツリーの上流方向のホップに Join または Prune アクションを次々と転送し、パスを作成 (Join) または削除 (Prune) します。

## ■ ステートのリフレッシュ



(注) このマニュアル内の「PIM join メッセージ」および「PIM prune メッセージ」という用語は、PIM join-prune メッセージに関して、Join または Prune アクションのうち実行されるアクションのみをわかりやすく示すために使用しています。

Join/Prune メッセージは、ソフトウェアからできるだけ短時間で送信されます。join-prune メッセージをフィルタリングするには、ルーティング ポリシーを定義します。join-prune メッセージ ポリシーの構成に関する詳細は、「[PIM スペース モードの構成](#)」セクションを参照してください。

PIM Join を上流に発信してルーティング テーブルに含まれる既知のすべての (S, G) に対して SPT を事前に構築できます。受信者が存在しない場合でも、PIM Join を上流に発信してルーティング テーブルに含まれる既知のすべての (S, G) に対する SPT を事前に構築するには、**ip pim pre-build-spt** コマンドを使用します。デフォルトで PIM (S, G) Join が上流に発信されるのは、(S, G) の OIF リストが空でない場合だけです。

## ステートのリフレッシュ

PIM では、3.5 分のタイムアウト間隔でマルチキャストエントリをリフレッシュする必要があります。ステートをリフレッシュすると、トライフィックがアクティブなリスナーだけに配信されるため、ルータで不要なリソースが使用されなくなります。

PIM ステートを維持するために、最終ホップである DR は、Join/Prune メッセージを 1 分に 1 回送信します。次に、(\*, G) ステートおよび (S, G) ステートの構築例を示します。

- (\*, G) ステートの構築例 : IGMP (\*, G) レポートを受信すると、DR は (\*, G) PIM Join メッセージを RP 方向に送信します。
- (S, G) ステートの構築例 : IGMP (S, G) レポートを受信すると、DR は (S, G) PIM Join メッセージを送信元方向に送信します。

180 秒以内にステートがリフレッシュされていない場合、PIM ソフトウェアは、上流ルータのマルチキャスト発信インターフェイスリストから転送パスを削除し、配信ツリーを再構築します。

## ランデブー ポイント

ランデブー ポイント (RP) は、マルチキャストネットワーク ドメイン内にあるユーザが指定したルータで、マルチキャスト共有ツリーの共有ルートとして動作します。必要に応じて複数の RP を設定し、さまざまなグループ範囲をカバーすることができます。

## スタティック RP

マルチキャストグループ範囲の RP は静的に設定できます。この場合、ドメイン内のすべてのルータに RP のアドレスを設定する必要があります。

スタティック RP を定義するのは、次のような場合です。

- ルータに Anycast RP アドレスを設定する場合

- スイッチに手動で RP を設定する場合

スタティック RP の構成に関する詳細は、「[スタティック RP の構成](#)」セクションを参照してください。

## BSR

ブートストラップルータ (BSR) を使用すると、PIM ドメイン内のすべてのルータで、BSR と同じ RP キャッシュが保持されるようになります。BSR では、BSR 候補 RP から RP セットを選択するよう設定できます。BSR は、ドメイン内のすべてのルータに RP セットをブロードキャストする役割を果たします。ドメイン内の RP を管理するには、1つまたは複数の候補 BSR を選択します。候補 BSR の1つが、ドメインの BSR として選定されます。

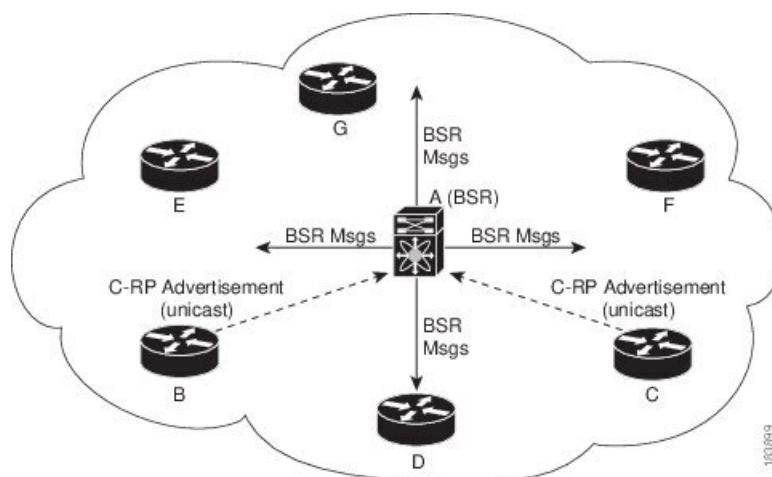


**注意** 同じネットワーク内では、Auto-RP プロトコルと BSR プロトコルを同時に設定できません。

次の図は、BSR メカニズム、ソフトウェアによって選択された BSR であるルータ A が、イ有効になっているすべてのインターフェイスから BSR メッセージを送信する場所を示しています（図の実線で表示）。このメッセージには RP セットが含まれておらず、ネットワーク内のすべてのルータに次々とフラッディングされます。ルータ B および C は候補 RP であり、選定された BSR に候補 RP アドバタイズメントを直接送信しています（図の破線部分）。

選定された BSR は、ドメイン内のすべての候補 RP から候補 RP メッセージを受信します。 BSR から送信されるブートストラップメッセージには、すべての候補 RP に関する情報が格納されています。各ルータでは共通のアルゴリズムを使用することにより、各マルチキャストグループに対応する同一の RP アドレスが選択されます。

図 1: BSR メカニズム



RP 選択プロセスの実行中、ソフトウェアは最も優先順位が高い RP アドレスを特定します。2つ以上の RP アドレスのプライオリティが等しい場合は、選択プロセスで RP ハッシュを使用することもできます。1つのグループに割り当てられる RP アドレスは1つだけです。

デフォルトでは、ルータはBSR メッセージの受信や転送を行えません。BSR メカニズムによって、PIM ドメイン内のすべてのルータに対して、マルチキャストグループ範囲に割り当てられた RP セットが動的に通知されるようにするには、BSR リスニング機能および転送機能をイネーブルにする必要があります。



(注) BSR メカニズムは、サードパーティ製ルータで使用可能な、ベンダー共通の RP 定義方式です。

BSR および候補 RP の構成に関する詳細は、「[BSR の構成](#)」と「[静的 RP の構成](#)」セクションを参照してください。

## Auto-RP

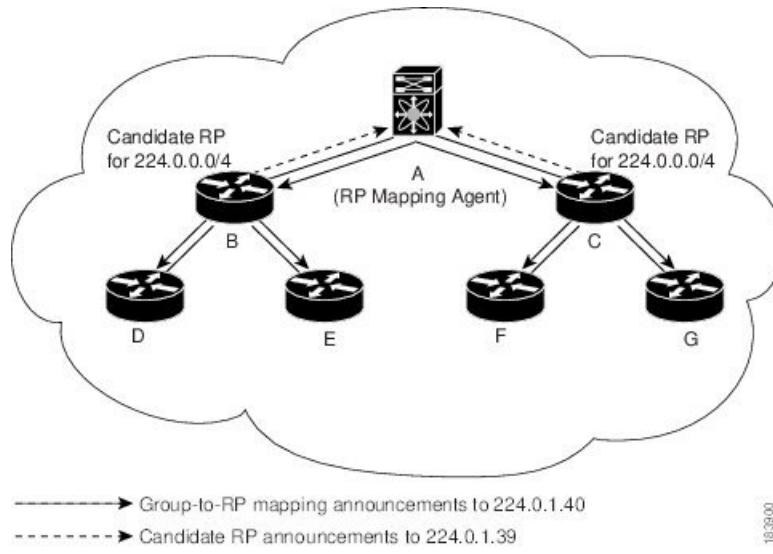
Auto-RP は、インターネット標準であるブートストラップルータ メカニズムに先立って導入されたシスコのプロトコルです。Auto-RP を設定するには、候補マッピングエージェントおよび候補 RP を選択します。候補 RP は、サポート対象グループ範囲を含んだ RP-Announce メッセージを Cisco RP-Announce マルチキャストグループ 224.0.1.39 に送信します。Auto-RP マッピングエージェントは候補 RP からの RP-Announce メッセージを受信して、グループと RP 間のマッピングテーブルを形成します。マッピングエージェントは、このグループと RP 間のマッピングテーブルを RP-Discovery メッセージに格納して、Cisco RP-Discovery マルチキャストグループ 224.0.1.40 にマルチキャストします。



注意 同じネットワーク内では、Auto-RP プロトコルと BSR プロトコルを同時に設定できません。

次の図に、Auto-RP メカニズムを示します。RP マッピングエージェントは、受信した RP 情報を、定期的に Cisco RP-Discovery グループ 224.0.1.40 にマルチキャストします (図の実線部分)。

図 2: Auto-RP のメカニズム



デフォルトでは、ルータは Auto-RP メッセージの受信や転送を行いません。Auto-RP メカニズムによって、PIM ドメイン内のルータに対して、グループと RP 間のマッピング情報が動的に通知されるようにするには、Auto-RP リスニング機能および転送機能をイネーブルにする必要があります。

Auto-RP の構成に関する詳細は、[「Auto-RP の構成」セクション](#)を参照してください。

## Anycast-RP

Anycast-RP には 2 つの実装方法があります。1 つ目はマルチキャスト ソース検出プロトコル (MSDP) 、もう 1 つは [RFC 4610](#) に基づいています。ここでは、PIM Anycast-RP の設定方法について説明します。

PIM Anycast-RP を使用すると、Anycast-RP セットというルータ グループを、複数のルータに設定された単一の RP アドレスに割り当てることができます。Anycast-RP セットとは、Anycast-RP として設定された一連のルータを表します。各マルチキャスト グループで複数の RP をサポートし、セット内のすべての RP に負荷を分散させることができるのは、この RP 方式だけです。Anycast-RP はすべてのマルチキャスト グループをサポートします。

