Cisco Nexus 3548 スイッチ NX-OS マルチキャスト ルーティング構成ガイド、リリース 10.6(x)

最終更新：2025 年 12 月 12 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

ここでは、次の内容について説明します。

対象読者

本書は、Cisco Nexus デバイスおよび Cisco Nexus 2000 シリーズ ファブリック エクステンダの設定と保守を行う、経験豊富なネットワーク管理者を対象としています。

このマニュアルは、次のような経験と知識を持つネットワーク管理者とサーバ管理者を対象としています。

Note VMware vNetwork Distributed Switch の知識は必要ありません。

- 仮想化の知識
- 仮想マシンを作成し、VMware vSwitch を実装する Virtual Machine Manager（VMM）ソフトウェアの使用
- Amazon Web Service（AWS）や Microsoft Azure などのプロバイダー クラウド上でアカウントを作成できること

- 仮想化の知識
- ハイパーバイザ ホスト マシン ソフトウェアを使用した、仮想マシンの作成および仮想スイッチの設定

- 仮想化の知識
- VMware vSwitch、Microsoft System Center Virtual Machine Manager（SCVMM）、または OpenStack など、スイッチ用の対応するハイパーバイザ管理ソフトウェアについての知識

表記法

（注） お客様のニーズを満たすためにドキュメントを更新するという継続的な取り組みの一環として、シスコでは設定タスクの文書化方法を変更しました。そのため、本ドキュメントには、従来とは異なるスタイルでの設定タスクが説明されている部分もあります。ドキュメントに新たに組み込まれるようになったセクションは、新しい表記法に従っています。

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
`太字の screen フォント`	ユーザが入力しなければならない情報は、太字のスクリーンフォントで示しています。

表記法	説明
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

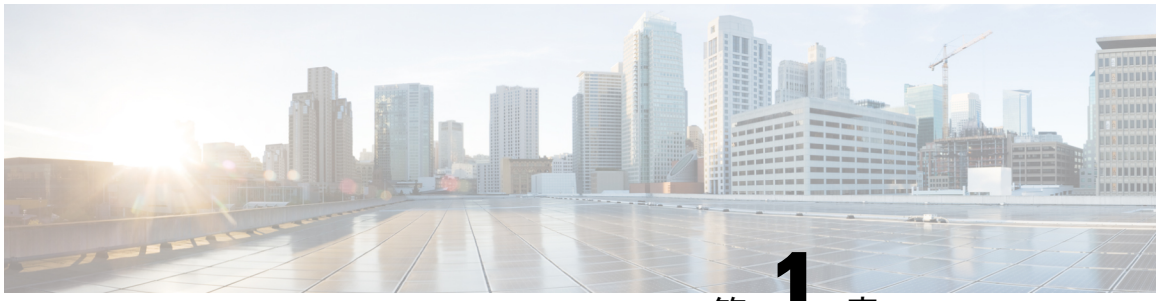
（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォーム（intercloud-fabric-doc-feedback@cisco.com）よりご連絡ください。

ご協力をよろしくお願いいたします。



第 1 章

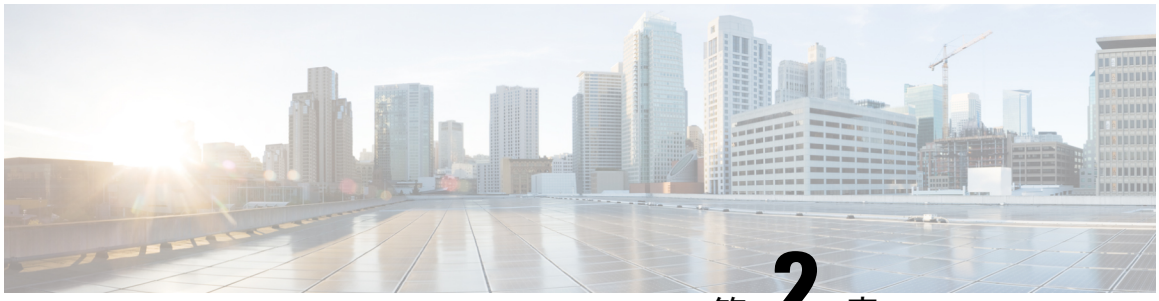
新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

表 *1 : Cisco Nexus NX-OS* リリース *10.6(x)* の新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
PIM の graceful-spt 機能がデフォルトになるように設定	PIM グレースフル SPT 機能をデフォルトにするためのサポートが追加されました。	10.6(1)F	PIM の注意事項と制約事項 （50 ページ） PIM 設定の確認 （75 ページ）

新機能および変更された機能に関する情報



第 2 章

概要

この章では、Cisco NX-OS のマルチキャスト機能について説明します。

この章は、次の項で構成されています。

ライセンス要件

Cisco NX-OS を動作させるには、機能とプラットフォームの要件に従って適切なライセンスを取得し、インストールする必要があります。

- 基本（Essential）ライセンスとアドオン ライセンスが、さまざまな機能セットに使用できます。
- ライセンスは、製品および購入オプションに応じて、永続的、一時的、または評価可能な場合があります。
- 高度な機能を使用するには、基本ライセンス以外の追加の機能ライセンスが必要です。
- 高度な機能を使用するには、基本ライセンス以外の追加ライセンスが必要です。
- ライセンスの適用と管理は、デバイスのコマンドライン インターフェイス（CLI）を介して行われます。

ハードウェアの取り付け手順の詳細については、次を参照してください。 *Cisco NX-OS* ライセンシング ガイド および *Cisco NX-OS* ライセンシング オプション ガイド。

サポートされるプラットフォーム

Nexus Switch プラットフォーム サポート マトリックスは、次をリストします：

- サポートされている Cisco Nexus 9000 および 3000 スイッチ モデル
- NX-OS ソフトウェア リリース バージョン

フル プラットフォーム機能マッピングは、「Nexus Switch プラットフォーム サポート マトリックス」 を参照します。

マルチキャストに関する情報

IP マルチキャストは、同一セットの IP パケットをネットワーク上の複数のホストに転送する手法です。IPv4 ネットワークで、マルチキャストを使用して、複数の受信者に効率的にデータを送信できます。

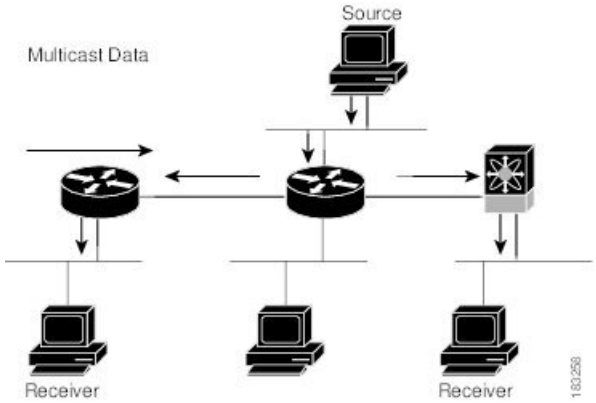
マルチキャストには、グループと呼ばれる IP マルチキャスト アドレスに送信されたマルチキャスト データの送信側と受信側の配信と検出の両方の手法が含まれます。グループと送信元 IP アドレスが入ったマルチキャスト アドレスは、しばしばチャネルと呼ばれます。Internet Assigned Number Authority（IANA）では、IPv4 マルチキャスト アドレスとして、224.0.0.0 ～ 239.255.255.255 を割り当てています。詳細については、http://www.iana.org/assignments/multicast-addresses を参照してください。

（注） マルチキャストに関連する RFC の完全なリストについては、「IP マルチキャストに関する IETF RFC」を参照してください。

ネットワーク上のルータは、受信者からのアドバタイズメントを検出して、マルチキャスト データの要求対象となるグループを特定します。その後、ルータは送信元からのデータを複製して、対象の受信者へと転送します。グループ宛のマルチキャスト データが送信されるのは、そのデータを要求する受信者を含んだ LAN セグメントだけです。

図 1 に、1 つの送信元から 2 つの受信者へと、マルチキャスト データを送信する場合の例を示します。この図で、中央のホストが属する LAN セグメントにはマルチキャスト データを要求する受信者が存在しないため、このホストは受信者にデータを転送しません。

図 *1 : 1* つの送信元から *2* つの受信者へのマルチキャスト トラフィック



Cisco Nexus 3500 シリーズ スイッチの一貫性チェッカー コマンド

整合性チェッカーは、ネットワーク システムのソフトウェア状態を、サポートされているモジュールのハードウェア状態と比較します。これにより、後のトラブルシューティングの時間を短縮できます。整合性チェッカーは、基本的なトラブルシューティングを補足するもので、ソフトウェアテーブルとハードウェアテーブル間の不整合な状態がネットワークの問題を引き起こしているシナリオを特定するのに役立ちます。これにより、問題を解決するための平均時間が短縮されます。

次の整合性チェッカー コマンドは、Cisco NX-OS リリース 9.3(3) のレイヤ 2 でサポートされています。

- show consistency-checker membership vlan <vlanid> [native-vlan]：ソフトウェアの VLAN メンバーシップがハードウェアにプログラムされているものと同じであることを判別します。
- show consistency-checker membership port-channels [interface <ch-id>]：すべてのモジュールのハードウェアのポート チャネル メンバーシップをチェックし、ソフトウェア状態で検証します。
- show consistency-checker stp-state vlan <vlan>：ソフトウェアのスパニング ツリーの状態が、ハードウェアでプログラミングされた状態と同じかどうかを判別します。このコマンドは、動作中（アップ）のインターフェイスでのみ実行されます。
- show consistency-checker l2 module <modnum>：学習した MAC アドレスがソフトウェアとハードウェア間で一貫していることを確認します。また、ハードウェアに存在するがソフトウェアには存在しない追加エントリと、ハードウェアに存在しないエントリも表示されます。
- show consistency-checker link-state module <moduleID>：インターフェイスのリンク状態ステータスについて、ソフトウェアとハードウェア間のプログラミングの一貫性を確認します。

次の整合性チェッカー コマンドは、Cisco NX-OS リリース 9.3(3):のレイヤ 3 でサポートされています。

- show consistency-checker l3-interface module <moduleid>：L3 インターフェイスの入力および出力転送テーブルについて、ソフトウェアとハードウェア間のプログラミングの整合性を確認します。
- test forwarding ipv4 [unicast] inconsistency [suppress_transient] [vrf vrf-name] [stop] ：レイヤ 3 整合性チェックを開始または停止します。
- show forwarding ipv4 [unicast] inconsistency [vrf vrf-name]：レイヤ 3 整合性チェックの結果を表示します。
- show consistency-checker forwarding single-route ipv4 <ip-prefix> vrf <vrf-name>：単独ルートの整合性チェックの結果を表示します。
- clear forwarding [ipv4 | ip] [unicast] inconsistency：IP 転送の不整合を解消します。
- show consistency-checker gwmacdb ：ルータ MAC の一貫性チェックの結果を表示します。

次の整合性チェッカー コマンドは、Cisco NX-OS リリース 9.3(3) からのマルチキャストでサポートされています。

- show consistency-checker l2 multicast group <grp-address> source <src-address> vlan <vlan-id> [dump-debug-logs]：ソフトウェアとハードウェア間の L2 IGMP エントリのレイヤ 2 マルチキャストの整合性を確認します。
- show consistency-checker l3 multicast group <grp-address> source <src-address> vrf <vrf-string> [dump-debug-logs]：ソフトウェアおよびハードウェア間 L3 マルチキャスト ルート エントリのレイヤ 3 マルチキャストの整合性を確認します。

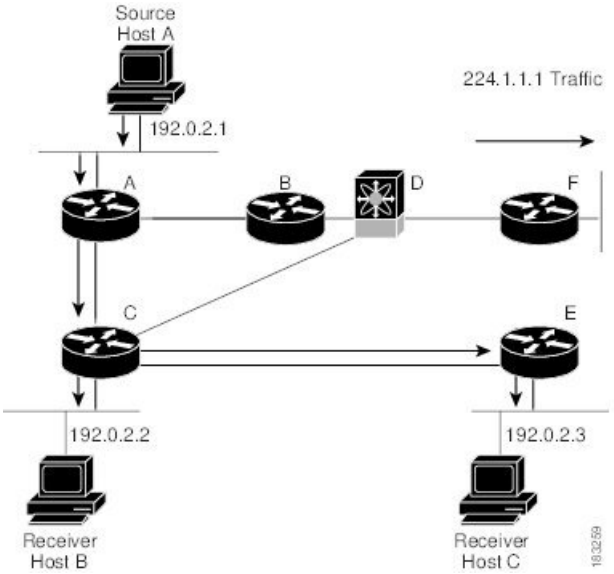
マルチキャスト配信ツリー

マルチキャスト配信ツリーとは、送信元と受信者を中継するルータ間の、マルチキャストデータの伝送パスを表します。マルチキャスト ソフトウェアはサポートするマルチキャスト方式に応じて、タイプの異なるツリーを構築します。

送信元ツリー

送信元ツリーは、送信元からネットワーク経由でマルチキャスト トラフィックを伝送する場合の最短パスです。特定のマルチキャスト グループへと送信されたマルチキャスト トラフィックが、同じグループのトラフィックを要求する受信者へと転送されます。送信元ツリーは、最短パスとしての特性から、最短パス ツリー（SPT）と呼ばれることがあります。図 2 では、ホスト A を起点とし、ホスト B および C に接続されているグループ 224.1.1.1 の送信元ツリーを示しています。

図 *2:* 送信元ツリー

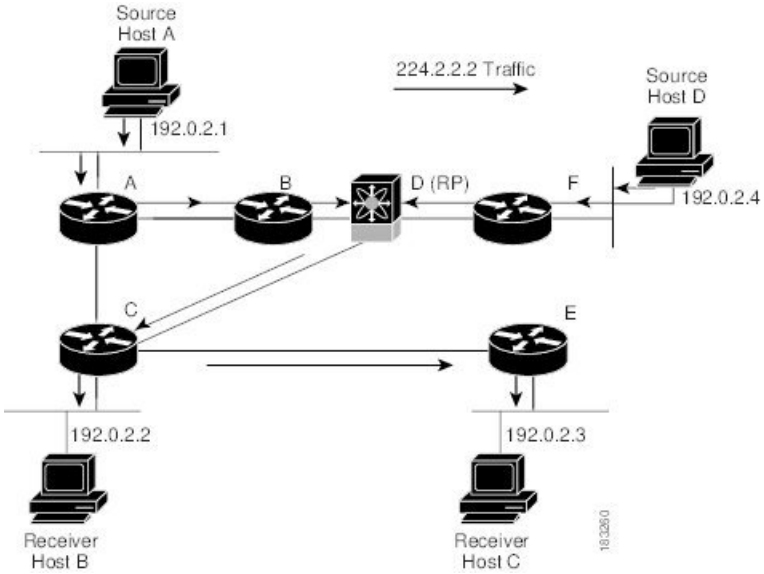


表記（S、G）は、グループ G の任意の送信元 S からのマルチキャスト トラフィックを表します。図 2 の SPT は、（192.1.1.1, 224.1.1.1）と記述されます。同じグループの複数の送信元からトラフィックを送信できます。

共有ツリー

共有ツリーとは、共有ルート、つまりランデブーポイント（RP）から各受信者に、ネットワーク経由でマルチキャスト トラフィックを伝送する共有配信パスを表します（RP は各ソースへの SPT を作成します。）共有ツリーは、RP ツリー（RPT）とも呼ばれます。図 3 では、ルータ D に RP を持つ、グループ 224.1.1.1 の共有ツリーを示しています。データは送信元ホスト A およびホスト D からルータ D（RP）に送信され、そこから受信者ホスト B およびホスト C にトラフィックが転送されます。

図 *3:* 共有ツリー



表記（*、G）は、グループGの任意の送信元からのマルチキャストトラフィックを表します。図 3 の共有ツリーは、（*、224.2.2.2）と記述されます。

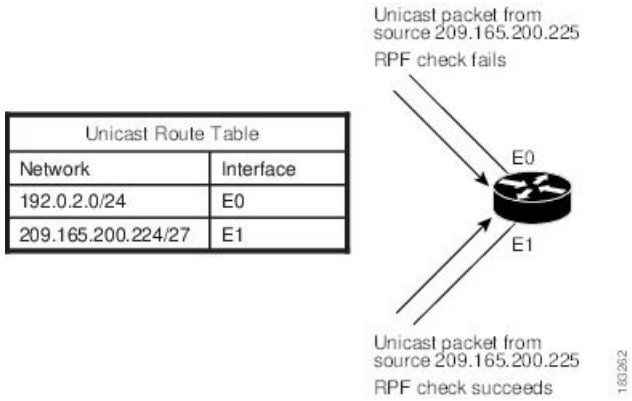
マルチキャスト転送

マルチキャストトラフィックは任意のホストを含むグループ宛に送信されるため、ルータはリバース パス フォワーディング（RPF）を使用して、グループのアクティブな受信者にデータをルーティングします。受信者がグループに加入すると、送信元方向へ向かうパス（SSMモードの場合）、またはRP方向へ向かうパス（ASMモードの場合）が形成されます。送信元から受信者へのパスは、受信者がグループに加入したときに作成されたパスと逆方向になります。

マルチキャスト パケットが着信するたびに、ルータは RPF チェックを実行します。パケットが送信元につながるインターフェイスに到着すると、パケットはグループの発信インターフェイス（OIF）リスト内の各インターフェイスから転送されます。それ以外の場合、パケットはドロップされます。

図 4 では、異なるインターフェイスから受信するパケットの RPF チェックの例を示します。E0 に着信したパケットは、RPF チェックに失敗します。これは、ユニキャスト テーブルで、対象の送信元ネットワークがインターフェイス E1 に関連付けられているためです。E1 に着信したパケットは、RPF チェックに合格します。これは、ユニキャスト ルート テーブルで、対象の送信元ネットワークがインターフェイス E1 に関連付けられているためです。

図 *4 : RPF* チェックの例



Cisco NX-OS PIM

Cisco NX-OS は Protocol Independent Multicast（PIM）スパース モードを使用したマルチキャストをサポートしています。PIM は IP ルーティング プロトコルに依存せず、使用されているすべてのユニキャスト ルーティング プロトコルが提供するユニキャスト ルーティング テーブルを利用できます。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 デンス モードは Cisco NX-OS ではサポートされていません。

（注） このマニュアルで、「PIM」という用語は PIM スパース モード バージョン 2 を表します。

マルチキャスト コマンドにアクセスするには、PIM機能をイネーブルにする必要があります。ドメイン内の各ルータのインターフェイス上で、PIM をイネーブルにしないかぎり、マルチキャスト機能はイネーブルになりません。PIM はIPv4 ネットワーク用に設定できます。デフォルトでは、IGMP がシステムで実行されています。

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。

配信ツリーは、リンク障害またはルータ障害のためにトポロジが変更されると、トポロジを反映して自動的に変更されます。PIMは、マルチキャスト対応の送信元と受信者の両方を動的に追跡します。

ルータはユニキャスト ルーティング テーブルおよび RPF ルートを使用して、マルチキャスト ルーティング情報を生成します。

（注） このマニュアルでは、「IPv4 用の PIM」という表現は、Cisco NX-OS における PIM スパース モードの導入を表します。PIM ドメインには、IPv4 ネットワークを含めることができます。

図 5 では、IPv4 ネットワークで 2 つの PIM ドメインを示します。

図 *5: IPv4* ネットワーク内の *PIM* ドメイン

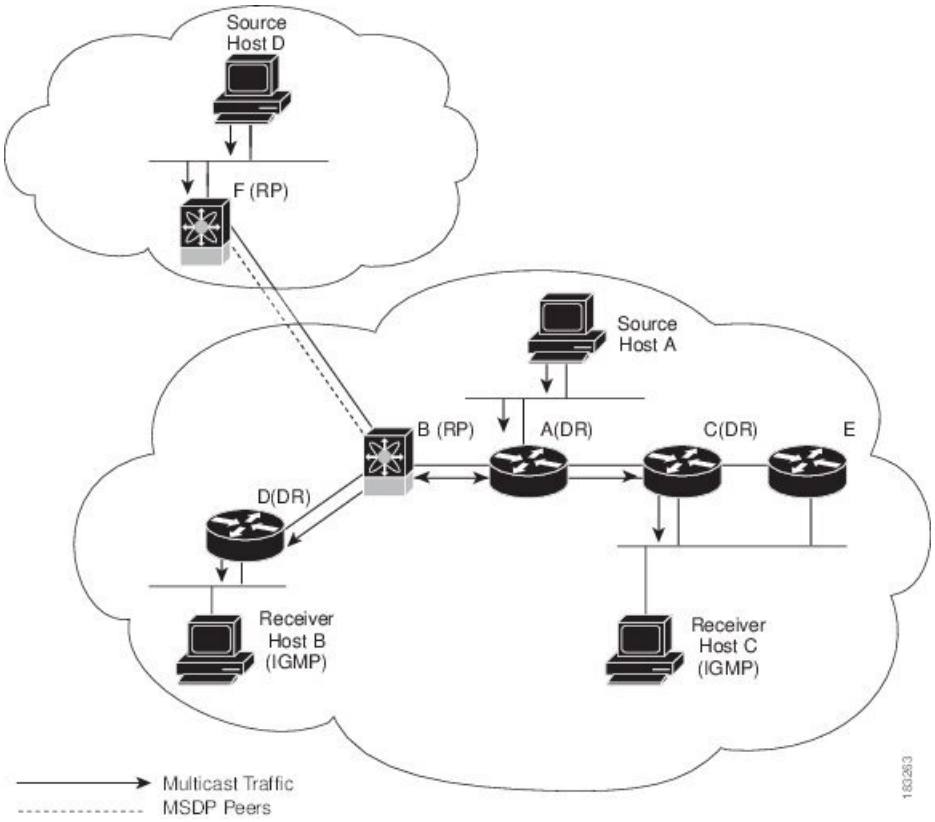


図 5 では、PIM の次の要素を示します。

- 矢印の付いた直線は、ネットワークで伝送されるマルチキャスト データのパスを表します。マルチキャスト データは送信元ホストの A および D から発信されます。
- 点線でつながれているルータ B および Fは、Multicast Source Discovery Protocol（MSDP）ピアです。MSDP を使用すると、他の PIM ドメイン内にあるマルチキャスト送信元を検出できます。
- ホスト B およびホスト C ではマルチキャスト データを受信するため、インターネット グループ管理プロトコル（IGMP）プロトコルを使用して、マルチキャスト グループへの加入要求をアドバタイズします。
- ルータ A、C、および D は指定ルータ（DR）です。LAN セグメントに複数のルータが接続されている場合は（C や E など）、PIM ソフトウェアによって DR となるルータが 1 つ選択されます。これにより、マルチキャストデータの窓口として、1 つのルータだけが使用されます。

ルータ B とルータ F は、それぞれ異なる PIM ドメインのランデブー ポイント（RP）です。RP は、複数の送信元と受信者を接続するため、PIM ドメイン内の共通ポイントとして機能します。

PIM は送信元と受信者間の接続に関して、2 つのマルチキャスト モードをサポートしています。

- Any Source Multicast（ASM）
- Source Specific Multicast（SSM）

Cisco NX-OS では上記モードを組み合わせて、さまざまな範囲のマルチキャスト グループに対応することができます。マルチキャスト用の RPF ルートを定義することもできます。

アーキテクチャ セールス マネージャ（ASM）

Any Source Multicast（ASM）は PIM ツリー構築モードの 1 つです。新しい送信元および受信者を検出する場合には共有ツリーを、受信者から送信元への最短パスを形成する場合は送信元ツリーを使用します。共有ツリーでは、ランデブー ポイント（RP）と呼ばれるネットワーク ノードをルートとして使用します。送信元ツリーは第 1 ホップ ルータをルートとし、アクティブな発信元である各送信元に直接接続されています。ASM モードでは、グループ範囲に対応する RP が必要です。RP は静的に設定することもできれば、Auto-RP プロトコルまたはブートストラップ ルータ（BSR）プロトコルを使用して、グループと RP 間の関連付けを動的に検出することもできます。

RP を設定する場合、デフォルト モードは ASM モードです。

ASM の構成に関する詳細は、「ASM または Bidir の構成」セクションを参照してください。

SSM

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する PIM モードです。送信元ツリーは、PIM 加入メッセージを送信元方向に送信することで構築されます。SSM モードでは、RP を設定する必要がありません。

SSM モードの場合、PIM ドメインの外部にある送信元と受信者を接続できます。

SSM の構成に関する詳細は、「SSM の構成」セクションを参照してください。

マルチキャスト用 RPF ルート

静的マルチキャスト RPF ルートを設定すると、ユニキャスト ルーティング テーブルの定義内容を無効にすることができます。この機能は、マルチキャスト トポロジとユニキャスト トポロジが異なる場合に使用されます。

マルチキャストの RPF ルートの構成に関する詳細は、「マルチキャストの RPF ルートの構成」セクションを参照してください。

IGMP

デフォルトでは、PIM のインターネット グループ管理プロトコル（IGMP）が、システムで実行されています。

IGMPプロトコルは、マルチキャストグループのメンバーシップを要求するため、マルチキャストデータを受信する必要があるホストで使用されます。グループ メンバーシップが確立されると、対象のグループのマルチキャストデータが要求元ホストのLANセグメントに転送されます。

