



Cisco Nexus 9000 シリーズ NX-OS マルチキャストルーティング構成ガイド、リリース 10.2(x)

最終更新：2025 年 7 月 3 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)

© 2021 –2022 Cisco Systems, Inc. All rights reserved.



目次

はじめに :

はじめに **xi**

対象読者 **xi**

表記法 **xi**

Cisco Nexus 9000 シリーズ スイッチの関連資料 **xii**

マニュアルに関するフィードバック **xii**

Communications, services, and additional information **xiii**

Cisco Bug Search Tool **xiii**

Documentation feedback **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 **5**

ライセンス要件 **5**

サポートされるプラットフォーム **5**

マルチキャストに関する情報 **5**

マルチキャスト配信ツリー **6**

送信元ツリー **6**

共有ツリー **7**

双方向共有ツリー **8**

マルチキャスト転送 **9**

Cisco NX-OS の PIM **10**

アーキテクチャ セールス マネージャ (ASM) **12**

Bidir **12**

SSM **12**

マルチキャスト用 RPF ルート	13
IGMP	13
IGMP スヌーピング	13
ドメイン内マルチキャスト	13
SSM	13
MSDP	13
MBGP	14
MRIB	14
仮想ポート チャンネルおよびマルチキャスト	15
マルチキャストに関する注意事項と制限事項	16
マルチキャストのハイ アベイラビリティ要件	16
仮想デバイス コンテキスト	16
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	17

第 3 章

IGMP の設定	19
IGMP について	19
IGMP のバージョン	20
IGMP の基礎	20
IGMP の前提条件	23
IGMP に関する注意事項と制限事項	23
IGMP のデフォルト設定	24
IGMP パラメータの設定	25
IGMP インターフェイス パラメータの設定	25
IGMP SSM 変換の設定	32
ルータ アラートの適用オプション チェックの設定	33
IGMP ホスト プロキシの設定	34
IGMP ホスト プロキシの概要	34
IGMP の加入処理	35
IGMP の脱退処理	35
IGMP ホスト プロキシの設定方法	35
IGMP SG プロキシの構成	36
IGMP SG プロキシ	36

IGMP SG プロキシの構成 37

IGMP プロセスの再起動 38

IGMP 構成の確認 39

IGMP の設定例 39

第 4 章

MLD の設定 41

MLD について 41

MLD のバージョン 42

MLD の基礎 42

MLD スヌーピング 44

MLD の前提条件 45

MLD の注意事項および制限事項 45

MLD のデフォルト設定 46

MLD スヌーピングの設定 47

MLD パラメータの設定 50

MLD インターフェイス パラメータの設定 51

MLD SSM 変換の設定 57

MLD の設定の確認 58

MLD スヌーピングの設定の確認 59

MLD の設定例 60

第 5 章

PIM および PIM6 の設定 61

PIM および PIM6 について 61

vPC を使用した PIM SSM 62

Hello メッセージ 63

Join-Prune メッセージ 64

ステートのリフレッシュ 64

ランデブー ポイント 65

スタティック RP 65

BSR 65

Auto-RP 66

PIM ドメインで設定された複数の RP	67
Anycast-RP	67
PIM 登録メッセージ	68
指定ルータ	69
指定フォワーダ	69
共有ツリーから送信元ツリーへの ASM スイッチオーバー	70
マルチキャスト フロー パスの可視性	70
管理用スコープの IP マルチキャスト	70
マルチキャスト カウンタ	71
マルチキャスト ヘビー テンプレート	71
マルチキャスト VRF-Lite ルート リーク	71
PIM グレースフル リスタート	72
生成 ID	72
PIM グレースフル リスタート動作	72
PIM のグレースフル リスタートおよびマルチキャスト トラフィック フロー	74
高可用性	74
PIM および PIM6 の前提条件	74
PIM および PIM6 に関する注意事項と制限事項	75
Hello メッセージに関する注意事項と制限事項	80
ランデブー ポイントの注意事項と制限事項	80
マルチキャスト VRF-lite ルート リークの注意事項と制限事項	81
デフォルト設定	81
PIM および PIM6 の設定	83
PIM および PIM6 の設定作業	83
PIM および PIM6 機能のイネーブル化	84
PIM または PIM6 スパース モード パラメータの設定	85
PIM6 スパース モード パラメータの設定	88
PIM6 スパース モード パラメータの構成	92
ASM と Bidir の設定	94
静的 RP の設定	94
BSR の設定	97

Auto-RP の設定	100
PIM Anycast-RP セットの設定	103
ASM 専用の共有ツリーの設定	109
SSM (PIM) の設定	111
vPC を介した PIM SSM の設定	113
マルチキャスト用 RPF ルートの設定	115
マルチキャスト マルチパスの設定	116
マルチキャスト VRF-Lite ルート リークの設定	117
RP 情報配信を制御するルート マップの設定	118
RP 情報配信を制御するルート マップの設定 (PIM)	119
RP 情報配信を制御するルート マップの設定 (PIM6)	120
メッセージフィルタリングの設定	121
メッセージフィルタリングの設定 (PIM)	123
メッセージフィルタリングの設定 (PIM6)	125
PIM および PIM6 プロセスの再起動	127
PIM プロセスの再起動	127
PIM6 プロセスの再起動	128
VRF モードでの PIM の BFD の設定	129
インターフェイス モードでの PIM の BFD の設定	130
マルチキャスト ヘビー テンプレートと拡張ヘビー テンプレートの有効化	131
PIM および PIM6 設定の検証	133
統計の表示	141
PIM および PIM6 の統計情報の表示	141
PIM および PIM6 統計情報のクリア	142
マルチキャスト サービス リフレクションの設定	142
マルチキャスト サービス リフレクションの注意事項と制限事項	143
前提条件	145
マルチキャスト サービス リフレクションの設定	145
マルチキャスト サービス リフレクションの設定例	150
ユニキャストからマルチキャスト NAT へ	152
PIM の設定例	155

SSM の設定例	156
PIM SSM over vPC の設定例	156
BSR の設定例	161
Auto-RP の設定例	162
PIM エニーキャスト RP の設定例	162
プレフィックススペースおよびルートマップベースの設定	164
出力	165
関連資料	166
標準	166
MIB	166

第 6 章

PIM 許可 RP の設定	167
はじめに	167
PIM 許可 RP の注意事項と制限事項	167
PIM 許可 RP に関する情報	168
PIM-SM の RP の構成	169
PIM Allow RP の有効化	170
許可 RP ポリシーに関する情報の表示	172

第 7 章

IGMP スヌーピングの構成	175
IGMP スヌーピングについて	175
IGMPv1 および IGMPv2	176
IGMPv3	177
IGMP スヌーピングクエリア	177
仮想化のサポート	178
IGMP スヌーピングの前提条件	178
IGMP スヌーピングに関する注意事項と制限事項	178
デフォルト設定	180
IGMP スヌーピング パラメータの設定	180
グローバル IGMP スヌーピング パラメータの設定	180
VLAN ごとの IGMP スヌーピング パラメータの設定	183

IGMP スヌーピング設定の確認	188
IGMP スヌーピング統計情報の表示	188
IGMP スヌーピング統計情報のクリア	189
IGMP スヌーピングの設定例	189

第 8 章

MSDP の設定 191

MSDP について	191
SA メッセージおよびキャッシング	192
MSDP ピア RPF 転送	193
MSDP メッシュ グループ	193
MSDP の前提条件	194
デフォルト設定	194
MSDP の設定	194
MSDP 機能の有効化	195
MSDP ピアの構成	196
MSDP ピア パラメータの設定	197
MSDP グローバル パラメータの設定	200
MSDP メッシュ グループの設定	202
MSDP プロセスの再起動	203
MSDP の設定の確認	204
MSDP のモニタリング	204
統計の表示	204
統計情報のクリア	205
MSDP の設定例	205
関連資料	206
標準	207

第 9 章

MVR の設定 209

MVR について	209
MVR の他の機能との相互運用性	210
MVR に関する注意事項と制約事項	210

デフォルトの MVR 設定	211
MVR の設定	211
MVR グローバル パラメータの設定	211
MVR インターフェイスの設定	213
VLAN からの IGMP クエリ転送の抑制	215
MVR 設定の確認	215
MVR 設定の例	218

第 10 章	Microsoft ネットワーク ロード バランシング (NLB) の設定	219
	ネットワーク ロード バランシング (NLB) について	219
	NLB の注意事項と制限事項	220
	Microsoft ネットワーク ロード バランシング (NLB) の前提条件	221
	マルチキャスト モード	222
	IGMP マルチキャスト モード	223
	NLB の設定の確認	225

付録 A :	IP マルチキャストについての IETF RFC	227
	IP マルチキャストについての IETF RFC	227

付録 B :	Cisco NX-OS のマルチキャストに関する設定の限界	229
	構成の制限値	229



はじめに

この前書きは、次の項で構成されています。

- [対象読者](#) (xi ページ)
- [表記法](#) (xi ページ)
- [Cisco Nexus 9000 シリーズ スイッチの関連資料](#) (xii ページ)
- [マニュアルに関するフィードバック](#) (xii ページ)
- [Communications, services, and additional information](#) (xiii ページ)

対象読者

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

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
<i>italic</i>	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。

表記法	説明
[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。
[]	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 9000 シリーズ スイッチの関連資料

Cisco Nexus 9000 シリーズ スイッチ全体のマニュアルセットは、次の URL にあります。

https://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

Communications, services, and additional information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit [Cisco DevNet](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



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 10.2(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
IGMPv3 は SSM をサポート	IGMPv3 の SSM サポートが追加されました。	10.2(2)F	IGMP の基礎 (20 ページ)
ユニキャストからマルチキャスト NAT へ	ユニキャストからマルチキャストへの NAT は、入力変換モードで機能します。マルチキャスト変換されたパケットは、出力変換してマルチキャストに戻すことができます。ユニキャストパケットの宛先アドレスは、NAT サービス リフレクションインターフェイスと一致する必要があります。	10.2(2)F	ユニキャストからマルチキャスト NAT へ (152 ページ)
マルチキャスト NLB	Cisco N9K-C9332D-GX2B プラットフォームスイッチでマルチキャスト NLB のサポートが追加されました。	10.2(1q)F	NLB の注意事項と制限事項 (220 ページ)

特長	説明	変更が行われたリリース	参照先
マルチキャスト NAT	Cisco N9K-C9332D-GX2B プラットフォームスイッチでマルチキャスト NAT のサポートが追加されました。	10.2(1q)F	
マルチキャスト GRE	Cisco N9K-C9332D-GX2B プラットフォームスイッチでマルチキャスト GRE のサポートが追加されました。	10.2(1q)F	PIM および PIM6 に関する注意事項と制限事項 (75 ページ)
MLD スヌーピング	Cisco N9K-C9332D-GX2B プラットフォームスイッチで MLD スヌーピングのサポートが追加されました。	10.2(1q)F	MLD の注意事項および制限事項 (45 ページ)
IGMP ホストプロキシ	Cisco N9K-C9332D-GX2B プラットフォームスイッチで IGMP ホストプロキシのサポートが追加されました。	10.2(1q)F	IGMP に関する注意事項と制限事項 (23 ページ)
レイヤ 2 およびレイヤ 3 マルチキャスト	Cisco N9K-C9332D-GX2B プラットフォームスイッチでレイヤ 2 およびレイヤ 3 マルチキャストのサポートが追加されました。	10.2(1q)F	マルチキャストに関する注意事項と制限事項 (16 ページ)
TRM フローのマルチキャストフローパスの可視性	TRM L3 モードとアンダーレイマルチキャストのサポートが追加されました。	10.2 (1) F	マルチキャストフローパスの可視性 (70 ページ)
マルチキャスト NAT : マルチキャストからユニキャストへ	マルチキャストからユニキャストへの NAT 変換は、出力モードでのみサポートされます。	10.2 (1) F	マルチキャストサービスリフレクションの注意事項と制限事項 (143 ページ)

特長	説明	変更が行われたリリース	参照先
グローバル境界マルチキャスト構成	ルータのすべてのインターフェイスで未認可グループまたはチャネルのマルチキャストプロトコルアクションおよびトラフィック転送を無効化します。	10.2 (1) F	MRIB (14 ページ)



第 2 章

概要

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

- [ライセンス要件 \(5 ページ\)](#)
- [サポートされるプラットフォーム \(5 ページ\)](#)
- [マルチキャストについて \(5 ページ\)](#)
- [マルチキャストに関する注意事項と制限事項 \(16 ページ\)](#)
- [マルチキャストのハイ アベイラビリティ要件 \(16 ページ\)](#)
- [仮想デバイス コンテキスト \(16 ページ\)](#)
- [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 \(17 ページ\)](#)

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、しばしばチャンネルと呼ばれます。Internet Assigned Number Authority (IANA) では、IPv4 マルチキャスト アドレスとして、224.0.0.0 ~ 239.255.255.255 を割り当てています。詳細については、次の URL を参照してください。
<http://www.iana.org/assignments/multicast-addresses>

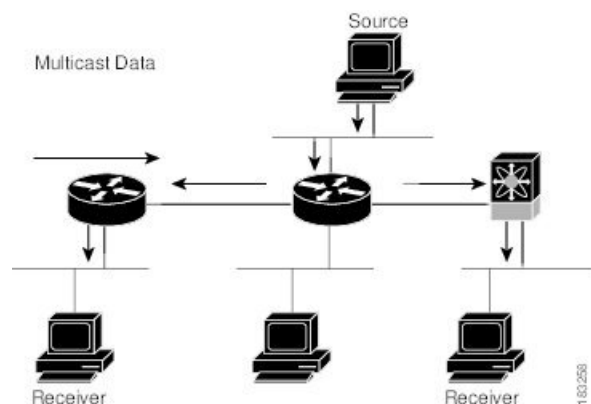


(注) マルチキャストに関連する RFC の完全なリストについては、「IP マルチキャストに関する IETF RFC」の章を参照してください。

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



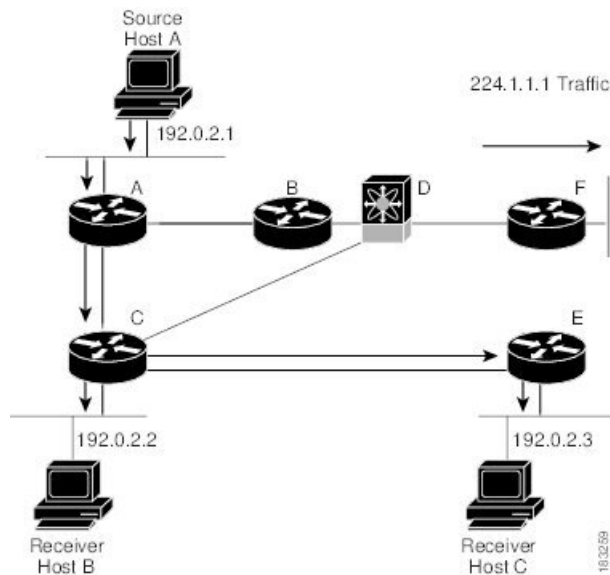
マルチキャスト配信ツリー

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。この図は、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

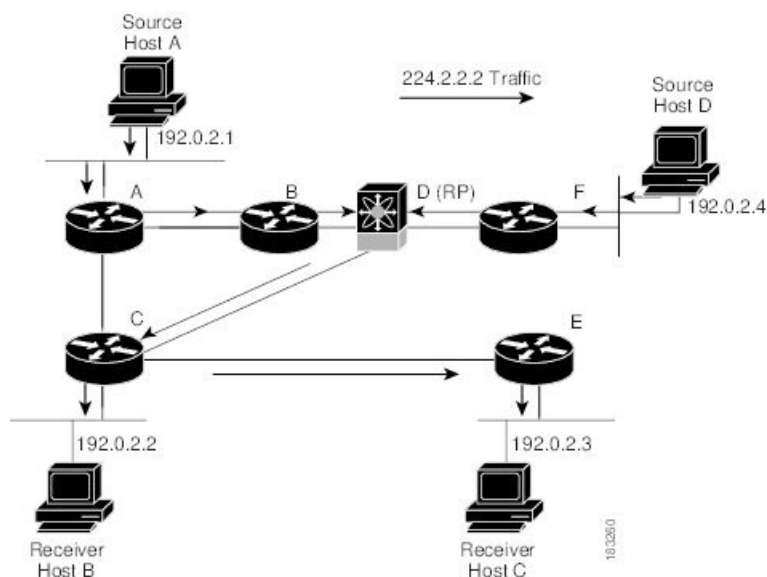


表記 (S,G) は、グループ G の任意の送信元からのマルチキャストトラフィックを表します。この図の SPT は、(192.0.2.1, 224.1.1.1) と記述されます。同じグループの複数の送信元からトラフィックを送信できます。

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。この図は、ルータ D に RP を持つ、グループ 224.2.2.2 の共有ツリーを示しています。データは送信元ホスト A およびホスト D からルータ D (RP) に送信され、そこから受信者ホスト B およびホスト C にトラフィックが転送されます。

図 3: 共有ツリー

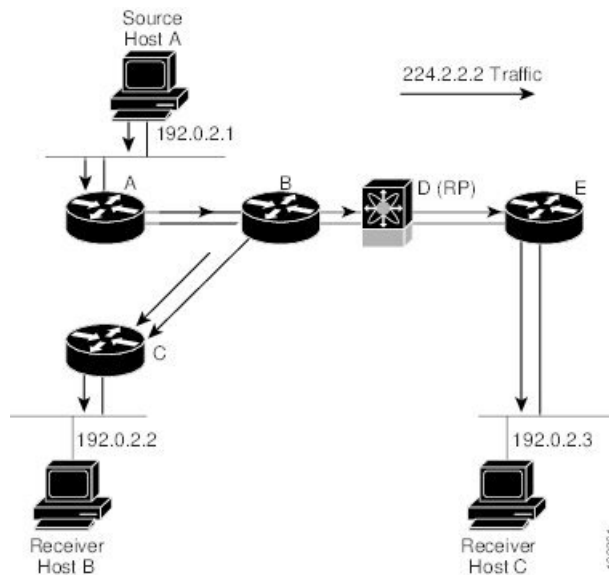


表記 (*,G) は、グループ G の任意の送信元からのマルチキャストトラフィックを表します。図の共有ツリーは、(*, 224.2.2.2) と記述されます。

双方向共有ツリー

双方向共有ツリーとは、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。マルチキャストデータは、RP への経路上にある受信者に転送されます。次の表に、双方向共有ツリーの利点を示します。マルチキャストトラフィックは、ルータ B および C を通して、ホスト A からホスト B に直接送られます。共有ツリーの場合、送信元ホスト A から送信されたデータは、まず RP (ルータ D) に送信され、ルータ B に転送されてからホスト B に伝送されます。

図 4: 双方向共有ツリー



表記 (*,G) は、グループ G の任意のソースからのマルチキャストトラフィックを表します。図の双方向ツリーは、(*, 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)、または RP 方向へ向かうパス (ASM または Bidir モード) 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。

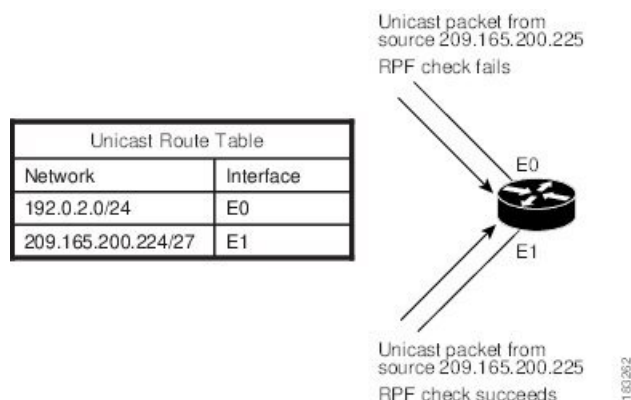
マルチキャストパケットが着信するたびに、ルータは RPF チェックを実行します。送信元に接続されたインターフェイスにパケットが着信した場合は、グループの発信インターフェイス (OIF) リスト内の各インターフェイスにパケットが転送されます。それ以外の場合、パケットはドロップされます。



- (注) Bidir モードでは、パケットが非 RPF インターフェイスに着信した際に、インターフェイスが指定フォワーダ (DF) として選択されていれば、パケットは RP に向かうアップストリーム方向にも転送されます。

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 5: RPF チェックの例



Cisco NX-OS の PIM

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



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

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

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

配信ツリーは、リンク障害またはルータ障害のためにトポロジが変更されると、トポロジを反映して自動的に変更されます。PIM はマルチキャスト対応の送信元および受信者を動的に追跡します。ただし、Bidir モードの場合、送信元ステートは生成されません。

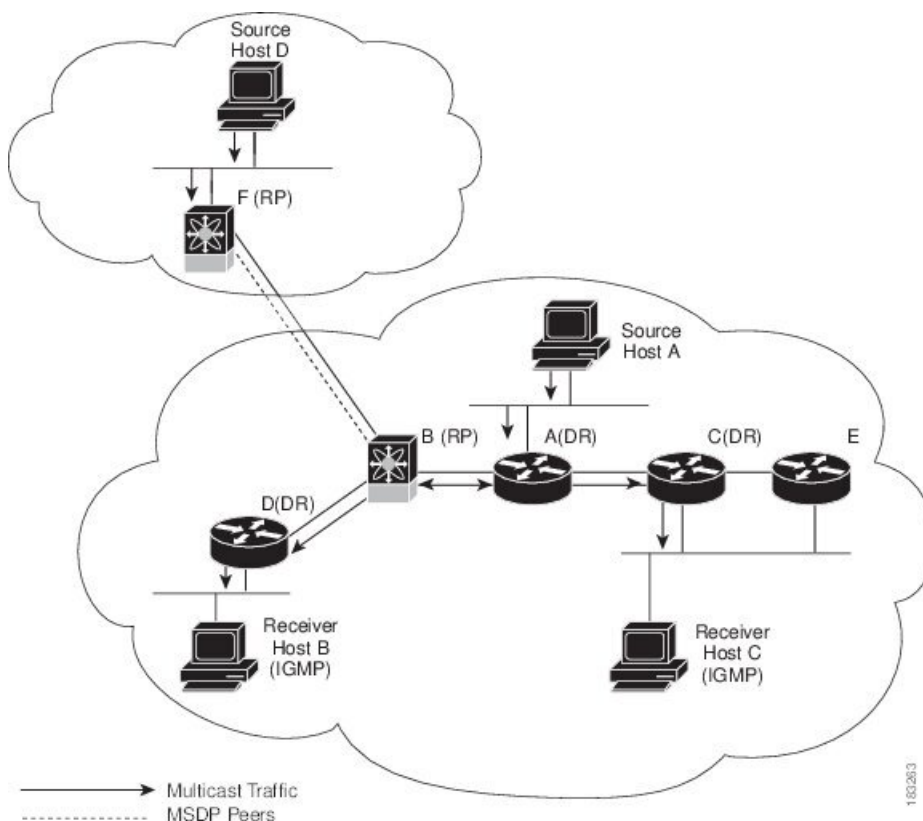
ルータはユニキャストルーティングテーブルおよび RPF ルートを使用して、マルチキャストルーティング情報を生成します。Bidir モードの場合は、追加のルーティング情報が生成されます。



(注) このマニュアルでは、「IPv4 用の PIM」という表現は、Cisco NX-OS における PIM スパース モードの実装を表します。

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

図 6: IPv4 ネットワーク内の PIM ドメイン



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

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

PIM は送信元と受信者間の接続に関して、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)
- 双方向共有ツリー (Bidir)

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 が学習されている場合、かつ Bidir-RP であるかどうか不明な場合、グループは ASM モードで動作します。

RP を設定する場合、デフォルト モードは ASM モードです。

Bidir

双方向共有ツリー (Bidir) は ASM モードと同様、受信者と RP の間の共有ツリーを構築する PIM モードです。ただし、グループに新しい受信者が追加された場合、送信元ツリーに切り替えることはできません。Bidir モードの場合、受信者に接続されたルータは代表フォワード (DF) と呼ばれます。これは、RP を経由することなく、代表ルータ (DR) から受信者に直接マルチキャスト データを転送できるためです。Bidir モードを利用するには、RP を設定する必要があります。

Bidir モードを使用すると、マルチキャスト送信元が多数存在する場合に、ルータに必要なリソース量を削減するとともに、RP の動作ステータスや接続ステータスに関係なく、運用を継続できます。

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。

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。

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 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には、(S, G) を使用して IGMPv3 を設定する必要があります。デフォルトでは IGMPv2 がイネーブルになっています。

IGMP スヌーピング

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

ドメイン内マルチキャスト

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

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 および Bidir 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。

MSDP

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



(注) Cisco NX-OS では、MSDP 設定が不要な PIM Anycast-RP をサポートしています。

MBGP

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

MRIB

Cisco NX-OS IPv4 マルチキャストルーティング情報ベース (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) インスタンスごとに、独立したルート情報を保持します。

Cisco NX-OS リリース 10.2(1) 以降、グローバル境界マルチキャスト設定がサポートされています。

グローバル マルチキャスト境界で許可または拒否される IP マルチキャスト グループおよびチャネルのグローバル範囲を定義するには、VRF コンフィギュレーションモードで **`{ip|ipv6} multicast group-range prefix-list <prefix-list-name>`** コマンドを設定する必要があります。このコマンドは、ルータのすべてのインターフェイスで、未認可グループまたはチャネルのマルチキャストプロトコルアクションおよびトラフィック転送をディセーブルにするために使用されます。prefix-list は境界を構成します。次に設定例を示します。

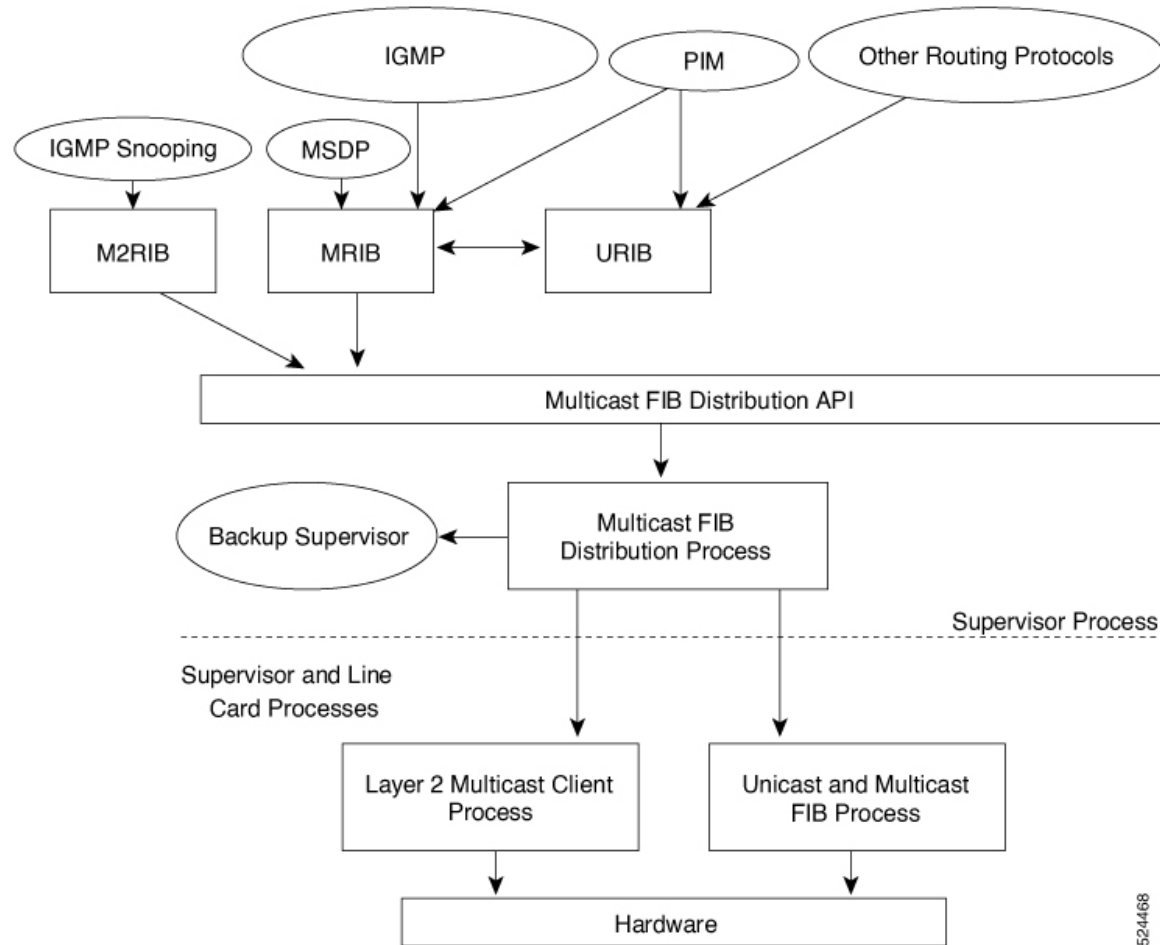
```
vrf context enterprise
ip multicast group-range prefix-list test
```

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

- マルチキャスト FIB (MFIB) 分散 (MFD) 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、プラットフォーム転送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、MFD API を使用してレイヤ 3 ルート アップデートを送信します。
- マルチキャスト FIB 配信プロセス：すべての関連モジュールおよびスタンバイ スーパーバイザに、マルチキャスト アップデート メッセージを配布します。このプロセスはスーパーバイザだけで実行されます。
- レイヤ 2 マルチキャスト クライアント プロセス：レイヤ 2 マルチキャスト ハードウェア転送パスを構築します。このプロセスは、スーパーバイザとモジュールの両方で実行されます。
- ユニキャストおよびマルチキャスト FIB プロセス：レイヤ 3 ハードウェア転送パスを管理します。このプロセスは、スーパーバイザとモジュールの両方で実行されます。

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

図 7: Cisco NX-OS マルチキャスト ソフトウェアのアーキテクチャ



524468

仮想ポート チャンネルおよびマルチキャスト

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

- PIM : Cisco Nexus 9000 シリーズ スイッチ対応の Cisco NX-OS ソフトウェアは、vPC での PIM Bidir をサポートしません。
- IGMP スヌーピング : vPC ピアの設定を同一にする必要があります。

より低い IP アドレスを持つ L2 デバイスでスヌーピング クエリアを設定して、L2 デバイスをクエリアとして強制することをお勧めします。これは、マルチシャード EtherChannel トランク (MCT) がダウンしているシナリオの処理に役立ちます。

マルチキャストに関する注意事項と制限事項

- Cisco NX-OS リリース 10.2(1q)F 以降、Cisco Nexus N9K-C9332D-GX2B プラットフォームスイッチではレイヤ 2 およびレイヤ 3 マルチキャストがサポートされます。
- Cisco NX-OS リリース 10.1(2) 以降、N9K-X9624D-R2 ラインカードではレイヤ 3 マルチキャストがサポートされます。
- レイヤ 3 イーサネットポートチャネルサブインターフェイスは、マルチキャストルーティングで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。
- 不明なマルチキャストトラフィックによるトラフィックストーム制御はサポートされていません。
- FEX ポートでのレイヤ 3 マルチキャストルーティングおよび FEX ポートチャネルでのレイヤ 3 マルチキャストルーティングは、Cisco Nexus 9300-FX および -EX プラットフォームスイッチでサポートされています。
- 双方向モードは、-R ラインカードを備えた Cisco Nexus 9500 プラットフォームスイッチではサポートされていません。
- IPv6 マルチキャストは、Cisco Nexus 9500 R シリーズラインカードではサポートされていません。

マルチキャストのハイアベイラビリティ要件

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

仮想デバイスコンテキスト

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

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。



第 3 章

IGMP の設定

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

- [IGMP について \(19 ページ\)](#)
- [IGMP の前提条件 \(23 ページ\)](#)
- [IGMP に関する注意事項と制限事項 \(23 ページ\)](#)
- [IGMP のデフォルト設定 \(24 ページ\)](#)
- [IGMP パラメータの設定 \(25 ページ\)](#)
- [IGMP ホスト プロキシの設定 \(34 ページ\)](#)
- [IGMP SG プロキシの構成 \(36 ページ\)](#)
- [IGMP プロセスの再起動 \(38 ページ\)](#)
- [IGMP 構成の確認 \(39 ページ\)](#)
- [IGMP の設定例 \(39 ページ\)](#)