ユニキャストルーティングプロトコルの機能に基づいて、PIM Register メッセージが最も近い RP に送信され、PIM Join/Prune メッセージが最も近い RP の方向に送信されます。いずれかの RP がダウンすると、これらのメッセージは、ユニキャストルーティングを使用して次に最も近い RP の方向へと送信されます。

PIM Anycast-RP の詳細については、[「RFC 4610」](#) を参照してください。

Anycast-RP の構成方法については、[「PIM Anycast-RP 設定の構成」セクション](#)を参照してください。

## PIM 登録メッセージ

PIM Register メッセージは、マルチキャスト送信元に直接接続された指定ルータ (DR) から RP にユニキャストされます。PIM Register メッセージには次の機能があります。

- ・マルチキャストグループに対する送信元からの送信がアクティブであることを RP に通知する
- ・送信元から送られたマルチキャストパケットを RP に配信し、共有ツリーの下流に転送する

DR は RP から Register-Stop メッセージを受信するまで、PIM Register メッセージを RP 宛に送信し続けます。RP が Register-Stop メッセージを送信するのは、次のいずれかの場合です。

- ・RP が送信中のマルチキャストグループに、受信者が存在しない場合
- ・RP が送信元への SPT に加入しているにもかかわらず、送信元からのトラフィックの受信が開始されていない場合

**ip pim register-source** コマンドを使用して、登録メッセージの送信元 IP アドレスが、RP がパケットを送信できる一意のルーティングアドレスではない場合に、登録メッセージの送信元 IP アドレスを設定するために使用します。このような状況は、受信したパケットが転送されないように送信元アドレスがフィルタリングされる場合、または送信元アドレスがネットワークに対して一意でない場合に発生します。このような場合、RP から送信元アドレスへ送信される応答は DR に到達せず、Protocol Independent Multicast Sparse Mode (PIM-SM) プロトコル障害が発生します。

次に、登録メッセージの IP 送信元アドレスを DR のループバック 3 インターフェイスに設定する例を示します。

```
switch # configuration terminal
switch(config)# vrf context Enterprise
switch(config-vrf)# ip pim register-source ethernet 2/3
switch(config-vrf)#
```



(注) Cisco NX-OS では RP の処理の停滞を防ぐため、PIM Register メッセージのレート制限が行われます。

PIM Register メッセージをフィルタリングするには、ルーティングポリシーを定義します。PIM レジスタ メッセージポリシーの構成に関する詳細は、「[メッセージ フィルタリングの構成](#)」セクションを参照してください。

## 指定ルータ

PIM の ASM モードおよび SSM モードでは、各ネットワーク セグメント上のルータの中から指定ルータ (DR) が選択されます。DR は、セグメント上の指定グループおよび送信元にマルチキャストデータを転送します。

LAN セグメントごとの DR は、「[vPC での PIM SSM](#)」セクションに記載された手順で決定されます。

SSM モードの場合、DR は送信元方向に (S,G) PIM join メッセージをトリガーします。受信者から送信元へのパスは、各ホップで決定されます。この場合、送信元が受信者または DR で認識されている必要があります。

ASM モードでは、DR は、受信した IGMP メンバーシップ レポートに応じて、送信元への (S, G) または (\*, G) PIM Join メッセージをトリガーします。DR が、直接接続されたホストまたは、受信者からの IGMP メンバーシップ レポートを受信すると、RP への最短パスが形成されます。さらに、DR は、送信元がアクティブになったときに PIM 登録メッセージを RP に送信します。結果は、そのグループの全ての受信者と共に同じマルチキャストグループへ送信する全ての送信元を接続する共有ツリーです。

DR 優先順位の構成に関する詳細は、「[PIM スペース モードの構成](#)」セクションを参照してください。

## 管理用スコープの IP マルチキャスト

管理用スコープの IP マルチキャスト方式を使用すると、マルチキャストデータの配信先に境界を設定することができます。詳細については、[RFC 2365](#) を参照してください。

インターフェイスを PIM 境界として設定し、PIM メッセージがこのインターフェイスから送信されないようにできます。ドメイン境界パラメータの構成に関する詳細は、「[メッセージ フィルタリングの構成](#)」セクションを参照してください。

Auto-RP スコープ パラメータを使用すると、存続可能時間 (TTL) 値を設定できます。詳細については、「[Auto-RP の構成](#)」セクションを参照してください。

## 仮想化のサポート

複数の仮想ルーティングおよびフォワーディング (VRF) インスタンスを定義することができます。各 VRF では、MRIB を含む独立マルチキャストシステム リソースが維持されます。

**PIM show** コマンドに VRF 引数を指定して実行すると、表示される情報のコンテキストを確認できます。VRF 引数を指定しない場合は、デフォルト VRF が使用されます。

VRF の構成に関する詳細は、「[Cisco Nexus 3600 NX-OS ユニキャスト ルーティング構成ガイド](#)」を参照してください。

## PIM の前提条件

PIM には以下の前提条件があります。

- 現在の仮想ルーティングおよびフォワーディング (VRF) モードが正しい (グローバルコマンドの場合)。この章の例で示すデフォルトのコンフィギュレーションモードは、デフォルト VRF に適用されます。

# PIM の注意事項と制約事項

PIM には、次の注意事項と制限事項があります。

- Cisco Nexus 3600 プラットフォーム スイッチは、vPC レッグまたは vPC の背後にあるルータとの PIM 隣接関係をサポートしていません。
- マルチキャストで RP として使用されるループバック インターフェイスには、ip pim sparse-mode 構成が必要です。これは追加の構成ガイドラインです。
- PIM は、いずれのバージョンの PIM デンス モードまたは PIM スパース モード バージョン 1 とも相互運用性がありません。
- PIM6 はサポートされていません。
- PIM Bidir は、サポートされていません。
- 同じネットワーク内では、Auto-RP プロトコルと BSR プロトコルを同時に構成しないことをお勧めします。
- 候補 RP インターバルを 15 秒以上に設定してください。
- PIM は、PIM Anycast-RP に使用されるループバック インターフェイス上に構成する必要があります。
- PIM では、VRF-Lite (インポートまたはエクスポートなし) のみがサポートされます。

# PIM のデフォルト設定

次の表に、PIM パラメータのデフォルト設定を示します。

表 1: PIM パラメータのデフォルト設定

パラメータ	デフォルト
共有ツリーだけを使用	無効
再起動時にルートをフラッシュ	無効
ネイバーの変更の記録	無効
Auto-RP メッセージアクション	無効
BSR メッセージアクション	無効
SSM マルチキャストグループ範囲またはポリシー	IPv4 の場合 232.0.0.0/8
PIM スパース モード	無効

パラメータ	デフォルト
DR プライオリティ	0
hello 認証モード	無効
ドメイン境界	無効
RP アドレス ポリシー	メッセージをフィルタリングしない
PIM Register メッセージ ポリシー	メッセージをフィルタリングしない
BSR 候補 RP ポリシー	メッセージをフィルタリングしない
BSR ポリシー	メッセージをフィルタリングしない
Auto-RP マッピング エージェント ポリシー	メッセージをフィルタリングしない
Auto-RP 候補 RP ポリシー	メッセージをフィルタリングしない
Join/Prune ポリシー	メッセージをフィルタリングしない
ネイバーとの隣接関係ポリシー	すべての PIM ネイバーと隣接関係を確立

## PIM の構成

PIM は、各インターフェイスに設定できます。



(注) Cisco NX-OS がサポートしているのは PIM スペース モードのバージョン 2 です。このマニュアルで PIM と記載されている場合は、PIM スペース モードのバージョン 2 を意味しています。

下のテーブルで説明されているマルチキャスト配信モードを使用すると、PIM ドメインに、それぞれ独立したアドレス範囲を構成できます。

表 2: PIM のマルチキャスト配信モード

マルチキャスト配信モード	RP 設定の必要性	説明
アーキテクチャセールスマネージャ (ASM)	はい	任意の送信元のマルチキャスト
SSM	いいえ	单一送信元のマルチキャスト
マルチキャスト用 RPF ルート	いいえ	マルチキャスト用 RPF ルート

## PIM 機能の有効化

PIM を設定する手順は、次のとおりです。

### 手順

**ステップ1** 「PIM のマルチキャスト配信モード」のテーブルに示したマルチキャスト配信モードについて、各モードで構成するマルチキャストグループの範囲を選択します。

**ステップ2** PIM または PIM6 機能を有効にします。 「PIM 機能の有効化」セクションを参照してください。

**ステップ3** PIM ドメインに参加させる各インターフェイスで、PIM スパース モードを設定します。 「PIM スパース モードの構成」セクションを参照してください。

**ステップ4** ステップ1で選択したマルチキャスト配信モードについて、次の設定作業を行います。

- ASM モードについては、「ASM の構成」セクションを参照してください。
- SSM モードについては、「SSM の構成」セクションを参照してください。
- マルチキャスト用 RPF ルートについては、「マルチキャスト用 RPF ルートの構成」セクションを参照してください。

**ステップ5** メッセージフィルタリングを構成する場合。「メッセージフィルタリングの構成」セクションを参照してください。

## PIM 機能の有効化

PIM コマンドにアクセスするには、PIM 機能をイネーブルにしておく必要があります。

### 始める前に

LAN Base Services ライセンスがインストールされていることを確認してください。

### 手順

	コマンドまたはアクション	目的
<b>ステップ1</b>	<b>configure terminal</b>  例： <pre>switch# configure terminal</pre> <pre>switch(config)#</pre>	コンフィギュレーション モードに入ります。
<b>ステップ2</b>	<b>feature pim</b>  例： <pre>switch(config)# feature pim</pre>	PIM をイネーブルにします。デフォルトではPIMはディセーブルになっています。

	コマンドまたはアクション	目的
ステップ 3	(任意) <b>show running-configuration pim</b> 例： switch(config)# <b>show running-configuration pim</b>	<b>feature</b> コマンドを含む PIM の実行コンフィギュレーション情報を表示します。
ステップ 4	(任意) <b>copy running-config startup-config</b> 例： switch(config)# <b>copy running-config startup-config</b>	設定変更を保存します。

