Cisco Nexus 36000 スイッチ NX-OS マルチキャスト ルーティング構成ガイド、リリース 10.4（X）

最終更新：2025 年 7 月 31 日

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

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html. Cisco product warranty information is available at https://www.cisco.com/c/en/us/products/warranty-listing.html. US Federal Communications Commission Notices are found here https://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.

目 次

対象読者 ix

表記法 x

Cisco Nexus Fabric Manager の関連資料 xii

通信、サービス、およびその他の情報 xiii

第 1 章 新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

第 2 章 概要 3

ライセンス要件 3

サポートされるプラットフォーム 3

マルチキャストについて 3

マルチキャスト配信ツリー 4

送信元ツリー 4

共有ツリー 5

マルチキャスト転送 6

PIM 7

アーキテクチャ セールス マネージャ（ASM） 9

SSM 9

マルチキャスト用 RPF ルート 9

IGMP 9

IGMP スヌーピング 10
ドメイン内マルチキャスト 10
SSM 10
MRIB 10
一般的なマルチキャスト制約事項 12
SW と HW マルチキャスト ルート間の不一致のトラブルシューティング 12
その他の参考資料 12
MIB 13

第 3 章 **IGMP の設定** 15
IGMP について 15
IGMP のバージョン 16
IGMP の基礎 16
仮想化のサポート 18
IGMP に関する注意事項と制限事項 19
IGMP のデフォルト設定 19
IGMP パラメータの設定 20
IGMP インターフェイス パラメータの設定 20
IGMP SSM 変換の設定 27
ルータ アラートの適用オプション チェックの設定 29
IGMP 構成の確認 30
IGMP の設定例 30
次の作業 31

第 4 章 **PIM の設定** 33
PIM に関する情報 33
vPC を使用した PIM SSM 34
Hello メッセージ 35
Join-Prune メッセージ 35
ステートのリフレッシュ 36
ランデブー ポイント 36

スタティック RP 36
BSR 37
Auto-RP 38
Anycast-RP 39
PIM 登録メッセージ 40
指定ルータ 40
管理用スコープの IP マルチキャスト 41
仮想化のサポート 41
PIM の前提条件 41
PIM の注意事項と制約事項 42
PIM のデフォルト設定 42
PIM の設定 43
PIM 機能の有効化 44
PIM スパース モードの設定 45
ASM を構成 48
静的 RP の設定 48
BSR の設定 49
Auto-RP の設定 52
PIM エニーキャスト RP セットの設定（PIM） 54
ASM 専用の共有ツリーの設定 56
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 57
SSM（PIM）の設定 58
vPC を介した PIM SSM の設定 59
マルチキャスト用 RPF ルートの設定 61
マルチキャスト マルチパスの無効化 61
RP 情報配信を制御するルート マップの設定 62
メッセージ フィルタリングの設定 63
メッセージ フィルタリングの設定 64
ルートのフラッシュ 66
PIM 設定の確認 67
統計の表示 68

PIM 統計情報の表示 68
PIM 統計情報のクリア 68
PIM の設定例 69
SSM の構成例 69
vPC を介した PIM SSM の構成例 70
BSR の設定例 73
PIM Anycast-RP の設定例 74
次の作業 76
その他の参考資料 76
関連資料 76
MIB 76

第 5 章 IGMP スヌーピングの構成 77
IGMP スヌーピングの情報 77
IGMPv1 および IGMPv2 78
IGMPv3 79
IGMPスヌーピングクエリア 79
ルータ ポートでの IGMP フィルタ処理 80
IGMP スヌーピングに関する注意事項と制限事項 80
IGMP スヌーピングのデフォルト設定 81
IGMP スヌーピング パラメータの設定 82
IGMP スヌーピング設定の確認 90
マルチキャスト ルートの間隔を設定 91
IGMP スヌーピング統計情報の表示 91
IGMP スヌーピングの設定例 91

第 6 章 MSDP の設定 93
MSDP について 93
SA メッセージおよびキャッシング 94
MSDP ピア RPF 転送 95
MSDP メッシュ グループ 95

MSDP の前提条件 95
デフォルト設定 96
MSDP の設定 96
MSDP 機能の有効化 97
MSDP ピアの構成 98
MSDP ピア パラメータの設定 99
MSDP グローバル パラメータの設定 102
MSDP メッシュ グループの設定 104
MSDP プロセスの再起動 105
MSDP の設定の確認 106
MSDP のモニタリング 107
統計の表示 107
統計情報のクリア 107
MSDP の設定例 107
関連資料 109
標準 109

第 7 章 **MVR の設定** 111
MVR について 111
MVR の他の機能との相互運用性 112
MVR と IGMP スヌーピング 112
MVR と vPC 112
MVR に関する注意事項と制約事項 113
MVR のデフォルト設定 113
MVR の設定 113
MVR グローバル パラメータの設定 114
MVR インターフェイスの設定 115
VLAN からの IGMP クエリ転送の抑制 117
MVR 設定の確認 118
MVR 設定の例 120

付録 A： IP マルチキャストについての IETF RFC 121
IP マルチキャストについての IETF RFC 121

対象読者

このマニュアルは、Cisco Nexus Fabric Manager の設置、設定、および維持に携わるネットワーク管理者を対象としています。

表記法

表記法

コマンドの説明には、次のような表記法が使用されます。

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

例では、次の表記法を使用しています。

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

表記法

表記法	説明
[ ]	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。

Cisco Nexus Fabric Manager の関連資料

Cisco Nexus Fabric Manager の関連資料

- Cisco Nexus 9000 シリーズ NX-OS 基本構成ガイド、リリース 7.x

  http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/fundamentals/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Fundamentals_Configuration_Guide_7x.html

- Cisco Nexus 9000 シリーズ NX-OS インターフェイス設定ガイド、リリース 7.x

  http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/interfaces/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Interfaces_Configuration_Guide_7x.html

- Cisco Nexus 9000 Series NX-OS システム管理構成ガイド、リリース 7.x

  http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/system_management/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_System_Management_Configuration_Guide_7x.html

- Cisco Nexus 9000 シリーズ NX-OS VXLAN 構成ガイド、リリース 7.x

  http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/vxlan/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x.html

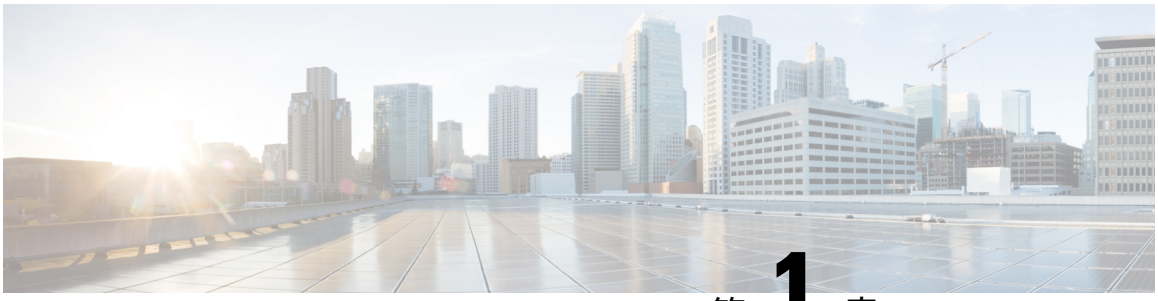
通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によって求めるビジネス成果を得るには、Cisco Services [英語] にアクセスしてください。
- サービスリクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet [英語] にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press [英語] にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

シスコバグ検索ツール

シスコバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイとして機能する、Webベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

通信、サービス、およびその他の情報



第 1 章

新機能および変更された機能に関する情報

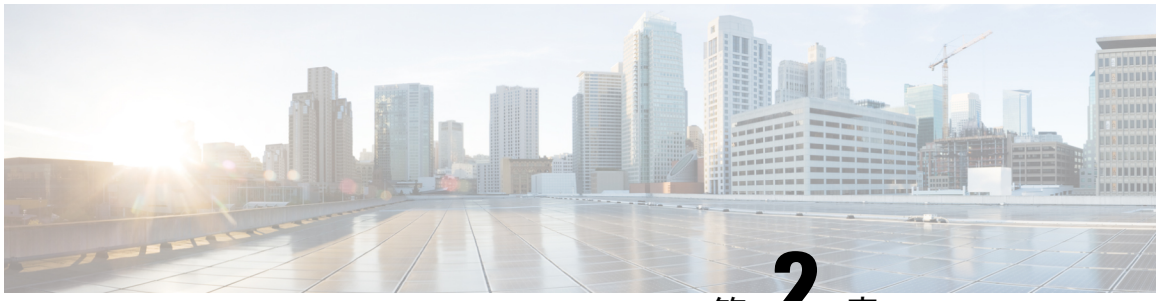
• 新機能および変更された機能に関する情報 （1 ページ）

新機能および変更された機能に関する情報

表 *1 : NX-OS* リリース *10.4(x)* の新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
NA	このリリースで追加された新機能はありません。	10.4(1)F	N/A

新機能および変更された機能に関する情報



第 2 章

概要

この章では、Cisco Nexus 3600 プラットフォーム スイッチの Cisco NX-OS マルチキャスト機能について説明します。

この章は、次の項で構成されています。

- ライセンス要件 （3 ページ）
- サポートされるプラットフォーム （3 ページ）
- マルチキャストについて （3 ページ）
- 一般的なマルチキャスト制約事項 （12 ページ）
- SW と HW マルチキャスト ルート間の不一致のトラブルシューティング （12 ページ）
- その他の参考資料 （12 ページ）

ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS* ライセンス ガイド』および『*Cisco NX-OS* ライセンス オプション ガイド』を参照してください。

サポートされるプラットフォーム

Cisco NX-OS リリース 7.0(3)I7(1) 以降では、Nexus スイッチ プラットフォーム サポート マトリクスに基づいて、選択した機能をさまざまな Cisco Nexus 9000 および 3000 スイッチで使用するために、どの Cisco NX-OS リリースが必要かを確認してください。

マルチキャストについて

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

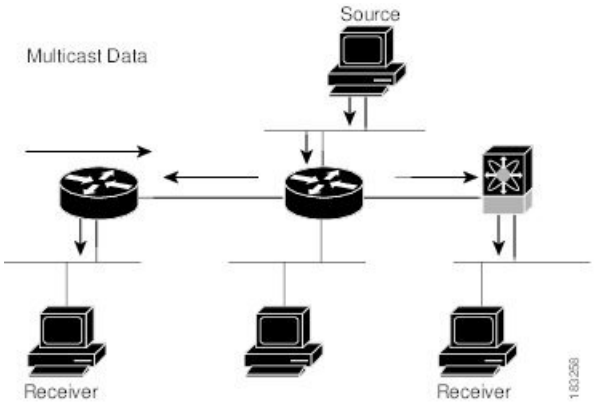
マルチキャストには、グループと呼ばれるIPマルチキャストアドレスに送信されたマルチキャスト データの送信側と受信側の配信と検出の両方の手法が含まれます。グループと送信元 IP アドレスが入ったマルチキャストアドレスは、しばしばチャネルと呼ばれます。Internet Assigned Number Authority（IANA）では、IPv4 マルチキャスト アドレスとして、224.0.0.0 ～ 239.255.255.255 を割り当てています。詳細については、http://www.iana.org/assignments/multicast-addresses を参照してください。

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

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

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

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



マルチキャスト配信ツリー

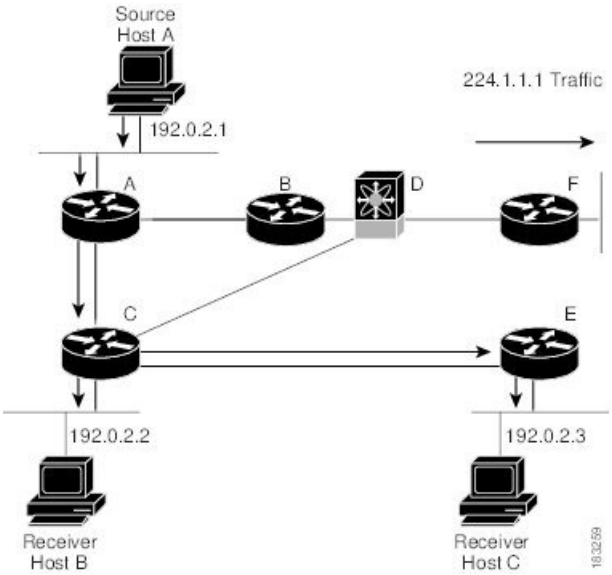
マルチキャスト配信ツリーとは、送信元と受信者を中継するルータ間の、マルチキャストデータの伝送パスを表します。マルチキャスト ソフトウェアはサポートするマルチキャスト方式に応じて、タイプの異なるツリーを構築します。

送信元ツリー

送信元ツリーは、送信元からネットワーク経由でマルチキャストトラフィックを伝送する場合の最短パスです。特定のマルチキャスト グループへと送信されたマルチキャスト トラフィックが、同じグループのトラフィックを要求する受信者へと転送されます。送信元ツリーは、最短パスとしての特性から、最短パス ツリー（SPT）と呼ばれることがあります。次の図は、ホ

ストAを起点とし、ホストBおよびCに接続されているグループ224.1.1.1の送信元ツリーを示しています。

図 *2*:送信元ツリー

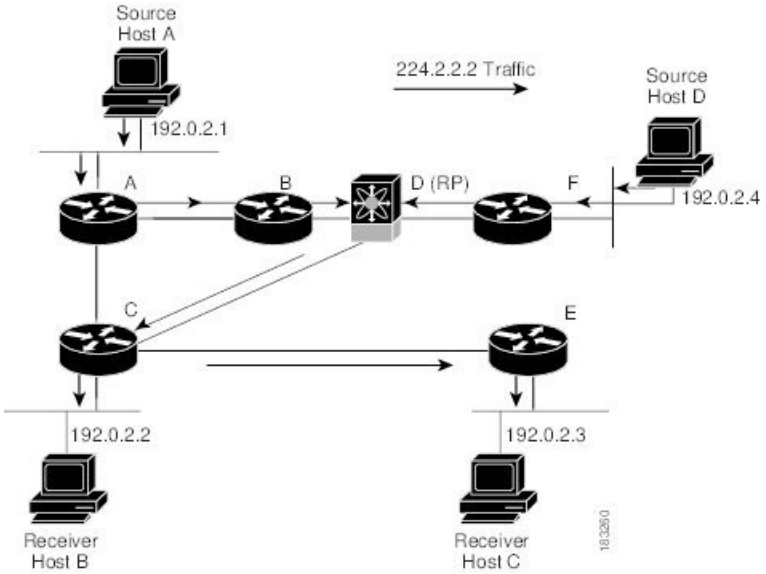


表記（S,G）は、グループGの任意の送信元からのマルチキャストトラフィックを表します。この図のSPTは、（192.0.2.1, 224.1.1.1）と記述されます。同じグループの複数の送信元からトラフィックを送信できます。

