



Cisco IOS XE Bengaluru 17.5.x (Catalyst 9200 スイッチ) IP 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

最終更新：2025 年 5 月 28 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

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

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

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

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: [www.cisco.com go trademarks](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. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

IP マルチキャスト ルーティング テクノロジーの概要	1
IP マルチキャスト テクノロジーに関する情報	1
IP マルチキャストについて	1
情報配信における IP マルチキャストの役割	2
IP マルチキャスト ルーティング プロトコル	2
Internet Group Management Protocol (インターネット グループ管理プロトコル)	3
プロトコル独立マルチキャスト	3
ランデブー ポイント	4
IGMP スヌーピング	4
IP マルチキャスト テーブル	5
ハードウェアおよびソフトウェアによる転送	6
部分的なルート	7
ソフトウェア ルート	7
非リバース パス フォワーディング トラフィック	8
マルチキャスト グループ伝送方式	8
IP マルチキャスト境界	10
IP マルチキャスト グループ アドレッシング	11
IP クラス D アドレス	11
IP マルチキャスト アドレスのスコーピング	11
レイヤ 2 マルチキャスト アドレス	13
シスコ エクスプレス フォワーディング、MFIB、およびレイヤ 2 転送	14
IP マルチキャスト 配信モード	16
Source Specific Multicast	16
マルチキャスト 高速ドロップ	16

Multicast Forwarding Information Base (マルチキャスト転送情報ベース)	17
S/M,224/4	18
マルチキャスト ハイ アベイラビリティ	19
IP マルチキャストに関する追加情報	19

第 2 章

基本的な IP マルチキャスト ルーティングの設定 21

基本的な IP マルチキャスト ルーティングに関する情報	21
マルチキャスト転送情報ベース (MFIB) の概要	21
IP マルチキャスト ルーティングのデフォルト設定	22
基本的な IP マルチキャスト ルーティングの設定方法	23
基本的な IP マルチキャスト ルーティングの設定	23
IP マルチキャスト転送の設定	25
スタティック マルチキャスト ルート (mroute) の設定	26
マルチキャスト VRF の設定	28
オプションの IP マルチキャスト ルーティングの設定	30
IP マルチキャスト境界の定義	30
sdr リスナー サポートの設定	32
基本的な IP マルチキャスト ルーティングのモニタリングおよびメンテナンス	35
キャッシュ、テーブル、およびデータベースのクリア	35
システムおよびネットワーク統計情報の表示	35
基本的な IP マルチキャストルーティングの設定例	37
例：IP マルチキャスト境界の設定	37
例：mrinfo 要求への応答	38
基本的な IP マルチキャスト ルーティングに関するその他の関連情報	38
基本的な IP マルチキャストルーティングの機能履歴	38

第 3 章

GRE トンネルを介するマルチキャスト ルーティングの設定 41

GRE トンネルを介するマルチキャスト ルーティングの設定の前提条件	41
GRE トンネルを介するマルチキャスト ルーティングの設定の制約事項	41
GRE トンネルを介するマルチキャスト ルーティングについて	42
GRE トンネルを介するマルチキャスト ルーティングの設定方法	42

非 IP マルチキャストエリアを接続する GRE トンネルの設定	42
非 IP マルチキャストエリアを接続するトンネリングの例	44
GRE トンネルを介するマルチキャストルーティングに関するその他の参考資料	45
GRE トンネルを介するマルチキャストルーティングの機能履歴	46

 第 4 章

IGMP の設定 47

IGMP および IGMP スヌーピングの前提条件	47
IGMP スヌーピングの前提条件	47
IGMP および IGMP スヌーピングの制約事項	48
IGMP 設定の制約事項	48
IGMP スヌーピングの制約事項	48
IGMP に関する情報	49
Internet Group Management Protocol の役割	49
IGMP マルチキャストアドレス	50
IGMP のバージョン	50
IGMP バージョン 1	50
IGMPv2	51
IGMP バージョン 3	51
IGMPv3 ホスト シグナリング	51
IGMP のバージョンの違い	51
IGMP の加入および脱退処理	55
IGMP の加入処理	55
IGMP の脱退処理	55
IGMP スヌーピング	56
マルチキャスト グループへの加入	57
マルチキャスト グループからの脱退	59
即時脱退	60
IGMP 脱退タイマーの設定	60
IGMP レポート抑制	60
IGMP スヌーピングとデバイススタック	61
IGMP フィルタリングおよびスロットリング	61

IGMP のデフォルト設定	62
IGMP スヌーピングのデフォルト設定	63
IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定	63
IGMP の設定方法	64
グループのメンバとしてデバイスを設定	64
IGMP バージョンの変更	65
IGMP ホストクエリーメッセージインターバルの変更	67
IGMPv2 の最大クエリー応答時間の変更	69
静的に接続されたメンバとしてデバイスを設定	70
IGMP プロファイルの設定	72
IGMP プロファイルの適用	74
IGMP グループの最大数の設定	76
IGMP スロットリングアクションの設定	77
直接接続の IGMP ホストがない場合にマルチキャストトラフィックが転送されるように デバイスを設定する方法	79
IGMP 拡張アクセスリストを使用して SSM ネットワークへのアクセスを制御する方法	80
IGMP スヌーピングを設定する方法	83
IGMP スヌーピングのイネーブル化	83
VLAN インターフェイスでの IGMP スヌーピングのイネーブル化またはディセーブル化	84
スヌーピング方法の設定	85
マルチキャストルータポートの設定	86
グループに加入するホストの静的な設定	88
IGMP 即時脱退のイネーブル化	89
IGMP 脱退タイマーの設定	90
IGMP 堅牢性変数の設定	92
IGMP 最終メンバークエリー回数の設定	93
TCN 関連コマンドの設定	95
TCN イベント後のマルチキャストフラッドング時間の制御	95
フラッドングモードからの回復	96
TCN イベント中のマルチキャストフラッドングのディセーブル化	97
IGMP スヌーピングクエリアの設定	99

IGMP レポート抑制のディセーブル化	100
IGMP のモニタリング	102
IGMP スヌーピング情報の監視	103
IGMP フィルタリングおよび IGMP スロットリングの設定のモニタリング	104
IGMP の設定例	105
例：マルチキャストグループのメンバとしてデバイスを設定	105
例：マルチキャストグループへのアクセスの制御	105
例：IGMP スヌーピングの設定	105
例：IGMP プロファイルの設定	106
例：IGMP プロファイルの適用	106
例：IGMP グループの最大数の設定	107
例：ルーテッドポートとしてのインターフェイス設定	107
例：SVI としてのインターフェイスの設定	107
例：直接接続された IGMP ホストがない場合に、マルチキャストトラフィックを転送するようにデバイスを設定	108
IGMP 拡張アクセスリストを使用して SSM ネットワークへのアクセスを制御する方法	108
例：グループ G のすべての状態を拒否	108
例：ソース S のすべての状態を拒否	109
例：グループ G のすべての状態を許可	109
例：ソース S のすべての状態を許可	109
例：グループ G のソース S をフィルタリング	110
IGMP に関するその他の関連資料	110
IGMP の機能の履歴	110
第 5 章	
IGMP プロキシの設定	111
IGMP プロキシの前提条件	111
IGMP プロキシについて	111
IGMP プロキシ	111
単一のアップストリームインターフェイス用の IGMP プロキシ	112
複数のアップストリームインターフェイス用の IGMP プロキシ	114

IGMP プロキシの設定方法	116
IGMP UDLR に対するアップストリーム UDL デバイスの設定	116
IGMP プロキシ サポート付きの IGMP UDLR に対するダウンストリーム UDL デバイスの設定	117
UDLR を使用しない IGMP プロキシ加入向けダウンストリームデバイスの設定	120
複数のアップストリーム インターフェイスの IGMP プロキシ向けダウンストリームデバイスの設定	122
IGMP プロキシの設定例	124
例：IGMP UDLR 向けアップストリーム UDL デバイスの設定	124
例：IGMP プロキシサポートによる IGMP UDLR 向けダウンストリーム UDL デバイスの設定	124
例：UDLR を使用しない IGMP プロキシ向けダウンストリームデバイスの設定	125
例：複数のアップストリーム インターフェイスの IGMP プロキシ向けダウンストリームデバイスの設定	125
IGMP プロキシに関するその他の関連資料	125
IGMP プロキシの機能履歴	126
<hr/>	
第 6 章	スイッチドイーサネットでの IP マルチキャストの抑制
	127
	スイッチドイーサネット ネットワークで IP マルチキャストを抑制するための前提条件
	127
	スイッチドイーサネット ネットワークでの IP マルチキャストについての情報
	127
	IP マルチキャスト トラフィックとレイヤ 2 スイッチ
	127
	IP マルチキャスト用の Catalyst スイッチの CGMP
	128
	IGMP スヌーピング
	129
	Router-Port Group Management Protocol (RGMP)
	129
	スイッチドイーサネット ネットワークでマルチキャストを抑制する例
	130
	IP マルチキャスト用のスイッチの設定
	130
	IGMP スヌーピングの設定
	130
	CGMP のイネーブル化
	130
	レイヤ 2 スイッチドイーサネット ネットワークでの IP マルチキャストの設定
	131
	スイッチドイーサネット ネットワークで IP マルチキャストを抑制する設定例
	133
	RGMP の設定例
	133

スイッチドイーサネットネットワークでの IP マルチキャスト抑制に関するその他の参考資料 133

スイッチドイーサネットでの IP マルチキャスト抑制の機能履歴 134

第 7 章

PIM (Protocol Independent Multicast) の設定 135

PIM の前提条件 135

PIM に関する制約事項 136

PIMv1 および PIMv2 の相互運用性 136

PIM スタブルルーティングの設定に関する制約事項 137

Auto-RP および BSR の設定に関する制約事項 137

Auto-RP 拡張の制約事項 138

PIM に関する情報 139

Protocol Independent Multicast の概要 139

PIM のバージョン 139

Multicast Source Discovery Protocol (MSDP) 140

PIM スパース モード (PIM-SM) 140

PIM スタブルルーティング 141

ランデブー ポイント 142

Auto-RP 143

PIM ネットワークでの Auto-RP の役割 144

マルチキャスト境界 144

Auto-RP のスパース - デンス モード 145

Auto-RP のメリット 146

PIM ドメイン境界 146

PIMv2 ブートストラップ ルータ 147

マルチキャスト転送 147

マルチキャスト配信のソース ツリー 148

マルチキャスト配信の共有ツリー 148

ソース ツリーの利点 149

共有ツリーの利点 150

PIM 共有ツリーおよびソース ツリー 150

Reverse Path Forwarding	152
RPF チェック	153
PIM ルーティングのデフォルト設定	154
PIM の設定方法	155
PIM スタブルーティングのイネーブル化	155
ランデブー ポイントの設定	157
マルチキャスト グループへの RP の手動割り当て	157
新規ネットワークでの Auto-RP の設定	160
既存の SM クラウドへの Auto-RP の追加	163
問題のある RP への Join メッセージの送信禁止	167
着信 RP アナウンスメント メッセージのフィルタリング	167
PIMv2 BSR の設定	169
PIM ドメイン境界の定義	169
IP マルチキャスト境界の定義	171
候補 BSR の設定	173
候補 RP の設定	174
Auto-RP によるスパース モードの設定	177
PIM 最短パス ツリーの使用の延期	181
PIM ルータクエリー メッセージ間隔の変更	183
PIM の動作の確認	185
PIM-SM ネットワークまたは PIM-SSM ネットワークでの IP マルチキャスト動作の確認	185
ファースト ホップ ルータでの IP マルチキャストの確認	186
SPT 上のルータでの IP マルチキャストの確認	187
ラスト ホップ ルータでの IP マルチキャスト動作の確認	188
PIM 対応ルータを使用した IP マルチキャストの到達可能性のテスト	192
マルチキャスト ping に応答するルータの設定	192
マルチキャスト ping に応答するように設定されたルータへの ping	194
PIM のモニタリングとトラブルシューティング	194
PIM 情報のモニタリング	194
RP マッピングおよび BSR 情報のモニタリング	196

PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング	196
PIM の設定例	197
例：PIM スタブルルーティングのイネーブル化	197
例：PIM スタブルルーティングの確認	197
例：マルチキャストグループへの RP の手動割り当て	198
例：Auto-RP の設定	198
例：Auto-RP でのスパースモード	198
例：Auto-RP 情報を拒否する IP マルチキャスト境界の定義	198
例：着信 RP アナウンスメントメッセージのフィルタリング	199
例：問題のある RP への Join メッセージの送信禁止	199
例：候補 BSR の設定	199
例：候補 RP の設定	200
PIM 機能の履歴	200

第 8 章

IP マルチキャストに対する PIM MIB 拡張の設定	201
IP マルチキャストに対する PIM MIB 拡張について	201
IP マルチキャストに対する SNMP トラップの PIM MIB 拡張	201
PIM MIB 拡張の利点	202
IP マルチキャストに対する PIM MIB 拡張の設定方法	202
IP マルチキャストに対する PIM MIB 拡張のイネーブル化	202
PIM MIB 拡張の設定例	204
IP マルチキャストに対する PIM MIB 拡張のイネーブル化の例	204
IP マルチキャストに対する PIM MIB 拡張に関するその他の参考資料	204
IP マルチキャストに対する PIM MIB 拡張の機能履歴	205

第 9 章

SSM の設定	207
SSM の設定の前提条件	207
SSM 設定の制約事項	208
SSM に関する情報	209
SSM コンポーネントの概要	209
SSM および Internet Standard Multicast (ISM)	209

SSM IP アドレスの範囲	210
SSM の動作	210
SSM マッピング	211
スタティック SSM マッピング	211
DNS ベースの SSM マッピング	212
SSM の設定方法	213
SSM の設定	213
Source-Specific Multicast (SSM) マッピングの設定	215
スタティック SSM マッピングの設定	215
DNS ベースの SSM マッピングの設定	217
SSM マッピングを使用したスタティック トラフィック転送の設定	219
SSM のモニタリング	220
SSM マッピングのモニタリング	221
SSM の次の作業	221
SSM に関するその他の関連資料	222
SSM の機能履歴	222

第 10 章	IPv6 マルチキャストの実装	223
	IPv6 マルチキャストルーティングの実装に関する情報	223
	IPv6 マルチキャストの概要	223
	IPv6 マルチキャストルーティングの実装	224
	IPv6 マルチキャスト リスナー ディスカバリ プロトコル	225
	マルチキャスト クエリアとマルチキャスト ホスト	225
	MLD アクセス グループ	225
	受信側の明示的トラッキング	225
	プロトコル独立マルチキャスト	225
	PIM スパース モード	226
	IPv6 BSR : RP マッピングの設定	227
	PIM-Source Specific Multicast (PIM-SSM)	227
	ルーティング可能アドレスの hello オプション	228
	PIM IPv6 スタブルーティング	228

ランデブー ポイント	229
スタティック mroute	230
MRIB	230
MFIB	231
MFIB	231
IPv6 マルチキャスト VRF Lite	232
IPv6 マルチキャストのプロセス スイッチングおよび高速スイッチング	232
IPv6 マルチキャストでの NSF と SSO のサポート	233
IPv6 対応の NTP	233
IPv6 マルチキャストの実装	233
IPv6 マルチキャスト ルーティングのイネーブル化	233
MLD プロトコルのカスタマイズおよび確認	234
インターフェイスでの MLD のカスタマイズおよび確認	234
MLD グループ制限の実装	236
受信側の明示的トラッキングによってホストの動作を追跡するための設定	238
MLD トラフィック カウンタのリセット	239
MLD インターフェイス カウンタのクリア	239
PIM の設定	240
PIM-SM の設定およびグループ範囲の PIM-SM 情報の表示	240
PIM オプションの設定	242
PIM トラフィック カウンタのリセット	243
PIM トポロジ テーブルをクリアすることによる MRIB 接続のリセット	244
PIM IPv6 スタブ ルーティングの設定	246
PIM IPv6 スタブ ルーティングの設定時の注意事項	246
IPv6 PIM ルーティングのデフォルト設定	247
IPv6 PIM スタブ ルーティングのイネーブル化	247
IPv6 PIM スタブ ルーティングのモニター	249
IPv6 PIM での組み込み RP サポートのディセーブル化	250
BSR の設定	250
BSR の設定および BSR 情報の確認	251
BSR への PIM RP アドバタイズメントの送信	252

限定スコープゾーン内で BSR を使用できるようにするための設定	253
BSR スイッチにスコープと RP のマッピングをアナウンスさせるための設定	254
SSM マッピングの設定	254
スタティック mroute の設定	256
IPv6 マルチキャストでの MFIB の使用	257
IPv6 マルチキャストでの MFIB の動作の確認	257
MFIB トラフィック カウンタのリセット	259
その他の参考資料	259
IPv6 マルチキャストの機能履歴	259

第 11 章

MLD スヌーピングの設定	261
IPv6 MLD スヌーピングの設定に関する情報	261
MLD スヌーピングの概要	261
MLD メッセージ	262
MLD クエリー	262
マルチキャスト クライアント エージングの堅牢性	263
マルチキャスト ルータ検出	263
MLD レポート	264
MLD Done メッセージおよび即時脱退	264
TCN 処理	265
IPv6 MLD スヌーピングの設定方法	265
MLD スヌーピングのデフォルト設定	265
MLD スヌーピング設定時の注意事項	266
スイッチでの MLD スヌーピングのイネーブル化またはディセーブル化	266
VLAN に対する MLD スヌーピングのイネーブル化またはディセーブル化	267
スタティックなマルチキャスト グループの設定	268
マルチキャスト ルータ ポートの設定	270
MLD 即時脱退のイネーブル化	271
MLD スヌーピング クエリーの設定	272
MLD リスナー メッセージ抑制のディセーブル化	274
MLD スヌーピング情報の表示	275

MLD スヌーピングの設定例	276
スタティックなマルチキャスト グループの設定：例	276
マルチキャスト ルータ ポートの設定：例	276
MLD 即時脱退のイネーブル化：例	276
MLD スヌーピング クエリーの設定：例	276
その他の参考資料	277
MLD スヌーピングの機能履歴	277

第 12 章

IP マルチキャストの最適化：大規模な IP マルチキャスト展開での PIM スパース モードの最適化	279
大規模な IP マルチキャスト展開での PIM スパース モードの最適化の前提条件	279
大規模な IP マルチキャスト展開での PIM スパース モードの最適化について	280
PIM 登録プロセス	280
PIM バージョン 1 の互換性	281
PIM 指定ルータ	281
PIM スパース モード登録メッセージ	281
メモリ要件を減らすために最短パス ツリーの使用を回避する	282
PIM 共有ツリーおよびソース ツリー（最短パス ツリー）	282
最短パスツリーの使用を回避または延期する利点	283
大規模な IP マルチキャスト展開で PIM スパース モードを最適化する方法	283
大規模な展開での PIM スパース モードの最適化	283
大規模なマルチキャスト展開での PIM スパース モードの最適化の設定例	286
大規模な IP マルチキャスト展開での PIM スパース モードの最適化の例	286
IP マルチキャストの最適化：大規模な IP マルチキャスト展開での PIM スパース モードの最適化に関するその他の関連資料	287
IP マルチキャストの最適化の機能履歴：大規模な IP マルチキャスト展開での PIM スパース モードの最適化	287

第 13 章

IP マルチキャストの最適化：マルチキャスト サブセカンド コンバージェンス	289
マルチキャスト サブセカンド コンバージェンスの前提条件	289
マルチキャスト サブセカンド コンバージェンスの制約事項	289
マルチキャスト サブセカンド コンバージェンスについて	290

マルチキャスト サブセカンド コンバージェンスの利点	290
マルチキャスト サブセカンド コンバージェンス スケーラビリティ拡張機能	290
PIM ルータ クエリ メッセージ	290
Reverse Path Forwarding	291
トポロジの変更とマルチキャスト ルーティングのリカバリ	291
マルチキャスト サブセカンド コンバージェンスの設定方法	291
PIM ルータ クエリ メッセージ間隔の変更	291
マルチキャスト サブセカンド コンバージェンス設定の確認	292
マルチキャスト サブセカンド コンバージェンスの設定例	293
PIM ルータ クエリ メッセージインターバルの変更例	293
IP マルチキャストの最適化：マルチキャスト サブセカンド コンバージェンスに関するその 他の参考資料	294
IP マルチキャストの最適化：マルチキャスト サブセカンド コンバージェンスの機能情報	294

第 14 章

IP マルチキャストの最適化：等コストパス間での IP マルチキャスト ロードスプリッティング 295

等コストパス間での IP マルチキャスト ロードスプリットの前提条件	295
等コストパス間での IP マルチキャスト ロードスプリッティングについて	296
ロードスプリットとロードバランシング	296
複数の等コストパスが存在する場合の IP マルチキャストのデフォルト動作	296
IP マルチキャストトラフィックをロードスプリットする方法	298
ECMP マルチキャストロードスプリットの概要	299
S ハッシュアルゴリズムを使用した、ソースアドレスに基づく ECMP マルチキャスト ロードスプリット	299
基本 S-G ハッシュアルゴリズムを使用した、ソースアドレスとグループアドレスに基 づく ECMP マルチキャストロードスプリット	299
S ハッシュおよび基本 S-G ハッシュアルゴリズムを使用した場合の副産物としての予測 可能性	300
S ハッシュおよび基本 S-G ハッシュアルゴリズムを使用した場合の副産物としての局在 化	300
ソースグループとネクストホップアドレスに基づく ECMP マルチキャストロードス プリッティング	301

RPF パス選択のための PIM ネイバークエリおよびハローメッセージへの ECMP マルチキャストロードスプリットの影響	302
PIM-SM および PIM-SSM での PIM アサート処理に対する ECMP マルチキャストロードスプリットの影響	303
ユニキャストルーティングが変わった場合の ECMP マルチキャストロードスプリットと再コンバージェンス	304
スタティック mroute での ECMP マルチキャストロードスプリットの使用	304
IP マルチキャストトラフィックのロードスプリッティングの代替方法	305
ECMP を介して IP マルチキャストトラフィックをロードスプリットする方法	305
ECMP マルチキャストロードスプリットのイネーブル化	305
IP マルチキャストロードスプリット的前提条件：ECMP	306
IP マルチキャストロードスプリッティング ECMP の制約事項	306
ソースアドレスに基づく ECMP マルチキャストロードスプリットのイネーブル化	307
ソースアドレスおよびグループアドレスに基づく ECMP マルチキャストロードスプリットのイネーブル化	309
ソースグループおよびネクストホップアドレスに基づく ECMP マルチキャストロードスプリットのイネーブル化	311
ECMP を介した IP マルチキャストトラフィックのロードスプリットの設定例	313
例：ソースアドレスに基づく ECMP マルチキャストロードスプリットのイネーブル化	313
ソースアドレスおよびグループアドレスに基づく ECMP マルチキャストロードスプリットのイネーブル化の例	314
ソースグループおよびネクストホップアドレスに基づく ECMP マルチキャストロードスプリットのイネーブル化の例	314
IP マルチキャストの最適化に関するその他の関連情報：等コストパス間での IP マルチキャストロードスプリッティング	314
IP マルチキャストの最適化の機能履歴：等コストパス間での IP マルチキャストロードスプリッティング	315
第 15 章	
IP マルチキャストの最適化：マルチキャスト向け SSM チャンnel ベース フィルタリング	317
マルチキャスト境界向け SSM チャンnel ベース フィルタリング的前提条件	317
マルチキャスト境界向け SSM チャンnel ベース フィルタリングについて	317
マルチキャスト境界のルール	318

マルチキャスト境界向け SSM チャンネル ベース フィルタリングの利点	318
マルチキャスト境界向け SSM チャンネル ベース フィルタリングの設定方法	318
マルチキャスト境界の設定	319
マルチキャスト境界向け SSM チャンネル ベース フィルタリングの設定例	320
トラフィックを許可および拒否するマルチキャスト境界の設定例	320
トラフィックを許可するマルチキャスト境界の設定例	320
トラフィックを拒否するマルチキャスト境界の設定例	320
IP マルチキャストの最適化：マルチキャスト向け SSM チャンネル ベース フィルタリングに関するその他の参考資料	321
IP マルチキャストの最適化の機能履歴：マルチキャスト向け SSM チャンネル ベース フィルタリング	321

第 16 章

IP マルチキャストの最適化：IGMP ステート制限	323
IGMP ステート制限の前提条件	323
IGMP ステート制限の制約事項	323
IGMP ステート制限に関する情報	323
IGMP ステート制限	324
IGMP ステート制限機能の設計	324
IGMP ステート リミッタのメカニズム	324
IGMP ステート制限の設定方法	325
IGMP ステート リミッタの設定	325
グローバルな IGMP ステート リミッタの設定	325
インターフェイスごとの IGMP ステート リミッタの設定	326
IGMP ステート制限の設定例	327
IGMP ステート リミッタの設定例	327
その他の参考資料	329
IP マルチキャストの最適化の機能履歴：IGMP ステート制限	329



第 1 章

IP マルチキャスト ルーティング テクノロジーの概要

- [IP マルチキャスト テクノロジーに関する情報 \(1 ページ\)](#)
- [IP マルチキャストに関する追加情報 \(19 ページ\)](#)

IP マルチキャスト テクノロジーに関する情報

ここでは、IP マルチキャストテクノロジーについて説明します。

IP マルチキャストについて

マルチキャストグループに対する転送速度の制御はサポートされていません。

IP 通信の一端である IP ユニキャストでは、送信元 IP ホストが特定の宛先 IP ホストにパケットを送信します。この場合、IP パケットに指定される宛先アドレスは、IP ネットワーク上で一意に識別される単一ホストのアドレスです。これらの IP パケットは、ネットワーク上の送信元ホストから、一連のデバイスによって宛先ホストに転送されます。送信元と宛先間のパス上の各ポイントでは、デバイスがユニキャストルーティングテーブルを使用して、パケットの IP 宛先アドレスに基づきユニキャスト転送先を決定します。

IP 通信で IP ユニキャストの対極にある IP ブロードキャストでは、送信元ホストはネットワークセグメント上のすべてのホストにパケットを送信します。IP ブロードキャストパケットの宛先アドレスでは、宛先 IP アドレスのホスト部分がすべて 1 に設定され、ネットワーク部分がサブネットのアドレスに設定されています。一連の IP ホスト（デバイスを含む）は、宛先アドレスとして IP ブロードキャストアドレスを指定されたパケットが、サブネット上のすべての IP ホスト向けであることを認識しています。特に設定しない限り、デバイスは IP ブロードキャストパケットを転送しないので、一般的に IP ブロードキャスト通信はローカルサブネットに限定されます。

IP マルチキャストは、IP ユニキャスト通信と IP ブロードキャスト通信の間に位置します。IP マルチキャスト通信によって、ホストは IP ネットワーク上の任意の場所にあるホストのグループに IP パケットを送信します。IP マルチキャスト通信では、特定のグループに情報を送信するために、IP マルチキャストグループアドレスという特殊な形式の IP 宛先アドレスを使

用します。IP マルチキャストグループアドレスは、パケットの IP 宛先アドレスフィールドに指定されます。

IP 情報をマルチキャストするには、レイヤ 3 スイッチおよびデバイスが IP マルチキャストグループのメンバに接続する出力インターフェイスすべてに着信 IP パケットを転送する必要があります。

IP マルチキャストはビデオ会議と同じものとして考えられる傾向があります。ネットワークに初めて導入する IP マルチキャストアプリケーションは多くの場合ビデオ会議ですが、ビデオは実用的で多様な IP マルチキャストアプリケーションのひとつに過ぎません。生産性の向上につながる他の IP マルチキャストアプリケーションとしては、マルチメディア会議、データ複製、リアルタイムデータマルチキャスト、シミュレーションアプリケーションなどがあります。

情報配信における IP マルチキャストの役割

IP マルチキャストは、単一の情報ストリームを何千もの潜在的な企業および家庭に同時に配信することによってトラフィックを削減する帯域幅節約テクノロジーです。マルチキャストを利用するアプリケーションには、ビデオ会議、企業コミュニケーション、通信教育、およびソフトウェア、株価情報、ニュースの配信などが含まれます。

IP マルチキャストルーティングにより、ホスト（ソース）は、IP マルチキャストグループアドレスと呼ばれる特別な形式の IP アドレスを使用して、IP ネットワーク内の任意の場所にあるホスト（レシーバ）にパケットを送信できます。ソースのホストは、マルチキャストグループアドレスをパケットの宛先 IP アドレスフィールドに挿入します。IP マルチキャストルータおよびマルチレイヤスイッチは、受信した IP マルチキャストパケットを、マルチキャストグループのメンバにつながるすべてのインターフェイスから転送します。どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージを受信します。

IP マルチキャストルーティングプロトコル

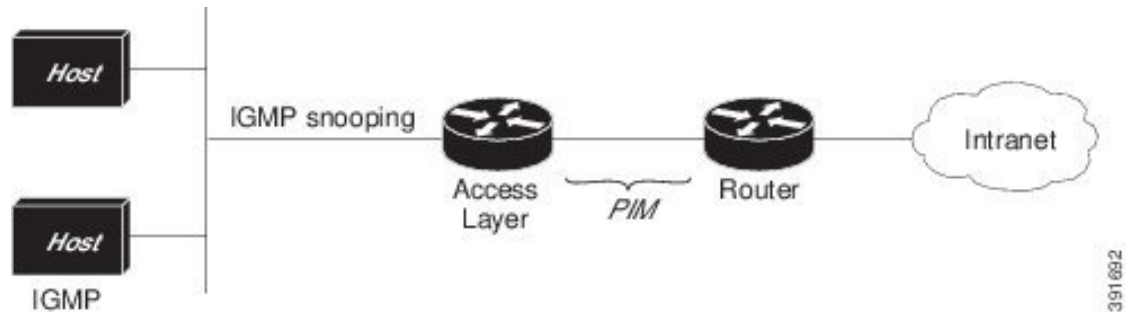
ソフトウェアでは、IP マルチキャストルーティングを実装するため、次のプロトコルがサポートされています。

- IGMP を LNA 上のホストとその LAN 上のルータ（およびマルチレイヤデバイス）間で使用して、ホストがメンバになっているマルチキャストグループを追跡します。IP マルチキャストルーティングに参加するには、マルチキャストホスト、ルータ、およびマルチレイヤデバイスで Internet Group Management Protocol (IGMP) が動作している必要があります。
- PIM (Protocol Independent Multicast) は、相互に転送されるマルチキャストパケット、および直接接続されている LAN に転送されるマルチキャストパケットを追跡するためにルータ間で使用されます。
- IGMP スヌーピングは、レイヤ 2 スイッチング環境でのマルチキャストに使用します。レイヤ 2 インターフェイスを動的に設定し、マルチキャストトラフィックが IP マルチキャスト

ストデバイスと関連付けられたインターフェイスにだけ転送されるようにすることによって、マルチキャストトラフィックのフラディングを削減します。

次の図に、これらのプロトコルが IP マルチキャスト環境内のどの部分で動作するかを示します。

図 1: IP マルチキャストルーティングプロトコル



IPv4 マルチキャスト標準に従い、MAC 宛先マルチキャストアドレスは 0100:5e で始まり、IP アドレスの末尾 23 ビットが付加されます。たとえば、IP 宛先アドレスが 239.1.1.39 の場合、MAC 宛先アドレスは 0100:5e01:0127 となります。

IPv4 宛先アドレスと MAC 宛先アドレスが一致しない場合、マルチキャストパケットは一致しません。デバイスは、ハードウェア内の一致しないパケットを MAC アドレステーブルに基づいて転送します。MAC 宛先アドレスが MAC アドレステーブルにない場合、デバイスは受信したポートと同じ VLAN 内のすべてのポートにパケットをフラディングします。

Internet Group Management Protocol (インターネットグループ管理プロトコル)

IP マルチキャストホストは IGMP メッセージを使用して、ローカルのレイヤ 3 スイッチまたはルータに要求を送信し、特定のマルチキャストグループに加入して、マルチキャストトラフィックの受信を開始します。IGMPv2 の一部の拡張機能を使用すると、IP ホストはレイヤ 3 スイッチまたはルータに対し、IP マルチキャストグループを脱退してマルチキャストグループトラフィックを受信しないように求める要求も送信します。

レイヤ 3 スイッチまたはルータは、IGMP によって得た情報を使用して、マルチキャストグループメンバーシップのリストをインターフェイス単位で維持します。インターフェイス上で少なくとも 1 つのホストが、マルチキャストグループトラフィックを受信するための IGMP 要求を送信している限り、そのインターフェイスのマルチキャストグループメンバーシップはアクティブです。

プロトコル独立マルチキャスト

プロトコル独立マルチキャスト (PIM) がプロトコルに依存しない理由は、使用されている任意のユニキャストルーティングプロトコルを利用してルーティングテーブルへの書き込みを行い (Enhanced Interior Gateway Routing Protocol (EIGRP)、Open Shortest Path First (OSPF)、およびスタティックルートを含む)、IP マルチキャストをサポートするからです。

PIM スパース モード (PIM-SM)

PIM はさらに、完全に独立したマルチキャスト ルーティング テーブルを作成する代わりに、ユニキャスト ルーティング テーブルを使用して Reverse Path Forwarding (RPF) チェック機能を実行します。PIM は、他のルーティングプロトコルが行うような、ルータ間でのマルチキャスト ルーティング アップデートの送受信は行いません。

PIM スパース モード (PIM-SM)

PIM スパース モード (PIM-SM) は、プルモデルを使用してマルチキャスト トラフィックを配信します。明示的にデータを要求した、アクティブな受信者のいるネットワークだけにトラフィックが転送されます。PIM-SM は、デスクトップビデオ会議や企業コンピューティングなど、少数の受信者がそれぞれ異なるマルチキャストを一般に同時使用するネットワークでの使用を目的としています。

ランデブー ポイント

また、PIM をスパースモードで動作するよう構成する場合は、1つまたは複数のデバイスをランデブー ポイント (RP) とするよう選択する必要があります。マルチキャスト グループへの送信者は、RP を使用してその存在を通知します。マルチキャスト パケットの受信者は、RP を使用して新しい送信者について学習します。1つのマルチキャスト グループのパケットが1つまたは複数の RP を使用できるように Cisco IOS ソフトウェアを構成できます。

RP アドレスは、パケットをグループに送信するホストの代わりに PIM Register メッセージを送信するためにファーストホップデバイスによって使用されます。また、RP アドレスは、ラストホップデバイスによって PIM join および prune メッセージを RP に送信してグループメンバシップについて通知するためにも使用されます。すべてのデバイス (RP デバイスを含む) で RP アドレスを設定する必要があります。

1台の PIM デバイスを、複数のグループの RP にできます。同じグループの PIM ドメイン内で一度に使用できる RP アドレスは1つだけです。アクセスリストで指定されている条件は、(異なるグループが異なる RP を持つことが可能なため) デバイスがいずれのグループの RP であるかを決定します。

IGMP スヌーピング

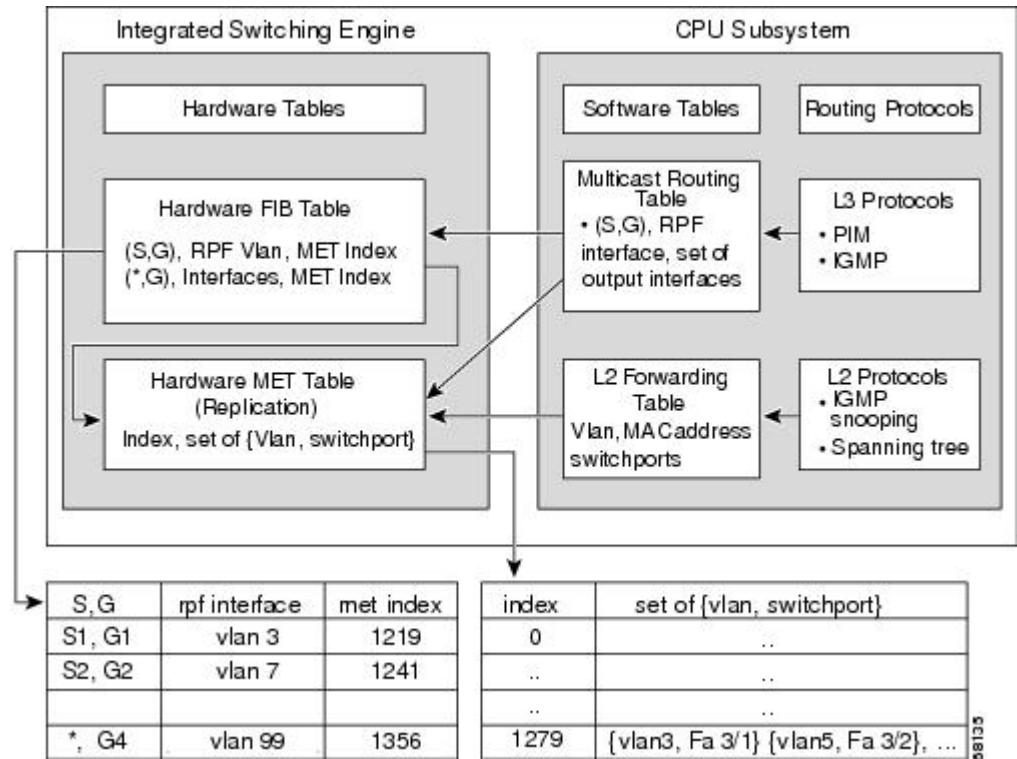
IGMP スヌーピングは、レイヤ2 スイッチング環境でのマルチキャストに使用します。IGMP スヌーピングを使用する場合、レイヤ3 スイッチまたはルータは、ホストとデバイス間で転送される IGMP パケットのレイヤ3 情報を検証します。スイッチが特定のマルチキャストグループのホストから IGMP Host Report を受信すると、スイッチはそのホストのポート番号を対応するマルチキャスト テーブル エントリに追加します。スイッチがホストから IGMP Leave Group メッセージを受信すると、スイッチはテーブル エントリからそのホストのポートを削除します。

IGMP 制御メッセージはマルチキャスト パケットとして送信されるので、レイヤ2 ヘッダーだけが検証される場合は、マルチキャスト データと区別できません。IGMP スヌーピングが稼働しているスイッチは、すべてのマルチキャスト データ パケットについて、関連する IGMP 制御情報が含まれているかどうかを調べます。低速の CPU を搭載したローエンドのスイッチに IGMP スヌーピングを実装すると、データを高速で送信する場合、パフォーマンスに重大な影響が出る可能性があります。

IP マルチキャスト テーブル

次に、デバイスがハードウェアで IP マルチキャスト パケットを転送する目的で使用する主なデータ構造図を示します。

図 2: IP マルチキャスト テーブルおよびプロトコル



Integrated Switching Engine は、個々の IP マルチキャスト ルートを識別する目的で、ハードウェア FIB テーブルを維持します。各エントリは、宛先グループの IP アドレスおよびオプションの送信元 IP アドレスで構成されます。マルチキャストトラフィックは、主に (S,G) および (*,G) の 2 種類のルート上を流れます。(S,G) ルートは、マルチキャスト送信元の IP アドレスと、マルチキャストグループ宛先の IP アドレスに基づいて、送信元からグループへ流れます>(* ,G) ルートのトラフィックは、PIM RP からグループ G のすべての受信者へ流れます>(* ,G) ルートを使用するのは、スパースモードグループだけです。Integrated Switching Engine ハードウェアには、合計 128,000 のルート用のスペースが準備されています。これらがユニキャストルート、マルチキャストルート、およびマルチキャスト高速ドロップエントリによって共有されます。

出力インターフェイスのリストは、Multicast Expansion Table (MET) に保存されます。MET には、最大 32,000 の出力インターフェイスリスト用のスペースがあります (RET には、最大 102 K エントリ (フラッディングセットに 32 K、マルチキャストエントリに 70,000 使用) が可能です)。MET リソースは、レイヤ 3 マルチキャストルートおよびレイヤ 2 マルチキャストエントリによって共有されます。ハードウェアで使用できる出力インターフェイスリストの実際数は、設定によって異なります。マルチキャストルートの総数が 32,000 を超えると、Integrated Switching Engine によってマルチキャストパケットをスイッチングできなくなる場合があります。

す。そのパケットは、CPUサブシステムによってきわめて低い速度で転送されることとなります。



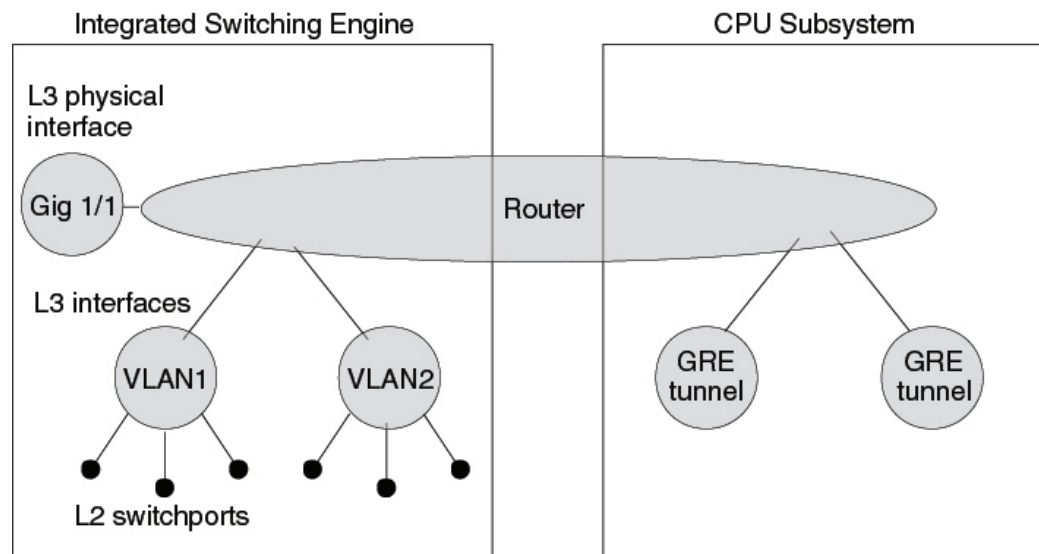
(注) (RET では 102 K エントリまでサポートされます (フラッディングセットに 32K、multicast エントリに 70 K を使用))。

ハードウェアおよびソフトウェアによる転送

Integrated Switching Engine は通常、パケットをハードウェアで非常に高速で転送します。CPU サブシステムは、例外パケットをソフトウェアで転送します。Integrated Switching Engine が大部分のパケットをハードウェアで転送していることは、統計レポートからわかります。

次に、ハードウェアとソフトウェアの転送コンポーネントの概念図を示します。

図 3: ハードウェアおよびソフトウェアの転送コンポーネント



Integrated Switching Engine は、通常の動作モードでは、ハードウェアで VLAN 間ルーティングを実行します。CPU サブシステムは、ソフトウェアによる転送のために、総称ルーティングカプセル化 (GRE) トンネルをサポートしています。

複製は、パケットの 1 コピーを送信する代わりに、パケットを複製して複数のコピーを送信する転送の一種です。レイヤ 3 で複製が行われるのは、マルチキャストパケットに限られます。ユニキャストパケットが複数のレイヤ 3 インターフェイス用に複製されることはありません。IP マルチキャスト動作では、着信した IP マルチキャストパケットごとに、そのパケットの多くの複製が送信されます。

IP マルチキャストパケットを伝送するルートのタイプは、次のとおりです。

- ハードウェアルート

- ソフトウェア ルート
- 部分的なルート

ハードウェア ルートは、**Integrated Switching Engine** ハードウェアがパケットのすべての複製を転送する場合に発生します。ソフトウェア ルートは、**CPU** サブシステムソフトウェアがパケットのすべての複製を転送する場合に発生します。部分的なルートは、**Integrated Switching Engine** が一部の複製をハードウェアで転送し、**CPU** サブシステムが一部の複製をソフトウェアで転送する場合に発生します。

部分的なルート



- (注) 以下に記載する条件が成立する場合、**CPU** サブシステムソフトウェアによって複製が転送されますが、ハードウェアによる複製の転送パフォーマンスに影響はありません。

あるルートに対するパケットの複製の一部が **CPU** サブシステムによって転送される条件は、次のとおりです。

- **ip igmp join-group** コマンドを使用して、マルチキャスト送信元の **RPF** インターフェイス上の **IP** マルチキャストグループのメンバとしてスイッチを設定している場合。
- スイッチが **PIM** スパース モードの送信元へのファースト ホップである場合。スイッチは **RP** に **PIM Register** メッセージを送信する必要があります。

ソフトウェア ルート



- (注) **RPF** インターフェイスまたは出力インターフェイスの設定について次の条件が1つでも成立すると、出力のすべての複製はソフトウェアで実行されます。

あるルートに対するパケットの複製の一部が **CPU** サブシステムソフトウェアによって転送される条件は、次のとおりです。

- インターフェイスがマルチキャスト ヘルパーを使用して設定されている場合
- インターフェイスが **GRE** トンネルまたはディスタンス ベクトルマルチキャストルーティング プロトコル (**DVMRP**) トンネルである場合
- インターフェイスが高等研究計画局 (**ARPA**) 以外のカプセル化を使用している場合

次のパケットは、常にソフトウェアによって転送されます。

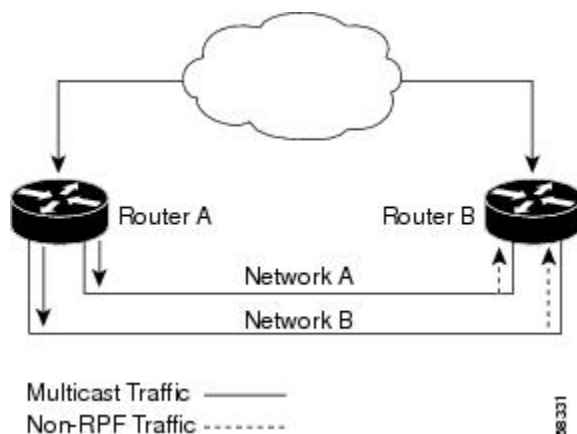
- **224.0.0.*** (* は 0 ~ 255) の範囲のマルチキャストグループに送信されるパケット。この範囲は、ルーティングプロトコルが使用します。レイヤ3スイッチングでは、この範囲以外のすべてのマルチキャストグループアドレスがサポートされています。
- **IP** オプション付きのパケット

非リバースパスフォワーディングトラフィック

Reverse Path Forwarding (RPF) チェックに失敗したトラフィックを、非RPFトラフィックといいます。Integrated Switching Engine は、非RPFトラフィックをフィルタリング（持続的にドロップ）するか、またはレート制限して転送します。

複数のレイヤ3スイッチまたはルータが同一のLANセグメントに接続されている冗長な構成で、送信元から発信インターフェイス上の受信側へマルチキャストトラフィックを転送するのは、1台の装置だけです。次の図に、一般的なネットワーク構成で非RPFトラフィックが発生した状況を示します。

図4:スタブネットワークにおける冗長マルチキャストルータの構成



この種のトポロジでは、PIM 指定ルータ (PIM DR) であるルータ A だけが共通の VLAN にデータを転送します。ルータ B は転送されたマルチキャストトラフィックを受信しますが、このトラフィックをドロップします。不正なインターフェイスでこのトラフィックが着信したため、RPF チェックに失敗するためです。このように RPF チェックに失敗するトラフィックを、「非 RPF トラフィック」といいます。

マルチキャストグループ伝送方式

IP 通信は、最初の図に示すように、トラフィックの送信者として機能するホストと、レシーバとして機能するホストで構成されます。送信者はソースと呼ばれます。従来の IP 通信は、単一のホストソースがパケットを別の単一ホスト (ユニキャスト伝送) またはすべてのホスト (ブロードキャスト伝送) に送信することによって行われます。IP マルチキャストは第三の方式を提供するものであり、ホストはすべてのホストのサブセットにパケットを送信できます (マルチキャスト伝送)。受信側のホストのこのサブセットをマルチキャストグループと呼びます。マルチキャストグループに属するホストは、グループメンバと呼ばれます。

マルチキャストは、このグループの概念に基づいています。マルチキャストグループは、特定のデータストリームを受信するためにグループに加入する任意の数のレシーバです。このマルチキャストグループには、物理的境界または地理的境界はありません。ホストは、インターネット上または任意のプライベートネットワーク上のどこにでも配置できます。ソースから特定のグループに対するデータを受信する必要があるホストはそのグループに加入する必要があります。

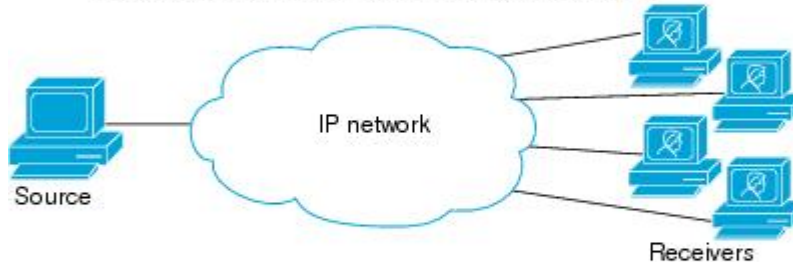
ります。グループに加入するには、ホスト レシーバで Internet Group Management Protocol (IGMP) を使用します。

マルチキャスト環境では、どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、そのグループに送信されたパケットはグループのメンバだけが受信できます。IP ユニキャストパケットと同様、マルチキャストパケットは、ベストエフォート型の信頼性を使用してグループに配信されます。

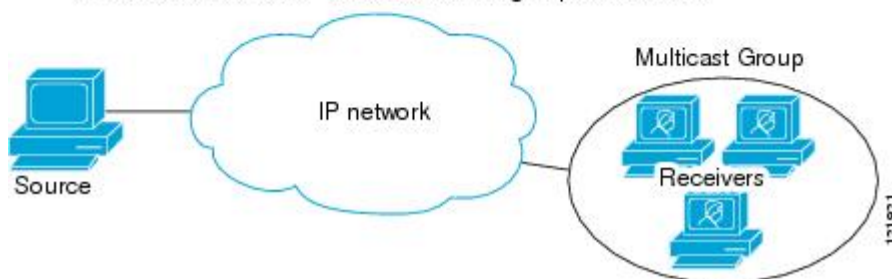
Unicast transmission—One host sends and the other receives.



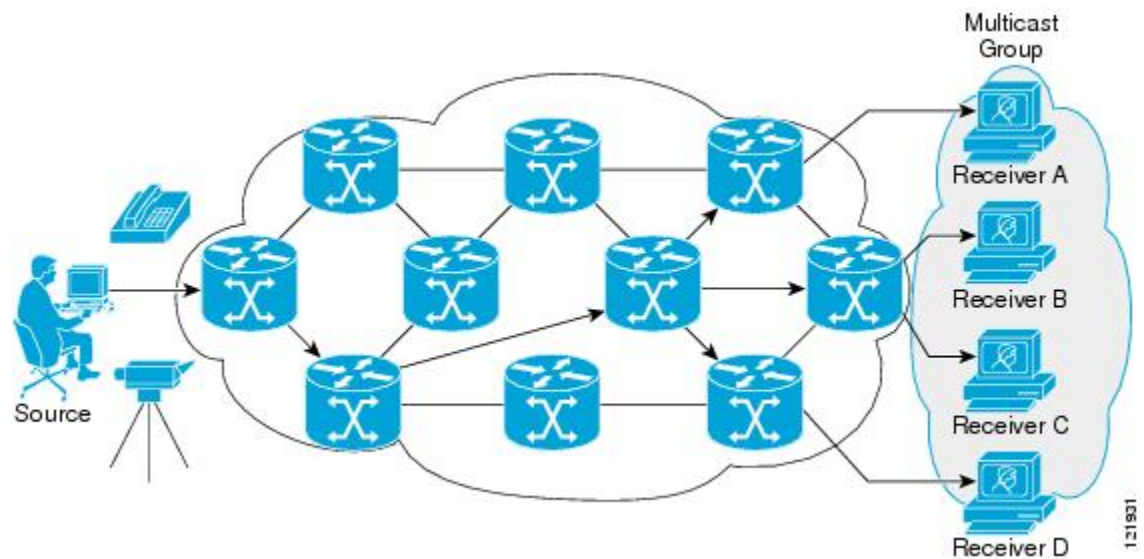
Broadcast transmission—One sender to all receivers.



Multicast transmission—One sender to a group of receivers.



