



Cisco Nexus 7000 シリーズ NX-OS マルチキャストルーティング コンフィギュレーションガイド

初版：2012年02月20日

最終更新：2012年08月23日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

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

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

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

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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

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

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

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2012 Cisco Systems, Inc. All rights reserved.



目次

はじめに **xi**

対象読者 **xi**

表記法 **xi**

Cisco Nexus 7000 シリーズ NX-OS ソフトウェアの関連資料 **xiii**

マニュアルに関するフィードバック **xv**

マニュアルの入手方法およびテクニカル サポート **xv**

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 **1**

概要 **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 PIM および PIM6 **10**

ASM **14**

Bidir **14**

SSM **14**

マルチキャスト用 RPF ルート **15**

IGMP および MLD **15**

IGMP スヌーピング **15**

ドメイン間マルチキャスト **15**

SSM **15**

MSDP **16**

MBGP **16**

MRIB および M6RIB	16
仮想ポート チャンネルおよびマルチキャスト	17
シャーシにFシリーズとMシリーズの両方のモジュールが搭載されている場合の マルチキャスト	18
マルチキャスト機能のライセンス要件	18
マルチキャスト機能のハイ アベイラビリティ要件	18
関連資料	18
シスコのテクニカル サポート	19
IGMP の設定	21
IGMP の情報	21
IGMP のバージョン	21
IGMP の基礎	22
仮想化のサポート	24
IGMP のライセンス要件	25
IGMP の前提条件	25
IGMP のデフォルト設定	25
IGMP パラメータの設定	26
IGMP インターフェイス パラメータの設定	26
IGMP SSM 変換の設定	34
ルータ アラートの適用オプション チェックの設定	35
IGMP プロセスの再起動	36
IGMP コンフィギュレーションの確認	37
IGMP の設定例	38
IGMP の機能の履歴	38
MLD の設定	41
MLD の情報	41
MLD のバージョン	42
MLD の基礎	43
仮想化のサポート	45
MLD のライセンス要件	45
MLD の前提条件	45
MLD の注意事項および制限事項	46

MLD のデフォルト設定	46
MLD パラメータの設定	47
MLD インターフェイス パラメータの設定	47
MLD SSM 変換の設定	54
MLD の設定の確認	56
MLD の設定例	57
関連資料	57
標準	57
MLD の機能の履歴	58
PIM および PIM6 の設定	59
PIM および PIM6 の情報	59
hello メッセージ	61
Join/Prune メッセージ	61
ステートのリフレッシュ	62
ランデブー ポイント	62
スタティック RP	62
BSR	63
Auto-RP	64
1 つの PIM ドメイン内の複数の RP	65
PIM BSR ブートストラップ/Auto-RP マッピング エージェントの選定プロセス	65
ブートストラップルータ (BSP) の選定プロセスの詳細	66
Auto-RP マッピング エージェントの選定プロセス	67
PIM RP 対 RP の選定プロセス	68
PIM BSR RP 候補対 BSR RP 候補の選定プロセス	69
PIM BSR RP 候補対 スタティック RP の選定プロセス	72
PIM Auto-RP 候補対 Auto-RP 候補の選定プロセス	75
PIM Auto-RP 候補対 スタティック RP の選定プロセス	75
Anycast-RP	76
PIM Register メッセージ	76
指定ルータ	77
Designated Forwarder	77
ASM モードにおける共有ツリーから送信元ツリーへのスイッチオーバー	78

管理用スコープの IP マルチキャスト	78
PIM の双方向フォワーディング検出	79
仮想化のサポート	79
ハイアベイラビリティ	79
PIM および PIM6 のライセンス要件	80
PIM および PIM6 の前提条件	80
PIM および PIM6 に関する注意事項と制限事項	80
デフォルト設定	81
PIM および PIM6 の設定	82
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
PIM スパースモードパラメータの設定	87
PIM6 スパースモードパラメータの設定	90
ASM および Bidir の設定	92
スタティック RP の設定	92
スタティック RP (PIM) の設定	93
スタティック RP (PIM6) の設定	94
BSR の設定	95
BSR (PIM) の設定	97
BSR (PIM6) の設定	98
Auto-RP の設定	99
Auto RP (PIM) の設定	101
PIM Anycast-RP セットの設定	102
PIM Anycast RP セット (PIM) の設定	102
PIM Anycast RP セット (PIM6) の設定	104
ASM 専用の共有ツリーの設定	105
ASM 専用の共有ツリー (PIM) の設定	106
ASM 専用の共有ツリー (PIM6) の設定	107
SSM の設定	108
SSM (PIM) の設定	108
SSM (PIM6) の設定	109

マルチキャスト用 RPF ルートの設定	110
マルチキャスト マルチパスのディセーブル化	111
RP 情報配信を制御するルート マップの設定	111
RP 情報配信を制御するルート マップ (PIM) の設定	112
RP 情報配信を制御するルート マップ (PIM6) の設定	113
メッセージフィルタリングの設定	114
メッセージフィルタリング (PIM) の設定	116
メッセージフィルタリング (PIM6) の設定	118
PIM プロセスおよび PIM6 プロセスの再起動	120
PIM プロセス (PIM) の再起動	120
PIM6 プロセスの再起動	121
VRF モードでの PIM の BFD の設定	122
インターフェイス モードでの PIM の BFD の設定	123
PIM および PIM6 の設定の確認	124
統計情報の表示	125
PIM および PIM6 の統計情報の表示	125
PIM および PIM6 の統計情報のクリア	126
PIM の設定例	126
SSM の設定例	126
BSR の設定例	127
Auto-RP の設定例	128
PIM Anycast RP の設定例	129
Prefix-Based および Route-Map-Based の設定	129
出力	130
関連資料	131
標準	131
MIB	132
PIM と PIM6 の機能履歴	132
IGMP スヌーピングの設定	133
IGMP スヌーピングの情報	133
IGMPv1 および IGMPv2	135
IGMPv3	135
IGMP スヌーピング クエリア	136

スタティック マルチキャスト MAC アドレス	136
VDC および VRF を使用した IGMP スヌーピング	137
IGMP スヌーピングのライセンス要件	137
IGMP スヌーピングの前提条件	138
IGMP スヌーピングに関する注意事項と制限事項	138
デフォルト設定	139
IGMP スヌーピング パラメータの設定	140
グローバル IGMP スヌーピング パラメータの設定	140
VLAN ごとの IGMP スヌーピング パラメータの設定	143
検索モードの変更	150
スタティック マルチキャスト MAC アドレスの設定	152
IGMP スヌーピングの設定確認	153
IGMP スヌーピング統計情報の表示	153
IGMP スヌーピングの設定例	153
関連資料	154
標準	154
CLI での IGMP スヌーピング機能の履歴	155
MSDP の設定	157
MSDP の情報	157
SA メッセージおよびキャッシング	159
MSDP ピア RPF 転送	159
MSDP メッシュ グループ	160
仮想化のサポート	160
MSDP のライセンス要件	160
MSDP の前提条件	160
デフォルト設定	161
MSDP の設定	161
MSDP 機能のイネーブル化	162
MSDP ピアの設定	163
MSDP ピア パラメータの設定	164
MSDP グローバルパラメータの設定	166
MSDP メッシュ グループの設定	169

MSDP プロセスの再起動	170
MSDP の設定の確認	170
MSDP のモニタリング	171
統計情報の表示	171
統計情報のクリア	172
MSDP の設定例	172
関連資料	173
標準	173
N7K-F132-15 モジュールを使用したマルチキャスト相互動作の設定	175
マルチキャスト相互動作に関する情報	175
N7K-F132-15 および M シリーズ モジュールでのマルチキャスト相互動作	176
仮想化のサポート	177
ハイ アベイラビリティ	177
マルチキャスト相互動作のライセンス要件	177
マルチキャスト相互動作の前提条件	177
注意事項と制限	178
混在シャーシを使用したレイヤ 3 マルチキャストの設定	178
マルチキャストの設定の確認	180
マルチキャスト相互動作の機能の履歴	180
IP マルチキャストに関する IETF RFC	181
IP マルチキャストに関する IETF RFC	181
Cisco NX-OS のマルチキャストに関する設定の上限	183
設定の制限値	183



はじめに

ここでは、『Cisco Nexus 7000 シリーズ NX-OS マルチキャストルーティング コンフィギュレーションガイド』の対象読者、構成、および表記法について説明します。また、関連マニュアルの入手方法についても説明します。

- [対象読者, xi ページ](#)
- [表記法, xi ページ](#)
- [Cisco Nexus 7000 シリーズ NX-OS ソフトウェアの関連資料, xiii ページ](#)
- [マニュアルに関するフィードバック, xv ページ](#)
- [マニュアルの入手方法およびテクニカルサポート, xv ページ](#)

対象読者

この出版物は Cisco Nexus シリーズ デバイスの設定と保守を行う経験豊富なネットワーク管理者を対象としています。

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、ユーザが値を入力する引数です。
[x]	角カッコで囲まれているものは、省略可能な要素（キーワードまたは引数）です。

表記法	説明
[x y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x y}	必ずいずれか 1 つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
variable	ユーザが値を入力する変数であることを表します。イタリック体を使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
screen フォント	スイッチが表示する端末セッションおよび情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ (<>) で囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。



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



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

Cisco Nexus 7000 シリーズ NX-OS ソフトウェアの関連資料

完全な Cisco Nexus 7000 シリーズ NX-OS マニュアルセットは、次の URL で入手できます。

http://www.cisco.com/en/us/products/ps9402/tsd_products_support_series_home.html

リリースノート

リリースノートは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9402/prod_release_notes_list.html

コンフィギュレーションガイド

これらのマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9402/products_installation_and_configuration_guides_list.html

このカテゴリのマニュアルは次のとおりです。

- 『Cisco Nexus 7000 Series NX-OS Configuration Examples』
- 『Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide』
- 『Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide』
- 『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide』
- 『Cisco Nexus 7000 Series NX-OS IP SLAs Configuration Guide』
- 『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide』
- 『Cisco Nexus 7000 Series NX-OS LISP Configuration Guide』
- 『Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide』
- 『Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide』
- 『Cisco Nexus 7000 Series NX-OS OTV Configuration Guide』
- 『Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide』
- 『Cisco Nexus 7000 Series NX-OS SAN Switching Guide』
- 『Cisco Nexus 7000 Series NX-OS Security Configuration Guide』

- 『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide』
- 『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide』
- 『Cisco Nexus 7000 Series NX-OS Verified Scalability Guide』
- 『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide』
- 『Cisco Nexus 7000 Series NX-OS Virtual Device Context Quick Start』
- 『Cisco Nexus 7000 Series NX-OS OTV Quick Start Guide』
- 『Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500』
- 『Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide』

コマンド リファレンス

これらのマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps9402/prod_command_reference_list.html

このカテゴリのマニュアルは次のとおりです。

- 『Cisco Nexus 7000 Series NX-OS Command Reference Master Index』
- 『Cisco Nexus 7000 Series NX-OS FabricPath Command Reference』
- 『Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference』
- 『Cisco Nexus 7000 Series NX-OS High Availability Command Reference』
- 『Cisco Nexus 7000 Series NX-OS Interfaces Command Reference』
- 『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference』
- 『Cisco Nexus 7000 Series NX-OS LISP Command Reference』
- 『Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide』
- 『Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference』
- 『Cisco Nexus 7000 Series NX-OS OTV Command Reference』
- 『Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference』
- 『Cisco Nexus 7000 Series NX-OS SAN Switching Command Reference』
- 『Cisco Nexus 7000 Series NX-OS Security Command Reference』
- 『Cisco Nexus 7000 Series NX-OS System Management Command Reference』
- 『Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference』
- 『Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference』
- 『Cisco NX-OS FCoE Command Reference for Cisco Nexus 7000 and Cisco MDS 9500』

その他のソフトウェアのマニュアル

次のランディング ページから始まるこれらのマニュアルを入手できます。

http://www.cisco.com/en/us/products/ps9402/tsd_products_support_series_home.html

- 『Cisco Nexus 7000 Series NX-OS MIB Quick Reference』
- 『Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide』
- 『Cisco Nexus 7000 Series NX-OS Troubleshooting Guide』
- 『Cisco NX-OS Licensing Guide』
- 『Cisco NX-OS System Messages Reference』
- 『Cisco NX-OS XML Interface User Guide』

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。

マニュアルの入手方法およびテクニカル サポート

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

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

『*What's New in Cisco Product Documentation*』は Really Simple Syndication (RSS) フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



第 1 章

新機能および変更された機能に関する情報

この章では、新機能と変更された機能について説明します。

- [新機能および変更された機能, 1 ページ](#)

新機能および変更された機能

次に、『Cisco Nexus 7000 シリーズ NX-OS マルチキャストルーティング コンフィギュレーションガイド』に記載されている新機能および変更された機能について、リリース固有の情報を示します。このマニュアルの最新バージョンは、次のシスコ Web サイトから入手できます。

http://www.cisco.com/en/US/products/ps9402/products_installation_and_configuration_guides_list.html

Cisco NX-OS リリースに関する追加情報をチェックするには、次のシスコ Web サイトから入手可能な『Cisco NX-OS Release Notes』を参照してください。 http://www.cisco.com/en/US/products/ps9402/prod_release_notes_list.html

次の表に、『Cisco Nexus 7000 シリーズ NX-OS マルチキャストルーティング コンフィギュレーションガイド』の新機能および変更された機能の要約と参照先を示します。

表 1: 新機能および変更された機能

機能	説明	変更されたリリース	参照先
ip igmp groups および ip igmp route コマンド	サマリー パラメータで更新されるコマンド。 <ul style="list-style-type: none">• ip igmp groups• ip igmp route	6.1(1)	第 2 章「IGMP の設定」
F2 モジュールの構成。	Cisco NX-OS は F2 モジュールの PIM Bidir モードをサポートしていません。	6.0(1)	第 4 章「PIM および PIM6 の設定」

機能	説明	変更されたリリース	参照先
F2 モジュールの構成。	F2モジュールは、いずれの形式のIPv4 または IPv6 トンネルもサポートしていません。	6.0(1)	第 4 章 「PIM および PIM6 の設定」
検索モードの MAC への設定およびスタティック MAC アドレスの割り当て	MAC ベースとしてフォワーディング検索モードを使用するように IGMP スヌーピングを設定したり、スタティック MAC アドレスを割り当てたりすることができます。	5.2(1)	第 5 章 「IGMP スヌーピングの設定」
GRE トンネルインターフェイスでの PIMv4 の設定	発信インターフェイス (OIF) を含む GRE トンネルインターフェイスにマルチキャストを設定できます。	5.2(1)	第 4 章 「PIM および PIM6 の設定」
F シリーズモジュールでのマルチキャスト相互動作の設定	F シリーズおよび M シリーズモジュールでのマルチキャスト相互動作を設定できます。	5.1(1)	第 7 章 「N7K-F132-15 モジュールを使用したマルチキャスト相互動作の設定」
マルチキャストルーティングの初期ホールドダウン期間	IPv4 ネットワークと IPv6 ネットワークの両方に初期ホールドダウン期間を指定できます。	4.2(1)	第 4 章 「PIM または PIM6 スパース モードの設定」
コマンドに対応するルートマップポリシーの使用	次のコマンドについては、コマンドラインで指定するのではなく、ルートマップポリシーにグループプレフィックスを指定できます。 <ul style="list-style-type: none"> • ip igmp join-group • ip igmp static-oif • ip pim rp-address • ip pim ssm range • ipv6 [icmp] mld join-group • ipv6 [icmp] mld static-oif • ipv6 pim rp-address • ipv6 pim ssm range 	4.2(1)	第 2 章 「IGMP の設定」 第 3 章 「MLD の設定」 第 4 章 「スタティック RP の設定」 第 4 章 「SSM の設定」

機能	説明	変更されたリリース	参照先
Virtual Port Channel (vPC; 仮想ポートチャンネル)	Nexus 7000 シリーズ デバイスの Cisco NX-OS ソフトウェアは、PIM SSM も BIDR on vPC もサポートしていません。Cisco NX-OS ソフトウェアは、PIM ASM on vPC を完全にサポートします。	4.1(4)	第1章「仮想ポートチャンネルおよびマルチキャスト」
Virtual Port Channel (vPC; 仮想ポートチャンネル)	virtual Port Channel (vPC; 仮想ポートチャンネル) : 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。	4.1(3)	第1章「仮想ポートチャンネルおよびマルチキャスト」 第2章「IGMP コンフィギュレーションの確認」 第4章「ASM および Bidir の設定」 第5章「IGMP スヌーピングに関する注意事項と制約事項」 第5章「IGMP スヌーピング統計情報の表示」
即時脱退	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 または MLD インターフェイスで IGMPv2 または MLDv1 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抑えることができるオプション。	4.1(3)	第2章「IGMP インターフェイス パラメータの設定」 第3章「MLD インターフェイス パラメータの設定」



第 2 章

概要

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

- [マルチキャストに関する情報, 5 ページ](#)
- [マルチキャスト機能のライセンス要件, 18 ページ](#)
- [マルチキャスト機能のハイ アベイラビリティ要件, 18 ページ](#)
- [関連資料, 18 ページ](#)
- [シスコのテクニカル サポート, 19 ページ](#)

マルチキャストに関する情報

IP マルチキャストは、ネットワーク内の複数のホストに同じ IP パケット セットを転送する機能です。マルチキャストは、IPv4 ネットワークと IPv6 ネットワークの両方で使用でき、複数の宛先への効率のよいデータ配信を提供します。



(注) Nexus 7000 シリーズ デバイス用の Cisco NX-OS Release 5.2(1) 以降では、プロトコル独立型マルチキャスト v4 (PIMv4) を設定し、発信インターフェイス (OIF) を含む総称ルーティングカプセル化 (GRE) トンネルを通して実行できます。Cisco NX-OS リリース以前では、トンネルインターフェイスは PIM をサポートしません。

マルチキャストは、マルチキャストデータの配信機能と、送信元および受信者の検出機能からなり、マルチキャストデータは、グループと呼ばれる IP マルチキャスト アドレス宛に送信されます。多くの場合、グループおよび送信元 IP アドレスを含むマルチキャストアドレスは、チャ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>

IPv6 マルチキャストアドレスは 0xFF から始まります。IPv6 のアドレッシングアーキテクチャは、RFC 4291 で規定されています。IANA で予約されているアドレスの詳細については、次の URL を参照してください。 <http://www.iana.org/assignments/ipv6-multicast-addresses>

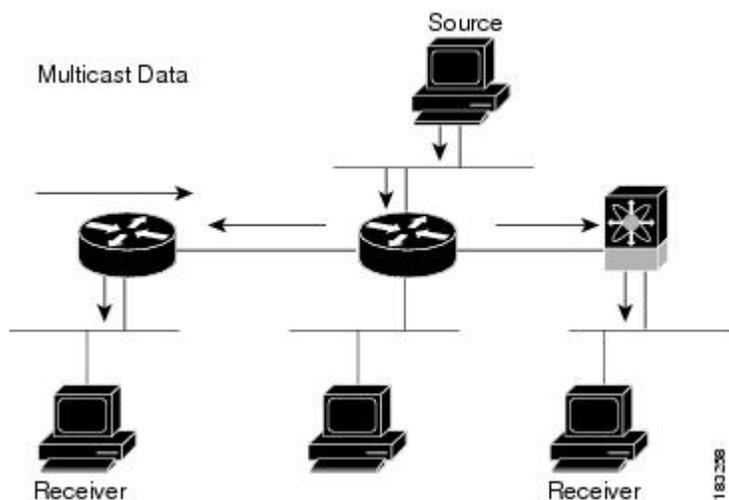


(注) マルチキャスト関連の RFC の一覧については、付録 A 「IP マルチキャストに関する IETF RFC」を参照してください。

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

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

図 1: 1 つの送信元から 2 つの受信者へのマルチキャストトラフィック



マルチキャスト配信ツリー

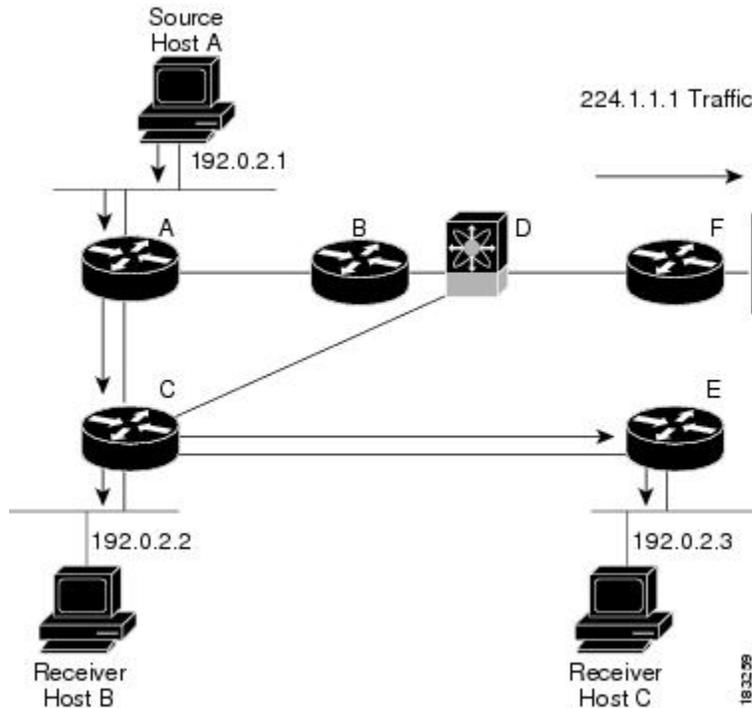
マルチキャスト配信ツリーとは、送信元と受信者の中継するルータ間の、マルチキャストデータの伝送パスを表します。マルチキャストソフトウェアはサポートするマルチキャスト方式に応じて、タイプの異なるツリーを構築します。

送信元ツリー

送信元ツリーは、ネットワーク経由でマルチキャストトラフィックを伝送する場合の最短パスです。送信元から特定のマルチキャストグループへと送信されたマルチキャストトラフィックが、同じグループにトラフィックを要求する受信者へと転送されます。送信元ツリーは、最短パスと

しての特性から、Shortest Path Tree (SPT; 最短パス ツリー) と呼ばれることがあります。次の表に、ホスト A を起点とし、ホスト B および C に接続されているグループ 224.1.1.1 の送信元ツリーを示します。

図 2: 送信元ツリー



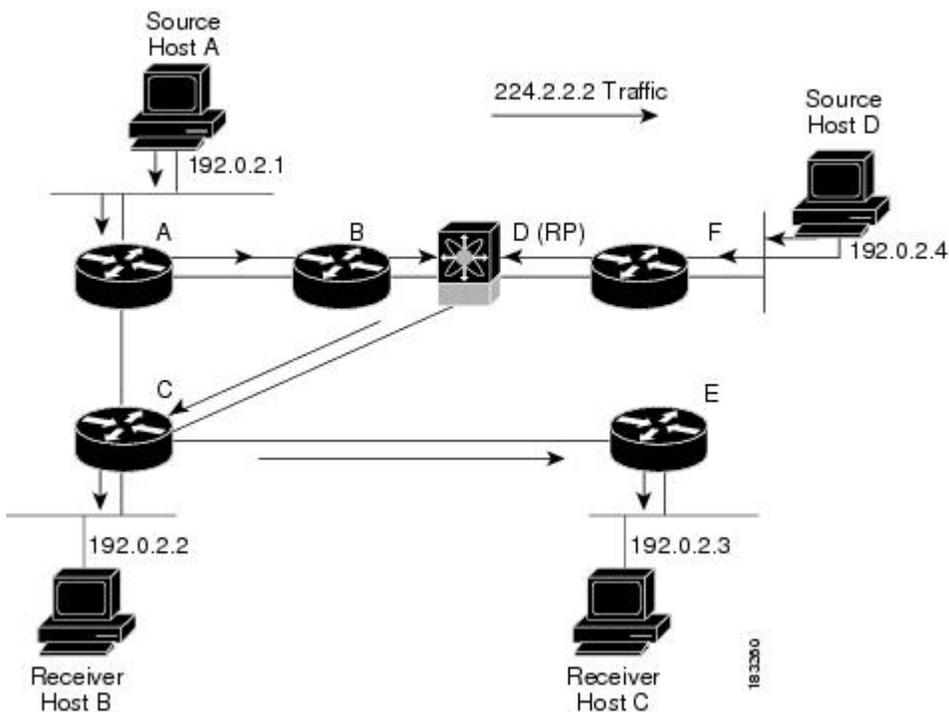
(S, G) は、グループ G の送信元 S から送信されるマルチキャストトラフィックを表します。この図の SPT は、(192.0.2.1, 224.1.1.1) と書き表されます。同じグループの複数の送信元からトラフィックを送信できます。

共有ツリー

共有ツリーとは、共有ルート、つまり Rendezvous Point (RP; ランデブーポイント) から各受信者に、ネットワーク経由でマルチキャストトラフィックを伝送する共有配信パスを表します (RP は各送信元への SPT を作成します)。共有ツリーは、RP Tree (RPT; RP ツリー) とも呼ばれます。次の図に、ルータ D を RP とする場合の、グループ 224.1.1.1 の共有ツリーを示します。デー

タはホスト A およびホスト D からルータ D (RP) に送信され、そこから受信者ホスト B およびホスト C にトラフィックが転送されます。

図 3: 共有ツリー



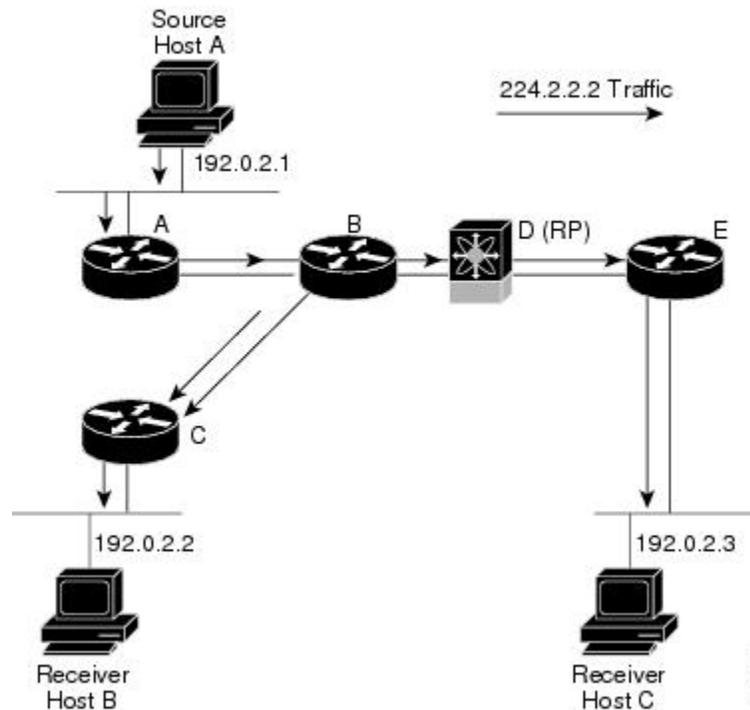
(* , G) は、グループ G の任意の送信元から送信されるマルチキャストトラフィックを表します。この図の共有ツリーは、(*, 224.2.2.2) と書き表されます。

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 を経由して、ホスト A からホスト

B に直接送信されます。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



(* , G) は、グループ G の任意の送信元から送信されるマルチキャスト トラフィックを表します。次の表の双方向ツリーは、(*, 224.2.2.2) と書き表されます。

マルチキャスト転送

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

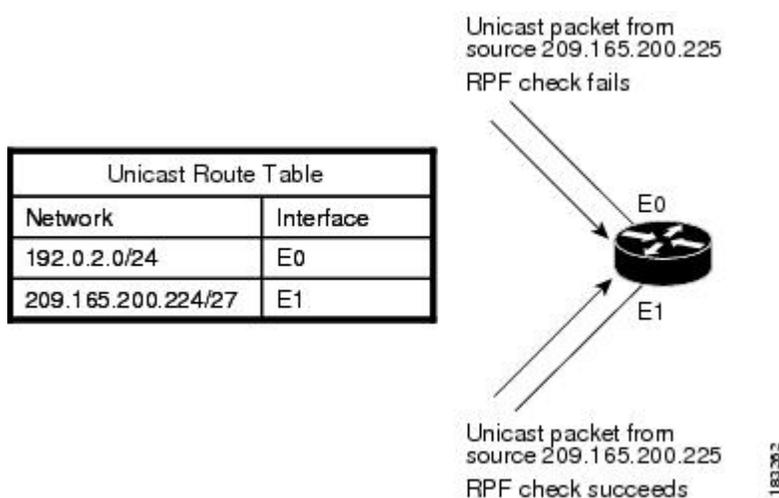
マルチキャストパケットが着信するたびに、ルータは RPF チェックを実行します。送信元に接続されたインターフェイスにパケットが着信した場合は、グループの Outgoing Interface (OIF; 発信インターフェイス) リスト内の各インターフェイスからパケットが転送されます。それ以外の場合、パケットはドロップされます。



