PIM および PIM6 の設定

この章では、IPv4 ネットワークおよび IPv6 ネットワークの Cisco NX-OS デバイスに Protocol Independent Multicast（PIM）および PIM6 機能を設定する方法を説明します。

PIM および PIM6 について

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。

Cisco NX-OS は、IPv4 ネットワーク（PIM）および IPv6 ネットワーク（PIM6）で PIM スパース モードをサポートしています。PIM スパース 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。PIM と PIM6 は、ルータ上で同時に実行するように設定できます。PIM および PIM6 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 および PIM6 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、および代表ルータ（DR）のプライオリティ設定を実行できます。

（注） Cisco NX-OS 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イネーブルにするには、各ルータでPIMおよびPIM6機能をイネーブルにしてから、マルチキャストに参加する各インターフェイスで、PIM または PIM6 スパース モードをイネーブルにする必要があります。IPv4ネットワークの場合はPIMを、IPv6ネットワークの場合は PIM6 を設定できます。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。IPv6 ネットワークでは、デフォルトで Multicast Listener Discovery（MLD）がイネーブルになります。

PIM および PIM6 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。
- 双方向共有ツリー（Bidir）：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ますが、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せん。Bidir モードを利用するには、RP を設定する必要があります。Bidir 転送では共有ツリーだけが使用されるため、送信元を検出する必要はありません。

（注） Cisco Nexus 9000 シリーズ スイッチは、PIM6 Bidir コマンドをサポートしていません。

これらの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。

ASM および Bidir 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。

PIM SSM モードの詳細については、RFC 3569 を参照してください。

PIM Bidir モードの詳細については、draft-ietf-pim-bidir-09.txt を参照してください。

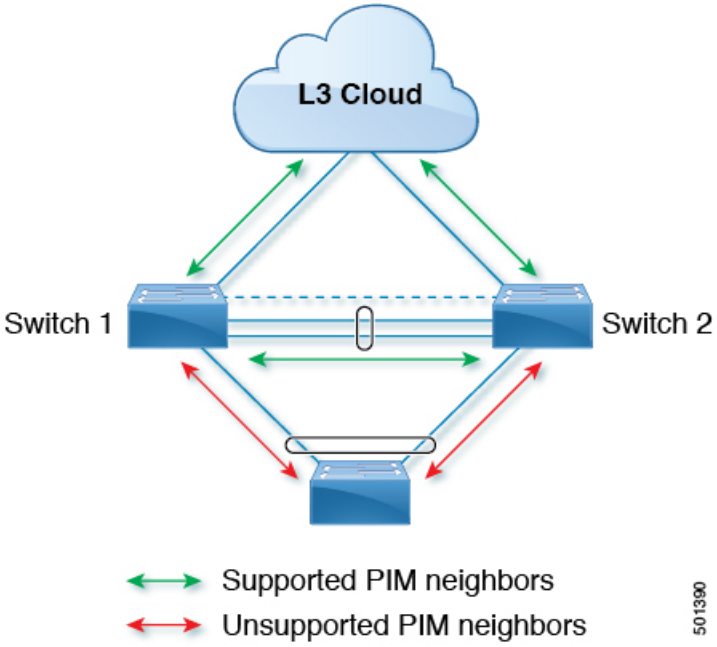
vPC を使用した PIM SSM

Cisco NX-OS リリース 7.0(3)I4(1) 以降、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 9000 シリーズ スイッチで PIM SSM を有効にできます。

vPC VLAN（vPC ピアリンクで伝送される VLAN）上のスイッチ仮想インターフェイス（SVI）とダウンストリーム デバイス間の PIM 隣接関係はサポートされません。この設定により、マルチキャスト パケットがドロップされる可能性があります。ダウンストリーム デバイスと PIM ネイバー関係が必要な場合は、vPC SVI ではなく、物理レイヤ 3 インターフェイスを Nexus スイッチで使用する必要があります。

vPC VLAN 上の SVI では、vPC ピアスイッチとの PIM 隣接関係が 1 つだけサポートされます。vPC-SVI の vPC ピアスイッチ以外のデバイスとの vPC ピアリンク上の PIM 隣接関係はサポートされていません。

（注） N9K-X9636C-R および N9K-X9636Q-R ライン カードを搭載した Cisco Nexus 9508 スイッチで、PIM SSM は Cisco NX-OS リリース 7.0(3)F2(1) 以降でサポートしますが、vPC 上の PIM SSM は Cisco NX-OS リリース 7.0(3)F3(1)までサポートしません。N9K-X9636C-RX ライン カードは、Cisco NX-OS リリース 7.0(3)F3(1) 以降、vPC の有無にかかわらず PIM SSM をサポートします。



PIM フラッディング メカニズムと送信元発見

送信元発見（SD）（PFM-SD）を使用した Protocol Independent Multicast (PIM) フラッディング メカニズムにより、マルチキャスト データ ストリームの送信中にランデブー ポイント（RP）が不要になります。この手法は、共有ツリーから短いパス（*, G）ツリーへの切り替えに関連する展

開の遅延に適しています。PIM のこの技術は、PIM レジスタ、RP、または共有ツリーを必要とせずに PIM スパース モード（SM）をサポートする方法を提供します。この手法は効率的で（S,G）ツリーのみを作成します。マルチキャスト ソース情報は、PIM フラッディング メカニズムを使用して、マルチキャスト ドメイン全体に伝播できます。PFM-SD モードは、Non-Blocking Multicast（NBM）と共存できます。PIM-SD モードの詳細については、RFC 8364 を参照してください。

Cisco NX-OS リリース 10.3（2）F 以降、PFM-SD 機能は、Cisco Nexus 9000 シリーズ、Nexus 9800 スイッチ、および N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636Q- R、N9K-X9636C-RX および N9K-X96136YC-R ライン カード。

Hello メッセージ

ルータがマルチキャスト IPv4 アドレス 224.0.0.13 または IPv6 アドレス ff02::d に PIM hello メッセージを送信して、PIM ネイバーとの隣接関係を確立すると、PIM プロセスが開始されます。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。

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留時間を経過すると、デバイスはそのリンクで PIM エラーが生じたと判断します。

設定された保留時間の変更は、インターフェイスで PIM を有効または無効にした後に送信される最初の 2 つの hello には反映されない場合があります。その後、インターフェイスで送信される最初の 2 つの hello については、設定された保留時間が使用されます。これにより、正しい保留時間の hello を受信するまで、PIM ネイバーは、初期ネイバー セットアップについて、誤ったネイバー タイムアウト値を設定する可能性があります。

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。

（注） PIM6 は MD5 認証をサポートしません。

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 Bidir 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 または Bidir 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。

（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。

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。

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
- デバイスに RP を手動で設定する場合

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。

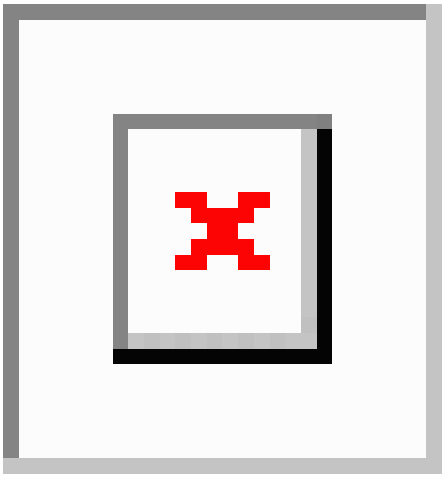
BSR は、Cisco Nexus 9300-FX、Cisco Nexus 9300-FX2、および Cisco Nexus 9300-FX3S プラットフォーム スイッチでサポートされています。

BSR は、Cisco Nexus 9300-EX/FX/FX2/FX3/GX/C および 9500-EX/FX/GX プラットフォーム スイッチでサポートされます。

次の図に、BSR メカニズムを示します。ここで、ルータ A（ソフトウェアによって選定された BSR）は、すべての有効なインターフェイスから BSR メッセージを送信しています（図の実線部分）。このメッセージには RP セットが含まれており、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 ハッシュが使用されます。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。

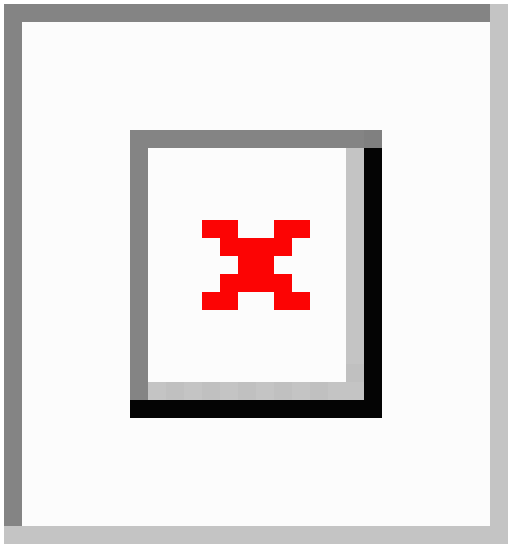
（注） PIM6 では BSR はサポートされていません。

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。

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、group-to-RP 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。

（注） Auto-RP は PIM6 ではサポートされていません。

⚠

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。

PIM ドメインで設定された複数の RP

このセクションでは、1 つの PIM ドメイン内に複数の RP が設定されている場合の選定プロセスのルールについて説明します。

Anycast-RP

Anycast-RP の実装方式には、マルチキャスト送信元検出プロトコル（MSDP）を使用する場合と、*RFC 4610*、『プロトコル独立マルチキャスト（*PIM*）を使用する *Anycast-RP*』に基づく場合の 2 種類があります。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 登録メッセージが最も近い RP に送信され、PIM 参加/プルーニング メッセージが最も近い RP に向けて送信されます。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 は、PIM Anycast RP および PIM Bidir RP に使用されるループバック インターフェイス上に設定する必要があります。

PIM Anycast-RP の詳細については、RFC 4610 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

PIM トリガー レジスタはデフォルトで有効になっています。

ip pim register-source を使用できます コマンドは、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ッド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。

```
ip pim register-source loopback 3
```

（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。

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、「Hello メッセージ」に記載された手順で決定されます。

ASM モードの場合、DR は RP に PIM Register パケットをユニキャストします。DR が、直接接続された受信者からの IGMP メンバーシップ レポートを受信すると、DR を経由するかどうかに関係なく、RP への最短パスが形成されます。これにより、同じマルチキャスト グループ上で送信を行うすべての送信元と、そのグループのすべての受信者を接続する共有ツリーが作成されます。

SSM モードの場合、DR は送信元方向に (S,G) PIM join または prune 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。

指定フォワーダ

PIM の Bidir モードでは、RP を検出する際に、各ネットワーク セグメント上のルータから指定フォワーダ（DF）が選択されます。DF は、セグメント上の指定グループにマルチキャスト データを転送します。DF は、ネットワーク セグメントから RP へのベスト メトリックに基づいて選定されます。

RPF インターフェイスで RP 方向へのパケットを受信したルータは、そのパケットを発信インターフェイス（OIF）リスト内のすべてのインターフェイスから転送します。パケットを受信したインターフェイスが属するルータが、LAN セグメントの DF に選定されている場合、そのパケットは、

着信インターフェイスを除く OIF リスト内のすべてのインターフェイスに転送されます。また、RPF インターフェイスを経由して RP にも転送されます。

（注） Cisco NX-OS では、RPF インターフェイスを MRIB の OIF リストに追加しますが、MFIB の OIF リストには追加しません。

共有ツリーから送信元ツリーへの ASM スイッチオーバー

（注） Cisco NX-OS では、RPF インターフェイスを MRIB の OIF リストに追加しますが、MFIB の OIF リストには追加しません。

ASM モードでは、共有ツリーだけを使用するように PIM パラメータを設定しないかぎり、受信者に接続された DR が、共有ツリーから送信元への最短パス ツリー（SPT）に切り替わります。

このスイッチオーバーの間、SPT および共有ツリーのメッセージが両方とも表示されることがあります。これらのメッセージの意味は異なります。共有ツリー メッセージは上流の RP に向かって伝播されますが、SPT メッセージは送信元に向かって送信されます。

SPT スイッチオーバーの詳細については、RFC 4601 の「Last-Hop Switchover to the SPT」の項を参照してください。

マルチキャスト フロー パスの可視性

Cisco NX-OS リリース 10.2（1）F 以降、TRM フローのマルチキャスト フロー パス可視化（FPV）とともに、TRM L3 モードおよびアンダーレイ マルチキャストでサポートされます。この機能により、Cisco Nexus 9000 シリーズ スイッチのすべてのマルチキャスト ステートをエクスポートできます。これは、送信元から受信者までのフロー パスの完全で信頼性の高い追跡性を確保するのに役立ちます。

Cisco Nexus 9000 シリーズ スイッチでマルチキャスト フロー パス データ エクスポートを有効にするには、**multicast flow-path export** コマンドを使用します。

この機能は次をサポートします。

- フロー パスの可視化（FPV）。
- 障害検出のためにフローの統計と状態のエクスポート。
- フローパスに沿ったスイッチの根本原因分析。これは、適切なデバッグ コマンドを実行することによって行われます。

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。

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。

マルチキャスト カウンタ

マルチキャスト フロー カウンタの収集は、2 つの異なる方法で有効にできます。

- 「マルチキャストヘビーテンプレートの有効化」セクションの説明に従って、マルチキャスト ヘビー テンプレートを有効にします。
- デフォルトのテンプレートで **hardware profile multicast flex-stats-enable** コマンドを構成します。

マルチキャスト カウンタをサポートするのは、Cisco Nexus 9300-EX、X9700-FX、9300-FX、および 9300-FX2 シリーズ スイッチだけです。これらのカウンタは、マルチキャスト トラフィックに関するより詳細な精度と可視性を提供します。具体的には、絶対マルチキャスト パケット数（すべてのマルチキャストS,Gルートのバイトとレート）を示します。これらのカウンタは、S,Gルートに対してのみ有効であり、*,G ルートに対しては有効ではありません。マルチキャスト ヘビー テンプレートが有効になっている場合、**show ip mroute detail** および **show ip mroute summary** コマンドの出力にマルチキャスト カウンタが表示されます。

Cisco NX-OSリリース 10.6（1）F 以降、IPv4 のマルチキャスト フロー カウンタ機能はCisco Nexus N9336C-SE1 でサポートされます。この機能を有効にするには、 **hardware profile multicast flex-stats-enable** コマンドを実行し、**copy running-config startup-config** コマンドを使用してスイッチをリロードします。

マルチキャスト ヘビー テンプレート

ずっと多くのマルチキャスト ルートをサポートし、**show ip mroute** コマンドの出力にマルチキャスト カウンタを表示するために、マルチキャスト ヘビー テンプレートを有効にすることができます。

マルチキャストヘビーテンプレートは、次のデバイスおよびリリースでサポートされています。

- Cisco Nexus N9K-X9732C-EX、N9K-X9736C-E、および N9K-X97160YC-EX ラインカード、Cisco NX-OS リリース 7.0(3)I3(2) 以降、ただし拡張性の向上のみ
- Cisco Nexus 9300-EX シリーズ スイッチ、Cisco NX-OS リリース 7.0(3)I6(1) 以降、拡張性とマルチキャスト カウンタの両方が向上
- Cisco Nexus 9300-FX シリーズ スイッチ、Cisco NX-OS リリース 7.0(3)I7(1) 以降、拡張性とマルチキャスト カウンタの両方が向上

マルチキャスト VRF-Lite ルート リーク

Cisco NX-OS リリース 7.0(3)I7(1) 以降、マルチキャスト レシーバーは VRF 間で IPv4 トラフィックを転送できます。以前のリリースでは、マルチキャスト トラフィックのフローは同じ VRF 内でのみ可能でした。

マルチキャスト VRF-lite リーキング機能は、受信側 VRF のマルチキャスト ルートでのリバース パス フォワーディング（RPF）ルックアップを、送信元 VRF で実行できるようにします。したがって、ソース VRF から発信されたトラフィックをレシーバ VRF に転送できます。

PIM グレースフル リスタート

プロトコル独立マルチキャスト（PIM）のグレースフル リスタートは、ルートプロセッサ（RP）スイッチオーバー後のマルチキャスト ルート（mroute）のコンバージェンスを改善する、マルチキャスト ハイ アベイラビリティ（HA）の拡張です。PIM のグレースフル リスタート機能では、RP スイッチオーバー時に、（RFC 4601 で定義された）生成 ID（GenID）値を、インターフェイス上の隣接 PIM ネイバーで、全ての（*,G）および（S,G）状態に対する PIM ジョイン メッセージを送信させるトリガーのための機構として利用します。これは、インターフェイスをリバース パス転送（RPF）インターフェイスとして使用します。このメカニズムにより、PIM ネイバーでは、新しくアクティブになった RP 上でこれらの状態を即座に再確立できます。

生成 ID

生成 ID（GenID）は、インターフェイスで Protocol Independent Multicast（PIM）転送が開始または再開されるたびに生成し直される、ランダムに生成された 32 ビット値です。PIM hello メッセージ内の GenID 値を処理するために、PIM ネイバーでは、RFC 4601 に準拠する PIM を実装した Cisco ソフトウェアを実行している必要があります。

（注） RFC 4601 に準拠しておらず、PIM hello メッセージ内の GenID の差異を処理できない PIM ネイバーは GenID を無視します。

PIM グレースフル リスタート動作

この図は、PIM グレースフル リスタート機能をサポートするデバイスのルートプロセッサ（RP）のスイッチオーバー後に実行される動作を示します。

図 *3 : RP* スイッチオーバー中の *PIM* グレースフル リスタート動作

PIM グレースフル リスタート動作は次のとおりです。

- 安定した状態で、PIM ネイバーは定期的に PIM ハロー メッセージをやりとりします。
- アクティブ RP は、マルチキャスト ルート（mroute）の状態をリフレッシュするために PIM join を定期的に受信します。
- アクティブ RP に障害が発生すると、スタンバイ RP が代わって新しいアクティブ RP になります。
- 新しいアクティブ RP は世代 ID（GenID）値を変更して、PIM ハロー メッセージで新しい GenID を隣接する PIM ネイバーに送信します。
- 新しい GenID を持つインターフェイスで PIM hello メッセージを受信する隣接 PIM ネイバーは、このインターフェイスを RPF インターフェイスとして使用するすべての (*, G) および (S, G) mroute に PIM グレースフル リスタートを送信します。
- これらの mroute 状態は、新しくアクティブになった RP 上でただちに再確立されます。

PIM のグレースフル リスタートおよびマルチキャスト トラフィック フロー

PIM ネイバーのマルチキャスト トラフィック フローは、マルチキャスト トラフィックで PIM グレースフル リスタート PIM のサポートを検出するか、デフォルトの PIM hello 保持時間間隔内に、障害が発生した RP ノードからの PIM hello メッセージを検出した場合には、影響を受けません。障害が発生した RP のマルチキャスト トラフィック フローは、非停止転送（NSF）対応かどうかに影響されません。

⚠

注意 デフォルトの PIM hello 保持時間は PIM hello 期間の 3.5 倍です。デフォルト値の 30 秒よりも小さい値で PIM hello 間隔を設定すると、マルチキャスト ハイ アベイラビリティ（HA）動作が設計どおりに機能しないことがあります。

高可用性

ルート プロセッサがリロードすると、VRF 間のマルチキャスト トラフィックは、同じ VRF 内で転送されるトラフィックと同じように動作します。

ハイ アベイラビリティの詳細については、『*Cisco Nexus 9000* シリーズ *NX-OS* ハイ アベイラビリティおよび冗長性ガイド』を参照してください。

PIM および PIM6 の前提条件

PIM には以下の前提条件があります。

PIM および PIM6 の利用条件は次のとおりです。

- デバイスにログインしている。

- 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 Bidir の場合、**hardware access-list tcam region mcast-bidir** コマンドを使用して ACL TCAM リージョン サイズを設定する必要があります。

  この **hardware access-list tcam region ing-sup** コマンドを使用して、ACL TCAM リージョン サイズを変更し、入力スーパーバイザ TCAM リージョンのサイズを設定します。

  詳細については、『ACL TCAM リージョン サイズの設定』を参照してください。

（注） この制限は、Cisco Nexus 9300-EX シリーズ スイッチには適用されません。

（注） デフォルトでは、mcast-bidir の領域サイズはゼロです。PIM Bidir をサポートするには、この領域に十分なエントリを割り当てる必要があります。

- Cisco Nexus 9300 シリーズ スイッチの場合、Bidir 範囲のマスク長が 24 ビット以上であることを確認してください。

PIM および PIM6 に関する注意事項と制限事項

PIM および PIM6 に関する注意事項および制限事項は次のとおりです。

- Cisco NX-OS PIM および PIM6 は、Cisco Nexus 9300-EX、Cisco Nexus 9300-FX、Cisco Nexus 9300-FX2、および Cisco Nexus 9300-FX3S プラットフォーム スイッチでサポートされています。
- セカンダリ IP アドレスを RP アドレスとして構成することはサポートされていません。
- ほとんどの Cisco Nexus デバイスでは、RPF 障害トラフィックはドロップされ、PIM アサートをトリガーするために非常に低レートで CPU に送信されます。Cisco Nexus 9000 シリーズ スイッチの場合、RPF 障害のトラフィックは、マルチキャスト送信元を学習するために、常に CPU にコピーされます。
- ほとんどの Cisco Nexus デバイスのファーストホップ送信元検出では、ファースト ホップからのトラフィックは送信元サブネット チェックに基づいて検出され、マルチキャスト パケットは送信元がローカル サブネットに属する場合に限り、CPU にコピーされます。Cisco Nexus 9000 シリーズ スイッチではローカル送信元を検出できないため、マルチキャスト パケットは、ローカル マルチキャスト送信元を学習するためにスーパーバイザに送信されます。