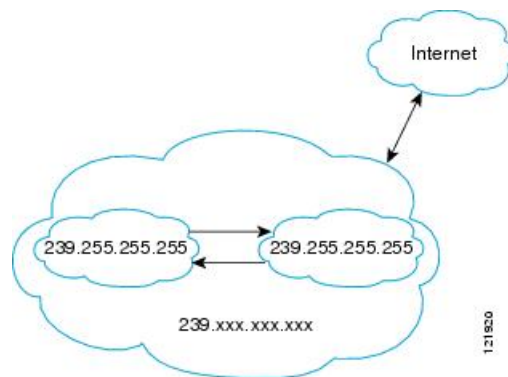
次の図では、レシーバ（指定したマルチキャストグループ）がソースからのビデオデータストリームを受信する必要があります。これらのレシーバは、ネットワーク内のルータに IGMP ホストレポートを送信することによってその意思を示します。この場合、ルータがソースからレシーバへのデータの配信を担います。ルータは、Protocol Independent Multicast (PIM) を使用して、マルチキャスト配信ツリーを動的に作成します。その後、ソースとレシーバ間のパスにあるネットワークセグメントにのみ、ビデオデータストリームが配信されます。



IP マルチキャスト境界

図に示すように、アドレス スコーピングは、同じ IP アドレスを持つ RP が含まれるドメインが相互にデータを漏出させることのないように、ドメイン境界を定義します。スコーピングは、大きなドメイン内のサブネット境界や、ドメインとインターネットの間の境界で実行されます。

図 5: 境界でのアドレス スコーピング



マルチキャスト グループ アドレッシングのインターフェイスに管理スコープの境界を設定するには、**ip multicast boundary** コマンドと *access-list* 引数を使用します。影響を受けるアドレス範囲は、標準アクセスリストによって定義されます。境界が設定されると、マルチキャスト データ パケットは境界を越えて出入りできなくなります。境界を定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

Internet Assigned Numbers Authority (IANA) は、マルチキャスト アドレス範囲 239.0.0.0 ~ 239.255.255.255 を管理スコープアドレスとして指定しています。この範囲のアドレスは、さまざまな組織で管理されるドメイン内で再使用されます。これらは、グローバルに一意ではなくローカルとみなされます。

filter-autorp キーワードを設定して、管理用スコープの境界で Auto-RP 検出と通知メッセージを検査し、フィルタできます。境界のアクセスコントロールリスト (ACL) に拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

IP マルチキャストグループアドレッシング

マルチキャストグループは、マルチキャストグループアドレスによって識別されます。マルチキャストパケットは、そのマルチキャストグループアドレスに配信されます。単一のホストを独自に識別するユニキャストアドレスとは異なり、マルチキャスト IP アドレスは特定のホストを識別しません。マルチキャストアドレスに送信されるデータを受信するには、アドレスが識別するグループにホストが参加する必要があります。データは、マルチキャストアドレスに送信され、そのグループに送信されたトラフィックを受信する意思を示してグループに加入しているすべてのホストによって受信されます。マルチキャストグループアドレスは、送信元でグループに割り当てられます。マルチキャストグループアドレスを割り当てるネットワーク管理者は、Internet Assigned Numbers Authority (IANA) で予約されるマルチキャストアドレスの範囲にアドレスが準拠していることを確認する必要があります。

IP クラス D アドレス

IP マルチキャストアドレスは、IANA によって IPv4 クラス D アドレス空間に割り当てられました。クラス D アドレスの上位 4 ビットは 1110 です。したがって、ホストグループアドレスの範囲は 224.0.0.0 ~ 239.255.255.255 であると考えられます。マルチキャストアドレスは送信元 (送信者) でマルチキャストグループの受信先として選択されます。



- (注) クラス D アドレスの範囲は、IP マルチキャストトラフィックのグループアドレスまたは宛先アドレスにだけ使用されます。マルチキャストデータグラムの送信元アドレスは常にユニキャスト送信元アドレスになります。

IP マルチキャストアドレスのスコーピング

さまざまなアドレス範囲の予測可能な動作を提供したり、より小規模なドメイン内でアドレスを再利用したりできるよう、マルチキャストアドレスの範囲はさらに分割されます。表に、マルチキャストアドレスの範囲を要約します。それに続いて、各範囲について簡単に説明します。

表 1: マルチキャストアドレス範囲の割り当て

名前	範囲	説明
予約済みリンクローカルアドレス	224.0.0.0 ~ 224.0.0.255	ローカルネットワークセグメントのネットワークプロトコルで使用するために予約されています。

名前	範囲	説明
グローバル スコープ アドレス	224.0.1.0 ~ 238.255.255.255	組織間およびインターネット上でマルチキャスト データを送信するために予約されています。
Source Specific Multicast	232.0.0.0 ~ 232.255.255.255	明示的にグループに参加している受信者だけにデータを転送する SSM データグラム配信モデル用に予約されています。
GLOP アドレス	233.0.0.0 ~ 233.255.255.255	割り当て済みの自律システム (AS) ドメイン番号をすでに持つ組織によって静的に定義されるアドレス用に予約されています。
限定スコープ アドレス	239.0.0.0 ~ 239.255.255.255	管理スコープアドレスまたはプライベート マルチキャスト ドメインで使用するための限定スコープアドレスとして予約されています。

予約済みリンクローカルアドレス

IANA では、ローカル ネットワーク セグメントのネットワーク プロトコルで使用するために 224.0.0.0 ~ 224.0.0.255 の範囲を予約しています。この範囲のアドレスを持つパケットはスコープ内ローカルであり、IP ルータによって転送されません。通常、リンク ローカル宛先アドレスを持つパケットは存続可能時間 (TTL) 値 1 を使用して送信されるため、ルータによって転送されません。

この範囲内の予約済みリンクローカルアドレスは、それぞれに予約されたネットワーク プロトコル機能を提供します。ネットワーク プロトコルは、これらのアドレスをルータの自動検出および重要なルーティング情報の伝達用に使用します。たとえば、Open Shortest Path First (OSPF) は、IP アドレスの 224.0.0.5 と 224.0.0.6 を使用してリンクステート情報を交換します。

IANA では、ネットワーク プロトコルやネットワーク アプリケーションに対する単一マルチキャスト アドレス要求を 224.0.1.xxx のアドレス範囲外に割り当てています。マルチキャスト ルータはこれらのマルチキャスト アドレスを転送します。



(注) ASR 903 RSP2 モジュールでは、デフォルトにより、予約済みのリンクローカルアドレスを持つすべてのパケットが CPU にバントされます。

グローバル スコープ アドレス

224.0.1.0 ~ 238.255.255.255 の範囲のアドレスは、グローバル スコープ アドレスと呼ばれます。これらのアドレスは、組織間およびインターネット上でのマルチキャスト データの送信に使用します。これらのアドレスの一部はマルチキャスト アプリケーションで使用するよう IANA によって予約されています。たとえば、IP アドレス 224.0.1.1 は、Network Time Protocol (NTP) 用に予約されています。

Source Specific Multicast アドレス

232.0.0.0/8 のアドレス範囲は、Source Specific Multicast (SSM) 用に予約されています。Cisco IOS ソフトウェアでは、**ip pim ssm** コマンドを使用して任意の IP マルチキャストアドレス用の SSM も設定できます。SSM は、1 対多通信での効率的なデータ配信メカニズムを可能にする Protocol Independent Multicast (PIM) の拡張版です。SSM については、[IP マルチキャスト配信モード \(16 ページ\)](#) の項を参照してください。

GLOP アドレス

GLOP アドレッシングでは (233/8 の RFC 2770、GLOP アドレッシングで提案されているように)、AS 番号をすでに予約している組織による静的に定義されたアドレス用に 233.0.0.0/8 の範囲を予約することを提案しています。これは、GLOP アドレッシングと呼ばれます。ドメインの AS 番号は 233.0.0.0/8 アドレス範囲の 2 番目と 3 番目のオクテットに組み込まれます。たとえば、AS 62010 は 16 進数形式で F23A と表されます。この 2 つのオクテット F2 および 3A を分割すると、結果は 10 進数でそれぞれ 242 および 58 となります。これらの値は、AS 62010 に使用するようにグローバルに予約される 233.242.58.0/24 のサブネットとなります。

限定スコープアドレス

239.0.0.0 ~ 239.255.255.255 の範囲は、管理スコープアドレス、またはプライベートマルチキャストドメインで使用する限定スコープアドレスとして予約されています。これらのアドレスは、ローカルグループまたは組織に使用するように制限されています。会社、大学および他の組織は、限定スコープアドレスを使用すると、ドメイン外に転送されないローカルマルチキャストアプリケーションを使用できます。通常、ルータは、このアドレス範囲のマルチキャストトラフィックが自律システム (AS) またはユーザー定義のドメイン外にフローしないようにするフィルタを使用して設定されます。AS またはドメイン内では、ローカルマルチキャスト境界を定義できるように、限定スコープアドレス範囲を細分化することもできます。



- (注) ネットワーク管理者はこの範囲内のマルチキャストアドレスを使用できます。これによって、インターネット内の他の場所と競合することはありません。

レイヤ2 マルチキャストアドレス

従来、LAN セグメントのネットワーク インターフェイス カード (NIC) が受信できるのは、Burned-In MAC Address またはブロードキャスト MAC アドレスに指定されたパケットだけでした。IP マルチキャストでは、複数のホストが共通の宛先 MAC アドレスを使用した単一のデータストリームを受信する必要があります。複数のホストが同じパケットを受信する場合、複数のマルチキャストグループを区別できるように、何らかの方法を考案する必要があります。そのための 1 つの方法は、IP マルチキャスト クラス D アドレスを MAC アドレスに直接マッピングすることです。この方法を使用すると、NIC は多くの異なる MAC アドレスを宛先とするパケットを受信できます。

Cisco グループ管理プロトコル (CGMP) は、IGMP によって実行される作業と同様の作業を実行するために、Catalyst スイッチに接続されたルータ上で使用されます。IP マルチキャスト

データ パケットと IGMP レポート メッセージ (いずれも MAC レベルで同じグループ アドレスにアドレス指定されます) を区別できない Catalyst スイッチの場合、CGMP が必要になります。

シスコ エクスプレス フォワーディング、MFIB、およびレイヤ2 転送

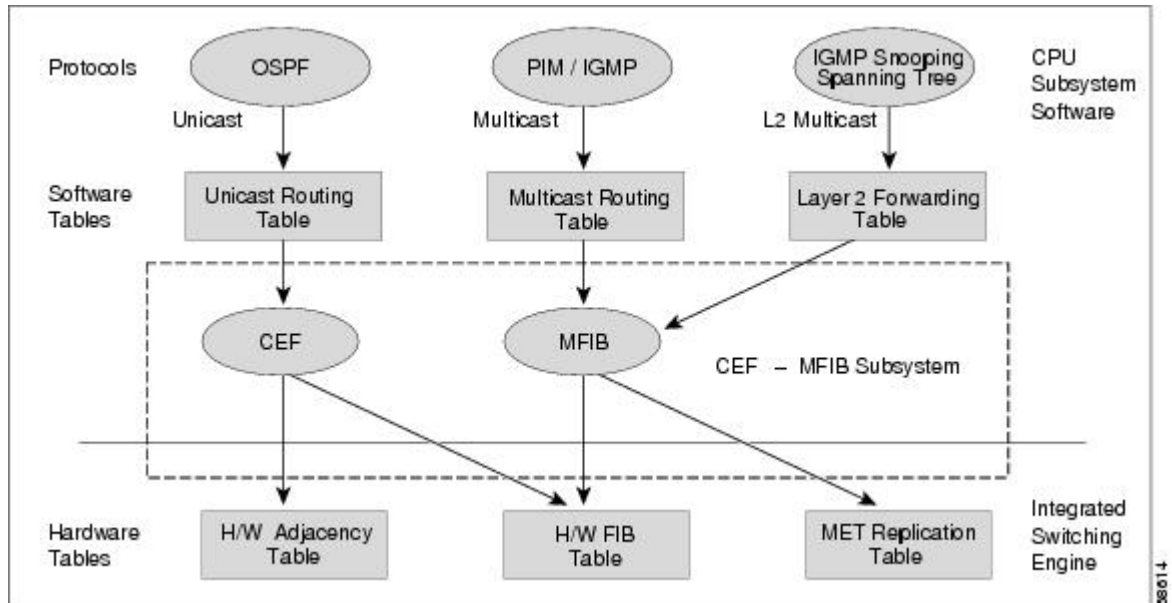
実装された IP マルチキャストは、中央集中型シスコ エクスプレス フォワーディングの拡張機能です。Cisco Express Forwarding は、ユニキャスト ルーティング テーブル (OSPF、EIGRP などのユニキャスト ルーティング プロトコルによって作成される) から情報を抽出し、この情報をハードウェアにロードします。

転送情報ベース (FIB) FIB のユニキャスト ルートを使用すると、上位層のルーティング テーブルでルートが変更された場合でも、ハードウェア ルーティング ステートの 1 つのルートを変更するだけです。ハードウェアでユニキャスト パケットを転送するために、Integrated Switching Engine は Ternary CAM (TCAM) から送信元および宛先ルートを検索し、ハードウェア FIB から隣接インデックスを取り出して、ハードウェア ネイバー テーブル関係からレイヤ 2 リライト情報およびネクストホップ アドレスを取得します。

マルチキャスト転送情報ベース (MFIB) サブシステムは、ユニキャストシスコ エクスプレス フォワーディングのマルチキャスト版です。この MFIB サブシステムは、PIM および IGMP によって作成されるマルチキャスト ルートを抽出し、ハードウェア転送のためのプロトコル独立フォーマットにします。MFIB サブシステムは、プロトコル固有の情報を削除し、必要なフォワーディング情報だけを残します。MFIB テーブルの各エントリは、(S,G) または (*,G) ルート、入力 RPF VLAN、およびレイヤ 3 出力インターフェイスのリストで構成されます。MFIB サブシステムは、プラットフォーム依存の管理ソフトウェアと連携して、このマルチキャスト ルーティング情報をハードウェア FIB およびハードウェア Replica Expansion Table (RET) にロードします。デバイスは、レイヤ 3 ルーティングとレイヤ 2 ブリッジングを同時に実行します。いずれの VLAN インターフェイスにも複数のレイヤ 2 スイッチ ポートを設定できます。

次の図に、シスコ デバイスがユニキャスト ルーティング、マルチキャスト ルーティング、およびレイヤ 2 ブリッジングの情報を組み合わせてハードウェアで転送を実行する機能の概要を示します。

図 6: ハードウェアでのシスコ エクスプレス フォワーディング、MFIB、およびレイヤ2 転送情報の組み合わせ



MFIB ルートは、シスコ エクスプレス フォワーディング ユニキャストルートと同様にレイヤ 3 であるため、該当するレイヤ 2 情報と結合する必要があります。MFIB ルートの例を示します。

```
(* ,203.0.113.1)
RPF interface is Vlan3
Output Interfaces are:
Vlan 1
Vlan 2
```

ルート (*,203.0.113.1) がハードウェア FIB テーブルにロードされ、出力インターフェイスのリストが MET にロードされます。出力インターフェイスのリストへのポインタ、MET インデックス、および RPF インターフェイスも、(*,203.0.113.1) ルートとともにハードウェア FIB にロードされます。ハードウェアにこの情報をロードすることで、レイヤ 2 情報との結合を開始できるようになります。VLAN1 上の出力インターフェイスについて、Integrated Switching Engine は VLAN 1 上でスパンニングツリーフォワーディングステートにあるすべてのスイッチポートにパケットを送信する必要があります。同じプロセスが VLAN2 に適用されます。VLAN 2 内のスイッチポートのセットを決定するために、レイヤ 2 転送テーブルが使用されます。

ハードウェアがパケットをルーティングする場合、すべての出力インターフェイスのすべてのスイッチポートにパケットを送信するだけでなく、ハードウェアは入力 VLAN の (パケットが到着したスイッチポートを除く) すべてのスイッチポートにも、パケットを送信します。たとえば、VLAN 3 に 2 つのスイッチポート、GigabitEthernet 3/1 および GigabitEthernet 3/2 があると仮定します。GigabitEthernet 3/1 上のホストがマルチキャストパケットを送信すると、GigabitEthernet 3/2 上のホストもそのパケットを受信しなければならない場合があります。GigabitEthernet 3/2 上のホストにマルチキャストパケットを送信するには、MET にロードされるポートセットに入力 VLAN のすべてのスイッチポートを追加する必要があります。

VLAN 1 に 1/1 および 1/2、VLAN 2 に 2/1 および 2/2、VLAN 3 に 3/1 および 3/2 が含まれていれば、このルート用の MET チェーンには、スイッチポート 1/1、1/2、2/1、2/2、3/1、および 3/2 が含まれることとなります。

IGMP スヌーピングがオンの場合、パケットは VLAN 2 のすべての出力スイッチポートに転送されるとは限りません。IGMP スヌーピングによって、グループメンバまたはルータが存在すると判断されたスイッチポートだけに、パケットが転送されます。たとえば、VLAN 1 で IGMP スヌーピングがイネーブルで、IGMP スヌーピングによってポート 1/2 だけにグループメンバが存在すると判断された場合、MET チェーンにはスイッチポート 1/1、1/2、2/1、2/2、3/1、および 3/2 が含まれることとなります。

IP マルチキャスト配信モード

IP マルチキャスト配信のモードは、送信元ホストではなく、受信側ホストのみによって異なります。送信元ホストは、パケットの IP 送信元アドレスとしての固有の IP アドレスと、パケットの IP 宛先アドレスとしてのグループアドレスを使用して、IP マルチキャストパケットを送信します。

Source Specific Multicast

Source Specific Multicast (SSM) は、ブロードキャストアプリケーションとしても知られる 1 対多アプリケーションをサポートする最善のデータグラム配信モデルです。SSM は、オーディオおよびビデオのブロードキャストアプリケーション環境を対象としたシスコの IP マルチキャストのコア ネットワーク テクノロジーです。

SSM 配信モードの場合、IP マルチキャスト レシーバホストは IGMP バージョン 3 (IGMPv3) を使用してチャンネル (S,G) を登録する必要があります。このチャンネルに登録することによって、ソースホストがグループ G に送信した IP マルチキャストトラフィックの受信をレシーバホストが要求していることを示します。ネットワークは、ソースホスト S からグループ G に送信された IP マルチキャストパケットを、チャンネル (S,G) に登録したネットワーク内のすべてのホストに配信します。

SSM では、ネットワーク内でグループアドレスを割り当てる必要はありません。各ソースホスト内で割り当てるだけです。同じソースホストで実行している各アプリケーションはそれぞれ異なる SSM グループを使用する必要があります。異なるソースホストで実行しているアプリケーションは、SSM グループアドレスを再利用できます。ネットワークに大量のトラフィックを発生させることはありません。

マルチキャスト高速ドロップ

PIM-SM、PIM-DM などの IP マルチキャストプロトコルでは、(S,G) または (*,G) ルートごとに、対応する着信インターフェイスがあります。このインターフェイスを、RPF インターフェイスといいます。予測される RPF インターフェイスとは異なるインターフェイスにパケットが到着することもあります。その場合、PIM によってパケットに特殊なプロトコル処理を行うために、そのパケットを CPU サブシステム ソフトウェアに転送する必要があります。PIM が実行する特殊なプロトコル処理の例としては、PIM アサートプロトコルがあります。

デフォルトでは、Integrated Switching Engine ハードウェアは、非 RPF インターフェイスに着信したすべてのパケットを CPU サブシステム ソフトウェアに送信します。ただし、これらの非 RPF パケットはほとんどの場合、マルチキャストルーティング プロトコルに必要ではないので、多くの場合、ソフトウェアによる処理は不要です。何の処置も行わなければ、ソフトウェアに送信される非 RPF パケットのため、CPU に負荷がかかるおそれがあります。

高速ドロップエントリをインストールするのではなく、シスコデバイスではダイナミックバッファ制限 (DBL) を使用します。このフローベースの輻輳回避メカニズムは、各トラフィックフローのキュー長を追跡することによりアクティブキュー管理を提供します。フローのキュー長がその設定された制限を超える場合、DBL がパケットをドロップします。CPU が過負荷にならないように、レート DBL は、CPU サブシステムに対する非 RPF トラフィックを制限します。パケットは CPU に対してフローごとにレート制限されます。CAM に高速ドロップエントリをインストールすることは不可能なため、スイッチで処理できる高速ドロップフローの数を制限する必要はありません。

リンクのダウン、ユニキャストルーティングテーブルの変更などのプロトコルイベントによって、安全に高速ドロップが可能なパケットの集合に影響が出ることがあります。以前は高速ドロップを行っても問題のなかったパケットを、トポロジの変更後、PIM ソフトウェアに処理させるため、CPU サブシステム ソフトウェアに転送する必要があります。CPU サブシステム ソフトウェアは、プロトコルイベントにตอบสนองして高速ドロップ エントリのフラッシュを行い、IOS の PIM コードが必要な RPF エラーをすべて処理できるようにします。

RPF エラーが繰り返し発生する可能性があるため、一部の一般的なトポロジでは、ハードウェアにおいて高速ドロップ エントリを使用することが重要です。高速ドロップ エントリがなければ、処理する必要のない RPF エラー パケットによって CPU が過負荷になります。

Multicast Forwarding Information Base (マルチキャスト転送情報ベース)

マルチキャスト転送情報ベース (MFIB) サブシステムは、シスコデバイス上の Integrated Switching Engine ハードウェアの IP マルチキャストルーティングをサポートします。MFIB は、論理的には CPU サブシステムソフトウェアの IP マルチキャストルーティングプロトコル (PIM、IGMP、MSDP、および DVMRP) と、ハードウェアで IP マルチキャストルーティングを管理するためのプラットフォーム固有のコードとの中間に存在します。MFIB は、マルチキャストルーティングプロトコルによって作成されたルーティングテーブル情報を、Integrated Switching Engine ハードウェアが効率的に処理して転送に使用可能な、簡易なフォーマットに変換します。

マルチキャストルーティングテーブルの情報を表示するには、**show ip mroute** コマンドを使用します。MFIB テーブルの情報を表示するには、**show ip mfib** コマンドを使用します。

MFIB テーブルには、IP マルチキャストルートの集合が含まれます。IP マルチキャストルートには (S,G) および (*,G) が含まれます。MFIB テーブルの各ルートに、オプションの 1 つまたは複数のフラグを対応付けることができます。ルートフラグは、ルートに一致するパケットの転送方法を指示します。たとえば、MFIB ルートに付けられた Internal Copy (IC) フラグは、スイッチ上のプロセスがパケットのコピーを受信する必要があることを意味します。MFIB ルートに対応付けできるフラグは、次のとおりです。

- **Internal Copy (IC) フラグ** : ルータ上のプロセスが、特定のルートに一致するすべてのパケットのコピーを受信する必要がある場合に設定します。
- **Signalling (S) フラグ** : このルートに一致するパケットを受信したときに、プロセスに通知する必要がある場合に設定します。シグナリングインターフェイス上でのパケット受信に応答して、プロトコルコードがMFIBステートを更新するなどの動作を行うことが考えられます。
- **Connected (C) フラグ** : このフラグをMFIBルートに設定した場合、直接接続されたホストによってルートに送信されたパケットだけをプロトコルプロセスに通知する必要があるという点を除き、**Signalling (S) フラグ**と同じ意味を持ちます。

ルートには、1つまたは複数のインターフェイスに対応するオプションのフラグを設定することもできます。たとえば、VLAN 1に関するフラグを設定した (S,G) ルートは、VLAN 1に着信するパケットをどのように扱うべきかと、このルートに一致するパケットをVLAN 1に転送すべきかを示します。MFIBでサポートされるインターフェイス単位のフラグは、次のとおりです。

- **Accepting (A)** : マルチキャストルーティングでRPFインターフェイスであることが明らかなインターフェイスに設定します。**Accepting (A)** をマークされたインターフェイスに着信したパケットは、すべての**Forwarding (F)** インターフェイスに転送されます。
- **Forwarding (F)** : 上記のように、**Accepting (A)** フラグと組み合わせて使用します。一連の転送インターフェイスは、マルチキャスト「olist」（出力インターフェイスリスト）と呼ばれるものを形成します。
- **Signalling (S)** : このインターフェイスにパケットが着信したとき、Cisco IOSの何らかのマルチキャストルーティングプロトコルプロセスに通知する必要がある場合に設定します。



(注) PIM-SM ルーティングを使用している場合、MFIB ルートには次の例のようなインターフェイスが含まれる場合があります。

```
PimTunnel [1.2.3.4]
```

これは、パケットが特定の宛先アドレスに対してトンネリングされていることを表すために、MFIB サブシステムが作成する仮想インターフェイスです。PimTunnel インターフェイスは、通常の **show interface** コマンドでは表示できません。

S/M,224/4

MFIBでは、マルチキャスト対応のインターフェイスごとに (S/M,224/4) エントリが作成されます。このエントリによって、直接接続されたネイバーから送信されたすべてのパケットが、PIM-SM RP に Register カプセル化されるようになります。一般に、PIM-SMによって (S,G) ルートが確立されるまでの間、ごく少数のパケットだけが (S/M,224/4) ルートを使用して転送されます。

たとえば、IP アドレス 10.0.0.1 および ネットマスク 255.0.0.0 のインターフェイスで、送信元アドレスがクラス A ネットワーク 10 に所属する IP マルチキャストパケットにすべて一致するルートが作成されるとします。このルートは、慣例的なサブネット/マスク長の表記では (10/8,224/4) と記述されます。インターフェイスに複数の IP アドレスが割り当てられている場合には、これらの IP アドレスごとに 1 つずつルートが作成されます。

マルチキャストハイアベイラビリティ

Cisco Catalyst 9200 シリーズスイッチはマルチキャストハイアベイラビリティをサポートします。これにより、スーパーバイザエンジンに障害が発生してもマルチキャストトラフィックのフローが中断されることはありません。MFIB ステートは、スイッチオーバーの前にスタンバイスーパーバイザエンジンに同期化され、スーパーバイザエンジンの障害時のスイッチオーバーのときに高速コンバージェンスでの NSF の可用性が確保されます。

マルチキャスト HA (SSO/NSF/ISSU) は、PIM スパースモードと SSM モードでサポートされます。つまり、IGMP および MLD スヌーピング用のレイヤ 2 でサポートされます。

IP マルチキャストに関する追加情報

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャストルーティングのコマンド」の項を参照してください。 <i>Command Reference (Catalyst 9200 Series Switches)</i>

標準および RFC

標準/RFC	タイトル
RFC 1112	『 <i>Host Extensions for IP Multicasting</i> 』
RFC 2236	『 <i>Internet Group Management Protocol, Version 2</i> 』
RFC 4601	『 <i>Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification</i> 』



第 2 章

基本的な IP マルチキャスト ルーティングの設定

- [基本的な IP マルチキャスト ルーティングに関する情報 \(21 ページ\)](#)
- [基本的な IP マルチキャスト ルーティングの設定方法 \(23 ページ\)](#)
- [基本的な IP マルチキャスト ルーティングのモニタリングおよびメンテナンス \(35 ページ\)](#)
- [基本的な IP マルチキャスト ルーティングの設定例 \(37 ページ\)](#)
- [基本的な IP マルチキャスト ルーティングに関するその他の関連情報 \(38 ページ\)](#)
- [基本的な IP マルチキャスト ルーティングの機能履歴 \(38 ページ\)](#)

基本的な IP マルチキャスト ルーティングに関する情報

IP マルチキャストは、ネットワーク リソース（特に、音声やビデオなどの帯域幅集約型サービス）を効率的に使用する方法です。IP マルチキャスト ルーティングにより、ホスト（ソース）は、IP マルチキャスト グループ アドレスと呼ばれる特別な形式の IP アドレスを使用し、IP ネットワーク内の任意の場所にあるホスト（レシーバ）にパケットを送信できます。

送信側ホストは、マルチキャスト グループ アドレスをパケットの IP 宛先アドレスフィールドに挿入します。IP マルチキャスト ルータおよびマルチレイヤ devices は、マルチキャスト グループのメンバに接続されたすべてのインターフェイスから着信した IP マルチキャスト パケットを転送します。どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージを受信します。

マルチキャスト 転送情報ベース (MFIB) の概要

device は、IP マルチキャスト用のマルチキャスト転送情報ベース (MFIB) アーキテクチャとマルチキャストルーティング情報ベース (MRIB) を使用します。

MFIB アーキテクチャは、マルチキャストコントロールプレーン (Protocol Independent Multicast (PIM) および Internet Group Management Protocol (IGMP)) とマルチキャスト フォワーディングプレーン (MFIB) の間におけるモジュール性と分離の両方を提供します。このアーキテクチャは、Cisco IOS IPv6 マルチキャスト導入環境において使用します。

MFIB 自体は、マルチキャストルーティングプロトコルを選ばないフォワーディングエンジンです。つまり、PIM または他のマルチキャストルーティングプロトコルに依存しません。これは次の処理に関与します。

- マルチキャストパケットの転送
- コントロールプレーンによって設定されたエントリとインターフェイスフラグを学習するための MRIB への登録
- コントロールプレーンに送信する必要があるデータ駆動型のイベントを処理する。
- 受信、ドロップ、および転送されたマルチキャストパケットの数、レート、およびバイトの保守

MRIB は、MRIB クライアント間の通信チャネルです。MRIB クライアントの例としては、PIM、IGMP、マルチキャストルーティング (mroute) テーブル、および MFIB があります。

IP マルチキャストルーティングのデフォルト設定

次の表に、IP マルチキャストルーティングのデフォルト設定を示します。

表 2: IP マルチキャストルーティングのデフォルト設定

機能	デフォルト設定
マルチキャストルーティング	すべてのインターフェイスでディ
PIM のバージョン	バージョン 2
PIM モード	モードは未定義
PIM スタブルーティング	未設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル。
PIM マルチキャスト境界	なし
候補 BSR	ディセーブル。
候補 RP	ディセーブル。
SPT しきい値レート	0 kb/s
PIM ルータ クエリー メッセージインターバル	30 秒

基本的な IP マルチキャスト ルーティングの設定方法

ここでは、基本的な IP マルチキャスト ルーティングの設定について説明します。

基本的な IP マルチキャスト ルーティングの設定

デフォルトでは、マルチキャスト ルーティングはディセーブルとなっており、モードは設定されていません。

この手順は必須です。

始める前に

PIM バージョンと PIM モードを設定する必要があります。スイッチはモード設定に従って、マルチキャスト ルーティング テーブルを読み込み、直接接続された LAN から受信したマルチキャスト パケットを転送します。

マルチキャスト ルーティング テーブルへのパケット読み込みでは、DM インターフェイスは常にテーブルに追加されます。SM インターフェイスがテーブルに追加されるのは、ダウンストリーム デバイスから定期的な Join メッセージを受信した場合、またはインターフェイスに直接接続されたメンバーが存在する場合に限ります。LAN から転送する場合、グループが認識している RP があれば、SM 動作が行われます。その場合、パケットはカプセル化され、その RP に送信されます。認識している RP がなければ、パケットは DM 方式でフラッディングされます。マルチキャスト送信元アドレスは、PIM デンスモードと PIM Any Source マルチキャストモードの両方で、直接接続された着信インターフェイス（同じサブネットの一部）に存在する必要があります。特定の送信元からのマルチキャストトラフィックが十分であれば、レシーバの先頭ホップルータからその送信元に Join メッセージが送信され、送信元を基点とする配信ツリーが構築されます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	<p>interface <i>interface-id</i></p> <p>例 :</p> <pre>Device(config)# interface gigabitethernet 1/0/1</pre>	<p>マルチキャスト ルーティングをイネーブルにするレイヤ3インターフェイスを指定し、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。</p> <p>次のいずれかのインターフェイスを指定する必要があります。</p> <ul style="list-style-type: none"> • ルーテッドポート：レイヤ3ポートとして no switchport インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。 • SVI： interface vlan <i>vlan-id</i> グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。 <p>これらのインターフェイスには、IP アドレスを割り当てる必要があります。</p>
ステップ 4	<p>ip pim {dense-mode sparse-mode sparse-dense-mode}</p> <p>例 :</p> <pre>Device(config-if)# ip pim sparse-dense-mode</pre>	<p>インターフェイスで PIM モードをイネーブルにします。</p> <p>デフォルトで、モードは設定されていません。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • dense-mode：デンス動作モードをイネーブルにします。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • sparse-mode : スパース動作モードをイネーブルにします。SMを設定する場合は、RP も設定する必要があります。 • sparse-dense-mode : グループが属するモードでインターフェイスが処理されるようにします。DM-SM 設定を推奨します。 <p>(注) インターフェイスで PIM を無効化するには、no ip pim インターフェイス コンフィギュレーション コマンドを使用します。</p>
ステップ 5	end 例 : <pre>Device(config-if) # end</pre>	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例 : <pre>Device# show running-config</pre>	入力を確認します。
ステップ 7	copy running-config startup-config 例 : <pre>Device# copy running-config startup-config</pre>	(任意) コンフィギュレーション ファイルに設定を保存します。

IP マルチキャスト転送の設定

次の手順を使用して、デバイスに着信パケットまたは発信パケットの IPv4 マルチキャスト転送情報ベース (MFIB) 割り込みレベルの IP マルチキャスト転送を設定できます。



- (注) **ip multicast-routing** コマンドを使用して IP マルチキャストルーティングを有効にした後、IPv4 マルチキャスト転送が有効になります。IPv4 マルチキャスト転送はデフォルトで有効になっているため、IPv4 マルチキャスト転送を無効にするには、**ip mfib** 形式の **no** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip mfib 例： Device(config)# ip mfib	IP マルチキャスト転送をイネーブルにします。
ステップ 4	exit 例： Device(config)# exit	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例： Device# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スタティック マルチキャストルート (mroute) の設定

- スタティック mroute は RPF 情報を計算するために使用されますが、トラフィックの転送には使用されません。
- スタティック mroute を再配布することはできません。

静的 mroute は、定義されているデバイスに厳密にローカルなものです。Protocol Independent Multicast (PIM) には独自のルーティング プロトコルがないため、ネットワーク全体にスタティック mroute を配布するメカニズムはありません。その結果、スタティック mroute の管理は、ユニキャスト スタティック ルートの管理よりも複雑になりがちです。

静的 mroute が設定されると、デバイスの静的 mroute テーブルと呼ばれる個別のテーブルに保存されます。設定されると、**ip mroute** コマンドによって、静的 mroute は、**source-address** および **mask** 引数に指定された送信元アドレスまたは送信元アドレス範囲の静的 mroute テーブルに入ります。送信元アドレスと一致する送信元、または **source-address** 引数に指定された送信元アドレス範囲にある送信元は、**rpf-address** 引数に指定された IP アドレスに関連付けられているインターフェイス、または **interface-type** および **interface-number** 引数に指定されたデバイス上のローカルインターフェイスに RPF を行います。IP アドレスが **rpf-address** 引数に指定されている場合、直接接続されたネイバーを検索するために、このアドレスでユニキャストルーティング テーブルから再帰ルックアップが実施されます。

複数の静的 mroute が設定されている場合、デバイスは mroute テーブルの最長一致ルックアップを実行します。(発信元アドレスの) 最長一致を含む mroute が見つかると、検索が終了し、一致するスタティック mroute の情報が使用されます。スタティック mroute が設定される順序は重要ではありません。

mroute のアドミニストレーティブ ディスタンスは、任意の距離引数に指定することができます。距離引数に値が指定されていない場合、mroute の距離はデフォルトのゼロになります。スタティック mroute が別の RPF 送信元と同じ距離である場合、スタティック mroute が優先されます。この規則には、2つだけ例外があります。直接接続されたルートとデフォルトのユニキャストルートです。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip mroute [vrf vrf-name] source-address mask { fallback-lookup {global vrf vrf-name } [protocol] {rpf-address interface-type interface-number}} [distance] 例： Device(config)# ip mroute 10.1.1.1 255.255.255.255 10.2.2.2	送信元 IP アドレス 10.1.1.1 が、IP アドレス 10.2.2.2 に関連付けられているインターフェイスを介して到達可能であるように設定されます。

	コマンドまたはアクション	目的
ステップ 4	exit 例： Device(config)# exit	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例： Device# show running-config	(任意) 入力を確認します。
ステップ 6	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

マルチキャスト VRF の設定

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip routing 例： Switch(config)# ip routing	IP ルーティングを有効にします。
ステップ 3	ip vrf vrf-name 例： Switch(config)# ip vrf vrf-name	VRF テーブルを設定し、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 4	ip multicast-routing vrf vrf-name 例： Switch(config-vrf)# ip multicast-routing vrf vrf-name	(任意) VRF テーブルでグローバル マルチキャストルーティングをイネーブルにします。
ステップ 5	rd route-distinguisher 例： Switch (config-vrf)# rd route-distinguisher	ルート識別子を指定して VRF テーブルを作成します。自律システム (AS) 番号および任意の数 (xxx.y) または IP アドレスおよび任意の数 (A.B.C.D:y) のどちらかを入力します。

	コマンドまたはアクション	目的
ステップ 6	route-target {export import both} <i>route-target-ext-community</i> 例 : <pre>Switch(config-vrf)# route-target {export import both} route-target-ext-community</pre>	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号 (xxx:y) または IP アドレスと任意の番号 (A.B.C.D:y) を入力します。 ルート ターゲット ext コミュニティ値は、ステップ 4 で入力した route-distinguisher 値と同じです。
ステップ 7	import map ルート マップ 例 : <pre>Switch(config-vrf)# import map route-map</pre>	(任意) VRF にルートマップを対応付けます。
ステップ 8	interface interface-id 例 : <pre>Switch (config)# interface interface-id</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て、VRF に対応付けるレイヤ 3 インターフェイスを指定します。有効なインターフェイスは、ルーテッドポートまたは SVI です。
ステップ 9	vrf forwarding vrf-name 例 : <pre>Switch (config-sg-tacacs+)# vrf forwarding vrf-name</pre>	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 10	ip address ip-addressmask 例 : <pre>Switch (config-if)# ip address ip-address mask</pre>	レイヤ 3 インターフェイスの IP アドレスを設定します。
ステップ 11	ip pim sparse-mode 例 : <pre>Switch(config-if)# ip pim sparse-mode</pre>	VRF に関連付けられているレイヤ 3 インターフェイス上で、PIM をイネーブルにします。
ステップ 12	end 例 : <pre>Switch(config-if)# end</pre>	特権 EXEC モードに戻ります。
ステップ 13	show ip vrf [brief detail interfaces] [vrf-name] 例 :	設定を確認します。設定した VRF に関する情報を表示します。

	コマンドまたはアクション	目的
	show ip vrf [brief detail interfaces] [vrf-name]	
ステップ 14	copy running-config startup-config 例： Switch# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

例

次に、VRF テーブル内にマルチキャストを設定する例を示します。

```
Switch(config)# ip routing
Switch(config)# ip vrf multiVrfA
Switch(config-vrf)# ip multicast-routing vrf multiVrfA
Switch(config-vrf)# interface GigabitEthernet3/1/0
Switch(config-if)# vrf forwarding multiVrfA
Switch(config-if)# ip address 172.21.200.203 255.255.255.0
Switch(config-if)# ip pim sparse-mode
```

オプションの IP マルチキャストルーティングの設定

ここでは、オプションの IP マルチキャストルーティングの設定について説明します。

IP マルチキャスト境界の定義

自動 RP メッセージが PIM ドメインに入らないようにする場合は、マルチキャスト境界を定義します。自動 RP 情報を伝達する 224.0.1.39 および 224.0.1.40 宛てのパケットを拒否するアクセスリストを作成します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	<p>access-list <i>access-list-number</i> deny <i>source</i> [<i>source-wildcard</i>]</p> <p>例 :</p> <pre>Device(config)# access-list 12 deny 224.0.1.39 access-list 12 deny 224.0.1.40</pre>	<p>標準アクセスリストを作成し、コマンドを必要な回数だけ実行します。</p> <ul style="list-style-type: none"> • <i>access-list-number</i> の範囲は 1 ~ 99 です。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。 • <i>source</i> には、自動 RP 情報を伝達するマルチキャストアドレス 224.0.1.39 および 224.0.1.40 を入力します。 • (任意) <i>source-wildcard</i> には、<i>source</i> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。</p>
ステップ 4	<p>interface <i>interface-id</i></p> <p>例 :</p> <pre>Device(config)# interface gigabitethernet 1/0/1</pre>	<p>設定するインターフェイスを指定して、インターフェイスコンフィギュレーションモードを開始します。</p> <p>次のいずれかのインターフェイスを指定する必要があります。</p> <ul style="list-style-type: none"> • ルーテッドポート : レイヤ3ポートとして no switchport インターフェイスコンフィギュレーションコマンドを入力して設定された物理ポートです。 • SVI : interface vlan <i>vlan-id</i> グローバルコンフィギュレーションコマンドを使用して作成された VLAN インターフェイスです。 <p>これらのインターフェイスには、IP アドレスを割り当てる必要があります。</p>
ステップ 5	<p>ip multicast boundary <i>access-list-number</i></p> <p>例 :</p>	<p>ステップ 2 で作成したアクセスリストを指定し、境界を設定します。</p>

	コマンドまたはアクション	目的
	Device(config-if)# ip multicast boundary 12	
ステップ 6	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例： Device# show running-config	入力を確認します。
ステップ 8	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

sdr リスナー サポートの設定

ここでは、sdr リスナーサポートの設定について説明します。

sdr リスナー サポート機能のイネーブル化

デフォルトでは、デバイスでセッションディレクトリのアドバタイズメントは受信されません。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	sdr 用にイネーブルにするインターフェイスを指定し、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。 次のいずれかのインターフェイス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
		<ul style="list-style-type: none"> • ルーテッドポート：レイヤ3ポートとして no switchport インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを IGMP スタティック グループに加入させる必要があります。設定例については、例：ルーテッドポートとしてのインターフェイス設定 (107 ページ) を参照してください。 • SVI： interface vlan vlan-id グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース - デンス モードをイネーブルにして、静的に接続されたメンバーとして VLAN を IGMP スタティック グループに加入させ、VLAN、IGMP スタティック グループ、および物理インターフェイスで IGMP スヌーピングをイネーブルにする必要があります。設定例については、例：SVIとしてのインターフェイスの設定 (107 ページ) を参照してください。 <p>これらのインターフェイスには、IP アドレスを割り当てる必要があります。</p>
ステップ 4	ip sap listen 例： Device(config-if)# ip sap listen	デバイスソフトウェアがセッションディレクトリ アナウンスメントをリスンできるようにします。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例：	入力を確認します。

	コマンドまたはアクション	目的
	Device# show running-config	
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

sdr キャッシュ エントリの存在期間の制限

デフォルトでは、エントリは sdr キャッシュ から削除されません。送信元が SAP 情報のアダプタイズを停止した場合に、古いアダプタイズメントが不必要に保持されないようにするため、エントリがアクティブである期間を制限できます。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip sap cache-timeout minutes 例： Device(config)# ip sap cache-timeout 30	Session Announcement Protocol (SAP) キャッシュ エントリがキャッシュ内にアクティブである期間を制限します。 デフォルトでは、エントリはキャッシュから削除されません。 <i>minutes</i> に指定できる範囲は 1 ~ 1440 分 (24 時間) です。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例： Device# show running-config	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	show ip sap 例： Device# show ip sap	SAP キャッシュを表示します。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

基本的な IP マルチキャスト ルーティングのモニタリングおよびメンテナンス

キャッシュ、テーブル、およびデータベースのクリア

特定のキャッシュ、テーブル、またはデータベースのすべての内容を削除できます。特定のキャッシュ、テーブル、またはデータベースの内容が無効である場合、または無効である可能性がある場合は、これらをクリアする必要があります。

次の表に示す特権 EXEC コマンドのいずれかを使用すると、IP マルチキャストのキャッシュ、テーブル、データベースをクリアできます。

表 3: キャッシュ、テーブル、およびデータベースをクリアするコマンド

コマンド	目的
clear ip igmp group {group [hostname IP address] vrf name group [hostname IP address]}	IGMP キャッシュ
clear ip mroute { * [hostname IP address] vrf name group [hostname IP address] }	IP マルチキャスト 除します。
clear ip sap [group-address "session-name"]	Session Directory P ッシュ) エントリを

システムおよびネットワーク統計情報の表示

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。



(注) このリリースでは、ルート単位の統計情報がサポートされていません。

また、リソースの使用状況を学習し、ネットワーク問題を解決するための情報を表示することもできます。さらに、ノードの到達可能性に関する情報を表示し、そのパケットが経由するネットワーク内のパスを検出することもできます。

次の表に示す特権 EXEC コマンドのいずれかを使用すると、さまざまなルーティング統計情報を表示できます。

表 4: システムおよびネットワーク統計情報を表示するコマンド

コマンド	目的
ping [<i>group-name</i> <i>group-address</i>]	マルチキャストグループアドレスに要求を送信します。
show ip igmp filter	IGMP フィルタ情報を表示します。
show ip igmp groups [<i>group-name</i> <i>group-address</i> <i>type-number</i>]	デバイスに直接接続され、IGMP に。
show ip igmp interface [<i>type number</i>]	インターフェイスのマルチキャスト
show ip igmp profile [<i>profile_number</i>]	IGMP プロファイル情報を表示しま
show ip igmp ssm-mapping [<i>hostname/IP address</i>]	IGMP SSM マッピング情報を表示し
show ip igmp static-group { <i>class-map</i> [<i>interface</i> [<i>type</i>]]}	スタティック グループ情報を表示し
show ip igmp membership [<i>name/group address</i> all tracked]	転送に関する IGMP メンバーシップ
show ip igmp vrf	選択した VPN ルーティング/転送イ
show ip mfib [<i>type number</i>]	IP マルチキャスト転送情報ベースを
show ip mrrib { <i>client</i> route vrf }	マルチキャスト ルーティング情報ベ
show ip mrm { <i>interface</i> manager status-report }	IP マルチキャスト ルーティング モ
show ip mroute [<i>group-name</i> <i>group-address</i>] [<i>source</i>] [count interface proxy pruned summary verbose]	IP マルチキャスト ルーティング テ
show ip msdp { count peer rpf-peer sa-cache summary vrf }	Multicast Source Discovery Protocol (M
show ip multicast [interface limit mpls redundancy vrf]	グローバル マルチキャスト情報を表
show ip pim all-vrfs { tunnel }	すべての VRF を表示します。
show ip pim autorp	グローバル Auto-RP 情報を表示しま
show ip pim boundary [<i>type number</i>]	境界情報を表示します。

コマンド	目的
<code>show ip pim bsr-router</code>	ブートストラップ ルータ情報 (ノード ID、優先度、アドレス)
<code>show ip pim interface [type number] [count detail df stats]</code>	PIM に対して設定されたインターフェイスのソフトウェア イメージで使用できる PIM 機能
<code>show ip pim neighbor [type number]</code>	デバイスによって検出された PIM ネイバールのソフトウェア イメージで使用できる PIM 機能
<code>show ip pim mdt [bgp]</code>	マルチキャスト トンネル情報を表示する
<code>show ip pim rp [group-name group-address]</code>	スパス モードのマルチキャスト ルーティング情報は、すべてのソフトウェア イメージで使用できる
<code>show ip pim rp-hash [group-name group-address]</code>	選択したグループに基づいて選択された PIM ルーティング
<code>show ip pim tunnel [tunnel verbose]</code>	登録済みのトンネルを表示します
<code>show ip pim vrf name</code>	VPN ルーティングおよび転送の PIM 機能
<code>show ip rpf {source-address name}</code>	デバイスの RPF の実行方法 (ユニキャスト、静的マルチキャストルーティング) の PIM 機能 コマンド パラメータは次のとおりです。 <ul style="list-style-type: none"> • Host name または IP address : ホスト名または IP アドレス • Select : グループ ベースの VRF • vrf : VPN ルーティング/転送
<code>show ip sap [group "session-name" detail]</code>	Session Announcement Protocol (SAP) の PIM 機能 コマンド パラメータは次のとおりです。 <ul style="list-style-type: none"> • A.B.C.D : IP グループ アドレス • WORD : セッション名 (二重引用符で囲む) • detail : セッションの詳細。

基本的な IP マルチキャストルーティングの設定例

ここでは、基本的な IP マルチキャストルーティングの設定例を紹介します。

例 : IP マルチキャスト境界の設定

次に、すべての管理用スコープのアドレスに対して境界を設定する例を示します。

例：mrinfo 要求への応答

```

デバイス(config)# access-list 1 deny 239.0.0.0 0.255.255.255
デバイス(config)# access-list 1 permit 224.0.0.0 15.255.255.255
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip multicast boundary 1

```

例：mrinfo 要求への応答

ソフトウェアは、マルチキャストルーティングされたシステム、シスコルータ、およびマルチレイヤデバイスによって送信された mrinfo 要求に応答します。ソフトウェアはネイバーに関する情報を、DVMRP トンネルおよびすべてのルーテッドインターフェイスを通して戻します。この情報にはメトリック（常に 1 に設定）、設定された TTL しきい値、インターフェイスのステータス、および各種フラグが含まれます。次の例のように、**mrinfo** 特権 EXEC コマンドを使用し、ルータまたは device 自体をクエリすることもできます。

```

デバイス# mrinfo
171.69.214.27 (mm1-7kd.cisco.com) [version cisco 11.1] [flags: PMS]:
171.69.214.27 -> 171.69.214.26 (mm1-r7kb.cisco.com) [1/0/pim/querier]
171.69.214.27 -> 171.69.214.25 (mm1-45a.cisco.com) [1/0/pim/querier]
171.69.214.33 -> 171.69.214.34 (mm1-45c.cisco.com) [1/0/pim]
171.69.214.137 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
171.69.214.203 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
171.69.214.18 -> 171.69.214.20 (mm1-45e.cisco.com) [1/0/pim]
171.69.214.18 -> 171.69.214.19 (mm1-45c.cisco.com) [1/0/pim]
171.69.214.18 -> 171.69.214.17 (mm1-45a.cisco.com) [1/0/pim]

```

基本的な IP マルチキャストルーティングに関するその他の関連情報

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャストルーティングのコマンド」の項を参照してください。 <i>Command Reference (Catalyst 9200 Series Switches)</i>

基本的な IP マルチキャストルーティングの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	IP マルチキャスト ルーティング	IP マルチキャストは、ネットワーク リソース（特に、音声やビデオなどの帯域幅集約型サービス）を効率的に使用する方法です。IP マルチキャストルーティングにより、ホスト（ソース）は、IP マルチキャストグループアドレスと呼ばれる特別な形式の IP アドレスを使用して、IP ネットワーク内の任意の場所にあるホスト（レシーバ）にパケットを送信できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 3 章

GRE トンネルを介するマルチキャストルーティングの設定

- [GRE トンネルを介するマルチキャストルーティングの設定の前提条件](#) (41 ページ)
- [GRE トンネルを介するマルチキャストルーティングの設定の制約事項](#) (41 ページ)
- [GRE トンネルを介するマルチキャストルーティングについて](#) (42 ページ)
- [GRE トンネルを介するマルチキャストルーティングの設定方法](#) (42 ページ)
- [GRE トンネルを介するマルチキャストルーティングに関するその他の参考資料](#) (45 ページ)
- [GRE トンネルを介するマルチキャストルーティングの機能履歴](#) (46 ページ)

GRE トンネルを介するマルチキャストルーティングの設定の前提条件

GRE を介するマルチキャストルーティングを設定する前に、IP マルチキャストルーティングテクノロジーと GRE トンネリングの概念についてよく理解しておく必要があります。

GRE トンネルを介するマルチキャストルーティングの設定の制約事項

次に、GRE トンネルを介するマルチキャストルーティングの設定の制約事項を示します。

- GRE トンネルを介する IPv6 マルチキャストはサポートされません。
- サポートされるマルチキャストルート (mroute) の総数は、すべてのトンネル全体で 1024 です。
- 双方向 PIM はサポートされていません。

- GRE トンネルを介するマルチキャストをサポートするには、マルチキャストルーティングを最初のホップルータ（FHR）、ランデブーポイント（RP）および最後のホップルータ（LHR）で設定する必要があります。
- Catalyst 9000 シリーズスイッチでは、トンネル送信元をループバックインターフェイス、物理インターフェイス、または L3 EtherChannel インターフェイスにできます。
- IPSec、ACL、トンネルカウンタ、暗号化サポート、フラグメンテーション、Cisco Discovery Protocol（CDP）、QoS、GRE キープアライブ、マルチポイント GRE などの機能の相互作用は、GRE トンネルでサポートされていません。

GRE トンネルを介するマルチキャストルーティングについて

この章では、非 IP マルチキャストエリア間で IP マルチキャストパケットをトンネリングするために、Generic Route Encapsulation（GRE）トンネルを設定する方法について説明します。その利点は、IP マルチキャストをサポートしないエリアを経由して、IP マルチキャストトラフィックをソースからマルチキャストグループに送信できることです。GRE トンネルを介するマルチキャストルーティングは、スプースモードおよび pim-ssm モードをサポートしています。また、スタティック RP および Auto-RP もサポートしています。スタティック RP と Auto-RP の設定の詳細については、ランデブーポイントと Auto-RP を参照してください。

非 IP マルチキャストエリアを接続するトンネリングの利点

- 送信元とグループメンバー（宛先）間のパスが IP マルチキャストをサポートしていない場合、それらの間のトンネルは IP マルチキャストパケットを転送できます。

GRE トンネルを介するマルチキャストルーティングの設定方法

ここでは、GRE トンネルを介したマルチキャストルーティングの設定手順について説明します。

非 IP マルチキャストエリアを接続する GRE トンネルの設定

マルチキャストルーティングをサポートしていないメディアで接続されている送信元と宛先の間の IP マルチキャストパケットを転送するように GRE トンネルを設定できます。

手順

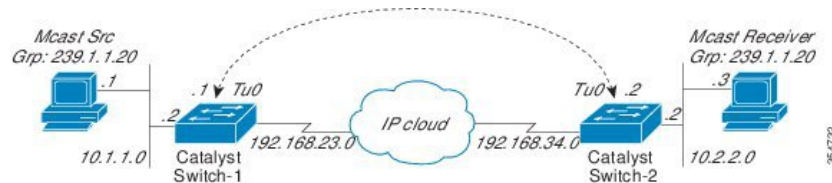
	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	ip multicast-routing 例： Device(config)# ip multicast-routing	IP マルチキャストルーティングをイネーブルにします。
ステップ 4	interface tunnel number 例： Device(config)# interface tunnel 0	トンネル 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 5	ip address ip_address subnet_mask 例： Device(config-if)# ip address 192.168.24.1 255.255.255.252	IP アドレスおよび IP サブネットを設定します。
ステップ 6	ip pim sparse-mode 例： Device(config-if)# ip pim sparse-mode	次の動作モードのいずれかでトンネル インターフェイス上で Protocol Independent Multicast (PIM) の動作のスパースモードをイネーブルにします。
ステップ 7	tunnel source { ip-address interface-name } 例： Device(config-if)# tunnel source 100.1.1.1	トンネル送信元を設定します。
ステップ 8	tunnel destination { hostname ip-address } 例：	トンネル宛先を設定します。

	コマンドまたはアクション	目的
	Device(config-if)# tunnel destination 100.1.5.3	
ステップ 9	end 例： Device(config-if)# end	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 10	show interface type number 例： Device# show interface tunnel 0	トンネルインターフェイスの情報を表示します。

非 IP マルチキャスト エリアを接続するトンネリングの例

次の例に、GRE トンネルを介した Catalyst スイッチ間のマルチキャストルーティングを示します。

図 7: 非 IP マルチキャスト エリアを接続するトンネル



上の図では、マルチキャスト送信元 (10.1.1.1) は、Catalyst スイッチ 1 に接続され、マルチキャストグループ 239.1.1.20 に設定されています。マルチキャスト受信者 (10.2.2.3) は、Catalyst スイッチ 2 に接続され、グループ 239.1.1.20 のマルチキャストパケットを受信するように設定されています。スイッチ 1 とスイッチ 2 は、マルチキャストルーティング用に設定されていない IP クラウドで分離されています。