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ン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ンネルに関する受信データをマルチキャスト送信します。

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

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

IGMP のバージョン

デバイスでは、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。



(注) Cisco Nexus 9000 シリーズ スイッチは、Cisco NX-OS リリース 7.0(3)I2(1) までは SSM をサポートしていません。

IGMPv2 の詳細については、[RFC 2236](#) を参照してください。

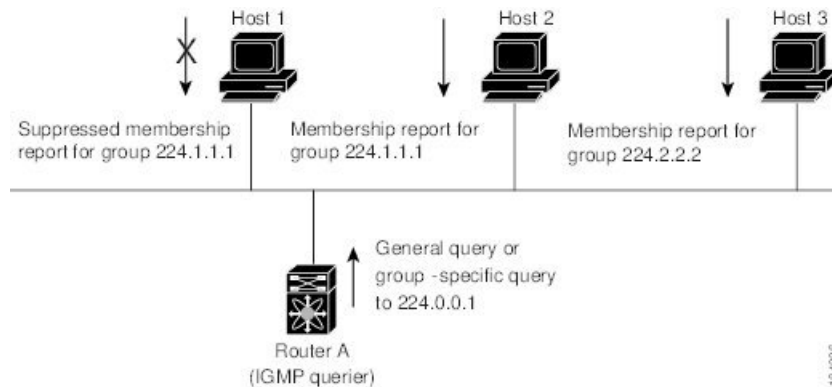
IGMPv3 の詳細については、[RFC 5790](#) を参照してください。

IGMP の基礎

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

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* の設定を参照してください。

図 8: IGMPv1 および IGMPv2 クエリ応答プロセス



下の図では、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。

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。

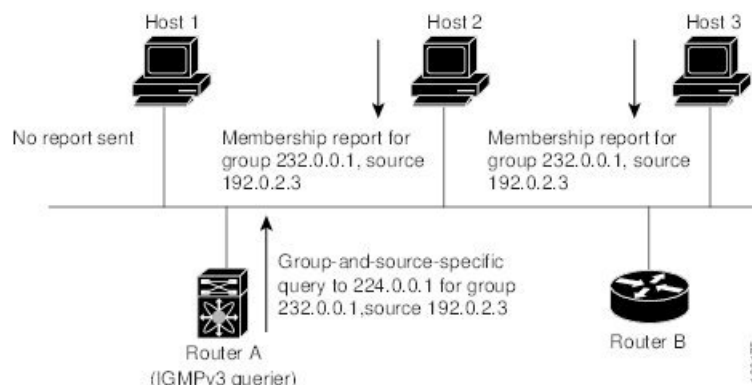
この図では、ホスト 1 からのメンバーシップレポートの送出が止められており、最初にホスト 2 からグループ 224.1.1.1 に関するメンバーシップレポートが送信されます。ホスト 1 はホスト 2 からレポートを受信します。ルータに送信する必要があるメンバーシップレポートは、グループにつき 1 つだけであるため、その他のホストではレポートの送出が止められ、ネットワークトラフィックが軽減されます。レポートの同時送信を防ぐため、各ホストではランダムな時間だけレポート送信が保留されます。クエリの最大応答時間パラメータを設定すると、ホストが応答をランダム化する間隔を制御できます。



(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。

この図のルータ 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。

図 9: IGMPv3 グループ/ソース固有のクエリ



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

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



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

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

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

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

IGMP の前提条件

IGMP の前提条件は、次のとおりです。

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

IGMP 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。

- Cisco NX-OS リリース 10.2(1q)F 以降、IGMP ホスト プロキシは Cisco Nexus N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。
- IGMP ホスト SG プロキシは、vPC ではサポートされていません。
- IGMPv3（RFC 5790）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。
- Cisco Nexus 9200 シリーズ スイッチでは、IGMP または送信元トラフィックが同じ IP アドレスから発信されている場合、S、G ルートは期限切れになりません。
- IGMP は、Nexus 9300-FX プラットフォーム スイッチでサポートされています。
- **igmp static-oif** でのルート マップの設定は、255 の範囲に制限されています。ルート マップが /8 や /4 などの /24 より大きい範囲で設定されている場合、次のログが表示されます。

```
2020 May 13 10:10:58 LO5S-NSWDDNGEF01B %IGMP-3-GROUP_RANGE_IGNORE: igmp [29534] Too many Groups in Group Range 224.4.1.0 - 224.4.13.255
2020 May 13 12:26:13 LO5S-NSWDDNGEF01B %IGMP-3-GROUP_RANGE_IGNORE: igmp [29534] Too many Groups in Group Range 224.4.1.0 - 224.4.13.255
2020 May 13 12:47:01 LO5S-NSWDDNGEF01B %IGMP-3-GROUP_RANGE_IGNORE: igmp [29534] Too many Groups in Group Range 224.4.0.64 - 224.4.3.64
```

この制限を回避するには、必要な範囲を複数の 255 以下の範囲に分割し、範囲ごとに複数のルート マップ シーケンスを使用します。

- デフォルト以外の IGMP 関連タイマーの設定は、L3 物理インターフェイスおよび SVI で行うことができます。またはクエリア IP が VLAN 構成モードで設定されている場合は VLAN 構成モードで行うことができます。その VLAN に PIM 対応の SVI がある場合、VLAN 構成モードでクエリア IP を構成することはお勧めしません。

クエリの最大応答時間（query-max-response-time）と IGMP クエリ間隔（query-interval）が L3 物理インターフェイスまたは SVI、IGMP クエリアで変更されると、タイムアウトはクエリ間隔の 2 倍に MRT を加えた値に自動的に調整されます。さらに変更するには、L3 物理インターフェイスに対して **ip igmp querier-timeout** コマンドを使用します。

ただし、SVI の場合、予想されるシェルの現在のクエリアが使用できなくなったときにクエリアの選択が行われるようにするには、VLAN 構成モードで、**show ip igmp interface vlan X** コマンドの出力に表示された値を、**ip igmp snooping querier-timeout** コマンドによって設定する必要があります。

L3 物理インターフェイスの場合は、**show ip igmp interface <intf>** コマンドを使用します。SVI の場合は、**show ip igmp snooping querier <VLAN>** コマンドを使用して、IGMP スヌーピングクエリアに関する情報を表示します。両方の構成コマンドは、正しい構成のための同じクエリア タイムアウトを表示するはずですが、

PIM hello 間隔は、PIM ネイバーがピアの可用性を決定する速さを決定します。使用できない PIM ネイバーがたまたま IGMP クエリアでもあった場合、新しいクエリアの選択が、ネイバーの期限切れと同時に発生します（90 秒：30 秒の PIM hello 間隔の 3 倍）。同時に、L2 スヌーピングクエリア タイマーは、新しいクエリア選択がいつ行われるかを指示します（デフォルトではクエリ間隔の 2 倍に MRT を加えた値）。

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
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

パラメータ	デフォルト
リンク ローカル マルチキャスト グループのレポート	無効
ルータ アラートの実施	無効
即時離脱	無効化

IGMP パラメータの設定

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



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

IGMP インターフェイスパラメータの設定

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

表 3: IGMP インターフェイスパラメータ

パラメータ	説明
IGMP のバージョン	インターフェイスでイネーブルにする IGMP のバージョン。有効な IGMP バージョンは 2 または 3 です。デフォルトは 2 です。
スタティック マルチキャスト グループ	インターフェイスに静的にバインドされるマルチキャスト グループ。(*, G) というステートでインターフェイスの加入先グループを設定するか、グループに加入する送信元 IP を、(S, G) というステートで指定します。match ip multicast コマンドで、使用するグループプレフィックス、グループ範囲、および送信元プレフィックスを示すルートマップ ポリシー名を指定できます。 (注) (S, G) ステートで設定しても、送信元ツリーが構築されるのは IGMPv3 がイネーブルな場合だけです。 ネットワーク上の全マルチキャスト対応ルータを含むマルチキャストグループを設定すると、このグループに ping 要求を送信することで、すべてのルータから応答を受け取ることができます。SSM 変換の詳細については、IGMP SSM 変換の設定を参照してください。

パラメータ	説明
発信インターフェイス (OIF) 上のスタティック マルチキャスト グループ	発信インターフェイスに静的にバインドされるマルチキャスト グループ。(*, G) というステートで発信インターフェイスの加入先グループを設定するか、グループに加入する送信元 IP を、(S, G) というステートで指定します。 match ip multicast コマンドで、使用するグループプレフィックス、グループ範囲、および送信元プレフィックスを示すルートマップ ポリシー名を指定できます。 (注) (S, G) ステートで設定しても、送信元ツリーが構築されるのは IGMPv3 がイネーブルな場合だけです。SSM 変換の詳細については、IGMP SSM 変換の設定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。
クエリーの最大応答時間	IGMP クエリーでアドバタイズされる最大応答時間。大きな値を設定すると、ホストの応答時間が延長されるため、ネットワークの IGMP メッセージを調整できます。この値は、クエリーインターバルよりも短く設定する必要があります。有効範囲は 1 ～ 25 秒です。デフォルトは 10 秒です。
クエリー インターバル	IGMP ホストクエリーメッセージの送信頻度。大きな値を設定すると、ソフトウェアによる IGMP クエリーの送信頻度が低くなるため、ネットワーク上の IGMP メッセージ数を調整できます。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 125 秒です。

パラメータ	説明
最終メンバーのクエリー応答インターバル	サブネット上の既知のアクティブ ホストから最後にホスト Leave メッセージを受信したあと、ソフトウェアが IGMP クエリーへの応答を送信するインターバル。このインターバル中に応答を受信されない場合、グループ ステートは解除されます。この値を使用すると、サブネット上でソフトウェアがトラフィックの送信を停止するタイミングを調整できます。この値を小さく設定すると、グループの最終メンバーまたは送信元が脱退したことを、より短時間で検出できます。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。
最終メンバーのクエリー回数	サブネット上の既知のアクティブ ホストから最後にホスト Leave メッセージを受信したあと、最終メンバーのクエリー応答インターバル中に、ソフトウェアが IGMP クエリーを送信する回数。有効範囲は 1 ～ 5 です。デフォルトは 2 です。 この値を 1 に設定すると、いずれかの方向でパケットが検出されなくなると、クエリー対象のグループまたはチャネルのマルチキャスト ステートが解除されます。次のクエリー インターバルが開始されるまでは、グループを再度関連付けることができます。
グループメンバーシップタイムアウト	ルータによって、ネットワーク上にグループのメンバーまたは送信元が存在しないと見なされるまでのグループ メンバーシップ インターバル。有効範囲は 3 ～ 65,535 秒です。デフォルト値は 260 秒です。
リンク ローカルマルチキャスト グループのレポート	224.0.0.0/24 内のグループにレポートを送信できるようにするためのオプション。リンク ローカル アドレスは、ローカル ネットワーク プロトコルだけで使用されます。非リンク ローカルグループには、常にレポートが送信されます。デフォルトではディセーブルになっています。
レポート ポリシー	ルートマップ ポリシーに基づく、IGMP レポートのアクセス ポリシー。 1
アクセス グループ	インターフェイスが接続されたサブネット上のホストについて、加入可能なマルチキャスト グループを制御するためのルートマップ ポリシーを設定するオプション。 (注) match ip multicast group コマンドだけがこのルートマップ ポリシーでサポートされます。ACL を照合するための match ip address コマンドはサポートされていません。

パラメータ	説明
即時離脱	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。

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

手順の概要

1. **configure terminal**
2. **interface interface**
3. **ip igmp version value**
4. **ip igmp join-group {group [source source] | route-map policy-name}**
5. **ip igmp static-oif {group [source source] | route-map policy-name}**
6. **ip igmp startup-query-interval seconds**
7. **ip igmp startup-query-count count**
8. **ip igmp robustness-variable value**
9. **ip igmp querier-timeout seconds**
10. **ip igmp query-timeout seconds**
11. **ip igmp query-max-response-time seconds**
12. **ip igmp query-interval interval**
13. **ip igmp last-member-query-response-time seconds**
14. **ip igmp last-member-query-count count**
15. **ip igmp group-timeout seconds**
16. **ip igmp report-link-local-groups**
17. **ip igmp report-policy** ポリシー
18. **ip igmp access-group** ポリシー
19. **ip igmp immediate-leave**
20. (任意) **show ip igmp interface [interface] [vrf vrf-name | all] [brief]**
21. (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 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します
ステップ 2	interface interface 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	インターフェイス設定モードを開始します。 (注) ステップ 3 でリストされているコマンドを使用して、IGMP インターフェイス パラメータを設定します。
ステップ 3	ip igmp version value 例 : <pre>switch(config-if)# ip igmp version 3</pre>	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 4	ip igmp join-group {group [source source] route-map policy-name} 例 : <pre>switch(config-if)# ip igmp join-group 230.0.0.0</pre>	指定したグループまたはチャンネルに参加するようにデバイス上のインターフェイスを設定します。デバイスは CPU 消費用のマルチキャストパケットのみを受け入れます。 注意 このコマンドを使用して生成されたトラフィックは、デバイス CPU で処理可能である必要があります。CPU の負荷制約のため、このコマンドを使用することは（特に形式を問わずスケーリングで使用する場合は）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 5	ip igmp static-oif {group [source source] route-map policy-name} 例 : <pre>switch(config-if)# ip igmp static-oif 230.0.0.0</pre>	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)

	コマンドまたはアクション	目的
		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 6	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 7	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 8	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 9	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 10	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。
ステップ 11	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 12	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 13	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。

	コマンドまたはアクション	目的
ステップ 14	ip igmp last-member-query-count count 例 : <pre>switch(config-if)# ip igmp last-member-query-count 3</pre>	ホストの Leave メッセージを受信してから、IGMP クエリ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 15	ip igmp group-timeout seconds 例 : <pre>switch(config-if)# ip igmp group-timeout 300</pre>	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 16	ip igmp report-link-local-groups 例 : <pre>switch(config-if)# ip igmp report-link-local-groups</pre>	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 17	ip igmp report-policy ポリシー 例 : <pre>switch(config-if)# ip igmp report-policy my_report_policy</pre>	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 18	ip igmp access-group ポリシー 例 : <pre>switch(config-if)# ip igmp access-group my_access_policy</pre>	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。
ステップ 19	ip igmp immediate-leave 例 : <pre>switch(config-if)# ip igmp immediate-leave</pre>	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。

	コマンドまたはアクション	目的
ステップ 20	(任意) show ip igmp interface [<i>interface</i>] [vrf <i>vrf-name</i> all] [brief] 例 : <pre>switch(config)# show ip igmp interface</pre>	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 21	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

IGMP SSM 変換の設定

SSM 変換を設定すると、IGMPv1 または IGMPv2 によるメンバーシップ レポートを受信したルータで、SSM がサポートされるようになります。メンバーシップ レポートでグループおよび送信元アドレスを指定する機能を備えているのは、IGMPv3 だけです。グループプレフィックスのデフォルト範囲は、232.0.0.0/8 です。

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

次の表に、SSM 変換の例を示します。

表 4: SSM 変換の例

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

次の表に、IGMP メンバーシップ レポートに SSM 変換を適用した場合に、IGMP プロセスによって構築される 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)

手順の概要

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

手順の詳細

手順

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

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. **[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 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	[no] ip igmp enforce-router-alert 例 : <pre>switch(config)# ip igmp enforce-router-alert</pre>	IGMPv2 パケットと IGMPv3 パケットに対するルータアラートの適用オプションチェックをイネーブルまたはディスエーブルにします。デフォルトでは、ルータアラートの適用オプションチェックはイネーブルです。
ステップ 3	(任意) show running-configuration igmp 例 : <pre>switch(config)# show running-configuration igmp</pre>	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 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

IGMP ホスト プロキシの設定

ここでは、次の内容について説明します。

IGMP ホスト プロキシの概要

IGMP ホスト プロキシサポートは、ポートチャネル (L3) アップリンクを備えた Cisco Nexus 9300 EX/FX/FX2/FX3/GX/GX2 スイッチのアンダーレイ マルチキャストに提供されます。この機能は、Cisco NX-OS Release 9.3(4) で導入されました。IGMP ホスト プロキシ機能は、PIM 対応のマルチキャスト ネットワーク ドメインを、PIM を認識しないドメインに接続するのに役立ちます。この機能は、インターフェイスをプロキシ インターフェイスとして設定し、内部 PIM ネットワークで受信した PIM の加入/プルーニングを、IGMP の加入/脱退に置き換えます。

IGMP の加入処理

ホストがマルチキャストグループに加入するとき、ホストは、加入するマルチキャストグループに1つ以上の送信要求されていないメンバーシップレポートを送信します。さらに、IGMP ジョインがデフォルトでIGMP クエリの受信時に送信されます。非要求モードは、レポートを定期的に送信するように構成できます。IGMPv2 レポートのみがアップストリームに送信されます。

IGMP の脱退処理

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

IGMP ホスト プロキシの設定方法

IGMP ホスト プロキシを構成するには、次の手順を実行します。

表 6: IGMP ホスト プロキシの設定

ステップ	コマンド	目的
ステップ 1	configure terminal 例: switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	interface interface-name 例 : switch(config)# interface port-channel 1	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 :	no shutdown 例: switch(config-if)# no shutdown	インターフェイスを no shutdown モードに設定します。
ステップ 4 :	ip address ip address 例: switch(config-if)# ip address 10.1.1.1	IP アドレスを設定します。

ステップ	コマンド	目的
ステップ 5	[no] ip igmp host-proxy [unsolicited time route-map route-map-name [unsolicited time] prefix-list prefix-list-name [unsolicited time]] 例: <pre>switch(config-if)# ip igmp host-proxy unsolicited 6</pre>	ルートマップの IGMP ホスト プロキシを設定します。
ステップ 7	show ip igmp groups 例: <pre>switch(config)# show ip igmp groups</pre>	IGMPv2 ホスト プロキシ グループだけを表示します (IGMPv3 は表示しません)。
ステップ 8	show ip igmp interface-name interface-number 例: <pre>switch(config)# show ip igmp port-channel 1</pre>	VRF の IGMP インターフェイスを表示します。
ステップ 9	show ip igmp local-groups interface-name interface-number 例: <pre>switch(config)# show ip igmp local-groups port-channel 1</pre>	VRF のための、IGMP ローカル ジョイン グループ メンバーシップを表示します。
ステップ 10	show ip pim host-proxy 例 : <pre>switch(config)# show ip pim host-proxy</pre>	PIM ホスト プロキシ インターフェイスを表示します。

IGMP SG プロキシの構成

ここでは、次の内容について説明します。

IGMP SG プロキシ

NX-OS リリース 10.2(2)F から、IGMP SG プロキシ機能がメディア ファブリックに導入されました。メディア ファブリックは、コントローラがファブリック内のルートをプログラムするパッシブ モードを使用します。このようなファブリックでは、PIM はパッシブ モードで動作します。パッシブファブリックが外部リンクを介してファブリックの外部からマルチキャストソースをプルした場合、IGMPv3 プロキシ レポートが、パッシブ ファブリック マルチキャスト ルートによって選択された RPF () インターフェイスに送信されます。このようなルートの RPF は、外部リンク経由です。これらの外部インターフェイスは、IGMP プロキシとして動作

するように構成されます。IGMP SG ホストプロキシ機能を機能させるには、RPF インターフェイスを新しいノブでプロビジョニングする必要があります。

IGMP SG プロキシの構成

IGMP SG プロキシを構成するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface interface-name**
3. **no shutdown**
4. **ip address ip address**
5. **[no] ip igmp host-proxy sg-proxy [unsolicited time | route-map route-map-name [unsolicited time] | prefix-list prefix-list-name [unsolicited time]]**

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-name 例 : switch(config)# interface port-channel 1	インターフェイス設定モードを開始します。
ステップ 3	no shutdown 例 : switch(config-if)# no shutdown	インターフェイスを no shutdown モードに設定します。
ステップ 4	ip address ip address 例 : switch(config-if)# ip address 10.1.1.1	IP アドレスを設定します。
ステップ 5	[no] ip igmp host-proxy sg-proxy [unsolicited time route-map route-map-name [unsolicited time] prefix-list prefix-list-name [unsolicited time]] 例 : switch(config-if)# ip igmp host-proxy sg-proxy unsolicited 4	IGMP SG プロキシを設定します。

IGMP プロセスの再起動

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

手順の概要

1. **restart igmp**
2. **configure terminal**
3. **ip igmp flush-routes**
4. (任意) **show running-configuration igmp**
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 igmp 例 : switch# restart igmp	IGMP プロセスを再起動します。
ステップ 2	configure terminal 例 : switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip igmp flush-routes 例 : switch(config)# ip igmp flush-routes	IGMP プロセスの再起動時に、ルートを削除します。デフォルトでは、ルートはフラッシュされません。
ステップ 4	(任意) show running-configuration igmp 例 : switch(config)# show running-configuration igmp	実行コンフィギュレーション情報を表示します。
ステップ 5	(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。

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	説明
show ip igmp interface [<i>interface</i>] [vrf <i>vrf-name</i> all] [brief]	すべてのインターフェイスまたは選択されたインターフェイス、デフォルト VRF、選択された VRF、またはすべての VRF について、IGMP 情報を表示します。IGMP が vPC モードの場合、vPC 統計情報を表示するには、このコマンドを使用します。
show ip igmp groups [{ <i>source</i> [<i>group</i>]}] { group [<i>source</i>]}] [<i>interface</i>] [summary] [vrf <i>vrf-name</i> 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 [{ <i>source</i> [<i>group</i>]}] { group [<i>source</i>]}] [<i>interface</i>] [summary] [vrf <i>vrf-name</i> 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。

```
configure terminal
ip igmp ssm-translate 232.0.0.0/8 10.1.1.1
interface ethernet 2/1
ip igmp version 3
ip igmp join-group 230.0.0.0
ip igmp startup-query-interval 25
ip igmp startup-query-count 3
ip igmp robustness-variable 3
ip igmp querier-timeout 300
ip igmp query-timeout 300
ip igmp query-max-response-time 15
ip igmp query-interval 100
```

```

ip igmp last-member-query-response-time 3
ip igmp last-member-query-count 3
ip igmp group-timeout 300
ip igmp report-link-local-groups
ip igmp report-policy my_report_policy
ip igmp access-group my_access_policy

```

次に、IGMP SG プロキシを設定した場合の出力例を示します。

```

switch# show ip igmp internal host-proxy sg-cache
IGMP Total Host proxy routes: 2
IGMP Host proxy routes for context default count: 2
Group Address      Source Address      RPF iif
231.1.1.1          80.80.80.1          Eth1/17
232.9.9.9          80.80.80.1          Eth1/18

switch# show ip pim host-proxy
PIM host proxy interfaces
=====
Type: SG - Host SG Proxy, H - Host Proxy
Vlan500 (SG)        loopback1 (SG)      loopback3 (SG)      loopback4 (SG)
      loopback10 (SG) Ethernet1/17 (SG)   Ethernet1/18 (SG) Ethernet1/19 (SG)
Ethernet1/20 (SG)

```

```

switch# show ip igmp local-groups
IGMP Locally Joined Group Membership for VRF "default"
Group Address      Source Address      Type      Interface      Last Reported
231.1.1.1          80.80.80.1          Local     Lo0             00:01:53
232.9.9.9          80.80.80.1          Local     Lo0             00:01:53
231.1.1.1          80.80.80.1          H-proxy   Eth1/17         00:01:14
232.9.9.9          80.80.80.1          H-proxy   Eth1/18         00:01:24
231.1.1.1          80.80.80.1          H-proxy   Eth1/19         03:10:30
232.9.9.9          80.80.80.1          H-proxy   Eth1/20         03:10:27

```



第 4 章

MLD の設定

この章では、IPv6 ネットワーク用に Cisco NX-OS デバイスでマルチキャスト リスナー検出 (MLD) を設定する方法を説明します。

- [MLD について \(41 ページ\)](#)
- [MLD の前提条件 \(45 ページ\)](#)
- [MLD の注意事項および制限事項 \(45 ページ\)](#)
- [MLD のデフォルト設定 \(46 ページ\)](#)
- [MLD スヌーピングの設定 \(47 ページ\)](#)
- [MLD パラメータの設定 \(50 ページ\)](#)
- [MLD の設定の確認 \(58 ページ\)](#)
- [MLD スヌーピングの設定の確認 \(59 ページ\)](#)
- [MLD の設定例 \(60 ページ\)](#)

MLD について

MLD 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 IPv6 プロトコルです。ソフトウェアは、MLD 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ン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。MLD パケットを受信したデバイスは、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ンネルに関する受信データをマルチキャスト送信します。

MLDv1 は IGMPv2 から、MLDv2 は IGMPv3 から派生したプロトコルです。IGMP は IP Protocol 2 メッセージタイプを使用しますが、MLD は ICMPv6 メッセージのサブセットである IP Protocol 58 メッセージタイプを使用します。

MLD プロセスはデバイス上で自動的に起動されます。インターフェイスでは MLD を手動でイネーブルにできません。MDL 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。

- PIM6 のイネーブル化
- ローカル マルチキャスト グループの静的なバインディング
- リンクローカル グループ レポートのイネーブル化

MLD のバージョン

デバイスは MLDv1 および MLDv2 をサポートしています。MLDv2 は MLDv1 リスナー レポートをサポートしています。

デフォルトでは、ソフトウェアが MLD プロセスを起動する際に、MLDv2 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 MLDv1 をイネーブルにできます。

MLDv2 には、次に示す MLDv1 からの重要な変更点があります。

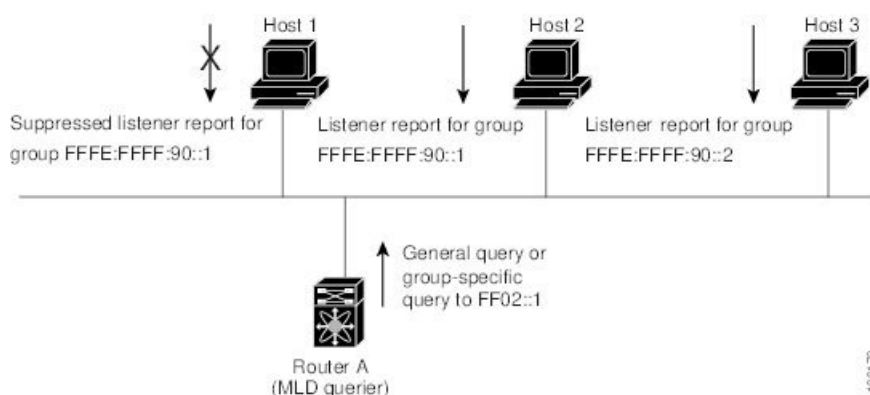
- 次の機能を提供し、各受信者から送信元までの最短パス ツリーを構築可能な Source-Specific Multicast (SSM) をサポートします。
 - グループおよび送信元を両方指定できるホスト メッセージ
 - MLDv1 ではグループについてのみ保持できたマルチキャスト ステートを、グループおよび送信元について保持可能
- ホストによるレポート抑制が行われなくなり、MLD クエリー メッセージを受信するたびに MLD リスナー レポートが送信されるようになりました。

MLDv1 の詳細については、[RFC 2710](#) を参照してください。MLDv2 の詳細については、[RFC 3810](#) を参照してください。

MLD の基礎

次の図に、ルータが MLD 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。

図 10: MLD クエリー応答プロセス



ホスト 1、2、および 3 は要求外の MLD リスナー レポート メッセージを送信して、グループまたはチャン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。ルータ A（サブネットの代表 MLD クエリア）は、リンクスコープの全ノードを対象として、マルチキャスト アドレス FF02::1 に定期的に共通のクエリ メッセージを送信し、マルチキャスト グループに対する各ホストの受信要求を検出します。グループ固有のクエリーは、特定のグループの情報を要求するホストを検出する場合に使用されます。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。これは、ルータが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するかどうかを判断するための時間です。

ホスト 1 からのリスナー レポートの送出は止められており、最初にホスト 2 からグループ FFFE:FFFF:90::1 に関するリスナー 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リスナー 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。



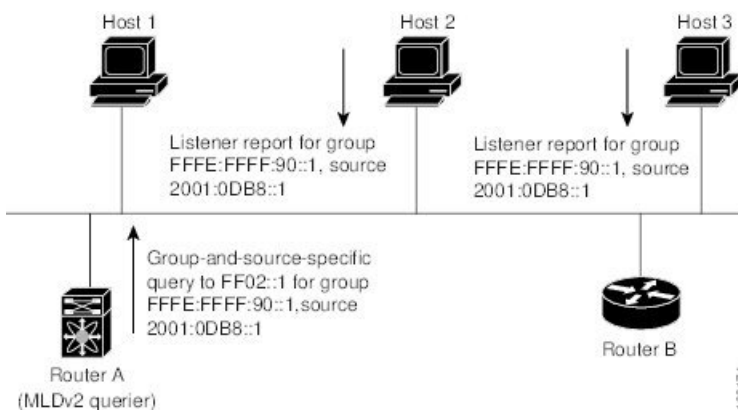
- (注) MLDv1 メンバーシップ レポートが抑制されるのは、同じポートに複数のホストが接続されている場合だけです。

ルータ A は、MLDv2 の group-and-source-specific 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リスナー レポートを送信して、そのクエリに応答します。この MLDv2 機能では、SSM がサポートされます。



- (注) MLDv2 では、すべてのホストがクエリに応答します。

図 11 : MLDv2 グループ/ソース固有のクエリー



IP アドレスが最下位のルータが、サブネットの MLD 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、非クエリアとして動作し、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。

代表クエリアから送信されるメッセージの存続可能時間（TTL）値は 1 です。つまり、サブネット上の直接接続されたルータからは、メッセージは転送されません。また、MLD の起動中に送信されるクエリーメッセージの頻度および回数を個別に設定することもできます。起動時のクエリーインターバルを短く設定することで、グループステートの確立時間を最小限に抑えることができます。通常は不要ですが、起動後のクエリーインターバルをチューニングすることで、ホストグループメンバーシップへの応答性と、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、ネットワークの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。

グループを脱退するマルチキャストホストは、MLDv1 に対して脱退を知らせるメッセージを送信するか、または対象のグループを除外したリスナーレポートを、リンクスコープ内の全ルータを含むマルチキャストアドレス FF02::2 に送信する必要があります。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、MLD クエリーメッセージが送信されます。これにより、最終メンバーのクエリー応答インターバルと呼ばれる、ユーザが設定可能なタイマーが起動されます。タイマーが切れる前にレポートが受信されない場合は、ソフトウェアによってグループステートが解除されます。ルータはグループステートが解除されないかぎり、このグループにマルチキャストトラフィックを送信し続けます。

輻輳ネットワークでのパケット損失を緩和するには、ロバストネス値を設定します。ロバストネス値は、MLD 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。

FF02::0/16 内に含まれるリンクローカルアドレスには、Internet Assigned Numbers Authority (IANA) が定義したリンクスコープが設定されています。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。MLD 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リスナーレポートが送信されます。ただし、リンクローカルアドレスにレポートが送信されるよう、ソフトウェアの設定を変更できます。

MLD スヌーピング

マルチキャストリスナー検出（MLD）スヌーピングにより、ホストとルータ間で IPv6 マルチキャストトラフィックを効率的に配信できます。これは、MLD クエリまたはレポートを送受信したポートのサブセットにブリッジドメイン内の IPv6 マルチキャストトラフィックを制限するレイヤ 2 機能です。このように、MLD スヌーピングは、マルチキャストトラフィックの受信に関心を示しているノードがないネットワークのセグメントでは帯域幅を節約できるという利点があります。これにより、ブリッジドメインでフラグディングが生じることがなく、帯域幅の使用量が削減され、ホストとルータで不要なパケット処理を節約できます。

MLD スヌーピング機能は、インターネットグループ管理プロトコル（IGMP）スヌーピングと似ていますが、MLD スヌーピングの機能は IPv6 マルチキャストトラフィックをスヌーピングすることであり、MLDv1（RFC 2710）および MLDv2（RFC 3810）コントロールプレーンパケットで動作する点が異なります。MLD はインターネット制御メッセージプロトコルバージョン 6（ICMPv6）のサブプロトコルです。MLD メッセージは ICMPv6 メッセージのサブセッ