(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 Designated Forwarder (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 PIM および PIM6

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



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

マルチキャストコマンドにアクセスするには、PIM または PIM6 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 または PIM6 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。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 を設定します。システムでは、IGMP および MLD がデフォルトで稼働しています。

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。

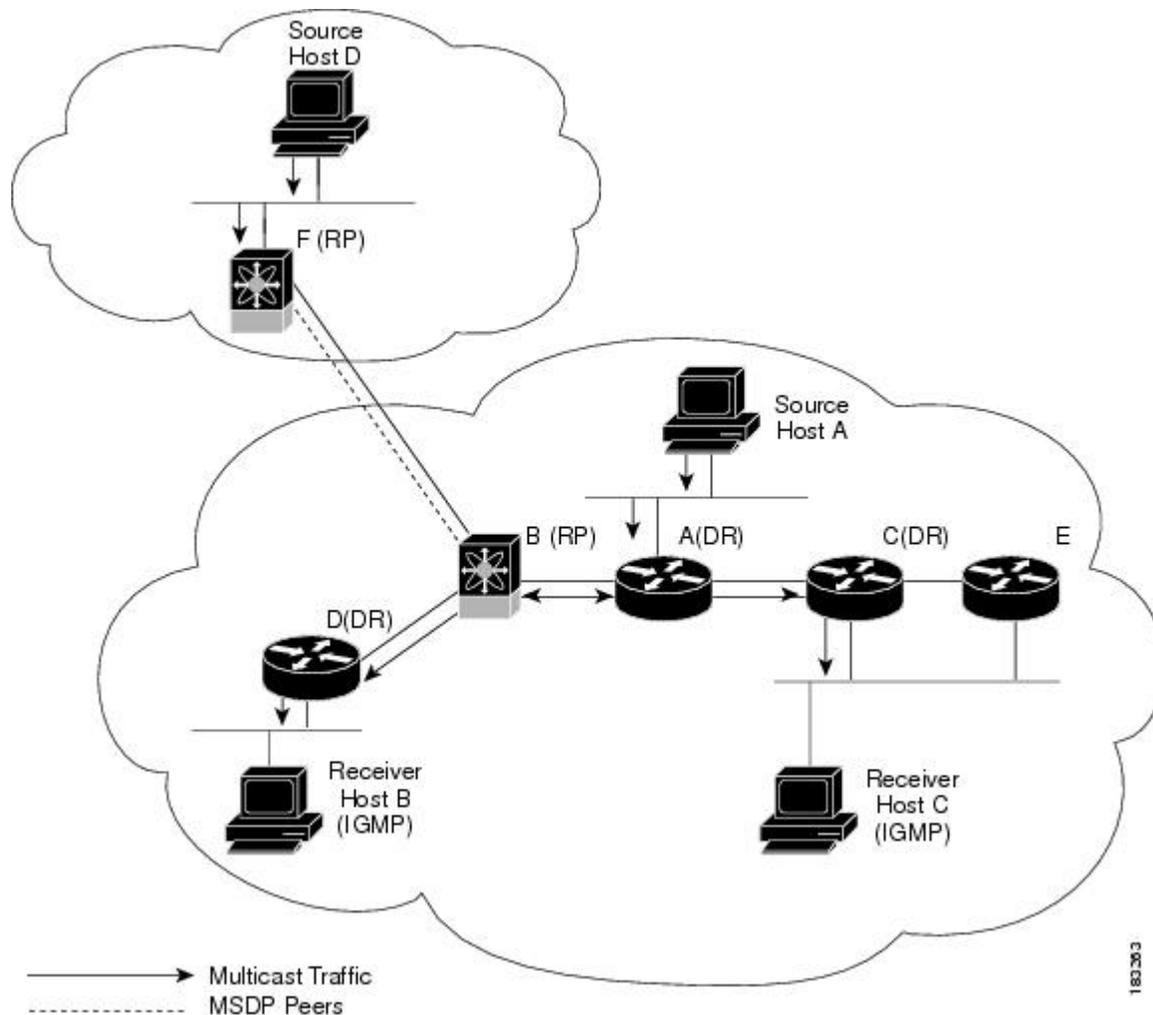
ルータはユニキャストルーティングテーブルおよび RPF ルートを使用して、マルチキャストを実行するためのマルチキャストルーティング情報を生成します。Bidir モードの場合は、追加ルーティング情報が生成されます。



(注) このマニュアルで、「IPv4 の PIM」および「IPv6 の PIM6」は、Cisco NX-OS に実装されている PIM スパースモードを表します。PIM ドメインには、IPv4 と IPv6 の両方のネットワークを含めることができます。

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

図 6 : IPv4 ネットワーク内の PIM ドメイン



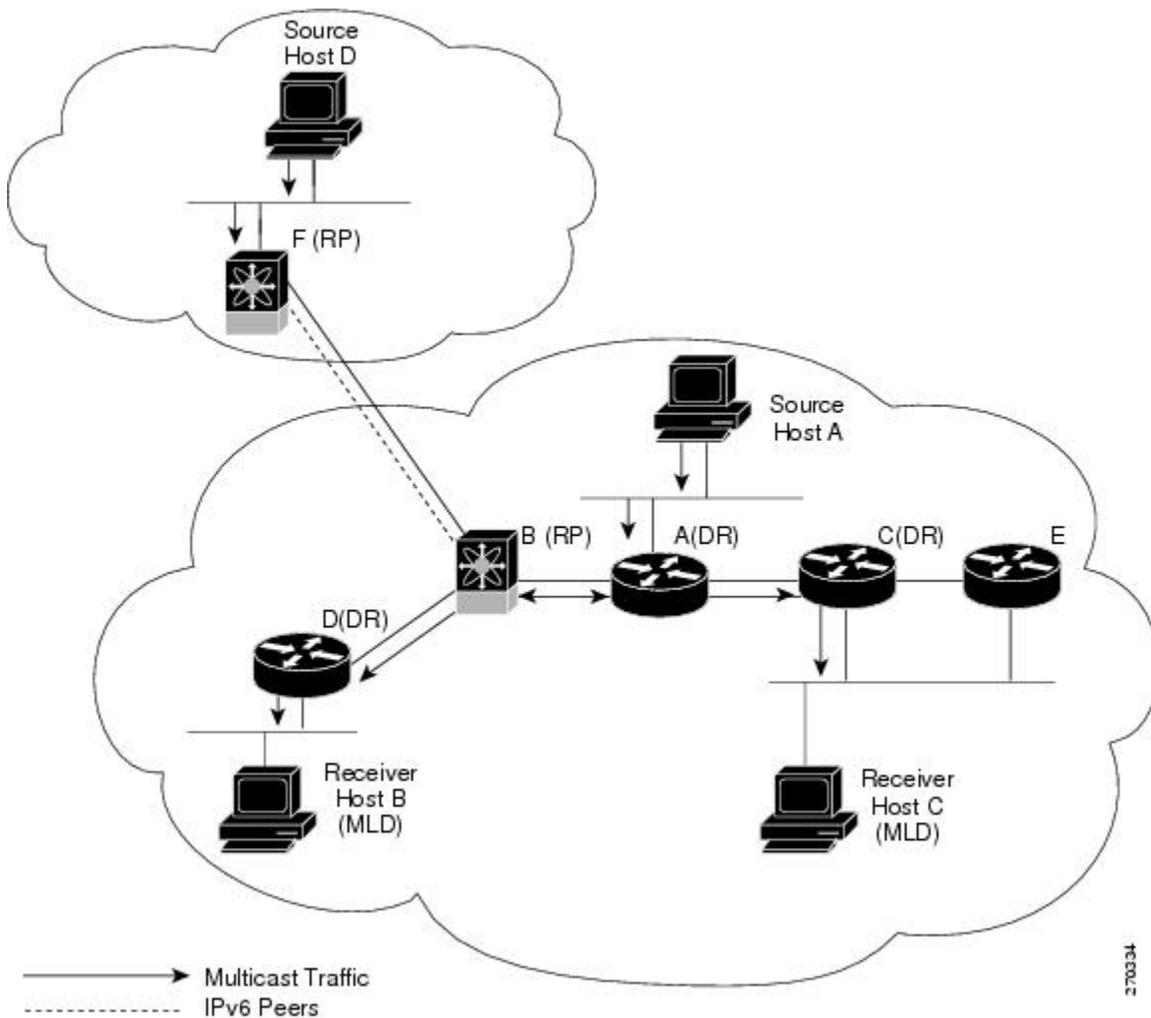
- 矢印の付いた直線は、ネットワークで伝送されるマルチキャストデータのパスを表します。マルチキャストデータは送信元ホストの A および D から発信されます。
- 点線でつながれているルータ B および F は、Multicast Source Discovery Protocol (MSDP) ピアです。MSDP を使用すると、他の PIM ドメイン内にあるマルチキャスト送信元を検出できます。
- ホスト B およびホスト C ではマルチキャストデータを受信するため、Internet Group Management Protocol (IGMP; インターネットグループ管理プロトコル) プ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

ルータが1つ選択されます。これにより、マルチキャストデータの窓口として、1つのルータだけが使用されます。

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

次の図に、IPv6 ネットワーク内の2つの PIM6 ドメインを示します。IPv6 ネットワークの場合、マルチキャスト データを受信する受信者は、Multicast Listener Discovery (MLD) 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。IPv6 では MSDP がサポートされないため、他の PIM ドメインに属するマルチキャスト送信元は検出できません。IPv6 ピアを設定し、Source-Specific Multicast (SSM) および Multiprotocol Border Gateway Protocol (MBGP) を使用すると、PIM6 ドメイン間でマルチキャスト データを転送することができます。

図 7: IPv6 ネットワーク内の PIM6 ドメイン



PIM は送信元と受信者間の接続に関して、3つのマルチキャスト モードをサポートしています。

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

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 Bootstrap Router (BSR; ブートストラップルータ) プロトコルを使用して、グループと RP 間の関連付けを動的に検出することもできます。学習された RP が 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

Bidirectional shared tree (Bidir; 双方向共有ツリー) 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 Designated Forwarder (DF) と呼ばれます。これは、RP を経由することなく、Designated Router (DR; 指定ルータ) 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

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

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

マルチキャスト用 RPF ルート

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

IGMP および MLD

システムは、PIM の場合はインターネット グループ管理プロトコル (IGMP) を、PIM6 の場合は Multicast Listener Discovery (MLD) をデフォルトで実行しています。

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

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

インターフェイスには MLDv1 または MLDv2 を設定できます。SSM モードをサポートする場合は、MLDv2 を使用するのが一般的です。デフォルトでは MLDv2 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。

ドメイン間マルチキャスト

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 または PIM6 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 および PIM6 を介して、外部の BGP 自律システム内の送信元と通信できます。

MBGP の詳細については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference』を参照してください。

MRIB および M6RIB

Cisco NX-OS IPv4 Multicast Routing Information Base (MRIB) は、PIM や IGMP などのマルチキャストプロトコルで生成されるルート情報を格納するためのリポジトリです。MRIB はルート情報自体には影響を及ぼしません。MRIB は Virtual Device Context (VDC; 仮想デバイス コンテキスト) の Virtual Routing and Forwarding (VRF; 仮想ルーティングおよびフォワーディング) インスタンスごとに、独立したルート情報を保持します。VDCs の詳細については、『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.2』を参照してください。

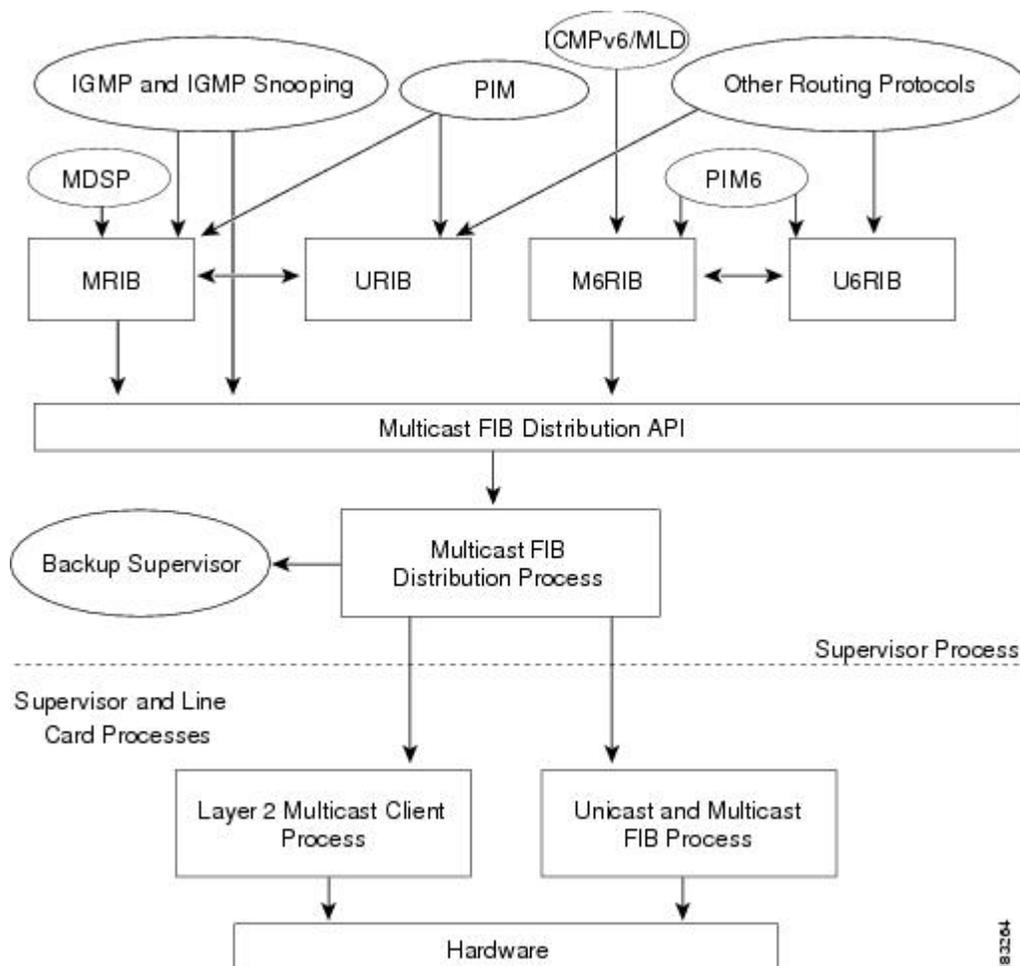
MRIB が IPv4 ルーティング情報を保持するのと同じように、M6RIB は、PIM6 や MLD などのプロトコルによって生成される IPv6 ルーティング情報を保持します。

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

- Multicast Forwarding Information Base (MFIB および M6FIB) Distribution (MFDM) API : MRIB や M6RIB を含むマルチキャストレイヤ 2 およびレイヤ 3 コントロールプレーン モジュールと、プラットフォーム フォワーディング プレーン間のインターフェイスを定義します。コントロールプレーン モジュールは、MFDM API を使用してレイヤ 3 ルート アップデートおよびレイヤ 2 ルックアップ情報を送信します。
- マルチキャスト FIB 配信プロセス : 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。

図 8：Cisco NX-OS マルチキャスト ソフトウェアのアーキテクチャ



仮想ポートチャネルおよびマルチキャスト

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

- PIM および PIM6：Nexus 7000 シリーズデバイス対応の Cisco NX-OS ソフトウェアは、vPC 上の PIM SSM または BIDR をサポートしません。Cisco NX-OS ソフトウェアは、vPC 上の PIM ASM を完全にサポートします。
- GMP 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。

シャーシに F シリーズと M シリーズの両方のモジュールが搭載されている場合のマルチキャスト

Cisco NX-OS Release 5.1 以降では、Cisco Nexus 7000 シリーズのシャーシに、レイヤ 2 専用モジュールである F シリーズ モジュールを追加できます。すでに M シリーズ モジュールが搭載されているシャーシにこのモジュールを追加する場合、マルチキャストをプロビジョニングできます。

マルチキャスト機能のライセンス要件

次に、ライセンスを必要とするマルチキャスト機能を示します。

- PIM および PIM6
- MSDP

マルチキャスト ライセンスの詳細については、「PIM および PIM6 のライセンス要件」および「MSDP のライセンス要件」を参照してください。次に、ライセンスが不要なマルチキャスト機能を示します。

- IGMP
- MLD
- IGMP スヌーピング

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

マルチキャスト機能のハイ アベイラビリティ要件

マルチキャストルーティングプロトコルを再起動すると、MRIB プロセスによってステートが回復されます。スーパーバイザのスイッチオーバーが発生した場合、MRIB はハードウェアからステートを回復し、マルチキャストプロトコルは定期的なメッセージアクティビティからステートを回復します。ハイ アベイラビリティの詳細については、『Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide』を参照してください。

関連資料

関連項目	参照先
VDC	『Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference』
CLI コマンド	『Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference』

シスコのテクニカルサポート

説明	リンク
<p>TACのホームページには、3万ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.comに登録済みのユーザは、このページから詳細情報にアクセスできます。</p>	<p>http://www.cisco.com/public/support/tac/home.shtml</p>



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 の情報, 21 ページ](#)
- [IGMP のライセンス要件, 25 ページ](#)
- [IGMP の前提条件, 25 ページ](#)
- [IGMP のデフォルト設定, 25 ページ](#)
- [IGMP パラメータの設定, 26 ページ](#)

IGMP の情報

IGMP は、ホストが特定のグループにマルチキャスト データを要求するために使用する IPv4 プロトコルです。ソフトウェアは、IGMP を介して取得した情報を使用し、マルチキャストグループまたはチャ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、IGMPv1 のほかに、IGMPv2 と IGMPv3 のレポート受信もサポートされています。

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

IGMPv3 には、次に示す IGMPv2 からの重要な変更点があります。

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

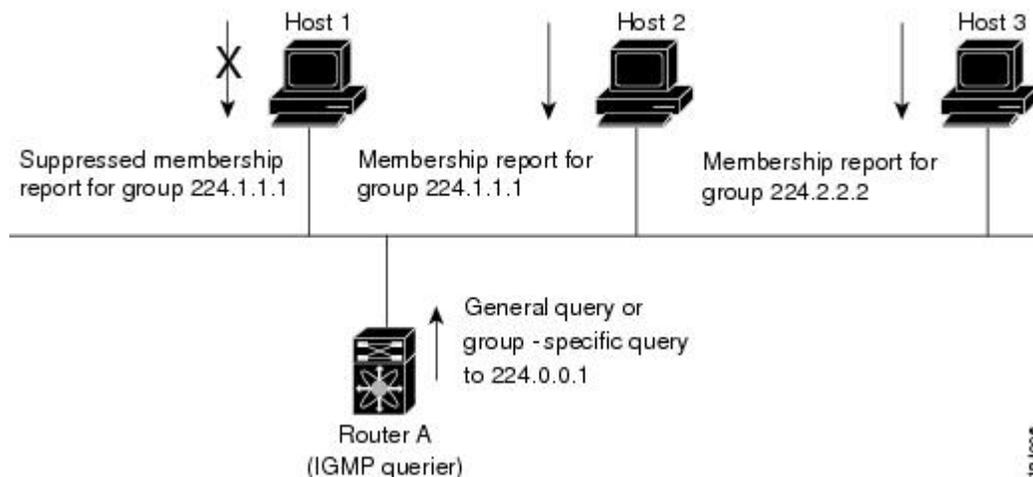
IGMPv2 の詳細については、[RFC 2236](#) を参照してください。

IGMPv3 の詳細については、[RFC 3376](#) を参照してください。

IGMP の基礎

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

図 9: IGMPv1 および IGMPv2 クエリー応答プロセス



次の図のルータ A (サブネットの代表 IGMP クエリア) は、すべてのホストが含まれる 224.0.0.1 ホストマルチキャストグループに定期的にクエリーメッセージを送信して、マルチキャストデータを要求しているホストを検出します。グループメンバーシップタイムアウト値を設定し、指定したタイムアウト値が経過すると、ルータはサブネット上にグループのメンバーまたは送信元

が存在しないと見なします。IGMP パラメータの設定方法については、「IGMP インターフェイスパラメータの設定」を参照してください。

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

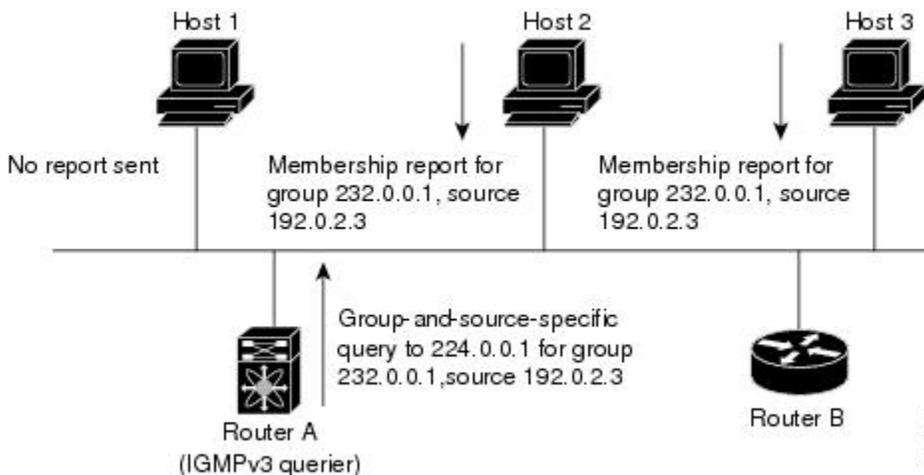
この図では、ホスト 1 からのメンバーシップレポートの送出手が止められており、最初にホスト 2 からグループ 224.1.1.1 に関するメンバーシップレポートが送信されます。ホスト 1 はホスト 2 からレポートを受信します。ルータに送信する必要があるメンバーシップレポートは、グループにつき 1 つだけであるため、その他のホストではレポートの送出手が止められ、ネットワークトラフィックが軽減されます。レポートの同時送信を防ぐため、各ホストではランダムな時間だけレポート送信が保留されます。クエリーの最大応答時間パラメータを設定すると、ホストのランダムな応答間隔を制御できます。



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

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

図 10: IGMPv3 グループ/ソース固有のクエリー





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

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



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

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

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

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

IGMP パラメータの設定方法については、「IGMP インターフェイスパラメータの設定」を参照してください。

仮想化のサポート

Virtual Device Context (VDC; 仮想デバイスコンテキスト) は、一連のシステムリソースを論理的に表現する用語です。各 VDC 内では、複数の Virtual Routing and Forwarding (VRF; 仮想ルーティングおよびフォワーディング) インスタンスを定義できます。VDC ごとに実行できる IGMP プロセスは 1 つです。IGMP プロセスは対象の VDC に含まれるすべての VRF をサポートし、その VDC 内で IGMP スヌーピング機能を実行します。IGMP スヌーピングの詳細については、「IGMP スヌーピングの設定」を参照してください。

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。

VDC の設定方法については、『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide』を参照してください。

VRF の設定方法については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

IGMP のライセンス要件

製品	ライセンス要件
Cisco NX-OS	IGMP にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

IGMP の前提条件

IGMP の前提条件は、次のとおりです。

- デバイスにログインしている。
- 現在の Virtual Device Context (VDC; 仮想デバイス コンテキスト) が正しい。VDC は、一連のシステム リソースを論理的に表現する用語です。 `switchto vdc` コマンドでは VDC 番号を指定できます。
- 現在の Virtual Routing and Forwarding (VRF; 仮想ルーティングおよびフォワーディング) モードが正しい (グローバル コンフィギュレーション コマンドの場合)。この章の例で示すデフォルトのコンフィギュレーションモードは、デフォルト VRF に適用されます。

IGMP のデフォルト設定

次の表に、IGMP パラメータのデフォルト設定を示します。

表 2: IGMP パラメータのデフォルト設定

パラメータ	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

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

IGMP パラメータの設定

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



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

IGMP インターフェイス パラメータの設定

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

表 3: IGMP インターフェイスパラメータ

パラメータ	説明
IGMP のバージョン	インターフェイスでイネーブルにする IGMP のバージョン。有効な IGMP バージョンは 2 または 3 です。デフォルトは 2 です。
スタティック マルチキャスト グループ	<p>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) という状態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) という状態で指定します。 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。</p> <p>(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。</p> <p>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。</p>
Outgoing Interface (OIF; 発信インターフェイス) 上のスタティック マルチキャスト グループ	<p>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) という状態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) という状態で指定します。 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。</p> <p>(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。</p>
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ることで、パケットの再送信回数を増やすことができます。有効範囲は 1 ~ 7 です。デフォルトは 2 です。

パラメータ	説明
クエリア タイムアウト	前クエリアがクエリーを停止してから、自身がクエリアとして処理を引き継ぐまで、ソフトウェアが待機する秒数。有効範囲は 1 ～ 65,535 秒です。デフォルト値は 255 秒です。
クエリーの最大応答時間	IGMP クエリーでアドバタイズされる最大応答時間。大きな値を設定すると、ホストの応答時間が延長されるため、ネットワークの IGMP メッセージのバースト性を調整できます。この値は、クエリーインターバルよりも短く設定する必要があります。有効範囲は 1 ～ 25 秒です。デフォルトは 10 秒です。
クエリー インターバル	IGMP ホスト クエリー メッセージの送信頻度。大きな値を設定すると、ソフトウェアによる IGMP クエリーの送信頻度が低くなるため、ネットワーク上の IGMP メッセージ数を調整できます。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 125 秒です。
最終メンバーのクエリー応答インターバル	サブネット上の既知のアクティブ ホストから最後にホスト Leave メッセージを受信したあと、ソフトウェアが IGMP クエリーへの応答を送信するインターバル。このインターバル中に応答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。デフォルトでは無効になっています。

パラメータ	説明
レポート ポリシー	ルートマップ ポリシーに基づく、IGMP レポートのアクセス ポリシー。 1
アクセス グループ	インターフェイスが接続されたサブネット上のホストについて、加入可能なマルチキャスト グループを制御するためのルートマップ ポリシー 1 を設定するオプション。
即時脱退	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。デフォルトでは無効になっています。 (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 7000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

マルチキャスト ルートマップの設定方法については、「RP 情報配信を制御するルートマップの設定」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	config t 例： switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	interface interface 例： switch(config)# interface ethernet 2/1 switch(config-if)#	ethernet slot/port などのインターフェイス タイプ および番号を入力して、インターフェイス モードを開始します。

	コマンドまたはアクション		目的
ステップ 3	オプション	説明	次のコマンドを使用して、IGMP インターフェイス パラメータを設定します。
	<p>ip igmp version <i>value</i></p> <p>例</p> <pre>switch(config-if)# ip igmp version 3</pre>	<p>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。</p> <p>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に設定されません。</p>	
	<p>ip igmp join-group {<i>group</i> [<i>source source</i>] <i>route-map policy-name</i>}</p> <p>例</p> <pre>switch(config-if)# ip igmp join-group 230.0.0.0</pre>	<p>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。グループアドレスだけを指定した場合は、(*, G) というステートが作成されます。送信元アドレスを指定した場合は、(S, G) というステートが作成されます。</p> <p>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。</p> <p>(注) (S, G) ステートで送信元ツリーを構築するには、IGMPv3 をイネーブルにする必要があります。</p> <p>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ル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。</p>	

コマンドまたはアクション		目的
オプション	説明	
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) IGMPv3 をイネーブルにした場合にのみ、 (S, G) ステートに対して送信元ツリーが作成されます。	
ip igmp startup-query-interval seconds 例 <pre>switch(config-if)# ip igmp 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。	
ip igmp startup-query-count count 例 <pre>switch(config-if)# ip igmp 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。	
ip igmp robustness-variable value 例 <pre>switch(config-if)# ip igmp robustness-variable 3</pre>	ロバストネス変数を設定します。 ネットワークのパケット損失が多い場合は、この値を大きくします。 値の範囲は 1 ~ 7 です。 デフォルトは 2 です。	
ip igmp querier-timeout seconds 例 <pre>switch(config-if)# ip igmp 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。	

コマンドまたはアクション		目的
オプション	説明	
ip igmp query-timeout <i>seconds</i> 例 <pre>switch(config-if)# ip igmp 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、 ip igmp querier-timeout コマンドと同じです。	
ip igmp query-max-response-time <i>seconds</i> 例 <pre>switch(config-if)# ip igmp query-max-response-time 15</pre>	IGMP クエリーでアドバタイズされる応答時間を設定します。有効範囲は 1 ~ 25 秒です。デフォルトは 10 秒です。	
ip igmp query-interval <i>interval</i> 例 <pre>switch(config-if)# ip igmp query-interval 100</pre>	IGMP ホストクエリーメッセージの送信頻度を設定します。有効範囲は 1 ~ 18,000 秒です。デフォルト値は 125 秒です。	
ip igmp last-member-query-response-time <i>seconds</i> 例 <pre>switch(config-if)# ip igmp 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。デフォルトは 1 秒です。	
ip igmp last-member-query-count <i>count</i> 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。	
ip igmp group-timeout <i>seconds</i> 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。	