## PIM スパース モードの設定

スパース モード ドメインに参加させる各スイッチインターフェイスで、PIM スパース モードを設定します。



(注) マルチキャストルートマップの構成に関する詳細は、「RP 情報配信を制御するためのルートマップの構成」セクションを参照してください。



(注) join-prune ポリシーを構成するには、「メッセージ フィルタリングの構成」セクションを参照してください。

### 始める前に

LAN Base Services ライセンスがインストールされていること、および PIM がイネーブル化されていることを確認します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#[	コンフィギュレーション モードに入ります。
ステップ 2	(任意) <b>ip pim auto-rp {listen [forward]   forward [listen]}</b> 例： switch(config)# <b>ip pim auto-rp listen</b>	Auto-RP メッセージの待ち受けまたは転送をイネーブルにします。デフォルトではこれらの機能がディセーブルになっているため、Auto-RP メッセージの受信と転送は行われません。

## ■ PIM スパース モードの設定

	コマンドまたはアクション	目的
ステップ 3	(任意) <b>ip pim bsr {listen [forward]   forward [listen]}</b> 例： switch(config)# <b>ip pim bsr forward</b>	BSR メッセージの待ち受けまたは転送をイネーブルにします。デフォルトではこれらの機能がディセーブルになっているため、BSR メッセージの待ち受けまたは転送は行われません。
ステップ 4	(任意) <b>ip pim rp [ip prefix] vrf vrf-name  all</b> 例： switch(config)# <b>show ip pim rp</b>	Auto-RP および BSR の受信/転送ステートなど、PIM RP 情報を表示します。
ステップ 5	(任意) <b>ip pim register-rate-limit rate</b> 例： switch(config)# <b>ip pim register-rate-limit 1000</b>	レート制限を毎秒のパケット数で設定します。指定できる範囲は 1 ~ 65,535 です。デフォルト設定は無制限です。
ステップ 6	(任意) <b>show running-configuration pim</b> 例： switch(config)# <b>show running-configuration pim</b>	Register レート制限を含めた PIM の実行コンフィギュレーション情報を表示します。
ステップ 7	<b>interface interface</b> 例： switch(config)# <b>interface ethernet 2/1</b> switch(config-if)#	<b>ethernet slot/port</b> などのインターフェイスタイプおよび番号を入力して、インターフェイスモードを開始します。
ステップ 8	<b>no switchport</b> 例： sswitch(config-if)# <b>no switchport</b>	そのインターフェイスを、レイヤ 3 ルーティングインターフェイスとして設定します。
ステップ 9	<b>ip pim sparse-mode</b> 例： switch(config-if)# <b>ip pim sparse-mode</b>	現在の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。デフォルトではディセーブルになっています。
ステップ 10	(任意) <b>ip pim dr-priority priority</b> 例： switch(config-if)# <b>ip pim dr-priority 192</b>	PIM hello メッセージの一部としてアドバタイズされる指定ルータ (DR) プライオリティを設定します。有効範囲は 1 ~ 4294967295 です。デフォルトは 1 です。
ステップ 11	(任意) <b>ip pim hello-authentication ah-md5 auth-key</b> 例： switch(config-if)# <b>ip pim hello-authentication ah-md5 my_key</b>	PIM hello メッセージ内の MD5 ハッシュ認証キーをイネーブルにします。暗号化されていない (クリアテキストの) キーか、または次に示す値のいずれかを入力したあと、スペースと MD5 認証キーを入力します。 • 0 : 暗号化されていない (クリアテキスト) キーを指定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• 3 : 3-DES 暗号化キーを指定します。</li> <li>• 7 : Cisco Type 7 暗号化キーを指定します。</li> </ul>
ステップ 12	<p>(任意) <b>ip pim hello-authentication keychain name</b></p> <p>例 :</p> <pre>switch(config-if)# ip pim hello-authentication keychain mykeychain</pre>	<p>PIM インターフェイスでキーチェーン認証を有効にします。ここで &lt;keychain&gt; はキーチェーンの名前です。</p> <p>(注)</p> <ul style="list-style-type: none"> <li>• キーチェーンを設定する前でも、特定のキーチェーン名を使用して認証を設定できますが、認証が成功するのは有効なキーとともにキーチェーンが存在する場合だけです。</li> <li>• キーチェーン認証が構成されている場合、古いパスワードベースの認証は（存在する場合でも）無視されます。</li> </ul>
ステップ 13	<p>(任意) <b>ip pim hello-interval interval</b></p> <p>例 :</p> <pre>switch(config-if)# ip pim hello-interval 25000</pre>	<p>hello メッセージの送信インターバルを、ミリ秒単位で設定します。範囲は 1 ~ 4294967295 です。デフォルト値は 30000 です。</p> <p>(注)</p> <p>最小値は 1 ミリ秒です。</p>
ステップ 14	<p>(任意) <b>ip pim border</b></p> <p>例 :</p> <pre>switch(config-if)# ip pim border</pre>	<p>インターフェイスを PIM ドメインの境界として設定し、対象のインターフェイスで、ブートストラップ、候補 RP、または Auto-RP の各メッセージが送受信されないようにします。デフォルトではディセーブルになっています。</p>
ステップ 15	<p>(任意) <b>ip pim neighbor-policy policy name</b></p> <p>例 :</p> <pre>switch(config-if)# ip pim neighbor-policy my_neighbor_policy</pre>	<p><b>match ip address</b> コマンドを使用し、ルートマップポリシーに基づいてどの PIM ネイバーと隣接関係になるかを構成します。ポリシーネームの文字数は最大 63 文字です。デフォルトでは、すべての PIM ネイバーと隣接関係が確立されます。</p> <p>(注)</p> <p>この機能の設定は、経験を積んだネットワーク管理者が行うことをお勧めします。</p>
ステップ 16	<p>(任意) <b>show ip pim interface [interface   brief] [vrf vrf-name   all]</b></p> <p>例 :</p> <pre>switch(config-if)# show ip pim interface</pre>	PIM インターフェイスの情報を表示します。

## ASM を構成

	コマンドまたはアクション	目的
ステップ 17	(任意) <b>copy running-config startup-config</b> 例： switch(config-if)# <b>copy running-config startup-config</b>	設定変更を保存します。

## ASM を構成

Any Source Multicast (ASM) は、マルチキャストデータの送信元と受信者の間に、共通のルートとして動作する RP 使用の設定が必要なマルチキャスト配信モードです。

ASM または モードを構成するには、スパース モードおよび RP の選択方式を設定します。RP の選択方式では、配信モードを指定して、マルチキャスト グループの範囲を割り当てます。

## 静的 RP の設定

RP を静的に設定するには、PIM ドメインに参加するルータのそれぞれに RP アドレスを設定します。

**match ip multicast** コマンドとともに使用するグループ プレフィックスにリスト化されるルートマップ ポリシー名を指定できます。



(注) RP アドレスは、ループバック インターフェイスを使用することを推奨します。

## 始める前に

Enterprise Services ライセンスがインストールされていること、および PIM がイネーブルになっていることを確認してください。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	<b>ip pim rp-address rp-address [group-list ip-prefix   route-map policy-name]</b> 例： switch(config)# <b>ip pim rp-address 192.0.2.33 group-list 224.0.0.0/9</b>	マルチキャスト グループ範囲に、PIM スタティック RP アドレスを設定します。 <b>match ip multicast</b> コマンドとともに使用するグループ プレフィックスにリスト化されるルートマップ ポリシー名を指定できます。 デフォルト モードは ASM です。 デフォルトの グループ範囲は 224.0.0.0 ~ 239.255.255.255 です。

	コマンドまたはアクション	目的
		この例では、指定したグループ範囲に PIM ASM モードを設定しています。
ステップ 3	(任意) <b>show ip pim group-range [ip-prefix   vrf vrf-name   all]</b> 例： switch(config)# <b>show ip pim group-range</b>	PIM モードとグループ範囲を表示します。
ステップ 4	(任意) <b>copy running-config startup-config</b> 例： switch(config)# <b>copy running-config startup-config</b>	設定変更を保存します。

## BSR の設定

BSR を設定するには、候補 BSR および候補 RP を選択します。



(注) 同じネットワーク内では、Auto-RP プロトコルと BSR プロトコルを同時に構成しないことをお勧めします。

候補 BSR の構成では、引数を指定できます（次の表を参照）。

表 3: 候補 BSR の引数

引数	説明
<i>interface</i>	ブートストラップメッセージで使用する、BSR 送信元 IP アドレスを取得するためのインターフェイスタイプおよび番号。
<i>hash-length</i>	ハッシュ長は、マスクを適用するために使用される上位桁の 1 の個数です。マスクでは、候補 RP のグループアドレス範囲の論理積をとることにより、ハッシュ値を算出します。マスクは、グループ範囲が等しい一連の RP に割り当たられる連続アドレスの個数を決定します。PIM の場合、この値の範囲は 0 ~ 32 であり、デフォルト値は 30 秒です。
<i>priority</i>	現在の BSR に割り当たされたプライオリティ。ソフトウェアにより、プライオリティが最も高い BSR が選定されます。BSR プライオリティが等しい場合は、IP アドレスが最上位の BSR が選定されます。この値の範囲は 0 (プライオリティが最小) ~ 255 であり、デフォルト値は 64 です。