GRE トンネルは、ループバック インターフェイスで送信元が特定されたスイッチ 1 とスイッチ 2 の間に設定されています。マルチキャストルーティングは、スイッチ 1 とスイッチ 2 で有効になっています。スパースモードで PIM をサポートするために、**ip pim sparse-mode** コマンドがトンネルインターフェイスに設定されています。トンネルインターフェイスのスパースモード設定により、スパースモードパケットをグループのランデブーポイント (RP) 設定に応じてトンネルを経由して転送できます。

スイッチ 1 の設定：

```
Device(config)# ip multicast-routing
Device(config)# interface Loopback0 //Tunnel source interface
Device(config-if)# ip address 2.2.2.2 255.255.255.255

Device(config)# interface Tunnel 10 //Tunnel interface configured for PIM
```

```

traffic
Device(config-if)# ip address 192.168.24.1 255.255.255.252
Device(config-if)# ip pim sparse-mode
Device(config-if)# ip nhrp map 192.168.24.3 4.4.4.4 //NHRP may optionally be
configured to dynamically discover tunnel end points.
Device(config-if)# ip nhrp map multicast 4.4.4.4
Device(config-if)# ip nhrp network-id 1
Device(config-if)# ip nhrp nhs 192.168.24.3
Device(config-if)# tunnel source Loopback0
Device(config-if)# tunnel destination 4.4.4.4

Device(config)# interface GigabitEthernet 0/0/0 //Source interface
Device(config-if)# ip address 10.1.1.2 255.255.255.0
Device(config-if)# ip pim sparse-mode

```

スイッチ 2 の設定 :

```

Device(config)# ip multicast-routing
Device(config)# interface Loopback0 //Tunnel source interface
Device(config-if)# ip address 4.4.4.4 255.255.255.255

Device(config)# interface Tunnel 10 //Tunnel interface configured for PIM
traffic
Device(config-if)# ip address 192.168.24.2 255.255.255.252
Device(config-if)# ip nhrp map 192.168.24.4 2.2.2.2 //NHRP may optionally be
configured to dynamically discover tunnel end points.
Device(config-if)# ip nhrp map multicast 2.2.2.2
Device(config-if)# ip nhrp network-id 1
Device(config-if)# ip nhrp nhs 192.168.24.4
Device(config-if)# ip pim sparse-mode
Device(config-if)# tunnel source Loopback0
Device(config-if)# tunnel destination 2.2.2.2

Device(config)# interface GigabitEthernet 0/0/0 //Receiver interface
Device(config-if)# ip address 10.2.2.2 255.255.255.0
Device(config-if)# ip pim sparse-mode

```

GRE トンネルを介するマルチキャストルーティングに関するその他の参考資料

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9200 Series Switches)</i> の「IP マルチキャストルーティング コマンド」の項を参照してください。

GRE トンネルを介するマルチキャストルーティングの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	GRE トンネルを介するマルチキャストルーティング	GRE トンネルを介するマルチキャストルーティングを使用すると、IP マルチキャストをサポートしないエリアを経由して、IP マルチキャストトラフィックを送信元からマルチキャストグループに送信できます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。



第 4 章

IGMP の設定

- [IGMP および IGMP スヌーピングの前提条件 \(47 ページ\)](#)
- [IGMP および IGMP スヌーピングの制約事項 \(48 ページ\)](#)
- [IGMP に関する情報 \(49 ページ\)](#)
- [IGMP の設定方法 \(64 ページ\)](#)
- [IGMP スヌーピングを設定する方法 \(83 ページ\)](#)
- [IGMP のモニタリング \(102 ページ\)](#)
- [IGMP の設定例 \(105 ページ\)](#)
- [IGMP に関するその他の関連資料 \(110 ページ\)](#)
- [IGMP の機能の履歴 \(110 ページ\)](#)

IGMP および IGMP スヌーピングの前提条件

IGMP スヌーピングの前提条件

IGMP スヌーピング クエリアを設定するときには、次の注意事項を順守します。

- VLAN をグローバル コンフィギュレーション モードに設定してください。
- IP アドレスおよび VLAN インターフェイスを設定してください。IGMP スヌーピング クエリアは、イネーブルの場合この IP アドレスをクエリーの送信元アドレスとして使用します。
- VLAN インターフェイス上で IP アドレスが設定されていない場合、IGMP スヌーピング クエリアは IGMP クエリア用に設定されたグローバル IP アドレスを使用しようとします。グローバル IP アドレスが指定されていない場合、IGMP クエリアは VLAN デバイスの仮想インターフェイス (SVI) IP アドレス (存在する場合) を使用しようとします。SVI IP アドレスが存在しない場合、デバイスはデバイス上で設定された利用可能な最初の IP アドレスを使用します。利用可能な最初の IP アドレスは、**show ip interface** 特権 EXEC コマンドの出力に表示されます。IGMP スヌーピングクエリアはデバイス上で利用可能な IP アドレスを検出できない場合、IGMP 一般クエリを生成しません。
- IGMP スヌーピング クエリアは IGMP バージョン 1 および 2 をサポートします。

- 管理上イネーブルである場合、IGMP スヌーピングクエリアはネットワークにマルチキャストルータの存在を検出すると、非クエリア ステートになります。
- 管理上イネーブルである場合、IGMP スヌーピング クエリアは操作上、次の状況でディセーブル ステートになります。
 - IGMP スヌーピングが VLAN でディセーブルの場合
 - PIM が、VLAN に対応する SVI でイネーブルの場合

IGMP および IGMP スヌーピングの制約事項

IGMP 設定の制約事項

次に、IGMP を設定する際の制約事項を示します。

- デバイスは IGMP バージョン 1、2、3 をサポートしています。



(注) IGMP バージョン 3 の場合、IGMP バージョン 3 BISS (基本的な IGMPv3 スヌーピング サポート) のみがサポートされます。

- IGMP バージョン 3 では新しいメンバーシップ レポート メッセージを使用しますが、これらは以前の IGMP スヌーピングデバイスで正しく認識されない可能性があります。
- IGMPv3 は、ISM および SSM と同時に動作可能です。ISM では、`exclude` と `include` の両方のモードのレポートを適用できます。SSM では、ラストホップルータは `include` モードのレポートだけを受け入れます。`exclude` モードのレポートは無視されます。
- ACLにより、指定のポートをマルチキャストルータポートではなく、マルチキャストホストポートとしてだけ指定できます。このポートで受信されたマルチキャストルータ制御パケットは、ドロップされます。

IGMP スヌーピングの制約事項

次に、IGMP スヌーピングの制約事項を示します。

- このデバイスは、宛先マルチキャスト IP アドレスのみに基づいて IGMPv3 スヌーピングをサポートします。送信元 IP アドレスやプロキシ レポートに基づいてスヌーピングをサポートすることはありません。
- IGMP フィルタリングまたはマルチキャスト VLAN レジストレーション (MVR) が実行されているデバイスは、IGMPv3 Join および Leave メッセージをサポートしません。

- IGMP レポート抑制は、マルチキャストクエリに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリに IGMPv3 レポートが含まれている場合はサポートされません。
- IGMP の脱退時間の設定は、IGMP バージョン 2 が稼働しているホストでのみサポートされます。IGMP バージョン 2 は、デバイスのデフォルトバージョンです。

ネットワークで実際の脱退にかかる待ち時間は、通常、設定した脱退時間どおりになります。ただし、脱退時間は、リアルタイムの CPU の負荷の状態、およびネットワークの遅延状態、インターフェイスから送信されたトラフィック量によって、設定された時間を前後することがあります。

- IGMP スロットリングアクションの制約事項は、レイヤ 2 ポートにだけ適用されます。 **ip igmp max-groups action replace** インターフェイス コンフィギュレーション コマンドは論理 EtherChannel インターフェイスで使用できますが、EtherChannel ポート グループに属するポートでは使用できません。

グループの最大数に関する制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups action {deny | replace}** コマンドを入力しても効果はありません。

インターフェイスによりマルチキャスト エントリが転送テーブルに追加されてから、スロットリングアクションを設定し、グループの最大数の制限を設定すると、転送テーブルのエントリは、スロットリングアクションに応じて期限切れになるか削除されます。

IGMP に関する情報

Internet Group Management Protocol の役割

IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。インターフェイスで PIM をイネーブルにすると、IGMP もイネーブルになります。IGMP は、特別なマルチキャストクエリアおよびホストを使用して、ネットワーク全体でマルチキャストトラフィックのフローを自動的に制御および制限する手段を提供します。

- クエリアは、クエリーメッセージを送信して、特定のマルチキャストグループのメンバーであるネットワーク デバイスを検出するネットワーク デバイス（ルータなど）です。
- ホストは、クエリアにホスト メンバーシップを通知するためのレポートメッセージ（クエリーメッセージに返信するメッセージ）を送信するレシーバで、ルータも含まれます。ホストでは、IGMP メッセージを使用して、マルチキャストグループに加入し、マルチキャストグループを脱退します。

ホストは、そのローカルマルチキャストデバイスに IGMP メッセージを送信することで、グループメンバーシップを識別します。IGMP では、デバイスは IGMP メッセージを受信し、定期的にクエリーを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

IGMP マルチキャストアドレス

IP マルチキャストトラフィックには、グループアドレス（クラス D IP アドレス）が使用されます。クラス D アドレスの上位 4 ビットは 1110 です。したがって、ホストグループアドレスの範囲は 224.0.0.0 ~ 239.255.255.255 であると考えられます。

224.0.0.0 ~ 224.0.0.255 のマルチキャストアドレスは、ルーティングプロトコルおよびその他のネットワーク制御トラフィックが使用するために予約されています。アドレス 224.0.0.0 は、どのグループにも割り当てられません。

IGMP パケットは IP マルチキャストグループアドレスを使用して次のように送信されます。

- IGMP 汎用クエリーは、アドレス 224.0.0.1（サブネット上のすべてのシステム）を宛先とします。
- IGMP グループ固有のクエリーは、クエリー対象デバイスのグループ IP アドレスを宛先とします。
- IGMP グループメンバーシップレポートは、レポート対象デバイスのグループ IP アドレスを宛先とします。
- IGMPv2 グループ脱退メッセージは、アドレス 224.0.0.2（サブネット上のすべてのデバイス）を宛先とします。
- IGMPv3 メンバーシップレポートはアドレス 224.0.0.22 を宛先とします。すべての IGMPv3 対応マルチキャストデバイスはこのアドレスをリッスンする必要があります。

IGMP のバージョン

デバイスは、IGMP バージョン 1、IGMP バージョン 2、および IGMP バージョン 3 をサポートしています。これらのバージョンは、デバイス上でそれぞれ相互運用できます。たとえば、IGMP スヌーピングがイネーブルになっていて、クエリアのバージョンが IGMPv2 で、デバイスがホストから IGMPv3 レポートを受信している場合、デバイスは IGMPv3 レポートをマルチキャストルータに転送できます。

IGMPv3 デバイスは、Source Specific Multicast (SSM; 送信元特定マルチキャスト) 機能を実行しているデバイスとの間で、メッセージを送受信できます。

IGMP バージョン 1

IGMP バージョン 1 (IGMPv1) にはクエリ応答モデルが使用されているため、マルチキャストルータおよびマルチレイヤデバイスは、ローカルサブネット上のどのマルチキャストグループがアクティブであるか（マルチキャストグループに関するホストが 1 台または複数存在するか）を判別できます。IGMPv1 では別のプロセスを使用して、ホストをマルチキャストグループに加入および脱退させることができます。詳細については、RFC 1112 を参照してください。

IGMPv2

IGMP バージョン 2 は IGMP 機能の拡張版です。IGMP 脱退処理などの機能を提供して、脱退遅延を短縮し、グループ固有のクエリー数を削減し、明示的な最大クエリー応答時間を短縮します。また、この作業を実行するために、マルチキャストプロトコルに依存することなく IGMP クエリアを選択する機能もルータに追加されます。詳細については、RFC 2236 を参照してください。



(注) IGMP バージョン 2 は、デバイスのデフォルトバージョンです。

IGMP バージョン 3

デバイスは IGMP バージョン 3 をサポートしています。

IGMPv3 デバイスは、Basic IGMPv3 Snooping Support (BISS) をサポートしています。BISS は、IGMPv1 および IGMPv2 スイッチでのスヌーピング機能と、IGMPv3 メンバーシップ レポートメッセージをサポートしています。ネットワークに IGMPv3 ホストがある場合、BISS によりマルチキャストトラフィックのフラッドは抑制されます。トラフィックは、IGMPv2 または IGMPv1 ホストの IGMP スヌーピング機能の場合とほぼ同じポートセットに抑制されません。

IGMPv3 デバイスは、Source Specific Multicast (SSM; 送信元特定マルチキャスト) 機能を実行しているデバイスとの間で、メッセージを送受信できます。

IGMPv3 ホスト シグナリング

IGMPv3 は、ホストがマルチキャスト グループのラスト ホップ デバイスにメンバーシップを伝える IETF 標準トラック プロトコルの第 3 バージョンです。IGMPv3 は、グループ メンバーシップを伝える能力をホストに与えます。これによってソースに関するフィルタリングが可能になります。ホストは、特定のソースを除いて、グループに送信するすべてのソースからトラフィックを受信したい (EXCLUDE と呼ばれるモード)、またはグループに送信する特定のソースからのみトラフィックを受信したい (INCLUDE と呼ばれるモード) と伝えることができます。

IGMPv3 は、ISM および SSM と同時に動作可能です。ISM では、EXCLUDE モードと INCLUDE モードの両方のレポートがラスト ホップ ルータによって受け入れられます。SSM では、INCLUDE モード レポートのみがラスト ホップ ルータによって受け入れられます。

IGMP のバージョンの違い

Internet Engineering Task Force (IETF) の Request for Comments (RFC) ドキュメントで定義されているように、IGMP には 3 種類のバージョンがあります。IGMPv2 は IGMPv1 の強化版で、ホストがマルチキャスト グループからの脱退を通知する機能が追加されています。IGMPv3 は IGMPv2 の強化版で、あるソース IP アドレスのセットから送信されたマルチキャストだけをリッスンする機能が追加されています。

表 5: IGMP のバージョン

IGMP のバージョン	説明
IGMPv1	どのマルチキャストグループがアクティブであるかをマルチキャストデバイスが判断できる基本的なクエリ応答メカニズムと、ホストがマルチキャストグループに加入および脱退できるようにするためのその他のプロセスを提供します。 RFC 1112 で、IP マルチキャスト用の IGMPv1 ホスト拡張が定義されています。
IGMPv2	IGMP の拡張で、IGMP の脱退処理、グループ固有のクエリおよび明示的な最大応答時間フィールドなどの機能が可能になっています。また、IGMPv2 ではこの作業を実行するために、マルチキャストプロトコルに依存することなく IGMP クエリアを選択する機能もデバイスに追加されます。IGMPv2 は RFC 2236 で定義されています。
IGMPv3	ソースフィルタリングを提供します。これにより、マルチキャストレシーバホストは、どのグループからマルチキャストトラフィックを受信するか、およびこのトラフィックがどのソースからのものと想定されているかをデバイスに知らせることができます。さらに、IGMPv3 は IGMPv3 メンバシップレポートの宛先 IP アドレスであるリンクローカルアドレス 224.0.0.22 をサポートしています。すべての IGMPv3 対応マルチキャストデバイスは、このアドレスをリッスンする必要があります。IGMPv3 は RFC 3376 で定義されています。



- (注) デフォルトでは、インターフェイスで PIM をイネーブルにすると、そのデバイスで IGMPv2 がイネーブルになります。IGMPv2 は、可能な限り IGMPv1 と下位互換性を保つよう設計されました。この下位互換性を実現するために、RFC 2236 は特別な相互運用性ルールを定義しています。ネットワークにレガシー IGMPv1 ホストが含まれている場合は、これらの運用性ルールをよく知っておく必要があります。IGMPv1 と IGMPv2 の相互運用性の詳細については、RFC 2236 『Internet Group Management Protocol, Version 2』を参照してください。

IGMPv1 を実行するデバイス

IGMPv1 デバイスは、「全ホスト」へのマルチキャストアドレスである 224.0.0.1 に IGMP クエリを送信して、アクティブマルチキャストレシーバが存在するマルチキャストグループを求めます。マルチキャストレシーバも、デバイスに IGMP レポートを送信して、特定のマルチキャストストリームの受信を待機していることを通知できます。ホストは非同期に、またはデバイスによって送信される IGMP クエリに対応して、レポートを送信できます。同じマルチキャストグループに複数のマルチキャストレシーバが存在する場合、これらのホストの 1 つ

のみで、IGMP レポートメッセージが送信されます。他のホストでは、レポートメッセージが抑制されます。

IGMPv1 では、IGMP クエリア選択はありません。セグメント内に複数のデバイスがある場合、すべてのデバイスが定期的に IGMP クエリーを送信します。IGMPv1 には、ホストがグループから脱退できる特別なメカニズムはありません。ホストで、特定のグループに対するマルチキャスト パケットを受信する必要がなくなった場合は、デバイスから送信される IGMP クエリー パケットに対する応答を行わないだけです。デバイスはクエリー パケットを送信し続けます。デバイスが 3 回 IGMP クエリーの応答を受信しないと、グループはタイムアウトし、デバイスはグループのセグメントへのマルチキャストパケットの送信を停止します。ホストがタイムアウト期間後にマルチキャストパケットを受信する場合、そのホストは新しい IGMP join をデバイスに送信するだけです。これにより、デバイスはマルチキャストパケットの転送を再開します。

LAN 上に複数のデバイスが存在する場合は、指定ルータ (DR) を選択して、接続されているホストに対するマルチキャスト トラフィックの重複を回避する必要があります。PIM デバイスは DR を選択する選定プロセスに従います。最も大きい IP アドレスを持つ PIM デバイスが DR になります。

DR は、次のタスクを担当します。

- PIM 登録メッセージ、PIM 加入メッセージ、および PIM プルーニング メッセージをランデブーポイント (RP) に送信し、ホストグループメンバーシップに関する情報を通知する。
- IGMP ホストクエリーメッセージを送信する。
- IGMP オーバーヘッドをホストおよびネットワークでできるだけ低く維持するために、ホストクエリーメッセージをデフォルトで 60 秒ごとに送信する。

IGMPv2 を実行するデバイス

IGMPv2 では、IGMPv1 のクエリーメッセージング機能が改善されました。

IGMPv2 のクエリーおよびメンバーシップレポートメッセージは、次の 2 つの例外を除き、IGMPv1 メッセージと同じです。

- IGMPv2 クエリーメッセージは、一般クエリー (IGMPv1 クエリーと同じ) とグループ固有クエリーの 2 つのカテゴリに分かれる。
- IGMPv1 メンバーシップレポートと IGMPv2 メンバーシップレポートの IGMP タイプコードが異なる。

IGMPv2 では、次の機能に対するサポートを追加することにより、IGMP の機能の強化も行われました。

- クエリア選択プロセス : IGMPv2 デバイスが、プロセスを実行するマルチキャストルーティングプロトコルに依存せずに、IGMP クエリアを選択できる機能を提供します。

- [Maximum Response Time] フィールド：IGMP クエリアを使用して最大クエリ応答時間を指定できる、クエリメッセージの新しいフィールド。このフィールドで、応答のバースト性を制御し、脱退遅延を調整するクエリ応答プロセスの調整ができます。
- グループ固有クエリメッセージ：すべてのグループではなく特定の1つのグループでクエリ操作を実行する目的で、IGMP クエリアを使用することができます。
- グループ脱退メッセージ：グループから脱退することをネットワーク上のデバイスに通知する手段をホストに提供します。

DR と IGMP クエリアが通常同じデバイスである IGMPv1 とは異なり、IGMPv2 では2つの機能は分離されます。DR と IGMP クエリアは異なる基準で選択され、同じサブネット上の異なるデバイスである場合があります。DR はサブネットで IP アドレスが最大のデバイスで、IGMP クエリアは最小の IP アドレスを持つデバイスです。

次のように、クエリメッセージは IGMP クエリアの選択に使用されます。

1. 各 IGMPv2 デバイスは起動時に、そのインターフェイスアドレスを一般クエリメッセージのソース IP アドレス フィールドに使用して、当該メッセージを全システムのグループアドレス 224.0.0.1 にマルチキャスト送信します。
2. IGMPv2 デバイスが一般クエリメッセージを受信すると、デバイスは自分のインターフェイスアドレスとメッセージのソース IP アドレスを比較します。サブネット上の最下位 IP アドレスが使用されているデバイスにより、IGMP クエリアが選択されます。
3. すべてのデバイス（クエリアは除く）でクエリタイマーが開始されます。IGMP クエリアから一般クエリメッセージを受信するたびに、タイマーはリセットされます。クエリタイマーが切れると、IGMP クエリアがダウンしたと見なされ、新しい IGMP クエリアを選択するために選択プロセスが再度実行されます。

デフォルトでは、タイマーはクエリインターバルの2倍です。

IGMPv3 を実行するデバイス

IGMPv3 では、ソースフィルタリングのサポートが追加されています。これにより、マルチキャストレシーバホストは、どのグループからマルチキャストトラフィックを受信するか、およびこのトラフィックがどのソースからのものと想定されているかをデバイスに知らせることができます。このメンバーシップ情報によって、レシーバがトラフィックを要求したソースからのトラフィックだけを転送できます。

IGMPv3 では、トラフィックを受信するソースに明示的に信号を送信するアプリケーションがサポートされます。IGMPv3 では、次の2つのモードで、レシーバにより、マルチキャストグループにメンバーシップの信号が送信されます。

- INCLUDE モード：このモードでは、レシーバはグループにメンバーシップをアナウンスし、トラフィックを受信する IP アドレスのリスト (INCLUDE リスト) を提供します。
- EXCLUDE モード：このモードでは、レシーバはグループにメンバーシップをアナウンスし、トラフィックを受信しない IP アドレスのリスト (EXCLUDE リスト) を提供します。つまり、ホストは IP アドレスが EXCLUDE リストに記載されていないソースからのトラ

フィックだけを受信します。インターネット標準マルチキャスト (ISM) サービスモデルの場合など、すべてのソースからトラフィックを受信するには、空の EXCLUDE リストを使用して EXCLUDE モードのメンバーシップを通知します。

IGMPv3 は SSM ネットワーク環境でホストがチャンネル加入者に信号を送信する業界指定の標準プロトコルです。IGMPv3 に依存する SSM では、ラスト ホップ デバイスおよびホストで実行されているオペレーティング システムのネットワーク スタック部分で IGMPv3 が使用でき、そのホスト上で動作しているアプリケーションで使用されている必要があります。

IGMPv3 では、ホストは 224.0.0.22 にメンバーシップ レポートを送信します。そのため、すべての IGMPv3 デバイスでこのアドレスをリッスンする必要があります。ただし、ホストは 224.0.0.22 をリッスンせず、応答しません。ホストはこのアドレスにレポートを送信するだけです。さらに、IGMPv3 では IGMPv3 ホストが他のホストによって送信されたレポートをリッスンしないため、メンバーシップ レポートの抑制はありません。したがって、一般クエリーが送信されると、ネットワークのすべてのホストが応答します。

IGMP の加入および脱退処理

IGMP の加入処理

ホストがマルチキャストグループに加入するとき、ホストは、加入するマルチキャストグループに 1 つ以上の送信要求されていないメンバーシップ レポートを送信します。IGMP 加入処理は、IGMPv1 ホストと IGMPv2 ホストで同じです。

IGMPv3 では、ホストの加入処理は次のように処理されます。

- ホストがグループに加入する場合は、空の EXCLUDE リストを使用して、224.0.0.22 に IGMPv3 メンバーシップ レポートを送信します。
- ホストが特定のチャンネルに加入する場合は、特定のソースアドレスを含む INCLUDE リストを使用して、224.0.0.22 に IGMPv3 メンバーシップ レポートを送信します。
- ホストが特定のソースを除くグループに加入する場合は、これらのソースを EXCLUDE リストで除外して、224.0.0.22 に IGMPv3 メンバーシップ レポートを送信します。



(注) LAN 上にある一部の IGMPv3 ホストでソースが除外され、その他のホストで同じソースが含まれている場合、デバイスは LAN 上でそのソースのトラフィックを送信します (つまり、この場合、包含が除外より優先されます)。

IGMP の脱退処理

ホストがグループから脱退するために使用する方法は、動作中の IGMP のバージョンによって異なります。

IGMPv1 の脱退処理

IGMPv1 には、ホストがあるグループからのマルチキャストトラフィックを受信しないことをそのサブネットのデバイスに通知するグループ脱退メッセージはありません。ホストでは、マルチキャストグループに対するトラフィックの処理が停止するだけで、そのグループに対する IGMP メンバーシップ レポートを使用した IGMP クエリーへの応答が終了します。その結果、IGMPv1 デバイスがサブネットの特定のマルチキャストグループにアクティブなレシーバがなくなったことを認識する唯一の方法は、デバイスがメンバーシップ レポートを受信しなくなったときになります。このプロセスを容易にするために、IGMPv1 デバイスは、サブネットの IGMP グループとカウントダウンタイマーを関連付けます。サブネットのグループがメンバーシップ レポートを受信すると、タイマーがリセットされます。IGMPv1 デバイスでは、このタイムアウト間隔は通常クエリー間隔の 3 倍 (3 分) です。このタイムアウト間隔は、すべてのホストがマルチキャストグループから脱退した後最大 3 分間、デバイスがサブネットにマルチキャストトラフィックを転送し続ける可能性があることを意味します。

IGMPv2 の脱退処理

IGMPv2 には、特定のグループのマルチキャストトラフィックの受信を停止することをホストが提示する手段を提供するグループ脱退メッセージが組み込まれています。IGMPv2 ホストがマルチキャストグループから脱退するとき、そのホストがそのグループのメンバーシップ レポートでクエリーに回答する最後のホストである場合、デバイス全体のマルチキャストグループ (224.0.0.2) にグループ脱退メッセージを送信します。

IGMPv3 の脱退処理

IGMPv3 は、IGMPv3 メンバーシップ レポートにソース、グループ、またはチャンネルを含めるか除外することによって、ホストが特定のグループ、ソース、またはチャンネルからのトラフィックの受信を停止できる機能を導入することで、脱退処理を拡張しています。

IGMP スヌーピング

レイヤ 2 は IGMP スヌーピングを使用して、レイヤ 2 インターフェイスを動的に設定し、マルチキャストトラフィックが IP マルチキャストデバイスと対応付けられたインターフェイスにのみ転送されるようにすることによって、マルチキャストトラフィックのフラッドを制限できます。名称が示すとおり、IGMP スヌーピングの場合は、LAN デバイスでホストとルータ間の IGMP 伝送をスヌーピングし、マルチキャストグループとメンバーシップ レポートを追跡する必要があります。デバイスがホストから特定のマルチキャストグループについての IGMP レポートを受信した場合、デバイスはホストのポート番号を転送テーブルエントリに追加します。ホストから IGMP Leave Group メッセージを受信した場合は、テーブルエントリからホストポートを削除します。マルチキャストクライアントから IGMP メンバーシップ レポートを受信しなかった場合にも、スイッチはエントリを定期的に削除します。



(注) IP マルチキャストおよび IGMP の詳細については、RFC 1112 および RFC 2236 を参照してください。

アクティブデバイスに設定されたマルチキャストルータは、すべての VLAN に対して定期的
に一般クエリを送信します。このマルチキャストトラフィックに関心のあるホストはすべて
Join 要求を送信し、転送テーブルのエントリに追加されます。デバイスは、IGMP Join 要求の
送信元となる各グループの IGMP スヌーピング IP マルチキャスト転送テーブルで、VLAN ご
とに 1 つずつエントリを作成します。

デバイスは、MAC アドレスに基づくグループではなく、IP マルチキャストグループに基づく
ブリッジングをサポートしています。マルチキャスト MAC アドレスに基づくグループの場
合、設定されている IP アドレスを設定済みの MAC アドレス（エイリアス）または予約済みの
マルチキャスト MAC アドレス（224.0.0.xxx の範囲内）に変換すると、コマンドがエラーにな
ります。デバイスでは IP マルチキャストグループを使用するので、アドレスエイリアスの問
題は発生しません。

IGMP スヌーピングによって、IP マルチキャストグループは動的に学習されます。ただし、**ip
igmp snooping vlan *vlan-id* static *ip_address* interface *interface-id*** グローバル コンフィギュレー
ション コマンドを使用すると、マルチキャストグループを静的に設定できます。グループ メ
ンバーシップをマルチキャストグループアドレスに静的に指定すると、その設定値は IGMP
スヌーピングによる自動操作より優先されます。マルチキャストグループメンバーシップの
リストは、ユーザが定義した設定値および IGMP スヌーピングによって学習された設定値の両
方で構成できます。

マルチキャストトラフィックはルーティングする必要がないのでマルチキャストインターフェ
イスを使用せずに、サブネットの IGMP スヌーピングをサポートするよう IGMP スヌーピング
クエリを設定できます。

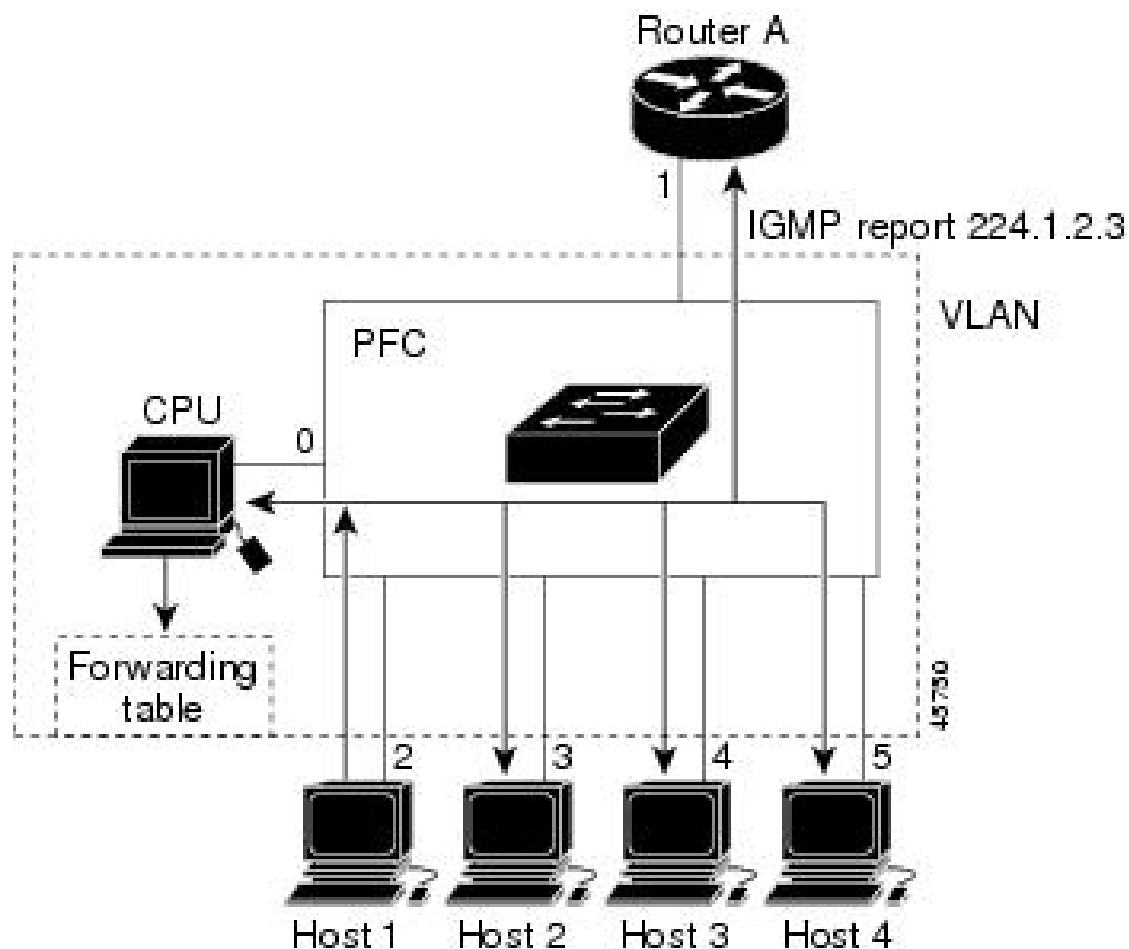
ポート スパニングツリー、ポートグループ、または VLAN ID が変更された場合、VLAN 上の
このポートから IGMP スヌーピングで学習されたマルチキャストグループは削除されます。

ここでは、IGMP スヌーピングの特性について説明します。

マルチキャストグループへの加入

図 8: 最初の IGMP Join メッセージ

デバイスに接続したホストが IP マルチキャストグループに加入し、なおかつそのホストが
IGMP バージョン 2 クライアントの場合、ホストは加入する IP マルチキャストグループを指定
した非送信請求 IGMP Join メッセージを送信します。別の方法として、ルータから一般クエリ
を受信したデバイスは、そのクエリを VLAN 内のすべてのポートに転送します。IGMP バ
ージョン 1 またはバージョン 2 のホストがマルチキャストグループに加入する場合、ホストはデ
バイスに Join メッセージを送信することによって応答します。デバイスの CPU は、そのグル
ープのマルチキャスト転送テーブルエントリがまだ存在していないのであれば、エントリを作成
します。CPU はさらに、Join メッセージを受信したインターフェイスを転送テーブル エント
リに追加します。そのインターフェイスと対応付けられたホストが、そのマルチキャストグ
ループ用のマルチキャストトラフィックを受信します。



ルータ A がデバイスに一般クエリを送信し、そこでそのクエリは同じ VLAN のすべてのメンバであるポート 2～5 に転送されます。ホスト 1 はマルチキャストグループ 224.1.2.3 に加入するために、グループに IGMP メンバーシップ レポート (IGMP Join メッセージ) をマルチキャストします。デバイスの CPU は IGMP レポートの情報を使用して、転送テーブルのエントリを設定します。転送テーブルにはホスト 1 およびルータに接続しているポート番号が含まれます。

表 6: IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1、2

デバイスのハードウェアは、IGMP 情報パケットをマルチキャストグループの他のパケットと区別できます。テーブルの情報は、224.1.2.3 マルチキャスト IP アドレス宛での、IGMP パケットではないフレームを、ルータおよびグループに加入したホストに対して送信するように、スイッチング エンジンに指示します。

図 9:2 番目のホストのマルチキャストグループへの加入

別のホスト（たとえば、ホスト 4）が、同じグループ用に非送信請求 IGMP Join メッセージを送信する場合、CPU がそのメッセージを受け取り、ホスト 4 のポート番号を転送テーブルに追加します。転送テーブルは CPU 宛てだけに IGMP メッセージを送るので、メッセージはデバイスの他のポートにフラッディングされません。認識されているマルチキャストトラフィックは、CPU 宛てではなくグループ宛てに転送されます。

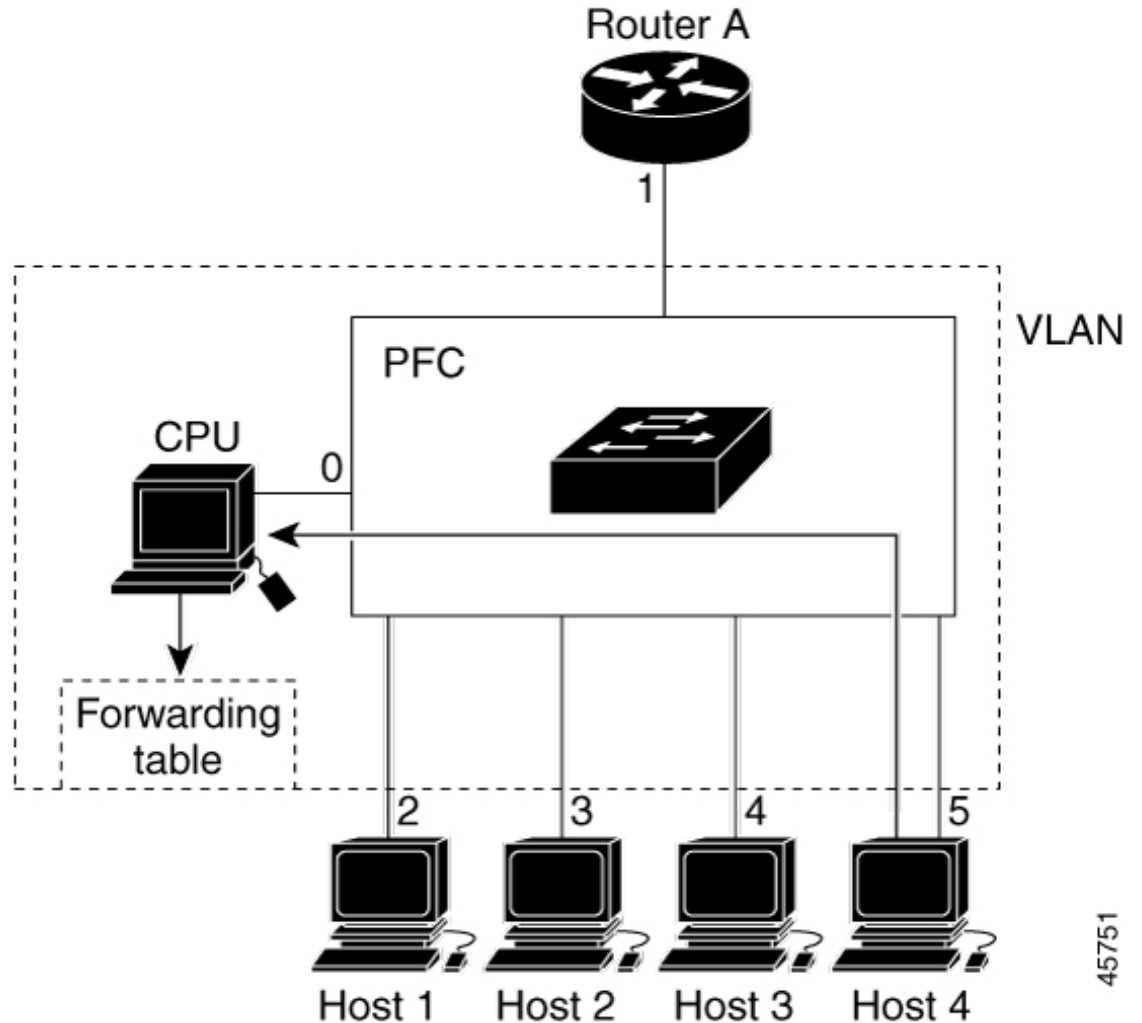


表 7: 更新された IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1, 2, 5

マルチキャストグループからの脱退

ルータはマルチキャスト一般クエリを定期的送信し、デバイスはそれらのクエリを VLAN のすべてのポートを通じて転送します。関心のあるホストがクエリに応答します。VLAN 内

の少なくとも1つのホストがマルチキャストトラフィックを受信するようなら、ルータは、その VLAN へのマルチキャストトラフィックの転送を続行します。デバイスは、その IGMP スヌーピングによって維持された IP マルチキャストグループの転送テーブルで指定されたホストに対してだけ、マルチキャストグループトラフィックを転送します。

ホストがマルチキャストグループから脱退する場合、何も通知せずに脱退することも、Leave メッセージを送信することもできます。ホストから Leave メッセージを受信したデバイスは、グループ固有のクエリを送信して、そのインターフェイスに接続された他のデバイスが所定のマルチキャストグループのトラフィックに関与しているかどうかを学習します。デバイスはさらに、転送テーブルでその MAC グループの情報を更新し、そのグループのマルチキャストトラフィックの受信に関心のあるホストだけが、転送テーブルに指定されるようにします。ルータが VLAN からレポートを受信しなかった場合、その VLAN 用のグループは IGMP キャッシュから削除されます。

即時脱退

デバイスは IGMP スヌーピングの即時脱退を使用して、先にデバイスからインターフェイスにグループ固有のクエリを送信しなくても、Leave メッセージを送信するインターフェイスを転送テーブルから削除できるようにします。VLAN インターフェイスは、最初の Leave メッセージで指定されたマルチキャストグループのマルチキャストツリーからプルニングされます。即時脱退によって、複数のマルチキャストグループが同時に使用されている場合でも、スイッチドネットワークのすべてのホストに最適な帯域幅管理が保証されます。

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。IGMP バージョン 2 は、デバイスのデフォルトバージョンです。



(注) 即時脱退機能を使用するのは、各ポートに接続されているホストが 1 つだけの VLAN に限定してください。ポートに複数のホストが接続されている VLAN 上で即時脱退をイネーブルにすると、一部のホストが誤ってドロップされる可能性があります。

IGMP 脱退タイマーの設定

まだ指定のマルチキャストグループに関心があるかどうかを確認するために、グループ固有のクエリを送信した後のデバイスの待機時間を設定できます。IGMP 脱退応答時間は、100 ~ 32767 ミリ秒の間で設定できます。

IGMP レポート抑制

IGMP レポート抑制は、マルチキャストクエリに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリに IGMPv3 レポートが含まれている場合はサポートされません。

デバイスは IGMP レポート抑制を使用して、マルチキャストルータクエリごとに 1 つの IGMP レポートのみをマルチキャストデバイスに転送します。IGMP レポート抑制がイネーブル（デフォルト）である場合、デバイスは最初の IGMP レポートをグループのすべてのホストからすべてのマルチキャストルータに送信します。デバイスは、グループの残りの IGMP レポートを

マルチキャストルータに送信しません。この機能により、マルチキャストデバイスにレポートが重複して送信されることを防ぎます。

マルチキャストルータクエリに IGMPv1 および IGMPv2 レポートに対する要求のみが含まれている場合、デバイスは最初の IGMPv1 レポートまたは IGMPv2 レポートのみを、グループのすべてのホストからすべてのマルチキャストルータに転送します。

マルチキャストルータクエリに IGMPv3 レポートに対する要求も含まれる場合、デバイスはグループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャストデバイスに転送します。

IGMP レポート抑制をディセーブルにすると、すべての IGMP レポートはマルチキャストルータに転送されます。

IGMP スヌーピングとデバイススタック

IGMP スヌーピング機能はデバイススタック間で機能します。つまり、1つのデバイスからの IGMP 制御情報は、スタックにあるすべてのデバイスに配信されます。スタックメンバが、どの IGMP マルチキャストデータ経由でスタックに入ったかに関係なく、データは、そのグループで登録されたホストに到達します。

スタック内のデバイスで障害が発生した場合、またはデバイスがスタックから削除された場合、そのデバイス上にあるマルチキャストグループのメンバのみが、マルチキャストデータを受信しません。スタック内にあるその他のデバイスでは、マルチキャストグループの他のすべてのメンバが、マルチキャストデータストリームを継続して受信します。ただし、アクティブなデバイスが削除された場合、レイヤ 2 およびレイヤ 3 (IP マルチキャストルーティング) の両方に共通のマルチキャストグループでは、コンバージェンスに時間がかかる場合があります。

IGMP フィルタリングおよびスロットリング

都市部や Multiple-Dwelling Unit (MDU) などの環境では、スイッチポート上のユーザが属する一連のマルチキャストグループを制御する必要があります。この機能を使用することにより、IP/TV などのマルチキャストサービスの配信を、特定タイプの契約またはサービス計画に基づいて制御できます。また、マルチキャストグループの数を、スイッチポート上でユーザが所属できる数に制限することもできます。

IGMP フィルタリング機能を使用すると、IP マルチキャストプロファイルを設定し、それらを各スイッチポートに関連付けて、ポート単位でマルチキャスト加入をフィルタリングできます。IGMP プロファイルにはマルチキャストグループを1つまたは複数格納して、グループへのアクセスを許可するか拒否するかを指定できます。マルチキャストグループへのアクセスを拒否する IGMP プロファイルがスイッチポートに適用されると、IP マルチキャストトラフィックのストリームを要求する IGMP Join レポートが廃棄され、ポートはそのグループからの IP マルチキャストトラフィックを受信できなくなります。マルチキャストグループへのアクセスがフィルタリングアクションで許可されている場合は、ポートからの IGMP レポートが転送されて、通常の処理が行われます。レイヤ 2 インターフェイスが加入できる IGMP グループの最大数も設定できます。

IGMP フィルタリングで制御されるのは、グループ固有のクエリーおよびメンバーシップ レポート (Join および Leave レポートを含む) だけです。一般 IGMP クエリーは制御されません。IGMP フィルタリングは、IP マルチキャストトラフィックの転送を指示する機能とは無関係です。フィルタリング機能は、マルチキャストトラフィックの転送に CGMP が使用されているか、または MVR が使用されているかに関係なく、同じように動作します。

IGMP フィルタリングが適用されるのは、IP マルチキャストグループアドレスを動的に学習する場合だけです。静的な設定には適用されません。

IGMP スロットリング機能を使用すると、レイヤ2 インターフェイスが加入できる IGMP グループの最大数を設定できます。IGMP グループの最大数が設定され、IGMP スヌーピング転送テーブルに最大数のエントリが登録されていて、インターフェイスで IGMP Join レポートを受信する場合、インターフェイスを設定することにより、IGMP レポートを廃棄するか、あるいは受信した IGMP レポートでランダムに選択されたマルチキャストエントリを上書きします。



(注) IGMP フィルタリングが実行されているデバイスは、IGMPv3 Join および Leave メッセージをサポートしていません。

IGMP のデフォルト設定

次の表に、デバイスの IGMP デフォルト設定を示します。

表 8: IGMP のデフォルト設定

機能	デフォルト設定
マルチキャストグループのメンバとしてのマルチレイヤデバイス	グループメンバーシップは未定義
マルチキャストグループへのアクセス	インターフェイスのすべてのグループを
IGMP のバージョン	すべてのインターフェイスでバージョン
IGMP ホストクエリーメッセージインターバル	すべてのインターフェイスで 60 秒
IGMP クエリータイムアウト	すべてのインターフェイスで 60 秒
IGMP 最大クエリー応答時間	すべてのインターフェイスで 10 秒
静的に接続されたメンバーとしてのマルチレイヤデバイス	ディセーブル

IGMP スヌーピングのデフォルト設定

次の表に、デバイスの IGMP スヌーピングのデフォルト設定を示します。

表 9: IGMP スヌーピングのデフォルト設定

機能	デフォルト設定
IGMP スヌーピング	グローバルおよび VLAN 単位でイネーブ
マルチキャスト ルータ	未設定
IGMP スヌーピング即時脱退	ディセーブル
スタティック グループ	未設定
TCN ¹ フラッドクエリ カウント	2
TCN クエリー送信要求	ディセーブル
IGMP スヌーピング クエリア	ディセーブル
IGMP レポート抑制	有効

¹ (1) TCN = トポロジ変更通知

IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定

次の表に、デバイスの IGMP フィルタリングおよびスロットリングのデフォルト設定を示します。

表 10: IGMP フィルタリングのデフォルト設定

機能	デフォルト設定
IGMP フィルタ	適用なし
IGMP グループの最大数	最大数の設定なし (注) 転送テーブルに登録されているグループが最大数に達した場合、デフォルトの IGMP スロットリングアクションは、そのグループの加入を拒否します。
IGMP プロファイル	未定義
IGMP プロファイル アクション	範囲で示されたアドレスを拒否

IGMP の設定方法

グループのメンバとしてデバイスを設定

デバイスをマルチキャストグループのメンバとして設定し、マルチキャストがネットワークに到達可能かどうかを検出できます。管理対象のすべてのマルチキャスト対応ルータおよびマルチレイヤデバイスがマルチキャストグループのメンバーである場合、グループに ping を送信すると、これらのすべてのデバイスが応答します。デバイスは、所属グループにアドレス指定された ICMP エコー要求パケットに応答します。もう 1 つの例は、ソフトウェア付属のマルチキャスト トレースルート ツールです。



注意 この手順を実行すると、グループアドレス用のデータトラフィックがすべて CPU に送られるため、CPU のパフォーマンスが低下する場合があります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface GigabitEthernet 1/0/1	マルチキャスト ルーティングをイネーブルにするレイヤ 3 インターフェイスを指定し、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。 次のいずれかのインターフェイスを指定する必要があります。 <ul style="list-style-type: none">ルーテッドポート：レイヤ 3 ポートとして no switchport インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • SVI : interface vlan <i>vlan-id</i> グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 <p>これらのインターフェイスには、IP アドレスを割り当てる必要があります。</p>
ステップ 4	ip igmp join-group <i>group-address</i> 例 : Device(config-if)# ip igmp join-group 225.2.2.2	<p>デバイスをマルチキャストグループに加入するように設定します。デフォルトで、グループのメンバーシップは定義されていません。</p> <p><i>group-address</i> には、マルチキャスト IP アドレスをドット付き 10 進表記で指定します。</p>
ステップ 5	end 例 : Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	show ip igmp interface [<i>interface-id</i>] 例 : Device# show ip igmp interface GigabitEthernet 1/0/1	入力を確認します。
ステップ 7	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IGMP バージョンの変更

スイッチでは、IGMP クエリー タイムアウトや最大クエリー応答時間などの機能を使用できる IGMP バージョン 2 がデフォルトで使用されます。

サブネット上のすべてのシステムで、同じバージョンをサポートする必要があります。スイッチは自動的にバージョン 1 のシステムを検出せず、バージョン 1 へのスイッチングも行いません。バージョン 2 のルータまたはスイッチは、常に IGMPv1 ホストと正しく連動しているため、バージョン 1 とバージョン 2 のホストはサブネット上で混在できます。

使用しているホストでバージョン 2 がサポートされていない場合は、スイッチをバージョン 1 に設定してください。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	ip igmp version {1 2 3} 例： Device(config-if)# ip igmp version 2	スイッチで使用する IGMP バージョンを指定します。 (注) バージョン 1 に変更すると、 ip igmp query-interval および ip igmp query-max-response-time インターフェイス コンフィギュレーション コマンドを設定できません。 デフォルトの設定に戻す場合は、 no ip igmp version インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	show ip igmp interface [interface-id] 例：	入力を確認します。

	コマンドまたはアクション	目的
	Device# <code>show ip igmp interface</code>	
ステップ 7	copy running-config startup-config 例 : Device# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

IGMP ホストクエリーメッセージインターバルの変更

デバイスは、IGMP ホストクエリーメッセージを定期的送信し、接続されたネットワーク上にあるマルチキャストグループを検出します。これらのメッセージは、TTL が 1 の全ホストマルチキャストグループ (224.0.0.1) に送信されます。デバイスはホストクエリーメッセージを送信し、ネットワーク上に存在するメンバーシップに関する情報をリフレッシュします。クエリーをいくつか実行したあとで、マルチキャストグループのメンバーであるローカルホストが存在しないことをソフトウェアが検出した場合、そのグループのリモート送信元からローカルネットワークへのマルチキャストパケット転送が停止され、プルーニングメッセージが送信元のアップストリーム方向へ送信されます。

デバイスは LAN (サブネット) 用の PIM DR を選択します。DR は、LAN 上のすべてのホストに IGMP ホストクエリーメッセージを送信します。SM の場合、DR は PIM 登録メッセージおよび PIM Join メッセージも RP ルータに向けて送信します。IGMPv2 では、DR は IP アドレスが最大である、ルータまたはマルチレイヤデバイスです。IGMPv1 では、DR は LAN 上で動作するマルチキャストルーティングプロトコルに従って選択されます。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> <code>enable</code>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# <code>configure terminal</code>	グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	interface <i>interface-id</i> 例 : <pre>Device(config)# interface gigabitethernet 1/0/1</pre>	<p>マルチキャスト ルーティングをイネーブルにするレイヤ3インターフェイスを指定し、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。</p> <p>次のいずれかのインターフェイスを指定する必要があります。</p> <ul style="list-style-type: none"> • ルーテッドポート：レイヤ3ポートとして no switchport インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 • SVI： interface vlan <i>vlan-id</i> グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 <p>これらのインターフェイスには、IP アドレスを割り当てる必要があります。</p>
ステップ 4	ip igmp query-interval <i>seconds</i> 例 : <pre>Device(config-if)# ip igmp query-interval 75</pre>	<p>DR が IGMP ホストクエリーメッセージを送信する頻度を設定します。</p> <p>デフォルトでは、DR は IGMP ホストクエリーメッセージを 60 秒ごとに送信し、ホストおよびネットワークでの IGMP オーバーヘッドを抑制します。</p> <p>指定できる範囲は 1 ~ 65535 です。</p>
ステップ 5	end 例 : <pre>Device(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 6	show ip igmp interface [<i>interface-id</i>] 例 : <pre>Device# show ip igmp interface</pre>	<p>Displays</p>
ステップ 7	copy running-config startup-config 例 : <pre>Device# copy running-config</pre>	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p>

	コマンドまたはアクション	目的
	<code>startup-config</code>	

IGMPv2 の最大クエリー応答時間の変更

IGMPv2 を使用している場合は、IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更できます。デバイスは最大クエリー応答時間を使用し、LAN 上に直接接続されたグループメンバが存在しないことを短時間で検出します。値を小さくすると、デバイスによるグループのプルーン速度が向上します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface GigabitEthernet 1/0/1	マルチキャストルーティングをイネーブルにするレイヤ3インターフェイスを指定し、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。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッドポート：レイヤ3ポートとして no switchport インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 • SVI： interface vlan vlan-id グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。

	コマンドまたはアクション	目的
ステップ 4	ip igmp query-max-response-time <i>seconds</i> 例： Device(config-if)# ip igmp query-max-response-time 15	IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更します。 デフォルトは 10 秒です。指定できる範囲は 1 ~ 25 です。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	show ip igmp interface [<i>interface-id</i>] 例： Device# show ip igmp interface	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

静的に接続されたメンバとしてデバイスを設定

ネットワーク セグメント上にグループ メンバが存在しなかったり、ホストで IGMP を使用してグループ メンバーシップを報告できないことがあります。しかし、そのネットワーク セグメントに対して、マルチキャストトラフィックの送信が必要な場合もあります。マルチキャストトラフィックをネットワーク セグメントに送り込むには、次のコマンドを使用します。

