Cisco Nexus 3000 Series 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 5.0(3)U1(2)

Cisco Nexus 3000 Series NX-OS Multicast Routing Configuration Guide, Release 5.0(3)U1(2)

2011 年 5 月

【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、米国シスコシステムズ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。

Cisco Nexus 3000 Series 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 5.0(3)U1(2)

CONTENTS

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 3000 Series 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 5.0(3)U1(2)』の新機能および変更された機能に関するリリース固有の情報を示します。このマニュアルの最新バージョンは、次のシスコ Web サイトから入手できます。

http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

この Cisco NX-OS リリースに関するその他の情報については、『*Cisco Nexus 3000 Series Switch NX-OS Release Notes*』を参照してください。このマニュアルは次のシスコ Web サイトで入手できます。

http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

表 1 に、『Cisco Nexus 3000 Series 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 5.0(3)U1(2)』の新機能および変更された機能と、それぞれが説明されているページを示します。

表 1　『Cisco NX-OS Release 5.0(3)U1(1)』の新機能および変更された機能

機能	説明	変更されたリリース	参照先
IGMP	スイッチが、一般的なクエリーの IGMP グローバル Leave メッセージへの応答として、一般的な Maximum Response Time（MRT; 最大応答時間）を使用できるように設定できます。	5.0(3)U1(2)	IGMP の設定
PIM	RPT から SPT への移行中にハードウェアで重複パケットを防止できます。	5.0(3)U1(2)	PIM の設定

はじめに

ここでは、『Cisco Nexus 3000 Series 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 5.0(3)U1(2)』の対象読者、構成、および表記法について説明します。また、関連マニュアルの入手方法についても説明します。

この章は、次の内容で構成されています。

対象読者

このマニュアルを使用するには、IP およびルーティングのテクノロジーに関する詳しい知識が必要です。

サポートされるスイッチ

ここでは、次の内容について説明します。

Cisco Nexus 3000 プラットフォーム スイッチ

表 1 で、Cisco Nexus 3000 シリーズ スイッチについて説明します。

（注） Cisco Nexus 3000 シリーズの詳細については、『*Cisco Nexus 3000 Series Hardware Installation Guide*』を参照してください。このマニュアルは、次の URL から入手できます。
http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

表 1　サポートされる Cisco Nexus 3000 プラットフォーム スイッチ

スイッチ	説明
Cisco Nexus 3064PQ スイッチ	新しい Cisco Nexus 3000 シリーズ スイッチの Cisco Nexus 3064 スイッチは、高パフォーマンス、高密度、超低遅延のイーサネット スイッチです。このコンパクトな 1 ラック ユニット（1RU）フォーム ファクタの 1 ギガビットおよび 10 ギガビット イーサネット スイッチは、ラインレートのレイヤ 2 および 3 スイッチングを提供します。また、業界最先端の Cisco NX-OS ソフトウェア オペレーティング システムを搭載しているため、世界各国で幅広く展開されている堅牢な機能を利用できます。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章とタイトル	説明
第 1 章「概要」	Cisco NX-OS マルチキャスト機能について説明します。
第 2 章「IGMP の設定」	Cisco NX-OS の IGMP 機能の設定方法について説明します。
第 3 章「PIM の設定」	Cisco NX-OS の PIM 機能の設定方法について説明します。
第 4 章「IGMP スヌーピングの設定」	Cisco NX-OS の IGMP スヌーピング機能の設定方法について説明します。
第 5 章「MSDP の設定」	Cisco NX-OS の MSDP 機能の設定方法について説明します。
付録 A「IP マルチキャストに関する IETF RFC」	Cisco NX-OS マルチキャスト機能に関連する RFC を掲載しています。

表記法

コマンドの説明では、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
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。

出力例では、次の表記法を使用しています。

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。

このマニュアルでは、次の表記法を使用しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

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

ヒント 「*問題解決に役立つ情報*」です。

関連資料

Cisco Nexus 3000 シリーズ スイッチおよび Cisco Nexus 2000 シリーズ Fabric Extender のマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

関連する Cisco Nexus 3000 シリーズのマニュアルは、次のとおりです。

リリース ノート

『*Cisco Nexus 3000 Series Release Notes*』

コンフィギュレーション ガイド

『*Cisco Nexus 3000 Series Configuration Limits for Cisco NX-OS Release 5.0(3)U1(1)*』

『*Cisco Nexus 3000 Series NX-OS Layer 2 Switching Configuration Guide*』

『*Cisco Nexus 3000 Series NX-OS Multicast Routing Configuration Guide*』

『*Cisco Nexus 3000 Series NX-OS Quality of Service Configuration Guide*』

『*Cisco Nexus 3000 Series NX-OS SAN Switching Configuration Guide*』

『*Cisco Nexus 3000 Series NX-OS Security Configuration Guide*』

『*Cisco Nexus 3000 Series NX-OS System Management Configuration Guide*』

『*Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide*』

『*Cisco NX-OS Fundamentals Configuration Guide*』

メンテナンスおよび操作ガイド

『*Cisco Nexus 3000 Series NX-OS Operations Guide*』

インストレーション ガイドおよびアップグレード ガイド

『*Cisco Nexus 3000 Series Hardware Installation Guide*』

『*Regulatory, Compliance, and Safety Information for the Cisco Nexus 5000 Series, Cisco Nexus 3000 Series, and Cisco Nexus 2000 Series*』

ライセンス ガイド

『*Cisco NX-OS Licensing Guide*』

コマンド リファレンス

『*Cisco Nexus 3000 Series Command Reference*』

テクニカル リファレンス

『*Cisco Nexus 3000 Series MIBs Reference*』

エラー メッセージおよびシステム メッセージ

『*Cisco NX-OS System Messages Reference*』

トラブルシューティング ガイド

『*Cisco Nexus 3000 Troubleshooting Guide*』

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は 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がデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

概要

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

この章は、次の内容で構成されています。

マルチキャストに関する情報

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。

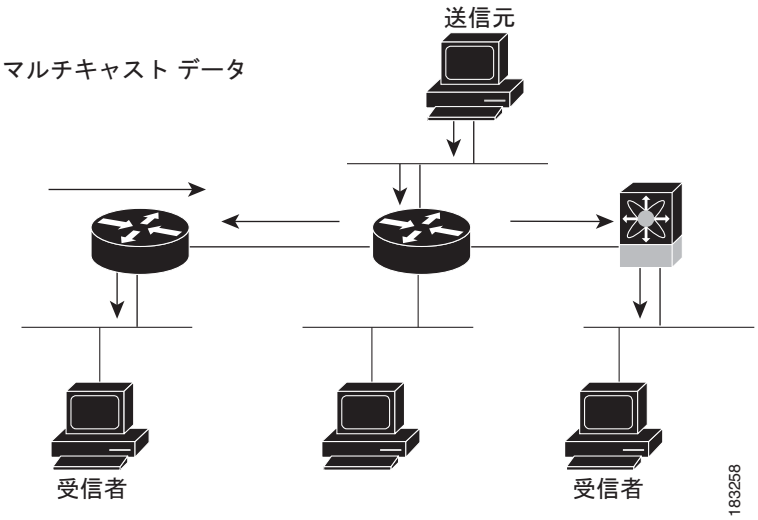
マルチキャストは、マルチキャスト データの配信機能と、送信元および受信者の検出機能からなり、マルチキャスト データは、グループと呼ばれる IP マルチキャスト アドレス宛に送信されます。多くの場合、グループおよび送信元 IP アドレスを含むマルチキャスト アドレスは、チャネルと呼ばれます。Internet Assigned Number Authority（IANA）では、IPv4 マルチキャスト アドレスとして、224.0.0.0 ～ 239.255.255.255 を割り当てています。詳細については、次の URL を参照してください。
http://www.iana.org/assignments/multicast-addresses

（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。

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

図 1-1　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



ここでは、次の内容について説明します。

マルチキャスト配信ツリー

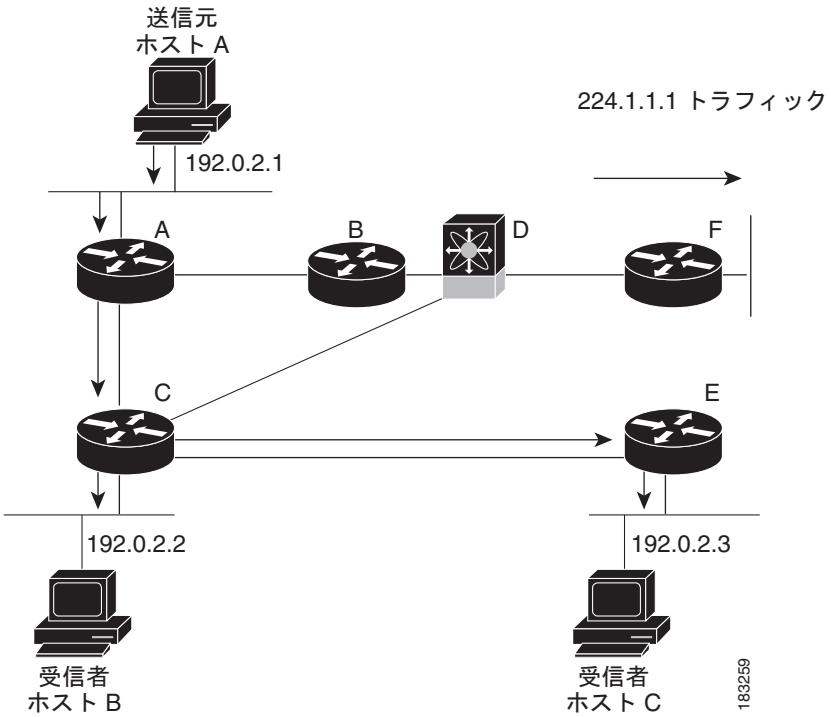
マルチキャスト配信ツリーとは、送信元と受信者を中継するルータ間の、マルチキャスト データの伝送パスを表します。マルチキャスト ソフトウェアはサポートするマルチキャスト方式に応じて、タイプの異なるツリーを構築します。

ここでは、次の内容について説明します。

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、Shortest Path Tree（SPT; 最短パス ツリー）と呼ばれることがあります。図 1-2 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 1-2　送信元ツリー

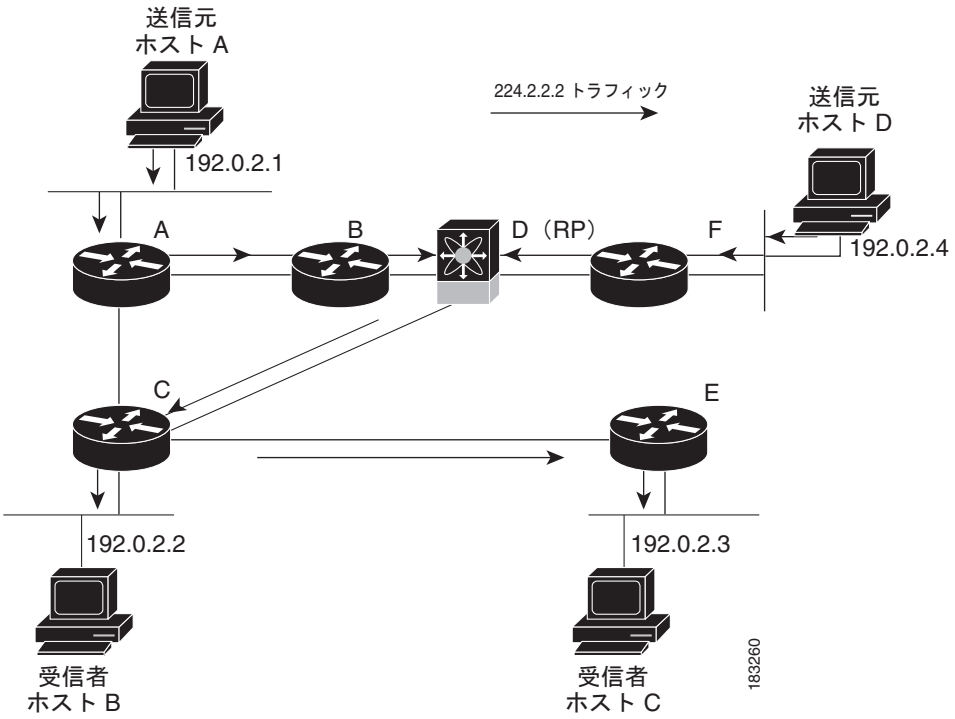


(S, G) は、グループ G の送信元 S から送信されるマルチキャスト トラフィックを表します。図 1-2 の SPT は、(192.1.1.1, 224.1.1.1) と書き表されます。同じグループの複数の送信元からトラフィックを送信できます。

共有ツリー

共有ツリーとは、共有ルート、つまり Rendezvous Point（RP; ランデブー ポイント）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 Tree（RPT; RP ツリー）とも呼ばれます。図 1-3 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 1-3　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。図 1-3 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

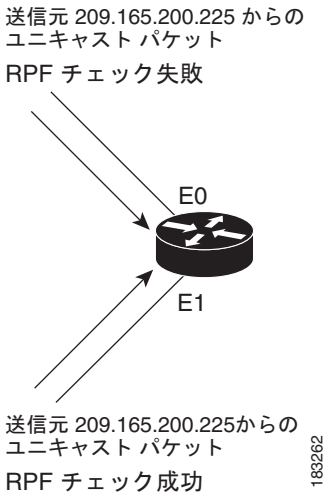
マルチキャスト トラフィックは任意のホストを含むグループ宛に送信されるため、ルータは Reverse Path Forwarding（RPF）を使用して、グループのアクティブな受信者にデータをルーティングします。受信者がグループに加入すると、送信元方向へ向かうパス（SSM モードの場合）、または RP 方向へ向かうパス（ASM モードの場合）が形成されます。送信元から受信者へのパスは、受信者がグループに加入したときに作成されたパスと逆方向になります。