インターフェイスにはIGMPv2またはIGMPv3を設定できます。SSMモードをサポートする場合は、IGMPv3を使用するのが一般的です。デフォルトではIGMPv2がイネーブルになっています。

IGMPの構成に関する詳細は、「IGMPの設定 （17ページ）」を参照してください。

IGMP スヌーピング

IGMP スヌーピングは、VLANで既知の受信者に接続された一部のポートだけにマルチキャストトラフィックを転送する機能です。対象ホストからのIGMP メンバーシップ レポート メッセージを調べる（スヌーピングする）ことにより、マルチキャストトラフィックは対象ホストが接続されたVLANポートだけに送信されます。システムでは、IGMP スヌーピングがデフォルトで稼働しています。

IGMP スヌーピングの構成に関する詳細は、「IGMP スヌーピングの構成 （93ページ）」を参照してください。

ドメイン内マルチキャスト

Cisco NX-OSでは、PIMドメイン間でマルチキャストトラフィック送信を実行するための方法が提供されます。

SSM

PIM ソフトウェアはSSMを使用して、受信者の指定ルータから既知の送信元IPアドレスへの最短パス ツリーを構築します。この場合、送信元は別のPIM ドメイン内にあってもかまいません。ASM モードの場合、別のPIM ドメインから送信元にアクセスするには、別のプロトコルを使用する必要があります。

ネットワークでPIMをイネーブルにすると、SSMを使用し、受信者の指定ルータがIPアドレスを把握している任意のマルチキャスト送信元への接続パスを確立できます。

SSMの構成に関する詳細は、「SSMの構成」セクションを参照してください。

MSDP

Multicast Source Discovery Protocol（MSDP）は、PIMと組み合わせて使用することで、異なるPIMドメイン内にあるマルチキャスト送信元を検出できるようにするマルチキャストルーティング プロトコルです。

（注） Cisco NX-OSでは、MSDP設定が不要なPIM Anycast-RPをサポートしています。PIM Anycast-RPの詳細については、「PIM Anycast-RPセットの構成」セクションを参照してください。

MSDP については、「MSDP の構成」を参照してください。

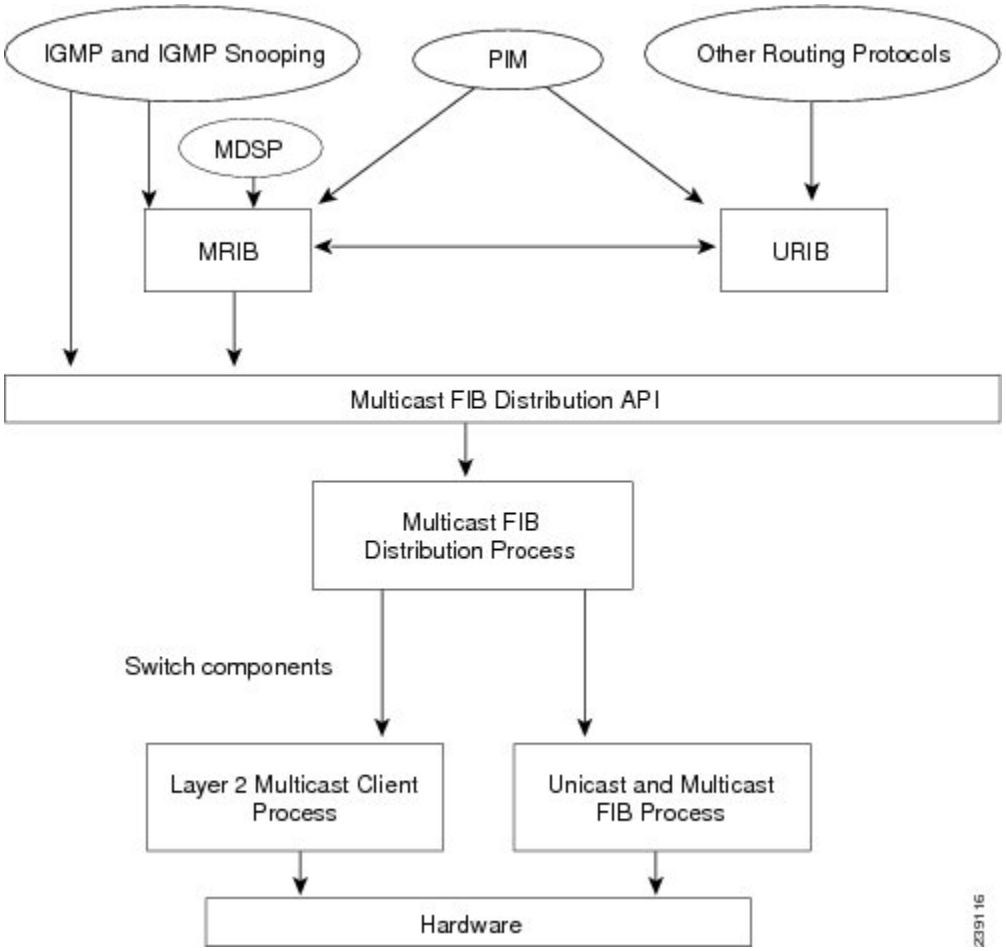
MRIB

Cisco NX-OS IPv4 Multicast Routing Information Base（MRIB）は、PIM や IGMP などのマルチキャストプロトコルで生成されるルート情報を格納するためのリポジトリです。MRIB はルート情報自体には影響を及ぼしません。MRIB は、各仮想ルーティングおよびフォワーディング（VRF）インスタンスの独立したルート情報を維持しています。

図 6 に、Cisco NX-OS マルチキャスト ソフトウェア アーキテクチャの主要コンポーネントを示します。

- マルチキャスト FIB（MFIB）配信（MFDM）API は、MRIB を含むマルチキャスト レイヤ 2 およびレイヤ 3 コントロール プレーン モジュールと、プラットフォーム フォワーディング プレーン間のインターフェイスを定義します。コントロールプレーンモジュールは、MFDM API を使用してレイヤ 3 ルート アップデートおよびレイヤ 2 ルックアップ情報を送信します。
- マルチキャスト FIB配信プロセスは、マルチキャスト更新メッセージをスイッチに配信します。
- レイヤ 2 マルチキャスト クライアント プロセス：レイヤ 2 マルチキャスト ハードウェア転送パスを構築します。
- ユニキャストおよびマルチキャスト FIB プロセス：レイヤ 3 ハードウェア転送パスを管理します。

図 *6 : Cisco NX-OS* マルチキャスト ソフトウェアのアーキテクチャ



SW と HW マルチキャスト ルート間の不一致のトラブルシューティング

症状

このセクションでは、アクティブなフローで MRIB に表示されるが、MFIB でプログラムされていない *、G、または S,G エントリに関連した症状、考えられる原因、および推奨されるアクションについて説明します。

考えられる原因

この問題は、ハードウェアの容量を超えて多数のアクティブフローを受信した場合に発生します。これにより、空きハードウェアインデックスがなくなって、一部のエントリがハードウェアでプログラムされなくなります。

ハードウェア リソースを解放するためにアクティブなフローの数が大幅に削減された場合、ハードウェアテーブルがいっぱいであったときに以前影響されていたフローについては、エントリ、タイムアウト、再入力が生じ、プログラミングがトリガーされるまで、MRIB と MFIB の間で不整合が見られることがあります。

現在、ハードウェア リソースが解放された後に、MRIBテーブルを調べて、ハードウェアの欠落しているエントリを再プログラムするメカニズムはありません。

改善処置

エントリを確実に再プログラミングするには、**clear ip mroute *** コマンドを使用します。

その他の参考資料

マルチキャストの実装に関する詳細情報については、次の項目を参照してください。

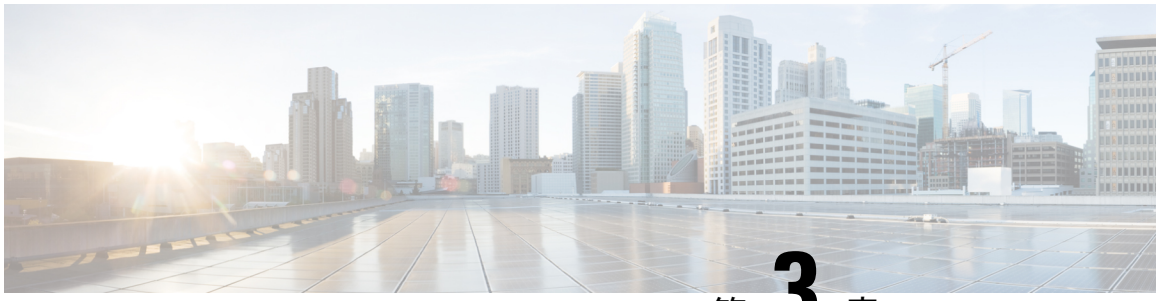
- 関連資料
- 付録 A、IP マルチキャスト向け IETF RFC
- シスコのテクニカル サポート

関連資料

関連項目	マニュアル タイトル
CLI コマンド	Cisco Nexus 3000 シリーズ NX-OS マルチキャスト ルーティング コマンド リファレンス

テクニカル サポート

説明	リンク
Technical Assistance Center（TAC）ホーム ページ：多数の技術関連の記事と、製品、テクノロジー、ソリューション、テクニカル ティップス、ツールへのリンクを提供する Web サイトです。必要な記事は検索して見つけることができます。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html



第 3 章

IGMP の設定

この章では、IPv4 ネットワーク用に Cisco NX-OS スイッチでインターネット グループ管理プロトコル（IGMP）を構成する方法について説明します。

この章は、次の項で構成されています。

IGMP に関する情報

IGMP は、ホストが特定のグループにマルチキャスト データを要求するために使用する IPv4 プロトコルです。ソフトウェアは、IGMP を介して取得した情報を使用し、マルチキャスト グループまたはチャネル メンバーシップのリストをインターフェイス単位で保持します。これらの IGMP パケットを受信したシステムは、既知の受信者が含まれるネットワーク セグメントに、要求されたグループまたはチャネルに関する受信データをマルチキャスト送信します。

IGMP プロセスはデフォルトで実行されています。インターフェイスでは IGMP を手動でイネーブルにできません。IGMP は、インターフェイスで次のいずれかの設定作業を行うと、自動的にイネーブルになります。

- Protocol-Independent Multicast（PIM）のイネーブル化
- ローカル マルチキャスト グループの静的なバインディング
- リンクローカル グループ レポートのイネーブル化

IGMP のバージョン

スイッチでは、IGMPv1 の他に、IGMPv2 と IGMPv3 のレポート受信もサポートされています。

デフォルトでは、ソフトウェアが IGMP プロセスを起動する際に、IGMPv2 がイネーブルになります。必要に応じて、各インターフェイスでは IGMPv3 をイネーブルにできます。

IGMPv3 には、次に示す IGMPv2 からの重要な変更点があります。

- 次の機能を提供し、各受信者から送信元までの最短パス ツリーを構築可能な Source-Specific Multicast（SSM）をサポートします。

グループおよび送信元を両方指定できるホスト メッセージ

IGMPv2 ではグループについてのみ保持できたマルチキャスト ステートを、グループおよび送信元についても保持可能

- ホストによるレポート抑制が行われなくなり、IGMP クエリー メッセージを受信するたびに IGMP メンバーシップ レポートが送信されるようになりました。

IGMPv2 の詳細については、RFC 2236 を参照してください。

IGMPv3 の詳細については、RFC 3376 を参照してください。

IGMP の基礎

図 1 に、ルータが IGMP を使用し、マルチキャスト ホストを検出する基本的なプロセスを示します。ホスト 1、2、および 3 は要求外の IGMP メンバーシップ レポート メッセージを送信して、グループまたはチャネルに関するマルチキャスト データの受信を開始します。

図 *7: IGMPv1* および *IGMPv2* クエリ応答プロセス

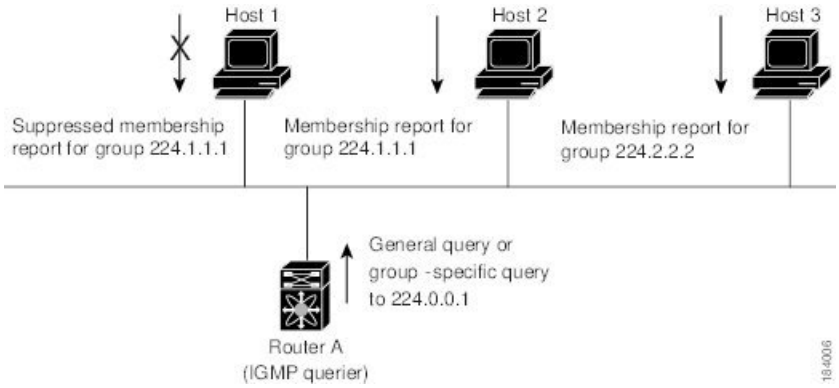


図 1 のルータ A（サブネットの代表 IGMP クエリア）は、すべてのホストが含まれる 224.0.0.1 ホスト マルチキャスト グループに定期的にクエリ メッセージを送信して、マルチキャスト データを要求しているホストを検出します。グループ メンバーシップ タイムアウト値を設定できます。指定したタイムアウト値が経過すると、ルータはサブネット上にグループのメンバーまたは送信元が存在しないと見なします。IGMP パラメータの構成方法については、「IGMP インターフェイス パラメータの構成」セクションを参照してください。

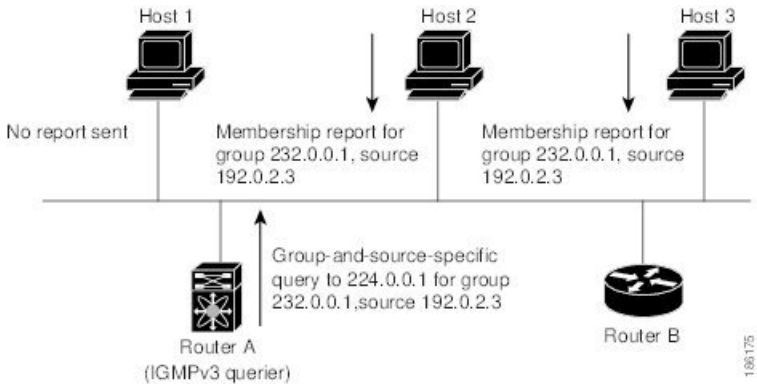
IP アドレスが最小のルータが、サブネットの IGMP クエリアとして選出されます。ルータは、自身よりも下位の IP アドレスを持つルータからクエリー メッセージを継続的に受信している間、クエリア タイムアウト値をカウントするタイマーをリセットします。ルータのクエリア タイマーが期限切れになると、そのルータは代表クエリアになります。そのあとで、このルータが、自身よりも下位の IP アドレスを持つルータからのホスト クエリー メッセージを受信すると、ルータは代表クエリアとしての役割をドロップしてクエリア タイマーを再度設定します。

図 1 では、ホスト 1 からのメンバーシップ レポートの送出が止められており、最初にホスト 2 からグループ 224.1.1.1 に関するメンバーシップ レポートが送信されます。ホスト 1 はホスト 2 からレポートを受信します。ルータに送信する必要があるメンバーシップ レポートは、グループにつき 1 つだけであるため、その他のホストではレポートの送出が止められ、ネットワーク トラフィックが軽減されます。レポートの同時送信を防ぐため、各ホストではランダムな時間だけレポート送信が保留されます。クエリの最大応答時間パラメータを設定すると、ホストが応答をランダム化する間隔を制御できます。

（注） IGMPv1 および IGMPv2 メンバーシップ レポートが抑制されるのは、同じポートに複数のホストが接続されている場合だけです。

図 2 のルータ A は、IGMPv3 グループ/ソース固有のクエリを LAN に送信します。ホスト 2 および 3 は、アドバタイズされたグループおよび送信元からデータを受信することを示すメンバーシップ レポートを送信して、そのクエリーに応答します。この IGMPv3 機能では、SSM がサポートされます。IGMPv1 ホストおよび IGMPv2 ホストが SSM をサポートするよう、SSM を変換する方法については、「IGMP SSM 変換の構成」セクションを参照してください。

図 *8 : IGMPv3* グループ/ソース固有のクエリ



（注） IGMPv3 ホストでは、IGMP メンバーシップ レポートの抑制が行われません。

代表クエリアから送信されるメッセージの存続可能時間（TTL）値は 1 です。つまり、サブネット上の直接接続されたルータからメッセージが転送されることはありません。IGMP の起動時に送信されるクエリ メッセージの頻度および回数を個別に設定したり、スタートアップ

クエリ インターバルを短く設定したりすることで、グループ ステートの確立時間を最小限に抑えることができます。通常は不要ですが、起動後のクエリーインターバルをチューニングすることで、ホスト グループ メンバーシップ メッセージへの応答性と、ネットワーク上のトラフィック量のバランスを調整できます。

⚠

注意 クエリーインターバルを変更すると、マルチキャスト転送能力が著しく低下することがあります。

マルチキャスト ホストがグループを脱退する場合、IGMPv2 以上を実行するホストでは、IGMP Leave メッセージを送信します。このホストがグループを脱退する最後のホストであるかどうかを確認するために、IGMP クエリ メッセージが送信されます。そして、最終メンバーのクエリ応答インターバルと呼ばれる、ユーザーが設定可能なタイマーが起動されます。タイマーが切れる前にレポートが受信されない場合は、ソフトウェアによってグループ ステートが解除されます。ルータはグループ ステートが解除されないかぎり、このグループにマルチキャスト トラフィックを送信し続けます。

輻輳ネットワークでのパケット損失を補正するには、ロバストネス値を設定します。ロバストネス値は、IGMP ソフトウェアがメッセージ送信回数を確認するために使用されます。

224.0.0.0/24 内に含まれるリンク ローカル アドレスは、インターネット割り当て番号局（IANA）によって予約されています。ローカル ネットワーク セグメント上のネットワーク プロトコルでは、これらのアドレスが使用されます。これらのアドレスは TTL が 1 であるため、ルータからは転送されません。IGMP プロセスを実行すると、デフォルトでは、非リンク ローカル アドレスにだけメンバーシップ レポートが送信されます。ただし、リンク ローカル アドレスにレポートが送信されるよう、ソフトウェアの設定を変更することができます。

IGMP パラメータの構成方法については、「IGMP インターフェイス パラメータの構成」セクションを参照してください。

仮想化のサポート

Cisco NX-OS は仮想ルーティングおよびフォーワーディング（VRF）をサポートします。また、複数の VRF インスタンスを定義できます。IGMP を使用して設定された VRF は、次の IGMP 機能をサポートします。

- IGMP の、インターフェイスごとのイネーブル化またはディセーブル化
- IGMPv1、IGMPv2、および IGMPv3 によりルータ側のサポートを提供
- IGMPv2 および IGMPv3 によりホスト側のサポートを提供
- IGMP クエリア パラメータの設定をサポート
- リンク ローカル マルチキャスト グループに対する IGMP レポートのサポート
- IGMP SSM 変換により IGMPv2 グループをソースのセットにマッピング
- Multicast Trace-route（Mtrace）リクエストを処理する Mtrace サーバ機能のサポート

VRF の構成に関する詳細は、『*Cisco Nexus 3548* スイッチ *NX-OS* ユニキャスト ルーティング構成ガイド』を参照してください。

制限事項

Cisco NX-OS Release 6.0(2)A1(1) よりも古い Cisco NX-OS リリースでは、ip igmp join-group コマンドを使用して Nexus 3548 スイッチをマルチキャスト グループにバインドできます。スイッチは、指定されたグループに対して Internet Group Management Protocol（IGMP）結合を生成し、このグループに送信されるマルチキャスト パケットはすべて CPU に送信されます。Nexus 3548 スイッチに接続された、グループに対して要求するレシーバがある場合、パケットのコピーもレシーバに送信されます。

Cisco NX-OS Release 6.0(2)A1(1) 以降のリリースでは、ip igmp join-group コマンドを使用して Outgoing Interface Lists（OILs）をプログラムすることはできません。ストリームに対して要求するレシーバがある場合でも、パケットは送信されません。Nexus 3548 スイッチをマルチキャスト グループにバインドするには、ip igmp join-group の代わりに ip igmp static-oif コマンドを使用します。

VRF を使用した IGMP

複数の仮想ルーティングおよびフォワーディング（VRF）インスタンスを定義することができます。IGMP プロセスはすべての VRF をサポートします。

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

VRF の構成に関する詳細は、『*Cisco Nexus 3548* スイッチ *NX-OS* ユニキャスト ルーティング構成ガイド』を参照してください。

IGMP のデフォルト設定

表 1 では、IGMP パラメータのデフォルト設定をリスト化しています。

表 *2 : IGMP* パラメータのデフォルト設定

パラメータ	デフォルト
IGMP のバージョン	2
スタートアップ クエリー インターバル	30 秒
スタートアップ クエリーの回数	2
ロバストネス値	2
クエリア タイムアウト	255 秒

パラメータ	デフォルト
クエリー タイムアウト	255 秒
クエリーの最大応答時間	10 秒
クエリー インターバル	125 秒
最終メンバーのクエリー応答インターバル	1 秒
最終メンバーのクエリー回数	2
グループ メンバーシップ タイムアウト	260 秒
リンク ローカル マルチキャスト グループのレポート	無効
ルータ アラートの実施	無効
即時離脱	無効化

IGMP パラメータの設定

IGMP グローバル パラメータおよびインターフェイス パラメータを設定すると、IGMP プロセスの動作を変更できます。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

IGMP インターフェイス パラメータの設定

次の表に、設定可能なオプションの IGMP インターフェイス パラメータを示します。

表 *3 : IGMP* インターフェイス パラメータ

パラメータ	説明
IGMP のバージョン	インターフェイスでイネーブルにする IGMP のバージョン。有効な IGMP バージョンは 2 または 3 です。デフォルトは 2 です。

パラメータ	説明
スタティック マルチキャスト グループ	インターフェイスに静的にバインドされるマルチキャスト グループ。(*, G) というステートでインターフェイスの加入先グループを設定するか、グループに加入する送信元 IP を、(S, G) というステートで指定します。**match ip multicast** コマンドで、使用するグループ プレフィックス、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。 （注） (S, G) ステートで設定しても、送信元ツリーが構築されるのは IGMPv3 がイネーブルな場合だけです。SSM の変換に関する詳細は、「IGMP SSM 変換の構成」セクションを参照してください。 ネットワーク上の全マルチキャスト対応ルータを含むマルチキャスト グループを設定すると、このグループに ping 要求を送信することで、すべてのルータから応答を受け取ることができます。
発信インターフェイス（OIF）上のスタティック マルチキャスト グループ	発信インターフェイスに静的にバインドされるマルチキャスト グループ。(*, G) というステートで発信インターフェイスの加入先グループを設定するか、グループに加入する送信元 IP を、(S, G) というステートで指定します。**match ip multicast** コマンドで、使用するグループ プレフィックス、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。 （注） (S, G) ステートで設定しても、送信元ツリーが構築されるのは IGMPv3 がイネーブルな場合だけです。SSM の変換に関する詳細は、「IGMP SSM 変換の構成」セクションを参照してください。
スタートアップ クエリー インターバル	スタートアップ クエリー インターバル。デフォルトでは、ソフトウェアができるだけ迅速にグループ ステートを確立できるように、このインターバルはクエリーインターバルより短く設定されています。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 31 秒です。
スタートアップ クエリーの回数	スタートアップ クエリー インターバル中に送信される起動時のクエリー数。有効範囲は 1 ～ 10 です。デフォルトは 2 です。
ロバストネス値	輻輳ネットワークでのパケット損失を許容範囲内に抑えるために使用される、調整可能なロバストネス変数。ロバストネス変数を大きくすれば、パケットの再送信回数を増やすことができます。有効範囲は 1 ～ 7 です。デフォルトは 2 です。
クエリア タイムアウト	前クエリアがクエリーを停止してから、自身がクエリアとして処理を引き継ぐまで、ソフトウェアが待機する秒数。有効範囲は 1 ～ 65,535 秒です。デフォルト値は 255 秒です。

パラメータ	説明
クエリーの最大応答時間	IGMP クエリーでアドバタイズされる最大応答時間。大きな値を設定すると、ホストの応答時間が延長されるため、ネットワークの IGMP メッセージを調整できます。この値は、クエリー インターバルよりも短く設定する必要があります。有効範囲は 1 ～ 25 秒です。デフォルトは 10 秒です。
クエリー インターバル	IGMP ホスト クエリー メッセージの送信頻度。大きな値を設定すると、ソフトウェアによる IGMP クエリーの送信頻度が低くなるため、ネットワーク上の IGMP メッセージ数を調整できます。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 125 秒です。
最終メンバーのクエリー応答インターバル	サブネット上の既知のアクティブ ホストから最後にホスト Leave メッセージを受信したあと、ソフトウェアが IGMP クエリーへの応答を送信するインターバル。このインターバル中に応答が受信されない場合、グループ ステートは解除されます。この値を使用すると、サブネット上でソフトウェアがトラフィックの送信を停止するタイミングを調整できます。この値を小さく設定すると、グループの最終メンバーまたは送信元が脱退したことを、より短時間で検出できます。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。
最終メンバーのクエリー回数	サブネット上の既知のアクティブ ホストから最後にホスト Leave メッセージを受信したあと、最終メンバーのクエリー応答インターバル中に、ソフトウェアが IGMP クエリーを送信する回数。有効範囲は 1 ～ 5 です。デフォルトは 2 です。 この値を 1 に設定すると、いずれかの方向でパケットが検出されなくなると、クエリー対象のグループまたはチャネルのマルチキャスト ステートが解除されます。次のクエリー インターバルが開始されるまでは、グループを再度関連付けることができます。
グループ メンバーシップ タイムアウト	ルータによって、ネットワーク上にグループのメンバーまたは送信元が存在しないと見なされるまでのグループ メンバーシップ インターバル。有効範囲は 3 ～ 65,535 秒です。デフォルト値は 260 秒です。
リンク ローカル マルチキャスト グループのレポート	224.0.0.0/24 内のグループにレポートを送信できるようにするためのオプション。リンク ローカル アドレスは、ローカル ネットワーク プロトコルだけで使用されます。非リンク ローカル グループには、常にレポートが送信されます。デフォルトではディセーブルになっています。

