Cisco Nexus 9000 シリーズ NX-OS マルチキャスト ルーティング コンフィギュレーション ガイド リリース 6.x

初版：2013 年 11 月 20 日

最終更新：2014 年 11 月 10 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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。 このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。 このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。 添付されていない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。 All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。 シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。 マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。 説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013-2014 Cisco Systems, Inc. All rights reserved.

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わる、ハードウェア設置者およびネットワーク管理者を対象としています。

表記法

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、角カッコ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。

表記法	説明
{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、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコ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。 角カッコ内の波カッコと縦棒は、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、screen 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 screen フォントで示しています。
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。

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、 へご連絡ください。 ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html から入手できます。

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、RSS フィードとして購読できます。また、リーダー アプリケーションを使用して、コンテンツをデスクトップに配信することもできます。 RSS フィードは無料のサービスです。

第 1 章

新機能および変更された機能に関する情報

この章では、『*Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 6.x*』に記載されている新しい機能と変更された機能に関するリリース固有の情報について説明します。

新機能および変更された機能に関する情報

次の表は、『*Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 6.x*』に記載されている新機能および変更機能をまとめたものです。それぞれの説明が記載されている箇所も併記されています。

表 *1*：*MDS NX-OS* リリース *6.x* の新機能と変更された機能

機能	説明	変更されたリリース	参照先
PIM	起動時あるいはIPアドレスまたはインターフェイス状態の変更後に指定ルータの選定への参加を遅らせる機能が追加されました。	6.1(2)I3(2)	PIM の設定，（33 ページ）
IGMP スヌーピング	IGMP スヌーピング レポートをフィルタリングする機能が追加されました。	6.1(2)I2(2)	IGMP スヌーピングの設定，（81 ページ）
IGMP	レイヤ 2 スイッチングのサポートが追加されました。	6.1(1)I2(2)	IGMP の設定，（15 ページ）

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
IGMP スヌーピング	この機能が導入されました。	6.1(1)I2(2)	IGMP スヌーピングの設定, （81 ページ）
PIM	PIM ASM に対する vPC のサポートが追加されました。	6.1(1)I2(2)	PIM の設定, （33 ページ）

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。

マルチキャストについて

IP マルチキャストは、ネットワーク内の複数のホストに同じ IP パケット セットを転送する機能です。 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。

マルチキャストは、マルチキャスト データの配信機能と、送信元および受信者の検出機能からなり、マルチキャスト データは、グループと呼ばれる IP マルチキャスト アドレス宛に送信されます。 多くの場合、グループおよび送信元 IP アドレスを含むマルチキャスト アドレスは、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、次の URL を参照してください。http://www.iana.org/assignments/multicast-addresses

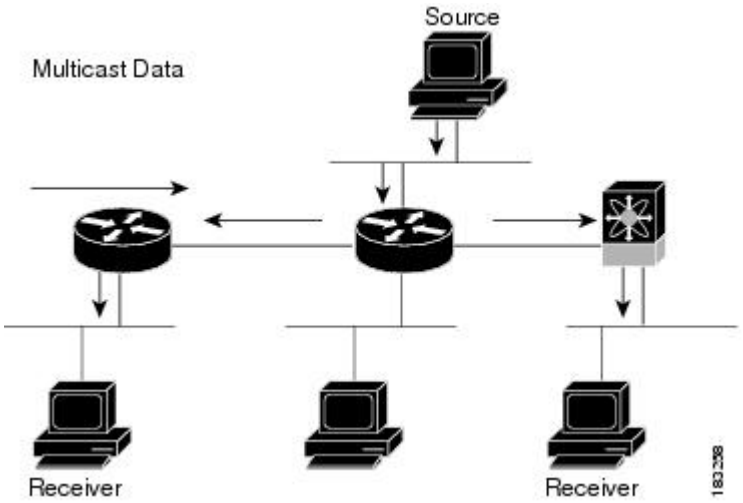
（注） マルチキャスト関連の RFC の一覧については、付録 A「IP マルチキャストに関する IETF RFC」を参照してください。

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。

次の図に、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



Multicast Distribution Tree（MDT）

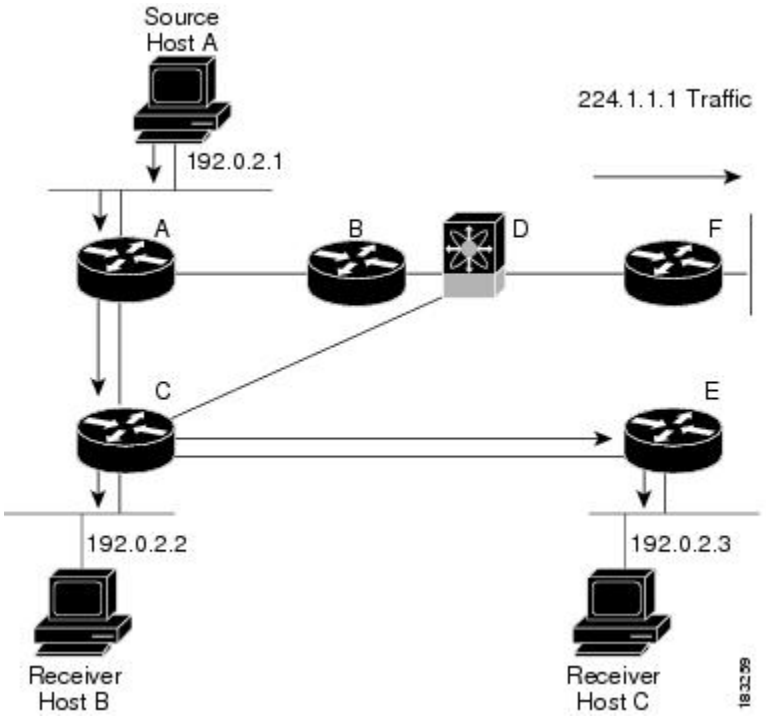
マルチキャスト配信ツリーとは、送信元と受信者を中継するルータ間の、マルチキャスト データの伝送パスを表します。マルチキャスト ソフトウェアはサポートするマルチキャスト方式に応じて、タイプの異なるツリーを構築します。

送信元ツリー

送信元ツリーは、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。送信元から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、同じグループに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。 次の表に、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ます。

図 *2*：送信元ツリー



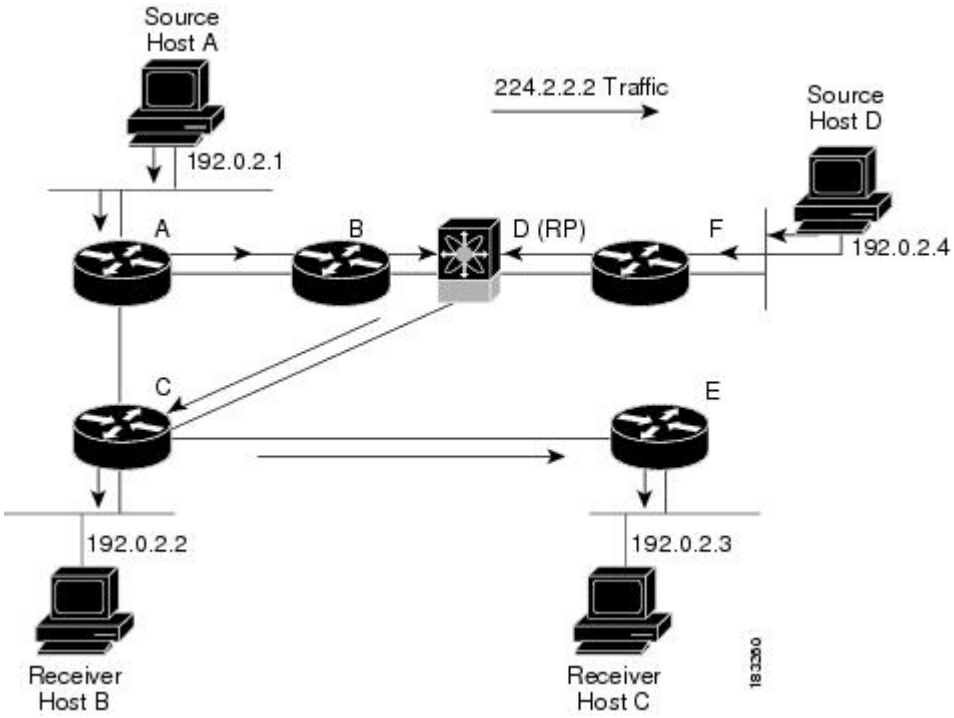
(S, G) は、グループ G の送信元 S から送信されるマルチキャスト トラフィックを表します。 この図の SPT は、(192.0.2.1, 224.1.1.1) と書き表されます。 同じグループの複数の送信元からトラフィックを送信できます。

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 は各送信元への 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。 次の図に、ルータ D を RP とする場合の、グループ 224.1.1.1 の共有ツリーを示します。 データはホスト 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



(*, G) は、グループ G の任意の送信元から送信されるマルチキャスト トラフィックを表します。この図の共有ツリーは、(*, 224.2.2.2) と書き表されます。

マルチキャスト転送

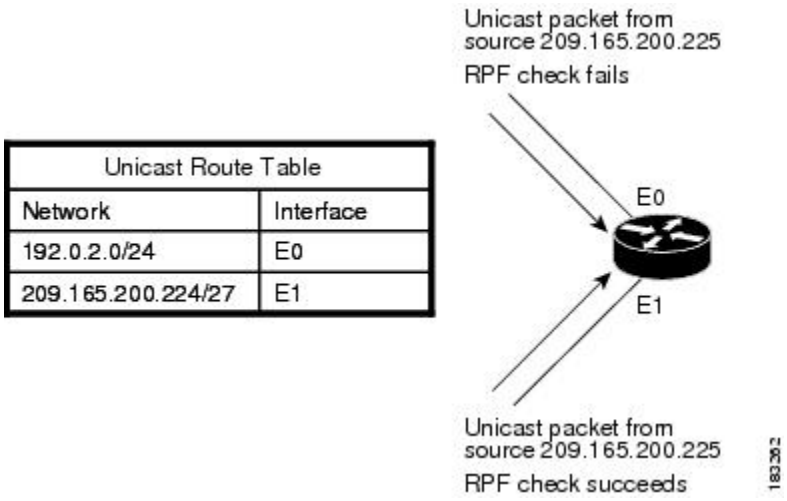
マルチキャスト トラフィックは任意のホストを含むグループ宛に送信されるため、ルータは Reverse Path Forwarding（RPF）を使用して、グループのアクティブな受信者にデータをルーティングします。 受信者がグループに参加すると、パスは RP（ASM モード）向けに形成されます。 送信元から受信者へのパスは、受信者がグループに加入したときに作成されたパスと逆方向になります。

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。 送信元に接続されたインターフェイスにパケットが着信した場合は、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パケットが転送されます。 それ以外の場合、パケットはドロップされます。

次の図に、異なるインターフェイスから着信したパケットについて、RPF チェックを行う場合の例を示します。 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 の 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。 Cisco NX-OS では、PIM デンス モードはサポートされません。

（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 がシステムで稼働しています。

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。

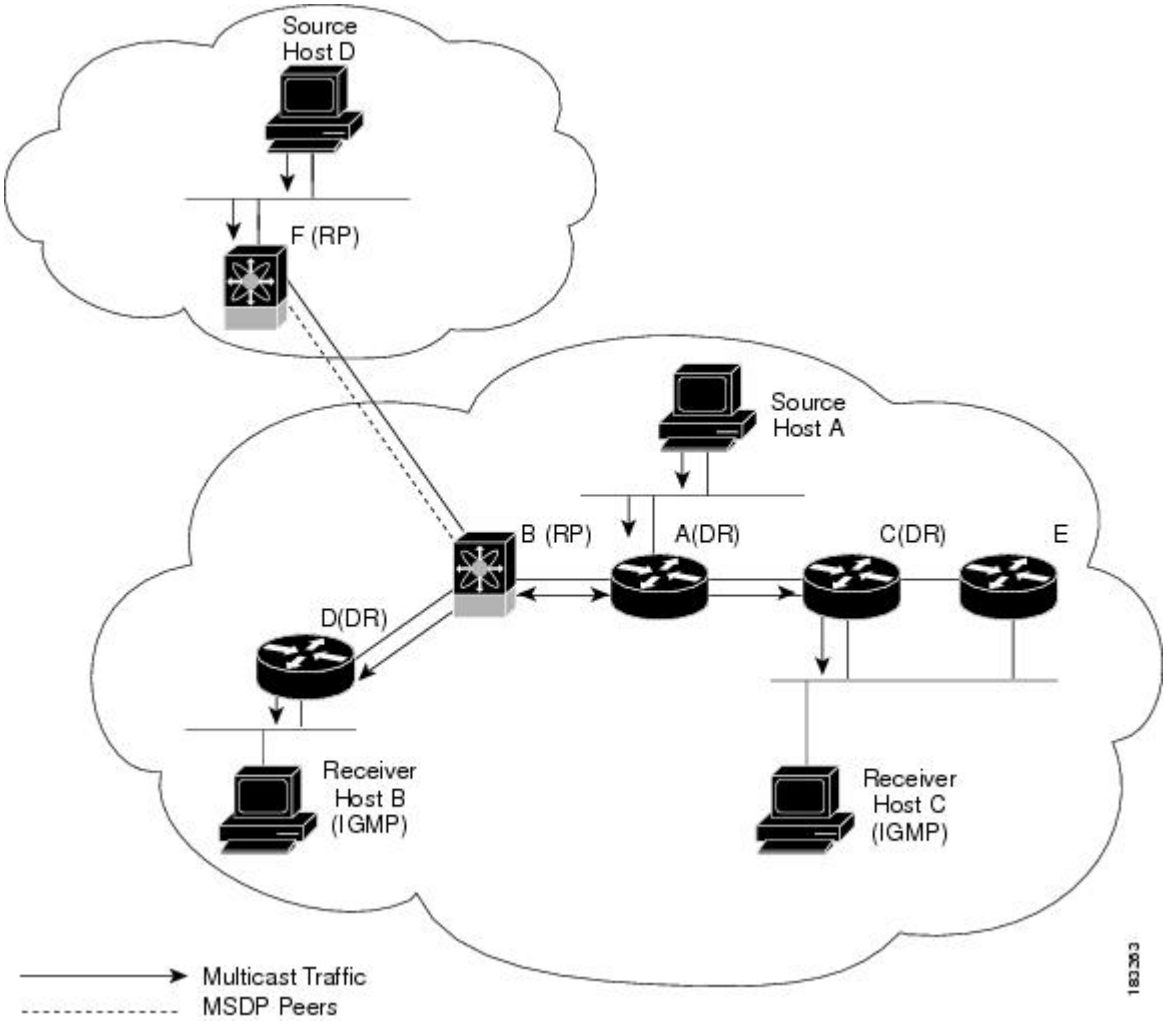
配信ツリーは、リンク障害またはルータ障害のためにトポロジが変更されると、トポロジを反映して自動的に変更されます。 PIM は、マルチキャスト対応の送信元と受信者の両方を動的に追跡します。