- Cisco NX-OS の PIM および PIM6 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。
- PIM SSM および PIM ASM は、すべての Cisco Nexus 9000 シリーズ スイッチでサポートされています。
- Cisco Nexus 9000 シリーズ スイッチは、vPC 上の PIM6 SSM をサポートしています。
- より低い IP アドレスを持つ L2 デバイスでスヌーピング クエリアを設定して、L2 デバイスをクエリアとして強制することをお勧めします。これは、マルチ シャーシ EtherChannel トランク (MCT) がダウンしているシナリオの処理に役立ちます。
- ランデブーポイントが PIM データ レジスタを受信すると、そのレジスタは処理のために CPU にパントされることが予期されます。この操作中に、レジスタのカプセル化が解除され、そのグループに関連する OIF がある場合は、そのデータ部分がソフトウェアで転送されます。
- (S,G) ルートは、spt-threshold infinity の設定に関係なく、データ パケットがパントされるとコントロールプレーンに作成されます。ルートは、コントロール プレーンを保護し、パケットのパントを制限するために作成されます。
- 次に示すように、サービスインターフェイスが作成される前に NAT フローが確立された場合は、**clear ip mroute** *group source* コマンドを使用して、影響を受けるルートを手動でクリアします。

```
2024 Jan 30 15:26:17.127933 MFX2-4
%IPFIB-SLOT1-2-MFIB_EGR_NAT_INVALID_INTF: Service Intf Ethernet1/31.100
not available, Impacted translation flow:
(118.4.0.1,2.1.13.153)->(228.4.11.49,204.0.1.59)L4(0,0)2024 Jan 30
15:26:23.039119 MFX2-4 %ETHPORT-5-IF_UP: Interface Ethernet1/31.100
is up in Layer3
```

- Cisco NX-OS リリース 9.2(3) 以降：
  - TOR 上の PIM6 は、マルチキャスト ヘビー、拡張ヘビー、およびデフォルトのテンプレートでサポートされています。
  - EX/FX/GX ライン カードを搭載した Cisco Nexus 9500 ボックスの PIM6 は、マルチキャスト ヘビー、拡張ヘビー、デュアル スタック マルチキャスト テンプレートでのみサポートされます。
- Cisco NX-OS リリース 9.3(3) 以降、SVI の PIM6 サポートは、vPC の有無にかかわらず、「EX」、「FX」、「FX2」で終わるスイッチの TOR に導入され、「EX」、「FX」で終わるスイッチの EOR に導入されました。
- SVI での PIM6 サポートは、MLD スヌーピングが有効になった後にのみ可能です。
- Cisco NX-OSリリース 9.3(5) 以降、SVI での PIM6 サポートが、Cisco Nexus 9300-GX プラットフォーム スイッチと、Cisco Nexus 9500 プラットフォーム スイッチで導入されました。
- Cisco Nexus 9000 シリーズ スイッチは、vPC で PIM ASM および SSM をサポートします。

- Cisco Nexus 9000 シリーズ 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。
- Cisco Nexus 9000 シリーズ スイッチでは、PIM スヌーピングはサポートされていません。
- Cisco Nexus 9000 シリーズ スイッチは、PIM6 ASM および SSM をサポートします。

（注） N9K-X9400 または N9K-X9500 ライン カードまたは N9K-C9504-FM、N9K-C9508-FM、および N9K-C9516-FM ファブリック モジュール（あるいはその両方）を備えた Cisco Nexus 9500 シリーズ スイッチのみが、PIM6 ASM および SSM をサポートします。他のラインカードまたはファブリック モジュールを備えた Cisco Nexus 9500 シリーズ スイッチは、PIM6 をサポートしていません。

- PIM 双方向マルチキャスト送信元 VLAN ブリッジングは、FEX ポートではサポートされていません。
- PIM6 双方向はサポートされていません。
- PIM6 は、Cisco NX-OS リリース 9.3(3) より前の SVI ではサポートされていません。
- PIM6 は、FEX ポート（レイヤ 2 およびレイヤ 3）ではサポートされていません。
- PIM 双方向は、Cisco Nexus 9300-EX、Cisco Nexus 9300-FX/FX2/FX3、および Cisco Nexus 9300-GX プラットフォーム スイッチでサポートされます。
- Cisco Nexus 9000 シリーズ スイッチは、vPC での PIM Bidir または vPC での PIM6 ASM、SSM、および双方向をサポートしていません。
- PIM Bidir プロトコルには次の制限があります。
  - 設計上、すべてのリンクで DF として機能するルータが 1 つだけある必要があります。
  - DF のルータがない場合、パケットはドロップされます。
  - 複数のルータが DF である場合、パケットが重複またはループする可能性があります。
  - トポロジが変更されると、1 つのルータが DF でなくなり、別のルータが新しい DF になる場合があります。
  - トポロジの変更中は、PIM DF の選択は迅速に行われますが、多くのマルチキャスト ルートが影響を受ける可能性があります。影響を受けるすべてのルートを処理し、フォワーディング プレーンを更新するために必要な時間は、影響を受けるルートの数によって異なります。ルート数が少ない場合は数ミリ秒ですが、ルートが数千ある場合は 1 分以上かかる場合があります。
- 次のデバイスは、レイヤ 3 ポート チャネル サブインターフェイスで PIM および PIM6 スパース モードをサポートしています。
  - Cisco Nexus 9300 シリーズ スイッチ

- Cisco Nexus 9300-EX シリーズ スイッチおよび Cisco Nexus 3232C および 3264Q スイッチ
- N9K-X9400 または N9K-X9500 ライン カードまたは N9K-C9504-FM、N9K-C9508-FM、および N9K-C9516-FM ファブリック モジュール（あるいはその両方）を備えた Cisco Nexus 9500 シリーズ スイッチ。

- マルチキャスト ヘビー テンプレートは、リアルタイム パケットとバイト統計をサポートしますが、VXLAN およびトンネルの出力または入力統計はサポートしません。
- リアルタイム/フレックス統計は、以下でサポートされています。
  - **hardware profile multicast flex-stats-enable** コマンドの構成を備えたデフォルトのテンプレート。
  - 構成のないヘビー テンプレート。

  リアルタイム統計は、拡張ヘビー テンプレートをサポートしていません。
- IPv4 上の GRE トンネルはマルチキャストをサポートします。IPv6 上の GRE トンネルはマルチキャストをサポートしていません。
- GRE トンネルでマルチキャストをサポートするのは、Cisco Nexus 9300-EX および 9300-FX/FX2/FX3 プラットフォームスイッチだけです。
- Cisco NX-OS リリース 10.2(1q)F 以降、マルチキャスト GRE は Cisco Nexus N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。
- GRE トンネルはホスト接続をサポートしていません。
- IGMP 機能はホスト接続の一部としてサポートされていないため、IGMP CLI は GRE トンネルでは使用できません。
- 静的トンネル OIF はマルチキャスト ルートに追加できない場合があります。IGMP CLI は GRE トンネルでは使用できず、マルチキャスト グループを発信インターフェイス（OIF）に静的にバインドする必要があるためです。
- SVI IP アドレスはトンネルの送信元またはトンネルの宛先として使用しないでください。
- トンネルの宛先は、L3 物理インターフェイスまたは L3 サブインターフェイスを介して到達可能である必要があります。
- トンネルの宛先に到達可能な L3 物理インターフェイスまたはサブインターフェイスでは、PIM が有効になっている必要があります。
- 同じデバイス上の複数の GRE トンネルでは、同じ送信元または同じ宛先を使用しないでください。
- GRE でカプセル化されたマルチキャスト トラフィックの ECMP 負荷共有はサポートされていません。トンネルの宛先に複数のリンクを介して到達できる場合、トラフィックはそのうちの 1 つのみに送信されます。
- マルチキャスト整合性チェッカーは、GRE トンネルではサポートされていません。

- GRE トンネルは、送信元または宛先インターフェイスが同じ VRF のメンバーである場合にのみ、VRF のメンバーになることができます。
- マルチキャスト VRF-Lite ルート リークは GRE ではサポートされていません。
- PIM Bidir は GRE ではサポートされていません。
- Cisco Nexus 3232C および 3264Q スイッチは、PIM6 をサポートしていません。
- インターフェイスに PIM/PIM6 ネイバーがない場合、そのインターフェイスは、最短/ECMP パスに基づいて RPF インターフェイスとして選択できます。送信元と受信者の間に複数の ECMP がある場合は、リンクの両側で PIM/PIM6 を有効にするようにしてください。
- Cisco NX-OS リリース 9.3(6) 以降、GRE 上のマルチキャストは、Cisco Nexus 9300-GX プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 9.3(6) 以降では、以下がサポートされます。
  - スイッチ 1 の着信 RPF インターフェイスは、デフォルトの VRF の下にあり、他の VRF ではスイッチ 2 にあります。
  - スイッチ 1 のトンネル インターフェイスはデフォルト VRF の下にあり、他の VRF ではスイッチ 2 にあります。
  - スイッチ 1 の発信インターフェイスは他の VRF にあり、デフォルトの VRF の下ではスイッチ 2 にあります。
- Cisco Nexus 9000 スイッチに GRE トンネルが存在すると、サブインターフェイスと共存できません（サブインターフェイスへのマルチキャスト転送で dot1q タグが欠落する場合があります）。これは、サブインターフェイスでのマルチキャスト トラフィックの受信に影響します。トラフィックは、サブインターフェイスではなく、親インターフェイスで受信されます。この影響は、標準/ネイティブ マルチキャスト パケットのみに影響し、マルチキャスト GRE（カプセル化およびカプセル化解除）パケットには影響しません。この制限は、Cisco Nexus 9300-GX プラットフォーム スイッチに適用されます。
- トンネル（機能トンネルまたは feature nv オーバーレイ）は、サブインターフェイスと共存できません（サブインターフェイスへのマルチキャスト転送で dot1q タグが欠落している可能性があります）。これは、サブインターフェイスでの受信マルチキャストトラフィックに影響します。この制限は、Cisco Nexus 9300-GX プラットフォーム スイッチに適用されます。
- GRE トンネルの送信元または宛先の設定が間違っている場合（送信元/宛先に互換性がないなど）、それらは自動的にシャットダウンされ、設定が回復された後でもシャットダウンされたままになります。回避策は、そのようなトンネルを手動でシャットダウン/シャットダウン解除することです。
- PIM-SM では、転送パスに変更があると、パケットの重複またはドロップが予想される動作になります。これにより、次のようなデメリットが発生します。
  - 共有ツリーでの受信から最短パス ツリー（SPT）に切り替える場合、通常、パケットがドロップされるときに小さなウィンドウが発生します。SPT 機能はこれを防止することができますが、重複が発生する場合があります。

- PIM レジスタまたはMSDPを介して受信した可能性のあるパケットを最初に転送するRPは、次にネイティブ転送のために SPT に参加しますが、そのため、RP が同じデータ パケットを2回転送する小さなウィンドウが生じます。1回はネイティブパケットとして、1 回は PIM 登録または MSDP カプセル化解除の後です。

これらの問題を解決するには、長い (S,G) 有効期限を設定するか、SSM/PIM Bidir を使用して、転送パスが変更されないようにします。

- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9808 プラットフォーム スイッチで PIM のサポートが提供されます。
  - Cisco NX-OS リリース 10.4(1)F 以降、PIM は、Cisco Nexus 9808 スイッチを搭載した Cisco Nexus X98900CD-A および X9836DM-A ライン カードでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、PIM は Cisco Nexus 9804 プラットフォーム スイッチ、Cisco Nexus X98900CD-A および X9836DM-A ライン カードでサポートされます。
- PFM-SD には、次の注意事項と制限事項 があります。
  - ポリシー ベースの PFM-SD 管理境界評価はサポートされていません。
  - マルチサイトのサポートはありません
  - PFM-SD モードは、VRF ごと、および一連のグループ範囲に対して有効にできます。PFM-SD モードはデフォルトでイネーブルになっていません。
  - PFM-SD 範囲の RP を設定しないでください。
  - PMN では、グループごとの複数の送信元の帯域幅管理はサポートされていません。
- PIM は、送信元、受信者、およびランデブー ポイント（RP）間のすべての L3 インターフェイスで構成する必要があります。
- アップストリーム ルータのインターフェイスでPIMが有効になっていない場合、トラフィックはドロップされます。
- HSRP 対応の PIM は、 Cisco NX-OS ではサポートされていません。
- マルチキャスト対応 BL がリロードされる場合、顧客は、ルートスケールに応じて、ファブリックポートトラッキングタイマーが 3 ー 5 前後に設定されていることを確認する必要があります。

  ファブリックポートトラッキングにより、L3out の起動が遅くなり、L3out を通過するルートでのユニキャストコンバージェンスが遅延します。これにより、PIM過負荷タイマー（3分）がマルチキャストステートとデータストリーム、およびストライプウィナー関連の作業を完了し、処理する準備を整えるのに十分な時間が提供されます。

  リロードされたBLが起動中である間は、代替またはバックアップBLがデータストリームを処理し、ストライプウィナー関連の作業を実行することが予想されるため、ポートトラッキングを増やしても現在実行中のデータストリームには影響しないことに注意してください。

- Cisco NX-OSリリース 10.6（1）F 以降、ip pim spt-switch-graceful コマンドはデフォルトで有効になっています。このコマンドを無効にするには、no ip pim spt-switch-graceful コマンドを使用します。この機能では、共有ツリーから最短パス ツリー（SPT）へのグレースフルスイッチオーバーを設定してパケット損失を最小化します。この場合、最初のデータ パケットを受信して最短パス ツリー（SPT）の完全な確立および検証が完了するまで、共有ツリーは使用されます。
  - 以前のリリースでは、このコマンドはデフォルトで有効になっていません。
  - この機能は、TRM VRF ではサポートされていません。
  - この機能は、 RPF として SVI ではサポートされていません。

Hello メッセージに関する注意事項と制限事項

Hello メッセージには、次の注意事項および制約事項が適用されます。

- PIM hello 間隔はデフォルト値が推奨されます。この値は変更しないでください。

ランデブー ポイントの注意事項と制限事項

ランデブー ポイント (RP) には、次の注意事項と制限事項が適用されます。

- 候補 RP インターバルを 15 秒以上に設定してください。
- 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。
- PIM6 は BSR と Auto-RP をサポートしていません。
- PIM は、PIM Anycast RP および PIM Bidir RP に使用されるループバック インターフェイス上に設定する必要があります。
- すべての Cisco NX-OS 7.x 以降のリリースでは、マルチキャストで RP を設定するために使用されるループバック インターフェイスに **ip**[**v6**] **pimsparse-mode** 設定が必要です。
- PIM RP（スタティック、BSR、またはAuto-RPのいずれか）の設定に使用されるインターフェイスには、**ip** [**v6**] **pim sparse-mode**が必要です。
- RPF 失敗パケットの過剰なパントを避けるために、Cisco Nexus 9000 シリーズ スイッチは、ASM のアクティブな送信元に対して S、G エントリを作成する場合があります。ただし、そのようなグループにはランデブー ポイント (RP) がありません。 送信元に対するリバース パス転送（RPF）が失敗した状況でも同様です。

  この動作は、Nexus 9200、9300-EX プラットフォーム スイッチ、およびN9K-X9700-EX LC プラットフォームには適用されません。
- デバイスにBSRポリシーが適用されており、BSRとして選定されないように設定されている場合、このポリシーは無視されます。これにより、次のようなデメリットが発生します。

- ポリシーで許可されているBSMをデバイスが受信した場合、意図に反してこのデバイスがBSRに選定されていると、対象のBSMがドロップされるために下流のルータではそのBSMを受信できなくなります。また、下流のデバイスでは、不正なBSRから送信されたBSMが正しくフィルタリングされるため、これらのデバイスではRP情報を受信できなくなります。
- BSRに異なるデバイスから送られたBSMが着信すると、新しいBSMが送信されますが、その正規のBSMは下流のデバイスでは受信されません。

- 送信元VRFが、たまたまRPである非フォワーダvPCピアにマルチキャストトラフィックを転送した場合、S、Gエントリはフォワーダ vPC ピアに作成されません。これにより、これらの送信元のマルチキャストトラフィックがドロップする可能性があります。これを回避するには、vPC ピアが同時にRPでもある場合は常に、トポロジにエニーキャストRPを設定する必要があります。

マルチキャスト VRF-lite ルート リークの注意事項と制限事項

マルチキャスト VRF-lite ルート リークには、次の注意事項と制限事項が適用されます。

- Cisco Nexus 9000 シリーズ スイッチは、マルチキャスト VRF-lite ルート リークをサポートします。
- マルチキャスト VRF-lite ルート リークは、-R ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチではサポートされていません。
- PIM スパース モードと PIM SSM は、マルチキャスト VRF-lite ルート リークでサポートされます。ただし、vPC を使用した PIM SSM は、マルチキャスト VRF-lite ルート リークではサポートされません。
- マルチキャスト VRF-lite ルート リークでは、スタティック ランデブー ポイント（RP）のみがサポートされます。
- 送信元とランデブー ポイント（RP）は同じ VRF にある必要があります。

デフォルト設定

この表に、PIM および PIM6 の各種パラメータについてのデフォルト設定を示します。

表 *1 : PIM* および *PIM6* のデフォルト パラメータ

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
ログ ネイバーの変更	無効

パラメータ	デフォルト
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** • 232.0.0.0/8 **IPv6** • ff32::/32 • ff33::/32 • ff34::/32 • ff35::/32 • ff36::/32 • ff37::/32 • ff38::/32 • ff39::/32 • ff3a::/32 • ff3b::/32 • ff3c::/32 • ff3d::/32 • ff3e::/32
PIM スパース モード	無効
DR プライオリティ	1
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

PIM および PIM6 の設定

パラメータ	デフォルト
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
BFD	無効化

PIM および PIM6 の設定

PIM は、各インターフェイスに設定できます。

PIM と PIM6 の両方を、同一のルータに同時に設定できます。インターフェイスで IPv4 または IPv6 のどちらが実行されているかに応じて、インターフェイスごとに PIM または PIM6 を設定できます。

（注） Cisco NX-OS は、PIM スパース モード バージョン 2 のみをサポートします。このマニュアルで「PIM」と記載されている場合は、PIM スパース モードのバージョン 2 を意味しています。

下の表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 または PIM6 ドメインに、それぞれ独立したアドレス範囲を設定できます。

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
Bidir	はい	双方向共有ツリー
SSM	いいえ	送信元固有マルチキャスト
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 および PIM6 の設定作業

次の手順では、PIM および PIM6 を設定します。

1. 各マルチキャスト配信モードで設定するマルチキャスト グループの範囲を選択します。
2. PIM および PIM6 をイネーブルにします。
3. 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、設定作業を行います。

- ASM モードまたは Bidir モードについては、ASM および Bidir の設定を参照してください。
- SSM モードについては、SSM の設定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 ルートの設定を参照してください。

4. メッセージ フィルタリングを設定します。

（注） 次の CLI コマンドを使用して PIM を設定します。

- 設定コマンドは、**ip pim** で始まります。 PIM の場合は 、PIM6 の場合は **ipv6 pim** を使用します。
- **show ip pim** で始まるコマンドを表示 PIM の場合は、PIM6 の場合は **show ipv6 pim** を使用します。

PIM および PIM6 機能のイネーブル化

PIM または PIM6 コマンドにアクセスするには、PIM または PIM6 機能をイネーブルにしておく必要があります。

（注） Cisco NX-OS リリース 7.0(3)I5(1) 以降、PIM または PIM6 を有効にするために、少なくとも 1 つのインターフェイスを IP PIM スパース モードで有効にする必要はなくなりました。

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を確認してください。

手順の概要

1. **configure terminal**
2. **feature pim**
3. **feature pim6**
4. （任意） **show running-configuration pim**
5. （任意） **show running-configuration pim6**
6. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**feature pim** 例： `switch(config)# feature pim`	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。
Step 3	**feature pim6** 例： `switch(config)# feature pim6`	PIM6 をイネーブルにします。デフォルトでは PIM6 はディセーブルになっています。
Step 4	（任意） **show running-configuration pim** 例： `switch(config)# show running-configuration pim`	PIMの実行コンフィギュレーション情報を示します。
Step 5	（任意） **show running-configuration pim6** 例： `switch(config)# show running-configuration pim6`	PIM6 の実行コンフィギュレーション情報を示します。
Step 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