- **ip igmp join-group** : デバイスはマルチキャストパケットの転送だけでなく、マルチキャストパケットを受け入れます。マルチキャストパケットを受信する場合は、高速スイッチングを実行できません。
- **ip igmp static-group** : デバイスは、パケットを転送するだけで、パケット自体は受け入れません。この方法を使用すると、高速スイッチングが可能です。発信インターフェイスが IGMP キャッシュに格納されますが、マルチキャストルート エントリに「L」（ローカル）フラグが付かないことから明らかなように、デバイス自体はメンバではありません。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例 : Device(config)# interface GigabitEthernet 1/0/1	マルチキャストルーティングをイネーブルにするレイヤ3インターフェイスを指定し、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。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッドポート：レイヤ3ポートとして no switchport インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 • SVI： interface vlan vlan-id グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	ip igmp static-group group-address 例 : Device(config-if)# ip igmp static-group 239.100.100.101	デバイスを静的に接続されたグループのメンバとして設定します。デフォルトでは、この機能はディセーブルになっています。
ステップ 5	end 例 : Device(config-if)# end	特権 EXEC 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	show ip igmp interface <i>[interface-id]</i> 例 : Device# show ip igmp interface GigabitEthernet 1/0/1	入力を確認します。
ステップ 7	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IGMP プロファイルの設定

IGMP プロファイルを作成するには、次の手順を実行します。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip igmp profile <i>profile number</i> 例 : Device(config)# ip igmp profile 3	設定するプロファイルに番号を割り当て、IGMP プロファイル コンフィギュレーション モードを開始します。指定できるプロファイル番号の範囲は 1 ~ 4294967295 です。IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。 <ul style="list-style-type: none"> deny : 一致するアドレスを拒否します。デフォルトで設定されています。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • exit : IGMP プロファイル コンフィギュレーション モードを終了します。 • no : コマンドを否定するか、または設定をデフォルトに戻します。 • permit : 一致するアドレスを許可するように指定します。 • range : プロファイルの IP アドレスの範囲を指定します。単一の IP アドレス、または開始アドレスと終了アドレスで指定された IP アドレス範囲を入力できます。 <p>デバイスのデフォルトでは、IGMP プロファイルが設定されていません。</p> <p>(注) プロファイルを削除するには、no ip igmp profile profile number グローバル コンフィギュレーション コマンドを使用します。</p>
ステップ 4	permit deny 例 : Device(config-igmp-profile) # permit	(任意) IP マルチキャスト アドレスへのアクセスを許可または拒否するアクションを設定します。アクションを設定しないと、プロファイルのデフォルト設定はアクセス拒否になります。
ステップ 5	range ip multicast address 例 : Device(config-igmp-profile) # range 229.9.9.0	アクセスを制御する IP マルチキャスト アドレスまたは IP マルチキャスト アドレスの範囲を入力します。範囲を入力する場合は、IP マルチキャスト アドレスの下限値、スペースを 1 つ、IP マルチキャスト アドレスの上限値を入力します。
		<p>range コマンドを複数回入力し、複数のアドレスまたはアドレス範囲を入力できます。</p> <p>(注) IP マルチキャスト アドレスまたは IP マルチキャスト アドレス範囲を削除するには、no range ip multicast address IGMP</p>

	コマンドまたはアクション	目的
		プロファイル コンフィギュレーション コマンドを使用します。
ステップ 6	end 例 : Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 7	show ip igmp profile profile number 例 : Device# show ip igmp profile 3	プロファイルの設定を確認します。
ステップ 8	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 9	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IGMP プロファイルの適用

IGMP プロファイルで定義されているとおりにアクセスを制御するには、プロファイルを該当するインターフェイスに適用する必要があります。IGMP プロファイルを適用できるのは、レイヤ2アクセスポートだけです。ルーテッドポートやSVIには適用できません。EtherChannelポートグループに所属するポートに、プロファイルを適用することはできません。1つのプロファイルを複数のインターフェイスに適用できますが、1つのインターフェイスに適用できるプロファイルは1つだけです。

スイッチポートにIGMPプロファイルを適用するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 :	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> enable	<ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface GigabitEthernet 1/0/1	物理インターフェイスを指定し、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。インターフェイスは、EtherChannel ポート グループに所属していないレイヤ 2 ポートでなければなりません。
ステップ 4	ip igmp filter profile number 例： Device(config-if)# ip igmp filter 321	インターフェイスに指定された IGMP プロファイルを適用します。指定できる範囲は 1 ~ 4294967295 です。 (注) インターフェイスからプロファイルを削除するには、 no ip igmp filter profile number インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例： Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IGMP グループの最大数の設定

レイヤ2インターフェイスが加入できる IGMP グループの最大数を設定するには、次の手順を実行します。

始める前に

この制限が適用されるのはレイヤ2ポートだけです。ルーテッドポートや SVI には IGMP グループの最大数を設定できません。このコマンドは、論理 EtherChannel インターフェイスでも使用できますが、EtherChannel ポートグループに属するポートでは使用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet1/0/2	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポートグループに所属しないレイヤ2ポート、または EtherChannel インターフェイスのいずれかにできます。
ステップ 4	ip igmp max-groups number 例： Device(config-if)# ip igmp max-groups 20	インターフェイスが加入できる IGMP グループの最大数を設定します。指定できる範囲は 0 ~ 4294967294 です。デフォルトでは最大数は設定されません。
ステップ 5	end 例： Device(config)# end	特権 EXEC 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	show running-config interface <i>interface-id</i> 例 : Device# show running-config interface gigabitethernet1/0/1	入力を確認します。
ステップ 7	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IGMP スロットリング アクションの設定

レイヤ2インターフェイスが加入できる IGMP グループの最大数を設定した後、受信した IGMP レポートの新しいグループで、既存のグループを上書きするようにインターフェイスを設定できます。

転送テーブルに最大数のエントリが登録されているときにスロットリングアクションを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface <i>interface-id</i> 例 : Device(config)# interface gigabitethernet1/0/1	設定する物理インターフェイスを指定し、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。インターフェイスは、EtherChannel ポートグループに所属しないレイヤ2ポート、または EtherChannel インターフェイスのいずれかにできます。トランク ポートをインターフェイスにすることはできません。

	コマンドまたはアクション	目的
ステップ 4	<p>ip igmp max-groups action {deny replace}</p> <p>例 :</p> <pre>Device(config-if)# ip igmp max-groups action replace</pre>	<p>インターフェイスが IGMP レポートを受信したときに、転送テーブルに最大数のエントリが登録されている場合は、次のいずれかのアクションをインターフェイスに指定します。</p> <ul style="list-style-type: none"> • deny : レポートを破棄します。このスロットリングアクションを設定すると、すでに転送テーブルに登録されていたエントリは、削除されることはありませんが期限切れになります。エントリが期限切れになり、最大数のエントリが転送テーブルに登録されていると、デバイスは、インターフェイスで受信した次の IGMP レポートを廃棄します。 • replace : 既存のグループを、IGMP レポートを受信した新しいグループで上書きします。このスロットリングアクションを設定すると、すでに転送テーブルに登録されていたエントリは削除されます。転送テーブルのエントリが最大数まで達したら、デバイスはランダムに選択したエントリを受信した IGMP レポートで上書きします。 <p>デバイスが転送テーブルのエントリを削除しないようにするには、インターフェイスにより転送テーブルにエントリが追加される前に、IGMP スロットリングアクションを設定します。</p> <p>(注) レポートの廃棄というデフォルトのアクションに戻すには、no ip igmp max-groups action インターフェイス コンフィギュレーション コマンドを使用します。</p>
ステップ 5	<p>end</p> <p>例 :</p>	<p>特権 EXEC モードに戻ります。</p>

	コマンドまたはアクション	目的
	Device(config-if)# end	
ステップ 6	show running-config interface interface-id 例 : Device# show running-config interface gigabitethernet1/0/1	入力を確認します。
ステップ 7	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

直接接続の IGMP ホストがない場合にマルチキャストトラフィックが転送されるようにデバイスを設定する方法

直接接続された IGMP ホストがない場合に、マルチキャストトラフィックを転送するようにデバイスを設定するには、次のオプション作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface type number 例 : Device(config)# interface gigabitethernet 1/0/1	インターフェイスコンフィギュレーションモードを開始します。 <ul style="list-style-type: none"><i>type</i> 引数および <i>number</i> 引数に、ホストに接続されているインターフェイスを指定します。

	コマンドまたはアクション	目的
ステップ 4	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> • ip igmp join-group <i>group-address</i> • ip igmp static-group {* <i>group-address</i> [source <i>source-address</i>]} <p>例 :</p> <pre>Device(config-if)# ip igmp join-group 225.2.2.2</pre> <p>例 :</p> <pre>Device(config-if)# ip igmp static-group 225.2.2.2</pre>	<p>最初の例では、指定したグループに加入するデバイスのインターフェイスを設定する例を示します。</p> <p>この方法では、デバイスは、マルチキャストパケットの転送に加えて、マルチキャストパケットを受信します。マルチキャストパケットを受信する場合は、高速スイッチングを実行できません。</p> <p>2番目の例では、インターフェイスでスタティックグループメンバーシップエントリを設定する例を示します。この方法の場合、デバイスはパケットそのものを受信せず、転送だけを実行します。したがって、この方法では、高速スイッチングを実行できます。発信インターフェイスがIGMPキャッシュに格納されますが、マルチキャストルートエントリに「L」（ローカル）フラグが付かないことから明らかなように、デバイス自体はメンバではありません。</p>
ステップ 5	<p>end</p> <p>例 :</p> <pre>Device#(config-if)# end</pre>	特権 EXEC モードに戻ります。
ステップ 6	<p>show ip igmp interface [<i>interface-type</i> <i>interface-number</i>]</p> <p>例 :</p> <pre>Device# show ip igmp interface</pre>	(任意) インターフェイスに関するマルチキャスト関連情報を表示します。

IGMP 拡張アクセス リストを使用して SSM ネットワークへのアクセスを制御する方法

ソースアドレス、グループアドレス、またはその両方に基づいて SSM トラフィックをフィルタする IGMP 拡張アクセスリストを使用して SSM ネットワークへのアクセスを制御するには、次のオプション作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip multicast-routing [distributed] 例 : Device(config)# ip multicast-routing distributed	IP マルチキャストルーティングを有効にします。 • distributed キーワードは、IPv4 マルチキャストの場合に必要です。
ステップ 4	ip pim ssm {default range access-list} 例 : Device(config)# ip pim ssm default	SSM サービスを設定します。 • default キーワードは SSM 範囲のアクセスリストを 232/8 と定義します。 • range キーワードは標準の IP アクセスリスト番号または SSM 範囲を定義する名前を指定します。
ステップ 5	ip access-list extended access-list-name 例 : Device(config)# ip access-list extended mygroup	名前付き拡張 IP アクセスリストを指定します。
ステップ 6	deny igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments] 例 : Device(config-ext-nacl)# deny igmp host 10.1.2.3 any	(任意) IGMP レポートから指定したソースアドレスまたはグループアドレスをフィルタリングすることで、サブネットのホストをメンバーシップから (S, G) チャンネルに制限します。 • サブネットメンバーシップから他の (S, G) チャンネルにホストを制限するには、この手順を繰り返します。(特に許可されない送信元またはグループは拒否されるため、これらの送信元は後続の permit ス

	コマンドまたはアクション	目的
		<p>テートメントより限定的になります)。</p> <ul style="list-style-type: none"> • アクセスリストは、暗黙の deny ステートメントで終了することに注意してください。 • 次に、ソース 10.1.2.3 に対してすべてのグループをフィルタリングして、効果的にソースを拒否する deny ステートメントを作成する例を示します。
ステップ 7	<p>permit igmp <i>source source-wildcard destination destination-wildcard</i> [<i>igmp-type</i>] [precedence precedence] [tos tos] [log] [time-range time-range-name] [fragments]</p> <p>例 :</p> <pre>Device(config-ext-nacl)# permit igmp any any</pre>	<p>IGMP レポートのソース アドレスまたはグループ アドレスが IP アクセス リストを渡すことができます。</p> <ul style="list-style-type: none"> • アクセスリストには少なくとも 1 つの permit ステートメントが必要です。 • 他のソースが IP アクセス リストを渡せるようにする場合は、この手順を繰り返します。 • この例では、前の deny ステートメントによって拒否されていない送信元およびグループに対するメンバーシップを許可する方法を示します。
ステップ 8	<p>exit</p> <p>例 :</p> <pre>Device(config-ext-nacl)# exit</pre>	<p>現在のコンフィギュレーションセッションを終了し、グローバルコンフィギュレーションモードに戻ります。</p>
ステップ 9	<p>interface type number</p> <p>例 :</p> <pre>Device(config)# interface ethernet 0</pre>	<p>IGMPv3 をイネーブルにできるホストに接続されているインターフェイスを選択します。</p>
ステップ 10	<p>ip igmp access-group access-list</p> <p>例 :</p> <pre>Device(config-if)# ip igmp access-group mygroup</pre>	<p>IGMP レポートに指定されたアクセス リストが適用されます。</p>

	コマンドまたはアクション	目的
ステップ 11	ip pim sparse-mode 例 : Device(config-if)# ip pim sparse-mode	インターフェイスで PIM-SM をイネーブルにします。 (注) スパスモードを使用する必要があります。
ステップ 12	SSM チャンネルメンバーシップのアクセスコントロールを必要とするすべてのインターフェイスでステップ 1～11 を繰り返します。	--
ステップ 13	ip igmp version 3 例 : Device(config-if)# ip igmp version 3	このインターフェイス上で IGMPv3 をイネーブルにします。デフォルトの IGMP バージョンは IGMP バージョン 2 です。SSM にはバージョン 3 が必要です。
ステップ 14	ホスト方向のインターフェイスすべてでステップ 13 を繰り返します。	--
ステップ 15	end 例 : Device(config-if)# end	特権 EXEC モードに戻ります。

IGMP スヌーピングを設定する方法

IGMP スヌーピングのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	ip igmp snooping 例： Device(config)# ip igmp snooping	ディセーブルにした後で、IGMP スヌーピングをグローバルにイネーブルにします。
ステップ 4	bridge-domain bridge-id 例： Device(config)# bridge-domain 100	(任意) ブリッジ ドメイン コンフィギュレーション モードを開始します。
ステップ 5	ip igmp snooping 例： Device(config-bdomain)# ip igmp snooping	(任意) 設定されたブリッジ ドメイン インターフェイス上で IGMP スヌーピングをイネーブルにします。 <ul style="list-style-type: none">指定されたブリッジ ドメインで IGMP スヌーピングが明示的にディセーブルにされた場合にだけ必要です。
ステップ 6	end 例： Device(config-bdomain)# end	特権 EXEC モードに戻ります。

VLAN インターフェイスでの IGMP スヌーピングのイネーブル化またはディセーブル化

VLAN インターフェイス上で IGMP スヌーピングを有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	ip igmp snooping vlan <i>vlan-id</i> 例 : Device(config)# ip igmp snooping vlan 7	VLAN インターフェイス上で IGMP スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 VLAN スヌーピングをイネーブルにするには、IGMP スヌーピングをグローバルにイネーブルに設定しておく必要があります。 (注) 特定の VLAN インターフェイス上で IGMP スヌーピングをディセーブルにするには、 no ip igmp snooping vlan <i>vlan-id</i> グローバルコンフィギュレーションコマンドを、指定した VLAN 番号に対して使用します。
ステップ 4	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

スヌーピング方法の設定

マルチキャスト対応のルータポートは、レイヤ 2 マルチキャスト エントリごとに転送テーブルに追加されます。デバイスは、次のいずれかの方法でポートを学習します。

- IGMP クエリおよび Protocol Independent Multicast (PIM) パケットのスヌーピング
- **ip igmp snooping mrouter** グローバル コンフィギュレーション コマンドによるマルチキャストルータポートへの静的な接続

VLAN インターフェイスがマルチキャストルータにアクセスする方法を変更するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip igmp snooping vlan <i>vlan-id</i> mrouter interface {GigabitEthernet Port-Channel TenGigabitEthernet} 例： Device(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet1/0/3	VLAN 上で IGMP スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp snooping 例： Device# show ip igmp snooping	設定を確認します。
ステップ 6	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

マルチキャスト ルータ ポートの設定

デバイスにマルチキャスト ルータ ポートを追加する (マルチキャスト ルータへのスタティック 接続を有効にする) には、次の手順を実行します。



(注) マルチキャストルータへのスタティック接続は、デバイスポートに限りサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i> 例 : Device(config)# ip igmp snooping vlan 5 mrouter interface GigabitEthernet 1/0/1	マルチキャストルータの VLAN ID およびマルチキャストルータに対するインターフェイスを指定します。 • 指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 • このインターフェイスには物理インターフェイスまたはポートチャネルを指定できます。ポートチャネル範囲は 1 ~ 128 です。 (注) VLAN からマルチキャストルータポートを削除するには、 no ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i> グローバルコンフィギュレーションコマンドを使用します。
ステップ 4	end 例 : Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp snooping mrouter [vlan <i>vlan-id</i>] 例 : Device# show ip igmp snooping mrouter	VLAN インターフェイス上で IGMP スヌーピングが有効になっていることを確認します。

	コマンドまたはアクション	目的
	<code>vlan 5</code>	
ステップ 6	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

グループに加入するホストの静的な設定

ホストまたはレイヤ 2 ポートは通常、マルチキャスト グループに動的に加入しますが、インターフェイス上にホストを静的に設定することもできます。

マルチキャスト グループのメンバーとしてレイヤ 2 ポートを追加するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip igmp snooping vlan <i>vlan-id</i> static <i>ip-address</i> interface <i>interface-id</i> 例 : Device(config)# ip igmp snooping vlan 105 static 230.0.0.1 interface gigabitethernet1/0/1	マルチキャスト グループのメンバーとしてレイヤ 2 ポートを静的に設定します。 <ul style="list-style-type: none"> <i>vlan-id</i> は、マルチキャスト グループの VLAN ID です。指定できる範囲は 1 ~ 1001 または 1006 ~ 4094 です。 <i>ip-address</i> は、グループの IP アドレスです。 <i>interface-id</i> は、メンバーポートです。物理インターフェイスまたはポートチャンネル (1 ~ 128) に設定できます。

	コマンドまたはアクション	目的
		(注) マルチキャストグループからレイヤ 2 ポートを削除するには、 no ip igmp snooping vlan <i>vlan-id</i> static mac-address interface <i>interface-id</i> グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp snooping groups 例： Device# show ip igmp snooping groups	メンバポートおよび IP アドレスを確認します。
ステップ 6	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

IGMP 即時脱退のイネーブル化

IGMP 即時脱退をイネーブルに設定すると、デバイスはポート上で IGMP バージョン 2 の Leave メッセージを検出した場合、ただちにそのポートを削除します。即時脱退機能は、VLAN の各ポートにレシーバが 1 つ存在する場合にだけ使用してください。



- (注) 即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。IGMP バージョン 2 は、デバイスのデフォルトバージョンです。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> enable	<ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip igmp snooping vlan <i>vlan-id</i> immediate-leave 例： Device(config)# ip igmp snooping vlan 21 immediate-leave	VLAN インターフェイス上で、IGMP 即時脱退をイネーブルにします。 (注) VLAN 上で IGMP 即時脱退をディセーブルにするには、 no ip igmp snooping vlan <i>vlan-id</i> immediate-leave グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp snooping vlan <i>vlan-id</i> 例： Device# show ip igmp snooping vlan 21	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。
ステップ 6	end 例： Device(config)# end	特権 EXEC モードに戻ります。

IGMP 脱退タイマーの設定

脱退時間はグローバルまたは VLAN 単位で設定できます。IGMP 脱退タイマーの設定をイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip igmp snooping last-member-query-interval time 例 : Device(config)# ip igmp snooping last-member-query-interval 1000	IGMP 脱退タイマーをグローバルに設定します。指定できる範囲は 100 ~ 32767 ミリ秒です。 デフォルトの脱退時間は 1000 ミリ秒です。 (注) IGMP 脱退タイマーをグローバルにリセットしてデフォルト設定に戻すには、 no ip igmp snooping last-member-query-interval グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	ip igmp snooping vlan vlan-id last-member-query-interval time 例 : Device(config)# ip igmp snooping vlan 210 last-member-query-interval 1000	(任意) VLAN インターフェイス上で IGMP 脱退時間を設定します。有効値は 100 ~ 32767 ミリ秒です。 (注) VLAN 上に脱退時間を設定すると、グローバルに設定された内容は上書きされます。 (注) 特定の VLAN から IGMP 脱退タイマーの設定を削除するには、 no ip igmp snooping vlan vlan-id last-member-query-interval グローバル コンフィギュレーション コマンドを使用します。
ステップ 5	end 例 :	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	<code>Device(config-if)# end</code>	
ステップ 6	show ip igmp snooping 例： <code>Device# show ip igmp snooping</code>	(任意) 設定された IGMP 脱退時間を表示します。
ステップ 7	copy running-config startup-config 例： <code>Device# copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

IGMP 堅牢性変数の設定

このデバイスで IGMP 堅牢性変数を設定するには、次の手順を使用します。

堅牢性変数は、IGMP メッセージの計算時に IGMP スヌーピングで使用される整数です。堅牢性変数により、想定されるパケット損失を考慮した微調整を実施できます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： <code>Device> enable</code>	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： <code>Device# configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip igmp snooping robustness-variable count 例： <code>Device(config)# ip igmp snooping robustness-variable 3</code>	IGMP 堅牢性変数を設定します。範囲は、1～3 回です。 堅牢性変数の推奨値は 2 です。IGMP スヌーピングの堅牢性変数の値をデフォルトの 2 から指定した値に変更するには、このコマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	ip igmp snooping vlan <i>vlan-id</i> robustness-variable <i>count</i> 例 : <pre>Device(config)#ip igmp snooping vlan 100 robustness-variable 3</pre>	(任意) VLAN インターフェイス上で IGMP 堅牢性変数を設定します。範囲は、1～3 回です。堅牢性変数の推奨値は 2 です。 (注) VLAN で堅牢性変数カウントを設定すると、グローバルに設定された値が上書きされます。
ステップ 5	end 例 : <pre>Device(config-if)# end</pre>	特権 EXEC モードに戻ります。
ステップ 6	show ip igmp snooping 例 : <pre>Device# show ip igmp snooping</pre>	(任意) 設定された IGMP 堅牢性変数カウントを表示します。
ステップ 7	copy running-config startup-config 例 : <pre>Device# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

IGMP 最終メンバー クエリ回数の設定

グループ固有またはグループソース固有の leave メッセージの受信に応答して、IGMP グループ固有またはグループソース固有の (IGMP バージョン 3 で) クエリメッセージをデバイスが送信する回数を設定するには、次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : <pre>Device> enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip igmp snooping last-member-query-count count 例 : Device(config)# ip igmp snooping last-member-query-count 3	IGMP 最終メンバー クエリ回数を設定します。指定できる範囲は 1～7 です。デフォルト値は 2 メッセージです。
ステップ 4	ip igmp snooping vlan vlan-id last-member-query-count count 例 : Device(config)# ip igmp snooping vlan 100 last-member-query-count 3	(任意) VLAN インターフェイス上で IGMP 最終メンバー クエリ回数を設定します。指定できる範囲は 1～7 です。 (注) VLAN で最終メンバー クエリ回数を設定すると、グローバルに設定されたタイマーが上書きされます。
ステップ 5	end 例 : Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	show ip igmp snooping 例 : Device# show ip igmp snooping	(任意) 設定された IGMP 最終メンバー クエリ回数を表示します。
ステップ 7	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

TCN 関連コマンドの設定

TCN イベント後のマルチキャスト フラッディング時間の制御

トポロジ変更通知 (TCN) イベント後にフラッディングするマルチキャストデータのトラフィックに対し、一般クエリー数を設定できます。TCN フラッドクエリ カウントを 1 に設定した場合は、1 つの一般クエリーを受信した後にフラッディングが停止します。カウントを 7 に設定した場合、一般クエリーを 7 つ受信するまでフラッディングが続きます。グループは、TCN イベント中に受信した一般的クエリーに基づいて学習されます。

クライアントロケーションが変更され、ブロックされていた後に現在は転送中の受信者が同じポートに存在する場合や、ポートが脱退メッセージを送信せずにダウンした場合などに TCN イベントが発生します。

TCN フラッドクエリー カウントを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip igmp snooping tcn flood query count count 例 : Device(config)# ip igmp snooping tcn flood query count 3	マルチキャスト トラフィックがフラッディングする IGMP の一般クエリー数を指定します。 指定できる範囲は 1 ~ 10 です。デフォルトのフラッディングクエリー カウントは 2 です。 (注) デフォルトのフラッディングクエリ カウントに戻すには、 no ip igmp snooping tcn flood query count グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	end 例 :	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device(config-if)# end	
ステップ 5	show ip igmp snooping 例： Device# show ip igmp snooping	TCN の設定を確認します。
ステップ 6	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

フラッディングモードからの回復

トポロジの変更が発生した場合、スパニングツリーのルートは特別な IGMP Leave メッセージ (グローバル Leave メッセージ) をグループマルチキャストアドレス 0.0.0.0 に送信します。ただし、スパニングツリープロトコルのルートであるかどうかにかかわらず、グローバルな Leave メッセージを送信するようにデバイスを設定できます。ルータはこの特別な Leave メッセージを受信した場合、即座に一般クエリを送信して、TCN 中のフラッディングモードからできるだけ早く回復するようにします。デバイスがスパニングツリープロトコルのルートであれば、このコンフィギュレーションに関係なく、Leave メッセージが常に送信されます。

Leave メッセージを送信できるようにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip igmp snooping tcn query solicit 例：	TCN イベント中に発生したフラッドモードから回復するプロセスの速度を上げるために、IGMP Leave メッセージ

	コマンドまたはアクション	目的
	<pre>Device(config)# ip igmp snooping tcn query solicit</pre>	<p>(グローバル脱退)を送信します。デフォルトでは、クエリー送信要求はディセーブルに設定されています。</p> <p>(注) デフォルトのクエリソリューションに戻すには、no ip igmp snooping tcn query solicit グローバル コンフィギュレーション コマンドを使用します。</p>
ステップ 4	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 5	<p>show ip igmp snooping</p> <p>例 :</p> <pre>Device# show ip igmp snooping</pre>	TCN の設定を確認します。
ステップ 6	<p>copy running-config startup-config</p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	(任意) コンフィギュレーション ファイルに設定を保存します。

TCN イベント中のマルチキャストフラッドのディセーブル化

デバイスは TCN を受信すると、一般クエリを 2 つ受信するまで、すべてのポートに対してマルチキャストトラフィックをフラッドします。異なるマルチキャストグループのホストに接続されているポートが複数ある場合、リンク範囲を超えてにデバイスよるフラッドが行われ、パケット損失が発生する可能性があります。TCN フラッドを制御するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>enable</p> <p>例 :</p> <pre>Device> enable</pre>	<p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例 : Device(config)# interface GigabitEthernet 1/0/1	設定するインターフェイスを指定して、インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	no ip igmp snooping tcn flood 例 : Device(config-if)# no ip igmp snooping tcn flood	<p>スパニングツリーの TCN イベント中に発生するマルチキャストトラフィックのフラッドをディセーブルにします。</p> <p>デフォルトでは、インターフェイス上のマルチキャストフラッドはイネーブルです。</p> <p>(注) インターフェイス上でマルチキャストフラッドを再度イネーブルにするには、ip igmp snooping tcn flood インターフェイス コンフィギュレーション コマンドを使用します。</p>
ステップ 5	end 例 : Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	show ip igmp snooping 例 : Device# show ip igmp snooping	TCN の設定を確認します。
ステップ 7	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IGMP スヌーピング クエリアの設定

特定の VLAN で IGMP スヌーピング クエリア機能をイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip igmp snooping querier 例 : Device(config)# ip igmp snooping querier	IGMP スヌーピング クエリアをイネーブルにします。
ステップ 4	ip igmp snooping querier address ip_address 例 : Device(config)# ip igmp snooping querier address 172.16.24.1	(任意) IGMP スヌーピング クエリアの IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。 (注) IGMP スヌーピングクエリアがデバイス上で IP アドレスを検出できない場合、IGMP 一般クエリを生成しません。
ステップ 5	ip igmp snooping querier query-interval interval-count 例 : Device(config)# ip igmp snooping querier query-interval 30	(任意) IGMP クエリアの間隔を設定します。指定できる範囲は 1 ~ 18000 秒です。
ステップ 6	ip igmp snooping querier tcn query [count count interval interval] 例 :	(任意) トポロジ変更通知 (TCN) クエリーの間隔を設定します。指定でき

	コマンドまたはアクション	目的
	Device(config)# ip igmp snooping querier tcn query interval 20	る count の範囲は 1 ~ 10 です。指定できる interval の範囲は 1 ~ 255 秒です。
ステップ 7	ip igmp snooping querier timer expiry timeout 例： Device(config)# ip igmp snooping querier timer expiry 180	(任意) IGMP クエリアが期限切れになる時間を設定します。指定できる範囲は 60 ~ 300 秒です。
ステップ 8	ip igmp snooping querier version version 例： Device(config)# ip igmp snooping querier version 2	(任意) クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。
ステップ 9	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 10	show ip igmp snooping vlan vlan-id 例： Device# show ip igmp snooping vlan 30	(任意) VLAN インターフェイス上で IGMP スヌーピングクエリアがイネーブルになっていることを確認します。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
ステップ 11	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

IGMP レポート抑制のディセーブル化

IGMP レポート抑制をディセーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	no ip igmp snooping report-suppression 例 : Device(config)# no ip igmp snooping report-suppression	IGMP レポート抑制をディセーブルにします。IGMP レポート抑制がディセーブルの場合、すべての IGMP レポートがマルチキャスト ルータに転送されます。 IGMP レポート抑制はデフォルトでイネーブルです。 IGMP レポート抑制がイネーブルの場合、デバイスはマルチキャスト ルータクエリごとに IGMP レポートを 1 つだけ転送します。 (注) IGMP レポート抑制を再びイネーブルにするには、 ip igmp snooping report-suppression グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	end 例 : Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp snooping 例 : Device# show ip igmp snooping	IGMP レポート抑制がディセーブルになっていることを確認します。
ステップ 6	copy running-config startup-config 例 :	(任意) コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
	Device# copy running-config startup-config	

IGMP のモニタリング

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。



(注) このリリースでは、ルート単位の統計情報がサポートされていません。

また、リソースの使用状況を学習し、ネットワーク問題を解決するための情報を表示することもできます。さらに、ノードの到達可能性に関する情報を表示し、そのパケットが経由するネットワーク内のパスを検出することもできます。

次の表に示す特権 EXEC コマンドのいずれかを使用すると、さまざまなルーティング統計情報を表示できます。

表 11: システムおよびネットワーク統計情報を表示するコマンド

コマンド	目的
show ip igmp filter	IGMP フィルタ情報を表示します。
show ip igmp groups [<i>type-number</i> <i>detail</i>]	デバイスに直接接続され、IGMP を実行します。
show ip igmp interface [<i>type number</i>]	インターフェイスのマルチキャスト情報を表示します。
show ip igmp membership [<i>name/group address</i> all tracked]	転送に関する IGMP メンバーシップ情報を表示します。
show ip igmp profile [<i>profile_number</i>]	IGMP プロファイル情報を表示します。
show ip igmp ssm-mapping [<i>hostname/IP address</i>]	IGMP SSM マッピング情報を表示します。
show ip igmp static-group { class-map [interface [<i>type</i>]]	スタティック グループ情報を表示します。
show ip igmp vrf	選択した VPN ルーティング/転送情報を表示します。 (注) show ip igmp vrf vrf-name snooping コマンドを使用して、VRF スヌーピング情報を表示します。 ip igmp snooping groups コマンドを使用して、VRF スヌーピンググループ情報を表示します。

IGMP スヌーピング情報の監視

ダイナミックに学習された、あるいはスタティックに設定されたルータ ポートおよび VLAN インターフェイスの IGMP スヌーピング情報を表示できます。また、IGMP スヌーピング用に設定された VLAN の IP アドレス マルチキャスト エントリを表示することもできます。

表 12: IGMP スヌーピング情報を表示するためのコマンド

コマンド	目的
<code>show ip igmp snooping detail</code>	動作状態情報を表示します。
<code>show ip igmp snooping groups [count dynamic [count] user [count]]</code>	デバイスまたは特定のパラメータに関する情報を表示します。 <ul style="list-style-type: none"> • count : 実エントリの数を返します。 • dynamic : IGMP スヌーピング エントリのみを表示します。 • user : ユーザーによって設定されたエントリのみを表示します。
<code>show ip igmp snooping groups [count [vlan <i>vlan-id</i> [A.B.C.D count]]</code>	デバイスまたは特定のパラメータに関する情報を表示します。 <ul style="list-style-type: none"> • count : グループの合計数を返します。 • vlan : VLAN ID によるグループを指定します。
<code>show ip igmp snooping igmpv2-tracking</code>	IGMP スヌーピング トラッキング情報を表示します。 (注) このコマンドでは、ワイヤレス アドレス エントリが表示されません。ワイヤレス エントリを表示させるには、ワイヤレス エントリを有効にします。
<code>show ip igmp snooping groups vlan <i>vlan-id</i> [<i>ip_address</i> count dynamic [count] user[count]]</code>	マルチキャスト VLAN または IP アドレス エントリに関するテーブル情報を表示します。 <ul style="list-style-type: none"> • vlan-id : VLAN ID の範囲を指定します。 • count : 実エントリの数を返します。 • dynamic : IGMP スヌーピング エントリのみを表示します。 • ip_address : 指定したグループのエントリのみを表示します。 • user : ユーザーによって設定されたエントリのみを表示します。

コマンド	目的
<code>show ip igmp snooping mrouter [vlan <i>vlan-id</i>]</code>	ダイナミックに学習され、手動で情報を表示します。 (注) IGMP スヌーピングを有効にするインターフェイスを自動的に学習します。 (任意) 個々の VLAN に関する
<code>show ip igmp snooping querier [detail vlan <i>vlan-id</i>]</code>	IP アドレス、および VLAN で受信する情報を表示します。 (任意) VLAN の詳細な IGMP (任意) 個々の VLAN に関する
<code>show ip igmp snooping querier [vlan <i>vlan-id</i>] detail</code>	IP アドレスおよび VLAN で受信する情報、VLAN の IGMP スヌーピングを表示します。
<code>show ip igmp snooping [vlan <i>vlan-id</i> [detail]]</code>	デバイス上のすべての VLAN に関する情報を表示します。 (任意) 個々の VLAN に関する VLAN ID の範囲は 1 ~ 1001

IGMP フィルタリングおよび IGMP スロットリングの設定のモニタリング

IGMP プロファイルの特性を表示したり、デバイス上のすべてのインターフェイスまたは指定されたインターフェイスの IGMP プロファイルや最大グループ設定を表示したりできます。また、デバイス上のすべてのインターフェイスまたは指定したインターフェイスに関する IGMP スロットリング設定を表示することもできます。

表 13: IGMP フィルタリングおよび IGMP スロットリング設定を表示するためのコマンド

コマンド	目的
<code>show ip igmp profile [<i>profile number</i>]</code>	特定の IGMP プロファイルまたはデバイス上で定義されているすべての IGMP プロファイルを表示します。
<code>show running-config [interface <i>interface-id</i>]</code>	インターフェイスが所属できる IGMP グループの数 (設定されている場合) や、インターフェイスで使用する IGMP プロファイルを含む、特定のインターフェイスまたはデバイス上のすべての IGMP の設定を表示します。

IGMP の設定例

例：マルチキャストグループのメンバとしてデバイスを設定

次に、マルチキャストグループ 255.2.2.2 へのデバイス加入を許可する例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip igmp join-group 255.2.2.2
Device(config-if)#
```

例：マルチキャストグループへのアクセスの制御

インターフェイスで参加数を制限するには、IGMPプロファイルと関連付けるフィルタ用のポートを設定します。

```
Device# configure terminal
Device(config)# ip igmp profile 10
Device(config-igmp-profile)# ?

IGMP profile configuration commands:
deny matching addresses are denied
exit Exit from igmp profile configuration mode
no Negate a command or set its defaults
permit matching addresses are permitted
range add a range to the set

Device(config-igmp-profile)# range 172.16.5.1
Device(config-igmp-profile)# exit
Device(config)# interface gigabitEthernet 2/0/10
Device(config-if)# ip igmp filter 10
```

例：IGMP スヌーピングの設定

次に、マルチキャストルータへの静的な接続をイネーブルにする例を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet1/0/2
Device(config)# end
```

次に、ポート上のホストを静的に設定する例を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet1/0/1
Device(config)# end
```

次に、VLAN 130 上で IGMP 即時脱退をイネーブルにする例を示します。

例 : IGMP プロファイルの設定

```
Device# configure terminal
Device(config)# ip igmp snooping vlan 130 immediate-leave
Device(config)# end
```

次に、IGMP スヌーピング クエリアの送信元アドレスを 10.0.0.64 に設定する例を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping querier 10.0.0.64
Device(config)# end
```

次の例では、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する方法を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping querier query-interval 25
Device(config)# end
```

次の例では、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する方法を示します。

```
Device# configure terminal
Device(config)# ip igmp snooping querier timer expiry 60
Device(config)# end
```

次に、IGMP スヌーピング クエリア機能をバージョン 2 に設定する例を示します。

```
Device# configure terminal
Device(config)# no ip igmp snooping querier version 2
Device(config)# end
```

例 : IGMP プロファイルの設定

次に、単一の IP マルチキャストアドレスへのアクセスを許可する IGMP プロファイル 4 を作成して、設定を確認する例を示します。アクションが拒否（デフォルト）である場合は、**show ip igmp profile** の出力には表示されません。

```
Device(config)# ip igmp profile 4
Device(config-igmp-profile)# permit
Device(config-igmp-profile)# range 229.9.9.0
Device(config-igmp-profile)# end
Device# show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

例 : IGMP プロファイルの適用

次に、ポートに IGMP プロファイル 4 を適用する例を示します。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip igmp filter 4
Device(config-if)# end
```

例：IGMP グループの最大数の設定

次の例では、ポートが加入できる IGMP グループ数を 25 に制限する方法を示します。

```
Device(config)# interface GigabitEthernet1/0/2
Device(config-if)# ip igmp max-groups 25
Device(config-if)# end
```

例：ルーテッドポートとしてのインターフェイス設定

次に、デバイスのインターフェイスをルーテッドポートとして設定する例を示します。**no switchport** コマンドを実行して複数の IP マルチキャストルーティングを設定する必要がある場合、インターフェイスでこの設定を行う必要があります。

```
Device# configure terminal
Device(config)# interface GigabitEthernet1/0/9
Device(config-if)# description interface to be use as routed port
Device(config-if)# no switchport
Device(config-if)# ip address 10.20.20.1 255.255.255.0
Device(config-if)# ip pim sparse-mode
Device(config-if)# ip igmp join-group 224.1.2.3 source 15.15.15.2
Device(config-if)# end
Device# configure terminal
Device# show run interface gigabitEthernet 1/0/9
```

```
Current configuration : 166 bytes
!
interface GigabitEthernet1/0/9
 no switchport
 ip address 10.20.20.1 255.255.255.0
 ip pim sparse-mode
 ip igmp static-group 224.1.2.3 source 15.15.15.2
end
```

例：SVI としてのインターフェイスの設定

次に、デバイスのインターフェイスを SVI として設定する例を示します。**noswitchport** コマンドを実行して複数の IP マルチキャストルーティングを設定する必要がある場合、インターフェイスでこの設定を行う必要があります。

```
Device(config)# interface vlan 150
Device(config-if)# ip address 10.20.20.1 255.255.255.0
Device(config-if)# ip pim sparse-mode
Device(config-if)# ip igmp join-group 224.1.2.3 source 15.15.15.2
Device(config-if)# end
Device# configure terminal
Device(config)# ip igmp snooping vlan 20 static 224.1.2.3 interface gigabitEthernet 1/0/9
Device# show run interface vlan 150
```

```
Current configuration : 137 bytes
!
interface vlan 150
 ip address 10.20.20.1 255.255.255.0
 ip pim sparse-mode
```

例：直接接続された IGMP ホストがない場合に、マルチキャストトラフィックを転送するようにデバイスを設定

```
ip igmp static-group 224.1.2.3 source 15.15.15.2
end
```

例：直接接続された IGMP ホストがない場合に、マルチキャストトラフィックを転送するようにデバイスを設定

ip igmp join-group コマンドを使用して、直接接続された IGMP ホストがない場合に、マルチキャストトラフィックを転送するようデバイスを設定する例を以下に示します。この方法では、デバイスは、マルチキャストパケットの転送に加えて、マルチキャストパケットを受信します。マルチキャストパケットを受信する場合は、高速スイッチングを実行できません。

この例では、デバイスでギガビットイーサネットインターフェイス 1/0/1 が、グループ 225.2.2.2 に加入するように設定されています。

```
interface GigabitEthernet1/0/1
ip igmp join-group 225.2.2.2
```

ip igmp static-group コマンドを使用して、直接接続された IGMP ホストがない場合に、マルチキャストトラフィックを転送するようデバイスを設定する例を以下に示します。この方法の場合、デバイスはパケットそのものを受信せず、転送だけを実行します。したがって、この方法では、高速スイッチングを実行できます。発信インターフェイスが IGMP キャッシュに格納されますが、マルチキャストルートエントリに「L」（ローカル）フラグが付かないことから明らかのように、デバイス自体はメンバではありません。

この例では、グループ 225.2.2.2 のスタティック グループ メンバーシップ エントリがファストイーサネットインターフェイス 0/1/0 で設定されます。

```
interface GigabitEthernet1/0/1
ip igmp static-group 225.2.2.2
```

IGMP 拡張アクセスリストを使用して SSM ネットワークへのアクセスを制御する方法

ここでは、IGMP 拡張アクセスリストを使用して SSM ネットワーク上でアクセスを制御する、次の設定例について説明します。



- (注) アクセスリストは非常に柔軟が高いことに留意してください。マルチキャストトラフィックのフィルタリングに使用できる **permit** ステートメントと **deny** ステートメントの組み合わせは多数あります。この項では、少しの例を示します。

例：グループ G のすべての状態を拒否

次に、グループ G のすべての状態を拒否する方法の例を示します。この例では、IGMPv3 レポートの SSM グループ 232.2.2.2 のすべての送信元がフィルタリングされるよう、ファスト

イーサネット インターフェイス 0/0/0 が設定されます。これにより、このグループが効率的に拒否されます。

```
ip access-list extended test1
 deny igmp any host 232.2.2.2
 permit igmp any any
!
interface GigabitEthernet 1/0/1
 ip igmp access-group test1
```

例：ソース S のすべての状態を拒否

次に、ソース S ですべての状態を拒否する方法の例を示します。この例では、IGMPv3 レポートの送信元の 10.2.1.32 のグループがフィルタリングされるよう、ギガビットイーサネット インターフェイス 1/1/0 が設定されます。これにより、このソースが効果的に拒否されます。

```
ip access-list extended test2
 deny igmp host 10.2.1.32 any
 permit igmp any any
!
interface GigabitEthernet1/0/1
 ip igmp access-group test2
```

例：グループ G のすべての状態を許可

次に、グループ G ですべての状態を許可する例を示します。この例では、IGMPv3 レポートの SSM グループ 232.1.1.10 に対するすべてのソースが受け付けられるよう、ギガビットイーサネット インターフェイス 1/2/0 が設定されます。これにより、このグループ全体が効果的に受け付けられます。

```
ip access-list extended test3
 permit igmp any host 232.1.1.10
!
interface GigabitEthernet 1/2/0
 ip igmp access-group test3
```

例：ソース S のすべての状態を許可

次に、ソース S ですべての状態を許可する例を示します。この例では、IGMPv3 レポートのソース 10.6.23.32 に対するすべてのグループが受け付けられるよう、ギガビットイーサネット インターフェイス 1/2 が設定されます。これにより、このソース全体が効果的に受け付けられます。

```
ip access-list extended test4
 permit igmp host 10.6.23.32 any
!
interface GigabitEthernet1/2/0
 ip igmp access-group test4
```

例：グループ G のソース S をフィルタリング

例：グループ G のソース S をフィルタリング

次に、グループ G の特定のソース S のフィルタリング例を示します。この例では、IGMPv3 レポートの SSM グループ 232.2.30.30 のソース 232.2.2.2 をフィルタリングするよう、ギガビットイーサネット インターフェイス 0/3/0 が設定されます。