パラメータ	説明
レポート ポリシー	ルートマップ ポリシーに基づく、IGMP レポートのアクセス ポリシー。 ヒント ルートマップ ポリシーを構成するには、『*Cisco Nexus 3548 NX-OS* ユニキャスト ルーティング構成ガイド』を参照してください。
アクセス グループ	インターフェイスが接続されたサブネット上のホストについて、加入可能なマルチキャスト グループを制御するためのルートマップ ポリシーを設定するオプション。
即時離脱	デバイスからグループ固有のクエリーが送信されないため、所定の IGMP インターフェイスで IGMPv2 グループ メンバーシップの脱退のための待ち時間を最小限にできるオプション。即時脱退をイネーブルにすると、デバイスではグループに関する Leave メッセージの受信後、ただちにマルチキャスト ルーティング テーブルからグループ エントリが削除されます。デフォルトではディセーブルになっています。 （注） このコマンドは、所定のグループに対するインターフェイスの背後に 1 つの受信者しか存在しない場合に使用します。

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

手順の概要

1. **configure terminal**
2. **interface** *interface*
3. **no switchport**
4. **ip igmp version** *value*
5. **ip igmp join-group** {**group** [**source** *source*] | **route-map** *policy-name*}
6. **ip igmp static-oif** {*group* [**source** *source*] | **route-map** *policy-name*}
7. **ip igmp startup-query-interval** *seconds*
8. **ip igmp startup-query-count** *count*
9. **ip igmp robustness-variable** *value*
10. **ip igmp querier-timeout** *seconds*
11. **ip igmp query-timeout** *seconds*
12. **ip igmp query-max-response-time** *seconds*
13. **ip igmp query-interval** *interval*
14. **ip igmp last-member-query-response-time** *seconds*
15. **ip igmp last-member-query-count** *count*
16. **ip igmp group-timeout** *seconds*
17. **ip igmp report-link-local-groups**

18. **ip igmp report-policy** ポリシー
19. **ip igmp access-group** ポリシー
20. **ip igmp immediate-leave**
21. （任意） **show ip igmp interface** [*interface*] [**vrf** *vrf-name* | **all**] [**brief**]
22. （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
ステップ 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。
ステップ 2	**interface** *interface* 例： `switch(config)# interface ethernet 2/1` `switch(config-if)#`	**ethernet** *slot/port* などのインターフェイス タイプおよび番号を入力して、インターフェイス モードを開始します。。
ステップ 3	**no switchport** 例： `switch(config-if)# no switchport` `switch(config-if)#`	
ステップ 4	**ip igmp version** *value* 例： `switch(config-if)# ip igmp version 3`	IGMP バージョンを指定値に設定します。有効な値は 2 または 3 です。デフォルトは 2 です。 このコマンドの **no** 形式を使用すると、バージョンは 2 に設定されます。
ステップ 5	**ip igmp join-group** {**group** [**source** *source*] | **route-map** *policy-name*} 例： `switch(config-if)# ip igmp join-group 230.0.0.0`	指定したグループまたはチャネルに参加するようにデバイス上のインターフェイスを設定します。デバイスは CPU 消費用のマルチキャスト パケットのみを受け入れます。 **注意** このコマンドを使用して生成されたトラフィックは、デバイス CPU で処理可能である必要があります。CPU の負荷制約のため、このコマンドを使用することは（特に形式を問わずスケーリングで使用することは）推奨されません。代わりに **ip igmp static-oif** コマンドの使用を検討してください。

	コマンドまたはアクション	目的
ステップ 6	**ip igmp static-oif** {*group* [**source** *source*] | **route-map** *policy-name*} 例： `switch(config-if)# ip igmp static-oif 230.0.0.0`	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。 （注） IGMPv3 をイネーブルにした場合にのみ、（S,G）ステートに対して送信元ツリーが作成されます。
ステップ 7	**ip igmp startup-query-interval** *seconds* 例： `switch(config-if)# ip igmp startup-query-interval 25`	ソフトウェアの起動時に使用されるクエリー インターバルを設定します。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 31 秒です。
ステップ 8	**ip igmp startup-query-count** *count* 例： `switch(config-if)# ip igmp startup-query-count 3`	ソフトウェアの起動時に使用されるクエリー数を設定します。有効範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 9	**ip igmp robustness-variable** *value* 例： `switch(config-if)# ip igmp robustness-variable 3`	ロバストネス変数を設定します。有効値の範囲は、1 ～ 7 です。デフォルトは 2 です。
ステップ 10	**ip igmp querier-timeout** *seconds* 例： `switch(config-if)# ip igmp querier-timeout 300`	クエリアとして処理を引き継ぐかどうかをソフトウェアが判断するための、クエリア タイムアウト値を設定します。有効範囲は 1 ～ 65,535 秒です。デフォルト値は 255 秒です。
ステップ 11	**ip igmp query-timeout** *seconds* 例： `switch(config-if)# ip igmp query-timeout 300`	クエリアとして処理を引き継ぐかどうかをソフトウェアが判断するための、クエリー タイムアウト値を設定します。有効範囲は 1 ～ 65,535 秒です。デフォルト値は 255 秒です。 （注） このコマンドの機能は、**ip igmp querier-timeout** コマンドと同じです。

	コマンドまたはアクション	目的
ステップ 12	**ip igmp query-max-response-time** *seconds* 例： `switch(config-if)# ip igmp query-max-response-time 15`	IGMP クエリーでアドバタイズされる応答時間を設定します。有効範囲は 1 ～ 25 秒です。デフォルトは 10 秒です。
ステップ 13	**ip igmp query-interval** *interval* 例： `switch(config-if)# ip igmp query-interval 100`	IGMP ホスト クエリー メッセージの送信頻度を設定します。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 125 秒です。
ステップ 14	**ip igmp last-member-query-response-time** *seconds* 例： `switch(config-if)# ip igmp last-member-query-response-time 3`	メンバーシップ レポートを送信してから、ソフトウェアがグループ ステートを解除するまでのクエリー インターバルを設定します。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。
ステップ 15	**ip igmp last-member-query-count** *count* 例： `switch(config-if)# ip igmp last-member-query-count 3`	ホストの Leave メッセージを受信してから、IGMP クエリーが送信される回数を設定します。有効範囲は 1 ～ 5 です。デフォルトは 2 です。
ステップ 16	**ip igmp group-timeout** *seconds* 例： `switch(config-if)# ip igmp group-timeout 300`	IGMPv2 のグループ メンバーシップ タイムアウトを設定します。有効範囲は 3 ～ 65,535 秒です。デフォルト値は 260 秒です。
ステップ 17	**ip igmp report-link-local-groups** 例： `switch(config-if)# ip igmp report-link-local-groups`	224.0.0.0/24 に含まれるグループに対して、レポート送信をイネーブルにします。非リンク ローカル グループには、常にレポートが送信されます。デフォルトでは、リンク ローカル グループにレポートは送信されません。
ステップ 18	**ip igmp report-policy** ポリシー 例： `switch(config-if)# ip igmp report-policy my_report_policy`	ルートマップ ポリシーに基づく、IGMP レポートのアクセス ポリシーを設定します。
ステップ 19	**ip igmp access-group** ポリシー 例： `switch(config-if)# ip igmp access-group my_access_policy`	インターフェイスが接続されたサブネット上のホストについて、加入可能なマルチキャスト グループを制御するためのルートマップ ポリシーを設定します。 （注） **match ip multicast group** コマンドだけがこのルート マップ ポリシーでサポートされます。ACL を照合するための **match ip address** コマンドはサポートされていません。

	コマンドまたはアクション	目的
ステップ 20	**ip igmp immediate-leave** 例： `switch(config-if)# ip igmp immediate-leave`	デバイスが、グループに関する Leave メッセージの受信後、ただちにマルチキャスト ルーティング テーブルからグループ エントリを削除できるようにします。このコマンドを使用すると、デバイスからグループ固有のクエリが送信されないため、所定の IGMP インターフェイスで IGMPv2 グループ メンバーシップの脱退のための待ち時間が最小限になります。デフォルトではディセーブルになっています。 （注） このコマンドは、所定のグループに対するインターフェイスの背後に 1 つの受信者しか存在しない場合に使用します。
ステップ 21	（任意） **show ip igmp interface** [*interface*] [**vrf** *vrf-name* | **all**] [**brief**] 例： `switch(config)# show ip igmp interface`	インターフェイスに関する IGMP 情報を表示します。
ステップ 22	（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。構成の変更を保存します

IGMP SSM 変換の設定

SSM 変換を設定すると、IGMPv1 または IGMPv2 によるメンバーシップ レポートを受信したルータで、SSM がサポートされるようになります。メンバーシップ レポートでグループおよび送信元アドレスを指定する機能を備えているのは、IGMPv3 だけです。グループ プレフィックスのデフォルト範囲は、232.0.0.0/8 です。PIM SSM 範囲を変更するには、「SSM（PIM）の構成」セクションを参照してください。

テーブル 3 に、SSM 変換の例を示します。22-10-2022 11:47

表 *4 : SSM* 変換の例

グループ プレフィックス	送信元アドレス
232.0.0.0/8	10.1.1.1
232.0.0.0/8	10.2.2.2
232.1.0.0/16	10.3.3.3

グループ プレフィックス	送信元アドレス
232.1.1.0/24	10.4.4.4

テーブル 4 に、IGMP メンバーシップ レポートに SSM 変換を適用した場合に、IGMP プロセスによって構築される MRIB ルートを示します。複数の変換を行う場合は、各変換内容に対して (S, G) ステートが作成されます。

表 *5: SSM* 変換適用後の例

IGMPv2 メンバーシップ レポート	作成される **MRIB** ルート
232.1.1.1	(10.4.4.4, 232.1.1.1)
232.2.2.2	(10.1.1.1、232.2.2.2) (10.2.2.2、232.2.2.2)

（注） これは、一部の Cisco IOS ソフトウェアに組み込まれている SSM マッピングと類似した機能です。

手順の概要

1. **configure terminal**
2. **ip igmp ssm-translate** *group-prefix source-addr*
3. （任意） **show running-configuration igmp**
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
ステップ 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。
ステップ 2	**ip igmp ssm-translate** *group-prefix source-addr* 例： `switch(config)# ip igmp ssm-translate 232.0.0.0/8 10.1.1.1`	ルータが IGMPv3 メンバーシップ レポートを受信したときと同様に、(S,G) ステートが作成されるよう、IGMP プロセスによる IGMPv1 または IGMPv2 メンバーシップ レポートの変換を設定します。
ステップ 3	（任意） **show running-configuration igmp** 例： `switch(config)# show running-configuration igmp`	**ssm-translate** コマンドラインを含む、実行コンフィギュレーション情報を表示します。

	コマンドまたはアクション	目的
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

ルータ アラートの適用オプション チェックの設定

IGMPv2 パケットと IGMPv3 パケットに対するルータ アラートの適用オプション チェックを設定できます。

手順の概要

1. **configure terminal**
2. （任意） **[no] ip igmp enforce-router-alert**
3. （任意） **show running-configuration igmp**
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
ステップ 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。
ステップ 2	（任意） **[no] ip igmp enforce-router-alert** 例： `switch(config-if)# ip igmp enforce-router-alert`	IGMPv2 パケットと IGMPv3 パケットに対するルータ アラートの適用オプション チェックを有効または無効にします。デフォルトでは、ルータ アラートの適用オプション チェックはイネーブルです。
ステップ 3	（任意） **show running-configuration igmp** 例： `switch(config)# show running-configuration igmp`	**enforce-router-alert** コマンド ラインを含む、実行コンフィギュレーション情報を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

IGMP ホスト プロキシの設定

ここでは、次の内容について説明します。

機能の概要

IGMP ホスト プロキシ機能は、PIM 対応のマルチキャスト ネットワーク ドメインを、PIM を認識しないドメインに接続するのに役立ちます。この機能は、インターフェイスをプロキシインターフェイスとして設定し、内部 PIM ネットワークで受信した PIM の加入/プルーニングを、IGMP の加入/脱退に置き換えます。

IGMP の加入処理

ホストがマルチキャスト グループに加入するとき、ホストは、加入するマルチキャスト グループに 1 つ以上の送信要求されていないメンバーシップ レポートを送信します。

IGMP の脱退処理

IGMPv2 Leave は、マルチキャスト ネットワークの最後のホストが脱退するときに送信されます。したがって、最後のホストから PIM プルーニングを受信すると、IGMPv2 Leaveがアップストリームに送信され、これ以上関心がないことを示します。

IGMP マルチキャスト アドレス

IP マルチキャスト トラフィックには、グループ アドレス（クラス D IP アドレス）が使用されます。クラス D アドレスの上位 4 ビットは 1110 です。したがって、ホスト グループ アドレスの範囲は 224.0.0.0 ～ 239.255.255.255 であると考えられます。

224.0.0.0 ～ 224.0.0.255 のマルチキャスト アドレスは、ルーティング プロトコルおよびその他のネットワーク制御トラフィックが使用するために予約されています。アドレス 224.0.0.0 は、どのグループにも割り当てられません。

IGMP パケットは IP マルチキャスト グループ アドレスを使用して次のように送信されます。

- IGMP 汎用クエリーは、アドレス 224.0.0.1（サブネット上のすべてのシステム）を宛先とします。
- IGMP グループ固有のクエリは、クエリ対象ルータのグループ IP アドレスを宛先とします。
- IGMP グループ メンバーシップ レポートは、レポート対象のルータのグループ IP アドレスを宛先とします。
- IGMPv2 グループ脱退メッセージは、アドレス 224.0.0.2（サブネット上のすべてのルータ）を宛先とします。

注意事項と制約事項

IGMP ホスト プロキシの構成については、次の注意事項と制限事項を参照してください。

- IGMPv3（RFC 3376）に従って送信元のリストを除外またはブロックすることはサポートされていません。
- IGMP ホスト プロキシ プロキシは、プロキシ インターフェイス上の IGMP 参加/プルーニングに対して受信した PIM 参加/プルーニングです。
- プロキシ インターフェイスが VLAN の場合は、スヌーピングを無効にします。
- IGMP のみを認識するネットワークに接続するために使用できます。
- ホスト プロキシ インターフェイスはレイヤ 3 インターフェイスです。
- （S、G）エントリには、IGMP ホスト プロキシ インターフェイスとして RPF があります。
- 理想的な構成ポイントは RP です。
- IGMP ホスト プロキシは、クエリ モードまたは非送信請求モードにすることができます。
- クエリアが存在しない状態でレポートを送信する必要がある場合は、IGMP ホスト プロキシを非送信請求モードで構成します。
- レイヤ 3 物理ポートで IGMP ホスト プロキシ非送信請求モードを構成します。
- IGMP ホスト プロキシ インターフェイスでは、IP が有効になっている必要があります。
- PIM は、ホスト プロキシ インターフェイスで有効にしないでください。
- IGMP スタティック/結合グループは、IGMP ホスト プロキシ インターフェイスで構成しないでください。

IGMP ホスト プロキシの設定方法

IGMP ホスト プロキシを構成するには、次の手順を実行します。

表 *6 : IGMP* ホスト プロキシの設定

ステップ	コマンド	目的
ステップ 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。
ステップ 2	**interface vlan** *interface*	VLAN インターフェイス モードを開始します。

ステップ	コマンド	目的
ステップ 3	**no shutdown**	インターフェイスを no shutdown モードに設定します。
ステップ 4	**ip address** *ip address*	IP アドレスを設定します。
ステップ 5	[**no**] **ip igmp host-proxy** [**unsolicited** [*time*] | **route-map** *route-map-name* [**unsolicited** [*time*]] | **prefix-list** *prefix-list-name* [**unsolicited** [*time*]]]	ルート マップの IGMP ホスト プロキシを設定します。
ステップ 6	**show ip igmp groups**	ホスト プロキシのため、H タイプの VRF の IGMP 接続グループ メンバーシップを表示します。
ステップ 7	**show ip igmp int vlan** *interface*	VRF の IGMP インターフェイスを表示します。
ステップ 8	**show ip igmp local-groups vlan** *interface*	VRF のための、IGMP ローカル ジョイン グループ メンバーシップを表示します。
ステップ 9	show ip pim host-proxy	PIM ホスト プロキシ インターフェイスを表示します。

IGMP 構成の確認

IGMP の設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show ip igmp interface [*interface*] [**vrf**] *vrf-name*| **all**] [**brief**]	すべてのインターフェイスまたは選択されたインターフェイス、デフォルト VRF、選択された VRF、またはすべての VRF について、IGMP 情報を表示します。
show ip igmp groups *group*|*interface*] [**vrf** *vrf-name* | **all**]	グループまたはインターフェイス、デフォルト VRF、選択された VRF、またはすべての VRF について、IGMP で接続されたグループのメンバーシップを表示します。
show ip igmp route*group* | *interface* **vrf** *vrf-name* | **all**	グループまたはインターフェイス、デフォルト VRF、選択された VRF、またはすべての VRF について、IGMP で接続されたグループのメンバーシップを表示します。

コマンド	目的
show ip igmp local-groups	IGMP ローカル グループ メンバーシップを表示します。
show running-configuration igmp	IGMP 実行コンフィギュレーション情報を表示します。
show startup-configuration igmp	IGMP 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。

これらのコマンドからの出力のフィールドに関する詳細は、『Cisco Nexus 3000 シリーズ マルチキャスト ルーティング コマンド リファレンス』を参照してください。

IGMP の設定例

次に、IGMP パラメータの設定例を示します。

```
switch# configure terminal
switch(config)# ip igmp ssm-translate 232.0.0.0/8 10.1.1.1
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip igmp version 3
switch(config-if)# ip igmp join-group 230.0.0.0
switch(config-if)# ip igmp startup-query-interval 25
switch(config-if)# ip igmp startup-query-count 3
switch(config-if)# ip igmp robustness-variable 3
switch(config-if)# ip igmp querier-timeout 300
switch(config-if)# ip igmp query-timeout 300
switch(config-if)# ip igmp query-max-response-time 15
switch(config-if)# ip igmp query-interval 100
switch(config-if)# ip igmp last-member-query-response-time 3
switch(config-if)# ip igmp last-member-query-count 3
switch(config-if)# ip igmp group-timeout 300
switch(config-if)# ip igmp report-link-local-groups
switch(config-if)# ip igmp report-policy my_report_policy
switch(config-if)# ip igmp access-group my_access_policy
switch(config-if)# ip igmp immediate-leave
```

次に、すべてのマルチキャスト レポート（加入）を受け付けるルート マップを設定する例を示します。

```
switch(config)# route-map foo
switch(config-route-map)# exit
switch(config)# interface vlan 10
switch(config-if)# no switchport
switch(config-if)# ip pim sparse-mode
switch(config-if)# ip igmp report-policy foo
```

次に、すべてのマルチキャスト レポート（加入）を拒否するルート マップを設定する例を示します。

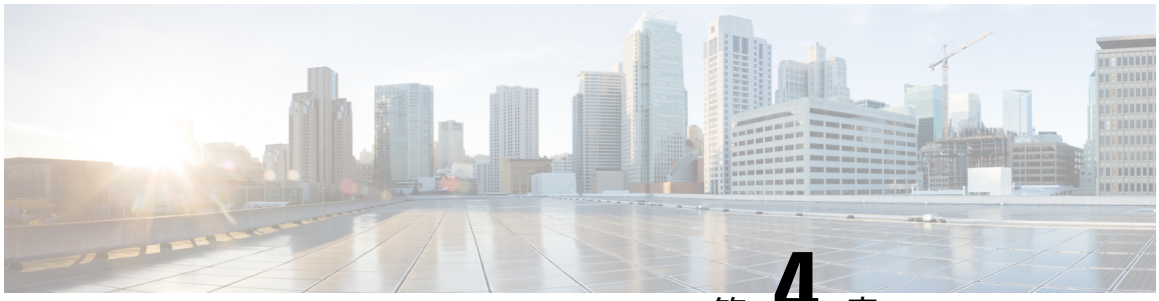
```
switch(config)# route-map foo deny 10
switch(config-route-map)# exit
switch(config)# interface vlan 5
```

```
switch(config-if)# ip pim sparse-mode
switch(config-if)# ip igmp report-policy foo
```

次の作業

PIM および IGMP の関連機能をイネーブルにするには、次の章を参照してください。

- IGMP スヌーピングの構成 （93 ページ）
- MSDP の設定 （113 ページ）



第 4 章

PIM の構成

この章では、IPv4 ネットワーク内の Cisco NX-OS スイッチで、Protocol Independent Multicast（PIM）および bidirectional PIM（PIM-Bidir）機能を構成する方法を説明します。

（注） PIM Any Source Multicast（ASM）および Source-Specific Multicast（SSM）は単方向です。PIM-Bidir は、双方向データ フローを許可する PIM の拡張形式です。PIM-Bidir は送信元固有の状態を排除し、ツリーを任意の数のソースにスケーリングできるようにします。その他の PIM モードおよび PIM-Bidir の違いは、PIM-Bidir に関する情報セクションで説明されています。PIM と PIM-Bidir の構成は似ています。テキストのメモと手順は、構成の違いを示します。

この章は、次の項で構成されています。

PIM に関する情報

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

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

（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有効化するには、各ルータで PIM 機能を有効化してから、マルチキャストに参加する各インターフェイスで、PIM スパース モードを有効化する必要があります。PIM は IPv4 ネットワーク用に設定できます。IPv4 ネットワーク上のルータで IGMP がイネーブルになっていない場合は、PIM によって自動的にイネーブルにされます。IGMP の構成については、IGMP の設定 （17 ページ） を参照してください。

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

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

モードを組み合わせて、さまざまな範囲のグループアドレスに対応することができます。詳細については、PIM の構成 （37 ページ） を参照してください。ASM モードで使用される PIM スパース モードと共有配信ツリーの詳細については、「RFC 4601」を参照してください。

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

PIM-Bidir の詳細については、RFC5015 を参照してください。

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

Hello メッセージ

ルータがマルチキャスト アドレス 224.0.0.13 に PIM hello メッセージを送信して、PIM ネイバー ルータとの隣接関係を確立すると、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 セグメント内でプライオリティが最大のルータを指定ルータ（DR）として選択します。DR 優先順位は、PIM hello メッセージの DR 優先順位値に基づいて決まります。全ルータの DR プライオリティ値が不明、またはプライオリティが等しい場合は、IP アドレスが最上位のルータが DR として選定されます。

注意 PIM hello 間隔を低い値（10 秒未満、またはネットワーク環境に応じて）に変更すると、マルチキャスト トラフィックが失われる可能性があります。

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

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

（注） スイッチで PIM がディセーブルである場合は、IGMP スヌーピング ソフトウェアが PIM hello メッセージを処理します。

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

Join-Prune メッセージ

受信者から送信された、新しいグループまたは送信元に対する 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、インターフェイスからランデブー ポイント方向（ASM モード）または送信元方向（SSM モード）に PIM Join メッセージを送信して、受信者と送信元を接続するツリーを作成します。ランデブー ポイント（RP）は共有ツリーのルートであり、ASM モードで PIM ドメイン内のすべての送信元およびホストによって使用されます。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。PIM Bidir モードでは、Designated Forwarder（DF）が DR の代わりに PIM Join メッセージの送信を実行します。

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） 「PIM-Bidir の詳細」セクション で説明されているように、PIM-Bidir はランデブー ポイント（RP）を使用して双方向ツリーを形成します。

（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。join-prune メッセージ ポリシーの構成に関する詳細は、「PIM スパース モードの構成 」セクションを参照してください。

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

ステートのリフレッシュ

PIM では、3.5 分のタイムアウト間隔でマルチキャスト エントリをリフレッシュする必要があります。ステートをリフレッシュすると、トラ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
- スイッチに手動で RP を設定する場合