候補 RP を表 4 で説明されている引数とキーワードで構成できます。

表 4: BSR 候補 RP の引数およびキーワード

引数またはキーワード	説明
<i>interface</i>	ポートストラップメッセージで使用する、BSR 送信元 IP アドレスを取るためのインターフェイスタイプおよび番号。
<b>group-list ip-prefix</b>	プレフィックス形式で指定された、この RP によって処理されるマルチストグループ。
<i>interval</i>	候補 RP メッセージの送信間隔 (秒)。この値の範囲は 1 ~ 65,535 であります。デフォルト値は 60 秒です。 (注) 候補 RP インターバルは 15 秒以上に設定することを推奨します。
<i>priority</i>	現在の RP に割り当てられたプライオリティ。ソフトウェアにより、グループ範囲内で優先度が最も高い RP が選定されます。優先度が等しい場合、IP アドレスが最上位の RP が選定されます。(最も高い優先度は最も低い値です。) この値の範囲は 0 (優先度が最大) ~ 255 であります。デフォルト値は 192 です。 (注) この優先度は BSR の BSR 候補の優先度とは異なります。BSR 候補の優先度は 0 ~ 255 の間で、大きい値ほど優先度が高くなります。



**ヒント** 候補 BSR および候補 RP は、PIM ドメインのすべての箇所と適切に接続されている必要があります。

BSR および候補 RP には同じルータを指定できます。多数のルータが設置されたドメインでは、複数の候補 BSR および候補 RP を選択することにより、BSR または RP に障害が発生した場合に、自動的に代替 BSR または代替 RP へとフェールオーバーすることができます。

候補 BSR および候補 RP を設定する手順は、次のとおりです。

1. PIM ドメインの各ルータで BSR メッセージの受信と転送を行うかどうかを設定します。候補 RP または候補 BSR として設定されたルータは、インターフェイスにドメイン境界機能が設定されていない場合、すべての BSR プロトコルメッセージの受信と転送を自動的に実行します。詳細については、「[PIM スペース モードの構成](#)」セクションを参照してください。
2. 候補 BSR および候補 RP として動作するルータを選択します。
3. 後述の手順に従い、候補 BSR および候補 RP をそれぞれ設定します。
4. BSR メッセージフィルタリングを設定します。「[メッセージフィルタリングの構成](#)」セクションを参照してください。

## BSR の設定

## 始める前に

Enterprise Services ライセンスがインストールされていること、およびPIM がイネーブルになっていることを確認してください。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config) #</pre>	コンフィギュレーション モードに入ります。
ステップ 2	<b>ip pim [bsr] bsr-candidate interface [hash-len hash-length] [priority priority]</b>  例： <pre>switch(config)# ip pim bsr-candidate ethernet 2/1 hash-len 24</pre>	候補ブートストラップ ルータ (BSP) を設定します。ブートストラップ メッセージで使用される送信元 IP アドレスは、インターフェイスの IP アドレスです。ハッシュ長は 0 ~ 32 であり、デフォルト値は 30 です。プライオリティは 0 ~ 255 であり、デフォルト値は 64 です。パラメータの詳細については、テーブル 10 を参照してください。
ステップ 3	<b>ip pim [bsr] rp-candidate interface group-list ip-prefix route-map policy-name priority priority interval interval</b>  例： <pre>switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24</pre>	BSR の候補 RP を設定します。プライオリティは 0 (プライオリティが最大) ~ 65,535 であり、デフォルト値は 192 です。インターバルは 1 ~ 65,535 秒であり、デフォルト値は 60 秒です。  (注) 候補 RP インターバルは 15 秒以上に設定することを推奨します。  この例では、ASM の候補 RP を設定しています。
ステップ 4	(任意) <b>show ip pim group-range [ip-prefix] [ vrf vrf-name   all]</b>  例： <pre>switch(config)# show ip pim group-range</pre>	PIM モードとグループ範囲を表示します。
ステップ 5	(任意) <b>copy running-config startup-config</b>  例： <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## Auto-RP の設定

Auto-RP を設定するには、候補マッピング エージェントおよび候補 RP を選択します。マッピング エージェントおよび候補 RP には同じルータを指定できます。



**注意** 同じネットワーク内では、Auto-RP プロトコルと BSR プロトコルを同時に設定できません。

Auto-RP マッピング エージェントの設定では、引数を指定できます。次の表を参照してください。

表 5: Auto-RP マッピング エージェントの引数

引数	説明
<i>interface</i>	ブートストラップ メッセージで使用する、Auto-RP マッピング エージェントの IP アドレスを取得するためのインターフェイス タイプおよび番号。
<b>scope ttl</b>	RP-Discovery メッセージが転送される最大ホップ数を表す存続可能時間 (TTL) 値。この値の範囲は 1 ~ 255 であり、デフォルト値は 32 です。 (注) <a href="#">「PIM スパース モードの構成」セクション</a> の境界 ドメイン 機能を参照してください。

複数の Auto-RP マッピング エージェントを設定した場合、1 つだけがドメインのマッピング エージェントとして選定されます。選定されたマッピング エージェントは、すべての候補 RP メッセージを配信します。すべてのマッピング エージェントが配信された候補 RP メッセージを受信し、受信した RP キャッシュを、RP-Discovery メッセージの一部としてアドバタイズします。

候補 RP の構成では、引数およびキーワードを指定できます (次の表を参照)。

表 6: Auto-RP 候補 RP の引数とキーワード

引数またはキーワード	説明
<i>interface</i>	ブートストラップ メッセージで使用する、候補 RP の IP アドレスを取得するためのインターフェイス タイプおよび番号。
<b>group-list ip-prefix</b>	現在の RP で処理されるマルチキャスト グループ。プレフィックス 形式で指定します。

引数またはキーワード	説明
<b>scope ttl</b>	RP-Discovery メッセージが転送される最大ホップ数を表す存続時間 (TTL) 値。この値の範囲は 1 ~ 255 であり、デフォルト値は 32 です。 (注) 「 <a href="#">PIM スペース モードの構成</a> 」セクションの境界ドメイン機能を参照してください。
<b>interval</b>	RP-Announce メッセージの送信間隔 (秒)。この値の範囲は 65,535 であり、デフォルト値は 60 です。 (注) 候補 RP インターバルは 15 秒以上に設定することを推奨します。



**ヒント** マッピング エージェントおよび候補 RP は、PIM ドメインのすべての箇所と適切に接続されている必要があります。

Auto-RP マッピング エージェントおよび候補 RP を設定する手順は、次のとおりです。

1. PIM ドメインの各ルータで、Auto-RP メッセージの受信と転送を行うかどうかを設定します。候補 RP または Auto-RP マッピング エージェントとして設定されたルータは、インターフェイスにドメイン境界機能が設定されていない場合、すべての Auto-RP プロトコルメッセージの受信と転送を自動的に実行します。詳細については、「[PIM スペース モードの構成](#)」セクションを参照してください。
2. マッピング エージェントおよび候補 RP として動作するルータを選択します。
3. 後述の手順に従い、マッピング エージェントおよび候補 RP をそれぞれ設定します。
4. Auto-RP メッセージフィルタリングを設定します。「[メッセージフィルタリングの構成](#)」セクションを参照してください。

## Auto RP の構成

### 始める前に

Enterprise Services ライセンスがインストールされていること、および PIM がイネーブルになっていることを確認してください。

## ■ PIM エニーキャスト RP セットの設定 (PIM)

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config) #</pre>	コンフィギュレーションモードに入ります。
ステップ 2	<b>ip pim {send-rp-discovery   auto-rp mapping-agent}</b> <i>interface [scope ttl]</i>  例： <pre>switch(config) # ip pim auto-rp mapping-agent ethernet 2/1</pre>	Auto-RP マッピング エージェントを設定します。 Auto-RP Discovery メッセージで使用される送信元 IP アドレスは、インターフェイスの IP アドレスです。 デフォルト スコープは 32 です。パラメータの詳細については、「自動 RP マッピング エージェントの引数」の表を参照してください。
ステップ 3	<b>ip pim {send-rp-announce   {auto-rp rp-candidate}}</b> <i>interface group-list ip-prefix [scope ttl] [interval interval] [bidir]</i>  例： <pre>switch(config) # ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24</pre>	Auto-RP の候補 RP を設定します。デフォルト スコープは 32 です。デフォルト インターバルは 60 秒です。デフォルトでは、ASM の候補 RP が作成されます。パラメータの詳細については、「自動 RP 候補 RP の引数とキーワード」の表を参照してください。  (注) 候補 RP インターバルは 15 秒以上に設定することを推奨します。  この例では、ASM の候補 RP を構成しています。
ステップ 4	(任意) <b>show ip pim group-range [ip-prefix   vrf-name   all]</b>  例： <pre>switch(config) # show ip pim group-range</pre>	PIM モードとグループ範囲を表示します。
ステップ 5	(任意) <b>copy running-config startup-config</b>  例： <pre>switch(config) # copy running-config startup-config</pre>	設定変更を保存します。

## PIM エニーキャスト RP セットの設定 (PIM)

PIM Anycast-RP セットを設定する手順は、次のとおりです。

ステップ 1 PIM エニーキャスト RP セット内のルータを選択します。

ステップ 2 PIM エニーキャスト RP セットの IP アドレスを選択します。

ステップ 3 このセクションの説明に従って、PIM エニーキャスト RP セット内の各ピア RP およびローカルアドレスを構成します。

## 始める前に

Enterprise Services ライセンスがインストールされていること、および PIM がイネーブルになっていることを確認してください。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例：  switch# <b>configure terminal</b> switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>interface loopback number</b>  例：  switch(config)# <b>interface loopback 0</b> switch(config-if)#	インターフェイス ループバックを設定します。  この例では、インターフェイス ループバックを 0 に設定しています。
ステップ 3	<b>ip address ip-prefix</b>  例：  switch(config-if)# <b>ip address 192.168.1.1/32</b>	このインターフェイスの IP アドレスを設定します。  この例では、Anycast-RP の IP アドレスを設定しています。
ステップ 4	<b>ip pim sparse-mode</b>  例：  switch(config-if)# <b>ip pim sparse-mode</b>	現在の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。デフォルトではディセーブルになっています。
ステップ 5	<b>exit</b>  例：  switch(config)# <b>exit</b>	コンフィギュレーション モードに戻ります。
ステップ 6	<b>ip pim anycast-rp anycast-rp-address anycast-rp-peer-address</b>  例：  switch(config)# <b>ip pim anycast-rp 192.0.2.3</b> 192.0.2.31  switch(config)# <b>ip pim anycast-rp 192.0.2.3</b> 192.0.2.32	指定した Anycast-RP アドレスに対応する PIM Anycast-RP ピア アドレスを設定します。各コマンドで同じ Anycast-RP アドレスを指定して実行すると、Anycast-RP セットが作成されます。RP の IP アドレスは、同一セット内の RP との通信に使用されます。  この例は、192.0.2.31 と 192.0.2.32 の Anycast-RP セットを示しており、ネットワークで使用される Anycast-RP は 192.0.2.3 になります。
ステップ 7	Anycast-RP セットに属する各ピア RP で、同じ Anycast-RP アドレスを使用してステップ 6 を繰り返します。	—
ステップ 8	<b>show ip pim group-range [ ip-prefix ] [ vrf { vrf-name   all } ]</b>	PIM モードとグループ範囲を表示します。