```
ip access-list extended test5
deny igmp host 10.4.4.4 host 232.2.30.30
permit igmp any any
!
interface GigabitEthernet0/3/0
ip igmp access-group test5
```

IGMP に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャストルーティングのコマンド」の項を参照してください。 <i>Command Reference (Catalyst 9200 Series Switches)</i>

IGMP の機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	IGMP	IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。インターフェイスで PIM をイネーブルにすると、IGMP もイネーブルになります。IGMP は、特別なマルチキャスト クエリアおよびホストを使用して、ネットワーク全体でマルチキャストトラフィックのフローを自動的に制御および制限する手段を提供します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 5 章

IGMP プロキシの設定

- [IGMP プロキシの前提条件](#) (111 ページ)
- [IGMP プロキシについて](#) (111 ページ)
- [IGMP プロキシの設定方法](#) (116 ページ)
- [IGMP プロキシの設定例](#) (124 ページ)
- [IGMP プロキシに関するその他の関連資料](#) (125 ページ)
- [IGMP プロキシの機能履歴](#) (126 ページ)

IGMP プロキシの前提条件

- IGMP UDL 上のすべてのデバイスに、同じサブネットアドレスがあること。UDL 上のすべてのデバイスで、同じサブネットアドレスを持つことができない場合、アップストリーム デバイスは、ダウンストリーム デバイスが接続されているすべてのサブネットに一致するセカンダリ アドレスで設定される必要があります。
- IP マルチキャストがイネーブルになり、PIM インターフェイスが設定されます。IGMP プロキシ用の PIM インターフェイスを設定する際、インターフェイスがスパースモード領域で稼働中で、静的 RP、ブートストラップ (BSR)、またはリスナー機能付きの Auto-RP を実行している場合は、PIM スパースモード (PIM-SM) を使用します。

IGMP プロキシについて

IGMP プロキシ

IGMP プロキシは、アップストリームネットワークがソースのマルチキャストグループに、ダウンストリームルータに直接接続されていない単方向リンクルーティング (UDLR) 環境のホストが加入できるようにします。

IGMP プロキシを実装するには、次の 2 つの方法があります。

- 単一のアップストリーム インターフェイス用の IGMP プロキシ

- 複数のアップストリーム インターフェイス用の IGMP プロキシ

単一のアップストリーム インターフェイス用の IGMP プロキシ

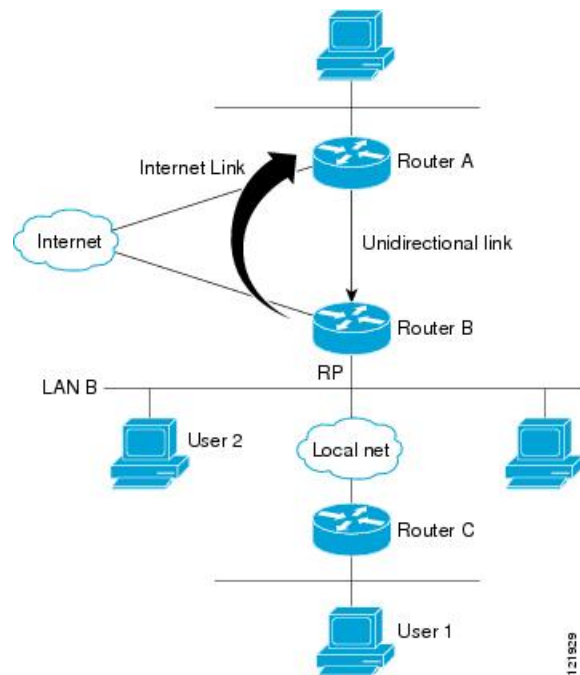
次の図は、2つの UDLR シナリオを示すトポロジ例です。

- 従来型の UDL ルーティングのシナリオ：直接接続されたレシーバがある UDL デバイス。
- IGMP プロキシのシナリオ：直接接続されたレシーバのない UDL デバイス。

IGMP UDL は、アップストリームおよびダウンストリーム デバイス上にある必要はありません。



(注) 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。



シナリオ 1：従来型の UDLR のシナリオ（受信先が直接接続されている UDL デバイス）

シナリオ 1 では、IGMP プロキシメカニズムは必要ありません。このシナリオでは、次の一連のイベントが発生します。

1. ユーザー 2 がグループ G の対象を要求する IGMP メンバーシップ レポートを送信します。
2. ルータ B は、IGMP メンバーシップ レポートを受信し、LAN B のグループ G の転送エントリーを追加し、UDLR アップストリーム デバイスであるルータ A に IGMP レポートをプロキシします。

3. IGMP レポートは、インターネット リンク間でプロキシされます。
4. ルータ A は IGMP プロキシを受信し、単方向リンクの転送エントリを保持します。

シナリオ 2 : IGMP プロキシのシナリオ (受信先が直接接続されていない UDL デバイス)

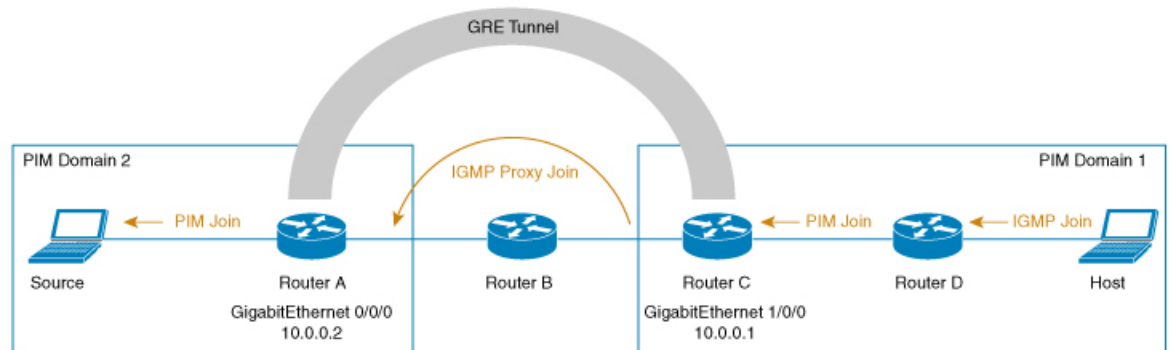
シナリオ 2 の場合、アップストリーム ネットワークがソースのマルチキャスト グループに、ダウンストリーム デバイスに直接接続されていないホストが加入できるように、IGMP プロキシメカニズムが必要です。このシナリオでは、次の一連のイベントが発生します。

1. ユーザー 1 がグループ G の対象を要求する IGMP メンバーシップ レポートを送信します。
2. ルータ C が RP (ルータ B) に PIM Join メッセージをホップバイホップで送信します。
3. ルータ B で PIM 加入メッセージを受信し、LAN B 上のグループ G に対する転送エントリが追加されます。
4. ルータ B では、その mroute テーブルが定期的にチェックされ、インターネット リンクを介してアップストリーム UDL デバイスに IGMP メンバーシップ レポートがプロキシされます。
5. ルータ A は単方向リンク (UDL) 転送エントリを作成し、維持します。

エンタープライズ ネットワークでは、サテライトを介して IP マルチキャスト トラフィックを受信し、ネットワーク中にトラフィックを転送することができる必要があります。シナリオ 2 は、受信ホストがダウンストリーム デバイスのルータ B に直接接続する必要があるため、単方向リンクルーティング (UDLR) だけでは不可能です。IGMP プロキシメカニズムを使用すると、マルチキャスト転送テーブル内の (*, G) エントリに対し IGMP レポートを作成することで、この制限が取り除かれます。そのため、このシナリオを機能させるには、インターフェイスでプロキシされた (*, G) 静的マルチキャストルート (mroute) エントリの IGMP レポートの転送をイネーブルにして (**ip igmp mroute-proxy** コマンドを使用)、mroute プロキシサービスをイネーブルにし (**ip igmp proxy-service** コマンドを使用)、PIM 対応ネットワークと可能性のあるメンバに導く必要があります。



-
- (注) PIM メッセージはアップストリームに転送されないため、各ダウンストリーム ネットワークとアップストリーム ネットワークのドメインは別になります。
-



シナリオ 3 : UDLR を使用しない IGMP プロキシシナリオ

シナリオ 3 では、IGMP プロキシメカニズムを使用して、ホストが UDLR リンクを使用せずにアップストリームネットワークからトラフィックを受信できるようにします。このシナリオでは、次の一連のイベントが発生します。

1. ホストは PIM ドメイン 1 にあり、IGMP メンバーシップレポート（参加要求）を **ルータ D** に送信してグループ G の対象を要求します。**ルータ D** は IGMP 参加を PIM 参加に変換し、**ルータ C** に送信します。この要求は、**ルータ C** から **ルータ A** にアップストリームで送信されます。ルータは 2 つの異なる PIM ドメイン（PIM ネイバーではない）にあり、代わりに GRE トンネルを介して接続されています。
2. **ルータ C** は GIM トンネルエンドポイント（**ルータ A**）に転送できるように、PIM 参加メッセージを IGMP プロキシ参加に変換します。



(注) IGMP プロキシ加入メッセージは、1 ホップでのみ転送できます。

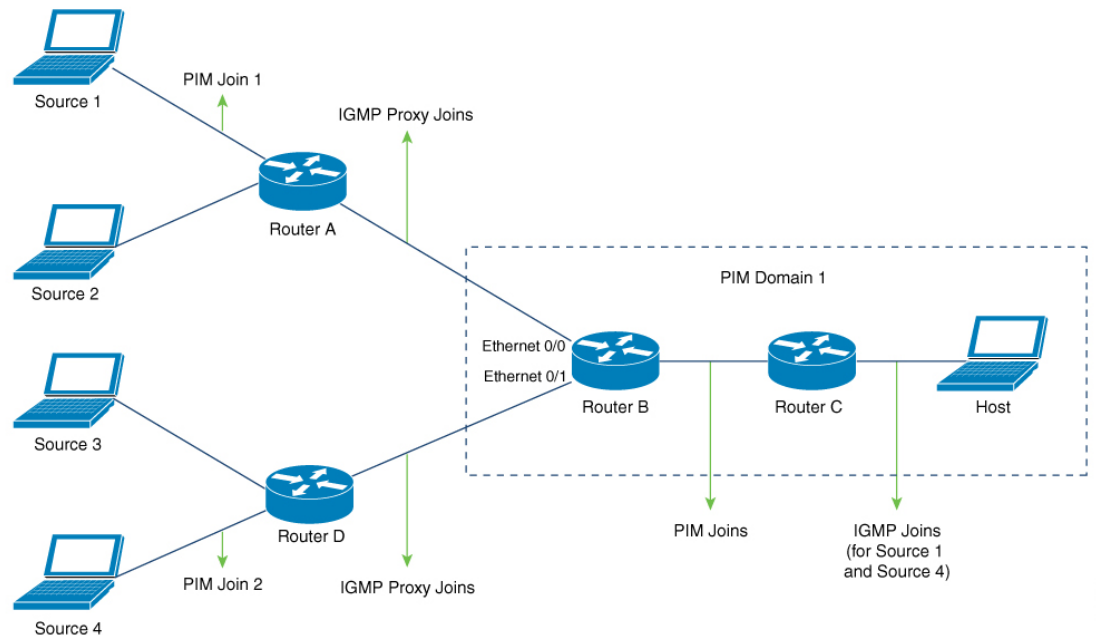
上の図では、GRE トンネルはルータ C とルータ A の間でこの単一のホップを提供しています（ルータ B をバイパス）。

GRE トンネルがない場合、異なる PIM ドメインのデバイスには、直接（バックツーバック）接続されたインターフェイスが必要です。

3. IGMP プロキシ参加が **ルータ A** に到達すると、PIM 参加メッセージとして送信元デバイスに転送されます。

複数のアップストリーム インターフェイス用の IGMP プロキシ

IGMP プロキシを使用すると、複数のアップストリームインターフェイスからデータを要求することもできます。ネットワーク内のアップストリームデバイス数が多い場合は、この方法で IGMP プロキシを実装できます。この方法を使用する場合、前のセクションで説明した 3 つのシナリオのいずれかのように、単一のアップストリームデバイスに IGMP プロキシを実装することもできます。



この方法では、IGMP プロキシを使用して、複数のアップストリームデバイスからトラフィックを受信できます。次の一連のイベントが発生します。

1. ホストは PIM ドメイン 1 にあり、複数の IGMP メンバーシップレポートをルータ C に送信して（加入要求）、異なるグループへの関心を要求します。ルータ C は IGMP 加入を PIM 加入に変換し、ルータ B に送信します。これらの要求は、ルータ B からルータ A にアップストリームで送信する必要があります。ルータは 2 つの異なる PIM ドメイン内にあります（PIM ネイバーではありません）。
2. ルータ B は PIM 加入メッセージを IGMP プロキシ加入メッセージに変換して、上位のインターフェイスに転送できるようにします。
3. クラスマップはグローバルに設定されます。このクラスマップには、マルチキャストグループに関する情報を記述します。次の条件が満たされると、異なるマルチキャストグループの IGMP プロキシ加入が送信されます。
 - グループに (*, G) または (S, G) エントリがある。
 - (*, G) または (S, G) エントリに NULL ではない OIF リストがある。
4. IGMP プロキシのインターバルで、異なるグループの IGMP プロキシ加入がそれぞれのアップストリームインターフェイスを介して送信されます。
5. IGMP プロキシ加入メッセージがルータ A に到達すると、PIM 加入メッセージとしてそれぞれの送信元デバイスに転送されます。

IGMP プロキシの設定方法

IGMP UDLR に対するアップストリーム UDL デバイスの設定

IGMP UDLR に対するアップストリーム UDL デバイスを設定するには、この作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number 例： Device(config)# interface gigabitethernet 1/0/0	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。 • <i>type</i> および <i>number</i> 引数に、アップストリームデバイスの UDL として使用するインターフェイスを指定します。
ステップ 4	ip igmp unidirectional-link 例： Device(config-if)# ip igmp unidirectional-link	インターフェイス上の IGMP を、IGMP UDLR に対して単方向になるよう設定します。
ステップ 5	end 例： Device(config-if)# end	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。

IGMP プロキシ サポート付きの IGMP UDLR に対するダウンストリーム UDL デバイスの設定

IGMP プロキシ サポート付きの IGMP UDLR に対するダウンストリーム UDL デバイスを設定するには、この作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number 例： Device(config)# interface gigabitethernet 0/0/0	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。 • <i>type</i> および <i>number</i> 引数に、IGMP UDLR に対するダウンストリーム デバイスの UDL として使用するインターフェイスを指定します。
ステップ 4	ip igmp unidirectional-link 例： Device(config-if)# ip igmp unidirectional-link	インターフェイス上の IGMP を、IGMP UDLR に対して単方向になるよう設定します。
ステップ 5	exit 例： Device(config-if)# exit	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、グローバル設定モードに戻ります。
ステップ 6	interface type number 例： Device(config)# interface gigabitethernet 1/0/0	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。 • <i>type</i> および <i>number</i> 引数で、間接的に接続されているホストの方向に向いているインターフェイスを選択します。

	コマンドまたはアクション	目的
ステップ 7	<p>ip igmp mroute-proxy <i>type number</i></p> <p>例 :</p> <pre>Device(config-if)# ip igmp mroute-proxy loopback 0</pre>	<p>プロキシされた (*, G) マルチキャスト スタティック ルート (mroute) エントリの IGMP レポートの転送をイネーブルにします。</p> <ul style="list-style-type: none"> この手順は、マルチキャスト転送テーブルにあるすべての (*, G) 転送エントリに対するプロキシサービスインターフェイスへの、IGMP レポートの転送をイネーブルにするために実行されます。 この例では、ギガビットイーサネットインターフェイス 1/0/0 で、ギガビットイーサネットインターフェイス 1/0/0 に転送される mroute テーブルのすべてのグループの ループバック インターフェイス 0 に IGMP レポートを送信するように要求する ip igmp mroute-proxy コマンドが設定されます。
ステップ 8	<p>exit</p> <p>例 :</p> <pre>Device(config-if)# exit</pre>	<p>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、グローバル設定モードに戻ります。</p>
ステップ 9	<p>interface <i>type number</i></p> <p>例 :</p> <pre>Device(config)# interface loopback 0</pre>	<p>指定したインターフェイスに対してインターフェイスコンフィギュレーションモードを開始します。</p> <ul style="list-style-type: none"> この例では、ループバック インターフェイス 0 が指定されます。
ステップ 10	<p>ip igmp helper-address udl <i>interface-type interface-number</i></p> <p>例 :</p> <pre>Device(config-if)# ip igmp helper-address udl gigabitethernet 0/0/0</pre>	<p>UDLR で IGMP ヘルパーを設定します。</p> <ul style="list-style-type: none"> このステップで、ダウンストリームデバイスが受信したホストから <i>interface-type</i> および <i>interface-number</i> 引数で指定されたインターフェイスに関連付けられた UDL に接続されているアップストリーム デバイスへの IGMP レ

	コマンドまたはアクション	目的
		<p>ポートをヘルパー処理できるようになります。</p> <ul style="list-style-type: none"> トポロジ例では、IGMP ヘルパーはダウンストリーム デバイスのループバック インターフェイス 0 に設定されます。そのため、ループバック インターフェイス 0 が、ホストからギガビットイーサネット インターフェイス 0/0/0 に接続されているアップストリーム デバイスへの IGMP レポートをヘルパー処理するように設定されます。
ステップ 11	<p>ip igmp proxy-service</p> <p>例 :</p> <pre>Device(config-if)# ip igmp proxy-service</pre>	<p>mroute プロキシサービスをイネーブルにします。</p> <ul style="list-style-type: none"> mroute プロキシサービスがイネーブルのときに、IGMP クエリインターバルに基づいて ip igmp mroute-proxy コマンド (ステップ 7 を参照) で設定されたインターフェイスに一致する、(*, G) 転送エントリの静的 mroute テーブルが、デバイスによって定期的にチェックされます。一致が存在する場合、1 つの IGMP レポートがこのインターフェイスで作成され、受信されます。 <p>(注)</p> <p>ip igmp proxy-service コマンドは、ip igmp helper-address (UDL) コマンドとともに使用することを目的としています。</p> <ul style="list-style-type: none"> この例では、ip igmp mroute-proxy コマンドで登録されているインターフェイスに対するすべてのグループのインターフェイスに対して IGMP レポートの転送をイネーブルにするように、ループバック インターフェイス 0 で ip igmp proxy-service コマンドが設定され

	コマンドまたはアクション	目的
		ます（ステップ 7 を参照してください）。
ステップ 12	end 例： Device(config-if)# end	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 13	show ip igmp interface 例： Device# show ip igmp interface	（任意）インターフェイスに関するマルチキャスト関連情報を表示します。
ステップ 14	show ip igmp udldr 例： Device# show ip igmp udldr	（任意）設定された UDL ヘルパー アドレスがあるインターフェイス上で、マルチキャストグループに直接接続されている UDLR 情報を表示します。

UDLR を使用しない IGMP プロキシ加入向けダウンストリームデバイスの設定

UDLR を使用せずに IGMP プロキシ向けダウンストリームデバイスを設定するには、次の作業を実行します。

（上の図によると、すべての手順はルータ C で行います）

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device > enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface type number 例： Device(config)# interface gigabitethernet 1/0/0	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。 <i>type</i> 引数および <i>number</i> 引数では、ホストに接続されているインターフェイスを指定します。

	コマンドまたはアクション	目的
ステップ 4	ip igmp mroute-proxy type number 例 : <pre>Device(config-if)# ip igmp mroute-proxy loopback 0</pre>	<p>マルチキャスト転送テーブル内のすべてのプロキシ(*, G) マルチキャスト静的ルート (mroute) エントリを転送するために、指定したプロキシサービスインターフェイスへの IGMP レポートの転送を有効にします。</p> <p>この例では、ループバック インターフェイス 0 が指定したプロキシサービスインターフェイスです。</p>
ステップ 5	exit 例 : <pre>Device(config-if)# exit</pre>	<p>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、グローバル設定モードに戻ります。</p>
ステップ 6	interface type number 例 : <pre>Device(config)# interface loopback 0</pre>	<p>指定したプロキシサービスインターフェイスのコンフィギュレーションモードを開始します。</p> <p>この例では、ループバック インターフェイス 0 が指定されます。</p>
ステップ 7	ip igmp helper-address ip-address 例 : <pre>Device(config-if)# ip igmp helper-address 10.0.0.2</pre>	<p>IGMP プロキシ加入用の IGMP ヘルパーを設定します。</p> <p><i>ip-address</i> 引数には、IGMP プロキシ加入メッセージを送る必要のあるアップストリームデバイスの IP アドレスを指定します。</p> <p>トポロジ例では、IGMP ヘルパーはダウンストリームデバイス (ルータ C) のループバック インターフェイス 0 に設定されます。</p> <p>このコマンドにより、ルータ D から受信した PIM 加入メッセージを IGMP プロキシ加入メッセージに変換し、アップストリームデバイス (ルータ A) に転送するためのループバック インターフェイス 0 が設定されます。</p>
ステップ 8	ip igmp proxy-service 例 : <pre>Device(config-if) ip igmp proxy-service</pre>	<p>mroute プロキシサービスをイネーブルにします。</p> <p>mroute プロキシサービスがイネーブルのときに、IGMP クエリインターバルに基づいて ip igmp mroute-proxy コマ</p>

	コマンドまたはアクション	目的
		<p>ンド（ステップ7を参照）で設定されたインターフェイスに一致する、(*,G) 転送エントリのスタティック mroute テーブルが、デバイスによって定期的にチェックされます。一致が存在する場合、1つの IGMP レポートがこのインターフェイスで作成され、受信されます。</p> <p>（注） ip igmp proxy-service コマンドは、ip igmp helper-address コマンドとともに使用することを目的としています。</p>
ステップ 9	end 例： Device(config-if)# end	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 10	show ip igmp interface 例： Device# show ip igmp interface	（任意）インターフェイスに関するマルチキャスト関連情報を表示します。

複数のアップストリーム インターフェイスの IGMP プロキシ向けダウンストリームデバイスの設定

複数のアップストリームインターフェイス向け IGMP プロキシのダウンストリームデバイスを設定するには、次の作業を実行します

（前の☒を参照して、アップストリーム デバイスに接続されているルータ B のインターフェイスですべての手順を実行してください）。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device > enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	class-map type multicast-flows name 例 : Device(config-if)# class-map type multicast-flows proxymap	異なるマルチキャストグループのアップリンク インターフェイスが定義されているクラスマップを使用して、インターフェイスを設定します。 マルチキャストグループの範囲は、225.0.0.1 ~ 225.0.0.10 です。
ステップ 4	interface type number 例 : Device(config)# interface ethernet 0/0	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。 <i>type</i> 引数および <i>number</i> 引数では、ホストに接続されているインターフェイスを指定します。
ステップ 5	ip igmp upstream-proxy class-map-name 例 : Device(config-if)# ip igmp upstream-proxy proxymap	IGMP プロキシとのインターフェイスをイネーブルにします。次の条件が満たされると、クラスマップ内にあるこれらのグループの IGMP プロキシ参加が送信されます。 <ul style="list-style-type: none"> • (*,G) または (S,G) mroute が、インターフェイスと同じ mvrf のグループに対して存在する。 • (*,G) または (S,G) mroute に NULL ではない OIF リストがある。
ステップ 6	ip igmp iif-starg 例 : Device(config-if)# ip igmp iif-starg	クラスマップで指定したグループの mroute の RPF インターフェイスをイーサネット 0/0 に変更します。
ステップ 7	ip igmp proxy-report-interval time 例 : Device(config-if)# ip igmp proxy-report-interval 130	プロキシレポートの送信間隔 (秒単位) を設定します。デフォルト値は 60 秒です。
ステップ 8	end 例 : Device(config-if)# end	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 9	show ip igmp interface 例 : Device# show ip igmp interface	(任意) インターフェイスに関するマルチキャスト関連情報を表示します。

IGMP プロキシの設定例

例：IGMP UDLR 向けアップストリーム UDL デバイスの設定

IGMP UDLR 向けアップストリーム UDL の設定例を以下に示します。

```
interface gigabitethernet 0/0/0
ip address 10.1.1.1 255.255.255.0
ip pim sparse-mode
!
interface gigabitethernet 1/0/0
ip address 10.2.1.1 255.255.255.0
ip pim sparse-mode
ip igmp unidirectional-link
!
interface gigabitethernet 2/0/0
ip address 10.3.1.1 255.255.255.0
```

例：IGMP プロキシサポートによる IGMP UDLR 向けダウンストリーム UDL デバイスの設定

IGMP プロキシサポートを使用して、IGMP UDLR 向けのダウンストリーム UDL デバイスを設定する例を以下に示します。

```
ip pim rp-address 10.5.1.1 5
access-list 5 permit 239.0.0.0 0.255.255.255
!
interface loopback 0
ip address 10.7.1.1 255.255.255.0
ip pim sparse-mode
ip igmp helper-address udl ethernet 0
ip igmp proxy-service
!
interface gigabitethernet 0/0/0
ip address 10.2.1.2 255.255.255.0
ip pim sparse-mode
ip igmp unidirectional-link
!
interface gigabitethernet 1/0/0
ip address 10.5.1.1 255.255.255.0
ip pim sparse-mode
ip igmp mroute-proxy loopback 0
!
interface gigabitethernet 2/0/0
ip address 10.6.1.1 255.255.255.0
```

例：UDLR を使用しない IGMP プロキシ向けダウンストリームデバイスの設定

UDLR を使用せずに IGMP プロキシのダウンストリームデバイスを設定する例を以下に示します。

```
interface Loopback0
ip address 2.2.2.2 255.255.0.0
ip pim sparse-dense-mode
ip igmp helper-address 99.99.99.1
ip igmp proxy-service
ip ospf 1 area 0
!
```

例：複数のアップストリームインターフェイスの IGMP プロキシ向けダウンストリームデバイスの設定

複数のアップストリームインターフェイスの IGMP プロキシ向けダウンストリームデバイスを設定する例を次に示します。

```
interface gigabitethernet0/0
ip address 99.99.99.1 255.255.255.0
ip pim passive
ip igmp upstream-proxy 12
ip igmp iif-starg
ip igmp proxy-report-interval 100
end

class-map type multicast-flows 12
group 229.0.0.1
group 228.0.0.1 to 228.0.0.10
```

IGMP プロキシに関するその他の関連資料

ここでは、IGMP のカスタマイズに関する関連資料について説明します。

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャストルーティングのコマンド」の項を参照してください。 <i>Command Reference (Catalyst 9200 Series Switches)</i>

標準および RFC

標準/RFC	タイトル
RFC 1112	『Host extensions for IP multicasting』
RFC 2236	『Internet Group Management Protocol, Version 2』
RFC 3376	『Internet Group Management Protocol, Version 3』

IGMP プロキシの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	IGMP プロキシ	IGMP プロキシは、アップストリーム ネットワークがソースのマルチキャスト グループに、ダウンストリーム ルータに直接接続されていない単方向リンク ルーティング (UDLR) 環境のホストが加入できるようにします。
Cisco IOS XE Gibraltar 16.12.1	UDLR を使用しない IGMP プロキシ	IGMP プロキシを使用すると、ホストでは UDLR リンクを使用せずにアップストリーム ネットワークからトラフィックを受信できます。
Cisco IOS XE Amsterdam 17.1.1	複数のアップストリーム インターフェイス用の IGMP プロキシ	IGMP プロキシを使用すると、ユーザーは複数のアップストリームデバイスからトラフィックを受信できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 6 章

スイッチドイーサネットでの IP マルチキャストの抑制

- [スイッチドイーサネット ネットワークで IP マルチキャストを抑制するための前提条件 \(127 ページ\)](#)
- [スイッチドイーサネット ネットワークでの IP マルチキャストについての情報 \(127 ページ\)](#)
- [スイッチドイーサネット ネットワークでマルチキャストを抑制する例 \(130 ページ\)](#)
- [スイッチドイーサネット ネットワークで IP マルチキャストを抑制する設定例 \(133 ページ\)](#)
- [スイッチドイーサネット ネットワークでの IP マルチキャスト抑制に関するその他の参考資料 \(133 ページ\)](#)
- [スイッチドイーサネットでの IP マルチキャスト抑制の機能履歴 \(134 ページ\)](#)

スイッチドイーサネット ネットワークで IP マルチキャストを抑制するための前提条件

このモジュールの作業を実行する前に、[IP マルチキャストルーティングテクノロジーの概要 \(1 ページ\)](#) モジュールで説明している概念をよく理解しておく必要があります。

スイッチドイーサネット ネットワークでの IP マルチキャストについての情報

IP マルチキャスト トラフィックとレイヤ 2 スイッチ

レイヤ 2 スイッチのデフォルト動作では、スイッチ上の宛先 LAN に属する各ポートに、すべてのマルチキャストトラフィックが転送されます。この動作では、スイッチの効率が低下します。その目的は、データを受信する必要があるポートへのトラフィックを制限することです。

この動作では、不要なマルチキャストトラフィックを減らす抑制メカニズムが必要です。これによって、スイッチのパフォーマンスが改善されます。

Cisco Group Management Protocol (CGMP)、Router Group Management Protocol (RGMP)、および IGMP スヌーピングは、レイヤ 2 スイッチング環境で IP マルチキャストを効果的に抑制します。

- CGMP および IGMP スヌーピングは、エンドユーザーまたはレシーバクライアントが含まれているサブネットで使用されます。
- RGMP は、コラプストバックボーンなどのルータのみに含まれているルーティング対象セグメントで使用されます。
- RGMP と CGMP は相互運用できません。ただし、インターネットグループ管理プロトコル (IGMP) は、CGMP および RGMP スヌーピングと相互運用できます。

IP マルチキャスト用の Catalyst スイッチの CGMP

CGMP は、IGMP によって実行される作業と同様の作業を実行するために、Catalyst スイッチに接続されたデバイスで使用される、シスコが開発したプロトコルです。IP マルチキャストデータパケットと IGMP レポートメッセージ（いずれも MAC レベルで同じグループアドレスにアドレス指定されます）を区別しない Catalyst スイッチの場合、CGMP が必要になります。スイッチは IGMP パケットを区別できますが、スイッチ上でソフトウェアを使用する必要があり、これがパフォーマンスに大きな影響を与えます。

マルチキャストデバイスとレイヤ 2 スイッチで CGMP を設定する必要があります。結果的に CGMP では、該当するレシーバに接続されている Catalyst スイッチのポートにだけ IP マルチキャストトラフィックが提供されます。トラフィックを明示的に要求していない他のすべてのポートは、これらのポートがマルチキャストルータに接続されていない限り、トラフィックを受信しません。マルチキャストルータポートは、すべての IP マルチキャストデータパケットを受信する必要があります。

マルチキャストグループに加入するとき、ホストは CGMP を使用して、送信要求されなくてもターゲットグループへの IGMP メンバーシップレポートメッセージをマルチキャストします。通常の IGMP 処理では、IGMP レポートが、スイッチを介してルータに渡されます。ルータ（このインターフェイス上で CGMP がイネーブルにされている必要がある）では、IGMP レポートを受信し、通常どおりに処理されますが、CGMP 加入メッセージも作成され、スイッチに送信されます。Join メッセージには、エンドステーションの MAC アドレスと加入したグループの MAC アドレスが含まれます。

スイッチは、CGMP Join メッセージを受信し、そのマルチキャストグループ用の連想メモリ (CAM) テーブルにポートを追加します。以後、このマルチキャストグループに対するすべての後続のトラフィックは、そのホストのポートに転送されます。

レイヤ 2 スイッチは、いくつかの宛先 MAC アドレスを 1 つの物理ポートに割り当てることができるよう、設計されています。この設計により、スイッチを階層構造で接続できるようになります。また、多数のマルチキャスト宛先アドレスを単一ポートに転送できます。

デバイスポートは、マルチキャストグループのエントリにも追加されます。IGMP コントロールメッセージもマルチキャストトラフィックとして送信されるため、マルチキャストデバイスは、各グループに対するすべてのマルチキャストトラフィックをリスンします。その他のマルチキャストトラフィックは、CGMP で作成された新しいエントリを含む CAM テーブルを使用して転送されます。

IGMP スヌーピング

IGMP スヌーピングは、レイヤ 2 LAN スイッチで実行される IP マルチキャスト抑制メカニズムです。IGMP スヌーピングでは、ホストとルータとの間で送信される IGMP パケットで、一部のレイヤ 3 情報 (IGMP Join/Leave メッセージ) を調査、すなわち「スヌープ」します。スイッチでは、特定のマルチキャストグループに対するホストから IGMP ホストレポートを受信するときに、関連付けられているマルチキャストテーブルエントリにホストのポート番号が追加されます。スイッチがホストから IGMP グループ脱退メッセージを受信すると、スイッチはホストのテーブルエントリを削除します。

IGMP 制御メッセージはマルチキャストパケットとして送信されるので、レイヤ 2 ではマルチキャストデータと区別できません。IGMP スヌーピングを実行しているスイッチでは、各マルチキャストデータパケットを検査し、永続的な IGMP コントロール情報が含まれているかどうかを特定できます。低速の CPU を搭載したローエンドのスイッチに IGMP スヌーピングを実装すると、データが高速で送信される場合に、パフォーマンスに重大な影響を与える可能性があります。解決策として、ハードウェアで IGMP チェックを実行できる特別な ASIC (特定用途向け集積回路) を備えたハイエンドのスイッチに IGMP スヌーピングを実装します。CGMP は特別なハードウェアを使用しない、ローエンドのスイッチのための新しいオプションです。

Router-Port Group Management Protocol (RGMP)

CGMP および IGMP スヌーピングは、アクティブなレシーバがあるルーティング対象ネットワークセグメントで動作するように設計されている、IP マルチキャスト抑制メカニズムです。両方とも、ホストとルータとの間で送信される IGMP コントロールメッセージに依存して、該当する受信先に接続されているスイッチポートが特定されます。

スイッチドイーサネットバックボーンネットワークセグメントは、通常、そのセグメント上にホストなしでスイッチに接続されているいくつかのルータで構成されています。ルータでは IGMP ホストレポートが生成されないため、CGMP および IGMP スヌーピングによって、マルチキャストトラフィックを抑制することができず、VLAN 上の各ポートにフラッディングされます。ルータでは、代わりに、Protocol Independent Multicast (PIM) メッセージが生成され、レイヤ 3 レベルで、マルチキャストトラフィックフローに加入またはマルチキャストトラフィックフローがプルーニングされます。

Router-Port Group Management Protocol (RGMP) は、ルータのみのネットワークセグメントに対する、IP マルチキャスト抑制メカニズムです。RGMP は、ルータ上およびレイヤ 2 スイッチ上でイネーブルにする必要があります。マルチキャストルータは、特定のグループに RGMP Join メッセージを送信することによって、データフローを受信したいことを示します。次に、CGMP Join メッセージの処理方法と同様に、スイッチによって、そのマルチキャストグループに対する転送テーブルに、適切なポートが追加されます。IP マルチキャストデータフローは、

関連するルータポートにのみ転送されます。ルータがそのデータフローを必要としなくなった場合、RGMP Leave メッセージを送信し、スイッチは転送エントリを削除します。

RGMP 対応されていないルータがある場合は、すべてのマルチキャストデータを受信し続けます。

スイッチドイーサネットネットワークでマルチキャストを抑制する例

IP マルチキャスト用のスイッチの設定

マルチキャストネットワークにスイッチングがある場合、IP マルチキャストの設定方法の詳細については、使用しているスイッチのマニュアルを参照してください。

IGMP スヌーピングの設定

ルータ上での設定は不要です。使用しているスイッチで IGMP スヌーピングをイネーブルにする方法についてはドキュメントを参照し、提示された手順に従ってください。

CGMP のイネーブル化

CGMP は、IGMP によって実行される作業と同様の作業を実行するために、Catalyst スイッチに接続されたデバイス上で使用されるプロトコルです。CGMP が必要となるのは、Catalyst スイッチで IP マルチキャストデータパケットと IGMP レポートメッセージを区別できないためです。これらはともに MAC レベルで、同じグループアドレスにアドレス指定されます。



- (注)
- CGMP は 802 または ATM メディア、または ATM 経由の LAN エミュレーション (LANE) でのみイネーブルにする必要があります。
 - CGMP は、Catalyst スイッチに接続されているデバイス上でのみ、イネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number 例 : Device(config)# interface ethernet 1	IGMPv3 をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 4	ip cgmp [proxy router-only] 例 : Device(config-if)# ip cgmp proxy	Cisco Catalyst 5000 ファミリ スイッチに接続されているデバイスのインターフェイス上で CGMP をイネーブルにします。 <ul style="list-style-type: none"> • proxy キーワードは、CGMP プロキシ機能をイネーブルにします。イネーブルにすると、CGMP 対応でないデバイスがプロキシルータによってアドバタイズされます。プロキシルータでは、非 CGMP 対応デバイスの MAC アドレスおよびグループアドレス 0000.0000.0000 が使用されている CGMP Join メッセージを送信することによって、他の非 CGMP 対応デバイスの存在がアドバタイズされます。
ステップ 5	end 例 : Device(config-if)# end	現在のコンフィギュレーションセッションを終了して、EXEC モードに戻ります。
ステップ 6	clear ip cgmp [interface-type interface-number] 例 : Device# clear ip cgmp	(任意) Catalyst スイッチのキャッシュからすべてのグループ エントリをクリアします。

レイヤ2スイッチドイーサネットネットワークでの IP マルチキャストの設定

RGMP を使用してレイヤ2スイッチドイーサネットネットワークで IP マルチキャストを設定するには、この作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number 例： Device(config)# interface ethernet 1	ホストに接続されているインターフェイスを選択します。
ステップ 4	ip rgmp 例： Device(config-if)# ip rgmp	イーサネット インターフェイス、ファストイーサネット インターフェイス、およびギガビットイーサネット インターフェイスで、RGMP をイネーブルにします。
ステップ 5	end 例： Device(config-if)# end	現在のコンフィギュレーションセッションを終了して、EXEC モードに戻ります。
ステップ 6	debug ip rgmp 例： Device# debug ip rgmp	（任意）RGMP 対応デバイスによって送信されたデバッグ メッセージを記録します。
ステップ 7	show ip igmp interface 例： Device# show ip igmp interface	（任意）インターフェイスに関するマルチキャスト関連情報を表示します。

スイッチドイーサネットネットワークで IP マルチキャストを抑制する設定例

RGMP の設定例

次に、ルータ上で RGMP を設定する方法の例を示します。