共有ツリー

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

図 *3:* 共有ツリー



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

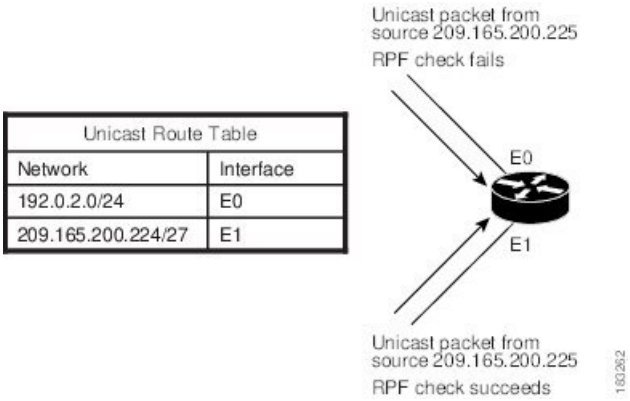
マルチキャスト転送

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

マルチキャスト パケットが着信するたびに、ルータは RPF チェックを実行します。送信元に接続されたインターフェイスにパケットが着信した場合は、グループの発信インターフェイス（OIF）リスト内の各インターフェイスにパケットが転送されます。それ以外の場合、パケットはドロップされます。

次の図に、異なるインターフェイスから着信したパケットについて、RPFチェックを行う場合の例を示します。E0 に着信したパケットは、RPF チェックに失敗します。これは、ユニキャスト テーブルで、対象の送信元ネットワークがインターフェイス E1 に関連付けられているためです。E1 に着信したパケットは、RPF チェックに合格します。これは、ユニキャスト ルート テーブルで、対象の送信元ネットワークがインターフェイス E1 に関連付けられているためです。

図 *4 : RPF* チェックの例



PIM

Cisco NX-OS は Protocol Independent Multicast（PIM）スパース モードを使用したマルチキャストをサポートしています。PIM は IP ルーティング プロトコルに依存せず、使用されているすべてのユニキャスト ルーティング プロトコルが提供するユニキャスト ルーティング テーブルを利用できます。PIM スパース モードでは、ネットワーク上の要求元だけにマルチキャスト トラフィックが伝送されます。PIM デンス モードは Cisco NX-OS ではサポートされていません。

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

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

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

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

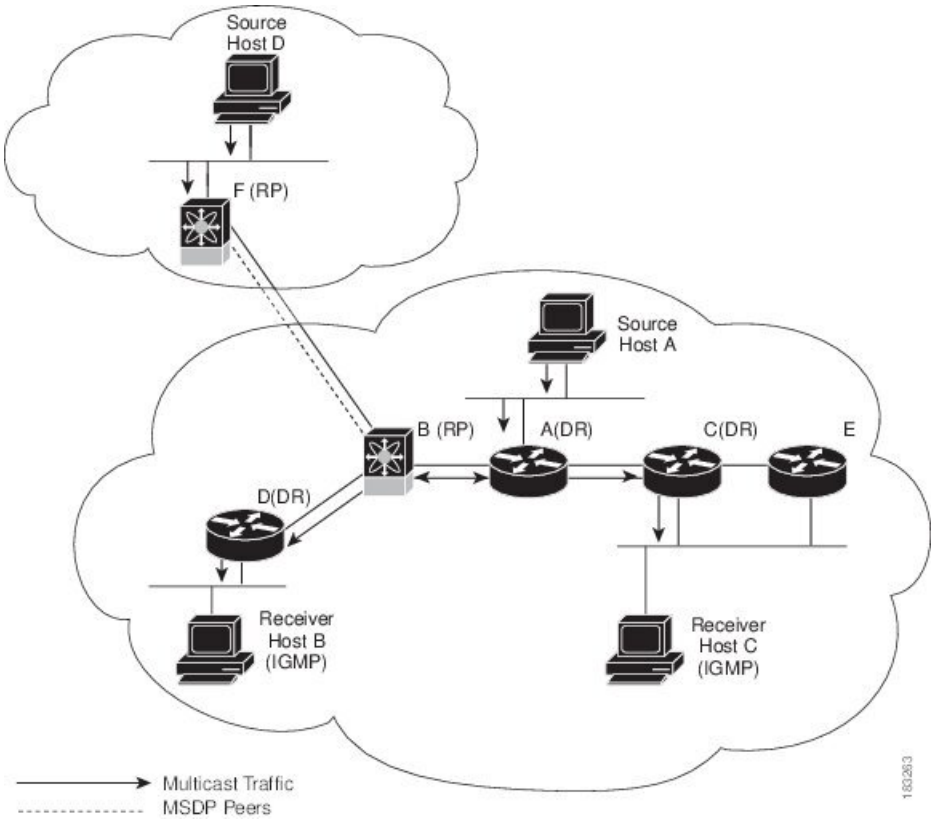
ルータはユニキャスト ルーティング テーブルおよび RPF ルートを使用して、マルチキャスト ルーティング情報を生成します。

次の図に、IPv4 ネットワーク内の 2 つの PIM ドメインを示します。

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

次の図に、IPv4 ネットワーク内の 2 つの PIM ドメインを示します。

図 *5: IPv4* ネットワーク内の *PIM* ドメイン



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

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

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

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

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

アーキテクチャ セールス マネージャ（ASM）

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

RP を設定する場合、デフォルト モードは ASM モードです。

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

SSM

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

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

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

マルチキャスト用 RPF ルート

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

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

IGMP

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

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

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

IGMP の構成に関する詳細は、「 IGMP の設定 （15 ページ） 」を参照してください。

IGMP スヌーピング

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

IGMP スヌーピングの構成に関する詳細は、「 IGMP スヌーピングの構成 （77 ページ） 」を参照してください。

ドメイン内マルチキャスト

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

SSM

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

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

SSM の構成に関する詳細は、「SSM （PIM） の設定 （58 ページ） 」セクションを参照してください。

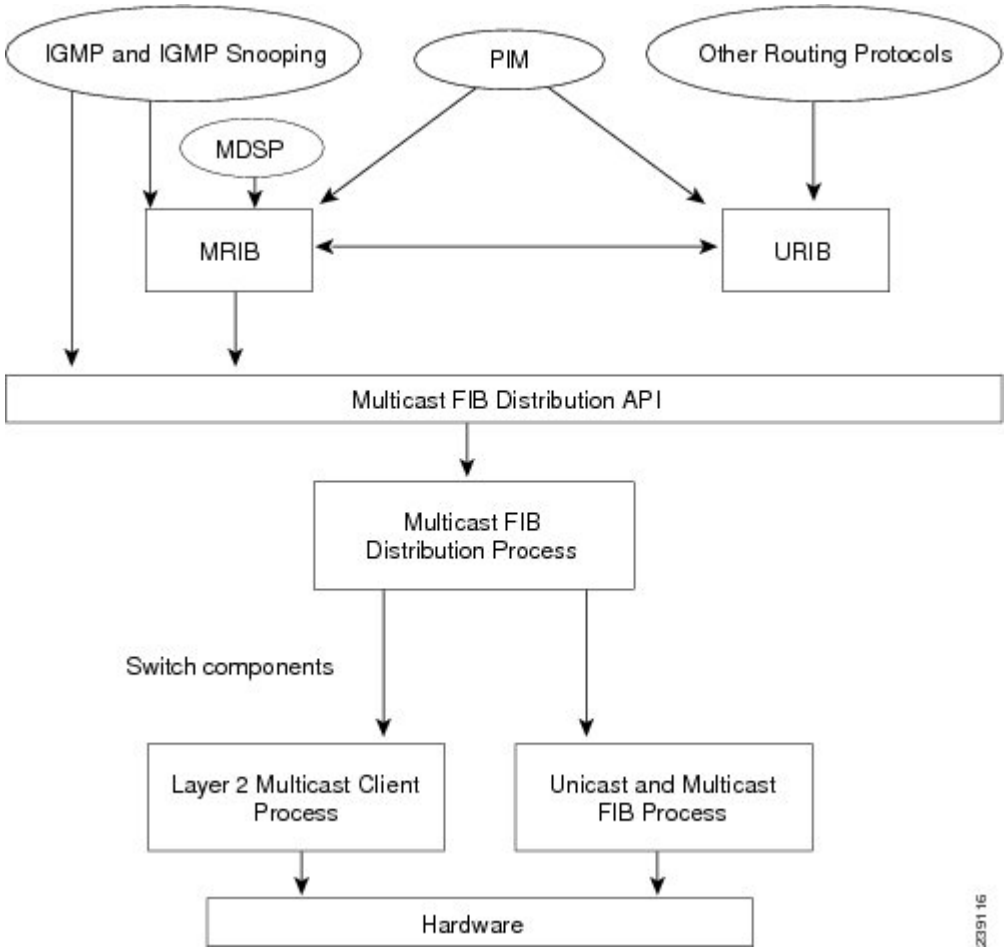
MRIB

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

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

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

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



一般的なマルチキャスト制約事項

以下は、マルチキャストの Cisco Nexus 3600 プラットフォーム スイッチの注意事項と制約事項です：

- Cisco Nexus 3600 プラットフォーム スイッチは、Pragmatic General Multicast（PGM）をサポートしていません。
- レイヤ 3 IPv6 マルチキャスト ルーティングはサポートされていません。
- レイヤ 2 IPv6 マルチキャスト パケットは、着信 VLAN でフラッディングされます。
- マルチキャストは、Cisco Nexus 3600 プラットフォーム スイッチではサポートされていません。

SW と HW マルチキャスト ルート間の不一致のトラブルシューティング

症状

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

考えられる原因

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

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

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

改善処置

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

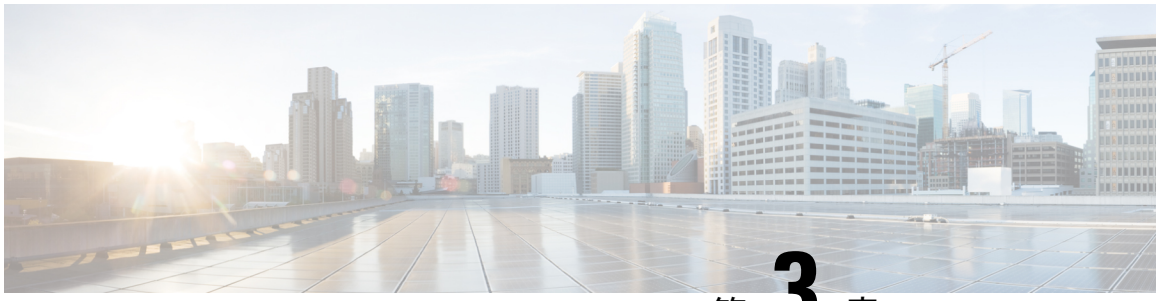
その他の参考資料

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

- IP マルチキャストについての IETF RFC

MIB

MIB	MIB のリンク
IP Multicast：IP マルチキャスト	MIB を検索してダウンロードするには、次の MI 動します。



第 3 章

IGMP の設定

この章では、IPv4 ネットワーク用に Cisco Nexus 3600 プラットフォーム スイッチでインターネット グループ管理プロトコル（IGMP）を構成する方法について説明します。

この章は、次の項で構成されています。

- IGMP について （15 ページ）
- IGMP に関する注意事項と制限事項 （19 ページ）
- IGMP のデフォルト設定 （19 ページ）
- IGMP パラメータの設定 （20 ページ）
- IGMP 構成の確認 （30 ページ）
- IGMP の設定例 （30 ページ）
- 次の作業 （31 ページ）

IGMP について

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

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

- PIM をイネーブルにします。
- 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をします。
- リンクローカル グループ レポートのイネーブル化

IGMP のバージョン

スイッチでは、IGMPv2 と IGMPv3、および IGMPv1 のレポート受信がサポートされています。

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

IGMPv3 には、次に示す IGMPv2 からの重要な変更点があります。

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

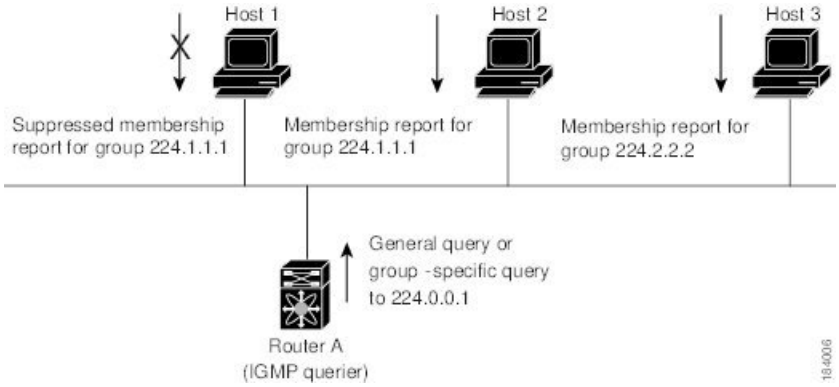
IGMPv2 の詳細については、RFC 2236 を参照してください。

IGMPv3 の詳細については、RFC 3376 を参照してください。

IGMP の基礎

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

図 *7: IGMPv1* および *IGMPv2* クエリ応答プロセス



IGMPv1 および IGMPv2 クエリ応答プロセスの図では、ルータ A（サブネットの代表 IGMP クエリア）は、すべてのホストが含まれる 224.0.0.1 ホスト マルチキャスト グループに定期的にクエリ メッセージを送信して、マルチキャスト データを受信するホストを検出します。グループ メンバーシップ タイムアウト値を設定できます。指定したタイムアウト値が経過すると、ルータはサブネット上にグループのメンバーまたは送信元が存在しないと見なします。IGMP

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

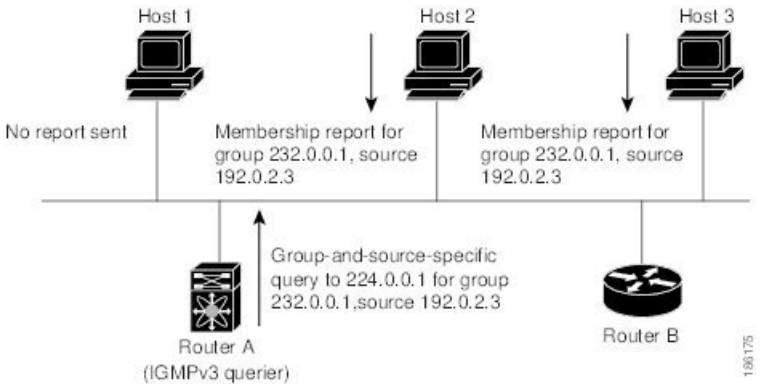
IP アドレスが最小のルータが、サブネットの IGMP クエリアとして選出されます。ルータは、自身よりも下位の IP アドレスを持つルータからクエリー メッセージを継続的に受信している間、クエリア タイムアウト値をカウントするタイマーをリセットします。ルータのクエリア タイマーが期限切れになると、そのルータは代表クエリアになります。そのあとで、このルータが、自身よりも下位の IP アドレスを持つルータからのホスト クエリー メッセージを受信すると、ルータは代表クエリアとしての役割をドロップしてクエリア タイマーを再度設定します。