## ■ ASM 専用の共有ツリーの設定

	コマンドまたはアクション	目的
ステップ 9	<b>copy running-config startup-config</b>  例： <code>switch(config) # copy running-config startup-config</code>	設定変更を保存します。

## ASM 専用の共有ツリーの設定

共有ツリーを構成できるのは、Any Source Multicast (ASM) グループの最終ホップルータだけです。この場合、新たな受信者がアクティブグループに加入した場合、このルータでは共有ツリーから SPT へのスイッチオーバーは実行されません。**match ip[v6] multicast** コマンドを使用して、共有ツリーの使用を強制するグループ範囲を指定できます。このオプションは、送信元ツリーに対する Join/Prune メッセージを受信した場合の、ルータの標準動作には影響を与えません。

デフォルトではこの機能がディセーブルになっているため、ソフトウェアは送信元ツリーへのスイッチオーバーを行います。



(注) ASM モードでは、最終ホップルータだけが共有ツリーから SPT に切り替わります。

### 始める前に

Enterprise Services ライセンスがインストールされていること、および PIM がイネーブルになっていることを確認してください。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： <code>switch# configure terminal</code> <code>switch(config) #</code>	コンフィギュレーションモードに入ります。
ステップ 2	<b>ip pim use-shared-tree-only group-list policy-name</b>  例： <code>switch(config) # ip pim use-shared-tree-only</code> <code>group-list my_group_policy</code>	共有ツリーだけを構築します。共有ツリーから SPT へのスイッチオーバーは実行されません。 <b>match ip multicast</b> コマンドで、使用するグループを示すルートマップポリシー名を指定します。デフォルトでは、送信元に対する (*, G) ステートのマルチキャストパケットを受信すると、ソフトウェアは PIM (S, G) Join メッセージを送信元方向に発信します。
ステップ 3	(任意) <b>show ip pim group-range [ip-prefix   vrf vrf-name   all]</b>	PIM モードとグループ範囲を表示します。

	コマンドまたはアクション	目的
	例： switch(config)# <b>show ip pim group-range</b>	
ステップ 4	(任意) <b>copy running-config startup-config</b>  例： switch(config-if)# <b>copy running-config startup-config</b>	設定変更を保存します。

## マルチキャストルーティング テーブルの最大エントリ数の設定

マルチキャストルーティング テーブル (MRT) の最大エントリ数を設定できます。

### 始める前に

Enterprise Services ライセンスがインストールされていること、および PIM がイネーブルになっていることを確認してください。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： switch# configure terminal switch(config)#[/td> <td>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。</td>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>hardware profile multicast max-limit max-entries</b>  例： switch(config)# hardware profile multicast max-limit 3000	マルチキャストルーティング テーブルの最大エントリ数を設定します。  マルチキャストルーティング テーブルの最大エントリ数の範囲は 0 ~ 8000 です。
ステップ 3	(任意) <b>show hardware profile status</b>  例： switch(config)# show hardware profile status	マルチキャストルーティング テーブル制限の情報を表示します。
ステップ 4	(任意) <b>copy running-config startup-config</b>  例： switch(config)# copy running-config startup-config	設定変更を保存します。

## SSM (PIM) の設定

Source-Specific Multicast (SSM) は、マルチキャスト送信元にデータを要求する受信者に対して、接続された DR 上のソフトウェアが対象の送信元への最短パスツリー (SPT) を構築するマルチキャスト配信モードです。

IPv4 ネットワーク上のホストから、送信元を特定してマルチキャストデータを要求するには、このホストおよびこのホストの DR で、IGMPv3 が実行されている必要があります。SSM モードでインターフェイスに PIM を設定する場合は、IGMPv3 をイネーブルにするのが一般的です。IGMPv1 または IGMPv2 が実行されているホストでは、SSM 変換を使用して、グループと送信元のマッピング設定を行うことができます。詳細については、「[IGMP の設定](#)」を参照してください。

コマンドラインで値を指定して、SSM で使用されるグループ範囲を構成できます。デフォルトでは、PIM に対する SSM グループ範囲は 232.0.0.0/8 です。

**match ip multicast** コマンドとともに使用するグループプレフィックスにリスト化されるルートマップポリシー名を指定できます。



(注) デフォルトの SSM グループ範囲を使用する場合は、SSM グループ範囲の設定は不要です。

### 始める前に

LAN Base Services ライセンスがインストールされていること、および PIM がイネーブル化されていることを確認します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# configure terminal switch(config)#	グローバルコンフィギュレーションモードを開始します。
ステップ 2	<b>[no] ip pim ssm {prefix-list name   range {ip-prefix   none}   route-map policy-name}</b> 例： switch(config)# ip pim ssm range 239.128.1.0/24 例： switch(config)# no ip pim ssm range none	次のオプションを使用できます。 <ul style="list-style-type: none"> <li>• <b>prefix-list</b> : SSM 範囲のプレフィックスリストポリシー名を指定します。</li> <li>• <b>range</b> : SSM のグループ範囲を設定します。デフォルトの範囲は 232.0.0.0/8 です。キーワード <b>none</b> を指定すると、すべてのグループ範囲が削除されます。</li> </ul>

コマンドまたはアクション	目的
	<ul style="list-style-type: none"> <li>route-map : match ip multicast コマンドで、使用するグループプレフィックスを示すルートマップポリシー名を指定できます。</li> </ul> <p><b>no</b> オプションを指定すると、SSM 範囲から指定のプレフィックスが削除されるか、プレフィックスリストまたはルートマップポリシーが削除されます。キーワード <b>none</b> を指定すると、<b>no</b> コマンドは SSM 範囲をデフォルト値の 232.0.0.0/8 にリセットします。</p> <p>(注) prefix-list、range、または route-map コマンドを使用して、SSM マルチキャストに最大 4 つの範囲を設定できます。</p>
<b>ステップ 3</b> (任意) <b>show ip pim group-range [ip-prefix   vrf vrf-name]</b> 例： <pre>switch(config)# show ip pim group-range</pre>	PIM モードとグループ範囲を表示します。
<b>ステップ 4</b> (任意) <b>copy running-config startup-config</b> 例： <pre>switch(config)# copy running-config startup-config</pre>	設定変更を保存します。

## vPC を介した PIM SSM の設定

vPC 上での PIM SSM が、SSM 範囲内で vPC ピア上での IGMPv3 Join と PIM S,G Join をサポートするように設定します。この設定は、レイヤ 2 またはレイヤ 3 ドメインの孤立した送信元または受信者に対してサポートされています。

(S,G) エントリには、ソースへのインターフェイスとして RPF があり、MRIB では \*,G 状態が維持されません。

### 始める前に

PIM および vPC 機能が有効なことを確認します。

Enterprise Services ライセンスがインストールされていること、および PIM がイネーブルになっていることを確認してください。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config) #</pre>	グローバル構成モードを開始します。
ステップ 2	<b>vrf context name</b>  例： <pre>switch(config)# vrf context Enterprise switch(config-vrf) #</pre>	新しい VRF を作成し、VRF 設定モードを開始します。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
ステップ 3	(任意) <b>[ no] ip pim ssm { prefix-list name   range { ip-prefix   none}   route-map policy-name}</b>  例： <pre>switch(config-vrf) # ip pim ssm range 234.0.0.0/24</pre>	次のオプションを使用できます。 <ul style="list-style-type: none"> <li>prefix-list : SSM 範囲のプレフィックスリストポリシー名を指定します。</li> <li>range : SSM のグループ範囲を設定します。デフォルトの範囲は 232.0.0.0/8 です。キーワード none を指定すると、すべてのグループ範囲が削除されます。</li> <li>route-map : match ip multicast コマンドで、使用するグループプレフィックスを示すルートマップポリシー名を指定できます。</li> </ul> <p>デフォルト範囲は、次のコマンドを使用してオーバーライドできます。この例のコマンドは、デフォルトの範囲を 234.0.0.0/24 にオーバーライドします。</p> <p>no オプションを指定すると、SSM 範囲から指定のプレフィックスが削除されるか、プレフィックスリストまたはルートマップポリシーが削除されます。キーワード none を指定すると、no コマンドは SSM 範囲をデフォルト値の 232.0.0.0/8 にリセットします。</p>
ステップ 4	(任意) <b>show ip pim group-range [ ip-prefix ] [ vrf { vrf-name   all } ]</b>  例： <pre>switch(config) # show ip pim group-range</pre>	PIM モードとグループ範囲を表示します。
ステップ 5	(任意) <b>copy running-config startup-config</b>  例： <pre>switch(config) # copy running-config startup-config</pre>	設定変更を保存します。

## マルチキャスト用 RPF ルートの設定

ユニキャスト トラフィック パスを分岐させてマルチキャストデータを配信するには、マルチキャスト用 RPF ルートを定義します。境界ルータにマルチキャスト用 RPF ルートを定義すると、外部ネットワークへの Reverse Path Forwarding (RPF) がイネーブルになります。

マルチキャストルートはトラフィック転送に直接使用されるわけではなく、RPF チェックのために使用されます。マルチキャスト用 RPF ルートは再配布できません。マルチキャスト転送に関する詳細は、「[マルチキャスト転送](#)」セクションを参照してください。