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、マルチキャストを実行するためのマルチキャスト 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 スパースモードの実装を表します。

次の図に、IPv4 ネットワーク内の 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



- 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、次のマルチキャスト モードをサポートしています。

- Any Source Multicast（ASM）

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。

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 が学習されている場合、グループは ASM モードで動作します。

RP を設定する場合、デフォルト モードは ASM モードです。

マルチキャスト用 RPF ルート

スタティック 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。

IGMP

システムは、PIM の場合はインターネット グループ管理プロトコル（IGMP）をデフォルトで実行しています。

IGMP 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 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。

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。

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。

MBGP

Multiprotocol BGP（MBGP）は BGP4 の拡張機能であり、ルータによるマルチキャスト ルーティング情報の伝送を可能にします。 このマルチキャスト情報を使用すると、PIM を介して、外部の BGP 自律システム（AS）内の送信元と通信できます。

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）インスタンスごとに、独立したルート情報を保持します。

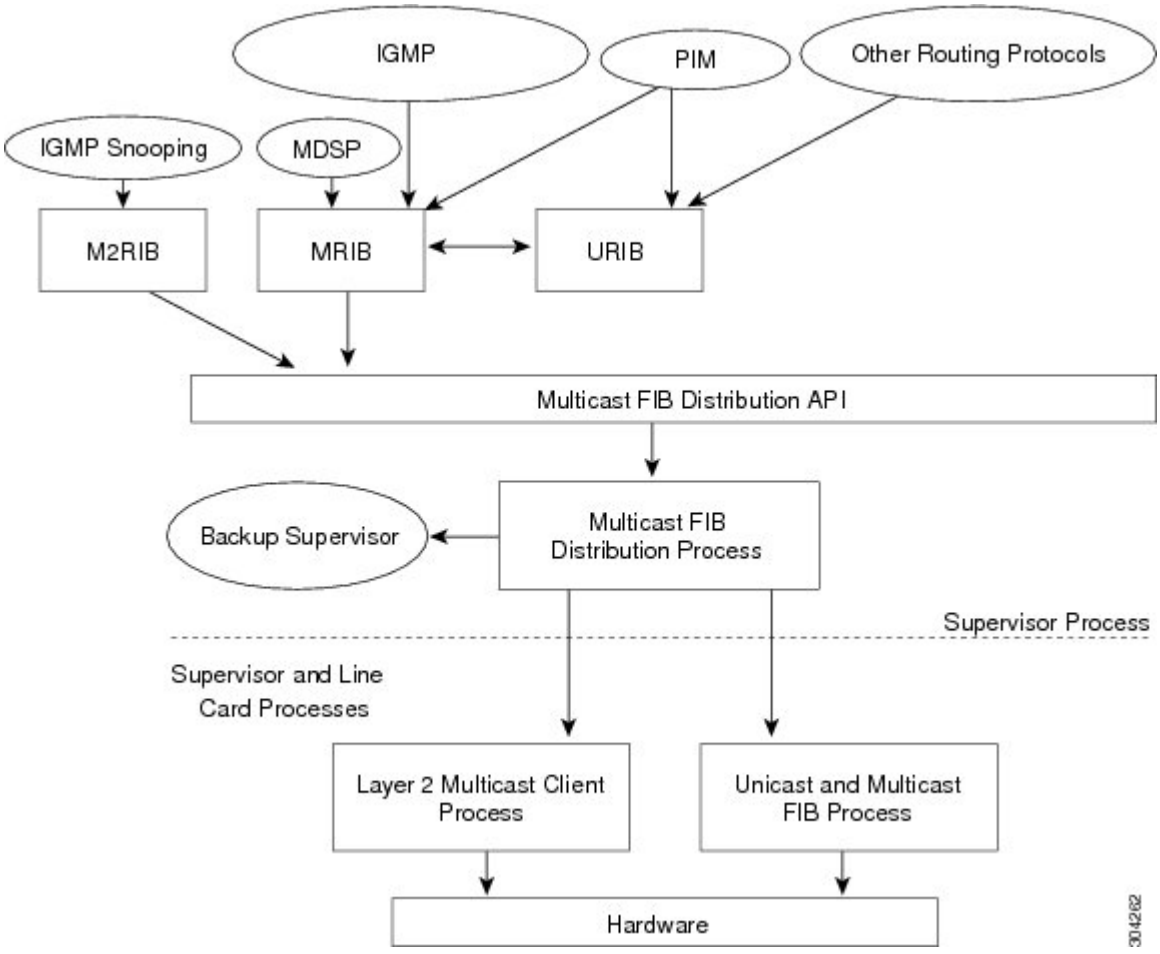
Cisco NX-OS マルチキャスト ソフトウェア アーキテクチャの主要コンポーネントは次のとおりです。

- Multicast FIB（MFIB）Distribution（MFDM）API：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 アップデートを送信します。

- マルチキャストFIB配信プロセス：すべての関連モジュールおよびスタンバイ スーパーバイザに、マルチキャスト アップデート メッセージを配布します。 このプロセスはスーパーバイザだけで実行されます。
- 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。 このプロセスは、スーパーバイザとモジュールの両方で実行されます。
- 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。 このプロセスは、スーパーバイザとモジュールの両方で実行されます。

次の図に、Cisco NX-OS マルチキャスト ソフトウェアのアーキテクチャを示します。

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



仮想ポート チャネルおよびマルチキャスト

仮想ポート チャネル（vPC）：1 台のデバイスで 2 台のアップストリーム スイッチのポート チャネルを使用できるようにします。 vPC を設定すると、次のマルチキャスト機能に影響が及ぶ場合があります。

- PIM：Cisco NX-OS デバイス用の Cisco NX-OS ソフトウェアは、vPC 上の PIM SSM をサポートしません。 Cisco NX-OS ソフトウェアは、vPC での PIM ASM を完全にサポートします。
- IGMP スヌーピング：vPC ピアの設定を同一にする必要があります。

マルチキャスト機能のライセンス要件

次に、ライセンスを必要とするマルチキャスト機能を示します。

- PIM
- MSDP

次に、ライセンスが不要なマルチキャスト機能を示します。

- IGMP
- IGMP スヌーピング

Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

マルチキャストに関する注意事項と制限事項

- レイヤ 3 IPv6 マルチキャスト ルーティングはサポートされていません。
- レイヤ 2 IPv6 マルチキャスト パケットは、着信 VLAN でフラッディングされます。

マルチキャスト機能のハイ アベイラビリティ要件

マルチキャスト ルーティング プロトコルを再起動すると、MRIB プロセスによってステートが回復されます。 スーパーバイザのスイッチオーバーが発生した場合、MRIB はハードウェアからステートを回復し、マルチキャストプロトコルは定期的なメッセージアクティビティからステートを回復します。 ハイ アベイラビリティの詳細については、『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

仮想デバイス コンテキスト

Cisco NX-OS では、仮想デバイスをエミュレートする Virtual Device Context（VDCs）に、OS およびハードウェア リソースを分割できます。 Cisco Nexus 9000 シリーズ スイッチは、現在のところ、複数の VDC をサポートしていません。 すべてのスイッチ リソースはデフォルト VDC で管理されます。

テクニカル サポート

説明	Link
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。	http://www.cisco.com/public/support/tac/home.shtml

第 3 章

IGMP の設定

この章では、IPv4 ネットワークの Cisco NX-OS デバイスに対するインターネット グループ管理プロトコル（IGMP）の設定方法を説明します。

IGMP について

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

デバイスでは、IGMPv1 のほかに、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。

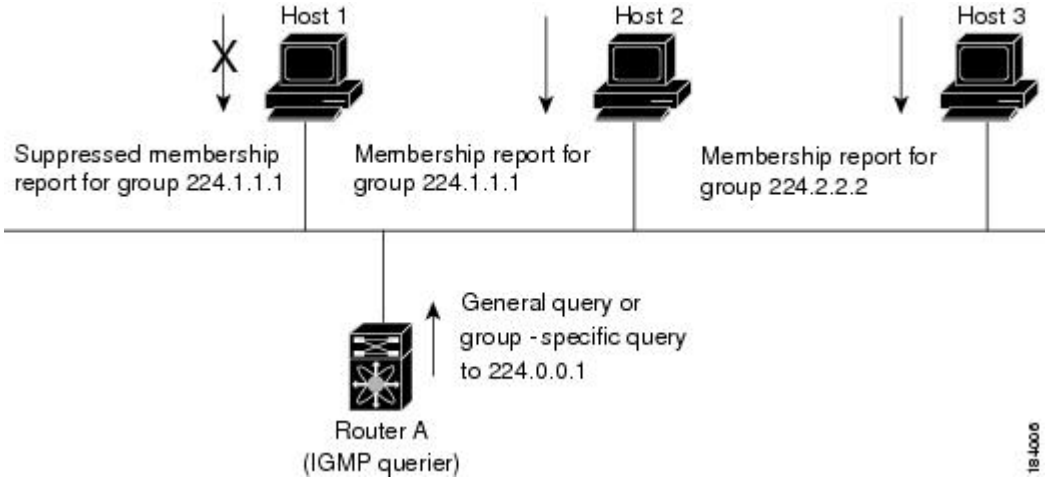
IGMPv2 の詳細については、RFC 2236 を参照してください。

IGMPv3 の詳細については、RFC 3376 を参照してください。

IGMP の基礎

次の図に、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*** クエリー応答プロセス



次の図のルータ 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ーメッセージを送信して、マルチキャストデータの受信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し、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。

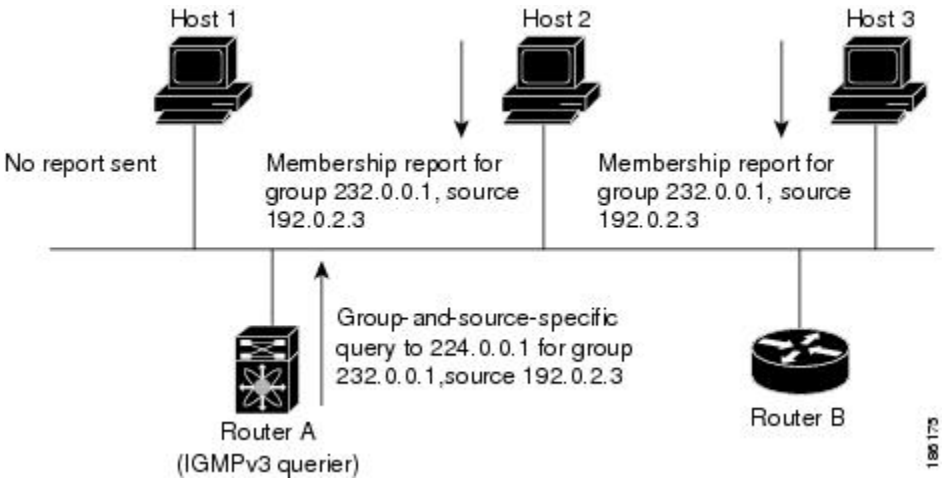
IP アドレスが最下位のルータが、サブネットの IGMP クエリアとして選出されます。 ルータは、自身よりも下位の IP アドレスを持つルータからクエリーメッセージを継続的に受信している間、クエリア タイムアウト値をカウントするタイマーをリセットします。 ルータのクエリア タイマーが期限切れになると、そのルータは代表クエリアになります。 そのあとで、このルータが、自身よりも下位の IP アドレスを持つルータからのホスト クエリー メッセージを受信すると、ルータは代表クエリアとしての役割をドロップしてクエリア タイマーを再度設定します。