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

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

次の図のルータ A は、IGMPv3 グループ/ソース固有のクエリを LAN に送信します。ホスト 2 および 3 は、アドバタイズされたグループおよび送信元からデータを受信することを示すメンバーシップ レポートを送信して、そのクエリーに応答します。この IGMPv3 機能では、SSM がサポートされます。IGMPv1 ホストおよび IGMPv2 ホストが SSM をサポートするよう、SSM を変換する方法については、「IGMP SSM 変換の設定 （27 ページ）」セクションを参照してください。

図 *8 : IGMPv3* グループ/ソース固有のクエリ



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

代表クエリアから送信されるメッセージの存続可能時間（TTL）値は 1 です。つまり、サブネット上の直接接続されたルータは、メッセージを転送しません。IGMP の起動時に送信されるクエリ メッセージの頻度および回数を個別に設定したり、スタートアップ クエリ インターバルを短く設定したりすることで、グループ ステートの確立時間を最小限に抑えることができます。不要ですが、起動後のクエリー インターバルをチューニングすることで、ホスト グループ メンバーシップ メッセージへの応答性と、ネットワーク上のトラフィック量のバランスを調整できます。

⚠

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

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

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

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

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

仮想化のサポート

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

- IGMP は、インターフェイスごとに有効化または無効化されています。
- IGMPv1、IGMPv2、および IGMPv3 によりルータ側のサポートを提供します。
- IGMPv2 および IGMPv3 によりホスト側のサポートを提供します。
- 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 レポートがサポートされています。

- IGMP SSM 変換により IGMPv2 グループを送信元のセットにマッピング
- マルチキャスト トレースルート（Mtrace）リクエストを処理する Mtrace サーバー機能のサポート

VRF 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。

IGMP に関する注意事項と制限事項

IGMP に関する注意事項および制限事項は次のとおりです。

- すべての外部マルチキャスト ルーター ポート(静的に構成されているか、動的に学習されている) は、グローバル LTL インデックスを使用します。ミスがある場合、VLAN X のトラフィックは、VLAN X を許可するすべてのマルチキャスト ルータ ポートに送信されます。
- ip igmp join-group コマンドを使用すると、スイッチをマルチキャスト グループにバインドできます。スイッチは、指定されたグループに対して Internet Group Management Protocol（IGMP）結合を生成し、このグループに送信されるマルチキャスト パケットはすべて CPU に送信されます。ip igmp join-group コマンドを使用して Outgoing Interface Lists（OILs）をプログラムすることはできません。ストリームに対して要求するレシーバがある場合でも、パケットは送信されません。スイッチをマルチキャスト グループにバインドするには、ip igmp join-group コマンドの代わりに ip igmp static-oif コマンドを使用します。
- IGMPv3（RFC 3376）に従って送信元のリストを除外またはブロックすることはサポートされていません。

IGMP のデフォルト設定

次の表に、IGMP パラメータのデフォルト設定を示します。

表 *2 : IGMP* パラメータのデフォルト設定

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

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

IGMP インターフェイス パラメータの設定

オプションの IGMP インターフェイス パラメータは、次のテーブルで構成できます。

表 *3: IGMP* インターフェイス パラメータ

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

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

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

パラメータ	説明
レポート ポリシー	ルートマップ ポリシーに基づく、IGMP レポートのアクセス ポリシー。 （注） ルートマップ ポリシーを構成するには、『Cisco Nexus 3600 NX-OS ユニキャスト ルーティング構成ガイド』を参照してください。
アクセス グループ	インターフェイスが接続されたサブネット上のホストについて、加入可能なマルチキャスト グループを制御するためのルートマップ ポリシーを構成するオプション。
即時離脱	デバイスからグループ固有のクエリーが送信されないため、所定の IGMP インターフェイスで IGMPv2 グループ メンバーシップの脱退のための待ち時間を最小限にできるオプション。即時脱退をイネーブルにすると、デバイスではグループに関する Leave メッセージの受信後、ただちにマルチキャスト ルーティング テーブルからグループ エントリが削除されます。デフォルトではディセーブルになっています。 （注） このコマンドは、所定のグループに対するインターフェイスの背後に 1 つの受信者しか存在しない場合に使用します。
global-leave-ignore-gss-mrt	Cisco NX-OS リリース 5.0（3）U1（2）以降では、IGMP グローバル Leave メッセージに応答するために低い MRT 値に対してグループ固有クエリに構成した最大応答時間（MRT）値を使用できます（IGMP leave は、グループ 0.0.0.0 にレポートします）。

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

手順の概要

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

14. **ip igmp last-member-query-response-time** *seconds*
15. **ip igmp last-member-query-count** *count*
16. **ip igmp group-timeout** *seconds*
17. **ip igmp report-link-local-groups**
18. **ip igmp report-policy** ポリシー
19. **ip igmp access-group** ポリシー
20. **ip igmp immediate-leave**
21. **ip igmp global-leave-ignore-gss-mrt**
22. （任意） **show ip igmp interface** [*interface*] [**vrf** *vrf-name* | **all**] [**brief**]
23. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interface** *interface*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		ethernet ethernetslot/port などのインターフェイス タイプおよび番号を入力して、インターフェイス モードを開始します。

ステップ 3	**no switchport**
	例：
	`switch(config-if)# no switchport`
	`switch(config-if)#`	

ステップ 4	**ip igmp version** *value* 例： `switch(config-if)# ip igmp version 3`	IGMP バージョンを指定値に設定します。有効な値は 2 または 3 です。デフォルトは 2 です。 このコマンドの **no** 形式を使用すると、バージョンは 2 に設定されます。
ステップ 5	**ip igmp join-group** {**group** [**source** *source*] | **route-map** *policy-name*} 例： `switch(config-if)# ip igmp join-group 230.0.0.0`	指定したグループまたはチャネルに参加するようにデバイス上のインターフェイスを設定します。デバイスは CPU 消費用のマルチキャスト パケットのみを受け入れます。 **注意** このコマンドを使用して生成されたトラフィックは、デバイス CPU で処理可能である必要があります。CPU の負荷制約のため、このコマンドを使用

	コマンドまたはアクション	目的
		することは（特に形式を問わずスケーリングで使用することは）推奨されません。代わりに **ip igmp static-oif** コマンドの使用を検討してください。
ステップ 6	**ip igmp static-oif** {*group* [**source** *source*] | **route-map** *policy-name*} 例： `switch(config-if)# ip igmp static-oif 230.0.0.0`	マルチキャスト グループを発信インターフェイスに静的にバインドし、デバイス ハードウェアで処理します。グループ アドレスのみを指定した場合は、（*,G）ステートが作成されます。送信元アドレスを指定した場合は、（S,G）ステートが作成されます。**match ip multicast** コマンドで、使用するグループ プレフィックス、グループ範囲、および送信元プレフィックスを示すルートマップ ポリシー名を指定できます。 （注） IGMPv3 をイネーブルにした場合にのみ、（S,G）ステートに対して送信元ツリーが作成されます。
ステップ 7	**ip igmp startup-query-interval** *seconds* 例： `switch(config-if)# ip igmp startup-query-interval 25`	ソフトウェアの起動時に使用されるクエリー インターバルを設定します。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 31 秒です。
ステップ 8	**ip igmp startup-query-count** *count* 例： `switch(config-if)# ip igmp startup-query-count 3`	ソフトウェアの起動時に使用されるクエリー数を設定します。有効範囲は 1 ～ 10 です。デフォルトは 2 です。
ステップ 9	**ip igmp robustness-variable** *value* 例： `switch(config-if)# ip igmp robustness-variable 3`	ロバストネス変数を設定します。有効値の範囲は、1 ～ 7 です。デフォルトは 2 です。
ステップ 10	**ip igmp querier-timeout** *seconds* 例： `switch(config-if)# ip igmp querier-timeout 300`	クエリアとして処理を引き継ぐかどうかをソフトウェアが判断するための、クエリア タイムアウト値を設定します。有効範囲は 1 ～ 65,535 秒です。デフォルト値は 255 秒です。
ステップ 11	**ip igmp query-timeout** *seconds* 例： `switch(config-if)# ip igmp query-timeout 300`	クエリアとして処理を引き継ぐかどうかをソフトウェアが判断するための、クエリー タイムアウト値を設定します。有効範囲は 1 ～ 65,535 秒です。デフォルト値は 255 秒です。 （注） このコマンドの機能は、**ip igmp querier-timeout** コマンドと同じです。

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

	コマンドまたはアクション	目的
ステップ 20	**ip igmp immediate-leave** 例： `switch(config-if)# ip igmp immediate-leave`	デバイスが、グループに関する Leave メッセージの受信後、ただちにマルチキャストルーティングテーブルからグループ エントリを削除できるようにします。このコマンドを使用すると、デバイスからグループ固有のクエリが送信されないため、所定の IGMP インターフェイスで IGMPv2 グループ メンバーシップの脱退のための待ち時間が最小限になります。デフォルトではディセーブルになっています。 （注） このコマンドは、所定のグループに対するインターフェイスの背後に 1 つの受信者しか存在しない場合に使用します。
ステップ 21	**ip igmp global-leave-ignore-gss-mrt** 例： `switch(config-if)# ip igmp global-leave-ignore-gss-mrt`	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、スイッチが一般的な最大応答時間（MRT）を使用できるようにします。
ステップ 22	（任意） **show ip igmp interface** [*interface*] [**vrf** *vrf-name* | **all**] [**brief**] 例： `switch(config)# show ip igmp interface`	インターフェイスに関する IGMP 情報を表示します。
ステップ 23	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。構成の変更を保存します

IGMP SSM 変換の設定

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

次の表に、SSM 変換の例を示します。

表 *4: SSM* 変換の例

グループ プレフィックス	送信元アドレス
232.0.0.0/8	10.1.1.1
232.0.0.0/8	10.2.2.2
232.1.0.0/16	10.3.3.3
232.1.1.0/24	10.4.4.4

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

表 *5: SSM* 変換適用後の例

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

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

	コマンドまたはアクション	目的
ステップ 2	**ip igmp ssm-translate** *group-prefix source-addr* 例： `switch(config)# ip igmp ssm-translate 232.0.0.0/8 10.1.1.1`	ルータが IGMPv3 メンバーシップ レポートを受信したときと同様に、(S,G) ステートが作成されるよう、IGMP プロセスによる IGMPv1 または IGMPv2 メンバーシップ レポートの変換を設定します。
ステップ 3	（任意） **show running-configuration igmp** 例： `switch(config)# show running-configuration igmp`	**ssm-translate** コマンド ラインを含む、実行コンフィギュレーション情報を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

ルータ アラートの適用オプション チェックの設定

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

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

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

IGMP 構成の確認

IGMP の設定情報を表示するには、次の作業のいずれかを行います。

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

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
```

次に、マルチキャスト グループ 224.1.1.0/24 の Join を受け入れるようにルート マップを構成する例を示します：