```
ip multicast-routing
ip pim sparse-mode
interface ethernet 0
 ip rgmp
```

スイッチドイーサネットネットワークでの IP マルチキャスト抑制に関するその他の参考資料

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャストルーティングのコマンド」の項を参照してください。 <i>Command Reference (Catalyst 9200 Series Switches)</i>

MIB

MIB	MIB のリンク
これらの機能によってサポートされる新しい MIB または変更された MIB はありません。またこれらの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャセットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

スイッチドイーサネットでの IP マルチキャスト抑制の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	スイッチドイーサネットでの IP マルチキャストの抑制	スイッチドイーサネットでの IP マルチキャストでは、不要なマルチキャストトラフィックを減らす抑制メカニズムが提供され、スイッチのパフォーマンスが向上します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 7 章

PIM（Protocol Independent Multicast）の設定

- PIM の前提条件（135 ページ）
- PIM に関する制約事項（136 ページ）
- PIM に関する情報（139 ページ）
- PIM の設定方法（155 ページ）
- PIM の動作の確認（185 ページ）
- PIM のモニタリングとトラブルシューティング（194 ページ）
- PIM の設定例（197 ページ）
- PIM 機能の履歴（200 ページ）

PIM の前提条件

PIM 設定プロセスを開始する前に、使用する PIM モードを決定します。この決定は、ネットワーク上でサポートするアプリケーションに基づきます。次の注意事項に従ってください。

- 一般に、本質的に 1 対多または多対多アプリケーションでは PIM-SM を正常に使用できません。
- 1 対多アプリケーションで最適なパフォーマンスを得るには、SSM が適しています。ただし、IGMP バージョン 3 サポートが必要です。

PIM スタブルルーティングを設定する前に、次の条件を満たしていることを確認します。

- スタブルータと中央のルータの両方に IP マルチキャストルーティングが設定されている必要があります。スタブルータのアップリンク インターフェイスで、PIM モードの設定も必要です。
- また、デバイスに Enhanced Interior Gateway Routing Protocol（EIGRP）スタブルルーティングまたは Open Shortest Path First（OSPF）スタブルルーティングが設定されている必要があります。

- PIM スタブルータは、ディストリビューション ルータ間の伝送トラフィックのルーティングは行いません。ユニキャスト (EIGRP) スタブルーティングではこの動作が強制されます。PIM スタブルータの動作を支援するためにユニキャスト スタブルーティングを設定する必要があります。

PIM に関する制約事項

次に、PIM を設定する際の制約事項を示します。

- ACLにより、指定のポートをマルチキャストルータポートではなく、マルチキャストホストポートとしてだけ指定できます。このポートで受信されたマルチキャストルータ制御パケットは、ドロップされます。
- PIM非ブロードキャストマルチアクセス (NBMA) モードは、イーサネットインターフェイスではサポートされません。
- Hot Standby Router Protocol (HSRP) 対応の PIM がサポートされます。

PIMv1 および PIMv2 の相互運用性

デバイス上でのマルチキャストルーティングの設定ミスを回避するには、ここに記載する情報を確認してください。

シスコの PIMv2 実装を使用すると、バージョン 1 とバージョン 2 間での相互運用性および変換が可能となります。ただし、若干の問題が発生する場合があります。

PIMv2 に差別的にアップグレードできます。PIM バージョン 1 および 2 を、1つのネットワーク内の異なるルータおよびマルチレイヤスイッチに設定できます。内部的には、共有メディアネットワーク上のすべてのルータおよびマルチレイヤスイッチで同じ PIM バージョンを実行する必要があります。したがって、PIMv2 デバイスが PIMv1 デバイスを検出した場合は、バージョン 1 デバイスがシャットダウンするかアップグレードされるまで、バージョン 2 デバイスはバージョン 1 にダウングレードされます。

PIMv2 は BSR を使用して各グループプレフィックスの RP 設定情報を検出し、PIM ドメイン内のすべてのルータおよびマルチレイヤスイッチにアナウンスします。自動 RP 機能を組み合わせることにより、PIMv2 BSR と同じ作業を PIMv1 で実行できます。ただし、自動 RP は PIMv1 から独立している、スタンドアロンのシスコ独自のプロトコルで、PIMv2 は IETF 標準の追跡プロトコルです。



(注) したがって、PIMv2 の使用を推奨します。BSR 機能は、Cisco ルータおよびマルチレイヤスイッチ上の Auto-RP と相互運用します。

PIMv2 デバイスを PIMv1 デバイスと相互運用させる場合は、自動 RP を事前に導入しておく必要があります。自動 RP マッピング エージェントでもある PIMv2 BSR は、自動 RP で選択され

た RP を自動的にアドバタイズします。つまり、自動 RP によって、グループ内のルータまたはマルチレイヤごとに 1 つの RP が設定されます。ドメイン内のルータおよびスイッチの中には、複数の RP を選択するために PIMv2 ハッシュ機能を使用しないものもあります。

PIMv1 の自動 RP 機能は PIMv2 RP 機能と相互運用するため、PIMv1 と PIMv2 が混在する領域内に SM グループを設定できます。すべての PIMv2 デバイスで PIMv1 を使用できますが、RP を PIMv2 にアップグレードすることを推奨します。PIMv2 への移行を簡単に行うには、以下を推奨します。

- 領域全体で Auto-RP を使用します。

自動 RP がまだ PIMv1 領域に設定されていない場合は、自動 RP を設定してください。

PIM スタブルルーティングの設定に関する制約事項

- 直接接続されたマルチキャスト (IGMP) レシーバおよび送信元だけが、レイヤ 2 アクセスドメインで許可されます。アクセスドメインでは、PIM プロトコルはサポートされません。
- PIM スタブルルーティングを使用するネットワークでは、ユーザーに対する IP トラフィックの唯一の許容ルートは、PIM スタブルルーティングを設定しているデバイス経由です。
- 冗長 PIM スタブルルータ トポロジはサポートされません。PIM スタブ機能では、非冗長アクセスルータ トポロジだけがサポートされます。

Auto-RP および BSR の設定に関する制約事項

Auto-RP および BSR を設定する場合は、ネットワーク設定と次の制約事項を考慮してください。

Auto-RP の制約事項

次に、Auto-RP の設定に関する制約事項を示します (ネットワーク設定で使用する場合)。

- ルーテッドインターフェイスが SM に設定されていると、すべてのデバイスが自動 RP グループの手動 RP アドレスによって設定されている場合も、自動 RP を使用できます。
- ルーテッドインターフェイスが SM で設定され、`ip pim autorp listener` グローバルコンフィギュレーション コマンドを入力する場合、すべてのデバイスが Auto-RP グループの手動 RP アドレスを使用して設定されていなくても、Auto-RP は引き続き使用できます。

BSR 設定の制約事項

次に、BSR の設定に関する制約事項を示します (ネットワーク設定で使用する場合)。

- 候補 BSR を自動 RP 用の RP マッピング エージェントとして設定します。
- グループプレフィックスが自動 RP によってアドバタイズされた場合は、異なる RP セットによって処理されたこれらのグループプレフィックスのサブ範囲が、PIMv2 BSR メカ

ニズムによってアドバタイズされないようにする必要があります。PIMv1 および PIMv2 ドメインが混在する環境では、バックアップ RP で同じグループプレフィックスが処理されるように設定します。このようにすると、RP マッピング データベースの最長一致検索によって、PIMv2 DR はこれらの PIMv1 DR から異なる RP を選択できなくなります。

Auto-RP および BSR の注意事項と制限事項

次に、Auto-RP および BSR の設定に関する制約事項を示します（ネットワーク設定で使用する場合）。

- 使用しているネットワークがすべて Cisco ルータおよびマルチレイヤスイッチである場合は、自動 RP または BSR のいずれかを使用できます。
- ネットワークに他社製のルータがある場合は、BSR を使用する必要があります。
- Cisco PIMv1 および PIMv2 ルータとマルチレイヤスイッチ、および他社製のルータがある場合は、自動 RP と BSR の両方を使用する必要があります。ネットワークに他のベンダー製のルータが含まれる場合には、シスコの PIMv2 デバイス上に自動 RP マッピング エージェントと BSR を設定します。BSR と他社製の PIMv2 デバイス間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。



(注) PIMv2 は 2 つの方法で使用できます。1 つはバージョン 2 をネットワーク内で排他的に使用する方法、もう 1 つは PIM バージョンの混在環境を採用してバージョン 2 に移行する方法です。

- ブートストラップ メッセージはホップ単位で送信されるため、PIMv1 デバイスの場合、これらのメッセージはネットワーク内の一部のルータおよびマルチレイヤスイッチに到達しません。このため、ネットワーク内に PIMv1 デバイスがあり、Cisco ルータおよびマルチレイヤスイッチだけが存在する場合は、自動 RP を使用してください。
- ネットワーク内に他社製のルータが存在する場合は、Cisco PIMv2 ルータまたはマルチレイヤスイッチに自動 RP マッピング エージェントおよび BSR を設定します。BSR と他社製の PIMv2 ルータ間のパス上に、PIMv1 デバイスが配置されていないことを確認してください。
- シスコ PIMv1 ルータおよびマルチレイヤスイッチと他社製の PIMv2 ルータを相互運用させる場合は、自動 RP と BSR の両方が必要です。シスコ PIMv2 デバイスを、自動 RP マッピング エージェントと BSR の両方に設定してください。

Auto-RP 拡張の制約事項

Auto-RP とブートストラップ ルータ (BSP) の同時配備はサポートされていません。

PIMに関する情報

Protocol Independent Multicast の概要

PIM (Protocol Independent Multicast) プロトコルは、受信側が開始したメンバーシップの現在の IP マルチキャスト サービス モードを維持します。PIM は、特定のユニキャストルーティングプロトコルに依存しません。つまり、IP ルーティングプロトコルに依存せず、ユニキャストルーティングテーブルへの入力に使用されるユニキャストルーティングプロトコル

(Enhanced Interior Gateway Routing Protocol (EIGRP)、Open Shortest Path First (OSPF)、およびスタティックルート) のいずれも利用できます。PIM は、ユニキャストルーティング情報を使用してマルチキャスト転送機能を実行します。

PIM はマルチキャストルーティングテーブルと呼ばれていますが、実際には完全に独立したマルチキャストルーティングテーブルを作成する代わりに、ユニキャストルーティングテーブルを使用してリバースパスフォワーディング (RPF) チェック機能を実行します。他のルーティングプロトコルとは異なり、PIM はルータ間のルーティングアップデートを送受信しません。

PIMは、RFC 4601 の Protocol Independent Multicast - Sparse Mode (PIM-SM) で定義されています。

PIM のバージョン

PIMv2 は、PIMv1 と比べて次の点が改善されています。

- マルチキャストグループごとに、複数のバックアップランデブーポイント (RP) を持つアクティブな RP が 1 つ存在します。この単一の RP で、PIMv1 内の同じグループにアクティブな RP が複数ある場合と同様の処理を行います。
- ブートストラップルータ (BSP) は耐障害性のある、自動化された RP ディスカバリメカニズム、および配信機能を提供します。これらの機能により、ルータおよびマルチレイヤスイッチはグループ/RP マッピングを動的に取得できます。
- PIM の Join メッセージおよびプルーニングメッセージを使用すると、複数のアドレスファミリーを柔軟に符号化できます。
- 現在以降の機能オプションを符号化するため、クエリーパケットではなく、より柔軟な hello パケット形式が使用されています。
- RP に送信される登録メッセージが、境界ルータによって送信されるか、あるいは指定ルータによって送信されるかを指定します。
- PIM パケットは IGMP パケット内に格納されず、独立したパケットとして処理されます。

Multicast Source Discovery Protocol (MSDP)

Multicast Source Discovery Protocol (MSDP) は、PIM SM を使用する場合のドメイン間送信元検出に使用されます。各 PIM 管理ドメインには独自の RP があります。あるドメイン内の RP が他のドメイン内の RP に新しい送信元を信号で伝えるために、MSDP が使用されます。

MSDP が設定されている状態で、あるドメイン内の RP が新しい送信元の PIM 登録メッセージを受信すると、その RP は、新しい Source-Active (SA) メッセージを他のドメイン内のすべての MSDP ピアに送信します。それぞれの中間 MSDP ピアは、この SA メッセージを発信側の RP から離してフラディングします。MSDP ピアは、この SA メッセージを自身の MSDP sa-cache にインストールします。他のドメイン内の RP が SA メッセージに記述されているグループへの加入要求を持っている場合（空でない発信インターフェイスリストで (*,G) エントリが存在することで示される）、そのグループはドメインの対象となり、RP から送信元方向に (S,G) Join メッセージが送信されます。

PIM スパース モード (PIM-SM)

PIM スパース モード (PIM-SM) は、プル モデルを使用してマルチキャストトラフィックを配信します。明示的にデータを要求したアクティブなレシーバを含むネットワークセグメントだけがトラフィックを受信します。

スパースモードのインターフェイスは、ダウンストリームのルータから定期的に参加メッセージを受信する場合またはインターフェイスに直接接続のメンバがある場合のみマルチキャストルーティングテーブルに追加されます。LAN から転送する場合、グループが認識している RP があれば、SM 動作が行われます。その場合、パケットはカプセル化され、その RP に送信されます。特定のソースからのマルチキャストトラフィックが十分である場合、レシーバのファーストホップルータは、ソースベースのマルチキャスト配信ツリーを構築するために参加メッセージをソースに向けて送信できます。

PIM-SM は、共有ツリー上のデータパケットを転送することによって、アクティブな送信元に関する情報を配布します。PIM-SM は少なくとも最初は共有ツリーを使用するので、ランデブーポイント (RP) を使用する必要があります。RP は管理上ネットワークで設定されている必要があります。詳細については、[ランデブーポイント \(142 ページ\)](#) を参照してください。

スパースモードでは、ルータは、トラフィックに対する明示的な要求がない限り、他のルータはグループのマルチキャストパケットを転送しないと見なします。ホストがマルチキャストグループに加入すると、直接接続されたルータは RP に PIM 参加メッセージを送信します。RP はマルチキャストグループを追跡します。マルチキャストパケットを送信するホストは、そのホストのファーストホップルータによって RP に登録されます。その後、RP は、ソースに参加メッセージを送信します。この時点で、パケットが共有配信ツリー上で転送されます。特定のソースからのマルチキャストトラフィックが十分である場合、ホストのファーストホップルータは、ソースベースのマルチキャスト配信ツリーを構築するために参加メッセージをソースに向けて送信できます。

送信元が RP に登録され、データは共有ツリーを下ってレシーバに転送されます。エッジルータは、RP を介してソースから共有ツリーでデータパケットを受信するときに、そのソースについて学習します。次に、エッジルータは、そのソースに向けて PIM (S,G) 参加メッセージを送信します。リバースパスに沿った各ルータは、RP アドレスのユニキャストルーティングメ

トリックをソースアドレスのメトリックと比較します。送信元アドレスのメトリックの方が良い場合は、ソースに向けて PIM (S, G) 加入メッセージを転送します。RP のメトリックと同じ、または RP のメトリックの方が良い場合は、RP と同じ方向に PIM (S, G) 加入メッセージが送信されます。この場合、共有ツリーとソース ツリーは一致すると見なされます。

共有ツリーがソースとレシーバの間の最適なパスでない場合、ルータは動的にソースツリーを作成し、共有ツリーの下方向へのトラフィックフローを停止します。この動作は、ソフトウェアのデフォルトの動作です。ネットワーク管理者は、**ip pim spt-threshold infinity** コマンドを使用して、トラフィックを強制的に共有ツリー上で保持することができます。

PIM-SM は、WAN リンク付きのネットワークを含む、任意のサイズのネットワークに合わせて拡大または縮小します。明示的な加入メカニズムによって、不要なトラフィックが WAN リンクでフラディングするのを防ぎます。

PIM スタブルルーティング

PIM スタブルルーティング機能は、すべてのデバイス ソフトウェア イメージで使用でき、エンドユーザーの近くにルーテッドトラフィックを移動することでリソースの使用状況を低減させます。

PIM スタブルルーティング機能は、ディストリビューション レイヤとアクセス レイヤの間のマルチキャストルーティングをサポートします。サポート対象の PIM インターフェイスは、アップリンク PIM インターフェイスと PIM パッシブ インターフェイスの 2 種類です。PIM パッシブ モードに設定されているルーテッド インターフェイスは、PIM 制御トラフィックの通過も転送も行いません。通過させたり転送したりするのは IGMP トラフィックだけです。

PIM スタブルルーティングを使用するネットワークでは、ユーザーに対する IP トラフィックの唯一の許容ルートは、PIM スタブルルーティングを設定しているデバイス経由です。PIM 受動インターフェイスは、VLAN などのレイヤ 2 アクセス ドメイン、または他のレイヤ 2 デバイスに接続されているインターフェイスに接続されます。直接接続されたマルチキャスト (IGMP) レシーバおよび送信元だけが、レイヤ 2 アクセス ドメインで許可されます。PIM 受動インターフェイスは、受信した PIM 制御パケットを送信または処理しません。

PIM スタブルルーティングを使用しているときは、IP マルチキャストルーティングを使用し、デバイスだけを PIM スタブルルーターとして設定するように、分散ルーターおよびリモートルーターを設定する必要があります。デバイスは分散ルーター間の伝送トラフィックをルーティングしません。デバイスのルーテッドアップリンク ポートも設定する必要があります。SVI の場合は、デバイスのアップリンクポートを使用できません。SVI アップリンク ポートの PIM が必要な場合は、Network Advantage ライセンスにアップグレードする必要があります。



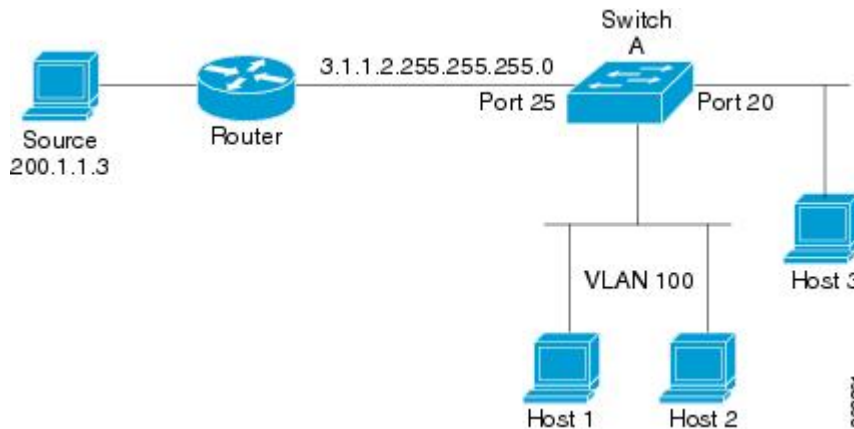
- (注) また、デバイスで PIM スタブルルーティングを設定するときは、EIGRP スタブルルーティングも設定する必要があります。

冗長 PIM スタブルルーター トポロジはサポートされません。単一のアクセス ドメインにマルチキャスト トラフィックを転送している複数の PIM ルーターがある場合、冗長 トポロジが存在します。PIM メッセージはブロックされ、PIM 資産および指定ルーター検出メカニズムは、PIM

受動インターフェイスでサポートされません。PIM スタブ機能では、非冗長アクセスルータトポロジーだけがサポートされます。非冗長トポロジーを使用することで、PIM 受動インターフェイスはそのアクセスドメインで唯一のインターフェイスおよび指定ルータであると想定します。

図 10: PIM スタブルータ設定

次の図では、デバイス A のルーテッドアップリンク ポート 25 がルータに接続され、PIM スタブルーティングが VLAN 100 インターフェイスとホスト 3 で有効になっています。この設定により、直接接続されたホストはマルチキャスト発信元 200.1.1.3 からトラフィックを受信できます。



ランデブーポイント

ランデブーポイント (RP) は、デバイスが PIM (Protocol Independent Multicast) スパースモード (SM) で動作している場合にデバイスが実行するロールです。RP が必要になるのは、PIM SM を実行しているネットワークだけです。PIM-SM モデルでは、マルチキャストデータを明示的に要求したアクティブなレシーバを含むネットワークセグメントだけにトラフィックが転送されます。

RP は、マルチキャストデータのソースとレシーバの接点として機能します。PIM SIM ネットワークでは、ソースが RP にトラフィックを送信する必要があります。このトラフィックは、それから共有配信ツリーを下ってレシーバに転送されます。デフォルトでは、レシーバのファーストホップデバイスがソースを認識すると、ソースに Join メッセージを直接送信し、ソースからレシーバへのソースベースの配信ツリーを作成します。ソースとレシーバ間の最短パス内に RP が配置されていない限り、このソースツリーに RP は含まれません。

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

Auto-RP

PIM-SMの最初のバージョンでは、すべてのリーフルータ（ソースまたはレシーバに直接接続されたルータ）は、RPのIPアドレスを使用して手動で設定する必要がありました。このような設定は、スタティックRP設定とも呼ばれます。スタティックRPの設定は、小規模のネットワークでは比較的容易ですが、大規模で複雑なネットワークでは困難を伴う可能性があります。

PIM-SMバージョン1の導入に続き、シスコは、Auto-RP機能を備えたPIM-SMのバージョンを実装しました。Auto-RPは、PIMネットワークにおけるグループからRPへのマッピングの配信を自動化します。Auto-RPには、次の利点があります。

- さまざまなグループにサービスを提供するために、ネットワーク内で複数のRPを設定することが比較的容易です。
- Auto-RPでは、複数のRP間で負荷を分散し、グループに加入するホストの場所に従ってRPを配置できます。
- Auto-RPにより、接続の問題の原因となる、矛盾した手動RP設定を回避できます。

複数のRPを使用して、異なるグループ範囲にサービスを提供したり、互いにバックアップとしての役割を果たしたりできます。Auto-RPが機能するためには、RP通知メッセージをRPから受信して競合を解決するRPマッピングエージェントとしてルータが指定されている必要があります。その場合、RPマッピングエージェントは、グループからRPへの一貫したマッピングを他のすべてのルータに送信します。これにより、すべてのルータは、サポート対象のグループに使用するRPを自動的に検出します。



- (注) ルータ インターフェイスがスパス モードに設定されている場合、Auto-RP グループに対してすべてのルータが1つのスタティックアドレスで設定されているときは、引き続きAuto-RP グループを使用できます。

Auto-RPが機能するためには、RP通知メッセージをRPから受信して競合を解決するRPマッピングエージェントとしてルータが指定されている必要があります。これにより、すべてのルータは、サポート対象のグループに使用するRPを自動的に検出します。インターネット割り当て番号局 (IANA) は、224.0.1.39 と 224.0.1.40 という2つのグループアドレスをAuto-RP用に割り当てています。Auto-RPの利点の1つは、指定したRPに対するすべての変更は、RPであるルータ上で設定するだけで、リーフルータ上で設定する必要がないことです。Auto-RPのもう1つの利点は、ドメイン内でRPアドレスの範囲を設定する機能を提供することです。スコーピングを設定するには、Auto-RPアドバタイズメントに許容されている存続可能時間 (TTL) 値を定義します。

RPの各設定方式には、それぞれの長所、短所、および複雑度のレベルがあります。従来のIPマルチキャストネットワークシナリオにおいては、Auto-RPを使用してRPを設定することを推奨します。Auto-RPは、設定が容易で、十分にテストされており、安定しているためです。代替の方法として、スタティックRP、Auto-RP、およびブートストラップルータを使用してRPを設定することもできます。

PIM ネットワークでの Auto-RP の役割

Auto-RP は、PIM ネットワークにおけるグループからランデブーポイント (RP) へのマッピングの配信を自動化します。Auto-RP が機能するためには、RP アナウンスメントメッセージを RP から受信して競合を解決する RP マッピング エージェントとしてデバイスが指定されている必要があります。

これにより、すべてのルータは、サポート対象のグループに使用する RP を自動的に検出します。インターネット割り当て番号局 (IANA) は、224.0.1.39 と 224.0.1.40 という 2 つのグループアドレスを Auto-RP 用に割り当てています。

マッピング エージェントは、Candidate-RP から RP になる意図の通知を受信します。その後、マッピング エージェントが RP 選定の結果を通知します。この通知は、他のマッピング エージェントによる決定とは別に行われます。

マルチキャスト境界

管理用スコープの境界を使用し、ドメインまたはサブドメイン外部へのマルチキャストトラフィックの転送を制限できます。この方法では、「管理用スコープのアドレス」と呼ばれる特殊なマルチキャストアドレス範囲が境界のメカニズムとして使用されます。管理用スコープの境界をルーテッドインターフェイスに設定すると、マルチキャストグループアドレスがこの範囲内にあるマルチキャストトラフィックは、このインターフェイスに出入りできず、このアドレス範囲内のマルチキャストトラフィックに対するファイアウォール機能が提供されます。

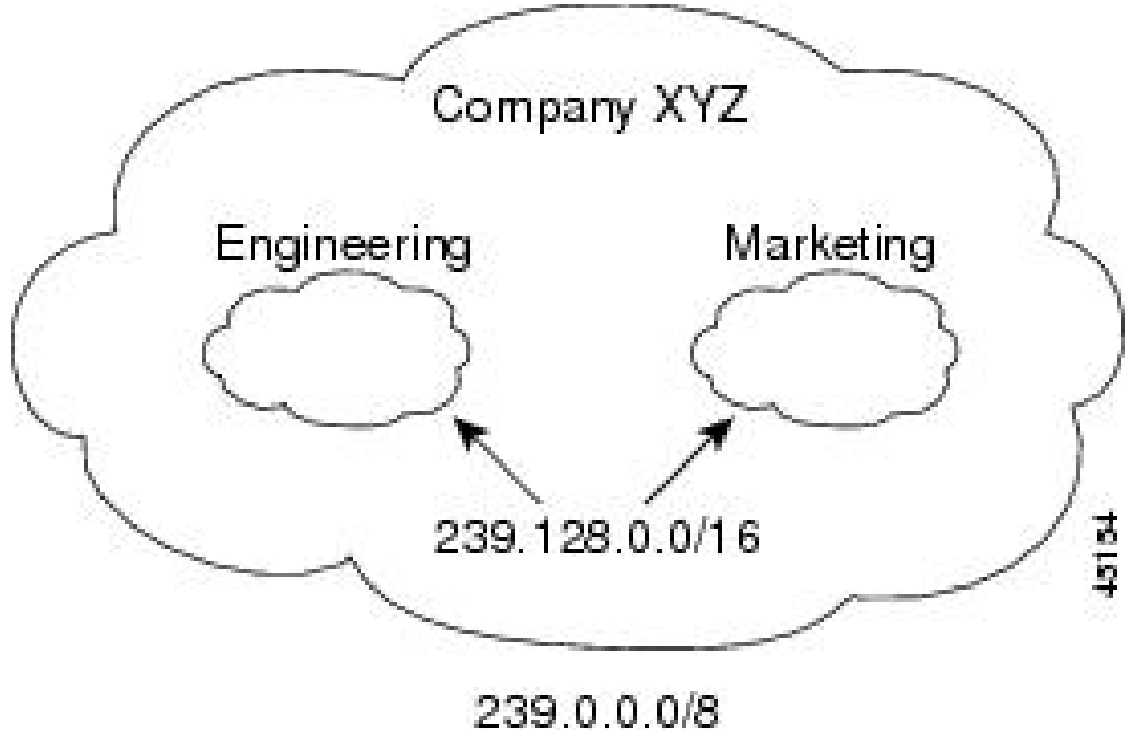


- (注) マルチキャスト境界および TTL しきい値は、マルチキャストドメインの有効範囲を制御しますが、TTL しきい値はこのデバイスではサポートされていません。ドメインまたはサブドメイン外部へのマルチキャストトラフィックの転送を制限するには、TTL しきい値でなくマルチキャスト境界を使用する必要があります。

図 11: 管理用スコープの境界

次の図に、XYZ社が自社ネットワーク周辺にあるすべてのルーテッドインターフェイス上で、管理用スコープの境界をマルチキャストアドレス範囲 239.0.0.0/8 に設定した例を示します。この境界では、239.0.0.0～239.255.255.255 の範囲のマルチキャストトラフィックはネットワークに入ったり、外へ出ることができません。同様に、エンジニアリング部およびマーケティング部では、各自のネットワークの周辺で、管理用スコープの境界を 239.128.0.0/16 に設定しました。この境界では、239.128.0.0～239.128.255.255 の範囲のマルチキャストトラフィックは、

それぞれのネットワークに入ったり、外部に出ることができません。



マルチキャストグループアドレスに対して、ルーテッドインターフェイス上に管理用スコープの境界を定義できます。影響を受けるアドレス範囲は、標準アクセスリストによって定義されます。この境界が定義されている場合、マルチキャストデータパケットはいずれの方向であっても境界を通過できません。境界を定めることで、同じマルチキャストグループアドレスをさまざまな管理ドメイン内で使用できます。

IANA は、マルチキャストアドレス範囲 239.0.0.0 ~ 239.255.255.255 を管理用スコープのアドレスとして指定しました。このアドレス範囲は、異なる組織によって管理されたドメイン内で再利用できます。このアドレスはグローバルではなく、ローカルで一意であるとみなされません。

filter-autorp キーワードを設定して、管理用スコープの境界で Auto-RP 検出と通知メッセージを検査し、フィルタできます。境界のアクセスコントロールリスト (ACL) に拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

Auto-RP のスパース-デンス モード

Auto-RP の前提条件として、**ip pim sparse-dense-mode** インターフェイス コンフィギュレーション コマンドを使用してすべてのインターフェイスをスパース-デンスモードで設定する必要があります。スパース-デンスモードで設定されたインターフェイスは、マルチキャストグループの動作モードに応じてスパースモードまたはデンスモードで処理されます。マルチキャストグループ内に既知の RP が存在する場合、インターフェイスはスパースモードで処理されま

す。グループ内に既知の RP が存在しない場合、デフォルトでは、インターフェイスはデンスモードで処理され、このインターフェイス上にデータがフラッディングされます (デンスモードフォールバックを回避することもできます。「Configuring Basic IP Multicast」モジュールを参照してください)。

Auto-RP を正常に実装し、224.0.1.39 および 224.0.1.40 以外のグループがデンスモードで動作することを回避するには、「シンク RP」 (「ラストリゾート RP」とも呼ばれます) を設定することを推奨します。シンク RP は、ネットワーク内に実際に存在するかどうかわからない静的に設定された RP です。デフォルトでは、Auto-RP メッセージはスタティック RP 設定よりも優先されるため、シンク RP の設定は Auto-RP の動作と干渉しません。未知のソースや予期しないソースをアクティブにできるため、ネットワーク内の可能なすべてのマルチキャストグループにシンク RP を設定することを推奨します。ソースの登録を制限するように設定された RP がない場合は、グループがデンスモードに戻り、データがフラッディングされる可能性があります。

Auto-RP のメリット

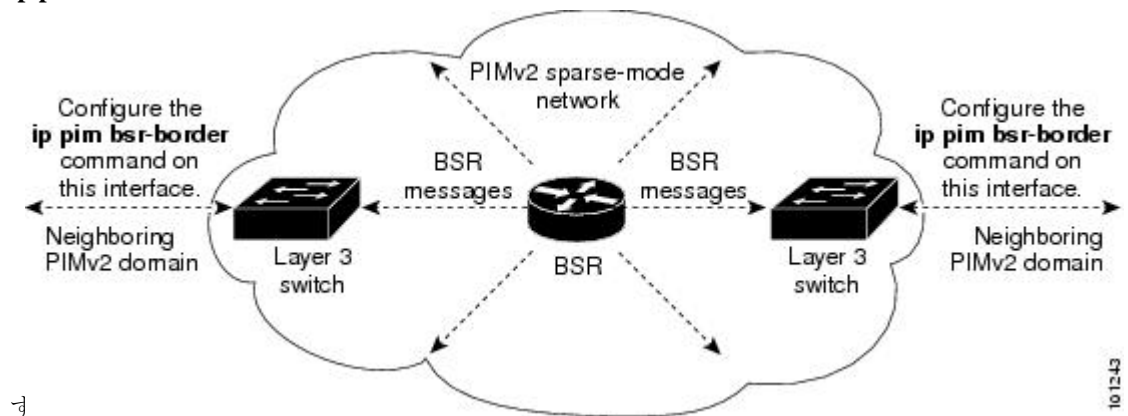
PIM ネットワークでの Auto-RP の利点

- Auto-RP では、RP 指定に対するすべての変更を、RP であるデバイス上でのみ設定されるようにし、リーフルータ上では設定されないようにすることができます。
- Auto-RP には、ドメイン内の RP アドレスの範囲を設定する機能があります。

PIM ドメイン境界

IP マルチキャストの普及に伴い、PIMv2 ドメインと別の PIMv2 ドメインが境界を挟んで隣接するケースが増えています。2つのドメインは同じ RP、BSR、候補 RP、候補 BSR のセットを共有していないことが多いため、PIMv2 BSR メッセージがドメインの内外に流れないようにする必要があります。メッセージのドメイン境界通過を許可すると、通常の BSR 選択メカニズムに悪影響が及んだり、境界に位置するすべてのドメインで単一の BSR が選択されたり、候補 RP アドバタイズメントが混在し、間違っただメイン内で RP が選択されたりします。

ip pim bsr-border コマンドを使用して PIM ドメインの境界を設定する方法を次の図に示しま



す。

PIMv2 ブートストラップルータ

PIMv2 ブートストラップルータ (BSR) は、グループ/RP マッピング情報をネットワーク内のすべての PIM ルータおよびマルチレイヤデバイスに配信する別の方法です。これにより、ネットワーク内のルータまたはスイッチごとに RP 情報を手動で設定する必要がなくなります。ただし、BSR は IP マルチキャストを使用してグループ/RP マッピング情報を配信する代わりに、特殊な BSR メッセージをホップ単位でフラッディングしてマッピング情報を配信します。

BSR は、BSR として機能するように設定されたドメイン内の一連の候補ルータおよびスイッチから選択されます。選択メカニズムは、ブリッジされた LAN で使用されるルートブリッジ選択メカニズムと類似しています。BSR の選択メカニズムの基準は、ネットワークを経由してホップ単位で送信される BSR メッセージに格納されている、デバイスの BSR プライオリティです。各 BSR デバイスは BSR メッセージを調べ、自身の BSR プライオリティよりも BSR プライオリティが同等以上で、BSR IP アドレスが大きなメッセージだけを、すべてのインターフェイスから転送します。この方法によって、BSR が選択されます。

選択された BSR によって、TTL 値が 1 である BSR メッセージが送信されます。隣接する PIMv2 ルータまたはマルチレイヤデバイスは BSR メッセージを受信し、TTL 値が 1 である他のすべてのインターフェイス (BSR メッセージの着信インターフェイスを除く) にマルチキャストします。この方法で、BSR メッセージは PIM ドメイン内をホップ単位で移動します。BSR メッセージには現在の BSR の IP アドレスが格納されているため、候補 RP はフラッディングメカニズムを使用し、どのデバイスが選択された BSR であるかを自動的に学習します。

候補 RP は候補 RP アドバタイズメントを送信し、対象となるグループ範囲を BSR に指示します。この情報は、ローカルな候補 RP キャッシュに格納されます。BSR はドメイン内の他のすべての PIM デバイスに、BSR メッセージ内のこのキャッシュの内容を定期的にあドバタイズします。これらのメッセージはネットワークをホップ単位で移動し、すべてのルータおよびスイッチに送信されます。BSR メッセージ内の RP 情報は、到達したルータおよびスイッチのローカルな RP キャッシュに格納されます。すべてのルータおよびスイッチには一般的な RP ハッシュアルゴリズムが使用されるため、指定されたグループには同じ RP が選択されます。

マルチキャスト転送

マルチキャストトラフィックの転送は、マルチキャスト対応ルータによって行われます。このようなルータは、すべてのレシーバにトラフィックを配信するために、IP マルチキャストがネットワーク上でたどるパスを制御する配信ツリーを作成します。

マルチキャストトラフィックは、すべてのソースをグループ内のすべてのレシーバに接続する配信ツリー上で、ソースからマルチキャストグループに流れます。このツリーは、すべてのソースで共有できます (共有ツリー)。または、各ソースに個別の配信ツリーを作成することもできます (ソース ツリー)。共有ツリーは一方向または双方向です。

ソース ツリーと共有ツリーの構造を説明する前に、マルチキャストルーティングテーブルで使用される表記について触れておきます。これらの表記には次のものが含まれます。

- (S, G) = (マルチキャストグループ G のユニキャスト ソース, マルチキャストグループ G)
- (*, G) = (マルチキャストグループ G のすべてのソース, マルチキャストグループ G)

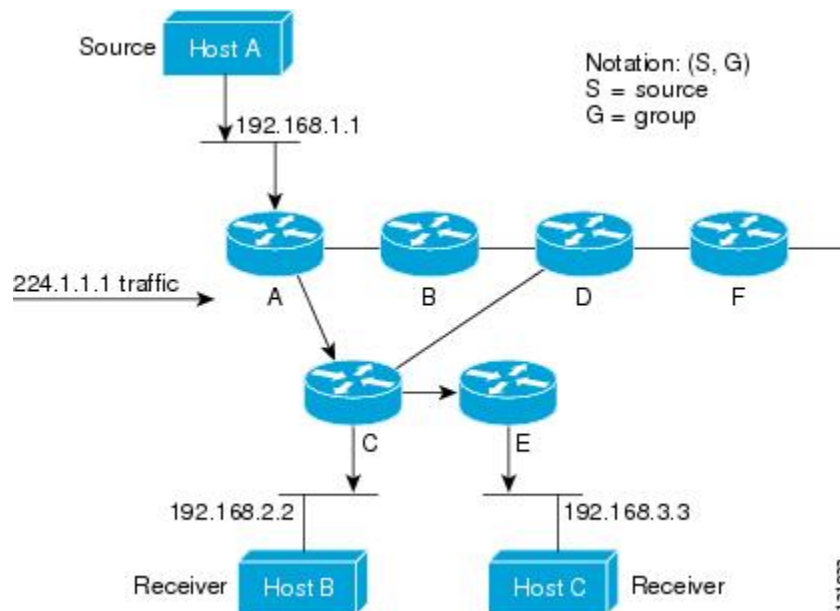
(S, G) という表記 (「S カンマ G」と読みます) は、最短パス ツリーの列挙です。S はソースの IP アドレス、G はマルチキャスト グループ アドレスを表します。

共有ツリーは (*, G) で表されます。ソース ツリーは (S, G) で表され、常にソースでルーティングされます。

マルチキャスト配信のソース ツリー

マルチキャスト配信ツリーの最も単純な形式は、ソース ツリーです。ソース ツリーは、ソースホストをルートとし、ネットワークを介してレシーバに接続するスパニングツリーを形成するブランチを持ちます。このツリーはネットワーク上での最短パスを使用するため、最短パス ツリー (SPT) とも呼ばれます。

次の図に、ソース (ホスト A) をルートとし、2つのレシーバ (ホスト B およびホスト C) に接続するグループ 224.1.1.1 の SPT の例を示します。



標準表記を使用すると、図の例の SPT は (192.168.1.1, 224.1.1.1) となります。

(S, G) という表記は、各グループに送信する個々のソースに個別の SPT が存在することを意味します。

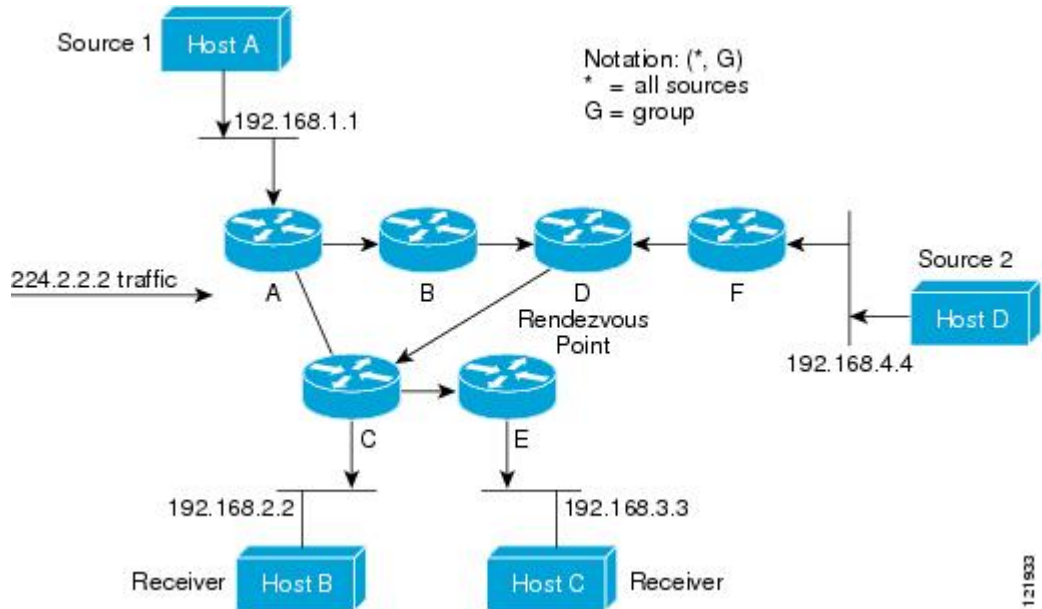
マルチキャスト配信の共有ツリー

ソースをルートとするソース ツリーとは異なり、共有ツリーはネットワーク内の選択されたポイントに配置された単一の共通ルートを使用します。この共有されたルートは、ランデブーポイント (RP) と呼ばれます。

次の図に、ルータ D にルートが配置されたグループ 224.2.2.2 の共有ツリーを示します。この共有ツリーは単方向です。ソーストラフィックは、ソース ツリー上の RP に向けて送信されます。このトラフィックは、次に RP から共有ツリーを下方向に転送され、すべてのレシーバに

到達します (レシーバがソースと RP の間に配置されていない場合は、直接サービスが提供されます)。

図 12: 共有ツリー



この例では、送信元 (ホスト A およびホスト D) からのマルチキャストトラフィックがルート (ルータ D) に移動した後、共有ツリーから 2 つの受信先 (ホスト B およびホスト C) へと到達します。マルチキャストグループ内のすべての送信元が一般的な共有ツリーを使用するため、(*, G) というワイルドカード表記 (「アスタリスク、カンマ、G」と読みます) でそのツリーを表します。この場合、* はすべてのソースを意味し、G はマルチキャストグループを表します。したがって、図の共有ツリーは (*, 224.2.2.2) と表記します。

ソース ツリーと共有ツリーは、どちらもループフリーです。ツリーが分岐する場所でのみ、メッセージが複製されます。マルチキャストグループのメンバは常に加入または脱退する可能性があるため、配信ツリーを動的に更新する必要があります。特定のブランチに存在するすべてのアクティブレシーバが特定のマルチキャストグループに対してトラフィックを要求しなくなると、ルータは配信ツリーからそのブランチをブルーニングし、そのブランチから下方向へのトラフィック転送を停止します。そのブランチの特定のレシーバがアクティブになり、マルチキャストトラフィックを要求すると、ルータは配信ツリーを動的に変更し、トラフィック転送を再開します。

ソース ツリーの利点

ソース ツリーには、ソースとレシーバの間に最適なパスを作成するという利点があります。この利点により、マルチキャストトラフィックの転送におけるネットワーク遅延を最小限に抑えることができます。ただし、この最適化は代償を伴います。ルータがソースごとにパス情報を維持する必要があるのです。何千ものソース、何千ものグループが存在するネットワークでは、このオーバーヘッドがすぐにルータ上でのリソースの問題につながる可能性があります。ネットワーク設計者は、マルチキャストルーティングテーブルのサイズによるメモリ消費について考慮する必要があります。

共有ツリーの利点

共有ツリーには、各ルータにおいて要求されるステートの量が最小限に抑えられるという利点があります。この利点により、共有ツリーだけが許容されるネットワークの全体的なメモリ要件が緩和されます。共有ツリーの欠点は、特定の状況でソースとレシーバの間のパスが最適パスではなくなり、パケット配信に遅延を生じる可能性があることです。たとえば、上の図のホスト A (ソース 1) とホスト 2 (レシーバ) 間の最短パスはルータ A とルータ B です。共有ツリーのルートとしてルータ D を使用するため、トラフィックはルータ A、B、D、そして次に C を通過する必要があります。ネットワーク設計者は、共有ツリー専用環境を実装する際にランデブーポイント (RP) の配置を慎重に考慮する必要があります。

ユニキャストルーティングでは、トラフィックは、ネットワーク上でソースから宛先ホストまでの単一パスに沿ってルーティングされます。ユニキャストルータは、ソースアドレスを考慮せず、宛先アドレスおよびその宛先へのトラフィックの転送方法だけを考慮します。ルータは、ルーティングテーブル全体をスキャンして宛先アドレスを取得し、適正なインターフェイスから宛先方向へユニキャストパケットのコピーを転送します。

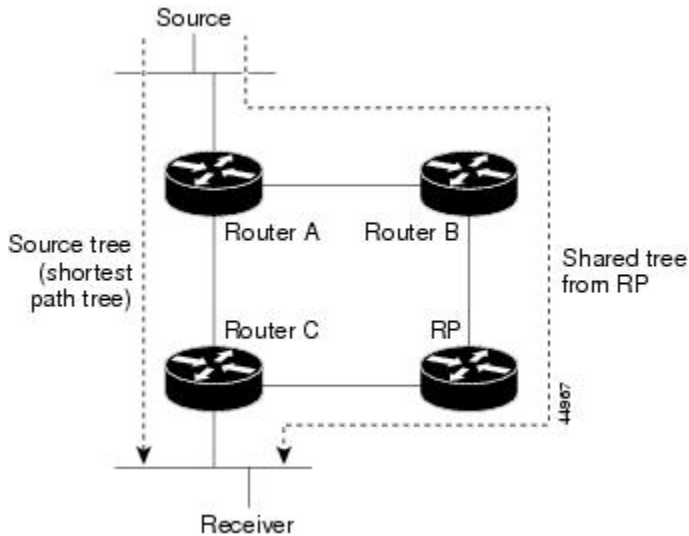
マルチキャスト転送では、ソースは、マルチキャストグループアドレスによって表される任意のホストグループにトラフィックを送信します。マルチキャストルータは、どの方向が (ソースへ向かう) アップストリーム方向で、どの方向 (1方向または複数の方向) が (レシーバへ向かう) ダウンストリーム方向であるかを決定する必要があります。複数のダウンストリームパスがある場合、ルータはパケットを複製し、それを適切なダウンストリームパス (最善のユニキャストルートメトリック) で下方向に転送します。これらのパスがすべてであるとは限りません。レシーバの方向ではなく、ソースから遠ざかる方向へのマルチキャストトラフィック転送は、Reverse Path Forwarding (RPF) と呼ばれます。RPF については、次の項を参照してください。

PIM 共有ツリーおよびソース ツリー

デフォルトでは、グループのメンバーで受信されるデータは、RP でルーティングされた単一のデータ配信ツリーを経由して、送信側からグループに送られます。

図 13: 共有ツリーおよびソース ツリー (最短パスツリー)

次の図に、このタイプの共有配信ツリーを示します。送信側からのデータは、RPに配信され、その共有ツリーに加入しているグループメンバに配布されます。



データレートによって保証されている場合は、送信元でルーティングされるデータ配信ツリーを、共有ツリーのリーフルータ (ダウンストリーム接続がないルータ) で使用できます。このタイプの配信ツリーは、SPTまたは送信元ツリーと呼ばれます。デフォルトでは、ソフトウェアは、送信元から最初のデータパケットを受信すると、送信元ツリーに切り替わります。

共有ツリーから送信元ツリーへの移動プロセスは、次のとおりです。

1. レシーバがグループに加入します。リーフルータ C は Join メッセージを RP に向けて送信します。
2. RP はルータ C とのリンクを発信インターフェイス リストに格納します。
3. 送信元がデータを送信します。ルータ A はデータをカプセル化して登録メッセージに格納し、RP に送信します。
4. RP はデータをルータ C に向けて共有ツリーの下方向に転送し、送信元に向けて Join メッセージを送信します。この時点で、データはルータ C に 2 回着信する可能性があります (カプセル化されたデータ、およびネイティブ状態のデータ)。
5. データがネイティブ状態 (カプセル化されていない状態) で着信すると、RP は登録停止メッセージをルータ A に送信します。
6. デフォルトでは、最初のデータ パケット受信時に、ルータ C が Join メッセージを送信元に送信するよう要求します。
7. ルータ C が (S, G) でデータを受信すると、ルータ C は共有ツリーの上位方向にある送信元に prune メッセージを送信します。
8. RP が (S, G) の発信インターフェイスからルータ C へのリンクを削除します。RP は送信元に向けてプルーニング メッセージを送信します。

送信元および RP に join および prune メッセージが送信されます。これらのメッセージはホップ単位で送信され、送信元または RP へのパス上にある各 PIM デバイスで処理されます。register および register-stop メッセージは、ホップバイホップで送信されません。これらのメッセージは、送信元に直接接続されている指定ルータによって送信され、グループの RP によって受信されます。

グループへ送信する複数の送信元で、共有ツリーが使用されます。共有ツリー上に存在するように、PIM デバイスを設定できます。

最初のデータ パケットがラスト ホップルータに着信すると、共有ツリーからソースツリーへと変更されます。この変更は、**ip pim spt-threshold** グローバル コンフィギュレーション コマンドを使用して設定したしきい値によって異なります。

SPT には共有ツリーよりも多くのメモリが必要ですが、遅延が短縮されます。SPT の使用を延期することもできます。リーフルータを SPT にすぐ移動せず、トラフィックがしきい値に最初に到達したあとで移動するように指定できます。

PIM リーフ ルータが、指定グループの SPT に加入する時期を設定できます。送信元の送信速度が指定速度 (キロビット/秒) 以上の場合、マルチレイヤ スイッチは PIM Join メッセージを送信元に向けて送信し、送信元ツリー (SPT) を構築します。送信元からのトラフィック速度がしきい値を下回ると、リーフルータは共有ツリーに再び切り替わり、プルーンングメッセージを送信元に送信します。

SPT しきい値を適用するグループを指定するには、グループ リスト (標準アクセス リスト) を使用します。値 0 を指定する場合、またはグループ リストを使用しない場合、しきい値はすべてのグループに適用されます。

Reverse Path Forwarding

ユニキャストルーティングでは、トラフィックは、ネットワーク上でソースから宛先ホストまでの単一パスに沿ってルーティングされます。ユニキャストルータは、ソース アドレスを考慮せず、宛先アドレスおよびその宛先へのトラフィックの転送方法だけを考慮します。ルータは、ルーティング テーブル全体をスキャンして宛先ネットワークを取得し、適正なインターフェイスから宛先の方向へユニキャスト パケットのコピーを転送します。

マルチキャスト転送では、ソースは、マルチキャスト グループアドレスによって表される任意のホスト グループにトラフィックを送信します。マルチキャストルータは、どの方向が (ソースへ向かう) アップストリーム方向で、どの方向 (1 方向または複数の方向) が (レシーバへ向かう) ダウンストリーム方向であるかを決定する必要があります。複数のダウンストリームパスがある場合、ルータはパケットを複製し、それを適切なダウンストリームパス (最善のユニキャストルート メトリック) で下方向に転送します。これらのパスがすべてであるとは限りません。レシーバの方向ではなく、ソースから遠ざかる方向へのマルチキャストトラフィック転送は、Reverse Path Forwarding (RPF) と呼ばれます。RPF は、マルチキャストデータグラム転送に使用されるアルゴリズムです。

Protocol Independent Multicast (PIM) は、ユニキャストルーティング情報を使用して、レシーバからソースへ向かうリバースパスに沿って配信ツリーを作成します。その後、マルチキャストルータは、その配信ツリーに沿ってソースからレシーバにパケットを転送します。RPF は、マルチキャスト転送における重要な概念です。RPF により、ルータは、配信ツリーの下方向へ

正しくマルチキャストトラフィックを転送できます。RPFは、既存のユニキャストルーティングテーブルを使用して、アップストリームネイバーとダウンストリームネイバーを決定します。ルータは、アップストリームインターフェイスで受信した場合にのみ、マルチキャストパケットを転送します。このRPFチェックにより、配信ツリーがループフリーであることを保証できます。

RPF チェック

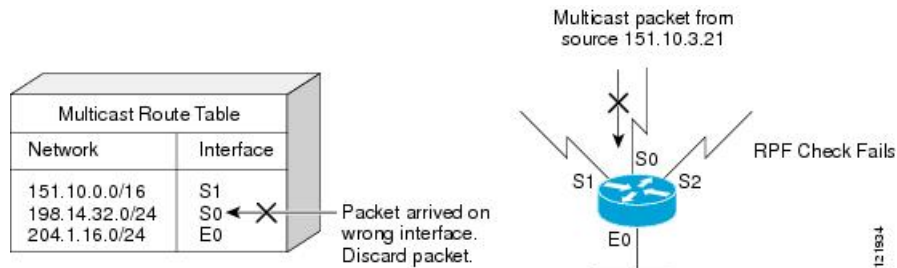
マルチキャストパケットがルータに到達すると、ルータはそのパケットに対してRPFチェックを実行します。RPFチェックが成功すると、パケットが転送されます。そうでない場合、パケットはドロップされます。

ソースツリーを下方向へ流れるトラフィックに対するRPFチェック手順は次のとおりです。

1. ルータは、ユニキャストルーティングテーブルでソースアドレスを検索して、ソースへのリバースパス上にあるインターフェイスにパケットが到達したかどうかを判定します。
2. ソースに戻すインターフェイスにパケットが到達した場合、RPFチェックは成功し、マルチキャストルーティングテーブルエントリの発信インターフェイスリストに示されているインターフェイスからパケットが転送されます。
3. ステップ2でRPFチェックに失敗した場合は、パケットがドロップされます。

図に、RPFチェックの失敗例を示します。

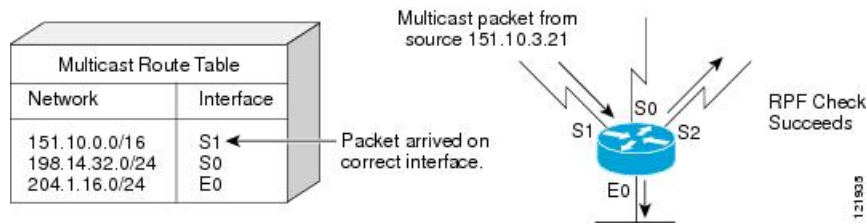
図 14: RPFチェックの失敗



図に示すように、ソース 151.10.3.21 からのマルチキャストパケットはシリアルインターフェイス 0 (S0) 上で受信されています。ユニキャストルートテーブルのチェック結果は、このルータが 151.10.3.21 にユニキャストデータを転送するために使用するインターフェイスは S1 であることを示しています。パケットはインターフェイス S0 に到達しているため、このパケットは廃棄されます。

図に RPF チェックの成功例を示します。

図 15: RPF チェックの成功



この例では、マルチキャストパケットはインターフェイス S1 に到達しています。ルータはユニキャストルーティングテーブルを参照し、S1 が適正なインターフェイスであることを知ります。RPF チェックが成功し、パケットが転送されます。

PIM はソースツリーと RP でルーティングされた共有ツリーを使用して、データグラムを転送します。RPF チェックは、それぞれ異なる方法で実行されます。

- PIM ルータまたはマルチレイヤスイッチが送信元ツリーの状態である場合（つまり (S, G) エントリがマルチキャストルーティングテーブル内にある場合）、マルチキャストパケットの送信元の IP アドレスに対して RPF チェックが実行されます。
- PIM ルータまたはマルチレイヤスイッチが共有ツリーステートである場合（および送信元ツリーステートが明示されていない場合）、（メンバーがグループに加入している場合は既知である）RP アドレスについて RPF チェックが実行されます。



(注) このスイッチでは DVMRP はサポートされません。

PIM SM は RPF 参照機能を使用し、加入およびプルーニングメッセージを送信する必要があるかどうかを決定します。

- (S, G) join (送信元ツリーステート) は送信元に向けて送信されます。
- (*,G) Join メッセージ (共有ツリーステート) は RP に向け送信されます。

PIM ルーティングのデフォルト設定

デバイス用の PIM ルーティングのデフォルト設定を次の表に示します。

表 14: マルチキャストルーティングのデフォルト設定

機能	デフォルト設定
マルチキャストルーティング	すべてのインターフェイスでディ
PIM のバージョン	バージョン 2
PIM モード	モードは未定義
PIM スタブルーティング	未設定

機能	デフォルト設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル。
PIM マルチキャスト境界	なし
候補 BSR	ディセーブル。
候補 RP	ディセーブル。
SPT しきい値レート	0 kb/s
PIM ルータ クエリー メッセージ インターバル	30 秒

PIM の設定方法

PIM スタブルルーティングのイネーブル化

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例 : Device (config)# interface gigabitethernet 1/0/1	PIM スタブルルーティングをイネーブルにするインターフェイスを指定し、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。 指定するインターフェイスは、次のいずれかである必要があります。これらのインターフェイスには、IP アドレス

	コマンドまたはアクション	目的
		<p>が割り当てられている必要があります。</p> <ul style="list-style-type: none"> • ルーテッドポート：レイヤ3ポートとして no switchport インターフェイスコンフィギュレーションコマンドを入力して設定された物理ポートです。 • SVI： interface vlan vlan-id グローバルコンフィギュレーションコマンドを使用して作成された VLAN インターフェイスです。
ステップ 4	ip pim passive 例： Device(config-if)# ip pim passive	インターフェイスに PIM スタブ機能を設定します。
ステップ 5	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show ip pim interface 例： Device# show ip pim interface	(任意) 各インターフェイスで有効になっている PIM スタブを表示します。
ステップ 7	show ip igmp groups detail 例： Device# show ip igmp groups detail	(任意) 特定のマルチキャスト送信元グループに参加した対象クライアントを表示します。
ステップ 8	show ip mroute 例： Device# show ip mroute	(任意) IP マルチキャストルーティングテーブルを表示します。
ステップ 9	show running-config 例：	入力を確認します。

	コマンドまたはアクション	目的
	Device# show running-config	
ステップ 10	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

ランデブーポイントの設定

インターフェイスがスパース-デンスモードで、グループをスパースグループとして扱う場合には、ランデブーポイント (RP) を設定する必要があります。次の方法を使用できます。

- RP をマルチキャストグループに手動で割り当てる
- PIMv1 から独立した、以下を含むスタンドアロンとしてのシスコ独自のプロトコル
- Internet Engineering Task Force (IETF) の標準追跡プロトコルの使用 (PIMv2 BSR の設定を含む)



- (注) 動作中の PIM バージョン、およびネットワーク内のルータタイプに応じて、自動 RP、BSR、またはこれらを組み合わせて使用できます。ネットワーク内の異なるバージョンの PIM を利用する方法については、[PIMv1 および PIMv2 の相互運用性 \(136 ページ\)](#) を参照してください。

マルチキャストグループへの RP の手動割り当て

ダイナミックメカニズム (自動 RP や BSR など) を使用してグループのランデブーポイント (RP) を取得する場合、RP を手動で割り当てる必要はありません。

マルチキャストトラフィックの送信側は、送信元の先頭ホップルータ (指定ルータ) から受信して RP に転送される登録メッセージを通し、自身の存在をアナウンスします。マルチキャストパケットの受信側は RP を使用し、マルチキャストグループに加入します。この場合は、明示的な Join メッセージが使用されます。



- (注) RP はマルチキャストグループのメンバーではなく、マルチキャスト送信元およびグループメンバーの合流地点として機能します。

アクセスリストで定義される複数のグループに、単一の RP を設定できます。グループに RP が設定されていない場合、マルチレイヤスイッチはデンスとしてグループに応答し、デンスモードの PIM 技術を使用します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip pim rp-address ip-address [access-list-number] [override] 例 : Device(config)# ip pim rp-address 10.1.1.1 20 override	PIM RP のアドレスを設定します。 デフォルトで、PIM RP アドレスは設定されていません。すべてのルータおよびマルチレイヤスイッチ (RP を含む) で、RP の IP アドレスを設定する必要があります。 (注) グループに RP が設定されていない場合、デバイスは PIM DM 技術を使用し、グループをデンスとして処理します。 1 台の PIM デバイスを、複数のグループの RP にできます。1 つの PIM ドメイン内で一度に使用できる RP アドレスは、1 つだけです。アクセスリスト条件により、デバイスがどのグループの RP であるかを指定します。 <ul style="list-style-type: none"> • <i>ip-address</i> には、RP のユニキャストアドレスをドット付き 10 進表記で入力します。 • (任意) <i>access-list-number</i> を指定する場合は、1 ~ 99 の IP 標準アクセスリスト番号を入力します。アク

	コマンドまたはアクション	目的
		<p>セス リストが設定されていない場合は、すべてのグループに RP が使用されます。</p> <ul style="list-style-type: none"> • (任意) override キーワードを指定すると、このコマンドによって設定された RP と、自動 RP または BSR で取得された RP との間に矛盾が生じた場合に、このコマンドによって設定された RP が優先されます。
ステップ 4	<p>access-list access-list-number {deny permit} source [source-wildcard]</p> <p>例 :</p> <pre>Device(config)# access-list 25 permit 10.5.0.1 255.224.0.0</pre>	<p>標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。</p> <ul style="list-style-type: none"> • access-list-number には、ステップ 2 で指定したアクセス リスト番号を入力します。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。 • permit キーワードは、条件が一致した場合にアクセスを許可します。 • source には、RP が使用されるマルチキャスト グループのアドレスを入力します。 • (任意) source-wildcard には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。</p>
ステップ 5	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 6	<p>show running-config</p> <p>例 :</p>	<p>入力を確認します。</p>

	コマンドまたはアクション	目的
	Device# <code>show running-config</code>	
ステップ 7	copy running-config startup-config 例 : Device# <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

新規ネットワークでの Auto-RP の設定



- (注) PIM ルータをローカル グループの RP として設定する場合は、次の手順のステップ 3 を省略します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> <code>enable</code>	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	show running-config 例 : Device# <code>show running-config</code>	すべての PIM デバイス上でデフォルトの RP が設定されていること、および RP が SM ネットワーク内にあることを確認します。RP は、 ip pim rp-address グローバルコンフィギュレーション コマンドによって設定済みです。 (注) SM-DM 環境の場合、このステップは不要です。 選択された RP は接続が良好で、ネットワークで使用可能となる必要があります。この RP は、グローバル グループ (224.x.x.x やその他のグローバル グループなど) に対して使用されます。この RP で処理されるグループ アドレス範囲は再設定しないでください。自

	コマンドまたはアクション	目的
		動 RP によって動的に検出された RP は、静的に設定された RP よりも優先されます。ローカルグループ用に2番目の RP を使用することもできます。
ステップ 3	configure terminal 例 : Device# configure terminal	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 4	ip pim send-rp-announce interface-id scope ttl group-list access-list-number interval seconds 例 : Device(config)# ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120	別の PIM デバイスをローカルグループの候補 RP として設定します。 <ul style="list-style-type: none"> • interface-id には、RP アドレスを識別するインターフェイスタイプおよび番号を入力します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • scope ttl には、ホップの存続可能時間の値を指定します。RP アナウンスメッセージがネットワーク内のすべてのマッピングエージェントに到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。指定できる範囲は 1 ~ 255 です。 • group-list access-list-number には、1 ~ 99 の範囲で標準の IP アクセスリスト番号を入力します。アクセスリストが設定されていない場合は、すべてのグループに RP が使用されます。 • interval seconds には、アナウンスメントメッセージを送信する頻度を指定します。デフォルトは 60 秒です。指定できる範囲は 1 ~ 16383 です。
ステップ 5	access-list access-list-number {deny permit} source [source-wildcard] 例 :	標準アクセスリストを作成し、コマンドを必要な回数だけ実行します。

	コマンドまたはアクション	目的
	<pre>Device(config)# access-list 10 permit 10.10.0.0</pre>	<ul style="list-style-type: none"> • access-list-number には、ステップ 3 で指定したアクセス リスト番号を入力します。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。 • permit キーワードは、条件が一致した場合にアクセスを許可します。 • source には、RP が使用されるマルチキャストグループのアドレス範囲を入力します。 • (任意) source-wildcard には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>(注) アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 6	<pre>ip pim send-rp-discovery scope ttl</pre> <p>例 :</p> <pre>Device(config)# ip pim send-rp-discovery scope 50</pre>	<p>接続が中断される可能性がないデバイスを検索し、RP マッピングエージェントの役割を割り当てます。</p> <p>scope ttl には、ホップの存続可能時間の値を指定し、RP ディスカバリパケットを制限します。ホップ数内にあるすべてのデバイスは、送信元デバイスから自動 RP ディスカバリ メッセージを受信します。これらのメッセージは他のデバイスに対し、矛盾 (グループ/RP 範囲の重なりなど) を回避するために使用されるグループ/RP マッピングを通知します。デフォルト設定はありません。指定できる範囲は 1 ~ 255 です。</p>
ステップ 7	<pre>end</pre> <p>例 :</p>	<p>特権 EXEC モードに戻ります。</p>

	コマンドまたはアクション	目的
	Device(config)# end	
ステップ 8	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 9	show ip pim rp mapping 例 : Device# show ip pim rp mapping	関連するマルチキャストルーティングエントリとともに保管されているアクティブな RP を表示します。
ステップ 10	show ip pim rp 例 : Device# show ip pim rp	ルーティングテーブルに保管されている情報を表示します。
ステップ 11	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

既存の SM クラウドへの Auto-RP の追加

ここでは、最初に自動 RP を既存の SM クラウドに導入し、既存のマルチキャストインフラストラクチャができるだけ破壊されないようにする方法について説明します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	show running-config 例 :	すべての PIM デバイス上でデフォルトの RP が設定されていること、および RP が SM ネットワーク内にあることを

	コマンドまたはアクション	目的
	Device# <code>show running-config</code>	<p>確認します。RP は、<code>ip pim rp-address</code> グローバルコンフィギュレーションコマンドによって設定済みです。</p> <p>(注) SM-DM 環境の場合、このステップは不要です。</p> <p>選択された RP は接続が良好で、ネットワークで使用可能となる必要があります。この RP は、グローバルグループ (224.x.x.x やその他のグローバルグループなど) に対して使用されます。この RP で処理されるグループアドレス範囲は再設定しないでください。自動 RP によって動的に検出された RP は、静的に設定された RP よりも優先されます。ローカルグループ用に 2 番目の RP を使用することもできます。</p>
ステップ 3	<p><code>configure terminal</code></p> <p>例 :</p> <p>Device# <code>configure terminal</code></p>	<p>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。</p>
ステップ 4	<p><code>ip pim send-rp-announce interface-id scope ttl group-list access-list-number interval seconds</code></p> <p>例 :</p> <p>Device(config)# <code>ip pim send-rp-announce gigabitethernet 1/0/5 scope 20 group-list 10 interval 120</code></p>	<p>別の PIM デバイスをローカルグループの候補 RP として設定します。</p> <ul style="list-style-type: none"> • <code>interface-id</code> には、RP アドレスを識別するインターフェイスタイプおよび番号を入力します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。 • <code>scope ttl</code> には、ホップの存続可能時間の値を指定します。RP アナウンスメッセージがネットワーク内のすべてのマッピングエージェントに到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。指定できる範囲は 1 ~ 255 です。 • <code>group-list access-list-number</code> には、1 ~ 99 の範囲で標準の IP アクセ

	コマンドまたはアクション	目的
		<p>スリスト番号を入力します。アクセスリストが設定されていない場合は、すべてのグループに RP が使用されます。</p> <ul style="list-style-type: none"> • interval seconds には、アナウンスメントメッセージを送信する頻度を指定します。デフォルトは 60 秒です。指定できる範囲は 1～16383 です。
ステップ 5	<p>access-list access-list-number {deny permit} source [source-wildcard]</p> <p>例 :</p> <pre>Device(config)# access-list 10 permit 224.0.0.0 15.255.255.255</pre>	<p>標準アクセスリストを作成し、コマンドを必要な回数だけ実行します。</p> <ul style="list-style-type: none"> • access-list-number には、ステップ 3 で指定したアクセス リスト番号を入力します。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。 • permit キーワードは、条件が一致した場合にアクセスを許可します。 • source には、RP が使用されるマルチキャストグループのアドレス範囲を入力します。 • (任意) source-wildcard には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 6	<p>ip pim send-rp-discovery scope ttl</p> <p>例 :</p> <pre>Device(config)# ip pim send-rp-discovery scope 50</pre>	<p>接続が中断される可能性がないデバイスを検索し、RP マッピングエージェントの役割を割り当てます。</p> <p>scope ttl には、ホップの存続可能時間の値を指定し、RP ディスカバリパケットを制限します。ホップ数内にあるすべてのデバイスは、送信元デバイスか</p>

	コマンドまたはアクション	目的
		<p>ら自動 RP ディスカバリ メッセージを受信します。これらのメッセージは他のデバイスに対し、矛盾 (グループ/RP 範囲の重なりなど) を回避するために使用されるグループ/RP マッピングを通知します。デフォルト設定はありません。指定できる範囲は 1 ~ 255 です。</p> <p>(注) RP マッピングエージェントとして設定されたデバイスを削除するには、no ip pim send-rp-discovery グローバル コンフィギュレーションコマンドを使用します。</p>
ステップ 7	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 8	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 9	show ip pim rp mapping 例 : Device# show ip pim rp mapping	関連するマルチキャストルーティング エントリとともに保管されているアクティブな RP を表示します。
ステップ 10	show ip pim rp 例 : Device# show ip pim rp	ルーティングテーブルに保管されている情報を表示します。
ステップ 11	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

問題のある RP への Join メッセージの送信禁止

ip pim accept-rp コマンドがネットワーク全体に設定されているかどうかを判別するには、**show running-config** 特権 EXEC コマンドを使用します。**ip pim accept-rp** コマンドが設定されていないデバイスがある場合は、後でこの問題を解決できます。ルータまたはマルチレイヤスイッチが **ip pim accept-rp** コマンドによってすでに設定されている場合は、このコマンドを再入力し、新規にアドバタイズされる RP を許可する必要があります。

着信 RP アナウンスメント メッセージのフィルタリング

マッピング エージェントにコンフィギュレーション コマンドを追加すると、故意に不正設定されたルータが候補 RP として動作し問題を引き起こさないようにできます。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip pim rp-announce-filter rp-list access-list-number group-list access-list-number 例： Device(config)# ip pim rp-announce-filter rp-list 10 group-list 14	着信 RP アナウンスメントメッセージをフィルタリングします。 ネットワーク内のマッピング エージェントごとに、このコマンドを入力します。このコマンドを使用しないと、すべての着信 RP アナウンスメントメッセージがデフォルトで許可されます。 rp-list access-list-number には、候補 RP アドレスのアクセスリストを設定します。アクセスリストが許可されている場合は、 group-list access-list-number 変数で指定されたグループ範囲に対してアクセスリストを使用できます。この変数を省略すると、すべてのマルチキャストグループにフィルタが適用されます。

	コマンドまたはアクション	目的
ステップ 4	<p>access-list access-list-number {deny permit} source [source-wildcard]</p> <p>例 :</p> <pre>Device(config)# access-list 10 permit 10.8.1.0 255.255.224.0</pre>	<p>複数のマッピング エージェントを使用する場合は、グループ/RP マッピング情報に矛盾が生じないようにするため、すべてのマッピングエージェント間でフィルタを統一する必要があります。</p> <p>標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。</p> <ul style="list-style-type: none"> • access-list-number には、ステップ 2 で指定したアクセス リスト番号を入力します。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。 • permit キーワードは、条件が一致した場合にアクセスを許可します。 • どのルータおよびマルチレイヤ スイッチからの候補 RP アナウンスメント (rp-list アクセスコントロール リスト (ACL)) がマッピングエージェントによって許可されるかを指定するアクセス リストを作成します。 • 許可または拒否するマルチキャストグループの範囲を指定するアクセス リスト (グループリスト ACL) を作成します。 • source には、RP が使用されるマルチキャスト グループのアドレス範囲を入力します。 • (任意) source-wildcard には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。</p>

	コマンドまたはアクション	目的
ステップ 5	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

PIMv2 BSR の設定

PIMv2 BSR を設定するプロセスには、次のオプションの作業が含まれることがあります。

- PIM ドメイン境界の定義
- IP マルチキャスト境界の定義
- 候補 BSR の設定
- 候補 RP の設定

PIM ドメイン境界の定義

PIM ドメイン境界を設定するには、次の手順を実行します。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 :	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	Device# configure terminal	
ステップ 3	interface interface-id 例 : Device(config)# interface gigabitethernet 1/0/1	設定するインターフェイスを指定して、インターフェイスコンフィギュレーションモードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 <ul style="list-style-type: none"> • ルーテッドポート : レイヤ3ポートとして no switchport インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 • SVI : interface vlan vlan-id グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	ip pim bsr-border 例 : Device(config-if)# ip pim bsr-border	PIM ドメイン用の PIM ブートストラップメッセージ境界を定義します。 境界に位置する他の PIM ドメインに接続されているインターフェイスごとに、このコマンドを入力します。このコマンドを実行すると、デバイスは、このインターフェイス上で PIMv2 BSR メッセージを送受信しないように指示されます。 (注) PIM 境界を削除するには、 no ip pim bsr-border インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	end 例 : Device(config)# end	特権 EXEC 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	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IP マルチキャスト境界の定義

自動 RP メッセージが PIM ドメインに入らないようにする場合は、マルチキャスト境界を定義します。自動 RP 情報を伝達する 224.0.1.39 および 224.0.1.40 宛てのパケットを拒否するアクセスリストを作成します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : # configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	access-list access-list-number deny source [source-wildcard] 例 : Device(config)# access-list 12 deny 224.0.1.39 access-list 12 deny 224.0.1.40	標準アクセスリストを作成し、コマンドを必要な回数だけ実行します。 • access-list-number の範囲は 1 ~ 99 です。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。 • source には、自動 RP 情報を伝達するマルチキャストアドレス

	コマンドまたはアクション	目的
		<p>224.0.1.39 および 224.0.1.40 を入力します。</p> <ul style="list-style-type: none"> • (任意) <i>source-wildcard</i> には、<i>source</i> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。</p>
ステップ 4	<p>interface <i>interface-id</i></p> <p>例 :</p> <pre>Device(config)# interface gigabitethernet 1/0/1</pre>	<p>設定するインターフェイスを指定して、インターフェイスコンフィギュレーションモードを開始します。</p> <p>次のいずれかのインターフェイスを指定する必要があります。</p> <ul style="list-style-type: none"> • ルーテッドポート : レイヤ3ポートとして no switchport インターフェイスコンフィギュレーションコマンドを入力して設定された物理ポートです。 • SVI : interface vlan <i>vlan-id</i> グローバルコンフィギュレーションコマンドを使用して作成された VLAN インターフェイスです。 <p>これらのインターフェイスには、IP アドレスを割り当てる必要があります。</p>
ステップ 5	<p>ip multicast boundary <i>access-list-number</i></p> <p>例 :</p> <pre>Device(config-if)# ip multicast boundary 12</pre>	<p>ステップ 2 で作成したアクセス リストを指定し、境界を設定します。</p>
ステップ 6	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>

	コマンドまたはアクション	目的
ステップ 7	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 8	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

候補 BSR の設定

候補 BSR を、1 つまたは複数設定できます。候補 BSR として機能するデバイスは、他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	ip pim bsr-candidate interface-id hash-mask-length [priority] 例 : Device(config)# ip pim bsr-candidate gigabitethernet 1/0/3 28 100	候補 BSR となるようにデバイスを設定します。 <ul style="list-style-type: none"> <i>interface-id</i> には、デバイスを候補 BSR に設定するとき BSR アドレスの取得元となる上のインターフェイスを入力します。このインターフェイスは PIM を使用してイネーブルにする必要があります。有効なインターフェイスは、物理ポート、ポートチャネル、VLAN などです。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>hash-mask-length</i> には、ハッシュ機能呼び出す前にグループアドレスとの AND 条件となるマスク長 (最大 32 ビット) を指定します。ハッシュ元が同じであるすべてのグループは、同じ RP に対応します。たとえば、マスク長が 24 の場合、グループアドレスの最初の 24 ビットだけが使用されます。 • (任意) <i>priority</i> を指定する場合は、0 ~ 255 の番号を入力します。プライオリティが大きな BSR が優先されます。このプライオリティ値が同じである場合は、大きな IP アドレスを持つデバイスが BSR として選択されます。デフォルトは 0 です。
ステップ 4	end 例 : Device (config) # end	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

候補 RP の設定

候補 RP を、1 つまたは複数設定できます。BSR と同様、RP は他のデバイスと正しく接続され、ネットワークのバックボーン部分に配置されている必要があります。RP は IP マルチキャストアドレス空間全体、またはその一部を処理します。候補 RP は候補 RP アドバタイズを BSR に送信します。

この手順は任意です。

始める前に

RP となるデバイスを決定するときは、次の可能性を考慮してください。

- 自動 RP だけが使用されている Cisco ルータおよびマルチレイヤスイッチで構成されるネットワークでは、すべてのデバイスを RP として設定できます。
- シスコの PIMv2 ルータおよびマルチレイヤスイッチと、他のベンダーのルータだけで構成されるネットワークでは、すべてのデバイスを RP として使用できます。
- シスコの PIMv1 ルータ、PIMv2 ルータ、および他のベンダーのルータで構成されるネットワークでは、シスコ PIMv2 ルータおよびマルチレイヤスイッチを RP として設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	ip pim rp-candidate interface-id [group-list access-list-number] 例 : Device(config)# ip pim rp-candidate gigabitethernet 1/0/5 group-list 10	候補 RP となるようにデバイスを設定します。 <ul style="list-style-type: none"> • <i>interface-id</i> には、対応する IP アドレスが候補 RP アドレスとしてアドレスバタイズされるインターフェイスを指定します。有効なインターフェイスは、物理ポート、ポートチャネル、VLAN などです。 • (任意) group-list access-list-number を指定する場合は、1 ~ 99 の IP 標準アクセスリスト番号を入力します。group-list を指定しない場合は、このデバイスがすべてのグループの候補 RP となります。

	コマンドまたはアクション	目的
ステップ 4	<p>access-list <i>access-list-number</i> {deny permit} <i>source</i> [<i>source-wildcard</i>]</p> <p>例 :</p> <pre>Device(config)# access-list 10 permit 239.0.0.0 0.255.255.255</pre>	<p>標準アクセス リストを作成し、コマンドを必要な回数だけ実行します。</p> <ul style="list-style-type: none"> • <i>access-list-number</i> には、ステップ 2 で指定したアクセス リスト番号を入力します。 • deny キーワードは、条件が一致した場合にアクセスを拒否します。 permit キーワードは、条件が一致した場合にアクセスを許可します。 • <i>source</i> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • (任意) <i>source-wildcard</i> には、<i>source</i> に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。</p>
ステップ 5	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 6	<p>show running-config</p> <p>例 :</p> <pre>Device# show running-config</pre>	<p>入力を確認します。</p>
ステップ 7	<p>copy running-config startup-config</p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p>

Auto-RP によるスパース モードの設定

始める前に

- Auto-RP を設定するときに必要なすべてのアクセスリストは、設定作業を開始する前に設定しておく必要があります。



- (注)
- グループ内に既知の RP がなく、インターフェイスがスパース-デンス モードに設定されている場合、インターフェイスはデンス モードであるように扱われ、データはインターフェイスを介してフラッディングされます。このデータのフラッディングを避けるために、Auto-RP リスナーを設定してから、インターフェイスをスパースモードとして設定します。
 - Auto-RP を設定するには、Auto-RP リスナー機能を設定するか (ステップ 5)、スパースモードを指定する (ステップ 7) 必要があります。
 - スパース-デンス モードを指定する場合、デンス モードのフェールオーバーがネットワークのデンスモードのフラッディングを引き起こす可能性があります。この状況を避けるため、Auto-RP リスナー機能で PIM スパース モードを使用します。

自動ランデブー ポイント (Auto-RP) を設定するには、次の手順に従います。Auto-RP は任意でエニーキャスト RP でも使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip multicast-routing 例 : Device(config)# ip multicast-routing	IP マルチキャスト ルーティングをイネーブルにします。
ステップ 4	ステップ 5 ~ 7 を実行するか、またはステップ 6 および 8 を実行します。	--

	コマンドまたはアクション	目的
ステップ 5	interface <i>type number</i> 例 : <pre>Device(config)# interface GigabitEthernet 1/0/0</pre>	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 6	ip pim sparse-mode 例 : <pre>Device(config-if)# ip pim sparse-mode</pre>	インターフェイスで PIM スパースモードをイネーブルにします。スパースモードで Auto-RP を設定している場合、次のステップで Auto-RP リスナーも設定する必要があります。 <ul style="list-style-type: none"> • ステップ 8 でスパース-デンスモードを設定している場合、このステップはスキップします。
ステップ 7	exit 例 : <pre>Device(config-if)# exit</pre>	インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 8	すべての PIM インターフェイス上でステップ 1 ~ 9 を繰り返します。	--
ステップ 9	ip pim send-rp-announce { <i>interface-type interface-number</i> <i>ip-address</i> } scope <i>ttl-value</i> [group-list <i>access-list</i>] [interval <i>seconds</i>] [bidir] 例 : <pre>Device(config)# ip pim send-rp-announce loopback0 scope 31 group-list 5</pre>	RP アナウンスメントをすべての PIM 対応インターフェイスに送信します。 <ul style="list-style-type: none"> • RP デバイスでのみこのステップを実行します。 • RP アドレスとして使用する IP アドレスを定義するには、<i>interface-type</i> 引数と <i>interface-number</i> 引数を使用します。 • 直接接続されている IP アドレスを RP アドレスとして指定するには、<i>ip-address</i> 引数を使用します。 (注) このコマンドに <i>ip-address</i> 引数が設定されている場合、RP 通知メッセージがこのアドレスが接続されているインターフェイスによって送信されます (つまり、RP 通知メッセージの IP

	コマンドまたはアクション	目的
		<p>ヘッダーのソースアドレスがそのインターフェイスの IP アドレスです)。</p> <ul style="list-style-type: none"> 次の例は、最大ホップ数が31でインターフェイスがイネーブルであることを示します。デバイスは、ループバック インターフェイス 0 に関連付けられた IP アドレスによって RP として識別されることを望みます。アクセスリスト5はこのデバイスが RP として機能しているグループを示しています。
<p>ステップ 10</p>	<p>ip pim send-rp-discovery [<i>interface-type interface-number</i>] scope <i>ttl-value</i> [interval <i>seconds</i>]</p> <p>例 :</p> <pre>Device(config)# ip pim send-rp-discovery loopback 1 scope 31</pre>	<p>デバイスを RP マッピング エージェントとして設定します。</p> <ul style="list-style-type: none"> RP マッピング エージェント デバイス上、または RP/RP マッピング エージェント複合デバイス上で、このステップを実行します。 <p>(注)</p> <p>Auto-RPによって、RP機能は1台のデバイス上で単独で実行でき、RP マッピング エージェントは1台または複数のデバイス上で実行できます。RP/RP マッピング エージェント複合デバイス上で、RP および RP マッピング エージェントを展開することができます。</p> <ul style="list-style-type: none"> RP マッピング エージェントのソースアドレスとして使用する IP アドレスを定義するには、オプションの <i>interface-type</i> 引数と <i>interface-number</i> 引数を使用します。 Auto-RP 検出メッセージの IP ヘッダーで持続可能時間 (TTL) 値を指定するには、scope キーワードと <i>ttl-value</i> 引数を使用します。 Auto-RP 検出メッセージが送信される間隔を指定するには、オプ

	コマンドまたはアクション	目的
		<p>ションの interval キーワードと <i>seconds</i> 引数を使用します。</p> <p>(注) Auto-RP 検出メッセージが送信される間隔をデフォルト値の 60 秒から減らすと、group-to-RP マッピングのより頻繁なフラッディングが発生します。一部のネットワーク環境では、間隔を短縮する欠点 (コントロール パケット オーバーヘッドの増加) が利点 (グループと RP のマッピングのより頻繁な更新) を上回る場合があります。</p> <ul style="list-style-type: none"> 例では、ループバック インターフェイス 1 で Auto-RP 検出メッセージを 31 ホップに制限していることを示しています。
ステップ 11	<p>ip pim rp-announce-filter rp-list access-list group-list access-list</p> <p>例 :</p> <pre>Device(config)# ip pim rp-announce-filter rp-list 1 group-list 2</pre>	<p>候補 RP (C-RP) から RP マッピング エージェントに送信された着信 RP アナウンスメントメッセージをフィルタリングします。</p> <ul style="list-style-type: none"> このステップは、RP マッピング エージェントでのみ実行します。
ステップ 12	<p>interface type number</p> <p>例 :</p> <pre>Device(config)# interface gigabitethernet 1/0/0</pre>	<p>PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。</p>
ステップ 13	<p>ip multicast boundary access-list [filter-autorp]</p> <p>例 :</p> <pre>Device(config-if)# ip multicast boundary 10 filter-autorp</pre>	<p>管理用スコープの境界を設定します。</p> <ul style="list-style-type: none"> このステップは、他のデバイスとの境界であるインターフェイス上で実行します。 この作業ではアクセスリストは表示されません。 アクセスリストエントリで deny キーワードを使用すると、そのエントリに一致するパケットのマルチキャスト境界が作成されます。

	コマンドまたはアクション	目的
ステップ 14	end 例 : Device(config-if)# end	グローバル コンフィギュレーション モードに戻ります。
ステップ 15	show ip pim autorp 例 : Device# show ip pim autorp	(任意) Auto-RP 情報を表示します。
ステップ 16	show ip pim rp [mapping] [rp-address] 例 : Device# show ip pim rp mapping	(任意) ネットワークで既知の RP を表示し、デバイスが各 RP について学習する方法を示します。
ステップ 17	show ip igmp groups [group-name group-address interface-type interface-number] [detail] 例 : Device# show ip igmp groups	(任意) デバイスに直接接続されている、インターネットグループ管理プロトコル (IGMP) を通じて学習されたレシーバを持つマルチキャストグループを表示します。 <ul style="list-style-type: none"> レシーバ情報が結果の画面に表示されるには、レシーバがこのコマンドが発行された時点でネットワーク上でアクティブである必要があります。
ステップ 18	show ip mroute [group-address group-name] [source-address source-name] [interface-type interface-number] [summary] [count] [active kbps] 例 : Device# show ip mroute cbone-audio	(任意) IP マルチキャストルーティング (mroute) テーブルの内容を表示します。

PIM 最短パス ツリーの使用の延期

マルチキャストルーティングが送信元ツリーから最短パスツリーに切り替わる前に到達する必要があるトラフィック レートしきい値を設定するには、次の手順を実行します。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	access-list access-list-number {deny permit} source [source-wildcard] 例 : Device(config)# access-list 16 permit 225.0.0.0 0.255.255.255	標準アクセス リストを作成します。 <ul style="list-style-type: none"> access-list-number の範囲は 1 ~ 99 です。 deny キーワードは、条件が一致した場合にアクセスを拒否します。 permit キーワードは、条件が一致した場合にアクセスを許可します。 source には、しきい値が適用されるマルチキャスト グループを指定します。 (任意) source-wildcard には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在します。
ステップ 4	ip pim spt-threshold {kbps infinity} [group-list access-list-number] 例 : Device(config)# ip pim spt-threshold infinity group-list 16	最短パスツリー (SPT) に移行するまでに到達する必要があるしきい値を指定します。 <ul style="list-style-type: none"> kbps を指定する場合は、トラフィック レートをキロビット/秒で指定します。デフォルト値は 0 キロビット/秒です。

	コマンドまたはアクション	目的
		<p>(注)</p> <p>有効範囲は 0 ~ 4294967 ですが、デバイスハードウェアの制限により、0 キロビット/秒以外は無効です。</p> <ul style="list-style-type: none"> • infinity を指定すると、指定されたグループのすべての送信元で共有ツリーが使用され、送信元ツリーに切り替わらなくなります。 • (任意) group-list access-list-number には、ステップ 2 で作成したアクセスリストを指定します。値 0 を指定する場合、またはグループリストを使用しない場合、しきい値はすべてのグループに適用されます。
ステップ 5	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 6	<p>show running-config</p> <p>例 :</p> <pre>Device# show running-config</pre>	入力を確認します。
ステップ 7	<p>copy running-config startup-config</p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

PIM ルータクエリーメッセージ間隔の変更

PIM ルータおよびマルチレイヤスイッチでは、各 LAN セグメント (サブネット) の代表ルータ (DR) になるデバイスを検出するため、PIM ルータクエリーメッセージが送信されます。DR は、直接接続された LAN 上のすべてのホストに IGMP ホストクエリーメッセージを送信します。

PIM DM 動作では、IGMPv1 が使用中の場合だけ、DR は意味を持ちます。IGMPv1 には IGMP クエリア選択プロセスがないため、選択された DR は IGMP クエリアとして機能します。PIM-SM 動作では、マルチキャスト送信元に直接接続されたデバイスが DR になります。DR は PIM 登録メッセージを送信し、送信元からのマルチキャストトラフィックを共有ツリーの下方向へ転送する必要があることを RP に通知します。この場合、DR は最大の IP アドレスを持つデバイスです。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： <pre>Device> enable</pre>	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： <pre>Device# configure terminal</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 3	interface interface-id 例： <pre>Device(config)# interface gigabitethernet 1/0/1</pre>	設定するインターフェイスを指定して、インターフェイスコンフィギュレーションモードを開始します。 次のいずれかのインターフェイスを指定する必要があります。 <ul style="list-style-type: none"> • ルーテッドポート：レイヤ3ポートとして no switchport インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 • SVI： interface vlan vlan-id グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	ip pim query-interval seconds 例：	デバイスが PIM ルータクエリメッセージを送信する頻度を設定します。

	コマンドまたはアクション	目的
	Device(config-if)# ip pim query-interval 45	デフォルトは 30 秒です。指定できる範囲は 1 ~ 65535 です。
ステップ 5	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show ip igmp interface [interface-id] 例 : Device# show ip igmp interface	入力を確認します。
ステップ 7	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

PIM の動作の確認

PIM-SM ネットワークまたは PIM-SSM ネットワークでの IP マルチキャスト動作の確認

PIM-SM ネットワーク環境または PIM-SSM ネットワーク環境で IP マルチキャストの動作を確認する際、まずラストホップルータから検証を開始し、SPTに沿って次々にルータの検証を続け、最後にファーストホップルータの検証を行う方法が効果的です。この確認の目的は、IP マルチキャストネットワークを介して IP マルチキャストトラフィックが適切にルーティングされていることを確認することです。

PIM-SM ネットワークまたは PIM-SSM ネットワークでの IP マルチキャスト動作を確認するには、次の作業を実行します。これらの作業は、ソースとレシーバが想定どおりに動作しない場合に障害のあるホップを検出するのに役立ちます。



- (注) パケットが想定された宛先に到達しない場合は、IP マルチキャストのファストスイッチングをディセーブルにすることを検討してください。ディセーブルにすると、ルータがプロセススイッチングモードになります。IP マルチキャストのファストスイッチングをディセーブルにした後、パケットが正しい宛先に到達するようになった場合、問題は IP マルチキャストのファストスイッチングに関連している可能性があります。

ファーストホップルータでの IP マルチキャストの確認

ファーストホップルータでの IP マルチキャスト動作を確認するには、ファーストホップルータに次のコマンドを入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	show ip mroute [group-address] 例 : Device# show ip mroute 239.1.2.3 (*, 239.1.2.3), 00:18:10/stopped, RP 172.16.0.1, flags: SPF Incoming interface: Serial1/0, RPF nbr 172.31.200.2 Outgoing interface list: Null (10.0.0.1, 239.1.2.3), 00:18:10/00:03:22, flags: FT Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0 Outgoing interface list: Serial1/0, Forward/Sparse, 00:18:10/00:03:19	ファーストホップルータの mroute に F フラグが設定されていることを確認しま す。
ステップ 3	show ip mroute active [kb/s] 例 : Device# show ip mroute active Active IP Multicast Sources - sending >= 4 kbps Group: 239.1.2.3, (?) Source: 10.0.0.1 (?)	グループに送信しているアクティブなマ ルチキャスト送信元に関する情報を表示 します。このコマンドの出力では、アク ティブなソースのマルチキャストパケッ トレートに関する情報が示されます。 (注)

	コマンドまたはアクション	目的
	<pre>Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)</pre>	<p>デフォルトでは、show ip mroute コマンドと active キーワードによる出力では、4kb/s以上のレートでグループにトラフィックを送信するアクティブなソースの情報が表示されます。より低いレートのトラフィック（4 kb/s 未満のトラフィック）をグループに送信しているアクティブなソースに関する情報を表示する場合は、<i>kb/s</i> 引数に 1 の値を指定します。この引数に 1 の値を指定すると、1 kb/s以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソーストラフィックに関する情報が効果的に表示されます。</p>

SPT 上のルータでの IP マルチキャストの確認

PIM-SM または PIM-SSM ネットワーク内の SPT 上のルータでの IP マルチキャスト動作を確認するには、SPT 上のルータに次のコマンドを入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	<p>enable</p> <p>例 :</p> <pre>Device> enable</pre>	<p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	<p>show ip mroute [<i>group-address</i>]</p> <p>例 :</p> <pre>Device# show ip mroute 239.1.2.3 (*, 239.1.2.3), 00:17:56/00:03:02, RP 172.16.0.1, flags: S Incoming interface: Null, RPF nbr 0.0.0.0 Outgoing interface list: GigabitEthernet0/0/0, Forward/Sparse, 00:17:56/00:03:02 (10.0.0.1, 239.1.2.3), 00:15:34/00:03:28, flags: T</pre>	<p>特定のグループの送信元に対する RPF ネイバーを確認します。</p>

	コマンドまたはアクション	目的
	Incoming interface: Serial1/0, RPF nbr 172.31.200.1 Outgoing interface list: GigabitEthernet0/0/0, Forward/Sparse, 00:15:34/00:03:02	
ステップ 3	show ip mroute active 例 : <pre>Device# show ip mroute active Active IP Multicast Sources - sending >= 4 kbps Group: 239.1.2.3, (?) Source: 10.0.0.1 (?) Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)</pre>	<p>グループに送信しているアクティブなマルチキャスト送信元に関する情報を表示します。このコマンドの出力では、アクティブなソースのマルチキャストパケットレートに関する情報が示されます。</p> <p>(注) デフォルトでは、show ip mroute コマンドと active キーワードによる出力では、4 kb/s 以上のレートでグループにトラフィックを送信するアクティブなソースの情報が表示されます。より低いレートのトラフィック (4 kb/s 未満のトラフィック) をグループに送信しているアクティブなソースに関する情報を表示する場合は、<i>kb/s</i> 引数に 1 の値を指定します。この引数に 1 の値を指定すると、1 kb/s 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されません。これによって、存在する可能性があるすべてのアクティブなソーストラフィックに関する情報が効果的に表示されます。</p>

ラストホップルータでの IP マルチキャスト動作の確認

ラストホップルータでの IP マルチキャスト動作を確認するには、ラストホップルータで次のコマンドを入力します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : <pre>Device> enable</pre>	<p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	show ip igmp groups 例 : <pre>Device# show ip igmp groups IGMP Connected Group Membership Group Address Interface Uptime Expires Last Reporter 239.1.2.3 GigabitEthernet1/0/0 00:05:14 00:02:14 10.1.0.6 224.0.1.39 GigabitEthernet0/0/0 00:09:11 00:02:08 172.31.100.1</pre>	ラストホップルータの IGMP メンバシップを確認します。この情報によって、ラストホップルータに直接接続され、IGMP を介して認識されるレシーバが使用されているマルチキャストグループが確認されます。
ステップ 3	show ip pim rp mapping 例 : <pre>Device# show ip pim rp mapping PIM Group-to-RP Mappings Group(s) 224.0.0.0/4 RP 172.16.0.1 (?), v2v1 Info source: 172.16.0.1 (?), elected via Auto-RP Uptime: 00:09:11, expires: 00:02:47</pre>	グループと RP 間のマッピングがラストホップルータで正しく生成されていることを確認します。 (注) PIM/SSM ネットワークでラストホップルータを確認する場合は、この手順を無視してください。PIM-SSM ではランデブーポイント (RP) が使用されないため、 show ip pim rp mapping コマンドは PIM/SSM ネットワーク内のルータでは動作しません。さらに、正しく設定されている場合は、PIM/SSM グループは show ip pim rp mapping コマンドの出力には表示されません。
ステップ 4	show ip mroute 例 : <pre>Device# show ip mroute (*, 239.1.2.3), 00:05:14/00:03:04, RP 172.16.0.1, flags: SJC Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1 Outgoing interface list: GigabitEthernet1/0, Forward/Sparse, 00:05:10/00:03:04 (10.0.0.1, 239.1.2.3), 00:02:49/00:03:29, flags: T Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1 Outgoing interface list: GigabitEthernet1/0, Forward/Sparse, 00:02:49/00:03:04 (*, 224.0.1.39), 00:10:05/00:00:00, RP 0.0.0.0, flags: DC Incoming interface: Null, RPF nbr 0.0.0.0</pre>	mroute テーブルがラストホップルータに正しく入力されていることを確認します。

	コマンドまたはアクション	目的
	<pre> Outgoing interface list: GigabitEthernet1/0, Forward/Sparse, 00:05:15/00:00:00 GigabitEthernet0/0, Forward/Sparse, 00:10:05/00:00:00 (172.16.0.1, 224.0.1.39), 00:02:00/00:01:33, flags: PTX Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1 </pre>	
ステップ 5	<pre> show ip interface [type number] 例 : Device# show ip interface GigabitEthernet 0/0/0 GigabitEthernet0/0/0 is up, line protocol is up Internet address is 172.31.100.2/24 Broadcast address is 255.255.255.255 Address determined by setup command MTU is 1500 bytes Helper address is not set Directed broadcast forwarding is disabled Multicast reserved groups joined: 224.0.0.1 224.0.0.22 224.0.0.13 224.0.0.5 224.0.0.6 Outgoing access list is not set Inbound access list is not set Proxy ARP is enabled Local Proxy ARP is disabled Security level is default Split horizon is enabled ICMP redirects are always sent ICMP unreachable are always sent ICMP mask replies are never sent IP fast switching is enabled IP fast switching on the same interface is disabled IP Flow switching is disabled IP CEF switching is disabled IP Fast switching turbo vector IP multicast fast switching is enabled IP route-cache flags are Fast Router Discovery is disabled IP output packet accounting is disabled IP access violation accounting is disabled TCP/IP header compression is disabled RTP/IP header compression is disabled Policy routing is disabled Network address translation is disabled WCCP Redirect outbound is disabled </pre>	<p>マルチキャスト高速スイッチングがイネーブルになっており、ラストホップルータの発信インターフェイスでのパフォーマンスが最適化されていることを確認します。</p> <p>(注) no ip mroute-cache インターフェイスコマンドを使用すると、IP マルチキャスト高速スイッチングがディセーブルになります。IP マルチキャスト高速スイッチングがディセーブルになると、プロセス スイッチドパスを介してパケットが転送されます。</p>

	コマンドまたはアクション	目的
	<pre> WCCP Redirect inbound is disabled WCCP Redirect exclude is disabled BGP Policy Mapping is disabled </pre>	
ステップ 6	show ip mfib 例 : Device# show ip mfib	IP マルチキャスト転送情報ベース (MFIB) の転送エントリとインターフェイスが表示されます。
ステップ 7	show ip pim interface count 例 : Device# show ip pim interface count State: * - Fast Switched, H - Hardware Switching Enabled Address Interface FS Mpackets In/Out 172.31.100.2 GigabitEthernet0/0/0 * 4122/0 10.1.0.1 GigabitEthernet1/0/0 * 0/3193	マルチキャストトラフィックがラストホップルータに転送されることを確認します。
ステップ 8	show ip mroute count 例 : Device# show ip mroute count IP Multicast Statistics 6 routes using 4008 bytes of memory 3 groups, 1.00 average sources per group Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc) Group: 239.1.2.3, Source count: 1, Packets forwarded: 3165, Packets received: 3165 RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0 Source: 10.0.0.1/32, Forwarding: 3165/20/28/4, Other: 0/0/0 Group: 224.0.1.39, Source count: 1, Packets forwarded: 21, Packets received: 120 Source: 172.16.0.1/32, Forwarding: 21/1/48/0, Other: 120/0/99 Group: 224.0.1.40, Source count: 1, Packets forwarded: 10, Packets received: 10 Source: 172.16.0.1/32, Forwarding: 10/1/48/0, Other: 10/0/0	マルチキャストトラフィックがラストホップルータに転送されることを確認します。
ステップ 9	show ip mroute active [kb/s] 例 :	ラストホップルータ上のグループにトラフィックを送信しているアクティブな

	コマンドまたはアクション	目的
	<pre>Device# show ip mroute active Active IP Multicast Sources - sending >= 4 kbps Group: 239.1.2.3, (?) Source: 10.0.0.1 (?) Rate: 20 pps/4 kbps(1sec), 4 kbps(last 50 secs), 4 kbps(life avg)</pre>	<p>マルチキャスト ソースに関する情報を表示します。このコマンドの出力では、アクティブなソースのマルチキャスト パケット レートに関する情報が示されます。</p> <p>(注)</p> <p>デフォルトでは、show ip mroute コマンドと active キーワードによる出力では、4kb/s以上のレートでグループにトラフィックを送信するアクティブなソースの情報が表示されます。より低いレートのトラフィック (4 kb/s 未満のトラフィック) をグループに送信しているアクティブなソースに関する情報を表示する場合は、kb/s 引数に 1 の値を指定します。この引数に 1 の値を指定すると、1 kb/s以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソース トラフィックに関する情報が効果的に表示されます。</p>

PIM 対応ルータを使用した IP マルチキャストの到達可能性のテスト

管理しているすべての PIM 対応ルータおよびアクセス サーバーが、マルチキャスト グループのメンバで、すべてのルータが応答する原因となる ping が送信されます。これは、効果的な管理およびデバッグのツールです。

PIM 対応ルータを使用して IP マルチキャストの到達可能性をテストするには、次の作業を実行します。

マルチキャスト ping に応答するルータの設定

ルータがマルチキャスト ping に応答するように設定するには、次の手順を実行します。1つのルータ上のすべてのインターフェイスと、マルチキャストネットワーク内のすべてのルータ上のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number 例 : Device (config)# interface gigabitethernet 1/0/0	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。 <i>type</i> 引数および <i>number</i> 引数には、ホストに直接接続されているインターフェイス、またはホストに対応しているインターフェイスを指定します。
ステップ 4	ip igmp join-group group-address 例 : Device (config-if)# ip igmp join-group 225.2.2.2	(任意) 指定したグループに加入するようにルータ上のインターフェイスを設定します。 この作業の目的として、マルチキャストネットワークに加入しているルータ上のすべてのインターフェイス上で、 <i>group-address</i> 引数に同じグループアドレスを設定します。 (注) この方法では、ルータは、マルチキャストパケットの転送に加えて、マルチキャストパケットを受信します。マルチキャストパケットを受信することにより、ルータの高速スイッチングは行われません。
ステップ 5	マルチキャストネットワークに加入しているルータ上のインターフェイスで、ステップ 3 とステップ 4 を繰り返します。	--

マルチキャスト ping に応答するように設定されたルータへの ping

	コマンドまたはアクション	目的
ステップ 6	end 例： Device(config-if)# end	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。

マルチキャスト ping に応答するように設定されたルータへの ping

マルチキャスト ping に応答するように設定されているルータに対して ping テストを開始するには、ルータで次の手順を実行します。このタスクは、ネットワーク内の IP マルチキャストの到達可能性のテストに使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	ping group-address 例： Device# ping 225.2.2.2	IP マルチキャスト グループアドレスを ping します。 正常な応答は、グループアドレスが機能していることを示します。

PIM のモニタリングとトラブルシューティング

PIM 情報のモニタリング

PIM 設定をモニターするには、次の表に記載された特権 EXEC コマンドを使用します。

表 15: PIM モニタリングコマンド

コマンド	目的
show ip pim all-vrfs tunnel [tunnel tunnel_number verbose]	すべての VRF を表示します。
show ip pim autorp	グローバル Auto-RP 情報を表示します。

コマンド	目的
show ip pim boundary	インターフェイスに設定された、管理スコープ IPv4 マルチキャスト境界によってフィルタリングされた mroute に関する情報を表示します。
show ip pim interface	Protocol Independent Multicast (PIM) のために設定されているインターフェイスに関する情報を表示します。
show ip pim neighbor	PIM ネイバー情報を表示します。
show ip pim rp [<i>group-name</i> <i>group-address</i>]	スパースモードのマルチキャストグループに関連付けられた RP ルータを表示します。このコマンドは、すべてのソフトウェア イメージで使用できます。
show ip pim tunnel [<i>tunnel</i> <i>verbose</i>]	Protocol Independent Multicast (PIM) トンネルインターフェイスに関する情報を表示します。
show ip pim vrf { <i>word</i> { <i>all-vrfs</i> <i>autorp</i> <i>boundary</i> <i>bsr-router</i> <i>interface</i> <i>mdt</i> <i>neighbor</i> <i>rp</i> <i>rp-hash</i> <i>tunnel</i> } }	VPN ルーティング/転送インスタンスを表示します。
show ip igmp groups detail	特定のマルチキャスト グループを結合した対象クライアントを表示します。

RP マッピングおよび BSR 情報のモニタリング

次の表に示す特権 EXEC モードを使用して、グループ/RP マッピングの一貫性を確認します。

表 16: RP マッピングのモニタリングコマンド

コマンド	目的
<code>show ip pim rp [hostname または IP address mapping [hostname または IP address elected in-use] metric [hostname または IP address]]</code>	<p>使用可能なすべての RP マッピングおよびメトリックを表示します。これにより、(BSR または Auto-RP メカニズムを通じて) デバイスがどのように RP を学習するかがわかります。</p> <ul style="list-style-type: none"> • (任意) <i>hostname</i> を指定する場合は、RP を表示するグループの IP 名を指定します。 • (任意) <i>IP address</i> を指定する場合は、RP を表示するグループの IP アドレスを指定します。 • (任意) シスコ デバイスによって認識されている (設定されている、または Auto-RP によって取得されている) すべてのグループ/RP マッピングを表示するには、mapping キーワードを使用します。 • (任意) metric キーワードを使用して、RP RPF メトリックを表示します。
<code>show ip pim rp-hash group</code>	<p>指定したグループに選択されている RP を表示します。つまり、PIMv2 ルータまたはマルチレイヤスイッチ上で、PIMv1 システムで選択されている RP と同じ RP が使用されていることを確認します。<i>group</i> には、RP 情報を表示するグループアドレスを入力します。</p>

BSR の情報をモニターするには、次の表に示す特権 EXEC コマンドを使用します。

表 17: VTP モニタリングコマンド

コマンド	目的
<code>show ip pim bsr</code>	選択された BSR に関する情報を表示します。
<code>show ip pim bsr-router</code>	BSRv2 に関する情報を表示します。

PIMv1 および PIMv2 の相互運用性に関するトラブルシューティング

PIMv1 および PIMv2 間の相互運用性に関する問題をデバッグするには、次の点を順にチェックします。

1. **show ip pim rp-hash** 特権 EXEC コマンドを使用して RP マッピングを確認し、すべてのシステムが同じグループの同じ RP に同意していることを確認します。
2. DR と RP の各バージョン間の相互運用性を確認し、RP が DR と適切に相互作用していることを確認します（この場合は、登録停止に応答し、カプセル化が解除されたデータパケットをレジスタから転送します）。

PIM の設定例

例 : PIM スタブルルーティングのイネーブル化

次の例では、IP マルチキャストルーティングがイネーブルになっており、スイッチ A の PIM アップリンク ポート 25 はルーテッドアップリンク ポートとして設定されています

(**spare-dense-mode** がイネーブル)。VLAN 100 インターフェイスとギガビットイーサネットポート 20 で PIM スタブルルーティングがイネーブルに設定されています。