トで、IPv6 パケット内で先頭の Next Header 値 58 により識別されます。MLDv1 のメッセージタイプには、リスナー クエリ、マルチキャスト アドレス固有 (MAS) クエリ、リスナー レポート、完了メッセージが含まれます。MLDv2 は、追加のクエリ タイプであるマルチキャスト アドレスおよびソース固有 (MASS) クエリを除き、MLDv1 と相互運用できるように設計されています。MLD で使用可能なプロトコル レベル タイマーは、IGMP で使用可能なものと同様です。

MLD スヌーピングがディセーブルの場合、すべてのマルチキャスト トラフィックは、関係があるかどうかに関係なく、すべてのポートにフラッドイングされます。MLD スヌーピングがイネーブルの場合、ファブリックは MLD インタレストに基づいて IPv6 マルチキャスト トラフィックを転送します。不明な IPv6 マルチキャスト トラフィックは、ブリッジ ドメインの IPv6 L3 不明マルチキャスト フラッドイング設定に基づいてフラッドイングされます。

フラッドイング モードは、不明な IPv6 マルチキャスト パケットを転送するために使用されます。フラッドイング モードでは、ブリッジ ドメイン内のすべてのエンドポイント グループ (EPG) およびすべてのポートがフラッドイング パケットを受信します。

MLD の前提条件

MLD の前提条件は、次のとおりです。

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

MLD の注意事項および制限事項

MLD には、次の注意事項と制限事項があります。

- Cisco Nexus 9200、9300、および 9300-EX シリーズ スイッチは MLD をサポートしていません。
- Cisco NX-OS リリース 10.2(1q)F 以降、MLD スヌーピングは Cisco N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。
- Cisco Nexus 3232C および 3264Q スイッチは、MLD をサポートしていません。
- MLDv2 (RFC 3810) に従う送信元のリストの除外またはブロックはサポートされていません。
- インターフェイスに静的にバインドされているマルチキャスト グループを拒否するようにルートマップを変更する場合。その後の MLD レポートはローカル グループによって拒否され、グループはエージングを開始します。グループへの MLD 脱退メッセージは、影響を与えることなく許可されます。これは既知の予期された動作です。

- MLD スヌーピングは、vPC の有無に関わりなく、新世代 ToR スイッチでのみサポートされます。これらは、スイッチ名の最後に「EX」、「FX」または「FX2」が付くスイッチモデルです。また、「EX」および「FX」ラインカードを搭載した EoR スイッチにも当てはまります。
- Cisco NX-OS リリース 9.3(5) 以降、IPv6 MLD スヌーピングは Cisco Nexus 9500 プラットフォーム スイッチでサポートされます。
- MLD スヌーピングは、EOR スイッチの N9K-X9636PQ、N9K-X9408PC-CFP2、N9K-X9432PQ、N9K-X9464PX、N9K-X9464TX、N9K-X9464TX2 の T2 ラインカードでもサポートされています。
- MLD スヌーピングは、T2、T2P、T3、TH、TH2、および T2 EOR を備えたすべての Cisco Nexus 9000 および Cisco Nexus 3000 プラットフォームでサポートされています。Cisco Nexus 9000 T2 TOR ではサポートされていません。N9K-C9372PX、N9K-C9372PX-E、N9K-C9372TX、N9K-C9372TX-E、N9K-C9332PQ、N9K-C93128TX、N9K-C9396PX、N9K-C9396TX が該当します。
- MLD スヌーピングは、FEX ポートおよびネットワーク負荷分散 (NLB) ではサポートされていません。VLAN が MAC モードの場合もサポートされません。
- 以下のコマンドが設定されている場合、MLD スヌーピング設定はグローバル レベルで拒否されます。
 - ip pim cpu-punt dr-only
 - ipv6 pim cpu-punt dr-only
 - ip pim non-dr flood
 - ipv6 pim non-dr flood
- Cisco NX-OS リリース 9.3(5) 以降、MLD スヌーピングは Cisco Nexus 9300-FX3 プラットフォーム スイッチでサポートされます。

MLD のデフォルト設定

表 7: MLD パラメータのデフォルト設定

パラメータ	デフォルト
MLD 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

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

MLD スヌーピングの設定

MLD スヌーピングは、グローバル コンフィギュレーション モードおよび VLAN コンフィギュレーション モードでイネーブルおよびディセーブルにできます。スヌーピングは、グローバル コンフィギュレーション モードではデフォルトで無効になっており、VLAN ごとに有効になっています。スヌーピングは、VLAN 上でスヌーピングが有効になっていて、グローバル コンフィギュレーション モードになっている場合にのみ、VLAN 上で動作します。

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	ipv6 mld snooping 例 : switch(config)# ipv6 mld snooping	MLD スヌープ ポリシーの管理状態を有効にします。
ステップ 3	system mld snooping 例 :	これは、Cisco Nexus 9000 シリーズプラットフォームで MLD スヌーピングを有効にするための追加要

	コマンドまたはアクション	目的
	<code>switch(config)# system mld snooping</code>	件です。Cisco Nexus 9000 シリーズプラットフォームでスヌーピングを完全に有効にするには、ステップ 2 とステップ 3 の両方が必要です。 このコマンドを設定した後、スイッチをリロードしてください。
ステップ 4	ipv6 mld snooping vxlan 例： <code>switch(config)# ipv6 mld snooping vxlan</code>	VXLAN VLAN で MLD スヌーピングを有効にします。
ステップ 5	hardware access-list tcam region ing-sup tcam-size 例： <code>switch(config)# hardware access-list tcam region ing-sup 768</code>	TCAM リージョンの ing-sup を 768 以上に設定します。 (注) 手順 3 と 4 を実行すると、設定を保存してシステムを再起動して ACL をカービングし、v6 および v4 ルーティングの異なるハードウェアプログラミングを有効にするように求められます。
ステップ 6	ipv6 mld snooping explicit-tracking 例： <code>switch(config)# ipv6 mld snooping explicit-tracking</code>	VLAN ごとに明示的のホスト トラッキングを有効または無効にします。このコマンドは、両方の MLD バージョン (v1 および v2) でデフォルトで有効になっています。
ステップ 7	ipv6 mld snooping report-suppression 例： <code>switch(config)# ipv6 mld snooping report-suppression</code>	レポート抑制を有効または無効にします。ホストから受信したすべての MLDv1 メンバーシップレポートは、すべてのマルチキャスト ルータ ポートに転送されます。レポート抑制が無効になっている場合、すべての MLD メンバーシップレポートがそのまま ルータに転送されるため、プロキシ レポートは実行されません。このコマンドは、デフォルトでイネーブルになっています。
ステップ 8	ipv6 mld snooping v2-report-suppression 例： <code>switch(config)# ipv6 mld snooping v2-report-suppression</code>	MLDv2 レポート抑制をイネーブルにします。MLDv2 レポート抑制は、デフォルトではディセーブルにされています。
ステップ 9	ipv6 mld snooping link-local-groups-suppression 例： <code>switch(config)# ipv6 mld snooping link-local-groups-suppression</code>	link-local-groups-suppression を設定します。

	コマンドまたはアクション	目的
ステップ 10	ipv6 mld snooping event-history vlan size {disabled large medium small} 例 : <pre>switch(config)# ipv6 mld snooping event-history vlan size medium</pre>	VLAN のイベント履歴バッファを設定します。デフォルト値は中 (medium) です。
ステップ 11	ipv6 mld snooping event-history vlan-events {disabled large medium small} 例 : <pre>switch(config)# ipv6 mld snooping event-history vlan-events medium</pre>	VLAN イベントのイベント履歴バッファを設定します。デフォルト値は中 (medium) です。
ステップ 12	ipv6 mld snooping event-history MLD-snoop-internal size {disabled large medium small} 例 : <pre>switch(config)# ipv6 mld snooping event-history MLD-snoop-internal size small</pre>	MLD スヌープ内部イベントのイベント履歴バッファを設定します。デフォルト値は小 (small) です。
ステップ 13	ipv6 mld snooping event-history mfdm size {disabled large medium small} 例 : <pre>switch(config)# ipv6 mld snooping event-history mfdm size small</pre>	MLD スヌープ MFDM イベントのイベント履歴バッファを設定します。デフォルト値は小 (small) です。
ステップ 14	ipv6 mld snooping event-history mfdm-sum {disabled large medium small} 例 : <pre>switch(config)# ipv6 mld snooping event-history mfdm-sum size small</pre>	MLD スヌープ MFDM イベント サマリーのイベント履歴バッファを設定します。デフォルト値は小 (small) です。
ステップ 15	ipv6 mld snooping event-history vpc size {disabled large medium small} 例 : <pre>switch(config)# ipv6 mld snooping event-history vpc size small</pre>	MLD スヌープ vPC イベントのイベント履歴バッファを設定します。デフォルト値は小 (small) です。
ステップ 16	vlan configuration vlan-id 例 : <pre>switch(config)# vlan configuration 6</pre>	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 17	[no] ipv6 mld snooping 例 : <pre>switch(config-vlan-config)# no ipv6 mld snooping</pre>	VLAN ごとに MLD スヌーピングを無効または有効にします。無効にすると、PIM6 は対応する「インターフェイス vlan」で機能なくなります。
ステップ 18	ipv6 mld snooping fast-leave 例 :	VLAN ごとに高速脱退機能をオンまたはオフにできます。これは MLDv2 ホストに適用され、1 つの

	コマンドまたはアクション	目的
	<code>switch(config-vlan-config)# ipv6 mld snooping fast-leave</code>	ホストだけがそのポートの背後で MLD を実行することがわかっているポートで使用されます。このコマンドはデフォルトでは無効になっています。これは VLAN モード コマンドです。
ステップ 19	ipv6 mld snooping mrouter interface interface-identifier 例 : <code>switch(config-vlan-config)# ipv6 mld snooping mrouter interface port-channel 1</code>	マルチキャスト ルータへの静的な接続を指定します。ルータへのインターフェイスは、コマンドを入力する VLAN 内にある必要があります。インターフェイスは管理上アップ状態、回線プロトコルでもアップ状態である必要があります。これは VLAN モード コマンドです。
ステップ 20	ipv6 mld snooping static-group group [source source] interface interface-identifier 例 : <code>switch(config-vlan-config)# ipv6 mld snooping static-group ffile::abcd interface port-channel 2</code>	特定の VLAN のレイヤ 2 ポートをマルチキャストグループのメンバーとしてスタティックに設定します。これは VLAN モード コマンドです。
ステップ 21	ipv6 mld snooping last-member-query-interval [interval] 例 : <code>switch(config-vlan-config)# ipv6 mld snooping last-member-query-interval 9</code>	特定のマルチキャスト グループにホストがまだ関係しているかどうかを判別するグループ固有のクエリを送信した後で、スイッチが待機する時間を設定します。スイッチによって送信される IGMP クエリの待機時間を設定します。デフォルトは 1 秒です。有効な範囲は、1 ～ 25 秒です。これは VLAN モード コマンドです。 MLD 高速脱退処理と MLD クエリ時間の両方を設定した場合は、高速脱退処理が優先するものと見なされます。
ステップ 22	ipv6 mld snooping querier リンクローカルアドレス 例 : <code>switch(config-vlan-config)# ipv6 mld snooping querier aaaa::abcd</code>	IPv6 MLD スヌーピングクエリア処理を有効または無効にします。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、MLD スヌーピングクエリアは、PIM および MLD を設定していない VLAN 内で MLD スヌーピングをサポートします。

MLD パラメータの設定

MLD 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、MLD プロセスの動作を変更できます。



- (注) MLD スヌーピングを設定する前に、**ipv6 mld snooping** および **system mld snooping** コマンドを使用して MLD 機能を有効にします。

MLD インターフェイス パラメータの設定

表 8: MLD インターフェイス パラメータ

パラメータ	説明
MLD のバージョン	インターフェイスでイネーブルにする MLD のバージョン。MLDv2 は MLDv1 をサポートしています。有効な MLD バージョンは 1 または 2 です。デフォルトは 2 です。
スタティック マルチキャスト グループ	インターフェイスに静的にバインドされるマルチキャスト グループ。(*, G) というステートでインターフェイスの加入先グループを設定するか、(S, G) というステートでグループに加入するソース IP を指定します。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、ソース ツリーが構築されるのは MLDv2 がイネーブルな場合だけです。 ネットワーク上の全マルチキャスト対応ルータを含むマルチキャスト グループを設定すると、このグループに ping 要求を送信することで、すべてのルータから応答を受け取ることができます。
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) というステートで出力インターフェイスの加入先グループを設定するか、(S, G) というステートでグループに加入するソース IP を指定します。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。 (S, G) ステートで設定しても、ソース ツリーが構築されるのは MLDv2 がイネーブルな場合だけです。 (注) ルート マップのグループプレフィックスには、長さ 120 以上のマスクが必要です。

パラメータ	説明
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。デフォルトは 30 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間隔で区切られる、スタートアップ時の送信クエリー数。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。
クエリーの最大応答時間	MLD クエリーでアドバタイズされる最大応答時間。大きな値を設定すると、ホストの応答時間が延長され、ネットワークの MLD メッセージのバースト性を調整できます。この値は、クエリーインターバルよりも短く設定する必要があります。有効範囲は 1 ～ 25 秒です。デフォルトは 10 秒です。
クエリー インターバル	MLD 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 MLD クエリーの送信頻度が低くなるため、ネットワーク上の MLD 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脱退メッセージを受信したあと、ソフトウェアが送信する MLD クエリーへの応答に対するクエリーインターバル。このインターバル中に応答を受信されない場合、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。

パラメータ	説明
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 MLD 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ン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ソース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	FF02::0/16 内のグループにレポートを送信できるようにするためのオプション。リンク ローカルアドレスは、ローカル ネットワーク プロトコルだけで使用されます。非リンク ローカルグループには、常にレポートが送信されます。デフォルトではディセーブルになっています。
レポート ポリシー	ルートマップ ポリシーに基づく、MLD レポートのアクセス ポリシー。
アクセス グループ	インターフェイスによりサービスを受けるサブネット上のホストが参加できるマルチキャストグループをコントロールするため、ルートマップ ポリシーを設定するオプション。 (注) match ip multicast group コマンドだけがこのルートマップ ポリシーでサポートされます。ACL を照合するための match ip address コマンドはサポートされていません。
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 MLD インターフェイスでの MLDv1 グループ メンバーシップを脱退するまでの待ち時間を最小限に抑えるオプション。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。

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

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します
ステップ 2	interface interface 例 : switch(config)# interface ethernet 2/1 switch(config-if)#	インターフェイス設定モードを開始します。 (注) ステップ 3 でリストされたコマンドを使用して、MLD インターフェイス パラメータを設定します。
ステップ 3	ipv6 mld version value 例 : switch(config-if)# ipv6 mld version 2	インターフェイスでイネーブルにする MLD のバージョン。MLDv2 は MLDv1 をサポートしています。有効な値は 1 または 2 です。デフォルトは 2 です。 このコマンドの <i>no</i> 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 4	ipv6 mld join-group {group [source source] route-map policy-name} 例 : switch(config-if)# ipv6 mld join-group FFFE::1	マルチキャスト グループをインターフェイスに静的にバインドします。グループ アドレス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) (S,G) ステートで送信元ツリーを構築できるのは、MLDv2 がイネーブルな場合だけです。 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 で処理する必要があります。
ステップ 5	ipv6 mld static-oif {group [source source] route-map policy-name} 例 : switch(config-if)# ipv6 mld static-oif FFFE::1	マルチキャスト グループを発信インターフェイスに静的にバインドし、デバイス ハードウェアで処理します。グループ アドレスのみを指定した場合は、(*,G) ステートが作成されます。送信元アドレスを指定した場合は、(S,G) ステートが作成されます。 match ip multicast コマンドで、使用する

	コマンドまたはアクション	目的
		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)ステートで送信元ツリーを構築できるのは、MLDv2 がイネーブルな場合だけです。 (注) ルート マップのエントリごとにサポートされるグループの最大数は 256 です。
ステップ 6	ipv6 mld startup-query-interval seconds 例 : <pre>switch(config-if)# ipv6 mld startup-query-interval 25</pre>	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 7	ipv6 mld startup-query-count count 例 : <pre>switch(config-if)# ipv6 mld startup-query-count 3</pre>	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 8	ipv6 mld robustness-variable value 例 : <pre>switch(config-if)# ipv6 mld robustness-variable 3</pre>	ロバストネス変数を設定します。パケット損失が発生しやすいネットワークには、より大きな値を使用します。有効値の範囲は、1 ～ 7 です。デフォルトは 2 です。
ステップ 9	ipv6 mld querier-timeout seconds 例 : <pre>switch(config-if)# ipv6 mld querier-timeout 300</pre>	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 10	ipv6 mld query-timeout seconds 例 : <pre>switch(config-if)# ipv6 mld query-timeout 300</pre>	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、ipv6 mld querier-timeout コマンドと同じです。
ステップ 11	ipv6 mld query-max-response-time seconds 例 : <pre>switch(config-if)# ipv6 mld query-max-response-time 15</pre>	MLD 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。

	コマンドまたはアクション	目的
ステップ 12	ipv6 mld query-interval interval 例 : <pre>switch(config-if)# ipv6 mld query-interval 100</pre>	MLD 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 13	ipv6 mld last-member-query-response-time seconds 例 : <pre>switch(config-if)# ipv6 mld last-member-query-response-time 3</pre>	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応答時間を設定します。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。
ステップ 14	ipv6 mld last-member-query-count count 例 : <pre>switch(config-if)# ipv6 mld last-member-query-count 3</pre>	ホストの Leave メッセージを受信してから、MLD 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 15	ipv6 mld group-timeout (秒単位) 例 : <pre>switch(config-if)# ipv6 mld group-timeout 300</pre>	MLDv2 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 16	ipv6 mld report-link-local-groups 例 : <pre>switch(config-if)# ipv6 mld report-link-local-groups</pre>	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 17	ipv6 mld report-policy ポリシー 例 : <pre>switch(config-if)# ipv6 mld report-policy my_report_policy</pre>	ルートマップ ポリシーに基づく、MLD レポートのアクセス ポリシーを設定します。
ステップ 18	ipv6 mld access-group ポリシー 例 : <pre>switch(config-if)# ipv6 mld access-group my_access_policy</pre>	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。
ステップ 19	ipv6 mld immediate-leave 例 : <pre>switch(config-if)# ipv6 mld immediate-leave</pre>	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

	コマンドまたはアクション	目的
		MLD インターフェイスで MLDv1 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 20	(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。

MLD SSM 変換の設定

SSM 変換を設定すると、MLDv1 リスナー 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。リスナー 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、MLDv2 だけです。グループプレフィックスのデフォルト範囲は、FF3x/96 です。

表 9: SSM 変換の例

グループ プレフィックス	送信元アドレス
FF30::0/16	2001:0DB8:0:ABCD::1
FF30::0/16	2001:0DB8:0:ABCD::2
FF30:30::0/24	2001:0DB8:0:ABCD::3
FF32:40::0/24	2001:0DB8:0:ABCD::4

次の表に、MLDv1 リスナー レポートに SSM 変換を適用した場合に、MLD プロセスによって構築される M6RIB ルートを示します。複数の変換を行う場合は、ルータにより、各変換内容に対して (S,G) ステートが作成されます。

表 10: SSM 変換適用後の例

MLDv1 リスナー レポート	作成される M6RIB ルート
FF32:40::40	(2001:0DB8:0:ABCD::4, FF32:40::40)
FF30:10::10	(2001:0DB8:0:ABCD::1, FF30:10::10) (2001:0DB8:0:ABCD::2, FF30:10::10)

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	ipv6 [icmp] mld ssm-translate group-prefix source-addr 例 : switch(config)# ipv6 mld ssm-translate FF30::0/16 2001:0DB8:0:ABCD::1	ルータが MLDv2 リスナー 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、MLD プロセスによる MLDv1 リスナー レポートの変換を設定します。
ステップ 3	(任意) show running-configuration ssm-translate 例 : switch(config)# show running-configuration ssm-translate	実行コンフィギュレーションの <i>ssm-translate</i> 設定行を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : switch(config)# copy running-config startup-config	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。

MLD の設定の確認

MLD 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。

show ipv6 mld 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、MLD 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 ipv6 mld local-groups	MLD ローカル グループ メンバーシップを表示します。

次に、**show ipv6 mld groups** コマンドの出力例を示します。この出力は、10 個のインターフェイスがグループ ff03:0:0:1::1 に MLD join を送信していることを示しています。そのうち 9 個のインターフェイスが MLDv1 join を送信しており、10 番目のインターフェイスがソース 2005:0:0:1::2 との MLDv2 join を送信しています。グループには 9 つのエントリがあり、10 番目のエントリがソース エントリとして追加されます。

```
switch# show ipv6 mld groups vrf vrf1
MLD Connected Group Membership for VRF "VRF1" - 52 total entries
Type: S - Static, D - Dynamic, L - Local, T - SSM Translated, H - Host Proxy
```

```

* - Cache Only
Group Address      Type Interface      Uptime    Expires    Last Reporter
ff03:0:0:1::1      D    Ethernet3/25.1      00:02:13  00:03:47   fe80::1
ff03:0:0:1::1      D    Ethernet3/25.3      00:02:13  00:04:12   fe80::2:0:0:1
ff03:0:0:1::1      D    Ethernet3/25.5      00:02:13  00:02:26   fe80::4:0:0:1
ff03:0:0:1::1      D    Ethernet3/25.4      00:02:13  00:03:31   fe80::3:0:0:1
ff03:0:0:1::1      D    Ethernet3/25.6      00:02:13  00:02:47   fe80::5:0:0:1
ff03:0:0:1::1      D    Ethernet3/25.7      00:02:13  00:03:10   fe80::6:0:0:1
ff03:0:0:1::1      D    Ethernet3/25.8      00:02:13  00:03:56   fe80::7:0:0:1
ff03:0:0:1::1      D    Ethernet3/25.9      00:02:13  00:03:28   fe80::8:0:0:1
2005:0:0:1::2      D    Ethernet3/25.10     2d15h     00:03:37   fe80::9:0:0:1

```

MLD スヌーピングの設定の確認

MLD 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入力します。

show ipv6 mld snooping [vlan vlan-id]	特定の VLAN またはすべての VLAN の MLD スヌーピング ステータスと詳細を表示します。
show ipv6 mld snooping mrouter [vlan vlan-id]	VLAN ごとのマルチキャスト ルーター ポートを表示します。
show ipv6 mld snooping querier [vlan vlan-id]	MLD スヌーピングが有効になっている VLAN の MLD クエリアの詳細を表示します。
show ipv6 mld snooping explicit-tracking vlan vlan-id	MLD スヌーピングの明示的な追跡情報を表示します。
show ipv6 mld snooping statistics global	グローバル MLD スヌーピング 統計を表示します。
show ipv6 mld snooping groups [vlan vlan-id] [detail]	グループ、そのグループ（ホスト タイプ）に対して受信されたレポート タイプ、およびレポートが受信されたポートのリストを表示します。ポートのリストには、マルチキャスト ルーター ポートは含まれていません。これは、レポートが受信されたポートのリストであり、グループに設定された転送ポートすべてのリストではありません。詳細出力以外の /* エントリは、ルーター ポートを示します。

MLD の設定例

次に、MLD の設定例を示します。

```
configure terminal
ipv6 mld ssm-translate FF30::0/16 2001:0DB8:0:ABCD::1
interface ethernet 2/1
  ipv6 mld version 2
  ipv6 mld join-group FFFE::1
  ipv6 mld startup-query-interval 25
  ipv6 mld startup-query-count 3
  ipv6 mld robustness-variable 3
  ipv6 mld querier-timeout 300
  ipv6 mld query-timeout 300
  ipv6 mld query-max-response-time 15
  ipv6 mld query-interval 100
  ipv6 mld last-member-query-response-time 3
  ipv6 mld last-member-query-count 3
  ipv6 mld group-timeout 300
  ipv6 mld report-link-local-groups
  ipv6 mld report-policy my_report_policy
  ipv6 mld access-group my_access_policy
```



第 5 章

PIM および PIM6 の設定

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

- [PIM および PIM6 について \(61 ページ\)](#)
- [PIM および PIM6 の前提条件 \(74 ページ\)](#)
- [PIM および PIM6 に関する注意事項と制限事項 \(75 ページ\)](#)
- [デフォルト設定 \(81 ページ\)](#)
- [PIM および PIM6 の設定 \(83 ページ\)](#)
- [PIM および PIM6 設定の検証 \(133 ページ\)](#)
- [統計の表示 \(141 ページ\)](#)
- [マルチキャスト サービス リフレクションの設定 \(142 ページ\)](#)
- [PIM の設定例 \(155 ページ\)](#)
- [関連資料 \(166 ページ\)](#)
- [標準 \(166 ページ\)](#)
- [MIB \(166 ページ\)](#)

PIM および PIM6 について

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

Cisco NX-OS は、IPv4 ネットワーク (PIM) および IPv6 ネットワーク (PIM6) で PIM スパース モードをサポートしています。PIM スパース モードでは、ネットワーク上の要求元だけにマルチキャストトラフィックが伝送されます。PIM と PIM6 は、ルータ上で同時に実行するように設定できます。PIM および PIM6 グローバル パラメータを使用すると、ランデブー ポイント (RP)、メッセージパケット フィルタリング、および統計情報を設定できます。PIM および PIM6 インターフェイスパラメータを使用すると、マルチキャスト機能のイネーブル化、PIM の境界の識別、PIM hello メッセージインターバルの設定、および代表ルータ (DR) のプライオリティ設定を実行できます。



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

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

PIM および PIM6 グローバル コンフィギュレーション パラメータを使用すると、マルチキャスト グループ アドレスの範囲を設定して、次に示す配信モードで利用できます。

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



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

これらのモードを組み合わせ、さまざまな範囲のグループアドレスに対応することができます。

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

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

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

vPC を使用した PIM SSM

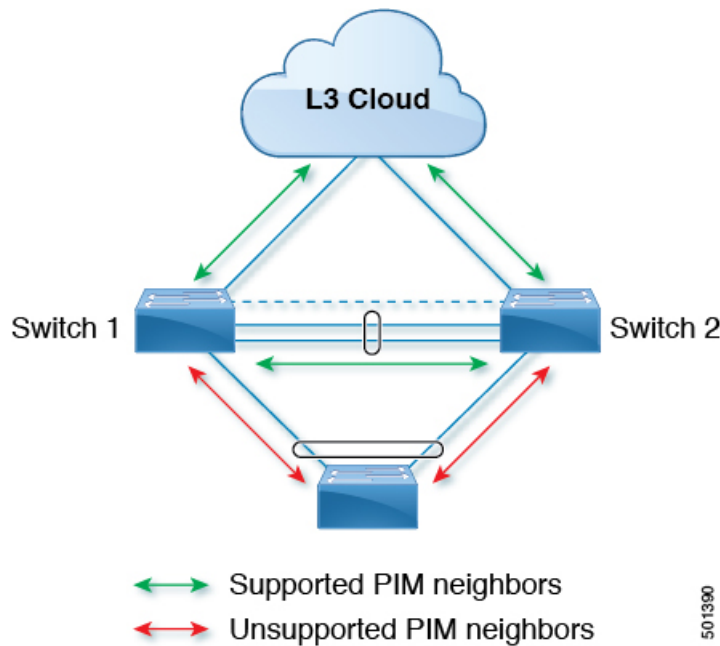
Cisco NX-OS リリース 7.0(3)I4(1) 以降、vPC 機能とともにアップストリーム レイヤ 3 クラウドを備えた Cisco Nexus 9000 シリーズ スイッチで PIM SSM を有効にできます。

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

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



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



501390

Hello メッセージ

ルータがマルチキャスト IPv4 アドレス 224.0.0.13 または IPv6 アドレス ff02::d に PIM hello メッセージを送信して、PIM ネイバーとの隣接関係を確立すると、PIM プロセスが開始されます。hello メッセージは 30 秒間隔で定期的に送信されます。PIM ソフトウェアはすべてのネイバーからの応答を確認すると、各 LAN セグメント内で優先順位が最大のルータを代表ルータ (DR) として選択します。DR 優先順位は、PIM hello メッセージの DR 優先順位値に基づいて決まります。全ルータの DR プライオリティ値が不明、またはプライオリティが等しい場合は、IP アドレスが最上位のルータが DR として選定されます。

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

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

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



(注) PIM6 は MD5 認証をサポートしません。

Join-Prune メッセージ

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

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

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



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

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

ステートのリフレッシュ

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

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

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

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

ランデブーポイント

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

スタティック RP

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

スタティック RP を定義するのは、次のような場合です。

- ルータに Anycast RP アドレスを設定する場合
- デバイスに RP を手動で設定する場合

BSR

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

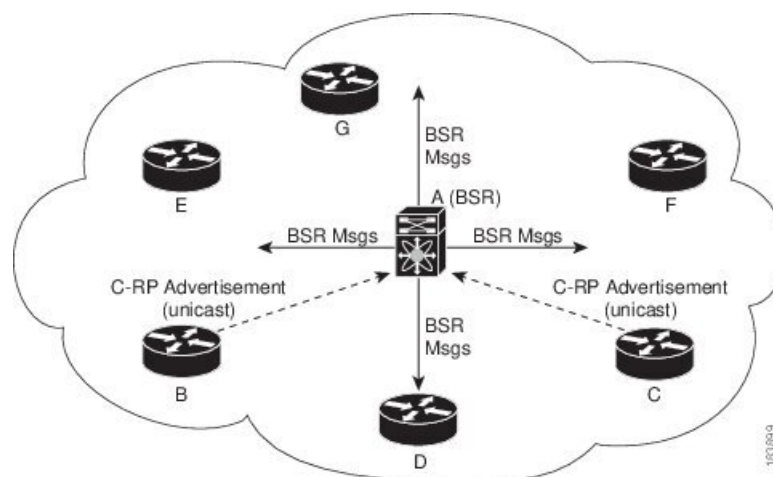
BSR は、Cisco Nexus 9300-FX、Cisco Nexus 9300-FX2、および Cisco Nexus 9300-FX3S プラットフォーム スイッチでサポートされています。

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

次の図に、BSR メカニズムを示します。ここで、ルータ A (ソフトウェアによって選定された BSR) は、すべての有効なインターフェイスから BSR メッセージを送信しています (図の実線部分)。このメッセージには RP セットが含まれており、ネットワーク内のすべてのルータに次々とフラッドされます。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 12: BSR メカニズム



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

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



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



(注) PIM6 では BSR はサポートされていません。

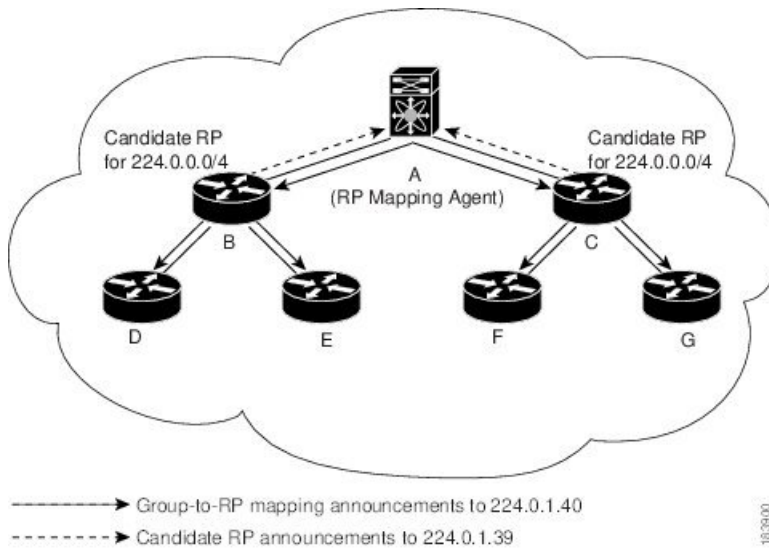
Auto-RP

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

マッピングテーブルを RP-Discovery メッセージに格納して、Cisco RP-Discovery マルチキャスト グループ 224.0.0.140 にマルチキャストします。