```
switch(config)# route-map route-map igmp-join-grp permit 10
switch(config-route-map)# match ip multicast group 224.1.1.0/24
switch(config-route-map)# exit
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip igmp join-group route-map igmp-join-grp
```

次に、マルチキャスト グループ 225.1.1.0/24 の OIF を作成するようにルート マップを構成する例を示します：

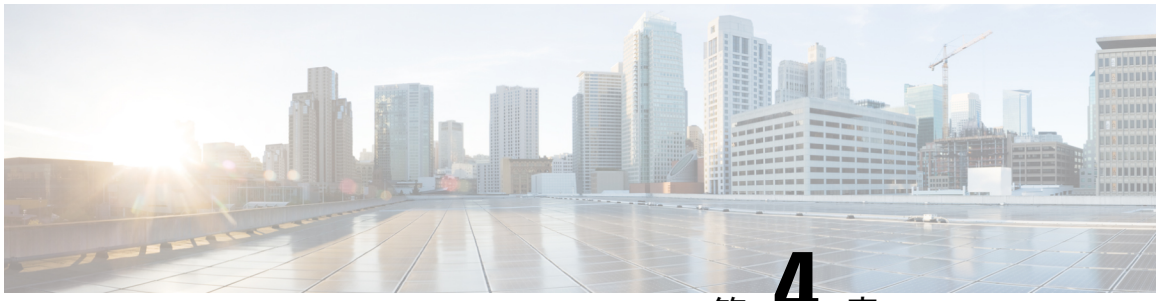
```
switch(config)# route-map route-map igmp-static-grp permit 10
switch(config-route-map)# match ip multicast group 225.1.1.0/24
switch(config-route-map)# exit
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip igmp static-oif route-map igmp-static-grp
```

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。

次の作業

-
- IGMP スヌーピングの構成 （77 ページ）



第 4 章

PIM の設定

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

この章は、次の項で構成されています。

- PIM に関する情報 （33 ページ）
- PIM の前提条件 （41 ページ）
- PIM の注意事項と制約事項 （42 ページ）
- PIM のデフォルト設定 （42 ページ）
- PIM の設定 （43 ページ）
- PIM 設定の確認 （67 ページ）
- 統計の表示 （68 ページ）
- PIM の設定例 （69 ページ）
- 次の作業 （76 ページ）
- その他の参考資料 （76 ページ）

PIM に関する情報

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

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

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

Cisco NX-OS でマルチキャスト機能を有効化するには、各ルータで PIM 機能を有効化してから、マルチキャストに参加する各インターフェイスで、PIM スパース モードを有効化する必要があります。PIM は IPv4 ネットワーク用に設定できます。IPv4 ネットワーク上のルータで IGMP がイネーブルになっていない場合は、PIM によって自動的にイネーブルにされます。IGMP の構成に関する詳細は、「IGMP の設定 （15 ページ）」を参照してください。

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

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

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

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

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

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

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

vPC を使用した PIM SSM

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

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

Hello メッセージ

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

⚠

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

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

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

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

Join-Prune メッセージ

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

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

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

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

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

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

ステートのリフレッシュ

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

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

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

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

ランデブー ポイント

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

スタティック RP

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

スタティック RP を定義するのは、次のような場合です。

- ルータに Anycast RP アドレスを設定する場合
- スイッチに手動で RP を設定する場合

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

BSR

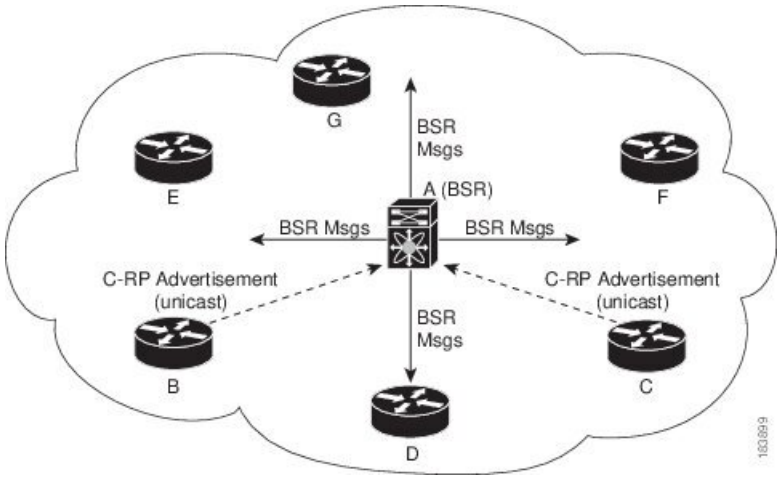
ブートストラップ ルータ（BSR）を使用すると、PIM ドメイン内のすべてのルータで、BSR と同じ RP キャッシュが保持されるようになります。BSR では、BSR 候補 RP から RP セットを選択するよう設定できます。BSR は、ドメイン内のすべてのルータに RP セットをブロードキャストする役割を果たします。ドメイン内の RP を管理するには、1 つまたは複数の候補 BSR を選択します。候補 BSR の 1 つが、ドメインの BSR として選定されます。

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

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

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

図 *9 : BSR* メカニズム



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

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

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

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

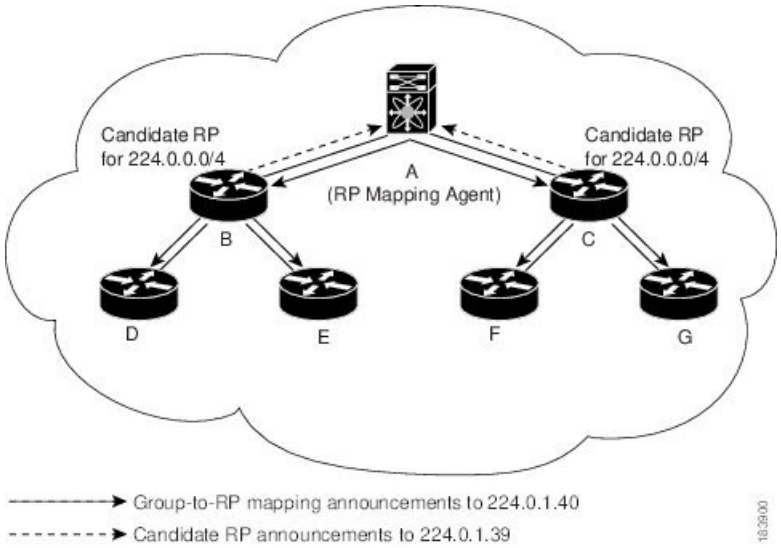
Auto-RP

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

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

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

図 *10 : Auto-RP* のメカニズム



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

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

Anycast-RP

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

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

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

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

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

PIM 登録メッセージ

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

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

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

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

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

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

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

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

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

指定ルータ

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

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

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

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

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

管理用スコープの IP マルチキャスト

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

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

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

仮想化のサポート

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

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

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

PIM の前提条件

PIM には以下の前提条件があります。

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

PIM の注意事項と制約事項

PIM には、次の注意事項と制限事項があります。

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

PIM のデフォルト設定

次の表に、PIM パラメータのデフォルト設定を示します。

表 *6 : PIM* パラメータのデフォルト設定

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

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

PIM の設定

PIM は、各インターフェイスに設定できます。

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

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

表 *7: PIM* のマルチキャスト配信モード

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

PIM を設定する手順は、次のとおりです。

手順

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

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

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

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

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

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

PIM 機能の有効化

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

始める前に

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**feature pim** 例： `switch(config)# feature pim`	PIM をイネーブルにします。デフォルトでは PIM はディセーブルになっています。

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

PIM スパース モードの設定

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

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

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

始める前に

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	（任意） **ip pim auto-rp** {**listen** [**forward**] | **forward** [**listen**]} 例： `switch(config)# ip pim auto-rp listen`	Auto-RP メッセージの待ち受けまたは転送をイネーブルにします。デフォルトではこれらの機能がディセーブルになっているため、Auto-RP メッセージの受信と転送は行われません。

	コマンドまたはアクション	目的
ステップ 3	（任意） **ip pim bsr** {**listen** [**forward**] | **forward** [**listen**]} 例： `switch(config)# ip pim bsr forward`	BSR メッセージの待ち受けまたは転送をイネーブルにします。デフォルトではこれらの機能がディセーブルになっているため、BSR メッセージの待ち受けまたは転送は行われません。
ステップ 4	（任意） **ip pim rp** [*ip prefix*] **vrf** *vrf-name*| **all** 例： `switch(config)# show ip pim rp`	Auto-RP および BSR の受信/転送ステートなど、PIM RP 情報を表示します。
ステップ 5	（任意） **ip pim register-rate-limit** *rate* 例： `switch(config)# ip pim register-rate-limit 1000`	レート制限を毎秒のパケット数で設定します。指定できる範囲は 1 ～ 65,535 です。デフォルト設定は無制限です。
ステップ 6	（任意） **show running-configuration pim** 例： `switch(config)# show running-configuration pim`	Register レート制限を含めた PIM の実行コンフィギュレーション情報を表示します。

ステップ 7	**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 8	**no switchport** 例： `sswitch(config-if)# no switchport`	そのインターフェイスを、レイヤ 3 ルーテッド インターフェイスとして設定します。
ステップ 9	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	現在のインターフェイスで PIM スパース モードをイネーブルにします。デフォルトではディセーブルになっています。
ステップ 10	（任意） **ip pim dr-priority** *priority* 例： `switch(config-if)# ip pim dr-priority 192`	PIM hello メッセージの一部としてアドバタイズされる指定ルータ（DR）プライオリティを設定します。有効範囲は 1 ～ 4294967295 です。デフォルトは 1 です。
ステップ 11	（任意） **ip pim hello-authentication ah-md5** *auth-key* 例： `switch(config-if)# ip pim hello-authentication ah-md5 my_key`	PIM hello メッセージ内の MD5 ハッシュ認証キーをイネーブルにします。暗号化されていない（クリアテキストの）キーか、または次に示す値のいずれかを入力したあと、スペースと MD5 認証キーを入力します。 • 0：暗号化されていない（クリアテキスト）キーを指定します。

	コマンドまたはアクション	目的
		• 3：3-DES 暗号化キーを指定します。 • 7：Cisco Type 7 暗号化キーを指定します。
ステップ 12	（任意） **ip pim hello-authentication keychain** *name* 例： `switch(config-if)# ip pim hello-authentication keychain mykeychain`	PIM インターフェイスでキーチェーン認証を有効にします。ここで <keychain> はキーチェーンの名前です。 （注） • キーチェーンを設定する前でも、特定のキーチェーン名を使用して認証を設定できますが、認証が成功するのは有効なキーとともにキーチェーンが存在する場合だけです。 • キーチェーン認証が構成されている場合、古いパスワードベースの認証は（存在する場合でも）無視されます。
ステップ 13	（任意） **ip pim hello-interval** *interval* 例： `switch(config-if)# ip pim hello-interval 25000`	hello メッセージの送信インターバルを、ミリ秒単位で設定します。範囲は 1 ～ 4294967295 です。デフォルト値は 30000 です。 （注） 最小値は 1 ミリ秒です。
ステップ 14	（任意） **ip pim border** 例： `switch(config-if)# ip pim border`	インターフェイスを PIM ドメインの境界として設定し、対象のインターフェイスで、ブートストラップ、候補 RP、または Auto-RP の各メッセージが送受信されないようにします。デフォルトではディセーブルになっています。
ステップ 15	（任意） **ip pim neighbor-policy** *policy name* 例： `switch(config-if)# ip pim neighbor-policy my_neighbor_policy`	**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どの PIM ネイバーと隣接関係になるかを構成します。ポリシー名の文字数は最大 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	（任意） **show ip pim interface** [*interface* | **brief**] [**vrf** *vrf-name* | **all**] 例： `switch(config-if)# show ip pim interface`	PIM インターフェイスの情報を表示します。

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

ASM を構成

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

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

静的 RP の設定

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

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

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

始める前に

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**ip pim rp-address** *rp-address* [**group-list** *ip-prefix* | **route-map** *policy-name*] 例： `switch(config)# ip pim rp-address 192.0.2.33 group-list 224.0.0.0/9`	マルチキャスト グループ範囲に、PIM スタティック RP アドレスを設定します。**match ip multicast** コマンドとともに使用するグループ プレフィックスにリスト化されるルートマップ ポリシー名を指定できます。デフォルト モードは ASM です。デフォルトのグループ範囲は 224.0.0.0 ～ 239.255.255.255 です。

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

BSR の設定

BSR を設定するには、候補 BSR および候補 RP を選択します。

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

候補 BSR の構成では、引数を指定できます（次の表を参照）。

表 *8 :* 候補 *BSR* の引数

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

候補 RP を表 4 で説明されている引数とキーワードで構成できます。

表 *9*: ***BSR*** 候補 ***RP*** の引数およびキーワード

引数またはキーワード	説明
interface	ブートストラップ メッセージで使用する、BSR 送信元 IP アドレスを取得するためのインターフェイス タイプおよび番号。
group-list *ip-prefix*	プレフィックス形式で指定された、この RP によって処理されるマルチキャスト グループ。
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、グループ範囲内で優先度が最も高い RP が選定されます。優先度が等しい場合は IP アドレスが最上位の RP が選定されます。（最も高い優先度は最も低い値です。）この値の範囲は 0（優先度が最大）～ 255 であり、デフォルトは 192 です。 （注） この優先度は BSR の BSR 候補の優先度とは異なります。BSR 候補の優先度は 0 ～ 255 の間で、大きい値ほど優先度が高くなります。

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

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

候補 BSR および候補 RP を設定する手順は、次のとおりです。

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

BSR の設定

始める前に

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

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

Auto-RP の設定

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

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

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

表 *10 : Auto-RP* マッピング エージェントの引数

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

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

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

表 *11 : Auto-RP* 候補 *RP* の引数とキーワード

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

引数またはキーワード	説明
scope *ttl*	RP-Discovery メッセージが転送される最大ホップ数を表す存続時間（TTL）値。この値の範囲は 1 ～ 255 であり、デフォルト 32 です。 （注） 「PIM スパース モードの構成」セクションの境界ドメイン機参照してください。
interval	RP-Announce メッセージの送信間隔（秒）。この値の範囲は 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

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

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

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

Auto RP の構成

始める前に

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**ip pim** {**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、**「自動 RP マッピング エージェントの引数」**の表を参照してください。
ステップ 3	**ip pim** {**send-rp-announce** | {**auto-rp rp-candidate**}} interface **group-list** *ip-prefix* [**scope** *ttl*] [**interval** *interval*] [**bidir**] 例： `switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24`	Auto-RP の候補 RP を設定します。デフォルト スコープは 32 です。デフォルト インターバルは 60 秒です。デフォルトでは、ASM の候補 RP が作成されます。パラメータの詳細については、**「自動 RP 候補 RP の引数とキーワード」**の表を参照してください。 （注） 候補 RP インターバルは 15 秒以上に設定することを推奨します。 この例では、ASM の候補 RP を構成しています。
ステップ 4	（任意） **show ip pim group-range** [*ip-prefix* | **vrf** *vrf-name* | **all**] 例： `switch(config)# show ip pim group-range`	PIM モードとグループ範囲を表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

PIM エニーキャスト RP セットの設定（PIM）

PIM Anycast-RP セットを設定する手順は、次のとおりです。

ステップ 1 PIM エニーキャスト RP セット内のルータを選択します。

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

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

始める前に

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**interface loopback** *number*
	例：
	`switch(config)# interface loopback 0`
	`switch(config-if)#`
		インターフェイス ループバックを設定します。
		この例では、インターフェイス ループバックを 0 に設定しています。

ステップ 3	**ip address** *ip-prefix* 例： `switch(config-if)# ip address 192.168.1.1/32`	このインターフェイスの IP アドレスを設定します。 この例では、Anycast-RP の IP アドレスを設定しています。
ステップ 4	**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 5	**exit** 例： `switch(config)# exit`	コンフィギュレーション モードに戻ります。

ステップ 6	**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`
	`switch(config)# ip pim anycast-rp 192.0.2.3 192.0.2.32`
		指定した Anycast-RP アドレスに対応する PIM Anycast-RP ピア アドレスを設定します。各コマンドで同じ Anycast-RP アドレスを指定して実行すると、Anycast-RP セットが作成されます。RP の IP アドレスは、同一セット内の RP との通信に使用されます。
		この例は、192.0.2.31 と 192.0.2.32 の Anycast-RP セットを示しており、ネットワークで使用される Anycast-RP は 192.0.2.3 になります。

ステップ 7	Anycast-RP セットに属する各ピア RP で、同じ Anycast-RP アドレスを使用してステップ 6 を繰り返します。	—
ステップ 8	**show ip pim group-range** [*ip-prefix*] [**vrf** { *vrf-name* | **all** }]	PIM モードとグループ範囲を表示します。

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

ASM 専用の共有ツリーの設定

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

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

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

始める前に

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

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

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

マルチキャスト ルーティング テーブルの最大エントリ数の設定

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

始める前に

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**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の範囲は 0 ～ 8000 です。
ステップ 3	（任意） **show hardware profile status** 例： `switch(config)# show hardware profile status`	マルチキャスト ルーティング テーブル制限の情報を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

SSM（PIM）の設定

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

IPv4 ネットワーク上のホストから、送信元を特定してマルチキャストデータを要求するには、このホストおよびこのホストの DR で、IGMPv3 が実行されている必要があります。SSM モードでインターフェイスに PIM を設定する場合は、IGMPv3 をイネーブルにするのが一般的です。IGMPv1 または IGMPv2 が実行されているホストでは、SSM 変換を使用して、グループと送信元のマッピング設定を行うことができます。詳細については、「IGMP の設定 （15 ページ）」を参照してください。

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

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

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

始める前に

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **ip pim ssm** {**prefix-list** *name* | **range** {*ip-prefix* | none} | route-map *policy-name*}
	例：
	`switch(config)# ip pim ssm range 239.128.1.0/24`
	例：
	`switch(config)# no ip pim ssm range none`
		次のオプションを使用できます。
		• **prefix-list**：SSM 範囲のプレフィックス リスト ポリシー名を指定します。
		• **range**：SSM のグループ範囲を設定します。デフォルトの範囲は 232.0.0.0/8 です。キーワード **none** を指定すると、すべてのグループ範囲が削除されます。

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

vPC を介した PIM SSM の設定

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

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

始める前に

PIM および vPC 機能が有効なことを確認します。

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**vrf context name**
	例：
	`switch(config)# vrf context Enterprise`
	`switch(config-vrf)#`
		新しい VRF を作成し、VRF 設定モードを開始します。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

ステップ 3	（任意） [**no**] **ip pim ssm** { *prefix-list name* | *range* { **ip-prefix** | **none**} | *route-map policy-name*} 例： `switch(config-vrf)# ip pim ssm range 234.0.0.0/24`	次のオプションを使用できます。 • prefix-list：SSM 範囲のプレフィックス リスト ポリシー名を指定します。 • range：SSM のグループ範囲を設定します。デフォルトの範囲は 232.0.0.0/8 です。キーワード none を指定すると、すべてのグループ範囲が削除されます。 • route-map：match ip multicast コマンドで、使用するグループ プレフィックスを示すルートマップ ポリシー名を指定できます。 デフォルト範囲は、次のコマンドを使用してオーバーライドできます。この例のコマンドは、デフォルトの範囲を 234.0.0.0/24 にオーバーライドします。 no オプションを指定すると、SSM 範囲から指定のプレフィックスが削除されるか、プレフィックスリストまたはルートマップ ポリシーが削除されます。キーワード none を指定すると、no コマンドは SSM 範囲をデフォルト値の 232.0.0.0/8 にリセットします。
ステップ 4	（任意） **show ip pim group-range** [*ip-prefix*] [**vrf** { *vrf-name* | **all** }] 例： `switch(config)# show ip pim group-range`	PIM モードとグループ範囲を表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	設定変更を保存します。

マルチキャスト用 RPF ルートの設定

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

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

始める前に

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

手順

	コマンドまたはアクション	目的

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

ステップ 2	**ip mroute** {*ip-addr mask* | *ip-prefix*} {*next-hop* | *nh-prefix* |} [*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。デフォルトのプリファレンスは 1 です。
ステップ 3	（任意） **show ip static-route** [**vrf** *vrf-name*] 例： `switch(config)# show ip static-route`	設定されているスタティック ルートを表示します。