### 始める前に

LAN Base Services ライセンスがインストールされていること、および PIM がイネーブル化されていることを確認します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： <pre>switch# configure terminal switch(config) #</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 2	<b>ip mroute {ip-addr mask   ip-prefix} {next-hop   nh-prefix}   [route-preference] [vrf vrf-name]</b> 例： <pre>switch(config) # ip mroute 192.0.2.33/24 192.0.2.1</pre>	RPF 計算で使用するマルチキャスト用 RPF ルートを設定します。ルート プリファレンスは 1 ~ 255 です。デフォルトのプリファレンスは 1 です。
ステップ 3	(任意) <b>show ip static-route [ vrf vrf-name]</b> 例： <pre>switch(config) # show ip static-route</pre>	設定されているスタティックルートを表示します。
ステップ 4	(任意) <b>copy running-config startup-config</b>	設定変更を保存します。

## マルチキャストマルチパスの無効化

デフォルトでは、使用可能な複数の ECMP パスがある場合、マルチキャストの RPF インターフェイスが自動的に選択されます。自動選択を無効にすると、マルチキャスト用に单一の RPF インターフェイスを指定できます。

## ■ RP 情報配信を制御するルートマップの設定

### 手順

	コマンドまたはアクション	目的
ステップ1	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config) #</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2	<b>ip multicast multipath none</b>  例： <pre>switch(config)# ip multicast multipath none</pre>	マルチキャストマルチパスの無効化
ステップ3	<b>clear ip mroute * vrf all</b>  例： <pre>switch(config)# clear ip mroute * vrf all</pre>	マルチパスルートをクリアし、マルチキャストマルチパス抑制をアクティブにします。

## RP 情報配信を制御するルートマップの設定

ルートマップは、一部の RP 設定のミスや悪意のある攻撃に対する保護機能を提供します。このセクションで説明されているコマンドのルートマップを使用します。

ルートマップを設定すると、ネットワーク全体について RP 情報の配信を制御できます。各クライアントルータで発信元の BSR またはマッピングエージェントを指定したり、各 BSR およびマッピングエージェントで、アドバタイズされる（発信元の）候補 RP のリストを指定したりできるため、目的の情報だけが配信されるようになります。



(注) **match ipv6 multicast** コマンドのみがルートマップで効果があります。

### 始める前に

Enterprise Services ライセンスがインストールされていること、および PIM6 がイネーブルになっていることを確認してください。

### 手順

	コマンドまたはアクション	目的
ステップ1	<b>configure terminal</b>  例： <pre>switch# configure terminal switch(config) #</pre>	コンフィギュレーションモードに入ります。

	コマンドまたはアクション	目的
ステップ 2	<b>route-map map-name [permit   deny] [sequence-number]</b> 例： <pre>switch(config)# route-map ASM_only permit 10 switch(config-route-map) #</pre>	ルートマップ コンフィギュレーションモードを開始します。構成方法は <b>permit</b> キーワードを使用します。
ステップ 3	<b>match ip multicast {rp ip-address [rp-type rp-type] [group ip-prefix]}   {group ip-prefix rp ip-address [rp-type rp-type]}</b> 例： <pre>switch(config)# match ip multicast group 224.0.0.4 rp 0.0.0.0/0 rp-type ASM</pre>	指定したグループ、RP、およびRP タイプを関連付けます。ユーザは RP のタイプ (ASM または Bidir) を指定できます。例で示すとおり、このコンフィギュレーションモードでは、グループおよび RP を指定する必要があります。
ステップ 4	(任意) <b>show route-map</b> 例： <pre>switch(config-route-map) # show route-map</pre>	設定済みのルートマップを表示します。
ステップ 5	(任意) <b>copy running-config startup-config</b> 例： <pre>switch(config-route-map) # copy running-config startup-config</pre>	設定変更を保存します。

## メッセージ フィルタリングの設定

次の表に、PIM および PIM6 でのメッセージ フィルタ処理の構成方法を示します。

表 7: PIM および PIM6 でのメッセージ フィルタリング

メッセージの種類	説明
スイッチに対しグローバル	
PIM Register ポリシー	PIM 登録メッセージをルートマップ ポリシーに基づいてフィルタリングできるようにし、この <b>match ip multicast</b> コマンドでグループまたはグループと送信元アドレスを指定できます。このポリシーは、RP として動作するルータに適用されます。デフォルトではこの機能がディセーブルになっているため、PIM Register メッセージのフィルタリングは行われません。
BSR 候補 RP ポリシー	ルートマップ ポリシーに基づく、BSR 候補 RP メッセージのフィルタリングを有効にします。 <b>match ip multicast</b> コマンドで、RP、グループアドレス、およびタイプ (ASM) を指定できます。このコマンドは、BSR の選定対象のルータで使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。

## ■ メッセージ フィルタリングの設定

メッセージの種類	説明
BSR ポリシー	ルートマップ ポリシーに基づく、BSR クライアント ルータによる BSR メッセージのフィルタリングをイネーブルにします。 <b>match ip multicast</b> コマンドで、BSR 送信元アドレスを指定できます。このコマンドは、BSR メッセージを受信するクライアント ルータで使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。
Auto-RP 候補 RP ポリシー	ルートマップ ポリシーに基づいた Auto-RP マッピング エージェントで Auto-RP 通知メッセージをフィルタリングできるようにし、 <b>match ip multicast</b> コマンドで RP アドレスとグループアドレスおよびタイプ ASM を指定できるようにします。このコマンドは、マッピング エージェントで使用できます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。
Auto-RP マッピング エージェント ポリシー	ルートマップ ポリシーに基づく、クライアント ルータによる Auto-RP Discovery メッセージのフィルタリングをイネーブルにします。 <b>match ip multicast</b> コマンドで、マッピング エージェント 送信元アドレスを指定できます。このコマンドは、Discovery メッセージを受信するクライアント ルータで使用できます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。
スイッチ インターフェイスごと	
Join/Prune ポリシー	ルートマップ ポリシーに基づく、Join/Prune メッセージのフィルタリングをイネーブルにします。 <b>match ip[v6] multicast</b> コマンドで、グループ、グループと送信元、またはグループと RP アドレスを指定できます。デフォルトでは、Join/Prune メッセージはフィルタリングされません。

マルチキャスト ルートマップの構成に関する詳細は、「[RP 情報配信を制御するためのルートマップの構成](#)」セクションを参照してください。

## メッセージ フィルタリングの設定

### 始める前に

Enterprise Services ライセンスがインストールされていること、および PIM がイネーブルになっていることを確認してください。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 :	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
	switch# <b>configure terminal</b> switch(config)#	
ステップ 2	(任意) <b>ip pim register-policy</b> <i>policy-name</i>  例： switch(config)# ip pim register-policy my_register_policy	ルートマップ ポリシーに基づく、PIM Register メッセージのフィルタリングをイネーブルにします。 <b>match ip multicast</b> コマンドを使用して、グループまたはグループおよび送信元アドレスを指定できます。
ステップ 3	(任意) <b>ip pim bsr rp-candidate-policy</b> <i>policy-name</i>  例： switch(config)# ip pim bsr rp-candidate-policy my_bsr_rp_candidate_policy	ルートマップ ポリシーに基づく、BSR 候補 RP メッセージのフィルタリングを有効にします。 <b>match ip multicast</b> コマンドで、RP、グループアドレス、およびタイプ (ASM) を指定できます。このコマンドは、BSR の選定対象のルータで使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。
ステップ 4	(任意) <b>ip pim bsr bsr-policy</b> <i>policy-name</i>  例： switch(config)# ip pim bsr bsr-policy my_bsr_policy	ルートマップ ポリシーに基づく、BSR クライアントルータによる BSR メッセージのフィルタリングをイネーブルにします。 <b>match ip multicast</b> コマンドで、BSR 送信元アドレスを指定できます。このコマンドは、BSR メッセージを受信するクライアントルータで使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。
ステップ 5	(任意) <b>ip pim auto-rp rp-candidate-policy</b> <i>policy-name</i>  例： switch(config)# ip pim auto-rp rp-candidate-policy my_auto_rp_candidate_policy	ルートマップ ポリシーに基づいた Auto-RP マッピングエージェントで Auto-RP 通知メッセージをフィルタリングできるようにし、 <b>match ip multicast</b> コマンドで RP アドレスとグループアドレスを指定できるようにします。このコマンドは、マッピングエージェントで使用できます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。
ステップ 6	(任意) <b>ip pim auto-rp mapping-agent-policy</b> <i>policy-name</i>  例： switch(config)# ip pim auto-rp mapping-agent-policy my_auto_rp_mapping_policy	ルートマップ ポリシーに基づく、クライアントルータによる Auto-RP Discovery メッセージのフィルタリングをイネーブルにします。 <b>match ip multicast</b> コマンドで、マッピングエージェント送信元アドレスを指定できます。このコマンドは、Discovery メッセージを受信するクライアントルータで使用できます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。
ステップ 7	<b>interface</b> <i>interface</i>  例： switch(config)# interface ethernet 2/1 switch(config-if) #	指定したインターフェイスでインターフェイスモードを開始します。

## ルートのフラッシュ

	コマンドまたはアクション	目的
ステップ 8	<b>no switchport</b> 例： switch(config-if)# <b>no switchport</b>	そのインターフェイスを、レイヤ3ルーティングインターフェイスとして設定します。
ステップ 9	(任意) <b>ip pim jp-policy policy-name [in   out]</b> 例： switch(config-if)# ip pim jp-policy my_jp_policy	ルートマップ ポリシーに基づく、Join/Prune メッセージのフィルタリングを有効にします。 <b>match ip multicast</b> コマンドで、グループ、グループと送信元、またはグループと RP アドレスを指定できます。 デフォルトでは、Join/Prune メッセージはフィルタリングされません。 このコマンドは、送信および着信の両方向のメッセージをフィルタリングします。
ステップ 10	(任意) <b>show run pim</b> 例： switch(config-if)# <b>show run pim</b>	PIM 構成コマンドを表示します。
ステップ 11	(任意) <b>copy running-config startup-config</b> 例： switch(config-if)# <b>copy running-config startup-config</b>	設定変更を保存します。