次の図に、Auto-RP メカニズムを示します。RP マッピングエージェントは、受信した RP 情報を、定期的に Cisco RP-Discovery グループ 224.0.0.140 にマルチキャストします（図の実線部分）。

図 13: Auto-RP のメカニズム



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



(注) Auto-RP は PIM6 ではサポートされていません。



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

PIM ドメインで設定された複数の RP

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

Anycast-RP

Anycast-RP の実装方式には、マルチキャスト送信元検出プロトコル (MSDP) を使用する場合と、RFC 4610、『プロトコル独立マルチキャスト (PIM) を使用する Anycast-RP』に基づく場合の 2 種類があります。ここでは、PIM Anycast-RP の設定方法について説明します。

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

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

PIM は、PIM Anycast RP および PIM Bidir RP に使用されるループバック インターフェイス上に設定する必要があります。

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

PIM 登録メッセージ

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

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

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

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

PIM トリガー レジスタはデフォルトで有効になっています。

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

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

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



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

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

指定ルータ

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

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

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

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

指定フォワーダ

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

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



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

共有ツリーから送信元ツリーへの ASM スイッチオーバー



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

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

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

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

マルチキャスト フロー パスの可視性

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

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

この機能は次をサポートします。

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

管理用スコープの IP マルチキャスト

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

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

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

マルチキャスト カウンタ

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

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

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

マルチキャストヘビーテンプレート

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

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

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

マルチキャスト VRF-Lite ルート リーク

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

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

PIM グレースフル リスタート

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

生成 ID

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



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

PIM グレースフル リスタート動作

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

図 14: *RP* スイッチオーバー中の *PIM* グレースフル リスタート動作

PIM グレースフル リスタート動作は次のとおりです。

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

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

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



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

高可用性

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

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

PIM および PIM6 の前提条件

PIM および PIM6 の利用条件は次のとおりです。

- デバイスにログインしている。

- 現在の仮想ルーティングおよびフォワーディング (VRF) モードが正しい (グローバルコマンドの場合)。この章の例で示すデフォルトのコンフィギュレーション モードは、デフォルト VRF に適用されます。
- PIM Bidir の場合、**hardware access-list tcam region mcast-bidir** コマンドを使用して ACL TCAM リージョン サイズを設定する必要があります。

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

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



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



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

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

PIM および PIM6 に関する注意事項と制限事項

PIM および PIM6 に関する注意事項および制限事項は次のとおりです。

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

- Cisco NX-OS の PIM および PIM6 は、いずれのバージョンの PIM デンス モードまたは PIM スパース モードバージョン 1 と相互運用性がありません。
- PIM SSM および PIM ASM は、すべての Cisco Nexus 9000 シリーズ スイッチでサポートされています。
- Cisco Nexus 9000 シリーズ スイッチは、vPC 上の PIM6 SSM をサポートしています。
- より低い IP アドレスを持つ L2 デバイスでスヌーピング クエリアを設定して、L2 デバイスをクエリアとして強制することをお勧めします。これは、マルチシャード EtherChannel トランク (MCT) がダウンしているシナリオの処理に役立ちます。
- ランデブー ポイントが PIM データ レジスタを受信すると、そのレジスタは処理のために CPU にパントされることが予期されます。この操作中に、レジスタのカプセル化が解除され、そのグループに関連する OIF がある場合は、そのデータ部分がソフトウェアで転送されます。
- (S,G) ルートは、spt-threshold infinity の設定に関係なく、データ パケットがパントされるとコントロールプレーンに作成されます。ルートは、コントロールプレーンを保護し、パケットのパントを制限するために作成されます。
- 次に示すように、サービスインターフェイスが作成される前に NAT フローが確立された場合は、**clear ip mroute group source** コマンドを使用して、影響を受けるルートを手動でクリアします。

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

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

- Cisco Nexus 9000 シリーズ スイッチは、vPC レッグまたは vPC の背後にあるルータとの PIM 隣接関係をサポートしていません。
- Cisco Nexus 9000 シリーズ スイッチでは、PIM スヌーピングはサポートされていません。
- Cisco Nexus 9000 シリーズ スイッチは、PIM6 ASM および SSM をサポートします。



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

- PIM 双方向マルチキャスト送信元 VLAN ブリッジングは、FEX ポートではサポートされていません。
- PIM6 双方向はサポートされていません。
- PIM6 は、Cisco NX-OS リリース 9.3(3) より前の SVI ではサポートされていません。
- PIM6 は、FEX ポート（レイヤ 2 およびレイヤ 3）ではサポートされていません。
- PIM 双方向は、Cisco Nexus 9300-EX、Cisco Nexus 9300-FX/FX2/FX3、および Cisco Nexus 9300-GX プラットフォーム スイッチでサポートされます。
- Cisco Nexus 9000 シリーズ スイッチは、vPC での PIM Bidir または vPC での PIM6 ASM、SSM、および双方向をサポートしていません。
- 次のデバイスは、レイヤ 3 ポート チャネル サブインターフェイスで PIM および PIM6 スパース モードをサポートしています。
 - Cisco Nexus 9300 シリーズ スイッチ
 - Cisco Nexus 9300-EX シリーズ スイッチおよび Cisco Nexus 3232C および 3264Q スイッチ
 - N9K-X9400 または N9K-X9500 ライン カードまたは N9K-C9504-FM、N9K-C9508-FM、および N9K-C9516-FM ファブリック モジュール（あるいはその両方）を備えた Cisco Nexus 9500 シリーズ スイッチ。
- マルチキャスト ヘビー テンプレートは、リアルタイム パケットとバイト統計をサポートしますが、VXLAN およびトンネルの出力または入力統計はサポートしません。
- リアルタイム/フレックス統計は、以下でサポートされています。
 - **hardware profile multicast flex-stats-enable** コマンドの構成を備えたデフォルトのテンプレート。

- 構成のないヘビー テンプレート。

リアルタイム統計は、拡張ヘビー テンプレートをサポートしていません。

- IPv4 上の GRE トンネルはマルチキャストをサポートします。IPv6 上の GRE トンネルはマルチキャストをサポートしていません。
- GRE トンネルでマルチキャストをサポートするのは、Cisco Nexus 9300-EX および 9300-FX/FX2/FX3 プラットフォームスイッチだけです。
- Cisco NX-OS リリース 10.2(1q)F 以降、マルチキャスト GRE は Cisco Nexus N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。
- GRE トンネルはホスト接続をサポートしていません。
- IGMP 機能はホスト接続の一部としてサポートされていないため、IGMP CLI は GRE トンネルでは使用できません。
- 静的トンネル OIF はマルチキャストルートに追加できない場合があります。IGMP CLI は GRE トンネルでは使用できず、マルチキャストグループを発信インターフェイス (OIF) に静的にバインドする必要があるためです。
- SVI IP アドレスはトンネルの送信元またはトンネルの宛先として使用しないでください。
- トンネルの宛先は、L3 物理インターフェイスまたは L3 サブインターフェイスを介して到達可能である必要があります。
- トンネルの宛先に到達可能な L3 物理インターフェイスまたはサブインターフェイスでは、PIM が有効になっている必要があります。
- 同じデバイス上の複数の GRE トンネルでは、同じ送信元または同じ宛先を使用しないでください。
- GRE でカプセル化されたマルチキャスト トラフィックの ECMP 負荷共有はサポートされていません。トンネルの宛先に複数のリンクを介して到達できる場合、トラフィックはそのうちの 1 つのみに送信されます。
- マルチキャスト整合性チェッカーは、GRE トンネルではサポートされていません。
- GRE トンネルは、送信元または宛先インターフェイスが同じ VRF のメンバーである場合にのみ、VRF のメンバーになることができます。
- マルチキャスト VRF-Lite ルート リークは GRE ではサポートされていません。
- PIM Bidir は GRE ではサポートされていません。
- Cisco Nexus 3232C および 3264Q スイッチは、PIM6 をサポートしていません。
- インターフェイスに PIM/PIM6 ネイバーがない場合、そのインターフェイスは、最短/ECMP パスに基づいて RPF インターフェイスとして選択できます。送信元と受信者の間に複数の ECMP がある場合は、リンクの両側で PIM/PIM6 を有効にするようにしてください。

- Cisco NX-OS リリース 9.3(6) 以降、GRE 上のマルチキャストは、Cisco Nexus 9300-GX プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 9.3(6) 以降では、以下がサポートされます。
 - スイッチ 1 の着信 RPF インターフェイスは、デフォルトの VRF の下にあり、他の VRF ではスイッチ 2 にあります。
 - スイッチ 1 のトンネルインターフェイスはデフォルト VRF の下にあり、他の VRF ではスイッチ 2 にあります。
 - スイッチ 1 の発信インターフェイスは他の VRF にあり、デフォルトの VRF の下ではスイッチ 2 にあります。
- Cisco Nexus 9000 スイッチに GRE トンネルが存在すると、サブインターフェイスと共存できません（サブインターフェイスへのマルチキャスト転送で dot1q タグが欠落する場合があります）。これは、サブインターフェイスでのマルチキャストトラフィックの受信に影響します。トラフィックは、サブインターフェイスではなく、親インターフェイスで受信されます。この影響は、標準/ネイティブ マルチキャスト パケットのみに影響し、マルチキャスト GRE（カプセル化およびカプセル化解除）パケットには影響しません。この制限は、Cisco Nexus 9300-GX プラットフォーム スイッチに適用されます。
- トンネル（機能トンネルまたは feature nv オーバーレイ）は、サブインターフェイスと共存できません（サブインターフェイスへのマルチキャスト転送で dot1q タグが欠落している可能性があります）。これは、サブインターフェイスでの受信マルチキャストトラフィックに影響します。この制限は、Cisco Nexus 9300-GX プラットフォーム スイッチに適用されます。
- GRE トンネルの送信元または宛先の設定が間違っている場合（送信元/宛先に互換性がないなど）、それらは自動的にシャットダウンされ、設定が回復された後でもシャットダウンされたままになります。回避策は、そのようなトンネルを手動でシャットダウン/シャットダウン解除することです。
- PIM-SM では、転送パスに変更があると、パケットの重複またはドロップが予想される動作になります。これにより、次のようなデメリットが発生します。
 - 共有ツリーでの受信から最短パスツリー（SPT）に切り替える場合、通常、パケットがドロップされるときに小さなウィンドウが発生します。SPT 機能はこれを防止することができますが、重複が発生する場合があります。
 - PIM レジスタまたは MSDP を介して受信した可能性のあるパケットを最初に転送する RP は、次にネイティブ転送のために SPT に参加しますが、そのため、RP が同じデータ パケットを 2 回転送する小さなウィンドウが生じます。1 回はネイティブ パケットとして、1 回は PIM 登録または MSDP カプセル化解除の後です。

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

- PIM は、送信元、受信者、およびランデブー ポイント（RP）間のすべての L3 インターフェイスで構成する必要があります。

- HSRP 対応の PIM は、Cisco NX-OS ではサポートされていません。
- マルチキャスト対応 BL がリロードされる場合、顧客は、ルートスケールに応じて、ファブリックポートトラッキングタイマーが 3〜5 前後に設定されていることを確認する必要があります。

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

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

Hello メッセージに関する注意事項と制限事項

Hello メッセージには、次の注意事項および制約事項が適用されます。

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

ランデブーポイントの注意事項と制限事項

ランデブーポイント (RP) には、次の注意事項と制限事項が適用されます。

- 候補 RP インターバルを 15 秒以上に設定してください。
- 同じネットワーク内では、Auto-RP プロトコルと BSR プロトコルを同時に設定できません。
- PIM6 は BSR と Auto-RP をサポートしていません。
- PIM は、PIM Anycast RP および PIM Bidir RP に使用されるループバック インターフェイス上に設定する必要があります。
- PIMRP（スタティック、BSR、または Auto-RP のいずれか）の設定に使用されるインターフェイスには、**ip [v6] pim sparse-mode**が必要です。
- RPF 失敗パケットの過剰なパントを避けるために、Cisco Nexus 9000 シリーズスイッチは、ASM のアクティブな送信元に対して S、G エントリを作成する場合があります。ただし、そのようなグループにはランデブーポイント (RP) がありません。送信元に対するリバースパス転送 (RPF) が失敗した状況でも同様です。

この動作は、Nexus 9200、9300-EX プラットフォームスイッチ、および N9K-X9700-EX LC プラットフォームには適用されません。

- デバイスに BSR ポリシーが適用されており、BSR として選定されないように設定されている場合、このポリシーは無視されます。これにより、次のようなデメリットが発生します。
 - ポリシーで許可されている BSM をデバイスが受信した場合、意図に反してこのデバイスが BSR に選定されていると、対象の BSM がドロップされるために下流のルータではその BSM を受信できなくなります。また、下流のデバイスでは、不正な BSR から送信された BSM が正しくフィルタリングされるため、これらのデバイスでは RP 情報を受信できなくなります。
 - BSR に異なるデバイスから送られた BSM が着信すると、新しい BSM が送信されますが、その正規の BSM は下流のデバイスでは受信されません。
- 送信元 VRF が、たまたま RP である非フォワーダ vPC ピアにマルチキャストトラフィックを転送した場合、S、G エントリはフォワーダ vPC ピアに作成されません。これにより、これらの送信元のマルチキャストトラフィックがドロップする可能性があります。これを回避するには、vPC ピアが同時に RP でもある場合は常に、トポロジにエニーキャスト RP を設定する必要があります。

マルチキャスト VRF-lite ルート リークの注意事項と制限事項

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

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

デフォルト設定

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

表 11: PIM および PIM6 のデフォルトパラメータ

パラメータ	デフォルト
共有ツリーだけを使用	無効

パラメータ	デフォルト
再起動時にルートをフラッシュ	無効
ログ ネイバーの変更	無効
Auto-RP メッセージアクション	無効
BSR メッセージアクション	無効
SSM マルチキャスト グループ範囲またはポリシー	IPv4 • 232.0.0.0/8 IPv6 • ff32::/32 • ff33::/32 • ff34::/32 • ff35::/32 • ff36::/32 • ff37::/32 • ff38::/32 • ff39::/32 • ff3a::/32 • ff3b::/32 • ff3c::/32 • ff3d::/32 • ff3e::/32
PIM スパース モード	無効
DR プライオリティ	1
hello 認証モード	無効
ドメイン境界	無効
RP アドレス ポリシー	メッセージをフィルタリングしない
PIM Register メッセージ ポリシー	メッセージをフィルタリングしない
BSR 候補 RP ポリシー	メッセージをフィルタリングしない
BSR ポリシー	メッセージをフィルタリングしない

パラメータ	デフォルト
Auto-RP マッピング エージェント ポリシー	メッセージをフィルタリングしない
Auto-RP 候補 RP ポリシー	メッセージをフィルタリングしない
Join/Prune ポリシー	メッセージをフィルタリングしない
ネイバーとの隣接関係ポリシー	すべての PIM ネイバーと隣接関係を確立
BFD	無効化

PIM および PIM6 の設定

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



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

下の表で説明されているマルチキャスト配信モードを使用すると、PIM または PIM6 ドメインに、それぞれ独立したアドレス範囲を設定できます。

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

PIM および PIM6 の設定作業

次の手順では、PIM および PIM6 を設定します。

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

- ASM モードまたは Bidir モードについては、[ASM および Bidir の設定](#)を参照してください。
- SSM モードについては、[SSM の設定](#)を参照してください。
- マルチキャスト用 RPF ルートについては、[マルチキャスト用 RPF ルートの設定](#)を参照してください。

4. メッセージフィルタリングを設定します。



(注) 次の CLI コマンドを使用して PIM を設定します。

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

PIM および PIM6 機能のイネーブル化

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



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

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	feature pim 例 : switch(config)# feature pim	PIM をイネーブルにします。デフォルトでは PIM はディセーブルになっています。
ステップ 3	feature pim6 例 : switch(config)# feature pim6	PIM6 をイネーブルにします。デフォルトでは PIM6 はディセーブルになっています。
ステップ 4	(任意) show running-configuration pim 例 : switch(config)# show running-configuration pim	PIM の実行コンフィギュレーション情報を示します。
ステップ 5	(任意) show running-configuration pim6 例 : switch(config)# show running-configuration pim6	PIM6 の実行コンフィギュレーション情報を示します。
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。

PIM または PIM6 スパース モード パラメータの設定

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

表 12: PIM および PIM6 スパース モードのパラメータ

パラメータ	説明
デバイスにグローバルに適用	

パラメータ	説明
Auto-RP メッセージアクション	Auto-RP メッセージの受信と転送をイネーブルにします。これらの機能はデフォルトではディセーブルになっているため、候補 RP またはマッピングエージェントとして設定されていないルータは、Auto-RP メッセージの受信と転送を行いません。 (注) PIM6 は、Auto-RP 方式をサポートしていません。
BSR メッセージアクション	BSR メッセージの受信と転送をイネーブルにします。これらの機能はデフォルトではディセーブルになっているため、候補 RP または BSR 候補として設定されていないルータは、BSR メッセージの受信と転送を行いません。 (注) PIM6 は BSR をサポートしていません。
Bidir RP 制限	IPv4 に設定可能な Bidir RP の数を設定します。PIM の各 VRF でサポートする Bidir RP の最大数を 8 以下にする必要があります。有効範囲は 0 ～ 8 です。デフォルト値は 6 です。 (注) PIM6 は Bidir をサポートしていません。
Register のレート制限	IPv4 または IPv6 Register のレート制限を毎秒のパケット数で設定します。指定できる範囲は 1 ～ 65,535 です。デフォルト設定は無制限です。
初期ホールドダウン期間	IPv4 または IPv6 の初期ホールドダウン期間を秒単位で設定します。このホールドダウン期間は、MRIB が最初に起動するのにかかる時間です。コンバージェンスを高速化するには、小さい値を入力します。指定できる範囲は 90 ～ 210 です。ホールドダウン期間をディセーブルにするには、0 を指定します。デフォルト値は 210 です。
デバイスの各インターフェイスに適用	
PIM スパース モード	インターフェイスで PIM または PIM6 をイネーブルにします。

パラメータ	説明
DR プライオリティ	現在のインターフェイスに、PIM hello メッセージの一部としてアドバタイズされる指定ルータ (DR) プライオリティを設定します。複数の PIM 対応ルータが存在するマルチアクセス ネットワークでは、DR プライオリティの最も高いルータが DR ルータとして選定されます。プライオリティが等しい場合は、IP アドレスが最上位のルータが DR に選定されます。DR は、直接接続されたマルチキャスト送信元に PIM Register メッセージを送信するとともに、直接接続された受信者に代わって、ランデブー ポイント (RP) 方向に PIM Join メッセージを送信します。有効範囲は 1 ～ 4294967295 です。デフォルトは 1 です。
指定ルータの遅延	PIMhello メッセージでアドバタイズされる DR プライオリティを指定期間にわたり 0 に設定することで、指定ルータ (DR) の選定への参加を遅延させます。この遅延中、DR は変更されず、現在のスイッチにはそのインターフェイスでのすべてのマルチキャストの状態を把握する時間が与えられます。遅延期間が終了すると、DR 選出を再び開始するために、正しい DR プライオリティが hello パケットで送信されます。値の範囲は 3 ～ 0xffff 秒です。
hello 認証モード	インターフェイスで、PIM hello メッセージ内の MD5 ハッシュ認証キー (パスワード) をイネーブルにして、直接接続されたネイバーによる相互認証を可能にします。PIMhello メッセージは、認証ヘッダー (AH) オプションを使用して符号化された IP セキュリティです。暗号化されていない (クリアテキストの) キーか、または次に示す値のいずれかを入力したあと、スペースと MD5 認証キーを入力します。 • 0 : 暗号化されていない (クリアテキストの) キーを指定します。 • 3 : 3-DES 暗号化キーを指定します。 • 7 : Cisco Type 7 暗号化キーを指定します。 認証キーの文字数は最大 16 文字です。デフォルトではディセーブルになっています。 (注) PIM6 は MD5 認証をサポートしません。
hello 間隔	hello メッセージの送信インターバルを、ミリ秒単位で設定します。範囲は 1000 ～ 18724286 です。デフォルト値は 30000 です。 (注) このパラメータの確認された範囲および関連付けられた PIM ネイバースケールについては、『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

パラメータ	説明
ドメイン境界	インターフェイスを PIM ドメインの境界として設定し、対象のインターフェイスで、ブートストラップ、候補 RP、または Auto-RP の各メッセージが送受信されないようにします。デフォルトではディセーブルになっています。 (注) PIM6 は、Auto-RP 方式をサポートしていません。
ネイバー ポリシー	prefix-list ポリシーに基づいて、どの PIM ネイバーと隣接関係になるかを設定します。³指定したポリシー名が存在しない場合、またはプレフィックス リストがポリシー内で設定されていない場合は、すべてのネイバーとの隣接関係が確立されます。デフォルトでは、すべての PIM ネイバーと隣接関係が確立されます。 (注) この機能の設定は、経験を積んだネットワーク管理者が行うことを推奨します。 (注) PIM ネイバー ポリシーは、プレフィックス リストのみをサポートします。ルートマップ内で使用される ACL はサポートしていません。

³ prefix-list ポリシーを設定するには、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

PIM6 スパース モード パラメータの設定

手順の概要

1. **configure terminal**
2. (任意) **ip pim auto-rp {listen [forward] | forward [listen]}**
3. (任意) **ip pim bsr {listen [forward] | forward [listen]}**
4. (任意) **ip pim bidir-rp-limit** 制限
5. (任意) **ip pim register-rate-limit** rate
6. (任意) **ip pim spt-threshold infinity group-list** route-map-name
7. (任意) **[ip | ipv4] routing multicast holddown** holddown-period
8. (任意) **show running-configuration pim**
9. **interface** interface
10. **ip pim sparse-mode**
11. (任意) **ip pim dr-priority** priority
12. (任意) **ip pim dr-delay** delay
13. (任意) **ip pim hello-authentication ah-md5** auth-key
14. (任意) **ip pim hello-interval** interval

15. (任意) **ip pim border**
16. (任意) **ip pim neighbor-policy prefix-list prefix-list**
17. (任意) **show ip pim interface [interface | brief] [vrf vrf-name | all]**
18. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	(任意) ip pim auto-rp {listen [forward] forward [listen]} 例 : <pre>switch(config)# ip pim auto-rp listen</pre>	Auto-RP メッセージの待ち受けまたは転送をイネーブルにします。デフォルトではこれらの機能がディセーブルになっているため、Auto-RP メッセージの受信と転送は行われません。
ステップ 3	(任意) ip pim bsr {listen [forward] forward [listen]} 例 : <pre>switch(config)# ip pim bsr forward</pre>	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 bidir-rp-limit 制限 例 : <pre>switch(config)# ip pim bidir-rp-limit 4</pre>	IPv4 に設定可能な Bidir RP の数を指定します。PIM の各 VRF でサポートする Bidir RP の最大数を 8 以下にする必要があります。有効範囲は 0 ～ 8 です。デフォルト値は、6 です。
ステップ 5	(任意) ip pim register-rate-limit rate 例 : <pre>switch(config)# ip pim register-rate-limit 1000</pre>	レート制限を毎秒のパケット数で設定します。指定できる範囲は 1 ～ 65,535 です。デフォルト設定は無制限です。
ステップ 6	(任意) ip pim spt-threshold infinity group-list route-map-name 例 : <pre>switch(config)# ip pim spt-threshold infinity group-list my_route-map-name</pre>	指定されたルート マップで定義されているグループプレフィックスに対して、IPv4 PIM (*,G) 状態のみを作成します。Cisco NX-OS リリース 3.1 は最大 1000 のルート マップ エントリを、リリース 3.1 より前の Cisco NX-OS は最大 500 のルート マップ エントリをサポートします。 (注) ip pim use-shared-tree-only group-list コマンドは、ip pim spt-threshold infinity group-list コマンドと同

	コマンドまたはアクション	目的
		じ機能を実行します。いずれかのコマンドを使用してこの手順を実行できます。 両方のコマンド (ip pim spt-threshold infinity group-list および ip pim use-shared-tree-only group-list) には、次の制限があります。 • これは、Cisco Nexus 9000 クラウド スケール スイッチの仮想ポート チャンネル (vPC) でのみサポートされます。 • NX-OS (非 vPC) のラスト ホップ ルーター (LHR) 構成でサポートされています。
ステップ 7	(任意) [ip ipv4] routing multicast holddown holddown-period 例 : <pre>switch(config)# ip routing multicast holddown 100</pre>	初期ホールドダウン期間を秒単位で設定します。指定できる範囲は 90 ~ 210 です。ホールドダウン期間をディセーブルにするには、0 を指定します。デフォルト値は 210 です。
ステップ 8	(任意) show running-configuration pim 例 : <pre>switch(config)# show running-configuration pim</pre>	Bidir RP 制限および Register のレート制限を含む、PIM 実行コンフィギュレーション情報を表示します。
ステップ 9	interface interface 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 10	ip pim sparse-mode 例 : <pre>switch(config-if)# ip pim sparse-mode</pre>	現在のインターフェイスで PIM スパース モードをイネーブルにします。デフォルトではディセーブルになっています。
ステップ 11	(任意) ip pim dr-priority priority 例 : <pre>switch(config-if)# ip pim dr-priority 192</pre>	PIM hello メッセージの一部としてアドバタイズされる指定ルータ (DR) プライオリティを設定します。有効範囲は 1 ~ 4294967295 です。デフォルトは 1 です。
ステップ 12	(任意) ip pim dr-delay delay 例 : <pre>switch(config-if)# ip pim dr-delay 3</pre>	PIM hello メッセージでアドバタイズされる DR プライオリティを指定期間にわたり 0 に設定することで、指定ルータ (DR) の選定への参加を遅延させます。この遅延中、DR は変更されず、現在のスイッチにはそのインターフェイスでのすべてのマルチキャストの状態を把握する時間が与えられます。遅延期間が終了すると、DR 選出を再び開始するた

	コマンドまたはアクション	目的
		めに、正しい DR プライオリティが hello パケットで送信されます。値の範囲は 3 ～ 0xffff 秒です。 (注) このコマンドは、起動時、または IP アドレスかインターフェイスの状態が変更された後にのみ、DR 選定への参加を遅延させます。これは、マルチキャストアクセスの非 vPC レイヤ 3 インターフェイス専用です。
ステップ 13	(任意) ip pim hello-authentication ah-md5 auth-key 例 : <pre>switch(config-if)# ip pim hello-authentication ah-md5 my_key</pre>	PIM hello メッセージ内の MD5 ハッシュ認証キーをイネーブルにします。暗号化されていない (クリアテキストの) キーか、または次に示す値のいずれかを入力したあと、スペースと MD5 認証キーを入力します。 • 0 : 暗号化されていない (クリアテキストの) キーを指定します。 • 3 : 3-DES 暗号化キーを指定します。 • 7 : Cisco Type 7 暗号化キーを指定します。 キーの文字数は最大 16 文字です。デフォルトではディセーブルになっています。
ステップ 14	(任意) ip pim hello-interval interval 例 : <pre>switch(config-if)# ip pim hello-interval 25000</pre>	hello メッセージの送信インターバルを、ミリ秒単位で設定します。範囲は 1000 ～ 18724286 です。デフォルト値は 30000 です。 (注) 最小値は 1 ミリ秒です。
ステップ 15	(任意) ip pim border 例 : <pre>switch(config-if)# ip pim border</pre>	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 16	(任意) ip pim neighbor-policy prefix-list prefix-list 例 : <pre>switch(config-if)# ip pim neighbor-policy prefix-list AllowPrefix</pre>	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 の各メッセージが受信されないようにします。デフォルトではディセーブルになっています。 また、prefix-list コマンドを使用して、プレフィックスリストポリシーに基づいて隣接する PIM ネイ

	コマンドまたはアクション	目的
		バーを設定します。ip prefix-list プレフィックス リストは最大 63 文字です。デフォルトでは、すべての PIM ネイバーと隣接関係が確立されます。 (注) この機能の設定は、経験を積んだネットワーク管理者が行うことを推奨します。
ステップ 17	(任意) show ip pim interface [<i>interface</i> brief] [vrf <i>vrf-name</i> all] 例 : <pre>switch(config-if)# show ip pim interface</pre>	PIM インターフェイスの情報を表示します。
ステップ 18	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

PIM6 スパース モード パラメータの構成

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
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) ipv6 pim register-rate-limit rate 例 : switch(config)# ipv6 pim register-rate-limit 1000	レート制限を毎秒のパケット数で設定します。指定できる範囲は 1 ～ 65,535 です。デフォルト設定は無制限です。
ステップ 3	(任意) ipv6 routing multicast holddown holddown-period 例 : switch(config)# ipv6 routing multicast holddown 100	初期ホールドダウン期間を秒単位で設定します。指定できる範囲は 90 ～ 210 です。ホールドダウン期間をディセーブルにするには、0 を指定します。デフォルト値は 210 です。
ステップ 4	(任意) show running-configuration pim6 例 : switch(config)# show running-configuration pim6	Register レート制限を含めた PIM6 の実行コンフィギュレーション情報を表示します。
ステップ 5	interface interface 例 : switch(config)# interface vlan 10 switch(config-if)#	指定したインターフェイスに対してインターフェイス コンフィギュレーションモードを開始します。
ステップ 6	ipv6 pim sparse-mode 例 : switch(config-if)# ipv6 pim sparse-mode	現在のインターフェイスで PIM スパース モードをイネーブルにします。デフォルトではディセーブルになっています。 Cisco NX-OS リリース 9.3(5) 以降では、Broadcom ベースのスイッチの SVI インターフェイスでこのコマンドを設定できます。
ステップ 7	(任意) ipv6 pim dr-priority priority 例 : switch(config-if)# ipv6 pim dr-priority 192	PIM6 hello メッセージの一部としてアドバタイズされる指定ルータ (DR) プライオリティを設定します。有効範囲は 1 ～ 4294967295 です。デフォルトは 1 です。
ステップ 8	(任意) ipv6 pim hello-interval interval 例 : switch(config-if)# ipv6 pim hello-interval 25000	hello メッセージの送信インターバルを、ミリ秒単位で設定します。範囲は 1000 ～ 18724286 です。デフォルト値は 30000 です。
ステップ 9	(任意) ipv6 pim border 例 : switch(config-if)# ipv6 pim border	インターフェイスを PIM6 ドメインの境界として設定し、対象のインターフェイスで、ブートストラップ、候補 RP、または Auto-RP の各メッセージが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。

	コマンドまたはアクション	目的
ステップ 10	(任意) ipv6 pim neighbor-policy prefix-list prefix-list 例 : <pre>switch(config-if)# ipv6 pim neighbor-policy prefix-list AllowPrefix</pre>	ipv6 prefix-list prefix-list コマンドを使用して、プレフィックス リスト ポリシーに基づいてどの PIM6 ネイバーと隣接関係になるかを設定します。プレフィックス リストは最大 63 文字です。デフォルトでは、すべての PIM6 ネイバーと隣接関係が確立されます。 (注) この機能の設定は、経験を積んだネットワーク管理者が行うことを推奨します。
ステップ 11	show ipv6 pim interface [interface brief] [vrf vrf-name all] 例 : <pre>switch(config-if)# show ipv6 pim interface</pre>	PIM6 インターフェイスの情報を表示します。
ステップ 12	copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	(任意) コンフィギュレーションの変更を保存します。

ASM と Bidir の設定

Any Source Multicast (ASM) および双方向共有ツリー (Bidir) のマルチキャスト配信モードでは、マルチキャストデータの送信元と受信者の間に、共通のルートとして動作する RP を設定する必要があります。

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

静的 RP の設定

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



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

match ip multicast コマンドで、使用するグループプレフィックスを示すルートマップポリシー名を指定できます。または、設定のプレフィックスリスト方法を指定することができます。



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

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

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

静的 RP の設定 (PIM)