この図では、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。 クエリーの最大応答時間パラメータを設定すると、ホストのランダムな応答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。

この図のルータ A は、IGMPv3 グループ/ソース固有のクエリーを 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。

図 *8*：*IGMPv3* グループ/ソース固有のクエリー



（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は、メッセージは転送されません。 IGMP の起動時に送信されるクエリー 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 クエリー 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 クエリー メッセージが送信されます。これにより、最終メンバーのクエリー応答インターバルと呼ばれる、ユーザ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緩和するには、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できます。

IGMP のライセンス要件

製品	ライセンス要件
Cisco NX-OS	IGMP にはライセンスは不要です。 ライセンス パッケージに含まれていない機能は nx-os イメージにバンドルされており、無料で提供されます。 Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

IGMP の前提条件

IGMP の前提条件は、次のとおりです。

- デバイスにログインしている。
- 現在の仮想ルーティングおよびフォワーディング（VRF）モードが正しい（グローバル コンフィギュレーション 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 のデフォルト設定

次の表に、IGMP パラメータのデフォルト設定を示します。

表 *2*：*IGMP* パラメータのデフォルト設定

パラメータ（Parameters）	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
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	ディセーブル

パラメータ（Parameters）	デフォルト
ルータ アラートの実施	ディセーブル
即時脱退	ディセーブル

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、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

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。 デフォルト値は 2 です。
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。 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。

パラメータ	説明
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。
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。 デフォルト値は 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ることで、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。 デフォルト値は 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。
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。

パラメータ	説明
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。 デフォルト値は 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。
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。 1
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。 （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。

パラメータ	説明
即時脱退	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 エントリを削除します。 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。

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

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)#`
		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** *interface*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	オプション / 説明 **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。 デフォルト値は 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。	次のコマンドを使用して、IGMP インターフェイス パラメータを設定します。

	コマンドまたはアクション		目的
	オプション	説明	
	ip igmp 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 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。	
	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。	
	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。	

コマンドまたはアクション		目的
オプション	**説明**	
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。 デフォルト値は 2 です。	
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。 デフォルト値は 2 です。	
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。	
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。	
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。	
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。	

	コマンドまたはアクション		目的
	オプション	説明	
	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。	
	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。 デフォルト値は 2 です。	
	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。	
	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。	
	ip igmp report-policy *policy* 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。	

	コマンドまたはアクション		目的
	オプション	説明	
	ip igmp access-group *policy* 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。	
	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 4	**show ip igmp interface** [*interface*] [**vrf** *vrf-name* | **all**] [**brief**] 例： `switch(config)# show ip igmp interface`		（任意） インターフェイスに関する IGMP 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 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

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。

マルチキャスト ホストが IGMPv3 をサポートしない場合、またはレイヤ 2 スイッチと相互運用するための（S、G）レポートではなくグループ結合を強制的に送信する場合に、IGMP SSM 変換機能は SSM ベースのマルチキャスト コア ネットワークを配置できるようにします。 IGMP SSM 変換機能には、同じ SSM グループに対して複数の送信元を設定する機能があります。 SSM 変換を設定する前に、Protocol Independent Multicast（PIM）をデバイスで設定する必要があります。

次の表に、SSM 変換の例を示します。

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
232.1.1.0/24	10.4.4.4

次の表に、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 プロセスによって作成される 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

	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**	**show running-configuration igmp** 例： `switch(config)# show running-configuration igmp`	（任意） **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示します。
ステップ **4**	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

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

	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	**[no] ip igmp enforce-router-alert** 例： `switch(config)# 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 チェックをイネーブルまたはディセーブルにします。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	**show running-configuration igmp** 例： `switch(config)# show running-configuration igmp`	（任意） 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	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

IGMP プロセスの再起動

IGMP 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。

手順

	コマンドまたはアクション	目的
ステップ 1	**restart igmp** 例： `switch# restart igmp`	IGMP プロセスを再起動します。

ステップ 2	**configure terminal**
	
	例：
	
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip igmp flush-routes** 例： `switch(config)# ip igmp flush-routes`	IGMP 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	**show running-configuration igmp** 例： `switch(config)# show running-configuration igmp`	（任意） 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 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

IGMP コンフィギュレーションの確認

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	説明
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。 IGMP が vPC モードの場合、vPC 統計情報を表示するには、このコマンドを使用します。
show ip igmp groups [{**source** [*group*]}] | {**group** [*source*]}] [**interface**] [**summary**] [**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 [{**source** [*group*]}] | {**group** [*source*]}] [**interface**] [**summary**] [**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 local-groups	IGMP ローカル グループ メンバーシップを表示します。

コマンド	説明
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。

IGMP の設定例

次に、IGMP パラメータの設定例を示します。

```
configure terminal
  ip igmp ssm-translate 232.0.0.0/8 10.1.1.1
  interface ethernet 2/1
    ip igmp version 3
    ip igmp join-group 230.0.0.0
    ip igmp startup-query-interval 25
    ip igmp startup-query-count 3
    ip igmp robustness-variable 3
    ip igmp querier-timeout 300
    ip igmp query-timeout 300
    ip igmp query-max-response-time 15
    ip igmp query-interval 100
    ip igmp last-member-query-response-time 3
    ip igmp last-member-query-count 3
    ip igmp group-timeout 300
    ip igmp report-link-local-groups
    ip igmp report-policy my_report_policy
    ip igmp access-group my_access_policy
```

第 4 章

PIM の設定

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

PIM について

マルチキャスト対応ルータ間で使用される PIM は、マルチキャスト配信ツリーを構築して、ルーティング ドメイン内にグループ メンバーシップをアドバタイズします。 PIM は、複数の送信元からのパケットが転送される共有配信ツリーと、単一の送信元からのパケットが転送される送信元配信ツリーを構築します。

Cisco NX-OS は、IPv4 ネットワーク（PIM）に対して 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 を設定できます。 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。

（注） Cisco NX-OS は、PIM デンス モードをサポートしていません。

Cisco NX-OS でマルチキャスト機能をイネーブルにするには、各ルータで PIM 機能をイネーブルにしてから、マルチキャストに参加する各インターフェイスで、PIM スパース モードをイネーブルに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。

PIM グローバル設定パラメータを使用して、マルチキャスト グループ アドレスの範囲を設定し、次の配信モードで処理されるようにします。

- 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。

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 プライオリティは、PIM hello メッセージの DR プライオリティ値に基づいて決まります。 全ルータの DR プライオリティ値が不明、またはプライオリティが等しい場合は、IP アドレスが最上位のルータが DR として選定されます。

hello メッセージには保持時間の値も含まれています。通常、この値は hello インターバルの 3.5 倍です。 ネイバーから後続の hello メッセージがないまま保持時間を経過すると、デバイスはそのリンクで 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。

Join/Prune メッセージ

DR が新しいグループの受信者または送信元から IGMP メンバーシップ レポート メッセージを受信すると、DR は、ランデブー ポイント（ASM モード）に向かってインターフェイスに PIM Join メッセージを送信することにより、受信者を送信元に接続するためのツリーを作成します。 ランデブー ポイント（RP）とは、ASM モードで PIM ドメイン内のすべての送信元およびホストにより使用される、共有ツリーのルートです。

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

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

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

Join/Prune メッセージは、ソフトウェアからできるだけ短時間で送信されます。 Join/Prune メッセージをフィルタリングするには、ルーティング ポリシーを定義します。

ステートのリフレッシュ

PIM では、3.5 分の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 を静的に設定できます。 この場合、ドメイン内のすべてのルータに RP のアドレスを設定する必要があります。

スタティック RP を定義するのは、次のような場合です。

- ルータに Anycast RP アドレスを設定する場合

- デバイスに RP を手動で設定する場合

BSR

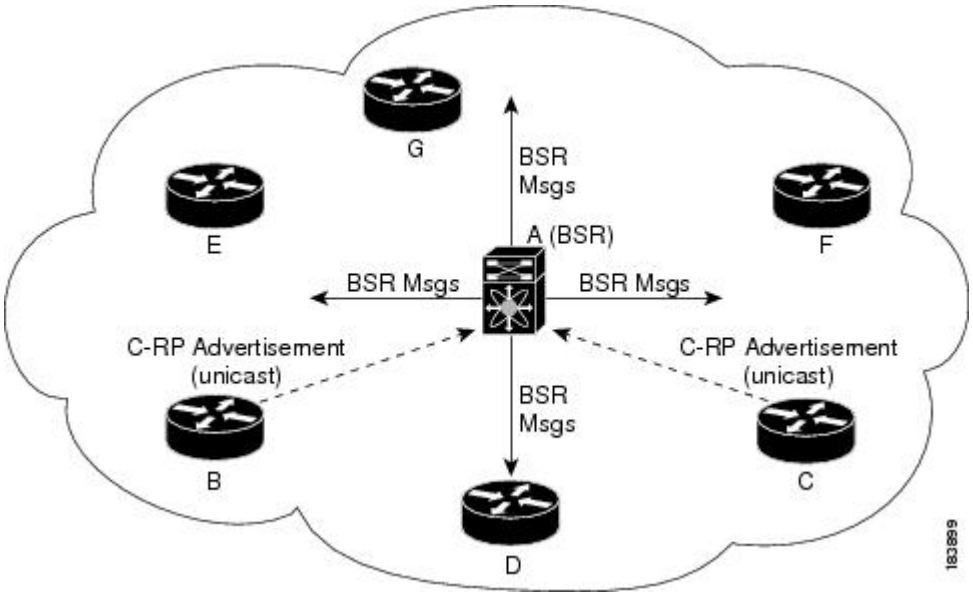
ブートストラップ ルータ（BSR）を使用すると、PIM ドメイン内のすべてのルータで、BSR と同じ RP キャッシュが保持されるようになります。 BSR では、BSR 候補 RP から RP セットを選択するよう設定できます。 BSR は、ドメイン内のすべてのルータに RP セットをブロードキャストする役割を果たします。 ドメイン内の RP を管理するには、1 つまたは複数の候補 BSR を選択します。 候補 BSR の 1 つが、ドメインの BSR として選定されます。

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

次の図に、BSR メカニズムを示します。 ルータ A（ソフトウェアによって選定された BSR）は、すべての有効なインターフェイスから BSR メッセージを送信しています（図の実線部分）。 このメッセージには RP セットが含まれており、ネットワーク内のすべてのルータに次々とフラッディングされます。 ルータ B および C は 候補 RP であり、選定された BSR に候補 RP アドバタイズメントを直接送信しています（図の破線部分）。

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

図 *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プライオリティが高い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があります。 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いません。 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。

ブートストラップ ルータの詳細については、RFC 5059 を参照してください。

（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。

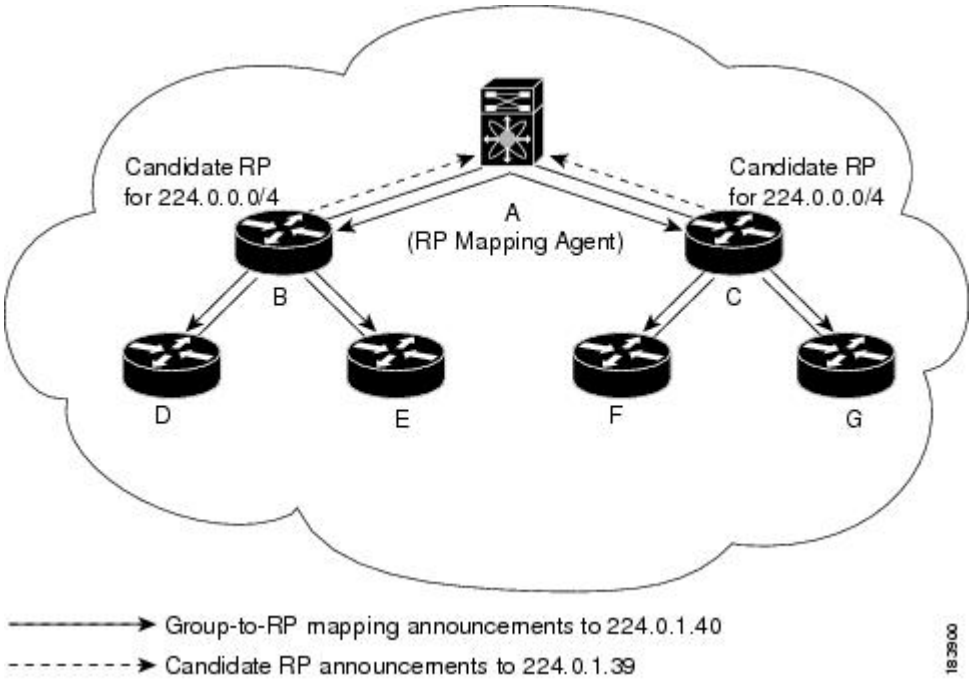
Auto-RP

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 メカニズムの前身として導入されたシスコのプロトコルです。 Auto-RP を設定するには、候補マッピング エージェントおよび候補 RP を選択します。 候補 RP は、サポート対象グループ範囲を含んだ RP-Announce メッセージを Cisco RP-Announce マルチキャスト グループ 224.0.1.39 に送信します。 Auto-RP マッピング エージェントは候補 RP からの RP-Announce メッセージを受信して、グループと RP 間のマッピング テーブルを形成します。 マッピング エージェントは、このグループと RP 間の マッピング テーブルを RP-Discovery メッセージに格納して、Cisco RP-Discovery マルチキャスト グループ 224.0.1.40 にマルチキャストします。