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

BSR

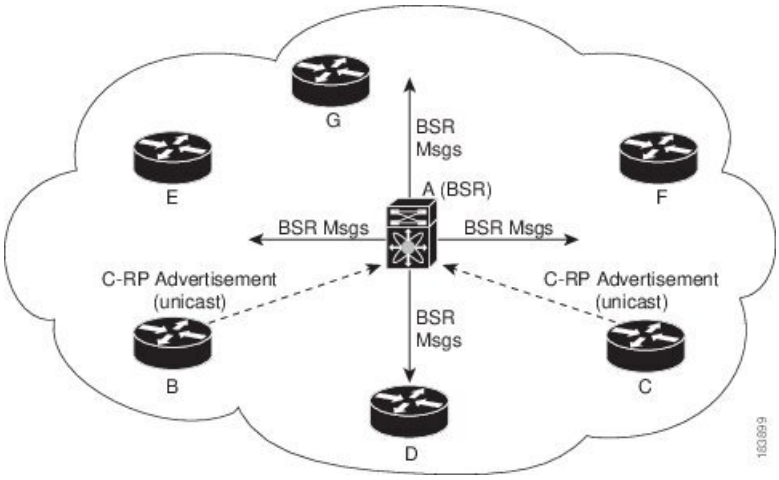
ブートストラップ ルータ（BSR）を使用すると、PIM ドメイン内のすべてのルータで、BSR と同じ RP キャッシュが保持されるようになります。BSR では、BSR 候補 RP から RP セットを選択するよう設定できます。BSR は、ドメイン内のすべてのルータに RP セットをブロードキャストする役割を果たします。ドメイン内の RP を管理するには、1 つまたは複数の候補 BSR を選択します。候補 BSR の 1 つが、ドメインの BSR として選定されます。

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

図 1 は、BSR メカニズム、ソフトウェアによって選択された BSR であるルータ A が、イ有効になっているすべてのインターフェイスから BSR メッセージを送信する場所を示しています（図の実線で表示）。このメッセージには RP セットが含まれており、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 *9: BSR* メカニズム



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

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

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

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

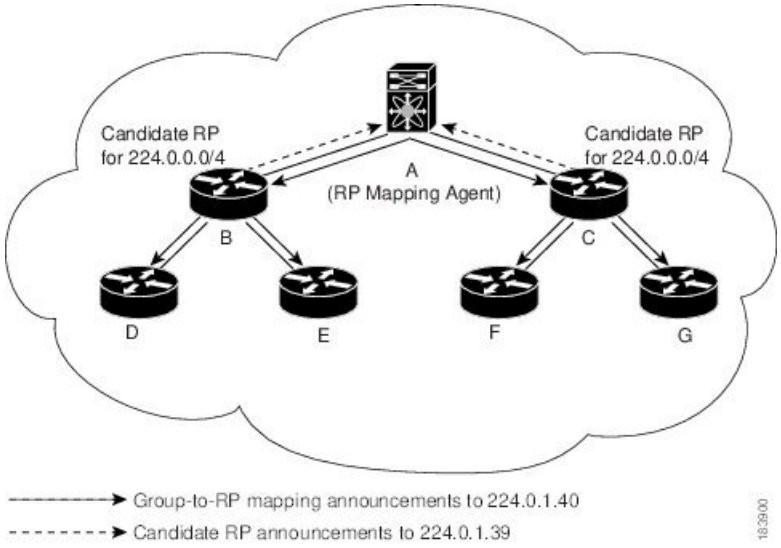
Auto-RP

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

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

図 2 では、Auto-RP の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 *10 : Auto-RP* のメカニズム



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

Auto-RP の構成に関する詳細は、Auto-RP の設定 （62 ページ） セクションを参照してください。

Anycast-RP

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

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

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

PIM Anycast-RP の詳細については、RFC 4610 を参照してください。

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

PIM 登録メッセージ

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

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

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

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

ip pim register-source コマンドを使用して、登録メッセージの送信元 IP アドレスが、RP がパケットを送信できる一意のルーテッド 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。

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

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

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

指定ルータ

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

LAN セグメントごとの DR は、「Hello メッセージ」セクション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（*、G）または（S、G）PIM Join メッセージを発信します。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。

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

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(2)F 以降、マルチキャスト フロー パス可視化（FPV）機能は、Cisco Nexus 3548-XL プラットフォーム スイッチでサポートされています。この機能により、Cisco Nexus 3548-XL プラットフォーム 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 3548-XL プラットフォーム 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。

マルチキャスト フロー パスの可視化の注意事項と制限事項

マルチキャスト フロー パスの可視化機能には、次の注意事項と制限事項

- Cisco NX-OS 10.2(2)F 以降、マルチキャスト フロー パスの可視化機能は Cisco Nexus 3548-XL プラットフォーム スイッチでサポートされています。
- この機能は、以下をサポートしていません。

- PIM Bidir
- VPC
- ルート リーク

- （*、G）、（S、G）を含む L3 ルートのみエクスポートできます。
- マルチキャスト ASM および SSM をサポートします。
- L3 ルーテッド ポート（任意のタイプ）と SVI L2 ファンアウトの両方をサポートします。
- L3 物理ポート、L2 物理ポート、ポートチャネルおよびポートチャネル サブインターフェイス、サブインターフェイスなどのインターフェイスをサポートします。

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。ドメイン境界パラメータの構成に関する詳細は、「メッセージ フィルタリングの構成」セクションを参照してください。

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

仮想化のサポート

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

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

VRF の構成に関する詳細は、『Cisco Nexus 3548 スイッチ NX-OS ユニキャスト ルーティング構成ガイド』を参照してください。

PIM-Bidir に関する情報

PIM-Bidir

PIM（PIM-Bidir）の双方向モードは、個々の PIM ドメイン内での効率的な多対多通信用に設計された PIM プロトコルの拡張機能です。双方向モードのマルチキャスト グループでは、最小限の追加オーバーヘッドで、任意の数の送信元にスケールできます。

PIM スパース モードで作成される共有ツリーは単方向性です。これは、データ ストリームが共有ツリーのルート、つまりランデブー ポイント（RP）にもたらされるように送信元ツリーを作成する必要があることを意味します。これにより、データ ストリームはブランチを下方向に転送され、レシーバに到達できます。これは双方向共有ツリーとみなされるため、送信元のデータは共有ツリーの上方向にある RP に向かって流れることはできません。

PIM-Bidir は PIM スパース モード（PIM-SM）のメカニズムから派生しており、多くの共有ツリー操作を共有しています。PIM Bidir も共有ツリー上の RP アップストリームに対して無条件の送信元トラフィックの転送が可能ですが、PIM-Bidir は、PIM-SM で使用されるような送信元の登録プロセスがないという点で異なります。PIM-Bidir のこれらの変更は、すべてのデバイスで（*、G）マルチキャスト ルーティング エントリだけに基づいてトラフィックを転送できるようにするには、必要にして十分なものです。この機能では、ソース固有のステートは不要であり、スケーリング機能を使用して任意の数のソースに対応できます。

双方向共有ツリー

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

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

図 3 および図 4 は、双方向共有ツリーに対するデバイスごとの単方向共有ツリーおよびソースツリーの状態の違いを示しています。

図 *11* : 単方向共有ツリーおよびソース ツリー

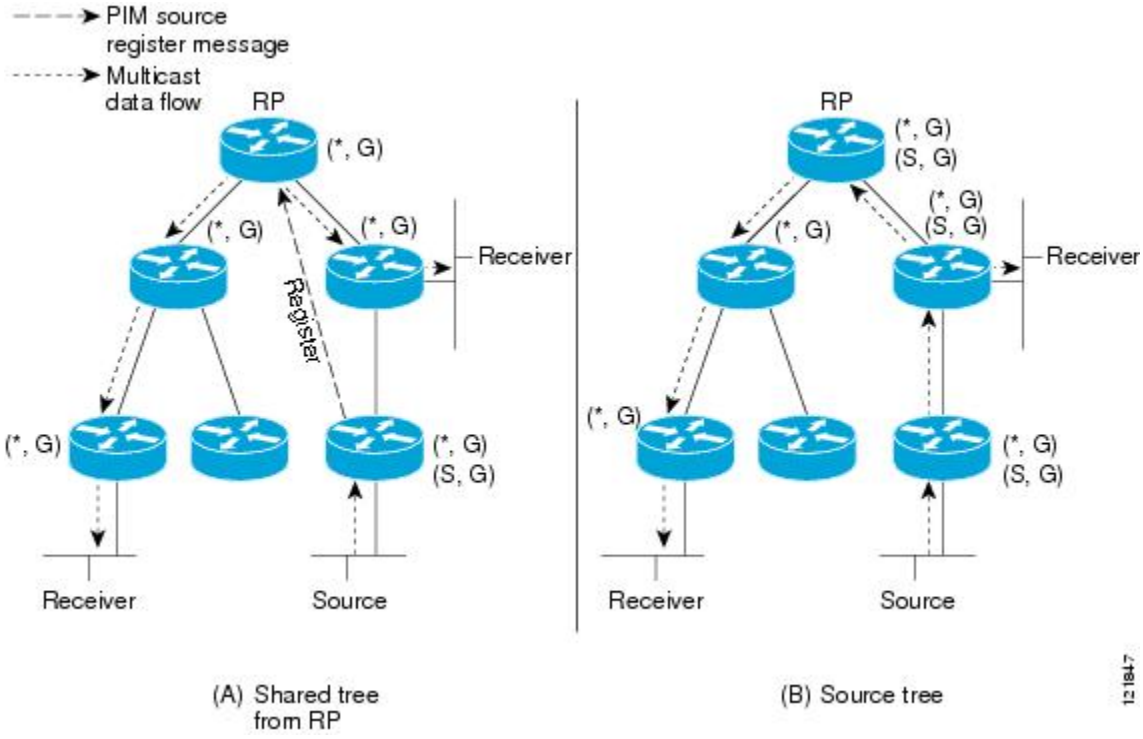
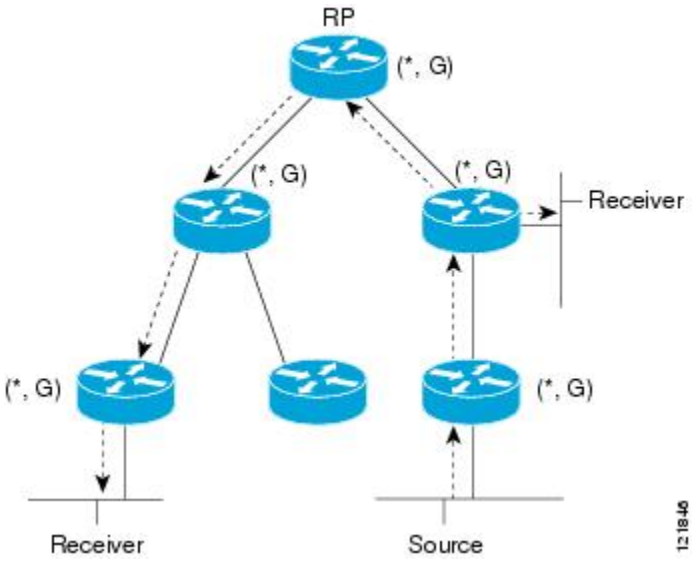


図 *12* : 双方向共有ツリー



RP からレシーバ方向へダウンストリームで転送されるパケットの場合、PIM-Bidir と PIM スパース モード（PIM-SM）間の基本的な違いはありません。ソースからアップストリームで RP 方向に渡されるトラフィックの場合、PIM-SM は実質的に PIM-SM から逸脱します。

PIM-SM は、トラフィックを 1 つのリバース パス転送（RPF）インターフェイスからのみ受け入れるため、ツリーのアップストリーム方向にトラフィックを転送できません。（共有ツリー

の）このインターフェイスは RP 方向を指し、そのため、ダウンストリーム トラフィック フローのみを許可します。アップストリーム トラフィックはまずユニキャスト登録メッセージにカプセル化され、これがソースの指定ルータ（DR）から RP に渡されます。次に、RP は送信元にルートがあるソース パス ツリー（SPT）を結合します。したがって、PIM-SM では、RP に宛てられた送信元からのトラフィックは、共有ツリー内でアップストリームにはフローしませんが、送信元の SPT に沿って RP に到達するまでダウンストリームでフローします。RP から、トラフィックは共有ツリーに沿ってすべてのレシーバに向けてフローします。

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

DF 選定

すべてのネットワーク セグメントおよびポイントツーポイント リンクで、すべての PIM デバイスは指定フォワーダー（DF）選出と呼ばれる手順に参加します。 この手順では、双方向グループのランデブー ポイント（RP）ごとに 1 つのデバイスを DF として選択します。 DF は、そのネットワークで受信したマルチキャスト パケットの転送を行います。

DF 選定は、ユニキャスト ルーティング メトリックに基づきます。RP に対して最も優先されるユニキャスト ルーティング メトリクスを持つデバイスが DF になります。 この方法を使用することによって、RP へのパラレル等コストパスがある場合にも、すべてのパケットのコピー 1 つだけが RP に送信されます。

DF は双方向グループのすべての RP に対して選定されます。その結果、任意のネットワーク セグメントで複数のデバイスが DF として選出され、各 RP に 1 つ選出される場合があります。複数のインターフェイスで DF として特定のデバイスを選出できます。

双方向グループ ツリー ビルディング

双方向グループの共有ツリーに参加する手順は、PIM スパース モード（PIM-SM）での手順とほとんど同じです。主な相違は、双方向グループでは、指定ルータ（DR）のロールがランデブー ポイント（RP）の指定フォワーダ（DF）によって継承されることです。

ローカル レシーバを持つネットワークでは、DF として選定されたデバイスのみがインターネット グループ管理プロトコル（IGMP）加入メッセージの受信時に発信インターフェイス リスト（oiflist）を読み込み、(*、G) 加入および脱退メッセージを RP 方向にアップストリームに送信します。ダウンストリーム デバイスが共有ツリーに参加する場合、PIM 加入および脱退メッセージのリバース パス転送（RPF）ネイバーが常に RP に向かうインターフェイスの DF に選定されます。

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

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

パケット転送

デバイスは双方向グループに対してのみ（*、G）エントリを作成します。（*、G）エントリの送信インターフェイス リストには、デバイスが指定フォワーダを確立し、Internet Group Management プロトコル（IGMP）または Protocol Independent Multicast（PIM）Join メッセージのいずれかを受信したすべてのインターフェイスのリストが含まれます。デバイスが送信者のみのブランチに位置している場合、（*、G）状態が作成されますが、RP アドレスがルータのローカル インターフェイスに属していない場合、oiflist には RPF インターフェイスのみが含まれます。この場合、oiflist は空です。

パケットがランデブー ポイントに向かって Reverse Path Forwarding（RPF）インターフェイスから受信された場合、パケットは（*、G）エントリの oiflist に基づいてダウンストリームで転送されます。それ以外の場合、受信インターフェイスの DF であるデバイスのみがパケットを RP 方向にアップストリームに転送します。その他のデバイスはすべてパケットを廃棄する必要があります。

PIM の注意事項と制約事項

PIM には、次の注意事項と制限事項があります。

- Cisco NX-OS の PIM は、いずれのバージョンの PIM デンス モードまたは PIM スパース モード バージョン 1 とも相互運用性がありません。
- Cisco Nexus 3500 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。
- 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 RP インターバルを 15 秒以上に設定してください。
- スイッチに 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 をスイッチが受信した場合、このスイッチが不正に 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ダウンストリーム ルータではその BSM を受信できなくなります。また、ダウンストリーム スイッチでは、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、これらのスイッチでは RP 情報を受信できなくなります。

  - BSR に異なるスイッチから送られた 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 はダウンストリーム スイッチで受信されなくなります。

- OpenFlow は、N3K-C3548-10GX プラットフォームでサポートされています。
- パッチ機能は、Cisco Nexus 3500 シリーズ プラットフォームではサポートされていません。
- サポートされる PIM マルチキャスト ルートの数を 8000 を超えて増やすには、**ip pim sg-expiry-timer infinity** コマンドを使用する必要があります。
- フローが開始されるマルチキャスト ストリームに一致する ACL ログが構成されている場合、ACL ログがパケットを消費するため、対応する S、G は作成されません。S、G ルート エントリを作成するには、ログ オプションを無効にする必要があります。
- RPF インターフェイスが SVI の場合、RPF 障害は *、G または S、G では発生しません。RPF としての SVI の場合、ハードウェアでのエントリの一致は、キーとしての VLAN、S、G に基づいて行われます。したがって、異なる VLAN 上のトラフィックはヒットせず、RPF 障害として CPU にパントされます。
- **ip pim spt-threshold infinity group-list** および **ip pim use-shared-tree-only group-list** コマンドは、スタンドアロン（非 vPC）のラスト ホップ ルータ（LHR）構成でサポートされています。Cisco NX-OS リリース 9.3(10) 以降、**ip pim spt-threshold infinity group-list** および **ip pim use-shared-tree-only group-list** コマンドは、Cisco Nexus 3548 スイッチの仮想ポート チャネル（vPC）でもサポートされています。
- **ip pim spt-threshold infinity group-list** および **ip pim use-shared-tree-only group-list** コマンドは、スタンドアロンの Cisco Nexus 3548 スイッチでサポートされています。Cisco NX-OS リリース 10.2(3) 以降、**ip pim spt-threshold infinity group-list** および **ip pim use-shared-tree-only group-list** コマンドは、Cisco Nexus 3548 スイッチの仮想ポート チャネル（vPC）でも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。
- PIM は、送信元、レシーバ、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。
- 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。
  - この機能は VPC ではサポートされていません。

PIM-Bidir の注意事項と制限事項

Cisco Nexus 3548 スイッチでの PIM-Bidir の使用には、いくつかの制限があります。特に、内部実装による制限として、一度グループ範囲がある VRF で Bidir として設定されたら、そのグループ範囲を他の VRF に対して再度使用することはできません。たとえば、グループ範囲 225.1.0.0/16 がデフォルト VRF で Bidir として構成されている場合、このグループ範囲のグループまたは一部を別の VRF で（ASM、Bidir、または SSM として）再利用することはできません。

PIM のデフォルト設定

表 1 では、PIM パラメータのデフォルト設定をリスト化しています。

表 *7: PIM* パラメータのデフォルト設定

パラメータ	デフォルト
共有ツリーだけを使用	無効
再起動時にルートをフラッシュ	無効
ネイバーの変更の記録	無効
Auto-RP メッセージ アクション	無効
BSR メッセージ アクション	無効
SSM マルチキャスト グループ範囲またはポリシー	IPv4 の場合 232.0.0.0/8
PIM スパース モード	無効
DR プライオリティ	0
hello 認証モード	無効
ドメイン境界	無効
RP アドレス ポリシー	メッセージをフィルタリングしない
PIM Register メッセージ ポリシー	メッセージをフィルタリングしない
BSR 候補 RP ポリシー	メッセージをフィルタリングしない
BSR ポリシー	メッセージをフィルタリングしない
Auto-RP マッピング エージェント ポリシー	メッセージをフィルタリングしない
Auto-RP 候補 RP ポリシー	メッセージをフィルタリングしない

パラメータ	デフォルト
Join/Prune ポリシー	メッセージをフィルタリングしない
ネイバーとの隣接関係ポリシー	すべての PIM ネイバーと隣接関係を確立

PIM の構成

PIM は、各インターフェイスに設定できます。

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

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

表 *8 : PIM* のマルチキャスト配信モード

マルチキャスト配信モード	RP 設定の必要性	説明
アーキテクチャ セールス マネージャ（ASM）	はい	任意の送信元のマルチキャスト
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 を設定する手順は、次のとおりです。

手順

ステップ 1 テーブル 2 に示したマルチキャスト配信モードについて、各モードで構成するマルチキャスト グループの範囲を選択します。

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

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

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

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

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

PIM 機能の有効化

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

始める前に

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

手順

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

PIM スパース モードの設定

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

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

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	**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。
ステップ 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。
ステップ 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。
ステップ 4	（任意） **ip pim rp** [*ip prefix*] **vrf** *vrf-name*| **all** 例： `switch(config)# show ip pim rp`	Auto-RP および BSR の受信/転送ステートなど、PIM RP 情報を表示します。
ステップ 5	（任意） **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。
ステップ 6	（任意） [**ip** |**ipv4**] **routing multicast holddown***holddown-period* 例：	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

	コマンドまたはアクション	目的
	`switch(config)# ip routing multicast holddown 100`	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。
ステップ 7	（任意） **show running-configuration pim** 例： `switch(config)# show running-configuration pim`	Register レート制限を含めた PIM の実行コンフィギュレーション情報を表示します。
ステップ 8	**interface** *interface* 例： `switch(config)# interface ethernet 2/1` `switch(config-if)#`	**ethernet** *slot/port* などのインターフェイス タイプおよび番号を入力して、インターフェイス モードを開始します。
ステップ 9	**no switchport** 例： `sswitch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 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。
ステップ 11	（任意） **ip pim dr-priority** *priority* 例： `switch(config-if)# ip pim dr-priority 192`	PIM hello メッセージの一部としてアドバタイズされる指定ルータ（DR）プライオリティを設定します。有効範囲は 1 ～ 4294967295 です。デフォルトは 1 です。
ステップ 12	（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）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。
ステップ 13	（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 1 ～ 4294967295 です。デフォルト値は 30000 です。 （注） 最小値は 1 ミリ秒です。

	コマンドまたはアクション	目的
ステップ 14	（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。
ステップ 15	（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。
ステップ 16	（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。
ステップ 17	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	設定変更を保存します。

ASM または Bidir の構成

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。

（注） ASM または PIM-Bidir の構成前に、最初に以前のセクションで説明されているように PIM を有効にします。

静的 RP の設定（PIM）

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

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

（注） 単方向 PIM を構成する場合は、ステップ 2 でコマンドの末尾からパラメータ [bidir] を削除し、次のようにします。**ip pim rp-address** *rp-address* [**group-list** *ip-prefix* | **route-map** *policy-name*]

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	**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。
ステップ 2	**ip pim rp-address** *rp-address* [**group-list** *ip-prefix* | **route-map** *policy-name*] 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** コマンドとともに使用するグループ プレフィックスにリスト化されるルートマップ ポリシー名を指定できます。デフォルト モードは ASM です。デフォルトのグループ範囲は 224.0.0.0 ～ 239.255.255.255 です。 この例では、指定したグループ範囲に PIM Bidir モードを設定しています。
ステップ 3	（任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name* | **all**] 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。

	コマンドまたはアクション	目的
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

BSR の設定

BSR を設定するには、候補 BSR および候補 RP を選択します。

⚠

注意 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 を表 3 で説明されている引数で構成できます。

表 *9*：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	ハッシュ長は、マスクを適用するために使用される上位桁の 1 の個数です。マスクでは、候補 RP のグループ アドレス範囲の論理積をとることにより、ハッシュ値を算出します。マスクは、グループ範囲が等しい一連の RP に割り当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。
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。

候補 RP を表 4 で説明されている引数とキーワードで構成できます。

表 *10*：*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スト グループ。

引数またはキーワード	説明
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 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。
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 プ範囲内で優先度が最も高い RP が選定されます。優先度が等しい場合 IP アドレスが最上位の RP が選定されます。（最も高い優先度は最も低 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 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 度は 0 ～ 255 の間で、大きい値ほど優先度が高くなります。

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

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

候補 BSR および候補 RP を設定する手順は、次のとおりです。

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

BSR の設定

（注）　PIM-ASM を構成した場合は、ステップ 3 でコマンドからパラメータ bidir を削除すると、コマンド エントリが以下を読み取ります。

ip pim [**bsr**] **rp-candidate** *interface* **group-list** *ip-prefix* [**priority** *priority*] [**interval** *interval*]

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	**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。
ステップ 2	**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。パラメータの詳細については、テーブル 10 を参照してください。
ステップ 3	（任意） **ip pim** [**bsr**] **rp-candidate** *interface* **group-list** *ip-prefix* **route-map** *policy-name* **priority** *priority* **interval** *interval* 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。 （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。 例では、PIM-Bidir 候補 RP を構成します。 （注） ASM 候補 RP を構成するには、コマンドの最後にあるパラメータ bidir を省略します。
ステップ 4	（任意） **show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] 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。
ステップ 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。

Auto-RP の設定

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

⚠

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

Auto-RP マッピング エージェントの設定では、テーブル 5 で説明された引数を指定できます。

表 *11 : 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。 （注） 「PIM スパース モードの構成」セクションの境界ドメイン機能を参照してください。

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

候補 RP をテーブル 6 で説明されている引数とキーワードで構成できます。

表 *12 : 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。プレフィックス形式で指定します。
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能時間（TTL）値。この値の範囲は 1 ～ 255 であり、デフォルト値は 32 です。 （注） 「PIM または PIM6 スパース モードの構成」セクションの境界ドメイン機能を参照してください。

引数またはキーワード	説明
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
bidir	指定しない場合、現在の RP は ASM モードになります。指定 場合、RP は bidir モードになります。

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

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

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

Auto RP の構成

（注）　ステップ 3 に示すコマンドでパラメータ bidir を使用するのは、双方向 PIM（PIM-Bidir）の場合のみです。 単方向 PIM を構成している場合、コマンドは次のようになります。**ip pim** {**send-rp-announce** | {**auto-rp rp-candidate**}} interface **group-list** *ip-prefix* [**scope** *ttl*] [**interval** *interval*]