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip pim rp-address <i>rp-address</i> [group-list <i>ip-prefix</i> prefix-list <i>name</i> override route-map <i>policy-name</i>] [bidir] 例 : <pre>switch(config)# ip pim rp-address 192.0.2.33 group-list 224.0.0.0/9</pre>	マルチキャストグループ範囲に、PIM スタティック RP アドレスを設定します。 match ip multicast コマンドで、静的 RP アドレスのプレフィックスリストポリシー名または使用するグループプレフィックスを示すルートマップポリシー名を指定できます。

静的 RP の設定 (PIM6)

	コマンドまたはアクション	目的
		bidir キーワードを指定しない場合、モードは ASM です。 override オプションにより、RP アドレスは、ルートマップで指定されたグループの動的に学習された RP アドレスをオーバーライドします。 この例では、指定したグループ範囲に PIM ASM モードを設定しています。
ステップ 3	(任意) show ip pim group-range [ip-prefix vrf vrf-name] 例 : <pre>switch(config)# show ip pim group-range</pre>	BSR の待ち受けおよび転送ステートなど、PIM RP 情報を表示します。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

静的 RP の設定 (PIM6)

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	ipv6 pim rp-address <i>rp-address</i> [group-list <i>ipv6-prefix</i> route-map <i>policy-nsmr</i>] 例 : <pre>switch(config)# ipv6 pim rp-address 2001:0db8:0:abcd::1 group-list ff1e:abcd:def1::0/24</pre>	マルチキャスト グループ範囲に、PIM6 スタティック RP アドレスを設定します。 match ip multicast コマンドで、使用するグループプレフィックスを示すルートマップポリシー名を指定できます。モードは ASM です。デフォルトのグループ範囲は ff00::0/8 です。 この例では、指定したグループ範囲に PIM ASM モードを設定しています。
ステップ 3	(任意) show ipv6 pim group-range [<i>ipv6-prefix</i> vrf <i>vrf-name</i>] 例 : <pre>switch(config)# show ipv6 pim group-range</pre>	PIM6 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 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

BSR の設定

BSR を設定するには、候補 BSR および候補 RP を選択します。



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

候補 BSR の設定では、引数を指定できます（次の表を参照）。



(注) PIM6 は BSR をサポートしていません。

表 13: 候補 BSR の引数

引数	説明
<i>interface</i>	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。
<i>hash-length</i>	マスクを適用するために使用される上位桁の 1 の個数です。マスクでは、候補 RP のグループアドレス範囲の論理積をとることにより、ハッシュ値を算出します。マスクは、グループ範囲が等しい一連の RP に割り当てられる連続アドレスの個数を決定します。PIM の場合、この値の範囲は 0 ～ 32 であり、デフォルト値は 30 秒です。PIM6 の場合、この値の範囲は 0 ～ 128 で、デフォルト値は 126 秒です。

BSR 候補 RP の引数およびキーワードの設定

引数	説明
<i>priority</i>	現在の BSR に割り当てられたプライオリティ。ソフトウェアにより、プライオリティが最も高い BSR が選定されます。BSR プライオリティが等しい場合は、IP アドレスが最上位の BSR が選定されます。この値の範囲は 0（プライオリティが最小）～ 255 であり、デフォルト値は 64 です。

BSR 候補 RP の引数およびキーワードの設定

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

表 14: 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
<i>interface</i>	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 <i>ip-prefix</i>	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。
<i>interval</i>	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。
<i>priority</i>	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、デフォルト値は 192 です。 (注) この優先度は BSR の BSR 候補の優先度とは異なります。BSR 候補の優先度は 0 ～ 255 の間で、大きい値ほど優先度が高くなります。
bidir	bidir を指定しない場合、現在の RP は ASM モードになります。 bidir を指定した場合は、RP は Bidir モードになります。
route-map <i>policy-name</i>	この機能を適用するグループプレフィックスを定義するルートマップポリシー名です。



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

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

候補 BSR および候補 RP を設定する手順は、次のとおりです。

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

BSR の設定 (PIM)

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip pim bsr {forward [listen] listen [forward]} 例 :	リッスンと転送を設定します。

	コマンドまたはアクション	目的
	<code>switch(config)# ip pim bsr listen forward</code>	リモート PE 上の各 VRF で確実にこのコマンドを入力してください。
ステップ 3	ip pim bsr bsr-candidate interface [hash-len hash-length] [priority priority] 例 : <pre>switch(config)# ip pim bsr-candidate ethernet 2/1 hash-len 24</pre>	候補ブートストラップ ルータ (BSP) を設定します。ブートストラップ メッセージで使用される送信元 IP アドレスは、インターフェイスの IP アドレスです。ハッシュ長は 0 ～ 32 であり、デフォルト値は 30 です。プライオリティは 0 ～ 255 であり、デフォルト値は 64 です。
ステップ 4	ip pim sparse-mode 例 : <pre>switch(config-if)# ip pim sparse-mode</pre>	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	(任意) ip pim bsr rp-candidate interface group-list ip-prefix route-map policy-name priority priority interval interval [bidir] 例 : <pre>switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24</pre>	BSR の候補 RP を設定します。プライオリティは 0 (プライオリティが最大) ～ 65,535 であり、デフォルト値は 192 です。インターバルは 1 ～ 65,535 秒であり、デフォルト値は 60 秒です。 Bidir オプションを使用して Bidir 候補 RP を作成します。 (注) 候補 RP インターバルは 15 秒以上に設定することを推奨します。 この例では、ASM の候補 RP を設定しています。
ステップ 6	(任意) show ip pim group-range [ip-prefix vrf vrf-name] 例 : <pre>switch(config)# show ip pim group-range</pre>	PIM モードとグループ範囲を表示します。
ステップ 7	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Auto-RP の設定

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



(注) Auto-RP は PIM6 ではサポートされていません。



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

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

表 15: Auto-RP マッピング エージェントの引数

引数	説明
<i>interface</i>	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。
<i>scope ttl</i>	RP-Discovery メッセージが転送される最大ホップ数を表す存続可能時間 (TTL) 値。この値の範囲は 1 ～ 255 であり、デフォルト値は 32 です。

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

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

表 16: 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
<i>interface</i>	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 <i>ip-prefix</i>	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。
<i>scope ttl</i>	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。
<i>interval</i>	RP-Announce メッセージの送信間隔 (秒)。この値の範囲は 1 ～ 65,535 であり、デフォルト値は 60 です。 (注) 候補 RP インターバルは 15 秒以上に設定することを推奨します。
bidir	指定しない場合、現在の RP は ASM モードになります。指定した場合、現在の RP は Bidir モードになります。
route-map <i>policy-name</i>	この機能を適用するグループプレフィックスを定義するルートマップ ポリシー名です。



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

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

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

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

自動 RP の設定 (PIM)

始める前に

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

手順の概要

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

手順の詳細

手順

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

	コマンドまたはアクション	目的
ステップ 2	ip pim {send-rp-discovery auto-rp mapping-agent} interface [scope ttl] 例 : <pre>switch(config)# ip pim auto-rp mapping-agent ethernet 2/1</pre>	Auto-RP マッピング エージェントを設定します。 Auto-RP Discovery メッセージで使用される送信元 IP アドレスは、インターフェイスの IP アドレスです。 デフォルト スコープは 32 です。
ステップ 3	ip pim {send-rp-announce auto-rp rp-candidate} interface {group-list ip-prefix prefix-list name route-map policy-name} [scope ttl] interval interval] [bidir] 例 : <pre>switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24</pre>	Auto-RP の候補 RP を設定します。デフォルト スコープは 32 です。デフォルト インターバルは 60 秒です。デフォルトでは、ASM の候補 RP が作成されます。 bidir オプションは、Bidir 候補 RP を構築する場合に使用します。 (注) 候補 RP インターバルは 15 秒以上に設定することを推奨します。 この例では、ASM の候補 RP を設定しています。
ステップ 4	ip pim sparse-mode 例 : <pre>switch(config-if)# ip pim sparse-mode</pre>	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	(任意) show ip pim group-range [ip-prefix vrf vrf-name] 例 : <pre>switch(config)# show ip pim group-range</pre>	PIM モードとグループ範囲を表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

PIM Anycast-RP セットの設定

PIM Anycast-RP セットを設定する手順は、次のとおりです。

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

PIM エニーキャスト RP セットの構成 (PIM)

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 <i>number</i> 例 : <pre>switch(config)# interface loopback 0 switch(config-if)#</pre>	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。

	コマンドまたはアクション	目的
ステップ 3	ip address ip-prefix 例 : <pre>switch(config-if)# ip address 192.168.1.1/32</pre>	このインターフェイスの IP アドレスを設定します。このルータの識別に役立つ一意の IP アドレスになります。
ステップ 4	ip pim sparse-mode 例 : <pre>switch(config-if)# ip pim sparse-mode</pre>	PIM スパース モードをイネーブルにします。
ステップ 5	ip router routing-protocol-configuration 例 : <pre>switch(config-if)# ip router ospf 1 area 0.0.0.0</pre>	エニーキャスト RP セット内の他のルータがインターフェイスに到達できるようにします。
ステップ 6	exit 例 : <pre>switch(config-if)# exit switch(config)#</pre>	インターフェイス コンフィギュレーション モードを終了します。
ステップ 7	interface loopback number 例 : <pre>switch(config)# interface loopback 1 switch(config-if)#</pre>	インターフェイス ループバックを設定します。 この例では、インターフェイス ループバック 1 を設定しています。
ステップ 8	ip address ip-prefix 例 : <pre>switch(config-if)# ip address 10.1.1.1/32</pre>	このインターフェイスの IP アドレスを設定します。これは、エニーキャスト RP アドレスとして機能する共通の IP アドレスである必要があります。
ステップ 9	ip pim sparse-mode 例 : <pre>switch(config-if)# ip pim sparse-mode</pre>	現在のインターフェイスで PIM スパース モードをイネーブルにします。デフォルトではディセーブルになっています。
ステップ 10	ip router routing-protocol-configuration 例 : <pre>switch(config-if)# ip router ospf 1 area 0.0.0.0</pre>	エニーキャスト RP セット内の他のルータがインターフェイスに到達できるようにします。
ステップ 11	exit 例 : <pre>switch(config-if)# exit switch(config)#</pre>	インターフェイス コンフィギュレーション モードを終了します。
ステップ 12	ip pim rp-address anycast-rp-address [group-list ip-address] 例 : <pre>switch(config)# ip pim rp-address 10.1.1.1 group-list 224.0.0.0/4</pre>	PIM エニーキャスト RP アドレスを設定します。

PIM エニーキャスト RP セットの設定 (PIM6)

	コマンドまたはアクション	目的
ステップ 13	ip pim anycast-rp anycast-rp-address anycast-rp-set-router-address 例 : <pre>switch(config)# ip pim anycast-rp 10.1.1.1 192.168.1.1</pre>	指定した Anycast-RP アドレスに対応する PIM Anycast-RP ピア アドレスを設定します。各コマンドで同じ Anycast-RP アドレスを指定して実行すると、Anycast-RP セットが作成されます。RP の IP アドレスは、同一セット内の RP との通信に使用されます。
ステップ 14	RP セットに属する各ピアルータ（ローカルルータを含む）で、同じ Anycast-RP アドレスを使用してステップ 13 を繰り返します。	—
ステップ 15	（任意） show ip pim rp 例 : <pre>switch(config)# show ip pim rp</pre>	PIM RP マッピングを表示します。
ステップ 16	（任意） show ip mroute ip-address 例 : <pre>switch(config)# show ip mroute 239.1.1.1</pre>	mroute エントリを表示します。
ステップ 17	（任意） show ip pim group-range [ip-prefix vrf vrf-name] 例 : <pre>switch(config)# show ip pim group-range</pre>	PIM モードとグループ範囲を表示します。
ステップ 18	（任意） copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

PIM エニーキャスト RP セットの設定 (PIM6)

始める前に

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

手順の概要

1. **configure terminal**
2. **interface loopback number**
3. **ipv6 address ipv6-prefix**
4. **ipv6 pim sparse-mode**
5. **ipv6 router routing-protocol-configuration**
6. **exit**

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 <i>number</i> 例 : <pre>switch(config)# interface loopback 0 switch(config-if)#</pre>	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	ipv6 address <i>ipv6-prefix</i> 例 : <pre>switch(config-if)# ipv6 address 2001:0db8:0:abcd::5/32</pre>	このインターフェイスの IP アドレスを設定します。 このルータの識別に役立つ一意の IP アドレスになります。
ステップ 4	ipv6 pim sparse-mode 例 : <pre>switch(config-if)# ipv6 pim sparse-mode</pre>	PIM6 スパース モードをイネーブルにします。
ステップ 5	ipv6 router <i>routing-protocol-configuration</i> 例 : <pre>switch(config-if)# ipv6 router ospfv3 1 area 0.0.0.0</pre>	エニーキャスト RP セット内の他のルータがインターフェイスに到達できるようにします。
ステップ 6	exit 例 :	インターフェイス コンフィギュレーション モードを終了します。

PIM エニーキャスト RP セットの設定 (PIM6)

	コマンドまたはアクション	目的
	<pre>switch(config-if)# exit switch(config)#</pre>	
ステップ 7	interface loopback number 例 : <pre>switch(config)# interface loopback 1 switch(config-if)#</pre>	インターフェイス ループバックを設定します。 この例では、インターフェイス ループバック 1 を設定しています。
ステップ 8	ipv6 address ipv6-prefix 例 : <pre>switch(config-if)# ipv6 address 2001:0db8:0:abcd::1111/32</pre>	このインターフェイスの IP アドレスを設定します。 これは、エニーキャスト RP アドレスとして機能する共通の IP アドレスである必要があります。
ステップ 9	ipv6 router routing-protocol-configuration 例 : <pre>switch(config-if)# ipv6 router ospfv3 1 area 0.0.0.0</pre>	エニーキャスト RP セット内の他のルータがインターフェイスに到達できるようにします。
ステップ 10	exit 例 : <pre>switch(config-if)# exit switch(config)#</pre>	インターフェイス コンフィギュレーション モードを終了します。
ステップ 11	ipv6 pim rp-address anycast-rp-address [group-list ip-address] 例 : <pre>switch(config)# ipv6 pim rp-address 2001:0db8:0:abcd::1111 group-list ff1e:abcd:def1::0/24</pre>	PIM6 エニーキャスト RP アドレスを設定します。
ステップ 12	ipv6 pim anycast-rp anycast-rp-address anycast-rp-set-router-address 例 : <pre>switch(config)# ipv6 pim anycast-rp 2001:0db8:0:abcd::5 2001:0db8:0:abcd::1111</pre>	指定した Anycast-RP アドレスに対応する PIM6 Anycast-RP ピア アドレスを設定します。各コマンドで同じ Anycast-RP アドレスを指定して実行すると、Anycast-RP セットが作成されます。RP の IP アドレスは、同一セット内の RP との通信に使用されます。
ステップ 13	RP セットに属する各ピアルータ（ローカルルータを含む）で、同じ Anycast-RP アドレスを使用してステップ 13 を繰り返します。	—
ステップ 14	（任意） show ipv6 pim rp 例 : <pre>switch(config)# show ipv6 pim rp</pre>	PIM RP マッピングを表示します。
ステップ 15	（任意） show ipv6 mroute ipv6-address 例 :	mroute エントリを表示します。

	コマンドまたはアクション	目的
	<code>switch(config)# show ipv6 mroute ff1e:2222::1:1:1:1</code>	
ステップ 16	(任意) show ipv6 pim group-range [ipv6-prefix] [vrf vrf-name all] 例: <code>switch(config)# show ipv6 pim group-range</code>	PIM6 モードとグループ範囲を表示します。
ステップ 17	(任意) copy running-config startup-config 例: <code>switch(config)# copy running-config startup-config</code>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ASM 専用の共有ツリーの設定

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



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

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



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

ASM 専用の共有ツリーの設定 (PIM)

始める前に

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

手順の概要

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

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip pim use-shared-tree-only group-list policy-name 例 : <pre>switch(config)# ip pim use-shared-tree-only group-list my_group_policy</pre>	共有ツリーだけを構築します。共有ツリーから SPT へのスイッチオーバーは実行されません。 match ip multicast コマンドで、使用するグループを示すルートマップ ポリシー名を指定します。デフォルトでは、送信元に対する (*, G) ステートのマルチキャスト パケットを受信すると、ソフトウェアは PIM (S, G) Join メッセージを送信元方向に発信します。 コマンドには次の制限があります。 • これは、Cisco Nexus 9000 クラウドスケール スイッチの仮想ポートチャネル (vPC) でのみサポートされます。 • NX-OS (非 vPC) のラスト ホップ ルーター (LHR) 構成でサポートされています。
ステップ 3	(任意) show ip pim group-range [ip-prefix vrf vrf-name] 例 : <pre>switch(config)# show ip pim group-range</pre>	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 : <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

ASM 専用の共有ツリーの設定 (PIM6)

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	ipv6 pim use-shared-tree-only group-list <i>policy-name</i> 例 : <pre>switch(config)# ipv6 pim use-shared-tree-only group-list my_group_policy</pre>	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。 matchipv6 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 ipv6 pim group-range [<i>ipv6-prefix</i> <i>vrf vrf-name</i>] 例 : <pre>switch(config)# show ipv6 pim group-range</pre>	PIM6 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 : <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

SSM (PIM) の設定

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

IPv4 ネットワーク上のホストから、送信元を特定してマルチキャストデータを要求するには、このホストおよびこのホストの DR で、IGMPv3 が実行されている必要があります。SSM モードでインターフェイスに PIM を設定する場合は、IGMPv3 をイネーブルにするのが一般的で

す。IGMPv1 または IGMPv2 が実行されているホストでは、SSM 変換を使用して、グループと送信元のマッピング設定を行うことができます。

SSM で使用される IPv4 グループ範囲のみを設定できます。



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

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch(config)# ip pim ssm range 239.128.1.0/24</pre> 例 : <pre>switch(config)# no ip pim ssm range none</pre>	次のオプションを使用できます。 • prefix-list : SSM 範囲のプレフィックス リスト ポリシー名を指定します。 • range : SSM のグループ範囲を設定します。デフォルトの範囲は 232.0.0.0/8 です。キーワード none を指定すると、すべてのグループ範囲が削除されます。 • route-map : match ip multicast コマンドで、使用するグループ プレフィックスを示すルート マップ ポリシー名を指定できます。 no オプションを指定すると、SSM 範囲から指定のプレフィックスが削除されるか、プレフィックスリ

	コマンドまたはアクション	目的
		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	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

vPC を介した PIM SSM の設定

vPC 上での PIM SSM が、SSM 範囲内で vPC ピア上での IGMPv3 Join と PIM S,G Join をサポートするように設定します。この設定は、レイヤ 2 またはレイヤ 3 ドメインの孤立した送信元または受信者に対してサポートされています。vPC 上で PIM SSM を設定する場合、ランデブーポイント (RP) の設定は必要ありません。

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

始める前に

PIM および vPC 機能が有効なことを確認します。

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch(config)# vrf context Enterprise switch(config-vrf)#</pre>	新しい VRF を作成し、VRF 設定モードを開始します。 <i>name</i> には最大 32 文字の英数字を使用できます。 大文字と小文字は区別されます。
ステップ 3	(任意) [no] ip pim ssm {prefix-list name range {ip-prefix none} route-map policy-name} 例 : <pre>switch(config-vrf)# ip pim ssm range 234.0.0.0/24</pre>	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。 デフォルトでは、SSM グループ範囲は 232.0.0.0/8 です。S,G joins がこの範囲で受信される限り、vPC 上の PIM SSM は機能します。デフォルトを他の範囲で上書きする場合は、このコマンドを使用してその範囲を指定する必要があります。この例のコマンドは、デフォルトの範囲を 234.0.0.0/24 にオーバーライドします。 no オプションを指定すると、SSM 範囲から指定のプレフィックスが削除されるか、プレフィックスリストまたはルートマップポリシーが削除されます。キーワード none を指定すると、no コマンドは SSM 範囲をデフォルト値の 232.0.0.0/8 にリセットします。
ステップ 4	(任意) show ip pim group-range [ip-prefix] [vrf vrf-name all] 例 :	PIM モードとグループ範囲を表示します。

	コマンドまたはアクション	目的
	<code>switch(config-vrf)# show ip pim group-range</code>	
ステップ 5	(任意) copy running-config startup-config 例 : <code>switch(config-vrf)# copy running-config startup-config</code>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

マルチキャスト用 RPF ルートの設定

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

マルチキャスト ルートはトラフィック転送に直接使用されるわけではなく、RPF チェックのために使用されます。マルチキャスト用 RPF ルートは再配布できません。



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



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

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
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 mroute {ip-addr mask ip-prefix} {next-hop nh-prefix interface} [route-preference] [vrf vrf-name] 例 : switch(config)# ip mroute 192.0.2.33/1 224.0.0.0/1	RPF 計算で使用するマルチキャスト用 RPF ルートを設定します。ルート プリファレンスは 1 ～ 255 です。デフォルト プリファレンスは 1 です。
ステップ 3	(任意) show ip static-route [multicast] [vrf vrf-name] 例 : switch(config)# show ip static-route multicast	設定されているスタティックルートを表示します。
ステップ 4	(任意) copy running-config startup-config	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

マルチキャスト マルチパスの設定

デフォルトでは、使用可能な複数の ECMP パスがある場合、マルチキャストの RPF インターフェイスが自動的に選択されます。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
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 resilient s-g-hash} 例 : switch(config)# ip multicast multipath none	次のオプションを使用して、マルチキャストマルチパスを構成します。 • none : URIB RPF ルックアップで複数の ECMP にまたがるハッシュを抑制して、マルチキャストマルチパスを無効にします。このオプションを使用すると、最も高い RPF ネイバー（ネクストホップ）アドレスが RPF インターフェイスに使用されます。

	コマンドまたはアクション	目的
		(注) ip multicast multipath none コマンドを使用して、ハッシュを完全に無効にします。 • s-g-hash : RPF インターフェイスを選択するために、（デフォルトの S/RP、G ベースハッシュではなく）S、G、ネクストホップ ハッシュを開始します。このオプションは、送信元およびグループアドレスに基づいてハッシュを構成します。これがデフォルトの設定です。 • resilient : ECMP パス リストが変更され、古い RPF 情報がまだ ECMP の一部である場合、このオプションは、再ハッシュを実行して潜在的に RPF 情報を変更する代わりに、古い RPF 情報を使用します。ip multicast multipath resilient コマンドは、URIB からのルート到達可能性通知にパスがある場合に、現在の RPF への回復力（スティッキネス）を維持するためのものです。 (注) no ip multicast multipath resilient コマンドは、スティッキネス アルゴリズムを無効にします。このコマンドは、ハッシュ アルゴリズムに依存しません。 (注) X9636C-R または X9636Q-R ライン カード、または C9508-FM-R ファブリック モジュールを備えた Cisco Nexus 9508 スイッチで、resilient オプションから none オプションに変更する場合は、最初に no ip multicast multipath elastic コマンドを入力し、次に、ip multicast multipath none コマンドを入力します。
ステップ 3	clear ip mroute * 例 : <pre>switch(config)# clear ip mroute *</pre>	マルチパス ルートをクリアし、マルチキャスト マルチパス抑制をアクティブにします。

マルチキャスト VRF-Lite ルート リークの設定

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

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 rpf select vrf src-vrf-name group-list group-list 例 : <pre>switch(config)# ip multicast rpf select vrf blue group-list 236.1.0.0/16</pre>	特定のマルチキャスト グループの RPF ルックアップに使用する VRF を指定します。 src-vrf-name は、ソース VRF の名前です。最大 32 文字の英数字で、大文字と小文字が区別されます。 group-list は、RPF のグループ範囲です。形式は A.B.C.D/LEN で、最大長は 32 です。
ステップ 3	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

RP 情報配信を制御するルートマップの設定

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

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



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

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

RP 情報配信を制御するルート マップの設定 (PIM)

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	route-map <i>map-name</i> [permit deny] [<i>sequence-number</i>] 例 : <pre>switch(config)# route-map ASM_only permit 10 switch(config-route-map)#</pre> 例 : <pre>switch(config)# route-map Bidir_only permit 10 switch(config-route-map)#</pre>	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。
ステップ 3	match ip multicast { rp <i>ip-address</i> [rp-type <i>rp-type</i>]} { group <i>ip-prefix</i> } { source <i>source-ip-address</i> }	指定したグループ、RP、および RP タイプを関連付けます。ユーザは RP のタイプ (ASM または Bidir) を指定できます。例で示すとおり、このコンフィギュレーション方法では、グループおよび RP を指定する必要があります。
	例 : <pre>switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type ASM</pre> 例 : <pre>switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type Bidir</pre>	(注) match ip multicast group-range <> CLI では、 route-map の下の group-range コマンドはサポートされていません。
ステップ 4	(任意) show route-map 例 : <pre>switch(config-route-map)# show route-map</pre>	設定済みのルート マップを表示します。

	コマンドまたはアクション	目的
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-route-map)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

RP 情報配信を制御するルート マップの設定 (PIM6)

手順の概要

1. **configure terminal**
2. **route-map map-name [permit | deny] [sequence-number]**
3. **match ipv6 multicast {rp ip-address [rp-type rp-type]} {group ipv6-prefix} {source source-ip-address}**
4. (任意) **show route-map**
5. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	route-map map-name [permit deny] [sequence-number] 例 : <pre>switch(config)# route-map ASM_only permit 10 switch(config-route-map)#</pre>	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。
ステップ 3	match ipv6 multicast {rp ip-address [rp-type rp-type]} {group ipv6-prefix} {source source-ip-address} 例 : <pre>switch(config-route-map)# match ipv6 multicast group ffe:abcd:def1::0/24 rp 2001:0db8:0:abcd::1 rp-type ASM</pre>	指定した グループ、RP、および RP タイプを関連付けます。RP のタイプ (ASM) を指定できます。例で示すとおり、このコンフィギュレーション方法では、グループおよび RP を指定する必要があります。
ステップ 4	(任意) show route-map 例 : <pre>switch(config-route-map)# show route-map</pre>	設定済みのルート マップを表示します。

	コマンドまたはアクション	目的
ステップ 5	(任意) copy running-config startup-config 例 : <pre>switch(config-route-map)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

メッセージ フィルタリングの設定



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

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

表 17: PIM および PIM6 でのメッセージ フィルタリング

メッセージの種類	説明
デバイスにグローバルに適用	
ネイバーの変更の記録	ネイバーのステート変更を通知する Syslog メッセージをイネーブルにします。デフォルトではディセーブルになっています。
PIM Register ポリシー	ルートマップポリシーに基づいて PIM Register メッセージをフィルタリングできるようにします。 ⁴ match ipv6 multicast コマンドを使用して、グループまたはグループと送信元アドレスを指定できます。このポリシーは、RP として動作するルータに適用されます。デフォルトではこの機能がディセーブルになっているため、PIM Register メッセージのフィルタリングは行われません。
BSR 候補 RP ポリシー	ルートマップポリシーに基づく、BSR 候補 RP メッセージのフィルタリングをイネーブルにします。RP とグループ アドレス、およびタイプ (Bidir または ASM) を、 match ip multicast コマンドで指定できます。このコマンドは、BSR の選定対象のルータで使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。 (注) PIM6 は BSR をサポートしていません。

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。 (注) PIM6 は BSR をサポートしていません。
Auto-RP 候補 RP ポリシー	ルートマップ ポリシーに基づく、Auto-RP マッピング エージェントによる Auto-RP アナウンス メッセージのフィルタリングをイネーブルにします。RP、グループ アドレス、およびタイプ (Bidir または ASM) を、match ip multicast コマンドで指定できます。このコマンドは、マッピング エージェントで使用できます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。 (注) PIM6 は、Auto-RP 方式をサポートしていません。
Auto-RP マッピング エージェント ポリシー	ルートマップ ポリシーに基づく、クライアント ルータによる Auto-RP Discovery メッセージのフィルタリングをイネーブルにします。 match ip multicast コマンドで、マッピング エージェント送信元アドレスを指定できます。このコマンドは、Discovery メッセージを受信するクライアント ルータで使用できます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。 (注) PIM6 は、Auto-RP 方式をサポートしていません。
各デバイスのインターフェイスに適用	
Join/Prune ポリシー	ルートマップ ポリシーに基づく、Join/Prune メッセージのフィルタリングをイネーブルにします。 match ip[v6] multicast コマンドで、グループ、グループと送信元、またはグループと RP アドレスを指定できます。デフォルトでは、Join/Prune メッセージはフィルタリングされません。

⁴ ルートマップ ポリシーの設定については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

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

- **jp-policy** コマンドは (S,G)、(*,G)、または (RP,G) を使用できます。
- **register-policy** コマンドは (S,G) または (*,G) を使用できます。

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

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

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

メッセージフィルタリングの設定 (PIM)

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	(任意) ip pim log-neighbor-changes 例 : <pre>switch(config)# ip pim log-neighbor-changes</pre>	ネイバーのステート変更を通知する Syslog メッセージをイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	(任意) ip pim register-policy policy-name 例 : <pre>switch(config)# ip pim register-policy my_register_policy</pre>	ルートマップ ポリシーに基づく、PIM Register メッセージのフィルタリングをイネーブルにします。 match ip multicast コマンドで、グループ アドレスまたはグループと送信元アドレスを指定できます。
ステップ 4	(任意) ip pim bsr rp-candidate-policy policy-name 例 : <pre>switch(config)# ip pim bsr rp-candidate-policy my_bsr_rp_candidate_policy</pre>	ルートマップ ポリシーに基づく、BSR 候補 RP メッセージのフィルタリングをイネーブルにします。 RP とグループ アドレス、およびタイプ (Bidir または ASM) を、 match ip multicast コマンドで指定できます。このコマンドは、BSR の選定対象のルータで使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。
ステップ 5	(任意) ip pim bsr bsr-policy policy-name 例 : <pre>switch(config)# ip pim bsr bsr-policy my_bsr_policy</pre>	ルートマップ ポリシーに基づく、BSR クライアント ルータによる BSR メッセージのフィルタリングをイネーブルにします。 match ip multicast コマンドで、BSR 送信元アドレスを指定できます。このコマンドは、BSR メッセージを受信するクライアント ルータで使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。
ステップ 6	(任意) ip pim auto-rp rp-candidate-policy policy-name 例 : <pre>switch(config)# ip pim auto-rp rp-candidate-policy my_auto_rp_candidate_policy</pre>	ルートマップ ポリシーに基づく、Auto-RP マッピング エージェントによる Auto-RP Announce メッセージのフィルタリングをイネーブルにします。 RP、グループ アドレス、およびタイプ (Bidir または ASM) を、 match ip multicast コマンドで指定できます。このコマンドは、マッピング エージェントで使用できます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。

	コマンドまたはアクション	目的
ステップ 7	(任意) ip pim auto-rp mapping-agent-policy <i>policy-name</i> 例 : <pre>switch(config)# ip pim auto-rp mapping-agent-policy my_auto_rp_mapping_policy</pre>	ルートマップポリシーに基づく、クライアントルータによる Auto-RP Discovery メッセージのフィルタリングをイネーブルにします。 match ip multicast コマンドで、マッピング エージェント送信元アドレスを指定できます。このコマンドは、Discovery メッセージを受信するクライアント ルータで使用できます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。
ステップ 8	interface <i>interface</i> 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	指定したインターフェイスでインターフェイス モードを開始します。
ステップ 9	(任意) ip pim jp-policy <i>policy-name</i> [in out] 例 : <pre>switch(config-if)# ip pim jp-policy my_jp_policy</pre>	ルートマップ ポリシーに基づく、Join/Prune メッセージのフィルタリングをイネーブルにします。 match ip multicast コマンドで、グループ、グループと送信元、またはグループと RP アドレスを指定できます。デフォルトでは、Join/Prune メッセージはフィルタリングされません。
ステップ 10	(任意) show run pim 例 : <pre>switch(config-if)# show run pim</pre>	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 : <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

メッセージフィルタリングの設定 (PIM6)