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

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

図 *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。

1 つの PIM ドメイン内の複数の RP

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

Anycast-RP

Anycast-RP の実装方式には、Multicast Source Discovery Protocol（MSDP）を使用する場合と、*RFC 4610*（『*Anycast-RP Using Protocol Independent Multicast (PIM)*』）に基づく場合の 2 種類があります。 ここでは、PIM Anycast-RP の設定方法について説明します。

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

ユニキャスト ルーティング プロトコルの機能に基づいて、PIM 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 は、PIM Anycast RP に使用されるループバック インターフェイス上に設定する必要があります。

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

PIM Register 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

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には、**ip pim register-source** コマンドを使用します。 このような状況は、受信したパケットが転送されないように送信元アドレスがフィルタリングされる場合、または送信元アドレスがネットワークに対して一意でない場合に発生します。 このような場合、RP から送信元アドレスへ送信される応答は DR に到達せず、Protocol Independent Multicast Sparse Mode（PIM-SM）プロトコル障害が発生します。

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

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

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

PIM Register メッセージをフィルタリングするには、ルーティング ポリシーを定義します。

指定ルータ

PIM の ASM モードでは、ソフトウェアは各ネットワーク セグメント上のルータの中から指定ルータ（DR）を選択します。 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。

各 LAN セグメントの DR は、「hello メッセージ」に記載された手順で決定されます。

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

ASM モードにおける共有ツリーから送信元ツリーへのスイッチオーバー

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

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

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

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

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 データの配信先を制限できます。 詳細については、RFC 2365 を参照してください。

インターフェイスを PIM 境界として設定し、PIM メッセージがこのインターフェイスから送信されないようにできます。

Auto-RP スコープ パラメータを使用すると、存続可能時間（TTL）値を設定できます。

PIM グレースフル リスタート

Protocol Independent Multicast（PIM）のグレースフル リスタートは、ルート プロセッサ（RP）スイッチオーバー後のマルチキャスト ルート（mroute）のコンバージェンスを向上するマルチキャ

スト ハイ アベイラビリティ（HA）の拡張です。 PIM のグレースフル リスタート機能では、RP スイッチオーバー時に、インターフェイス上の PIM ネイバーに、このインターフェイスをリバース パス転送（RPF）インターフェイスとして使用するすべての (*, G) および (S, G) 状態に対する PIM Join メッセージの送信をトリガーするためのメカニズムとして生成 ID（GenID）の値（RFC 4601 で規定）を使用します。 このメカニズムにより、PIM ネイバーでは、新しくアクティブになった RP 上でこれらの状態を即座に再確立できます。

生成 ID

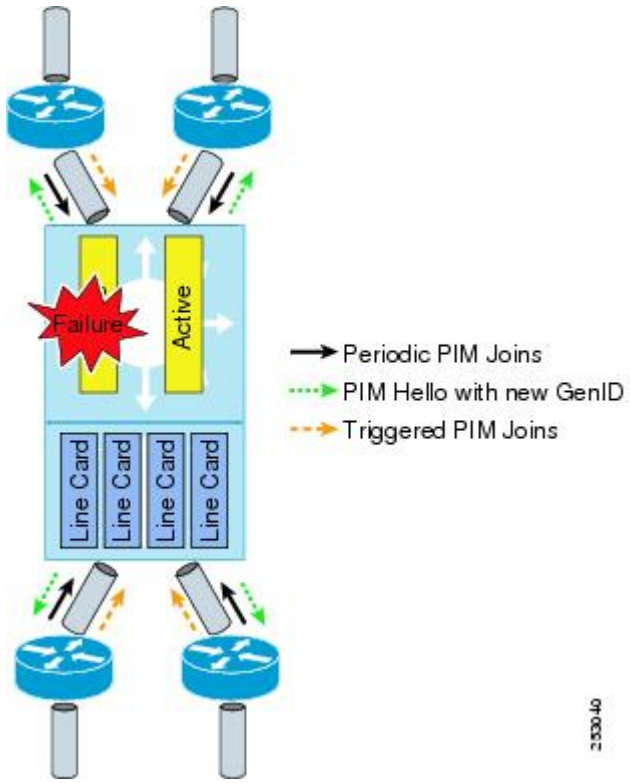
生成 ID（GenID）は、インターフェイスで Protocol Independent Multicast（PIM）転送が開始または再開されるたびに生成し直される、ランダムに生成された 32 ビット値です。 PIM hello メッセージ内の GenID 値を処理するために、PIM ネイバーでは、RFC 4601 に準拠する PIM を実装した Cisco ソフトウェアを実行している必要があります。

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

PIM グレースフル リスタート動作

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

図 *11*：*RP* スイッチオーバー中の *PIM* グレースフル リスタート動作



PIM グレースフル リスタート動作は次のとおりです。

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

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

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

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

ハイ アベイラビリティ

ハイ アベイラビリティの詳細については、『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』を参照してください。

PIM のライセンス要件

製品	ライセンス要件
Cisco NX-OS	PIM には Enterprise Services ライセンスが必要です。 Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。

PIM の前提条件

PIM の前提条件は次のとおりです。

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

PIM 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。

- ほとんどの Cisco Nexus デバイスでは、RPF 障害トラフィックはドロップされ、PIM アサートを発生するために非常に低レートで CPU に送信されます。 Cisco Nexus 9000 シリーズ スイッチの場合、RPF 障害のトラフィックは、マルチキャスト送信元を学習するために、常に CPU にコピーされます。
- ほとんどの Cisco Nexus デバイスのファーストホップ ソース検出では、ファースト ホップからのトラフィックは送信元サブネット チェックに基づいて検出され、送信元がローカル サブネットに属する場合に限り、マルチキャスト パケットが CPU にコピーされます。 Cisco Nexus 9000 シリーズ スイッチではローカル送信元を検出できないため、マルチキャスト パケットは、ローカル マルチキャスト送信元を学習するためにスーパーバイザに送信されます。
- Cisco NX-OS PIM は、PIM デンス モードのすべてのモード、または PIM スパース モードのバージョン 1 と相互運用しません。
- 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。
- デバイスに BSR ポリシーが適用されており、BSR として選定されないように設定されている場合、このポリシーは無視されます。 これにより、次のようなデメリットが発生します。
  - ポリシーで許可されている BSM をデバイスが受信した場合、意図に反してこのデバイスが BSR に選定されていると、対象の BSM がドロップされるために下流のルータではその BSM を受信できなくなります。 また、下流のデバイスでは、不正な BSR から送信された BSM が正しくフィルタリングされるため、これらのデバイスでは RP 情報を受信できなくなります。
  - BSR に異なるデバイスから送られた BSM が着信すると、新しい BSM が送信されますが、その正規の BSM は下流のデバイスでは受信されません。
- PIM hello 間隔のデフォルト値が推奨されます。この値は変更しないでください。
- Cisco NX-OS PIM は、vPC 上の SSM をサポートしませんが、Cisco NX-OS PIM は vPC 上の ASM をサポートします。

（注） Cisco Nexus 9000 シリーズ スイッチが PIM SSM をサポートしていなくても、PIM SSM コマンドがソフトウェアで表示される場合があります。 PIM SSM を設定しようとしても、設定はアクティブになりません。

デフォルト設定

次の表に、PIM パラメータのデフォルト設定を示します。

表 *6* : ***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	ディセーブル
再起動時にルートをフラッシュ	ディセーブル
ログ ネイバーの変更	ディセーブル
Auto-RP メッセージ アクション	ディセーブル
BSR メッセージ アクション	ディセーブル
PIM スパース モード	ディセーブル
DR プライオリティ	1
hello 認証モード	ディセーブル
ドメイン境界	ディセーブル
RP アドレス ポリシー	メッセージをフィルタリングしない
PIM Register メッセージ ポリシー	メッセージをフィルタリングしない
BSR 候補 RP ポリシー	メッセージをフィルタリングしない
BSR ポリシー	メッセージをフィルタリングしない
Auto-RP マッピング エージェント ポリシー	メッセージをフィルタリングしない
Auto-RP 候補 RP ポリシー	メッセージをフィルタリングしない
Join/Prune ポリシー	メッセージをフィルタリングしない
ネイバーとの隣接関係ポリシー	すべての PIM ネイバーと隣接関係を確立
BFD	ディセーブル

PIM の設定

PIM は、各インターフェイスに設定できます。

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

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設定できます（次の表を参照）。

マルチキャスト配信モード	RP 設定の必要性	説明
ASM	Yes	任意の送信元のマルチキャスト
マルチキャスト用 RPF ルート	No	マルチキャスト用 RPF ルート

PIM の設定作業

次の手順で PIM を設定します。

1. 各マルチキャスト配信モードで設定するマルチキャスト グループの範囲を選択します。
2. PIM をイネーブルにします。
3. ステップ 1 で選択したマルチキャスト配信モードについて、次の設定作業を行います。
   - ASM モードについては、「ASM の設定」を参照してください。
   - マルチキャスト用 RPF ルートについては、「マルチキャスト用 RPF ルートの設定」を参照してください。
4. メッセージ フィルタリングを設定します。

（注） 次の CLI コマンドを使用して PIM を設定します。

- 設定コマンドは、**ip pim** で始まります。
- 表示コマンドは、**show ip pim** で始まります。

（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。

PIM 機能のイネーブル化

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。

はじめる前に

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

手順

	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	**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	**show running-configuration pim** 例： `switch(config)# show running-configuration pim`	（任意） PIM の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`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

PIM スパース モード パラメータの設定

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

表 *7*：*PIM* スパース モードのパラメータ

パラメータ	説明
デバイスにグローバルに適用	

パラメータ	説明
Auto-RP メッセージ アクション	Auto-RP メッセージの待ち受けと転送をイネーブルにします。 これらの機能はデフォルトではディセーブルになっているため、候補RPまたはマッピング エージェントとして設定されていないルータは、Auto-RP メッセージの受信と転送を行いません。
BSR メッセージ アクション	BSR メッセージの待ち受けと転送をイネーブルにします。 これらの機能はデフォルトではディセーブルになっているため、候補 RP または BSR 候補として設定されていないルータは、BSR メッセージの受信と転送を行いません。
Register のレート制限	IPv4 Register のレート制限を毎秒のパケット数で設定します。 範囲は 1 ～ 65,535 です。 デフォルト設定は無制限です。
初期ホールドダウン期間	IPv4 の初期ホールドダウン期間を秒単位で設定します。 このホールドダウン期間は、MRIBが最初に起動するのにかかる時間です。 コンバージェンスを高速化するには、小さい値を入力します。 範囲は 90 ～ 210 です。 ホールドダウン期間をディセーブルにするには、0 を指定します。 デフォルトは 210 です。
デバイスの各インターフェイスに適用	
PIM スパース モード	インターフェイスで PIM をイネーブルにします。
DR プライオリティ	現在のインターフェイスに、PIM hello メッセージの一部としてアドバタイズされる指定ルータ（DR）プライオリティを設定します。 複数の PIM 対応ルータが存在するマルチアクセス ネットワークでは、DR プライオリティの最も高いルータが DR ルータとして選定されます。 プライオリティが等しい場合は、IP アドレスが最上位のルータが DR に選定されます。 DR は、直接接続されたマルチキャスト送信元に PIM Register メッセージを送信するとともに、直接接続された受信者に代わって、ランデブー ポイント（RP）方向に PIM Join メッセージを送信します。 有効範囲は 1 ～ 4294967295 です。 デフォルトは 1 です。
指定ルータの遅延	PIM hello メッセージでアドバタイズされる DR プライオリティを指定期間にわたり 0 に設定することで、指定ルータ（DR）の選定への参加を遅延させます。 この遅延中、DR は変更されず、現在のスイッチにはそのインターフェイスでのすべてのマルチキャストの状態を把握する時間が与えられます。 遅延期間が終了すると、DR 選出を再び開始するために、正しい DR プライオリティが hello パケットで送信されます。 値の範囲は 3 ～ 0xffff 秒です。

パラメータ	説明
hello 認証モード	インターフェイスで、PIM hello メッセージ内の MD5 ハッシュ認証キー（パスワード）をイネーブルにして、直接接続されたネイバーによる相互認証を可能にします。 PIM hello メッセージは、認証ヘッダー（AH）オプションを使用して符号化された IP セキュリティ です。 暗号化されていない（クリアテキストの）キーか、または次に示す値のいずれかを入力したあと、スペースと MD5 認証キーを入力します。 • 0：暗号化されていない（クリアテキストの）キーを指定します。 • 3：3-DES 暗号化キーを指定します。 • 7：Cisco Type 7 暗号化キーを指定します。 認証キーの文字数は最大 16 文字です。 デフォルトではディセーブルになっています。
hello 間隔	hello メッセージの送信インターバルを、ミリ秒単位で設定します。 範囲は 1000 ～ 18724286 です。 デフォルトは 30000 です。 （注） このパラメータの確認された範囲および関連付けられた PIM ネイバー スケールについては、『*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*』を参照してください。
ドメイン境界	インターフェイスを PIM ドメインの境界として設定し、対象のインターフェイスで、ブートストラップ、候補 RP、または Auto-RP の各メッセージが送受信されないようにします。 デフォルトではディセーブルになっています。
ネイバー ポリシー	ルートマップ ポリシーに基づいて PIM ネイバーの隣接関係を設定します。[2] 隣接関係は、**match ip** address コマンドを使用して IP アドレスで指定できます。 指定したポリシー名が存在しない場合、または IP アドレスがポリシー内で設定されていない場合は、すべてのネイバーとの隣接関係が確立されます。 デフォルトでは、すべての PIM ネイバーと隣接関係が確立されます。 （注） この機能の設定は、経験を積んだネットワーク管理者が行うことを推奨します。