マルチキャスト パケットが着信するたびに、ルータは RPF チェックを実行します。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 Outgoing Interface（OIF; 発信インターフェイス）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。

図 1-4 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 1-4　RPF チェックの例

ユニキャスト ルート テーブル	
ネットワーク	インターフェイス
192.0.2.0/24	E0
209.165.200.224/27	E1



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 がシステムで実行されています。

マルチキャスト対応ルータ間で使用される PIM は、マルチキャスト配信ツリーを構築して、ルーティング ドメイン内にグループ メンバ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。

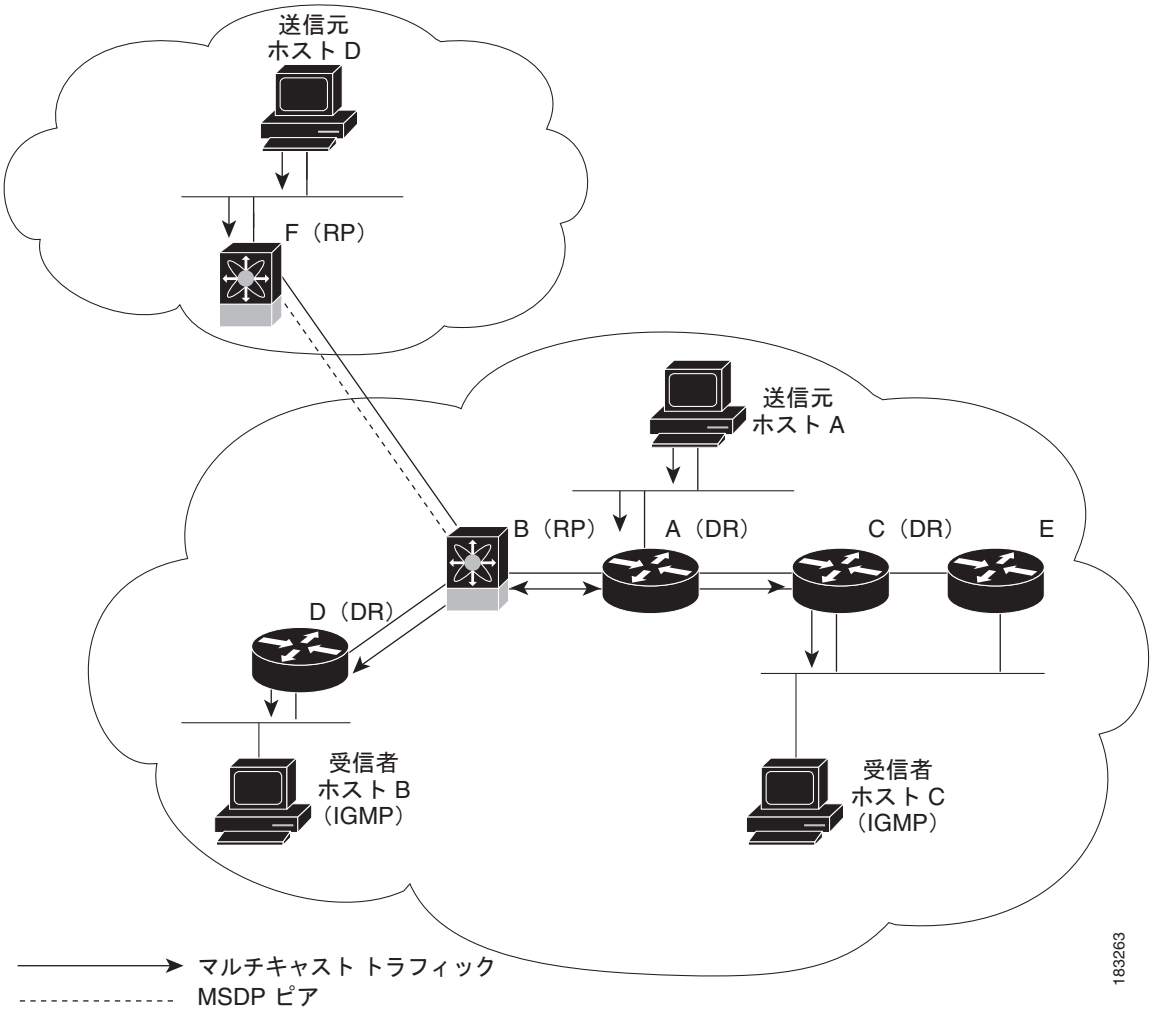
配信ツリーは、リンク障害またはルータ障害のためにトポロジが変更されると、トポロジを反映して自動的に変更されます。PIM は、マルチキャスト対応の送信元と受信者の両方を動的に追跡します。

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。PIM ドメインには、IPv4 ネットワークを含めることができます。

図 1-5 に、IPv4 ネットワーク内の 2 つの PIM ドメインを示します。

図 1-5　IPv4 ネットワーク内の PIM ドメイン



次に、図 1-5 で示した PIM の要素について説明します。

- 矢印の付いた直線は、ネットワークで伝送されるマルチキャスト データのパスを表します。マルチキャスト データは送信元ホストの A および D から発信されます。
- 点線でつながれているルータ B および F は、Multicast Source Discovery Protocol（MSDP）ピアです。MSDP を使用すると、他の PIM ドメイン内にあるマルチキャスト送信元を検出できます。
- ホスト B およびホスト C ではマルチキャスト データを受信するため、Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）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 Designated Router（DR; 指定ルータ）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 Rendezvous Point（RP; ランデブー ポイント）です。RP は、複数の送信元と受信者を接続するため、PIM ドメイン内の共通ポイントとして機能します。

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

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

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

ここでは、次の内容について説明します。

- 「ASM」（P.1-7）
- 「SSM」（P.1-7）
- 「マルチキャスト用 RPF ルート」（P.1-7）

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、Rendezvous Point（RP; ランデブー ポイント）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 Bootstrap Router（BSR; ブートストラップ ルータ）プロトコルを使用して、グループと RP 間の関連付けを動的に検出することもできます。

RP を設定する場合、デフォルト モードは ASM モードです。

ASM の設定方法については、「ASM の設定」（P.3-15）を参照してください。

SSM

Source-Specific Multicast（SSM）は、マルチキャスト送信元への加入要求を受信する LAN セグメント上の指定ルータを起点として、送信元ツリーを構築する PIM モードです。送信元ツリーは、PIM 加入メッセージを送信元方向に送信することで構築されます。SSM モードでは、RP を設定する必要がありません。

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

SSM の設定方法については、「SSM の設定」（P.3-26）を参照してください。

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。

マルチキャスト用 RPF ルートの設定方法については、「マルチキャスト用 RPF ルートの設定」（P.3-28）を参照してください。

IGMP

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

IGMP プロトコルは、マルチキャスト グループのメンバ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 メンバシップが確立されると、対象のグループのマルチキャスト データが要求元ホストの LAN セグメントに転送されます。

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

IGMP の設定については、第 2 章「IGMP の設定」を参照してください。

IGMP スヌーピング

IGMP スヌーピングは、VLAN で既知の受信者に接続された一部のポートだけにマルチキャスト トラフィックを転送する機能です。対象ホストからの IGMP メンバシップ 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動しています。

IGMP スヌーピングの設定方法については、第 4 章「IGMP スヌーピングの設定」を参照してください。

ドメイン内マルチキャスト

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

ここでは、次の内容について説明します。

SSM

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

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

SSM の設定方法については、「SSM の設定」（P.3-26）を参照してください。

MSDP

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

（注）　Cisco NX-OS では、MSDP 設定が不要な PIM Anycast-RP をサポートしています。PIM Anycast-RP の詳細については、「PIM Anycast-RP セットの設定」（P.3-22）を参照してください。

MSDP の詳細については、第 5 章「MSDP の設定」を参照してください。

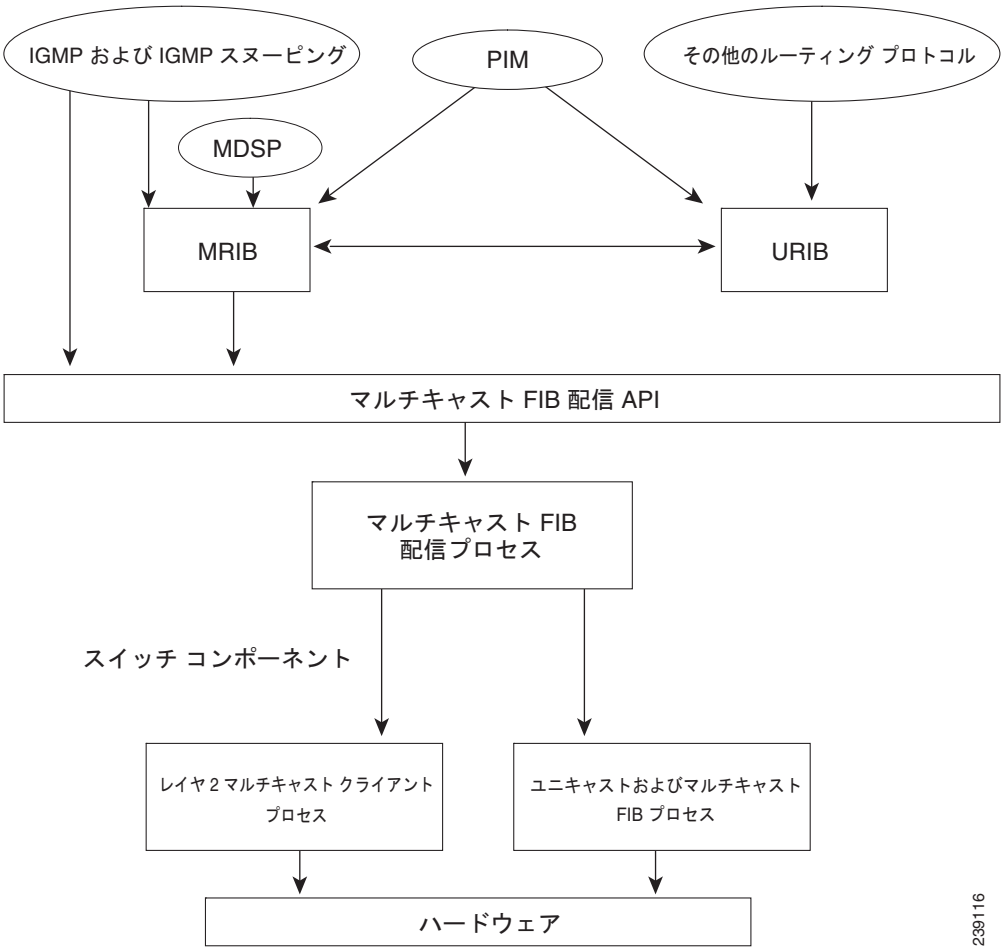
MRIB

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

図 1-6 に、Cisco NX-OS マルチキャスト ソフトウェア アーキテクチャのおもなコンポーネントを示します。

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

図 1-6　Cisco NX-OS マルチキャスト ソフトウェアのアーキテクチャ



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 の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。

その他の関連資料

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

- 「関連資料」（P.1-11）
- 付録 A「IP マルチキャストに関する IETF RFC」
- 「シスコのテクニカル サポート」（P.1-11）

関連資料

関連項目	参照先
CLI コマンド	『*Cisco Nexus 3000 Series Command Reference*』

シスコのテクニカル サポート

説明	リンク
Technical Assistance Center（TAC）ホーム ページ：多数の技術関連の記事と、製品、テクノロジー、ソリューション、テクニカル ティップス、ツールへのリンクを提供する Web サイトです。必要な記事は検索して見つけることができます。Cisco.com の登録ユーザであれば、ログインしてさらに多くの情報を参照できます。	http://www.cisco.com/public/support/tac/home.shtml

CHAPTER 2

IGMP の設定

この章では、IPv4 ネットワークの Cisco NX-OS スイッチに対する Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）の設定方法を説明します。

この章は、次の内容で構成されています。

IGMP の情報

IGMP は、ホストが特定のグループにマルチキャスト データを要求するために使用する IPv4 プロトコルです。ソフトウェアは、IGMP を介して取得した情報を使用し、マルチキャスト グループまたはチャネル メンバ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

ここでは、次の内容について説明します。

IGMP のバージョン

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

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

IGMPv3 には、次に示す IGMPv2 からの重要な変更点があります。

- 次の機能を提供し、各受信者から送信元までの最短パス ツリーを構築可能な Source-Specific Multicast（SSM）をサポートします。
  - グループおよび送信元を両方指定できるホスト メッセージ
  - IGMPv2 ではグループについてのみ保持できたマルチキャスト ステートを、グループおよび送信元について保持可能
- 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 メンバシップ レポートが送信されるようになりました。

IGMPv2 の詳細については、RFC 2236 を参照してください。

IGMPv3 の詳細については、RFC 3376 を参照してください。

IGMP の基礎

図 2-1 に、ルータが IGMP を使用し、マルチキャスト ホストを検出する基本的なプロセスを示します。ホスト 1、2、および 3 は要求外の IGMP メンバシップ 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 2-1　IGMPv1 および IGMPv2 クエリー応答プロセス