始める前に

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

手順の概要

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

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	(任意) ipv6 pim log-neighbor-changes 例 : <pre>switch(config)# ipv6 pim log-neighbor-changes</pre>	ネイバーのステート変更を通知する Syslog メッセージをイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	(任意) ipv6 pim register-policy policy-name 例 : <pre>switch(config)# ipv6 pim register-policy my_register_policy interface interfaceEnters interface mode on the specified interface. switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	ルートマップ ポリシーに基づく、PIM Register メッセージのフィルタリングをイネーブルにします。 match ipv6 multicast コマンドで、グループまたはグループと送信元アドレスを指定できます。デフォルトではディセーブルになっています。
ステップ 4	(任意) ipv6 pim jp-policy policy-name [in out] 例 : <pre>switch(config-if)# ipv6 pim jp-policy my_jp_policy</pre>	ルートマップ ポリシーに基づく、join-prune メッセージのフィルタリングをイネーブルにします。 match ipv6 multicast コマンドで、グループ、グループと送信元、またはグループと RP アドレスを指定できます。デフォルトでは、Join/Prune メッセージはフィルタリングされません。 このコマンドは、送信および着信の両方向のメッセージをフィルタリングします。
ステップ 5	(任意) show run pim6 例 : <pre>switch(config-if)# show run pim6</pre>	PIM6 コンフィギュレーション コマンドを表示します。
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

PIM および PIM6 プロセスの再起動

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

PIM または PIM6 を再起動すると、次の処理が実行されます。

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

PIM プロセスの再起動

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	restart pim 例 : <pre>switch# restart pim</pre>	PIM プロセスを再起動します。 （注） 再起動プロセス中にはトラフィック損失が発生する可能性があります。
ステップ 2	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	ip 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	(任意) show running-configuration pim 例 : switch(config)# show running-configuration pim	flush-routes コマンドを含む、PIM 実行コンフィギュレーション情報を示します。
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。

PIM6 プロセスの再起動

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	restart pim6 例 : switch# restart pim6	PIM6 プロセスを再起動します。
ステップ 2	configure terminal 例 : switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	ipv6 pim flush-routes 例 : switch(config)# ipv6 pim flush-routes	PIM6 プロセスの再起動時に、ルートを削除します。 デフォルトでは、ルートはフラッシュされません。
ステップ 4	(任意) show running-configuration pim6 例 : switch(config)# show running-configuration pim6	flush-routes コマンドを含む、PIM6 実行コンフィギュレーション情報を示します。
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。

VRF モードでの PIM の BFD の設定



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



(注) BFD は PIM6 ではサポートされていません。

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
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。

■ インターフェイス モードでの PIM の BFD の設定

	コマンドまたはアクション	目的
	switch# configure terminal switch(config)#	
ステップ 2	vrf context vrf-name 例 : switch# vrf context test switch(config-vrf)#	VRF 設定モードを開始します。
ステップ 3	ip pim bfd 例 : switch(config-vrf)# ip pim bfd	指定された VRF で BFD をイネーブルにします。 (注) グローバル コンフィギュレーション モードで ip pim bfd コマンドを入力して、VRF インスタンス上の BFD をイネーブルにすることもできます。

インターフェイス モードでの PIM の BFD の設定

始める前に

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

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface interface-type 例 : switch(config)# interface ethernet 7/40 switch(config-if)#	インターフェイス設定モードを開始します。

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

マルチキャスト ヘビー テンプレートと拡張ヘビー テンプレートの有効化

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

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

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

始める前に

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



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

手順の概要

1. **configure terminal**
2. **system routing template-name**
3. **vdc vdc-name**
4. **limit-resource m4route-mem [minimum min-value]maximum max-value**
5. **exit**

6. **ip routing multicast mfdm-buffer-route-count size**
7. **ip pim mtu size**
8. **exit**
9. **show system routing mode**
10. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	system routing template-name 例 : <pre>switch(config)# system routing template-multicast-heavy switch(config)# system routing template-multicast-ext-heavy switch(config)# system routing template-dual-stack-mcast</pre>	マルチキャストテンプレートを有効にします。テンプレートとしては、 template-multicast-heavy または template-multicast-ext-heavy または template-dual-stack-mcast が可能です。 template-multicast-heavy または template-multicast-ext-heavy テンプレートを使用する場合は、コマンドを有効にした後にシステムをリロードする必要があります。
ステップ 3	vdc vdc-name 例 : <pre>switch(config)# vdc vdc1</pre>	VDC を指定し、VDC コンフィギュレーションモードを開始します。
ステップ 4	limit-resource m4route-mem [minimum min-value]maximum max-value 例 : <pre>switch(config-vdc)# limit-resource m4route-mem minimum 150 maximum 150</pre>	VDC の IPv4 マルチキャストルートマップメモリリソース制限を設定します。このコマンドを設定した後、スタートアップコンフィギュレーションに保存して、デバイスをリロードします。
ステップ 5	exit 例 : <pre>switch(config-vdc)# exit</pre>	VDC コンフィギュレーションモードを終了します。
ステップ 6	ip routing multicast mfdm-buffer-route-count size 例 : <pre>switch(config)# ip routing multicast mfdm-buffer-route-count 400</pre>	マルチキャスト mfdm バッファルートサイズを設定します。

	コマンドまたはアクション	目的
ステップ 7	ip pim mtu size 例 : <pre>switch(config)# ip pim mtu 1500</pre>	PIM コントロールプレーン トラフィックのフレーム サイズを大きくし、コンバージェンスを向上させます。
ステップ 8	exit 例 : <pre>switch(config)# exit</pre>	グローバル コンフィギュレーション モードを終了します。
ステップ 9	show system routing mode 例 : <pre>switch# show system routing mode Configured System Routing Mode: Multicast Extended Heavy Scale Applied System Routing Mode: Multicast Extended Heavy Scale Switch#</pre>	構成されたルーティングモード：つまりマルチキャスト ヘビーまたはマルチキャスト拡張ヘビーまたはデュアル スタックが表示されます。
ステップ 10	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

PIM および PIM6 設定の検証

PIM および PIM6 の設定情報を表示するには、次の作業のいずれかを行います。PIM の場合はコマンドの **show ip** 形式、PIM6 の場合はコマンドの **show ipv6** 形式を使用します。

コマンド	説明
show ip[v6] mroute [<i>ip-address</i>] [detail summary]	IP または IPv6 マルチキャスト ルーティング テーブルを表示します。 detail オプションは、詳細なルート属性を表示します。 summary オプションは、ルートカウントとパケットレートを表示します。 (注) このコマンドは、マルチキャスト ヘビー テンプレートが有効になっている場合、Cisco Nexus 9300-EX および 9300-FX シリーズ スイッチのマルチキャスト カウンタも表示します。以下のサンプル出力を参照してください。
show ip[v6] pim df [<i>vrf vrf-name</i> all]	各 RP の Designated Forwarder (DF) 情報をインターフェイス別に表示します。
show ip[v6] pim group-range [<i>ip-prefix</i>] [<i>vrf vrf-name</i> all]	学習済みまたは設定済みのグループ範囲およびモードを表示します。同様の情報については、 show ip[v6] pim rp コマンドを参照してください。
show ip[v6] pim interface [<i>interface</i> brief] [<i>vrf vrf-name</i> all]	情報をインターフェイス別に表示します。
show ip[v6] pim neighbor [<i>interface interface</i> <i>ip-prefix</i>] [<i>vrf vrf-name</i> all]	ネイバーをインターフェイス別に表示します。
show ip[v6] pim oif-list group [<i>source</i>] [<i>vrf vrf-name</i> all]	発信インターフェイス (OIF) リスト内のすべてのインターフェイスを表示します。

コマンド	説明
show ip[v6] pim route [<i>source</i> <i>group</i> [<i>source</i>]] [<i>vrf vrf-name</i> all]	各マルチキャストルートの情報を表示します。指定した (S, G) に対して、PIM Join メッセージを受信したインターフェイスなどを表示できます。
show ip[v6] pim rp [<i>ip-prefix</i>] [<i>vrf vrf-name</i> all]	ソフトウェアの既知のランデブーポイント (RP) およびその学習方法と、それらのグループ範囲を表示します。同様の情報については、 show ip[v6] pim group-range コマンドを参照してください。
show ip pim rp-hash group [<i>vrf vrf-name</i> all]	ブートストラップルータ (BSP) RP ハッシュ情報を表示します。

コマンド	説明
<code>show ip [v6] pim config-sanity</code>	

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

統計の表示

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

PIM および PIM6 の統計情報の表示

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



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

コマンド	説明
show ip[v6] pim policy statistics	レジスタ、RP、および Join/Prune メッセージのポリシーについて、ポリシー統計情報を表示します。
show ip[v6] pim statistics [vrf vrf-name]	グローバル統計情報を表示します。

PIM および PIM6 統計情報のクリア

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

コマンド	説明
clear ip[v6] pim interface statistics interface	指定したインターフェイスのカウンタをクリアします。
clear ip[v6] pim policy statistics	レジスタ、RP、およびjoin-prune メッセージポリシーについて、ポリシーカウンタをクリアします。
clear ip[v6] pim statistics [vrf vrf-name]	PIMプロセスで使用されるグローバルカウンタをクリアします。

マルチキャスト サービス リフレクションの設定

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

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

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

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

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

ユニキャストからマルチキャストへの NAT (UM NAT)

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

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

マルチキャスト サービス リフレクションの注意事項と制限事項

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

- マルチキャスト サービス リフレクション機能は Cisco NX-OS リリース 9.3(5) で導入され、Cisco Nexus 9300-FX、FX2、FXP、EX シリーズ スイッチでサポートされています。
- Cisco NX-OS リリース 9.3(5)F 以降、マップ インターフェイスの最大複製の範囲は 1 ～ 40 です。
- Cisco NX-OS リリース 9.3(3)F 以降、マルチキャスト NAT は、Cisco Nexus C9300-GX でサポートされます。
- Cisco NX-OS リリース 10.2(1)F 以降、マルチキャスト NAT は、Cisco Nexus C9300-GX2B でサポートされます。
- Cisco NX-OS リリース 10.1(1)F 以降、NBM を使用したマルチキャスト サービス リフレクションは、Cisco Nexus 9300-FX3、Cisco Nexus C9316D-GX、Cisco Nexus C93600CD-GX、および Cisco Nexus C9364C-GX プラットフォーム スイッチでサポートされています。
- マルチキャスト サービス リフレクション機能は、以下のプラットフォームではサポートされていません
 - クラウド スケール ライン カード搭載の Cisco Nexus 9500 シリーズ スイッチ
 - R シリーズ ライン カード搭載の Cisco Nexus 9500 シリーズ スイッチ
 - Cisco Nexus 3600-R シリーズ スイッチ
 - Cisco Nexus 9200 シリーズ スイッチ
 - Cisco Nexus 9364C スイッチ
- マルチキャスト サービス リフレクション機能は、Protocol Independent Multicast (PIM) スパース モード (ASM または SSM) でのみサポートされます。
- マルチキャスト サービス リフレクション機能は、vPC 環境では機能しません。
- マルチキャストからユニキャストへの NAT は、Cisco NX-OS リリース 10.2(1)F からサポートされています。
- マルチキャストからユニキャストへの NAT 変換は、出力モードでのみサポートされます。

- マルチキャストからユニキャストへの NAT 変換は、Cisco Nexus 9300-FX、FX2 スイッチでサポートされています。
- マルチキャストからユニキャストへの変換は、Cisco NX-OS リリース 10.1(x) ではサポートされていません。
- PIM パッシブ モードでのマルチキャストからユニキャスト NAT への PMN サポート。
- リリース 10.2(2)F から、ユニキャストからマルチキャストへの NAT 変換がサポートされます。
- マルチキャストからマルチキャストおよびユニキャストからユニキャストへの NAT 構成は、同時に同時に行うことはできません。
- ユニキャスト NAT、マルチキャスト NAT、および PBR 機能は、同じデバイスでは同時にサポートされません。
- 出力 NAT 機能は、デフォルトの VRF でのみサポートされ、他の VRF ではサポートされません。
- FEX はサポートされていません。
- NAT ルールが事前変換済み (S1, G1) ペアに設定されている場合、マルチキャスト サービス リフレクション機能は、このペアの非 NAT レシーバーをサポートしません（つまり、出力 NAT は事前変換済み (S, I, G1) レシーバーをサポートするのに対し、入力 NAT はそれらをサポートしません）。変換されていない受信側 OIF は、出力 NAT でサポートされます。
- SVI は、RPF および OIF ではサポートされていません。
- 変換後の出力 NAT グループのサブインターフェイス レシーバーはサポートされていません。
- マルチキャスト サービス リフレクション構成用に選択されたハードウェア ループバックポートは、「リンク ダウン」状態で、SFP が接続されていない物理ポートである必要があります。
- マスク長が 0 ～ 4 の場合、マルチキャスト NAT 変換は行われません。このマスク長の制限は、グループアドレスのみに適用され、送信元アドレスには適用されません。
- Cisco NX-OS リリース 10.2(1q)F 以降、マルチキャスト NAT は Cisco Nexus N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。
- インターフェイスでの IGMP 静的結合の場合、結合を生成するために /24 のグループ範囲マスクが使用されます。送信元マスク長は /32 と見なされます。**ip igmp static** 結合コマンドで結合を生成する際に、送信元マスク長の変動は考慮されません。

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

- 入力 ACL が適用されて、すでに流れている未変換のマルチキャストトラフィックをブロックする場合、(S,G) エントリは削除されません。その理由は、ACL がパケットをドロップ

プしても、マルチキャスト ルート エントリが引き続きトラフィックによってヒットされるためです。

- 出力インターフェイスで変換されたソース トラフィック (S2、G2) をブロックする出力 ACL が適用されている場合、変換されたトラフィックに対して出力 ACL がサポートされていないため、出力 ACL は機能しません。

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

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

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

前提条件

マルチキャスト サービス リフレクション機能には、次の前提条件があります。

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

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

マルチキャスト サービス リフレクションの設定

始める前に

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

手順の概要

1. **configure terminal**
2. **vrf context name**
3. **[no] ip service-reflect source-interface interface-name interface-number**

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

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	vrf context name 例 : <pre>switch(config)# vrf context test switch(config-vrf)#</pre>	新しい VRF を作成し、VRF 設定モードを開始します。 <i>name</i> には最大 32 文字の英数字を使用できます。大文字と小文字は区別されます。NAT ルールは、vrf コンテキストで構成されます。 (注) デフォルト以外の VRF は、出力 NAT ではサポートされていません。

	コマンドまたはアクション	目的
ステップ 3	[no] ip service-reflect source-interface interface-name interface-number 例 : <pre>switch(config-vrf)# ip service-reflect source-interface loopback10</pre>	NAT ソースとしてループバックを設定します。このインターフェイスは、トラフィックを NAT ルーターにプルします。インターフェイスは、変換後のルートの RPF になります。このコマンドは、VRF ごとに設定されます。
ステップ 4	[no] ip service-reflect destination in-grp to out-grp mask-len g-mlen source in-src to out-src mask-len s-mlen [to-udp udp-to-src-port udp-to-dest-port] [to-udp-src-port udp-to-src-port] [to-udp-dest-port udp-to-dest-port] 例 : <pre>switch(config-vrf)# ip service-reflect destination 228.1.1.1 to 238.1.1.1 mask-len 32 source 80.80.80.80 to 90.90.90.90 mask-len 32 to-udp-src-port 500 to-udp-dest-port 600</pre>	入力 NAT の NAT ルールを設定します。
ステップ 5	[no] ip service-reflect mode egress prefix 例 : <pre>switch(config-vrf)# ip service-reflect mode egress 225.1.1.0/24</pre>	出力 NAT モードを設定します。インターフェイスにルーティングされたマルチキャスト パケットを照合し、リライトします。 (注) 出力 NAT は、デフォルトの VRF でのみサポートされます。
ステップ 6	[no] ip service-reflect destination in-grp to out-grp mask-len g-mlen source in-src to out-src mask-len s-mlen [to-udp udp-to-src-port udp-to-dest-port] [to-udp-src-port udp-to-src-port] [to-udp-dest-port udp-to-dest-port] [static-oif out-if] 例 : <pre>switch(config-vrf)# ip service-reflect destination 225.1.1.1 to 227.1.1.1 mask-len 32 source 10.10.10.100 to 20.10.10.101 mask-len 32 to-udp-src-port 33 to-udp-dest-port 66 static-oif Ethernet1/8</pre>	出力 NAT の NAT ルールを設定します。
ステップ 7	[no] multicast service-reflect interface all map interface interface-name max-replication replication 例 : <pre>switch(config-vrf)# multicast service-reflect interface all map interface Ethernet1/54 max-replication 3</pre>	マップ インターフェイスの最大レプリケーション数を指定します。範囲は 1 ～ 40 です。デフォルト値は 40 です。 このコマンドの no 形式は、構成を削除します。
ステップ 8	exit 例 : <pre>switch(config-vrf)# exit switch(config)#</pre>	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	interface interface-name interface-number 例 : <pre>switch(config)# interface loopback10 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 10	ip address prefix 例 : <pre>switch(config-if)# ip address 1.1.1.1/24</pre>	ループバック インターフェイスの IP アドレスを設定します。このルータの識別に役立つ一意の IP アドレスになります。
ステップ 11	ip pim sparse-mode 例 : <pre>switch(config-if)# ip pim sparse-mode</pre>	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 12	ip igmp static-oif {group [source source] route-map policy-name} 例 : <pre>switch(config-if)# ip igmp static-oif 230.1.1.1</pre>	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。 設定されたループバック インターフェイスが NAT 対象のマルチキャスト ストリームに参加できるようにします。
ステップ 13	no system multicast dcs-check 例 : <pre>switch(config-if)# no system multicast dcs-check</pre>	ルート学習のために、非 FHR デバイスの CPU にマルチキャスト パケットをパントできるようにします。これは通常、または の機能が有効になっているときに使用されます。ip pim border-router ip igmp host-proxy このコマンドは、Cisco Nexus 9300 シリーズおよび Cisco Nexus 9200 シリーズの EOR スイッチ、Cisco Nexus 9504 および Cisco Nexus 9508 の EOR および TOR スイッチ、および N3K-C3636C-R、N3K-C36180YC-R TOR スイッチではサポートされていません。
ステップ 14	ip pim border-router 例 : <pre>switch(config-if)# ip pim border-router</pre>	PIM-SM ドメインの外部のソースからのトラフィックがドメイン内の受信者に到達することを確認し、リモートから送信されたトラフィックがこのドメイン内のローカルの受信者に到達できるようにします。

	コマンドまたはアクション	目的
		PIM メッセージが PIM ドメイン境界を通過できない場合は、PIM 境界ルータが必要です。
ステップ 15	nbm external-link 例 : <pre>switch(config-if)# nbm external-link</pre>	マルチサイト ソリューションで複数のファブリックを接続するために、NBM インターフェイスを外部リンクとして設定します。 (注) このコマンドは、機能 NBM が有効になっていて、 ip pim border-router コマンドが有効になっているリンク上でのみ必要です。
ステップ 16	exit 例 : <pre>switch(config-if)# exit switch(config)#</pre>	インターフェイス コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 17	[no] multicast service-reflect interface all map interface interface-name vrf vrf-name 例 : <pre>switch(config)# multicast service-reflect interface all map interface loopback10 vrf test</pre>	すべてのファンアウト インターフェイスをサービス インターフェイスにマッピングします。 (注) vrf vrf-name オプションは、出力 NAT ではサポートされていません。 (注) ステップ 17、18、および 19 のコマンドは、出力 NAT の場合にのみ必要です。Egress NAT ルール構成で使用する各 OIF は、これらのマッピング構成のいずれかを使用して、1つのサービスインターフェイスにマッピングする必要があります。
ステップ 18	[no] multicast service-reflect interface interface-name map interface interface-name vrf vrf-name 例 : <pre>switch(config)# multicast service-reflect interface ethernet1/18 map interface loopback10 vrf test</pre>	ファンアウト インターフェイスからサービス インターフェイスへの 1 対 1 のマッピングを設定します。
ステップ 19	[no] multicast service-reflect interface interface-1, interface-2, interface-3 map interface interface-name vrf vrf-name 例 : <pre>switch(config)# multicast service-reflect interface ethernet 1/1-10, ethernet1/12-14, ethernet1/16 map interface loopback10 vrf test</pre>	ファンアウト インターフェイスからサービス インターフェイスへの 多対 1 のマッピングを設定します。

	コマンドまたはアクション	目的
ステップ 20	exit 例 : switch(config)# exit	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 21	show ip mroute sr 例 : switch# show ip mroute sr	サービス リフレクション mroute エントリを表示します。
ステップ 22	show forwarding distribution multicast route 例 : switch# show forwarding distribution multicast route	出力 NAT の変換前および変換後のルート情報、および入力 NAT の変換前のルート情報に関する情報を表示します。
ステップ 23	show forwarding distribution multicast route group 例 : switch# show forwarding distribution multicast route group	マルチキャスト FIB 配布 IPv4 マルチキャスト ルートに関する情報を表示します。

マルチキャスト サービス リフレクションの設定例

次の例は、マルチキャスト NAT 入出力ポートの設定を示しています。

```

interface loopback0
  ip address 20.1.1.2/24
  ip pim sparse-mode
  ip igmp static-oif 225.1.1.1

hardware access-list tcam region mcast-nat 512

<<Ingress NAT>>

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

<<Egress NAT>>

ip route 30.1.1.0/24 10.1.1.1
ip pim ssm range 232.0.0.0/8
ip service-reflect mode egress 225.1.1.0/24
ip service-reflect destination 225.1.1.1 to 224.1.1.1 mask-len 32 source 30.1.1.1 to 20.1.1.1 mask-len 32 static-oif port-channel40
ip service-reflect destination 225.1.1.1 to 224.1.1.100 mask-len 32 source 30.1.1.1 to 20.1.1.100 mask-len 32 static-oif port-channel40
ip service-reflect destination 225.1.1.1 to 224.1.1.101 mask-len 32 source 30.1.1.1 to 20.1.1.101 mask-len 32 static-oif port-channel40
ip service-reflect destination 235.1.1.1 to 234.1.1.1 mask-len 32 source 30.1.1.70 to 20.1.1.70 mask-len 32

```

```

multicast service-reflect interface all map interface Ethernet1/21
hardware access-list tcam region mcast-nat 512
interface Ethernet1/21
  link loopback
  no shutdown
interface Ethernet1/21.1
  encapsulation dot1q 10
  no shutdown
interface Ethernet1/21.2
  encapsulation dot1q 20
  no shutdown
interface Ethernet1/21.3
  encapsulation dot1q 30
  no shutdown
interface Ethernet1/21.4
  encapsulation dot1q 40
  no shutdown

```

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

```

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

(30.1.1.70/32, 235.1.1.1/32), uptime: 01:05:12, ip mrib pim
  NAT Mode: Ingress
  NAT Route Type: Pre
  Incoming interface: Ethernet1/1, RPF nbr: 10.1.1.1
  Outgoing interface list: (count: 1)
    loopback0, uptime: 01:05:12, mrib
      SR: (20.1.1.70, 234.1.1.1)

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

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

switch# show forwarding distribution multicast route
IPv4 Multicast Routing Table for table-id: 1
Total number of groups: 22
Legend:
  C = Control Route
  D = Drop Route
  G = Local Group (directly connected receivers)
  O = Drop on RPF Fail

```

```

P = Punt to supervisor
L = SRC behind L3
d = Decap Route
Es = Extranet src entry
Er = Extranet recv entry
Nf = VPC None-Forwarder
dm = MVPN Decap Route
em = MVPN Encap Route
IPre = Ingress Service-reflect Pre
EPre = Egress Service-reflect Pre
Pst = Ingress/Egress Service-reflect Post

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

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

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

(20.1.1.101/32, 224.1.1.101/32), RPF Interface: loopback0, flags: Pst
Upstream Nbr: 20.1.1.101
Received Packets: 0 Bytes: 0
Number of Outgoing Interfaces: 1
Outgoing Interface List Index: 2
    port-channel40

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

```

ユニキャストからマルチキャスト NAT へ

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

ユニキャストからマルチキャストへの NAT は、1:1 の変換をサポートします。マルチキャストから別のマルチキャストへの変換がサポートされるチェーン変換。マルチキャストからマルチ

キャストへの変換は、1 対多でサポートされます。変換が機能するためには、ソース IP、ブリおおよびポストがサービス インターフェイス ループバック 上にある必要があります。

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

ユニキャストからマルチキャストへの NAT でサポートされるスケール

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



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

出力 NAT プラットフォーム再循環サービス インターフェイス

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

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

ユニキャストからマルチキャストへの NAT 変換

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

ip service-reflect source-interface <interface>

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

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

MRIB 表示コマンド

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

show ip mroute sr umnat

ユニキャストからマルチキャストへの NAT の設定は次のとおりです。

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

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

ip service-reflect destination 227.1.1.1 to 229.1.1.1
mask-len 32 source 57.1.1.51 to 21.1.1.2
mask-len 32 static-oif Ethernet1/7

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

MFDM Show コマンド

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

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

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

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

MFIB 表示コマンド

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

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

ACLQOS Show コマンド

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

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

ユニキャストからマルチキャストへの NAT 変換ルールの設定

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

```
ip service-reflect destination 1.2.3.4 to 227.1.1.1 mask-len 32 source 21.1.1.1 to
57.1.1.51 mask-len 32 to-udp-src-port 1000 to-udp-dest-port 500
{
  "mribRule": {
    "attributes": {
      "childAction": "",
      "dn":
        "system/forwarding/default/rule/psrp-[1.2.3.4]-postgrp-[227.1.1.1]-gr-32-presrc-[21.1.1.1]-postsrc-[57.1.1.51]-sr-32-srcp-1000-destp-500-oif-[unspecified]",
      "grpMasklen": "32",
      "modTs": "2021-07-24T02:13:54.360+00:00",
      "postTransGrp": "227.1.1.1",
      "postTransSrc": "57.1.1.51",
      "preTransGrp": "1.2.3.4",
      "preTransSrc": "21.1.1.1",
      "srcMasklen": "32",
      "staticOif": "unspecified",
      "status": "",
      "udpDestPort": "500",
      "udpSrcPort": "1000"
    }
  }
}
```

PIM の設定例

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

SSM の設定例

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

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

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

2. SSM をサポートする IGMP のパラメータを設定します。通常は、SSM をサポートするために、PIM インターフェイスに IGMPv3 を設定します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip igmp version 3
```

3. デフォルト範囲を使用しない場合は、SSM 範囲を設定します。

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

4. メッセージフィルタリングを設定します。

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

次に、PIM SSM モードの設定例を示します。

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

PIM SSM over vPC の設定例

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

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

switch1# **show vpc** (primary vPC) --> Shows vPC-related information.

Legend:

(*) - local vPC is down, forwarding via vPC peer-link

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

vPC Peer-link status

id	Port	Status	Active vlans
1	Po1000	up	101-102

vPC status

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

switch2# **show vpc** (secondary vPC)

Legend:

(*) - local vPC is down, forwarding via vPC peer-link

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

vPC Peer-link status

id	Port	Status	Active vlans
1	Po1000	up	101-102

vPC status

id	Port	Status	Consistency	Reason	Active vlans
1	Po1	up	success	success	102

```
2      Po2      up      success      success      101
```

switch1# **show ip igmp snooping group vlan 101** (primary vPC IGMP snooping states) -->
Shows if S,G v3 joins are received and on which VLAN. The same VLAN should be OIF in the MRIB output.

Type: S - Static, D - Dynamic, R - Router port, F - Fabricpath core port

Vlan	Group	Address	Ver	Type	Port list
101	*/*		-	R	Po1000 Vlan101
101	225.1.1.1		v3		
		100.6.160.20		D	Po2

switch2# **show ip igmp snooping group vlan 101** (secondary vPC IGMP snooping states)

Type: S - Static, D - Dynamic, R - Router port, F - Fabricpath core port

Vlan	Group	Address	Ver	Type	Port list
101	*/*		-	R	Po1000 Vlan101
101	225.1.1.1		v3		
		100.6.160.20		D	Po2

switch1# **show ip pim route** (primary vPC PIM route) --> Shows the route information in the PIM protocol.

PIM Routing Table for VRF "default" - 3 entries

```
(10.6.159.20/32, 225.1.1.1/32), expires 00:02:37
  Incoming interface: Ethernet1/19, RPF nbr 10.6.159.20
  Oif-list:           (1) 00000000, timeout-list: (0) 00000000
  Immediate-list:    (1) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list:    (0) 00000000
  Timeout-interval: 2, JP-holdtime round-up: 3
```

```
(100.6.160.20/32, 225.1.1.1/32), expires 00:01:19
  Incoming interface: Vlan102, RPF nbr 100.6.160.20
  Oif-list:           (0) 00000000, timeout-list: (0) 00000000
  Immediate-list:    (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list:    (0) 00000000
  Timeout-interval: 2, JP-holdtime round-up: 3
```

```
(*, 232.0.0.0/8), expires 00:01:19
  Incoming interface: Null0, RPF nbr 0.0.0.0
  Oif-list:           (0) 00000000, timeout-list: (0) 00000000
  Immediate-list:    (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list:    (0) 00000000
  Timeout-interval: 2, JP-holdtime round-up: 3
```

switch2# **show ip pim route** (secondary vPC PIM route)

PIM Routing Table for VRF "default" - 3 entries

```
(10.6.159.20/32, 225.1.1.1/32), expires 00:02:51
  Incoming interface: Vlan102, RPF nbr 100.6.160.100
  Oif-list:           (0) 00000000, timeout-list: (0) 00000000
  Immediate-list:    (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list:    (0) 00000000
  Timeout-interval: 3, JP-holdtime round-up: 3
```

```
(100.6.160.20/32, 225.1.1.1/32), expires 00:02:51
  Incoming interface: Vlan102, RPF nbr 100.6.160.20
  Oif-list:           (0) 00000000, timeout-list: (0) 00000000
  Immediate-list:    (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list:    (0) 00000000
  Timeout-interval: 3, JP-holdtime round-up: 3
```

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

```
switch2# show ip pim route (secondary vPC PIM route)
PIM Routing Table for VRF "default" - 3 entries
```

```
(10.6.159.20/32, 225.1.1.1/32), expires 00:02:29
  Incoming interface: Vlan102, RPF nbr 100.6.160.100
  Oif-list: (0) 00000000, timeout-list: (0) 00000000
  Immediate-list: (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list: (0) 00000000
  Timeout-interval: 3, JP-holdtime round-up: 3
```

```
(100.6.160.20/32, 225.1.1.1/32), expires 00:02:29
  Incoming interface: Vlan102, RPF nbr 100.6.160.20
  Oif-list: (0) 00000000, timeout-list: (0) 00000000
  Immediate-list: (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list: (0) 00000000
  Timeout-interval: 3, JP-holdtime round-up: 3
```

```
(*, 232.0.0.0/8), expires 00:02:29
  Incoming interface: Null0, RPF nbr 0.0.0.0
  Oif-list: (0) 00000000, timeout-list: (0) 00000000
  Immediate-list: (0) 00000000, timeout-list: (0) 00000000
  Sgr-prune-list: (0) 00000000
  Timeout-interval: 3, JP-holdtime round-up: 3
```

```
switch1# show ip mroute (primary vPC MRIB route) --> Shows the IP multicast routing
table.
```

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

```
(10.6.159.20/32, 225.1.1.1/32), uptime: 03:16:40, pim ip
  Incoming interface: Ethernet1/19, RPF nbr: 10.6.159.20
  Outgoing interface list: (count: 1)
    Vlan102, uptime: 03:16:40, pim

(100.6.160.20/32, 225.1.1.1/32), uptime: 03:48:57, igmp ip pim
  Incoming interface: Vlan102, RPF nbr: 100.6.160.20
  Outgoing interface list: (count: 1)
    Vlan101, uptime: 03:48:57, igmp

(*, 232.0.0.0/8), uptime: 6d06h, pim ip
  Incoming interface: Null, RPF nbr: 0.0.0.0
  Outgoing interface list: (count: 0)
```

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

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

```
Total number of routes: 3
Total number of (*,G) routes: 0
Total number of (S,G) routes: 2
Total number of (*,G-prefix) routes: 1
```

```
(10.6.159.20/32, 225.1.1.1/32), uptime: 03:24:28, pim(1) ip(0)
  Data Created: Yes
```