PIM または PIM6 スパース モード パラメータの設定

スパース モード ドメインに参加させる各デバイス インターフェイスで、PIM または PIM6 スパース モードを設定します。次の表に、設定可能なスパース モード パラメータを示します。

表 *2 : PIM* および *PIM6* スパース モードのパラメータ

パラメータ	説明
デバイスにグローバルに適用	

パラメータ	説明
Auto-RP メッセージ アクション	Auto-RP メッセージの受信と転送をイネーブルにします。これらの機能はデフォルトではディセーブルになっているため、候補 RP またはマッピング エージェントとして設定されていないルータは、Auto-RP メッセージの受信と転送を行いません。 （注） PIM6 は、Auto-RP 方式をサポートしていません。
BSR メッセージ アクション	BSR メッセージの受信と転送をイネーブルにします。これらの機能はデフォルトではディセーブルになっているため、候補 RP または BSR 候補として設定されていないルータは、BSR メッセージの受信と転送を行いません。 （注） PIM6 は BSR をサポートしていません。
Bidir RP 制限	IPv4 に設定可能な Bidir RP の数を設定します。PIM の各 VRF でサポートする Bidir RP の最大数を 8 以下にする必要があります。有効範囲は 0 ～ 8 です。デフォルト値は 6 です。 （注） PIM6 は Bidir をサポートしていません。
Register のレート制限	IPv4 または IPv6 Register の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。
初期ホールドダウン期間	IPv4 または IPv6 の初期ホールドダウン期間を秒単位で設定します。このホールドダウン期間は、MRIB が最初に起動するのにかかる時間です。コンバージェンスを高速化するには、小さい値を入力します。指定できる範囲は 90 ～ 210 です。ホールドダウン期間をディセーブルにするには、0 を指定します。デフォルト値は 210 です。
デバイスの各インターフェイスに適用	
PIM スパース モード	インターフェイスで PIM または PIM6 をイネーブルにします。

パラメータ	説明
DR プライオリティ	現在のインターフェイスに、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。複数の PIM 対応ルータが存在するマルチアクセス ネットワークでは、DR プライオリティの最も高いルータが DR ルータとして選定されます。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 に選定されます。DR は、直接接続されたマルチキャスト送信元に PIM Register メッセージを送信するとともに、直接接続された受信者に代わって、ランデブー ポイント（RP）方向に PIM Join メッセージを送信します。有効範囲は 1 ～ 4294967295 です。デフォルトは 1 です。
指定ルータの遅延	PIM hello メッセージでアドバタイズされる DR プライオリティを指定期間にわたり 0 に設定することで、指定ルータ（DR）の選定への参加を遅延させます。この遅延中、DR は変更されず、現在のスイッチにはそのインターフェイスでのすべてのマルチキャストの状態を把握する時間が与えられます。遅延期間が終了すると、DR 選出を再び開始するために、正しい DR プライオリティが hello パケットで送信されます。値の範囲は 3 ～ 0xffff 秒です。
hello 認証モード	インターフェイスで、PIM hello メッセージ内の MD5 ハッシュ認証キー（パスワード）をイネーブルにして、直接接続されたネイバーによる相互認証を可能にします。PIM hello メッセージは、認証ヘッダー（AH）オプションを使用して符号化された IP セキュリティ です。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（クリアテキストの）キーを指定します。 • 3：3-DES 暗号化キーを指定します。 • 7：Cisco Type 7 暗号化キーを指定します。 認証キーの文字数は最大 16 文字です。デフォルトではディセーブルになっています。 （注） PIM6 は MD5 認証をサポートしません。
Hello 認証キーチェーン	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 <keychain> はキーチェーンの名前です。 （注） PIM6 はキーチェーン認証をサポートしません。

パラメータ	説明
hello 間隔	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 1000 ～ 18724286 です。デフォルト値は 30000 です。 （注） このパラメータの確認された範囲および関連付けられた PIM ネイバー スケールについては、『*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*』を参照してください。
ドメイン境界	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。 （注） PIM6 は、Auto-RP 方式をサポートしていません。
ネイバー ポリシー	prefix-list 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設定します。[1]指定したポリシー名が存在しない場合、またはプレフィックス リストがポリシー内で設定されていない場合は、すべてのネイバーとの隣接関係が確立されます。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。 （注） 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推奨します。 （注） PIM ネイバー ポリシーは、プレフィックス リストのみをサポートします。ルートマップ内で使用される ACL はサポートしていません。

[1] prefix-list ポリシーを設定するには、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*を参照してください。

PIM6 スパース モード パラメータの設定

手順の概要

1. **configure terminal**
2. （任意） **ip pim auto-rp** {**listen** [**forward**] | **forward** [**listen**]}
3. （任意） **ip pim bsr** {**listen** [**forward**] | **forward** [**listen**]}
4. （任意） **ip pim bidir-rp-limit** 制限
5. （任意） **ip pim register-rate-limit** *rate*
6. （任意） **ip pim spt-threshold infinity group-list** *route-map-name*
7. （任意） [**ip** | **ipv4**] **routing multicast holddown** *holddown-period*

8. （任意） **show running-configuration pim**
9. **interface** *interface*
10. **ip pim sparse-mode**
11. （任意） **ip pim dr-priority** *priority*
12. （任意） **ip pim dr-delay** *delay*
13. （任意） **ip pim hello-authentication ah-md5** *auth-key*
14. （任意） **ip pim hello-authentication keychain** *name*
15. （任意） **ip pim hello-interval** *interval*
16. （任意） **ip pim border**
17. （任意） **ip pim neighbor-policy prefix-list** *prefix-list*
18. （任意） **show ip pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**]
19. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	（任意） **ip pim auto-rp** {**listen** [**forward**] | **forward** [**listen**]} 例： `switch(config)# ip pim auto-rp listen`	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。
Step 3	（任意） **ip pim bsr** {**listen** [**forward**] | **forward** [**listen**]} 例： `switch(config)# ip pim bsr forward`	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。
Step 4	（任意） **ip pim bidir-rp-limit** 制限 例： `switch(config)# ip pim bidir-rp-limit 4`	IPv4 に設定可能な Bidir RP の数を指定します。PIM の各 VRF でサポートする Bidir RP の最大数を 8 以下にする必要があります。有効範囲は 0 ～ 8 です。デフォルト値は、6 です。
Step 5	（任意） **ip pim register-rate-limit** *rate* 例： `switch(config)# ip pim register-rate-limit 1000`	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。

	コマンドまたはアクション	目的
Step 6	（任意） **ip pim spt-threshold infinity group-list** *route-map-name* 例： `switch(config)# ip pim spt-threshold infinity group-list my_route-map-name`	指定されたルートマップで定義されているグループプレフィックスに対して、IPv4 PIM（*, G）状態のみを作成します。Cisco NX-OS リリース 3.1 は最大 1000 のルート マップ エントリを、リリース 3.1 より前の Cisco NX-OS は最大 500 のルート マップ エントリをサポートします。 （注） **ip pim use-shared-tree-only group-list** コマンドは、**ip pim spt-threshold infinity group-list** コマンドと同じ機能を実行します。いずれかのコマンドを使用してこの手順を実行できます。 両方のコマンド（**ip pim spt-threshold infinity group-list** および **ip pim use-shared-tree-only group-list**）には、次の制限があります。 • これは、Cisco Nexus 9000 クラウド スケール スイッチの仮想ポート チャネル（vPC）でのみサポートされます。 • NX-OS（非 vPC）のラスト ホップ ルーター（LHR）構成でサポートされています。
Step 7	（任意） [**ip** | **ipv4**] **routing multicast holddown** *holddown-period* 例： `switch(config)# ip routing multicast holddown 100`	初期ホールドダウン期間を秒単位で設定します。指定できる範囲は 90 ～ 210 です。ホールドダウン期間をディセーブルにするには、0 を指定します。デフォルト値は 210 です。
Step 8	（任意） **show running-configuration pim** 例： `switch(config)# show running-configuration pim`	Bidir RP 制限および Register のレート制限を含む、PIM 実行コンフィギュレーション情報を表示します。

Step 9	**interface** *interface*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

Step 10	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	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。
Step 11	（任意） **ip pim dr-priority** *priority* 例：	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。

	コマンドまたはアクション	目的
	`switch(config-if)# ip pim dr-priority 192`	有効範囲は 1 ～ 4294967295 です。デフォルトは 1 です。
Step 12	（任意） **ip pim dr-delay** *delay* 例： `switch(config-if)# ip pim dr-delay 3`	PIM hello メッセージでアドバタイズされる DR プライオリティを指定期間にわたり 0 に設定することで、指定ルータ（DR）の選定への参加を遅延させます。この遅延中、DRは変更されず、現在のスイッチにはそのインターフェイスでのすべてのマルチキャストの状態を把握する時間が与えられます。遅延期間が終了すると、DR 選出を再び開始するために、正しい DR プライオリティが hello パケットで送信されます。値の範囲は 3 ～ 0xffff 秒です。 （注） このコマンドは、起動時、または IP アドレスかインターフェイスの状態が変更された後にのみ、DR 選定への参加を遅延させます。これは、マルチキャスト アクセスの非 vPC レイヤ 3 インターフェイス専用です。
Step 13	（任意） **ip pim hello-authentication ah-md5** *auth-key* 例： `switch(config-if)# ip pim hello-authentication ah-md5 my_key`	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（クリアテキストの）キーを指定します。 • 3：3-DES 暗号化キーを指定します。 • 7：Cisco Type 7 暗号化キーを指定します。 キーの文字数は最大 16 文字です。デフォルトではディセーブルになっています。
Step 14	（任意） **ip pim hello-authentication keychain** *name* 例： `switch(config-if)# ip pim hello-authentication keychain mykeychain`	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<keychain>はキーチェーンの名前です。 （注） • 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。

	コマンドまたはアクション	目的
		• 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。
Step 15	（任意） **ip pim hello-interval** *interval* 例： `switch(config-if)# ip pim hello-interval 25000`	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 1000 ～ 18724286 です。デフォルト値は 30000 です。 （注） 最小値は 1 ミリ秒です。
Step 16	（任意） **ip pim border** 例： `switch(config-if)# ip pim border`	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。
Step 17	（任意） **ip pim neighbor-policy prefix-list** *prefix-list* 例： `switch(config-if)# ip pim neighbor-policy prefix-list AllowPrefix`	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。 また、prefix-list コマンドを使用して、プレフィックス リスト ポリシーに基づいて隣接する PIM ネイバーを設定します。**ip prefix-list** プレフィックス リストは最大 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。 （注） 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推奨します。
Step 18	（任意） **show ip pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**] 例： `switch(config-if)# show ip pim interface`	PIM インターフェイスの情報を表示します。
Step 19	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	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。

PIM6 スパース モード パラメータの構成

手順の概要

1. **configure terminal**
2. （任意） **ipv6 pim register-rate-limit** *rate*
3. （任意） **ipv6 routing multicast holddown** *holddown-period*
4. （任意） **show running-configuration pim6**
5. **interface** *interface*
6. **ipv6 pim sparse-mode**
7. （任意） **ipv6 pim dr-priority** *priority*
8. （任意） **ipv6 pim hello-interval** *interval*
9. （任意） **ipv6 pim border**
10. （任意） **ipv6 pim neighbor-policy prefix-list** *prefix-list*
11. **show ipv6 pim interface** [*interface* | brief] [vrf *vrf-name* | all]
12. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	（任意） **ipv6 pim register-rate-limit** *rate* 例： `switch(config)# ipv6 pim register-rate-limit 1000`	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。
Step 3	（任意） **ipv6 routing multicast holddown** *holddown-period* 例： `switch(config)# ipv6 routing multicast holddown 100`	初期ホールドダウン期間を秒単位で設定します。指定できる範囲は 90 ～ 210 です。ホールドダウン期間をディセーブルにするには、0 を指定します。デフォルト値は 210 です。
Step 4	（任意） **show running-configuration pim6** 例： `switch(config)# show running-configuration pim6`	Register レート制限を含めた PIM6 の実行コンフィギュレーション情報を表示します。
Step 5	**interface** *interface* 例：	指定したインターフェイスに対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。

	コマンドまたはアクション	目的
	`switch(config)# interface vlan 10` `switch(config-if)#`	
Step 6	**ipv6 pim sparse-mode** 例： `switch(config-if)# ipv6 pim sparse-mode`	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。 Cisco NX-OS リリース 9.3(5) 以降では、Broadcom ベースのスイッチの SVI インターフェイスでこのコマンドを設定できます。
Step 7	（任意） **ipv6 pim dr-priority** *priority* 例： `switch(config-if)# ipv6 pim dr-priority 192`	PIM6 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。
Step 8	（任意） **ipv6 pim hello-interval** *interval* 例： `switch(config-if)# ipv6 pim hello-interval 25000`	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 1000 ～ 18724286 です。デフォルト値は 30000 です。
Step 9	（任意） **ipv6 pim border** 例： `switch(config-if)# ipv6 pim border`	インターフェイスを PIM6 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。
Step 10	（任意） **ipv6 pim neighbor-policy prefix-list** *prefix-list* 例： `switch(config-if)# ipv6 pim neighbor-policy prefix-list AllowPrefix`	**ipv6 prefix-list***prefix-list* コマンドを使用して、プレフィックス リスト ポリシーに基づいてどの PIM6 ネイバーと隣接関係になるかを設定します。プレフィックス リストは最大 63 文字です。デフォルトでは、すべての PIM6 ネイバーと隣接関係が確立されます。 （注） 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推奨します。
Step 11	**show ipv6 pim interface** [*interface* | brief] [vrf *vrf-name* | all] 例： `switch(config-if)# show ipv6 pim interface`	PIM6 インターフェイスの情報を表示します。
Step 12	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意）コンフィギュレーションの変更を保存します。

PIM フラッディングメ カニズムと送信元発見を一緒に構成

PFM-SD を構成するには、次の手順に従います：

手順の概要

1. **configure terminal**
2. **[no] ip pim pfm-sd range** {*prefix* | { **route-map** *route-map-name* } | { **prefix-list** *prefix-list-name* }}
3. **[no] ip pim pfm-sd originator-id** {*interface*}
4. **[no] ip pim pfm-sd announcement interval** { *interval* }
5. **[no] ip pim pfm-sd announcement gap** { *interval* }
6. **[no] ip pim pfm-sd announcement rate** { *rate* }
7. [no] ip pim pfm-sd gsh holdtime { holdtime }
8. **interface** {*interface port*}
9. **[no] ip pim pfm-sd** {**boundary** [*direction*]}
10. **end**
11. （任意） **show ip pim pfm-sd** { **cache** [*local*] | [*remote-discovery*]]}
12. （任意） **show ip pim interface** {*interface port*}
13. （任意） **show ip pim vrf internal**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

Step 2	**[no] ip pim pfm-sd range** {*prefix* | { **route-map** *route-map-name* } | { **prefix-list** *prefix-list-name* }} 例： `switch(config)# ip pim pfm-sd range route-map r1`	特定のマルチキャスト グループ範囲に対して PFM-SD をイネーブルにします。ルート マップ/プレフィックス リストでは、最大 10 の範囲がサポートされます。
Step 3	**[no] ip pim pfm-sd originator-id** {*interface*} 例： `switch(config)# ip pim pfm-sd originator-id lo5`	PFM-SD アナウンスの発信者を構成します。
Step 4	**[no] ip pim pfm-sd announcement interval** { *interval* } 例： `switch(config)# ip pim pfm-sd announcement interval 170`	アナウンスの周期を設定します。デフォルト インターバル値は 60 秒です。

	コマンドまたはアクション	目的
Step 5	**[no] ip pim pfm-sd announcement gap** { *interval* } 例： `switch(config)# ip pim pfm-sd announcement gap 1600`	送信される PFM-SD メッセージ間のギャップを構成します。間隔のデフォルト値は 1000 ミリ秒です。
Step 6	**[no] ip pim pfm-sd announcement rate** { *rate* } 例： `switch(config)# ip pim pfm-sd announcement rate 10`	インターフェイスごとの PFM-SD メッセージ レートを構成します。デフォルト値は 6 です。
Step 7	[no] ip pim pfm-sd gsh holdtime { holdtime } 例： `switch(config)# ip pim pfm-sd gsh holdtime 250`	PFM-SD 送信元 ホールドタイムを構成します。デフォルトのホールドタイムは 210 秒です。

Step 8	**interface** {*interface port*}
	例：
	`switch(config)# interface eth1/1`
	`switch(config-if)#`
		インターフェイスを設定し、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。

Step 9	**[no] ip pim pfm-sd** {**boundary** [*direction*]} 例： `switch(config-if)# ip pim pfm-sd boundary in`	PFM-SD 境界を構成します。方向については、**in**、**out**、および **both** オプションが使用できます。

Step 10	**end**
	例：
	`switch(config-if)# end`
	`switch#`
		インターフェイス構成モードを終了し、特権 EXEC モードを開始します。

Step 11	（任意） **show ip pim pfm-sd** { **cache** [*local*] | [*remote-discovery*]]} 例： `switch# show ip pim pfm-sd cache local`	PIM PFM-SD ローカルまたはリモート ディスカバリ キャッシュ情報を表示します。
Step 12	（任意） **show ip pim interface** {*interface port*} 例： `switch# show ip pim interface ethernet 1/17`	VRF の PIM インターフェイス ステータスを表示します。
Step 13	（任意） **show ip pim vrf internal** 例： `switch# show ip pim vrf internal`	PIM 対応の VRF を表示します。

ASM と Bidir の設定

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。

Any Source Multicast（ASM）および双方向共有ツリー（Bidir）のマルチキャスト配信モードでは、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 を設定する必要があります。

ASM または Bidir モードを設定するには、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。

（注） RP アドレスがループバック インターフェイスを使用することをお勧めします。また、RP アドレスを持つインターフェイスで、**ip pim sparse-mode** が有効になっている必要があります。

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。または、設定のプレフィックスリスト方法を指定することができます。

（注） Cisco NX-OS は RP を検索するには、最長一致プレフィックスを常に使用します。そのため、動作はルート マップまたはプレフィックス リストでのグループ プレフィックスの位置にかかわらず同じです。

次の設定例は、Cisco NX-OS を使用して同じ出力を生成します（231.1.1.0/24 はシーケンス番号に関係なく常に拒否されます）。

```
ip prefix-list plist seq 10 deny 231.1.1.0/24
ip prefix-list plist seq 20 permit 231.1.0.0/16
ip prefix-list plist seq 10 permit 231.1.0.0/16
ip prefix-list plist seq 20 deny 231.1.1.0/24
```

静的 RP の設定（PIM）

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。

手順の概要

1. **configure terminal**

2. **ip pim rp-address** *rp-address* [**group-list** *ip-prefix* | **prefix-list** *name* |**override** |**route-map** *policy-name*] [**bidir**]
3. （任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*]
4. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**ip pim rp-address** *rp-address* [**group-list** *ip-prefix*	**prefix-list** *name* |**override** |**route-map** *policy-name*] [**bidir**] 例： `switch(config)# ip pim rp-address 192.0.2.33 group-list 224.0.0.0/9`	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。 **match ip multicast** コマンドで、静的 RP アドレスのプレフィックスリスト ポリシー名または使用するグループ 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。 **bidir** キーワードを指定しない場合、モードは ASM です。 **override** オプションにより、RP アドレスは、ルートマップで指定されたグループの動的に学習された RP アドレスをオーバーライドします。 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。
Step 3	（任意） **show ip pim group-range** [*ip-prefix*	**vrf** *vrf-name*] 例： `switch(config)# show ip pim group-range`	BSR の待ち受けおよび転送ステートなど、PIM RP 情報を表示します。
Step 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

静的 RP の設定（PIM6）

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。

手順の概要

1. **configure terminal**
2. **ipv6 pim rp-address** *rp-address* [**group-list** *ipv6-prefix* | **route-map** *policy-nsmr*]
3. （任意） **show ipv6 pim group-range** [*ipv6-prefix* | **vrf** *vrf-name*]
4. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**ipv6 pim rp-address** *rp-address* [**group-list** *ipv6-prefix*	**route-map** *policy-nsmr*] 例： `switch(config)# ipv6 pim rp-address 2001:0db8:0:abcd::1 group-list ff1e:abcd:def1::0/24`	マルチキャスト グループ範囲に、PIM6 スタティック RP アドレスを設定します。**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。モードは ASM です。デフォルトのグループ範囲は ff00::0/8 です。 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。
Step 3	（任意） **show ipv6 pim group-range** [*ipv6-prefix*	**vrf** *vrf-name*] 例： `switch(config)# show ipv6 pim group-range`	PIM6 モードとグループ範囲を表示します。
Step 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

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。

候補 BSR の設定では、引数を指定できます（次の表を参照）。

（注）　PIM6 は BSR をサポートしていません。

表 *3:* 候補 *BSR* の引数

引数	説明
interface	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。
hash-length	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 に割り当て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。PIM6 の場合、この値の範囲は 0 ～ 128 で、デフォルト値は 126 秒です。
priority	現在の BSR に割り当てら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。