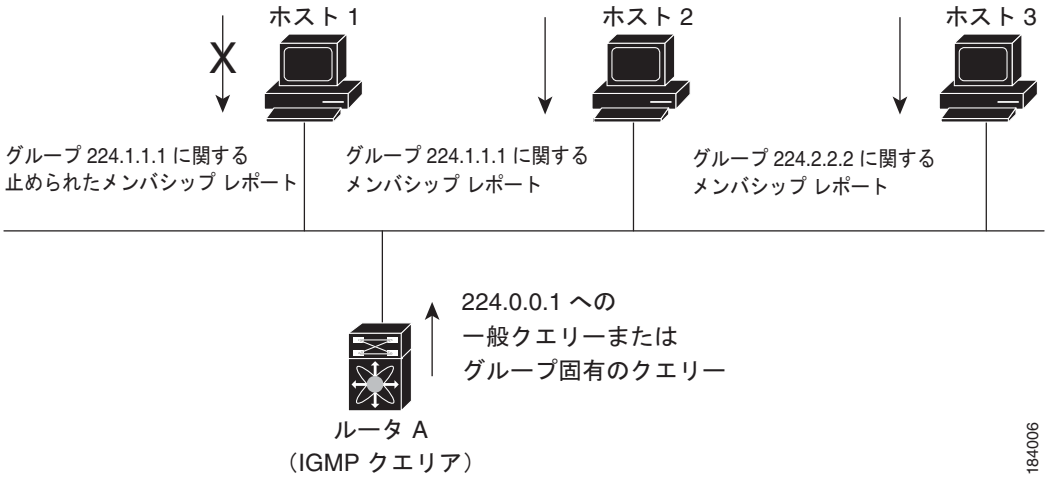


図 2-1 のルータ A（サブネットの代表 IGMP クエリア）は、すべてのホストが含まれる 224.0.0.1 ホスト マルチキャスト グループに定期的にクエリー メッセージを送信して、マルチキャスト データを要求しているホストを検出します。グループ メンバシップ タイムアウト値を設定し、指定したタイムアウト値が経過すると、ルータはサブネット上にグループのメンバーまたは送信元が存在しないと見なします。IGMP パラメータの設定方法については、「IGMP インターフェイス パラメータの設定」（P.2-6）を参照してください。

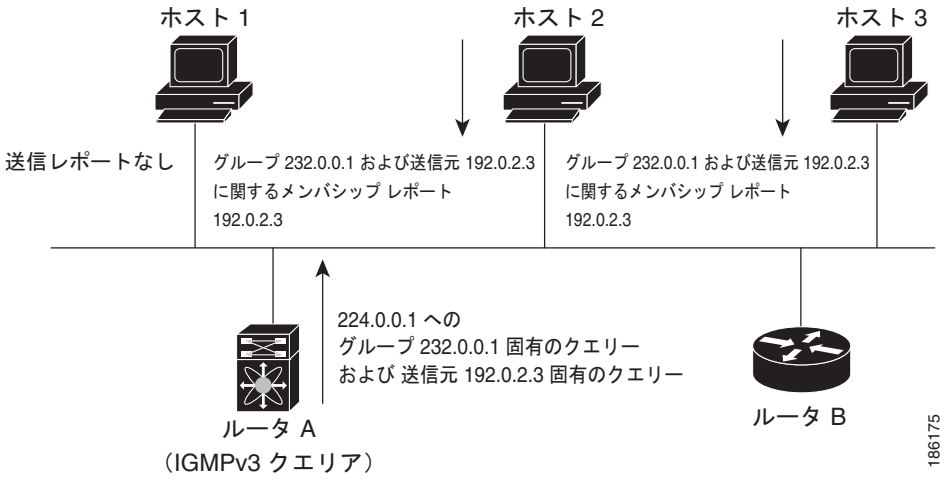
IP アドレスが最下位のルータが、サブネットの IGMP クエリアとして選出されます。ルータは、自身よりも下位の IP アドレスを持つルータからクエリー メッセージを継続的に受信している間、クエリア タイムアウト値をカウントするタイマーをリセットします。ルータのクエリア タイマーが期限切れになると、そのルータは代表クエリアになります。そのあとで、このルータが、自身よりも下位の IP アドレスを持つルータからのホスト クエリー メッセージを受信すると、ルータは代表クエリアとしての役割をドロップしてクエリア タイマーを再度設定します。

図 2-1 では、ホスト 1 からのメンバシップ 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 メンバシップ レポートが抑制されるのは、同じポートに複数のホストが接続されている場合だけです。

図 2-2 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シップ レポートを送信して、そのクエリーに応答します。この IGMPv3 機能では、SSM がサポートされます。IGMPv1 ホストおよび IGMPv2 ホストが SSM をサポートするよう、SSM を変換する方法については、「IGMP SSM 変換の設定」（P.2-11）を参照してください。

図 2-2　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 Time-To-Live（TTL; 存続可能時間）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、Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）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 パラメータの設定方法については、「IGMP インターフェイス パラメータの設定」（P.2-6）を参照してください。

仮想化のサポート

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

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

VRF の設定の詳細については、『*Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

IGMP のライセンス要件

次の表に、この機能のライセンス要件を示します。

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すべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS の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。 **（注）**　レイヤ 3 インターフェイスをイネーブルにするため、スイッチに LAN Base Services ライセンスをインストールする必要があります。

IGMP のデフォルト設定

表 2-1 に、IGMP パラメータのデフォルト設定を示します。

表 2-1　IGMP パラメータのデフォルト設定

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

ここでは、次の内容について説明します。

- 「IGMP インターフェイス パラメータの設定」（P.2-6）
- 「IGMP SSM 変換の設定」（P.2-11）
- 「ルータ アラートの適用オプション チェックの設定」（P.2-12）

（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

表 2-2 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 2-2　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 プレフィクス、グループ範囲、および送信元プレフィクスを示すルートマップ ポリシー名を指定できます。 **（注）** (S, G) ステートで設定しても、送信元ツリーが構築されるのは IGMPv3 がイネーブルな場合だけです。SSM 変換の詳細については、「IGMP SSM 変換の設定」（P.2-11）を参照してください。 ネットワーク上の全マルチキャスト対応ルータを含むマルチキャスト グループを設定すると、このグループに ping 要求を送信することで、すべてのルータから応答を受け取ることができます。
Outgoing Interface（OIF; 発信インターフェイス）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 プレフィクス、グループ範囲、および送信元プレフィクスを示すルートマップ ポリシー名を指定できます。 **（注）** (S, G) ステートで設定しても、送信元ツリーが構築されるのは IGMPv3 がイネーブルな場合だけです。SSM 変換の詳細については、「IGMP SSM 変換の設定」（P.2-11）を参照してください。
スタートアップ クエリー インターバル	スタートアップ クエリー インターバル。デフォルトでは、ソフトウェアができるだけ迅速にグループ ステートを確立できるように、このインターバルはクエリー インターバルより短く設定されています。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 31 秒です。
スタートアップ クエリーの回数	スタートアップ クエリー インターバル中に送信される起動時のクエリー数。有効範囲は 1 ～ 10 です。デフォルト値は 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 メッセージのバースト性を調整できます。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。デフォルト値は 10 秒です。

表 2-2　IGMP インターフェイス パラメータ （続き）

パラメータ	説明
クエリー インターバル	IGMP ホスト クエリー メッセージの送信頻度。大きな値を設定すると、ソフトウェアによる IGMP クエリーの送信頻度が低くなるため、ネットワーク上の IGMP メッセージ数を調整できます。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 125 秒です。
最終メンバーのクエリー応答インターバル	サブネット上の既知のアクティブ ホストから最後にホスト Leave メッセージを受信したあと、ソフトウェアが IGMP クエリーへの応答を送信するインターバル。このインターバル中に応答が受信されない場合、グループ ステートは解除されます。この値を使用すると、サブネット上でソフトウェアがトラフィックの送信を停止するタイミングを調整できます。この値を小さく設定すると、グループの最終メンバーまたは送信元が脱退したことを、より短時間で検出できます。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。
最終メンバーのクエリー回数	サブネット上の既知のアクティブ ホストから最後にホスト Leave メッセージを受信したあと、最終メンバーのクエリー応答インターバル中に、ソフトウェアが IGMP クエリーを送信する回数。有効範囲は 1 ～ 5 です。デフォルト値は 2 です。 **注意**　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[1]を設定するオプション。
即時脱退	スイッチ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、スイッチではグループに関する Leave メッセージの受信後、ただちにマルチキャスト ルーティング テーブルからグループ エントリが削除されます。デフォルトではディセーブルになっています。 **（注）**　このコマンドは、所定のグループに対するインターフェイスの背後に 1 つの受信者しか存在しない場合に使用します。
global-leave-ignore-gss-mrt	Cisco NX-OS Release 5.0(3)U1(2) からは、IGMP グローバル Leave メッセージ（グループ 0.0.0.0 への IGMP Leave レポート）への応答として、グループ固有クエリーで、より低い Maximum Response Time（MRT; 最大応答時間）値に対し、設定済み MRT 値を使用できます。

1. ルートマップ ポリシーの設定方法については、『*Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

マルチキャスト ルート マップの設定方法については、「RP 情報配信を制御するルート マップの設定」（P.3-29）を参照してください。

手順の概要

1. **configure terminal**
2. **interface** *interface*
3. **no switchport**
4. **ip igmp version** *value*
   ip igmp join-group {*group* [**source** *source*] | **route-map** *policy-name*}
   ip igmp static-oif {*group* [**source** *source*] | **route-map** *policy-name*}
   ip igmp startup-query-interval *seconds*
   ip igmp startup-query-count *count*
   ip igmp robustness-variable *value*
   ip igmp querier-timeout *seconds*
   ip igmp query-timeout *seconds*
   ip igmp query-max-response-time *seconds*
   ip igmp query-interval *interval*
   ip igmp last-member-query-response-time *seconds*
   ip igmp last-member-query-count *count*
   ip igmp group-timeout *seconds*
   ip igmp report-link-local-groups
   ip igmp report-policy *policy*
   ip igmp access-group *policy*
   ip igmp immediate-leave
   ip igmp global-leave-ignore-gss-mrt
5. （任意）**show ip igmp interface** [*interface*] [**vrf** *vrf-name* | **all**] [**brief**]
6. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal` `switch(config)#`	コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface* 例： `switch(config)# interface ethernet 2/1` `switch(config-if)#`	**ethernet** *slot/port* などのインターフェイス タイプおよび番号を入力して、インターフェイス モードを開始します。
ステップ 3	**no switchport** 例： `switch(config-if)# no switchport` `switch(config-if)#`	そのインターフェイスを、レイヤ 3 インターフェイスとして設定します。

	コマンド	目的
ステップ 4	**ip igmp version** *value* **例：** `switch(config-if)# ip igmp version 3`	IGMP バージョンを指定値に設定します。有効な値は 2 または 3 です。デフォルト値は 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。
	ip igmp join-group {**group** [**source** *source*] | **route-map** *policy-name*} **例：** `switch(config-if)# ip igmp join-group 230.0.0.0`	マルチキャスト グループをインターフェイスに静的にバインドします。グループ アドレスだけを指定した場合は、(*, G) という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) という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 プレフィクス、グループ範囲、および送信元プレフィ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) ステートで送信元ツリーを構築するには、IGMPv3 をイネーブルにする必要があります。 ⚠ **注意** スイッチの CPU は、このコマンドを使用して生成されたトラフィックを処理する必要があります。
	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、スイッチ ハードウェアで処理します。グループ アドレスだけを指定した場合は、(*, G) という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) という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 プレフィクス、グループ範囲、および送信元プレフィ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) ステートで送信元ツリーを構築するには、IGMPv3 をイネーブルにする必要があります。
	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。
	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。ネットワークのパケット損失が多い場合は、この値を大きくします。有効範囲は 1 ～ 7 です。デフォルト値は 2 です。

コマンド	目的
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。デフォルト値は 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。
ip igmp last-member-query-response-time *seconds* **例：** `switch(config-if)# ip igmp last-member-query-response-time 3`	メンバシップ 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`	PIM 対応インターフェイスが加入できるマルチキャスト 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。
ip igmp access-group *policy* **例：** `switch(config-if)# ip igmp access-group my_access_policy`	PIM 対応インターフェイスが加入できるマルチキャスト 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。

	コマンド	目的
	ip igmp immediate-leave **例：** `switch(config-if)# ip igmp immediate-leave`	スイッチが、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。このコマンドは、スイッチ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 メンバシップの脱退のための待ち時間を最小限にできます。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。
	ip igmp global-leave-ignore-gss-mrt **例：** `switch(config-if)# ip igmp global-leave-ignore-gss-mrt`	スイッチが、一般的なクエリーの IGMP グローバル Leave メッセージへの応答として、一般的な Maximum Response Time（MRT; 最大応答時間）を使用できるようにします。
ステップ 5	**show ip igmp interface** [*interface*] [**vrf** *vrf-name* | **all**] [**brief**] **例：** `switch(config)# show ip igmp interface`	（任意）インターフェイスの IGMP 情報を表示します。
ステップ 6	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）コンフィギュレーションの変更を保存します。

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 プレフィクスのデフォルト範囲は、232.0.0.0/8 です。PIM SSM 範囲の変更方法については、「SSM の設定」（P.3-26）を参照してください。

表 2-3 に、SSM 変換の例を示します。

表 2-3　SSM 変換の例

グループ プレフィクス	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

表 2-4 に、IGMP メンバシップ 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 2-4　SSM 変換適用後の例

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

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

手順の概要

1. **configure terminal**
2. **ip igmp ssm-translate** *group-prefix source-addr*
3. （任意）**show running-configuration igmp**
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal` `switch(config)#`	コンフィギュレーション モードを開始します。
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）コンフィギュレーションの変更を保存します。