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

PIM スパース モード パラメータの設定

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 pim auto-rp** {**listen** [**forward**] | **forward** [**listen**]} 例： `switch(config)# ip pim auto-rp listen`	（任意） 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 メッセージの受信または転送は行われません。
ステップ 3	**ip pim bsr** {**listen** [**forward**] | **forward** [**listen**]} 例： `switch(config)# ip pim bsr forward`	（任意） 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 メッセージの受信または転送は行われません。
ステップ 4	**ip pim register-rate-limit** *rate* 例： `switch(config)# ip pim register-rate-limit 1000`	（任意） レート制限を毎秒のパケット数で設定します。 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 5	**ip pim spt-threshold infinity group-list** *route-map-name* 例： `switch(config)# ip pim spt-threshold infinity group-list my_route-map-name`	（任意） 指定されたルート マップで定義されているグループ プレフィックスに対して、IPv4 PIM（*, G）状態のみを作成します。 Cisco NX-OS Release 3.1 は最大 1000 のルート マップ エントリを、Release 3.1 以前の Cisco NX-OS は最大 500 のルート マップ エントリをサポートします。 このコマンドは、仮想ポート チャネル（vPC/vPC+）にはサポートされません。 （注） **ip pim use-shared-tree-only group-list** コマンドは、**ip pim spt-threshold infinity group-list** コマンドと同じ機能を実行します。 この手順を行うには、いずれかのコマンドを使用できます。

	コマンドまたはアクション	目的
ステップ 6	**[ip | ipv4] routing multicast holddown** *holddown-period* 例： `switch(config)# ip routing multicast holddown 100`	（任意） 初期ホールドダウン期間を秒単位で設定します。 範囲は 90 ～ 210 です。 ホールドダウン期間をディセーブルにするには、0 を指定します。 デフォルトは 210 です。
ステップ 7	**show running-configuration pim** 例： `switch(config)# show running-configuration pim`	（任意） PIM 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)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 9	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	現在のインターフェイスで PIM スパース モードをイネーブルにします。 デフォルトではディセーブルになっています。
ステップ 10	**ip pim dr-priority** *priority* 例： `switch(config-if)# ip pim dr-priority 192`	（任意） PIM hello メッセージの一部としてアドバタイズされる指定ルータ（DR）プライオリティを設定します。 有効範囲は 1 ～ 4294967295 です。 デフォルトは 1 です。
ステップ 11	**ip pim dr-delay** *delay* 例： `switch(config-if)# ip pim dr-delay 3`	（任意） PIM hello メッセージでアドバタイズされる DR プライオリティを指定期間にわたり 0 に設定することで、指定ルータ（DR）の選定への参加を遅延させます。 この遅延中、DR は変更されず、現在のスイッチにはそのインターフェイスでのすべてのマルチキャストの状態を把握する時間が与えられます。 遅延期間が終了すると、DR 選出を再び開始するために、正しい DR プライオリティが hello パケットで送信されます。 値の範囲は 3 ～ 0xffff 秒です。 （注） このコマンドは、起動時にのみ、または IP アドレスかインターフェイスの状態が変更された後にのみ、DR 選定に参加することを遅延させます。 これは、マルチキャスト アクセスの非 vPC レイヤ 3 インターフェイス専用です。

	コマンドまたはアクション	目的
ステップ 12	**ip pim hello-authentication ah-md5** *auth-key* 例： `switch(config-if)# ip pim hello-authentication ah-md5 my_key`	（任意） PIM hello メッセージ内の MD5 ハッシュ認証キーをイネーブルにします。暗号化されていない（クリアテキストの）キーか、または次に示す値のいずれかを入力したあと、スペースと MD5 認証キーを入力します。 • 0：暗号化されていない（クリアテキストの）キーを指定します。 • 3：3-DES 暗号化キーを指定します。 • 7：Cisco Type 7 暗号化キーを指定します。 キーの文字数は最大 16 文字です。デフォルトではディセーブルになっています。
ステップ 13	**ip pim hello-interval** *interval* 例： `switch(config-if)# ip pim hello-interval 25000`	（任意） hello メッセージの送信インターバルを、ミリ秒単位で設定します。 範囲は 1000 ～ 18724286 です。 デフォルトは 30000 です。 （注） 最小値は 1 ミリ秒です。
ステップ 14	**ip pim border** 例： `switch(config-if)# ip pim border`	（任意） 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	**ip pim neighbor-policy** *policy-name* 例： `switch(config-if)# ip pim neighbor-policy my_neighbor_policy`	（任意） 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。 **match ip address** コマンドを使用し、ルートマップ ポリシーに基づいて PIM ネイバーの隣接関係も設定します。 ポリシー名の文字数は最大 63 文字です。 デフォルトでは、すべての PIM ネイバーと隣接関係が確立されます。 （注） この機能の設定は、経験を積んだネットワーク管理者のみが行うことを推奨します。

	コマンドまたはアクション	目的
ステップ 16	**show ip pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**] 例： `switch(config-if)# show ip pim interface`	（任意） PIM インターフェイスの情報を表示します。
ステップ 17	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ASM の設定

Any Source Multicast（ASM）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 モードを有効にするには、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。

スタティック RP の設定

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

match ip multicast コマンドで、使用するグループ プレフィックスを示すルートマップ ポリシー名を指定できます。

ip pim rp-address コマンドは、次の機能を追加して拡張されました。

- 既存のルート マップ方式の他に設定のプレフィックス リスト方式が追加されました。
- ポリシー アクションのサポートが追加されました（ルート マップまたはプレフィックス リスト）。

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

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

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

スタティック RP の設定

はじめる前に

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)#`
		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 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** コマンドで、使用するグループ プレフィックスを示すルートマップ ポリシー名を指定できます。 モードは ASM です。 デフォルトのグループ範囲は ff00::0/8 です。 この例では、指定したグループ範囲に PIM ASM モードを設定しています。
ステップ 3	**show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] 例： `switch(config)# show ip pim group-range`	（任意） 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 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

BSR の設定

BSR を設定するには、候補 BSR および候補 RP を選択します。

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

候補 BSR の設定では、引数を指定できます（次の表を参照）。

表 *8*：候補 *BSR* の引数

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

BSR 候補 RP の引数およびキーワードの設定

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

表 *9*：*BSR* 候補 *RP* の引数およびキーワード

引数またはキーワード	説明
interface	ブートストラップ メッセージで使用する、BSR 送信元 IP アドレスを取得するためのインターフェイス タイプおよび番号。
group-list *ip-prefix*	プレフィックス形式で指定された、この RP によって処理されるマルチキャスト グループ。

引数またはキーワード	説明
間隔	候補 RP メッセージの送信間隔（秒）。 この値の範囲は 1 ～ 65,535 であり、デフォルト値は 60 秒です。 （注） 候補 RP インターバルは 15 秒以上に設定することを推奨します。
priority	現在の RP に割り当てられたプライオリティ。 ソフトウェアにより、グループ範囲内でプライオリティが最も高い RP が選定されます。プライオリティが等しい場合は、IP アドレスが最上位の RP が選定されます。 （最も小さい数値が最も高いプライオリティになります）。この値の範囲は 0（最も高いプライオリティ）～ 255 で、デフォルトは 192 です。 （注） このプライオリティは BSR 候補プライオリティとは異なります。BSR 候補プライオリティは、0 ～ 255 の間で、高い値ほどプライオリティが高くなります。
route-map *policy-name*	この機能を適用するグループ プレフィックスを定義するルートマップ ポリシー名です。

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

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

候補 BSR および候補 RP を設定する手順は、次のとおりです。

1. PIM ドメインの各ルータで BSR メッセージの受信と転送を行うかどうかを設定します。 候補 RP または候補 BSR として設定されたルータは、インターフェイスにドメイン境界機能が設定されていない場合、すべてのブートストラップ ルータ プロトコル メッセージの受信と転送を自動的に実行します。
2. 候補 BSR および候補 RP として動作するルータを選択します。
3. 後述の手順に従い、候補 BSR および候補 RP をそれぞれ設定します。
4. BSR メッセージ フィルタリングを設定します。

BSR の設定

はじめる前に

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)#`
		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 pim bsr** {**forward** [**listen**] | **listen** [**forward**]} 例： `switch(config)# ip pim bsr listen forward`	リッスンと転送を設定します。 リモート PE 上の各 VRF で確実にこのコマンドを入力してください。
ステップ 3	**ip pim bsr** [**bsr-candidate**] *interface* [**hash-len** *hash-length*] [**priority** *priority*] 例： `switch(config)# ip pim bsr-candidate ethernet 2/1 hash-len 24`	候補ブートストラップ ルータ（BSP）を設定します。 ブートストラップ メッセージで使用される送信元 IP アドレスは、インターフェイスの IP アドレスです。 ハッシュ長は 0 ～ 32 であり、デフォルト値は 30 です。 プライオリティは 0 ～ 255 であり、デフォルト値は 64 です。
ステップ 4	**ip** [**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`	（任意） BSR の候補 RP を設定します。 プライオリティは 0（プライオリティが最大）～ 65,535 であり、デフォルト値は 192 です。 インターバルは 1 ～ 65,535 秒であり、デフォルト値は 60 秒です。 （注） 候補 RP インターバルは 15 秒以上に設定することを推奨します。 この例では、ASM の候補 RP を設定しています。
ステップ 5	**show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] 例： `switch(config)# show ip pim group-range`	（任意） PIM モードおよび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 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Auto-RP の設定

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

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

Auto-RP マッピング エージェントの設定では、引数を指定できます（次の表を参照）。

表 *10*：*Auto-RP* マッピング エージェントの引数

引数	説明
interface	ブートストラップ メッセージで使用する、Auto-RP マッピング エージェントの IP アドレスを取得するためのインターフェイス タイプおよび番号。
scope *ttl*	RP-Discovery メッセージが転送される最大ホップ数を表す存続可能時間（TTL）値。 この値の範囲は 1 ～ 255 であり、デフォルト値は 32 です。

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

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

表 *11*：*Auto-RP* 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、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。

引数またはキーワード	説明
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。
間隔	RP-Announce メッセージの送信間隔（秒）。 この値の範囲は 1 ～ 65,535 であり、デフォルト値は 60 です。 （注） 候補 RP インターバルは 15 秒以上に設定することを推奨します。
route-map *policy-name*	この機能を適用するグループプレフィックスを定義するルートマップポリシー名です。

ヒント 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。
2. マッピング エージェントおよび候補 RP として動作するルータを選択します。
3. 後述の手順に従い、マッピング エージェントおよび候補 RP をそれぞれ設定します。
4. Auto-RP メッセージ フィルタリングを設定します。

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

Auto RP の設定

はじめる前に

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)#`
		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 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。
ステップ 3	**ip pim** {**send-rp-announce** | **auto-rp rp-candidate**} *interface* {**group-list** *ip-prefix* | **route_map** *policy-name*} [**scope** *ttl*] **interval** *interval*] 例： `switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24`	Auto-RP の候補 RP を設定します。 デフォルト スコープは 32 です。 デフォルト インターバルは 60 秒です。 デフォルトでは、ASM の候補 RP が作成されます。 （注） 候補 RP インターバルは 15 秒以上に設定することを推奨します。 この例では、ASM の候補 RP を設定しています。
ステップ 4	**show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] 例： `switch(config)# show ip pim group-range`	（任意） PIM モードおよびグループ範囲を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

PIM Anycast-RP セットの設定

PIM Anycast-RP セットを設定する手順は、次のとおりです。

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

PIM Anycast RP セットの設定

はじめる前に

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)#`
		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`	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 192.0.2.3/32`	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	**ip pim sparse-mode** 例： `switch(config)# ip pim sparse-mode`	PIM をイネーブルにします。
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	RP セットに属する各 RP（ローカル ルータを含む）で、同じ Anycast-RP アドレスを使用してステップ 5 を繰り返します。	—
ステップ 7	**show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] 例： `switch(config)# show ip pim group-range`	（任意） 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

	コマンドまたはアクション	目的
		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 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ASM 専用の共有ツリーの設定

共有ツリーを設定できるのは、Any Source Multicast（ASM）グループの最終ホップ ルータだけです。この場合、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 multicast** コマンドで、共有ツリーを適用するグループ範囲を指定できます。 このオプションは、送信元ツリーに対する Join/Prune メッセージを受信した場合の、ルータの標準動作には影響を与えません。