BSR 候補 RP の引数およびキーワードの設定

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

表 *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
interface	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。
group-list *ip-prefix*	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キャスト グループ。
interval	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、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。

引数またはキーワード	説明
priority	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は、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数値です。）この値の範囲は 0（優先度が最大）～ 255 であり、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。
bidir	bidir を指定しない場合、現在の RP は ASM モードになります。bidir を指定した場合は、RP は Bidir モードになります。
route-map *policy-name*	この機能を適用するグループ プレフィックスを定義するルート マップ ポリシー名です。

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限り、すべてのブートストラップ ルータ 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。
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。

BSR の設定（PIM）

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。

手順の概要

1. **configure terminal**

2. **ip pim bsr** {**forward** [**listen**] | **listen** [**forward**]}
3. **ip pim bsr bsr-candidate** *interface* [**hash-len** *hash-length*] [**priority** *priority*]
4. **ip pim sparse-mode**
5. （任意） **ip pim bsr rp-candidate** *interface* **group-list** *ip-prefix* **route-map** *policy-name* **priority** *priority* **interval** *interval* [**bidir**]
6. （任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*]
7. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**ip pim bsr** {**forward** [**listen**]	**listen** [**forward**]} 例： `switch(config)# ip pim bsr listen forward`	リッスンと転送を設定します。 リモート PE 上の各 VRF で確実にこのコマンドを入力してください。
Step 3	**ip pim bsr bsr-candidate** *interface* [**hash-len** *hash-length*] [**priority** *priority*] 例： `switch(config)# ip pim bsr-candidate ethernet 2/1 hash-len 24`	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。
Step 4	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	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。
Step 5	（任意） **ip pim bsr rp-candidate** *interface* **group-list** *ip-prefix* **route-map** *policy-name* **priority** *priority* **interval** *interval* [**bidir**] 例： `switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24`	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。 **Bidir** オプションを使用して Bidir 候補 RP を作成します。 （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。

	コマンドまたはアクション	目的
Step 6	（任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] 例： `switch(config)# show ip pim group-range`	PIM モードとグループ範囲を表示します。
Step 7	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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） Auto-RP は PIM6 ではサポートされていません。

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。こ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
interface	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。
scope *ttl*	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。

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 の設定では、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
interface	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。
group-list *ip-prefix*	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 形式で指定します。
scope *ttl*	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 時間（TTL）値。この値の範囲は 1 ～ 255 であり、デフォルト値 32 です。
interval	RP-Announce メッセージの送信間隔（秒）。この値の範囲は 1 ～ 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。
bidir	指定しない場合、現在の RP は ASM モードになります。指定した 場合、現在の RP は Bidir モードになります。
route-map *policy-name*	この機能を適用するグループプレフィックスを定義するルートマ プ ポリシー名です。

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 ドメインのルータごとに、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。
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。

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。

自動 RPの設定（PIM）

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。

手順の概要

1. **configure terminal**
2. **ip pim** {**send-rp-discovery** | **auto-rp mapping-agent**} *interface* [**scope** *ttl*]
3. **ip pim** {**send-rp-announce** | **auto-rp rp-candidate**} *interface* {**group-list** *ip-prefix* | **prefix-list** *name* | **route-map** *policy-name*} [**scope** *ttl*] **interval** *interval*] [**bidir**]
4. **ip pim sparse-mode**
5. （任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*]
6. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**ip pim** {**send-rp-discovery**	**auto-rp mapping-agent**} *interface* [**scope** *ttl*] 例： `switch(config)# ip pim auto-rp mapping-agent ethernet 2/1`	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。
Step 3	**ip pim** {**send-rp-announce**	**auto-rp rp-candidate**} *interface* {**group-list** *ip-prefix*	**prefix-list** *name*	**route-map** *policy-name*} [**scope** *ttl*] **interval** *interval*] [**bidir**] 例： `switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24`	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。**bidir** オプションは、Bidir 候補 RP を構築する場合に使用します。 （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。

	コマンドまたはアクション	目的
Step 4	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	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。
Step 5	（任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] 例： `switch(config)# show ip pim group-range`	PIM モードとグループ範囲を表示します。
Step 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

PIM Anycast-RP セットの設定

PIM Anycast-RP セットを設定する手順は、次のとおりです。

1. PIM Anycast-RP セットに属するルータを選択します。
2. PIM Anycast-RP セットの IP アドレスを選択します。
3. 後述の手順に従い、PIM Anycast-RP セットに属するそれぞれのピア RP を設定します。

PIM エニーキャスト RP セットの構成（PIM）

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。

手順の概要

1. **configure terminal**
2. **interface loopback** *number*
3. **ip address** *ip-prefix*
4. **ip pim sparse-mode**
5. **ip router** *routing-protocol-configuration*
6. **exit**
7. **interface loopback** *number*
8. **ip address** *ip-prefix*
9. **ip pim sparse-mode**
10. **ip router** *routing-protocol-configuration*
11. **exit**
12. **ip pim rp-address** *anycast-rp-address* [**group-list** *ip-address*]
13. **ip pim anycast-rp** *anycast-rp-address anycast-rp-set-router-address*

14. RP セットに属する各ピア ルータ（ローカル ルータを含む）で、同じ Anycast-RP アドレスを使用してステップ 13 を繰り返します。
15. （任意） **show ip pim rp**
16. （任意） **show ip mroute** *ip-address*
17. （任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*]
18. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**interface loopback** *number*
	例：
	`switch(config)# interface loopback 0`
	`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。

Step 3	**ip address** *ip-prefix* 例： `switch(config-if)# ip address 192.168.1.1/32`	このインターフェイスの IP アドレスを設定します。このルータの識別に役立つ一意の IP アドレスになります。
Step 4	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	PIM スパース モードをイネーブルにします。
Step 5	**ip router** *routing-protocol-configuration* 例： `switch(config-if)# ip router ospf 1 area 0.0.0.0`	エニーキャスト RP セット内の他のルータがインターフェイスに到達できるようにします。

Step 6	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

Step 7	**interface loopback** *number*
	例：
	`switch(config)# interface loopback 1`
	`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 1 を設定しています。

	コマンドまたはアクション	目的
Step 8	**ip address** *ip-prefix* 例： `switch(config-if)# ip address 10.1.1.1/32`	このインターフェイスのIPアドレスを設定します。これは、エニーキャスト RP アドレスとして機能する共通の IP アドレスである必要があります。
Step 9	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	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。
Step 10	**ip router** *routing-protocol-configuration* 例： `switch(config-if)# ip router ospf 1 area 0.0.0.0`	エニーキャストRPセット内の他のルータがインターフェイスに到達できるようにします。

Step 11	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

Step 12	**ip pim rp-address** *anycast-rp-address* [**group-list** *ip-address*] 例： `switch(config)# ip pim rp-address 10.1.1.1 group-list 224.0.0.0/4`	PIM エニーキャスト RP アドレスを設定します。
Step 13	**ip pim anycast-rp** *anycast-rp-address anycast-rp-set-router-address* 例： `switch(config)# ip pim anycast-rp 10.1.1.1 192.168.1.1`	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。
Step 14	RP セットに属する各ピア ルータ（ローカル ルータを含む）で、同じAnycast-RPアドレスを使用してステップ 13 を繰り返します。	—
Step 15	（任意） **show ip pim rp** 例： `switch(config)# show ip pim rp`	PIM RP マッピングを表示します。
Step 16	（任意） **show ip mroute** *ip-address* 例： `switch(config)# show ip mroute 239.1.1.1`	mroute エントリを表示します。
Step 17	（任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] 例：	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
	`switch(config)# show ip pim group-range`	
Step 18	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

PIM エニーキャスト RP セットの設定（PIM6）

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。

手順の概要

1. **configure terminal**
2. **interface loopback** *number*
3. **ipv6 address** *ipv6-prefix*
4. **ipv6 pim sparse-mode**
5. **ipv6 router** *routing-protocol-configuration*
6. **exit**
7. **interface loopback** *number*
8. **ipv6 address** *ipv6-prefix*
9. **ipv6 router** *routing-protocol-configuration*
10. **exit**
11. **ipv6 pim rp-address** *anycast-rp-address* [**group-list** *ip-address*]
12. **ipv6 pim anycast-rp** *anycast-rp-address anycast-rp-set-router-address*
13. RP セットに属する各ピア ルータ（ローカル ルータを含む）で、同じ Anycast-RP アドレスを使用してステップ 13 を繰り返します。
14. （任意） **show ipv6 pim rp**
15. （任意） **show ipv6 mroute** *ipv6-address*
16. （任意） **show ipv6 pim group-range** [*ipv6-prefix*] [**vrf** *vrf-name* | **all**]
17. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

	コマンドまたはアクション	目的

Step 2	**interface loopback** *number*
	例：
	`switch(config)# interface loopback 0`
	`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。

Step 3	**ipv6 address** *ipv6-prefix* 例： `switch(config-if)# ipv6 address 2001:0db8:0:abcd::5/32`	このインターフェイスの IP アドレスを設定します。このルータの識別に役立つ一意の IP アドレスになります。
Step 4	**ipv6 pim sparse-mode** 例： `switch(config-if)# ipv6 pim sparse-mode`	PIM6 スパース モードをイネーブルにします。
Step 5	**ipv6 router** *routing-protocol-configuration* 例： `switch(config-if)# ipv6 router ospfv3 1 area 0.0.0.0`	エニーキャスト RP セット内の他のルータがインターフェイスに到達できるようにします。

Step 6	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

Step 7	**interface loopback** *number*
	例：
	`switch(config)# interface loopback 1`
	`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 1 を設定しています。

Step 8	**ipv6 address** *ipv6-prefix* 例： `switch(config-if)# ipv6 address 2001:0db8:0:abcd::1111/32`	このインターフェイスの IP アドレスを設定します。これは、エニーキャスト RP アドレスとして機能する共通の IP アドレスである必要があります。
Step 9	**ipv6 router** *routing-protocol-configuration* 例： `switch(config-if)# ipv6 router ospfv3 1 area 0.0.0.0`	エニーキャスト RP セット内の他のルータがインターフェイスに到達できるようにします。

Step 10	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

Step 11	**ipv6 pim rp-address** *anycast-rp-address* [**group-list** *ip-address*]	PIM6 エニーキャスト RP アドレスを設定します。

	コマンドまたはアクション	目的
	例： `switch(config)# ipv6 pim rp-address 2001:0db8:0:abcd::1111 group-list ff1e:abcd:def1::0/24`	
Step 12	**ipv6 pim anycast-rp** *anycast-rp-address anycast-rp-set-router-address* 例： `switch(config)# ipv6 pim anycast-rp 2001:0db8:0:abcd::5 2001:0db8:0:abcd::1111`	指定した Anycast-RP アドレスに対応する PIM6 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。
Step 13	RP セットに属する各ピア ルータ（ローカル ルータを含む）で、同じ Anycast-RP アドレスを使用してステップ 13 を繰り返します。	—
Step 14	（任意） **show ipv6 pim rp** 例： `switch(config)# show ipv6 pim rp`	PIM RP マッピングを表示します。
Step 15	（任意） **show ipv6 mroute** *ipv6-address* 例： `switch(config)# show ipv6 mroute ff1e:2222::1:1:1:1`	mroute エントリを表示します。
Step 16	（任意） **show ipv6 pim group-range** [*ipv6-prefix*] [**vrf** *vrf-name* | **all**] 例： `switch(config)# show ipv6 pim group-range`	PIM6 モードとグループ範囲を表示します。
Step 17	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

ASM 専用の共有ツリーの設定

共有ツリーを設定できるのは、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、受信者がアクティブ グループに加入しても、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** コマンドで、共有ツリーを適用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。

（注） Cisco NX-OS ソフトウェアは、vPC での共有ツリー機能をサポートしません。vPC の詳細については、『*Cisco Nexus 9000* シリーズ *NX-OS* インターフェイス設定ガイド』を参照してください。

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。

ASM 専用の共有ツリーの設定（PIM）

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。

手順の概要

1. **configure terminal**
2. **ip pim use-shared-tree-only group-list** *policy-name*
3. （任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*]
4. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**ip pim use-shared-tree-only group-list** *policy-name* 例： `switch(config)# ip pim use-shared-tree-only group-list my_group_policy`	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。**match ip multicast** 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。 コマンドには次の制限があります。 • これは、Cisco Nexus 9000 クラウド スケール スイッチの仮想ポート チャネル（vPC）でのみサポートされます。 • NX-OS（非 vPC）のラスト ホップ ルーター（LHR）構成でサポートされています。

	コマンドまたはアクション	目的
Step 3	（任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] 例： `switch(config)# show ip pim group-range`	PIM モードとグループ範囲を表示します。
Step 4	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	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。

ASM 専用の共有ツリーの設定（PIM6）

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。

手順の概要

1. **configure terminal**
2. **ipv6 pim use-shared-tree-only group-list** *policy-name*
3. （任意） **show ipv6 pim group-range** [*ipv6-prefix* | **vrf** *vrf-name*]
4. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**ipv6 pim use-shared-tree-only group-list** *policy-name* 例： `switch(config)# ipv6 pim use-shared-tree-only group-list my_group_policy`	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。**match ipv6 multicast** 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。
Step 3	（任意） **show ipv6 pim group-range** [*ipv6-prefix* | **vrf** *vrf-name*]	PIM6 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)# show ipv6 pim group-range`	
Step 4	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	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。

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。

SSM で使用される IPv4 グループ範囲のみを設定できます。

（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

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。

手順の概要

1. **configure terminal**
2. [**no**] **ip pim ssm** {**prefix-list** *name* | **range** {*ip-prefix* | none} | route-map *policy-name*}
3. （任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*]
4. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	[**no**] **ip pim ssm** {**prefix-list** *name* | **range** {*ip-prefix* | none} | route-map *policy-name*}
	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。
		• **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。
		• **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。
		• **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。
		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。
		（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。

Step 3	（任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] 例： `switch(config)# show ip pim group-range`	PIM モードとグループ範囲を表示します。
Step 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

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。vPC 上で PIM SSM を設定する場合、ランデブー ポイント（RP）の設定は必要ありません。

(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。

手順の概要

1. **configure terminal**
2. **vrf context** *name*
3. （任意） [**no**] **ip pim ssm** {**prefix-list** *name* | **range** {*ip-prefix* | **none**} | **route-map** *policy-name*}
4. （任意） **show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**]
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**vrf context** *name*
	例：
	`switch(config)# vrf context Enterprise`
	`switch(config-vrf)#`
		新しい VRF を作成し、VRF 設定モードを開始します。*name* には最大 32 文字の英数字を使用できます。大文字と小文字は区別されます。

Step 3	（任意） [**no**] **ip pim ssm** {**prefix-list** *name*	**range** {*ip-prefix*	**none**}	**route-map** *policy-name*} 例： `switch(config-vrf)# ip pim ssm range 234.0.0.0/24`	次のオプションを使用できます。 • **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。 • **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

	コマンドまたはアクション	目的
		none を指定すると、すべてのグループ範囲が削除されます。 • **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。 デフォルトでは、SSM グループ範囲は 232.0.0.0/8 です。S,G joins がこの範囲で受信される限り、vPC 上の PIM SSM は機能します。デフォルトを他の範囲で上書きする場合は、このコマンドを使用してその範囲を指定する必要があります。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。 **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。
Step 4	（任意） **show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] 例： `switch(config-vrf)# show ip pim group-range`	PIM モードとグループ範囲を表示します。
Step 5	（任意） **copy running-config startup-config** 例： `switch(config-vrf)# copy running-config startup-config`	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。

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（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。

（注） IPv6 ではスタティック マルチキャスト ルートはサポートされていません。

（注） **ip multicast multipath sg-hash CLI** が設定されていない場合、マルチキャスト トラフィックは RFP チェックに失敗する可能性があります。

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 PIM または PIM6 がイネーブルになっていることを確認してください。

手順の概要

1. **configure terminal**
2. **ip mroute** {*ip-addr mask* | *ip-prefix*} {*next-hop* | *nh-prefix* | *interface*} [*route-preference*] [**vrf** *vrf-name*]
3. （任意） **show ip static-route** [**multicast**] [**vrf** *vrf-name*]
4. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**ip mroute** {*ip-addr mask* | *ip-prefix*} {*next-hop* | *nh-prefix* | *interface*} [*route-preference*] [**vrf** *vrf-name*] 例： `switch(config)# ip mroute 192.0.2.33/1 224.0.0.0/1`	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 プリファレンスは 1 です。
Step 3	（任意） **show ip static-route** [**multicast**] [**vrf** *vrf-name*] 例： `switch(config)# show ip static-route multicast`	設定されているスタティック ルートを表示します。
Step 4	（任意） **copy running-config startup-config**	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。

マルチキャスト マルチパスの設定

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。

手順の概要

1. **configure terminal**
2. **ip multicast multipath** {**none** | **resilient** | **s-g-hash**}
3. **clear ip mroute ***

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**ip multicast multipath** {**none**	**resilient**	**s-g-hash**} 例： `switch(config)# ip multicast multipath none`	次のオプションを使用して、マルチキャスト マルチパスを構成します。 • **none**：URIB RPF ルックアップで複数の ECMP にまたがるハッシュを抑制して、マルチキャスト マルチパスを無効にします。このオプションを使用すると、最も高い RPF ネイバー（ネクストホップ）アドレスが RPF インターフェイスに使用されます。 （注） **ip multicast multipath none** コマンドを使用して、ハッシュを完全に無効にします。 • **s-g-hash**：RPF インターフェイスを選択するために、（デフォルトの S/RP、G ベース ハッシュではなく）S、G、ネクストホップ ハッシュを開始します。このオプションは、送信元およびグループ アドレスに基づいてハッシュを構成します。これがデフォルトの設定です。 • **resilient**：ECMP パス リストが変更され、古い RPF 情報がまだ ECMP の一部である場合、このオプションは、再ハッシュを実行して潜在的に RPF 情報を変更する代わりに、古い RPF 情報を使用します。**ip multicast multipath resilient** コマンドは、URIB からのルート到達可能性通知にパスがある場合に、現在の RPF への回復力（スティッキネス）を維持するためのものです。 （注）

	コマンドまたはアクション	目的
		no ip multicast multipath resilient コマンドは、スティッキネスアルゴリズムを無効にします。このコマンドは、ハッシュアルゴリズムに依存しません。 （注） X9636C-R または X9636Q-R ライン カード、または C9508-FM-R ファブリック モジュールを備えた Cisco Nexus 9508 スイッチで、**resilient** オプションから **none** オプションに変更する場合は、最初に **no ip multicast multipath elastic** コマンドを入力し、次に、**ip multicast multipath none** コマンドを入力します。
Step 3	**clear ip mroute *** 例： `switch(config)# clear ip mroute *`	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。

マルチキャスト VRF-Lite ルート リークの設定

Cisco NX-OS リリース 7.0(3)I7(1) 以降では、マルチキャスト VRF-lite ルート リークを設定できます。これにより、VRF 間の IPv4 マルチキャスト トラフィックが可能になります。

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。

手順の概要

1. **configure terminal**
2. **ip multicast rpf select vrf** *src-vrf-name* **group-list** *group-list*
3. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

	コマンドまたはアクション	目的
Step 2	**ip multicast rpf select vrf** *src-vrf-name* **group-list** *group-list* 例： `switch(config)# ip multicast rpf select vrf blue group-list 236.1.0.0/16`	特定のマルチキャスト グループの RPF ルックアップに使用する VRF を指定します。 src-vrf-name は、ソース VRF の名前です。最大 32 文字の英数字で、大文字と小文字が区別されます。 *group-list* は、RPF のグループ範囲です。形式は A.B.C.D/LEN で、最大長は 32 です。
Step 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

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。

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） ルート マップに影響を与えるコマンドは、**match ip[v6] multicast** だけです。

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 または PIM6 がイネーブルになっていることを確認してください。

RP 情報配信を制御するルート マップの設定（PIM）

手順の概要

1. **configure terminal**
2. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
3. **match ip multicast** {**rp** *ip-address* [**rp-type** *rp-type*]} {**group** *ip-prefix*} {**source** *source-ip-address*}
4. （任意） **show route-map**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
	例：
	`switch(config)# route-map ASM_only permit 10`
	`switch(config-route-map)#`
	例：
	`switch(config)# route-map Bidir_only permit 10`
	`switch(config-route-map)#`
		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。

Step 3	**match ip multicast** {**rp** *ip-address* [**rp-type** *rp-type*]} {**group** *ip-prefix*} {**source** *source-ip-address*}
	例：
	`switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type ASM`
	例：
	`switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type Bidir`
		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方法では、グループおよびRPを指定する必要があります。
		（注）
		match ip multicast group-range <> CLI では、**route-map** の下の **group-range** コマンドはサポートされていません。

Step 4	（任意） **show route-map** 例： `switch(config-route-map)# show route-map`	設定済みのルート マップを表示します。
Step 5	（任意） **copy running-config startup-config** 例： `switch(config-route-map)# copy running-config startup-config`	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。

RP 情報配信を制御するルート マップの設定（PIM6）

手順の概要

1. **configure terminal**
2. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
3. **match ipv6 multicast** {**rp** *ip-address* [**rp-type** *rp-type*]} {**group** *ipv6-prefix*} {**source** *source-ip-address*}