コマンドまたはアクション		目的
オプション	説明	
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。	
ip igmp report-policy policy 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。	
ip igmp access-group policy 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。	
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ーが送信されないため、所定の IGMP インターフェイスで IGMPv2 グループメンバーシップの脱退のための待ち時間が最小限になります。デフォルトでは無効になっています。 (注) このコマンドは、所定のグループに対するインターフェイスの背後に 1 つの受信者しか存在しない場合に使用します。	
ステップ 4 show ip igmp interface [interface] [vrf vrf-name all] [brief] 例 : <pre>switch(config)# show ip igmp interface</pre>		(任意) インターフェイスの IGMP 情報を表示します。

	コマンドまたはアクション	目的
ステップ 5	copy running-config startup-config 例： <pre>switch(config)# 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。

IGMP SSM 変換の設定

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

次の表に、SSM 変換の例を示します。

表 4: SSM 変換の例

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

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

表 5: SSM 変換適用後の例

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



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

手順

	コマンドまたはアクション	目的
ステップ 1	config t Example: 例： switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	ip igmp ssm-translategroup-prefix source-addr 例： switch(config)# ip igmp ssm-translate 232.0.0.0/8 10.1.1.1	ルータが IGMPv3 メンバーシップ レポートを受信したときと同様に、(S,G) ステートが作成されるよう、IGMP プロセスによる IGMPv1 または IGMPv2 メンバーシップ レポートの変換を設定します。
ステップ 3	show running-configuration igmp 例： switch(config)# show running-configuration igmp	(任意) <i>ssm-translate</i> コマンドラインを含む、実行コンフィギュレーション情報を示します。
ステップ 4	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

ルータ アラートの適用オプションチェックの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t switch(config)#	コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	ip igmp enforce-router-alert 例： switch(config)# ip igmp enforce-router-alert	IGMPv2 パケットと IGMPv3 パケットに対するルータ アラートの適用オプションチェックをイネーブルにします。デフォルトでは、ルータアラートの適用オプションチェックはイネーブルです。
ステップ 3	no ip igmp enforce-router-alert 例： switch(config)# no ip igmp enforce-router-alert	IGMPv2 パケットと IGMPv3 パケットに対するルータ アラートの適用オプションチェックをディセーブルにします。デフォルトでは、ルータアラートの適用オプションチェックはイネーブルです。
ステップ 4	show running-configuration igmp 例： switch(config)# show running-configuration igmp	(任意) enforce-router-alert コマンドラインを含む、実行コンフィギュレーション情報を示します。
ステップ 5	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

IGMP プロセスの再起動

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

手順

	コマンドまたはアクション	目的
ステップ 1	restart igmp 例： switch# restart igmp	IGMP プロセスを再起動します。
ステップ 2	config t 例： switch# config t switch(config)#	コンフィギュレーションモードに入ります。

	コマンドまたはアクション	目的
ステップ 3	ip igmp flush-routes 例： switch(config)# ip igmp flush-routes	IGMP プロセスの再起動時に、ルートを削除します。デフォルトでは、ルートはフラッシュされません。
ステップ 4	show running-configuration igmp 例： switch(config)# show running-configuration igmp	(任意) <i>flush-routes</i> コマンドラインを含む、実行コンフィギュレーション情報を示します。
ステップ 5	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

IGMP コンフィギュレーションの確認

IGMP の設定情報を表示するには、次の作業のいずれかを行います。

show ip igmp interface [<i>interface</i>] [<i>vrf 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 [group]</i> }] { <i>group [source]</i> }] [<i>interface</i>] [summary] [<i>vrf 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 [group]</i> }] { <i>group [source]</i> }] [<i>interface</i>] [summary] [<i>vrf 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。
--	------------------------------------

これらのコマンド出力のフィールドの詳細については、『Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference』を参照してください。

IGMP の設定例

次に、IGMP パラメータの設定例を示します。

```

config t
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

```

IGMP の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 6: IGMP の機能の履歴

機能名	リリース	機能情報
ip igmp groups および ip igmp route コマンド	6.1(1)	サマリー パラメータで更新されるコマンド。 <ul style="list-style-type: none"> • ip igmp groups • ip igmp route
vPC	4.1(3)	show ip igmp interface コマンドを使用して、vPC 統計情報を表示します。 この機能に関する詳細については、次の項を参照してください。 <ul style="list-style-type: none"> • <i>IGMP</i> コンフィギュレーションの確認

機能名	リリース	機能情報
即時脱退	4.1(3)	<p>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 または MLD インターフェイスで IGMPv2 または MLDv1 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抑えます。</p> <p>詳細については、「<i>IGMP</i> インターフェイスパラメータの設定」を参照してください。</p>



第 4 章

MLD の設定

この章では、IPv6 ネットワーク用の Cisco NX-OS デバイスに Multicast Listener Discovery (MLD) を設定する方法を説明します。

- [MLD の情報, 41 ページ](#)
- [MLD のライセンス要件, 45 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, 46 ページ](#)
- [MLD のデフォルト設定, 46 ページ](#)
- [MLD パラメータの設定, 47 ページ](#)
- [MLD の設定の確認, 56 ページ](#)
- [MLD の設定例, 57 ページ](#)
- [関連資料, 57 ページ](#)
- [標準, 57 ページ](#)
- [MLD の機能の履歴, 58 ページ](#)

MLD の情報

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せん。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。

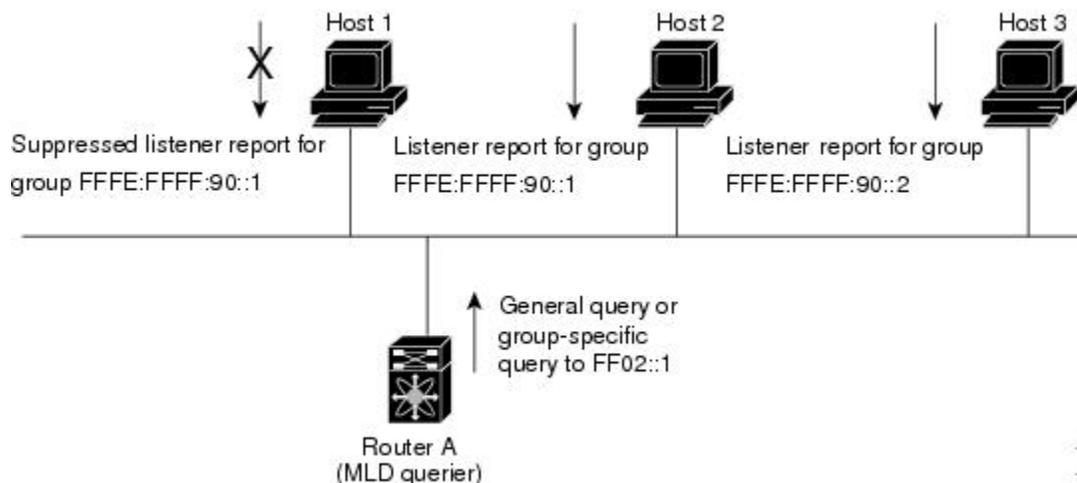
- 次の機能を提供し、各受信者から送信元までの最短パス ツリーを構築可能な Source-Specific Multicast (SSM) をサポートします。
 - グループおよび送信元を両方指定できるホスト メッセージ
 - MLDv1 ではグループについてのみ保持できたマルチキャスト ステートを、グループおよび送信元について保持可能
- ホストによるレポート抑制が行われなくなり、MLD クエリー メッセージを受信するたびに MLD リスナー レポートが送信されるようになりました。

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。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。

図 11 : MLD クエリー応答プロセス



この図のルータ 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ー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し、指定したタイムアウト値が経過すると、ルータはサブネット上にグループのメンバーまたは送信元が存在しないと見なします。

この図では、ホスト 1 からのリスナー レポートの送出手が止められており、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手が止められ、ネットワーク トラフィックが軽減されます。レポートの同時送信を防ぐため、各ホストではランダムな時間だけレポート送信が保留されます。クエリーの最大応答時間パラメータを設定すると、ホストのランダムな応答間隔を制御できます。



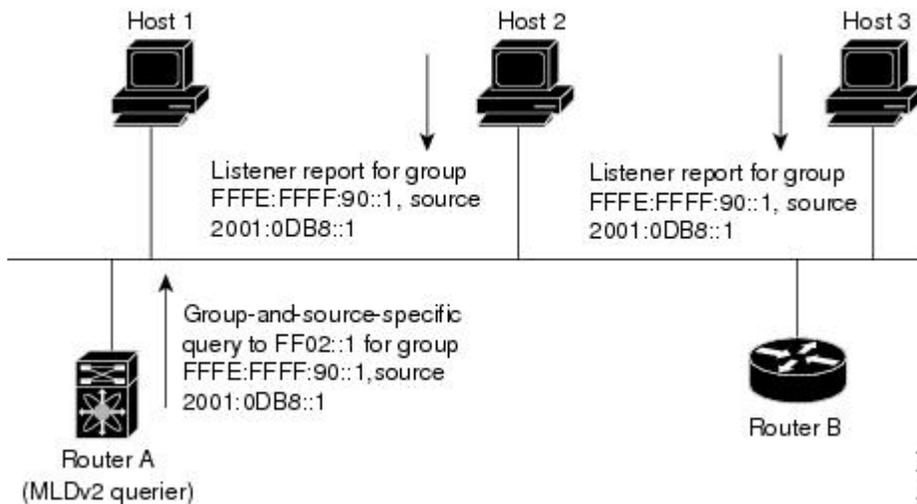
(注) MLDv1 メンバーシップ レポートが抑制されるのは、同じポートに複数のホストが接続されている場合だけです。

この図のルータ A は、MLDv2 グループ/ソース固有のクエリーを LAN に送信します。ホスト 2 および 3 は、アドバタイズされたグループおよび送信元からデータを受信することを示すリスナー レポートを送信して、そのクエリーに応答します。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ーに応答します。

図 12: 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 Time-To-Live (TTL; 存続可能時間) 値は 1 です。つまり、サブネット上の直接接続されたルータからは、メッセージは転送されません。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。

仮想化のサポート

Virtual Device Context (VDC; 仮想デバイスコンテキスト) は、一連のシステムリソースを論理的に表現する用語です。各 VDC 内では、複数の Virtual Routing and Forwarding (VRF; 仮想ルーティングおよびフォワーディング) インスタンスを定義できます。VDC ごとに実行できる MLD プロセスは 1 つです。MLD プロセスは、対象の VDC に含まれるすべての VRF をサポートします。

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

VDC の設定方法については、『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide』を参照してください。

VRF の設定方法については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

MLD のライセンス要件

製品	ライセンス要件
Cisco NX-OS	MLD にはライセンスは不要です。ライセンスパッケージに含まれていない機能はすべて Cisco NX-OS システムイメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『Cisco NX-OS Licensing Guide』を参照してください。

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 Virtual Device Context (VDC; 仮想デバイス コンテキスト) が正しい。VDC は、一連のシステム リソースを論理的に表現する用語です。 `switchto vdc` コマンドでは VDC 番号を指定できます。
- 現在の Virtual Routing and Forwarding (VRF; 仮想ルーティングおよびフォワーディング) モードが正しい (グローバル コ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。

- レイヤ 2 ネットワークでマルチキャスト転送を必要とする IPv6 マルチキャスト ネットワークに対して IGMP 最適化マルチキャスト転送 (OMF) をディセーブルにする必要があります。
- IPv6 パケットの転送が必要な VLAN の IGMP 最適化マルチキャスト転送をディセーブルにする必要があります。

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
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

パラメータ	デフォルト
最終メンバーのクエリー回数	2
グループ メンバーシップ タイムアウト	260 秒
リンク ローカル マルチキャスト グループのレポート	ディセーブル
即時脱退	ディセーブル

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



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

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。

パラメータ	説明
スタティック マルチキャスト グループ	<p>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。</p> <p>(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MLDv2がイネーブルな場合だけです。</p> <p>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。</p>
Outgoing Interface (OIF; 発信インターフェイス) 上のスタティック マルチキャスト グループ	<p>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。</p> <p>(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MLDv2がイネーブルな場合だけです。</p>
スタートアップクエリーインターバル	<p>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。</p>
スタートアップクエリーの回数	<p>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。</p>
ロバストネス値	<p>輻輳ネットワークでのパケット損失を許容範囲内に抑えるために使用される、調整可能なロバストネス変数。ロバストネス変数を大きくすることで、パケットの再送信回数を増やすことができます。有効範囲は1～7です。デフォルトは2です。</p>
クエリア タイムアウト	<p>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。</p>
クエリーの最大応答時間	<p>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。</p>

パラメータ	説明
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 Leave 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 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	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。デフォルトでは無効になっています。
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。 2
アクセスグループ	インターフェイスが接続されたサブネット上のホストについて、加入可能なマルチキャストグループを制御するためのルートマップポリシー 1 を設定するオプション。

パラメータ	説明
即時脱退	<p>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 MLDv1 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抑えることができるオプション。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。デフォルトでは無効になっています。</p> <p>(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。</p>

- ² ルートマップ ポリシーの設定方法については、『Cisco Nexus 7000 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	config t 例： <pre>switch# config t 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	interface interface 例： <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	<i>ethernet</i> などのインターフェイス タイプおよび番号を入力して、インターフェイス モードを開始します。
ステップ 3	オプション	次の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できます。
	ipv6 mld version value 例 <pre>switch(config-if)# ipv6 mld version 2</pre>	

コマンドまたはアクション		目的
オプション	説明	
<p>ipv6 mld join-group {group [source source] route-map policy-name}</p> <p>例</p> <pre>switch(config-if)# ipv6 mld join-group FFFE::1</pre>	<p>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。</p> <p>(注) (S, G) ステートで送信元ツリーを構築するには、MLDv2 をイネーブルにする必要があります。</p> <p>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。</p>	
<p>ipv6 mld static-oif {group [source source] route-map policy-name}</p> <p>例</p> <pre>switch(config-if)# ipv6 mld static-oif FFFE::1</pre>	<p>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。</p> <p>(注) (S, G) ステートで送信元ツリーを構築するには、MLDv2 をイネーブルにする必要があります。</p>	

コマンドまたはアクション		目的
オプション	説明	
ipv6 mld startup-query-interval <i>seconds</i> 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。	
ipv6 mld startup-query-count <i>count</i> 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。	
ipv6 mld robustness-variable <i>value</i> 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。ネットワークのパケット損失が多い場合は、この値を大きくします。値の範囲は 1 ~ 7 です。デフォルトは 2 です。	
ipv6 mld querier-timeout <i>seconds</i> 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。	
ipv6 mld query-timeout <i>seconds</i> 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。	
ipv6 mld query-max-response-time <i>seconds</i> 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
オプション	説明	
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。	
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。デフォルトは 1 秒です。	
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。	
ipv6 mld group-timeout seconds 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。	
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。	
ipv6 mld report-policy policy 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。	
ipv6 mld access-group policy 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。	

コマンドまたはアクション		目的
オプション	説明	
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ーが送信されないため、所定の 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。デフォルトでは無効になっています。 (注) このコマンドは、所定のグループに対するインターフェイスの背後に 1 つの受信者しか存在しない場合に使用します。	
ステップ 4	show ipv6 mld interface [interface] [vrf vrf-name all] [brief] 例 : <pre>switch(config)# show ipv6 mld interface</pre>	(任意) インターフェイスの MLD 情報を表示します。
ステップ 5	copy running-config startup-config 例 : <pre>switch(config)# 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。

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。PIM SSM 範囲の変更方法については、「SSM の設定」を参照してください。

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、MLD v1 リスナー レポートに SSM 変換を適用した場合に、MLD プロセスによって作成される M6RIB 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 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	config t 例 : switch# config t switch(config)#	コンフィギュレーション モードに入ります。 コンフィギュレーション モードに入ります。
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	show running-configuration ssm-translate 例 : switch(config)# show running-configuration ssm-translate	(任意) 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。

	コマンドまたはアクション	目的
ステップ 4	copy running-config startup-config 例： <pre>switch(config)# 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。

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 interface [interface] [vrf vrf-name all] [brief]	すべてのインターフェイスまたは選択されたインターフェイス、デフォルト VRF、選択された VRF、またはすべての VRF について、MLD 情報を表示します。
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 route [group interface] [vrf vrf-name all]	グループまたはインターフェイス、デフォルト VRF、選択された VRF、またはすべての VRF について、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。

これらのコマンド出力のフィールドの詳細については、『Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference』を参照してください。

MLD の設定例

```

config t
  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

```

関連資料

関連項目	参照先
VDC	『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide』
CLI コマンド	『Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference』

標準

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

MLD の機能の履歴

表 11 : MLD の機能の履歴

機能名	リリース	機能情報
即時脱退	4.1(3)	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 または MLD インターフェイスで IGMPv2 または MLDv1 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抑えます。 • MLD インターフェイス パラメータの設定



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 の情報, 59 ページ](#)
- [PIM および PIM6 のライセンス要件, 80 ページ](#)
- [PIM および PIM6 の前提条件, 80 ページ](#)
- [PIM および PIM6 に関する注意事項と制限事項, 80 ページ](#)
- [デフォルト設定, 81 ページ](#)
- [PIM および PIM6 の設定, 82 ページ](#)
- [PIM および PIM6 の設定の確認, 124 ページ](#)
- [統計情報の表示, 125 ページ](#)
- [PIM の設定例, 126 ページ](#)
- [関連資料, 131 ページ](#)
- [標準, 131 ページ](#)
- [MIB, 132 ページ](#)
- [PIM と PIM6 の機能履歴, 132 ページ](#)

PIM および PIM6 の情報



(注) Cisco NX-OS Release 5.0(2a) 以降では、双方向フォワーディング検出 (BFD) が PIM をサポートします。『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

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

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、Rendezvous Point (RP; ランデブーポイント)、メッセージパケットフィルタリング、および統計情報を設定できます。PIM 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 Designated Router (DR; 指定ルータ) のプライオリティ設定を実行できます。詳細については、「PIM または PIM6 スパースモードの設定」を参照してください。



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

Cisco NX-OS でマルチキャスト機能をイネーブルにするには、各ルータで PIM または 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。IGMP および MLD の設定方法については、「IGMP の設定」および「MLD の設定」を参照してください。



(注) Nexus 7000 シリーズデバイス用の Cisco NX-OS Release 5.2(1) 以降では、PIMv4 を設定し、発信インターフェイス (OIFs) を含む総称ルーティングカプセル化 (GRE) トンネルを通して実行できます。

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 3 つのツリー配信モードで利用できます。

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

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。

3つのモードを組み合わせて、さまざまな範囲のグループアドレスに対応することができます。詳細については、「PIM および PIM6 の設定」を参照してください。

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。

hello メッセージ

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

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

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

hello メッセージ認証の設定方法については、「PIM または PIM6 スパースモードの設定」を参照してください。

Join/Prune メッセージ

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

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

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



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

Join/Prune メッセージは、ソフトウェアからできるだけ短時間で送信されます。Join/Prune メッセージをフィルタリングするには、ルーティングポリシーを定義します。Join/Prune メッセージのポリシーの設定方法については、「PIM または PIM6 スパースモードの設定」を参照してください。

ステートのリフレッシュ

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

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

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

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

ランデブーポイント

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

スタティック RP

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

スタティック RP を定義するのは、次のような場合です。

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

スタティック RP の設定方法については、「スタティック RP の設定」を参照してください。

BSR

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



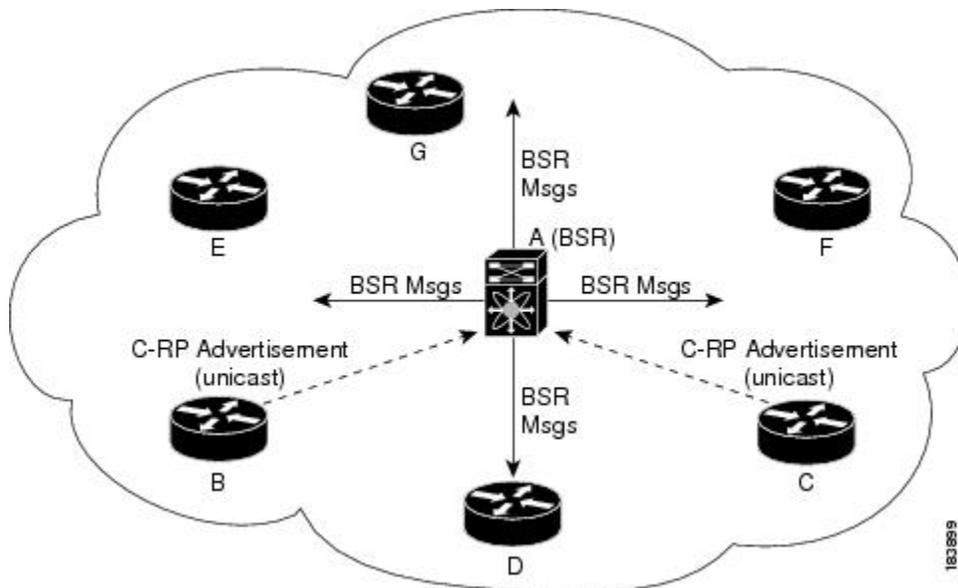
注意

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

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

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

図 13: BSR メカニズム



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

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

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



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

BSR および候補 RP の設定方法については、「*BSR の設定*」を参照してください。

Auto-RP

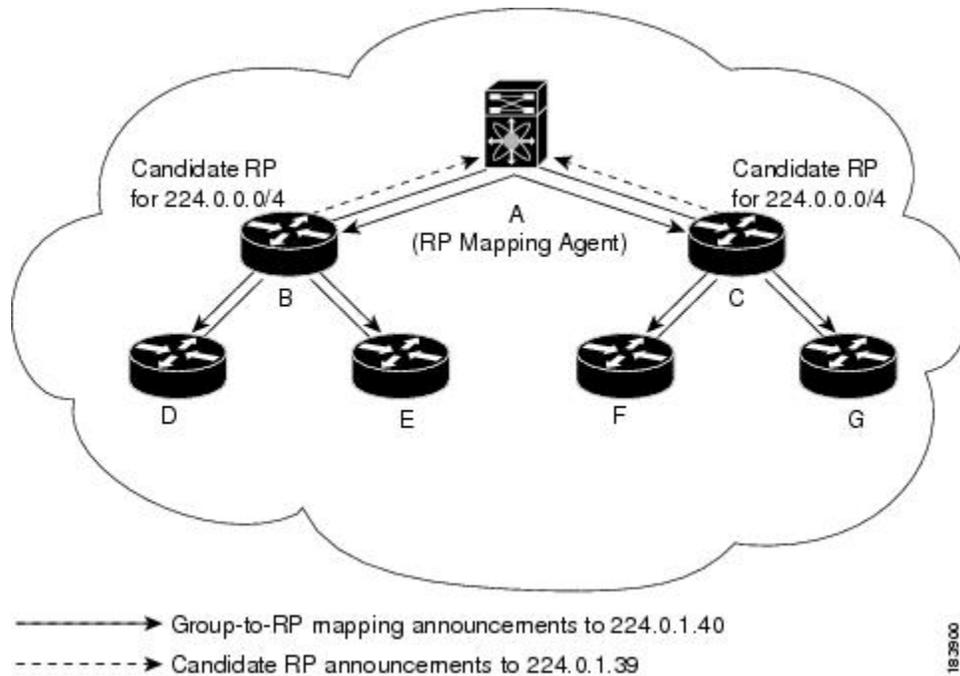
Auto-RP は、インターネット標準であるブートストラップルータメカニズムの前身となったシスコのプロトコルです。Auto-RP を設定するには、候補マッピングエージェントおよび候補 RP を選択します。候補 RP は、サポート対象グループ範囲を含んだ RP-Announce メッセージを Cisco RP-Announce マルチキャストグループ 224.0.1.39 に送信します。Auto-RP マッピングエージェントは候補 RP からの RP-Announce メッセージを受信して、グループと RP 間のマッピングテーブルを形成します。マッピングエージェントは、このグループと RP 間の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



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

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

図 14 : *Auto-RP* のメカニズム



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



(注) Auto-RP は PIM6 ではサポートされていません。

Auto-RP の設定方法については、「*Auto-RP* の設定」を参照してください。

1 つの PIM ドメイン内の複数の RP

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

PIM BSR ブートストラップ/*Auto-RP* マッピング エージェントの選定プロセス

この項では、BSR ブートストラップ *Auto-RP* マッピング エージェントの選定プロセスについて説明します。

ブートストラップルータ (BSP) の選定プロセスの詳細

- BSR プライオリティが異なる場合は、プライオリティが最も高い（数値が最も大きい）BSR が PIM ドメインの BSR ルータとして選定されます（設定例 1 を参照）。
 - 設定例 1（異なる BSR 候補プライオリティ）：この例の場合、プライオリティが最も高い N7K-1 というラベルのデバイスが、PIM ドメインの BSR 候補として選定されます。N7K-2 というラベルが設定されたデバイスのプライオリティは、デフォルトの 64 です。

N7K-1 の設定：

```
interface loopback0
 ip address 192.168.1.1/32
 ip pim sparse-mode

ip pim bsr bsr-candidate loopback0 priority 128

ip pim bsr forward listen
```

N7K-2 の設定：

```
interface loopback0
 ip address 192.168.2.1/32
 ip pim sparse-mode

ip pim bsr bsr-candidate loopback0

ip pim bsr forward listen
```

N7K-1 の確認：

```
show ip pim rp
PIM RP Status Information for VRF "default"
BSR: 192.168.1.1*, next Bootstrap message in: 00:00:12,
priority: 128, hash-length: 30
```

N7K-2 の確認：

```
show ip pim rp
PIM RP Status Information for VRF "default"
BSR: 192.168.1.1, uptime: 00:04:27, expires: 00:02:00,
priority: 128, hash-length: 30
```

- BSR プライオリティが同じ場合は、BSR 候補 IP アドレスが最上位である BSR が、PIM ドメインの BSR ルータとして選定されます（設定例 2 を参照）。
 - 設定例 2（同じ BSR 候補プライオリティ）：この例の場合、BSR 候補 IP アドレスが最上位である N7K-2 というラベルのデバイスが、PIM ドメインの BSR として選定されます。

N7K-1 の設定 :

```
interface loopback0
  ip address 192.168.1.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0

ip pim bsr forward listen
```

N7K-2 の設定 :

```
interface loopback0
  ip address 192.168.2.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0

ip pim bsr forward listen
```

N7K-1 の確認 :

```
show ip pim rp
PIM RP Status Information for VRF "default"
  BSR: 192.168.2.1, uptime: 01:45:20, expires: 00:01:54,
  priority: 64, hash-length: 30
```

N7K-2 の確認 :

```
show ip pim rp
PIM RP Status Information for VRF "default"
  BSR: 192.168.2.1*, next Bootstrap message in: 00:00:30,
  priority: 64, hash-length: 30
```

Auto-RP マッピング エージェントの選定プロセス

- マッピング エージェント IP アドレスが最上位であるルータが、PIM 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。Auto-RP マッピング エージェントにプライオリティを設定することはできません（設定例を参照）。
 - 設定例（最上位の IP アドレス）：この例の場合、マッピング エージェント IP アドレスが最上位である N7K-2 というラベルのデバイスが、PIM 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。

N7K-1 の設定 :

```
interface loopback0
  ip address 192.168.1.1/32
  ip pim sparse-mode

ip pim auto-rp mapping-agent loopback0

ip pim auto-rp forward listen
```

N7K-2 の設定 :

```
interface loopback0
  ip address 192.168.2.1/32
  ip pim sparse-mode

ip pim auto-rp mapping-agent loopback0

ip pim auto-rp forward listen
```

N7K-1 の確認 :

```
show ip pim rp
PIM RP Status Information for VRF "default"
BSR disabled
Auto-RP RPA: 192.168.2.1, next Discovery message in: 00:00:52
```

N7K-2 の確認 :

```
show ip pim rp
PIM RP Status Information for VRF "default"
BSR disabled
Auto-RP RPA: 192.168.2.1*, next Discovery message in: 00:00:47
```

PIM RP 対 RP の選定プロセス

この表は、ネットワーク内で BSR、Auto-RP、またはスタティック RP 設定を使用して複数の RP が設定されている場合に、マルチキャストグループの RP の選択に使用されるプロセスを示しています。

BSR-RP 対 BSR-RP	BSR-RP 対 スタティック RP	Auto-RP 対 Auto-RP	Auto-RP 対 スタティック RP
1. 最も詳細な RP グループリスト			
2. 最も低い RP プライオリティ	2. 最上位の RP IP アドレス	2. 最上位の RP IP アドレス	2. 最上位の RP IP アドレス
3. 最上位の RP IP アドレス	—	—	—