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	**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。
ステップ 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。パラメータの詳細については、テーブル 12 を参照してください。
ステップ 3	**ip pim** {**send-rp-announce** | {**auto-rp rp-candidate**}} interface **group-list** *ip-prefix* [**scope** *ttl*] [**interval** *interval*] [**bidir**] 例： `switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24 bidir`	Auto-RP の候補 RP を設定します。デフォルト スコープは 32 です。デフォルト インターバルは 60 秒です。デフォルトでは、ASM の候補 RP が作成されます。パラメータの詳細については、テーブル 4 ～ 6 を参照してください。 （注） 候補 RP インターバルは 15 秒以上に設定することを推奨します。 この例では、双方向候補 RP を構成します。 （注） この例では、コマンドの末尾にある bidir パラメータを省略して、ASM 候補 RP を作成します。
ステップ 4	（任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name* | **all**] 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。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

PIM エニーキャスト RP セットの設定（PIM）

PIM Anycast-RP セットを設定する手順は、次のとおりです。

ステップ 1 PIM エニーキャスト RP セット内のルータを選択します。

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

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

手順

	コマンドまたはアクション	目的
ステップ 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。
ステップ 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。
ステップ 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。 この例では、Anycast-RP の IP アドレスを設定しています。
ステップ 4	**exit** 例： `switch(config)# exit`	コンフィギュレーション モードに戻ります。
ステップ 5	**ip pim anycast-rp** *anycast-rp-address anycast-rp-peer-address* 例： `switch(config)# ip pim anycast-rp 192.0.2.3 192.0.2.31`	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。
ステップ 6	Anycast-RP セットに属する各ピア RP で、同じ Anycast-RP アドレスを使用してステップ 5 を繰り返します。	—
ステップ 7	**ip**[**autoconfig** | *ip-address* [**secondary**]]	PIM モードとグループ範囲を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

ASM 専用の共有ツリーの設定（PIM）

共有ツリーを構成できるのは、Any Source Multicast（ASM）グループの最終ホップ ルータだけです。この場合、新たな受信者がアクティブ グループに加入した場合、このルータでは共有ツリーから SPT へのスイッチオーバーは実行されません。**match ip[v6] multicast** コマンドを使用

して、共有ツリーの使用を強制するグループ範囲を指定できます。このオプションは、送信元ツリーに対する Join/Prune メッセージを受信した場合の、ルータの標準動作には影響を与えません。

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

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	**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。
ステップ 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。 （注） このコマンドは、スタンドアロン（非 vPC）のラスト ホップ ルータ（LHR）構成でサポートされています。 （注） **ip pim use-shared-tree-only group-list** コマンドは、スタンドアロンの Cisco Nexus 3548 スイッチでサポートされています。Cisco NX-OS リリース 10.2(3) 以降、このコマンドは Cisco Nexus 3548 スイッチの仮想ポート チャネル（vPC）でもサポートされています。

	コマンドまたはアクション	目的
ステップ 3	（任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name* | **all**] 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。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	設定変更を保存します。

SSM（PIM）の設定

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

（注） SSM と PIM-Bidir と組み合わせて構成することはできません。

IPv4 ネットワーク上のホストから、送信元を特定してマルチキャスト データを要求するには、このホストおよびこのホストの DR で、IGMPv3 が実行されている必要があります。SSM モードでインターフェイスに PIM を設定する場合は、IGMPv3 をイネーブルにするのが一般的です。IGMPv1 または IGMPv2 が実行されているホストでは、SSM 変換を使用して、グループと送信元のマッピング設定を行うことができます。詳細については、「IGMP の設定 （17 ページ）」を参照してください。

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

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

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

始める前に

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

手順

<table>
<tr><th></th><th>コマンドまたはアクション</th><th>目的</th></tr>
<tr><td>ステップ 1</td><td>configure terminal
例：
<pre>switch# configure terminal
switch(config)#</pre></td><td>グローバル コンフィギュレーション モードを開始します。</td></tr>
<tr><td>ステップ 2</td><td><table>
<tr><th>オプション</th><th>説明</th></tr>
<tr><td>コマンド</td><td>目的</td></tr>
<tr><td>ip pim ssm range {ip-prefix | none} | route-map policy-name}
例：
<pre>switch(config)# ip pim ssm range 239.128.1.0/24</pre></td><td>SSM モードで処理するグループ範囲を最大 4 つまで設定します。match ip multicast コマンドとともに使用するグループ プレフィックスにリスト化されるルートマップ ポリシー名を指定できます。デフォルトの範囲は 232.0.0.0/8 です。キーワード none が指定されている場合、すべてのグループ範囲が削除されます。</td></tr>
<tr><td>no ip pim ssm range {range ip-prefix | none} | route-map policy-name}
例：
<pre>switch(config)# no ip pim ssm range none</pre></td><td>SSM 範囲から指定のプレフィックスを削除するか、ルートマップ ポリシーを削除します。キーワード none が指定されている場合、SSM 範囲を 232.0.0.0/8 のデフォルトにリセットします。</td></tr>
</table></td><td></td></tr>
<tr><td>ステップ 3</td><td>（任意） show ip pim group-range [ip-prefix | vrf vrf-name]
例：
<pre>switch(config)# show ip pim group-range</pre></td><td>PIM モードとグループ範囲を表示します。</td></tr>
<tr><td>ステップ 4</td><td>（任意） copy running-config startup-config
例：
<pre>switch(config)# copy running-config startup-config</pre></td><td>設定変更を保存します。</td></tr>
</table>

マルチキャスト用 RPF ルートの設定

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

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	**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。
ステップ 2	**ip mroute** {*ip-addr mask* | *ip-prefix*} {*next-hop* | *nh-prefix* |} [*route-preference*] [**vrf** *vrf-name*] 例： `switch(config)# ip mroute 192.0.2.33/24 192.0.2.1`	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。
ステップ 3	（任意） **show ip static-route** [**vrf** *vrf-name*] 例： `switch(config)# show ip static-route`	設定されているスタティック ルートを表示します。
ステップ 4	（任意） **copy running-config startup-config**	設定変更を保存します。

RP 情報配信を制御するルート マップの設定（PIM）

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。「メッセージ フィルタリングの構成」セクションで説明されているコマンドのルート マップを使用します。

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

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	**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。
ステップ 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。構成方法は **permit** キーワードを使用します。
ステップ 3	**match ip multicast** {**rp** *ip-address* [**rp-type** *rp-type*] [**group** *ip-prefix*]} | {**group** *ip-prefix* **rp** *ip-address* [**rp-type** *rp-type*]} 例： `switch(config)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 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。ユーザは RP のタイプ（ASM または Bidir）を指定できます。例で示すとおり、このコンフィギュレーション モードでは、グループおよび RP を指定する必要があります。 （注） BSR RP、Auto-RP、およびスタティック RP では、group-range キーワードは使用できません。このコマンドは、permit と deny の両方を許可します。一部の match mask コマンドは、permit または deny を許可しません。
ステップ 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。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config-route-map)# copy running-config startup-config`	設定変更を保存します。

メッセージ フィルタリングの設定

テーブル 7 に、PIM および PIM6 でのメッセージ フィルタリングの構成方法を示します。

表 *13 : PIM* および *PIM6* でのメッセージ フィルタリング

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

メッセージの種類	説明
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。

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

（注） ルートマップ ポリシーの構成に関する詳細は、『Cisco Nexus 3548 スイッチ NX-OS ユニキャスト ルーティング構成ガイド』

メッセージ フィルタリングの設定

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	**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。
ステップ 2	（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** コマンドを使用して、グループまたはグループおよび送信元アドレスを指定できます。
ステップ 3	（任意） **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有効にします。*match ip multicast* コマンドで、RP、グループ アドレス、およびタイプ（ASM）を指定できます。このコマンドは、BSR の選定対象のルータで使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。

	コマンドまたはアクション	目的
ステップ 4	（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。
ステップ 5	（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 ポリシーに基づいた Auto-RP マッピング エージェントで Auto-RP 通知メッセージをフィルタリングできるようにし、**match ip multicast** コマンドで RP アドレスとグループ アドレスを指定できるようにします。 このコマンドは、マッピング エージェントで使用できます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。
ステップ 6	（任意） **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。
ステップ 7	**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。
ステップ 8	**no switchport** 例： `switch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 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有効にします。 **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。 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。

	コマンドまたはアクション	目的
ステップ 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。
ステップ 11	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	設定変更を保存します。

ルートのフラッシュ

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	**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。
ステップ 2	**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。
ステップ 3	**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。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

PIM 設定の確認

PIM の設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show ip mroute { *source* | *group* [*source*]} [**vrf** *vrf-name* | **all**]	IP マルチキャスト ルーティング テーブルを表示します。
show ip pim group-range [**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 pim rp** コマンドを参照してください。
show ip 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 pim neighbor [**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 pim oif-list *group* [*source*] [**vrf** *vrf-name* | **all**]	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 pim route {**source group** | **group** [**source**]} [**vrf** *vrf-name* | **all**]	マルチキャスト ルート（S、G）の PIM 加入を受信したインターフェイスなど、各マルチキャストルートの情報を表示します。
show ip pim rp [**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 pim group-range** コマンドを参照してください。
show ip pim rp-hash [**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。
show running-configuration pim	実行コンフィギュレーション情報を表示します。
show startup-configuration pim	実行コンフィギュレーション情報を表示します。
show ip pim vrf [*vrf-name* | **all**] [**detail**]	各 VRF の情報を表示します。
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。

統計の表示

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

PIM 統計情報の表示

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

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

これらのコマンドから出力でフィールドに関する詳細は、『Cisco Nexus 3000 シリーズ NX-OS マルチキャスト ルーティング コマンド リファレンス』を参照してください。

PIM 統計情報のクリア

テーブル 8 にリスト化されたコマンドを使用して PIM および PIM6 統計をクリアできます。PIM に **show ip** 形式のコマンドを使用します。

表 *14*: 統計情報をクリアする *PIM* コマンド

コマンド	説明
clear ippim 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 pim policy statistics	Register、RP、および Join/Prune メッセージのポリシーについて、ポリシーカウンタをクリアします。
clear ip pim statistics [**vrf** *vrf-name* | **all**]	PIMプロセスで使用されるグローバルカウンタをクリアします。

PIM の設定例

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

SSM の構成例

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

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)# no switchport
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。「IGMP の設定 （17 ページ）」を参照してください。通常は、SSM をサポートするために、PIM インターフェイスに IGMPv3 を設定します。

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

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
```

次に、SSM モードで PIM を構成する方法の例を示します。

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

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. **手順 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 パラメータを構成します。すべてのインターフェイスで PIM をイネーブルにすることを推奨します。

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

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

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

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

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

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

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

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

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

PIM Anycast-RP の設定例

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

1. **手順 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 パラメータを構成します。すべてのインターフェイスで PIM をイネーブルにすることを推奨します。

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

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

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

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

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

4. **ステップ 4**：すべてのルータで Anycast-RP として使用される RP-address を構成します。

   ```
   switch# configure terminal
   switch(config)# ip pim rp-address 192.0.2.3
   ```

5. **ステップ 5**：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
   ```

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

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

```
ip pim anycast-rp 192.0.2.3 192.0.2.31
ip pim anycast-rp 192.0.2.3 192.0.2.32
```

BSR を使用した PIM-Bidir の構成例

次のセクションでは、BSR で PIM-Bidir モードを構成する方法を示します。手順は、特定のグループ範囲に対して Auto-RP またはスタティック RP を使用して PIM を構成するために使用する手順と似ています。

BSR メカニズムを使用して ASM モードで Bidir 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. **手順 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 パラメータを構成します。すべてのインターフェイスで PIM をイネーブルにすることを推奨します。

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

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

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

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

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

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

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

次に、BSR メカニズムを使用して PIM Bidir モードを構成する例、特に同一のルータに BSR と RP を構成する場合の例を示します。

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

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、ユーザーが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、入力マルチキャスト ストリーム (S1、G1) から出力 (S2、G2) インターフェイスへのマル

チキャスト ネットワーク アドレス変換 (NAT) です。この機能は、一般にマルチキャスト サービス リフレクション機能 (SR 機能) と呼ばれます。

SR 機能は、次の 2 つのフレーバーでサポートされています。

- 通常モード マルチキャスト NAT

通常モードでは、S1、G1 インターフェイスとして着信するパケットは S2、G2 インターフェイスに変換され、発信パケットの宛先 MAC アドレスは G2 インターフェイス（たとえば、変換されたグループ）のマルチキャスト MAC アドレスとして変換されます。

- 書き換えなしのマルチキャスト NAT を使用したファストパスとファストパス

ファスト パス モードでは、S1、G1 インターフェイスは S2、G2 インターフェイスに変換され、発信パケットの宛先 MAC アドレスには、G1 インターフェイスに対応するマルチキャスト MAC アドレスがあります（たとえば、事前に変換されたグループの MAC アドレス）。)。

（注） マルチキャスト サービス リフレクション機能は、リリース 7.0(3)I7(2) 以降の Cisco Nexus 3548-X プラットフォームでのみサポートされます。

SR 機能は、ループバック インターフェイスで構成されます。SR 機能の詳細については、次のセクションを参照してください。

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

Cisco Nexus 3548-X プラットフォーム スイッチで SR 機能を構成する前に、次の注意事項と制限事項をお読みください。

- SR 機能は、N3K-C3548-10GX プラットフォームでのみサポートされ、N3K-C3548-10GE プラットフォームではサポートされません。
- SR 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。
- show ip mroute 詳細統計情報は、SSM のファストパスまたはファストパス書き換えなしモードでは使用できません。ASM 統計が利用可能です。
- 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 サービス リフレクション機能は、CLI ハードウェア プロファイル **multicast service-reflect port x** によって定義されたハードウェア ループバック ポートを使用します。
- 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。
- マルチキャスト NAT 通常モード ソリューションの合計スループットは 5 Gbps です。

- 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。
- IP マルチキャストでは、問題の送信元への RPF パスがユニキャスト ルーティング テーブルで使用可能な場合、直接接続されていないソースのマルチキャスト（S、G）ルートを作成できます。ルートは、スタティックまたはダイナミック（ルーティング プロトコル経由）、またはマルチキャスト コマンド **ip mroute** *ip-sa/mask gateway* を介して行うことができます。

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 サービス リフレクトは、通常モードまたはファスト パス モードのソース非変換をサポートしていません。変換されたソースは、入力マルチキャスト ストリーム S1、G1 発信インターフェイス リスト（oiflist）として構成されたループバック ポートのサブネットに分類される必要があります。
- 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。
- 送信元グループ（S1、G1）のマルチキャスト転送は、変換ルータのサービス リフレクト マルチキャスト ルータではサポートされません。

マルチキャスト サービス リフレクション機能

次の順序でマルチキャスト サービス リフレクション機能を構成します。

1. 最初にマルチキャスト サービス リフレクト ループバック ポートを構成します。
2. マルチキャスト サービス リフレクト モードを構成します。
3. マルチキャスト サービス リフレクト ルールを構成します。

マルチキャスト サービス リフレクト ループバック ポートの構成

テーブル 9 にリストされている CLI コマンドを使用して、マルチキャスト サービス リフレクト ループバック ポートを構成します。

表 *15:* マルチキャスト サービス リフレクト ループバック ポートの構成

コマンド	説明
hardware profile multicast service-reflect port ?*<1-48> Loopback port-num*	<1-48> の範囲からマルチキャスト サービス リフレクト ループバック ポートを作成します。

（注） 選択されたループバック ポートは、他の目的には使用できなくなり、マルチキャスト サービス リフレクション機能専用になります。ループバック ポートを構成した後、リロードが必要です。

サービス リフレクト ポートは通常モードでのみ必要であり、ファスト パス モードでは必要ありません。

```
(config)# hardware profile multicast service-reflect port 12
```

マルチキャスト サービス リフレクト モードの構成

テーブル 10 にリストされている CLI コマンドを使用して、マルチキャスト サービス リフレクトモードを構成します。書き換えあり/書き換えなしのファストパスモードは、UDP宛先ポート D1 を別の宛先ポート D2 に変換します。

（注） マルチキャスト サービス リフレクト モードを構成した後、リロードが必要です。

表 *16 :* マルチキャスト サービス リフレクト モードの構成

コマンド	説明
ip service-reflect mode ? *regular* *fast-pass* *fast-pass no-rewrite*	マルチキャスト サービス リフレクト モードを構成します。 この機能は、次のフレーバーでサポートされています。通常モード、ファストパス モード、ファストパス書き換えなしモード。 通常モード：通常モードは、G1 インターフェイスを G2 インターフェイスに変換します。マルチキャスト プロトコルに従って、G2 インターフェイスの MAC アドレスを書き換えます。 ファストパス モードは、G1 インターフェイスを G2 インターフェイスに変換します。G2 インターフェイスの MAC アドレスは書き換えません。G2 インターフェイスの MAC アドレスは、マルチキャスト プロトコルに従って引き続き有効です。これは、/9 マスク長制限により、G2 インターフェイスの MAC アドレスを G1 インターフェイスの MAC アドレスと同じに保つためです。このモードでは、グループ変換のマスク長は9以下である必要があります。 書き換えなしオプションを使用したファストパス モードは、G1 インターフェイスを G2 インターフェイスに変換しますが、G2 インターフェイスの MAC アドレスは書き換えません。G2 インターフェイスの MAC アドレスは、マルチキャスト プロトコルに従って無効です。G2 インターフェイスの MAC アドレスがトポロジで考慮されていない場合は、十分な注意を払ってこのモード オプションを使用してください。グループ変換のマスク長に制限はありません。
ip service-reflect mode regular	通常モードを構成します。

マルチキャスト リフレクト ルールの構成

次に、テーブル 11 にリストされている CLI コマンドを使用して、マルチキャスト サービス リフレクト ルールを構成します。

（注） スイッチが UDP ポートに関係なく（S、G）トラフィックを受信し、異なる UDP ポートをキーとして使用する同じ S、G の複数のルールがある場合、すべての S、G UDP ルールの状態が作成され、ハードウェア リソースが割り当てられます。

表 *17:* マルチキャスト リフレクト ルールの構成

コマンド	説明
config # **ip service-reflect destination** *G1* **to** *G2* **mask-len** *M1* **source** *S1* **to** *S2* **mask-len** *M2* *G1*：*ABCD* 着信グループ アドレス（マルチキャスト） *G2*：*ABCD* 発信グループ アドレス（マルチキャスト） *M1*：*<0-32>* グループ マスク長 *デフォルト値は *32* *S1*：*ABCD* 着信送信元アドレス *S2*：*ABCD* 発信送信元アドレス *M2: <0-32>* 送信元マスク長 *デフォルト値は *32*	入力インターフェイス（S1、G1）を出力インターフェイス（S2、G2）に SR 変換するルールを指定します。
config # **ip service-reflect destination** *G1* **to** *G2* **mask-len** *M1***source** *S2* *G1*：*ABCD* 着信グループ アドレス（マルチキャスト） *G2*：*ABCD* 発信グループ アドレス（マルチキャスト） *M1*：*<0-32>* グループ マスク長 *S2*：*ABCD* 発信元アドレス	入力インターフェイス（*、G1）を（S2、G2）インターフェイスに SR 変換するルールを指定します。 （注） * は S1 を意味します。ABCD 着信送信元アドレス考慮されません。

デフォルト（32）サブネット マスクと非デフォルト（32 未満）サブネット マスクについては、次の例を参照してください。

例 1：

```
#ip service-reflect destination 225.0.0.2 to 226.0.0.2 mask-len 32 source 10.0.0.2 to
12.0.0.2 mask-len 32
```

例 1 の構成ルールは、次の（S1、G1）から（S2、G2）へのマッピング ルールをインストールします。

```
a. (10.0.0.2, 225.0.0.2) -> (12.0.0.2, 226.0.0.2)
```

例2：

```
#ip service-reflect destination 225.0.0.2 to 226.0.0.2 mask-len 31 source 10.0.0.2 to
12.0.0.2 mask-len 31
```

例 2 の構成ルールは、次の（S1、G1）から（S2、G2）へのマッピング ルールをインストールします。

```
a. (10.0.0.2, 225.0.0.0) -> (12.0.0.2, 226.0.0.2)
b. (10.0.0.2, 225.0.0.0) -> (12.0.0.2, 226.0.0.2)
a. (10.0.0.2, 225.0.0.0) -> (12.0.0.2, 226.0.0.2)
b. (10.0.0.2, 225.0.0.0) -> (12.0.0.2, 226.0.0.2)
```

例 3：

```
#ip service-reflect destination 225.0.0.2 to 226.0.0.2 mask-len 31 source 10.0.0.2 to
12.0.0.2 mask-len 32
```

例 3 の構成ルールは、次の（S1、G1）から（S2、G2）へのマッピング ルールをインストールします。

```
a. (10.0.0.2, 225.0.0.0) -> (12.0.0.2, 226.0.0.2)
b. (10.0.0.2, 225.0.0.3) -> (12.0.0.2, 226.0.0.3)
```

例 4：

```
ip service-reflect destination 225.0.0.2 to 226.0.0.2 mask-len 32 source 10.0.0.2 to
12.0.0.2 mask-len 32 udp-dest-port 3000
```

例 4 の構成ルールは、次の（S1、G1）から（S2、G2）へのマッピング ルールをインストールします。

```
a. (10.0.0.2, 225.0.0.2, 3000) -> (12.0.0.2, 226.0.0.2)
```

例 5：

```
ip service-reflect destination 225.0.0.2 to 226.0.0.2 mask-len 32 source 10.0.0.2 to
12.0.0.2 mask-len 32 udp-dest-port 3000 to 4000
```

例 5 の構成ルールは、次の（S1、G1）から（S2、G2）へのマッピング ルールをインストールします。

```
a. (10.0.0.2, 225.0.0.2, 3000) -> (12.0.0.2, 226.0.0.2, 4000)
```

通常モードの構成

次のテーブルに示す CLI 手順を使用して、ループバック ポート、通常の SR モード、および通常モードの SR ルールを構成します。

ステップ	コマンド	説明
ステップ 1	**# feature pim**	G1 および G2 インターフェイスの PIM 機能を構成します。
ステップ 2	**# ip pim rp-address 10.0.0.2 group-list 225.0.0.2/32 //S1,G1**	
ステップ 3	**#ip pim rp-address 11.0.0.2 group-list 226.0.0.2/32 //S2,G2**	
ステップ 4	(config) # **hardware profile multicast service-reflect port 12**	ポート 12 などの SR ループバック ポートを選択し、ループバックを構成します。
ステップ 5	(config) # **ip service-reflect mode regular**	マルチキャスト サービス リフレクト モードを構成します。
ステップ 6	**# ip service-reflect destination 225.0.0.2 to 226.0.0.2 mask-len 32 source 10.0.0.2 to 12.0.0.2 mask-len 32 // G1 to G2, S1 to S2**	SR ルールを構成します。

ステップ	コマンド	説明
ステップ 7	**# interface Ethernet1/10** **# no switchport** **# ip address 10.0.0.1/24** **# ip pim sparse-mode** **# no shutdown** **#interface Ethernet1/11** **# no switchport** **# ip address 11.0.0.1/24** **# ip pim sparse-mode** **# no shutdown**	入力インターフェイス（例：1/10）または出力インターフェイス（例：SR ボックスで 1/11）を構成します。
ステップ 8	**# interface loopback0** **# ip address 12.0.0.1/8** **# ip pim sparse-mode** **# ip igmp static-oif 225.0.0.2** **# interface loopback1** **# ip address 17.0.0.1/8** **# ip pim sparse-mode** **# ip igmp static-oif 227.0.0.2**	SR ボックスのループバック ポートを構成します。 これは S2 サブネットに属します（翻訳された S1）。 これは、G1 のスタティック OIF です。 これは S2 サブネットに属します（翻訳された S1）。 これは、G1 のスタティック OIF です。 複数のマルチキャスト NAT ルールの場合、S2 の一意のサブネットごとにループバック構成を追加します。
ステップ 9	(config) # **test ethpm l3 enable-show-iport**	通常モードで test ethpm l3 enable-show-iport コマンドを使用して、外部ループバック ポートにアクセスします。
ステップ 10	(config) # **copy r s** (config) # **reload**	実行コンフィギュレーションスタートアップ コンフィギュレーションに保存してリロードします。 ステップ（4）および（5）で説明されている構成は、通常モード機能のために存在する必要があり、リロードが必要です。

ファストパス モードを構成します。

表 12 に概説されている CLI 手順を使用して、ループバック ポート、ファスト パス SR モード、およびファスト パスまたはファスト パスの書き換え無しの SR ルールを構成します。

（注） ファスト パス モードでは、ハードウェア ループバック ポートの構成は必要ありません。

表 *18 :* ファストパス モードを構成します。

ステップ	コマンド	説明
ステップ 1	**# feature pim**	G1 および G2 インターフェイスの PIM 機能を構成します。
ステップ 2	**# ip pim rp-address 10.0.0.2 group-list 225.0.0.2/32 //RP for G1, G1**	
ステップ 3	**# ip pim rp-address 11.0.0.2 group-list 226.0.0.2/32 //S2,G2**	
ステップ 4	(config) # **ip service-reflect mode fast-pass** または (config) # **ip service-reflect mode fast-pass no-rewrite**	マルチキャスト サービス リフレクションのファスト パス モードまたはファスト パス モードの書き換えなしモードを構成します。
ステップ 5	**# ip service-reflect destination 225.0.0.2 to 226.0.0.2 mask-len 9 source 10.0.0.2 to 12.0.0.2 mask-len 32 // G1 to G2, S1 to S2**	SR ルールを構成します。
ステップ 6	**# interface Ethernet 1/10** **# no switchport** **# ip address 10.0.0.1/20** **# ip pim sparse-mode** **# no shutdown** **# interface Ethernet 1/11** **# no switchport** **# ip address 11.0.0.1/20** **# ip pim sparse-mode** **# no shutdown**	入力インターフェイス（例：1/10）または出力インターフェイス（例：SR ボックスで 1/11）を構成します。