4. （任意） **show route-map**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
	例：
	`switch(config)# route-map ASM_only permit 10`
	`switch(config-route-map)#`
		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。

Step 3	**match ipv6 multicast** {**rp** *ip-address* [**rp-type** *rp-type*]} {**group** *ipv6-prefix*} {**source** *source-ip-address*} 例： `switch(config-route-map)# match ipv6 multicast group ff1e:abcd:def1::0/24 rp 2001:0db8:0:abcd::1 rp-type ASM`	指定した グループ、RP、および RP タイプを関連付けます。RP のタイプ（ASM）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方法では、グループおよび RP を指定する必要があります。
Step 4	（任意） **show route-map** 例： `switch(config-route-map)# show route-map`	設定済みのルート マップを表示します。
Step 5	（任意） **copy running-config startup-config** 例： `switch(config-route-map)# copy running-config startup-config`	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。

メッセージ フィルタリングの設定

（注） rp-candidate-policy でのプレフィックスの照合では、プレフィックスが c-rp によるアドバタイズの内容と比較して完全に一致する必要があります。部分一致は許容されません。

次の表に、PIM および PIM6 でのメッセージ フィルタリングの設定方法を示します。

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
デバイスにグローバルに適用	
ネイバーの変更の記録	ネイバーのステート変更を通知する Syslog メッセージ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。
PIM Register ポリシー	ルート マップ ポリシーに基づいて PIM Register メッセージをフィルタリングできるようにします。[2]**match ipv6 multicast** コマンドを使用して、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イネーブルにします。RP とグループ アドレス、およびタイプ（Bidir または ASM）を、**match ip multicast** コマンドで指定できます。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。 （注） PIM6 は BSR をサポートしていません。
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。**match ip multicast** 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。 （注） PIM6 は BSR をサポートしていません。
Auto-RP 候補 RP ポリシー	ルートマップ ポリシーに基づく、Auto-RP マッピング エージェントによる Auto-RP アナウンス メッセージのフィルタリングをイネーブルにします。RP、グループ アドレス、およびタイプ（Bidir または ASM）を、**match ip multicast** コマンドで指定できます。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。 （注） PIM6 は、Auto-RP 方式をサポートしていません。

メッセージの種類	説明
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。**match ip multicast** 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。 （注） PIM6 は、Auto-RP 方式をサポートしていません。
各デバイスのインターフェイスに適用	
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。**match ip**[**v6**] **multicast** 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。

[2] ルート マップ ポリシーの設定については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

次のコマンドでは、ルートマップをフィルタリング ポリシーとして使用できます（各ステートメントについて **permit** または **deny** のいずれか）。

- **jp-policy** コマンドは (S,G)、(*,G)、または (RP,G) を使用できます。
- **register-policy** コマンドは (S,G) または (*,G) を使用できます。
- **igmp report-policy** コマンドは (*,G) または (S,G) を使用できます。
- **state-limit reserver-policy** コマンドは (*,G) または (S,G) を使用できます。
- **auto-rp rp-candidate-policy** コマンドは (RP,G) を使用できます。
- **bsr rp-candidate-policy** コマンドは (RP,G) を使用できます。
- **autorp mapping-agent policy** コマンドは (S) を使用できます。
- **bsr bsr-policy** コマンドは (S) を使用できます。

次のコマンドでは、ルート マップ アクション（**permit** または **deny**）が無視された場合に、ルート マップをコンテナとして使用できます。

- **ip pim rp-address route map** コマンドは G のみを使用できます。
- **ip pim ssm-range route map** は G のみを使用できます。
- **ip igmp static-oif route map** コマンドは (S,G)、(*,G)、(S,G-range)、(*,G-range) を使用できます。

- **ip igmp join-group route map** コマンドは (S,G)、(*,G)、(S,G-range、(*,G-range)) を使用できます。

メッセージ フィルタリングの設定（PIM）

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。

手順の概要

1. **configure terminal**
2. （任意） **ip pim log-neighbor-changes**
3. （任意） **ip pim register-policy** *policy-name*
4. （任意） **ip pim bsr rp-candidate-policy** *policy-name*
5. （任意） **ip pim bsr bsr-policy** *policy-name*
6. （任意） **ip pim auto-rp rp-candidate-policy** *policy-name*
7. （任意） **ip pim auto-rp mapping-agent-policy** *policy-name*
8. **interface** *interface*
9. （任意） **ip pim jp-policy** *policy-name* [**in** | **out**]
10. （任意） **show run pim**
11. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	（任意） **ip pim log-neighbor-changes** 例： `switch(config)# ip pim log-neighbor-changes`	ネイバーのステート変更を通知する Syslog メッセージ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。
Step 3	（任意） **ip pim register-policy** *policy-name* 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。**match ip multicast** コマンドで、グループ アドレスまたはグループと送信元アドレスを指定できます。

	コマンドまたはアクション	目的
Step 4	（任意） **ip pim bsr rp-candidate-policy** *policy-name* 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イネーブルにします。RP とグループ アドレス、およびタイプ（Bidir または ASM）を、**match ip multicast** コマンドで指定できます。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。
Step 5	（任意） **ip pim bsr bsr-policy** *policy-name* 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。**match ip multicast** 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。
Step 6	（任意） **ip pim auto-rp rp-candidate-policy** *policy-name* 例： `switch(config)# ip pim auto-rp rp-candidate-policy my_auto_rp_candidate_policy`	ルートマップ ポリシーに基づく、Auto-RP マッピング エージェントによる Auto-RP Announce メッセージのフィルタリングをイネーブルにします。RP、グループアドレス、およびタイプ（Bidir または ASM）を、**match ip multicast** コマンドで指定できます。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。
Step 7	（任意） **ip pim auto-rp mapping-agent-policy** *policy-name* 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。**match ip multicast** 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。

Step 8	**interface** *interface*
	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。

Step 9	（任意） **ip pim jp-policy** *policy-name* [**in** | **out**] 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イネーブルにします。**match ip multicast** 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。

	コマンドまたはアクション	目的
Step 10	（任意） **show run pim** 例： `switch(config-if)# show run pim`	PIM 構成コマンドを表示します。
Step 11	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	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。

メッセージ フィルタリングの設定（PIM6）

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。

手順の概要

1. **configure terminal**
2. （任意） **ipv6 pim log-neighbor-changes**
3. （任意） **ipv6 pim register-policy** *policy-name*
4. （任意） **ipv6 pim jp-policy** *policy-name* [**in** | **out**]
5. （任意） **show run pim6**
6. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	（任意） **ipv6 pim log-neighbor-changes** 例： `switch(config)# ipv6 pim log-neighbor-changes`	ネイバーのステート変更を通知する Syslog メッセージ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。
Step 3	（任意） **ipv6 pim register-policy** *policy-name* 例：	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。**match ipv6 multicast** コマンドで、グループまたはグ

	コマンドまたはアクション	目的
	`switch(config)# ipv6 pim register-policy my_register_policyinterface interfaceEnters interface mode on the specified interface. switch(config)# interface ethernet 2/1 switch(config-if)#`	ループと送信元アドレスを指定できます。デフォルトではディセーブルになっています。
Step 4	（任意） **ipv6 pim jp-policy** *policy-name* [**in** | **out**] 例： `switch(config-if)# ipv6 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イネーブルにします。**match ipv6 multicast** 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。
Step 5	（任意） **show run pim6** 例： `switch(config-if)# show run pim6`	PIM6 コンフィギュレーション コマンドを表示します。
Step 6	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	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。

PIM および PIM6 プロセスの再起動

スタティック RP が設定されている場合、PIM プロセスを再起動し、オプションとして、すべてのルートをフラッシュすることができます。デフォルトでは、ルートはフラッシュされません。

（注） Auto-RP または BSR が設定されている場合、マルチキャスト トラフィックはドロップされます（最大 60 秒間）。

フラッシュされたルートは、マルチキャスト ルーティング情報ベース（MRIB および M6RIB）、およびマルチキャスト転送情報ベース（MFIB および M6FIB）から削除されます。

PIM または PIM6 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。

PIM プロセスの再起動

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。

手順の概要

1. **restart pim**
2. **configure terminal**
3. **ip pim flush-routes**
4. （任意） **show running-configuration pim**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	**restart pim** 例： `switch# restart pim`	PIM プロセスを再起動します。 （注） 再起動プロセス中にはトラフィック損失が発生する可能性があります。

Step 2	**configure terminal**
	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。

Step 3	**ip pim flush-routes** 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。
Step 4	（任意） **show running-configuration pim** 例： `switch(config)# show running-configuration pim`	**flush-routes** コマンドを含む、PIM 実行コンフィギュレーション情報を示します。
Step 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

PIM6 プロセスの再起動

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。

手順の概要

1. **restart pim6**
2. **configure terminal**
3. **ipv6 pim flush-routes**
4. （任意） **show running-configuration pim6**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	**restart pim6** 例： `switch# restart pim6`	PIM6 プロセスを再起動します。

Step 2	**configure terminal**
	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。

Step 3	**ipv6 pim flush-routes** 例： `switch(config)# ipv6 pim flush-routes`	PIM6 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。
Step 4	（任意） **show running-configuration pim6** 例： `switch(config)# show running-configuration pim6`	**flush-routes** コマンドを含む、PIM6 実行コンフィギュレーション情報を示します。
Step 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

VRF モードでの PIM の BFD の設定

（注） VRF またはインターフェイスを使用して、PIM の双方向フォワーディング検出（BFD）を設定できます。

（注） BFD は PIM6 ではサポートされていません。

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、PIM がイネーブルになっていること、および BFD がイネーブルになっていることを確認してください。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **ip pim bfd**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**vrf context** *vrf-name*
	例：
	`switch# vrf context test`
	`switch(config-vrf)#`
		VRF 設定モードを開始します。

Step 3	**ip pim bfd** 例： `switch(config-vrf)# ip pim bfd`	指定された VRF で BFD をイネーブルにします。 （注） グローバル コンフィギュレーション モードで **ip pim bfd** コマンドを入力して、VRF インスタンス上の BFD をイネーブルにすることもできます。

インターフェイス モードでの PIM の BFD 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、PIM がイネーブルになっていること、および BFD がイネーブルになっていることを確認してください。

手順の概要

1. **configure terminal**
2. **interface** *interface-type*
3. **ip pim bfd instance**
4. （任意） **show running-configuration pim**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**interface** *interface-type*
	例：
	`switch(config)# interface ethernet 7/40`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

Step 3	**ip pim bfd instance** 例： `switch(config-if)# ip pim bfd instance`	指定したインターフェイスの BFD をイネーブルにします。VRF の BFD をイネーブルにするかどうかに関係なく、PIM インターフェイスの BFD をイネーブルまたはディセーブルにすることができます。
Step 4	（任意） **show running-configuration pim** 例： `switch(config-if)# show running-configuration pim`	PIM の実行コンフィギュレーション情報を表示します。
Step 5	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	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。

マルチキャスト ヘビー テンプレートと拡張ヘビー テンプレートの有効化

最大 32K の IPv4 mroute をサポートするために、マルチキャスト ヘビー テンプレートを有効にすることができます。

128K IPv4 ルートをサポートするには、マルチキャスト拡張ヘビー テンプレートを有効にし、マルチキャスト ルート メモリを設定する必要があります。

ヘビー テンプレートを使用すると、**show ip mroute** コマンドはマルチキャスト トラフィック カウンタを表示します。

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。

（注） **feature tunnel** コマンドが設定されている場合は、マルチキャスト ヘビー テンプレートを有効にしないでください。これは、マルチキャスト ヘビー テンプレートが適用されると、**feature tunnel** コマンドによってマルチキャスト機能が中断される可能性があるためです。

手順の概要

1. **configure terminal**
2. **system routing** *template-name*
3. **vdc** *vdc-name*
4. **limit-resource m4route-mem** [**minimum** *min-value*]**maximum** *max-value*
5. **exit**
6. **ip routing multicast mfdm-buffer-route-count** *size*
7. **ip pim mtu** *size*
8. **exit**
9. **show system routing mode**
10. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

	コマンドまたはアクション	目的

Step 2	**system routing** *template-name*
	例：
	`switch(config)# system routing template-multicast-heavy`
	`switch(config)# system routing template-multicast-ext-heavy`
	`switch(config)# system routing template-dual-stack-mcast`
		マルチキャストテンプレートを有効にします。テンプレートとしては、template-multicast-heavy または template-multicast-ext-heavy または template-dual-stack-mcast が可能です。template-multicast-heavy または template-multicast-ext-heavy テンプレートを使用する場合は、コマンドを有効にした後にシステムをリロードする必要があります。

Step 3	**vdc** *vdc-name* 例： `switch(config)# vdc vdc1`	VDC を指定し、VDC コンフィギュレーション モードを開始します。
Step 4	**limit-resource m4route-mem** [**minimum** *min-value*]**maximum** *max-value* 例： `switch(config-vdc)# limit-resource m4route-mem minimum 150 maximum 150`	VDC の IPv4 マルチキャスト ルート マップ メモリ リソース制限を設定します。このコマンドを設定した後、スタートアップ コンフィギュレーションに保存して、デバイスをリロードします。
Step 5	**exit** 例： `switch(config-vdc)# exit`	VDC コンフィギュレーション モードを終了します。
Step 6	**ip routing multicast mfdm-buffer-route-count** *size* 例： `switch(config)# ip routing multicast mfdm-buffer-route-count 400`	マルチキャスト mfdm バッファ ルート サイズを設定します。
Step 7	**ip pim mtu** *size* 例： `switch(config)# ip pim mtu 1500`	PIM コントロール プレーン トラフィックのフレーム サイズを大きくし、コンバージェンスを向上させます。
Step 8	**exit** 例： `switch(config)# exit`	グローバル コンフィギュレーション モードを終了します。

Step 9	**show system routing mode**
	例：
	`switch# show system routing mode`
	`Configured System Routing Mode: Multicast Extended Heavy Scale`
	`Applied System Routing Mode: Multicast Extended Heavy Scale`
	`Switch#`
		構成されたルーティング モード：つまりマルチキャスト ヘビーまたはマルチキャスト拡張ヘビーまたはデュアル スタックが表示されます。

	コマンドまたはアクション	目的
Step 10	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

SG-RouterID ハッシュ

SG-RouterID ハッシュ機能は、Router-ID を利用して、等コスト マルチパス（ECMP）によるスパインリーフ トポロジでの一貫性のないハッシュの問題を解決します。ハッシュに矛盾があると、マルチキャスト トラフィックのレプリケーションが非効率になり、リソース消費が増加します。

SG-RouterID ハッシュは、一貫したルータ ID を使用してこれに対処し、すべてのリーフ ノードが特定のマルチキャスト フローの同じスパイン ノードにハッシュようにします。

ルータ ID は、ネットワーク全体に一貫したマルチキャスト トラフィック分散を確保する上で重要な役割を果たします。ルータ ID は VRF ごとに構成され、PIM hello メッセージでアドバタイズされます。

SG-RouterID ハッシュの仕組み

Summary

SG-RouterID ハッシュは、SG-Next-Hopハッシュと同様に機能します。主な違いは、ネクスト ホップがルータ ID で構成された PIM ネイバーの場合、ハッシュ計算でネクスト ホップ アドレスではなくルータ ID が使用されることです。

Workflow

SG-RouterID ハッシュでは、次の手順が使用されます：

1. ルータ ID は VRF ごとに構成されます。
2. 設定されたルータ ID は、PIM の hello メッセージでアドバタイズされます。
3. インターフェイス ID hello オプション（RFC 6395）を使用すると、ルータ ID とインターフェイス ID の両方がアドバタイズされます。

   各インターフェイスには、ifIndex から派生した 32 ビットのインターフェイス ID があります。
4. ネクストホップのハッシュを計算する場合：

タイミング（When）	結果
ネクストホップが PIM ネイバーであり、ルータ ID をアドバタイズしました。	ネクストホップ アドレスの代わりに、SG ネクストホップハッシュ関数への入力としてルータ ID を活用。

タイミング（When）	結果
ネクストホップが PIM ネイバーではないか、ルータ ID がアドバタイズされていません。	ネクストホップ アドレスを SG ネクストホップ ハッシュ関数への入力として活用（通常どおり）します。

5. インターフェイス ID でのタイブレークの場合：

タイミング（When）	結果
複数のベスト ネクストホップが見つかりました	Interface-ID をタイブレーカーとして使用してハッシュを再計算します。
ネイバーがインターフェイス ID をアドバタイズしていません	ハッシュ計算では Interface-ID 0 を活用。

SG-RouterID ハッシュの利点

- **[複製の削減（Reduced Replication）]：** すべてのリーフ ノードで一貫したハッシュを確保することにより、SG-RouterID ハッシュ機能はマルチキャスト トラフィックの複製を最小限に抑えます。これは、同じデータ ストリームがネットワーク間で不必要に重複して複数回送信されることがないことを意味します。
- **[データ使用量の削減 （Reduced Data Usage）]：** レプリケーションの削減は、直接データ使用量の削減につながります。送信される重複トラフィックが少ないため、貴重な帯域幅リソースが節約されます。
- **[状態の削減（Reduced State）]：** 一貫したハッシュによって転送プロセスが簡素化され、ルータが維持する必要がある状態情報の量が削減されます。これにより、ネットワーク全体のパフォーマンスと拡張性が向上します。

SG-RouterID ハッシュの構成

このタスクでは、複数のリーフノードが同じ ECMPネ クストホップを共有するトポロジで一貫したハッシュを保証するように SG-RouterID ハッシュ機能を設定する方法について説明します。

SG-RouterID ハッシュ機能を設定するには、次の手順を活用：

始める前に

SG-RouterID ハッシュ機能を設定する前に、次の条件を満たしていることを確認します。

- デバイスのソフトウェアが SG-RouterID ハッシュ機能をサポートしていることを確認します。設定すると、この機能をサポートしていないソフトウェアバージョンへのダウングレードはブロックされます。
- 一貫したハッシュには、一貫した ECMP ネクスト ホップ セットが必要です。受信者が同じスパインのセットへの接続を離れる場合 (つまり、 ECMP ネクストホップと同じスパインを認識しない場合)、リーフは同じスパインを選択しない可能性があります。

- リーフ ノードに PIM ネイバーではないネクスト ホップがある場合、それらのすべてが同じスパインにハッシュされない可能性があります。

手順

Step 1 SG-RouterID ハッシュを有効にする。

例：

（IPv4）

```
configure terminal
ip multicast multipath sg-routerid
end
```

例：

（IPv6）

```
configure terminal
ipv6 multicast multipath sg-routerid
end
```

- このコマンドは、 VRFで SG-RouterID ハッシュをオンにします。
- このコマンドは、ハッシュがリーフによって実行されるため、スパイン リーフ トポロジのリーフ ノードで主に必要です。
- この機能を無効にするには、`no ip[v6] multicast multipath sg-routerid` を活用します。

（注）
この機能は、NBM および TRM には適用されません。

Step 2 ルータ ID を構成します。

例：

（IPv4）

```
configure terminal
vrf context <VRF-NAME>
ip pim router-id <ip-address>
end
```

例：

（IPv6）

```
configure terminal
vrf context <VRF-NAME>
ipv6 pim router-id <ip-address>
end
```

- SG-RouterID ハッシュに参加している各ルータで、各 VRF のルータ ID を設定します。
- リーフはハッシュにこれらのルータ ID を使用するため、スパイン リーフ トポロジのスパイン ノードでは主にルータ ID の構成が必要です。

- IPv6 の場合、このコマンドには 32 ビットのルータ ID（任意の IPv4 アドレスまたは識別子）が必要です。

Step 3 （任意） PIM ネイバーを優先する

例：

（IPv4）

```
configure terminal
ip multicast rpf prefer-nbr
end
```

例：

（IPv6）

```
configure terminal
ipv6 multicast rpf prefer-nbr
end
```

- このコマンドは、ハッシュの実行時に PIM ネイバーを優先するようにデバイスを構成します。
- この動作を無効にするには、`no ip[v6] multicast rpf prefer-nbr` 活用。

SG-RouterID ハッシュ構成の確認

SG-RouterID ハッシュの構成を確認するには、次のコマンドを活用：

手順

Step 1 マルチパス構成の確認

例：

```
show ip[v6] multicast vrf <VRF-NAME>
```

- このコマンドは、指定されたVRFのマルチパス構成を表示します。
- 構成されたマルチパス ハッシュとして sg-routerid が出力に表示されていることを確認します。

Step 2 PIM ネイバー情報の確認

例：

```
show ip[v6] pim neighbor internal
```

- このコマンドは、内部 PIM ネイバー情報を表示します。
- 各 PIM ネイバーのルータ ID とインターフェイス ID の出力を確認します。
- ネイバーでルータ ID が構成されている場合は、 の出力に表示されます。