ルータ アラートの適用オプション チェックの設定

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

手順の概要

1. **configure terminal**

2. **ip igmp enforce-router-alert**
   no ip igmp enforce-router-alert
3. （任意）**show running-configuration igmp**
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal` `switch(config)#`	コンフィギュレーション モードを開始します。
ステップ 2	**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。
	no ip igmp enforce-router-alert 例： `switch(config)# no 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）**enforce-router-alert** コマンドラインを含む、実行コンフィギュレーション情報を示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）コンフィギュレーションの変更を保存します。

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

コマンド	目的
show ip igmp route [*group* | *interface*] [**vrf** *vrf-name* | **all**]	グループまたはインターフェイス、デフォルト VRF、選択された VRF、またはすべての VRF について、IGMP で接続されたグループのメンバシップを表示します。
show ip igmp local-groups	IGMP ローカル グループ メンバシップを表示します。
show running-configuration igmp	IGMP 実行コンフィギュレーション情報を表示します。
show startup-configuration igmp	IGMP スタートアップ コンフィギュレーション情報を表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 3000 Series Command Reference*』を参照してください。

IGMP の設定例

次に、IGMP パラメータの設定例を示します。

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

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

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

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

```
switch(config)# route-map foo deny 10
switch(config-route-map)# exit
switch(config)# interface vlan 5
switch(config-if)# ip pim sparse-mode
switch(config-if)# ip igmp report-policy foo
```

次の作業

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

- 第 4 章「IGMP スヌーピングの設定」
- 第 5 章「MSDP の設定」

IGMP の機能の履歴

表 2-5 に、この機能のリリース履歴を示します。

表 2-5　IGMP の機能の履歴

機能名	リリース	機能情報
IGMP	5.0(3)U1(1)	この機能が導入されました。

CHAPTER 3

PIM の設定

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

この章は、次の内容で構成されています。

PIM の情報

マルチキャスト対応ルータ間で使用される PIM は、マルチキャスト配信ツリーを構築して、ルーティング ドメイン内にグループ メンバシップをアドバタイズします。PIM は、複数の送信元からのパケットが転送される共有配信ツリーと、単一の送信元からのパケットが転送される送信元配信ツリーを構築します。マルチキャストの詳細については、「マルチキャストに関する情報」（P.1-1）を参照してください。

Cisco NX-OS は、IPv4 ネットワーク（PIM）対応の PIM スパース モードをサポートします （PIM スパース モードでは、ネットワーク上の要求元だけにマルチキャスト トラフィックが伝送されます）。PIM は、ルータ上で同時に実行するように設定できます。PIM グローバル パラメータを使用すると、Rendezvous Point（RP; ランデブー ポイント）、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 Designated Router（DR; 指定ルータ）のプライオリティ設定を実行できます。詳細については、「PIM スパース モードの設定」（P.3-11）を参照してください。

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

Cisco NX-OS でマルチキャスト機能を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 Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）がイネーブルになっていない場合は、PIM によって自動的にイネーブルにされます。IGMP の設定については、第 2 章「IGMP の設定」を参照してください。

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

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

モードを組み合わせて、さまざまな範囲のグループ アドレスに対応することができます。詳細については、「PIM の設定」（P.3-9）を参照してください。

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

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

（注）　Cisco Nexus 3000 シリーズ スイッチ対応の Cisco NX-OS では、マルチキャストの Equal-Cost MultiPathing（ECMP; 等コスト マルチパス）がデフォルトでオンになっています。ECMP はオフにできません。プレフィクスに対し複数のパスが存在する場合は、PIM がルーティング テーブル内で最も低いアドミニストレーティブ ディスタンスを持つパスを選択します。Cisco NX-OS は、宛先までの 16 のパスをサポートします。

ここでは、次の内容について説明します。

hello メッセージ

ルータがマルチキャスト アドレス 224.0.0.13 に PIM hello メッセージを送信して、PIM ネイバー ルータとの隣接関係を確立すると、PIM プロセスが開始されます。hello メッセージは 30 秒間隔で定期的に送信されます。PIM ソフトウェアはすべてのネイバーからの応答を確認すると、各 LAN セグメント内でプライオリティが最大のルータを Designated Router（DR; 指定ルータ）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。

注意　PIM の hello 間隔を低い値に変更する場合は、ネットワーク環境に適応しているかどうかを確認することを推奨します。

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

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

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

hello メッセージ認証の設定方法については、「PIM スパース モードの設定」（P.3-11）を参照してください。

Join/Prune メッセージ

受信者から送信された、新しいグループまたは送信元に対する IGMP メンバシップ レポート メッセージを受信すると、DR は、インターフェイスからランデブー ポイント方向（ASM モード）または送信元方向（SSM モード）に PIM Join メッセージを送信して、受信者と送信元を接続するツリーを作成します。Rendezvous Point（RP; ランデブー ポイント）は共有ツリーのルートであり、ASM モードで PIM ドメイン内のすべての送信元およびホストによって使用されます。SSM では RP を使用せず、送信元と受信者間の最小コスト パスである Shortest Path Tree（SPT; 最短パス ツリー）が構築されます。

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

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

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

Join/Prune メッセージは、ソフトウェアからできるだけ短時間で送信されます。Join/Prune メッセージをフィルタリングするには、ルーティング ポリシーを定義します。Join/Prune メッセージのポリシーの設定方法については、「PIM スパース モードの設定」（P.3-11）を参照してください。

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

ステートのリフレッシュ

PIM では、3.5 分の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

Rendezvous Point（RP; ランデブー ポイント）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。

ここでは、次の内容について説明します。

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
- スイッチに手動で RP を設定する場合

スタティック RP の設定方法については、「スタティック RP の設定」（P.3-16）を参照してください。

BSR

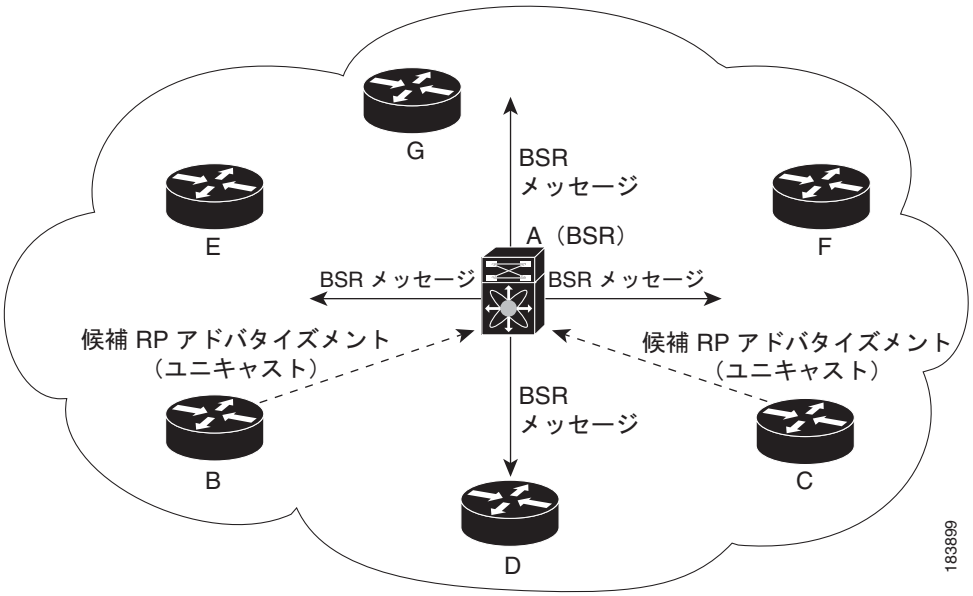
Bootstrap Router（BSR; ブートストラップ ルータ）を使用すると、PIM ドメイン内のすべてのルータで、BSR と同じ RP キャッシュが保持されるようになります。BSR では、BSR 候補 RP から RP セットを選択するよう設定できます。BSR は、ドメイン内のすべてのルータに RP セットをブロードキャストする役割を果たします。ドメイン内の RP を管理するには、1 つまたは複数の候補 BSR を選択します。候補 BSR の 1 つが、ドメインの BSR として選定されます。

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

図 3-1 に、BSR メカニズムの仕組みを示します。ここで、ルータ A（ソフトウェアによって選定された BSR）は、すべての有効なインターフェイスから BSR メッセージを送信しています（図の実線部分）。このメッセージには RP セットが含まれており、ネットワーク内のすべてのルータに次々とフラッディングされます。ルータ B および C は 候補 RP であり、選定された BSR に候補 RP アドバタイズメントを直接送信しています（図の破線部分）。

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

図 3-1　　BSR メカニズム



RP 選択プロセスの実行中、ソフトウェアは最も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もできます。1 つのグループに割り当てられる RP アドレスは 1 つだけです。

デフォルトでは、ルータは BSR メッセージの受信や転送を行いません。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。

BSR および候補 RP の設定方法については、「BSR の設定」（P.3-17）を参照してください。

Auto-RP

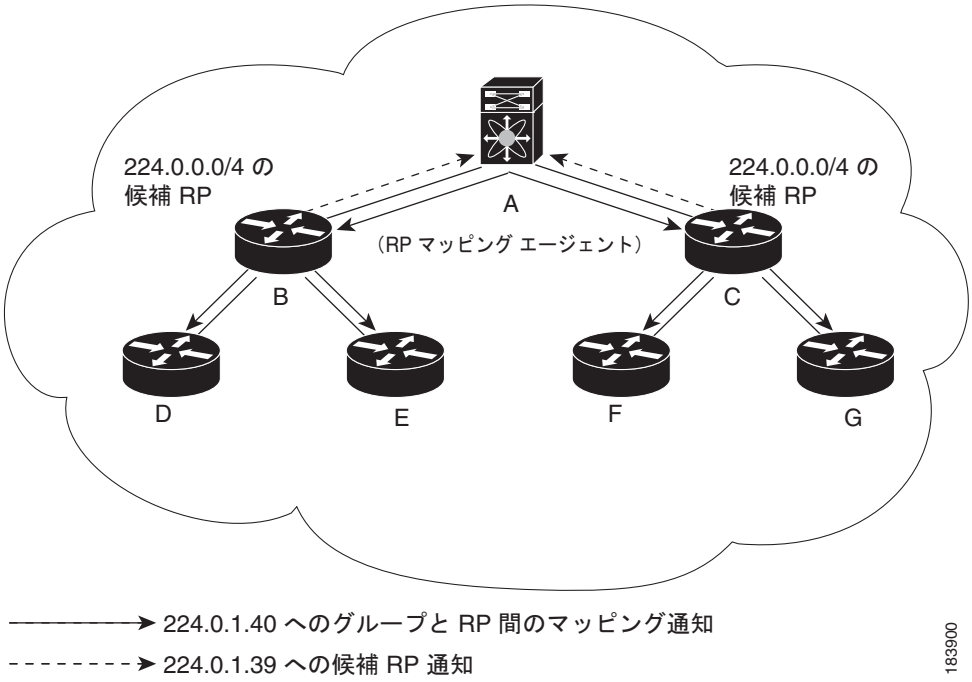
Auto-RP は、インターネット標準であるブートストラップ ルータ メカニズムの前身となったシスコのプロトコルです。Auto-RP を設定するには、候補マッピング エージェントおよび候補 RP を選択します。候補 RP は、サポート対象グループ範囲を含んだ RP-Announce メッセージを Cisco RP-Announce

マルチキャスト グループ 224.0.1.39 に送信します。Auto-RP マッピング エージェントは候補 RP からの RP-Announce メッセージを受信して、グループと RP 間のマッピング テーブルを形成します。マッピング エージェントは、このグループと RP 間の マッピング テーブルを RP-Discovery メッセージに格納して、Cisco RP-Discovery マルチキャスト グループ 224.0.1.40 にマルチキャストします。

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

図 3-2 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 3-2　Auto-RP のメカニズム



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

Auto-RP の設定方法については、「Auto-RP の設定」（P.3-19）を参照してください。

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

Anycast-RP の設定方法については、「PIM Anycast-RP セットの設定」（P.3-22）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 Designated Router（DR; 指定ルータ）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

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

PIM Register メッセージをフィルタリングするには、ルーティング ポリシーを定義します。PIM Register メッセージのポリシーの設定方法については、「ASM 専用の共有ツリーの設定」（P.3-23）を参照してください。

指定ルータ

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

各 LAN セグメントの DR は、「hello メッセージ」（P.3-2）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 メンバシップ レポートを受信すると、DR を経由するかどうかに関係なく、RP への最短パスが形成されます。これにより、同じマルチキャスト グループ上で送信を行うすべての送信元と、そのグループのすべての受信者を接続する共有ツリーが作成されます。

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

DR プライオリティの設定方法については、「PIM スパース モードの設定」（P.3-11）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。ドメイン境界パラメータの設定方法については、「PIM スパース モードの設定」（P.3-11）を参照してください。

Auto-RP スコープ パラメータを使用すると、Time-To-Live（TTL; 存続可能時間）値を設定できます。詳細については、「ASM 専用の共有ツリーの設定」（P.3-23）を参照してください。

仮想化のサポート

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

PIM の **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 の設定の詳細については、『*Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

PIM のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	PIM には、LAN Base Services ライセンスが必要です。Cisco NX-OS の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 の注意事項と制約事項

PIM には、次の注意事項と制限事項があります。

- Cisco NX-OS 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。
- スイッチに BSR ポリシーが適用されており、BSR として選定されないように設定されている場合、このポリシーは無視されます。これにより、次のようなデメリットが発生します。
  - ポリシーで許可されている BSM をスイッチが受信した場合、このスイッチが不正に BSR に選定されていると、対象の BSM がドロップされるためにダウンストリーム ルータではその BSM を受信できなくなります。また、ダウンストリーム スイッチでは、不正な BSR から送信された BSM が正しくフィルタリングされるため、これらのスイッチでは RP 情報を受信できなくなります。
  - BSR に異なるスイッチから送られた BSM が着信すると、新しい BSM が送信されますが、その正規の BSM はダウンストリーム スイッチで受信されなくなります。