（注） Cisco NX-OS ソフトウェアは、vPC での共有ツリー機能をサポートしません。 vPC の詳細については、『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

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

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

ASM 専用の共有ツリーの設定

はじめる前に

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)#`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 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。
ステップ 3	**show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name*] 例： `switch(config)# show ip pim group-range`	（任意） PIM モードおよびグループ範囲を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

マルチキャスト用 RPF ルートの設定

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

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

はじめる前に

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)#`
		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 mroute** {*ip-addr mask* | *ip-prefix*} {*next-hop* | *nh-prefix* | *interface*} [*route-preference*] [**vrf** *vrf-name*] 例： `switch(config)# ip mroute 192.0.2.33/1 224.0.0.0/1`	RPF 計算で使用するマルチキャスト用 RPF ルートを設定します。 ルート プリファレンスは 1 ～ 255 です。 デフォルト プリファレンスは 1 です。
ステップ 3	**show ip static-route** [**multicast**] [**vrf** *vrf-name*] 例： `switch(config)# show ip static-route multicast`	（任意） 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	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

マルチキャスト マルチパスのディセーブル化

デフォルトでは、使用可能な複数の ECMP パスがある場合、マルチキャストの RPF インターフェイスが自動的に選択されます。 自動選択をディセーブルにすると、マルチキャストに単一の RPF インターフェイスを指定することができます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ip multicast multipath** {**none** | **s-g-hash next-hop-based**} 例： `switch(config)# ip multicast multipath none`	マルチキャスト マルチパスをディセーブルにするか、デフォルトの (S/RP G) ベースのハッシュの代わりに (S, G, Nexthop) に基づいてハッシュを開始します。
ステップ 3	**clear ip mroute *** 例： `switch(config)# clear ip mroute *`	マルチパス ルートをクリアし、マルチキャスト マルチパス抑制をアクティブにします。

RP 情報配信を制御するルート マップの設定

ルート マップは、一部の RP 設定のミスや悪意のある攻撃に対する保護機能を提供します。

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

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。

RP 情報配信を制御するルート マップの設定

手順

	コマンドまたはアクション	目的

ステップ 1	**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	**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。

	コマンドまたはアクション	目的
ステップ 3	**match ip multicast** {**rp** *ip-address* [**rp-type** *rp-type*]} {{**group-range** {*gadrr_start* **to** *gadrr_end*} | {**group ip-prefix**}} {**source** *source-ip-address*} 例： `switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type ASM`	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）を指定できます。 例で示すとおり、このコンフィギュレーション方式では、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 または deny 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	**show route-map** 例： `switch(config-route-map)# show route-map`	（任意） 設定されたルート マップを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-route-map)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

メッセージ フィルタリングの設定

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

以下の表に示す PIM メッセージのフィルタリングを設定できます。

表 *12*：*PIM* メッセージのフィルタリング

メッセージ タイプ	説明
デバイスにグローバルに適用	
ネイバーの変更の記録	ネイバーのステート変更を通知する Syslog メッセージをイネーブルにします。 デフォルトではディセーブルになっています。

メッセージ タイプ	説明
PIM Register ポリシー	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。[3] ここでは、**match ip** multicast コマンドで、グループ アドレスまたはグループと送信元アドレスを指定できます。 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、ルータによる BSR 候補 RP メッセージのフィルタリングをイネーブルにします。ここでは、**match ip** コマンドで、RP およびグループ アドレスを指定できます。 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。ここでは、**match ip** 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 ポリシーに基づく、Auto-RP マッピング エージェントによる Auto-RP Announce メッセージのフィルタリングをイネーブルにします。ここでは、**match ip multicast** コマンドで、RP およびグループ アドレスを指定できます。 このコマンドは、マッピング エージェントで使用できます。 デフォルトでは、Auto-RP メッセージはフィルタリングされません。
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。
デバイスの各インターフェイスに適用	
Join/Prune ポリシー	ルートマップ ポリシーに基づく、Join/Prune メッセージのフィルタリングをイネーブルにします。ここでは、**match ip** 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。

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

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

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

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

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

メッセージ フィルタリング（PIM）の設定

はじめる前に

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)#`
		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 pim log-neighbor-changes** 例： `switch(config)# ip pim log-neighbor-changes`	（任意） 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。

	コマンドまたはアクション	目的
ステップ 3	**ip pim register-policy** *policy-name* 例： `switch(config)# ip pim register-policy my_register_policy`	（任意） ルートマップ ポリシーに基づく、PIM Register メッセージのフィルタリングをイネーブルにします。**match ip multicast** コマンドで、グループ アドレスまたはグループと送信元アドレスを指定できます。
ステップ 4	**ip pim bsr rp-candidate-policy** *policy-name* 例： `switch(config)# ip pim bsr rp-candidate-policy my_bsr_rp_candidate_policy`	（任意） ルートマップ ポリシーに基づいてルータが BSR 候補 RP メッセージをフィルタリングできるようにします。**match ip multicast** コマンドで、RP、グループ アドレスを指定できます。 このコマンドは、BSR の選定対象のルータで使用できます。 デフォルトでは、BSR メッセージはフィルタリングされません。
ステップ 5	**ip pim bsr bsr-policy** *policy-name* 例： `switch(config)# ip pim bsr bsr-policy my_bsr_policy`	（任意） 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 6	**ip pim auto-rp rp-candidate-policy** *policy-name* 例： `switch(config)# ip pim auto-rp rp-candidate-policy my_auto_rp_candidate_policy`	（任意） ルートマップ ポリシーに基づく、Auto-RP マッピング エージェントによる Auto-RP Announce メッセージのフィルタリングをイネーブルにします。**match ip multicast** コマンドで、RP、グループ アドレスを指定できます。 このコマンドは、マッピング エージェントで使用できます。 デフォルトでは、Auto-RP メッセージはフィルタリングされません。
ステップ 7	**ip pim auto-rp mapping-agent-policy** *policy-name* 例： `switch(config)# ip pim auto-rp mapping-agent-policy my_auto_rp_mapping_policy`	（任意） 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。

	コマンドまたはアクション	目的

ステップ 8	**interface** *interface*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		指定したインターフェイスでインターフェイス モードを開始します。

ステップ 9	**ip pim jp-policy** *policy-name* [**in** | **out**] 例： `switch(config-if)# ip pim jp-policy my_jp_policy`	（任意） ルートマップ ポリシーに基づく、Join/Prune メッセージのフィルタリングをイネーブルにします。**match ip multicast** コマンドで、グループ、グループと送信元、またはグループと RP アドレスを指定できます。デフォルトでは、Join/Prune メッセージはフィルタリングされません。
ステップ 10	**show run pim** 例： `switch(config-if)# show run pim`	（任意） PIM コンフィギュレーション コマンドを表示します。
ステップ 11	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

PIM プロセスの再起動

PIMプロセスを再起動し、オプションとして、すべてのルートをフラッシュすることができます。デフォルトでは、ルートはフラッシュされません。

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

PIM を再起動すると、次の処理が実行されます。

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

PIM プロセスの再起動

はじめる前に

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	**restart pim** 例： `switch# restart pim`	PIM プロセスを再起動します。

ステップ 2	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 3	**ip pim flush-routes** 例： `switch(config)# ip pim flush-routes`	PIM プロセスの再起動時に、ルートを削除します。デフォルトでは、ルートはフラッシュされません。
ステップ 4	**show running-configuration pim** 例： `switch(config)# show running-configuration pim`	（任意） **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 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VRF モードでの PIM の BFD の設定

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

はじめる前に

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

手順

	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	**vrf context** *vrf-name*
	
	例：
	`switch# vrf context test`
	`switch(config-vrf)#`
		VRF コンフィギュレーション モードを開始します。

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

インターフェイス モードでの PIM の BFD の設定

はじめる前に

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

手順

	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。

	コマンドまたはアクション	目的

ステップ 2	**interface** *interface-type*
	
	例：
	`switch(config)# interface ethernet 7/40`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

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

PIM の設定の確認

PIM の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	説明
show ip mroute	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 df [**vrf** *vrf-name*]	各 RP の Designated Forwarder（DF）情報をインターフェイス別に表示します。

コマンド	説明
show ip pim group-range [**vrf** *vrf-name*]	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*]	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*]	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*]	発信インターフェイス（OIF）リスト内のすべてのインターフェイスを表示します。
show ip pim route [*source group* | *group* [*source*]][**vrf** *vrf-name*]	各マルチキャスト ルートの情報を表示します。指定した (S, G) に対して、PIM Join メッセージを受信したインターフェイスなどを表示できます。
show ip pim rp [**vrf** *vrf-name*]	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 *group-address*	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。 RP ハッシュの詳細については、RFC 5059 を参照してください。
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。

コマンド	説明
show startup-configuration pim	スタートアップ コンフィギュレーション情報を表示します。
show ip pim vrf [*vrf-name* | **all**] [**detail**]	各 VRF の情報を表示します。

統計情報の表示

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

PIM の統計情報の表示

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

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。
show ip pim statistics [**vrf** *vrf-name*]	グローバル統計情報を表示します。

PIM の統計情報のクリア

これらのコマンドを使用すると、PIM 統計情報をクリアできます。

コマンド	説明
clear ip pim interface statistics *interface*	指定したインターフェイスのカウンタをクリアします。
clear ip 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*]	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。

BSR の設定例

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

1. ドメインに参加させるインターフェイスで PIM スパース モード パラメータを設定します。 すべてのインターフェイスで PIM をイネーブルにすることを推奨します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim sparse-mode
```

2. ルータが BSR メッセージの受信と転送を行うかどうかを設定します。

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

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

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

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

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

5. メッセージ フィルタリングを設定します。

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

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

```
configure terminal
  interface ethernet 2/1
    ip pim sparse-mode
    exit
  ip pim bsr forward listen
ip pim bsr-candidate ethernet 2/1 hash-len 30
  ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24
  ip pim log-neighbor-changes
```

PIM Anycast RP の設定例

PIM Anycast-RP 方式を使用して ASM モードを設定するには、PIM ドメイン内の各ルータで、次の手順を実行します。

1. ドメインに参加させるインターフェイスで PIM スパース モード パラメータを設定します。 すべてのインターフェイスで PIM をイネーブルにすることを推奨します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip pim sparse-mode
```

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

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

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

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

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

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

5. メッセージ フィルタリングを設定します。

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

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

```
configure terminal
interface ethernet 2/1
ip pim sparse-mode
exit
interface loopback 0
ip address 192.0.2.3/32
exit
ip pim anycast-rp 192.0.2.3 192.0.2.31
ip pim anycast-rp 192.0.2.3 192.0.2.32
ip pim log-neighbor-changes
```

Prefix-Based および Route-Map-Based の設定

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

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

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

ip pim rp-address 172.21.0.11 prefix-list plist11
ip pim rp-address 172.21.0.22 prefix-list plist22
ip pim rp-address 172.21.0.33 prefix-list plist33
route-map rmap11 deny 10
 match ip multicast group 231.129.128.0/17
route-map rmap11 deny 20
 match ip multicast group 231.129.0.0/16
route-map rmap11 deny 30
 match ip multicast group 231.128.0.0/9
route-map rmap11 permit 40
 match ip multicast group 231.0.0.0/8

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

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

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

出力

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

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

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

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

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

(*, 231.129.1.1/32), uptime: 00:14:25, igmp pim ip
  Incoming interface: Ethernet2/1, RPF nbr: 10.165.20.1
  Outgoing interface list: (count: 1)
    loopback1, uptime: 00:14:25, igmp

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

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

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

関連資料

関連項目	参照先
VRF の設定	『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』

Standards

Standards	Title
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 リンク
PIM に関連した MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

第 5 章

IGMP スヌーピングの設定

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）スヌーピングを設定する方法を説明します。

IGMP スヌーピングについて

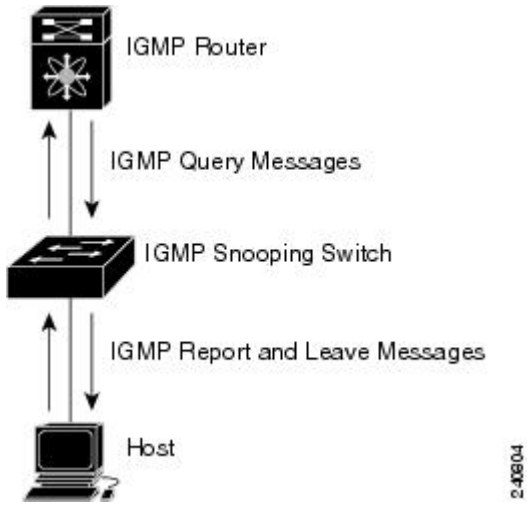
（注） デバイスの IGMP スヌーピングはディセーブルにしないことを推奨します。 IGMP スヌーピングをディセーブルにすると、デバイス内で不正なフラッディングが過度に発生し、マルチキャストのパフォーマンスが低下する場合があります。

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 トラフィックを調べて、該当する受信側が入っているポートを検出します。 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。 デバイスでは、IGMP スヌーピングがデフォルトでイネーブルになっています。

この図に、ホストと IGMP ルータ間に設置された 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 *12*：*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。