ステップ 4	（任意） **copy running-config startup-config**	設定変更を保存します。

マルチキャスト マルチパスの無効化

デフォルトでは、使用可能な複数の ECMP パスがある場合、マルチキャストの RPF インターフェイスが自動的に選択されます。自動選択を無効にすると、マルチキャスト用に単一の RPF インターフェイスを指定できます。

手順

	コマンドまたはアクション	目的

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

ステップ 2	**ip multicast multipath none** 例： `switch(config)# ip multicast multipath none`	マルチキャスト マルチパスの無効化
ステップ 3	**clear ip mroute * vrf all** 例： `switch(config)# clear ip mroute * vrf all`	マルチパス ルートをクリアし、マルチキャスト マルチパス抑制をアクティブにします。

RP 情報配信を制御するルート マップの設定

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

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

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

始める前に

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

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的

ステップ 2	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
	例：
	`switch(config)# route-map ASM_only permit 10`
	`switch(config-route-map)#`
		ルートマップ コンフィギュレーション モードを開始します。構成方法は **permit** キーワードを使用します。

ステップ 3	**match ip multicast** {**rp** *ip-address* [**rp-type** *rp-type*] [**group** *ip-prefix*]} | {**group** *ip-prefix* **rp** *ip-address* [**rp-type** *rp-type*]} 例： `switch(config)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type ASM`	指定したグループ、RP、および RP タイプを関連付けます。ユーザは RP のタイプ（ASM または Bidir）を指定できます。例で示すとおり、このコンフィギュレーション モードでは、グループおよび RP を指定する必要があります。
ステップ 4	（任意） **show route-map** 例： `switch(config-route-map)# show route-map`	設定済みのルート マップを表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config-route-map)# copy running-config startup-config`	設定変更を保存します。

メッセージ フィルタリングの設定

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

表 *12 : PIM* および *PIM6* でのメッセージ フィルタリング

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

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

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

メッセージ フィルタリングの設定

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

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

ステップ 7	**interface** *interface*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		指定したインターフェイスでインターフェイス モードを開始します。

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

ルートのフラッシュ

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

PIM を再起動すると、次の処理が実行されます：

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	**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 モードに入ります。

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`	**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`	設定変更を保存します。

PIM 設定の確認

PIM の設定情報を表示するには、次の作業のいずれかを行います。

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

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

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

統計の表示

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

PIM 統計情報の表示

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

表 *13 : 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。

PIM 統計情報のクリア

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

表 *14* : 統計情報をクリアする *PIM* コマンド

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

PIM の設定例

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

SSM の構成例

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

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

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

2. **ステップ 2**：SSM をサポートする IGMP のパラメータを構成します。「IGMP の設定 （15 ページ）」を参照してください。通常は、SSM をサポートするために、PIM インターフェイスに IGMPv3 を設定します。

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

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

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

4. **ステップ 4**：メッセージ フィルタ処理を構成します。

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

次に、SSM モードで PIM を構成する方法の例を示します。

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

vPC を介した PIM SSM の構成例

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

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

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

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

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

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

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

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

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

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

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


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

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

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

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

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

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

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

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

BSR の設定例

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

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

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

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

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

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

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

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

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

5. **ステップ 5**：メッセージ フィルタ処理を構成します。

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

6. **ステップ 6**：BSR の動作を確認します。

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

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

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

PIM Anycast-RP の設定例

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

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

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

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

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

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

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

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

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

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

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

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

（注） 同様の構成を使用して、複数の RP セットを作成できます。

6. **ステップ 6**：エニーキャスト RP の動作を確認します。

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

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

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

次の作業

PIM の関連機能を構成するには、次の章を参照してください：

- IGMP の設定 （15 ページ）
- IGMP スヌーピングの構成 （77 ページ）

その他の参考資料

PIM の実装に関する詳細情報については、次の項目を参照してください。

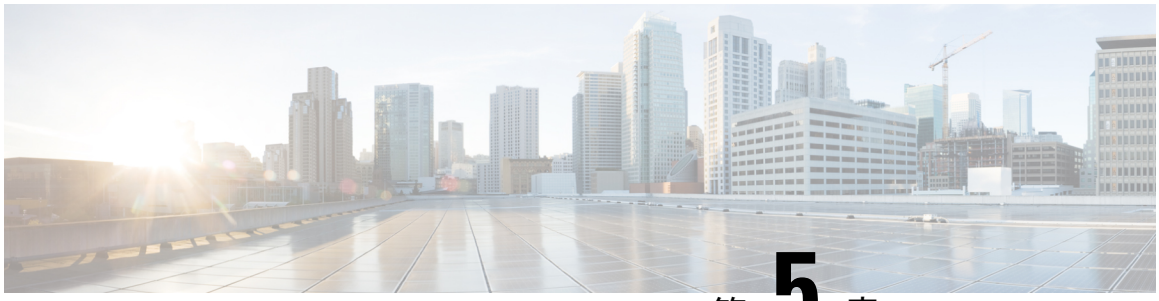
- 関連資料
- MIB

関連資料

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

MIB

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



第 5 章

IGMP スヌーピングの構成

この章では、Cisco Nexus 3600 プラットフォーム スイッチにインターネット グループ管理プロトコル（IGMP）スヌーピングを構成する方法を説明します。

この章は、次の項で構成されています。

- IGMP スヌーピングの情報 （77 ページ）
- IGMP スヌーピングに関する注意事項と制限事項 （80 ページ）
- IGMP スヌーピングのデフォルト設定 （81 ページ）
- IGMP スヌーピング パラメータの設定 （82 ページ）
- IGMP スヌーピング設定の確認 （90 ページ）
- マルチキャスト ルートの間隔を設定 （91 ページ）
- IGMP スヌーピング統計情報の表示 （91 ページ）
- IGMP スヌーピングの設定例 （91 ページ）

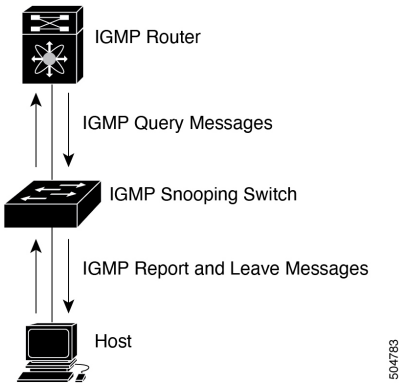
IGMP スヌーピングの情報

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

インターネット グループ管理プロトコル（IGMP）スヌーピング ソフトウェアは、VLAN 内のレイヤ 2 IP マルチキャスト トラフィックを調査し、関係する受信機が常駐するポートを発見します。IGMP スヌーピングではポート情報を利用することにより、マルチアクセス LAN 環境における帯域幅消費量を削減し、VLAN 全体へのフラッディングを回避します。IGMP スヌーピング機能は、マルチキャスト対応ルータに接続されたポートを追跡して、ルータによる IGMP メンバーシップ レポートの転送機能を強化します。トポロジの変更通知には、IGMP スヌーピング ソフトウェアが応答します。デフォルトでは、IGMP スヌーピングがスイッチでイネーブルにされています。

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

図 *11 : IGMP* スヌーピング スイッチ



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

IGMP の詳細については、「 IGMP の設定 （15 ページ）」を参照してください。

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

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

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

このセクションは、次のトピックで構成されています。

IGMPv1 および IGMPv2

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

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

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

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

IGMPv3

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

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

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

IGMPスヌーピングクエリア

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

IGMP スヌーピング クエリアがイネーブルの場合、スイッチは定期的にクエリーを送信します（構成されたクエリア アドレスの送信元アドレスを使用します）。これらのクエリーは、IP マルチキャスト トラフィックを受信するホストからの IGMP レポート メッセージをトリガーします。

ルータ ポートでの IGMP フィルタ処理

IGMP フィルタ処理を使用すると、スイッチをレイヤ 3 マルチキャスト スイッチに接続するルータ ポートをスイッチに構成できます。スイッチは、手動で構成されたすべてのスタティック ルータ ポートをルータ ポート リストに保存します。

IGMP パケットを受信すると、スイッチは 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、PIM hello メッセージまたはスイッチが受信した IGMP クエリーを介して、ポートをルータ ポートとして認識します。

IGMP スヌーピングに関する注意事項と制限事項

IGMP スヌーピングに関する注意事項および制約事項は次のとおりです。

- Cisco Nexus 3600 プラットフォーム スイッチは、IPv4 の IGMP スヌーピングのみをサポートします。
- Cisco Nexus 3600 プラットフォーム スイッチは、vPC を使用した IGMP スヌーピングをサポートします。
- IGMP スヌーピング構成は、vPC ペアの両方の vPC ピアで同一である必要があります。両方の vPC ピアで IGMP スヌーピングを有効または無効にします。

（注） 両方の vPC ピアで IGMP スヌーピングを有効または無効にすると、異なる MVR 送信元 VLAN から同じ MVR 受信者 VLAN への IGMP クエリの転送も有効になります。結果の IGMP クエリは、異なるバージョンとクエリ間隔でクエリを送信する場合があります。Cisco NX-OS リリース 7.0（3）I3（1）より前の動作を維持する場合は、 **mvr-suppress-query** コマンドを使用します。IGMP 一般クエリ転送の抑制の詳細については、「VLAN からの IGMP クエリ転送の抑制 （117 ページ）」 を参照してください。

- Cisco NX-OS リリース 7.0（3）I3（1）より前のリリースで、vPC ピアを構成している場合、2 台のデバイス間の IGMP スヌーピング構成オプションに相違があると、次のような結果になります。
  - 一方のデバイスで IGMP スヌーピングを有効にして、他方で無効にすると、スヌーピングが無効であるデバイスではすべてのマルチキャスト トラフィックがフラッディングします。
  - マルチキャスト ルータまたはスタティック グループの設定の相違は、トラフィック損失の原因になり得ます。
  - 高速脱退、明示的な追跡、およびレポート抑制のオプションをトラフィックの転送に使用する場合、これらのオプションに相違が生じる可能性があります。

- デバイス間でクエリー パラメータが異なると、一方のデバイスではマルチキャスト ステートが期限切れとなり、もう一方のデバイスでは転送が継続されます。この相違によって、トラフィック損失または転送の長時間化が発生します。
- IGMP スヌーピング クエリアを両方のデバイスで設定している場合、クエリーがトラフィックで確認されると、IGMP スヌーピング クエリアはシャットダウンするので、一方のクエリアだけがアクティブになります。

IGMP スヌーピングのデフォルト設定

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

表 *15*：デフォルト *IGMP* スヌーピング パラメータ

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

（注）

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

IGMP スヌーピング パラメータの設定

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

表 *16 : 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、VLAN ごとに IGMP スヌーピングを有効にします。デフォルトではイネーブルになっています。 （注） グローバル設定が無効になっている場合、すべての VLAN は、有効かどうかに関係なく無効として扱われます。
アクセス グループ	VLAN ごとに IGMP Join をフィルタ処理するポリシーを構成します。
明示的な追跡	各ポートに接続されたそれぞれのホストから送信される IGMPv3 メンバーシップ レポートを、VLAN 別に追跡します。デフォルトではイネーブルになっています。
高速脱退	ソフトウェアが IGMP Leave レポートを受信した場合に、IGMP クエリー メッセージを送信することなく、グループ ステートを解除できるようにします。このパラメータは、IGMPv2 ホストに関して、各 VLAN ポート上のホストが 1 つしか存在しない場合に使用されます。デフォルトではディセーブルになっています。
最終メンバー クエリ間隔	IGMP クエリーの送信後に待機する時間を設定します。この時間が経過すると、ソフトウェアは、特定のマルチキャスト グループについてネットワーク セグメント上に受信要求を行うホストが存在しないと見なします。いずれのホストからも応答がないまま、最終メンバのクエリ インターバルの期限が切れると、対応する VLAN ポートからグループが削除されます。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。

パラメータ	説明
プロキシ脱退メッセージ	プロキシ脱退メッセージの宛先アドレスを、脱退するグループのアドレスに変更します。 通常、IGMP スヌーピング モジュールによって生成される IGMP プロキシ脱退メッセージは、すべてのホストがグループを脱退するとき、224.0.0.2 マルチキャスト ルータ アドレスを使用します。マルチキャストアプリケーションがレポートの受信に依存し、パケットの宛先アドレスに基づいてマルチキャスト トラフィックを開始または停止するメッセージを残す場合は、この構成を実装する必要があります。
レポートをフラッドして脱退	VLAN のすべてのアクティブ インターフェイスまたは特定のインターフェイスのみで IGMP レポートをフラッドします。そして、脱退します。 IGMP レポートは、通常、IGMP スヌーピング モジュールによって検出されるとマルチキャスト ルータ ポートに転送されるので、VLAN でフラッディングされません。ただし、このコマンドを実行すると、スイッチはマルチキャスト ルータ ポートに加えて、VLAN に属するカスタム ポートにも IGMP レポートを送信します。マルチキャスト アプリケーションがトラフィックを送信するために IGMP レポートを表示する機能を必要とする場合は、この構成を実装する必要があります。
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、VLAN ごとにマルチキャスト対応ルータに送信されるメンバーシップ レポート トラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。

パラメータ	説明
マルチキャスト ルータ	マルチキャスト ルータへのスタティック接続を設定します。ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。
スタティック グループ	VLAN のレイヤ 2 ポートをマルチキャスト グループのスタティック メンバーとして設定します。
リンクローカル グループ抑制	スイッチまたは各VLANに対して、リンクローカル グループ抑制を設定します。デフォルトではイネーブルになっています。
IGMPv3 レポート抑制	スイッチまたは、VLANごとにIGMPv3 レポート抑制およびプロキシレポートを構成します。デフォルトでは、スイッチ全体で無効になっており、VLAN ごとに有効になっています。

手順の概要

1. **configure terminal**
2. **ip igmp snooping**
3. **vlan configuration** *vlan-id*
4.
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**ip igmp snooping** 例： `switch(config)# ip igmp snooping`	デバイスの IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。 （注） このコマンドの no 形式により、グローバル設定がディセーブルになっている場合は、個々の VLAN でIGMP スヌーピングがイネーブルであるかどうかに関係なく、すべての VLAN で IGMP スヌーピン

	コマンドまたはアクション	目的
		グがディセーブルになります。 IGMP スヌーピングをディセーブルにすると、レイヤ2マルチキャスト フレームがすべてのモジュールにフラッディングします。

ステップ 3	**vlan configuration** *vlan-id*
	例：
	`switch(config)# vlan configuration 100`
	`switch(config-vlan-config)#`
		VLAN を構成し、VLAN コンフィギュレーション モードを開始します。

ステップ 4		

オプション	説明
コマンド	目的
ip igmp snooping 例： `switch(config-vlan-config)# ip igmp snooping`	現在の VLAN に対して IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。
ip igmp snooping access-group route-map-name 例： `switch(config-vlan-config)# ip igmp snooping access-group rmap`	VLAN ごとに IGMP Join をフィルタ処理するポリシーを構成します。デフォルトではディセーブルになっています。
ip igmp snooping explicit-tracking 例： `switch(config-vlan-config)# ip igmp snooping explicit-tracking`	各ポートに接続されたそれぞれのホストから送信される IGMPv3 メンバーシップ レポートを、VLAN 別に追跡します。デフォルトは、すべての VLAN でイネーブルです。
ip igmp snooping fast-leave 例： `switch(config-vlan-config)# ip igmp snooping fast-leave`	IGMPv2 プロトコルのホスト レポート抑制メカニズムのために、明示的に追跡できない

	コマンドまたはアクション		目的
	オプション	説明	
		IGMPv2 ホストをサポートします。高速脱退がイネーブルの場合、IGMP ソフトウェアは、各 VLAN ポートに接続されたホストが 1 つだけであると見なします。デフォルトは、すべての VLAN でディセーブルです。	
	ip igmp snooping last-member-query-interval *seconds* 例： `switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3`	いずれのホストからも IGMP クエリー メッセージへの応答がないまま、最終メンバのクエリー インターバルの期限が切れた場合に、関連する VLAN ポートからグループを削除します。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。	
	[**no**] **ip igmp snooping proxy-leave use-group-address** 例： `switch(config-vlan-config)# ip igmp snooping proxy-leave use-group-address`	プロキシ脱退メッセージの宛先アドレスを、脱退するグループのアドレスに変更します。 通常、IGMP スヌーピング モジュールによって生成される IGMP プロキシ脱退メッセージは、すべてのホストがグループを脱退するとき、224.0.0.2 マルチキャスト ルータ ア	

	コマンドまたはアクション		目的
	オプション	説明	
		ドレスを使用します。マルチキャスト アプリケーションがレポートの受信に依存し、パケットの宛先アドレスに基づいてマルチキャスト トラフィックを開始または停止するメッセージを残す場合は、この構成を実装する必要があります。	
	[**no**] **ip igmp snooping report-flood** { **all** | **interface ethernet** *slot/port*} 例： `switch(config-vlan-config)# ip igmp snooping report-flood interface ethernet 1/2 ip igmp snooping report-flood interface ethernet 1/3`	VLAN のすべてのアクティブ インターフェイスまたは特定のインターフェイスのみで IGMP レポートをフラッドします。そして、脱退します。 IGMP レポートは、通常、IGMP スヌーピング モジュールによって検出されるとマルチキャスト ルータ ポートに転送されるので、VLAN でフラッディングされません。ただし、このコマンドを実行すると、スイッチはマルチキャスト ルータ ポートに加えて、VLAN に属するカスタム ポートにも IGMP レポートを送信しま	

	コマンドまたはアクション		目的
	オプション	説明	
		す。マルチキャスト アプリケーションがトラフィックを送信するために IGMP レポートを表示する機能を必要とする場合は、この構成を実装する必要があります。	
	ip igmp snooping querier *ip-address* 例： `switch(config-vlan-config)# ip igmp snooping querier 172.20.52.106`	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、スヌーピング クエリアを設定します。IP アドレスは、メッセージの送信元として使用します。	
	ip igmp snooping report-suppression 例： `switch(config-vlan-config)# ip igmp snooping report-suppression`	マルチキャスト対応ルータに送信されるメンバシップ レポート トラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。 （注） グローバル コンフィギュレーション モードでこのコ	

	コマンドまたはアクション		目的
	オプション	説明	
		マンドを実行し、すべてのインターフェイスを変更することもできます。	
	ip igmp snooping mrouter interface *interface* 例： `switch(config-vlan-config)# ip igmp snooping mrouter interface ethernet 2/1`	マルチキャスト ルータへのスタティック接続を設定します。ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。**ethernet** *slot/port* のように、インターフェイスは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-config)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1`	VLAN のレイヤ 2 ポートをマルチキャスト グループのスタティック メンバーとして設定します。**ethernet** *slot/port* のように、インターフェイスはタイプおよび番号で指定できます。	
	ip igmp snooping link-local-groups-suppression 例： `switch(config-vlan-config)# ip igmp snooping link-local-groups-suppression`	リンクローカル グループ抑制を設定します。デフォルトではイネーブルになっています。 （注） グローバル コンフィギュレーション モードでこのコマンドを実行し、	

	コマンドまたはアクション		目的
	オプション	説明	
		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-config)# ip igmp snooping v3-report-suppression`	IGMPv3 レポート抑制およびプロキシレポートを設定します。デフォルトでは、スイッチ全体のグローバル コマンドでディセーブルになっており、VLAN ごとにイネーブルになっています。 （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	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`		設定変更を保存します。

IGMP スヌーピング設定の確認

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

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

コマンド	目的
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。

マルチキャスト ルートの間隔を設定

スイッチのマルチキャストルートの作成または削除のレートが高い場合（たとえば、IGMP加入要求または脱退要求が多すぎる場合）、スイッチは要求が行われるのと同じ速さでマルチキャスト ルートをハードウェアにプログラムできません。この問題を解決するには、マルチキャスト ルートがハードウェアにプログラムされるまでの間隔を設定します。

1 秒あたりのマルチキャストルートの作成または削除が非常に少ない場合は、低い間隔（最大 50 ミリ秒）を設定します。間隔を小さくすると、デフォルトの間隔である 1 秒を使用する場合よりも高速にハードウェアをプログラムできます。

1 秒あたりのマルチキャストルートの作成数または削除数が非常に多い場合は、間隔を高く構成します（最大 2 秒）。間隔を長くすると、要求をドロップすることなく、ハードウェアをより長い期間にわたってプログラムできます。

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。この出力で、仮想ポート チャネル（vPC）の統計情報を確認できます。

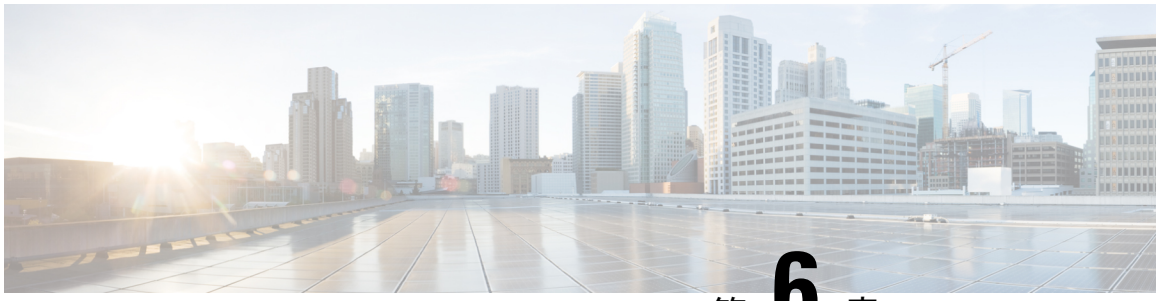
IGMP スヌーピング統計情報をクリアにするには、 **clear ip igmp snooping statistics vlan** コマンドを使用します。

IGMP スヌーピングの設定例

次に、IGMP スヌーピング パラメータの設定例を示します。

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



第 6 章

MSDP の設定

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

- MSDP について （93 ページ）
- MSDP の前提条件 （95 ページ）
- デフォルト設定 （96 ページ）
- MSDP の設定 （96 ページ）
- MSDP の設定の確認 （106 ページ）
- MSDP のモニタリング （107 ページ）
- MSDP の設定例 （107 ページ）
- 関連資料 （109 ページ）
- 標準 （109 ページ）

MSDP について

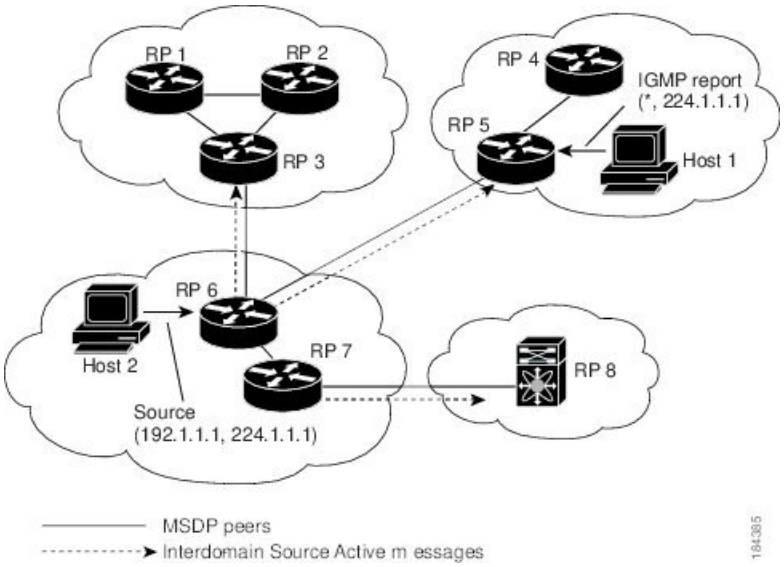
マルチキャスト ソース検出プロトコル（MSDP）を使用すると、複数のボーダー ゲートウェイ プロトコル（BGP）対応のプロトコル独立マルチキャスト（PIM）スパース モード ドメイン間で、マルチキャスト ソース情報を交換できます。また、MSDP を使用して Anycast-RP 設定を作成し、RP 冗長性および負荷共有機能を提供できます。BGP の詳細については、*Cisco Nexus 9000* シリーズ *NX-OS* ユニキャスト ルーティング設定ガイドを参照してください

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

次の図に、4 つの PIM ドメインを示します。接続された RP（ルータ）は、アクティブな送信元情報を相互に交換するため、MSDP ピアと呼ばれます。各 MSDP ピアは他のピアにマルチキャスト送信元情報の独自のセットをアドバタイズします。送信元ホスト 2 はグループ 224.1.1.1