(注) BSR-RP 対 Auto-RP は、同じネットワーク内で同時に実行しないことが推奨されるため、この表には示していません。

PIM BSR RP 候補対 BSR RP 候補の選定プロセス

- 最も詳細なグループリストを持つ BSR RP 候補が、設定済みのグループリスト内に指定されているあらゆるマルチキャストアドレスに対し、RP として選定されます。最も詳細なグループリストは、BSR RP 候補プライオリティや最上位の BSR RP 候補 IP アドレスよりも優先されます（設定例 1 を参照）。
 - 設定例 1（最も詳細なグループリスト）：この例の場合、224.1.1.0/24 グループリスト内に指定されているすべてのマルチキャストアドレスに対し、N7K-1 というラベルのデバイスが RP として選定されます。あまり詳細でない 224.0.0.0/4 グループリスト内のマルチキャストアドレスに対しては、N7K-2 というラベルのデバイスが選定されます。

N7K-1 の設定：

```
interface loopback0
  ip address 192.168.1.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim bsr rp-candidate loopback0 group-list 224.1.1.0/24
ip pim bsr forward listen
```

N7K-2 の設定：

```
interface loopback0
  ip address 192.168.2.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim bsr rp-candidate loopback0 group-list 224.0.0.0/4
ip pim bsr forward listen
```

N7K-1 の確認：

```
show ip pim group 224.1.1.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.1.1.0/24     ASM      192.168.1.1    -

show ip pim group 224.3.0.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.0.0.0/4     ASM      192.168.2.1    -
```

N7K-2 の確認：

```
show ip pim group 224.1.1.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.1.1.0/24     ASM      192.168.1.1    -

show ip pim group 224.3.0.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.0.0.0/4     ASM      192.168.2.1    -
```

- 複数の BSR RP 候補が同じグループリスト（224.0.0.0/4 など）をアドバタイズした場合は、グループリスト内に指定されているあらゆるマルチキャストアドレスに対し、プライオリ

ティが最も高い（数値が最も小さい）BSR RP 候補が RP として選定されます（設定例 2 を参照）。

- 設定例 2（同じグループリストで、RP プライオリティが異なる）：この例の場合、224.0.0.0/4 グループリスト内に指定されているすべてのマルチキャストアドレスに対し、RP 候補プライオリティが最も低い N7K-1 というラベルのデバイスが RP として選定されます。N7K-2 というラベルのデバイスのプライオリティは、デフォルトの 192 です。

N7K-1 の設定：

```
interface loopback0
  ip address 192.168.1.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim bsr rp-candidate loopback0 group-list 224.0.0.0/4 priority 10
ip pim bsr forward listen
```

N7K-2 の設定：

```
interface loopback0
  ip address 192.168.2.1/32
  ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim bsr rp-candidate loopback0 group-list 224.0.0.0/4
ip pim bsr forward listen
```

N7K-1 の確認：

```
show ip pim rp
PIM RP Status Information for VRF "default"
BSR: 192.168.2.1, uptime: 00:09:14, expires: 00:01:37,
  priority: 64, hash-length: 30
Auto-RP disabled
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None

RP: 192.168.1.1*, (0), uptime: 00:08:15, expires: 00:01:57,
  priority: 10, RP-source: 192.168.2.1 (B), group ranges:
224.0.0.0/4

RP: 192.168.2.1, (0), uptime: 00:08:15, expires: 00:01:57,
  priority: 192, RP-source: 192.168.2.1 (B), group ranges:
224.0.0.0/4

show ip pim group 224.1.1.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.0.0.0/4      ASM       192.168.1.1
```

N7K-2 の確認 :

```

show ip pim rp
PIM RP Status Information for VRF "default"
BSR: 192.168.2.1*, next Bootstrap message in: 00:00:55,
  priority: 64, hash-length: 30
Auto-RP disabled
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None

RP: 192.168.1.1, (0), uptime: 00:11:34, expires: 00:02:26,
  priority: 10, RP-source: 192.168.1.1 (B), group ranges:
224.0.0.0/4

RP: 192.168.2.1*, (0), uptime: 00:12:21, expires: 00:02:22,
  priority: 192, RP-source: 192.168.2.1 (B), group ranges:
224.0.0.0/4

show ip pim group 224.1.1.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.0.0.0/4      ASM      192.168.1.1      -

```

- 複数の BSR RP 候補が同じグループリスト (224.0.0.0/4 など) をアドバタイズした場合で、それらが同じ BSR RP 候補プライオリティで設定されている場合は、グループリスト内に指定されているあらゆるマルチキャストアドレスに対し、IP アドレスが最上位である BSR RP 候補が RP として選定されます (設定例 3 を参照)。

◦ 設定例 3 (RP プライオリティおよびグループリストが同じ) : この例の場合、224.0.0.0/4 グループリスト内に指定されているすべてのマルチキャストアドレスに対し、RP 候補 IP アドレスが最上位である N7K-2 というラベルのデバイスが RP として選定されます。

N7K-1 の設定 :

```

interface loopback0
 ip address 192.168.1.1/32
 ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim bsr rp-candidate loopback0 group-list 224.0.0.0/4
ip pim bsr forward listen

```

N7K-2 の設定 :

```

interface loopback0
 ip address 192.168.2.1/32
 ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim bsr rp-candidate loopback0 group-list 224.0.0.0/4
ip pim bsr forward listen

```

N7K-1 の確認 :

```
show ip pim group 224.1.1.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.0.0.0/4      ASM       192.168.2.1    -
```

N7K-2 の確認 :

```
show ip pim group 224.1.1.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.0.0.0/4      ASM       192.168.2.1    -
```

PIM BSR RP 候補対スタティック RP の選定プロセス

- 最も詳細なグループリストを持つ RP が、設定済みのグループリスト内に指定されているあらゆるマルチキャストアドレスに対し、RP として選定されます。最も詳細なグループリストは、最上位の RP IP アドレスよりも優先されます（設定例 1 を参照）。（RP プライオリティは、BSR RP 候補をスタティック RP と比較する際には適用されません）。
 - 設定例 1（最も詳細なグループリスト）：この例の場合、224.1.1.0/24 グループリスト内に指定されているすべてのマルチキャストアドレスに対し、N7K-1 というラベルのデバイスが BSR RP として選定されます。あまり詳細でない 224.0.0.0/4 グループリスト内のマルチキャストアドレスに対しては、スタティック RP ステートメントにより、N7K-2 というラベルのデバイスが RP として選定されます。

N7K-1 の設定 :

```
interface loopback0
 ip address 192.168.1.1/32
 ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim rp-address 192.168.2.1 group-list 224.0.0.0/4
ip pim bsr rp-candidate loopback0 group-list 224.1.1.0/24
ip pim forward listen
```

N7K-2 の設定 :

```
interface loopback0
 ip address 192.168.2.1/32
 ip pim sparse-mode

ip pim rp-address 192.168.2.1 group-list 224.0.0.0/4
ip pim bsr forward listen
```

N7K-1 の確認 :

```
show ip pim group 224.1.1.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.1.1.0/24     ASM       192.168.1.1    -

show ip pim group 224.3.0.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.0.0.0/4     ASM       192.168.2.1    -
```

N7K-2 の確認 :

```
show ip pim group 224.1.1.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.1.1.0/24     ASM       192.168.1.1    -

show ip pim group 224.3.0.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.0.0.0/4     ASM       192.168.2.1    -
```

- スタティック RP および BSR RP 候補が同じグループリスト (224.0.0.0/4 など) をアドバタイズした場合は、グループリスト内に指定されているあらゆるマルチキャストアドレスに対し、RP IP アドレスが最上位である候補が RP として選定されます (設定例 2 を参照)。
 - 設定例 2 (同じ RP グループリスト) : この例の場合、224.0.0.0/4 グループリスト内に指定されているすべてのマルチキャストアドレスに対し、RP IP アドレスが最上位である N7K-2 というラベルのデバイスが RP として選定されます。

N7K-1 の設定 :

```
interface loopback0
 ip address 192.168.1.1/32
 ip pim sparse-mode

ip pim rp-address 192.168.1.1 group-list 224.0.0.0/4

ip pim bsr forward listen
```

N7K-2 の設定 :

```
interface loopback0
 ip address 192.168.2.1/32
 ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim rp-address 192.168.1.1 group-list 224.0.0.0/4
ip pim bsr rp-candidate loopback0 group-list 224.0.0.0/4
ip pim bsr forward listen
```

N7K-1 の確認 :

```
show ip pim group 224.1.1.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.0.0.0/4     ASM       192.168.2.1
```

N7K-2 の確認 :

```
show ip pim group 224.1.1.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.0.0.0/4      ASM       192.168.2.1    -
```

- スタティック RP は設定できず、そのデフォルト値は 0 です。したがって、RP プライオリティは影響を与えません。BSR RP 候補には、0～255 の値を設定できます。システムでは、最も詳細なグループリストを持つデバイスが選定されます。両方のデバイスが同じグループリストを持つ場合は、RP IP アドレスが最上位であるデバイスが選定されます（設定例 3 を参照）。
 - 設定例 3（同じグループリストで同じ RP プライオリティ）：この例の場合、224.0.0.0/4 グループリスト内に指定されているすべてのマルチキャストアドレスに対し、RPIP アドレスが最上位である N7K-2 というラベルのデバイスが RP として選定されます。BSR RP とスタティック RP の間で RP プライオリティは比較されません。

N7K-1 の設定 :

```
interface loopback0
 ip address 192.168.1.1/32
 ip pim sparse-mode

ip pim bsr bsr-candidate loopback0
ip pim rp-address 192.168.2.1 group-list 224.0.0.0/4
ip pim bsr rp-candidate loopback0 group-list 224.0.0.0/4 priority 0

ip pim bsr forward listen
```

N7K-2 の設定 :

```
interface loopback0
 ip address 192.168.2.1/32
 ip pim sparse-mode

ip pim rp-address 192.168.2.1 group-list 224.0.0.0/4

ip pim bsr forward listen
```

N7K-1 の確認：

```

show ip pim rp
PIM RP Status Information for VRF "default"
BSR: 192.168.1.1*, next Bootstrap message in: 00:00:52,
  priority: 64, hash-length: 30
Auto-RP disabled
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None

RP: 192.168.1.1*, (0), uptime: 00:01:57, expires: 00:02:25,
priority: 0, RP-source: 192.168.1.1 (B), group ranges:
  224.0.0.0/4
RP: 192.168.2.1, (0), uptime: 02:16:09, expires: never,
priority: 0, RP-source: (local), group ranges:
  224.0.0.0/4

show ip pim group 224.1.1.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.0.0.0/4      ASM       192.168.2.1     -

```

N7K-2 の確認：

```

show ip pim rp
PIM RP Status Information for VRF "default"
BSR: 192.168.1.1, uptime: 00:29:47, expires: 00:01:45,
  priority: 64, hash-length: 30
Auto-RP disabled
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None

RP: 192.168.1.1, (0), uptime: 00:06:59, expires: 00:02:05,
priority: 0, RP-source: 192.168.1.1 (B), group ranges:
  224.0.0.0/4
RP: 192.168.2.1*, (0), uptime: 00:13:15, expires: never,
priority: 0, RP-source: (local), group ranges:
  224.0.0.0/4

show ip pim group 224.1.1.0
PIM Group-Range Configuration for VRF "default"
Group-range      Mode      RP-address      Shared-tree-only range
224.0.0.0/4      ASM       192.168.2.1     -

```

PIM Auto-RP 候補対 Auto-RP 候補の選定プロセス

Auto-RP 候補の選定は、BSR RP 候補の選定プロセスと似ていますが、プライオリティはサポートされていません（「PIM BSR RP 候補対 BSR RP 候補の選定プロセス」を参照）。Auto-RP にプライオリティを設定することはできません。デフォルト値は 0 です。

PIM Auto-RP 候補対 スタティック RP の選定プロセス

Auto-RP 候補対スタティック RP の選定には、BSR RP 候補対スタティック RP の選定プロセスと同じルールが使用されます（「PIM BSR RP 候補対 スタティック RP の選定プロセス」を参照）。

Anycast-RP

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

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

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

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

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

Anycast-RP の設定方法については、「*PIM Anycast-RP セットの設定*」を参照してください。

PIM Register メッセージ

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

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

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

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

登録メッセージの IP 送信元アドレスが 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、`ip pim register-source` コマンドを使用して登録メッセージの IP 送信元アドレスを設定できます。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。PIM Register メッセージのポリシーの設定方法については、「ASM 専用の共有ツリーの設定」を参照してください。

指定ルータ

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

各 LAN セグメントの DR は、「hello メッセージ」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、RP 方向または送信元方向に (*, G) または (S, G) PIM Join メッセージを発信します。受信者から送信元へのパスは、各ホップで決定されます。この場合、送信元が受信者または DR で認識されている必要があります。

DR プライオリティの設定方法については、「PIM または PIM6 スパースモードの設定」を参照してください。

Designated Forwarder

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 Designated Forwarder (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 Outgoing Interface (OIF; 発信インターフェイス) 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から転送されます。また、RPF インターフェイスを経由して RP 方向にも転送されます。



(注) Cisco NX-OS は F2 モジュールの PIM Bidir モードをサポートしていません。



(注) Cisco NX-OS では、RPF インターフェイスが Multicast Routing Information Base (MRIB) の OIF リストに追加されますが、Multicast Forwarding Information Base (MFIB) の OIF リストには追加されません。

ASM モードにおける共有ツリーから送信元ツリーへのスイッチオーバー



(注) Cisco NX-OS では、RPF インターフェイスが Multicast Routing Information Base (MRIB) の OIF リストに追加されますが、Multicast Forwarding Information Base (MFIB) の OIF リストには追加されません。

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 Shortest-Path Tree (SPT; 最短パス ツリー) に切り替わります。共有ツリーだけを使用するための設定方法については、「ASM 専用の共有ツリーの設定」を参照してください。

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。

管理用スコープの IP マルチキャスト

管理用スコープの IP マルチキャスト方式を使用すると、マルチキャストデータの配信先を制限できます。詳細については、RFC 2365 を参照してください。

インターフェイスを PIM 境界として設定し、PIM メッセージがこのインターフェイスから送信されないようにできます。ドメイン境界パラメータの設定方法については、「PIM または PIM6 スパースモードの設定」を参照してください。

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

PIM の双方向フォワーディング検出

Cisco NX-OS Release 5.0(2a) 以降では、双方向フォワーディング検出 (BFD) により、ネットワーク内の障害をすばやく検出できます。BFD の詳細については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x』を参照してください。

PIM では、hello インターバルの一部として設定された保持時間が経過すると、リンク グループまたはネイバー グループの障害が検出されます。しかし、BFD はより効率的な障害検出手段を提供します。このプロトコルは、2つのエンドポイント間にリンク経由でセッションを確立し、転送エンジンを使用します。BFD をイネーブルにすると、PIM プロセスはネイバーを検出するたびに BFD セッションを追加しようとします。BFD セッションがすでに存在する場合、PIM はセッションを重複して作成せずに、BFD セッションのステートを含むコールバックを受信します。PIM の BFD は、VRF 単位またはインターフェイス単位でイネーブルにすることができます。

VRF またはインターフェイスの BFD をディセーブルにした場合、インターフェイスが PIM インターフェイスでなくなった場合、および隣接する BFD セッションがダウンした場合、PIM はその BFD セッションを削除します。

仮想化のサポート

Virtual Device Context (VDC; 仮想デバイス コンテキスト) は、一連のシステム リソースを論理的に表現する用語です。各 VDC 内では、複数の Virtual Routing and Forwarding (VRF; 仮想ルーティングおよびフォワーディング) インスタンスを定義できます。システムでは、VDC 内の VRF ごとに、MRIB や M6RIB などの独立したマルチキャスト システム リソースが用意されます。

PIM および PIM6 の **show** コマンドに VRF 引数を指定して実行すると、表示される情報のコンテキストを確認できます。VRF 引数を指定しない場合は、デフォルト VRF が使用されます。

VDC の設定方法については、『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide』を参照してください。

VRF の設定方法については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

ハイ アベイラビリティ

ハイ アベイラビリティの詳細については、『Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide』を参照してください。

PIM および PIM6 のライセンス要件

製品	ライセンス要件
DCNM	<Feature-1>にはライセンスは不要です。ライセンスパッケージに含まれていない機能は Cisco DCNM にバンドルされており、無料で提供されます。DCNM ライセンス方式の詳細については、『 <i>Cisco DCNM Licensing Guide</i> 』を参照してください。
DCNM	<Feature-1>には LAN Enterprise ライセンスが必要です。DCNM ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『 <i>Cisco DCNM Licensing Guide</i> 』を参照してください。
Cisco NX-OS	PIM および PIM6 には Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『 <i>Cisco NX-OS Licensing Guide</i> 』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 Virtual Device Context (VDC; 仮想デバイス コンテキスト) が正しい。VDC は、一連のシステム リソースを論理的に表現する用語です。 `switchto vdc` コマンドでは VDC 番号を指定できます。
- 現在の Virtual Routing and Forwarding (VRF; 仮想ルーティングおよびフォワーディング) モードが正しい (グローバル コマンドの場合)。この章の例で示すデフォルトのコンフィギュレーションモードは、デフォルト VRF に適用されます。

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。

- トンネルインターフェイスは、Cisco NX-OS Release 5.2(1) までは PIM をサポートしません。リリース 5.2(1) から、GRE トンネルインターフェイス上にマルチキャストを設定できるようになりました。
- Cisco NX-OS の PIM および PIM6 は、いずれの形式の PIM デンス モード/PIM スパース モードバージョン 1 とも相互運用性がありません。
- 同じネットワーク内では、Auto-RP プロトコルと BSR プロトコルを同時に設定できません。
- 候補 RP インターバルを 15 秒以上に設定してください。

- デバイスに BSR ポリシーが適用されており、BSR として選定されないように設定されている場合、このポリシーは無視されます。これにより、次のようなデメリットが発生します。
 - ポリシーで許可されている BSM をデバイスが受信した場合、意図に反してこのデバイスが BSR に選定されていると、対象の BSM がドロップされるために下流のルータではその BSM を受信できなくなります。また、下流のデバイスでは、不正な BSR から送信された BSM が正しくフィルタリングされるため、これらのデバイスでは RP 情報を受信できなくなります。
 - BSR に異なるデバイスから送られた BSM が着信すると、新しい BSM が送信されますが、その正規の BSM は下流のデバイスでは受信されません。
- F2 モジュールは、いずれの形式の IPv4 または IPv6 トンネルもサポートしていません。
- リリース 5.x 以降では、PIM の BFD を使用して高速障害検出をサポートすることを推奨します。
- PIM hello 間隔のデフォルト値が推奨されます。この値は変更しないでください。



(注) アグレッシブ PIM タイマーがテストされ、PIM タイマーを変更する必要がある配置でサポートされます。ただしこのテストは限られており、SSO/ISSU はこのような配置で保証されません。の詳細については、『Cisco Nexus 7000 Series NX-OS Verified Scalability Guide』を参照してください。

- Cisco NX-OS PIM および PIM6 は、vPC での BIDR PIM または SSM をサポートしません。

デフォルト設定

表 12: 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	ディセーブル
再起動時にルートをフラッシュ	ディセーブル
ネイバーの変更の記録	ディセーブル
Auto-RP メッセージアクション	ディセーブル
BSR メッセージアクション	ディセーブル
SSM マルチキャスト グループ範囲 またはポリシー	IPv4 では 232.0.0.0/8、IPv6 では FF3x::/96

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

PIM および PIM6 の設定

PIM と PIM6 は、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 のいずれ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 がサポートしているのは PIM スパース モードのバージョン 2 だけです。このマニュアルで「PIM」と記載されている場合は、PIM スパース モードのバージョン 2 を意味しています。

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（次の表を参照）。

マルチキャスト配信モード	RP 設定の必要性	説明
ASM	Yes	任意の送信元のマルチキャスト
Bidir	Yes	双方向共有ツリー
SSM	No	単一送信元のマルチキャスト
マルチキャスト用 RPF ルート	No	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。

- この表に示したマルチキャスト配信モードについて、各モードに設定するマルチキャストグループの範囲を選択します。
- この表に示したマルチキャスト配信モードについて、各モードに設定するマルチキャストグループの範囲を選択します。
- PIM および PIM6 機能をイネーブルにします。
- ステップ 1 で選択したマルチキャスト配信モードについて、次の設定作業を行います。
 - ASM モードまたは 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。
- メッセージフィルタリングを設定します。



(注) 次に、PIM または PIM6 の設定に使用される CLI コマンドの相違点を示します。

- PIM コマンドは **ip pim** で始まり、PIM6 コマンドは **ipv6 pim** で始まります。
- PIM コマンドは **show ip pim** で始まり、PIM6 コマンドは **show ipv6 pim** で始まります。



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

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。

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	feature pim 例： switch(config)# feature pim	PIM をイネーブルにします。デフォルトでは PIM はディセーブルになっています。
ステップ 3	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	show running-configuration pim 例： switch(config)# show running-configuration pim	(任意) feature コマンドを含む、PIM の実行コンフィギュレーション情報を示します。
ステップ 5	show running-configuration pim6 例： switch(config)# show running-configuration pim6	(任意) feature コマンドを含む、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	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

PIM 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 13: 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	
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。
Bidir RP 制限	IPv4 および IPv6 に設定可能な Bidir RP の数を設定します。PIM と PIM6 を組み合わせている場合は、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。デフォルトは、IPv4 の場合が 6、IPv6 の場合が 2 です。
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。有効な範囲は 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
指定ルータのプライオリティ	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。
hello 認証モード	<p>インターフェイスで、PIM hello メッセージ内の MD5 ハッシュ認証キー (パスワード) をイネーブルにして、直接接続されたネイバーによる相互認証を可能にします。PIM hello メッセージは、認証ヘッダー (AH) オプションを使用して符号化された IP セキュリティです。暗号化されていない (クリアテキストの) キーか、または次に示す値のいずれかを入力したあと、スペースと MD5 認証キーを入力します。</p> <ul style="list-style-type: none"> • 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。 <p>認証キーの文字数は最大 16 文字です。デフォルトでは無効になっています。</p> <p>(注) PIM6 は hello 認証をサポートしません。</p>
hello 間隔	<p>hello メッセージの送信インターバルを、ミリ秒単位で設定します。指定できる範囲は 1000 ~ 18724286 です。デフォルト値は 30000 です。</p> <p>(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 7000 Series NX-OS Verified Scalability Guide』を参照してください。</p>
ドメイン境界	<p>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。デフォルトでは無効になっています。</p> <p>(注) PIM6 は、Auto-RP 方式をサポートしていません。</p>

パラメータ	説明
ネイバー ポリシー	<p>ルートマップ ポリシーに基づいて PIM ネイバーの隣接関係を設定します。³ 隣接関係は、match ip[v6] address コマンドを使用して IP アドレスで指定できます。指定したポリシー名が存在しない場合、または IP アドレスがポリシー内で設定されていない場合は、すべてのネイバーとの隣接関係が確立されます。デフォルトでは、すべての PIM ネイバーと隣接関係が確立されます。</p> <p>(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。</p>

- ³ ルートマップ ポリシーの設定方法については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

PIM スパース モード パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： <pre>switch# config t 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	ip pim auto-rp {listen [forward] [forward [listen]]} 例： <pre>switch(config)# ip pim auto-rp listen</pre>	(任意) Auto-RP メッセージの受信と転送をイネーブルにします。デフォルトではこれらの機能がディセーブルになっているため、Auto-RP メッセージの受信と転送は行われません。
ステップ 3	ip pim bsr {listen [forward] [forward [listen]]} 例： <pre>switch(config)# ip pim bsr forward</pre>	(任意) Auto-RP メッセージの受信と転送をイネーブルにします。デフォルトではこれらの機能がディセーブルになっているため、Auto-RP メッセージの受信と転送は行われません。
ステップ 4	show ip pim rp [ip-prefix] [forward vrf [vrf-name all]] 例： <pre>switch(config)# show ip pim rp</pre>	(任意) Auto-RP メッセージの受信と転送をイネーブルにします。デフォルトではこれらの機能がディセーブルになっているため、Auto-RP メッセージの受信と転送は行われません。
ステップ 5	ip pim bidir-rp-limit limit 例： <pre>switch(config)# ip pim bidir-rp-limit 4</pre>	(任意) IPv4 に設定可能な Bidir RP の数を指定します。PIM と PIM6 を組み合わせている場合は、各 VRF でサポートする Bidir RP の最大数を 8 以下にする必

	コマンドまたはアクション	目的
		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 6	ip pim register-rate-limit rate 例： switch(config)# ip pim register-rate-limit 1000	(任意) レート制限を毎秒の packets 数で設定します。有効な範囲は 1 ~ 65,535 です。デフォルト設定は無制限です。
ステップ 7	[ip ipv4] routing multicast holddown holddown-period 例： switch(config)# ip routing multicast holddown 100	(任意) 初期ホールドダウン期間を秒単位で設定します。指定できる範囲は 90 ~ 210 です。ホールドダウン期間をディセーブルにするには、0 を指定します。デフォルト値は 210 です。
ステップ 8	show running-configuration pim 例： switch(config)# show running-configuration pim	(任意) 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： switch(config)# interface ethernet 2/1 switch(config-if)#	ethernet slot/port などのインターフェイス タイプおよび番号を入力して、インターフェイス モードを開始します。
ステップ 10	ip pim sparse-mode 例： switch(config-if)# ip pim sparse-mode	現在のインターフェイスで PIM スパース モードをイネーブルにします。デフォルトでは無効になっています。
ステップ 11	ip pim dr-priority priority 例： switch(config-if)# ip pim dr-priority 192	(任意) PIM hello メッセージの一部としてアドバタイズされる Designated Router (DR; 指定ルータ) プライオリティを設定します。有効範囲は 1 ~ 4294967295 です。デフォルトは、1 です。
ステップ 12	ip pim hello-authentication ah-md5 auth-key 例： switch(config-if)# ip pim hello-authentication ah-md5 my_key	(任意) PIM hello メッセージ内の MD5 ハッシュ認証キーをイネーブルにします。暗号化されていない (クリアテキストの) キーか、または次に示す値のいずれかを入力したあと、スペースと MD5 認証キーを入力します。 <ul style="list-style-type: none"> • 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。

	コマンドまたはアクション	目的
		キーの文字数は最大16文字です。デフォルトでは無効になっています。
ステップ 13	ip pim hello-interval <i>interval</i> 例： <pre>switch(config-if)# ip pim hello-interval 25000</pre>	(任意) hello メッセージの送信インターバルを、ミリ秒単位で設定します。指定できる範囲は 1000 ~ 18724286 です。デフォルト値は 30000 です。 (注) Cisco NX-OS Release 5.2(1) 以前は、最小値は 1 ミリ秒でした。
ステップ 14	ip pim border 例： <pre>switch(config-if)# ip pim border</pre>	(任意) インターフェイスを PIM ドメインの境界として設定し、対象のインターフェイスで、ブートストラップ、候補 RP、または Auto-RP の各メッセージが送受信されないようにします。デフォルトでは無効になっています。
ステップ 15	ip pim neighbor-policy <i>policy-name</i> 例： <pre>switch(config-if)# ip pim neighbor-policy my_neighbor_policy</pre>	(任意) インターフェイスを PIM ドメインの境界として設定し、対象のインターフェイスで、ブートストラップ、候補 RP、または Auto-RP の各メッセージが送受信されないようにします。デフォルトでは無効になっています。 (任意) <code>match ip address</code> コマンドを使用し、ルートマップポリシーに基づいて PIM ネイバーの隣接関係を設定します。ポリシー名の文字数は最大63文字です。デフォルトでは、すべての PIM ネイバーと隣接関係が確立されます。 (注) この機能の設定は、経験を積んだネットワーク管理者が行うことを推奨します。
ステップ 16	show ip pim interface [<i>interface</i> <i>brief</i>] [<i>vrf</i> [<i>vrf-name</i> <i>all</i>]] 例： <pre>switch(config-if)# show ip pim interface</pre>	(任意) PIM インターフェイス情報を表示します。
ステップ 17	copy running-config startup-config 例： <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。 (任意) <code>match ip address</code> コマンドを使用し、ルートマップポリシーに基づいて PIM ネイバーの隣接関係を設定します。ポリシー名の文字数は最大63文字です。デフォルトでは、すべての PIM ネイバーと隣接関係が確立されます。