Cisco NX-OS IGMP スヌーピング ソフトウェアには、次の独自機能があります。

- 宛先および送信元の IP アドレスに基づいたマルチキャスト パケットの転送が可能な送信元フィルタリング
- MAC アドレスではなく、IP アドレスに基づいたマルチキャスト転送
- MAC アドレスに基づいた代わりのマルチキャスト転送
- 不明なトラフィックをルータにのみ転送し、非データ駆動で状態作成を実行する Optimized Multicast Flooding（OMF）

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。

IGMPv1 および IGMPv2

IGMPv1 と IGMPv2 は両方とも、メンバーシップ レポート抑制をサポートします。つまり、同一サブネット上の 2 つのホストが同一グループのマルチキャスト データを受信する場合、他方のホストからメンバー レポートを受信するホストは、そのレポートを送信しません。 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 での IGMPv3 スヌーピングの実装では完全な IGMPv3 スヌーピングがサポートされています。これにより、IGMPv3 レポートの（S、G）情報に基づいて、抑制されたフラッディングが提供されます。 この送信元ベースのフィルタリングにより、デバイスは対象のマルチキャスト グループにトラフィックを送信する送信元に基づいて、マルチキャスト トラフィックの宛先ポートを制限できます。

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。 この明示的な追跡機能は、高速脱退メカニズムをサポートしています。 IGMPv3 ではすべてのホストがメンバーシップ レポートを送信するため、レポート抑制機能を利用すると、デバイスから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量を制限できます。 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。

VLAN の任意の IP ドレスを使用するようにクエリアを設定できます。

ベスト プラクティスとして、簡単にクエリアを参照するには、一意の IP アドレス（スイッチ インターフェイスまたは Hot Standby Router Protocol（HSRP）仮想 IP アドレスでまだ使用されていない）を設定する必要があります。

（注） クエリアの IP アドレスは、ブロードキャスト IP アドレス、マルチキャスト IP アドレス、または 0（0.0.0.0）にしないでください。

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。

IGMP スヌーピング クエリアは、RFC 2236 に記述されているようにクエリア選択を実行します。クエリア選択は、次の構成で発生します。

- 異なるスイッチ上の同じ VLAN に同じサブネットに複数のスイッチ クエリアが設定されている場合。
- 設定されたスイッチ クエリアが他のレイヤ 3 SVI クエリアと同じサブネットにある場合。

仮想化のサポート

IGMP スヌーピングに対して、複数の仮想ルーティングおよび転送（VRF）インスタンスを定義できます。

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 の設定については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

IGMP スヌーピングのライセンス要件

製品	ライセンス要件
Cisco NX-OS	IGMP スヌーピングにはライセンスは不要です。 ライセンス パッケージに含まれていない機能は nx-os イメージにバンドルされており、無料で提供されます。 Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

IGMP スヌーピングの前提条件

IGMP スヌーピングの前提条件は、次のとおりです。

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

IGMP スヌーピングに関する注意事項と制限事項

IGMP に関する注意事項および制約事項は次のとおりです。

- レイヤ 3 IPv6 マルチキャスト ルーティングはサポートされていません。
- レイヤ 2 IPv6 マルチキャスト パケットは、着信 VLAN でフラッディングされます。
- レイヤ 2 ネットワークでマルチキャスト転送を必要とする IPv6 マルチキャスト ネットワークに対して IGMP Optimized Multicast Flooding（OMF）をディセーブルにする必要があります。
- IPv6 パケットの転送が必要な VLAN の IGMP 最適化マルチキャスト転送をディセーブルにする必要があります。
- 仮想ポート チャネル（vPC）ピアを設定している場合、2 台のデバイス間の IGMP スヌーピング設定オプションに相違があると、次のような結果になります。
  - 一方のデバイスで IGMP スヌーピングをイネーブルにして、他方でディセーブルにすると、スヌーピングがディセーブルであるデバイスではすべてのマルチキャスト トラフィックがフラッディングします。
  - マルチキャスト ルータまたはスタティック グループの設定の相違は、トラフィック損失の原因になり得ます。
  - 高速脱退、明示的な追跡、およびレポート抑制のオプションをトラフィックの転送に使用する場合、これらのオプションに相違が生じる可能性があります。
  - デバイス間でクエリー パラメータが異なると、一方のデバイスではマルチキャスト ステートが期限切れとなり、もう一方のデバイスでは転送が継続されます。 この相違によって、トラフィック損失または転送の長時間化が発生します。
  - IGMP スヌーピング クエリアを両方のデバイスで設定している場合、クエリーがトラフィックで確認されると、IGMP スヌーピング クエリアはシャットダウンするので、一方のクエリアだけがアクティブになります。
- **ip igmp snooping proxy general-queries** コマンドを使用する場合は、**ip igmp snooping group-timeout** コマンドをイネーブルにする必要があります。 これを「never」に設定することをお勧めします。 そのようにしない場合、マルチキャスト パケットが損失する場合があります。

デフォルト設定

パラメータ	デフォルト
IGMP スヌーピング	イネーブル
明示的な追跡	イネーブル
高速脱退	ディセーブル
最終メンバのクエリー インターバル	1 秒
スヌーピング クエリア	ディセーブル
レポート抑制	イネーブル
リンクローカル グループ抑制	イネーブル
デバイス全体での IGMPv3 レポート抑制	ディセーブル
VLAN ごとの IGMPv3 レポート抑制	イネーブル

IGMP スヌーピング パラメータの設定

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

（注） 他のコマンドを有効にする前に、IGMP スヌーピングをグローバルにイネーブルにする必要があります。

グローバル IGMP スヌーピング パラメータの設定

IGMP スヌーピング プロセスの動作をグローバルに変更するには、次の表に示すオプションの IGMP スヌーピング パラメータを設定します。

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ディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。
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 タイムアウトを設定します。
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 グループ抑制を設定します。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）を設定します。デフォルトではイネーブルになっています。
Proxy	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。
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 レポートを設定します。 デフォルトではディセーブルになっています。

IGMP スヌーピング パラメータの注記

次に、IGMP スヌーピング パラメータの一部についての補足的な注記を示します。

- IGMP スヌーピング プロキシ パラメータ

  IGMP 一般クエリー（GQ）の各インターバルでスヌーピング スイッチにかかる負担を減らすために、Cisco NX-OS ソフトウェアには、マルチキャスト ルータに設定されたクエリー インターバルから、IGMP スヌーピング スイッチの定期的な一般クエリー動作を分離する方法が用意されています。

  IGMP 一般クエリーをすべてのスイッチ ポートにフラッディングする代わりに、一般クエリーをマルチキャスト ルータから消費するようにデバイスを設定できます。 デバイスが一般クエリーを受信すると、現在アクティブなすべてのグループに対してプロキシ レポートを

生成し、ルータのクエリーで指定される MRT で指定された期間でプロキシ レポートを配布します。 同時に、マルチキャスト ルータの一般クエリーのアクティビティに関係なく、デバイスは、ラウンドロビン方式で VLAN の各ポート上に IGMP 一般クエリーを送信します。これは、次の式によって求められるレートで VLAN のすべてのインターフェイスを順に処理します。

レート = {VLAN 内のインターフェイスの数} * {設定された MRT} * {VLAN の数}

このモードでクエリーを実行する場合、デフォルト MRT 値は 5,000 ミリ秒（5 秒）です。VLAN にスイッチポートが 500 個あるデバイスの場合、システムですべてのインターフェイスを一巡するには 2,500 秒（40 分）かかります。 これは、デバイス自体がクエリアの場合でも同様です。

この動作は、随時 1 台のホストだけが一般クエリーに応答し、デバイスのパケット/秒 IGMP 機能を下回るレートによる同時レポート レートを保持することを確実にします（約 3,000 ～ 4,000 pps）。

（注） このオプションを使用する場合は、**ip igmp snooping group-timeout** パラメータの値を大きくするか、タイムアウトにしないようにします。

ip igmp snooping proxy general-queries [**mrt**] コマンドを使用すると、スヌーピング機能はマルチキャスト ルータからの一般クエリーにプロキシ応答するようになる一方で、指定された MRT 値を持つ各スイッチポートに対するラウンドロビン一般クエリーの送信も行われます。（デフォルトの MRT 値は 5 秒です。）

- IGMP スヌーピング グループ タイムアウト パラメータ

  グループ タイムアウト パラメータを設定すると 3 回連続で一般クエリーの処理できない事象に基づくメンバーシップの期限切れ動作がディセーブルになります。 グループ メンバーシップは、デバイスがそのポートで明示的に IGMP 脱退を受信するまで、特定のスイッチポートに残ります。

  ip igmp snooping group-timeout {*timeout* | **never**} コマンドは 3 回連続で一般クエリーを受信しなかったときの IGMP スヌーピング グループ メンバーシップの期限切れ動作を変更するかディセーブルにします。

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。

	コマンドまたはアクション		目的
ステップ 2	オプション	説明	次のコマンドを使用して、IGMP スヌーピングを設定できます。
	ip igmp snooping `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。	
	ip igmp snooping event-history `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 group-timeout {*minutes* | **never**} `switch(config)# ip igmp snooping group-timeout never`	デバイス上のすべての VLAN のグループ メンバーシップ タイムアウト値を設定します。	
	ip igmp snooping link-local-groups-suppression `switch(config)# ip igmp snooping link-local-groups-suppression`	デバイス全体のリンクローカル グループ抑制を設定します。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 optimise-multicast-flood `switch(config)# ip igmp snooping optimise-multicast-flood` 説明：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。	
	ip igmp snooping proxy general-inquiries [**mrt** *seconds*] `switch(config)# ip igmp snooping proxy general-inquiries` 説明：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。	
	ip igmp snooping v3-report-suppression `switch(config)# ip igmp snooping v3-report-suppression` 説明：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。	
	ip igmp snooping report-suppression `switch(config)# ip igmp snooping report-suppression` 説明：IGMPv3 レポート抑制およびプロキシ レポートを設定します。デフォルトではディセーブルになっています。	
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）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。

VLAN ごとの IGMP スヌーピング パラメータの設定

IGMP スヌーピング プロセスの動作を VLAN ごとに変更するには、この表に示すオプションの IGMP スヌーピング パラメータを設定します。

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。 （注） グローバルな設定がディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。
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。
グループ タイムアウト	指定した VLAN のグループ メンバーシップ タイムアウトを設定します。
最終メンバのクエリーインターバル	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ー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）を設定します。 デフォルトではイネーブルになっています。
Proxy	指定した VLAN 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。
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設定することもできます。 • タイムアウト：IGMPv2 のタイムアウト値 • インターバル：クエリー送信間の時間 • 最大応答時間：クエリー 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ー数 • スタートアップ インターバル：起動時のクエリー インターバル
ロバストネス変数	指定した VLAN のロバストネス値を設定します。
レポート抑制	各 VLAN に対して、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。
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	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。
IGMPv3 レポート抑制	各 VLAN に対して、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 VLAN ごとに有効になっています。
Version	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を明確に作成した後にのみ適用されます。 VLANの作成については、『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

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)#`
		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`	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
		（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 2`
	`switch(config-vlan-config)#`
		VLAN に対して目的の IGMP スヌーピング パラメータを設定します。これらの設定は、指定した VLAN を作成するまで適用されません。

ステップ 4	オプション：**ip igmp snooping** `switch(config-vlan-config)# ip igmp snooping` 説明：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。	これらのコマンドでは IGMP スヌーピング パラメータを設定します。

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* `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 ポリシーをベースとするIGMP スヌーピング レポートにフィルタを設定します。	
ip igmp snooping explicit-tracking `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 `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 group-timeout {*minutes* | **never**} `switch(config-vlan-config)# ip igmp snooping group-timeout never`	指定したVLAN のグループ メンバーシップ タイムアウトを設定します。	
ip igmp snooping last-member-query-interval *seconds* `switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3`	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、最終メンバのクエリー インターバルの期限が切れた場合に、対応する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。	

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 `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 proxy general-queries [**mrt** *seconds*] `switch(config-vlan-config)# ip igmp snooping proxy general-queries`	指定した VLAN 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。	
ip igmp snooping querier *ip-address* `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* `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に、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* `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。 デフォルト値は 125 秒です。	

コマンドまたはアクション		目的
オプション	説明	
ip igmp snooping query-max-response-time *seconds* `switch(config-vlan-config)# ip igmp snooping query-max-response-time 12`	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、クエリー メッセージのスヌーピング MRT を設定します。 デフォルト値は 10 秒です。	
ip igmp snooping report-policy {**prefix-list** | **route-map**} *policy-name* **interface** *interface slot/port* `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 ポリシーをベースとする IGMP スヌーピング レポートにフィルタを設定します。	
ip igmp snooping startup-query-count *value* `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* `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 をイネーブルにしていない場合に、起動時のスヌーピング クエリー インターバルを設定します。	
ip igmp snooping robustness-variable *value* `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。	

コマンドまたはアクション		目的
オプション	**説明**	
ip igmp snooping report-suppression `switch(config-vlan-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。	
ip igmp snooping mrouter interface *interface* `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** *slot*/*port* のように、インターフェイスをタイプおよび番号で指定できます。	
ip igmp snooping static-group *group-ip-addr* [**source** *source-ip-addr*] **interface** *interface* `switch(config-vlan-config)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1`	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。 **ethernet** *slot*/*port* のように、インターフェイスをタイプおよび番号で指定できます。	
ip igmp snooping link-local-groups-suppression `switch(config-vlan-config)# ip igmp snooping link-local-groups-suppression`	指定した VLAN のリンクローカル 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。	
ip igmp snooping v3-report-suppression `switch(config-vlan-config)# ip igmp snooping v3-report-suppression`	指定した VLAN の 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 VLAN ごとに有効になっています。	