Step 3 MRIB PIM キャッシュを確認します。

例：

```
show routing multicast internal pim-cache
```

- このコマンドにより、MRIB PIM キャッシュ情報が表示されます。
- 関連する VRF の「VRFの IF データベース」セクションを探します。
- ルータ ID とインターフェイス ID の「PIM ネイバー」エントリを確認します。
- 出力例：

```
Interface: Ethernet1/1, DR: 192.0.2.2,
PIM Neighbor: 192.0.2.1 uptime: 15:50:33
Interface-ID: 0.0.0.1:436208128
```

これにより、MRIB が PIM から正しいルータ ID とインターフェイス ID を学習したことが確認できます。

PIM および PIM6 設定の検証

PIM および PIM6 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。PIM の場合はコマンドの **show ip** 形式、PIM6 の場合はコマンドの **show ipv6** 形式を使用します。

コマンド	説明
show ip[**v6**] **mroute** [*ip-address*] [**detail** | **summary**]	IP または IPv6 マルチキャスト ルーティング テーブルを表示します。 **detail** オプションは、詳細なルート属性を表示します。 **summary** オプションは、ルートカウントとパケットレートを表示します。 （注） このコマンドは、マルチキャスト ヘビー テンプレートが有効になっている場合、Cisco Nexus 9300-EX および 9300-FX シリーズ スイッチのマルチキャストカウンタも表示します。以下のサンプル出力を参照してください。

コマンド	説明
show ip[**v6**] **pim df** [**vrf** *vrf-name* | **all**]	各 RP の Designated Forwarder（DF）情報をインターフェイス別に表示します。
show ip[**v6**] **pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**]	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、**show ip**[**v6**] **pim rp** コマンドを参照してください。
show ip[**v6**] **pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**]	情報をインターフェイス別に表示します。
show ip[**v6**] **pim neighbor** [**interface** *interface* | *ip-prefix*] [**vrf** *vrf-name* | **all**]	ネイバーをインターフェイス別に表示します。
show ip[**v6**] **pim oif-list** *group* [*source*] [**vrf** *vrf-name* | **all**]	発信インターフェイス（OIF）リスト内のすべてのインターフェイスを表示します。
show ip[**v6**] **pim route** [*source* | *group* [*source*]] [**vrf** *vrf-name* | **all**]	各マルチキャストルートの情報を表示します。指定した (S, G) に対して、PIM Join メッセージを受信したインターフェイスなどを表示できます。
show ip[**v6**] **pim rp** [*ip-prefix*] [**vrf** *vrf-name* | **all**]	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、**show ip**[**v6**] **pim group-range** コマンドを参照してください。
Show ip pim vrf *vrf* **detail**	PIM グレースフル SPT スイッチオーバー機能が稼働しているかどうかを表示します。

コマンド	説明
show ip pim rp-hash *group* [**vrf** *vrf-name* | **all**]	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。

コマンド	説明
show ip [**v6**] **pim config-sanity**	

コマンド	説明
	PIM 設定エラーが検出された場合、次のメッセージを表示します。 静的 RP の場合： • *interface_name* は PIM を有効にする必要があります • *interface_name* は UP である必要があります Anycast RP の場合： • Anycast-RP の *rp_address* はローカルインターフェイスで設定する必要があります • Anycast-RP の *rp_address* 、*interface_name* は PIM 対応である必要があります • Anycast-RP *rp_address* は、グループ範囲の RP として設定されていません • *interface_name* は PIM 対応である必要があります • *interface_name* は UP である必要があります • *rp_address* に設定された Anycast-RP のメンバーのいずれもローカルではありません BSR RP の場合： • BSR RP 候補インターフェイス *interface_name* が PIM/IP に対応していま

コマンド	説明
	せん • BSR RP 候補インターフェイス *interface_name* が IP に対応していません • BSR RP 候補インターフェイス *interface_name* が PIM に対応していません • *interface_name* は PIM 対応である必要があります（should be PIM enabled） • BSR 候補インターフェイス *interface_name* が PIM/IP に対応していません • BSR 候補インターフェイス *interface_name* が IP に対応していません • BSR 候補インターフェイス *interface_name* が PIM に対応していません Auto-RP の場合：

コマンド	説明
	• Auto-RP RP 候補インターフェイス *interface_name* が PIM/IP に対応していません • Auto-RP RP 候補インターフェイス *interface_name* が IP に対応していません • Auto-RP RP 候補インターフェイス *interface_name* が PIM に対応していません • *interface_name* は PIM 対応である必要があります • Auto-RP 候補インターフェイス *interface_name* が PIM/IP に対応していません • Auto-RP 候補インターフェイス *interface_name* が IP に対応していません • Auto-RP 候補インターフェイス *interface_name* が PIM に対応していません
show running-config pim [**6**]	実行コンフィギュレーション情報を表示します。
show startup-config pim [**6**]	スタートアップ コンフィギュレーション情報を表示します。
show ip[**v6**] **pim vrf** [*vrf-name* | **all**] [**detail**]	各 VRF の情報を表示します。

次の例は、**show ip mroute summary** コマンドのマルチキャスト カウンタを含む出力例を示しています。

```
switch# show ip mroute summary
IP Multicast Routing Table for VRF "default"
Route Statistics unavailable - only liveness detected

Total number of routes: 701
Total number of (*,G) routes: 0
Total number of (S,G) routes: 700
Total number of (*,G-prefix) routes: 1
Group count: 700, rough average sources per group: 1.0

Group: 224.1.24.0/32, Source count: 1
Source          packets      bytes           aps   pps       bit-rate     oifs
192.205.38.2    3110         158610          51    0         27.200  bps  5

Group: 224.1.24.1/32, Source count: 1
Source          packets      bytes           aps   pps       bit-rate     oifs
192.205.38.2    3106         158406          51    0         27.200  bps  5
```

次の例は、**show ip mroute***ip-address***summary** コマンドのマルチキャスト カウンタを含む出力例を示しています。

```
switch# show ip mroute 224.1.24.1 summary
IP Multicast Routing Table for VRF "default"
Route Statistics unavailable - only liveness detected

Total number of routes: 701
Total number of (*,G) routes: 0
Total number of (S,G) routes: 700
Total number of (*,G-prefix) routes: 1
Group count: 700, rough average sources per group: 1.0

Group: 224.1.24.1/32, Source count: 1
Source          packets      bytes           aps   pps       bit-rate     oifs
192.205.38.2    3114         158814          51    0         27.200  bps  5
```

次の例は、**show ip mroute detail** コマンドのマルチキャスト カウンタを含むサンプル出力を示しています。

```
switch# show ip mroute detail
IP Multicast Routing Table for VRF "default"

Total number of routes: 701
Total number of (*,G) routes: 0
Total number of (S,G) routes: 700
Total number of (*,G-prefix) routes: 1

(192.205.38.2/32, 224.1.24.0/32), uptime: 13:03:24, nbm(5) pim(0) ip(0)
  Data Created: No
  Stats: 3122/159222 [Packets/Bytes], 27.200  bps
  Stats: Active Flow
  Incoming interface: Ethernet1/51, uptime: 13:03:24, internal
  Outgoing interface list: (count: 5)
    Ethernet1/39, uptime: 13:03:24, nbm
    Ethernet1/40, uptime: 13:03:24, nbm
    Ethernet1/38, uptime: 13:03:24, nbm
    Ethernet1/37, uptime: 13:03:24, nbm
    Ethernet1/36, uptime: 13:03:24, nbm
```

次の例は、 **show ip mroute** *ip-address* **detail** コマンドのマルチキャスト カウンタを含む出力例を示しています。

```
switch# show ip mroute 224.1.24.1 detail
IP Multicast Routing Table for VRF "default"

Total number of routes: 701
Total number of (*,G) routes: 0
Total number of (S,G) routes: 700
Total number of (*,G-prefix) routes: 1

(192.205.38.2/32, 224.1.24.1/32), uptime: 13:00:32, nbm(5) ip(0) pim(0)
  Data Created: No
  Stats: 3110/158610 [Packets/Bytes], 27.200  bps
  Stats: Active Flow
  Incoming interface: Ethernet1/50, uptime: 12:59:04, internal
  Outgoing interface list: (count: 5)
    Ethernet1/39, uptime: 12:59:04, nbm
    Ethernet1/40, uptime: 12:59:04, nbm
    Ethernet1/38, uptime: 12:59:04, nbm
    Ethernet1/37, uptime: 12:59:04, nbm
    Ethernet1/36, uptime: 13:00:32, nbm
```

統計の表示

次に、PIM および PIM6 の統計情報を、表示およびクリアするためのコマンドについて説明します。

PIM および PIM6 の統計情報の表示

これらのコマンドを使用すると、PIMおよびPIM6の統計情報とメモリ使用状況を表示できます。

（注） PIM の場合はコマンドの **show ip** 形式、PIM6 の場合はコマンドの **show ipv6** 形式を使用します。

コマンド	説明
show ip[**v6**] **pim policy statistics**	レジスタ、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。
show ip[**v6**] **pim statistics** [**vrf** *vrf-name*]	グローバル統計情報を表示します。

PIM および PIM6 統計情報のクリア

これらのコマンドを使用すると、PIM および PIM6 統計情報をクリアできます。PIM の場合はコマンドの **show ip** 形式、PIM6 の場合はコマンドの **show ipv6** 形式を使用します。

コマンド	説明
clear ip[**v6**] **pim interface statistics** *interface*	指定したインターフェイスのカウンタをクリアします。
clear ip[**v6**] **pim policy statistics**	レジスタ、RP、およびjoin-pruneメッセージポリシーについて、ポリシーカウンタをクリアします。
clear ip[**v6**] **pim statistics** [**vrf** *vrf-name*]	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。

ヌルレジスタ パッキング

Cisco NX-OSリリース 10.5(1)F 以降では、1 つのヌルレジスタパケットで複数のマルチキャスト (S, G) を送信し、PIM ルータでのパケット処理のオーバーヘッドを削減するようにヌルレジスタパッキングを構成できます。この機能は、RFC 9465 に従って実装されています。

RP と DR は S, G ごとに選択されるため、RP と DR でこの機能を構成します。DR は、各 (S, G) のヌルレジスタを定期的に RP に送信します。この機能を使用すると、複数の (S, G) が 1 つのパック済みヌルレジスタにパッキングされ、RP に送信されます。パッキングを有効にするには、RP と DR の両方で構成を有効にする必要があります。

ヌルレジスタパッキングの構成

ヌルレジスタパッキングを構成するには、次のコマンドを実行します。この機能は、構成されている場合、 PIM グローバル MTU を使用しません。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **ip pim register-packing [mtu <mtu-size>] [reg-probe-timer <interval>]**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

	コマンドまたはアクション	目的

Step 2	**vrf context** *vrf-name*
	例：
	`switch# vrf context test`
	`switch(config-vrf)#`
		VRF 設定モードを開始します。

Step 3	**ip pim register-packing [mtu <mtu-size>] [reg-probe-timer <interval>]**
	例：
	`switch# ip pim register-packing mtu 1500`
	`switch# ip pim register-packing reg-probe-timer 400`
	`switch# ip pim register-packing mtu 700 reg-probe-timer 400`
		ヌルレジスタパッキングを構成します。
		単に機能を有効にするには、 **ip pim register-packing** を実行します。
		MTU またはプローブ間隔のいずれか、または両方を指定することも、いずれも指定しないことも選択できます。
		<mtu-size>：デフォルト値は 576 で、576 ～ 9216 の値を選択できます。
		<interval>：デフォルト値は 60 で、60 ～ 65535 の値を選択できます。

マルチキャスト サービス リフレクションの設定

マルチキャスト サービス リフレクション機能は、外部で受信したマルチキャスト宛先アドレスを、組織の内部アドレッシング ポリシーに準拠したアドレスに変換できます。これは、外部で受信したマルチキャスト ストリーム (S1,G1) から内部ドメインの (S2, G2) への、マルチキャスト ネットワーク アドレス変換（NAT）です。送信元 IP アドレスのみを変換する IP NAT とは異なり、マルチキャスト サービス リフレクションは、送信元と宛先アドレスの両方を変換します。

入力 NAT では、着信（S、G）を別の送信元、グループ、またはその両方に変換できます。ドメイン内のすべての受信者は、変換後のフローに参加できます。この機能は、マルチキャスト トラフィックが次の場合に役立ちます。

- アドレスが重複している可能性がある別のドメインからネットワークに入る
- ネットワーク内のアプリケーションによって認識されないアドレスが付属しています

出力 NAT では、既存のフロー（S、G）を、発信インターフェイスごとに異なる送信元またはグループアドレスに変換できます。この機能は、特定のソース、グループアドレスのみを受け入れる可能性のある外部エンティティへのマルチキャスト配信に役立ちます。また、フローが外部エンティティに公開されるときに、内部アドレス空間を非表示にする方法として機能することもできます。

マルチキャスト サービス リフレクション機能は、VRF コンフィギュレーション モードのループバック インターフェイスで設定されます。S1、G1 として着信するフローは S2、G2 に変換され、宛先 MAC アドレスは変換済みアドレス（G2）のマルチキャスト MAC アドレスに書き換えられます。

ユニキャストからマルチキャストへの NAT（UM NAT）

Cisco NX-OS リリース 10.2(2)F 以降、ユニキャストからマルチキャスト NAT (UMNAT) への変換がサポートされています。UMNAT は入力 NAT であり、出力 NAT のソフトウェア設計に従います。

UM NAT では、事前変換されたユニキャスト トラフィックが到着するポートでユニキャスト帯域幅の予約を設定することにより、そのポートのマルチキャスト トラフィックがポートの帯域幅すべてを消費してしまわないようにする必要があります。

マルチキャスト サービス リフレクションの注意事項と制限事項

マルチキャスト サービス リフレクション機能には、次の注意事項と制限事項があります。

- マルチキャスト サービス リフレクション機能は Cisco NX-OS リリース 9.3(5) で導入され、Cisco Nexus 9300-FX、FX2、FXP、EX シリーズ スイッチでサポートされています。
- Cisco NX-OS リリース 9.3(5)F 以降、マップ インターフェイスの最大複製の範囲は 1 ～ 40 です。
- Cisco NX-OS リリース 9.3(3)F 以降、マルチキャスト NAT は、Cisco Nexus C9300-GX でサポートされます。
- Cisco NX-OS リリース 10.2(1)F 以降、マルチキャスト NAT は、Cisco Nexus C9300-GX2B でサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、マルチキャスト NAT は、Cisco Nexus C9332D-H2R でサポートされます。
- Cisco NX-OS リリース 10.4(2)F 以降、マルチキャスト NAT は、Cisco Nexus C93400LD-H1 でサポートされます。
- Cisco NX-OS リリース 10.4(3)F 以降、マルチキャスト NAT は、Cisco Nexus C9364C-H1 および C9300-FX3 でサポートされます。
- Cisco NX-OS リリース 10.5(2)F 以降、マップ インターフェイスの最大複製の範囲が 1 ～ 250 に増加しています。この拡張範囲は、マルチキャスト NAT をサポートするすべてのプラットフォームでサポートされます。
  - 40 を超えるマップ インターフェイスが構成されている場合、10.5(2)F よりも前のリリースにダウングレードすると、エラーが発生します。このエラーを回避するには、サービス リフレクション構成を削除し、レプリケーション インターフェイスの数を 40 以下に減らして、ソフトウェアのダウングレードを実行します。
  - 250 のレプリケーション マップ インターフェイスのプロビジョニングには、最大 3 分かかる場合があります。
- Cisco NX-OS リリース 10.1(1)F 以降、NBM を使用したマルチキャスト サービス リフレクションは、Cisco Nexus 9300-FX3、Cisco Nexus C9316D-GX、Cisco Nexus C93600CD-GX、および Cisco Nexus C9364C-GX プラットフォーム スイッチでサポートされています。

- マルチキャストサービスリフレクション機能は、以下のプラットフォームではサポートされていません
  - クラウド スケール ライン カード搭載の Cisco Nexus 9500 シリーズ スイッチ
  - R シリーズ ライン カード搭載の Cisco Nexus 9500 シリーズ スイッチ
  - Cisco Nexus 3600-R シリーズ スイッチ
  - Cisco Nexus 9200 シリーズ スイッチ
  - Cisco Nexus 9364C スイッチ
- マルチキャストサービスリフレクション機能は、Protocol Independent Multicast（PIM）スパース モード（ASM または SSM）でのみサポートされます。
- マルチキャスト サービス リフレクション機能は、vPC 環境では機能しません。
- マルチキャストからユニキャストへの NAT は、Cisco NX-OS リリース 10.2(1)F からサポートされています。
- マルチキャストからユニキャストへの NAT 変換は、出力モードでのみサポートされます。
- マルチキャストからユニキャストへの NAT 変換は、Cisco Nexus 9300-FX、FX2 スイッチでサポートされています。
- マルチキャストからユニキャストへの変換は、Cisco NX-OS リリース 10.1(x) ではサポートされていません。
- PIM パッシブ モードでのマルチキャストからユニキャスト NAT への PMN サポート。
- リリース 10.2(2)F から、ユニキャストからマルチキャストへの NAT 変換がサポートされます。
- マルチキャストからマルチキャストおよびユニキャストからユニキャストへの NAT 構成は、同時に同時に行うことはできません。
- ユニキャスト NAT、マルチキャスト NAT、および PBR 機能は、同じデバイスでは同時にサポートされません。
- 出力 NAT 機能は、デフォルトの VRF でのみサポートされ、他の VRF ではサポートされません。
- FEX はサポートされていません。
- NAT ルールが事前変換済み（S1, G1）ペアに設定されている場合、マルチキャスト サービス リフレクション機能は、このペアの非 NAT レシーバーをサポートしません（つまり、出力 NAT は事前変換済み（S,1, G1）レシーバーをサポートするのに対し、入力 NAT はそれらをサポートしません）。変換されていない受信側 OIF は、出力 NAT でサポートされます。
- SVI は、RPF および OIF ではサポートされていません。
- 変換後の出力NAT グループのサブインターフェイス レシーバーはサポートされていません。

- マルチキャストサービスリフレクション構成用に選択されたハードウェアループバックポートは、「リンクダウン」状態で、SFPが接続されていない物理ポートである必要があります。
- マスク長が 0 ～ 4 の場合、マルチキャスト NAT 変換は行われません。このマスク長の制限は、グループ アドレスのみに適用され、送信元アドレスには適用されません。
- Cisco NX-OS リリース 10.2(1q)F 以降、マルチキャスト NAT は Cisco Nexus N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。
- インターフェイスでの IGMP 静的結合の場合、結合を生成するために /24 のグループ範囲マスクが使用されます。送信元マスク長は /32 と見なされます。**ip igmp static** 結合コマンドで結合を生成する際に、送信元マスク長の変動は考慮されません。

マルチキャストサービスリフレクション機能用に設定されたデバイスの入力および出力インターフェイス ACL には、次の制限があります。

- 入力 ACL が適用されて、すでに流れている未変換のマルチキャスト トラフィックをブロックする場合、（S,G）エントリは削除されません。その理由は、ACL がパケットをドロップしても、マルチキャストルートエントリが引き続きトラフィックによってヒットされるためです。
- 出力インターフェイスで変換されたソーストラフィック（S2、G2）をブロックする出力ACLが適用されている場合、変換されたトラフィックに対して出力ACLがサポートされていないため、出力 ACL は機能しません。

  マルチキャスト出力NATは、 PMNパッシブ モードでサポートされます。PIMパッシブ モードでは、外部コントローラがフローの帯域幅管理を実行し、変換前と変換後の両方のフローをプロビジョニングします。

  事前変換済みフローの場合、コントローラはスイッチ Rest API を呼び出して、事前変換済みフローが OIF なしで受信される RPF インターフェイスに対し、プロビジョニングを行います。

  変換後のフローの場合、コントローラはスイッチ Rest API を呼び出して、サービス リフレクト送信元ループバック インターフェイスと同じ RPF インターフェイスと、SR ルールで定義されたインターフェイスと同じ OIF をプロビジョニングします。

前提条件

マルチキャスト サービス リフレクション機能には、次の前提条件があります。

マルチキャストサービスリフレクション機能をサポートするプラットフォームでは、マルチキャスト NAT を設定する前に TCAM を分割する必要があります。次のコマンドを使用します。

hardware access-list tcam region mcast-nat *region tcam-size*

マルチキャスト サービス リフレクションの設定

始める前に

- マルチキャスト対応のネットワークで、Protocol Independent Multicast Sparse Mode（PIM-SM）または PIM Source-Specific Multicast（PIM-SSM）のいずれかが動作していることを確認します。
- マルチキャストサービスリフレクション用仮想インターフェイスがNATルータで設定され、マルチキャスト サービス リフレクション ルールがインストールされ、動作することを確認します。