デフォルト設定

表 3-1 に、PIM パラメータのデフォルト設定を示します。

表 3-1　PIM パラメータのデフォルト設定

パラメータ	デフォルト
共有ツリーだけを使用	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
ネイバーの変更の記録	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
SSM マルチキャスト グループ範囲またはポリシー	IPv4 の場合 232.0.0.0/8
PIM スパース モード	ディセーブル
DR プライオリティ	0
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

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（表 3-2 を参照）。

表 3-2　PIM のマルチキャスト配信モード

マルチキャスト配信モード	RP 設定の必要性	説明
ASM	必要	任意の送信元のマルチキャスト

表 3-2　PIM のマルチキャスト配信モード （続き）

マルチキャスト配信モード	RP 設定の必要性	説明
SSM	不可	単一送信元のマルチキャスト
マルチキャスト用 RPF ルート	不可	マルチキャスト用 RPF ルート

PIM を設定する手順は、次のとおりです。

ステップ 1　表 3-2 に示したマルチキャスト配信モードについて、各モードに設定するマルチキャスト グループの範囲を選択します。

ステップ 2　PIM 機能をイネーブルにします。「PIM 機能のイネーブル化」（P.3-10）を参照してください。

ステップ 3　PIM ドメインに参加させる各インターフェイスで、PIM スパース モードを設定します。「PIM スパース モードの設定」（P.3-11）を参照してください。

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

- ASM モードについては、「ASM の設定」（P.3-15）を参照してください。
- SSM モードについては、「SSM の設定」（P.3-26）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」（P.3-28）を参照してください。

ステップ 5　メッセージ フィルタリングを設定します。「メッセージ フィルタリングの設定」（P.3-30）を参照してください。

ここでは、次の内容について説明します。

（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。

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

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

手順の概要

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

手順の詳細

	コマンドまたは処理	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal` `switch(config)#`	コンフィギュレーション モードを開始します。
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）**feature** コマンドを含む、PIM の実行コンフィギュレーション情報を示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）コンフィギュレーションの変更を保存します。

PIM スパース モードの設定

スパース モード ドメインに参加させる各スイッチ インターフェイスで、PIM スパース モードを設定します。このとき、表 3-3 に示すスパース モード パラメータを設定できます。

表 3-3　PIM スパース モード パラメータ

パラメータ	説明
スイッチに対しグローバル	
Auto-RP メッセージ アクション	Auto-RP メッセージの受信と転送をイネーブルにします。これらの機能はデフォルトではディセーブルになっているため、候補 RP またはマッピング エージェントとして設定されていないルータは、Auto-RP メッセージの受信と転送を行いません。
BSR メッセージ アクション	BSR メッセージの受信と転送をイネーブルにします。これらの機能はデフォルトではディセーブルになっているため、候補 RP または BSR 候補として設定されていないルータは、BSR メッセージの受信と転送を行いません。
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。指定できる範囲は 1 ～ 65,535 です。デフォルト設定は無制限です。

表 3-3　PIM スパース モード パラメータ （続き）

パラメータ	説明
初期ホールドダウン期間	IPv4 初期ホールドダウン期間を秒単位で設定します。このホールドダウン期間は、MRIB が最初に起動するのにかかる時間です。コンバージェンスを高速化するには、小さい値を入力します。指定できる範囲は 90 ～ 210 です。ホールドダウン期間をディセーブルにするには、0 を指定します。デフォルト値は 210 です。
スイッチ インターフェイス単位	
PIM スパース モード	インターフェイス上の 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 Designated Router（DR; 指定ルータ）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、Rendezvous Point（RP; ランデブー ポイント）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。
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、Authentication Header（AH; 認証ヘッダー）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 インターバル	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。指定できる範囲は 1 ～ 4294967295 です。デフォルト値は 30000 です。
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[1] に基づいて、PIM ネイバーの隣接関係を設定します。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。

1. ルートマップ ポリシーの設定方法については、『*Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

マルチキャスト ルート マップの設定方法については、「RP 情報配信を制御するルート マップの設定」（P.3-29）を参照してください。

（注）　Join/Prune ポリシーの設定方法については、「メッセージ フィルタリングの設定」（P.3-30）を参照してください。

はじめる前に

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

手順の概要

1. **configure terminal**
2. （任意）**ip pim auto-rp** {**listen** [**forward**] | **forward** [**listen**]}
3. （任意）**ip pim bsr** {**listen** [**forward**] | **forward** [**listen**]}
4. （任意）**show ip pim rp** [*ip-prefix*] [**vrf** *vrf-name* | **all**]
5. （任意）**ip pim register-rate-limit** *rate*
6. （任意）[**ip** | **ipv4**] **routing multicast holddown** *holddown-period*
7. （任意）**show running-configuration pim**
8. **interface** *interface*
9. **no switchport**
10. **ip pim sparse-mode**
11. （任意）**ip pim dr-priority** *priority*
12. （任意）**ip pim hello-authentication ah-md5** *auth-key*
13. （任意）**ip pim hello-interval** *interval*
14. （任意）**ip pim border**
15. （任意）**ip pim neighbor-policy** *policy-name*
16. （任意）**show ip pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**]
17. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
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 メッセージの受信と転送をイネーブルにします。デフォルトではこれらの機能がディセーブルになっているため、Auto-RP メッセージの受信と転送は行われません。

	コマンド	目的
ステップ 3	**ip pim bsr** {**listen** [**forward**] | **forward** [**listen**]} 例： switch(config)# ip pim bsr forward	（任意）BSR メッセージの受信と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 メッセージの受信と転送は行われません。
ステップ 4	**show ip pim rp** [*ip-prefix*] [**vrf** *vrf-name* | **all**] 例： switch(config)# show ip pim rp	（任意）Auto-RP および BSR の受信 / 転送ステートなど、PIM RP 情報を表示します。
ステップ 5	**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。指定できる範囲は 1 ～ 65,535 です。デフォルト設定は無制限です。
ステップ 6	[**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。指定できる範囲は 90 ～ 210 です。ホールドダウン期間をディセーブルにするには、0 を指定します。デフォルト値は 210 です。
ステップ 7	**show running-configuration pim** 例： switch(config)# show running-configuration pim	（任意）Register レート制限を含めた PIM の実行コンフィギュレーション情報を表示します。
ステップ 8	**interface** *interface* 例： switch(config)# interface ethernet 2/1 switch(config-if)#	**ethernet** *slot/port* などのインターフェイス タイプおよび番号を入力して、インターフェイス モードを開始します。
ステップ 9	**no switchport** 例： switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 10	**ip pim sparse-mode** 例： switch(config-if)# ip pim sparse-mode	現在のインターフェイスで PIM スパース モードをイネーブルにします。デフォルトではディセーブルになっています。
ステップ 11	**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 Designated Router（DR; 指定ルータ）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。

	コマンド	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。指定できる範囲は 1 ～ 4294967295 です。デフォルト値は 30000 です。 **（注）** hello インターバルでは、アグレッシブ値はサポートされません。3000 ミリ秒未満の値は、hello インターバルの値としてアグレッシブです。
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）**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を設定します。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が行うことを推奨します。
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）コンフィギュレーションの変更を保存します。

ASM の設定

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

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。

ここでは、次の内容について説明します。

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 プレフィクスを示すルートマップ ポリシー名を指定できます。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal` `switch(config)#`	コンフィギュレーション モードを開始します。
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 プレフィクスを示すルートマップ ポリシー名を指定できます。デフォルト モードは ASM です。デフォルトのグループ範囲は 224.0.0.0 ～ 239.255.255.255 です。 この例では、指定したグループ範囲に PIM ASM モードを設定しています。

	コマンド	目的
ステップ 3	**show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] 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)# copy running-config startup-config	（任意）コンフィギュレーションの変更を保存します。

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（表 3-4 を参照）。

表 3-4　候補 BSR の引数

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

候補 RP の設定では引数を指定できます（表 3-5 を参照）。

表 3-5　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。

表 3-5　BSR 候補 RP の引数およびキーワード （続き）

引数またはキーワード	説明
interval	候補 RP メッセージの送信間隔（秒）。この値の範囲は 1 ～ 65,535 であり、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。この値の範囲は 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。

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。

ステップ 1　PIM ドメインの各ルータで BSR メッセージの受信と転送を行うかどうかを設定します。候補 RP または候補 BSR として設定されたルータは、インターフェイスにドメイン境界機能が設定されていない場合、すべての BSR プロトコル メッセージの受信と転送を自動的に実行します。詳細については、「PIM スパース モードの設定」（P.3-11）を参照してください。

ステップ 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。

ステップ 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。

ステップ 4　BSR メッセージ フィルタリングを設定します。「メッセージ フィルタリングの設定」（P.3-30）を参照してください。

はじめる前に

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

手順の概要

1. **configure terminal**
2. **ip pim** [**bsr**] **bsr-candidate** *interface* [**hash-len** *hash-length*] [**priority** *priority*]
3. **ip pim** [**bsr**] **rp-candidate** *interface* **group-list** *ip-prefix* [**priority** *priority*] [**interval** *interval*]
4. （任意）**show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**]
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**ip pim** [**bsr**] **bsr-candidate** *interface* [**hash-len** *hash-length*] [**priority** *priority*] 例： switch(config)# ip pim bsr-candidate ethernet 2/1 hash-len 24	候補 BootStrap Router（BSR; ブートストラップ ルータ）を設定します。ブートストラップ メッセージで使用される送信元 IP アドレスは、インターフェイスの IP アドレスです。ハッシュ長は 0 ～ 32 であり、デフォルト値は 30 です。プライオリティは 0 ～ 255 であり、デフォルト値は 64 です。パラメータの詳細については、表 3-4 を参照してください。
ステップ 3	**ip pim** [**bsr**] **rp-candidate** *interface* **group-list** *ip-prefix* [**priority** *priority*] [**interval** *interval*] 例： switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24	BSR の候補 RP を設定します。プライオリティは 0（プライオリティが最大）～ 65,535 であり、デフォルト値は 192 です。インターバルは 1 ～ 65,535 秒であり、デフォルト値は 60 秒です。 **（注）**　候補 RP インターバルは 15 秒以上に設定することを推奨します。 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* | **all**] 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）コンフィギュレーションの変更を保存します。

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（表 3-6 を参照）。

表 3-6　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 Time-To-Live（TTL; 存続可能時間）値。この値の範囲は 1 ～ 255 であり、デフォルト値は 32 です。 **（注）** 「PIM スパース モードの設定」（P.3-11）の境界ドメイン機能を参照してください。

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

候補 RP の設定では引数を指定できます（表 3-7 を参照）。

表 3-7　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。プレフィクス形式で指定します。
scope *ttl*	RP-Discovery メッセージが転送される最大ホップ数を表す Time-To-Live（TTL; 存続可能時間）値。この値の範囲は 1 ～ 255 であり、デフォルト値は 32 です。 **（注）** 「PIM スパース モードの設定」（P.3-11）の境界ドメイン機能を参照してください。
interval	RP-Announce メッセージの送信間隔（秒）。この値の範囲は 1 ～ 65,535 であり、デフォルト値は 60 です。 **（注）** 候補 RP インターバルは 15 秒以上に設定することを推奨します。

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。

ステップ 1　PIM ドメインの各ルータで、Auto-RP メッセージの受信と転送を行うかどうかを設定します。候補 RP または Auto-RP マッピング エージェントとして設定されたルータは、インターフェイスにドメイン境界機能が設定されていない場合、すべての Auto-RP プロトコル メッセージの受信と転送を自動的に実行します。詳細については、「PIM スパース モードの設定」（P.3-11）を参照してください。

ステップ 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。

ステップ 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。

ステップ 4　Auto-RP メッセージ フィルタリングを設定します。「メッセージ フィルタリングの設定」（P.3-30）を参照してください。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **例：** `switch# configure terminal` `switch(config)#`	コンフィギュレーション モードを開始します。
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。パラメータの詳細については、表 3-6 を参照してください。
ステップ 3	**ip pim** {**send-rp-announce**	{**auto-rp rp-candidate**}} *interface* **group-list** *ip-prefix* [**scope** *ttl*] [**interval** *interval*] **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。パラメータの詳細については、表 3-7 を参照してください。 **（注）**　候補 RP インターバルは 15 秒以上に設定することを推奨します。 この例では、ASM の候補 RP を設定しています。
ステップ 4	**show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name*	**all**] **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）コンフィギュレーションの変更を保存します。