PIM6 スパース モード パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t 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	ipv6 pim bsr {listen[forward] forward[listen]} 例： switch(config)# ip pim auto-rp listen	(任意) BSR メッセージの受信と転送をイネーブルにします。デフォルトではこれらの機能がディセーブルになっているため、BSR メッセージの受信と転送は行われません。
ステップ 3	show ipv6 pim rp [ipv6-prefix][vrfvrf-name all] 例： switch(config)# show ipv6 pim rp	(任意) BSR の受信/転送ステートなど、PIM6 RP 情報を表示します。
ステップ 4	ipv6 pim bidir-rp-limit limit 例： switch(config)# ipv6 pim bidir-rp-limit 4	(任意) IPv6 に設定可能な Bidir RP の数を指定します。PIM と PIM6 を組み合わせている場合は、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。デフォルトは 2 です。
ステップ 5	ipv6 pim register-rate-limit rate 例： switch(config)# ipv6 pim register-rate-limit 1000	(任意) レート制限を毎秒のパケット数で設定します。有効な範囲は 1 ~ 65,535 です。デフォルト設定は無制限です。
ステップ 6	ipv6 routing multicast holddown holddown-period 例： switch(config)# ipv6 routing multicast holddown 100	(任意) 初期ホールドダウン期間を秒単位で設定します。指定できる範囲は 90 ~ 210 です。ホールドダウン期間をディセーブルにするには、0 を指定します。デフォルト値は 210 です。
ステップ 7	show running-configuration pim6 例： switch(config)# show running-configuration pim6	(任意) Bidir RP 制限および Register のレート制限を含む、PIM6 実行コンフィギュレーション情報を表示します。

	コマンドまたはアクション	目的
ステップ 8	interface <i>interface</i> 例： switch(config)# interface ethernet 2/1 switch(config-if)#	指定したインターフェイスでインターフェイスモードを開始します。
ステップ 9	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。デフォルトでは無効になっています。
ステップ 10	ipv6 pim dr-priority <i>priority</i> 例： switch(config-if)# ipv6 pim dr-priority 192	(任意) PIM6 hello メッセージの一部としてアドバタイズされる Designated Router (DR; 指定ルータ) プライオリティを設定します。有効範囲は 1 ~ 4294967295 です。デフォルトは、1 です。
ステップ 11	ipv6 pim hello-interval <i>interval</i> 例： switch(config-if)# ipv6 pim hello-interval 25000	(任意) hello メッセージの送信インターバルを、ミリ秒単位で設定します。指定できる範囲は 1000 ~ 18724286 です。デフォルト値は 30000 です。 (注) Cisco NX-OS Release 5.2(1) 以前は、最小値は 1 ミリ秒でした。
ステップ 12	ipv6 pim border 例： switch(config-if)# ipv6 pim border	(任意) 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 の各メッセージが送受信されないようにします。デフォルトでは無効になっています。 (注) Cisco NX-OS Release 5.2(1) 以前は、最小値は 1 ミリ秒でした。
ステップ 13	ipv6 pim neighbor-policy <i>policy-name</i> 例： switch(config-if)# ip pim border	(任意) match ipv6 address コマンドを使用し、ルートマップポリシーに基づいて PIM6 ネイバーの隣接関係を設定します。ポリシー名の文字数は最大 63 文字です。デフォルトでは、すべての 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 14	show ipv6 pim interface [<i>interface</i> <i>brief</i>] [<i>vrfvrf-name</i> all] 例： switch(config-if)# show ipv6 pim interface	(任意) PIM6 インターフェイス情報を表示します。

	コマンドまたはアクション	目的
ステップ 15	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 および Bidir の設定

Any Source Multicast (ASM) および Bidirectional shared tree (Bidir; 双方向共有ツリー) 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 モードを有効にするには、スパスモードおよび RP の選択方式を設定します。RP の選択方式では、配信モードを指定して、マルチキャスト グループの範囲を割り当てます。



(注) Bidir モードは virtual Port Channel (vPC; 仮想ポートチャネル) ではサポートされません。vPC の詳細については、『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide』を参照してください。

スタティック RP の設定

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

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

Cisco NX-OS Release 5.1(3) 以降、**ip pim rp-address** コマンドは次の機能で拡張されています。

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



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

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

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

この動作は、Cisco IOS とは異なります。 **ip pim rp-address** コマンドのその他の例の動作については、『Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference』を参照してください。

スタティック RP (PIM) の設定

はじめる前に

Enterprise Services ライセンスがインストールされていること、および PIM 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。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t 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	ipv6 pim rp-address rp-address [group-list ipv6-prefix route-map policy-name] [bidir] 例： switch(config)# ip pim rp-address 192.0.2.33 group-list 224.0.0.0/9 例： switch(config)# ip pim rp-address 192.0.2.34 group-list 224.128.0.0/9 bidir	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。 bidir キーワードを指定しない場合、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。 例 1 では、指定したグループ範囲に PIM6 ASM モードを設定しています。 例 2 では、指定したグループ範囲に PIM6 Bidir モードを設定しています。
ステップ 3	show ip pim group-range ipv6-prefix vrf vrf-name all 例： switch(config)# show ip pim group-range	(任意) BSR の受信/転送ステートなど、PIM6 RP 情報を表示します。
ステップ 4	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

スタティック RP (PIM6) の設定

はじめる前に

Enterprise Services ライセンスがインストールされていること、および PIM 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。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例 : switch# config t 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	ipv6 pim rp-address <i>rp-address</i> [group-list <i>ipv6-prefix</i> route-map <i>policy-nsmr</i>] [bidir] 例 : switch(config)# ipv6 pim rp-address 2001:0db8:0:abcd::1 group-list ffile:abcd:def1::0/24 例 : switch(config)# ipv6 pim rp-address 2001:0db8:0:abcd::2 group-list ffile:abcd:def2::0/96 bidir	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。 bidir キーワードを指定しない場合、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。 例 1 では、指定したグループ範囲に PIM6 ASM モードを設定しています。 例 2 では、指定したグループ範囲に PIM6 Bidir モードを設定しています。
ステップ 3	show ipv6 pim rp <i>ipv6-prefix</i> vrf <i>vrf-name</i> all 例 : switch(config)# show ipv6 pim group-range	(任意) PIM6 モードおよびグループ範囲を表示します。
ステップ 4	copy running-config startup-config 例 : switch(config)# show ipv6 pim group-range	(任意) PIM6 モードおよびグループ範囲を表示します。

BSR の設定

BSR を設定するには、候補 BSR および候補 RP を選択します。



注意

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

候補 BSR の設定では、引数を指定できます（次の表を参照）。

表 14：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。
<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 15：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。

引数またはキーワード	説明
<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、グループ範囲内でプライオリティが最も高い RP が選定されます。プライオリティが等しい場合は、IP アドレスが最上位の RP が選定されます。(最も小さい数値が最も高いプライオリティになります)。この値の範囲は 0 (最も高いプライオリティ) ~ 255 で、デフォルトは 192 です。 (注) このプライオリティは BSR 候補プライオリティとは異なります。BSR 候補プライオリティは、0 ~ 255 の間で、高い値ほどプライオリティが高くなります。
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、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

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

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

候補 BSR および候補 RP を設定する手順は、次のとおりです。

- 1 PIM ドメインの各ルータで BSR メッセージの受信と転送を行うかどうかを設定します。候補 RP または候補 BSR として設定されたルータは、インターフェイスにドメイン境界機能が設定されていない場合、すべての BSR プロトコルメッセージの受信と転送を自動的に実行します。詳細については、「PIM または PIM6 スパース モードの設定」を参照してください。
- 2 候補 BSR および候補 RP として動作するルータを選択します。
- 3 後述の手順に従い、候補 BSR および候補 RP をそれぞれ設定します。
- 4 BSR メッセージフィルタリングを設定します。「メッセージフィルタリングの設定」を参照してください。

BSR (PIM) の設定

はじめる前に

Enterprise Services ライセンスがインストールされていること、および PIM 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。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	ip pim bsr listen forward <i>listen</i> / <i>forward</i> <i>forward</i> / <i>listen</i> 例： switch(config)# ip pim bsr listen forward	リッスンと転送を設定します。 リモート PE 上の各 VRF で確実にこのコマンドを入力してください。
ステップ 3	ip pim bsr[bsr-candidate] interface [hash-len hash-length] [priority priority 例： switch(config)# ip pim bsr-candidate ethernet 2/1 hash-len 24	候補ブートストラップルータ (BSP) を設定します。ブートストラップメッセージで使用される送信元 IP アドレスは、インターフェイスの IP アドレスです。ハッシュ長は 0 ~ 32 であり、デフォルト値は 30 です。プライオリティは 0 ~ 255 であり、デフォルト値は 64 です。
ステップ 4	ip [bsr] rp-candidate interfacegroup-list ip-prefix route-map lpolicy-name prioritypriority interval interval bidir 例： switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24 例： switch(config)# ip pim rp-candidate ethernet 2/1 group-list 239.0.0.0/24 bidir	(任意) IPv6 に設定可能な Bidir RP の数を指定します。PIM と PIM6 を組み合わせている場合は、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。デフォルトは 2 です。 BSR の候補 RP を設定します。プライオリティは 0 (プライオリティが最大) ~ 65,535 であり、デフォルト値は 192 です。インターバルは 1 ~ 65,535 秒であり、デフォルト値は 60 秒です。 (注) 候補 RP インターバルは 15 秒以上に設定することを推奨します。 例 1 では、ASM の候補 RP を設定しています。 例 2 では、Bidir の候補 RP を設定しています。

	コマンドまたはアクション	目的
ステップ 5	show ip pim group-range <i>ip-prefix</i> vrfvrf-name all 例： <pre>switch(config)# show ip pim group-range</pre>	(任意) PIM モードおよびグループ範囲を表示します。
ステップ 6	ipv6 routing multicast holdddownholdddown-period 例： <pre>switch(config)# ipv6 routing multicast holdddown 100</pre>	(任意) コンフィギュレーションの変更を保存します。

BSR (PIM6) の設定

はじめる前に

Enterprise Services ライセンスがインストールされていること、および PIM 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。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： <pre>switch# config t 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	ip pim [bsr] bsr-candidate interface [hash-len hash-length priority priority] 例： <pre>switch(config)# ipv6 pim bsr-candidate ethernet 2/1 hash-len 24 priority 192</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 ~ 128 で、デフォルト値は 126 です。プライオリティは 0 (プライオリティが最小) ~ 255 で、デフォルト値は 64 です。
ステップ 3	ipv6 [bsr] rp-candidate interface group-list ipv6-prefix [route-map policy-name priority priority interval interval]bidir	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。

	コマンドまたはアクション	目的
	<p>例 :</p> <pre>switch(config)# ipv6 pim rp-candidate ethernet 2/1 group-list ffile:abcd:def1::0/24</pre> <p>例 :</p> <pre>switch(config)# ipv6 pim rp-candidate ethernet 2/1 group-list ffile:abcd:def2::0/24 bidir</pre>	<p>例 1 では、ASM の候補 RP を設定しています。</p> <p>例 2 では、Bidir の候補 RP を設定しています。</p>
ステップ 4	<p>show ipv6 pim group-range <i>ipv6-prefix</i> <i>vrfvrf-name</i> all</p> <p>例 :</p> <pre>switch(config)# show ipv6 pim group-range</pre>	<p>(任意) PIM6 モードおよびグループ範囲を表示します。</p>
ステップ 5	<p>copy running-config startup-config <i>holddown-period</i></p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	<p>(任意) コンフィギュレーションの変更を保存します。</p>

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 (次の表を参照)。

表 16 : 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。

引数	説明
scope ttl	RP-Discovery メッセージが転送される最大ホップ数を表す存続可能時間 (TTL) 値。この値の範囲は 1 ~ 255 であり、デフォルト値は 32 です。 (注) 「PIM または PIM6 スパースモードの設定」の境界ドメイン機能を参照してください。

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

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

表 17: Auto-RP 候補 RP の引数およびキーワード

引数またはキーワード	説明
<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。
scope ttl	RP-Discovery メッセージが転送される最大ホップ数を表す存続可能時間 (TTL) 値。この値の範囲は 1 ~ 255 であり、デフォルト値は 32 です。 (注) 「PIM または PIM6 スパースモードの設定」の境界ドメイン機能を参照してください。
<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 ドメインの各ルータで、Auto-RP メッセージの受信と転送を行うかどうかを設定します。候補 RP または Auto-RP マッピング エージェントとして設定されたルータは、インターフェイスにドメイン境界機能が設定されていない場合、すべての Auto-RP プロトコル メッセージの受信と転送を自動的に実行します。詳細については、「PIM または PIM6 スパース モードの設定」を参照してください。
- 2 マッピング エージェントおよび候補 RP として動作するルータを選択します。
- 3 後述の手順に従い、マッピング エージェントおよび候補 RP をそれぞれ設定します。
- 4 Auto-RP メッセージ フィルタリングを設定します。「メッセージ フィルタリングの設定」を参照してください。

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。

Auto RP (PIM) の設定

はじめる前に

Enterprise Services ライセンスがインストールされていること、および PIM 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。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	ip pim {send-rp-discovery { auto-rp mapping-agent }} interface [scope ttl] 例： switch(config)# ip pim auto-rp mapping-agent ethernet 2/1	Auto-RP マッピング エージェントを設定します。Auto-RP Discovery メッセージで使用される送信元 IP アドレスは、インターフェイスの IP アドレスです。デフォルト スコープは 32 です。
ステップ 3	ip pim { send-rp-announce {auto-rp rp-candidate }} autointerface {group-list ip-prefix route_map policy-name} [scope ttl] interval interval] [bidir	Auto-RP の候補 RP を設定します。デフォルト スコープは 32 です。デフォルト インターバルは 60 秒です。デフォルトでは、ASM

	コマンドまたはアクション	目的
	<p>例 :</p> <pre>switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24</pre> <p>例 :</p> <pre>switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24 bidir</pre>	<p>の候補 RP が作成されます。パラメータの詳細については、表 4-8 を参照してください。</p> <p>(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。</p> <p>例 1 では、ASM の候補 RP を設定しています。</p> <p>例 2 では、Bidir の候補 RP を設定しています。</p>
ステップ 4	<p>show ip pim group-range <i>lip-prefix</i>] vrf <i>vrf-name</i> all]</p> <p>例 :</p> <pre>switch(config)# show ip pim group-range</pre>	<p>(任意) PIM モードおよびグループ範囲を表示します。</p>
ステップ 5	<p>copy running-config startup-config <i>rate</i></p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	<p>(任意) コンフィギュレーションの変更を保存します。</p>

PIM Anycast-RP セットの設定

PIM Anycast-RP セットを設定する手順は、次のとおりです。

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

PIM Anycast RP セット (PIM) の設定

はじめる前に

Enterprise Services ライセンスがインストールされていること、および PIM 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。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t 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 loopback number 例： switch(config)# interface loopback 0	インターフェイス ループバックを設定します。 この例では、インターフェイス ループバックを 0 に設定しています。
ステップ 3	ip address ip-prefix 例： switch(config-if)# ip address 192.0.2.3/32	このインターフェイスの IP アドレスを設定します。 この例では、Anycast-RP の IP アドレスを設定しています。
ステップ 4	ip pim sparse-mode	PIM をイネーブルにします。
ステップ 5	exit 例： switch(config)# exit	コンフィギュレーションモードに戻ります。
ステップ 6	ip pim anycast-rp anycast-rp-address anycast-rp-peer-address 例： switch(config)# ip pim anycast-rp 192.0.2.3 192.0.2.31	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 7	RP セットに属する各 RP（ローカルルータを含む）で、同じ Anycast-RP アドレスを使用してステップ 5 を繰り返します。	--
ステップ 8	show ip pim group-range [ip-prefix] [vrf vrf-name all] 例： switch(config)# show ip pim group-range	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。

	コマンドまたはアクション	目的
ステップ 9	copy running-config startup-config [ip-prefix] [vrf vrf-name all] 例 : <pre>switch(config)# 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。

PIM Anycast RP セット (PIM6) の設定

はじめる前に

Enterprise Services ライセンスがインストールされていること、および PIM 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。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例 : <pre>switch# config t 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	interface loopback number 例 : <pre>switch(config)# interface loopback 0</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 ipv6-prefix 例 : <pre>switch(config-if)# ipv6 address 2001:0db8:0:abcd::3/32</pre>	このインターフェイスの IP アドレスを設定します。 この例では、Anycast-RP の IP アドレスを設定しています。
ステップ 4	ip pim sparse-mode	PIM をイネーブルにします。
ステップ 5	exit 例 : <pre>switch(config)# exit</pre>	コンフィギュレーションモードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	ipv6 pim anycast-rp <i>anycast-rp-address</i> <i>anycast-rp-peer-address</i> 例： <pre>switch(config)# ipv6 pim anycast-rp 2001:0db8:0:abcd::3 2001:0db8:0:abcd::31</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 7	RP セットに属する各 RP（ローカルルータを含む）で、同じ Anycast-RP アドレスを使用してステップ 5 を繰り返します。	--
ステップ 8	show ipv6 pim group-range [<i>ipv6-prefix</i>] [<i>vrf vrf-name</i> all] 例： <pre>switch(config)# show ipv6 pim group-range</pre>	(任意) PIM6 モードおよびグループ範囲を表示します。
ステップ 9	copy running-config startup-config [<i>ip-prefix</i>] [<i>vrf vrf-name</i> all] 例： <pre>switch(config)# 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 専用の共有ツリーの設定

共有ツリーを設定できるのは、Any Source Multicast (ASM) グループの最終ホップルータだけです。この場合、新たな受信者がアクティブグループに加入した場合、このルータでは共有ツリーから SPT へのスイッチオーバーは実行されません。**match ip[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 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x』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。

- 1 [Menu Item 1] > [Sub-menu Item 3] を選択して [<Feature-1>] タブを開きます。
- 2 新しい<Feature-1>を作成する場合は、[New] をクリックし、<Feature-1>の名前を入力し、[OK] をクリックします。 <Feature-1> は表示されるリストおよびリストの内容に追加されます。
<Feature-1> を変更する場合、既存の <Feature-1> のリストから選択します。
- 3
- 4 [Save] をクリックして変更を保存します。

<上記の手順を理解するために不可欠でない場合は、他の図を含めないでください>

ASM 専用の共有ツリー (PIM) の設定

はじめる前に

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

手順

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

	コマンドまたはアクション	目的
ステップ 4	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 専用の共有ツリー (PIM6) の設定

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例 : <pre>switch# config t 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	ipv6 pim use-shared-tree-only group-list policy-name 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。 match ipv6 multicast コマンドで、使用するグループを示すルートマップポリシー名を指定します。 デフォルトでは、送信元に対する (*, G) ステートのマルチキャスト パケットを受信すると、ソフトウェアは PIM (S, G) Join メッセージを送信元方向に発信します。
ステップ 3	show ipv6 pim group-range [ip-prefix]vrf vrf-name all 例 : <pre>switch(config)# show ipv6 pim group-range</pre>	(任意) PIM6 モードおよびグループ範囲を表示します。
ステップ 4	copy running-config startup-config 例 : <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。

SSM の設定

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

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

コマンドラインに値を指定することにより、SSM で使用するグループ範囲を設定できます。デフォルトでは、PIM の SSM グループ範囲は 232.0.0.0/8 で、PIM6 の SSM グループ範囲は FF3x/96 です。

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。



(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。

SSM (PIM) の設定

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t 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	[no] ip pim ssm range { ip-prefix none route-mappolicy-name } 例： switch(config)# ip pim ssm range 239.128.1.0/24	SSM モードで処理するグループ範囲を最大 4 つまで設定します。match ip multicast コマンドで、使用するグループプレフィックスを示すルートマップポリシー名を指定できます。デフォルトの範囲は 232.0.0.0/8 です。キーワード none を指定すると、すべてのグループ範囲が削除されます。

	コマンドまたはアクション	目的
	例 : <pre>switch(config)# no ip pim ssm range none</pre>	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、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、SSM 範囲はデフォルトの 232.0.0.0/8 にリセットされます。
ステップ 3	show ip pim group-range [ip-prefix] vrfvrf-name all] 例 : <pre>switch(config)# show ip pim group-range</pre>	
ステップ 4	copy running-config startup-config 例 : <pre>switch(config)# 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。

SSM (PIM6) の設定

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例 : <pre>switch# config t 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	[no] ipv6 pim ssm range { ipv6-prefix none route-mappolicy-name } 例 : <pre>switch(config)# ipv6 pim ssm range FF30::0/32</pre>	SSM モードで処理するグループ範囲を最大 4 つまで設定します。 match ip multicast コマンドで、使用するグループプレフィックスを示すルートマップポリシー名を指定できます。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。デフォルトの範囲は FF3x/96 です。

	コマンドまたはアクション	目的
ステップ 3	show ipv6 pim group-range [<i>ipv6-prefix</i>] vrfvrf-name all]	(任意) PIM6 モードおよびグループ範囲を表示します。
ステップ 4	copy running-config startup-config 例 : switch(config)# copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

マルチキャスト用 RPF ルートの設定

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

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



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

はじめる前に

Enterprise Services ライセンスがインストールされていること、および PIM 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。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例 : switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	ip mroute { <i>ip-addr mask</i> <i>ip-prefix</i> } { <i>next-hop</i> <i>nh-prefix</i> <i>interface</i> } [<i>route-preference</i>] [vrf <i>vrf-name</i>] 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。

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

マルチキャスト マルチパスのディセーブル化

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

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	ip multicast multipath none 例： switch(config)# ip multicast multipath none	マルチキャストマルチパスをディセーブルにします。
ステップ 3	clear ip mroute * vrf vrf-name 例： switch(config)# clear ip mroute *	マルチパス ルートをクリアし、マルチキャストマルチパス抑制をアクティブにします。

RP 情報配信を制御するルートマップの設定

ルートマップは、一部の RP 設定のミスや悪意のある攻撃に対する保護機能を提供します。ルートマップを使用できるコマンドについては、「メッセージフィルタリングの設定」を参照してください。

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

詳細については、「*BSR* の設定」および「*Auto-RP* の設定」を参照してください。



(注) ルートマップに影響を与えるコマンドは、*match ipv6 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 (PIM) の設定

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	route-map map-name [permit deny] [sequence-number] 例： switch(config)# route-map ASM_only permit 10 switch(config-route-map)# 例： switch(config)# route-map Bidir_only permit 10 switch(config-route-map)#	ルートマップ コンフィギュレーション モードを開始します。 (注) このコンフィギュレーションモードでは、 permit キーワードを使用します。
ステップ 3	match ip multicast {{rp ip-address [rp-type rp-type]} {{group-range {gaddr_start to gaddr_end} {group ip-prefix}} {source source-ip-address}} 例： switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type ASM	指定したグループ、RP、および RP タイプを関連付けます。ユーザは RP のタイプ (ASM または Bidir) を指定できます。例で示すとおり、このコンフィギュレーションモードでは、グループおよび RP を指定する必要があります。

	コマンドまたはアクション	目的
	例 : <pre>switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type Bdir</pre>	(注) BSR RP、Auto-RP、およびスタティック RP では、 <code>group-range</code> キーワードは使用できません。このコマンドは、 <code>permit</code> と <code>deny</code> の両方を許可します。一部の <code>match mask</code> コマンドは、 <code>permit</code> または <code>deny</code> を許可しません。
ステップ 4	show route-map 例 : <pre>switch(config-route-map)# show route-map</pre>	(任意) 設定済みのルートマップを表示します。
ステップ 5	copy running-config startup-config 例 : <pre>switch(config-route-map)# copy running-config startup-config</pre>	(任意) 設定済みのルートマップを表示します。

RP 情報配信を制御するルートマップ (PIM6) の設定

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例 : <pre>switch# config t 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	route-map map-name [permit deny] [sequence-number] 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。 (注) このコンフィギュレーションモードでは、 <code>permit</code> キーワードを使用します。

	コマンドまたはアクション	目的
ステップ 3	<p>match ipv6 multicast {{rp ip-address [rp-type rp-type]} {{group-range {gaddr_start to gaddr_end} {group ip-prefix}} {source source-ip-address}}</p> <p>例 :</p> <pre>switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type ASM</pre> <p>例 :</p> <pre>switch(config-route-map)# match ip multicast group 224.0.0.0/4 rp 0.0.0.0/0 rp-type Bdir</pre>	<p>指定したグループ、RP、およびRPタイプを関連付けます。ユーザはRPのタイプ（ASMまたはBidir）を指定できます。例で示すとおり、このコンフィギュレーションモードでは、グループおよびRPを指定する必要があります。</p> <p>(注) BSR RP、Auto-RP、およびスタティック RP では、group-range キーワードは使用できません。このコマンドは、permit と deny の両方を許可します。一部の match mask コマンドは、permit または deny を許可しません。</p>
ステップ 4	<p>show route-map</p> <p>例 :</p> <pre>switch(config-route-map)# show route-map</pre>	<p>(任意) 設定済みのルートマップを表示します。</p>
ステップ 5	<p>copy running-config startup-config</p> <p>例 :</p> <pre>switch(config-route-map)# copy running-config startup-config</pre>	<p>(任意) 設定済みのルートマップを表示します。</p>

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 18: 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。デフォルトでは無効になっています。

メッセージの種類	説明
PIM Register ポリシー	ルートマップポリシーに基づく、PIM Register メッセージのフィルタリングをイネーブルにします。 ⁴ match ip[v6] multicast コマンドで、グループアドレスまたはグループと送信元アドレスを指定できます。このポリシーは、RP として動作するルータに適用されます。デフォルトではこの機能がディセーブルになっているため、PIM Register メッセージのフィルタリングは行われません。
BSR 候補 RP ポリシー	ルートマップポリシー 1 に基づく、BSR 候補 RP メッセージのフィルタリングをイネーブルにします。 match ip[v6] multicast コマンドで、RP、グループアドレス、およびタイプ (Bidir または ASM) を指定できます。このコマンドは、BSR の選定対象のルータで使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。
BSR ポリシー	ルートマップポリシー 1 に基づく、BSR クライアントルータによる BSR メッセージのフィルタリングをイネーブルにします。 match ip[v6] multicast コマンドで、BSR 送信元アドレスを指定できます。このコマンドは、BSR メッセージを受信するクライアントルータで使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。
Auto-RP 候補 RP ポリシー	ルートマップポリシー 1 に基づく、Auto-RP マッピングエージェントによる Auto-RP Announce メッセージのフィルタリングをイネーブルにします。 match ip multicast コマンドで、RP、グループアドレス、およびタイプ (Bidir または ASM) を指定できます。このコマンドは、マッピングエージェントで使用できます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。 (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 1 に基づく、クライアントルータによる Auto-RP Discovery メッセージのフィルタリングをイネーブルにします。 match ip multicast コマンドで、マッピングエージェント送信元アドレスを指定できます。このコマンドは、Discovery メッセージを受信するクライアントルータで使用できます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。 (注) PIM6 は、Auto-RP 方式をサポートしていません。
デバイスの各インターフェイスに適用	

メッセージの種類	説明
Join/Prune ポリシー	ルートマップポリシー 1 に基づく、Join/Prune メッセージのフィルタリングをイネーブルにします。 match ip[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方法については、『Cisco Nexus 7000 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** では (S,G)、(*,G)、または (RP,G) を使用できます
- **register-policy** では (S,G) または (*,G) を使用できます
- **igmp report-policy** では (*,G) または (S,G) を使用できます
- **state-limit reserver-policy** では (*,G) または (S,G) を使用できます
- **auto-rp rp-candidate-policy** では (RP,G) を使用できます
- **bsr rp-candidate-policy** では (RP,G) を使用できます
- **autorp mapping-agent policy** では (S) を使用できます
- **bsr bsr-policy** では (S) を使用できます

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

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

メッセージフィルタリング (PIM) の設定

はじめる前に

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

手順

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

	コマンドまたはアクション	目的
ステップ 7	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>	(任意) ルートマップ ポリシーに基づく、クライアント ルータによる Auto-RP Discovery メッセージのフィルタリングをイネーブルにします。 match ip multicast コマンドで、マッピング エージェント送信元アドレスを指定できます。このコマンドは、Discovery メッセージを受信するクライアントルータで使用できます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。
ステップ 8	interface <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	ip pim jp-policy <i>policy-name</i>[in out] 例： <pre>switch(config-if)# ip pim jp-policy my_jp_policy</pre>	(任意) ルートマップ ポリシーに基づく、Join/Prune メッセージのフィルタリングをイネーブルにします。 match ip multicast コマンドで、グループ、グループと送信元、またはグループと RP アドレスを指定できます。デフォルトでは、Join/Prune メッセージはフィルタリングされません。 Cisco NX-OS Release 4.2(3) 以降では、このコマンドは着信方向と発信方向の両方でメッセージをフィルタリングします。
ステップ 10	show run pim 例： <pre>switch(config-if)# show run pim</pre>	(任意) PIM コンフィギュレーション コマンドを表示します。
ステップ 11	copy running-config startup-config <i>interval</i> 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。