```

VPC Flags
  RPF-Source Forwarder
Stats: 1/51 [Packets/Bytes], 0.000   bps
Stats: Inactive Flow
Incoming interface: Ethernet1/19, RPF nbr: 10.6.159.20
Outgoing interface list: (count: 1)
  Vlan102, uptime: 03:24:28, pim

(100.6.160.20/32, 225.1.1.1/32), uptime: 03:56:45, igmp(1) ip(0) pim(0)
Data Created: Yes
VPC Flags
  RPF-Source Forwarder
Stats: 1/51 [Packets/Bytes], 0.000   bps
Stats: Inactive Flow
Incoming interface: Vlan102, RPF nbr: 100.6.160.20
Outgoing interface list: (count: 1)
  Vlan101, uptime: 03:56:45, igmp (vpc-svi)

(*, 232.0.0.0/8), uptime: 6d06h, pim(0) ip(0)
Data Created: No
Stats: 0/0 [Packets/Bytes], 0.000   bps
Stats: Inactive Flow
Incoming interface: Null, RPF nbr: 0.0.0.0
Outgoing interface list: (count: 0)

switch2# show ip mroute detail (secondary vPC MRIB route)
IP Multicast Routing Table for VRF "default"

Total number of routes: 3
Total number of (*,G) routes: 0
Total number of (S,G) routes: 2
Total number of (*,G-prefix) routes: 1

(10.6.159.20/32, 225.1.1.1/32), uptime: 03:26:24, igmp(1) pim(0) ip(0)
Data Created: Yes
Stats: 1/51 [Packets/Bytes], 0.000   bps
Stats: Inactive Flow
Incoming interface: Vlan102, RPF nbr: 100.6.160.100
Outgoing interface list: (count: 1)
  Ethernet1/17, uptime: 03:26:24, igmp

(100.6.160.20/32, 225.1.1.1/32), uptime: 04:06:32, igmp(1) ip(0) pim(0)
Data Created: Yes
VPC Flags
  RPF-Source Forwarder
Stats: 1/51 [Packets/Bytes], 0.000   bps
Stats: Inactive Flow
Incoming interface: Vlan102, RPF nbr: 100.6.160.20
Outgoing interface list: (count: 1)
  Vlan101, uptime: 04:03:24, igmp (vpc-svi)

(*, 232.0.0.0/8), uptime: 6d06h, pim(0) ip(0)
Data Created: No
Stats: 0/0 [Packets/Bytes], 0.000   bps
Stats: Inactive Flow
Incoming interface: Null, RPF nbr: 0.0.0.0
Outgoing interface list: (count: 0)

```

BSR の設定例

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

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

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

2. ルータが BSR メッセージの受信と転送を行うかどうかを設定します。

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

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

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

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

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

5. メッセージフィルタリングを設定します。

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

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

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

Auto-RP の設定例

Auto-RP メカニズムを使用して Bidir モードで PIM を設定するには、PIM ドメイン内のルータごとに、次の手順を実行します。

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

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

2. ルータが Auto-RP メッセージの受信と転送を行うかどうかを設定します。

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

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

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

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

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

5. メッセージ フィルタリングを設定します。

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

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

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

PIM エニーキャスト RP の設定例

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

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

```
switch# configure terminal
switch(config)# interface ethernet 2/1
```

```
switch(config-if)# ip pim sparse-mode
```

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

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

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

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

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

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

5. メッセージフィルタリングを設定します。

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

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

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

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

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

```

ip pim sparse-mode
exit
ip pim anycast-rp 192.0.2.3 192.0.2.31
ip pim anycast-rp 192.0.2.3 192.0.2.32
ip pim log-neighbor-changes

```

プレフィックスベースおよびルートマップベースの設定

```

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

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

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

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

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

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

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

```

出力

```

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

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

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

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

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

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

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

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

dc3rtg-d2(config-if)# show ip pim group-range
PIM Group-Range Configuration for VRF "default"

```

Group-range	Mode	RP-address	Shared-tree-only range
232.0.0.0/8	ASM	-	-
231.0.0.0/8	ASM	172.21.0.11	-
231.128.0.0/9	ASM	172.21.0.22	-
231.129.0.0/16	ASM	172.21.0.33	-
231.129.128.0/17	Unknown	-	-

関連資料

関連項目	マニュアル タイトル
ACL TCAM リージョン	『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』
VRF の設定	『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』

標準

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

MIB

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



第 6 章

PIM 許可 RP の設定

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

- [はじめに \(167 ページ\)](#)
- [PIM 許可 RP の注意事項と制限事項 \(167 ページ\)](#)
- [PIM 許可 RP に関する情報 \(168 ページ\)](#)
- [PIM-SM の RP の構成 \(169 ページ\)](#)
- [PIM Allow RP の有効化 \(170 ページ\)](#)
- [許可 RP ポリシーに関する情報の表示 \(172 ページ\)](#)

はじめに

この章では、異なるランデブー ポイント (RP) を持つ Protocol Independent Multicast (PIM) Sparse Mode (SM) ドメインを相互接続するために、IPv4 および IPv6 ネットワークで PIM Allow RP 機能を設定する方法について説明します。PIM 許可 RP を使用すると、着信 (*, G) Join を処理し、別の RP が識別されたときに、受信側デバイスが独自の RP を使用して状態を作成し、共有ツリーを構築できるようになります。これにより、受信デバイスは別の RP からの (*, G) Join を受け入れることができます。

PIM 許可 RP の注意事項と制限事項

- PIM 許可 RP は、PIM SM ドメインの接続のみをサポートします。
- PIM 許可 RP はダウンストリーム トラフィックにのみ適用されます。つまり、共有ツリーの構築にのみ適用されます。
- PIM 許可 RP は、ルート マップのみを使用するように制限されています。
- PIM 許可 RP は、Cisco NX-OS リリース 10.2(2)F より前では IPv6 マルチキャストをサポートしていません。
- IPv6 PIM 許可 RP は、Cisco NX-OS リリース 10.2(2)F からサポートされています。

- PIM 許可 RP は、「送信元」を持つ RPM をサポートしていません。PIM 許可 RP PIM 許可 RP に関する情報。
- 存在しない RPM を使用して Allow-RP 設定を追加すると、すべての 結合/プルーニングが拒否されます。
- PERMIT-ALL または DENY-ALL を持つ RPM を使用して Allow-RP 構成を追加すると、すべての結合/プルーニングがそれに応じて受け入れられるか破棄されます。

PIM 許可 RP に関する情報

ランデブー ポイント

ランデブー ポイント (RP) は、デバイスが PIM (Protocol Independent Multicast) スパース モード (SM) で動作している場合にデバイスが実行するロールです。RP が必要になるのは、PIM SM を実行しているネットワークだけです。PIM-SM モデルでは、マルチキャスト データを明示的に要求したアクティブなレシーバを含むネットワーク セグメントだけにトラフィックが転送されます。マルチキャスト データの配信方法は、PIM デンス モード (PIMDM) とは対照的です。PIMDM では、マルチキャスト トラフィックが最初にネットワークのすべてのセグメントにフラッディングされます。ダウンストリーム ネイバーを持たないルータ、または直接レシーバに接続されているルータは、不要なトラフィックをプルーニングします。RP は、マルチキャスト データのソースとレシーバの接点として機能します。PIM SIM ネットワークでは、ソースが RP にトラフィックを送信する必要があります。このトラフィックは、それから共有配信ツリーを下ってレシーバに転送されます。

デフォルトでは、レシーバのファーストホップデバイスがソースを認識すると、ソースに Join メッセージを直接送信し、ソースからレシーバへのソースベースの配信ツリーを作成します。ソースとレシーバ間の最短パス内に RP が配置されていない限り、このソース ツリーに RP は含まれません。ほとんどの場合、ネットワークにおける RP の配置は複雑な判断を必要としません。

デフォルトでは、RP が必要になるのは、ソースおよびレシーバとの新しいセッションを開始する場合だけです。その結果、RP では、トラフィックのフローまたは処理によるオーバーヘッドはほとんど発生しません。PIM バージョン 2 で実行される処理は PIM バージョン 1 よりも少なくなっています。これは、ソースを定期的に RP に登録するだけでステートを作成できるためです。

PIM 許可 RP

ネットワークには、パブリッシャ、コンシューマ、トランスポートの 3 種類があります。多くのパブリッシャ ネットワークはコンテンツを発信でき、多くのコンシューマ ネットワークがそのコンテンツに関心を持つことがあり得ます。サービスプロバイダーが所有および運用するトランスポート ネットワークは、パブリッシャとコンシューマ ネットワークを接続します。

コンシューマとトランスポート ネットワークは、次のように接続されます。特定のグループ範囲またはすべてのグループ範囲 (デフォルトルートと同様) に対して、サービスプロバイダーは、RP-A などの特定のランデブー ポイント (RP) を定義します。コンシューマデバイスからの RP-A のリバース パス転送により、(*, G) Join がトランスポート ネットワークに送信されま

す。同じグループに対して、サービス プロバイダーは、RP-B などの異なる RP を定義できます。RP-B は、G のトランスポート ネットワーク内で共有ツリーを構築するために使用されます。RP-A と RP-B は通常、異なる RP であり、各 RP は異なるグループ範囲に対して定義されます。RFC 4601 では、デバイスが (*, G) Join を受信したとき、(*, G) Join で指定された RP が、受信デバイスが予期するものと異なる場合（不明な RP）、着信 (*, G) Join は無視する必要がありますと定めています。

PIM 許可 RP 機能は、Cisco NX-OS Release 8.4(1) で導入されました。この機能により、受信デバイスは、着信 (*, G) Join が処理されて別の RP が識別されたとき、独自の RP を使用して状態を作成し、共有ツリーを構築できます。これにより、受信デバイスは別の RP からの (*, G) Join を受け入れることができます。ルートマップは、(*, G) join の対象となる RP アドレスまたはグループアドレス（あるいはその両方）を制御するために使用されます。(*, G) join メッセージの RP アドレスとグループアドレスは、ルートマップで指定された RP とグループアドレスと照合されます。

PIM Allow RP は、ダウンストリーム トラフィックにのみ適用されます。

PIM-SM の RP の構成

始める前に

すべてのアクセスリストは、設定作業を開始する前に設定しておく必要があります。アクセスリストの構成方法については、[Cisco Nexus 9000 シリーズ NX-OS セキュリティ構成ガイド](#)の「IP ACL の構成」の章を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します
ステップ 2	interface interface 例 : <pre>switch(config)# interface gigabitethernet 1/0/0 switch(config-if)#</pre>	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。 interface タイプ番号です。
ステップ 3	ip pim sparse-mode 例 : <pre>switch(config-if)# ip pim sparse-mode</pre>	PIM をイネーブルにします。スパースモードを使用する必要があります。
ステップ 4	no shut 例 :	インターフェイスを有効化します。

	コマンドまたはアクション	目的
	<code>switch(config-if)# no shut</code>	
ステップ 5	Exit 例 : <code>switch(config-if)# exit</code>	グローバル コンフィギュレーション モードに戻ります。 IP マルチキャストを使用するすべてのインターフェイスでステップ 3 ~ 5 を繰り返します。
ステップ 6	ip pim rp-address rp-address[group-listip-prefix route-mappolicy-name] 例 : <code>switch(config)# ip pim rp-address 30.2.2.2 group-list 224.0.0.0/4</code>	マルチキャスト グループ範囲に、PIM スタティック RP アドレスを設定します。match ip multicast コマンドで、使用するグループプレフィックスを示すルートマップポリシー名を指定できます。このコマンドは、VRF モードでも使用できます。
ステップ 7	end 例 : <code>Switch (config)# end</code>	ルート マップ構成モードを終了します。
ステップ 8	(任意) show ip pim rp [vrf/rp-address] 例 : <code>switch# show ip pim rp</code>	ネットワークで既知の RP を表示し、ルータが各 RP について学習する方法を示します。
ステップ 9	(任意) show ip mroute 例 : <code>switch# show ip mroute</code>	IP mroute テーブルの内容を表示します。

PIM Allow RP の有効化

次の設定手順では、RPM の組み合わせのいずれかを一度に設定できます。グループのみ、RP のみ、グループ RP、グループ範囲のみです。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル設定モードを開始します。
ステップ 2	route-map map-name permitsequence-numberdeny 例 : <code>switch(config)# route-map mcast-grp permit 10</code>	ルートマップ構成モードを開始します。この構成モードでは、permit キーワードを使用する点に注意してください。

	コマンドまたはアクション	目的
ステップ 3	match ip multicast group group-address 例 : <pre>Switch(config-route-map)# match ip multicast group 224.0.0.0/4</pre>	IP マルチキャスト グループの照合を行います。 (注) 一度に構成できる RPM の組み合わせは、グループのみ、RP のみ、グループ RP、グループ範囲のみのいずれか1つだけです。たとえば、この手順（グループのみ）を構成する場合は、手順 9 に進む必要があります。 これは、以下の手順（手順 4 から手順 8）にも当てはまります。
ステップ 4	match ip multicast group-range {group address_start to group address_end} 例 : <pre>switch(config-route-map) # match ip multicast group-range 230.1.1.1 to 230.1.1.255</pre>	指定されたグループ アドレスとの間で IP マルチキャスト グループ範囲を照合します。
ステップ 5	match ip multicast rprp-address 例 : <pre>switch (config-route-map) # match ip multicast 222.0.0.0/4</pre>	IP マルチキャストと指定された RP を照合します。
ステップ 6	match ip multicast rp rp-addressrp-type type 例 : <pre>switch (config-route-map)# match ip multicast rp 1.1.1.1/32 rp-type ASM</pre>	IP マルチキャスト RP アドレスと指定された RP タイプを照合します。サポートされている RP タイプは ASM のみです。
ステップ 7	match ip multicast group addressrpaddress 例 : <pre>switch(config-route-map)# match ip multicast group 230.1.1.1/4 rp 1.1.1.1/32</pre>	IP マルチキャスト グループ アドレスと RP アドレスを照合します。
ステップ 8	match ip multicast group-range {group address_start to group address_end}rpaddress 例 : <pre>switch (config-route-map)# match ip multicast group-range 230.1.1.1 to 230.1.1.255 rp 1.1.1.1/32</pre>	指定されたアドレスと RP アドレスとの間で IP マルチキャスト グループ範囲を照合します。
ステップ 9	ip pim allow-rp route-map-name 例 : <pre>switch(config-route-map)# ip pim allow-rp test-route-map</pre>	PIM Allow RP を有効にします。スパスモードの RP アドレスを許可します。このコマンドは、VRF レベルでも構成されます。ルート マップは、(*,G) join の対象となる RP アドレスまたはグループ アドレス（あるいはその両方）を制御するために使用されます。(*,G) join メッセージの RP アドレスとグ

	コマンドまたはアクション	目的
		ループアドレスは、ルートマップで指定された RP とグループアドレスと照合されます。
ステップ 10	ipv6 pim allow-rp route-map-name 例： switch(config-route-map)# ipv6 pim allow-rp test-route-map	IPv6 PIM Allow RP を有効にします。
ステップ 11	(任意) show ip pim policy statistics allow-rp-policy show ipv6 pim policy statistics allow-rp-policy 例： switch(config)# show ip pim policy statistics allow-rp-policy	ポリシー統計を表示するには、次の手順に従います。
ステップ 12	end 例： Switch (config-route-map)# end	ルート マップ構成モードを終了します。

許可 RP ポリシーに関する情報の表示

次のコマンドは、VRF モードでも使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Enable 例： switch# enable	特権 EXEC モードを有効にします。
ステップ 2	show ip pim policy statistics allow-rp-policy 例： switch# show ip pim policy statistics allow-rp-policy	現在の許可 RP ポリシーとそのカウンタに関する統計を表示します。
ステップ 3	show ipv6 pim policy statistics allow-rp-policy 例： switch# show ipv6 pim policy statistics allow-rp-policy	現在の許可 RP ポリシーに関する IPv6 統計を表示します。
ステップ 4	clear ip pim policy statistics allow-rp-policy 例：	許可 RP ポリシーのポリシーとカウンタをクリアします。

	コマンドまたはアクション	目的
	<pre>switch# clear ip pim policy statistics allow-rp-policy</pre>	
ステップ 5	clear ipv6 pim policy statistics allow-rp-policy 例 : <pre>switch# clear ipv6 pim policy statistics allow-rp-policy</pre>	IPv6 の許可 RP ポリシーのポリシーとカウンタをクリアします。



第 7 章

IGMP スヌーピングの構成

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

- [IGMP スヌーピングについて（175 ページ）](#)
- [IGMP スヌーピングの前提条件（178 ページ）](#)
- [IGMP スヌーピングに関する注意事項と制限事項（178 ページ）](#)
- [デフォルト設定（180 ページ）](#)
- [IGMP スヌーピング パラメータの設定（180 ページ）](#)
- [IGMP スヌーピング設定の確認（188 ページ）](#)
- [IGMP スヌーピング統計情報の表示（188 ページ）](#)
- [IGMP スヌーピング統計情報のクリア（189 ページ）](#)
- [IGMP スヌーピングの設定例（189 ページ）](#)

IGMP スヌーピングについて

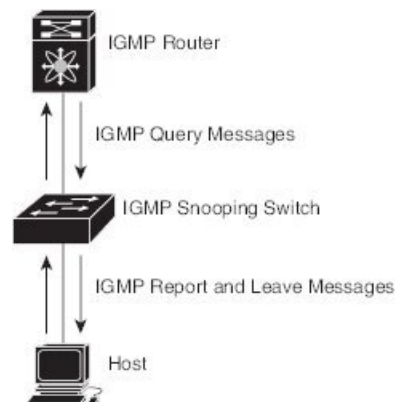


- (注) デバイスの IGMP スヌーピングはディセーブルにしないことを推奨します。IGMP スヌーピングをディセーブルにすると、デバイス内で誤ったフラッドイングが過度に発生し、マルチキャストのパフォーマンスが低下する場合があります。

IGMP スヌーピング ソフトウェアは、VLAN 内のレイヤ 2 IP マルチキャスト トラフィックを調べて、該当する受信側が入っているポートを検出します。IGMP スヌーピングではポート情報を利用することにより、マルチアクセス LAN 環境における帯域幅消費量を削減し、VLAN 全体へのフラッドイングを回避します。IGMP スヌーピングは、マルチキャスト対応ルータに接続されたポートを追跡して、ルータによる IGMP メンバシップレポートの転送機能を強化します。トポロジの変更通知には、IGMP スヌーピング ソフトウェアが応答します。デバイスでは、IGMP スヌーピングがデフォルトでイネーブルになっています。

この図に、ホストと IGMP ルータ間に設置された IGMP スヌーピング スイッチを示します。IGMP スヌーピング スイッチは、IGMP メンバ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 15: IGMP スヌーピング スイッチ



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

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

- 宛先および送信元の IP アドレスに基づいたマルチキャスト パケットの転送が可能な送信元フィルタリング
- MAC アドレスではなく、IP アドレスに基づいたマルチキャスト転送
- MAC アドレスに基づいた代わりのマルチキャスト転送

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

IGMPv1 および IGMPv2

IGMPv1 と IGMPv2 は両方とも、メンバーシップ レポート抑制をサポートします。つまり、同一サブネット上の 2 つのホストが同一グループのマルチキャスト データを受信する場合、他方のホストからメンバー レポートを受信するホストは、そのレポートを送信しません。メンバーシップ レポート抑制は、同じポートを共有しているホスト間で発生します。

各 VLAN スイッチ ポートに接続されているホストが 1 つしかない場合は、IGMPv2 の高速脱退機能を設定できます。高速脱退機能を使用すると、最終メンバ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 での IGMPv3 スヌーピングの実装では完全な IGMPv3 スヌーピングがサポートされています。これにより、IGMPv3 レポートの (S、G) 情報に基づいて、抑制されたフラグディングが提供されます。この送信元ベースのフィルタリングにより、デバイスは対象のマルチキャストグループにトラフィックを送信する送信元に基づいて、マルチキャストトラフィックの宛先ポートを制限できます。

ソフトウェアのデフォルト設定では、各 VLAN ポートに接続されたホストが追跡されます。この明示的な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。IGMPv3 ではすべてのホストがメンバーシップレポートを送信するため、レポート抑制機能を利用すると、デバイスから他のマルチキャスト対応ルータに送信されるトラフィック量を制限できます。レポート抑制をイネーブルにすると、過去にいずれの IGMPv1 ホストまたは IGMPv2 ホストからも対象のグループへの要求がなかった場合には、プロキシレポートが作成されます。プロキシ機能により、ダウンストリームホストが送信するメンバーシップレポートからグループステートが構築され、アップストリーム クエリアからのクエリーに応答するためにメンバーシップレポートが生成されます。

IGMPv3 メンバーシップレポートには LAN セグメント上のグループ メンバの一覧が含まれていますが、最終ホストが脱退すると、メンバーシップクエリーが送信されます。最終メンバ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あるために、Protocol-Independent Multicast (PIM) がインターフェイス上でディセーブルになっている場合は、メンバーシップクエリーを送信するように IGMP スヌーピング クエリアを設定する必要があります。このクエリアは、マルチキャスト送信元と受信者を含み、その他のアクティブ クエリアを含まない VLAN で定義します。

VLAN で任意の IP アドレスを使用するようにクエリアを設定できます。

ベスト プラクティスとして、簡単にクエリアを参照できるようにするには、一意の IP アドレス (スイッチ インターフェイスまたはホット スタンバイ ルータ プロトコル (HSRP) 仮想 IP アドレスでまだ使用されていないもの) を設定する必要があります。



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

IGMP スヌーピング クエリアがイネーブルな場合は、定期的に IGMP クエリーが送信されるため、IP マルチキャスト トラフィックを要求するホストから IGMP レポート メッセージが発信されます。IGMP スヌーピングはこれらの IGMP レポートを待ち受けて、適切な転送を確立します。

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

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

仮想化のサポート

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

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

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

IGMP スヌーピングの前提条件

IGMP スヌーピングには、次の前提条件が適用されます。

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

IGMP スヌーピングに関する注意事項と制限事項

IGMP 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 9000 シリーズ スイッチは、IPv4 の IGMP スヌーピングをサポートしていますが、IPv6 の MLD スヌーピングはサポートしていません。
- PVLAN の IGMP スヌーピングはサポートされていません。
- 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 でフラッドされます。
- N9K-X9636C-R、N9K-X9636Q-R、および N9K-X9636C-RX ラインカードを搭載した Cisco Nexus 9508 および 9504 プラットフォーム スイッチは、vPC での IGMP スヌーピングをサポートします。

- IGMP スヌーピング設定は、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 vlan <id>** コマンドを使用します。
- Cisco NX-OS リリース 7.0(3)I3(1) より前のリリースで、vPC ピアを設定している場合、2 台のデバイス間の IGMP スヌーピング設定オプションに相違があると、次のような結果になります。
 - 一方のデバイスで IGMP スヌーピングを有効にして、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グディングします。
 - マルチキャスト ルータまたはスタティック グループの設定の相違は、トラフィック損失の原因になり得ます。
 - 高速脱退、明示的な追跡、およびレポート抑制のオプションをトラフィックの転送に使用する場合、これらのオプションに相違が生じる可能性があります。
 - デバイス間でクエリー パラメータが異なると、一方のデバイスではマルチキャスト ステートが期限切れとなり、もう一方のデバイスでは転送が継続されます。この相違によって、トラフィック損失または転送の長時間化が発生します。
 - IGMP スヌーピング クエリアを両方のデバイスで設定している場合、クエリーがトラフィックで確認されると、IGMP スヌーピング クエリアはシャットダウンするので、一方のクエリアだけがアクティブになります。
 - **ip igmp snooping group-timeout** を有効にする必要があります **ip igmp snooping proxy general-queries** を使用する場合のコマンドを参照してください。これを「never」に設定することをお勧めします。そのように設定しないと、マルチキャスト パケットが損失する場合があります。
 - 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 **l2l** インデックスを使用します。その結果、両方のマルチキャスト ルーター ポート (レイヤ 2 トランク) が VLAN X と VLAN Y の両方を伝送する場合、VLAN X のトラフィックは VLAN X と VLAN Y の両方のマルチキャスト ルーター ポートに送信されます。
 - インターフェイスに静的にバインドされているマルチキャスト グループを拒否するように ルート マップを変更する場合。その後の IGMP レポートはローカル グループによって拒否され、グループはエージングを始めます。グループへの IGMP 脱退メッセージは、影響を与えることなく許可されます。これは既知の予期された動作です。

デフォルト設定

パラメータ	デフォルト
IGMP スヌーピング	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
Optimise-multicast-flood	無効
デバイス全体での IGMPv3 レポート抑制	無効
VLAN ごとの IGMPv3 レポート抑制	有効 (Enabled)

IGMP スヌーピング パラメータの設定



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



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

グローバル IGMP スヌーピング パラメータの設定

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

IGMP スヌーピング パラメータの注記

- IGMP スヌーピング プロキシ パラメータ

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

IGMP 一般クエリーをすべてのスイッチ ポートにフラッディングする代わりに、マルチキャスト ルータからの一般クエリーを消費するようにデバイスを設定できます。デバイスが一般クエリーを受信すると、現在アクティブなすべてのグループに対してプロキシ レポートを生成し、ルータのクエリーで指定された MRT で指定されている期間でプロキシ レポートを配布します。同時に、マルチキャスト ルータの定期的な一般クエリーのアクティビティに関係なく、デバイスは、ラウンドロビン方式で VLAN の各ポート上に IGMP 一般クエリーを送信します。これは、次の式によって算出されるレートで VLAN のすべてのインターフェイスを順に処理します。

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

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

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



(注) このオプションを使用する場合は、**ip igmp snooping group-timeout** を変更する必要があります。パラメータを高い値に設定するか、タイムアウトしないようにします。

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

- IGMP スヌーピング グループ タイムアウト パラメータ

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

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

手順

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 次のコマンドを使用して、グローバル IGMP スヌーピング パラメータを設定します。

オプション	説明
ip igmp snooping <pre>switch(config)# ip igmp snooping</pre>	デバイスの IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。 (注) このコマンドの no 形式により、グローバル設定がディセーブルになっている場合は、個々の VLAN で IGMP スヌーピングがイネーブルであるかどうかに関係なく、すべての VLAN で IGMP スヌーピングがディセーブルになります。IGMP スヌーピングをディセーブルにすると、レイヤ 2 マルチキャストフレームがすべてのモジュールにフラッディングします。
ip igmp snooping event-history <pre>switch(config)# ip igmp snooping event-history</pre>	イベント履歴バッファのサイズを設定します。デフォルトは small です。
ip igmp snooping group-timeout {minutes never } <pre>switch(config)# ip igmp snooping group-timeout never</pre>	デバイス上のすべての VLAN のグループメンバーシップタイムアウト値を設定します。
ip igmp snooping link-local-groups-suppression <pre>switch(config)# ip igmp snooping link-local-groups-suppression</pre>	デバイス全体のリンクローカル グループ抑制を構成します。デフォルトではイネーブルになっています。
ip igmp snooping proxy general-inquiries [mrt seconds] <pre>switch(config)# ip igmp snooping proxy general-inquiries</pre>	デバイスの IGMP スヌーピングプロキシを設定します。デフォルトは 5 秒です。

オプション	説明
ip igmp snooping v3-report-suppression <pre>switch(config)# ip igmp snooping v3-report-suppression</pre>	マルチキャスト対応ルータに送信されるメンバシップ レポート トラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。
ip igmp snooping report-suppression <pre>switch(config)# ip igmp snooping report-suppression</pre>	IGMPv3 レポート抑制およびプロキシレポートを設定します。デフォルトではディセーブルになっています。

ステップ 3 copy running-config startup-config

例：

```
switch(config)# copy running-config startup-config
```

(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

VLAN ごとの IGMP スヌーピング パラメータの設定

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



(注) このコンフィギュレーション モードを使用して目的の IGMP スヌーピング パラメータを設定します。ただし、この設定は指定した VLAN を明示的に作成した後にのみ適用されます。VLAN の作成については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

手順

ステップ 1 configure terminal

例：

```
switch# configure terminal
switch(config)#
```

グローバル コンフィギュレーション モードを開始します。

ステップ 2 ip igmp snooping

例：

```
switch(config)# ip igmp snooping
```

IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。

(注)

このコマンドの **no** 形式により、グローバル設定がディセーブルになっている場合は、個々の VLAN で IGMP スヌーピングがイネーブルであるかどうかに関係なく、すべての VLAN で IGMP スヌーピングがディセーブルになります。IGMP スヌーピングをディセーブルにすると、レイヤ 2 マルチキャストフレームがすべてのモジュールにフラッディングします。

ステップ 3 vlan configuration vlan-id

例：

```
switch(config)# vlan configuration 2
switch(config-vlan-config)#
```

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

ステップ 4 次のコマンドを使用して、VLAN ごとの IGMP スヌーピング パラメータを設定します。

オプション	説明
ip igmp snooping <pre>switch(config-vlan-config)# ip igmp snooping</pre>	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 {prefix-list route-map} <i>policy-name</i> interface <i>interface</i> <i>slot/port</i> <pre>switch(config-vlan-config)# ip igmp snooping access-group prefix-list plist interface ethernet 2/2</pre>	プレフィックス リストまたはルート マップ ポリシーに基づいて、IGMP スヌーピング レポートにフィルタを設定します。デフォルトではディセーブルになっています。 (注) Cisco NX-OS リリース 7.0(3)F3(3) 以降、N9K-X9636C-R、N9K-X9636C-RX、および N9K-X9636Q-R ラインカードを備えた Cisco Nexus 9508 スイッチは、このコマンドをサポートします。
ip igmp snooping explicit-tracking <pre>switch(config-vlan-config)# ip igmp snooping explicit-tracking</pre>	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	IGMPv2 プロトコルのホスト レポート抑制メカニズムのために、明示的に追跡できない IGMPv2 ホストをサポートします。

オプション	説明
<code>switch(config-vlan-config)# ip igmp snooping fast-leave</code>	高速脱退がイネーブルの場合、IGMP ソフトウェアは、各 VLAN ポートに接続されたホストが 1 つだけであると見なします。デフォルトは、すべての VLAN でディセーブルです。
ip igmp snooping group-timeout <code>{minutes never}</code> <code>switch(config-vlan-config)# ip igmp snooping group-timeout never</code>	指定した VLAN のグループ メンバーシップ タイムアウトを設定します。
ip igmp snooping last-member-query-interval 秒 <code>switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3</code>	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。
ip igmp snooping proxy general-queries [mrt seconds] <code>switch(config-vlan-config)# ip igmp snooping proxy general-queries</code>	指定した VLAN の IGMP スヌーピング プロキシを設定します。デフォルトは 5 秒です。
[no] ip igmp snooping proxy-leave use-group-address <code>switch(config-vlan-config)# ip igmp snooping proxy-leave use-group-address</code>	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。
ip igmp snooping querier <code>ip-address</code> <code>switch(config-vlan-config)# ip igmp snooping querier 172.20.52.106</code>	マルチキャストトラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、スヌーピング クエリアを設定します。IP アドレスは、メッセージの送信元として使用します。
ip igmp snooping querier-timeout 秒 <code>switch(config-vlan-config)# ip igmp snooping querier-timeout 300</code>	マルチキャストトラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合の、IGMPv2 のスヌーピング クエリア タイムアウト値を設定します。デフォルト値は 255 秒です。

VLAN ごとの IGMP スヌーピング パラメータの設定

オプション	説明
ip igmp snooping query-interval 秒 <pre>switch(config-vlan-config)# ip igmp snooping query-interval 120</pre>	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、スヌーピング クエリー インターバルを設定します。デフォルト値は 125 秒です。
ip igmp snooping query-max-response-time 秒 <pre>switch(config-vlan-config)# ip igmp snooping query-max-response-time 12</pre>	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、クエリー メッセージのスヌーピング MRT を設定します。デフォルト値は 10 秒です。
[no] ip igmp snooping report-flood {all interface ethernet slot/port} <pre>switch(config-vlan-config)# ip igmp snooping report-flood interface ethernet 1/2 ip igmp snooping report-flood interface ethernet 1/3</pre>	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。 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。
ip igmp snooping report-policy {prefix-list route-map} <i>policy-name interface interface slot/port</i> <pre>switch(config-vlan-config)# ip igmp snooping report-policy route-map rmap interface ethernet 2/4</pre>	プレフィックス リストまたはルート マップ ポリシーに基づいて、IGMP スヌーピング レポートにフィルタを設定します。デフォルトではディセーブルになっています。
ip igmp snooping startup-query-count <i>value</i> <pre>switch(config-vlan-config)# ip igmp snooping startup-query-count 5</pre>	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、起動時に送信されるクエリー数に対してスヌーピングを設定します。
ip igmp snooping startup-query-interval 秒 <pre>switch(config-vlan-config)# ip igmp snooping startup-query-interval 15000</pre>	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、起動時のスヌーピング クエリー インターバルを設定します。

オプション	説明
ip igmp snooping robustness-variable <i>value</i> <pre>switch(config-vlan-config)# ip igmp snooping robustness-variable 5</pre>	指定した VLAN のロバストネス値を設定します。デフォルト値は 2 です。
ip igmp snooping report-suppression <pre>switch(config-vlan-config)# ip igmp snooping report-suppression</pre>	マルチキャスト対応ルータに送信されるメンバシップ レポートトラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。
ip igmp snooping mrouter interface <i>interface</i> <pre>switch(config-vlan-config)# ip igmp snooping mrouter interface ethernet 2/1</pre>	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 <i>group-ip-addr</i> [source <i>source-ip-addr</i>] interface <i>interface</i> <pre>switch(config-vlan-config)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1</pre>	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 <pre>switch(config-vlan-config)# ip igmp snooping link-local-groups-suppression</pre>	指定した VLAN のリンクローカル グループ抑制を設定します。デフォルトではイネーブルになっています。
ip igmp snooping v3-report-suppression <pre>switch(config-vlan-config)# ip igmp snooping v3-report-suppression</pre>	指定した VLAN の IGMPv3 レポート抑制およびプロキシ レポートを設定します。デフォルトでは VLAN ごとに有効になっています。
ip igmp snooping version <i>value</i> <pre>switch(config-vlan-config)# ip igmp snooping version 2</pre>	指定した VLAN の IGMP バージョン番号を設定します。

ステップ 5 copy running-config startup-config

例：