## ルートのフラッシュ

フラッシュされたルートは、Multicast Routing Information Base (MRIB) および Multicast Forwarding Information Base (MFIB) から削除されます。

PIM を再起動すると、次の処理が実行されます：

- PIM データベースが削除されます。
- MRIB および MFIB は影響を受けず、トラフィックは引き続き転送されます。
- マルチキャスト ルートの所有権が MRIB 経由で検証されます。
- ネイバーから定期的に送信される PIM Join メッセージおよび Prune メッセージを使用して、データベースにデータが再度読み込まれます。

## 始める前に

LAN Base Services ライセンスがインストールされていること、および PIM がイネーブル化されていることを確認します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>restart pim</b> 例： switch# restart pim	PIM プロセスを再起動します。
ステップ 2	<b>configure terminal</b> 例： switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 3	<b>ip pim flush-routes</b> 例： switch(config)# ip pim flush-routes	PIM プロセスの再起動時に、ルートを削除します。 デフォルトでは、ルートはフラッシュされません。
ステップ 4	<b>show running-configuration pim</b> 例： switch(config)# show running-configuration pim	<b>flush-routes</b> コマンドを含む、PIM 実行コンフィギュレーション情報をお示します。
ステップ 5	<b>copy running-config startup-config</b> 例： switch(config)# copy running-config startup-config	設定変更を保存します。

## PIM 設定の確認

PIM の設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
<b>show ip mroute { source   group [ source ] } [ vrf vrf-name   all ]</b>	IP マルチキャストルーティング テーブルを表示します。
<b>show ip pim group-range [ vrf vrf-name   all ]</b>	学習済みまたは設定済みのグループ範囲およびモードを表示します。同様の情報については、 <b>show ip pim rp</b> コマンドを参照してください。
<b>show ip pim interface [ interface   brief ] [ vrf vrf-name   all ]</b>	情報をインターフェイス別に表示します。
<b>show ip pim neighbor [ vrf vrf-name   all ]</b>	ネイバーをインターフェイス別に表示します。
<b>show ip pim oif-list group [ source ] [ vrf vrf-name   all ]</b>	OIF リスト内のすべてのインターフェイスを表示します。

## ■ 統計の表示

コマンド	目的
<b>show ip pim route {source group   group [ source ]} [ vrf vrf-name   all ]</b>	マルチキャストルート (S、G) の PIM 加入を受信したインターフェイスなど、各マルチキャストルートの情報を表示します。
<b>show ip pim rp [ vrf vrf-name   all ]</b>	ソフトウェアの既知のランデブー ポイント (RP) およびその学習方法と、それらのグループ範囲を表示します。同様の情報については、 <b>show ip pim group-range</b> コマンドを参照してください。
<b>show ip pim rp-hash [ vrf vrf-name   all ]</b>	ブートストラップ ルータ (BSP) RP ハッシュ情報を表示します。
<b>show running-configuration pim</b>	実行コンフィギュレーション情報を表示します。
<b>show startup-configuration pim</b>	実行コンフィギュレーション情報を表示します。
<b>show ip pim vrf [ vrf-name   all ] [ detail ]</b>	各 VRF の情報を表示します。

これらのコマンドからの出力のフィールドに関する詳細は、『Cisco Nexus 3000 シリーズ コマンドリファレンス』を参照してください。

## 統計の表示

次に、PIM の統計情報を、表示およびクリアするコマンドについて説明します。

### PIM 統計情報の表示

下のテーブルにリスト化されているコマンドを使用して、PIM 統計とメモリを表示できます。PIM に **show ip** 形式のコマンドを使用します。

表 8: PIM 統計情報コマンド

コマンド	説明
<b>show ip pim policy statistics</b>	Register、RP、および Join/Prune メッセージのポリシーについて、ポリシー統計情報を表示します。

### PIM 統計情報のクリア

次の表に一覧になっているコマンドを使用して、PIM 統計情報をクリアできます。

表 9: 統計情報をクリアする PIM コマンド

コマンド	説明
<b>clear ippim interface statistics interface</b>	指定したインターフェイスのカウンタをクリアします。
<b>clear ip pim policy statistics</b>	Register、RP、およびJoin/Prune メッセージのポリシーについて、ポリシーカウンタをクリアします。
<b>clear ip pim statistics [vrf vrf-name   all]</b>	PIM プロセスで使用されるグローバルカウンタをクリアします。

## PIM の設定例

ここでは、さまざまなデータ配信モードおよび RP 選択方式を使用し、PIM を設定する方法について説明します。

## SSM の構成例

SSM モードで PIM を設定するには、PIM ドメイン内の各ルータで、次の手順を実行します。

- 手順 1: ドメインに参加させるインターフェイスで PIM スparse モードパラメータを構成します。すべてのインターフェイスで PIM をイネーブルにすることを推奨します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip pim sparse-mode
```

- ステップ 2: SSM をサポートする IGMP のパラメータを構成します。「[IGMP の設定](#)」を参照してください。通常は、SSMをサポートするために、PIMインターフェイスにIGMPv3を設定します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip igmp version 3
```

- ステップ 3: デフォルト範囲を使用しない場合は、SSM 範囲を構成します。

```
switch# configure terminal
switch(config)# ip pim ssm range 239.128.1.0/24
```

- ステップ 4: メッセージフィルタ処理を構成します。

```
switch# configure terminal
switch(config)# ip pim log-neighbor-changes
```

次に、SSM モードで PIM を構成する方法の例を示します。

## ■ vPC を介した PIM SSM の構成例

```
configure terminal
interface ethernet 2/1
no switchport
ip pim sparse-mode
ip igmp version 3
exit
ip pim ssm range 239.128.1.0/24
ip pim log-neighbor-changes
```

## vPC を介した PIM SSM の構成例

この例は、デフォルトの SSM 範囲である 232.0.0.0/8 ~ 225.1.1.1/32 をオーバーライドする方法を示しています。vPCを介したPIMSSMをサポートするために特別な構成は必要ありません。デフォルトの SSM を別の範囲 (225.1.1.1 など) に変更する場合は、次の例でその方法を示します。

```
switch# configure terminal
switch(config)# vrf context Enterprise
switch(config-vrf)# ip pim ssm range 225.1.1.1/32
switch(config-vrf)# show ip pim group-range
PIM Group-Range Configuration for VRF "default"
Group-range Action Mode RP-address Shrd-tree-range Origin
225.1.1.1/32 Accept SSM -- Local

switch1# show vpc (primary vPC) --> Shows vPC-related information. Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id: 10
Peer status: peer adjacency formed ok
vPC keep-alive status: peer is alive
Configuration consistency status: success
Per-vlan consistency status: success
Type-2 consistency status: success
vPC role: primary
Number of vPCs configured: 2
Peer Gateway: Disabled
Dual-active excluded VLANs: -
Graceful Consistency Check: Enabled
Auto-recovery status: Disabled
Delay-restore status: Timer is off.(timeout = 30s)
Delay-restore SVI status: Timer is off.(timeout = 10s)

vPC Peer-link status
-----
id Port Status Active vlans
-- -----
1 Po1000 up 101-102

vPC status
-----
id Port Status Consistency Reason Active vlans
-- -----
1 Po1 up success success 102
2 Po2 up success success 101

switch2# show vpc (secondary vPC)
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id: 10
Peer status: peer adjacency formed ok
vPC keep-alive status: peer is alive
```

```

Configuration consistency status: success
Per-vlan consistency status: success
Type-2 consistency status: success
vPC role: primary
Number of vPCs configured: 2
Peer Gateway: Disabled
Dual-active excluded VLANs: -
Graceful Consistency Check: Enabled
Auto-recovery status: Disabled
Delay-restore status: Timer is off.(timeout = 30s)
Delay-restore SVI status: Timer is off.(timeout = 10s)

vPC Peer-link status
-----
id Port Status Active vlans
-- -----
1 Po1000 up 101-102
vPC status
-----
id Port Status Consistency Reason Active vlans
-- -----
1 Po1 up success success 102
2 Po2 up success success 101

switch1# show ip igmp snooping group vlan 101 (primary vPC IGMP snooping states) -->
Shows if S,G v3 joins are received and on which VLAN. The same VLAN should be OIF in the
MRIB
output.
Type: S - Static, D - Dynamic, R - Router port, F - Fabricpath core port
Vlan Group Address Ver Type Port list
101 /* - R Eth9/5
101 225.1.1.1 v3
100.6.160.20 D Eth9/3

switch2# show ip igmp snooping group vlan 101 (secondary vPC IGMP snooping states)
Type: S - Static, D - Dynamic, R - Router port, F - Fabricpath core port

Vlan Group Address Ver Type Port list
101 /* - R Eth9/5
101 225.1.1.1 v3
100.6.160.20 D Eth9/3

switch1# show ip pim route (primary vPC PIM route) --> Shows the route information in
the PIM protocol.
PIM Routing Table for VRF "default" - 3 entries
(10.6.159.20/32, 225.1.1.1/32), expires 00:02:37
Incoming interface: Ethernet1/19, RPF nbr 10.6.159.20
Oif-list: (1) 00000000, timeout-list: (0) 00000000
Immediate-list: (1) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 2, JP-holddtime round-up: 3
(100.6.160.20/32, 225.1.1.1/32), expires 00:01:19
Incoming interface: Vlan102, RPF nbr 100.6.160.20
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 2, JP-holddtime round-up: 3
(*, 232.0.0.0/8), expires 00:01:19
Incoming interface: Null0, RPF nbr 0.0.0.0
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 2, JP-holddtime round-up: 3