メッセージフィルタリング (PIM6) の設定

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t 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	ipv6 pim log-neighbor-changes 例： switch(config)# ipv6 pim log-neighbor-changes	(任意) ネイバーのステート変更を通知する Syslog メッセージをイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	ipv6 pim register-policy <i>policy-name</i> 例： switch(config)# ipv6 pim register-policy my_register_policy	(任意) ルートマップ ポリシーに基づく、PIM Register メッセージのフィルタリングをイネーブルにします。 match ipv6 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。デフォルトでは無効になっています。
ステップ 4	ipv6 pim bsr rp-candidate-policy <i>policy-name</i> 例： switch(config)# ipv6 pim bsr rp-candidate-policy my_bsr_rp_candidate_policy	(任意) ルートマップポリシーに基づく、BSR 候補 RP メッセージのフィルタリングをイネーブルにします。 match ipv6 multicast コマンドで、RP、グループアドレス、およびタイプ (Bidir または ASM) を指定できます。このコマンドは、BSR の選定対象のルータで使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。
ステップ 5	ipv6 pim bsr bsr-policy <i>policy-name</i> 例： switch(config)# ipv6 pim bsr bsr-policy my_bsr_policy	(任意) ルートマップポリシーに基づく、BSR クライアントルータによる BSR メッセージのフィルタリングをイネーブルにします。 match ipv6 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	interface interface 例： switch(config)# interface ethernet 2/1 switch(config-if)#	指定したインターフェイスでインターフェイスモードを開始します。
ステップ 7	ipv6 pim jp-policy policy-name[in out] 例： switch(config-if)# ipv6 pim jp-policy my_jp_policy	(任意) ルートマップポリシーに基づく、Join/Prune メッセージのフィルタリングをイネーブルにします。 match 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

	コマンドまたはアクション	目的
		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。 Cisco NX-OS Release 4.2(3) 以降では、このコマンドは着信方向と発信方向の両方でメッセージをフィルタリングします。
ステップ 8	show run pim6 例： switch(config-if)# show run pim6	(任意) 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 9	copy running-config startup-config interval 例： switch(config-if)# copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

PIM プロセスおよび PIM6 プロセスの再起動

PIM プロセスおよび PIM6 プロセスを再起動し、オプションとして、すべてのルートをフラッシュすることができます。デフォルトでは、ルートはフラッシュされません。

フラッシュされたルートは、Multicast Routing Information Base (MRIB と M6RIB) および Multicast Forwarding Information Base (MFIB と 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 (PIM) の再起動

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	restart pim 例： switch# restart pim	PIM プロセスを再起動します。
ステップ 2	config t 例： switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 3	ip pim flush-routes 例： switch(config)# ip pim flush-routes	PIM プロセスの再起動時に、ルートを削除します。デフォルトでは、ルータはフラッシュされません。
ステップ 4	show running-configuration pim 例： switch(config)# show running-configuration pim	(任意) flush-routes コマンドを含む、PIM 実行コンフィギュレーション情報を表示します。
ステップ 5	copy running-config startup-config policy-name 例： switch(config)# copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

PIM6 プロセスの再起動

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	restart pim6 例： switch# restart pim	PIM プロセスを再起動します。

	コマンドまたはアクション	目的
ステップ 2	config t 例： switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 3	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	show running-configuration pim6 例： switch(config)# show running-configuration pim6	(任意) 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表示します。
ステップ 5	copy running-config startup-config policy-name 例： switch(config)# copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

VRF モードでの PIM の BFD の設定



(注) PIM の BFD は、VRF またはインターフェイスごとに設定できます。

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t switch(config)#	コンフィギュレーションモードに入ります。

	コマンドまたはアクション	目的
ステップ 2	vrf context <i>vrf-name</i> 例： <pre>switch# vrf convrf-name text test switch(config-vrf)#</pre>	VRF コンフィギュレーションモードを開始します。
ステップ 3	ip pim bfd 例： <pre>switch(config-vrf)# ip pim bfd</pre>	指定した VRF の BFD をイネーブルにします。 (注) コンフィギュレーションモードで ip pim bfd コマンドを入力して、VRF の BFD をイネーブルにすることもできます。 VRF 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

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	config t Example: 例： <pre>switch(config)# interface ethernet 7/40 switch(config-if)#</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	interface <i>interface-type</i> 例： <pre>switch(config)# interface ethernet 7/40 switch(config-if)#</pre>	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	config tip 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、RIM 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。

	コマンドまたはアクション	目的
ステップ 4	exit 例： switch(config)# exit	VRF または 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 5	show running-configuration pim 例： switch(config)# show running-configuration pim	(任意) PIM 実行コンフィギュレーション情報を表示します。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

PIM および PIM6 の設定の確認

PIM および PIM6 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。PIM コマンドでは **show ip** という形式を、PIM6 コマンドでは **show ipv6** という形式を使用します。

コマンド	説明
show ip [v6] mroute { <i>source group</i> <i>group [source]</i> } [vrf <i>vrf-name</i> all]	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。
show ip [v6] pim df [vrf <i>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 [vrf <i>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。同様の情報に関し、 show ip pim rp コマンドも参照してください。
show ip [v6] pim interface [<i>interface</i> brief] [vrf <i>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 [vrf <i>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 <i>group [source]</i> [vrf <i>vrf-name</i> all]	OIF リスト内のすべてのインターフェイスを表示します。

コマンド	説明
show ip [v6] pim route {source group group [source]} [vrf vrf-name all]	各マルチキャスト ルートの情報を表示します。指定した (S, G) に対して、PIM Join メッセージを受信したインターフェイスなどを表示できます。
show ip [v6] pim rp [vrf vrf-name all]	ソフトウェアの既知の Rendezvous Point (RP; ランデブー ポイント) およびその学習方法と、それらのグループ範囲を表示します。同様の情報に関し、 show ip pim group-range コマンドも参照してください。
show ip [v6] pim rp-hash [vrf vrf-name all]	ブートストラップ ルータ (BSP) RP ハッシュ情報を表示します。RP ハッシュの詳細については、 <i>RFC 5059</i> を参照してください。
show running-configuration 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-configuration 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 [vrf-name all] [detail]	各 VRF の情報を表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference*』を参照してください。

統計情報の表示

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

次の表に、PIM および PIM6 の統計情報とメモリ使用状況を表示するコマンドを示します。PIM コマンドでは **show ip** という形式を、PIM6 コマンドでは **show ipv6** という形式を使用します。

コマンド	説明
show ip [v6] pim policy statistics	Register、RP、および Join/Prune メッセージのポリシーについて、ポリシー統計情報を表示します。

コマンド	説明
<code>show ip [v6] pim statistics [vrf vrf-name all]</code>	グローバル統計情報を表示します。PIM が vPC モードの場合は、vPC 統計情報を表示します。

これらのコマンド出力のフィールドの詳細については、『Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference』を参照してください。

PIM および PIM6 の統計情報のクリア

PIM および PIM6 の統計情報をクリアするには、次の表に示す各種コマンドを使用します。PIM コマンドでは `show ip` という形式を、PIM6 コマンドでは `show ipv6` という形式を使用します。

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

PIM の設定例



(注) その他の設定例については、「1つの PIM ドメイン内の複数の RP」を参照してください。

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# config t
```

```
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。「IGMP の設定」を参照してください。通常は、SSM をサポートするために、PIM インターフェイスに IGMPv3 を設定します。

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

次に、PIM SSM モードの設定例を示します。

```
config t
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
```

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# config t
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# config t
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# config t
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# config t
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# config t
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。

```
config t
  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# config t
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# config t
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# config t
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# config t
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# config t
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。

```
config t
  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 Anycast RP の設定例

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

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

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

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

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

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

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

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

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

Prefix-Based および Route-Map-Based の設定

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

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

ip prefix-list plist33 seq 10 deny 231.129.128.0/17
```

```

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

ip pim rp-address 21.21.0.11 prefix-list plist11
ip pim rp-address 21.21.0.22 prefix-list plist22
ip pim rp-address 21.21.0.33 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 21.21.0.11 route-map rmap11
ip pim rp-address 21.21.0.22 route-map rmap22
ip pim rp-address 21.21.0.33 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: 21.21.0.11, (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: 21.21.0.22, (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: 21.21.0.33, (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: 1.1.0.1
  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: 1.1.0.1
  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: 1.1.0.1
  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: 0.0.0.0
  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: 0.0.0.0
  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      SSM       -               -
231.0.0.0/8      ASM       21.21.0.11     -
231.128.0.0/9    ASM       21.21.0.22     -
231.129.0.0/16   ASM       21.21.0.33     -
231.129.128.0/17 Unknown    -               -

```

関連資料

関連項目	参照先
VDC	『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.2』
CLI コマンド	『Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference』
VRF およびポリシーベース ルーティングの設定	『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x』

標準

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

MIB

MIB	MIB リンク
<ul style="list-style-type: none"> • IPMCAST-MIB • PIM MIB : Cisco Nexus 7000 シリーズ デバイスの Cisco Release 5.2(1) 以降 	<p>MIBを検索およびダウンロードするには、次の URL にアクセスしてください。</p> <p>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</p>

PIM と PIM6 の機能履歴

機能名	リリース	機能情報
pim register-source コマンドのサポート。	5.2(1)	登録メッセージの IP 送信元アドレスの設定のサポート。
PIM (IPv4) に対する BFD サポート	5.0(2)	BFD は IPv4 の PIM に対してサポートされています。
vPC	4.1(3)	<p>Nexus 7000 シリーズ デバイス対応の Cisco NX-OS ソフトウェアは、vPC 上の PIM SSM または BIDR をサポートしません。Cisco NX-OS ソフトウェアは、vPC 上の PIM ASM を完全にサポートします。</p> <p>show ip pim statistics コマンドで vPC 統計を表示します。</p>



第 6 章

IGMP スヌーピングの設定

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

- [IGMP スヌーピングの情報, 133 ページ](#)
- [IGMP スヌーピングのライセンス要件, 137 ページ](#)
- [IGMP スヌーピングの前提条件, 138 ページ](#)
- [IGMP スヌーピングに関する注意事項と制限事項, 138 ページ](#)
- [デフォルト設定, 139 ページ](#)
- [IGMP スヌーピングパラメータの設定, 140 ページ](#)
- [IGMP スヌーピングの設定確認, 153 ページ](#)
- [IGMP スヌーピング統計情報の表示, 153 ページ](#)
- [IGMP スヌーピングの設定例, 153 ページ](#)
- [関連資料, 154 ページ](#)
- [標準, 154 ページ](#)
- [CLIでのIGMP スヌーピング機能の履歴, 155 ページ](#)

IGMP スヌーピングの情報



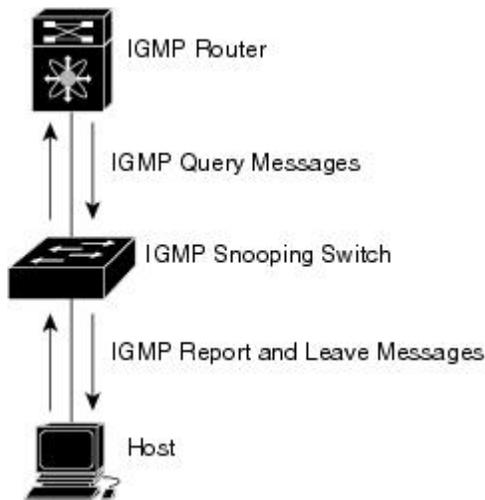
(注) デバイスの IGMP スヌーピングはディセーブルにしないことを推奨します。IGMP スヌーピングをディセーブルにすると、デバイス内で不正なフラッディングが過度に発生し、マルチキャストのパフォーマンスが低下する場合があります。

IGMP スヌーピングソフトウェアは、VLAN内のレイヤ2 IP マルチキャストトラフィックを調べて、該当する受信側が入っているポートを検出します。IGMP スヌーピングではポート情報を利

用することにより、マルチアクセス LAN 環境における帯域幅消費量を削減し、VLAN 全体へのフラディングを回避します。IGMP スヌーピング機能は、マルチキャスト対応ルータに接続されたポートを追跡して、ルータによる IGMP メンバーシップ レポートの転送機能を強化します。トポロジの変更通知には、IGMP スヌーピング ソフトウェアが応答します。デバイスでは、IGMP スヌーピングがデフォルトでイネーブルになっています。

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

図 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。

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

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

- 送信元フィルタリングにより、宛先および送信元の IP アドレスに基づいて、マルチキャスト パケットを転送できます。
- MAC アドレスではなく、IP アドレスに基づいてマルチキャスト転送を実行します。
- Nexus 7000 シリーズデバイス用の Cisco Release 5.2(1) 以降では、マルチキャスト転送は MAC アドレスに基づきます。
- 不明なトラフィックをルータのみに転送し、データによる状態の作成を実行しない Optimized Multicast Flooding (OMF)。

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

IGMPv1 および IGMPv2

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

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

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



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

IGMPv3

Cisco NX-OS にはフル機能の IGMPv3 スヌーピングが実装されており、IGMPv3 レポートに含まれる (S, G) 情報に基づいて、フラッドを制御することができます。この送信元ベースのフィルタリングにより、デバイスは対象のマルチキャスト グループにトラフィックを送信する送信元に基づいて、マルチキャスト トラフィックの宛先ポートを制限できます。

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

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

IGMP スヌーピング クエリア

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

VLAN の任意の IP ドレスを使用するようにクエリアを設定できます。

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



(注) クエリアの IP アドレスは、ブロードキャスト IP、マルチキャスト IP、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。

スタティック マルチキャスト MAC アドレス

Nexus 7000 シリーズ デバイス用の Cisco Release 5.2(1) 以降では、マルチキャスト MAC アドレスの発信インターフェイスをスタティックに設定します。また、MAC ベースの検索モードを使用するように IGMP スヌーピングを設定できます。

以前は、宛先 MAC アドレスではなく宛先 IP アドレスを使用してレイヤ 2 マルチキャストテーブルの検索を実行していました。ただし、一部のアプリケーションでは、単一のユニキャストクラスター IP およびマルチキャストクラスター MAC アドレスを共有しします。システムは、共有マルチキャスト MAC アドレスを持つ最終ホップルータによってユニキャストクラスター IP アドレス宛てのトラフィックを転送します。このアクションは、エンドホストまたはクラスターの宛先 IP アドレスにスタティック マルチキャスト MAC アドレスを割り当てることによって実現できます。

デフォルトの検索モードは IP のままですが、検索タイプを MAC アドレスベースに設定できます。検索モードは、グローバルでも、VLAN 単位でも設定できます。

- VDC が M シリーズモジュールからのポートのみを含み、グローバル検索モードが IP に設定されている場合、VLAN は 2 つの検索モードのいずれかに設定できます。ただし、グローバ

ル検索モードが MAC アドレスに設定されると、すべての VLAN の動作可能な検索モードは MAC アドレス モードに変更されます。

- VDC が M シリーズ モジュールと F シリーズ モジュールの両方のポートを含んでいる場合、いずれかの VLAN の検索モードを MAC アドレスに変更すると、すべての VLAN の動作検索モードが MAC アドレス ベースに変更されます。シャーシ内のこれらのモジュールによって、同じ検索モードをグローバルに、VLAN に使用できます。同様に、グローバル検索モードが MAC アドレス ベースの場合、すべての VLAN の動作可能な検索モードも MAC アドレス モードになります。



(注) 検索モードを変更すると、中断が発生します。マルチキャスト転送は、すべてのマルチキャスト エントリが新しい検索モードでプログラムされるまで、最適ではありません。また、32 個の IP アドレスが 1 つの MAC アドレスにマッピングされる場合、デバイスの準最適の転送が表示されることがあります。

VDC および VRF を使用した IGMP スヌーピング

Virtual Device Context (VDC; 仮想デバイス コンテキスト) は、一連のシステム リソースを論理的に表現する用語です。各 VDC 内では、複数の Virtual Routing and Forwarding (VRF; 仮想ルーティングおよびフォワーディング) インスタンスを定義できます。VDC ごとに実行できる IGMP プロセスは 1 つです。IGMP プロセスは対象の VDC に含まれるすべての VRF をサポートし、その VDC 内で IGMP スヌーピング機能を実行します。

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

VDC の設定方法については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

VRF の設定方法については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

IGMP スヌーピングのライセンス要件

製品	ライセンス要件
Cisco NX-OS	IGMP スヌーピングにはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『 <i>Cisco NX-OS Licensing Guide</i> 』を参照してください。

製品	ライセンス要件
Cisco DCNMS	IGMP スヌーピングにはライセンスは不要です。DCNM ライセンス方式の詳細については、『 <i>Fundamentals Configuration Guide, Cisco DCNM for LAN</i> 』を参照してください。

IGMP スヌーピングの前提条件

IGMP スヌーピングの前提条件は、次のとおりです。

- デバイスにログインしている。
- 現在の Virtual Device Context (VDC; 仮想デバイス コンテキスト) が正しい。VDC は、一連のシステムリソースを論理的に表現する用語です。switchto vdc コマンドでは VDC 番号を指定できます。
- 現在の Virtual Routing and Forwarding (VRF; 仮想ルーティングおよびフォワーディング) モードが正しい (グローバル コマンドの場合)。この章の例で示すデフォルトのコンフィギュレーション モードは、デフォルト VRF に適用されます。

IGMP スヌーピングに関する注意事項と制限事項

IGMP に関する注意事項および制約事項は次のとおりです。

- レイヤ 2 ネットワークでマルチキャスト転送を必要とする IPv6 マルチキャスト ネットワークに対して IGMP 最適化マルチキャスト転送 (OMF) をディセーブルにする必要があります。
- IPv6 パケットの転送が必要な VLAN の IGMP 最適化マルチキャスト転送をディセーブルにする必要があります。
- virtual Port Channel (vPC; 仮想ポートチャネル) ピアを設定している場合、2 台のデバイス間の IGMP スヌーピング設定オプションに相違があると、次のような結果になります。
 - 一方のデバイスで IGMP スヌーピングをイネーブルにして、他方でディセーブルにすると、スヌーピングがディセーブルであるデバイスではすべてのマルチキャストトラフィックがフラグディングします。
 - 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。
- FEX ポートの背後にあるルータを持つ VLAN を含む構成では、OMF の機能をディセーブルにする必要があります。OMF はこのような設定ではサポートされていません。

ユニキャスト宛先 IP アドレスとマルチキャスト宛先 MAC アドレスを使用するネットワーク アプリケーション

ユニキャスト宛先 IP アドレスとマルチキャスト宛先 MAC アドレスを使用するネットワーク アプリケーションは、IGMP スヌーピングの設定でスイッチの MAC ベースのフォワーディング ルックアップを使用しなければならない場合があります。

このようなアプリケーションに使用する宛先 MAC アドレスが非 IP マルチキャスト MAC アドレスである場合は、**mac address-table multicast** コマンドを使用して静的にポートメンバーシップを設定します。

また、宛先 MAC アドレスが IP マルチキャストの範囲内 (0100.5E00.0000 ~ 0100.5E7F.FFFF) にある場合、対応するレイヤ 3 IP マルチキャストアドレスのスタティック IGMP スヌーピングのメンバーシップエントリを使用して、ポートメンバーシップを設定します。たとえば、アプリケーションが宛先 MAC アドレス 0100.5E01.0101 を使用する場合は、その MAC アドレスにマッピングされる IP マルチキャストアドレスのスタティック IGMP スヌーピングのメンバーシップエントリを設定します。この例は、**ip igmp snooping static-group 239.1.1.1** 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	イネーブル
明示的な追跡	イネーブル
高速脱退	ディセーブル
最終メンバのクエリーインターバル	1 秒
スヌーピングクエリア	ディセーブル
レポート抑制	イネーブル

パラメータ	デフォルト
リンクローカル グループ抑制	イネーブル
デバイス全体での IGMPv3 レポート抑制	ディセーブル
VLAN ごとの IGMPv3 レポート抑制	イネーブル

IGMP スヌーピングパラメータの設定



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



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

グローバル IGMP スヌーピングパラメータの設定

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

パラメータ	説明
IGMP スヌーピング	アクティブな VDC 上で IGMP スヌーピングをイネーブルにします。デフォルトでは有効になっています。 (注) グローバルな設定がディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。
イベント履歴	IGMP スヌーピング履歴バッファのサイズを設定します。デフォルトは small です。
グループ タイムアウト	デバイス上のすべての VLAN のグループ メンバーシップ タイムアウトを設定します。
リンクローカル グループ抑制	デバイスのリンクローカルグループ抑制を設定します。デフォルトでは有効になっています。

パラメータ	説明
Optimise-multicast-flood	デバイス上のすべての VLAN で Optimized Multicast Flood (OMF) を設定します。デフォルトでは有効になっています。
プロキシ	デバイスの IGMP スヌーピングプロキシを設定します。デフォルトは 5 秒です。
レポート抑制	デバイスのマルチキャスト対応ルータに送信されるメンバーシップレポートトラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトでは有効になっています。
IGMPv3 レポート抑制	デバイスの IGMPv3 レポート抑制およびプロキシレポートを設定します。デフォルトでは無効になっています。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： <pre>switch# config t switch(config)#</pre>	コンフィギュレーションモードに入ります。

	コマンドまたはアクション		目的
ステップ 2	オプション	説明	次のコマンドを使用して、IGMP スヌーピングを設定できます。
	ip igmp snooping 例 <code>switch(config)# ip igmp snooping</code>	デバイスの IGMP スヌーピングをイネーブルにします。デフォルトでは有効になっています。 (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 例 <code>switch(config)# ip igmp snooping event-history</code>	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} 例 <code>switch(config)# ip igmp snooping group-timeout never</code>	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 例 <code>switch(config)# ip igmp snooping link-local-groups-suppression</code>	デバイス全体のリンクローカルグループ抑制を設定します。デフォルトでは有効になっています。	
ip igmp snooping optimise-multicast-flood 例 <code>switch(config)# ip igmp snooping optimise-multicast-flood</code>	デバイス上のすべての VLAN で OMF を最適化します。デフォルトでは有効になっています。		

コマンドまたはアクション		目的
オプション	説明	
ip igmp snooping proxy general-inquiries {mrt seconds} 例 <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。	
ip igmp snooping v3-report-suppression 例 <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ーシップレポートトラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトでは有効になっています。	
ip igmp snooping report-suppression 例 <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。デフォルトでは無効になっています。	
ステップ 3 copy running-config startup-config 例: <pre>switch(config)# 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。	

VLAN ごとの IGMP スヌーピングパラメータの設定

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

パラメータ	説明
IGMP スヌーピング	VLAN ごとに IGMP スヌーピングをイネーブルにします。デフォルトでは有効になっています。 (注) グローバルな設定がディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。

パラメータ	説明
明示的な追跡	各ポートに接続されたそれぞれのホストから送信される IGMPv3 メンバーシップレポートを、VLAN 別に追跡します。デフォルトでは有効になっています。
高速脱退	ソフトウェアが IGMP Leave レポートを受信した場合に、IGMP クエリーメッセージを送信することなく、グループステートを解除できるようにします。このパラメータは、IGMPv2 ホストに関して、各 VLAN ポート上のホストが 1 つしか存在しない場合に使用されます。デフォルトでは無効になっています。
グループ タイムアウト	指定した VLAN のグループ メンバーシップ タイムアウトを設定します。
最終メンバのクエリーインターバル	IGMP クエリーの送信後に待機する時間を設定します。この時間が経過すると、ソフトウェアは、特定のマルチキャストグループについてネットワークセグメント上に受信要求を行うホストが存在しないと見なします。いずれのホストからも応答がないまま、最終メンバのクエリーインターバルの期限が切れると、対応する VLAN ポートからグループが削除されます。有効範囲は 1 ~ 25 秒です。デフォルトは 1 秒です。
Optimise-multicast-flood	指定した VLAN で Optimized Multicast Flood (OMF) を設定します。デフォルトでは有効になっています。
プロキシ	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。
スヌーピング クエリア	マルチキャストトラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、インターフェイスにスヌーピング クエリアを設定します。スヌーピング クエリアに次の値を設定することもできます。 <ul style="list-style-type: none"> • タイムアウト：IGMPv2 のタイムアウト値 • インターバル：クエリー送信間の時間 • 最大応答時間：クエリーメッセージの MRT • スタートアップカウント：起動時に送信されるクエリー数 • スタートアップインターバル：起動時のクエリーインターバル
ロバストネス変数	指定した VLAN のロバストネス値を設定します。

パラメータ	説明
レポート抑制	各 VLAN に対して、マルチキャスト対応ルータに送信されるメンバーシップ レポート トラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトでは有効になっています。
マルチキャスト ルータ	マルチキャストルータへのスタティックな接続を設定します。ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。
スタティック グループ	VLAN のレイヤ 2 ポートをマルチキャストグループのスタティック メンバーとして設定します。
リンクローカル グループ抑制	各 VLAN に対して、リンクローカル グループ抑制を設定します。デフォルトでは有効になっています。
IGMPv3 レポート抑制	各 VLAN に対して、IGMPv3 レポート抑制およびプロキシ レポートを設定します。デフォルトでは VLAN ごとに有効になっています。
バージョン	指定した VLAN の IGMP バージョン番号を設定します。



- (注) Cisco Release 5.1(1) 以降は、次の手順のステップ 3 が **vlan** から **vlan configuration vlan-id** に変更されました。このコンフィギュレーションモードを使用して、必要な IP IGMP スヌーピングパラメータを設定します。ただし、設定は、指定した VLAN を明示的に作成するまで適用されません。VLAN の作成の詳細については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	ip igmp snooping 例： switch(config)# ip igmp snooping	現在の VDC に対して IGMP スヌーピングをイネーブルにします。デ

	コマンドまたはアクション	目的						
		<p>フォルトでは有効になっていません。</p> <p>(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ディングします。</p>						
ステップ 3	<table border="1"> <thead> <tr> <th data-bbox="430 1428 777 1480">オプション</th> <th data-bbox="777 1428 1196 1480">説明</th> </tr> </thead> <tbody> <tr> <td data-bbox="430 1480 777 1583"> vlan <i>vlan-id</i> switch(config)# vlan 2 switch(config-vlan)# </td> <td data-bbox="777 1480 1196 1583">VLAN コンフィギュレーションモードを開始します。</td> </tr> <tr> <td data-bbox="430 1583 777 1835"> vlan configuration <i>vlan-id</i> switch(config)# vlan configuration 2 switch(config-vlan-config)# </td> <td data-bbox="777 1583 1196 1835">Cisco Release 5.1(1) 以降は、このコマンドを使用して、VLAN の必要な 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 を明示的に作成するまで適用されません。</td> </tr> </tbody> </table>	オプション	説明	vlan <i>vlan-id</i> switch(config)# vlan 2 switch(config-vlan)#	VLAN コンフィギュレーションモードを開始します。	vlan configuration <i>vlan-id</i> switch(config)# vlan configuration 2 switch(config-vlan-config)#	Cisco Release 5.1(1) 以降は、このコマンドを使用して、VLAN の必要な 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 を明示的に作成するまで適用されません。	NX-OS のリリースに応じて、次の表に示すコマンドのいずれかを使用します。
オプション	説明							
vlan <i>vlan-id</i> switch(config)# vlan 2 switch(config-vlan)#	VLAN コンフィギュレーションモードを開始します。							
vlan configuration <i>vlan-id</i> switch(config)# vlan configuration 2 switch(config-vlan-config)#	Cisco Release 5.1(1) 以降は、このコマンドを使用して、VLAN の必要な 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 を明示的に作成するまで適用されません。							

	コマンドまたはアクション	目的	
ステップ 4	オプション ip igmp snooping switch(config-vlan-config)# ip igmp snooping	説明 現在の VLAN に対して IGMP スヌーピングをイネーブルにします。デフォルトでは有効になっています。	これらのコマンドでは IGMP スヌーピングパラメータを設定します。
	ip igmp snooping explicit-tracking switch(config-vlan-config)# ip igmp snooping explicit-tracking	各ポートに接続されたそれぞれのホストから送信される IGMPv3 メンバーシップ レポートを、VLAN 別に追跡します。デフォルトは、すべての VLAN でイネーブルです。	
	ip igmp snooping fast-leave switch(config-vlan-config)# ip igmp snooping fast-leave	IGMPv2 プロトコルのホストレポート抑制メカニズムのために、明示的に追跡できない IGMPv2 ホストをサポートします。高速脱退がイネーブルの場合、IGMP ソフトウェアは、各 VLAN ポートに接続されたホストが 1 つだけであると見なします。デフォルトは、すべての VLAN でディセーブルです。	
	ip igmp snooping group-timeout {minutes never} switch(config-vlan-config)# ip igmp snooping group-timeout never	指定した VLAN のグループメンバーシップタイムアウトを設定します。	
	ip igmp snooping last-member-query-interval seconds switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3	いずれのホストからも IGMP クエリーメッセージへの応答がないまま、最終メンバのクエリーインターバルの期限が切れた場合に、対応する VLAN ポートからグループを削除します。有効範囲は 1 ~ 25 秒です。デフォルトは 1 秒です。	
	ip igmp snooping optimised-multicast-flood switch(config-vlan-config)# ip igmp snooping optimised-multicast-flood	選択された VLAN の OMF を最適化します。デフォルトでは有効になっています。	

コマンドまたはアクション		目的
オプション	説明	
ip igmp snooping proxy general-queries mrt seconds switch(config-vlan-config)# ip igmp snooping proxy general-queries	指定した VLAN の IGMP スヌーピングプロキシを設定します。デフォルトは 5 秒です。	
ip igmp snooping querier <i>ip-address</i> switch(config-vlan-config)# ip igmp snooping querier 172.20.52.106	マルチキャストトラフィックをルーティングする必要がないため、PIM をイネーブルにしている場合に、スヌーピングクエリアを設定します。IP アドレスは、メッセージの送信元として使用します。	
ip igmp snooping querier-timeout seconds switch(config-vlan-config)# ip igmp snooping querier-timeout 300	マルチキャストトラフィックをルーティングする必要がないため、PIM をイネーブルにしている場合に、IGMPv2 のスヌーピングクエリアタイムアウト値を設定します。デフォルト値は 255 秒です。	
ip igmp snooping query-interval seconds switch(config-vlan-config)# ip igmp snooping query-interval 120	マルチキャストトラフィックをルーティングする必要がないため、PIM をイネーブルにしている場合に、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 seconds switch(config-vlan-config)# ip igmp snooping query-max-response-time 12	マルチキャストトラフィックをルーティングする必要がないため、PIM をイネーブルにしている場合に、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。	

コマンドまたはアクション		目的
オプション	説明	
ip igmp snooping startup-query-count <i>value</i> switch(config-vlan-config)# ip igmp snooping startup-query-count 5	マルチキャストトラフィックをルーティングする必要がないため、PIM をイネーブルにしている場合に、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 <i>seconds</i> switch(config-vlan-config)# ip igmp snooping startup-query-interval 15000	マルチキャストトラフィックをルーティングする必要がないため、PIM をイネーブルにしている場合に、起動時のスヌーピングクエリーインターバルを設定します。	
ip igmp snooping robustness-variable <i>value</i> switch(config-vlan-config)# ip igmp snooping robustness-variable 5	指定した VLAN のロバストネス値を設定します。デフォルト値は 2 です。	
ip igmp snooping report-suppression switch(config-vlan-config)# ip igmp snooping report-suppression	マルチキャスト対応ルータに送信されるメンバーシップレポートトラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトでは有効になっています。	
ip igmp snooping mrouter interface <i>interface</i> switch(config-vlan-config)# ip igmp snooping mrouter interface ethernet 2/1	マルチキャストルータへのスタティックな接続を設定します。ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。 ethernet slot/port のように、インターフェイスをタイプおよび番号で指定できます。	

コマンドまたはアクション		目的
オプション	説明	
ip igmp snooping static-group [group-ip-addr]source [source-ip-addr] interface interface switch(config-vlan-config)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1	VLAN のレイヤ 2 ポートをマルチキャスト グループのスタティック メンバーとして設定します。 ethernet slot/port のように、インターフェイスをタイプ および番号で指定できます。	
ip igmp snooping link-local-groups-suppression switch(config-vlan-config)# ip igmp snooping link-local-groups-suppression	指定した VLAN のリンクローカルグループ抑制を設定します。デフォルトでは有効になっています。	
ip igmp snooping v3-report-suppression switch(config-vlan-config)# ip igmp snooping v3-report-suppression	指定した VLAN の IGMPv3 レポート抑制およびプロキシレポートを設定します。デフォルトでは VLAN ごとに有効になっています。	
ip igmp snooping version value switch(config-vlan-config)# ip igmp snooping version 2	指定した VLAN の IGMP バージョン番号を設定します。	
ステップ 5 例 : switch(config)# copy running-config startup-config	copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

検索モードの変更

Nexus 7000 シリーズ シャーシ用の Cisco Release 5.2(1) 以降では、検索モードを MAC アドレスに基づくように、グローバルにまたは VLAN ごとに設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t 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	layer-2 multicast lookup mac 例： switch(config)# layer-2 multicast lookup mac	検索モードを MAC アドレスに基づくようにグローバルに変更します。デフォルトの IP 検索モードに戻すには、このコマンドの no 形式を使用します。
ステップ 3	vlan vlan-id 例： switch(config)# vlan 5 switch(config-vlan)# layer-2 multicast lookup mac switch(config-vlan)# layer-2 multicast lookup mac switch(config-vlan)#	検索モードを指定した VLAN の MAC アドレスに基づくように変更します。これらの VLAN のデフォルトの IP 検索モードに戻すには、このコマンドの no 形式を使用します。
ステップ 4	exit 例： switch(config)# exit switch#	コンフィギュレーションモードまたはVLAN コンフィギュレーションモードを終了します。
ステップ 5	show ip igmp snooping lookup-mode vlan vlan-id] 例： switch# show ip igmp snooping lookup-mode	(任意) IGMP スヌーピング検索モードを表示します。
ステップ 6	copy running-config startup-config 例： switch# 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。

スタティック マルチキャスト MAC アドレスの設定

Nexus 7000 シリーズ シャーシ用の Cisco Release 5.2(1) 以降では、マルチキャスト MAC アドレスの発信インターフェイスをスタティックに設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例 : <pre>switch# config t 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	mac address-table multicast multicast-mac-addr vlan vlan-id interface slot/port 例 : <pre>switch(config)# mac address-table multicast 01:00:5f:00:00:00 vlan 5 interface ethernet 2/5</pre>	マルチキャスト MAC アドレスの指定した発信インターフェイスをスタティックに設定します。
ステップ 3	exit 例 : <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードまたは VLAN コンフィギュレーション モードを終了します。
ステップ 4	show ip igmp snooping mac-oif [detail vlan vlan-id [detail]] 例 : <pre>switch# show feature-set</pre>	(任意) IGMP スヌーピング スタティック MAC アドレスを表示します。
ステップ 5	copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	(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 スヌーピングの設定確認

<code>show ip igmp snooping [vlan vlan-id]</code>	IGMP スヌーピング設定を VLAN 別に表示します。
<code>show ip igmp snooping groups [source [group] group [source]] [vlan vlan-id] [detail]</code>	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。
<code>show ip igmp snooping querier [vlan vlan-id]</code>	IGMP スヌーピングクエリアを VLAN 別に表示します。
<code>show ip igmp snooping mroute [vlan vlan-id]</code>	マルチキャスト ルータ ポートを VLAN 別に表示します。
<code>show ip igmp snooping explicit-tracking [vlan vlan-id]</code>	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。
<code>show ip igmp snooping lookup-mode [vlan vlan-id]</code>	IGMP スヌーピング検索モードを表示します。
<code>show ip igmp snooping mac-oif [detail vlan vlan-id [detail]]</code>	IGMP スヌーピング スタティック MAC アドレスを表示します。

IGMP スヌーピング統計情報の表示

IGMP スヌーピング統計情報を表示するには、`show ip igmp snooping statistics vlan` コマンドを使用します。この出力で、virtual Port Channel (vPC; 仮想ポートチャネル) の統計情報を確認できます。

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

これらのコマンドの使用方法については、『Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference』を参照してください。

IGMP スヌーピングの設定例

次に、IGMP スヌーピング パラメータの設定例を示します。