にマルチキャスト データを送信します。MSDP プロセスでは、RP 6 上で PIM Register メッセージを介して送信元に関する情報を学習すると、ドメイン内の送信元に関する情報が、Source-Active（SA）メッセージの一部として MSDP ピアに送信されます。SA メッセージを受信した RP 3 および RP 5 は、MSDP ピアに SA メッセージを転送します。RP 5 は、ホスト 1 からグループ 224.1.1.1 上のマルチキャスト データに対する要求を受信すると、192.1.1.1 のホスト 2 方向に PIM Join メッセージを送信して、送信元への最短パス ツリーを構築します。

図 *12*：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 ピア逆パス転送（RPF）により、SA メッセージのループを防止するには、BGP を使用します。

（注） PIM ドメイン内で Anycast RP（ロード バランシングおよびフェールオーバーを実行できる RP のセット）を使用する場合、BGP を設定する必要はありません。

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

MSDP の詳細については、RFC 3618 を参照してください。

SA メッセージおよびキャッシング

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

- データ送信元の送信元アドレス

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

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

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

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

MSDP ピア RPF 転送

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

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

MSDP メッシュ グループ

MSDP メッシュ グループを使用すると、ピア RPF フラッディングで生成される SA メッセージ数を抑えることができます。メッシュ内のすべてのルータ間にピアリング関係を設定してから、これらのルータのメッシュ グループを作成すると、あるピアから発信される SA メッセージが他のすべてのピアに送信されます。メッシュ内のピアが受信した SA メッセージは転送されません。

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

MSDP の前提条件

MSDP の前提条件は、次のとおりです。

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

デフォルト設定

次の表に、MSDP パラメータのデフォルト設定を示します。

表 *17 : 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 ドメイン内で以下のように MSDP ピアを設定します。

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

5. 各 MSDP ピアでオプションのグローバル パラメータを設定します。
6. 各 MSDP ピアでオプションのメッシュ グループを設定します。

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

（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 機能の有効化

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**feature msdp** 例： `switch# feature msdp`	MSDP 機能をイネーブルにして、MSDP コマンドを実行できるようにします。デフォルトでは、MSDP 機能はディセーブルになっています。
ステップ 3	（任意） **show running-configuration msdp** 例： `switch# show running-configuration msdp`	MSDP の実行コンフィギュレーション情報を示します。

	コマンドまたはアクション	目的
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MSDP ピアの構成

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

始める前に

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

MSDP ピアとして設定するルータのドメイン内で、PIM が設定されていることを確認します。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**ip msdp peer** *peer-ip-address* **connect-source** *interface* [**remote-as** *as-number*] 例： `switch(config)# ip msdp peer 192.168.1.10 connect-source ethernet 2/1 remote-as 8`	MSDP ピアを設定してピア IP アドレスを指定します。ソフトウェアは、インターフェイスの送信元 IP アドレスを使用して、ピアとの TCP 接続を行います。インターフェイスは *type slot/port* という形式で表します。AS 番号がローカル AS と同じ場合、対象のピアは PIM ドメイン内にあります。それ以外の場合、対象のピアは PIM ドメインの外部にあります。

	コマンドまたはアクション	目的
		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。 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	（任意） **show ip msdp summary** [**vrf** [*vrf-name* | **all**]] **例**： `switch# show ip msdp summary`	MSDP ピアの要約情報を表示します。
ステップ 5	（任意） **copy running-config startup-config** **例**： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MSDP ピア パラメータの設定

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

表 *18 : MSDP* ピア パラメータ

パラメータ	説明（**Description**）
Description	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。

パラメータ	説明（Description）
TCP キーチェーン	TCP キーチェーンは、MSDP ピアリング認証に使用されます。
SA ポリシー（IN）	着信 SA メッセージのルートマップ ポリシー。デフォルトでは、すべての SA メッセージが受信されます。 （注） ルートマップポリシーの設定方法については、*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*を参照してください。
SA ポリシー（OUT）	発信 SA メッセージのルートマップ ポリシー。デフォルトでは、発信される SA メッセージには登録済みの全送信元が含まれます。 （注） ルートマップポリシーの設定方法については、*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*を参照してください。
SA の上限	ピアで許可され、SA キャッシュに格納される (S, G) エントリ数。デフォルトでは、上限はありません。

始める前に

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

手順の概要

1. **configure terminal**
2. **ip msdp description** *peer-ip-address description*
3. **ip msdp shutdown** *peer-ip-address*
4. **ip msdp password** *peer-ip-address password*
5. **ip msdp sa-policy** *peer-ip-address policy-name* **in**
6. **ip msdp sa-policy** *peer-ip-address policy-name* **out**
7. **ip msdp sa-limit** *peer-ip-address limit*
8. （任意） **ip msdp keychain** *peer-ip-address name*
9. （任意） **show ip msdp peer** [*peer-address*] [**vrf** [*vrf-name* | **all**]]
10. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。
		（注）
		ステップ 2 でリストされたコマンドを使用して、MSDP ピア パラメータを設定します。

ステップ 2	**ip msdp description** *peer-ip-address description* 例： `switch(config)# ip msdp description 192.168.1.10 peer in Engineering network`	ピアの説明を示すストリングを設定します。デフォルトでは、ピアの説明は設定されていません。
ステップ 3	**ip msdp shutdown** *peer-ip-address* 例： `switch(config)# ip msdp shutdown 192.168.1.10`	ピアをシャットダウンします。デフォルトでは、各ピアは定義した時点でイネーブルになります。
ステップ 4	**ip msdp password** *peer-ip-address password* 例： `switch(config)# ip msdp password 192.168.1.10 my_md5_password`	ピアの MD5 パスワードをイネーブルにします。デフォルトでは、MD5 パスワードはディセーブルになっています。
ステップ 5	**ip msdp sa-policy** *peer-ip-address policy-name* **in** 例： `switch(config)# ip msdp sa-policy 192.168.1.10 my_incoming_sa_policy in`	着信 SA メッセージのルートマップ ポリシーをイネーブルにします。デフォルトでは、すべての SA メッセージが受信されます。
ステップ 6	**ip msdp sa-policy** *peer-ip-address policy-name* **out** 例： `switch(config)# ip msdp sa-policy 192.168.1.10 my_outgoing_sa_policy out`	発信 SA メッセージのルートマップ ポリシーをイネーブルにします。デフォルトでは、発信される SA メッセージには登録済みの全送信元が含まれます。
ステップ 7	**ip msdp sa-limit** *peer-ip-address limit* 例： `switch(config)# ip msdp sa-limit 192.168.1.10 5000`	ピアから受信可能な（S,G）エントリ数の上限を設定します。デフォルトでは、上限はありません。
ステップ 8	（任意） **ip msdp keychain** *peer-ip-address name* 例： `switch(config)# ip msdp keychain 192.168.1.10 5000 mykeychain`	ピアのキーチェーン認証を有効にします。ここで <keychain> はキーチェーンの名前です。 （注） • キーチェーンを設定する前でも、特定のキーチェーン名を使用して認証を設定できますが、

	コマンドまたはアクション	目的
		認証が成功するのは有効なキーとともにキーチェーンが存在する場合だけです。 • キーチェーン認証が構成されている場合、古いパスワードベースの認証は（存在する場合でも）無視されます。
ステップ 9	（任意） **show ip msdp peer** [*peer-address*] [**vrf** [*vrf-name* | **all**]] 例： `switch(config)# show ip msdp peer 192.168.1.10`	MSDP ピアの詳細情報を表示します。
ステップ 10	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

MSDP グローバル パラメータの設定

次の表に示されているオプションのMSDP グローバル パラメータが設定可能です。

表 *19 : MSDP* グローバル パラメータ

パラメータ	説明
発信元インターフェイスの名前	SA メッセージ エントリの RP フィールドで使用される IP アドレス。Anycast RP を使用する場合は、すべての RP に対して同じ IP アドレスを使用します。このパラメータを使用すると、各 MSDP ピアの RP に一意の IP アドレスを定義できます。デフォルトでは、ローカル システムの RP アドレスが使用されます。 （注） RP アドレスにはループバック インターフェイスを使用することを推奨します。
グループの上限	指定したプレフィックスに対して作成される (S, G) エントリの最大数。グループの上限を超えた場合、そのグループは無視され、違反状態が記録されます。デフォルトでは、グループの上限は定義されていません。

パラメータ	説明
SA インターバル	Source-Active（SA）メッセージを送信する間隔。有効値の範囲は60～65,535秒です。デフォルトは 60 秒です。

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**ip msdp originator-id** *interface* 例： `switch(config)# ip msdp originator-id loopback0`	ピアの説明を示すストリングを設定します。デフォルトでは、ピアの説明は設定されていません。 SA メッセージ エントリの RP フィールドで使用される IP アドレスを設定します。デフォルトでは、ローカル システムの RP アドレスが使用されます。 （注） RP アドレスにはループバック インターフェイスを使用することを推奨します。
ステップ 3	**ip msdp group-limit** *limit* **source** *source-prefix* 例： `switch(config)# ip msdp group-limit 1000 source 192.168.1.0/24`	指定したプレフィックスに対してソフトウェアが作成する (S, G) エントリの最大数。グループの上限を超えた場合、そのグループは無視され、違反状態が記録されます。デフォルトでは、グループの上限は定義されていません。

	コマンドまたはアクション	目的
ステップ 4	**ip msdp sa-interval** *seconds* 例： `switch(config)# ip msdp sa-interval 80`	Source-Active（SA）メッセージを送信する間隔。有効値の範囲は 60 ～ 65,535 秒です。デフォルトは 60 秒です。
ステップ 5	（任意） **show ip msdp summary** [**vrf** [*vrf-name* | **all**]] 例： `switch(config)# show ip msdp summary`	MDSP コンフィギュレーションのサマリーを表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MSDP メッシュ グループの設定

グローバル コンフィギュレーション モードでオプションの MSDP メッシュ グループを設定するには、メッシュ内の各ピアを指定します。同じルータに複数のメッシュ グループを設定したり、各メッシュ グループに複数のピアを設定したりできます。

始める前に

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

手順の概要

1. **configure terminal**
2. **ip msdp mesh-group** *peer-ip-addr mesh-name*
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。
4. （任意） **show ip msdp mesh-group** [*mesh-group*] [**vrf** [*vrf-name* | **all**]]
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	
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	（任意） **show ip msdp mesh-group** [*mesh-group*] [**vrf** [*vrf-name* | **all**]] 例： `switch# show ip msdp mesh-group`	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	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MSDP プロセスの再起動

始める前に

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

手順の概要

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

手順の詳細

手順

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

	コマンドまたはアクション	目的
	`switch# restart msdp`	

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

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

MSDP の設定の確認

MSDP の設定情報を表示するには、次の作業のいずれかを行います。

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

MSDP のモニタリング

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

統計の表示

次のコマンドを使用して、MSDP 統計情報を表示できます。

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

統計情報のクリア

MSDP 統計情報は、以下のコマンドを使用してクリアできます。

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

-

MSDP の設定例

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

1. 他のルータとの MSDP ピアリング関係を設定します。

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

2. オプションのピア パラメータを設定します。

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

3. オプションのグローバル パラメータを設定します。

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

4. 各メッシュ グループ内のピアを設定します。

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

次の例は、MSDP ピアリングのサブセットの構成例を示します。

RP 3: 192.168.3.10（AS 7）

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

RP 5: 192.168.5.10（AS 8）

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

RP 6: 192.168.6.10（AS 9）

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

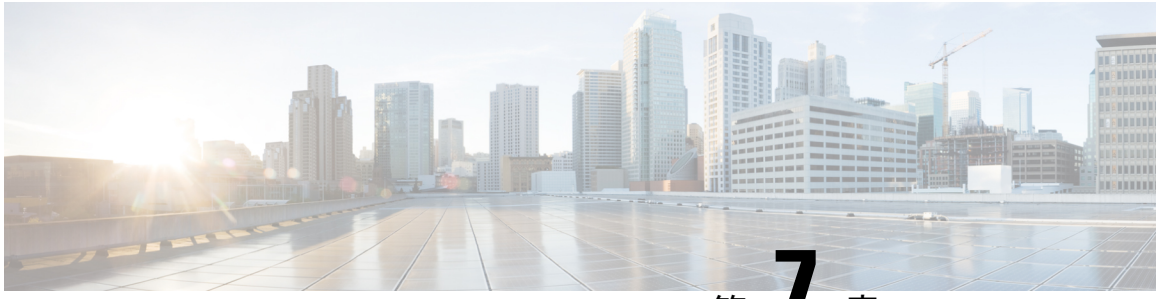
関連資料

関連項目	マニュアル タイトル
MBGP の設定	『*Cisco Nexus 3600* シリーズ *NX-OS* ユニキャスト設定ガイド』

標準

標準	タイトル
RFC 4624	マルチキャスト ソース検出プロトコル（MSDP）

標準



第 7 章

MVR の設定

この章では、Cisco Nexus 3600 プラットフォーム スイッチでマルチキャスト VLAN 登録（MVR）を構成する方法について説明します。

この章は、次の項で構成されています。

- MVR について （111 ページ）
- MVR に関する注意事項と制約事項 （113 ページ）
- MVR のデフォルト設定 （113 ページ）
- MVR の設定 （113 ページ）
- MVR 設定の確認 （118 ページ）
- MVR 設定の例 （120 ページ）

MVR について

一般的なレイヤ 2 マルチ VLAN ネットワークでは、マルチキャスト グループへの加入者を複数の VLAN に設定できます。それらの VLAN 間でデータ分離を維持するには、送信元 VLAN 上のマルチキャスト ストリームをルータに渡す必要があります。そこで、そのストリームがすべての加入者 VLAN で複製され、アップストリーム帯域幅が消費されます。

マルチキャスト VLAN レジストレーション（MVR）を使用すると、レイヤ 2 スイッチでマルチキャスト データを共通の割り当て済み VLAN の送信元から加入者 VLAN に転送し、ルータのバイパスによってアップストリーム帯域幅を節約できます。スイッチは、MVR IP マルチキャスト ストリームのマルチキャスト データを、IGMP レポートまたは MVR のスタティック コンフィギュレーションのいずれかを使用して、ホストが加入した MVR ポートに対してだけ転送します。スイッチは、MVR ホストから受信した IGMP レポートを送信元ポートに対してだけ転送します。他のトラフィックでは、VLAN 分離が保持されます。

MVR では、マルチキャスト ストリームを送信元から伝送するために、少なくとも 1 つの VLAN を共通 VLAN として指定する必要があります。そのような複数のマルチキャスト VLAN（MVR VLAN）をシステムで設定でき、さらにグローバルなデフォルト MVR VLAN とインターフェイス固有のデフォルト MVR VLAN を設定できます。MVR を使用した各マルチキャスト グループは、MVR VLAN に割り当てられます。

MVR を使用すると、ポート上の加入者は、IGMP Join および Leave メッセージを送信することで、MVR VLAN 上のマルチキャスト ストリームへの加入および脱退を行うことができます。MVR グループからの IGMP Leave メッセージは、Leave メッセージを受信する VLAN の IGMP 設定に従って処理されます。IGMP 高速脱退が VLAN でイネーブルになっている場合、ポートがただちに削除されます。それ以外の場合は、他のホストがポートに存在するかどうかを判断するために、IGMP クエリーがグループに送信されます。

MVR の他の機能との相互運用性

MVR と IGMP スヌーピング

MVR は IGMP スヌーピングの基本メカニズムで動作しますが、この 2 つの機能はそれぞれ単独で動作します。それぞれ、もう一方の機能の動作に影響を与えずにイネーブルまたはディセーブルに設定できます。IGMP スヌーピングがグローバルに、あるいは VLAN でディセーブルになっている場合、および MVR が VLAN でイネーブルになっている場合、IGMP スヌーピングは VLAN で内部的にイネーブルになります。非 MVR レシーバ ポート上で MVR グループ用に受信した Join、または MVR レシーバ ポート上で非 MVR グループ用に受信した Join は、IGMP スヌーピングによって処理されます。

MVR と vPC

- IGMP スヌーピングと同様に、仮想ポート チャネル（vPC）ピア スイッチで受信された IGMP 制御メッセージは、ピア間で交換され、MVR グループ情報を同期できます。
- MVR 設定は、ピア間で一貫している必要があります。
- no ip igmp snooping mrouter vpc-peer-link コマンドは MVR に適用されます。このコマンドを使用する際、VLAN に孤立ポートがない限り、マルチキャスト トラフィックは送信元 VLAN およびレシーバ VLAN のピア リンクに送信されません。
- show mvr member コマンドは、vPC ピア スイッチのマルチキャスト グループを表示します。ただし、vPC ピア スイッチは、グループの IGMP メンバーシップ レポートを受信しない場合、マルチキャスト グループを表示しません。

MVR と vPC

- IGMP スヌーピングと同様に、仮想ポート チャネル（vPC）ピア スイッチで受信された IGMP 制御メッセージは、ピア間で交換され、MVR グループ情報を同期できます。
- MVR 設定は、ピア間で一貫している必要があります。
- no ip igmp snooping mrouter vpc-peer-link コマンドは MVR に適用されます。このコマンドを使用する際、VLAN に孤立ポートがない限り、マルチキャスト トラフィックは送信元 VLAN およびレシーバ VLAN のピア リンクに送信されません。

- show mvr member コマンドは、vPC ピア スイッチのマルチキャスト グループを表示します。ただし、vPC ピア スイッチは、グループの IGMP メンバーシップ レポートを受信しない場合、マルチキャスト グループを表示しません。

MVR に関する注意事項と制約事項

MVR には、次のガイドラインと制限事項があります。

- N3K-C36180YC-R および N3K-C3636C-R ラインカードを備えた Cisco Nexus 3600 プラットフォーム スイッチでは、MVR がサポートされます。
- MVR は、個々のポート、ポート チャネル、仮想イーサネット（vEth）ポートなどのレイヤ 2 イーサネット ポートでのみサポートされます。
- MVR レシーバ ポートはアクセス ポートでなければなりません。トランク ポートにはできません。MVR 送信元ポートは、アクセス ポートまたはトランク ポートのどちらかにする必要があります。
- Flex Link ポートでの MVR の設定はサポートされません。
- プライオリティ タギングは、MVR レシーバ ポートではサポートされません。
- MVR VLAN の合計数は 250 未満にする必要があります。

MVR のデフォルト設定

次の表に、MVR パラメータのデフォルト設定を示します。

表 *20* : デフォルトの *MVR* パラメータ

パラメータ	デフォルト
MVR	グローバルおよびインターフェイス単位でディセーブル
グローバル MVR VLAN	未設定
インターフェイス（ポートごと）	受信ポートでも送信元ポートでもない

MVR の設定

MVR グローバルおよびインターフェイス パラメータを構成して、MVR プロセスの動作に影響を与えることができます。

MVR グローバル パラメータの設定

MVR とさまざまな構成パラメータをグローバルに有効にすることができます。

手順の概要

1. **configure terminal**
2. [**no**] **mvr**
3. [**no**] **mvr-vlan** *vlan-id*
4. [**no**] **mvr-group** *addr* [*/mask*] [*count groups*] [**vlan** *vlan-id*]
5. （任意） **clear mvr counters** [**source-ports** | **receiver-ports**]
6. （任意） **show mvr**
7. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	[**no**] **mvr**
	例：
	`switch(config)# mvr`
	`switch(config-mvr)#`
		MVR をグローバルに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。
		MVR を無効にするには、このコマンドの no 形式を使用します。

ステップ 3	[**no**] **mvr-vlan** *vlan-id* 例： `switch(config-mvr)# mvr-vlan 7`	グローバルなデフォルト MVR VLAN を指定します。MVR VLAN は、後続のレシーバが加入するマルチキャスト メッセージの送信元です。指定できる範囲は 1 ～ 4094 です。 MVR VLAN をクリアするには、コマンドの no 形式を使用します。
ステップ 4	[**no**] **mvr-group** *addr* [*/mask*] [*count groups*] [**vlan** *vlan-id*] 例： `switch(config-mvr)# mvr-group 230.1.1.1 count 4`	指定した IPv4 アドレスのマルチキャスト グループ（およびオプションとしてのネットマスク長）をグローバルなデフォルト MVR VLAN に追加します。このコマンドを繰り返して、追加グループを MVR VLAN に追加することができます。 IP アドレスは a.b.c.d/m 形式で入力します。m はネットマスクのビット数（1 ～ 31）です。

	コマンドまたはアクション	目的
		オプションとして、指定したIPドレスから始まる連続マルチキャストIPアドレスを使用して、いくつかのMVRグループを指定できます。countキーワードを使用して、その後に1～64の番号を指定します。 オプションで、vlanキーワードを使用してグループのMVR VLANを指定できます。それ以外の場合、グループはデフォルトのMVR VLANに割り当てられます。 グループ設定をクリアするには、コマンドのno形式を使用します。
ステップ5	（任意） **clear mvr counters** [**source-ports** | **receiver-ports**] 例： `switch(config-mvr)# clear mvr counters`	MVR IGMPパケット カウンタをクリアします。
ステップ6	（任意） **show mvr** 例： `switch(config-mvr)# show mvr`	グローバルMVR設定を表示します。
ステップ7	（任意） **copy running-config startup-config** 例： `switch(config-mvr)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

MVR インターフェイスの設定

Cisco NX-OSデバイスでMVRインターフェイスを設定できます。

手順の概要

1. **configure terminal**
2. **mvr**
3. **interface** {**ethernet slot/port** | **port-channel channel-number** | **ethernet** *number*}
4. [**no**] **mvr-type** {**source** |**receiver**}
5. （任意） [**no**] **mvr-vlan** {**vlan-id**}
6. [**no**] **mvr-group addr** [**/mask**] {**vlan** *vlan-id*}
7. **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**mvr**
	例：
	`switch(config)# mvr`
	`switch(config-mvr)#`
		MVR をグローバルに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。
		（注）
		MVR がグローバルにイネーブルになっている場合は、このコマンドは必要ありません。

ステップ 3	**interface** {**ethernet slot/port** | **port-channel channel-number** | **ethernet** *number*}
	例：
	`switch(config-mvr)# interface ethernet 2/2`
	`switch(config-mvr-if)#`
		設定するレイヤ 2 ポートを指定して、インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	[**no**] **mvr-type** {**source** |**receiver**}
	例：
	`switch# configure terminal`
	`switch(config)#`
		MVR ポートを、次のポート タイプのいずれかに設定します。
		• 送信元：マルチキャスト データを送受信するアップリンク ポートが MVR 送信元として構成されます。そのポートは、自動的に MVR マルチキャスト グループのスタティック レシーバになります。送信元ポートを MVR VLAN のメンバにする必要があります。
		• 受信者：MVR マルチキャスト グループに登録するホストに接続されているアクセス ポートが MVR受信者として設定されます。レシーバ ポートでデータを受信するのは、IGMP Leave および Join メッセージを使用してそのポートがマルチキャスト グループのメンバになっている場合だけです。
		MVR 特性を使用して非MVR ポートを設定しようとすると、その設定はキャッシュされますが、そのポートが MVR ポートがになるまで有効になりません。デフォルトのポート モードは非 MVR です。

	コマンドまたはアクション	目的
ステップ 5	（任意） [**no**] **mvr-vlan** {**vlan-id**} 例： `switch(config-mvr-if)# mvr-vlan 7`	インターフェイスで受信された Join 用にグローバルなデフォルト MVR VLAN を上書きするインタフェースのデフォルト MVR VLAN を指定します。MVR VLAN は、後続のレシーバが加入するマルチキャストメッセージの送信元です。指定できる範囲は 1 ～ 4094 です。
ステップ 6	[**no**] **mvr-group addr** [**/mask**] {**vlan** *vlan-id*} 例： `switch(config-mvr-if)# mvr-group 225.1.3.1 vlan 100`	指定した IPv4 アドレスのマルチキャスト グループ（およびオプションのネットマスク長）をインターフェイス MVR VLAN に追加し、グローバル MVR グループ設定を上書きします。このコマンドを繰り返して、付加的なグループを MVR VLAN に追加することができます。 IP アドレスは a.b.c.d/m 形式で入力します。m はネットマスクのビット数（1 ～ 31）です。 オプションとして、グループの MVR VLAN を vlan キーワードを使用して指定することができます。このキーワードを使用しない場合、グループはインターフェイスのデフォルト（指定した場合）またはグローバルなデフォルト MVR VLAN に割り当てられます。 IPv4 アドレスとネットワークマスクをクリアするには、コマンドの形式を使用します。
ステップ 7	**copy running-config startup-config** 例： `switch(config-mvr-if)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VLAN からの IGMP クエリ転送の抑制

ソース VLAN からレシーバ VLAN への IGMP 一般クエリを抑制するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **mvr-config**
3. **mvr-suppress-query vlan** *vlan-ID*

手順の詳細

手順

	コマンドまたはアクション	目的

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

ステップ 2	**mvr-config**
	例：
	`switch# mvr-config`
	`switch(config-mvr)#`
		グローバル MVR 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	**mvr-suppress-query vlan** *vlan-ID*
	例：
	`switch(config-mvr)# mvr-suppress-query vlan 1-5`
	`switch(config-mvr)#`
		一般クエリを抑制する必要がある MVR ID またはソース VLAN 範囲を表示します。VLAN ID の値は 1 ～ 3967 です。VLAN ID は、1 ～ 5、10、または 2 ～ 5、7 ～ 19 の範囲で表すこともできます。

MVR 設定の確認

MVR の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show mvr	MVR サブシステムの設定およびステータスを表示します。
show mvr groups	MVR グループの設定を表示します。
show ip igmp snooping [**vlan** *vlan-id*]	指定した VLAN 上の IGMP スヌーピング情報を表示します。
show mvr interface {*ethernet slot/port* | **port-channel number**}	指定したインターフェイスの MVR 設定を表示します。
show mvr members [**count**]	すべての MVR 受信者メンバーの数と詳細を表示します。
show mvr members interface {**ethernet slot/port** | **port-channel number**}	指定したインターフェイスの MVR メンバの詳細を表示します。
show mvr members vlan *vlan-id*	指定した VLAN の MVR メンバの詳細を表示します。

コマンド	目的
show mvr receiver-ports [**ethernet slot/port** | **port-channel number**]	すべてのインターフェイスまたは指定したインターフェイスのすべての MVR レシーバ ポートを表示します。
show mvr source-ports [**ethernet slot/port** | **port-channel number**]	すべてのインターフェイスまたは指定したインターフェイスのすべての MVR 送信元ポートを表示します。

次に、MVR パラメータを確認する例を示します。