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。

ステップ 1　PIM Anycast-RP セットに属するルータを選択します。

ステップ 2　PIM Anycast-RP セットの IP アドレスを選択します。

ステップ 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 およびローカル アドレスを設定します。

はじめる前に

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

手順の概要

1. **configure terminal**
2. **interface loopback** *number*
3. **ip address** *ip-prefix*
4. **exit**
5. **ip pim anycast-rp** *anycast-rp-address anycast-rp-peer-address*
6. RP セットに属する各ピア RP で、同じ *anycast-rp* を使用してステップ 5 を繰り返します。
7. （任意）**show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**]
8. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal` `switch(config)#`	コンフィギュレーション モードを開始します。
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	**exit** 例： `switch(config)# exit`	コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 5	**ip pim anycast-rp** *anycast-rp-address anycast-rp-peer-address* 例： switch(config)# ip pim anycast-rp 192.0.2.3 192.0.2.31	指定した Anycast-RP アドレスに対応する PIM Anycast-RP ピア アドレスを設定します。各コマンドで同じ Anycast-RP アドレスを指定して実行すると、Anycast-RP セットが作成されます。RP の IP アドレスは、同一セット内の RP との通信に使用されます。
ステップ 6	Anycast-RP セットに属する各ピア RP で、同じ Anycast-RP アドレスを使用してステップ 5 を繰り返します。	—
ステップ 7	**ip** [**autoconfig** | *ip-address* [**secondary**]]	（任意）リンクローカル プレフィクスと修正 EUI-64 形式のインターフェイス識別情報からリンクローカル アドレスを生成します。ここで、EUI-64 インターフェイス識別情報は関連する HSRP 仮想 MAC アドレスから作成されます。ip-address。 （任意）仮想ルータの仮想 IP アドレス（HSRP グループ）。この IP アドレスはインターフェイス IP アドレスと同じサブネット内になければなりません。その HSRP グループ内の 1 つ以上のルータに仮想 IP アドレスを設定する必要があります。グループ内の他のルータはこのアドレスを選択します。IP アドレスには IPv4 アドレスを指定できます。
ステップ 8	**show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] 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 9	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）コンフィギュレーションの変更を保存します。

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。

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。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal` `switch(config)#`	コンフィギュレーション モードを開始します。
ステップ 2	**ip pim use-shared-tree-only group-list** *policy-name* 例： `switch(config)# ip pim use-shared-tree-only group-list my_group_policy`	共有ツリーだけを構築します。共有ツリーから SPT へのスイッチオーバーは実行されません。**match ip multicast** コマンドで、使用するグループを示すルートマップ ポリシー名を指定します。デフォルトでは、送信元に対する (*, G) ステートのマルチキャスト パケットを受信すると、ソフトウェアは PIM (S, G) Join メッセージを送信元方向に発信します。
ステップ 3	**show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] 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)# copy running-config startup-config`	（任意）コンフィギュレーションの変更を保存します。

マルチキャスト ルーティング テーブルの最大エントリ数の設定

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

はじめる前に

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

手順の概要

1. **configure terminal**
2. **hardware profile multicast max-limit** *max-entries*
3. （任意）**show hardware profile status**
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**hardware profile multicast max-limit** *max-entries* 例： switch(config)# **hardware profile multicast max-limit** *3000*	マルチキャスト ルーティング テーブルの最大エントリ数を設定します。 マルチキャスト ルーティング テーブルの最大エントリ数は 0 ～ 4000 の範囲で指定できます。
ステップ 3	**show hardware profile status** 例： switch(config)# show hardware profile status	（任意）マルチキャスト ルーティング テーブルの制限に関する情報を表示します。
ステップ 4	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）コンフィギュレーションの変更を保存します。

RPT から SPT へのスイッチオーバー時の重複パケットの防止

Cisco NX-OS Release 5.0(3)U1(2) からは、RPT から SPT への移行中にハードウェアで重複パケットを防止できます。

（注）　このコマンドを使用して RPT から SPT へのスイッチオーバー時にパケットが重複しないようにすると、スイッチは 2 分ごとに 500 ルートのみというレートで送信元 (S, G) ルート インジェクションをサポートします。マルチキャスト ルーティング テーブルでは、送信元 (S, G) ルートに 500 のフリー エントリが必要です。

手順の概要

1. **configure terminal**
2. **hardware profile multicast prefer-source-tree**
3. （任意）**show hardware profile status**
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **例：** `switch# configure terminal` `switch(config)#`	コンフィギュレーション モードを開始します。
ステップ 2	**hardware profile multicast prefer-source-tree** **例：** `switch(config)# hardware profile multicast prefer-source-tree`	RPT から SPT への移行中にハードウェアで重複パケットを防止します。
ステップ 3	**show hardware profile status** **例：** `switch(config)# show ip pim group-range`	（任意）マルチキャスト ルーティング テーブルの制限に関する情報を表示します。
ステップ 4	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）コンフィギュレーションの変更を保存します。

SSM の設定

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

IPv4 ネットワーク上のホストから、送信元を特定してマルチキャスト データを要求するには、このホストおよびこのホストの DR で、IGMPv3 が実行されている必要があります。SSM モードでインターフェイスに PIM を設定する場合は、IGMPv3 をイネーブルにするのが一般的です。IGMPv1 または IGMPv2 が実行されているホストでは、SSM 変換を使用して、グループと送信元のマッピング設定を行うことができます。詳細については、第 2 章「IGMP の設定」を参照してください。

コマンドラインに値を指定することにより、SSM で使用するグループ範囲を設定できます。デフォルトでは、PIM に対する SSM グループ範囲は 232.0.0.0/8 です。

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

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

はじめる前に

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal` `switch(config)#`	コンフィギュレーション モードを開始します。
ステップ 2	**ip pim ssm range** {*ip-prefix* | **none**} | **route-map** *policy-name*} 例： `switch(config)# ip pim ssm range 239.128.1.0/24`	SSM モードで処理するグループ範囲を最大 4 つまで設定します。**match ip multicast** コマンドで、使用するグループ プレフィクスを示すルートマップ ポリシー名を指定できます。デフォルトの範囲は 232.0.0.0/8 です。キーワード **none** を指定すると、すべてのグループ範囲が削除されます。
	no ip pim ssm {**range** {*ip-prefix* | **none**} | **route-map** *policy-name*} 例： `switch(config)# no ip pim ssm range none`	SSM 範囲から指定のプレフィクスを削除するか、ルートマップ ポリシーを削除します。キーワード **none** を指定すると、SSM 範囲はデフォルトの 232.0.0.0/8 にリセットされます。

	コマンド	目的
ステップ 3	**show ip pim group-range** [*ip-prefix*] [**vrf** *vrf-name* | **all**] 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)# copy running-config startup-config	（任意）コンフィギュレーションの変更を保存します。

マルチキャスト用 RPF ルートの設定

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

マルチキャスト ルートはトラフィック転送に直接使用されるわけではなく、RPF チェックのために使用されます。マルチキャスト用 RPF ルートは再配布できません。マルチキャスト転送の詳細については、「マルチキャスト転送」（P.1-4）を参照してください。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
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 192.0.2.33/24 192.0.2.1	RPF 計算で使用するマルチキャスト用 RPF ルートを設定します。ルート プリファレンスは 1 ～ 255 です。デフォルト プリファレンスは 1 です。

	コマンド	目的
ステップ 3	**show ip static-route** [**vrf** *vrf-name*] 例： switch(config)# show ip static-route	（任意）設定済みのスタティック ルートを表示します。
ステップ 4	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）コンフィギュレーションの変更を保存します。

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 マップを使用できるコマンドについては、「メッセージ フィルタリングの設定」（P.3-30）を参照してください。

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

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

はじめる前に

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
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。このコンフィギュレーション モードでは、**permit** キーワードを使用します。
ステップ 3	**match ip multicast** {{**rp** *ip-address* [**rp-type** *rp-type*] [**group** *ip-prefix*]} | {**group** *ip-prefix* [**rp** *ip-address* [**rp-type** *rp-type*]]} 例： switch(config)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type ASM	指定した グループ、RP、および RP タイプを関連付けます。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 モードでは、グループおよび RP を指定する必要があります。
ステップ 4	**show route-map** 例： switch(config-route-map)# show route-map	（任意）設定済みのルート 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）コンフィギュレーションの変更を保存します。

メッセージ フィルタリングの設定

表 3-8 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 3-8　PIM メッセージのフィルタリング

メッセージ タイプ	説明
スイッチに対しグローバル	
ネイバーの変更の記録	ネイバーのステート変更を通知する Syslog メッセージをイネーブルにします。デフォルトではディセーブルになっています。
PIM Register ポリシー	ルートマップ ポリシー[1] 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。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。

表 3-8　PIM メッセージのフィルタリング （続き）

メッセージ タイプ	説明
BSR 候補 RP ポリシー	ルートマップ ポリシー [1] に基づく、BSR 候補 RP メッセージのフィルタリングをイネーブルにします。**match ip multicast** コマンドで、RP、グループ アドレス、およびタイプ（ASM）を指定できます。このコマンドは、BSR の選定対象のルータで使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。
BSR ポリシー	ルートマップ ポリシー [1] に基づく、BSR クライアント ルータによる BSR メッセージのフィルタリングをイネーブルにします。**match ip multicast** コマンドで、BSR 送信元アドレスを指定できます。このコマンドは、BSR メッセージを受信するクライアント ルータで使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。
Auto-RP 候補 RP ポリシー	ルートマップ ポリシー [1] 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、およびタイプ（ASM）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 [1] に基づく、クライアント ルータによる Auto-RP Discovery メッセージのフィルタリングをイネーブルにします。**match ip multicast** コマンドで、マッピング エージェント送信元アドレスを指定できます。このコマンドは、Discovery メッセージを受信するクライアント ルータで使用できます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。
スイッチ インターフェイス単位	
Join/Prune ポリシー	ルートマップ ポリシー [1] 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。

1. ルートマップ ポリシーの設定方法については、『*Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

マルチキャスト ルート マップの設定方法については、「RP 情報配信を制御するルート マップの設定」（P.3-29）を参照してください。

はじめる前に

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

手順の概要

1. **configure terminal**
2. （任意）**ip pim log-neighbor-changes**
3. （任意）**ip pim register-policy** *policy-name*
4. （任意）**ip pim bsr rp-candidate-policy** *policy-name*
5. （任意）**ip pim bsr bsr-policy** *policy-name*
6. （任意）**ip pim auto-rp rp-candidate-policy** *policy-name*

7. （任意）**ip pim auto-rp mapping-agent-policy** *policy-name*
8. **interface** *interface*
9. **no switchport**
10. （任意）**ip pim jp-policy** *policy-name* [**in** | **out**]
11. （任意）**show run pim**
12. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal` `switch(config)#`	コンフィギュレーション モードを開始します。
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。
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 ポリシーに基づく、BSR 候補 RP メッセージのフィルタリングをイネーブルにします。**match ip multicast** コマンドで、RP、グループ アドレス、およびタイプ（ASM）を指定できます。このコマンドは、BSR の選定対象のルータで使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。
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、およびタイプ（ASM）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。

	コマンド	目的
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。
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	**no switchport** 例： switch(config-if)# no switchport	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 10	**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。 このコマンドは、送信および着信の両方向のメッセージをフィルタリングします。
ステップ 11	**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 12	**copy running-config startup-config** 例： switch(config-if)# copy running-config startup-config	（任意）コンフィギュレーションの変更を保存します。

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。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンド	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)#`	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）コンフィギュレーションの変更を保存します。

PIM 設定の確認

PIM の設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show ip mroute {*source group* | *group* [*source*]} [**vrf** *vrf-name* | **all**]	IP マルチキャスト ルーティング テーブルを表示します。
show ip pim group-range [**vrf** *vrf-name* | **all**]	学習済みまたは設定済みのグループ範囲およびモードを表示します。同様の情報に関し、**show ip pim rp** コマンドも参照してください。
show ip pim interface [*interface* | **brief**] [**vrf** *vrf-name* | **all**]	情報をインターフェイス別に表示します。
show ip pim neighbor [**vrf** *vrf-name* | **all**]	ネイバーをインターフェイス別に表示します。

コマンド	目的
show ip pim oif-list *group* [*source*] [**vrf** *vrf-name* | **all**]	OIF リスト内のすべてのインターフェイスを表示します。
show ip pim route {source group | group [source]} [**vrf** *vrf-name* | **all**]	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* | **all**]	ソフトウェアの既知の Rendezvous Point（RP; ランデブー ポイント）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。同様の情報に関し、**show ip pim group-range** コマンドも参照してください。
show ip pim rp-hash [**vrf** *vrf-name* | **all**]	BootStrap Router（BSR; ブートストラップ ルータ）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。
show startup-configuration pim	実行コンフィギュレーション情報を表示します。
show ip pim vrf [*vrf-name* | **all**] [**detail**]	各 VRF の情報を表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 3000 Series Command Reference*』を参照してください。

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コマンドについて説明します。

ここでは、次の内容について説明します。

PIM 統計情報の表示

表 3-9 に、PIM の統計情報とメモリ使用状況を表示するコマンドを示します。PIM の場合は、このコマンドの **show ip** 形式を使用します。

表 3-9　PIM 統計情報コマンド

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

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 3000 Series Command Reference*』を参照してください。

PIM 統計情報のクリア

PIM 統計情報をクリアするには、表 3-10 に示す各種コマンドを使用します。PIM の場合は、このコマンドの **show ip** 形式を使用します。

表 3-10　統計情報をクリアする PIM コマンド

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* | **all**]	PIM プロセスで使用されるグローバル カウンタをクリアします。

PIM の設定例

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

ここでは、次の内容について説明します。

- 「SSM の設定例」（P.3-36）
- 「BSR の設定例」（P.3-37）
- 「PIM Anycast-RP の設定例」（P.3-38）

SSM の設定例

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

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

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

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

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

ステップ 3　デフォルト範囲を使用しない場合は、SSM 範囲を設定します。

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

ステップ 4　メッセージ フィルタリングを設定します。

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

次に、SSM モードを設定する例を示します。

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

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。

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

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

ステップ 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
```

ステップ 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
```