```
switch(config)# copy running-config startup-config
```

(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

IGMP スヌーピング設定の確認

コマンド	説明
show ip igmp snooping [vlan vlan-id]	IGMP スヌーピング設定を VLAN 別に表示します。
show ip igmp snooping groups [source [group] group [source]] [vlan vlan-id] [detail]	グループに関する IGMP スヌーピング情報を VLAN 別に表示します。
show ip igmp snooping querier [vlan vlan-id]	IGMP スヌーピング クエリアを VLAN 別に表示します。
show ip igmp snooping mroute [vlan vlan-id]	マルチキャスト ルータ ポートを VLAN 別に表示します。
show ip igmp snooping explicit-tracking [vlan vlan-id] [detail]	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。 (注) vPC VLAN の場合、 detail キーワードを入力して、Cisco NX-OS リリース 7.0(3)I7(1) 以降の両方の vPC ピア スイッチでこのコマンドを表示する必要があります。 detail キーワードを入力しなかった場合、このコマンドはネイティブ レポートを受信した vPC スイッチにのみ表示されます。

IGMP スヌーピング統計情報の表示

次のコマンドを使用して、IGMP スヌーピング統計情報を表示できます。

コマンド	説明
show ip igmp snooping statistics vlan	IGMP スヌーピング統計情報を表示します。この出力で、仮想ポートチャネル (vPC) の統計情報を確認できます。

コマンド	説明
show ip igmp snooping {report-policy access-group} statistics [vlan vlan]	IGMP スヌーピングのフィルタが設定されている場合、VLAN ごとに詳細な統計情報を表示します。

IGMP スヌーピング統計情報のクリア

次のコマンドを使用して、IGMP スヌーピング統計情報をクリアできます。

コマンド	説明
clear ip igmp snooping statistics vlan	IGMP スヌーピングの統計情報をクリアします。
clear ip igmp snooping {report-policy access-group} statistics [vlan vlan]	IGMP スヌーピング フィルタの統計情報をクリアします。

IGMP スヌーピングの設定例



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

次に、IGMP スヌーピング パラメータを設定する例を示します。

```
config t
ip igmp snooping
vlan configuration 2
ip igmp snooping
ip igmp snooping explicit-tracking
ip igmp snooping fast-leave
ip igmp snooping last-member-query-interval 3
ip igmp snooping querier 172.20.52.106
ip igmp snooping report-suppression
ip igmp snooping mrouter interface ethernet 2/1
ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
ip igmp snooping link-local-groups-suppression
ip igmp snooping v3-report-suppression
```

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

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

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

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

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

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

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

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



第 8 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 \(191 ページ\)](#)
- [MSDP の前提条件 \(194 ページ\)](#)
- [デフォルト設定 \(194 ページ\)](#)
- [MSDP の設定 \(194 ページ\)](#)
- [MSDP の設定の確認 \(204 ページ\)](#)
- [MSDP のモニタリング \(204 ページ\)](#)
- [MSDP の設定例 \(205 ページ\)](#)
- [関連資料 \(206 ページ\)](#)
- [標準 \(207 ページ\)](#)

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。

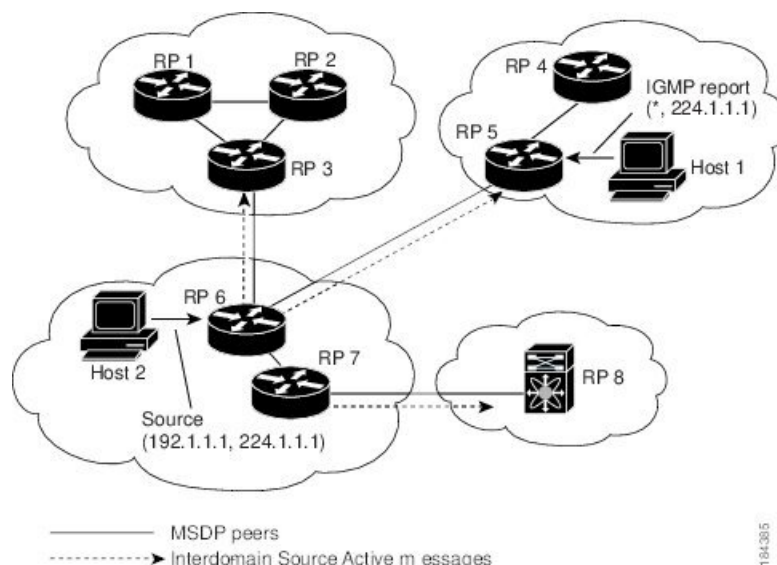
MSDP は、すべての Cisco Nexus 9000 シリーズスイッチでサポートされています。

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し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、RP6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RP3およびRP5は、MSDPピアにSAメッセージを転送します。RP5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 16: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、RP1、RP2、RP3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) を使用する場合は、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するグループ 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 フラッドイングと呼ばれます。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 フラッドイングで生成される 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 18: 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 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch# feature msdp</pre>	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。

	コマンドまたはアクション	目的
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。
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 :	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。

	コマンドまたはアクション	目的
	switch(config)# ip msdp peer 192.168.1.10 connect-source ethernet 2/1 remote-as 8	す。インターフェイスは <i>type slot/port</i> という形式で表します。AS 番号がローカル AS と同じ場合、対象のピアは PIM ドメイン内にあります。それ以外の場合、対象のピアは PIM ドメインの外部にあります。デフォルトでは、MSDP ピアリングはディセーブルになっています。 (注) このコマンドを使用すると、MSDP ピアリングがイネーブルになります。
ステップ 3	ピア IP アドレス、インターフェイス、および AS 番号を必要に応じて変更し、各 MSDP ピアリング関係についてステップ 2 を繰り返します。	—
ステップ 4	(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 19: MSDP ピア パラメータ

パラメータ	説明
説明	ピアの説明を示すストリング。デフォルトでは、ピアの説明は設定されていません。
管理シャットダウン	MSDP ピアをシャットダウンするパラメータ。コンフィギュレーションの設定はこのコマンドの影響を受けません。このパラメータを使用すると、ピアがアクティブになる前に、複数のパラメータ設定を有効にできます。シャットダウンを実行すると、その他のピアとの TCP 接続は強制終了されます。デフォルトでは、各ピアは定義した時点でイネーブルになります。

パラメータ	説明
MD5 パスワード	ピアの認証に使用される MD5 共有パスワードキー。デフォルトでは、MD5 パスワードはディセーブルになっています。
SA ポリシー (IN)	着信 SA メッセージのルートマップポリシー。デフォルトでは、すべての SA メッセージが受信されます。 (注) ルートマップポリシーの設定方法については、 <i>Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide</i> 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、 <i>Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide</i> 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) **show ip msdp peer [peer-address] [vrf [vrf-name | all]]**
9. (任意) **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch(config)# ip msdp description 192.168.1.10 peer in Engineering network</pre>	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 : <pre>switch(config)# ip msdp shutdown 192.168.1.10</pre>	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 : <pre>switch(config)# ip msdp password 192.168.1.10 my_md5_password</pre>	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 : <pre>switch(config)# ip msdp sa-policy 192.168.1.10 my_incoming_sa_policy in</pre>	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 : <pre>switch(config)# ip msdp sa-policy 192.168.1.10 my_outgoing_sa_policy out</pre>	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 : <pre>switch(config)# ip msdp sa-limit 192.168.1.10 5000</pre>	ピアから受信可能な (S,G) エントリ数の上限を設定します。デフォルトでは、上限はありません。
ステップ 8	(任意) show ip msdp peer [peer-address] [vrf [vrf-name all]] 例 : <pre>switch(config)# show ip msdp peer 192.168.1.10</pre>	MSDP ピアの詳細情報を表示します。

	コマンドまたはアクション	目的
ステップ 9	(任意) copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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 20: 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 フィールドで使用する 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。
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 : <pre>switch# configure terminal switch(config)#</pre>	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 <i>interface</i> 例 : <pre>switch(config)# ip msdp originator-id loopback0</pre>	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 사용되는 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 <i>limit source source-prefix</i> 例 : <pre>switch(config)# ip msdp group-limit 1000 source 192.168.1.0/24</pre>	指定したプレフィックスに対してソフトウェアが作成する (S, G) エントリの最大数。グループの上限を超えた場合、そのグループは無視され、違反状態が記録されます。デフォルトでは、グループの上限は定義されていません。
ステップ 4	ip msdp sa-interval <i>seconds</i> 例 : <pre>switch(config)# ip msdp sa-interval 80</pre>	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 [<i>vrf [vrf-name all]</i>] 例 : <pre>switch(config)# show ip msdp summary</pre>	MSDP 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 : <pre>switch(config)# copy running-config startup-config</pre>	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： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip msdp mesh-group peer-ip-addr mesh-name 例： switch(config)# ip msdp mesh-group 192.168.1.10 my_mesh_1	MSDP メッシュを設定してピア IP アドレスを指定します。同じルータに複数のメッシュを設定したり、各メッシュグループに複数のピアを設定したりできます。デフォルトでは、メッシュグループは設定されていません。
ステップ 3	ピア IP アドレスを変更し、メッシュ内の各 MSDP ピアについてステップ 2 を繰り返します。	—
ステップ 4	(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：	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。

	コマンドまたはアクション	目的
	<code>switch(config)# copy running-config startup-config</code>	

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せん。

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 : <code>switch# restart msdp</code>	MSDP プロセスを再起動します。
ステップ 2	configure terminal 例 : <code>switch# configure terminal</code> <code>switch(config)#</code>	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 : <code>switch(config)# ip msdp flush-routes</code>	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 : <code>switch(config)# show running-configuration include flush-routes</code>	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 :	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。

	コマンドまたはアクション	目的
	<code>switch(config)# copy running-config startup-config</code>	

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
<code>show ip msdp count [as-number] [vrf [vrf-name all]]</code>	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。
<code>show ip msdp mesh-group [mesh-group] [vrf [vrf-name all]]</code>	MSDP メッシュ グループ設定を表示します。
<code>show ip msdp peer [peer-address] [vrf [vrf-name all]]</code>	MSDP ピアの MSDP 情報を表示します。
<code>show ip msdp rp [rp-address] [vrf [vrf-name all]]</code>	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。
<code>show ip msdp sources [vrf [vrf-name all]]</code>	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。
<code>show ip msdp summary [vrf [vrf-name all]]</code>	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
<code>show ip msdp policy statistics sa-policy peer-address {in out} [vrf [vrf-name all]]</code>	MSDP ピアの MSDP ポリシー統計情報を表示します。

コマンド	説明
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
```

次に、下に示す MSDP ピアリングのサブセットの設定例を示します。

RP 3: 192.168.3.10 (AS 7) <pre>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</pre>
RP 5: 192.168.5.10 (AS 8) <pre>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</pre>
RP 6: 192.168.6.10 (AS 9) <pre>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</pre>

関連資料

関連項目	マニュアル タイトル
MBGP の設定	『Cisco Nexus 9000 シリーズ NX-OS ユニキャスト ルーティング構成ガイド』 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)



第 9 章

MVR の設定

この章では、Cisco NX-OS デバイス上で MVR 機能を設定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 \(209 ページ\)](#)
- [MVR の他の機能との相互運用性 \(210 ページ\)](#)
- [MVR に関する注意事項と制約事項 \(210 ページ\)](#)
- [デフォルトの MVR 設定 \(211 ページ\)](#)
- [MVR の設定 \(211 ページ\)](#)
- [MVR 設定の確認 \(215 ページ\)](#)
- [MVR 設定の例 \(218 ページ\)](#)

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、MVRIP 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 チャンネル (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。
- **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。

- MVR は、N9K-X9636C-R、N9K-X9636C-RX、または N9K-X9636Q-R ラインカードを備えた Cisco Nexus 9508 スイッチでのみサポートされます。
- MVR は、個々のポート、ポート チャンネル、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。

デフォルトの MVR 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 21: 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 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 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	[no]mvr 例 : <pre>switch(config)# mvr switch(config-mvr)#</pre>	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 をディセーブルにするには、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 : <pre>switch(config-mvr)# mvr-vlan 7</pre>	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 : <pre>switch(config-mvr)# mvr-group 230.1.1.1 count 4</pre>	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 <i>a.b.c.d/m</i> 形式で入力します。<i>m</i> はネットマスクのビット数（1 ～ 31）です。 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 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 : <pre>switch(config-mvr)# clear mvr counters</pre>	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 : <pre>switch(config-mvr)# show mvr</pre>	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 :	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。

	コマンドまたはアクション	目的
	<code>switch(config-mvr)# copy running-config startup-config</code>	

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* | **vethernet** *number*}
4. **[no] mvr-type** {*source* | *receiver*}
5. (任意) **[no] mvr-vlan** *vlan-id*
6. (任意) **[no] mvr-group** *addr* [/mask] [**vlan** *vlan-id*]
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 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch(config)# mvr switch(config-mvr)#</pre>	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 { <i>ethernet slot/port</i> port-channel <i>channel-number</i> vethernet <i>number</i> }	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 { <i>source</i> <i>receiver</i> }	MVR ポートを、次のポート タイプのいずれかに設定します。

	コマンドまたはアクション	目的
	<code>switch(config-mvr-if)# mvr-type source</code>	• source : 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 送信元として設定されます。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。 • receiver : 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。
ステップ 5	(任意) [no] mvr-vlan vlan-id 例 : <code>switch(config-mvr-if)# mvr-vlan 7</code>	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	(任意) [no] mvr-group addr [/mask] [vlan vlan-id] 例 : <code>switch(config-mvr-if)# mvr-group 225.1.3.1 vlan 100</code>	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 <i>a.b.c.d/m</i> 形式で入力します。<i>m</i> 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 no 形式を使用します。

	コマンドまたはアクション	目的
ステップ 7	(任意) copy running-config startup-config 例 : <pre>switch(config-mvr-if)# copy running-config startup-config</pre>	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 : <pre>switch# configure terminal switch(config)#</pre>	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 : <pre>switch# mvr-config switch(config-mvr)#</pre>	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 : <pre>switch(config-mvr)# mvr-suppress-query vlan 1-5 switch(config-mvr)#</pre>	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	説明
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 <i>vlan-id</i>]	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 <i>slot/port</i> port-channel <i>number</i>}	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 <i>slot/port</i> port-channel <i>number</i>}	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 <i>vlan-id</i>	指定した VLAN の MVR メンバの詳細を表示します。
show mvr receiver-ports [ethernet <i>slot/port</i> port-channel <i>number</i>]	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 <i>slot/port</i> port-channel <i>number</i>]	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 mode.
- 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
switch(config-mvr-if)## copy running-config startup-config
```



第 10 章

Microsoft ネットワーク ロード バランシング (NLB) の設定

この章では、Cisco NX-OS デバイス上で Microsoft ネットワーク ロード バランシング (NLB) 機能を設定する方法について説明します。

- [ネットワーク ロード バランシング \(NLB\) について \(219 ページ\)](#)
- [NLB の注意事項と制限事項 \(220 ページ\)](#)
- [Microsoft ネットワーク ロード バランシング \(NLB\) の前提条件 \(221 ページ\)](#)
- [マルチキャスト モード \(222 ページ\)](#)
- [IGMP マルチキャスト モード \(223 ページ\)](#)
- [NLB の設定の確認 \(225 ページ\)](#)

ネットワーク ロード バランシング (NLB) について

Network Load Balancing (NLB) テクノロジーは、クライアントからの要求を一連のサーバ全体に分散するために使用します。NLB には 3 つの主要なモードがあります。それらはユニキャスト、マルチキャスト、およびインターネットグループ管理プロトコル (IGMP) マルチキャストです。

- **ユニキャスト モード**はクラスタに仮想 IP と仮想 MAC アドレスを割り当てます。このメソッドは、不明なユニキャストフラッドに依存します。仮想MACアドレスはスイッチポートで学習されないため、仮想MACアドレス宛てのトラフィックは VLAN 内でフラッドされます。これは、すべてのクラスタサーバが仮想MACアドレス宛てのトラフィックを受信することを意味します。この方法の欠点は、一つは、VLAN内のすべてのデバイスがこのトラフィックを受信することです。この動作を軽減する唯一の方法は、トラフィックを受信するインターフェイスにフラッドを回避するために、NLBのサーバインターフェイスだけにNLB VLANを制限します。
- **マルチキャスト モード**では、非 Internet Assigned Numbers Authority (IANA) マルチキャスト MAC アドレス (03xx.xxxx.xxxx) にユニキャスト IP アドレスを割り当てます。IGMP スヌーピングでは、このアドレスをダイナミックに登録しません。この結果、VLAN で NLB トラフィックのフラッドが発生します。PIM 対応の SVI または IGMP スヌーピングクエリアを必要としないということは、NLB がカスタムの非 IP マルチキャストア

アプリケーションで動作することを意味します。詳細については、[マルチキャスト モード \(222 ページ\)](#) を参照してください。

- **IGMP マルチキャスト モード**では、仮想ユニキャスト IP アドレス、および IANA 範囲 (01:00:5E:XX:XX:XX) 内の仮想マルチキャスト MAC アドレスをクラスタに割り当てます。クラスタ化されたサーバーは、設定されたマルチキャスト グループに対する IGMP join を送信するため、スイッチでは、クラスタ化されたサーバーを指し示すために、その IGMP スヌーピングテーブルのエントリをダイナミックに設定します。これにより、ユニキャストフラッドが防止されます。構成例については、[IGMP マルチキャスト モード \(223 ページ\)](#) を参照してください。

このセクションでは、マルチキャストおよび IGMP マルチキャスト モード NLB のNexus 9000 シリーズスイッチを設定する例を示します。先ほど述べたように、マルチキャスト MAC アドレスにマッピングするユニキャスト IP アドレスがあるので、マルチキャスト NLB は必要です。

- 静的アドレス解決プロトコル (ARP) マルチキャスト。
- MAC アドレスをユニキャスト IP アドレスに変換しますが、その IP アドレスへのトラフィックは VLAN をフラッドします。

NLB の注意事項と制限事項

ネットワーク ロード バランシング (NLB) の設定については、次の注意事項と制限事項があります。

- Cisco NX-OS リリース 9.3(5) 以降、マルチキャスト NLB は、Cisco Nexus 9300-FX3 プラットフォーム スイッチでサポートされています。
- Cisco NX-OS リリース 10.2(1q)F 以降、マルチキャスト NLB は Cisco Nexus N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。
- マルチキャスト NLB は、Cisco Nexus 9300-EX、Cisco Nexus 9300-FX、Nexus 9300-FX2 プラットフォーム スイッチ、N9K-X9700-EX ラインカード、N9K-X9700-FX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチ、N9K-C9500-FM-E ファブリック カードおよび N9K-C9500-FM-E2 ファブリック カードを備えた Cisco Nexus 9500 プラットフォーム スイッチでサポートされています。Cisco NX-OS リリース 9.3(6) 以降、マルチキャスト NLB は、Cisco Nexus 9300-GX プラットフォーム スイッチでサポートされます。
 - マルチキャスト NLB は、N9K-C9508-FM-2 を搭載した Cisco Nexus 9500 モジュールではサポートされていません。
 - マルチキャスト NLB は、Cisco Nexus 9300 および 9364C スイッチではサポートされていません。
 - L2 (スイッチドマルチキャスト) および L3 (ルーテッドマルチキャスト) は、マルチキャスト NLB 用に構成された VLAN から、またはその内部ではサポートされていません。これにはリンク ローカル マルチキャスト グループも含まれます。したがっ

て、これらのグループを使用するコントロールプレーンプロトコルは、これらの VLAN での設定はサポートされません。

- HSRP および VRRP は、上記の制限に含まれていないことに注意してください。

- Microsoft ネットワーク ロード バランシング (NLB) ユニキャスト モードのフラッディングは、Cisco Nexus 9000 スイッチではサポートされていません。NLB 仮想 IP アドレスを NLB 仮想 MAC アドレスにマップするには、静的 ARP エントリを構成する必要があります。さらに、NLB 仮想 MAC アドレスを特定の出力インターフェイスにマップするように、静的 MAC アドレス エントリを構成する必要があります。
- FEX HIF インターフェイスは、マルチキャスト NLB フローを受信できません。
- インターフェイスセットのどのポートも UP になっていない場合、トラフィックは VLAN のすべてのポートにフラッディングします。
- L2 および L3 の通常のマルチキャストは、NLB VLAN から、またはその内部ではサポートされていません。
- NLB VLAN に入る NLB トラフィックは、ソース インターフェイスにループバックされる場合があります。このループバックされた NLB トラフィックの存続時間 (TTL) は、VLAN 内であってもデクリメントされます。
- マルチキャスト モード：サーバー/ファイアウォールが移動した場合、管理者は静的マルチキャスト MAC テーブルの設定を更新する必要があります。
- サーバまたはファイアウォールが移動した場合、管理者はスタティック グループの設定を更新する必要があります。
- ユニキャスト、マルチキャスト、および IGMP マルチキャスト モードの NLB は、VXLAN VTEP に基づく Cisco Nexus 9000 シリーズ スイッチではサポートされていません。回避策は、(それぞれのモードで NLB をサポートする) 中間デバイスの背後に NLB クラスタを移動し、VXLAN ファブリックに外部プレフィックスとしてクラスタ IP アドレスを挿入することです。

Microsoft ネットワーク ロード バランシング (NLB) の前提条件

Microsoft ネットワーク ロード バランシング (NLB) には、次の前提条件があります。

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

- マルチキャスト NLB では、マルチキャスト MAC アドレスにマッピングされるユニキャスト IP アドレスがあることが必須です。

マルチキャスト モード

マルチキャスト モードでは、非 Internet Assigned Numbers Authority (IANA) マルチキャスト MAC アドレス (03xx.xxxx.xxxx) にユニキャスト IP アドレスを割り当てます。IGMP スヌーピングでは、このアドレスをダイナミックに登録しません。この結果、VLAN で NLB トラフィックのフラグディングが発生します。このモードで設定する方法の例のオプション 2A を参照してください。次の例で、IGMP マルチキャスト モードを設定する方法を説明します。

例1：スタティック ARP + MAC ベースの L2 マルチキャスト ルックアップ + 参加 + 非 IP マルチキャスト MAC

このオプションは、PIM 対応の SVI または IGMP スヌーピング クエリアを必要としません。非 IP マルチキャスト アプリケーション (カスタム アプリケーション) で動作します。



- (注) マルチキャスト モードをサポートするには、スイッチで **hardware profile multicast nlb** CLI を有効にする必要があります。

1. マルチキャスト MAC アドレスにユニキャスト IP アドレスをマッピングする、非 IP アドレスでマルチキャスト範囲の時間を設定します。スタティック ARP エントリ:

```
interface Vlan10
no shutdown
ip address 10.1.2.1/24
ip arp 10.1.2.200 03bf.0000.1111
```

2. [Mac の VLAN ベースのレイヤ 2 マルチキャスト リファレンス (デフォルトでは、マルチキャストの参照は宛先マルチキャスト IP アドレスに基づいています)]:



- (注) マルチキャスト MAC アドレスと IP アドレスのユニキャスト パケットを抑制する VLAN で MAC ベースの参照を使用します。

```
vlan configuration 10
layer-2 multicast lookup mac
```

3. NLB のサーバおよび冗長インターフェイスに接続されているインターフェイスを指すスタティック MAC アドレス テーブル エントリの設定:

```
mac address-table multicast 03bf.0000.1111 vlan 10 interface Ethernet8/2
mac address-table multicast 03bf.0000.1111 vlan 10 interface Ethernet8/4
mac address-table multicast 03bf.0000.1111 vlan 10 interface Ethernet8/7
```

IGMP マルチキャスト モード

IGMP マルチキャスト モードでは、仮想ユニキャスト IP アドレス、および IANA 範囲 (01:00:5E:XX:XX:XX) 内の仮想マルチキャスト MAC アドレスをクラスタに割り当てます。クラスタ化されたサーバーは、設定されたマルチキャスト グループに対する IGMP join を送信するため、スイッチでは、クラスタ化されたサーバーを指し示すために、その IGMP スヌーピング テーブルのエントリをダイナミックに設定します。これにより、ユニキャストフラッドイングが防止されます。次に、IGMP マルチキャスト モードを設定する方法の 3 つの例について説明します。

オプション 1：静的 ARP + MAC ベースの L2 マルチキャスト ルックアップ + ダイナミック参加

このオプションにより、サーバーとファイアウォールは、対応するグループにダイナミックに参加または脱退することができます。ターゲットトラフィックの受信を有効または無効にします (たとえばメンテナンス モード)。



(注) IGMP マルチキャスト モードをサポートするには、スイッチで **hardware profile multicast nlb CLI** を有効にする必要があります。

1. Protocol Independent Multicast (PIM) の IP アドレスでマルチキャスト範囲のマルチキャスト MAC アドレスにユニキャスト IP アドレスにマッピングするスタティック ARP エントリ。使用可能なインターフェイスの設定:

```
interface Vlan10
no shutdown
ip address 10.1.2.1/24
ip pim sparse-mode
ip arp 10.1.2.200 0100.5E01.0101
```

2. [Mac の VLAN ベースのレイヤ 2 マルチキャスト リファレンス (デフォルトでは、マルチキャストの参照は宛先マルチキャスト IP アドレスに基づいています)]:

```
vlan configuration 10
layer-2 multicast lookup mac
```

オプション 2：静的 ARP + MAC ベースの L2 マルチキャスト ルックアップ + ダイナミック参加と IGMP スヌーピング クエリア

オプション 2 は PIM 対応の SVI を必要とせず、サーバーとファイアウォールは、対応するグループにダイナミックに参加または脱退することができます。ターゲットトラフィックの受信を有効または無効にします (たとえばメンテナンス モード)。



(注) IGMP マルチキャスト モードをサポートするには、スイッチで **hardware profile multicast nlb CLI** を有効にする必要があります。

1. オプション1などのスタティックARPエントリを設定します。ただし、スイッチ仮想インターフェイス (SVI) でPIMを有効にしないでください。

```
interface Vlan10
no shutdown
ip address 10.1.2.1/24
ip arp 10.1.2.200 0100.5E01.0101
```

2. MacのVLANベースのレイヤ2マルチキャストの検索を有効にし、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 クエリアをイネーブルにする:

```
vlan configuration 10
ip igmp snooping querier 10.1.1.254
layer-2 multicast lookup mac
```

オプション3: スタティック ARP + MAC ベースの L2 マルチキャスト ルックアップ + 静的参加 + IP マルチキャスト MAC

オプション3 では PIM 対応 SVI または IGMP スヌーピング クエリアは必要ではありません。



- (注) IGMP マルチキャスト モードをサポートするには、スイッチで **hardware profile multicast nlb** CLI を有効にする必要があります。

1. ユニキャスト IP アドレスを IP アドレス マルチキャスト範囲内のマルチキャスト MAC アドレスにマップする静的 ARP エントリを設定します。

```
interface Vlan10
no shutdown
ip address 10.1.2.1/24
ip arp 10.1.2.200 0100.5E01.0101
```

2. Mac ベースのレイヤ2マルチキャストルックアップをVLANで有効にします (デフォルトでは、マルチキャストルックアップは宛先マルチキャストIPアドレスに基づいています)。

```
vlan configuration 10
layer-2 multicast lookup mac
```

マルチキャストMACアドレスとIPアドレスのユニキャストパケットを抑制するVLANでMACベースの参照を使用します。

3. NLBのサーバに接続されているインターフェイスのスタティックでIGMPスヌーピンググループエントリを設定して、トラフィックを必要とする:

```
vlan configuration 10
ip igmp snooping static-group 239.1.1.1 interface Ethernet8/2
ip igmp snooping static-group 239.1.1.1 interface Ethernet8/4
ip igmp snooping static-group 239.1.1.1 interface Ethernet8/7
```

トラフィックが同じポートチャネルで入出力しているマルチキャストNLBを使用していて、異なるモジュールにもそのポートチャネルのメンバーがある場合は、次の手順を実行します。

1. グローバルモードで次のコマンドを実行します。

```
hardware profile multicast nlb
hardware profile multicast nlb port-channel
clear ip igmp snooping groups (For ingress and egress VLANs)
```

2. 上記の各オプションの構成手順を続行します。

NLB の設定の確認

NLB の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	説明
show ip arp virtual-address	ARP テーブルを表示します。
show ip igmp snooping groups [source [group] group [source]] [vlan vlan-id] [detail]	グループに関する IGMP スヌーピング情報を VLAN 別に表示します。
show ip igmp snooping mac-oif vlan vlan-id	IGMP スヌーピング スタティック MAC アドレスを表示します。



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、<https://www.ietf.org/search/?query=RFC> を参照してください。

- [IP マルチキャストについての IETF RFC（227 ページ）](#)

IP マルチキャストについての IETF RFC

次の表に、IP マルチキャストに関連する RFC を示します。

RFC	タイトル
RFC 2236	インターネット グループ管理プロトコル
RFC 2365	管理用スコープの IP マルチキャスト
RFC 2710	『Multicast Listener Discovery (MLD) for IPv6』
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
RFC 3446	『Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)』
RFC 3569	『An Overview of Source-Specific Multicast (SSM)』
RFC 3618	Multicast Source Discovery Protocol (MSDP)
RFC 3810	『Multicast Listener Discovery Version 2 (MLDv2) for IPv6』
RFC 4601	『Protocol Independent Multicast - Sparse Mode (PIM-SM) Specification (Revised)』
RFC 4610	『Anycast-RP Using Protocol Independent Multicast (PIM)』

RFC	タイトル
RFC 5132	『 <i>IP Multicast MIB</i> 』



付録 **B**

Cisco NX-OS のマルチキャストに関する設定の限界

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

- [構成の制限値 \(229 ページ\)](#)

構成の制限値

Cisco NX-OS がサポートする機能には、設定の最大制限があります。一部の機能には、最大値以下の制限をサポートする設定があります。

設定制限は『[Cisco Nexus 9000 シリーズ NX-OS 検証済みスケーラビリティ ガイド](#)』にまとめられています。

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。