```
Device(config)# ip multicast-routing
Device(config)# interface GigabitEthernet3/0/25
Device(config-if)# no switchport
Device(config-if)# ip address 3.1.1.2 255.255.255.0
Device(config-if)# ip pim sparse-dense-mode
Device(config-if)# exit
Device(config)# interface vlan100
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface GigabitEthernet3/0/20
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface vlan100
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# ip pim passive
Device(config-if)# exit
Device(config)# interface GigabitEthernet3/0/20
Device(config-if)# no switchport
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# ip pim passive
Device(config-if)# end
```

例 : PIM スタブルルーティングの確認

各インターフェイスの PIM スタブが有効になっていることを確認するには、特権 EXEC モードで **show ip pim interface** コマンドを使用します。

```
Device# show ip pim interface
Address Interface Ver/ Nbr Query DR DR
Mode Count Intvl Prior
3.1.1.2 GigabitEthernet3/0/25 v2/SD 1 30 1 3.1.1.2
100.1.1.1 Vlan100 v2/P 0 30 1 100.1.1.1
10.1.1.1 GigabitEthernet3/0/20 v2/P 0 30 1 10.1.1.1
```

例：マルチキャストグループへの RP の手動割り当て

例：マルチキャストグループへの RP の手動割り当て

次に、マルチキャストグループ 225.2.2.2 の場合だけ、RP のアドレスを 147.106.6.22 に設定する例を示します。

```
Device(config)# access-list 1 permit 225.2.2.2 0.0.0.0
Device(config)# ip pim rp-address 147.106.6.22 1
```

例：Auto-RP の設定

次に、最大ホップ数が 31 であるすべての PIM 対応インターフェイスから RP アナウンスメントを送信する例を示します。ポート 1 の IP アドレスが RP です。アクセスリスト 5 はこのデバイスが RP として機能しているグループを示しています。

```
Device(config)# ip pim send-rp-announce gigabitethernet1/0/1 scope 31 group-list 5
Device(config)# access-list 5 permit 224.0.0.0 15.255.255.255
```

例：Auto-RP でのスパースモード

次の例では、Auto-RP でスパースモードを設定しています。

```
Device(config)# ip multicast-routing
Device(config)# ip pim autorp listener
Device(config)# ip pim send-rp-announce Loopback0 scope 16 group-list 1
Device(config)# ip pim send-rp-discovery Loopback1 scope 16
Device(config)# no ip pim dm-fallback
Device(config)# access-list 1 permit 239.254.2.0 0.0.0.255
Device(config)# access-list 1 permit 239.254.3.0 0.0.0.255
.
.
.
Device(config)# access-list 10 permit 224.0.1.39
Device(config)# access-list 10 permit 224.0.1.40
Device(config)# access-list 10 permit 239.254.2.0 0.0.0.255
Device(config)# access-list 10 permit 239.254.3.0 0.0.0.255
```

例：Auto-RP 情報を拒否する IP マルチキャスト境界の定義

次に、自動 RP 情報を拒否する IP マルチキャスト境界のコンフィギュレーション例の一部を示します。

```
Device(config)# access-list 1 deny 224.0.1.39
Device(config)# access-list 1 deny 224.0.1.40
Device(config)# access-list 1 permit all
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip multicast boundary 1
```

例：着信 RP アナウンスメント メッセージのフィルタリング

次に、候補 RP アナウンスメントが不正な候補 RP から許可されないようにするために使用される自動 RP マッピング エージェントの設定例を示します。

```
Device(config)# ip pim rp-announce-filter rp-list 10 group-list 20
Device(config)# access-list 10 permit host 172.16.5.1
Device(config)# access-list 10 permit host 172.16.2.1
Device(config)# access-list 20 deny 239.0.0.0 0.0.255.255
Device(config)# access-list 20 permit 224.0.0.0 15.255.255.255
```

マッピング エージェントは2つのデバイス (172.16.5.1 および 172.16.2.1) からの候補 RP アナウンスメントだけを許可します。マッピング エージェントは2つのデバイスからの候補 RP アナウンスメントのうち、グループ範囲が 224.0.0.0 ~ 239.255.255.255 であるマルチキャストグループ宛てのアナウンスメントだけを許可します。マッピング エージェントは、ネットワーク内の他のデバイスからの候補 RP アナウンスメントを許可しません。さらに、候補 RP アナウンスメントが 239.0.0.0 ~ 239.255.255.255 の範囲のグループに宛てたものである場合、マッピング エージェントは 172.16.5.1 または 172.16.2.1 からの候補 RP アナウンスメントを許可しません。この範囲は、管理の有効範囲付きアドレス範囲です。

例：問題のある RP への Join メッセージの送信禁止

すべてのインターフェイスが SM の場合はデフォルト設定の RP を使用し、既知のグループ 224.0.1.39 および 224.0.1.40 をサポートします。自動 RP はこれら2つの既知のグループを使用し、RP マッピング情報を収集、配信します。**ip pim accept-rp auto-rp** コマンドが設定されている場合は、RP を許可する別の **ip pim accept-rp** コマンドを次のように設定してください。

```
Device(config)# ip pim accept-rp 172.10.20.1 1
Device(config)# access-list 1 permit 224.0.1.39
Device(config)# access-list 1 permit 224.0.1.40
```

例：候補 BSR の設定

次に、候補 BSR の設定例を示します。この例では、アドバタイズ済み BSR アドレスとしてポートの IP アドレス 172.21.24.18 を、hash-mask-length として 30 ビットを使用します。プライオリティは 10 です。

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip address 172.21.24.18 255.255.255.0
Device(config-if)# ip pim sparse-mode
Device(config-if)# ip pim bsr-candidate gigabitethernet1/0/2 30 10
```

例：候補 RP の設定

次に、デバイスが自身を候補 RP として PIM ドメイン内の BSR にアドバタイズするよう設定する例を示します。標準アクセスリスト番号 4 により、ポートで識別されるアドレスを持つ RP に対応するグループプレフィックスが指定されます。この RP は、プレフィックスが 239 であるグループを処理します。

```
Device(config)# ip pim rp-candidate gigabitethernet1/0/2 group-list 4
Device(config)# access-list 4 permit 239.0.0.0 0.255.255.255
```

PIM 機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	PIM	PIM (Protocol Independent Multicast) プロトコルは、受信側が開始したメンバーシップの現在の IP マルチキャスト サービス モードを維持します。PIM は、特定のユニキャストルーティングプロトコルに依存しません。つまり、IP ルーティングプロトコルに依存せず、ユニキャストルーティングテーブルへの入力に使用されるユニキャストルーティングプロトコル (Enhanced Interior Gateway Routing Protocol (EIGRP)、Open Shortest Path First (OSPF)、およびスタティック ルート) のいずれも利用できます。PIM は、ユニキャストルーティング情報を使用してマルチキャスト転送機能を実行します。
Cisco IOS XE Gibraltar 16.12.1	双方向 PIM	双方向 PIM は、IP マルチキャスト用ルーティングプロトコルの PIM スイートのバリエーションです。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 8 章

IP マルチキャストに対する PIM MIB 拡張の設定

- [IP マルチキャストに対する PIM MIB 拡張について \(201 ページ\)](#)
- [IP マルチキャストに対する PIM MIB 拡張の設定方法 \(202 ページ\)](#)
- [PIM MIB 拡張の設定例 \(204 ページ\)](#)
- [IP マルチキャストに対する PIM MIB 拡張に関するその他の参考資料 \(204 ページ\)](#)
- [IP マルチキャストに対する PIM MIB 拡張の機能履歴 \(205 ページ\)](#)

IP マルチキャストに対する PIM MIB 拡張について

IP マルチキャストに対する SNMP トラップの PIM MIB 拡張

Protocol Independent Multicast (PIM) は、マルチキャストデータ パケットをマルチキャストグループにルーティングするために使用される IP マルチキャストルーティングプロトコルです。RFC 2934 は、IPv4 用の PIM MIB を定義します。PIM MIB は、Simple Network Management Protocol (SNMP) を使用してユーザーがリモートに PIM を監視および設定できるようにする管理対象オブジェクトを記述したものです。

PIM MIB 拡張では、次の新しいクラスの PIM 通知を導入しています。

- **neighbor-change** : この通知は、次の条件により発生します。
 - ルータの PIM インターフェイスが (インターフェイス コンフィギュレーション モードで **ip pim** コマンドを使用して) 無効化、または有効化されている。
 - ルータの PIM ネイバーの隣接関係が失効している (RFC 2934 の定義による)。
- **rp-mapping-change** : この通知は、自動 RP メッセージまたはブートストラップルータ (BSP) メッセージのいずれかが原因で、ランデブー ポイント (RP) マッピング情報が変更された場合に、発生します。
- **invalid-pim-message** : この通知は、次の条件により発生します。

- 無効な (*,G)Join または Prune メッセージがデバイスで受信された（たとえば、パケットで指定された RP がマルチキャストグループの RP でない Join または Prune メッセージをルータが受信した場合）
- 無効な PIM 登録メッセージがデバイスで受信された（たとえば、RP ではないマルチキャストグループから登録メッセージをルータが受信した場合）

PIM MIB 拡張の利点

PIM MIB 拡張：

- ユーザーは、RP マッピングの変更を検出することで、ネットワークのマルチキャストトポロジの変更を確認できます。
- PIM 対応インターフェイスで PIM プロトコルをモニターするトラップが提供されます。
- マルチキャストの隣接関係がマルチキャストインターフェイスで期限切れになったときに、ユーザーがルーティングの問題を特定するのを支援します。
- ユーザーが RP 設定エラー（たとえば、Auto-RP などのダイナミック RP 割り当てプロトコルのフラッピングによるエラーなど）をモニターできるようにします。

IP マルチキャストに対する PIM MIB 拡張の設定方法

IP マルチキャストに対する PIM MIB 拡張のイネーブル化

IP マルチキャストに対する PIM MIB 拡張を有効にするには、次のタスクを実行します。



- (注)
- pimInterfaceVersion オブジェクトは RFC 2934 から削除されたので、ソフトウェアではサポートされていません。
 - 次の MIB テーブルは、シスコソフトウェアでサポートされていません。
 - pimIpMRouteTable
 - pimIpMRouteNextHopTable

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	snmp-server enable traps pim [neighbor-change rp-mapping-change invalid-pim-message] 例 : Device(config)# snmp-server enable traps pim neighbor-change	デバイスが PIM 通知を送信できるようにします。 <ul style="list-style-type: none"> neighbor-change : このキーワードは、デバイスの PIM インターフェイスがディセーブル、またはイネーブルである、あるいはデバイスの PIM 隣接関係が失効していることを示す通知をイネーブル化します。 rp-mapping-change : このキーワードは、Auto-RP メッセージまたは BSR メッセージによる RP マッピング情報の変更を示す通知をイネーブル化します。 invalid-pim-message : このキーワードは、無効な PIM プロトコル操作のモニタリングに関する通知をイネーブル化します（たとえば、パケットに指定された RP がマルチキャスト グループの RP ではない Join または Prune メッセージをデバイスが受信する場合、または RP ではないマルチキャスト グループから登録メッセージをデバイスが受信する場合）。
ステップ 4	snmp-server host <i>host-address</i> [traps informs] <i>community-string</i> pim 例 :	PIM SNMP 通知操作の受信者を指定します。

	コマンドまたはアクション	目的
	Device(config)# snmp-server host 10.10.10.10 traps public pim	

PIM MIB 拡張の設定例

IP マルチキャストに対する PIM MIB 拡張のイネーブル化の例

次の例に、ルータの PIM インターフェイスが有効になっていることを示す通知を生成するようにルータを設定する方法を示します。最初の行では、IP アドレスが 10.0.0.1 のホストに SNMP v2c トラップとして送信されるよう、PIM トラップが設定されます。2 行目では、トラップ通知の neighbor-change クラスをホストに送信するよう、ルータが設定されます。

```
snmp-server host 10.0.0.1 traps version 2c public pim
snmp-server enable traps pim neighbor-change
interface ethernet0/0
 ip pim sparse-mode
```

IP マルチキャストに対する PIM MIB 拡張に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。 <i>Command Reference (Catalyst 9200 Series Switches)</i>

標準および RFC

標準/RFC	タイトル
draft-kouvelas-pim-bidir-new-00.txt	『A New Proposal for Bi-directional PIM』
RFC 1112	『Host Extensions for IP Multicasting』
RFC 1918	『Address Allocation for Private Internets』
RFC 2770	『GLOP Addressing in 233/8』
RFC 3569	『An Overview of Source-Specific Multicast (SSM)』

IP マルチキャストに対する PIM MIB 拡張の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	IP マルチキャストに対する PIM MIB 拡張	Protocol Independent Multicast (PIM) は、マルチキャストデータパケットをマルチキャストグループにルーティングするために使用される IP マルチキャストルーティングプロトコルです。RFC 2934 は、IPv4 用の PIM MIB を定義します。PIM MIB は、Simple Network Management Protocol (SNMP) を使用してユーザーがリモートに PIM を監視および設定できるようにする管理対象オブジェクトを記述したものです。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 9 章

SSM の設定

- [SSM の設定の前提条件](#) (207 ページ)
- [SSM 設定の制約事項](#) (208 ページ)
- [SSM に関する情報](#) (209 ページ)
- [SSM の設定方法](#) (213 ページ)
- [SSM のモニタリング](#) (220 ページ)
- [SSM の次の作業](#) (221 ページ)
- [SSM に関するその他の関連資料](#) (222 ページ)
- [SSM の機能履歴](#) (222 ページ)

SSM の設定の前提条件

次に、Source-Specific Multicast (SSM) および SSM マッピングを設定するための前提条件を示します。

- SSM マッピングを設定する前に、次の作業を実行する必要があります。
 - IP マルチキャスト ルーティングをイネーブルにします。
 - PIM スパース モードをイネーブルにします。
 - SSM を設定します。
- スタティック SSM マッピングを設定する場合は、事前にアクセス コントロール リスト (ACL) を設定して、送信元アドレスにマッピングされるグループ範囲を定義する必要があります。
- SSM マッピングを設定し、DNS ルックアップで使用できるようにするには、稼働中の DNS サーバーにレコードを追加する必要があります。稼働中の DNS サーバーがない場合は、DNS サーバーをインストールする必要があります。



(注) 実行中の DNS サーバーにレコードを追加するには、*Cisco Network Registrar* などの製品を使用できます。

SSM 設定の制約事項

次に、SSM を設定する際の制約事項を示します。

- IGMPv3 で SSM を使用するには、Cisco IOS ルータ、アプリケーションが稼働しているホスト、そしてアプリケーション自体が SSM をサポートしている必要があります。
- SSM にまだ対応していない、ネットワーク内の既存のアプリケーションは、(S, G) チャンネル加入をサポートするように変更されないと、SSM 範囲内では機能しません。そのため、既存のアプリケーションが指定の SSM 範囲内のアドレスを使用する場合、ネットワークで SSM をイネーブルにすると問題が発生することがあります。
- IGMP スヌーピング：IGMPv3 で使用される新しいメンバーシップ レポート メッセージは、旧型の IGMP スヌーピングデバイスでは正しく認識されない場合があります。
- SSM をレイヤ 2 スイッチング メカニズムとともに使用する場合は、ある程度のアドレス管理が必要となります。Cisco Group Management Protocol (CGMP)、IGMP スヌーピング、または Router-Port Group Management Protocol (RGMP) でサポートされるのはグループ固有のフィルタリングだけであり、(S, G) チャンネル固有のフィルタリングはサポートされていません。同じスイッチドネットワーク内の異なるレシーバーが異なる (S, G) チャンネルを要求し、これらのチャンネルが同じグループを共有している場合、レシーバーは上記のような既存メカニズムの利点を活用できません。どちらのレシーバーも、すべての (S, G) チャンネルトラフィックを受信し、不要なトラフィックを入力から除外します。SSM は、独立した多くのアプリケーションに SSM 範囲のグループアドレスを再利用できるので、このような状況では、スイッチドネットワークのトラフィック フィルタリング機能が低下する可能性があります。そのため、アプリケーションに対して SSM 範囲の IP アドレスをランダムに使用し、SSM 範囲内の 1 つのアドレスがさまざまなアプリケーションに再利用される可能性を小さくすることが重要です。たとえば、TV チャンネルセットを提供するアプリケーションサービスで、SSM を使用する場合は、各 TV (S, G) チャンネルに異なるグループを使用する必要があります。このようにすれば、同じアプリケーションサービス内の異なるチャンネルに複数のレシーバが接続されていても、レイヤ 2 デバイスを含むネットワークでトラフィック エイリアシングが発生しなくなります。
- PIM-SSM では、ラストホップ ルータは、そのインターフェイス上に適切な (S, G) 加入登録があると、定期的に (S, G) Join メッセージを送信し続けます。このため、レシーバが (S, G) 加入を送信する限り、ソースが長時間（または二度と）トラフィックを送信しなくてもレシーバからソースへの最短パス ツリー (SPT) 状態が維持されます。

送信元がトラフィックを送信し、レシーバーがグループに加入している場合にだけ (S, G) ステートが維持される PIM-SM では、これとは対照的な状況が発生します。PIM-SM では、送信元がトラフィックの送信を 3 分以上停止すると、(S, G) ステートは削除され、その送信元からのパケットが RPT を通じて再度到達した場合のみに再確立されます。PI-SSM では、送信元がアクティブであることをレシーバに通知するメカニズムがないので、レシーバが (S, G) チャンネルの受信を要求している限り、(S, G) ステートを維持する必要があります。

次に、SSM マッピングを設定する際の制約事項を示します。

- SSM マッピング機能で、SSM の利点をすべて共有できるわけではありません。SSM マッピングでは、ホストからグループ G の加入が取得され、1つまたは複数のソースに関連付けられているアプリケーションでこのグループを指定できるため、グループ G ごとにこのようなアプリケーション1つのみをサポートできます。それにもかかわらず、完全な SSM アプリケーションは、SSM マッピングにも使用される同じグループを共有することができます。
- 完全な SSM への移行ソリューションとして SSM マッピングだけを使用する場合は、ラストホップルータの IGMPv3 をイネーブルにする際に十分に注意してください。SSM マッピングと IGMPv3 を両方イネーブルにした場合、すでに IGMPv3 をサポートしている (SSM はサポートしていない) ホストは IGMPv3 グループ レポートを送信します。SSM マッピングは、このような IGMPv3 グループ レポートをサポートしていないので、ルータは送信元をこれらのレポートと正しく関連付けることができません。

SSM に関する情報

Source-Specific Multicast (SSM; 送信元特定マルチキャスト) 機能は、IP マルチキャストの拡張機能であり、この機能を使用すると、受信者に転送されるデータグラムトラフィックは、その受信者が明示的に加入しているマルチキャスト送信元からのトラフィックだけになります。SSM 用にマルチキャスト グループを設定する場合、SSM 配信ツリー (共有ツリーはない) だけが作成されます。

ここでは、Source-Specific Multicast (SSM) の設定方法を説明します。この項の SSM コマンドの詳細な説明については、『*IP Multicast Command Reference*』を参照してください。

SSM コンポーネントの概要

SSM は、1対多のアプリケーション (ブロードキャストアプリケーション) に最適なデータグラム配信モデルです。SSM は、オーディオおよびビデオのブロードキャスト アプリケーション環境を対象としたシスコの IP マルチキャスト ソリューションの中核的なネットワークングテクノロジーです。このデバイスは、次のコンポーネントをサポートしているため、SSM の実装が可能です。

- Protocol Independent Multicast Source-Specific Mode (PIM-SSM)

PIM-SSM は、SSM の実装をサポートするルーティング プロトコルで、PIM Sparse Mode (PIM-SM) に基づいています。

- Internet Group Management Protocol version 3 (IGMPv3)

SSM および Internet Standard Multicast (ISM)

インターネットの現行の IP マルチキャスト インフラストラクチャや多くの企業のイントラネットは、PIM-SM プロトコルと Multicast Source Discovery Protocol (MSDP) に基づいています。これらのプロトコルには、Internet Standard Multicast (ISM) サービス モデルの限界がありま

す。たとえば、ISM では、ネットワークは、実際にマルチキャストトラフィックを送信しているホストについての情報を維持する必要があります。

ISM サービスは、任意の送信元からマルチキャストホストグループと呼ばれるレシーバーグループへの IP データグラムの配信でなりたっています。マルチキャストホストグループのデータグラムトラフィックは、任意の IP ユニキャスト送信元アドレス (S) と IP 宛先アドレスとしてのマルチキャストグループアドレス (G) のデータグラムで構成されます。システムは、ホストグループのメンバーになることによって、このトラフィックを受信します。ホストグループのメンバーシップには IGMP バージョン 1、2、または 3 によるホストグループのシグナリングが必要です。

SSM では、データグラムは (S, G) チャンネルに基づいて配信されます。SSM と ISM のどちらでも、ソースになるためにシグナリングは必要ありません。ただし、SSM では、レシーバーは特定の送信元からのトラフィックの受信または非受信を決めるために (S, G) への加入または脱退を行う必要があります。つまり、レシーバーは加入した (S, G) チャンネルからだけトラフィックを受信できます。一方、ISM では、レシーバーは受信するトラフィックの送信元の IP アドレスを知る必要はありません。チャンネル加入シグナリングの標準的な方法として、IGMP を使用してモードメンバーシップレポートを包含することが提案されていますが、この手法をサポートしているのは IGMP version 3 だけです。

SSM IP アドレスの範囲

IP マルチキャストグループアドレス範囲の設定済みのサブセットに SSM 配信モデルを適用することにより、SSM と ISM サービスを一緒に使用できます。Cisco IOS ソフトウェアでは、224.0.0.0 ~ 239.255.255.255 の IP マルチキャストアドレス範囲の SSM 設定が可能です。SSM 範囲が定義されている場合、既存の IP マルチキャスト受信アプリケーションが SSM 範囲のアドレスの使用を試行しても、トラフィックを受信できません。

SSM の動作

確立されているネットワークは、IP マルチキャストサービスが PIM SSM に基づいているので、SSM サービスをサポートできます。SSM サービスだけが必要な場合は、ドメイン間の PIM-SM に必要な全プロトコル範囲 (MSDP、Auto-RP、またはブートストラップルータ (BSR)) ではなく、SSM を単独でネットワークに配置することもできます。

PIM-SM 用に設定されているネットワークに SSM を配置する場合、SSM をサポートするのはラストホップルータだけです。レシーバーに直接接続されていないルータは SSM をサポートする必要はありません。一般的に、ラストホップ以外のルータに必要なのは、SSM 範囲内の PIM-SM だけです。このようなルータは SSM 範囲内での MSDP シグナリング、登録、PIM-SM 共有ツリー操作を抑制するために、ほかのアクセスコントロール設定が必要になる場合もあります。

SSM の範囲を設定し SSM をイネーブルにするには、**ip pim ssm** グローバル コンフィギュレーション コマンドを使用します。この設定による影響は次のとおりです。

- SSM 範囲内のグループは、IGMPv3 include モードメンバーシップレポートを通じて、(S, G) チャンネルに加入できます。

- SSM 範囲のアドレスの PIM 動作は、PIM-SM の派生モードである PIM-SSM に変更されます。このモードでは、ルータで生成されるのは PIM (S, G) の join と prune のメッセージだけであり、(S, G) の Rendezvous Point Tree (RPT) や (*, G) の RPT メッセージは生成されません。RPT 動作に関連する着信メッセージは無視されるか拒否されます。着信 PIM 登録メッセージに対しては即座に register-stop メッセージで応答が行われます。ラストホップルータ以外のルータでは、PIM-SSM は PIM-SM と下位互換性を保ちます。したがって、ラストホップルータ以外のルータは SSM グループに PIM-SM を使用できません (SSM をサポートしていない場合など)。
- SSM 範囲内の Source-Active (SA) メッセージは、受け入れ、生成、転送のいずれも実行されません。

SSM マッピング

典型的なセットトップボックス (STB) 配置では、各 TV チャンネルは独立した 1 つの IP マルチキャストグループを使用し、その TV チャンネルの送信を行うアクティブなサーバーは 1 つです。1 つのサーバーから複数の TV チャンネルへの送信は可能ですが、各チャンネルのグループはそれぞれ異なります。このようなネットワーク環境で、ルータが特定のグループの IGMPv1 または IGMPv2 のメンバーシップレポートを受信した場合、レポートの宛先は、そのマルチキャストグループに関連付けられている TV チャンネルの well-known TV サーバーになります。

SSM マッピングが設定されている場合、特定グループの IGMPv1 または IGMPv2 のメンバーシップレポートを受信したルータは、レポートを、このグループに関連付けられている well-known 送信元の 1 つ以上のチャンネルメンバーシップに変換します。

ルータは、IGMPv1 または IGMPv2 のメンバーシップレポートを受信すると、SSM マッピングを使用して、そのグループに 1 つ以上の送信元 IP アドレスを決定します。その後、SSM マッピングによって、そのメンバーシップレポートが IGMPv3 レポートに変換され、IGMPv3 レポートを受信した場合と同様に処理が続行されます。IGMPv1 または IGMPv2 メンバーシップレポートの受信が続き、そのグループの SSM マッピングが同じである限り、ルータは PIM join を送信し、グループに加入し続けます。

SSM マッピング機能を使用すると、ラストホップルータはスタティックに設定されたルータ上のテーブルまたは DNS サーバーを通じて、送信元アドレスを決定できます。スタティックに設定されたテーブルまたは DNS マッピングが変更された場合、ルータは加入しているグループに関連付けられている現在の送信元から脱退します。