手順の概要

1. **configure terminal**
2. **vrf context** *name*
3. **[no] ip service-reflect source-interface** *interface-name interface-number*
4. **[no] ip service-reflect destination** *in-grp* **to** *out-grp* **mask-len** *g-mlen* **source** *in-src* **to** *out-src* **mask-len** *s-mlen*[**to-udp** *udp-to-src-port udp-to-dest-port*] [**to-udp-src-port** *udp-to-src-port*] [**to-udp-dest-port** *udp-to-dest-port*]
5. **[no] ip service-reflect mode egress** *prefix*
6. **[no] ip service-reflect destination** *in-grp* **to** *out-grp* **mask-len** *g-mlen* **source** *in-src* **to** *out-src* **mask-len** *s-mlen*[**to-udp** *udp-to-src-port udp-to-dest-port*] [**to-udp-src-port** *udp-to-src-port*] [**to-udp-dest-port** *udp-to-dest-port*] [**static-oif** *out-if*]
7. **[no] multicast service-reflect interface all map interface** *interface-name* **max-replication** *replication*
8. **exit**
9. **interface** *interface-name interface-number*
10. **ip address** *prefix*
11. **ip pim sparse-mode**
12. **ip igmp static-oif** {*group* [**source** *source*] |**route-map** *policy-name*}
13. **no system multicast dcs-check**
14. **ip pim border-router**
15. **nbm external-link**
16. **exit**
17. **[no] multicast service-reflect interface all map interface** *interface-name* **vrf** *vrf-name*
18. **[no] multicast service-reflect interface** *interface-name* **map interface** *interface-name***vrf** *vrf-name*
19. **[no] multicast service-reflect interface** *interface-1, interface-2, interface-3***map interface** *interface-name***vrf** *vrf-name*
20. **exit**
21. **show ip mroute sr**
22. **show forwarding distribution multicast route**
23. **show forwarding distribution multicast route group**

手順の詳細

手順

	コマンドまたはアクション	目的

Step 1	**configure terminal**
	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。

Step 2	**vrf context** *name*
	例：
	`switch(config)# vrf context test`
	`switch(config-vrf)#`
		新しい VRF を作成し、VRF 設定モードを開始します。*name* には最大 32 文字の英数字を使用できます。大文字と小文字は区別されます。NAT ルールは、vrf コンテキストで構成されます。
		（注）
		デフォルト以外の VRF は、出力 NAT ではサポートされていません。

Step 3	**[no] ip service-reflect source-interface** *interface-name interface-number* 例： `switch(config-vrf)# ip service-reflect source-interface loopback10`	NAT ソースとしてループバックを設定します。このインターフェイスは、トラフィックを NAT ルーターにプルします。インターフェイスは、変換後のルートの RPF になります。このコマンドは、VRF ごとに設定されます。
Step 4	**[no] ip service-reflect destination** *in-grp* **to** *out-grp* **mask-len** *g-mlen* **source** *in-src* **to** *out-src* **mask-len** *s-mlen*[**to-udp** *udp-to-src-port udp-to-dest-port*] [**to-udp-src-port** *udp-to-src-port*] [**to-udp-dest-port** *udp-to-dest-port*] 例： `switch(config-vrf)# ip service-reflect destination 228.1.1.1 to 238.1.1.1 mask-len 32 source 80.80.80.80 to 90.90.90.90 mask-len 32 to-udp-src-port 500 to-udp-dest-port 600`	入力 NAT の NAT ルールを設定します。
Step 5	**[no] ip service-reflect mode egress** *prefix* 例： `switch(config-vrf)# ip service-reflect mode egress 225.1.1.0/24`	出力 NAT モードを設定します。インターフェイスにルーティングされたマルチキャスト パケットを照合し、リライトします。 （注） 出力 NAT は、デフォルトの VRF でのみサポートされます。
Step 6	**[no] ip service-reflect destination** *in-grp* **to** *out-grp* **mask-len** *g-mlen* **source** *in-src* **to** *out-src* **mask-len** *s-mlen*[**to-udp** *udp-to-src-port udp-to-dest-port*]	出力 NAT の NAT ルールを設定します。

	コマンドまたはアクション	目的
	[**to-udp-src-port** *udp-to-src-port*] [**to-udp-dest-port** *udp-to-dest-port*] [**static-oif** *out-if*] 例： `switch(config-vrf)# ip service-reflect destination 225.1.1.1 to 227.1.1.1 mask-len 32 source 10.10.10.100 to 20.10.10.101 mask-len 32 to-udp-src-port 33 to-udp-dest-port 66 static-oif Ethernet1/8`	
Step 7	**[no] multicast service-reflect interface all map interface** *interface-name* **max-replication** *replication* 例： `switch(config-vrf)# multicast service-reflect interface all map interface Ethernet1/54 max-replication 3`	マップインターフェイスの最大レプリケーション数を指定します。範囲は 1 ～ 40 です。デフォルト値は 40 です。 Cisco NX-OS リリース 10.5(2)F 以降、範囲は 1 ～ 250 に増加しています。デフォルト値は 40 です。 このコマンドの **no** 形式は、構成を削除します。
Step 8	**exit** 例： `switch(config-vrf)# exit switch(config)#`	VRF コンフィギュレーション モードを終了して、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。
Step 9	**interface** *interface-name interface-number* 例： `switch(config)# interface loopback10 switch(config-if)#`	インターフェイス設定モードを開始します。
Step 10	**ip address** *prefix* 例： `switch(config-if)# ip address 1.1.1.1/24`	ループバック インターフェイスの IP アドレスを設定します。このルータの識別に役立つ一意の IP アドレスになります。
Step 11	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	インターフェイスで PIM スパース モードをイネーブルにします。デフォルトではディセーブルになっています。
Step 12	**ip igmp static-oif** {*group* [**source** *source*] |**route-map** *policy-name*} 例： `switch(config-if)# ip igmp static-oif 230.1.1.1`	マルチキャスト グループを発信インターフェイスに静的にバインドし、デバイス ハードウェアで処理します。グループ アドレスのみを指定した場合は、（*, G）ステートが作成されます。送信元アドレスを指定した場合は、（S, G）ステートが作成されます。**match ip multicast** コマンドで、使用するグループ プレフィックス、グループ範囲、および送信元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。

	コマンドまたはアクション	目的
		設定されたループバック インターフェイスが NAT 対象のマルチキャスト ストリームに参加できるようにします。
Step 13	**no system multicast dcs-check** 例： `switch(config-if)# no system multicast dcs-check`	ルート学習のために、非 FHR デバイスの CPU にマルチキャスト パケットをパントできるようにします。これは通常、 または の機能が有効になっているときに使用されます。**ip pim border-router ip igmp host-proxy** このコマンドは、Cisco Nexus 9300 シリーズおよび Cisco Nexus 9200 シリーズの EOR スイッチ、Cisco Nexus 9504 および Cisco Nexus 9508 の EOR および TOR スイッチ、および N3K-C3636C-R、N3K-C36180YC-R TOR スイッチではサポートされていません。
Step 14	**ip pim border-router** 例： `switch(config-if)# ip pim border-router`	PIM-SM ドメインの外部のソースからのトラフィックがドメイン内の受信者に到達することを確認し、リモートから送信されたトラフィックがこのドメイン内のローカルの受信者に到達できるようにします。 PIM メッセージが PIM ドメイン境界を通過できない場合は、PIM 境界ルータが必要です。
Step 15	**nbm external-link** 例： `switch(config-if)# nbm external-link`	マルチサイト ソリューションで複数のファブリックを接続するために、NBM インターフェイスを外部リンクとして設定します。 （注） このコマンドは、機能 NBM が有効になっていて、**ip pim border-router** コマンドが有効になっているリンク上でのみ必要です。

Step 16	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了して、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。

Step 17	**[no] multicast service-reflect interface all map interface** *interface-name* **vrf** *vrf-name* 例： `switch(config)# multicast service-reflect interface all map interface loopback10 vrf test`	すべてのファンアウトインターフェイスをサービス インターフェイスにマッピングします。 （注） **vrf** *vrf-name* オプションは、出力 NAT ではサポートされていません。 （注）

	コマンドまたはアクション	目的
		ステップ 17、18、および 19 のコマンドは、出力 NAT の場合にのみ必要です。Egress NAT ルール構成で使用される各 OIF は、これらのマッピング構成のいずれかを使用して、1 つのサービス インターフェイスにマッピングする必要があります。
Step 18	**[no] multicast service-reflect interface** *interface-name* **map interface** *interface-name***vrf** *vrf-name* 例： `switch(config)# multicast service-reflect interface ethernet1/18 map interface loopback10 vrf test`	ファンアウト インターフェイスからサービス インターフェイスへの 1 対 1 のマッピングを設定します。
Step 19	**[no] multicast service-reflect interface** *interface-1, interface-2, interface-3***map interface** *interface-name***vrf** *vrf-name* 例： `switch(config)# multicast service-reflect interface ethernet 1/1-10, ethernet1/12-14, ethernet1/16 map interface loopback10 vrf test`	ファンアウト インターフェイスからサービス インターフェイスへの 多対 1 のマッピングを設定します。
Step 20	**exit** 例： `switch(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
Step 21	**show ip mroute sr** 例： `switch# show ip mroute sr`	サービス リフレクション mroute エントリを表示します。
Step 22	**show forwarding distribution multicast route** 例： `switch# show forwarding distribution multicast route`	出力 NAT の変換前および変換後のルート情報、および入力 NAT の変換前のルート情報に関する情報を表示します。
Step 23	**show forwarding distribution multicast route group** 例： `switch# show forwarding distribution multicast route group`	マルチキャスト FIB 配布 IPv4 マルチキャスト ルートに関する情報を表示します。

マルチキャスト サービス リフレクションの設定例

次の例は、マルチキャスト NAT 入出力ポートの設定を示しています。

```
interface loopback0
  ip address 20.1.1.2/24
```

```
  ip pim sparse-mode
  ip igmp static-oif 225.1.1.1

hardware access-list tcam region mcast-nat 512

<<Ingress NAT>>

ip route 30.1.1.0/24 10.1.1.1
ip pim ssm range 232.0.0.0/8
ip service-reflect source-interface loopback0
ip service-reflect mode ingress 235.1.1.0/24
ip service-reflect destination 235.1.1.1 to 234.1.1.1 mask-len 32 source 30.1.1.70 to
20.1.1.70 mask-len 32
hardware access-list tcam region mcast-nat 512

<<Egress NAT>>

ip route 30.1.1.0/24 10.1.1.1
ip pim ssm range 232.0.0.0/8
ip service-reflect mode egress 225.1.1.0/24
ip service-reflect destination 225.1.1.1 to 224.1.1.1 mask-len 32 source 30.1.1.1 to 20.1.1.1
 mask-len 32 static-oif port-channel40
ip service-reflect destination 225.1.1.1 to 224.1.1.100 mask-len 32 source 30.1.1.1 to
20.1.1.100 mask-len 32 static-oif port-channel40
ip service-reflect destination 225.1.1.1 to 224.1.1.101 mask-len 32 source 30.1.1.1 to
20.1.1.101 mask-len 32 static-oif port-channel40
ip service-reflect destination 235.1.1.1 to 234.1.1.1 mask-len 32 source 30.1.1.70 to
20.1.1.70 mask-len 32
multicast service-reflect interface all map interface Ethernet1/21
hardware access-list tcam region mcast-nat 512
interface Ethernet1/21
  link loopback
  no shutdown
interface Ethernet1/21.1
  encapsulation dot1q 10
  no shutdown
interface Ethernet1/21.2
  encapsulation dot1q 20
  no shutdown
interface Ethernet1/21.3
  encapsulation dot1q 30
  no shutdown
interface Ethernet1/21.4
  encapsulation dot1q 40
  no shutdown
```

次の例は、マルチキャスト サービス リフレクションの show コマンドの表示/出力を示しています。

```
switch# show ip mroute sr
IP Multicast Routing Table for VRF "default"
(30.1.1.1/32, 225.1.1.1/32), uptime: 01:29:45, ip mrib pim
  NAT Mode: Egress
  NAT Route Type: Pre
  Incoming interface: Ethernet1/1, RPF nbr: 10.1.1.1
  Outgoing interface list: (count: 1)
    loopback0, uptime: 01:29:45, mrib
       SR: (20.1.1.1, 224.1.1.1) OIF: port-channel40
       SR: (20.1.1.100, 224.1.1.100) OIF: port-channel40
       SR: (20.1.1.101, 224.1.1.101) OIF: port-channel40

(30.1.1.70/32, 235.1.1.1/32), uptime: 01:05:12, ip mrib pim
  NAT Mode: Ingress
  NAT Route Type: Pre
```

```
  Incoming interface: Ethernet1/1, RPF nbr: 10.1.1.1
  Outgoing interface list: (count: 1)
    loopback0, uptime: 01:05:12, mrib
       SR: (20.1.1.70, 234.1.1.1)

switch# show ip mroute 234.1.1.1 detail
IP Multicast Routing Table for VRF "default"
Total number of routes: 26
Total number of (*,G) routes: 19
Total number of (S,G) routes: 6
Total number of (*,G-prefix) routes: 1

(20.1.1.70/32, 234.1.1.1/32), uptime: 01:06:30, mrib(0) ip(0) pim(0) static(1)
  RPF-Source: 20.1.1.70 [0/0]
  Data Created: Yes
  Stats: 499/24259 [Packets/Bytes], 27.200  bps
  Stats: Active Flow
  Incoming interface: loopback0, RPF nbr: 20.1.1.70
  LISP dest context id: 0  Outgoing interface list: (count: 1) (bridge-only: 0)
    port-channel40, uptime: 00:59:20, static

switch# show forwarding distribution multicast route
IPv4 Multicast Routing Table for table-id: 1
Total number of groups: 22
Legend:
   C = Control Route
   D = Drop Route
   G = Local Group (directly connected receivers)
   O = Drop on RPF Fail
   P = Punt to supervisor
   L = SRC behind L3
   d = Decap Route
   Es = Extranet src entry
   Er = Extranet recv entry
   Nf = VPC None-Forwarder
   dm = MVPN Decap Route
   em = MVPN Encap Route
   IPre = Ingress Service-reflect Pre
   EPre = Egress Service-reflect Pre
   Pst = Ingress/Egress Service-reflect Post

  (30.1.1.70/32, 235.1.1.1/32), RPF Interface: Ethernet1/1, flags: IPre
    Upstream Nbr: 10.1.1.1
    Received Packets: 25 Bytes: 1625
    Number of Outgoing Interfaces: 1
    Outgoing Interface List Index: 4
      port-channel40

  (20.1.1.1/32, 224.1.1.1/32), RPF Interface: loopback0, flags: Pst
    Upstream Nbr: 20.1.1.1
    Received Packets: 0 Bytes: 0
    Number of Outgoing Interfaces: 1
    Outgoing Interface List Index: 2
      port-channel40

  (20.1.1.100/32, 224.1.1.100/32), RPF Interface: loopback0, flags: Pst
    Upstream Nbr: 20.1.1.100
    Received Packets: 0 Bytes: 0
    Number of Outgoing Interfaces: 1
    Outgoing Interface List Index: 2
      port-channel40

  (20.1.1.101/32, 224.1.1.101/32), RPF Interface: loopback0, flags: Pst
    Upstream Nbr: 20.1.1.101
    Received Packets: 0 Bytes: 0
```

```
    Number of Outgoing Interfaces: 1
    Outgoing Interface List Index: 2
      port-channel40

switch# show forwarding multicast route group 235.1.1.1 source 30.1.1.70
slot  1
=======
  (30.1.1.70/32, 235.1.1.1/32), RPF Interface: Ethernet1/1, flags: c
    Received Packets: 18 Bytes: 1170
    Outgoing Interface List Index: 4
    Number of next hops: 1
    oiflist flags: 16384
  Outgoing Interface List Index: 0x4
    port-channel40
```

ユニキャストからマルチキャスト NAT へ

ユニキャストからマルチキャストへの NAT は、入力変換モードで機能します。マルチキャスト変換されたパケットは、出力変換してマルチキャストに戻すことができます。ユニキャスト パケットの宛先アドレスは、NAT サービス リフレクション インターフェイスと一致する必要があります。

ユニキャストからマルチキャストへの NAT は、1:1 の変換をサポートします。マルチキャストから別のマルチキャストへの変換がサポートされるチェーン変換。マルチキャストからマルチキャストへの変換は、1 対多でサポートされます。変換が機能するためには、ソース IP、プリおよびポストがサービス インターフェイス ループバック上にある必要があります。

ユニキャストからマルチキャストへの NAT は、N9K-C93180YC-FX、N9K-C93180YC2-FX、N9K-C93180YC-FX-24、N9K-C93108TC-FX、N9K-C93108TC2-FX、N9K-C93108TC-FX-24、N9K-C9348GC-F、N9K-C9348GC-FXP、N9K-C9348GC2-FXP、N9K-C9358GY-FXP、N9K-C92348GC、N9K-X9732C-FX、N9K-C9336C-FX2、N9K-C93240YC-FX2、N9K-C93300YC-FX2、N9K-C93240YC-FX2-Z、N9K-C93360YC-FX2、N9K-C93216TC-FX2、N9K-C9336C-FX2-E、N9K-C93180YC-FX3S、N9K-C93180YC-FX3、N9K-C93108TC-FX3P、N9K-C93360YC-FX3、N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX、N9K-C9364D-GX2A、N9K-C9332D-GX2B、N9K-C93560LD-GX2B、および N9K-C9348D-GX2A プラットフォームでサポートされています。

ユニキャストからマルチキャストへの NAT でサポートされるスケール

各変換フローには、1 つの ACL をインストールする必要があります。これは 2 パス ソリューションであるため、サービス インターフェイスの帯域幅によって変換数が制限されます。ユニキャストからマルチキャストへの変換のみを行うボックスの場合、最大2047の変換までスケールアップできます。

（注） ユニキャストからマルチキャストへの NAT 変換を組み合わせたセットアップでは、変換の最大数は 1976 を超えてはなりません。

出力 NAT プラットフォーム再循環サービス インターフェイス

変換後のマルチキャスト グループ IP に基づいて、プラットフォーム再循環インターフェイスの設定には、ユニキャストからマルチキャストへの NAT フローを提供する宛先プレフィックスを選択するためのオプションがあります。各フローの帯域幅要件に基づいて、複数のより小さな帯域幅フローは、同じ再循環インターフェイスを共有できます。再循環インターフェイスを使用して変換後のルートを追跡するために、マルチキャストからユニキャスト NAT およびユニキャストからマルチキャスト NAT への個別の結合データベースが維持されています。

ユニキャストからマルチキャストの場合、MFDM は親インターフェイスをサービス ループバック インターフェイスとして選択し、同じサービス インターフェイスを複数のルートで共有できるようにします。パケットがサービス ループバック インターフェイスから再循環された後に FIB ルックアップが実行されるため、MFDM は RPF をサービス ループバック インターフェイスとして上書きします。ACL は、redirect_ptr および nat_ptr をドライブする修飾子としてユニキャスト送信元 IP および宛先 IP を使用し、ユニキャストからマルチキャスト NAT にプログラムされます。redirect_ptr は、サービス ループバック インターフェイスから出るパケットをドライブします。nat_ptr は、ユニキャストからマルチキャストへの NAT 設定に基づいて、送信元 IP、宛先 IP、および L4 ポート情報を変換します。redirect_ptr は、同じサービス ループバック インターフェイスを共有する複数のルートで共有されます。

ユニキャストからマルチキャストへの NAT 変換

ユニキャストからマルチキャストへの変換では、ユーザーがソース インターフェイスを構成する必要があります。ここでは、変換後のマルチキャスト ソースがソース インターフェイス サブネットに分類される必要があります。ユニキャストからマルチキャストへの変換では、着信トラフィックがユニキャスト アドレスであるため、モード設定は必要ありません。送信元インターフェイスを設定するためのコマンドは次のとおりです。

ip service-reflect source-interface <interface>

ルール構成では、変換のためにユニキャスト アドレスとマルチキャスト アドレスを受け取ります。次に、例を示します。

```
ip service-reflect destination 1.2.3.4 to 227.1.1.1
mask-len 32 source 21.1.1.1 to 57.1.1.51
mask-len 32 to-udp-src-port 1000 to-udp-dest-port 500
```

MRIB 表示コマンド

次に、MRIB ユニキャストからマルチキャスト NAT への show コマンドを示します。

show ip mroute sr umnat

ユニキャストからマルチキャストへの NAT の設定は次のとおりです。

```
ip service-reflect destination 1.2.3.4 to 227.1.1.1
mask-len 32 source 21.1.1.1 to 57.1.1.51
mask-len 32 to-udp-src-port 1000 to-udp-dest-port 500

ip service-reflect destination 1.2.3.5 to 227.1.1.1
mask-len 32 source 21.1.1.1 to 57.1.1.51
mask-len 32

ip service-reflect destination 227.1.1.1 to 229.1.1.1
```

```
mask-len 32 source 57.1.1.51 to 21.1.1.2
mask-len 32 static-oif Ethernet1/7

switch(config)# show ip mroute sr umnat
IP Multicast Routing Table for VRF "default"
(21.1.1.1/32, 1.2.3.4/32)
Translation:
SR: (57.1.1.51/32, 227.1.1.1/32) udp src: 1000, udp dst : 500
Outgoing interface list: (count: 1)
loopback100, uptime: 1d01h, static
Chained translations:
SR: (21.1.1.2, 229.1.1.1) OIF: Ethernet1/7
(21.1.1.1/32, 1.2.3.5/32)
Translation:
SR: (57.1.1.51/32, 227.1.1.1/32) udp src: 0, udp dst : 0
Outgoing interface list: (count: 1)
loopback100, uptime: 1d01h, static
Chained translations:
SR: (21.1.1.2, 229.1.1.1) OIF: Ethernet1/7
```