ステップ 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
```

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

PIM Anycast-RP の設定例

PIM 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。

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

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

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

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

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

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

ステップ 4　すべてのルータで Anycast-RP として使用される RP-address を設定します。

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

ステップ 5　Anycast-RP セットに加える各ルータについて、Anycast-RP パラメータとして Anycast-RP の IP アドレスを指定します。同じ作業を、Anycast-RP の各 IP アドレスで繰り返します。この例では、2 つの Anycast-RP を指定しています。

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

ステップ 6　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 を使用して、PIM ASM モードを設定する例を示します。

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

次の作業

PIM の関連機能を設定するには、次の章を参照してください。

- 第 2 章「IGMP の設定」
- 第 4 章「IGMP スヌーピングの設定」
- 第 5 章「MSDP の設定」

その他の関連資料

PIM の実装に関する詳細情報については、次の項目を参照してください。

- 「関連資料」（P.3-39）
- 「規格」（P.3-39）
- 「MIB」（P.3-39）
- 付録 A「IP マルチキャストに関する IETF RFC」
- 「PIM 機能の履歴」（P.3-40）

関連資料

関連項目	参照先
CLI コマンド	『*Cisco Nexus 3000 Series Command Reference*』
VRF の設定	『*Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。	—

MIB

MIB	MIB のリンク
IPMCAST-MIB	適切な MIB を選択してダウンロードするには、次の URL を参照してください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

PIM 機能の履歴

表 3-11 に、この機能のリリース履歴を示します。

表 3-11　PIM 機能の履歴

機能名	リリース	機能情報
PIM	5.0(3)U1(1)	この機能が導入されました。

CHAPTER 4

IGMP スヌーピングの設定

この章では、Cisco NX-OS スイッチ上で Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピングを設定する方法について説明します。

この章は、次の内容で構成されています。

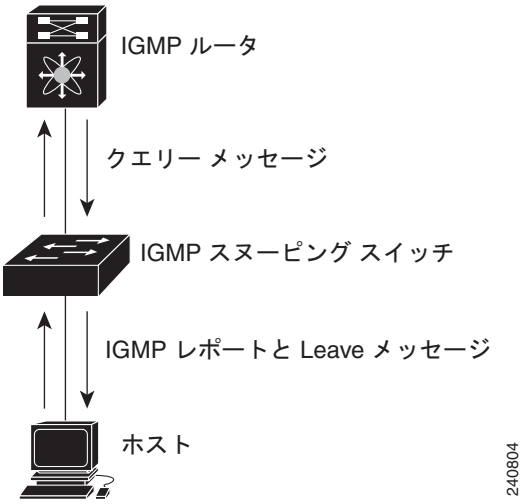
IGMP スヌーピングの情報

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

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）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 トラフィックを検査して、対象の受信者が接続され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 メンバシップ レポートの転送機能を強化します。トポロジの変更通知には、IGMP スヌーピング ソフトウェアが応答します。デフォルトでは、IGMP スヌーピングがスイッチでイネーブルにされています。

図 4-1 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 4-1　IGMP スヌーピング スイッチ



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

IGMP の詳細については、第 2 章「IGMP の設定」を参照してください。

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

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

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

ここでは、次の内容について説明します。

IGMPv1 および IGMPv2

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

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

IGMPv1 では、明示的な IGMP Leave メッセージが存在しないため、特定のグループについてマルチキャスト データを要求するホストが存続しないことを示すために、メンバシップ 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。この発信元をベースとするフィルタリングにより、マルチキャスト グループにトラフィックを送信する発信元に基づくポートのセットにマルチキャスト トラフィックを制限するようにスイッチがイネーブルにされます。

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

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

IGMP スヌーピング クエリア

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

IGMP スヌーピング クエリアがイネーブルな場合は、定期的に IGMP クエリーが送信されるため、IP マルチキャスト トラフィックを要求するホストから IGMP レポート メッセージが発信されます。IGMP スヌーピングはこれらの IGMP レポートを受信し、必要に応じて転送します。

ルータ ポートにおける IGMP フィルタリング

IGMP フィルタリングにより、スイッチをレイヤ 3 マルチキャスト スイッチにつなぐルータ ポートをスイッチ上に設定できるようになります。スイッチは、手動で設定されたすべてのスタティック ルート ポートを、スイッチのルータ ポート リストに保存します。

スイッチは IGMP パケットを受信すると、VLAN 内のルータ ポートを介してトラフィックを転送します。スイッチは、受信した PIM hello メッセージまたは IGMP クエリーから、ポートがルータ ポートとして認識します。

VRF を使用した IGMP スヌーピング

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

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

VRF の設定の詳細については、『*Cisco Nexus 3000 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

次の表に、この機能のライセンス要件を示します。

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すべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS の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。 **（注）** レイヤ 3 インターフェイスをイネーブルにするため、スイッチに LAN Base Services ライセンスをインストールする必要があります。

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。

- スイッチにログインしている。
- 現在の Virtual Routing and Forwarding（VRF; 仮想ルーティングおよびフォワーディング）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。

デフォルト設定

表 4-1 に、IGMP スヌーピング パラメータのデフォルト設定を示します。

表 4-1　デフォルト IGMP スヌーピング パラメータ

パラメータ	デフォルト
IGMP スヌーピング	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
最終メンバーのクエリー 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

表 4-1　デフォルト IGMP スヌーピング パラメータ （続き）

パラメータ	デフォルト
リンクローカル グループ抑制	イネーブル
スイッチ全体での 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

IGMP スヌーピング プロセスの動作を変更するには、表 4-2 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。

表 4-2　IGMP スヌーピング パラメータ

パラメータ	説明
IGMP スヌーピング	スイッチまたは各 VLAN に対して、IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。 （注）　グローバル設定がディセーブルになっていると、個々の VLAN がイネーブルであるかどうかに関係なく、すべての VLAN がディセーブルと見なされます。
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 メンバシップ レポートを、VLAN 別に追跡します。デフォルトではイネーブルになっています。
高速脱退	ソフトウェアが IGMP Leave レポートを受信した場合に、IGMP クエリー メッセージを送信することなく、グループ ステートを解除できるようにします。このパラメータは、IGMPv2 ホストに関して、各 VLAN ポート上のホストが 1 つしか存在しない場合に使用されます。デフォルトではディセーブルになっています。
最終メンバーのクエリー 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、最終メンバーのクエリー 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。
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。
レポート抑制	スイッチまたは各 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。レポート抑制がディセーブルの場合、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転送されます。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 ルータへの静的な接続を設定します。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。

表 4-2　IGMP スヌーピング パラメータ （続き）

パラメータ	説明
スタティック グループ	VLAN のレイヤ 2 ポートをマルチキャスト グループのスタティック メンバーとして設定します。
リンクローカル グループ抑制	スイッチまたは各 VLAN に対して、リンクローカル グループ抑制を設定します。デフォルトではイネーブルになっています。
IGMPv3 レポート抑制	スイッチまたは各 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、スイッチ全体でディセーブルになっており、VLAN ごとにイネーブルになっています。

手順の概要

1. **configure terminal**
2. **ip igmp snooping**
3. **vlan** *vlan-id*
4. **ip igmp snooping**
   ip igmp snooping explicit-tracking
   ip igmp snooping fast-leave
   ip igmp snooping last-member-query-interval *seconds*
   ip igmp snooping querier *ip-address*
   ip igmp snooping report-suppression
   ip igmp snooping mrouter interface *interface*
   ip igmp snooping static-group *group-ip-addr* [**source** *source-ip-addr*] **interface** *interface*
   ip igmp snooping link-local-groups-suppression
   ip igmp snooping v3-report-suppression
   （任意）**copy running-config startup-config**

手順の詳細

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

	コマンド	目的
ステップ 3	**vlan** *vlan-id* 例： switch(config)# vlan 2 switch(config-vlan)#	VLAN コンフィギュレーション モードを開始します。
ステップ 4	**ip igmp snooping** 例： switch(config-vlan)# ip igmp snooping	現在の VLAN に対して IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。
	ip igmp snooping explicit-tracking 例： switch(config-vlan)# 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 メンバシップ レポートを、VLAN 別に追跡します。デフォルトではすべての VLAN でイネーブルになっています。
	ip igmp snooping fast-leave 例： switch(config-vlan)# 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。デフォルトでは、すべての VLAN でディセーブルになっています。
	ip igmp snooping last-member-query-interval *seconds* 例： switch(config-vlan)# 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、最終メンバーのクエリー 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。
	ip igmp snooping querier *ip-address* 例： switch(config-vlan)# 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。メッセージ内では、送信元として IP アドレスが使用されます。
	ip igmp snooping report-suppression 例： switch(config-vlan)# 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。レポート抑制がディセーブルの場合、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転送されます。デフォルトではイネーブルになっています。 **（注）** グローバル コンフィギュレーション モードでこのコマンドを実行し、すべてのインターフェイスを変更することもできます。
	ip igmp snooping mrouter interface *interface* 例： switch(config-vlan)# ip igmp snooping mrouter interface ethernet 2/1	マルチキャスト ルータへの静的な接続を設定します。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* 例： switch(config-vlan)# 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。

コマンド	目的
ip igmp snooping link-local-groups-suppression **例：** `switch(config-vlan)# ip igmp snooping link-local-groups-suppression`	リンクローカル グループ抑制を設定します。デフォルトではイネーブルになっています。 **（注）** グローバル コンフィギュレーション モードでこのコマンドを実行し、すべてのインターフェイスを変更することもできます。
ip igmp snooping v3-report-suppression **例：** `switch(config-vlan)# ip igmp snooping v3-report-suppression`	IGMPv3 レポート抑制およびプロキシ レポートを設定します。デフォルトでは、スイッチ全体のグローバル コマンドでディセーブルになっており、VLAN ごとにイネーブルになっています。 **（注）** グローバル コンフィギュレーション モードでこのコマンドを実行し、すべてのインターフェイスを変更することもできます。
ステップ 5 **copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）コンフィギュレーションの変更を保存します。

IGMP スヌーピング設定の検証

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

コマンド	目的
show ip igmp snooping [**vlan** *vlan-id*]	IGMP スヌーピング設定を VLAN 別に表示します。
show ip igmp snooping groups [*source* [*group*] | *group* [*source*]] [**vlan** *vlan-id*] [**detail**]	グループに関する IGMP スヌーピング情報を VLAN 別に表示します。
show ip igmp snooping 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。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 3000 Series Command Reference*』を参照してください。

IGMP スヌーピング統計情報の表示

IGMP スヌーピング統計情報を表示するには、**show ip igmp snooping statistics vlan** コマンドを使用します。

IGMP スヌーピング統計情報を消去するには、**clear ip igmp snooping statistics vlan** コマンドを使用します。

これらのコマンドの詳細については、『*Cisco Nexus 3000 Series Command Reference*』を参照してください。

IGMP スヌーピングの設定例

次に、IGMP スヌーピング パラメータの設定例を示します。