ステップ	コマンド	説明
ステップ 7	**# interface loopback0** **# ip address 12.0.0.1/8** **# ip pim sparse-mode** **# ip igmp static-oif 225.0.0.2** **# interface loopback1** **# ip address 17.0.0.1/8** **# ip pim sparse-mode** **# ip igmp static-oif 227.0.0.2**	SR ボックスのループバック ポートを構成します。 複数のマルチキャスト NAT ルールに関して、S2 固有サブネットごとにループバック構成を追加します。
ステップ 8	(config) # **copy r s** (config) # **reload**	実行コンフィギュレーションスタートアップ コンフィギュレーションに保存してリロードします。 手順（4）で説明されている構成は、ファスト パス モード機能のために存在する必要があり、リロードが必要です。

通常モードの show コマンドの表示

マルチキャスト サービス リフレクション機能の show コマンドを表示するには、次のセクションを参照してください。

- ストリームのレート確認
- マルチキャスト ルートの確認
- マルチキャスト ルートの表示

ストリームのレート確認

インターフェイス設定に関する情報を表示するには、show interface ethernet コマンドを使用します。

（注） **show ip mroute detail** のマルチキャスト グループ統計情報は、SSM を使用したファストパス モードおよびファストパス書き換えなしモードでは使用できません。統計は、ASMマルチキャストで使用できます。

show int eth < *slot/port* > | i rate コマンドを使用して、次の例に示すようにストリームのレートを確認します：

show int eth 1/10 | i rate

```
30 seconds input rate 1536904 bits/sec, 3000 packets/sec \\ 1X of (S1,G1) UDP stream
0 seconds output rate 208 bits/sec, 0 packets/sec
input rate 1.54 Mbps, 3.00 Kpps; output rate 152 bps, 0 pps
```

show int eth 1/12 | i rate

```
30 seconds input rate 3072112 bits/sec, 5999 packets/sec \\ 2X Stream
30 seconds output rate 2811704 bits/sec, 5999 packets/sec \\ 2X Stream
input rate 3.07 Mbps, 6.00 Kpps; output rate 3.05 Mbps, 6.00 Kpps
```

上記のコマンドは、ループバック ポート経由でコマンドを実行するために必要です。

```
# test ethpm l3 enable-show-iport // To show the loopback port
```

show int eth 1/11 | i rate

```
30 seconds input rate 160 bits/sec, 0 packets/sec
30 seconds output rate 1683024 bits/sec, 2999 packets/sec \\ 1X of (S2,G2) UDP stream
input rate 136 bps, 0 pps; output rate 1.52 Mbps, 3.00 Kpps
```

マルチキャスト ルートの確認

次の例で説明するように、show ip mroute および show ip mroute sr コマンドを使用してマルチキャスト ルートを確認し、サービス リフレクト ルートのみを表示します：

show ip mroute sr

```
IP Multicast Routing Table for VRF "default"

(*, 225.0.0.2/32), uptime: 00:27:44, static pim ip // (*,G1) route
Incoming interface: Ethernet1/10, RPF nbr: 10.0.0.2, uptime: 00:27:33
Outgoing interface list: (count: 1)
loopback0, uptime: 00:27:44, static

(10.0.0.2/32, 225.0.0.2/32), uptime: 00:24:01, ip mrib pim // (S1,G1) route
Incoming interface: Ethernet1/10, RPF nbr: 10.0.0.2, uptime: 00:24:01
Outgoing interface list: (count: 1)
loopback0, uptime: 00:24:01, mrib

(10.1.1.11/32, 230.1.1.2/32), uptime: 00:15:57, pim mrib ip
Translated Route Info: (169.1.1.11, 225.1.1.2)
Incoming interface: Ethernet1/47, RPF nbr: 10.1.1.11, uptime: 00:15:57, internal
Outgoing interface list: (count: 1)
loopback0, uptime: 00:15:57, mrib

(12.0.0.2/32, 226.0.0.2/32), uptime: 00:24:01, ip pim // (S2,G2) route
Incoming interface: loopback0, RPF nbr: 12.0.0.2, uptime: 00:24:01
Outgoing interface list: (count: 1)
Ethernet1/11, uptime: 00:12:59, pim
```

マルチキャスト ルートの表示

次の例に示すように、**show forwarding multicast** route コマンドを使用して、転送マルチキャスト ルートの詳細を表示します。

show forwarding multicast route

```
IPv4 Multicast Routing table table-id:0x1
Total number of groups: 2


(*, 225.0.0.2/32), RPF Interface: Ethernet1/10, flags: G
Received Packets: 1 Bytes: 64
```

```
Number of Outgoing Interfaces: 1
Outgoing Interface List Index: 1
loopback0 Outgoing Packets:0 Bytes:0

(10.0.0.2/32, 225.0.0.2/32), RPF Interface: Ethernet1/10, flags: c
Received Packets: 507775 Bytes: 32497600
Number of Outgoing Interfaces: 1
Outgoing Interface List Index: 6000
Ethernet1/12 Outgoing Packets:0 Bytes:0

(12.0.0.2/32, 226.0.0.2/32), RPF Interface: loopback0, flags:
Received Packets: 0 Bytes: 0
Number of Outgoing Interfaces: 1
Outgoing Interface List Index: 3
Ethernet1/11 Outgoing Packets:0 Bytes:0
```

ファストパス モードの Show コマンドの表示

マルチキャスト サービス リフレクション機能のファストパス モードの show コマンドを表示するには、次のセクションを参照してください。

- ストリームのレート確認
- マルチキャスト ルートの確認
- マルチキャスト ルートの表示

ストリームのレート確認

fast-pass モードのインターフェイス構成に関する詳細を表示するには、show interface ethernet コマンドを使用します。show int eth <slot/port> | i rate コマンドを使用して、次の例に示すようにストリームのレートを確認します：

show int eth 1/10 | i rate

```
30 seconds input rate 512632 bits/sec, 1000 packets/sec \\1X Stream of (S1,G1) Stream
30 seconds output rate 208 bits/sec, 0 packets/sec
input rate 95.38 Kbps, 168 pps; output rate 136 bps, 0 pps
```

show int eth 1/11 | i rate

```
30 seconds input rate 72 bits/sec, 0 packets/sec
30 seconds output rate 495584 bits/sec, 999 packets/sec \\ 1X stream of (S2,G2) stream
input rate 144 bps, 0 pps; output rate 110.10 Kbps, 205 pps
```

マルチキャスト ルートの確認

show ip mroute および show ip mroute sr コマンドを使用してマルチキャスト ルートを確認し、次の例で説明するように、ファスト パス モードのサービス リフレクト ルートを表示します。

show ip mroute

show ip mroute sr（サービス リフレクト ルートのみ表示）

```
IP Multicast Routing Table for VRF "default"

(*, 225.0.0.2/32), uptime: 00:29:17, pim ip static
Incoming interface: Ethernet1/10, RPF nbr: 10.0.0.2, uptime: 00:28:51 Outgoing interface
```

```
 list: (count: 1)
loopback0, uptime: 00:16:15, static

(10.0.0.2/32, 225.0.0.2/32), uptime: 00:25:05, ip mrib pim
Incoming interface: Ethernet1/10, RPF nbr: 10.0.0.2, uptime: 00:25:05 Outgoing interface
 list: (count: 1)
loopback0, uptime: 00:16:15, mrib

(12.0.0.2/32, 226.0.0.2/32), uptime: 00:14:58, ip pim
Incoming interface: loopback0, RPF nbr: 12.0.0.2, uptime: 00:14:58 Outgoing interface
list: (count: 1)
Ethernet1/11, uptime: 00:14:58, pim
```

マルチキャスト ルートの表示

次の例に示すように、転送マルチキャスト ルートの詳細を表示するには、show forwarding multicast route コマンドを使用します。

show forwarding multicast route

```
IPv4 Multicast Routing table table-id:0x1
Total number of groups: 2

(*, 225.0.0.2/32), RPF Interface: Ethernet1/10, flags: G Received Packets: 10 Bytes: 640
Number of Outgoing Interfaces: 1
Outgoing Interface List Index: 2
loopback0 Outgoing Packets:0 Bytes:0

(10.0.0.2/32, 225.0.0.2/32), RPF Interface: Ethernet1/10, flags: c Received Packets:
1010555 Bytes: 64675520
Number of Outgoing Interfaces: 1
Outgoing Interface List Index: 3
Ethernet1/11 Outgoing Packets:0 Bytes:0

(12.0.0.2/32, 226.0.0.2/32), RPF Interface: loopback0, flags: Received Packets: 0 Bytes:
 0
Number of Outgoing Interfaces: 1
Outgoing Interface List Index: 3
Ethernet1/11 Outgoing Packets:0 Bytes:0
```

次の作業

PIM の関連機能を構成するには、次の章を参照してください：

その他の参考資料

PIM の実装に関する詳細情報については、次の項目を参照してください。

- 関連資料
- 標準
- MIB
- 付録 A、IP マルチキャスト向け IETF RFC

関連資料

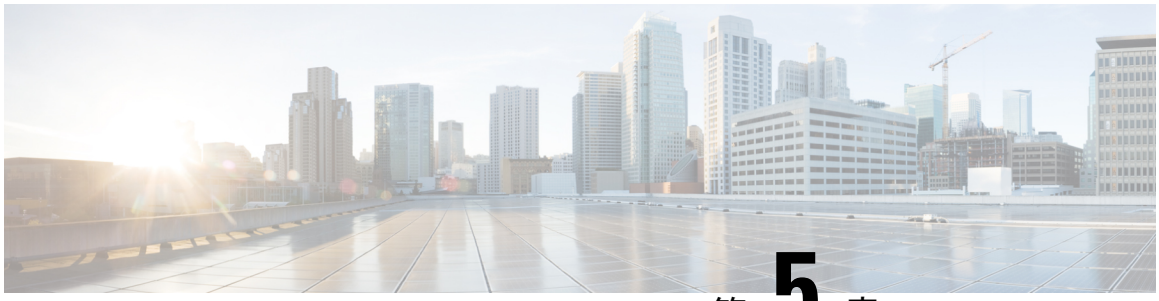
関連項目	マニュアル タイトル
CLI コマンド	Cisco Nexus 3000 シリーズ マルチキャスト ルーティング コマンド リファレンス
VRF の設定	Cisco Nexus 3548 スイッチ NX-OS ユニキャスト ルーティング構成ガイド

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

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



第 5 章

IGMP スヌーピングの構成

この章では、Cisco NX-OS デバイスにインターネット グループ管理プロトコル（IGMP）スヌーピングを構成する方法を説明します。

この章は、次の項で構成されています。

IGMP スヌーピングの情報

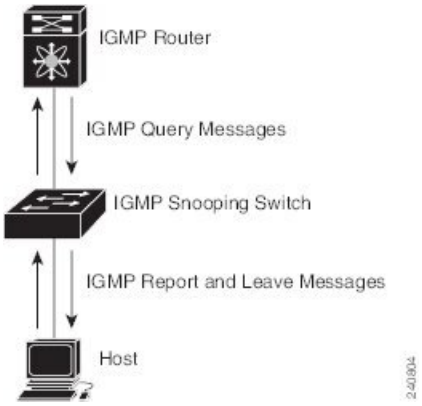
（注） スイッチでは、IGMP スヌーピングをディセーブルにしないことを推奨します。IGMP スヌーピングをディセーブルにすると、スイッチで不正なフラッディングが過度に発生し、マルチキャストのパフォーマンスが低下する場合があります。

インターネット グループ管理プロトコル（IGMP）スヌーピング ソフトウェアは、VLAN 内のレイヤ 2 IP マルチキャスト トラフィックを調査し、関係する受信機が常駐するポートを発見します。IGMP スヌーピングではポート情報を利用することにより、マルチアクセス LAN 環境における帯域幅消費量を削減し、VLAN 全体へのフラッディングを回避します。IGMP スヌーピング機能は、マルチキャスト対応ルータに接続されたポートを追跡して、ルータによる

IGMP メンバーシップ レポートの転送機能を強化します。トポロジの変更通知には、IGMP スヌーピング ソフトウェアが応答します。デフォルトでは、IGMP スヌーピングがスイッチでイネーブルにされています。

次の図では、ホストと IGMP ルータ間にある IGMP スヌーピング スイッチを示します。IGMP スヌーピング スイッチは、IGMP メンバーシップ レポートおよび Leave メッセージをスヌーピングして、必要な場合にだけ接続された IGMP ルータに転送します。

図 *13 : IGMP* スヌーピング スイッチ



IGMP スヌーピング ソフトウェアは、IGMPv1、IGMPv2、および IGMPv3 コントロール プレーン パケットの処理に関与し、レイヤ 3 コントロール プレーン パケットを代行受信して、レイヤ 2 の転送処理を操作します。

IGMP の詳細については、「IGMP の設定 （17 ページ）」を参照してください。

Cisco NX-OS IGMP スヌーピング ソフトウェアには、次のような独自の機能があります。

- 送信元フィルタリングにより、宛先および送信元の IP アドレスに基づいて、マルチキャスト パケットを転送できます。
- MAC アドレスでなく、IP アドレスに基づいてマルチキャスト転送を実行します。
- Optimized Multicast Flooding（OMF）により、未知のトラフィックをルータだけに転送して、データに基づくステート作成を行いません。

IGMP スヌーピングの詳細については、「RFC 4541」を参照してください。

このセクションは、次のトピックで構成されています。

IGMPv1 および IGMPv2

IGMPv1 および IGMPv2 は、メンバーシップ レポートの抑制機能をサポートしています。つまり、同じサブネットに属する 2 つのホストが、同じグループのマルチキャスト データを要求している場合、一方のホストからメンバー レポートを受信した他方のホストで、レポートの送信が抑制されます。メンバーシップ レポート抑制は、同じポートを共有しているホスト間で発生します。

各 VLAN スイッチ ポートに接続されているホストが 1 つしかない場合は、IGMPv2 の高速脱退機能を設定できます。高速脱退機能を使用すると、最終メンバーのクエリー メッセージがホストに送信されません。ソフトウェアは IGMP Leave メッセージを受信すると、ただちに該当するポートへのマルチキャスト データ転送を停止します。

IGMPv1 では、明示的な IGMP Leave メッセージが存在しないため、特定のグループについてマルチキャストデータを要求するホストが存続しないことを示すために、メンバーシップ メッセージ タイムアウトが利用されます。

（注） 高速脱退機能がイネーブルになっている場合、他のホストの存在は確認されないため、最終メンバーのクエリー インターバル設定が無視されます。

IGMPv3

Cisco NX-OS にはフル機能の IGMPv3 スヌーピングが実装されており、IGMPv3 レポートに含まれる（S、G）情報に基づいて、フラッディングを制御することができます。この発信元をベースとするフィルタリングにより、マルチキャスト グループにトラフィックを送信する発信元に基づくポートのセットにマルチキャスト トラフィックを制限するようにスイッチがイネーブルにされます。

ソフトウェアのデフォルト設定では、各 VLAN ポートに接続されたホストが追跡されます。この明示的なトラッキング機能は、高速脱退メカニズムをサポートしています。すべての IGMPv3 ホストがメンバーシップ レポートを送信するため、レポート抑制は、スイッチにより他のマルチキャスト対応ルータに送信されるトラフィックの量を制限します。レポート抑制をイネーブルにすると、過去にいずれの IGMPv1 ホストまたは IGMPv2 ホストからも対象のグループへの要求がなかった場合には、プロキシ レポートが作成されます。プロキシ機能により、ダウンストリーム ホストが送信するメンバーシップ レポートからグループ ステートが構築され、アップストリーム クエリアからのクエリーに応答するためにメンバーシップ レポートが生成されます。

IGMPv3 メンバーシップ レポートには LAN セグメント上のグループ メンバの一覧が含まれていますが、最終ホストが脱退すると、メンバーシップ クエリーが送信されます。最終メンバーのクエリーインターバルについてパラメータを設定すると、タイムアウトまでにどのホストからも応答がなかった場合に、グループ ステートが解除されます。

IGMPスヌーピングクエリア

マルチキャスト トラフィックをルーティングする必要がないために、Protocol-Independent Multicast（PIM）がインターフェイス上でディセーブルになっている場合は、メンバーシップ クエリーを送信するように IGMP スヌーピング クエリアを設定する必要があります。このクエリアは、マルチキャスト送信元と受信者を含み、その他のアクティブ クエリアを含まない VLAN で定義します。

IGMP スヌーピング クエリアがイネーブルな場合は、定期的に IGMP クエリーが送信されるため、IP マルチキャスト トラフィックを要求するホストから IGMP レポート メッセージが発信

されます。IGMP スヌーピングはこれらの IGMP レポートを待ち受けて、適切な転送を確立します。

現在は、スイッチ クエリアと IGMP スヌーピング クエリアに対して同じ SVI IP アドレスを設定できます。そうすれば、両方のクエリアが同時にアクティブになって、一般的なクエリーを定期的に VLAN に送信するようになります。これを回避するには、IGMP スヌーピング クエリアとスイッチ クエリアで別々の IP アドレスを使用します。

IGMP スヌーピング フィルタ

Cisco NX-OS リリース 6.0(2)A4(1) は、スヌーピング レイヤでの IGMP パケットのフィルタリングをサポートします。インターフェイス レベルで IGMP スヌーピング レポートを除外できます。このフィルタリングは、プレフィックス リストまたはルート マップ ポリシーに基づいています。ルータは、定義されたプレフィックスリストまたはルートマップポリシーとグループを比較し、指定されたアクションを実行します。したがって、指定したプレフィックスリストまたはルートマップに一致するグループのみが、IGMPスヌーピング レポートにフィルタリングされます。

IGMP スヌーピングに関する注意事項と制限事項

IGMP スヌーピングに関する注意事項および制約事項は次のとおりです。

- PVLAN の IGMP スヌーピングはサポートされていません。
- VLAN 上の IGMPv3 ホストが離脱すると、他のホストでトラフィックがドロップする可能性があります。これは主に、すでに離脱したポートから 2 回連続して離脱を受信した場合に見られ、これが VLAN 上の他のレシーバに影響を与えます。

  この損失を回避するには、**no ip igmp snooping explicit-tracking** コマンドを使用して VLAN 構成で明示的なホスト トラッキングを無効にする必要があります。

  例：

  ```
  configure terminal
  vlan configuration 10
  no ip igmp snooping explicit-tracking
  ```

- ホップバイホップ トポロジでは、IGMP スヌーピング クエリアではない中間ボックス（2 番目のデバイス）で SVI を構成すると、別のダウンストリーム L2 スイッチ（3 番目のデバイス）の背後にある他のレシーバ ポートの 1 つが離脱を送信すると、その背後にあるホストへのトラフィック損失を引き起こします。これは、v3 抑制が無効になっているためであり、IGMPv3 Leave が 2 番目のデバイスで消費されます。この問題の回避策は次のとおりです。
  - PIM DR と IGMP クエリアは、ホップバイホップ トポロジの同じボックスに同じ場所に配置する必要があります。最初のデバイスの SVI は、DR を 2 番目のデバイスから最初のデバイスにシフトするように **ip pim dr-priority 10** を使用して構成する必要があり、デフォルトの抑制は 2 番目のデバイス、3 番目のデバイスなどで無効にする必要があります。

- IGMPV3 抑制は、2 番目のデバイスや 3 番目のデバイスなどのすべてのホップで、影響を受ける VLAN の VLAN 構成で有効にする必要があります。

例：

```
configure terminal
vlan configuration 203
ip igmp snooping v3-report-suppression
```

IGMP スヌーピングの前提条件

IGMP スヌーピングには、次の前提条件が適用されます。

- スイッチ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。

IGMP スヌーピングのデフォルト設定

次のテーブルでは、IGMP スヌーピング パラメータのデフォルト設定をリスト化しています。

表 *19*：デフォルト *IGMP* スヌーピング パラメータ

パラメータ	デフォルト
IGMP スヌーピング	有効
明示的な追跡	有効
高速脱退	無効
最終メンバー クエリ間隔	1 秒
スヌーピング クエリア	無効
レポート抑制	有効
リンクローカル グループ抑制	有効
スイッチ全体での IGMPv3 レポート抑制	無効
VLAN ごとの IGMPv3 レポート抑制	有効（Enabled）

（注）

- マルチキャスト ルータ ポートを送信元ポートとして SPAN セッションが設定されている場合、送信元ポートに実際に転送されているトラフィックがない場合でも、宛先ポートはすべてのマルチキャスト トラフィックを認識します。これは、マルチキャスト/SPAN 実装の現在の制限によるものです。
- Cisco Nexus 3548 シリーズ スイッチは、未知のマルチキャスト トラフィックをすべての VLAN のマルチキャスト ルータ ポートに複製しますが、マルチキャスト トラフィックは 1 つの特定の VLAN で受信されます。これはデフォルトの動作であり、構成できません。

IGMP スヌーピングの構成

表 *20 : IGMP* スヌーピング パラメータ

パラメータ	説明
IGMP スヌーピング	IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。 （注） グローバルな設定が無効になっている場合は、すべての VLAN が有効化されてるかどうか関係なく無効化されていると見なされます。
イベント履歴	IGMP スヌーピング履歴バッファのサイズを設定します。デフォルトは small です。
グループ タイムアウト	デバイス上のすべての VLAN のグループ メンバーシップ タイムアウトを構成します。
リンクローカル グループ抑制	デバイスのリンクローカル グループ抑制を構成します。デフォルトではイネーブルになっています。
Optimise-multicast-flood	デバイス上のすべての VLAN で Optimized Multicast Flood（OMF）を構成します。デフォルトではイネーブルになっています。
プロキシ	デバイスの IGMP スヌーピング プロキシを設定します。デフォルトは 5 秒です。

パラメータ	説明
レポート抑制	デバイスのマルチキャスト対応ルータに送信されるメンバーシップ レポート トラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。
IGMPv3 レポート抑制	デバイスの IGMPv3 レポート抑制およびプロキシ レポートを構成します。デフォルトではディセーブルになっています。

手順の概要

1. **configure terminal**
2.
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
ステップ 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
ステップ 2	オプション / 説明 コマンド / 目的 **ip igmp snooping** 例： `switch(config-vlan-config)# ip igmp snooping` 現在の VLAN に対して IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。 （注） このコマンドの no 形式により、グローバル設定がディセーブルに	

	コマンドまたはアクション		目的
	オプション	説明	
		なっている場合は、個々の VLAN で IGMP スヌーピングがイネーブルであるかどうかに関係なく、すべての VLAN で IGMP スヌーピングがディセーブルになります。 IGMP スヌーピングを無効にすると、レイヤ 2 マルチキャストフレームがすべてのモジュールにフラッディングします。	
	ip igmp snooping event-history 例： `switch(config)# ip igmp snooping event-history`	イベント履歴バッファのサイズを設定します。デフォルトは small です。	
	ip igmp snooping syslog-threshold percentage 例： `switch(config)# ip igmp snooping syslog-threshold 80`	IGMP スヌーピングテーブルの syslog しきい値を構成します。	
	ip igmp snooping link-local-groups-suppression 例： `switch(config)# ip igmp snooping link-local-groups-suppression`	デバイス全体のリンクローカル グループ抑制を構成します。デフォルトではイネーブルになっています。	
	ip igmp snooping optimise-multicast-flood 例： `switch(config)# ip igmp snooping optimise-multicast-flood`	デバイス上のすべての VLAN で OMF を最適化します。デフォルトではイネーブルになっています。	

	コマンドまたはアクション		目的
	オプション	説明	
	ip igmp snooping v3-report-suppression 例： `switch(config)# ip igmp snooping v3-report-suppression`	IGMPv3 レポート抑制およびプロキシレポートを設定します。デフォルトでは、スイッチ全体のグローバル コマンドでディセーブルになっており、VLAN ごとにイネーブルになっています。	
	ip igmp snooping report-suppression 例： `switch(config)# ip igmp snooping report-suppression`	マルチキャスト対応ルータに送信されるメンバシップ レポート トラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。	
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`		設定変更を保存します。