	コマンドまたはアクション		目的
	オプション	説明	
	ip igmp snooping version *value* `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	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`		（任意）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。

IGMP スヌーピング設定の検証

コマンド	説明
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 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 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 explicit-tracking [**vlan** *vlan-id*]	IGMP スヌーピングの明示的な追跡情報を VLAN 別に表示します。

IGMP スヌーピング統計情報の表示

次のコマンドを使用して、IGMP スヌーピング統計情報を表示できます。

コマンド	説明
show ip igmp snooping statistics vlan	IGMP スヌーピング統計情報を表示します。 この出力で、仮想ポート チャネル（vPC）の統計情報を確認できます。
show ip igmp snooping {**report-policy** | **access-group**} **statistics** [**vlan** *vlan*]	IGMP スヌーピングのフィルタが設定されると、VLAN ごとに詳細な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	説明
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。
clear ip igmp snooping {**report-policy** | **access-group**} **statistics** [**vlan** *vlan*]	IGMP スヌーピング フィルタの統計情報をクリアします。

IGMP スヌーピングの設定例

（注） この項での設定は、指定された VLAN を作成した後にのみ適用されます。 VLAN の作成については、『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

次に、IGMP スヌーピング パラメータの設定例を示します。

```
config t
  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 report-suppression
    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
    ip igmp snooping v3-report-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 範囲で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 範囲で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。

第 6 章

MSDP の設定

この章では、Cisco NX-OS デバイスで Multicast Source Discovery Protocol（MSDP）を設定する手順について説明します。

MSDP について

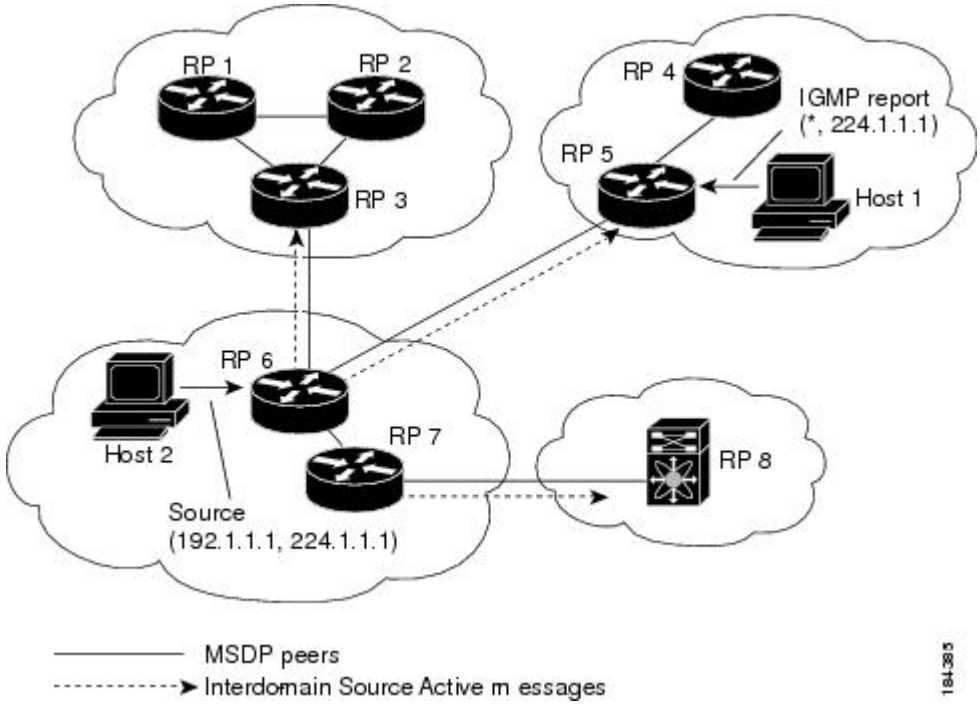
Multicast Source Discovery Protocol（MSDP）を使用すると、複数のボーダ ゲートウェイ プロトコル（BGP）対応 Protocol Independent Multicast（PIM）スパース モード ドメイン間で、マルチキャスト送信元情報を交換できます。 また、MSDP を使用して Anycast-RP 設定を作成し、RP 冗長性およびロード シェアリングを提供できます。 BGP の詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

受信者が別のドメイン内の送信元から送信されたグループに加入する場合、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。

次の図に、4 つの PIM ドメインを示します。 接続された RP（ルータ）は、アクティブな送信元情報を相互に交換するため、MSDP ピアと呼ばれます。 各 MSDP ピアは他のピアにマルチキャスト送信元情報の独自のセットをアドバタイズします。 送信元ホスト 2 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 1 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 2 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 *13*：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。

（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、BGP を設定する必要はありません。

（注） PIM Anycast（RFC 4610）を使用して、MSDP の代わりに Anycast-RP 機能を提供できます。

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、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。 SA キャッシュはデフォルトでイネーブルになっており、ディセーブルにできません。

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 または MBGP 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。 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。

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。

MSDP のライセンス要件

製品	ライセンス要件
Cisco NX-OS	MSDP には Enterprise Services ライセンスが必要です。 Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』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。

- デバイスにログインしている。
- 現在の仮想ルーティングおよびフォワーディング（VRF）モードが正しい（グローバル コマンドの場合）。 この章の例で示すデフォルトのコンフィギュレーション モードは、デフォルト VRF に適用されます。
- MSDP を設定するネットワークに PIM が設定済みである。

デフォルト設定

次の表に、MSDP パラメータのデフォルト設定を示します。

表 *13*：*MSDP* パラメータのデフォルト設定

パラメータ（Parameters）	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。

パラメータ（Parameters）	デフォルト
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。
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、次のように、各 PIM ドメイン内で MSDP ピアを設定します。

1. MSDP ピアとして動作させるルータを選択します。
2. MSDP 機能をイネーブルにします。
3. ステップ 1 で選択した各ルータで、MSDP ピアを設定します。
4. 各 MSDP ピアでオプションの MSDP ピア パラメータを設定します。
5. 各 MSDP ピアでオプションのグローバル パラメータを設定します。
6. 各 MSDP ピアでオプションのメッシュ グループを設定します。

（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。 MSDP をイネーブルにするには、**ip msdp peer** または **ip msdp originator-id** コマンドを使用します。

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

MSDP 機能のイネーブル化

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	**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	**show running-configuration msdp** 例： `switch# show running-configuration msdp`	（任意） MSDPの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`	（任意） 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。

MSDP ピアの設定

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。

はじめる前に

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 と MSDP がイネーブルになっていることを確認してください。

MSDP ピアを設定するルータのドメイン内で、PIM が設定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	**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。
ステップ 3	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 4	**show ip msdp summary** [**vrf** [*vrf-name* | **all**]] 例： `switch# show ip msdp summary`	（任意） MSDP ピアの要約情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

MSDP ピア パラメータの設定

次の表に、設定可能なオプションの MSDP ピア パラメータを示します。 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 *14* : *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 ポリシーの設定方法については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。
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 ポリシーの設定方法については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』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。

はじめる前に

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 と MSDP 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

<table>
<tr><th></th><th colspan="2">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 colspan="2">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 colspan="2"><table>
<tr><th>オプション</th><th>説明</th></tr>
<tr><td>ip msdp description
peer-ip-address description
例：
<pre>switch(config)# ip msdp description 192.168.1.10 peer in Engineering network</pre></td><td>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。</td></tr>
<tr><td>ip msdp shutdown
peer-ip-address
例：
<pre>switch(config)# ip msdp shutdown 192.168.1.10</pre></td><td>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。</td></tr>
<tr><td>ip msdp password
peer-ip-address password
例：
<pre>switch(config)# ip msdp password 192.168.1.10 my_md5_password</pre></td><td>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。</td></tr>
<tr><td>ip msdp sa-policy
peer-ip-address policy-name
in
例：
<pre>switch(config)# ip msdp sa-policy 192.168.1.10 my_incoming_sa_policy in</pre></td><td>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。</td></tr>
<tr><td>ip msdp sa-policy
peer-ip-address policy-name
out
例：
<pre>switch(config)# ip msdp sa-policy 192.168.1.10 my_outgoing_sa_policy out</pre></td><td>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。</td></tr>
</table></td><td>次のコマンドでは、MSDP ピア パラメータを設定します。</td></tr>
</table>

	コマンドまたはアクション	目的
	オプション: **ip msdp sa-limit** *peer-ip-address limit* 説明: 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。 例： `switch(config)# ip msdp sa-limit 192.168.1.10 5000`	
ステップ 3	**show ip msdp peer** [*peer-address*] [**vrf** [*vrf-name* | **all**]] 例： `switch(config)# show ip msdp peer 192.168.1.10`	（任意） MSDP ピアの詳細情報を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

MSDP グローバル パラメータの設定

次の表に、設定可能なオプションの MSDP グローバル パラメータを示します。

表 *15* : *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。 （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。

パラメータ	説明
グループの上限	指定したプレフィックスに対して作成される (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。

はじめる前に

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 と MSDP 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)#`
		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
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。

	コマンドまたはアクション	目的

	オプション / **説明**
	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作成される (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。
	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 3	**show ip msdp summary** [**vrf** [*vrf-name* | **all**]] 例： `switch(config)# show ip msdp summary`	（任意） MDSP の設定のサマリーを表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

MSDP メッシュ グループの設定

グローバル コンフィギュレーション モードでオプションの MSDP メッシュ グループを設定するには、メッシュ内の各ピアを指定します。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。

はじめる前に

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 と MSDP 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)#`
		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 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。
ステップ 3	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 4	**show ip msdp mesh-group** [*mesh-group*] [**vrf** [*vrf-name* | **all**]] 例： `switch# show ip msdp mesh-group`	（任意） MSDP メッシュ グループ設定に関する情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

MSDP プロセスの再起動

はじめる前に

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。

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。

	コマンドまたはアクション	目的

ステップ 2	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

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	**show running-configuration | include flush-routes** 例： `switch(config)# show running-configuration | include flush-routes`	（任意） 実行コンフィギュレーションの flush-routes 設定行を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

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* | **all**]]	MSDP (S,G) 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* | **all**]]	MSDP ピアの MSDP 情報を表示します。
show ip msdp rpf [*rp-address*] [**vrf** [*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 [**vrf** [*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。

コマンド	説明
show ip msdp summary [**vrf** [*vrf-name* | **all**]]	MSDP ピア設定の要約を表示します。

MSDP のモニタリング

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。

統計情報の表示

次のコマンドを使用して、MSDP 統計情報を表示できます。

コマンド	説明
show ip msdp [*as-number*] **internal event-history** {**errors** | **messages**}	メモリの割り当てに関する統計情報を表示します。
show ip msdp policy statistics sa-policy *peer-address* {**in** | **out**} [**vrf** [*vrf-name* | **all**]]	MSDP ピアの MSDP ポリシー統計情報を表示します。
show ip msdp {**sa-cache** | **route**} [*source-address*] [*group-address*] [**vrf** [*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

次のコマンドを使用して、MSDP 統計情報をクリアできます。

コマンド	説明
clear ip msdp peer [*peer-address*] [**vrf** *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*]	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*]	MSDP ピア の統計情報をクリアします。

コマンド	説明
clear ip msdp {**sa-cache** | **route**} [*group-address*] [**vrf** [*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、各 MSDP ピアで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、下に示した 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
```

関連資料

関連項目	参照先
MBGP の設定	『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』

Standards

Standards	Title
RFC 4624	『Multicast Source Discovery Protocol (MSDP) MIB』

付 録 A

IP マルチキャストに関する 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 マルチキャストに関する IETF RFC

次の表に、IP マルチキャストに関連する RFC を示します。

RFC	Title
RFC 2236	*Internet Group Management Protocol*（インターネットグループ管理プロトコル）
RFC 2365	管理用スコープの *IP* マルチキャスト
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 3376	*Internet Group Management Protocol*（インターネットグループ管理プロトコル）
RFC 3446	『*Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*』
RFC 3618	*Multicast Source Discovery Protocol*（*MSDP*）
RFC 4601	『*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*』

IP マルチキャストに関する IETF RFC

RFC	Title
RFC 4610	『*Anycast-RP Using Protocol Independent Multicast (PIM)*』
RFC 5059	『*Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*』
RFC 5132	『*IP Multicast MIB*』

付 録 B

Cisco NX-OS のマルチキャストに関する設定の上限

この付録では、Cisco NX-OS のマルチキャストに関する設定の制限について説明します。

設定の制限値

Cisco NX-OS がサポートする機能には、設定の最大制限があります。 一部の機能には、サポートしている上限値がこの最大制限を下回る設定のものもあります。

設定の制限は、『*Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*』に記載されています。

索 引

記号

数字

A

B

D

F

I

J

M

O

P

R

S

V

か

き

く

し

す

せ

ち

と

は

ひ

ふ

ま

め

ら

り

る