```

## ■ vPC を介した PIM SSM の構成例

```

switch2# show ip pim route (secondary vPC PIM route)
PIM Routing Table for VRF "default" - 3 entries (10.6.159.20/32, 225.1.1.1/32), expires
00:02:51
Incoming interface: Vlan102, RPF nbr 100.6.160.100
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holddate round-up: 3
(100.6.160.20/32, 225.1.1.1/32), expires 00:02:51
Incoming interface: Vlan102, RPF nbr 100.6.160.20
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000

PIM SSM Over vPC Configuration Example
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holddate round-up: 3
(*, 232.0.0.0/8), expires 00:02:51
Incoming interface: Null0, RPF nbr 0.0.0.0
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holddate round-up: 3

switch2# show ip pim route (secondary vPC PIM route)
PIM Routing Table for VRF "default" - 3 entries
(10.6.159.20/32, 225.1.1.1/32), expires 00:02:29
Incoming interface: Vlan102, RPF nbr 100.6.160.100
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holddate round-up: 3
(100.6.160.20/32, 225.1.1.1/32), expires 00:02:29
Incoming interface: Vlan102, RPF nbr 100.6.160.20
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holddate round-up: 3
(*, 232.0.0.0/8), expires 00:02:29
Incoming interface: Null0, RPF nbr 0.0.0.0
Oif-list: (0) 00000000, timeout-list: (0) 00000000
Immediate-list: (0) 00000000, timeout-list: (0) 00000000
Sgr-prune-list: (0) 00000000
Timeout-interval: 3, JP-holddate round-up: 3

switch1# show ip mroute (primary vPC MRIB route) --> Shows the IP multicast routing
table.
IP Multicast Routing Table for VRF "default"
(10.6.159.20/32, 225.1.1.1/32), uptime: 03:16:40, pim ip
Incoming interface: Ethernet1/19, RPF nbr: 10.6.159.20
Outgoing interface list: (count: 1)
Vlan102, uptime: 03:16:40, pim
(100.6.160.20/32, 225.1.1.1/32), uptime: 03:48:57, igmp ip pim
Incoming interface: Vlan102, RPF nbr: 100.6.160.20
Outgoing interface list: (count: 1)
Vlan101, uptime: 03:48:57, igmp
(*, 232.0.0.0/8), uptime: 6d06h, pim ip
Incoming interface: Null, RPF nbr: 0.0.0.0
Outgoing interface list: (count: 0)

switch1# show ip mroute detail (primary vPC MRIB route) --> Shows if the (S,G) entries
have the RPF as the interface toward the source and no *,G states are maintained for the
SSM group range in the MRIB.
IP Multicast Routing Table for VRF "default"

```

```

Total number of routes: 3
Total number of (*,G) routes: 0
Total number of (S,G) routes: 2
Total number of (*,G-prefix) routes: 1
(10.6.159.20/32, 225.1.1.1/32), uptime: 03:24:28, pim(1) ip(0)
Data Created: Yes
VPC Flags
RPF-Source Forwarder
Stats: 1/51 [Packets/Bytes], 0.000 bps
Stats: Inactive Flow
Incoming interface: Ethernet1/19, RPF nbr: 10.6.159.20
Outgoing interface list: (count: 1)
Vlan102, uptime: 03:24:28, pim
(100.6.160.20/32, 225.1.1.1/32), uptime: 03:56:45, igmp(1) ip(0) pim(0)
Data Created: Yes
VPC Flags
RPF-Source Forwarder
Stats: 1/51 [Packets/Bytes], 0.000 bps
Stats: Inactive Flow
Incoming interface: Vlan102, RPF nbr: 100.6.160.20
Outgoing interface list: (count: 1)
Vlan101, uptime: 03:56:45, igmp (vpc-svi)
(*, 232.0.0.0/8), uptime: 6d06h, pim(0) ip(0)
Data Created: No
Stats: 0/0 [Packets/Bytes], 0.000 bps
Stats: Inactive Flow
Incoming interface: Null, RPF nbr: 0.0.0.0
Outgoing interface list: (count: 0)

switch2# show ip mroute detail (secondary vPC MRIB route)
IP Multicast Routing Table for VRF "default"
Total number of routes: 3
Total number of (*,G) routes: 0
Total number of (S,G) routes: 2
Total number of (*,G-prefix) routes: 1
(10.6.159.20/32, 225.1.1.1/32), uptime: 03:26:24, igmp(1) pim(0) ip(0)
Data Created: Yes
Stats: 1/51 [Packets/Bytes], 0.000 bps
Stats: Inactive Flow
Incoming interface: Vlan102, RPF nbr: 100.6.160.100
Outgoing interface list: (count: 1)
Ethernet1/17, uptime: 03:26:24, igmp
(100.6.160.20/32, 225.1.1.1/32), uptime: 04:06:32, igmp(1) ip(0) pim(0)
Data Created: Yes
VPC Flags
RPF-Source Forwarder
Stats: 1/51 [Packets/Bytes], 0.000 bps
Stats: Inactive Flow
Incoming interface: Vlan102, RPF nbr: 100.6.160.20
Outgoing interface list: (count: 1)
Vlan101, uptime: 04:03:24, igmp (vpc-svi)
(*, 232.0.0.0/8), uptime: 6d06h, pim(0) ip(0)
Data Created: No
Stats: 0/0 [Packets/Bytes], 0.000 bps
Stats: Inactive Flow
Incoming interface: Null, RPF nbr: 0.0.0.0
Outgoing interface list: (count: 0)

```

## BSR の設定例

BSR メカニズムを使用して ASM モードで PIM を設定するには、PIM ドメイン内の各ルータで、次の手順を実行します。

## PIM Anycast-RP の設定例

- 手順 1: ドメインに参加させるインターフェイスで PIM スparse モード パラメータを構成します。すべてのインターフェイスで PIM をイネーブルにすることを推奨します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip pim sparse-mode
```

- 手順 2: ルータが BSR メッセージの受信と転送を行うかどうかを構成します。

```
switch# configure terminal
switch(config)# ip pim bsr forward listen
```

- 手順 3: BSR として動作させるルータのそれぞれに、BSR パラメータを構成します。

```
switch# configure terminal
switch(config)# ip pim bsr-candidate ethernet 2/1 hash-len 30
```

- 手順 4: 候補 RP として動作させるルータのそれぞれに、RP パラメータを構成します。

```
switch# configure terminal
switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24
```

- ステップ 5: メッセージ フィルタ処理を構成します。

```
switch# configure terminal
switch(config)# ip pim log-neighbor-changes
```

- ステップ 6: BSR の動作を確認します。

```
switch# show ip pim rp
```

次に、BSR メカニズムを使用して PIM ASM モードを設定し、同一のルータに BSR と RP を設定する場合の例を示します。

```
configure terminal
interface ethernet 2/1
no switchport
ip pim sparse-mode
exit
ip pim bsr forward listen
ip pim bsr-candidate ethernet 2/1 hash-len 30
ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24
ip pim log-neighbor-changes
```

## PIM Anycast-RP の設定例

PIM エニーキャスト RP 方式を使用して ASM モードを設定するには、PIM ドメイン内のルータごとに、次の手順を実行します。

- 手順 1: ドメインに参加させるインターフェイスで PIM スparse モード パラメータを構成します。すべてのインターフェイスで PIM をイネーブルにすることを推奨します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip pim sparse-mode
```

- ステップ 2: Anycast-RP セット内のすべてのルータに適用する RP アドレスを構成します。

```
switch# configure terminal
switch(config)# interface loopback 0
switch(config-if)# ip address 192.0.2.3/32
```

3. **ステップ3** : Anycast-RP セットに加える各ルータで、その Anycast-RP セットに属するルータ間で通信に使用するアドレスを指定し、ループバックを構成します。

```
switch# configure terminal
switch(config)# interface loopback 1
switch(config-if)# ip address 192.0.2.31/32
```

4. **ステップ4** : ルータはエニーキャスト RP ピアでもあるため、インターフェイスに一意のピアアドレス（ドメイン全体でルーティング可能なアドレス）を構成します（たとえば、ループバック 2）。

```
switch# configure terminal
switch(config)# interface loopback 2
switch(config-if)# ip address 193.0.2.31/32
switch(config-if)# ip pim sparse-mode
```

(注) 一意にルーティング可能なアドレスを使用して、すべてのエニーキャスト ピア ルータで同様の構成を行う必要があります。

5. **ステップ5** : すべてのエニーキャストピアを RP セットに追加します。

```
switch# configure terminal
switch(config)# interface loopback 2
switch(config-if)# ip pim anycast-rp 192.0.2.3 193.0.2.31
switch(config-if)# ip pim anycast-rp 192.0.2.3 193.0.2.32
```

(注) 同様の構成を使用して、複数の RP セットを作成できます。

6. **ステップ6** : エニーキャスト RP の動作を確認します。

```
switch# show ip pim interface brief
switch# show ip pim rp
```

次に、2 つの Anycast-RP を使用して、PIM ASM モードを設定する例を示します。

```
configure terminal
interface ethernet 2/1
no switchport
ip pim sparse-mode
exit
interface loopback 0
ip address 192.0.2.3/32
exit
ip pim anycast-rp 192.0.2.3 192.0.2.31
ip pim anycast-rp 192.0.2.3 192.0.2.32
```

## ■ 次の作業

# 次の作業

PIM の関連機能を構成するには、次の章を参照してください：

- [IGMP の設定](#)
- [IGMP スヌーピングの構成](#)

# その他の参考資料

PIM の実装に関する詳細情報については、次の項目を参照してください。

- [関連資料](#)
- [MIB](#)

# 関連資料

関連項目	マニュアルタイトル
VRF の構成	[Cisco Nexus 3600 NX-OS ユニキャストルーティング構成ガイド (Cisco Nexus 3600 Series Unicast Routing Configuration Guide) ]

# MIB

MIB	MIB のリンク
IPMCAST-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 <a href="http://mibs.cloudapps.cisco.com/ITDIT/MIBS&gt;MainServlet">http://mibs.cloudapps.cisco.com/ITDIT/MIBS&gt;MainServlet</a>

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。