MFDM Show コマンド

次に、MFDM ユニキャストからマルチキャスト NAT への show コマンドを示します。

```
ip service-reflect destination 10.2.3.4 to 239.1.1.1
mask-len 32 source 10.1.1.1 to 8.8.8.8
mask-len 32 to-udp-src-port 10 to-udp-dest-port 20

ip service-reflect destination 10.2.3.5 to 225.1.1.1
mask-len 32 source 10.1.1.2 to 9.9.9.9
mask-len 32

switch(config)# show forwarding distribution multicast route sr um-nat
(10.1.1.1, 10.2.3.4 -> 8.8.8.8, 239.1.1.1) L4(0,0) SrcIf(Ethernet1/31)
(10.1.1.2, 10.2.3.5 -> 9.9.9.9, 225.1.1.1) L4(0,0) SrcIf(Ethernet1/32)
```

MFIB 表示コマンド

次に、MFIB ユニキャストからマルチキャストへの NAT の表示コマンドを示します。

```
show forwarding multicast-sr internal-db
Encap 3 (10.1.1.1, 10.2.3.4 -> 8.8.8.8, 239.1.1.1) L4(0,0) SrcIf(Ethernet1/31) Flags(0x0)
Encap 4 (10.1.1.2, 10.2.3.5 -> 9.9.9.9, 225.1.1.1) L4(0,0) SrcIf(Ethernet1/32) Flags(0x0)
```

ACLQOS Show コマンド

ユニキャストからマルチキャストへの NAT のデータベースを表示するには、次のコマンドを使用します。

```
sh system internal aclqos multicast sr hw-to-redir-db <=
Displays ACL hardware index to Redirect index database
```

ユニキャストからマルチキャストへの NAT 変換ルールの設定

次に、ユニキャストからマルチキャストへの NAT の変換ルール設定の例を示します。

```
ip service-reflect destination 1.2.3.4 to 227.1.1.1 mask-len 32 source 21.1.1.1 to 57.1.1.51
 mask-len 32 to-udp-src-port 1000 to-udp-dest-port 500
{
"mribRule": {
"attributes": {
"childAction": "",
```

```
"dn":
"sys/mib/inst/dm-default/sr/rule/pregp-[1.2.3.4]-postgp-[227.1.1.1]-gm-32-presrc-[21.1.1.1]-postsrc-[57.1.1.51]-sm-32-srcudp-1000-destudp-500-oif-[unspecified]",
"grpMasklen": "32",
"modTs": "2021-07-24T02:13:54.360+00:00",
"postTransGrp": "227.1.1.1",
"postTransSrc": "57.1.1.51",
"preTransGrp": "1.2.3.4",
"preTransSrc": "21.1.1.1",
"srcMasklen": "32",
"staticOif": "unspecified",
"status": "",
"udpDestPort": "500",
"udpsrcPort": "1000"
}
}
}
```


マルチキャストからユニキャスト NAT

マルチキャストからユニキャストへの NAT は、コンテンツをパブリック クラウドにホストするために使用されます。クラウドがマルチキャストをサポートしていない可能性があるため、変換が必要です。変換後、ユニキャスト パケットはユニキャスト転送ロジックに従ってルーティングされます。

異なるサイトに接続する場合も同様の使用例が見られます。コアがエンド ツー エンドのマルチキャストをサポートしていない場合、コンテンツはさまざまなサイトにユニキャストとして配信されます。境界ボックスは、マルチキャストをユニキャストに変換し、消費のためにさまざまなサイトに配信します。

MU NAT の場合、PMN は、事前に変換されたマルチキャスト フローの帯域幅管理を引き続き実行します。変換されたユニキャスト フローの場合、変換されたユニキャスト トラフィックが中断することなく送信されるように、発信インターフェイスはユニキャスト帯域幅を予約する必要があります。PMN は、NAT 関係を示すためにフロー操作 MO も発行します。ユニキャスト変換ごとに内部で 3 つの再循環が発生するため、再循環ポート帯域幅の 3 分の 1 だけが想定されていることを確認する必要があります。再循環に使用されるサービス リフレクト マップ インターフェイスで輻輳が発生した場合、PMN は障害 MO を公開しません。

PIM パッシブ モードでは、コントローラは帯域幅管理を実行し、Rest API を呼び出して事前変換されたフローをプロビジョニングします。PMN は、NAT 関係を示すために、フロー操作 MO を公開します。

MU NAT PIM パッシブの例

以下は、MUNAT Rest API 呼び出しとペイロード情報です。

Re-circ インターフェイスの設定

```
url: 172.28.249.173/api/mo/sys/mca/config/natsr/mappings.json?rsp-subtree=full
Payload:
{
"mcaNatMapDestPrefixSif": {
"attributes": {
"destPrefix": "112.10.3.0/24",
"domName": "default",
```

```
"maxEnatReplications": "40",
"siIfName": "eth1/15",
"status": ""
}
}
}
```

サービス リフレクト ルール

```
url: <ip_switch>/api/mo/sys/mrib/inst/dom-default/sr/rule.json?rsp-subtree=full
Payload:
{
"mribRule": {
"attributes": {
"grpMasklen": "32",
"postTransGrp": "112.3.3.51",
"postTransSrc": "11.1.1.3",
"preTransGrp": "225.10.1.50",
"preTransSrc": "112.3.1.2",
"srcMasklen": "32",
"staticOif": "unspecified",
"status": "",
"udpDestPort": "0",
"udpsrcPort": "0"
}
}
}
```

NBM フロー

```
url: <ip_switch>/api/mo/sys/nbm/show/flows/dom-default.json?rsp-subtree=full
Payload:
{
"nbmConfFlow": {
"attributes": {
"bwKbps": "50000",
"group": "225.1.1.1",
"ingressIf": "eth1/2",
"policer": "ENABLED",
"source": "112.3.1.2",
"status": ""
}
}
}
```

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 の設定例

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。

1. ドメインに参加させるインターフェイスで PIM スパース モード パラメータを設定します。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)# ip pim sparse-mode
```

2. SSM をサポートする IGMP のパラメータを設定します。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)# ip igmp version 3
```

3. デフォルト範囲を使用しない場合は、SSM 範囲を設定します。

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

4. メッセージ フィルタリングを設定します。

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

次に、PIM SSM モードの設定例を示します。

```
configure terminal
  interface ethernet 2/1
    ip pim sparse-mode
    ip igmp version 3
    exit
  ip pim ssm range 239.128.1.0/24
  ip pim log-neighbor-changes
```

PIM SSM over vPC の設定例

この例は、デフォルトの SSM 範囲である 232.0.0.0/8 ～ 225.1.1.0/24 をオーバーライドする方法を示しています。S, G Join がこの範囲で受信される限り、vPC 上の PIM SSM は機能します。

```
switch# configure terminal
switch(config)# vrf context Enterprise
switch(config-vrf)# ip pim ssm range 225.1.1.0/24
switch(config-vrf)# show ip pim group-range --> Shows the configured SSM group range.
PIM Group-Range Configuration for VRF "Enterprise"
Group-range        Mode      RP-address       Shared-tree-only range
225.1.1.0/24       SSM       -                -

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                          : secondary
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     Po1000 Vlan101
101   225.1.1.1          v3
        100.6.160.20           D     Po2

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     Po1000 Vlan101
101   225.1.1.1          v3
        100.6.160.20           D     Po2


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-holdtime 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-holdtime 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-holdtime 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 00:02:51
  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-holdtime 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
  Sgr-prune-list: (0) 00000000
  Timeout-interval: 3, JP-holdtime 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-holdtime 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-holdtime 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-holdtime 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-holdtime 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。

1. ドメインに参加させるインターフェイスで PIM スパース モード パラメータを設定します。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)# ip pim sparse-mode
```

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設定します。

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

3. BSR として動作させるルータのそれぞれに、BSR パラメータを設定します。

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

4. 候補 RP として動作させるルータのそれぞれに、RP パラメータを設定します。

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

5. メッセージ フィルタリングを設定します。

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

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
    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
```

Auto-RP の設定例

Auto-RP メカニズムを使用して Bidir モードで PIM 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。

1. ドメインに参加させるインターフェイスで PIM スパース モード パラメータを設定します。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)# ip pim sparse-mode
```

2. ルータが 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。

```
switch# configure terminal
switch(config)# ip pim auto-rp forward listen
```

3. マッピング エージェントとして動作させるルータのそれぞれに、マッピング エージェント パラメータを設定します。

```
switch# configure terminal
switch(config)# ip pim auto-rp mapping-agent ethernet 2/1
```

4. 候補 RP として動作させるルータのそれぞれに、RP パラメータを設定します。

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

5. メッセージ フィルタリングを設定します。

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

次に、Auto-RP メカニズムを使用して PIM Bidir モードを設定し、同一のルータにマッピング エージェントと RP を設定する場合の例を示します。

```
configure terminal
  interface ethernet 2/1
    ip pim sparse-mode
    exit
  ip pim auto-rp listen
  ip pim auto-rp forward
  ip pim auto-rp mapping-agent ethernet 2/1
  ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24 bidir
  ip pim log-neighbor-changes
```

PIM エニーキャスト 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。

1. ドメインに参加させるインターフェイスで PIM スパース モード パラメータを設定します。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)# ip pim sparse-mode
```

2. Anycast-RP セット内のすべてのルータに適用する RP アドレスを設定します。

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

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、ループバックを設定します。

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

4. Anycast-RP セットに加える各ルータについて、Anycast-RP パラメータとして Anycast-RP の IP アドレスを指定します。同じ作業を、Anycast-RP の各 IP アドレスで繰り返します。この例では、2 つの Anycast-RP を指定しています。

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

5. メッセージ フィルタリングを設定します。

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

次の例は、IPv6 の PIM エニーキャスト RP を設定する方法を示しています。

```
configure terminal
interface loopback 0
ipv6 address 2001:0db8:0:abcd::5/32
ipv6 pim sparse-mode
ipv6 router ospfv3 1 area 0.0.0.0
exit
interface loopback 1
ipv6 address 2001:0db8:0:abcd::1111/32
ipv6 pim sparse-mode
ipv6 router ospfv3 1 area 0.0.0.0
exit
ipv6 pim rp-address 2001:0db8:0:abcd::1111 group-list ff1e:abcd:def1::0/24
ipv6 pim anycast-rp 2001:0db8:0:abcd::5 2001:0db8:0:abcd::1111
```

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

```
configure terminal
interface ethernet 2/1
ip pim sparse-mode
exit
interface loopback 0
ip address 192.0.2.3/32
ip pim sparse-mode
exit
interface loopback 1
ip address 192.0.2.31/32
ip pim sparse-mode
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
ip pim log-neighbor-changes
```

PFM-SD 構成例

双方向モードで PIM を構成するには、PIM ドメイン内の各ルータで、次の手順を実行します。

1. PFM-SD 機能が有効になっているすべてのスイッチで PFM-SD の範囲を構成します。

```
switch(config)# ip pim pfm-sd range 224.0.0.0/4
```

2. FHR でのみ PFM-SD 発信元を構成します。

```
switch(config)# ip pim pfm-sd originator-id loopback0
```

3. PFM-SD アナウンス間隔を構成します（オプション）。

```
switch(config)# ip pim pfm-sd announcement interval 100
```

4. PFM-SD アナウンス ギャップを構成します（オプション）。

```
switch(config)# ip pim pfm-sd announcement gap 1200
```

5. PFM-SD アナウンス レートを構成します（オプション）。

```
switch(config)# ip pim pfm-sd announcement rate 10
```

6. PFM_SD gsh ホールド時間を構成します（オプション）。

```
switch(config)# ip pim pfm-sd gsh holdtime 60
```

7. PFM-SD トラフィックをブロックするために必要な次のオプションを使用して、eth1/2 で PFM-SD 境界を構成します。
   - **in**：着信 PFM-SD トラフィックをブロックします。
   - **out**：発信 PFM-SD トラフィックをブロックします。
   - **both**：着信および発信の両方の PFM-SD トラフィックをブロックします。

```
switch(config)# interface ethernet1/2
switch(config-if)# ip pim pfm-sd boundary in
```

次の例は、**show run pim** コマンドのサンプル出力を示しています。

```
switch(config-if)# show run pim

!Command: show running-config pim
!Running configuration last done at: Mon Dec  5 09:01:34 2022
!Time: Mon Dec  5 09:01:40 2022

version 10.3(2) Bios:version 07.69
feature pim

ip pim prune-on-expiry
ip pim pfm-sd range 224.0.0.0/4
ip pim pfm-sd originator-id loopback0
ip pim pfm-sd announcement interval 100
ip pim pfm-sd announcement gap 1200
ip pim pfm-sd announcement rate 10
ip pim pfm-sd gsh holdtime 60
interface Ethernet1/2
ip pim pfm-sd boundary in
```

次の例は、**show ip pim pfm-sd cache** コマンドのサンプル出力を示しています。

```
switch# show ip pim pfm-sd cache
Legend * - Originator down
PIM PFM Local Cache-Info - VRF "default"
Group: 224.0.0.0, Source count: 1
Source     Originator     Last announced     Holdtime
1.21.21.2  55.55.55.55    00:00:44           00:07:58
```

次の例は、**show ip pim pfm-sd cache remote-discovery** コマンドのサンプル出力を示しています。

```
switch# show ip pim pfm-sd cache remote-discovery
PIM PFM Remote Discovery Cache-Info - VRF "default"
Group: 224.0.0.0, Source count: 1
```

```
Source     Originator     Last announced     Holdtime
1.21.21.2  55.55.55.55    00:00:44           00:07:58
```

次の例は、**show ip pim vrf internal** コマンドのサンプル出力を示しています。

```
switch# show ip pim vrf internal
PIM Enabled VRFs
VRF Name     VRF   Table       Interface   BFD         MVPN
             ID    ID          Count       Enabled     Enabled
default      1     0x00000001  8          no          no
PIM RP change: no
…..
PIM VxLAN VNI ID: 0
PIM pfm-sd : Enabled
group range : 224.0.0.0/4
originator interface : loopback0
originator ip : 55.55.55.55
announcement interval : 100 seconds
announcement gap : 1200 milliseconds
announcement rate : 10
holdtime : 60 seconds
```

次の例は、**show ip pim interface interface port** コマンドのサンプル出力を示しています。

```
switch# show ip pim interface ethernet 1/17
PIM Interface Status for VRF "default"
Ethernet1/17, Interface status: protocol-up/link-up/admin-up
IP address: 17.17.17.1, IP subnet: 17.17.17.0/24
……
PIM border-router interface: no
PIM pfm-sd boundary: none
pfm-sd packets sent : 0
pfm-sd packets received :1
pfm-sd packets forwarded :1
```

プレフィックスベースおよびルートマップベースの設定

```
ip prefix-list plist11 seq 10 deny 231.129.128.0/17
ip prefix-list plist11 seq 20 deny 231.129.0.0/16
ip prefix-list plist11 seq 30 deny 231.128.0.0/9
ip prefix-list plist11 seq 40 permit 231.0.0.0/8

ip prefix-list plist22 seq 10 deny 231.129.128.0/17
ip prefix-list plist22 seq 20 deny 231.129.0.0/16
ip prefix-list plist22 seq 30 permit 231.128.0.0/9
ip prefix-list plist22 seq 40 deny 231.0.0.0/8

ip prefix-list plist33 seq 10 deny 231.129.128.0/17
ip prefix-list plist33 seq 20 permit 231.129.0.0/16
ip prefix-list plist33 seq 30 deny 231.128.0.0/9
ip prefix-list plist33 seq 40 deny 231.0.0.0/8

ip pim rp-address 172.21.0.11 prefix-list plist11
ip pim rp-address 172.21.0.22 prefix-list plist22
ip pim rp-address 172.21.0.33 prefix-list plist33
route-map rmap11 deny 10
 match ip multicast group 231.129.128.0/17
route-map rmap11 deny 20
 match ip multicast group 231.129.0.0/16
route-map rmap11 deny 30
 match ip multicast group 231.128.0.0/9
route-map rmap11 permit 40
```

```
 match ip multicast group 231.0.0.0/8

route-map rmap22 deny 10
 match ip multicast group 231.129.128.0/17
route-map rmap22 deny 20
 match ip multicast group 231.129.0.0/16
route-map rmap22 permit 30
 match ip multicast group 231.128.0.0/9
route-map rmap22 deny 40
 match ip multicast group 231.0.0.0/8

route-map rmap33 deny 10
 match ip multicast group 231.129.128.0/17
route-map rmap33 permit 20
 match ip multicast group 231.129.0.0/16
route-map rmap33 deny 30
 match ip multicast group 231.128.0.0/9
route-map rmap33 deny 40
 match ip multicast group 231.0.0.0/8

ip pim rp-address 172.21.0.11 route-map rmap11
ip pim rp-address 172.21.0.22 route-map rmap22
ip pim rp-address 172.21.0.33 route-map rmap33
```

出力

```
dc3rtg-d2(config-if)# show ip pim rp
PIM RP Status Information for VRF "default"
BSR disabled
Auto-RP disabled
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None

RP: 172.21.0.11, (0), uptime: 00:12:36, expires: never,
  priority: 0, RP-source: (local), group-map: rmap11, group ranges:
      231.0.0.0/8  231.128.0.0/9 (deny)
      231.129.0.0/16 (deny) 231.129.128.0/17 (deny)
RP: 172.21.0.22, (0), uptime: 00:12:36, expires: never,
  priority: 0, RP-source: (local), group-map: rmap22, group ranges:
      231.0.0.0/8 (deny) 231.128.0.0/9
      231.129.0.0/16 (deny) 231.129.128.0/17 (deny)
RP: 172.21.0.33, (0), uptime: 00:12:36, expires: never,
  priority: 0, RP-source: (local), group-map: rmap33, group ranges:
      231.0.0.0/8 (deny) 231.128.0.0/9 (deny)
      231.129.0.0/16  231.129.128.0/17 (deny)

dc3rtg-d2(config-if)# show ip mroute
IP Multicast Routing Table for VRF "default"

(*, 231.1.1.1/32), uptime: 00:07:20, igmp pim ip
  Incoming interface: Ethernet2/1, RPF nbr: 10.165.20.1
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:07:20, igmp

(*, 231.128.1.1/32), uptime: 00:14:27, igmp pim ip
  Incoming interface: Ethernet2/1, RPF nbr: 10.165.20.1
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:14:27, igmp

(*, 231.129.1.1/32), uptime: 00:14:25, igmp pim ip
  Incoming interface: Ethernet2/1, RPF nbr: 10.165.20.1
```

```
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:14:25, igmp

(*, 231.129.128.1/32), uptime: 00:14:26, igmp pim ip
  Incoming interface: Null, RPF nbr: 10.0.0.1
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:14:26, igmp

(*, 232.0.0.0/8), uptime: 1d20h, pim ip
  Incoming interface: Null, RPF nbr: 10.0.0.1
  Outgoing interface list: (count: 0)

dc3rtg-d2(config-if)# show ip pim group-range
PIM Group-Range Configuration for VRF "default"
Group-range        Mode      RP-address       Shared-tree-only range
232.0.0.0/8        ASM       -                -
231.0.0.0/8        ASM       172.21.0.11      -
231.128.0.0/9      ASM       172.21.0.22      -
231.129.0.0/16     ASM       172.21.0.33      -
231.129.128.0/17   Unknown   -                -
```

技術サポート コマンド

次のコマンドを実行して、ハードウェア テーブル ダンプを収集します。

手順の概要

1. **show tech-support forwarding multicast detail**

手順の詳細

手順

	コマンドまたはアクション	目的
Step 1	**show tech-support forwarding multicast detail**	ハードウェア テーブル ダンプを収集します。

例

```
show tech-support forwarding multicast hardware module 1
Module:1 Unit:0 Slice: 0 Table:tah_ara_lub_bdstatetable     <<<<<<
ENTRY: 1
        info_leaf_flood_dst_ptr : 0x00000001
        info_leaf_igmp_mld_dst_ptr : 0x00001002
        info_leaf_fid : 0x00000001
        info_leaf_vrf : 0x00000001
……
Module:1 Unit:0 Slice: 0 Table:tah_ara_qsmt_dhs_met_access     <<<<<<
ENTRY: 1
        met_entry_bridge_only : 0x00000001
        met_entry_no_prune_on_mct : 0x00000001
……
```

関連資料

関連項目	マニュアル タイトル
ACL TCAM リージョン	『*Cisco Nexus 9000 Series NX-OS Security Configuratio*
VRF の設定	『*Cisco Nexus 9000* シリーズ *NX-OS* ユニキャスト ル設定ガイド』

標準

標準
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既サポートに変更はありません。

MIB

MIB	MIB のリンク
PIM に関連した MIB	サポートされている MIB を検索およびダウンロード次の URL にアクセスしてください。 https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

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。