IGMP スヌーピング パラメータの設定

IGMP スヌーピング プロセスの動作に影響を与えるには、次の表に示すオプションの IGMP スヌーピング パラメータを構成します。

表 *21 : IGMP* スヌーピング パラメータ

パラメータ	説明
IGMP スヌーピング	VLAN ごとに IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。 グローバルな設定が無効になっている場合は、すべての VLAN が有効化されてるかどうか関係なく無効化されていると見なされます。
アクセス グループ	スヌーピング レイヤで IGMP パケットをフィルタ処理します。デフォルトではディセーブルになっています。
明示的な追跡	各ポートに接続されたそれぞれのホストから送信される IGMPv3 メンバーシップ レポートを、VLAN 別に追跡します。デフォルトではイネーブルになっています。
高速脱退	ソフトウェアが IGMP Leave レポートを受信した場合に、IGMP クエリー メッセージを送信することなく、グループ ステートを解除できるようにします。このパラメータは、IGMPv2 ホストに関して、各 VLAN ポート上のホストが 1 つしか存在しない場合に使用されます。デフォルトではディセーブルになっています。
最終メンバー クエリ間隔	IGMP クエリーの送信後に待機する時間を設定します。この時間が経過すると、ソフトウェアは、特定のマルチキャスト グループについてネットワーク セグメント上に受信要求を行うホストが存在しないと見なします。いずれのホストからも応答がないまま、最終メンバのクエリ インターバルの期限が切れると、対応する VLAN ポートからグループが削除されます。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。
Optimise-multicast-flood	指定した VLAN で Optimized Multicast Flood（OMF）を構成します。デフォルトではイネーブルになっています。
レポート ポリシー	スヌーピング レイヤで IGMP パケットをフィルタ処理します。デフォルトではディセーブルになっています。

パラメータ	説明
スヌーピング クエリア	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、インターフェイスにスヌーピング クエリアを設定します。 スヌーピング クエリアに次の値を構成することもできます。 • タイムアウト：IGMPv2 のタイムアウト値 • 間隔：クエリ送信間の時間 • 最大応答時間：クエリ メッセージの MRT • スタートアップ カウント：起動時に送信されるクエリ数 • スタートアップ間隔：起動時のクエリ間隔
堅牢性変数	指定した VLAN のロバストネス値を設定します。
マルチキャスト ルータ	マルチキャスト ルータへのスタティック接続を設定します。ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。
スタティック グループ	VLAN のレイヤ 2 ポートをマルチキャスト グループのスタティック メンバーとして設定します。
リンクローカル グループ抑制	スイッチまたは各VLANに対して、リンクローカル グループ抑制を設定します。デフォルトではイネーブルになっています。
バージョン	指定した VLAN の IGMP バージョン番号を設定します。

（注） このコンフィギュレーション モードを使用して目的の IGMP スヌーピング パラメータを設定します。ただし、この設定は指定した VLAN を明示的に作成した後にのみ適用されます。

手順の概要

1. **configure terminal**

2. **ip igmp snooping**
3. **vlan configuration** *vlan-id*
4.
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
ステップ 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
ステップ 2	**ip igmp snooping** 例： `switch(config)# ip igmp snooping`	デバイスの IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。 （注） このコマンドの no 形式により、グローバル設定がディセーブルになっている場合は、個々の VLAN で IGMP スヌーピングがイネーブルであるかどうかに関係なく、すべての VLAN で IGMP スヌーピングがディセーブルになります。 IGMP スヌーピングをディセーブルにすると、レイヤ 2 マルチキャスト フレームがすべてのモジュールにフラッディングします。
ステップ 3	**vlan configuration** *vlan-id* 例： `switch(config)# vlan configuration 100` `switch(config-vlan-config)#`	VLAN を構成し、VLAN コンフィギュレーション モードを開始します。
ステップ 4	オプション / 説明 コマンド / 目的 **ip igmp snooping** 例： `switch(config-vlan-config)# ip igmp snooping` / 現在の VLAN に対して IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。	

	コマンドまたはアクション		目的
	オプション	説明	
	ip igmp snooping access-group {prefix-list | route-map} policy-name interface *interface slot/port* 例： `switch(config-vlan-config)# ip igmp snooping access-group prefix-list plist interface ethernet 2/2`	プレフィックス リストまたはルート マップ ポリシーに基づいて、IGMP スヌーピング アクセス グループにフィルタを構成します。	
	ip igmp snooping explicit-tracking 例： `switch(config-vlan-config)# ip igmp snooping explicit-tracking`	各ポートに接続されたそれぞれのホストから送信される IGMPv3 メンバーシップ レポートを、VLAN 別に追跡します。デフォルトは、すべての VLAN でイネーブルです。	
	ip igmp snooping fast-leave 例： `switch(config-vlan-config)# ip igmp snooping fast-leave`	IGMPv2 プロトコルのホスト レポート抑制メカニズムのために、明示的に追跡できない IGMPv2 ホストをサポートします。高速脱退がイネーブルの場合、IGMP ソフトウェアは、各 VLAN ポートに接続されたホストが 1 つだけであると見なします。デフォルトは、すべての VLAN でディセーブルです。	
	ip igmp snooping last-member-query-interval *seconds* 例：	いずれのホストからも IGMP クエリー メッセージへの応答がないまま、最終メンバの	

	コマンドまたはアクション		目的
	オプション	説明	
	`switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3`	クエリー インターバルの期限が切れた場合に、関連する VLAN ポートからグループを削除します。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。	
	ip igmp snooping link-local-groups-suppression 例： `switch(config-vlan-config)# ip igmp snooping link-local-groups-suppression`	リンクローカル グループ抑制を設定します。デフォルトではイネーブルになっています。 （注） グローバル コンフィギュレーション モードでこのコマンドを実行し、すべてのインターフェイスを変更することもできます。	
	ip igmp snooping mrouter interface *interface* 例： `switch(config-vlan-config)# ip igmp snooping mrouter interface ethernet 2/1`	マルチキャスト ルータへのスタティック接続を設定します。ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。「ethernet スロット番号/ポート番号」などのように、タイプと番号でインターフェイスを指定できます。	

	コマンドまたはアクション		目的
	オプション	説明	
	ip igmp snooping optimise-multicast-flood 例： `switch(config-vlan-config)# ip igmp snooping optimise-multicast-flood`	選択された VLAN の OMF を最適化します。デフォルトではイネーブルになっています。	
	ip igmp snooping querier *ip-address* 例： `switch(config-vlan-config)# ip igmp snooping querier 172.20.52.106`	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、スヌーピング クエリアを設定します。IP アドレスは、メッセージの送信元として使用します。	
	ip igmp snooping querier-timeout *seconds* 例： `switch(config-vlan-config)# ip igmp snooping querier-timeout 300`	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合の、IGMPv2 のスヌーピング クエリア タイムアウト値を設定します。デフォルト値は 255 秒です。	
	ip igmp snooping query-interval *seconds* 例： `switch(config-vlan-config)# ip igmp snooping query-interval 120`	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、スヌーピング クエリー インターバルを設定します。デ	

	コマンドまたはアクション		目的
	オプション	説明	
		フォルト値は 125 秒です。	
	ip igmp snooping report-policy { **prefix-list** | **route-map** } **policy-name interface** *interface slot/port* 例： `switch(config-vlan-config)# ip igmp snooping report-policy route-map rmap interface ethernet 2/4`	プレフィックス リストまたはルート マップ ポリシーに基づいて、IGMP スヌーピング レポートにフィルタを構成します。	
	ip igmp snooping startup-query-count value 例： `switch(config-vlan-config)# ip igmp snooping startup-query-count 5`	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、起動時に送信されるクエリー数に対してスヌーピングを設定します。	
	ip igmp snooping startup-query-interval *seconds* 例： `switch(config-vlan-config)# ip igmp snooping startup-query-interval 15000`	マルチキャスト トラフィックをルーティングする必要がないため、PIM を有効にしていない場合に、起動時のスヌーピング クエリ間隔を構成します	
	ip igmp snooping robustness-variable value 例： `switch(config-vlan-config)# ip igmp snooping robustness-variable 5`	指定した VLAN のロバストネス値を設定します。デフォルト値は 2 です。	
	ip igmp snooping static-group *group-ip-addr* [**source source -ip-addr**] **interface** *interface*	VLAN のレイヤ 2 ポートをマルチキャスト グループのスタティック メ	

	コマンドまたはアクション		目的
	オプション	説明	
	例： `switch(config-vlan-config)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1`	ンバーとして設定します。**ethernet** *slot/port* などタイプと数でインターフェイスを指定できます。	
	ip igmp snooping version value 例： `switch(config-vlan-config)# ip igmp snooping version 2`	指定した VLAN の IGMP バージョン番号を設定します。	
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`		設定変更を保存します。

IGMP スヌーピング設定の確認

IGMP スヌーピングの設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show ip igmp snooping [**vlan** *vlan-id*]	IGMP スヌーピング設定を VLAN 別に表示します。
show ip igmp snooping groups [*source* [*group*] | *group* [*source*]] [**vlan** *vlan-id*] [**detail**]	グループに関する IGMP スヌーピング情報を VLAN 別に表示します。
show ip igmp snooping look-up mode [**vlan** *vlan-id*]	VLAN ごとに IGMP スヌーピング ルックアップ モード情報を表示します。
show ip igmp snooping mac-oif [**detail** | **vlan** *vlan-id*]	IGMP スヌーピングのスタティック mac oif 情報を VLAN ごとおよびすべての詳細ごとに表示します
show ip igmp snooping mroute [**vlan** *vlan-id*]	マルチキャスト ルータ ポートを VLAN 別に表示します。
show ip igmp snooping otv groups [*source* [*group*] | *group* [*source*]] [**vlan** *vlan-id*]	VLAN ごとに IGMP スヌーピング OTV 情報を表示します。

コマンド	目的
show ip igmp snooping querier [**vlan** *vlan-id*]	IGMP スヌーピング クエリアを VLAN 別に表示します。
show ip igmp snooping [**vlan** *vlan-id*]	IGMP スヌーピング設定を VLAN 別に表示します。

これらのコマンドからの出力のフィールドに関する詳細は、『Cisco Nexus 3000 シリーズ マルチキャスト ルーティング コマンド リファレンス』を参照してください。

IGMP スヌーピング統計情報の表示

コマンド	目的
show ip igmp snooping statistics [**global** | **vlan** *vlan-id*]	グローバルまたは VLAN ごとのパケットとエラー カウンタの統計情報を表示します。

IGMP スヌーピング統計情報のクリア

次のコマンドを使用して、IGMP スヌーピング統計情報をクリアできます。

コマンド	目的
clear ip igmp snooping statistics vlan	IGMP スヌーピングの統計情報をクリアします。

IGMP スヌーピングの設定例

次に、IGMP スヌーピング パラメータの設定例を示します。

```
configure terminal
ip igmp snooping
vlan configuration 2
ip igmp snooping
ip igmp snooping explicit-tracking
ip igmp snooping fast-leave
ip igmp snooping last-member-query-interval 3
ip igmp snooping querier 172.20.52.106
ip igmp snooping mrouter interface ethernet 2/1
ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
ip igmp snooping link-local-groups-suppression
```

次に、プレフィックス リストを設定し、これらを使用して IGMP スヌーピング レポートをフィルタ処理する例を示します。

```
ip prefix-list plist seq 5 permit 224.1.1.1/32
ip prefix-list plist seq 10 permit 224.1.1.2/32
ip prefix-list plist seq 15 deny 224.1.1.3/32
ip prefix-list plist seq 20 deny 225.0.0.0/8 eq 32

vlan configuration 2
ip igmp snooping report-policy prefix-list plist interface Ethernet 2/2
ip igmp snooping report-policy prefix-list plist interface Ethernet 2/3
```

上記の例では、プレフィックス リストは 224.1.1.1 と 224.1.1.2 を許可していますが、224.1.1.3 と 225.0.0.0/8 範囲のすべてのグループを拒否しています。プレフィックス リストは、一致がない場合は暗黙的な「拒否」になります。その他すべてを許可する場合、ip prefix-list plist seq 30 permit 224.0.0.0/4 eq 32 を追加します。

次に、ルート マップを設定し、これらを使用して IGMP スヌーピング レポートをフィルタ処理する例を示します。

```
route-map rmap permit 10
match ip multicast group 224.1.1.1/32
route-map rmap permit 20
match ip multicast group 224.1.1.2/32
route-map rmap deny 30
match ip multicast group 224.1.1.3/32
route-map rmap deny 40
match ip multicast group 225.0.0.0/8

vlan configuration 2
ip igmp snooping report-policy route-map rmap interface Ethernet 2/4
ip igmp snooping report-policy route-map rmap interface Ethernet 2/5
```

上記の例では、ルートマップは 224.1.1.1 と 224.1.1.2 を許可していますが、224.1.1.3 と 225.0.0.0/8 範囲のすべてのグループを拒否しています。ルートマップは、一致がない場合は暗黙的な「拒否」になります。その他すべてを許可する場合、route-map rmap permit 50 match ip multicast group 224.0.0.0/4 を追加します。

その他の参考資料

IGMP スヌーピングの実装に関する詳細情報については、次の項目を参照してください。

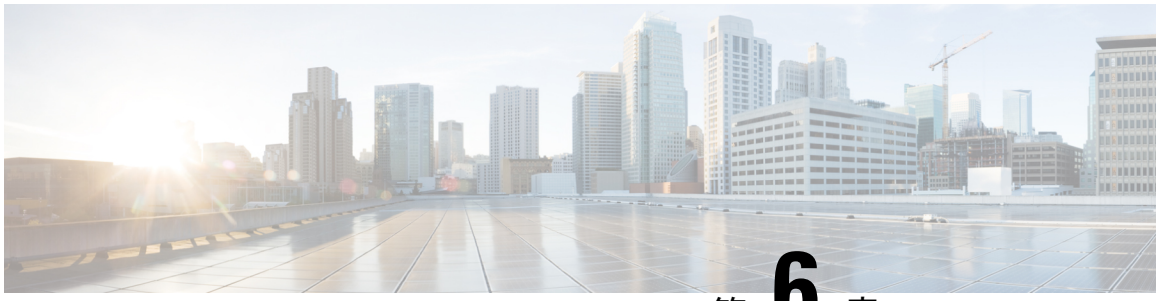
- 標準
- 関連資料

関連資料

関連項目	マニュアル タイトル
CLI コマンド	Cisco Nexus 3548 スイッチ マルチキャスト ルーティング コマンド リファレンス

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	-



第 6 章

MSDP の設定

この章では、Cisco NX-OS スイッチに Multicast Source Discovery Protocol（MSDP）を構成する方法について説明します。

この章は、次の項で構成されています。

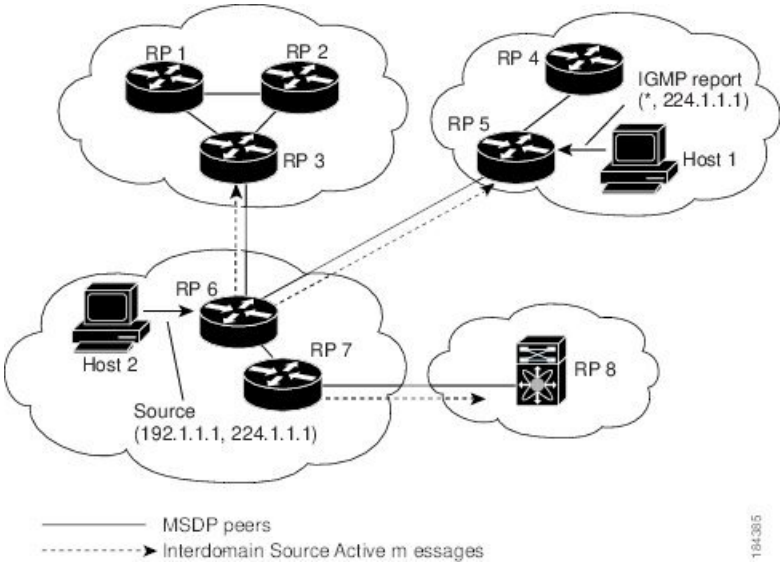
MSDP についての情報

MSDP を使用すると、複数のボーダ ゲートウェイ プロトコル（BGP）対応 Protocol Independent Multicast（PIM）スパース モード ドメイン間で、マルチキャスト送信元情報を交換できます。PIM に関する詳細は、「 PIM の構成 （37 ページ） 」を参照してください。BGP に関する詳細は、「*Cisco Nexus 3548* スイッチ *NX-OS* ユニキャスト ルーティング構成ガイド」を参照してください。

受信者が要求するグループが別のドメイン内の送信元から送信されたグループと一致した場合、ランデブー ポイント（RP）は送信元方向に PIM Join メッセージを送信して、最短パス ツリーを構築します。指定ルータ（DR）は、送信元ドメイン内の送信元ツリーにパケットを転送します。これらのパケットは、必要に応じて送信元ドメイン内の RP を経由し、送信元ツリーの各ブランチを通って他のドメインへと送信されます。受信者を含むドメインでは、対象のドメインの RP が送信元ツリー上に配置されている場合があります。ピアリング関係は転送制御プロトコル（TCP）接続を介して構築されます。

図 1 に、4 つの PIM ドメインを示します。接続された各 RP（ルータ）は、独自にマルチキャスト送信元のセットを保持しているため、RP は MSDP ピアと呼ばれます。送信元ホスト 1 はグループ 224.1.1.1 にマルチキャスト データを送信します。MSDP プロセスでは、RP 6 上で PIM Register メッセージを介して送信元に関する情報を学習すると、ドメイン内の送信元に関する情報が、Source-Active（SA）メッセージの一部として MSDP ピアに送信されます。SA メッセージを受信した RP 3 および RP 5 は、MSDP ピアに SA メッセージを転送します。RP 5 は、ホスト 2 から 224.1.1.1 のマルチキャスト データに対する要求を受信すると、192.1.1.1 のホスト 1 方向に PIM Join メッセージを送信して、送信元への最短パス ツリーを構築します。

図 *14*：異なる *PIM* ドメインに属する *RP* 間の *MSDP* ピアリング



各 RP 間で MSDP ピアリング設定を行うには、フル メッシュを作成します。一般的な MSDP フル メッシュは、RP 1、RP 2、RP 3 のように自律システム内に作成され、自律システム間には作成されません。ループ抑制および MSDP ピア Reverse Path Forwarding（RPF）により、SA メッセージのループを防止するには、BGP を使用します。メッシュ グループの詳細については、「MSDP メッシュ グループ」セクションを参照してください。

（注） PIM ドメイン内で Anycast RP（ロード バランシングおよびフェールオーバーを実行するための RP のセット）を使用する場合、MSDP を設定する必要はありません。詳細については、「PIM Anycast-RP セットの構成」セクションを参照してください。

MSDP の詳細については、RFC 3618 を参照してください。

SA メッセージおよびキャッシング

MSDP ピアによる Source-Active（SA）メッセージの交換を通じて、MSDP ソフトウェアは、アクティブな送信元に関する情報を伝播させます。SA メッセージには、次の情報が格納されています。

- データ送信元の送信元アドレス
- データ送信元で使用されるグループ アドレス
- RP の IP アドレスまたは設定済みの送信元 ID

PIM Register メッセージによって新しい送信元がアドバタイズされると、MSDP プロセスはそのメッセージを再カプセル化して SA メッセージに格納し、即座にすべての MSDP ピアに転送します。

SA キャッシュには、SA メッセージを介して学習したすべての送信元情報が保持されます。キャッシングを使用すると、既知のグループの情報がすべてキャッシュに格納されるため、新たな受信者を迅速にグループに加入させることができます。キャッシュに格納する送信元エントリ数を制限するには、SA 制限ピア パラメータを設定します。特定のグループ プレフィックスに対してキャッシュに格納する送信元エントリ数を制限するには、グループ制限グローバル パラメータを設定します。

MSDP ソフトウェアは 60 秒おきに、または SA インターバルのグローバル パラメータの設定に従って、SA キャッシュ内の各グループに SA メッセージを送信します。対象の送信元およびグループに関する SA メッセージが、SA インターバルから 3 秒以内に受信されなかった場合、SA キャッシュ内のエントリは削除されます。

MSDP ピア RPF 転送

MSDP ピアは、発信元 RP から離れた場所で SA メッセージを受信し、そのメッセージの転送を行います。このアクションは、ピア RPF フラッディングと呼ばれます。このルータは BGP ルーティング テーブルを調べ、SA メッセージの発信元 RP 方向にあるネクスト ホップ ピアを特定します。このピアを Reverse Path Forwarding（RPF）ピアと呼びます。

MSDP ピアは、非 RPF ピアから送信元 RP へ向かう同じ SA メッセージを受信すると、そのメッセージをドロップします。それ以外の場合、すべての MSDP ピアにメッセージが転送されます。

MSDP メッシュ グループ

MSDP メッシュ グループを使用すると、ピア RPF フラッディングで生成される SA メッセージ数を抑えることができます。図 6-1 で、RPs 1、2 および 3 は RP 6 から SA メッセージを受信します。メッシュ内のすべてのルータ間にピアリング関係を設定してから、これらのルータのメッシュ グループを作成すると、あるピアから発信される SA メッセージが他のすべてのピアに送信されます。メッシュ内のピアが受信した SA メッセージは転送されません。RP 3 が発信する SA メッセージは、RP 1 および RP 2 に転送されますが、これらの RP は受信したメッセージをメッシュ内のその他の RP には転送しません。

ルータは複数のメッシュ グループに参加できます。デフォルトでは、メッシュ グループは設定されていません。

仮想化のサポート

複数の仮想ルーティングおよびフォワーディング（VRF）インスタンスを定義することができます。MSDP 設定を選択された VRF に適用します。

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

VRF の構成に関する詳細は、『*Cisco Nexus 3548* スイッチ *NX-OS* ユニキャスト ルーティング構成ガイド』を参照してください。

MSDP の前提条件

MSDP の前提条件は、次のとおりです。

- スイッチ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。
- MSDP を設定するネットワークに PIM が設定済みである。
- MSDP を設定する PIM ドメインに BGP が設定済みである。

MSDP のデフォルト設定

テーブル 1 では、MSDP パラメータのデフォルト設定をリスト化しています。

表 *22 : MSDP* パラメータのデフォルト設定

パラメータ	デフォルト
説明	ピアの説明はありません。
管理シャットダウン	ピアは定義された時点でイネーブルになります。
MD5 パスワード	すべての MD5 パスワードがディセーブルになっています。
SA ポリシー（IN）	すべての SA メッセージが受信されます。
SA ポリシー（OUT）	発信される SA メッセージには登録済みの全送信元が含まれます。
SA の上限	上限は定義されていません。
発信元インターフェイスの名前	ローカル システムの RP アドレスです。

パラメータ	デフォルト
グループの上限	グループの上限は定義されていません。
SA インターバル	60 秒

MSDP の設定

MSDP ピアリングを有効にするには、各 PIM ドメイン内で MSDP ピアを設定します。

MSDP ピアリングの設定手順は次のとおりです。

ステップ 1 MSDP ピアとして動作させるルータを選択します。

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

ステップ 3 ステップ 1 で選択した各ルータで、MSDP ピアを構成します。「MSDP ピアの構成」セクションを参照してください。

ステップ 4 各 MSDP ピアでオプションの MSDP ピア パラメータを構成します。「MSDP ピア パラメータの構成」セクションを参照してください。

ステップ 5 各 MSDP ピアのオプション グローバル パラメータを構成します。「MSDP グローバル パラメータの構成」セクションを参照してください。

ステップ 6 各 MSDP ピアでオプションのメッシュ グループを構成します。「MSDP メッシュ グループの構成」セクションを参照してください。

（注） MSDP をイネーブルにする前に入力された MSDP コマンドは、キャッシュに格納され、MSDP がイネーブルになると実行されます。**ip msdp peer** または **ip msdp originator-id** コマンドを使用して、MSDP を有効にします。

ここでは次の項目について説明します。

- MSDP 機能の有効化
- MSDP ピアの設定
- MSDP ピア パラメータの設定
- MSDP グローバル パラメータの設定
- リモート マルチキャスト ソース サポート
- MSDP メッシュ グループの設定
- MSDP プロセスの再起動

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

MSDP 機能の有効化

手順の概要

1. **configure terminal**
2. **feature msdp**
3. （任意） **show running-configuration** | **grep** *feature*
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
ステップ 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。
ステップ 2	**feature msdp** 例： `switch# feature msdp`	MSDP 機能をイネーブルにして、MSDP コマンドを実行できるようにします。デフォルトでは、MSDP 機能はディセーブルになっています。
ステップ 3	（任意） **show running-configuration**	**grep** *feature* 例： `switch# show running-configuration | grep feature`	指定した **feature** コマンドを表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

MSDP ピアの構成

現在の PIM ドメインまたは別の PIM ドメイン内にある各 MSDP ピアとピアリング関係を構築するには、MSDP ピアを設定します。最初の MSDP ピアリング関係を設定すると、ルータ上で MSDP がイネーブルになります。

始める前に

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

MSDP ピアを設定するルータのドメイン内で、BGP および PIM が設定されていることを確認します。

手順の概要

1. **configure terminal**
2. **ip msdp peer** *peer-ip-address* **connect-source** *interface* [**remote-as** *as-number*]
3. （任意） **show ip msdp summary** [**vrf** *vrf-name* | **all**]
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
ステップ 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。
ステップ 2	**ip msdp peer** *peer-ip-address* **connect-source** *interface* [**remote-as** *as-number*] 例： `switch(config)# ip msdp peer 192.168.1.10 connect-source ethernet 2/1 remote-as 8`	MSDP ピアを設定してピア IP アドレスを指定します。ソフトウェアは、インターフェイスの送信元IP アドレスを使用して、ピアとの TCP 接続を行います。インターフェイスは、*type slot/port* という形式で表します。AS 番号がローカル AS と同じ場合、対象のピアはPIM ドメイン内にあります。それ以外の場合、対象のピアは PIM ドメインの外部にあります。デフォルトでは、MSDP ピアリングはディセーブルになっています。 （注） このコマンドを使用すると、MSDP ピアリングがイネーブルになります。 （注） ピア IP アドレス、インターフェイス、および AS 番号を必要に応じて変更し、各 MSDP ピアリング関係についてステップ 2 を繰り返します。
ステップ 3	（任意） **show ip msdp summary** [**vrf** *vrf-name*	**all**] 例：	MSDP ピアの概要を表示します。