```
switch# show mvr
MVR Status : enabled
Global MVR VLAN : 100
Number of MVR VLANs : 4
```

次に、MVR グループ設定を確認する例を示します。

```
switch# show mvr groups
* - Global default MVR VLAN.
Group start Group end Count MVR-VLAN Interface
Mask
------------- --------------- ------ -------- -----------
228.1.2.240 228.1.2.255 /28 101
230.1.1.1 230.1.1.4 4 *100
235.1.1.6 235.1.1.6 1 340
225.1.3.1 225.1.3.1 1 *100 Eth1/10
```

次に、MVR インターフェイス設定とステータスを確認する例を示します。

```
switch# show mvr interface
Port VLAN Type Status MVR-VLAN
---- ---- ---- ------ --------
Po10 100 SOURCE ACTIVE 100-101
Po201 201 RECEIVER ACTIVE 100-101,340
Po202 202 RECEIVER ACTIVE 100-101,340
Po203 203 RECEIVER ACTIVE 100-101,340
Po204 204 RECEIVER INACTIVE 100-101,340
Po205 205 RECEIVER ACTIVE 100-101,340
Po206 206 RECEIVER ACTIVE 100-101,340
Po207 207 RECEIVER ACTIVE 100-101,340
Po208 208 RECEIVER ACTIVE 2000-2001
Eth1/9 340 SOURCE ACTIVE 340
Eth1/10 20 RECEIVER ACTIVE 100-101,340
Eth2/2 20 RECEIVER ACTIVE 100-101,340
Eth102/1/1 102 RECEIVER ACTIVE 100-101,340
Eth102/1/2 102 RECEIVER INACTIVE 100-101,340
Eth103/1/1 103 RECEIVER ACTIVE 100-101,340
Eth103/1/2 103 RECEIVER ACTIVE 100-101,340
Status INVALID indicates one of the following misconfiguration:
a) Interface is not a switchport.
b) MVR receiver is not in access.
c) MVR source is in fex-fabric mode.
```

次に、すべての MVR メンバを表示する例を示します。