```
configure terminal
  ip igmp snooping
  vlan 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
```

次の作業

PIM の関連機能をイネーブルにするには、次の章を参照してください。

- 第 2 章「IGMP の設定」
- 第 5 章「MSDP の設定」

その他の関連資料

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

- 「関連資料」（P.4-9）
- 「規格」（P.4-9）
- 「IGMP スヌーピングの機能の履歴」（P.4-10）

関連資料

関連項目	参照先
CLI コマンド	『*Cisco Nexus 3000 Series Command Reference*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。	—

IGMP スヌーピングの機能の履歴

表 4-3 に、この機能のリリース履歴を示します。

表 4-3　IGMP スヌーピングの機能の履歴

機能名	リリース	機能情報
IGMP スヌーピング	5.0(3)U1(1)	この機能が導入されました。

CHAPTER 5

MSDP の設定

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

この章は、次の内容で構成されています。

MSDP の情報

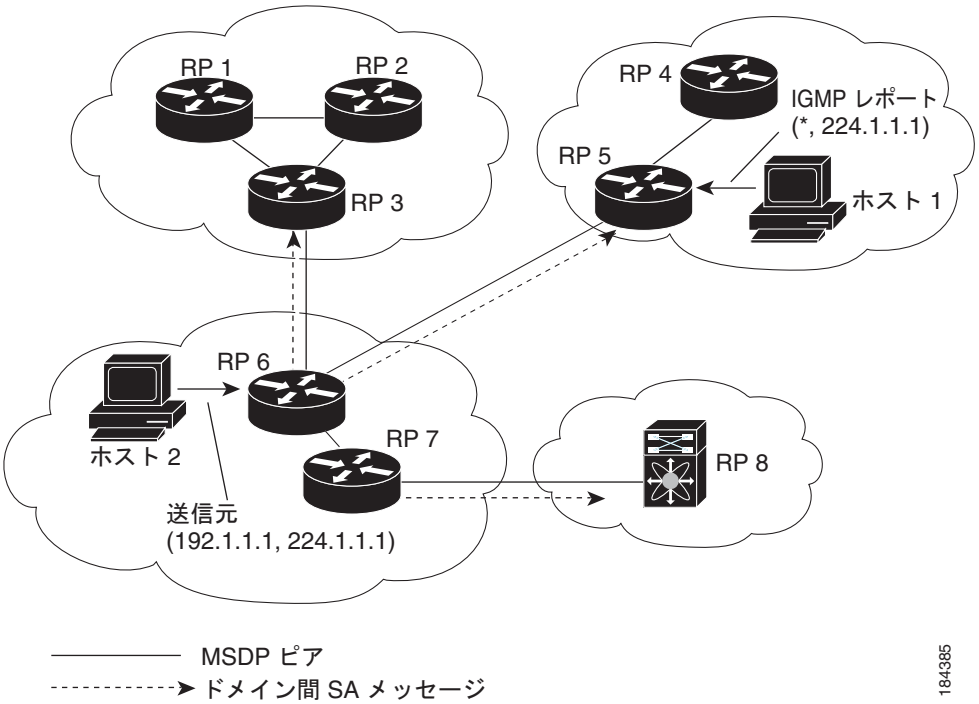
MSDP を使用すると、複数の Border Gateway Protocol（BGP; ボーダ ゲートウェイ プロトコル）対応 Protocol Independent Multicast（PIM）スパース モード ドメイン間で、マルチキャスト送信元情報を交換できます。PIM の詳細については、第 3 章「PIM の設定」を参照してください。BGP の詳細については、『*Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

受信者が要求するグループが別のドメイン内の送信元から送信されたグループと一致した場合、Rendezvous Point（RP; ランデブー ポイント）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。Designated Router（DR; 指定ルータ）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 Transmission Control Protocol（TCP; 転送制御プロトコル）接続を介して構築されます。

図 5-1 に、4 つの PIM ドメインを示します。接続された各 RP（ルータ）は、独自にマルチキャスト送信元のセットを保持しているため、RP は MSDP ピアと呼ばれます。送信元ホスト 1 はグループ 224.1.1.1 にマルチキャスト データを送信します。MSDP プロセスでは、RP 6 上で PIM Register メッセージを介して送信元に関する情報を学習すると、ドメイン内の送信元に関する情報が、Source-Active（SA）メッセージの一部として MSDP ピアに送信されます。SA メッセージを受信した

RP 3 および RP 5 は、MSDP ピアに SA メッセージを転送します。RP 5 は、ホスト 2 から 224.1.1.1 のマルチキャスト データに対する要求を受信すると、192.1.1.1 のホスト 1 方向に PIM Join メッセージを送信して、送信元への最短パス ツリーを構築します。

図 5-1　異なる PIM ドメインに属する RP 間の MSDP ピアリング



各 RP 間で MSDP ピアリング設定を行うには、フル メッシュを作成します。一般的な MSDP フル メッシュは、RP 1、RP 2、RP 3 のように自律システム内に作成され、自律システム間には作成されません。ループ抑制および MSDP ピア Reverse Path Forwarding（RPF）により、SA メッセージのループを防止するには、BGP を使用します。メッシュ グループの詳細については、「MSDP メッシュ グループ」（P.5-3）を参照してください。

（注） PIM ドメイン内で Anycast RP（ロード バランシングおよびフェールオーバーを実行するための RP のセット）を使用する場合、MSDP を設定する必要はありません。詳細については、「PIM Anycast-RP セットの設定」（P.3-22）を参照してください。

MSDP の詳細については、RFC 3618 を参照してください。

ここでは、次の内容について説明します。

- 「SA メッセージおよびキャッシング」（P.5-3）
- 「MSDP ピア RPF 転送」（P.5-3）
- 「MSDP メッシュ グループ」（P.5-3）
- 「仮想化のサポート」（P.5-3）

SA メッセージおよびキャッシング

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

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

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

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

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

MSDP ピア RPF 転送

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

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

MSDP メッシュ グループ

MSDP メッシュ グループを使用すると、ピア RPF フラッディングで生成される SA メッセージ数を抑えることができます。図 5-1 の RP 1、RP 2、および RP 3 は、RP 6 から SA メッセージを受信しています。メッシュ内のすべてのルータ間にピアリング関係を設定してから、これらのルータのメッシュ グループを作成すると、あるピアから発信される SA メッセージが他のすべてのピアに送信されます。メッシュ内のピアが受信した SA メッセージは転送されません。RP 3 が発信する SA メッセージは、RP 1 および RP 2 に転送されますが、これらの RP は受信したメッセージをメッシュ内のその他の RP には転送しません。

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

仮想化のサポート

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

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

VRF の設定の詳細については、『*Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

MSDP のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	MSDP には、LAN Base Services ライセンスが必要です。Cisco NX-OS の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。

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

デフォルト設定

表 5-1 に、MSDP パラメータのデフォルト設定を示します。

表 5-1　MSDP パラメータのデフォルト設定

パラメータ	デフォルト
説明	ピアの説明はありません。
管理シャットダウン	ピアは定義された時点でイネーブルになります。
MD5 パスワード	すべての MD5 パスワードがディセーブルになっています。
SA ポリシー（IN）	すべての SA メッセージが受信されます。
SA ポリシー（OUT）	発信される SA メッセージには登録済みの全送信元が含まれます。
SA の上限	上限は定義されていません。
発信元インターフェイスの名前	ローカル システムの RP アドレスです。
グループの上限	グループの上限は定義されていません。
SA インターバル	60 秒

MSDP の設定

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

MSDP ピアリングの設定手順は次のとおりです。

ステップ 1　MSDP ピアとして動作させるルータを選択します。

ステップ 2　MSDP 機能をイネーブルにします。「MSDP 機能のイネーブル化」（P.5-5）を参照してください。

ステップ 3　ステップ 1 で選択した各ルータで、MSDP ピアを設定します。「MSDP ピアの設定」（P.5-6）を参照してください。

ステップ 4　各 MSDP ピアでオプションの MSDP ピア パラメータを設定します。「MSDP ピア パラメータの設定」（P.5-8）を参照してください。

ステップ 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。「MSDP グローバル パラメータの設定」（P.5-10）を参照してください。

ステップ 6　各 MSDP ピアでオプションのメッシュ グループを設定します。「MSDP メッシュ グループの設定」（P.5-11）を参照してください。

（注）　MSDP をイネーブルにする前に入力された MSDP コマンドは、キャッシュに格納され、MSDP がイネーブルになると実行されます。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。

ここでは、次の内容について説明します。

（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

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

手順の概要

1. **configure terminal**
2. **feature msdp**
3. （任意）**show running-configuration | grep** *feature*

4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal` `switch(config)#`	コンフィギュレーション モードを開始します。
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 | grep** *feature* 例： `switch# show running-configuration | grep feature`	（任意）指定された **feature** コマンドを表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意）コンフィギュレーションの変更を保存します。

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

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

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

手順の概要

1. **configure terminal**
2. **ip msdp peer** *peer-ip-address* **connect-source** *interface* [**remote-as** *as-number*]
3. 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。
4. （任意）**show ip msdp summary** [**vrf** *vrf-name* | *known-vrf-name* | **all**]
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
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* | *known-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）コンフィギュレーションの変更を保存します。

MSDP ピア パラメータの設定

表 5-2 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 5-2　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。[1] デフォルトでは、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 SA メッセージのルートマップ ポリシー。[1] 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。
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。

1. ルートマップ ポリシーの設定方法については、『*Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

マルチキャスト ルート マップの設定方法については、「RP 情報配信を制御するルート マップの設定」（P.3-29）を参照してください。

（注） メッシュ グループの設定方法については、「MSDP メッシュ グループの設定」（P.5-11）を参照してください。

はじめる前に

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

手順の概要

1. **configure terminal**
2. **ip msdp description** *peer-ip-address string*
   ip msdp shutdown *peer-ip-address*
   ip msdp password *peer-ip-address password*
   ip msdp sa-policy *peer-ip-address policy-name* **in**
   ip msdp sa-policy *peer-ip-address policy-name* **out**
   ip msdp sa-limit *peer-ip-address limit*
3. （任意）**show ip msdp peer** [*peer-address*] [**vrf** *vrf-name* | *known-vrf-name* | **all**]
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal` `switch(config)#`	コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp description** *peer-ip-address string* 例： `switch(config)# ip msdp description 192.168.1.10 peer in Engineering network`	ピアの説明を示すストリングを設定します。デフォルトでは、ピアの説明は設定されていません。
	ip msdp shutdown *peer-ip-address* 例： `switch(config)# ip msdp shutdown 192.168.1.10`	ピアをシャットダウンします。デフォルトでは、各ピアは定義した時点でイネーブルになります。
	ip msdp password *peer-ip-address password* 例： `switch(config)# ip msdp password 192.168.1.10 my_md5_password`	ピアの MD5 パスワードをイネーブルにします。デフォルトでは、MD5 パスワードはディセーブルになっています。
	ip msdp sa-policy *peer-ip-address policy-name* **in** 例： `switch(config)# ip msdp sa-policy 192.168.1.10 my_incoming_sa_policy in`	着信 SA メッセージのルートマップ ポリシーをイネーブルにします。デフォルトでは、すべての SA メッセージが受信されます。
	ip msdp sa-policy *peer-ip-address policy-name* **out** 例： `switch(config)# ip msdp sa-policy 192.168.1.10 my_outgoing_sa_policy out`	発信 SA メッセージのルートマップ ポリシーをイネーブルにします。デフォルトでは、発信される SA メッセージには登録済みの全送信元が含まれます。
	ip msdp sa-limit *peer-ip-address limit* 例： `switch(config)# ip msdp sa-limit 192.168.1.10 5000`	ピアから受信可能な (S, G) エントリ数の上限を設定します。デフォルトでは、上限はありません。

	コマンド	目的
ステップ 3	**show ip msdp peer** [*peer-address*] [**vrf** *vrf-name* | *known-vrf-name* | **all**] 例： switch# show ip msdp peer 1.1.1.1	（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）コンフィギュレーションの変更を保存します。

MSDP グローバル パラメータの設定

表 5-3 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 5-3　MSDP グローバル パラメータ

パラメータ	説明
発信元インターフェイスの名前	SA メッセージ エントリの RP フィールドで使用される IP アドレス。Anycast RP を使用する場合は、すべての RP に対して同じ IP アドレスを使用します。このパラメータを使用すると、各 MSDP ピアの RP に一意の IP アドレスを定義できます。デフォルトでは、ローカル システムの RP アドレスが使用されます。
グループの上限	指定したプレフィ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。デフォルト値は 60 秒です。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
ステップ 2	**ip msdp originator-id** *interface* 例： switch(config)# ip msdp originator-id loopback0	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。インターフェイスは *type slot/port* という形式で表します。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。
	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。デフォルト値は 60 秒です。
ステップ 3	**show ip msdp summary** [**vrf** *vrf-name* | *known-vrf-name* | **all**] 例： switch# show ip msdp summary	（任意）MSDP 設定の要約を表示します。
ステップ 4	**copy running-config startup-config** 例： switch(config)# copy running-config startup-config	（任意）コンフィギュレーションの変更を保存します。

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

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

手順の概要

1. **configure terminal**
2. **ip msdp mesh-group** *peer-ip-addr mesh-name*
3. 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。

4. （任意）**show ip msdp mesh-group** [*mesh-group*] [**vrf** *vrf-name* | *known-vrf-name* | **all**]
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
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*	*known-vrf-name*	**all**] 例： switch# show ip msdp summary	（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）コンフィギュレーションの変更を保存します。

MSDP プロセスの再起動

MSDP プロセスを再起動し、オプションとして、すべてのルートをフラッシュすることができます。

はじめる前に

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**restart msdp** 例： switch# restart msdp	MSDP プロセスを再起動します。
ステップ 2	**configure terminal** 例： switch# configure terminal switch(config)#	コンフィギュレーション モードを開始します。
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）コンフィギュレーションの変更を保存します。

MSDP の設定の確認

MSDP の設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show ip msdp count [*as-number*] [**vrf** *vrf-name* | *known-vrf-name* | **all**]	MSDP (S, G) エントリ数およびグループ数を AS 番号別に表示します。
show ip msdp mesh-group [*mesh-group*] [**vrf** *vrf-name* | *known-vrf-name* | **all**]	MSDP メッシュ グループ設定を表示します。
show ip msdp peer [*peer-address*] [**vrf** *vrf-name* | *known-vrf-name* | **all**]	MSDP ピアの MSDP 情報を表示します。
show ip msdp rpf [*rp-address*] [**vrf** *vrf-name* | *known-vrf-name* | **all**]	RP アドレスへの BGP パス上にあるネクストホップ AS を表示します。
show ip msdp sources [**vrf** *vrf-name* | *known-vrf-name* | **all**]	MSDP で学習された送信元と、グループ上限設定に関する違反状況を表示します。
show ip msdp summary [**vrf** *vrf-name* | *known-vrf-name* | **all**]	MSDP ピア設定の要約を表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 3000 Series Command Reference*』を参照してください。

統計情報の表示

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

ここでは、次の内容について説明します。

統計情報の表示

MSDP 統計情報を表示するには、表 5-4 に示す各種コマンドを使用します。

表 5-4　MSDP 統計情報コマンド

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

統計情報のクリア

MSDP 統計情報をクリアするには、表 5-5 に示す各種コマンドを使用します。

表 5-5　MSDP 統計情報をクリアするコマンド

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

MSDP の設定例

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

ステップ 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
```

ステップ 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
```

ステップ 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
```

ステップ 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、図 5-1 で示した 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
```

その他の関連資料

MSDP の実装に関する詳細情報については、次の項目を参照してください。

- 「関連資料」（P.5-16）
- 「規格」（P.5-16）
- 付録 A「IP マルチキャストに関する IETF RFC」

関連資料

関連項目	参照先
CLI コマンド	『*Cisco Nexus 3000 Series Command Reference*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能で変更された既存規格のサポートはありません。	—

IGMP の機能の履歴

表 5-6 に、この機能のリリース履歴を示します。

表 5-6　MSDP の機能の履歴

機能名	リリース	機能情報
MSDP	5.0(3)U1(1)	この機能が導入されました。

APPENDIX 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、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）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。

RFC	タイトル
RFC 2236	『*Internet Group Management Protocol, Version 2*』
RFC 2365	『*Administratively Scoped IP Multicast*』
RFC 2858	『*Multiprotocol Extensions for BGP-4*』
RFC 3376	『*Internet Group Management Protocol, Version 3*』
RFC 3446	『*Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*』
RFC 3569	『*An Overview of Source-Specific Multicast (SSM)*』
RFC 3618	『*Multicast Source Discovery Protocol (MSDP)*』
RFC 4541	『*Considerations for Internet Group Management Protocol (IGMP) Snooping Switches*』
RFC 4601	『*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*』
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*』

INDEX

記号

A

B

D

E

I

M

O

P

R

S

る