```
config t
 ip igmp snooping
  vlan 2
   ip igmp snooping
   ip igmp snooping explicit-tracking
```

```

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

```

次に、Cisco Release 5.1(1)以降のIGMP スヌーピング パラメータの設定例を示します。

```

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

```

これらの設定は、指定したVLANを明示的に作成するまで適用されません。VLANの作成の詳細については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

関連資料

関連項目	参照先
VDC	『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide』
CLI コマンド	『Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference』

標準

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

CLI での IGMP スヌーピング機能の履歴

機能名	リリース	機能情報
検索モードの MAC への設定およびスタティック MAC アドレスの割り当て	5.2(1)	MAC ベースとしてフォワーディング検索モードを使用するように IGMP スヌーピングを設定したり、スタティック MAC アドレスを割り当てたりすることができます。
vlan configuration vlan-id	5.1(1)	実際に VLAN を作成する前に VLAN を設定できるように、コマンドが追加されました。
vPC	4.1(3)	<p>vPC に適用される注意事項と制限事項の一覧。</p> <p><code>show ip igmp snooping statistics vlan</code> コマンドを使用して vPC 統計情報を表示します。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> • IGMP スヌーピングに関する注意事項と制限事項 • IGMP スヌーピング統計情報の表示



第 7 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 の情報, 157 ページ](#)
- [MSDP のライセンス要件, 160 ページ](#)
- [MSDP の前提条件, 160 ページ](#)
- [デフォルト設定, 161 ページ](#)
- [MSDP の設定, 161 ページ](#)
- [MSDP の設定の確認, 170 ページ](#)
- [MSDP のモニタリング, 171 ページ](#)
- [MSDP の設定例, 172 ページ](#)
- [関連資料, 173 ページ](#)
- [標準, 173 ページ](#)

MSDP の情報

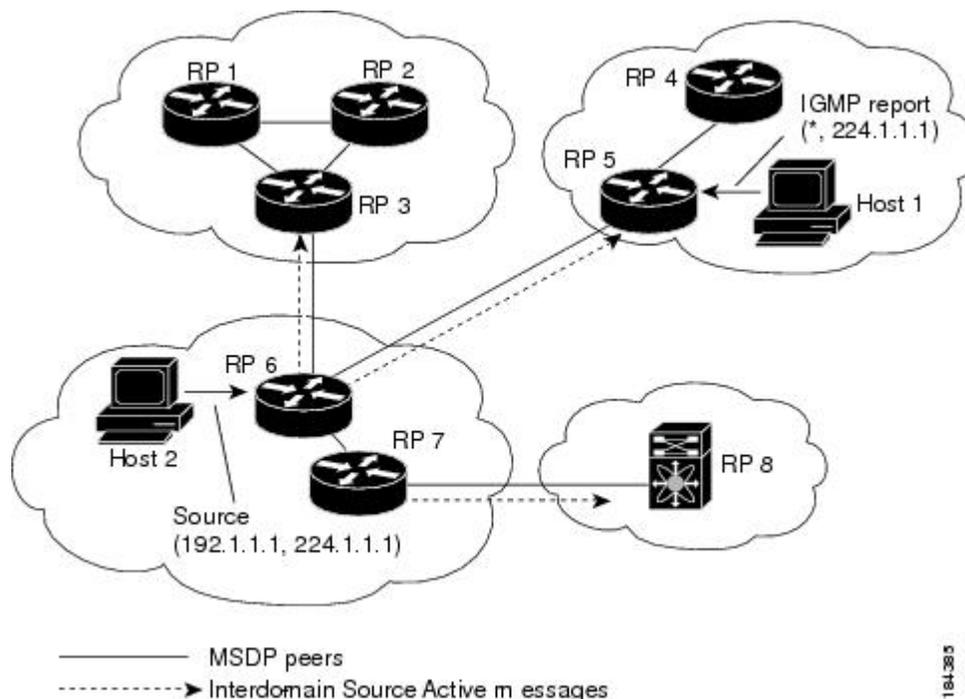
Multicast Source Discovery Protocol (MSDP) を使用すると、複数の Border Gateway Protocol (BGP; ボーダゲートウェイプロトコル) 対応 Protocol Independent Multicast (PIM) スパースモードドメイン間で、マルチキャスト送信元情報を交換できます。また、MSDPを使用して Anycast-RP 設定を作成し、RP 冗長性およびロードシェアリングを提供できます。PIMの詳細については、「*PIM* および *PIM6* の設定」を参照してください。BGPの詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

受信者が別のドメイン内の送信元から送信されたグループに加入する場合、ランデブーポイント (RP) は送信元方向に PIM Join メッセージを送信して、最短パスツリーを構築します。Designated Router (DR; 指定ルータ) は、送信元ドメイン内の送信元ツリーにパケットを転送します。これらのパケットは、必要に応じて送信元ドメイン内の RP を経由し、送信元ツリーの各ブランチを通っ

て他のドメインへと送信されます。受信者を含むドメインでは、対象のドメインの RP が送信元ツリー上に配置されている場合があります。ピアリング関係は Transmission Control Protocol (TCP; 転送制御プロトコル) 接続を介して構築されます。

次の図に、4つの PIM ドメインを示します。接続された RP (ルータ) は、アクティブな送信元情報を相互に交換するため、MSDP ピアと呼ばれます。各 MSDP ピアは他のピアにマルチキャスト送信元情報の独自のセットをアドバタイズします。送信元ホスト 2 はグループ 224.1.1.1 にマルチキャストデータを送信します。MSDP プロセスでは、RP 6 上で PIM Register メッセージを介して送信元に関する情報を学習すると、ドメイン内の送信元に関する情報が、Source-Active (SA) メッセージの一部として MSDP ピアに送信されます。SA メッセージを受信した RP 3 および RP 5 は、MSDP ピアに SA メッセージを転送します。RP 5 は、ホスト 1 から 224.1.1.1 のマルチキャストデータに対する要求を受信すると、192.1.1.1 のホスト 2 方向に PIM Join メッセージを送信して、送信元への最短パス ツリーを構築します。

図 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、RP 1、RP 2、RP 3 のように自律システム内に作成され、自律システム間には作成されません。ループ抑制および MSDP ピア RPF により、SA メッセージのループを防止するには、BGP を使用します。



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



(注) PIM Anycast (RFC 4610) を使用して、MSDP の代わりに Anycast-RP 機能を提供できます。PIM の詳細については、「PIM および PIM6 の設定」を参照してください。

MSDP の詳細については、RFC 3618 を参照してください。

SA メッセージおよびキャッシング

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

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

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

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

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

MSDP ピア RPF 転送

MSDP ピアは、発信元 RP から離れた場所で SA メッセージを受信し、そのメッセージの転送を行います。このアクションは、ピア RPF フラッ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。

仮想化のサポート

Virtual Device Context (VDC; 仮想デバイス コンテキスト) は、一連のシステムリソースを論理的に表現する用語です。各 VDC 内では、複数の Virtual Routing and Forwarding (VRF; 仮想ルーティングおよびフォワーディング) インスタンスを定義できます。MSDP 設定は現在の VDC 内で選択された VRF に適用されます。

`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。

VDC の設定方法については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

VRF の設定方法については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

MSDP のライセンス要件

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

MSDP の前提条件

MSDP の前提条件は、次のとおりです。

- デバイスにログインしている。
- 現在の Virtual Device Context (VDC; 仮想デバイス コンテキスト) が正しい。VDC は、一連のシステムリソースを論理的に表現する用語です。`switchto vdc` コマンドでは VDC 番号を指定できます。

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

デフォルト設定

表 19: MSDP パラメータのデフォルト設定

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

MSDP の設定

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

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

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



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



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

MSDP 機能のイネーブル化

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	feature msdp 例： switch# feature msdp	MSDP 機能をイネーブルにして、MSDP コマンドを実行できるようにします。デフォルトでは、MSDP 機能はディセーブルになっています。
ステップ 3	show running-configuration grep feature 例： switch# show running-configuration grep feature	(任意) 指定された feature コマンドを表示します。
ステップ 4	copy running-config startup-config feature 例： switch(config)# copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

MSDP ピアの設定

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

はじめる前に

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例 : <pre>switch# config t 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	ip msdp peer peer-ip-address connect-source interface [remote-as as-number] 例 : <pre>switch(config)# ip msdp peer 192.168.1.10 connect-source ethernet 2/1 remote-as 8</pre>	MSDP ピアを設定してピア IP アドレスを指定します。ソフトウェアは、インターフェイスの送信元 IP アドレスを使用して、ピアとの TCP 接続を行います。インターフェイスは <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。	—

	コマンドまたはアクション	目的
ステップ 4	show ip msdp summary [vrf <i>vrf-name</i> <i>known-vrf-name</i> all] 例： switch# show ip msdp summary	(任意) MSDP ピアの要約情報を表示します。
ステップ 5	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

MSDP ピアパラメータの設定

次の表に、設定可能なオプションの MSDP ピアパラメータを示します。これらのパラメータは、各ピアの IP アドレスを使用して、グローバル コンフィギュレーション モードで設定します。

表 20: MSDP ピアパラメータ

パラメータ	説明
説明	ピアの説明を示すストリング。デフォルトでは、ピアの説明は設定されていません。
管理シャットダウン	MSDP ピアをシャットダウンするパラメータ。コンフィギュレーションの設定はこのコマンドの影響を受けません。このパラメータを使用すると、ピアがアクティブになる前に、複数のパラメータ設定を有効にできます。シャットダウンを実行すると、その他のピアとの TCP 接続は強制終了されます。デフォルトでは、各ピアは定義した時点でイネーブルになります。
MD5 パスワード	ピアの認証に使用される MD5 共有パスワードキー。デフォルトでは、MD5 パスワードはディセーブルになっています。
SA ポリシー (IN)	着信 SA メッセージのルート マップ ポリシー ⁵ 。デフォルトでは、すべての SA メッセージが受信されます。

パラメータ	説明
SA ポリシー (OUT)	発信 SA メッセージのルートマップポリシー ⁶ 。デフォルトでは、発信される SA メッセージには登録済みの全送信元が含まれます。
SA の上限	ピアで許可され、SA キャッシュに格納される (S, G) エントリ数。デフォルトでは、上限はありません。

⁵ ルートマップポリシーの設定方法については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

⁶ ルートマップポリシーの設定方法については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

はじめる前に

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

手順

	コマンドまたはアクション	目的								
ステップ 1	config t 例： <pre>switch# config t 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	<table border="1"> <thead> <tr> <th>オプション</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td> ip msdp description <i>peer-ip-address</i> 例： <pre>switch(config)# ip msdp description 192.168.1.10 peer in Engineering network</pre> </td> <td>ピアの説明を示すストリングを設定します。デフォルトでは、ピアの説明は設定されていません。</td> </tr> <tr> <td> ip msdp shutdown <i>peer-ip-address</i> 例： <pre>switch(config)# ip msdp shutdown 192.168.1.10</pre> </td> <td>ピアをシャットダウンします。デフォルトでは、各ピアは定義した時点でイネーブルになります。</td> </tr> <tr> <td> ip msdp password <i>peer-ip-address password</i> 例： <pre>switch(config)# ip msdp password 192.168.1.10 my_md5_password</pre> </td> <td>ピアの MD5 パスワードをイネーブルにします。デフォルトでは、MD5 パスワードはディセーブルになっています。</td> </tr> </tbody> </table>	オプション	説明	ip msdp description <i>peer-ip-address</i> 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。	ip msdp shutdown <i>peer-ip-address</i> 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。	ip msdp password <i>peer-ip-address password</i> 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。	次のコマンドでは、MSDP ピア パラメータを設定します。
オプション	説明									
ip msdp description <i>peer-ip-address</i> 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。									
ip msdp shutdown <i>peer-ip-address</i> 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。									
ip msdp password <i>peer-ip-address password</i> 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。									

	コマンドまたはアクション	目的
	<p>オプション</p> <p>ip msdp sa-policy <i>peer-ip-address policy-name</i> in</p> <p>例 :</p> <pre>switch(config)# ip msdp sa-policy 192.168.1.10 my_incoming_sa_policy in</pre> <p>ip msdp sa-policy <i>peer-ip-address policy-name</i> out</p> <p>例 :</p> <pre>switch(config)# ip msdp sa-policy 192.168.1.10 my_outgoing_sa_policy out</pre> <p>ip msdp sa-limit <i>peer-ip-address limit out</i></p> <p>例 :</p> <pre>switch(config)# ip msdp sa-limit 192.168.1.10 5000</pre>	<p>説明</p> <p>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。</p> <p>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せん。</p> <p>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。</p>
ステップ 3	<p>show ip msdp peer [<i>peer-address</i>] [<i>vrf vrf-name</i> <i>known-vrf-name</i> <i>all</i>]</p> <p>例 :</p> <pre>switch# show ip msdp peer 1.1.1.1</pre>	(任意) MSDP ピアの詳細情報を表示します。
ステップ 4	<p>copy running-config startup-config</p> <p>例 :</p> <pre>switch(config)# 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。

MSDP グローバルパラメータの設定

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

表 21: MSDP グローバルパラメータ

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

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t switch(config)#	コンフィギュレーションモードに入ります。

	コマンドまたはアクション	目的
ステップ 2	オプション ip msdp originator-id interface 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 フィールドで使用される IP アドレスを設定します。インターフェイスは type slot/port という形式で表します。デフォルトでは、ローカルシステムの RP アドレスが使用されます。 (注) RP アドレスにはループバック インターフェイスを使用することを推奨します。
	ip msdp group-limit limit source source-prefix 例： <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作成される (S, G) エントリの最大数。グループの上限を超えた場合、そのグループは無視され、違反状態が記録されます。デフォルトでは、グループの上限は定義されていません。
	ip msdp sa-interval seconds 例： <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 3	show ip msdp summary [vrf vrf-name known-vrf-name all] 例： <pre>switch# show ip msdp summary</pre>	(任意) MSDP 設定の要約を表示します。
ステップ 4	copy running-config startup-config 例： <pre>switch(config)# 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。

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。

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

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	ip msdp mesh-group peer-ip-addr mesh-name 例： switch(config)# ip msdp mesh-group 192.168.1.10 my_mesh_1	MSDP メッシュを設定してピア IP アドレスを指定します。同じルータに複数のメッシュを設定したり、各メッシュグループに複数のピアを設定したりできます。デフォルトでは、メッシュグループは設定されていません。
ステップ 3	ピア IP アドレスを変更し、メッシュ内の各 MSDP ピアについてステップ 2 を繰り返します。	—
ステップ 4	show ip msdp mesh-group [mesh-group] [vrf vrf-name known-vrf-name all] 例： switch# show ip msdp summary	(任意) MSDP メッシュグループ設定に関する情報を表示します。
ステップ 5	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

MSDP プロセスの再起動

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	restart msdp 例： switch# restart msdp	MSDP プロセスを再起動します。
ステップ 2	config t 例： switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 3	ip msdp flush-routes	MSDP プロセスの再起動時に、ルートを削除します。デフォルトでは、ルートはフラッシュされません。
ステップ 4	show running-configuration include flush-routes 例： switch(config)# show running-configuration include flush-routes	(任意) 実行コンフィギュレーションの flush-routes 設定行を表示します。
ステップ 5	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) コンフィギュレーションの変更を保存します。

MSDP の設定の確認

show ip msdp count [<i>as-number</i>] [<i>vrf vrf-name</i> <i>known-vrf-name</i> <i>all</i>]	MSDP (S,G) エントリ数およびグループ数を AS 番号別に表示します。
---	---

show ip msdp mesh-group [<i>mesh-group</i>] [vrf <i>vrf-name</i> <i>known-vrf-name</i> all]	MSDP メッシュ グループ設定を表示します。
show ip msdp peer [<i>peer-address</i>] [vrf <i>vrf-name</i> <i>known-vrf-name</i> all]	MSDP ピアの MSDP 情報を表示します。
show ip msdp rpf [<i>rp-address</i>] [vrf <i>vrf-name</i> <i>known-vrf-name</i> all]	RP アドレスへの BGP パス上にあるネクストホップ AS を表示します。
show ip msdp sources [vrf <i>vrf-name</i> <i>known-vrf-name</i> all]	MSDP で学習された送信元と、グループ上限設定に関する違反状況を表示します。
show ip msdp summary [vrf <i>vrf-name</i> <i>known-vrf-name</i> all]	MSDP ピア設定の要約を表示します。

これらのコマンド出力のフィールドの詳細については、『Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference』を参照してください。

MSDP のモニタリング

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

統計情報の表示

MSDP 統計情報を表示するには、この表に示す各種コマンドを使用します。

show ip msdp [<i>as-number</i>] internal event-history { errors messages }	メモリの割り当てに関する統計情報を表示します。
show ip msdp policy statistics sa-policy <i>peer-address</i> { in out } [vrf <i>vrf-name</i> <i>known-vrf-name</i> all]	MSDP ピアの MSDP ポリシー統計情報を表示します。
show ip msdp { sa-cache route } [<i>source-address</i>] [<i>group-address</i>] [vrf <i>vrf-name</i> <i>known-vrf-name</i> all] [<i>asn-number</i>] [peer <i>peer-address</i>]	MSDP SA ルートキャッシュを表示します。送信元アドレスを指定した場合は、その送信元に対応するすべてのグループが表示されます。グループアドレスを指定した場合は、そのグループに対応するすべての送信元が表示されます。

統計情報のクリア

MSDP 統計情報をクリアするには、この表に示す各種コマンドを使用します。

表 22: MSDP 統計情報をクリアするコマンド

	説明
clear ip msdp peer [<i>peer-address</i>] [vrf <i>vrf-name</i> <i>known-vrf-name</i>]	MSDP ピアとの TCP 接続をクリアします。
clear ip msdp policy statistics sa-policy <i>peer-address</i> { in out } [vrf <i>vrf-name</i> <i>known-vrf-name</i>]	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 [<i>peer-address</i>] [vrf <i>vrf-name</i> <i>known-vrf-name</i>]	MSDP ピアの統計情報をクリアします。
clear ip msdp { sa-cache route } [<i>group-address</i>] [vrf <i>vrf-name</i> <i>known-vrf-name</i> all]	SA キャッシュ内のグループ エントリをクリアします。

MSDP の設定例

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

- 1 他のルータとの MSDP ピアリング関係を設定します。

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

次に、下に示した MSDP ピアリングのサブセットの設定例を示します。

RP 3: 192.168.3.10 (AS 7)

```

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

```

RP 5: 192.168.5.10 (AS 8)

```

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

```

RP 6: 192.168.6.10 (AS 9)