```
switch# show mvr members
MVR-VLAN Group Address Status Members
-------- ------------- ------- -------
100 230.1.1.1 ACTIVE Po201 Po202 Po203 Po205 Po206
100 230.1.1.2 ACTIVE Po205 Po206 Po207 Po208
```

```
340 235.1.1.6 ACTIVE Eth102/1/1
101 225.1.3.1 ACTIVE Eth1/10 Eth2/2
101 228.1.2.241 ACTIVE Eth103/1/1 Eth103/1/2
```

次に、すべてのインターフェイスのすべての MVR レシーバ ポートを表示する例を示します。

```
switch# show mvr receiver-ports
Port MVR-VLAN Status Joins Leaves
(v1,v2,v3)
------------ -------- -------- ------------ ------------
Po201 100 ACTIVE 8 2
Po202 100 ACTIVE 8 2
Po203 100 ACTIVE 8 2
Po204 100 INACTIVE 0 0
Po205 100 ACTIVE 10 6
Po206 100 ACTIVE 10 6
Po207 100 ACTIVE 5 0
Po208 100 ACTIVE 6 0
Eth1/10 101 ACTIVE 12 2
Eth2/2 101 ACTIVE 12 2
Eth102/1/1 340 ACTIVE 16 15
Eth102/1/2 340 INACTIVE 16 16
Eth103/1/1 101 ACTIVE 33 0
Eth103/1/2 101 ACTIVE 33 0
```

次に、すべてのインターフェイスのすべての MVR 送信元ポートを表示する例を示します。

```
switch# show mvr source-ports
Port MVR-VLAN Status
------------ -------- --------
Po10 100 ACTIVE
Eth1/9 340 ACTIVE
```

MVR 設定の例

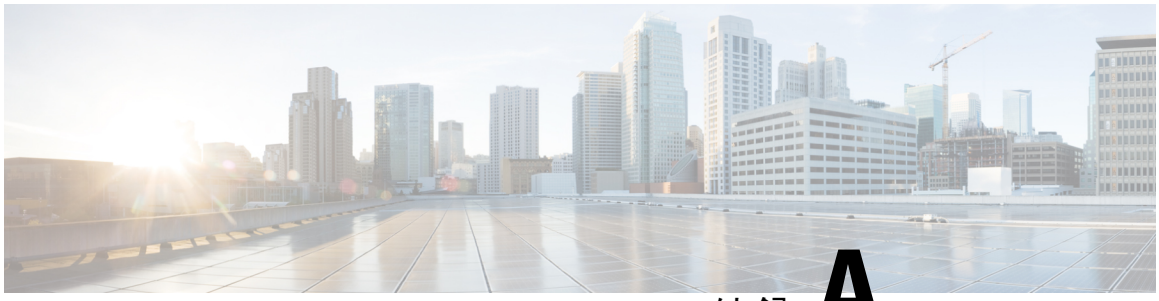
次の例は、MVR をグローバルにイネーブルにし、グローバル パラメータを設定する方法を示しています。

```
switch# configure terminal
switch(config)# mvr
switch(config-mvr)# mvr-vlan 100
switch(config-mvr)# mvr-group 230.1.1.1 count 4
switch(config-mvr)# mvr-group 228.1.2.240/28 vlan 101
switch(config-mvr)# mvr-group 235.1.1.6 vlan 340

switch# show mvr
MVR Status : enabled
Global MVR VLAN : 100
Number of MVR VLANs : 3
```

次の例は、イーサネット ポートを MVR レシーバ ポートとして設定する方法を示しています。

```
switch# configure terminal
switch(config)# mvr
switch(config-mvr)# interface ethernet 1/10
switch(config-mvr-if)# mvr-group 225.1.3.1 vlan 100
switch(config-mvr-if)# mvr-type receiver
```



付録 A

IP マルチキャストについての IETF RFC

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

- IP マルチキャストについての IETF RFC （121 ページ）

IP マルチキャストについての IETF RFC

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

IP マルチキャストについての IETF RFC

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