	コマンドまたはアクション	目的
	`switch# show ip msdp summary`	
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

MSDP ピア パラメータの設定

テーブル2に示されているオプションのMSDP ピア パラメータが構成可能です。これらのパラメータは、各ピアの IP アドレスを使用して、グローバル コンフィギュレーション モードで設定します。

表 *23 : MSDP* ピア パラメータ

パラメータ	説明
説明	ピアの説明を示すストリング。デフォルトでは、ピアの説明は設定されていません。
管理シャットダウン	MSDP ピアをシャットダウンするパラメータ。コンフィギュレーションの設定はこのコマンドの影響を受けません。このパラメータを使用すると、ピアがアクティブになる前に、複数のパラメータ設定を有効にできます。シャットダウンを実行すると、その他のピアとの TCP 接続は強制終了されます。デフォルトでは、各ピアは定義した時点でイネーブルになります。
MD5 パスワード	ピアの認証に使用される MD5 共有パスワード キー。デフォルトでは、MD5パスワードはディセーブルになっています。
SA ポリシー（IN）	着信 SA メッセージのルートマップ ポリシー。デフォルトでは、すべての SA メッセージが受信されます。 （注） ルートマップポリシーを構成するには、『*Cisco Nexus 3548* スイッチ *NX-OS* ユニキャスト ルーティング構成ガイド』を参照してください。

パラメータ	説明
SA ポリシー（OUT）	発信 SA メッセージのルートマップ ポリシー。デフォルトでは、発信される SA メッセージには登録済みの全送信元が含まれます。 （注） ルートマップポリシーを構成するには、『*Cisco Nexus 3548* スイッチ *NX-OS* ユニキャスト ルーティング構成ガイド』を参照してください。
SA の上限	ピアで許可され、SA キャッシュに格納される (S, G) エントリ数。デフォルトでは、上限はありません。

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

（注） メッシュ グループの構成に関する詳細は、「MSDP メッシュ グループの設定 （125 ページ）」セクションを参照してください。

始める前に

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

手順の概要

1. **configure terminal**
2. **ip msdp description** *peer-ip-address description*
3. **ip msdp shutdown** *peer-ip-address*
4. **ip msdp password** *peer-ip-address password*
5. **ip msdp sa-policy** *peer-ip-address policy-name* **in**
6. **ip msdp sa-policy** *peer-ip-address policy-name* **out**
7. **ip msdp sa-limit** *peer-ip-address limit*
8. （任意） **show ip msdp peer** [*peer-address*] [**vrf** [*vrf-name* | *known-vrf-name* | **all**]
9. （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
ステップ 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。 （注） ステップ 2 でリストされたコマンドを使用して、MSDP ピア パラメータを設定します。
ステップ 2	**ip msdp description** *peer-ip-address description* 例： `switch(config)# ip msdp description 192.168.1.10 peer in Engineering network`	ピアの説明を示すストリングを設定します。デフォルトでは、ピアの説明は設定されていません。
ステップ 3	**ip msdp shutdown** *peer-ip-address* 例： `switch(config)# ip msdp shutdown 192.168.1.10`	ピアをシャットダウンします。デフォルトでは、各ピアは定義した時点でイネーブルになります。
ステップ 4	**ip msdp password** *peer-ip-address password* 例： `switch(config)# ip msdp password 192.168.1.10 my_md5_password`	ピアの MD5 パスワードをイネーブルにします。デフォルトでは、MD5 パスワードはディセーブルになっています。
ステップ 5	**ip msdp sa-policy** *peer-ip-address policy-name* **in** 例： `switch(config)# ip msdp sa-policy 192.168.1.10 my_incoming_sa_policy in`	着信 SA メッセージのルートマップ ポリシーをイネーブルにします。デフォルトでは、すべての SA メッセージが受信されます。
ステップ 6	**ip msdp sa-policy** *peer-ip-address policy-name* **out** 例： `switch(config)# ip msdp sa-policy 192.168.1.10 my_outgoing_sa_policy out`	発信 SA メッセージのルートマップ ポリシーをイネーブルにします。デフォルトでは、発信される SA メッセージには登録済みの全送信元が含まれます。
ステップ 7	**ip msdp sa-limit** *peer-ip-address limit* 例： `switch(config)# ip msdp sa-limit 192.168.1.10 5000`	ピアから受信可能な（S,G）エントリ数の上限を設定します。デフォルトでは、上限はありません。
ステップ 8	（任意） **show ip msdp peer** [*peer-address*] [**vrf** [*vrf-name* | *known-vrf-name* | **all**] 例： `switch# show ip msdp peer 192.168.1.10`	詳細な MSDP ピア情報を表示します。

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

MSDP グローバル パラメータの設定

テーブル 3 に示されているオプションのMSDP グローバル パラメータが構成可能です。

表 *24* : *MSDP* グローバル パラメータ

パラメータ	説明
発信元インターフェイスの名前	SA メッセージ エントリの RP フィールドで使用される IP アドレス。Anycast RP を使用する場合は、すべての RP に対して同じ IP アドレスを使用します。このパラメータを使用すると、各 MSDP ピアの RP に一意の IP アドレスを定義できます。デフォルトでは、ローカルシステムの RP アドレスが使用されます。
グループの上限	指定したプレフィックスに対してソフトウェアが作成する (S, G) エントリの最大数。グループの上限を超えた場合、そのグループは無視され、違反状態が記録されます。デフォルトでは、グループの上限は定義されていません。
SA インターバル	Source-Active（SA）メッセージを送信する間隔。有効値の範囲は 60 ～ 65,535 秒です。デフォルトは 60 秒です。

始める前に

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

手順の概要

1. **configure terminal**
2. **ip msdp originator-id** *interface*
3. **ip msdp group-limit** *limit* **source** *source-prefix*
4. **ip msdp sa-interval** *seconds*
5. （任意） **show ip msdp summary** [**vrf** *vrf-name* | **all**]

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
ステップ 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。
ステップ 2	**ip msdp originator-id** *interface* 例： `switch(config)# ip msdp originator-id loopback0`	ピアの説明を示すストリングを設定します。デフォルトでは、ピアの説明は設定されていません。 SA メッセージ エントリの RP フィールドで使用される IP アドレスを設定します。デフォルトでは、ローカル システムの RP アドレスが使用されます。 （注） RP アドレスにはループバック インターフェイスを使用することを推奨します。
ステップ 3	**ip msdp group-limit** *limit* **source** *source-prefix* 例： `switch(config)# ip msdp group-limit 1000 source 192.168.1.0/24`	指定したプレフィックスに対してソフトウェアが作成する (S, G) エントリの最大数。グループの上限を超えた場合、そのグループは無視され、違反状態が記録されます。デフォルトでは、グループの上限は定義されていません。
ステップ 4	**ip msdp sa-interval** *seconds* 例： `switch(config)# ip msdp sa-interval 80`	Source-Active（SA）メッセージを送信する間隔。有効値の範囲は 60 ～ 65,535 秒です。デフォルトは 60 秒です。
ステップ 5	（任意） **show ip msdp summary** [**vrf** *vrf-name* | **all**] 例： `switch(config)# show ip msdp summary`	MSDP 構成の概要を表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

リモート マルチキャスト ソース サポート

マルチキャスト トラフィックがアタッチされない送信元から受信された場合、(S,G) ルートは形成されず、すべてのトラフィックは継続してCPUをヒットします。この機能を有効にして、トラフィックが CPU に送信されるのを回避し、設定された mroute でハードウェア内で処理されるようにできます。

この機能が有効の場合、送信元へのスタティック mroute は **ip mroute** src-ip *next-hop* コマンドを使用して構成します。事前構築された spt が **ip pim pre-build-spt** コマンドを使用して有効になっている場合は、（S、G）ルートが形成され、トラフィックが CPU をヒットしなくなります。また、これらのソースには、登録メッセージが定期的に送信され、MSDP SA メッセージがピアに送信されます。

手順の概要

1. **configure terminal**
2. **ip mfwd mstatic register**
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
ステップ 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。
ステップ 2	**ip mfwd mstatic register** 例： `switch(config)# ip mfwd mstatic register`	リモート マルチキャスト ソースのサポートを有効にします。
ステップ 3	（任意） copy running-config startup-config 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

MSDP メッシュ グループの設定

メッシュで各ピアを指定して、グローバル構成モードでオプションの MSDP メッシュ グループを構成できます。同じルータに複数のメッシュ グループを設定したり、各メッシュ グループに複数のピアを設定したりできます。

始める前に

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

手順の概要

1. **configure terminal**
2. **ip msdp mesh-group** *peer-ip-addr mesh-name*
3. （任意） **show ip msdp mesh-group** [*mesh-group*] [**vrf** [*vrf-name* | *known-vrf-name* | **all**]
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
ステップ 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。
ステップ 2	**ip msdp mesh-group** *peer-ip-addr mesh-name* 例： `switch(config)# ip msdp mesh-group 192.168.1.10 my_mesh_1`	MSDP メッシュを設定してピア IP アドレスを指定します。同じルータに複数のメッシュを設定したり、各メッシュ グループに複数のピアを設定したりできます。デフォルトでは、メッシュ グループは設定されていません。 （注） ピア IP アドレスを変更し、メッシュ内の各 MSDP ピアについてステップ 2 を繰り返します。
ステップ 3	（任意） **show ip msdp mesh-group** [*mesh-group*] [**vrf** [*vrf-name*	*known-vrf-name*	**all**] 例： `switch# show ip msdp mesh-group`	MSDP メッシュ グループ構成に関する詳細を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

MSDP プロセスの再起動

MSDP 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。

始める前に

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

手順の概要

1. **restart msdp**
2. **configure terminal**
3. **ip msdp flush-routes**
4. （任意） **show running-configuration | include flush-routes**
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
ステップ 1	**restart msdp** 例： `switch# restart msdp`	MSDP プロセスを再起動します。
ステップ 2	**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。
ステップ 3	**ip msdp flush-routes** 例： `switch(config)# ip msdp flush-routes`	MSDP プロセスの再起動時に、ルートを削除します。デフォルトでは、ルートはフラッシュされません。
ステップ 4	（任意） **show running-configuration | include flush-routes** 例： `switch(config)# show running-configuration | include flush-routes`	実行コンフィギュレーションの flush-routes 構成行を表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

MSDP の設定の確認

MSDP の設定情報を表示するには、次の作業のいずれかを行います。

コマンド	説明
show ip msdp count [*as-number*] [**vrf** *vrf-name* |*known-vrf-name* | **all**]	MSDP（S,G）のエントリ数およびグループ数を自律システム（AS）番号別に表示します。
show ip msdp mesh-group [*mesh-group*] [**vrf** *vrf-name* | **all**]	MSDP メッシュ グループ設定を表示します。
show ip msdp peer [*peer-address*] [**vrf** *vrf-name* | *known-vrf-name* | **all**]	MSDP ピアの MSDP 情報を表示します。
show ip msdp rpf [*peer-address*] [**vrf** *vrf-name* | *known-vrf-name* | **all**]	RP アドレスへの BGP パス上にあるネクストホップ AS を表示します。
show ip msdp sources [*peer-address*] [**vrf** *vrf-name* | *known-vrf-name* | **all**]	MSDP で学習された送信元と、グループ上限設定に関する違反状況を表示します。
show ip msdp summary [*peer-address*] [**vrf** *vrf-name* | *known-vrf-name* | **all**]	MSDP ピア設定の要約を表示します。
show ip igmp snooping	vPC マルチキャスト最適化が有効か無効かを表示します。

これらのコマンドから出力でフィールドに関する詳細は、『Cisco Nexus 3000 シリーズ NX-OS マルチキャスト ルーティング コマンド リファレンス』を参照してください。

統計の表示

次に、MSDP の統計情報を、表示およびクリアするための機能について説明します。

統計の表示

テーブル 4 でリスト化されているコマンドを使用して、MSDP 統計情報を表示できます。

表 *25 : MSDP* 統計情報コマンド

コマンド	目的
show ip msdp policy statistics sa-policy *peer-address* { **in** | **out**} [**vrf** *vrf-name* | *known-vrf-name* | **all**]	MSDP ピアの MSDP ポリシー統計情報を表示します。

コマンド	目的
show ip msdp { **sa-cache** | **route**}[*source-address*][*group-address*][**vrf** *vrf-name* | *known-vrf-name* | **all**] [*asn-number*] [**peer** *peer-address*]	MSDP SA ルート キャッシュを表示します。送信元アドレスを指定した場合は、その送信元に対応するすべてのグループが表示されます。グループ アドレスを指定した場合は、そのグループに対応するすべての送信元が表示されます。

統計情報のクリア

表 5 に一覧になっているコマンドを使用して、MSDP 統計情報をクリアできます。

表 *26 :* 統計情報のクリア コマンド

コマンド	説明
clear ip msdp peer [*peer-address*] [**vrf** *vrf-name* | *known-vrf-name*]	MSDP ピアとの TCP 接続をクリアします。
clear ip msdp policy statistics sa-policy *peer-address* {**in** | **out**} [**vrf** *vrf-name* | *known-vrf-name*]	MSDP ピア SA ポリシーの統計情報カウンタをクリアします。
clear ip msdp statistics [*peer-address*] [**vrf** *vrf-name* | *known-vrf-name*]	MSDP ピア の統計情報をクリアします。
clear ip msdp {**sa-cache** | **route**} [*group-address*] [**vrf** *vrf-name* | *known-vrf-name* | **all**]	SA キャッシュ内のグループ エントリをクリアします。

MSDP の設定例

MSDP ピア、一部のオプション パラメータ、およびメッシュ グループを設定するには、MSDP ピアごとに次の手順を実行します。

1. 他のルータとの MSDP ピアリング関係を設定します。

```
switch# configure terminal
switch(config)# ip msdp peer 192.168.1.10 connect-source ethernet 1/0 remote-as 8
```

2. オプションのピア パラメータを設定します。

```
switch# configure terminal
switch(config)# ip msdp password 192.168.1.10 my_peer_password_AB
```

3. オプションのグローバル パラメータを設定します。

```
switch# configure terminal
switch(config)# ip msdp sa-interval 80
```

4. 各メッシュ グループ内のピアを設定します。

```
switch# configure terminal
switch(config)# ip msdp mesh-group 192.168.1.10 mesh_group_1
```

次に、下に示す MSDP ピアリングのサブセットの設定例を示します。

RP 3: 192.168.3.10（AS 7）

```
configure terminal
  ip msdp peer 192.168.1.10 connect-source ethernet 1/1
  ip msdp peer 192.168.2.10 connect-source ethernet 1/2
  ip msdp peer 192.168.6.10 connect-source ethernet 1/3 remote-as 9
  ip msdp password 192.168.6.10 my_peer_password_36
  ip msdp sa-interval 80
  ip msdp mesh-group 192.168.1.10 mesh_group_123
  ip msdp mesh-group 192.168.2.10 mesh_group_123
  ip msdp mesh-group 192.168.3.10 mesh_group_123
```

RP 5: 192.168.5.10（AS 8）

```
configure terminal
  ip msdp peer 192.168.4.10 connect-source ethernet 1/1
  ip msdp peer 192.168.6.10 connect-source ethernet 1/2 remote-as 9
  ip msdp password 192.168.6.10 my_peer_password_56
  ip msdp sa-interval 80
```

RP 6: 192.168.6.10（AS 9）

```
configure terminal
  ip msdp peer 192.168.7.10 connect-source ethernet 1/1
  ip msdp peer 192.168.3.10 connect-source ethernet 1/2 remote-as 7
  ip msdp peer 192.168.5.10 connect-source ethernet 1/3 remote-as 8
  ip msdp password 192.168.3.10 my_peer_password_36
  ip msdp password 192.168.5.10 my_peer_password_56
  ip msdp sa-interval 80
```

次に、Cisco NX-OS Release 5.0(3)U2(1) を実行するスイッチの IGMP スヌーピング情報に関する情報を表示する例を示します。また、仮想ポート チャネル（vPC）のマルチキャスト最適化のステータスを示します。

```
switch# show ip igmp snooping
Global IGMP Snooping Information:
IGMP Snooping enabled
Optimised Multicast Flood (OMF) disabled
IGMPv1/v2 Report Suppression enabled
IGMPv3 Report Suppression disabled
Link Local Groups Suppression enabled
VPC Multicast optimization disabled
IGMP Snooping information for vlan 1
IGMP snooping enabled
Optimised Multicast Flood (OMF) disabled
IGMP querier present, address: 10.1.1.7, version: 2, interface Ethernet1/13
Switch-querier disabled
IGMPv3 Explicit tracking enabled
IGMPv2 Fast leave disabled
IGMPv1/v2 Report suppression enabled
```

```
IGMPv3 Report suppression disabled
Link Local Groups suppression enabled
Router port detection using PIM Hellos, IGMP Queries
Number of router-ports: 1
Number of groups: 0
Active ports:
Eth1/11 Eth1/13
switch#
```

その他の参考資料

MSDP の実装に関する詳細情報については、次の項目を参照してください。

- 関連資料
- 標準
- 付録 A、IP マルチキャスト向け IETF RFC

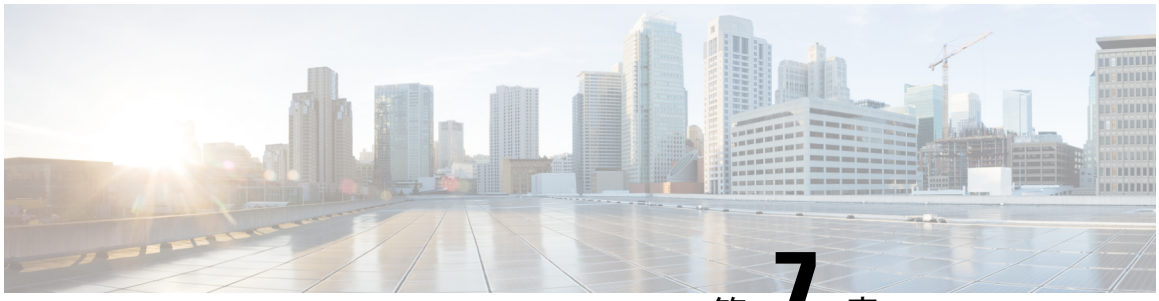
関連資料

関連項目	マニュアル タイトル
CLI コマンド	Cisco Nexus 3000 シリーズ NX-OS マルチキャスト コマンド リファレンス

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	-

標準



第 7 章

マルチキャスト エクストラネットの構成

この章では、Cisco NX-OS スイッチでマルチキャスト エクストラネットを構成する方法を説明します。

この章は、次の項で構成されています。

マルチキャスト エクストラネットに関する詳細

現在の NX-OS マルチキャスト実装では、マルチキャスト トラフィックは同じ VRF 内のみでフローできます。マルチキャスト エクストラネット機能では、企業ネットワークのソースとは異なる VRF にマルチキャスト レシーバが存在する場合があります。

マルチキャスト エクストラネットを使用すると、レシーバ VRF のマルチキャスト ルートの RPF ルックアップをソース VRF で実行できるため、有効な RPF インターフェイスを返すことができます。これにより、レシーバ VRF からソース VRF へのソースまたは RP ツリーが形成され、ソース VRF から発信されたトラフィックをレシーバ VRF の OIF に転送できるようになります。

別の VRF で RPF 選択をサポートするには、**ip multicast rpf select vrf** コマンドを使用します。

マルチキャスト エクストラネットの注意事項と制限事項

マルチキャスト エクストラネットには、次の注意事項と制限事項があります。

- 送信元と RP は同じ VRF にある必要があります。
- マルチキャスト NAT とマルチキャスト エクストラネットは、同じボックスの同じグループに対して共存しないようにしてください。
- Auto RP は、マルチキャスト エクストラネットではサポートされていません。

- 必要なマルチキャスト ルートと VRF の数によって、マルチキャストによるメモリ消費量が決まります。
- マルチキャスト VPN（MVPN）エクストラネットは、マルチキャスト エクストラネットではサポートされていません。
- RPF ルックアップは、**ip multicast rpf select vrf** コマンドで指定された VRF で実行されます。フォールバック モードはサポートされていません。
- ファストパス モードでの ASM マルチキャスト グループ変換では、未変換グループのスタティック OIF を IGMPv2 インターフェイスで構成する必要があります。送信元固有のスタティック OIF 構成（IGMPv3）はサポートされていません。

マルチキャスト エクストラネットの構成

始める前に

開始する前に、PIM が有効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-range*
3. （任意） **show ip mroute**
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
ステップ 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。
ステップ 2	**ip multicast rpf select vrf** *src-vrf-name* **group-list** *group-range* 例： `switch(config)# ip multicast rpf select vrf red group-list 224.1.1.0/24`	別の VRF での RPF 選択をサポートします。サポートを無効にするには、このコマンドの **no** 形式を使用します。 **vrf** *src-vrf-name* は送信元 VRF 名です。名前は最大 32 文字の英数字で、大文字と小文字が区別されます。 **group-list** *group-range* は RPF 選択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。

	コマンドまたはアクション	目的
ステップ 3	（任意） **show ip mroute** 例： `switch(config)# show ip mroute`	IPv4 マルチキャスト ルートの実行コンフィギュレーション情報を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

マルチキャスト エクストラネット構成の確認

マルチキャストエクストラネット構成情報を表示するには、次のタスクのうちいずれかを実行します。

表 *27:*

コマンド	目的
show ip mroute	IPv4 マルチキャスト ルートの実行コンフィギュレーション情報を表示します。

次の例では、IPv4 マルチキャスト ルートのルーティング構成に関する情報を表示する方法を示します。

```
switch(config)# show ip mroute
IP Multicast Routing Table for VRF "default"

(*, 225.1.1.207/32), uptime: 00:13:33, ip pim

Incoming interface: Vlan147, RPF nbr: 147.147.147.2, uptime: 00:13:33

Outgoing interface list: (count: 0)

Extranet receiver in vrf blue:

(*, 225.1.1.207/32) OIF count: 1

(40.1.1.2/32, 225.1.1.207/32), uptime: 00:00:06, mrib ip pim

Incoming interface: Vlan147, RPF nbr: 147.147.147.2, uptime: 00:00:06

Outgoing interface list: (count: 0)

Extranet receiver in vrf blue:

(40.1.1.2/32, 225.1.1.207/32) OIF count: 1
```

```
switch(config)#
```

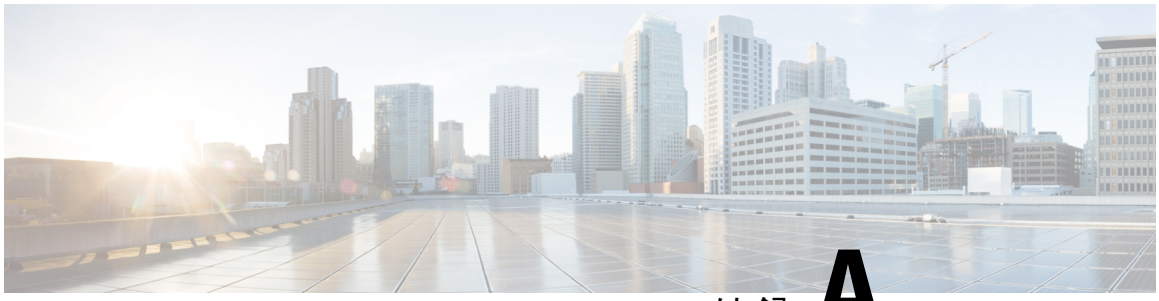
これらのコマンドからの出力でフィールドに関する詳細情報は、『Cisco Nexus 3000 シリーズ マルチキャスト ルーティング コマンド リファレンス』を参照してください。

関連資料

関連項目	マニュアル タイトル
CLI コマンド	Cisco Nexus 3000 シリーズ マルチキャスト ルーティング コマンド リファレンス

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—



付録 A

IP マルチキャストについての IETF RFC

この付録には、IP マルチキャスト関連の、インターネット技術特別調査委員会（IETF）策定の RFC を掲載しています。IETF RFC の詳細については、http://www.ietf.org/rfc.html を参照してください。

• IP マルチキャストについての IETF RFC （137 ページ）

IP マルチキャストについての IETF RFC

RFC	タイトル
RFC 2236	『*Internet Group Management Protocol, Version 2*』
RFC 2365	管理用スコープの *IP* マルチキャスト
RFC 2858	*BGP-4* のマルチプロトコル拡張
RFC 3376	インターネット グループ管理プロトコル、バージョン *3*
RFC 3446	『*Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*』
RFC 3569	送信元特定マルチキャスト（*SSM*）の概要
RFC 3618	*Multicast Source Discovery Protocol*（*MSDP*）
RFC 4541	*Internet Group Management Protocol*（*IGMP*）スヌーピング スイッチの考慮事項
RFC 4601	『*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*』
RFC 4610	『*Anycast-RP Using Protocol Independent Multicast (PIM)*』
RFC 5132	『*IP Multicast MIB*』

IP マルチキャストについての IETF RFC

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。