```

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

```

関連資料

関連項目	参照先
VDC	『Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference』
CLI コマンド	『Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference』
ポリシーベースルーティングおよびMBGP の設定	『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide』

標準

標準	タイトル
RFC 4624	Multicast Source Discovery Protocol (MSDP) MIB



第 8 章

N7K-F132-15 モジュールを使用したマルチキャスト相互動作の設定

この付録では、MシリーズとN7K-F132-15の両方のモジュールを搭載したシャーシでマルチキャストがどのように相互動作するかについて説明します。

- [マルチキャスト相互動作に関する情報, 175 ページ](#)
- [N7K-F132-15 および M シリーズ モジュールでのマルチキャスト相互動作, 176 ページ](#)
- [マルチキャスト相互動作のライセンス要件, 177 ページ](#)
- [マルチキャスト相互動作の前提条件, 177 ページ](#)
- [注意事項と制限, 178 ページ](#)
- [混在シャーシを使用したレイヤ 3 マルチキャストの設定, 178 ページ](#)
- [マルチキャストの設定の確認, 180 ページ](#)
- [マルチキャスト相互動作の機能の履歴, 180 ページ](#)

マルチキャスト相互動作に関する情報

Cisco NX-OS Release 5.1 以降では、Cisco Nexus 7000 シリーズのシャーシに、レイヤ 2 専用モジュールである N7K-F132-15 モジュールを追加できます。すでに M シリーズ モジュールが搭載されているシャーシにこのモジュールを追加すると、N7K-F132-15 と M シリーズの両方のモジュールを搭載したシャーシでマルチキャスト機能を提供できます。

N7K-F132-15 および M シリーズ モジュールでのマルチキャスト相互動作



(注) N7K-F132-15 モジュールでレイヤ 3 のルーティングとマルチキャストを実行するには、Cisco Nexus 7000 シリーズのシャーシに N7K-M シリーズのモジュールを搭載する必要があります。これは、同じ仮想デバイス コンテキスト (VDC) で M シリーズと N7K-F132-15 の両方のモジュールからのインターフェイスが必要になるためです。VDC の詳細については、『*Cisco Nexus 7000 Series Virtual Device Context Configuration Guide*』を参照してください。

レイヤ 3 のルーティングとマルチキャストは、N7K-F132-15 モジュールを搭載したシャーシに N7K-M シリーズ モジュールを追加すると自動的に行われるようになります。N7K-F132-15 および M シリーズの両方のモジュールを搭載したシャーシは、レイヤ 2 とレイヤ 3 のネットワークの境界に配置できます。

N7K-F132-15 と M シリーズの両方のモジュールを搭載したシャーシ内の、プロキシルーティング機能を使用する N7K-F132-15 モジュール上で、VLAN ごとに VLAN インターフェイスを設定する必要があります。VLAN インターフェイスの設定については、『*Cisco Nexus 7000 Series Interfaces Configuration Guide*』を参照してください。

デフォルトでは、VDC 内の N7K-M シリーズ モジュール上の物理インターフェイスはすべて、同じ VDC 内のレイヤ 2 専用 N7K-F132-15 モジュール上の VLAN インターフェイスが設定された VLAN に対し、プロキシルーティング ポートとして機能するようになります。M シリーズ モジュール上の物理インターフェイスは、管理のもとでシャットダウンでき、その後も引き続きプロキシルータとしてトラフィックを伝送します。

N7K-F132-15 モジュール上のインターフェイスに着信したパケットは、同じ VDC 内の M シリーズ モジュール上のインターフェイスの 1 つに自動的に転送され、ルーティングされます。M シリーズ モジュール上のインターフェイスでは、同じ VDC 内の N7K-F132-15 モジュール上のインターフェイスにレイヤ 3 マルチキャスト パケットが着信した場合に、そのパケットに対する出力レプリケーションも実行されます。N7K-F132-15 モジュールでのルーティングの相互動作に関する追加情報については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

レイヤ 3 マルチキャスト パケットに対し、VDC 内の M シリーズ モジュール上のどのインターフェイスで VLAN インターフェイスの出力レプリケーションを実行するかを指定できます。マルチキャスト出力レプリケーション実行の際は、使用可能なすべての M シリーズ プロキシルーティング インターフェイス間で、すべての VLAN インターフェイスの負荷が自動的に再分配されます。プロキシマルチキャスト レプリケータ間での負荷再分配は、自動で行うか手動で行うかを指定できます。負荷再分配を手動で行うように指定した場合、再分配を実行するにはコマンドを入力します。このコマンドは、モジュールを挿入または削除する際に便利です。



- (注) 手動による出力マルチキャスト レプリケーションロードバランシングを設定し、再分配のコマンドを入力する場合、このコマンドは設定には含まれません。 **copy running-config startup-config** コマンドを入力しても、コピーされるコマンドの中にこのコマンドは含まれません。

仮想化のサポート

同じVDCでMシリーズとN7K-F132-15の両方のモジュールからのインターフェイスが必要です。

VDCの詳細については、『Cisco Nexus 7000 Series Virtual Device Context Configuration Guide』を参照してください。

ハイアベイラビリティ

ハイアベイラビリティの詳細については、『Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide』を参照してください。

マルチキャスト相互動作のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	マルチキャストレプリケーションにライセンスは必要ありません。 ただし、PIMおよびPIM6にはEnterprise Servicesライセンスが必要です。Cisco NX-OSライセンス方式の詳細と、ライセンスの取得および適用の方法については、『Cisco NX-OS Licensing Guide』を参照してください。

マルチキャスト相互動作の前提条件

マルチキャスト相互動作を実現するには、有効なライセンスがインストールされていることと、Cisco Nexus 7000シリーズのシャーシに次のシリーズのモジュールが1つ以上搭載されていることが必要です。

- Mシリーズ
- N7K-F132-15

注意事項と制限

マルチキャストでは、同じVDCでMシリーズとN7K-F132-15の両方のモジュールからのインターフェイスが必要です。

混在シャーシを使用したレイヤ3マルチキャストの設定

プロキシルーティング機能を使用すると、N7K-F132-15 および M シリーズ モジュールを搭載したシャーシにレイヤ3ゲートウェイを設定できます。特定のVLANでルーティングを可能にするには、VLANインターフェイスを設定します。レイヤ3ルーティングおよびVLANインターフェイスの詳細については、『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide』を参照してください。

デフォルトでは、レイヤ3のルーティングとマルチキャストは、N7K-F132-15 モジュールを搭載したシャーシにN7K-M モジュールを追加すると自動的に行われるようになります。レイヤ3のルーティング、マルチキャスト、およびロードバランシングは、使用可能なN7K-Mシリーズ間で、N7K-Mシリーズモジュールのプロキシルーティングを使用することによりデフォルトで動作します。

オプションとして、負荷再分配の強制のほかに、出力マルチキャストレプリケーションに使用するN7K-Mシリーズモジュール上の物理インターフェイスを指定できます。

はじめる前に

混在シャーシ内の、プロキシルーティング機能を使用するN7K-F132-15モジュール上で、VLANごとにVLANインターフェイスを設定する必要があります。

同じVDCでMシリーズとN7K-F132-15の両方のモジュールからのインターフェイスが必要です。

VDCからインターフェイスを削除し、次にこのコマンドを入力すると、VDCをリロードするときに削除されたインターフェイスだけが表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	config t 例： switch# config t switch(config)#	グローバルコンフィギュレーションモードを開始します。
ステップ 2	hardware proxy layer-3 replication {use exclude} {module mod-number interface slot/port} [module-type fl]	N7K-F132-15 モジュール上でレイヤ3マルチキャストパケットの出力プロキシレプリケーションを提供するために、N7K-Mシリーズモジュール上に特定のモジュールと物理インターフェイスを設定します。

	コマンドまたはアクション	目的
	例 : <pre>switch(config)# hardware proxy layer-3 replication exclude interface ethernet 2/1-16, ethernet 3/1, ethernet 4/1-2</pre>	
ステップ 3	hardware proxy layer-3 replication rebalance-mode {auto manual} 例 : <pre>switch(config)# hardware proxy layer-3 replication rebalance-mode auto</pre>	プロキシルーティングレプリケーションインターフェイス間にロード バランシングを設定します。 auto スイッチを選択すると、すべての N7K-M シリーズレプリケータ間で、設定済みの VLAN インターフェイスマルチキャストレプリケーションのトラフィックの負荷が自動的に再分配されます。デフォルト値は manual です。 (注) <i>manual</i> モードでは、スイッチの初回起動時に、シャーシ内の M シリーズモジュール上にある使用可能なプロキシルーティングインターフェイス間で、すべてのトラフィックの負荷が自動的に分配されます。
ステップ 4	hardware proxy layer-3 replication trigger rebalance 例 : <pre>switch(config)# hardware proxy layer-3 replication trigger rebalance</pre>	ステップ 3 で再度 manual を設定した場合、このコマンドは、すべてのプロキシルーティングマルチキャストレプリケーションインターフェイス間で 1 回のみロード バランシングを実行するために使用します。このコマンドは、ステップ 3 で auto を設定した場合は効力を持ちません。 (注) このコマンドは 1 回のみイベントになるため、設定には保存されません。
ステップ 5	exit 例 : <pre>switch(config)# exit switch#</pre>	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	show hardware proxy layer-3 detail 例 : <pre>switch# show hardware proxy layer-3 detail</pre>	(任意) プロキシ レイヤ 3 の機能に関する情報を表示します。
ステップ 7	copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	(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。

この例では、混在シャーシ内の N7K-F132-15 モジュール上にある VLAN に対し出力マルチキャストレプリケーションを実行するため、および負荷を再分配するために、N7K-M シリーズモジュール上に特定の物理インターフェイスを指定する方法を示しています。

```
switch# config t
switch(config)# hardware proxy layer-3 replication exclude interface ethernet 2/1-16, 3/1,
4/1-2
switch(config)# hardware proxy layer-3 replication rebalance mode manual
switch(config)# hardware proxy layer-3 replication trigger rebalance
switch(config)#
```

マルチキャストの設定の確認

マルチキャスト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。

show hardware proxy layer-3 detail	M シリーズと N7K-F132-15 の両方のモジュールを搭載した混在シャーシにおけるレイヤ 3 プロキシルーティング機能に関する情報を表示します。
show hardware proxy layer-3 counters {brief detail } }	プロキシ転送のために N7K-F132-15 モジュールから各 M シリーズモジュールに送信されたパケット数に関する情報を表示します。 (注) カウンタを 0 にリセットするには、 clear hardware proxy layer-3 counters コマンドを入力します。

マルチキャスト相互動作の機能の履歴

表 23: マルチキャスト相互動作の機能の履歴

機能名	リリース	機能情報
Cisco Nexus 7000 シリーズのシャーシに搭載された F シリーズおよび M シリーズモジュール間のマルチキャスト相互動作	5.1(1)	この機能は、N7K-F132-15 モジュールとともに、このリリースで導入されました。



付録

A

IP マルチキャストに関する IETF RFC

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

- [IP マルチキャストに関する IETF RFC, 181 ページ](#)

IP マルチキャストに関する IETF RFC

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

RFC	タイトル
RFC 2236	『Internet Group Management Protocol』
RFC 2365	『Administratively Scoped IP Multicast』
RFC 2858	『Multiprotocol Extensions for BGP-4』
RFC 3376	『Internet Group Management Protocol』
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 4291	『IP Version 6 Addressing Architecture』

RFC	タイトル
RFC 4541	『 <i>Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches</i> 』
RFC 4601	『 <i>Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)</i> 』
RFC 4610	『 <i>Anycast-RP Using Protocol Independent Multicast (PIM)</i> 』
RFC 5059	『 <i>Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)</i> 』
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上限

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

- [設定の制限値, 183 ページ](#)

設定の制限値

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

設定の制限は、『*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*』に記載されています。



索引

記号

- (*, G) [7](#)
 - 説明 [7](#)
- (S, G) [6, 26, 62, 133](#)
 - IGMPv3 スヌーピング [133](#)
 - OIF 上のスタティック グループ [26](#)
 - スタティック グループ [26](#)
 - ステートの構築 [62](#)
 - 説明 [6](#)

数字

- 1 つの PIM ドメイン内に複数の RP [65](#)

A

- Anycast-RP [76, 102, 157](#)
 - Anycast-RP セットの設定 [102](#)
 - MSDP (注) [157](#)
 - 説明 [76](#)
- Anycast-RP、説明 [76](#)
- ASM モード [105](#)
 - 共有ツリーのみを設定 [105](#)
- Auto-RP [64, 67, 99, 111](#)
 - 候補 RP、設定 [99](#)
 - 候補 RP の設定手順 [99](#)
 - マッピング エージェント [99, 111](#)
 - 設定 [99](#)
 - ルート マップの設定 [111](#)
 - マッピング エージェントの設定手順 [99](#)
 - マッピング エージェントの選定プロセス [67](#)
- Auto-RP [67](#)
 - トラブルシューティング [67](#)

B

- BFD [59](#)
 - PIM [59](#)
- BGP [16, 157](#)
 - MSDP [157](#)
 - 自律システム [16](#)
 - MBGP [16](#)
- Bidir モード [14](#)
 - 説明 [14](#)
- BSR [65](#)
 - トラブルシューティング [65](#)
- BSR [63, 65, 95](#)
 - 候補 BSR [63, 95](#)
 - 設定 [95](#)
 - 説明 [63](#)
 - 候補 RP、設定 [95](#)
 - 候補 RP 選定プロセス [65](#)
 - 候補 RP の設定手順 [95](#)
 - 設定 [95](#)
 - メッセージ [63](#)
 - 受信と転送のイネーブル化 [63](#)
- BSR RP 候補の選定 [69, 72, 73, 74](#)
 - 同じ RP プライオリティが設定された同じグループ リスト [69](#)
 - 同じグループ リスト [73](#)
 - 同じグループ リスト、同じ RP プライオリティ [74](#)
 - 異なる RP プライオリティが設定された同じグループ リスト [69](#)
 - 最も詳細なグループ リスト [69, 72](#)
- BSR 候補プライオリティ [65, 66](#)
 - 同じ [66](#)
 - 異なる [65](#)

DDF [9, 77](#)Bidir モード (注) [9](#)説明 [77](#)DR [61, 77, 108](#)SSM モード [108](#)プライオリティおよび PIM hello メッセージ [61](#)**F**feature msdp [162](#)F シリーズ モジュール [18, 175](#)**I**IGMP [21, 22, 25, 26, 36, 38](#)IGMPv3 [21](#)IGMPv2 からの変更 [21](#)イネーブル化 [21](#)クエリア [22](#)説明 [22](#)設定、例 [38](#)説明 [21](#)前提条件 [25](#)バージョン、説明 [21](#)バージョン、デフォルト (IGMPv2) [21](#)パラメータ [25, 26](#)設定 [26](#)デフォルト設定 [25](#)プロセスの再起動 [36](#)IGMP show コマンド [37](#)show ip igmp groups [37](#)show ip igmp interface [37](#)show ip igmp local-groups [37](#)show ip igmp route [37](#)show running-configuration igmp [37](#)show startup-configuration igmp [37](#)IGMPv3 [21](#)IGMPv2 からの変更 [21](#)IGMP クエリア [22](#)説明 [22](#)IGMP コマンド [26, 34, 35, 36](#)iip igmp enforce-router-alert [35](#)ip igmp flush-routes [35, 36](#)ip igmp querier-timeout [26](#)ip igmp query-interval [26](#)ip igmp query-max-response-time [26](#)

IGMP コマンド (続き)

ip igmp query-timeout [26](#)ip igmp robustness-variable [26](#)ip igmp ssm-translate [34](#)ip igmp startup-query-count [26](#)ip igmp static-oif [26](#)ip igmp version [26](#)IGMP スヌーピング [133, 136, 137, 139, 140, 143, 153](#)クエリア、説明 [136](#)スイッチの例 [133](#)説明 [133](#)統計情報 [153](#)独自の機能 [133](#)パラメータ、設定 [140, 143](#)パラメータ、デフォルト設定 [139](#)メンバーシップ レポート抑制 [133](#)IGMP スヌーピング [143, 153](#)vPC 統計情報 [153](#)トラブルシューティング [143](#)IGMP スヌーピング show コマンド [153](#)show ip igmp snooping [153](#)show ip igmp snooping explicit-tracking [153](#)show ip igmp snooping groups [153](#)show ip igmp snooping mroute [153](#)show ip igmp snooping querier [153](#)IGMP スヌーピング コマンド [140, 143](#)ip igmp snooping [140, 143](#)ip igmp snooping explicit-tracking [140, 143](#)ip igmp snooping fast-leave [140, 143](#)ip igmp snooping last-member-query-interval [140, 143](#)ip igmp snooping link-local-groups-suppression [140, 143](#)ip igmp snooping mrouter interface [143](#)ip igmp snooping querier [140, 143](#)ip igmp snooping report-suppression [140, 143](#)ip igmp snooping static-group [143](#)ip igmp snooping v3-report-suppression [140, 143](#)IGMP スヌーピング設定 [139, 140, 143](#)IGMPv3 レポート抑制 [140, 143](#)イネーブル化 [140, 143](#)高速脱退 [143](#)最終メンバのクエリー インターバル [143](#)スタティック グループ [143](#)スヌーピング クエリア [143](#)パラメータ [139, 140, 143](#)設定 [140, 143](#)デフォルト設定 [139](#)マルチキャスト ルータ [143](#)明示的な追跡 [143](#)リンクローカル グループ抑制 [140, 143](#)レポート抑制 [140, 143](#)

IGMP の設定 [22, 25, 26, 38](#)

Outgoing Interface (OIF; 発信インターフェイス) 上の
スタティック マルチキャスト グループ [26](#)

アクセス グループ [26](#)

クエリア タイムアウト [26](#)

クエリー インターバル [26](#)

クエリーの最大応答時間 [22, 26](#)

クエリー メッセージの回数 [22](#)

グループ メンバーシップ タイムアウト [22, 26](#)

最終メンバーのクエリー応答インターバル [26](#)

最終メンバーのクエリー回数 [26](#)

スタートアップ クエリー インターバル [26](#)

スタートアップ クエリーの回数 [26](#)

スタティック マルチキャスト グループ [26](#)

即時脱退 [26](#)

パラメータ [26](#)

パラメータ、デフォルト設定 [25](#)

メンバーのクエリー応答インターバル [22](#)

リンク ローカルアドレスに対するレポート [22](#)

リンク ローカル マルチキャスト グループのレポー
ト [26](#)

例 [38](#)

レポート ポリシー [26](#)

ロバストネス値 [22, 26](#)

IGMP メンバーシップ レポート [22, 34](#)

IGMPv3 抑制 [22](#)

SSM 変換 [34](#)

マルチキャスト データの受信開始 [22](#)

ip igmp startup-query-interval [26](#)

J

Join およびステートの構築 [62](#)

M

MD5 ハッシュ値を使用した hello の認証 [61](#)

MFIB および M6FIB [16, 77, 78, 120](#)

OIF リストおよび RPF インターフェイス (注) [77, 78](#)
説明 [16](#)

ルートのフラッシュ [120](#)

MLD [41, 42, 43, 45, 57](#)

MLDv2 [42](#)

MLDv1 からの変更 [42](#)

イネーブル化 [42](#)

仮想化、VDC および VRF [41](#)

MLD (続き)

クエリア [43](#)

説明 [43](#)

設定、例 [57](#)

説明 [43](#)

前提条件 [45](#)

バージョン、説明 [42](#)

ライセンス要件 [45](#)

リスナー レポート [42](#)

MLD show コマンド [56](#)

show ipv6 mld groups [56](#)

show ipv6 mld interface [56](#)

show ipv6 mld local-groups [56](#)

show ipv6 mld route [56](#)

MLDv2 [42](#)

MLDv1 からの変更 [42](#)

MLD クエリア [43](#)

説明 [43](#)

MLD コマンド [54](#)

ipv6 mld ssm-translate [54](#)

MLD の設定 [41, 42, 43, 46, 57](#)

クエリーの最大応答時間 [42](#)

クエリー メッセージの頻度および回数 [43](#)

グループ メンバーシップ タイムアウト [42](#)

最終メンバーのクエリー応答インターバル [43](#)

パラメータ、デフォルト設定 [46](#)

リンク ローカルアドレスに対するレポート [41](#)

例 [57](#)

ロバストネス値 [43](#)

MRIB および M6RIB [16](#)

説明 [16](#)

MSDP [16, 157, 159, 160, 161, 171, 172](#)

Anycast-RP (注) [157](#)

SA キャッシュ、説明 [159](#)

SA メッセージ、および PIM Register メッセージ [159](#)

前提条件 [160](#)

統計情報 [172](#)

ドメイン間マルチキャスト プロトコル [16](#)

パラメータ、デフォルト設定 [161](#)

ピアリング、設定手順 [161](#)

メッシュグループ、説明 [160](#)

MSDP show コマンド [171](#)

show ip msdp [171](#)

MSDP コマンド [162, 163, 164, 166, 169, 170](#)

ip msdp description [164](#)

ip msdp flush-routes [170](#)

ip msdp group-limit [166](#)

ip msdp mesh-group [169](#)

ip msdp originator-id [166](#)

MSDP コマンド (続き)

- ip msdp password [164](#)
- ip msdp peer [163](#)
- ip msdp sa-interval [166](#)
- ip msdp sa-limit [164](#)
- ip msdp sa-policy [164](#)
- ip msdp shutdown [164](#)

MSDP コンフィギュレーション [161, 162, 163, 164, 166, 169](#)

- [Description] フィールド [164](#)
- group limit [166](#)
- MD5 パスワード [164](#)
- SA メッセージ [164, 166](#)
 - interval [166](#)
 - 制限 [164](#)
 - ポリシー IN [164](#)
 - ポリシー OUT [164](#)
- イネーブル化 [162](#)
- 管理シャットダウン [164](#)
- コマンド、キャッシュ (注) [161](#)
- 発信元インターフェイスの名前 [166](#)
- パラメータ、デフォルト設定 [161](#)
- ピアおよびピアリング関係 [163](#)
- ピアリング、設定手順 [161](#)
- メッシュグループ [169](#)

O

OIF [9, 77](#)

- DF [77](#)
- RPF チェック [9](#)

P

PIM [5, 65](#)

- トラブルシューティング [5](#)
- 複数の RP [65](#)

PIM [59, 61](#)

- BFD [59](#)
- 障害検出 [61](#)
- トンネルインターフェイス [59](#)

PIM6 コマンド [84, 85, 87, 90, 92, 95, 102, 105, 114, 120](#)

- feature pim6 [84](#)
- ipv6 pim anycast-rp [102](#)
- ipv6 pim bidir-rp-limit [85, 87, 90](#)
- ipv6 pim border [85, 87, 90](#)
- ipv6 pim bsr-candidate [95](#)
- ipv6 pim bsr bsr-policy [114](#)
- ipv6 pim bsr listen [85, 87, 90](#)

PIM6 コマンド (続き)

- ipv6 pim bsr rp-candidate-policy [114](#)
- ipv6 pim dr-priority [85, 87, 90](#)
- ipv6 pim flush-routes [120](#)
- ipv6 pim hello-interval [85, 87, 90](#)
- ipv6 pim jp-policy [114](#)
- ipv6 pim log-neighbor-changes [114](#)
- ipv6 pim neighbor-policy [85, 87, 90](#)
- ipv6 pim register-policy [114](#)
- ipv6 pim register-rate-limit [85, 87, 90](#)
- ipv6 pim rp-address [92](#)
- ipv6 pim rp-candidate [95](#)
- ipv6 pim sparse-mode [85, 87, 90](#)
- ipv6 pim use-shared-tree-only [105](#)

PIM および PIM6 [10, 59, 62, 76, 79, 80, 81, 82, 114, 125, 126, 177](#)

- イネーブル化 [59](#)
- スパース モード [59](#)
- 設定、説明 [82](#)
- 設定手順 [82](#)
- 前提条件 [80](#)
- デンス モード [10](#)
- 統計情報 [125, 126](#)
 - クリア [126](#)
 - 表示 [125](#)
- パラメータ、デフォルト設定 [81](#)
- ライセンス要件 [80, 177](#)

PIM および PIM6 show コマンド [124, 125](#)

- show {ip | ipv6} mroute [124](#)
- show {ip | ipv6} pim df [124](#)
- show {ip | ipv6} pim group-range [124](#)
- show {ip | ipv6} pim interface [124](#)
- show {ip | ipv6} pim neighbor [124](#)
- show {ip | ipv6} pim oif-list [124](#)
- show {ip | ipv6} pim policy statistics [125](#)
- show {ip | ipv6} pim route [124](#)
- show {ip | ipv6} pim rp [124](#)
- show {ip | ipv6} pim rp-hash [124](#)
- show {ip | ipv6} pim statistics [125](#)
- show {ip | ipv6} pim vrf [124](#)
- show running-configuration {pim | pim6} [124](#)
- show startup-configuration {pim | pim6} [124](#)

PIM および PIM6 ドメイン [10, 78](#)

- 説明 [10](#)
- PIM [10](#)

PIM および PIM6 の設定 [82](#)

- 設定手順 [82](#)

PIM および PIM6 の設定 [81, 82, 84, 85, 87, 90, 114, 120, 126, 127, 128](#)

- Auto-RP 候補 RP ポリシー (PIM のみ) [114](#)
- Auto-RP マッピング エージェント ポリシー (PIM のみ) [114](#)

PIM および PIM6 の設定 (続き)

- Auto-RP メッセージアクション (PIM のみ) [85, 87, 90](#)
- Bidir RP 制限 [85, 87, 90](#)
- BSR 候補 RP ポリシー [114](#)
- BSR ポリシー [114](#)
- BSR メッセージアクション [85, 87, 90](#)
- hello 間隔 [85, 87, 90](#)
- hello 認証モード [85, 87, 90](#)
- join-prune policy [114](#)
- PIM Register ポリシー [114](#)
- Register のレート制限 [85, 87, 90](#)
- 機能、イネーブル化 [84](#)
- 指定ルータのプライオリティ [85, 87, 90](#)
- スパス モード、イネーブル化 [85, 87, 90](#)
- 説明 [82](#)
- ドメイン境界 [85, 87, 90](#)
- ネイバーの変更の記録 [114](#)
- ネイバー ポリシー [85, 87, 90](#)
- パラメータ、デフォルト設定 [81](#)
- プロセスの再起動 [120](#)
- 例 [126, 127, 128](#)

- Auto-RP を使用した Bidir モード [128](#)
- BSR を使用した ASM モード [127](#)
- SSM モード [126](#)

PIM および PIM6 の統計情報コマンド [126](#)

- clear {ip | ipv6} pim interface statistics [126](#)
- clear {ip | ipv6} pim policy statistics [126](#)
- clear {ip | ipv6} pim statistics [126](#)

PIM コマンド [84, 85, 87, 90, 92, 95, 99, 102, 105, 114, 120](#)

- feature pim [84](#)
- ip pim anycast-rp [102](#)
- ip pim auto-rp listen [85, 87, 90](#)
- ip pim auto-rp mapping-agent [99](#)
- ip pim auto-rp mapping-agent-policy [114](#)
- ip pim auto-rp rp-candidate [99](#)
- ip pim auto-rp rp-candidate-policy [114](#)
- ip pim bidir-rp-limit [85, 87, 90](#)
- ip pim border [85, 87, 90](#)
- ip pim bsr-candidate [95](#)
- ip pim bsr bsr-policy [114](#)
- ip pim bsr listen [85, 87, 90](#)
- ip pim bsr rp-candidate-policy [114](#)
- ip pim dr-priority [85, 87, 90](#)
- ip pim flush-routes [120](#)
- ip pim hello-authentication ah-md5 [85, 87, 90](#)
- ip pim hello-interval [85, 87, 90](#)
- ip pim jp-policy [114](#)
- ip pim log-neighbor-changes [114](#)
- ip pim neighbor-policy [85, 87, 90](#)
- ip pim register-policy [114](#)

PIM コマンド (続き)

- ip pim register-rate-limit [85, 87, 90](#)
- ip pim rp-address [92](#)
- ip pim rp-candidate [95](#)
- ip pim sparse-mode [85, 87, 90](#)
- ip pim use-shared-tree-only [105](#)
- ip routing multicast holddown [85, 87, 90](#)

PIM ドメイン [157](#)PIM メッセージ [61, 62, 76](#)

- Anycast-RP [76](#)
- Join/Prune および Join または Prune (注) [61](#)
- Join/Prune のフィルタリング [61](#)
- register [76](#)
- 説明 [76](#)
- フィルタリング [76](#)

R

RP [14, 62, 63, 65, 76, 92, 111](#)

- アドレスの選択 [63](#)
- スタティック アドレス、設定 [92](#)
- スタティック、説明 [62](#)
- 説明 [62](#)
- 選択プロセス [63](#)
- デフォルト モード (ASM) [14](#)
- ルート マップ、設定 [111](#)

RP-Discovery メッセージ [64](#)RP-Discovery メッセージ、および Auto-RP [64](#)RPF [10](#)PIM [10](#)

RPT。「マルチキャスト配信ツリー、共有」を参照 [7](#)

RP アドレス [92](#)

S

SA メッセージ、説明 [157, 159](#)SPT [6, 61, 78](#)

- SSM モード [61](#)
- 説明 [6](#)
- 送信元ツリーへのスイッチオーバー [78](#)

SSM マッピング。「SSM 変換」を参照 [34](#)SSM 変換 [22, 34, 43, 54](#)

- IGMPv1 および IGMPv2 [22](#)
- MLD [54](#)
- MLDv1 [43](#)
- 説明 [34](#)

SSM モード [14, 15, 108](#)DR [108](#)

SSM モード (続き)

説明 [14](#)ドメイン間マルチキャストプロトコル [15](#)

V

VLAN インターフェイス [178](#)vPC [16, 138, 153](#)IGMP スヌーピング設定時の注意事項 [138](#)およびマルチキャスト [16](#)統計情報の表示 [153](#)vPC [105](#)

か

仮想化、VDC および VRF [79, 137, 160](#)管理用スコープの IP、説明 [78](#)

き

境界パラメータ [78](#)

く

クリア [172](#)グループ範囲、設定 [108](#)

け

検索モード [136](#)

し

初期ホールドダウン期間 [85, 87, 90](#)自律システム [16](#)MBGP [16](#)

す

ステータスのリフレッシュ [62](#)

せ

説明 [77](#)

ち

注意事項および制約事項 [80](#)

と

統計情報 [171](#)表示 [171](#)ドメイン間マルチキャストプロトコル [15, 16](#)MSDP [16](#)SSM [15](#)トラブルシューティング [5, 65, 67](#)Auto-RP [67](#)BSR [65](#)トラブルシューティング [68, 69, 105, 133, 143](#)トンネルインターフェイス [5](#)

は

バージョン [26](#)

ひ

ピア RPF フラッドイング、説明 [159](#)

ふ

プレフィックスリスト [92](#)プロキシルーティング [178](#)

ま

マッピング エージェント 「Auto-RP」を参照 [99](#)マルチキャスト [5, 6, 8, 15, 16, 18, 21, 43, 59, 78, 120, 133](#)IPv4 アドレス [5](#)IPv6 アドレス [6](#)説明 [5](#)ドメイン間プロトコル [15, 16](#)MSDP [16](#)

- マルチキャスト (続き)
 - ドメイン間プロトコル (続き)
 - SSM [15](#)
 - トンネルインターフェイス [5](#)
 - ハイ アベイラビリティ [18](#)
 - 配信モード [59](#)
 - ASM [59](#)
 - Bidir [59](#)
 - SSM [59](#)
 - フォワーディング [8](#)
 - プロセスの再起動 [120](#)
 - PIM および PIM6 [120](#)
 - プロトコル [21, 43, 133](#)
 - IGMP [21](#)
 - IGMP スヌーピング [133](#)
 - MLD [43](#)
- マルチキャスト [5, 136](#)
 - スタティック MAC アドレス [136](#)
 - トラブルシューティング [5](#)
- マルチキャスト配信ツリー [6](#)
 - SPT、説明 [6](#)
- マルチキャスト配信ツリー [8, 10, 59](#)
 - PIM [10](#)
 - ソース [59](#)
 - 双方向 [8](#)
- マルチキャストプロセスの再起動 [120, 170](#)
 - MSDP [170](#)
 - PIM および PIM6 [120](#)

め

- メッセージ [63](#)
 - 説明 [63](#)
- メッセージフィルタリング [114](#)

ら

- ライセンス要件 [137](#)
- ライセンス要件、マルチキャスト [18](#)

り

- リバースパス転送。「RPF」を参照 [9](#)

る

- ルートマップ [92](#)
- ルートマップ [111](#)
 - Auto-RP マッピング エージェントの設定 [111](#)
 - RP の設定 [111](#)

れ

- レイヤ 3 [178](#)