スタティック SSM マッピング

スタティック SSM マッピングでは、ラストホップルータは、グループへの送信を行う送信元を決定するために、継続的にスタティック マップを使用します。スタティック SSM マッピングを使用するには、グループ範囲を定義した ACL を設定する必要があります。グループ範囲を定義する ACL を設定した後、**ip igmp ssm-map static** グローバル コンフィギュレーション コマンドを使用して、ACL で許可されたグループを送信元にマッピングできます。

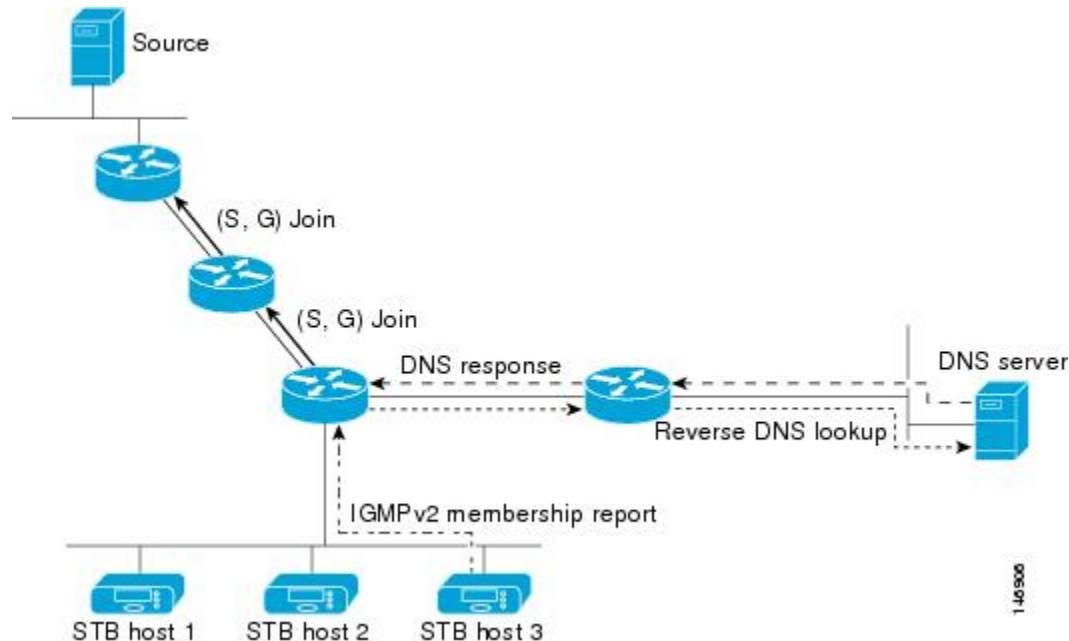
DNSが必要とされないか、またはローカルでDNSマッピングが変更される場合、小規模なネットワークではスタティック SSM マッピングを設定できます。設定されたスタティック SSM マッピングは、DNS マッピングよりも優先されます。

DNS ベースの SSM マッピング

DNSベースのSSMマッピングを使用して、ラストホップルータが継続的に逆DNSルックアップを実行し、グループに送信する送信元を決定するようにすることも可能です。DNSベースのSSMマッピングが設定されると、ルータはグループ名を含むドメイン名を構築し、DNSへの逆ルックアップを実行します。ルータはIPアドレスリソースを検索し、それらをグループに関連付けられた送信元アドレスとして使用します。SSMマッピングでサポートできる送信元数は、グループごとに最大20です。ルータは各グループに設定されているすべてのソースに加入します。

図 16: DNS ベースの SSM マッピング

次の図は、DNS ベースの SSM マッピングを示します。



ラストホップルータが1つのグループの複数の送信元に加入できるようにするSSMマッピングメカニズムによって、TVブロードキャストの送信元に冗長性を持たせることができます。この場合、ラストホップルータは、SSMマッピングを使用し、同じTVチャンネルに対して2つのビデオ送信元に同時に加入することにより冗長性を提供します。ただし、ラストホップルータでのビデオトラフィックの重複を防ぐため、ビデオ送信元がサーバー側でスイッチオーバーメカニズムを使用する必要があります。一方のビデオ送信元はアクティブ、もう一方のバックアップビデオ送信元はパッシブになります。パッシブの送信元は待機状態になり、アクティブな送信元の障害が検出された場合に、そのTVチャンネルにビデオトラフィックを送信します。サーバー側のスイッチオーバーメカニズムによって、実際にそのTVチャンネルにビデオトラフィックを送信するサーバーは1つだけになります。

G1、G2、G3、G4を含むグループの1つ以上の送信元アドレスを検索するには、DNS サーバーに次のような DNS レコードを設定する必要があります。

```
G4.G3.G2.G1 [multicast-domain] [timeout] IN A source-address-1
IN A source-address-2
IN A source-address-n
```

DNS リソース レコードの設定の詳細については、DNS サーバーのマニュアルを参照してください。

SSM の設定方法

SSM の設定

SSM を設定するには、次の手順を実行します。

この手順は任意です。

始める前に

Source Specific Multicast (SSM) 範囲の定義にアクセスリストを使用する場合、**ip pim ssm** コマンドでアクセスリストを参照する前にアクセスリストを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip pim ssm [default range access-list] 例： Device(config)# ip pim ssm range 20	IP マルチキャストアドレスの SSM 範囲を定義します。

	コマンドまたはアクション	目的
ステップ 4	interface type number 例 : Device(config)# interface gigabitethernet 1/0/1	IGMPv3 をイネーブルに設定可能なホストに接続されているインターフェイスを選択し、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。 次のいずれかのインターフェイスを指定する必要があります。 <ul style="list-style-type: none"> • ルーテッドポート：レイヤ3ポートとして no switchport インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 • SVI： interface vlan vlan-id グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 5	ip pim {sparse-mode } 例 : Device(config-if)# ip pim sparse-mode	インターフェイスに対して PIM をイネーブルにします。
ステップ 6	ip igmp version 3 例 : Device(config-if)# ip igmp version 3	このインターフェイス上で IGMPv3 をイネーブルにします。デフォルトでは、IGMP のバージョン 2 が設定されます。
ステップ 7	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 8	show running-config 例 : Device# show running-config	入力を確認します。

	コマンドまたはアクション	目的
ステップ 9	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

Source-Specific Multicast (SSM) マッピングの設定

Source Specific Multicast (SSM) マッピング機能は、管理上または技術上の理由からエンドシステムで SSM をサポートできないかまたはサポートが望ましくない場合に SSM 移行手段として使用できます。SSM マッピングを使用すると、IGMPv3 をサポートしないレガシー STB へのビデオ配信や、IGMPv3 ホストスタックを使用しないアプリケーションに SSM を活用できます。

スタティック SSM マッピングの設定

スタティック SSM マッピングを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip igmp ssm-map enable 例 : Device(config)# ip igmp ssm-map enable	設定されている SSM 範囲で、グループの SSM マッピングをイネーブルにします。 (注) このコマンドでは、デフォルトで、DNS ベースの SSM マッピングがイネーブルにされます。

	コマンドまたはアクション	目的
ステップ 4	no ip igmp ssm-map query dns 例 : <pre>Device(config)# no ip igmp ssm-map query dns</pre>	(任意) DNS ベースの SSM マッピングをディセーブルにします。 (注) スタティック SSM マッピングだけを使用する場合は、DNS ベースの SSM マッピングをディセーブルにします。デフォルトでは、 ip igmp ssm-map コマンドによって DNS ベースの SSM マッピングがイネーブルになります。
ステップ 5	ip igmp ssm-map static access-list source-address 例 : <pre>Device(config)# ip igmp ssm-map static 11 172.16.8.11</pre>	スタティック SSM マッピングを設定します。 <ul style="list-style-type: none"> • access-list 引数に入力した ACL によって、source-address 引数に入力したソース IP アドレスにマッピングされるグループが決まります。 (注) 追加のスタティック SSM マッピングを設定することもできます。SSM マッピングを追加設定した場合、ルータが SSM 範囲のグループの IGMPv1 または IGMPv2 のメンバーシップレポートを受信すると、デバイスは、設定されている各 ip igmp ssm-map static コマンドに基づいて、そのグループに関連付けられている送信元アドレスを特定します。デバイスは各グループに最大 20 の送信元を関連付けます。 必要な場合は、ステップを繰り返して、追加のスタティック SSM マッピングを設定します。
ステップ 6	end 例 : <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例 :	入力を確認します。

	コマンドまたはアクション	目的
	Device# show running-config	
ステップ 8	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

DNS ベースの SSM マッピングの設定

DNS ベースの SSM マッピングを設定するには、DNS サーバー ゾーンを作成するか、または既存のゾーンにレコードを追加する必要があります。DNS ベースの SSM マッピングを使用するルータが他の目的にも DNS を使用している場合は、通常の設定の DNS サーバーを使用する必要があります。そのルータで使用されている DNS 実装が DNS ベースの SSM マッピングだけの場合は、ルート ゾーンが空であるか、またはそれ自身を指すようなフォールス DNS セットアップが可能です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip igmp ssm-map enable 例 : Device(config)# ip igmp ssm-map enable	設定されている SSM 範囲で、グループの SSM マッピングをイネーブルにします。
ステップ 4	ip igmp ssm-map query dns 例 : Device(config)# ip igmp ssm-map query dns	(任意) DNS ベースの SSM マッピングをイネーブルにします。 • デフォルトでは、 ip igmp ssm-map コマンドによって DNS ベースの SSM マッピングがイネーブルにな

	コマンドまたはアクション	目的
		<p>ります。実行コンフィギュレーションに保存されるのは、このコマンドを no 形式で使用した場合だけです。</p> <p>(注) DNS ベースの SSM マッピングがディセーブルの場合、このコマンドを使用して DNS ベースの SSM マッピングを再度イネーブルにします。</p>
ステップ 5	<p>ip domain multicast <i>domain-prefix</i></p> <p>例 :</p> <pre>Device(config)# ip domain multicast ssm-map.cisco.com</pre>	<p>(任意) DNS ベースの SSM マッピングに使用するドメインプレフィックスを変更します。</p> <ul style="list-style-type: none"> デフォルトでは、ip-addr.arpa ドメインプレフィックスが使用されます。
ステップ 6	<p>ip name-server <i>server-address1</i> [<i>server-address2...server-address6</i>]</p> <p>例 :</p> <pre>Device(config)# ip name-server 10.48.81.21</pre>	<p>名前とアドレスの解決に使用する 1 つまたは複数のネームサーバーのアドレスを指定します。</p>
ステップ 7	冗長性のために追加の DNS サーバーを設定する場合は、必要に応じて、ステップ 6 を繰り返します。	
ステップ 8	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 9	<p>show running-config</p> <p>例 :</p> <pre>Device# show running-config</pre>	入力を確認します。
ステップ 10	<p>copy running-config startup-config</p> <p>例 :</p> <pre>Device# copy running-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

	コマンドまたはアクション	目的
	<code>startup-config</code>	

SSM マッピングを使用したスタティック トラフィック転送の設定

ラスト ホップ ルータ上の SSM マッピングでスタティック トラフィック転送を設定する場合は、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例 : Device(config)# interface gigabitethernet 1/0/1	SSM マッピングを使用してマルチキャスト グループにスタティックにトラフィックを転送するインターフェイスを選択し、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。 次のいずれかのインターフェイスを指定する必要があります。 <ul style="list-style-type: none"> ルーテッドポート：レイヤ3ポートとして no switchport インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 SVI： interface vlan vlan-id グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。 (注)

	コマンドまたはアクション	目的
		SSM マッピングを使用したトラフィックのスタティック転送は、DNS ベースの SSM マッピングとスタティックに設定された SSM マッピングのいずれかで機能します。
ステップ 4	ip igmp static-group group-address source ssm-map 例 : <pre>Device(config-if)# ip igmp static-group 239.1.2.1 source ssm-map</pre>	そのインターフェイスから (S,G) チャンネルへのスタティック転送用の SSM マッピングを設定します。 このコマンドは、特定グループに SSM トラフィックをスタティックに転送する場合に使用します。チャンネルの送信元アドレスを決定するには DNS ベースの SSM マッピングを使用します。
ステップ 5	end 例 : <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例 : <pre>Device# show running-config</pre>	入力を確認します。
ステップ 7	copy running-config startup-config 例 : <pre>Device# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

SSM のモニタリング

SSM をモニターするには、次の表の特権 EXEC コマンドを使用します。

表 18: SSM のモニタリングコマンド

コマンド	目的
show ip igmp groups detail	IGMPv3 による (S,G) チャンネル加入登録を表示します。

コマンド	目的
show ip mroute	マルチキャストグループがSSMサービスをサポートしているかどうか、または送信元固有のホストレポートが受信されたかどうかを表示します。

SSM マッピングのモニタリング

SSM マッピングをモニターするには、次の表の特権 EXEC コマンドを使用します。

表 19: SSM マッピングをモニターするコマンド

コマンド	目的
show ip igmp ssm-mapping	SSM マッピングについての情報を表示
show ip igmp ssm-mapping <i>group-address</i>	SSM マッピングが特定のグループに存在しているかどうかを表示します。
show ip igmp groups [<i>group-name</i> <i>group-address</i> <i>interface-type interface-number</i>] [detail]	ルータに直接接続されているレシーバが学習されたレシーバを持つマルチキャストグループを表示します。
show host	デフォルトのドメイン名、名前ルックアップテーブル、名前サーバーホストのリスト、および最近のキャッシュされたリストを表示
debug ip igmp <i>group-address</i>	送受信された IGMP パケットと IGMP ホストレポートを表示します。

SSM の次の作業

次の設定を行えます。

- IGMP
- PIM
- IP マルチキャスト ルーティング
- サービス検出ゲートウェイ

SSM に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャストルーティングのコマンド」の項を参照してください。 <i>Command Reference (Catalyst 9200 Series Switches)</i>

標準および RFC

標準/RFC	タイトル
RFC 4601	『 <i>Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification</i> 』

SSM の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	SSM	SSM は、受信者が明示的に参加したマルチキャストソースからのみデータグラムトラフィックが受信者に転送される IP マルチキャストの拡張機能です。SSM 用にマルチキャストグループを設定する場合、SSM 配信ツリー（共有ツリーはない）だけが作成されます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 10 章

IPv6 マルチキャストの実装

- [IPv6 マルチキャストルーティングの実装に関する情報 \(223 ページ\)](#)
- [IPv6 マルチキャストの実装 \(233 ページ\)](#)
- [その他の参考資料 \(259 ページ\)](#)
- [IPv6 マルチキャストの機能履歴 \(259 ページ\)](#)

IPv6 マルチキャスト ルーティングの実装に関する情報

この章では、スイッチに IPv6 マルチキャスト ルーティングを実装する方法について説明します。

従来の IP 通信では、ホストはパケットを単一のホスト（ユニキャスト伝送）またはすべてのホスト（ブロードキャスト伝送）に送信できます。IPv6 マルチキャストは、第三の方式を提供するものであり、ホストが単一のデータストリームをすべてのホストのサブセット（グループ伝送）に同時に送信できるようにします。

IPv6 マルチキャストの概要

IPv6 マルチキャスト グループは、特定のデータ ストリームを受信する受信側の任意のグループです。このグループには、物理的境界または地理的境界はありません。受信側は、インターネット上または任意のプライベート ネットワーク内の任意の場所に配置できます。特定のグループへのデータ フローの受信に関与する受信側は、ローカル スイッチに対してシグナリングすることによってそのグループに加入する必要があります。このシグナリングは、MLD プロトコルを使用して行われます。

スイッチは、MLD プロトコルを使用して、直接接続されているサブネットにグループのメンバーが存在するかどうかを学習します。ホストは、MLD レポート メッセージを送信することによってマルチキャストグループに加入します。ネットワークでは、各サブネットでマルチキャストデータのコピーを1つだけ使用して、潜在的に無制限の受信側にデータが伝送されます。トラフィックの受信を希望する IPv6 ホストはグループ メンバと呼ばれます。

グループ メンバに伝送されるパケットは、単一のマルチキャストグループ アドレスによって識別されます。マルチキャストパケットは、IPv6 ユニキャストパケットと同様に、ベストエフォート型の信頼性を使用してグループに伝送されます。

マルチキャスト環境は、送信側と受信側で構成されます。どのホストも、グループのメンバーであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバーだけがメッセージをリッスンして受信できます。

マルチキャストアドレスがマルチキャストグループの受信先として選択されます。送信者は、データグラムの宛先アドレスとしてグループのすべてのメンバーに到達するためにそのアドレスを使用します。



(注) RFC 4291 によると、FF0x::/12 (IPv6 宛先アドレスの T フラグが 0 に設定されている) は、永続的に割り当てられた (「既知の」) IPv6 マルチキャストアドレス範囲です。

Cisco Catalyst 9200 シリーズ スイッチでは、このアドレス範囲のパケットのデフォルトの動作は、入力 VLAN でのフラッドです。

マルチキャストグループ内のメンバーシップはダイナミックです。ホストはいつでも加入および脱退できます。マルチキャストグループ内のメンバーの場所または数に制約はありません。ホストは、一度に複数のマルチキャストグループのメンバーにすることができます。

マルチキャストグループがどの程度アクティブであるか、その期間、およびメンバーシップはグループおよび状況によって異なります。メンバーを含むグループにアクティビティがない場合もあります。

IPv6 マルチキャストルーティングの実装

Cisco IOS ソフトウェアでは、IPv6 マルチキャストルーティングを実装するため、次のプロトコルがサポートされています。

- MLD は、直接接続されているリンク上のマルチキャストリスナー (特定のマルチキャストアドレスを宛先としたマルチキャストパケットを受信するために使用するノード) を検出するために IPv6 スイッチで使用されます。MLD には 2 つのバージョンがあります。MLD バージョン 1 はバージョン 2 のインターネットグループ管理プロトコル (IGMP) for IPv4 をベースとしています。MLD バージョン 2 はバージョン 3 の IGMP for IPv4 をベースとしています。Cisco IOS ソフトウェアの IPv6 マルチキャストでは、MLD バージョン 2 と MLD バージョン 1 の両方が使用されます。MLD バージョン 2 は、MLD バージョン 1 と完全な下位互換性があります (RFC 2710 で規定)。MLD バージョン 1 だけをサポートするホストは、MLD バージョン 2 を実行しているスイッチと相互運用します。MLD バージョン 1 ホストと MLD バージョン 2 ホストの両方が混在する LAN もサポートされています。
- PIM-SM は、相互に転送されるマルチキャストパケット、および直接接続されている LAN に転送されるマルチキャストパケットを追跡するためにスイッチ間で使用されます。
- PIM in Source Specific Multicast (PIM-SSM) は PIM-SM と類似していますが、IP マルチキャストアドレスを宛先とした特定の送信元アドレス (または特定の送信元アドレスを除くすべてのアドレス) からのパケットを受信する対象をレポートする機能を別途備えています。

IPv6 マルチキャスト リスナー ディスカバリ プロトコル

キャンパスネットワークでマルチキャストの実装を開始するには、ユーザーは最初に、誰がマルチキャストを受信するかを定義する必要があります。MLD プロトコルは、直接接続されているリンク上のマルチキャストリスナー（たとえば、マルチキャストパケットを受信するノード）の存在を検出するため、およびこれらのネイバー ノードを対象にしている特定のマルチキャストアドレスを検出するために、IPv6 スイッチによって使用されます。これは、ローカル グループおよび送信元固有のグループ メンバーシップの検出に使用されます。

MLD プロトコルは、特別なマルチキャスト クエリアおよびホストを使用して、ネットワーク全体でマルチキャストトラフィックのフローを自動的に制御および制限する手段を提供します。

マルチキャスト クエリアとマルチキャスト ホスト

マルチキャスト クエリアは、クエリー メッセージを送信して、特定のマルチキャスト グループのメンバーであるネットワーク デバイスを検出するネットワーク デバイス（スイッチなど）です。

マルチキャスト ホストは、受信側（スイッチを含む）としてレポート メッセージを送信し、クエリアにホスト メンバーシップを通知します。

同じ送信元からのマルチキャスト データ ストリームを受信する一連のクエリアおよびホストは、マルチキャスト グループと呼ばれます。クエリアおよびホストは、MLD レポートを使用して、マルチキャスト グループに対する加入および脱退を行ったり、グループトラフィックの受信を開始したりします。

MLD では、メッセージの伝送にインターネット制御メッセージプロトコル（ICMP）が使用されます。すべての MLD メッセージはホップ制限が 1 のリンクローカルであり、すべてにスイッチアラート オプションが設定されています。スイッチアラート オプションは、ホップバイホップ オプション ヘッダーの実装を意味します。

MLD アクセス グループ

MLD アクセス グループは、Cisco IOS IPv6 マルチキャスト スイッチでの受信側アクセス コントロールを実現します。この機能では、受信側が加入できるグループのリストを制限し、SSM チャネルへの加入に使用される送信元を許可または拒否します。

受信側の明示的トラッキング

明示的トラッキング機能を使用すると、スイッチが IPv6 ネットワーク内のホストの動作を追跡できるようになります。また、この機能により、高速脱退メカニズムを MLD バージョン 2 のホスト レポートで使用できるようになります。

プロトコル独立マルチキャスト

PIM（Protocol Independent Multicast）は、相互に転送されるマルチキャストパケット、および直接接続されている LAN に転送されるマルチキャストパケットを追跡するためにスイッチ間

で使用されます。PIM は、ユニキャストルーティング プロトコルとは独立して動作し、他のプロトコルと同様に、マルチキャスト ルート アップデートの送受信を実行します。ユニキャストルーティング テーブルに値を入力するために LAN でどのユニキャストルーティング プロトコルが使用されているかどうかにかかわらず、Cisco IOS PIM では、独自のルーティング テーブルを構築および管理する代わりに、既存のユニキャスト テーブル コンテンツを使用し、Reverse Path Forwarding (RPF) チェックを実行します。

PIM-SM または PIM-SSM のいずれかを使用するように IPv6 マルチキャストを設定することも、ネットワークで PIM-SM と PIM-SSM の両方を使用することもできます。

PIM スパース モード

IPv6 マルチキャストでは、PIM-SM を使用したドメイン内マルチキャストルーティングがサポートされています。PIM-SM は、ユニキャストルーティングを使用して、マルチキャスト ツリー構築用のリバースパス情報を提供しますが、特定のユニキャストルーティング プロトコルには依存しません。

PIM-SM は、トラフィックに対して明示的な要求がある場合を除いて、各マルチキャストに関与しているスイッチの数が比較的少なく、これらのスイッチがグループのマルチキャスト パケットを転送しないときに、マルチキャスト ネットワークで使用されます。PIM-SM は、共有 ツリー上のデータ パケットを転送することによって、アクティブな送信元に関する情報を配布します。PIM-SM は最初に共有 ツリーを使用しますが、これには RP の使用が必要となります。

要求は、ツリーのルート ノードに向けてホップバイホップで送信される PIM join を使用して行われます。PIM-SM のツリーのルート ノードは、共有 ツリーの場合は RP、最短パス ツリー (SPT) の場合はマルチキャスト送信元に直接接続されているファーストホップスイッチになります。RP はマルチキャストグループを追跡し、マルチキャストパケットを送信するホストはそのホストのファーストホップスイッチによって RP に登録されます。

PIM join がツリーの上位方向に送信されると、要求されたマルチキャストトラフィックがツリーの下位方向に転送されるように、パス上のスイッチがマルチキャスト転送ステートを設定します。マルチキャストトラフィックが不要になったら、スイッチはルート ノードに向けてツリーの上位方向に PIM prune を送信し、不必要なトラフィックをプルニング (削除) 送信します。この PIM prune がホップごとにツリーを上位方向に移動する際、各スイッチはその転送状態を適切に更新します。最終的に、マルチキャストグループまたは送信元に関連付けられている転送ステータスは削除されます。

マルチキャストデータの送信側は、マルチキャストグループを宛先としたデータを送信します。送信側の指定スイッチ (DR) は、これらのデータ パケットを受け取り、ユニキャストでカプセル化し、RP に直接送信します。RP は、カプセル化されたこれらのデータ パケットを受信し、カプセル化を解除し、共有 ツリー上に転送します。そのあと、パケットは、RP ツリー上のスイッチの (*,G) マルチキャスト ツリー ステータスに従って、RP ツリー ブランチの任意の場所に複製され、そのマルチキャストグループのすべての受信側に最終的に到達します。RP へのデータ パケットのカプセル化のプロセスは登録と呼ばれ、カプセル化されたパケットは PIM レジスタ パケットと呼ばれます。

IPv6 BSR : RP マッピングの設定

ドメイン内の PIM スイッチは、各マルチキャストグループを正しい RP アドレスにマッピングできる必要があります。PIM-SM 対応の BSR プロトコルは、グループと RP のマッピング情報をドメイン全体に迅速に配布するためのダイナミック適応メカニズムを備えています。IPv6 BSR 機能を使用すると、到達不能になった RP が検出され、マッピングテーブルが変更されます。これにより、到達不能な RP が今後使用されなくなり、新しいテーブルがドメイン全体に迅速に配布されるようになります。

すべての PIM-SM マルチキャストグループを RP の IP または IPv6 アドレスに関連付ける必要があります。新しいマルチキャスト送信側が送信を開始すると、そのローカル DR がこれらのデータパケットを PIM register メッセージにカプセル化し、そのマルチキャストグループの RP に送信します。新しいマルチキャスト受信側が加入すると、そのローカル DR がそのマルチキャストグループの RP に PIM join メッセージを送信します。PIM スイッチは、(*, G) join メッセージを送信するとき、RP 方向への次のスイッチを認識して、G (グループ) がそのスイッチにメッセージを送信できるようにする必要があります。また、PIM スイッチは、(*, G) ステートを使用してデータパケットを転送するとき、G を宛先としたパケットの正しい着信インターフェイスを認識する必要があります。これは、他のインターフェイスに着信するパケットを拒否する必要があるためです。

ドメイン内の少数のスイッチが候補ブートストラップスイッチ (C-BSR) として設定され、単一の BSR がそのドメイン用に選択されます。また、ドメイン内の一連のスイッチが候補 RP (C-RP) として設定されます。通常、これらのスイッチは、C-BSR として設定されているものと同じスイッチです。候補 RP は、候補 RP アドバタイズメント (C-RP-Adv) メッセージをそのドメインの BSR に定期的にユニキャストし、RP になる意思をアドバタイズします。C-RP-Adv メッセージには、アドバタイズを行っている C-RP のアドレス、およびグループアドレスとマスク長のフィールドの任意のリストが含まれています。これらのフィールドは、立候補のアドバタイズの対象となるグループプレフィックスを示します。BSR は、定期的に発信するブートストラップメッセージ (BSM) にこれらの一連の C-RP とそれに対応するグループプレフィックスを含めます。BSM は、ドメイン全体にホップバイホップで配布されます。

双方向 BSR がサポートされているため、双方向 RP を C-RP メッセージおよび BSM の双方向範囲でアドバタイズできます。システム内のすべてのスイッチは、BSM で双方向範囲を使用できる必要があります。使用できない場合は、双方向 RP 機能が機能しません。

PIM-Source Specific Multicast (PIM-SSM)

PIM-SSM は、SSM の実装をサポートするルーティングプロトコルであり、PIM-SM から派生したものです。ただし、PIM-SM では PIM join を受けてすべてのマルチキャスト送信元からデータが送信されるのに対し、SSM 機能では、受信側が明示的に加入しているマルチキャスト送信元だけからその受信側にデータグラムトラフィックが転送されます。これにより、帯域利用率が最適化され、不要なインターネットブロードキャストトラフィックが拒否されます。さらに、SSM では、RP と共有ツリーを使用する代わりに、マルチキャストグループの送信元アドレスで見つかった情報を使用します。この情報は、MLD メンバーシップレポートによってラストホップスイッチにリレーされる送信元アドレスを通して受信側から提供されます。その結果として、送信元に直接つながる最短パスツリーが得られます。

SSM では、データグラムは (S, G) チャンネルに基づいて配信されます。1 つの (S, G) チャンネルのトラフィックは、IPv6 ユニキャスト送信元アドレス S とマルチキャストグループアドレス G を IPv6 宛先アドレスとして使用するデータグラムで構成されます。システムは、(S, G) チャンネルのメンバになることによって、このトラフィックを受信します。シグナリングは不要ですが、受信側は特定の送信元からのトラフィックを受信する場合は (S, G) チャンネルに加入し、トラフィックを受信しない場合はチャンネルから脱退する必要があります。

SSM を動作させるには、MLD バージョン 2 が必要です。MLD を使用すると、ホストが送信元の情報を提供できるようになります。MLD を使用して SSM を動作させるには、Cisco IOS IPv6 スイッチ、アプリケーションが実行されているホスト、およびアプリケーション自体で SSM がサポートされている必要があります。

ルーティング可能アドレスの hello オプション

IPv6 内部ゲートウェイプロトコルを使用してユニキャストルーティングテーブルを構築する場合、アップストリームスイッチアドレスを検出するための手順では、PIM ネイバーとネクストホップスイッチが同じスイッチを表しているかぎり、これらのアドレスは常に同じであるものと想定されます。ただし、スイッチがリンク上に複数のアドレスを持つ場合は、このことが当てはまるとはかぎりません。

この状況は IPv6 において、2 つの一般的な状況で発生することがあります。1 つめの状況は、ユニキャストルーティングテーブルが IPv6 内部ゲートウェイプロトコル (マルチキャスト BGP など) によって構築されない場合に発生します。2 つめの状況は、RP のアドレスがダウンストリームスイッチとサブネットプレフィックスを共有している場合に発生します (RP スイッチアドレスはドメインワイドにする必要があるため、リンクローカルアドレスにはできないことに注意してください)。

ルーティング可能アドレスの hello オプションによって、PIM プロトコルでこのような状況を回避できます。このためには、PIM hello メッセージがアドバタイズされるインターフェイス上のすべてのアドレスを含む PIM hello メッセージオプションを追加します。PIM スイッチが何らかのアドレスのアップストリームスイッチを検出すると、RPF 計算の結果は、PIM ネイバーのアドレス自体に加えて、このオプションのアドレスとも比較されます。このオプションにはそのリンク上の PIM スイッチの考えられるアドレスがすべて含まれているため、対象の PIM スイッチがこのオプションをサポートしている場合、常に RPF 計算の結果が含まれます。

PIM メッセージにサイズ制限があることと、ルーティング可能アドレスの hello オプションが単一の PIM hello メッセージ内に収まる必要があるため、インターフェイスで設定できるアドレスの制限は 16 個になっています。

PIM IPv6 スタブルルーティング

PIM スタブルルーティング機能は、エンドユーザーの近くにルーテッドトラフィックを移動し、リソースの利用率を軽減します。

PIM スタブルルーティングを使用するネットワークでは、ユーザーに対する IPv6 トラフィックの唯一の許容ルートは、PIM スタブルルーティングを設定しているスイッチ経由です。PIM 受動インターフェイスは、VLAN などのレイヤ 2 アクセスドメイン、または他のレイヤ 2 デバイスに接続されているインターフェイスに接続されます。直接接続されたマルチキャストレ

シーバおよび送信元のみが、レイヤ 2 アクセス ドメインで許可されます。PIM 受動インターフェイスは、受信した PIM 制御パケットを送信または処理しません。

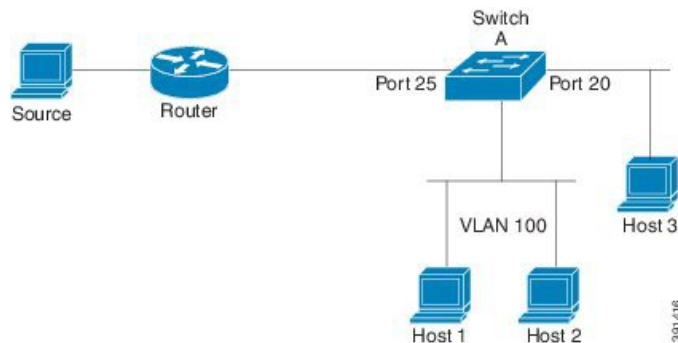
PIM スタブルルーティングを使用しているときは、IPv6 マルチキャストルーティングを使用し、スイッチだけを PIM スタブルータとして設定するように、分散ルータおよびリモートルータを設定する必要があります。スイッチは分散ルータ間の伝送トラフィックをルーティングしません。スイッチのルーテッドアップリンクポートも設定する必要があります。SVI の場合は、スイッチのアップリンクポートを使用できません。

また、PIM スタブルルーティングをスイッチに設定するときは、EIGRP スタブルルーティングも設定する必要があります。

冗長 PIM スタブルータ トポロジーはサポートされません。単一のアクセス ドメインにマルチキャストトラフィックを転送している複数の PIM ルータがある場合、冗長トポロジーが存在します。PIM メッセージはブロックされ、PIM アサートおよび指定されたルータ選出メカニズムは PIM 受動インターフェイスではサポートされません。PIM スタブル機能では、非冗長アクセスルータ トポロジーだけがサポートされます。非冗長トポロジーを使用することで、PIM 受動インターフェイスはそのアクセス ドメインで唯一のインターフェイスおよび指定ルータであると想定します。

次に示す図では、スイッチ A ルーテッドアップリンクポート 25 がルータに接続され、PIM スタブルルーティングが VLAN 100 インターフェイスとホスト 3 でイネーブルになっています。この設定により、直接接続されたホストはマルチキャスト発信元からトラフィックを受信できます。

図 17: PIM スタブルータ設定



ランデブーポイント

IPv6 PIM では、組み込み RP がサポートされています。組み込み RP サポートを利用すると、デバイスは、静的に設定されている RP の代わりに、マルチキャストグループ宛先アドレスを使用して RP 情報を学習できるようになります。デバイスが RP である場合、RP として静的に設定する必要があります。

デバイスは、MLD レポート内、または PIM メッセージおよびデータパケット内の組み込み RP グループアドレスを検索します。このようなアドレスが見つかったら、デバイスはアドレス自体からグループの RP を学習します。この学習された RP は、グループのすべてのプロトコル

アクティビティに使用されます。デバイスが RP である場合、組み込み RP を RP として設定する必要があり、デバイスはそのようにアドバタイズされます。

組み込み RP よりも優先するスタティック RP を選択するには、特定の組み込み RP グループ範囲またはマスクをスタティック RP のアクセスリストに設定する必要があります。PIM がスパースモードで設定されている場合は、RP として動作する 1 つ以上のデバイス選択も必要です。RP は、共有配布ツリーの選択ポイントに配置された単一の共通ルートであり、各ボックスでスタティックに設定されます。

PIM DR は、共有ツリーの下位方向に配布するために、直接接続されているマルチキャスト送信元から RP にデータを転送します。データは次の 2 つの方法のいずれかを使用して RP に転送されます。

- データは、登録パケットにカプセル化され、DR として動作するファーストホップデバイスによって直接 RP にユニキャストされます。
- RP 自身が送信元ツリーに加入している場合は、PIM スパースモードの項で説明したように、RPF 転送アルゴリズムに従ってマルチキャスト転送されます。

RP アドレスは、パケットをグループに送信するホストの代わりに PIM Register メッセージを送信するためにファーストホップデバイスによって使用されます。また、RP アドレスは、ラストホップデバイスによって PIM join および prune メッセージを RP に送信してグループメンバーシップについて通知するためにも使用されます。すべてのデバイス（RP デバイスを含む）で RP アドレスを設定する必要があります。

1 台の PIM デバイスを、複数のグループの RP にできます。特定のグループの PIM ドメイン内で一度に使用できる RP アドレスは 1 つだけです。アクセスリストで指定されている条件によって、デバイスがどのグループの RP であるかが判別されます。

IPv6 マルチキャストでは、PIM accept register 機能がサポートされています。これは、RP で PIM-SM register メッセージのフィルタリングを実行するための機能です。ユーザーは、アクセスリストを照合するか、または登録されている送信元の AS パスとルートマップに指定されている AS パスを比較できます。

スタティック mroute

IPv6 スタティック mroute は、RPF チェックを変化させるために使用する IPv4 スタティック mroute とほぼ同様に動作します。IPv6 スタティック mroute は、IPv6 スタティック ルートと同じデータベースを共有し、RPF チェックに対するスタティック ルートサポートを拡張することによって実装されます。スタティック mroute では、等コストマルチパス mroute がサポートされています。また、ユニキャスト専用スタティック ルートもサポートされています。

MRIB

マルチキャストルーティング情報ベース (MRIB) は、マルチキャストルーティングプロトコル (ルーティングクライアント) によってインスタンス化されるマルチキャストルーティングエントリのプロトコル非依存リポジトリです。その主要機能は、ルーティングプロトコル

とマルチキャスト転送情報ベース (MFIB) 間の非依存性を実現することです。また、クライアント間の調整および通信ポイントとしても機能します。

ルーティングクライアントは、MRIB が提供するサービスを使用して、ルーティング エントリをインスタンス化し、他のクライアントによってルーティング エントリに加えられた変更を取得します。MRIB では、ルーティングクライアント以外に、転送クライアント (MFIB インスタンス) や特別なクライアント (MLD など) も扱われます。MFIB は、MRIB からその転送 エントリを取得し、パケットの受信に関連するイベントについて MRIB に通知します。これらの通知は、ルーティングクライアントによって明示的に要求されることも、MFIB によって自発的に生成されることもあります。

MRIB のもう 1 つの重要な機能は、同じマルチキャストセッション内でマルチキャスト接続を確立する際に、複数のルーティングクライアントの調整を可能にすることです。また、MRIB では、MLD とルーティングプロトコル間の調整も可能です。

MFIB

MFIB は、IPv6 ソフトウェア用のプラットフォーム非依存およびルーティングプロトコル非依存ライブラリです。その主な目的は、転送テーブルが変更されたときに、Cisco IOS プラットフォームに、IPv6 マルチキャスト転送テーブルおよび通知を読み取るインターフェイスを提供することです。MFIB が提供する情報には、明確に定義された転送セマンティクスが含まれています。この情報は、プラットフォームが特定のハードウェアまたはソフトウェア転送メカニズムに容易に変換できる設計になっています。

ネットワーク内でルーティングまたはトポロジが変更されると、IPv6 ルーティング テーブルがアップデートされ、これらの変更が MFIB に反映されます。MFIB は、IPv6 ルーティング テーブル内の情報に基づいて、ネクストホップアドレス情報を管理します。MFIB エントリとルーティングテーブル エントリの間には 1 対 1 の相互関係があるため、MFIB には既知のすべてのルートが含まれ、高速スイッチングや最適スイッチングなどのスイッチングパスに関連付けられているルート キャッシュ管理の必要がなくなります。

MFIB



- (注) 分散型 MFIB は、アクティブスイッチがスタック内の他のメンバースイッチに MFIB 情報を配布するスタック環境でのみ意味を持ちます。次のセクションでは、ラインカードは単にスタックのメンバー スイッチです。

MFIB (MFIB) は、分散型プラットフォームでマルチキャスト IPv6 パケットをスイッチングするために使用されます。MFIB には、ラインカード全体の複製に関するプラットフォーム固有の情報も含めることができます。転送ロジックのコアを実装する基本 MFIB ルーチンは、すべての転送環境に共通です。

MFIB は、次の機能を実装します。

- ラインカードで生成されたデータ駆動型プロトコル イベントを PIM にリレーします。

- MFIB プラットフォーム アプリケーション プログラム インターフェイス (API) を提供し、ハードウェア アクセラレーション エンジンのプログラミングを担っている、プラットフォーム固有のコードに MFIB の変更を伝播します。また、この API には、ソフトウェアでパケットをスイッチングしたり (パケットがデータ駆動型イベントのトリガーとなっている場合に必要)、ソフトウェアにトラフィックの統計情報をアップロードしたりする エントリ ポイントも含まれています。

また、MFIB および MRIB サブシステムを組み合わせると、スイッチが各ラインカードで MFIB データベースの「カスタマイズ」コピーを保有したり、MFIB 関連のプラットフォーム固有の情報を RP からラインカードに転送したりできるようになります。

IPv6 マルチキャスト VRF Lite



- (注) IPv6 マルチキャスト VRF Lite をサポートするためには、スイッチで Network Advantage ライセンスを実行している必要があります。

IPv6 マルチキャスト VRF Lite 機能は、複数の仮想ルーティングおよび転送 (VRF) コンテキストに対する IPv6 マルチキャスト サポートを提供します。これらの VRF の範囲は、VRF が定義されているデバイスに制限されています。

この機能により、別の VRF に属するデバイス間の通信は、明示的に設定されていない限り許可されないため、より高いレベルのセキュリティでのルーティングと転送の切り分けができます。IPv6 マルチキャスト VRF Lite 機能は、特定の VRF に属するトラフィックの管理とトラブルシューティングを容易にします。

IPv6 マルチキャストのプロセススイッチングおよび高速スイッチング

統合 MFIB は、IPv6 マルチキャストでの PIM-SM および PIM-SSM に対するファストスイッチングおよびプロセススイッチングの両サポートを提供するために使用されます。プロセススイッチングでは、のが各パケットの調査、書き換え、および転送を行う必要があります。最初にパケットが受信され、システムメモリにコピーされます。次に、スイッチがルーティングテーブル内でレイヤ3ネットワークアドレスを検索します。そのあと、レイヤ2フレームがネクストホップの宛先アドレスで書き換えられ、発信インターフェイスに送信されます。また、は、巡回冗長検査 (CRC) も計算します。このスイッチング方式は、IPv6 パケットをスイッチングする方式の中でスケラビリティが最も低い方式です。

IPv6 マルチキャストの高速スイッチングを使用すると、スイッチは、プロセススイッチングよりも高いパケット転送パフォーマンスを実現できます。従来ルートキャッシュに格納される情報は、IPv6 マルチキャストスイッチング用にいくつかのデータ構造に格納されます。これらのデータ構造では、ルックアップが最適化され、パケット転送を効率的に行えるようになっています。

IPv6 マルチキャスト転送では、PIM プロトコル ロジックで許可されていれば、最初のパケットのファストスイッチングが行われます。IPv6 マルチキャストの高速スイッチングでは、MAC

カプセル化ヘッダーが事前に計算されます。IPv6 マルチキャストの高速スイッチングでは、MFIB を使用して、IPv6 送信先プレフィックスベースのスイッチング判定が行われます。IPv6 マルチキャストの高速スイッチングでは、MFIB に加えて、隣接関係テーブルを使用して、レイヤ 2 アドレッシング情報が付加されます。隣接関係テーブルでは、すべての MFIB エントリのレイヤ 2 ネクストホップアドレスが管理されます。

隣接が検出されると、隣接関係テーブルにそのデータが入力されます。（ARP などを使用して）隣接エントリが作成されるたびに、その隣接ノードのリンク層ヘッダーが事前に計算され、隣接関係テーブルに格納されます。ルートが決定されると、そのヘッダーはネクストホップおよび対応する隣接エントリを指します。そのあと、そのヘッダーはパケットスイッチング時のカプセル化に使用されます。

ロードバランシングと冗長性の両方に対応するようにスイッチが設定されている場合など、ルートには送信先プレフィックスへの複数のパスが存在することがあります。解決されたパスごとに、そのパスのネクストホップインターフェイスに対応する隣接へのポインタが追加されます。このメカニズムは、複数のパスでのロードバランシングに使用されます。

IPv6 マルチキャストでの NSF と SSO のサポート

Network Advantage ライセンスを実行しているスイッチは、IPv6 のノンストップフォワーディング (NSF) およびステートフルスイッチオーバー (SSO) をサポートします。

詳細については、『*Stack Manager and High Availability Configuration Guide*』の「*Configuring NSF with SSO*」を参照してください。

IPv6 対応の NTP

ネットワーク タイム プロトコル (NTP) は、マシンのネットワークの時刻同期を行うように設計されたプロトコルです。NTP は UDP 上で動作し、UDP は IPv4 上で動作します。NTP バージョン 4 (NTPv4) は、NTP バージョン 3 を拡張したもので、IPv4 と IPv6 の両方をサポートします。

詳細については、Cisco.com の『*Cisco IOS IPv6 Configuration Library*』を参照してください。

IPv6 マルチキャストの実装

IPv6 マルチキャスト ルーティングのイネーブル化

IPv6 マルチキャストルーティングを有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipv6 multicast-routing 例： Device(config)# ipv6 multicast-routing	すべての IPv6 対応インターフェイスでマルチキャスト ルーティングをイネーブルにし、イネーブルになっているすべてのスイッチ インターフェイスで PIM および MLD に対してマルチキャスト転送をイネーブルにします。
ステップ 4	copy running-config startup-config 例： Device(config)# copy running-config startup-config	（任意）コンフィギュレーション ファイルに設定を保存します。

MLD プロトコルのカスタマイズおよび確認

インターフェイスでの MLD のカスタマイズおよび確認

インターフェイスの MLD をカスタマイズして確認するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	Device# configure terminal	
ステップ 3	interface <i>type number</i> 例 : Device (config)# interface GigabitEthernet 1/0/1	インターフェイスのタイプと番号を指定し、スイッチをインターフェイスコンフィギュレーションモードにします。
ステップ 4	ipv6 mld join-group [<i>group-address</i>] [include exclude] { <i>source-address</i> source-list [<i>acl</i>]} 例 : Device (config-if)# ipv6 mld join-group FF04::10	指定したグループおよび送信元に対して MLD レポートを設定します。
ステップ 5	ipv6 mld access-group <i>access-list-name</i> 例 : Device (config-if)# ipv6 access-list acc-grp-1	ユーザーに IPv6 マルチキャストの受信側アクセスコントロールの実行を許可します。
ステップ 6	ipv6 mld static-group [<i>group-address</i>] [include exclude] { <i>source-address</i> source-list [<i>acl</i>]} 例 : Device (config-if)# ipv6 mld static-group ff04::10 include 100::1	指定したインターフェイスにマルチキャストグループのトラフィックをスタティックに転送し、MLD ジョイナがインターフェイスに存在するかにインターフェイスが動作するようにします。
ステップ 7	ipv6 mld query-max-response-time <i>seconds</i> 例 : Device (config-if)# ipv6 mld query-timeout 130	スイッチがインターフェイスのクエリアとして引き継ぐまでのタイムアウト値を設定します。
ステップ 8	exit 例 : Device (config-if)# exit	このコマンドを 2 回入力して、インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードを開始します。
ステップ 9	show ipv6 mld groups [link-local] [<i>group-name</i> <i>group-address</i>] [<i>interface-type</i> <i>interface-number</i>] [detail explicit] 例 :	スイッチに直接接続されており、MLD を介して学習したマルチキャストグループを表示します。

	コマンドまたはアクション	目的
	Device# <code>show ipv6 mld groups</code> GigabitEthernet 1/0/1	
ステップ 10	show ipv6 mld groups summary 例 : Device# <code>show ipv6 mld groups summary</code>	MLD キャッシュに存在する (*,G) および (S,G) メンバーシップ レポートの番号を表示します。
ステップ 11	show ipv6 mld interface [type number] 例 : Device# <code>show ipv6 mld interface</code> GigabitEthernet 1/0/1	インターフェイスのマルチキャスト関連情報を表示します。
ステップ 12	debug ipv6 mld [group-name group-address interface-type] 例 : Device# <code>debug ipv6 mld</code>	MLD プロトコル アクティビティに対するデバッグをイネーブルにします。
ステップ 13	debug ipv6 mld explicit [group-name group-address] 例 : Device# <code>debug ipv6 mld explicit</code>	ホストの明示的トラッキングに関連する情報を表示します。
ステップ 14	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

MLD グループ制限の実装

インターフェイス単位の MLD 制限とグローバル MLD 制限は相互に独立して機能します。インターフェイス単位の MLD 制限とグローバル MLD 制限の両方を同じスイッチで設定できます。MLD 制限の数は、グローバルの場合もインターフェイス単位の場合も、デフォルトでは設定されません。ユーザーが制限を設定する必要があります。インターフェイス単位のステート制限またはグローバル ステート制限を超えるメンバーシップ レポートは無視されます。

MLD グループ制限のグローバルな実装

MLD グループ制限をグローバルに実装するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipv6 mld [vrf vrf-name] state-limit number 例： Device(config)# ipv6 mld state-limit 300	MLD ステートの数をグローバルに制限します。
ステップ 4	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

MLD グループ制限のインターフェイス単位での実装

MLD グループ制限をインターフェイスごとに実装するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number 例： Device(config)# interface	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。

	コマンドまたはアクション	目的
	<code>GigabitEthernet 1/0/1</code>	
ステップ 4	<code>ipv6 mld limit number [except]access-list</code> 例： <code>Device(config-if)# ipv6 mld limit 100</code>	MLD ステートの数をインターフェイス単位で制限します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

受信側の明示的トラッキングによってホストの動作を追跡するための設定

明示的トラッキング機能を使用すると、スイッチが IPv6 ネットワーク内のホストの動作を追跡できるようになります。また、高速脱退メカニズムを MLD バージョン 2 のホストレポートで使用できるようになります。

受信側の明示的トラッキングを設定してホストの動作を追跡するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code> 例： <code>Device> enable</code>	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	<code>configure terminal</code> 例： <code>Device# configure terminal</code>	グローバル コンフィギュレーションモードを開始します。
ステップ 3	<code>interface type number</code> 例： <code>Device(config)# interface GigabitEthernet 1/0/1</code>	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーションモードにします。
ステップ 4	<code>ipv6 mld explicit-tracking access-list-name</code> 例： <code>Device(config-if)# ipv6 mld explicit-tracking list1</code>	ホストの明示的トラッキングをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

MLD トラフィック カウンタのリセット

MLD トラフィックカウンタをリセットするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	clear ipv6 mld traffic 例： Device# clear ipv6 mld traffic	すべての MLD トラフィック カウンタをリセットします。
ステップ 4	show ipv6 mld traffic 例： Device# show ipv6 mld traffic	MLD トラフィック カウンタを表示します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

MLD インターフェイス カウンタのクリア

MLD インターフェイスカウンタをクリアするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> enable	パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	clear ipv6 mld counters interface-type 例： Device# clear ipv6 mld counters Ethernet1/0	MLD インターフェイスカウンタをクリアします。
ステップ 4	copy running-config startup-config	（任意）コンフィギュレーション ファイルに設定を保存します。

PIM の設定

ここでは、PIM の設定方法について説明します。

PIM-SM の設定およびグループ範囲の PIM-SM 情報の表示

PIM-SM を設定し、グループ範囲の PIM-SM 情報を表示するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipv6 pim rp-address ipv6-address[group-access-list] 例：	特定のグループ範囲の PIM RP のアドレスを設定します。

	コマンドまたはアクション	目的
	Device(config)# ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C acc-grp-1	
ステップ 4	exit 例 : Device(config)# exit	グローバル コンフィギュレーション モードを終了し、スイッチを特権EXECモードに戻します。
ステップ 5	show ipv6 pim interface [state-on] [state-off] [type-number] 例 : Device# show ipv6 pim interface	PIM に対して設定されたインターフェイスに関する情報を表示します。
ステップ 6	show ipv6 pim group-map [group-name group-address] [group-range group-mask] [info-source {bsr default embedded-rp static}] 例 : Device# show ipv6 pim group-map	IPv6 マルチキャスト グループ マッピング テーブルを表示します。
ステップ 7	show ipv6 pim neighbor [detail] [interface-type interface-number count] 例 : Device# show ipv6 pim neighbor	Cisco IOS ソフトウェアで検出された PIM ネイバーを表示します。
ステップ 8	show ipv6 pim range-list [config] [rp-address rp-name] 例 : Device# show ipv6 pim range-list	IPv6 マルチキャスト範囲リストに関する情報を表示します。
ステップ 9	show ipv6 pim tunnel [interface-type interface-number] 例 : Device# show ipv6 pim tunnel	インターフェイス上の PIM レジスタのカプセル化およびカプセル化解除トンネルに関する情報を表示します。
ステップ 10	debug ipv6 pim [group-name group-address interface interface-type bsr group mvpn neighbor] 例 : Device# debug ipv6 pim	PIM プロトコルアクティビティに対するデバッグをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 11	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

PIM オプションの設定

PIM オプションを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	ipv6 pim spt-threshold infinity [group-list access-list-name] 例： Device (config)# ipv6 pim spt-threshold infinity group-list acc-grp-1	PIM リーフスイッチが指定したグループの SPT に加入するタイミングを設定します。
ステップ 4	ipv6 pim accept-register { list access-list route-map map-name } 例： Device (config)# ipv6 pim accept-register route-map reg-filter	RP のレジスタを許可または拒否します。
ステップ 5	interface type number 例： Device (config)# interface GigabitEthernet 1/0/1	インターフェイスのタイプと番号を指定し、スイッチをインターフェイスコンフィギュレーションモードにします。
ステップ 6	ipv6 pim dr-priority value 例：	PIM スwitch の DR プライオリティを設定します。

	コマンドまたはアクション	目的
	Device(config-if)# ipv6 pim dr-priority 3	
ステップ 7	ipv6 pim hello-interval seconds 例： Device(config-if)# ipv6 pim hello-interval 45	インターフェイスにおける PIM hello メッセージの頻度を設定します。
ステップ 8	ipv6 pim join-prune-interval seconds 例： Device(config-if)# ipv6 pim join-prune-interval 75	指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。
ステップ 9	exit 例： Device(config-if)# exit	このコマンドを 2 回入力して、インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードを開始します。
ステップ 10	ipv6 pim join-prune statistic [interface-type] 例： Device(config-if)# show ipv6 pim join-prune statistic	各インターフェイスの最後の集約パケットに関する平均 join-prune 集約を表示します。
ステップ 11	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

PIM トラフィック カウンタのリセット

PIM が誤動作する場合、または予想される PIM パケット数が送受信されていることを確認するために、ユーザーは PIM トラフィック カウンタをクリアできます。トラフィック カウンタがクリアされたら、ユーザーは `show ipv6 pim traffic` コマンドを入力して、PIM が正しく機能していること、および PIM パケットが正しく送受信されていることを確認できます。

PIM トラフィックカウンタをリセットするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例：	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。

PIM トポジテーブルをクリアすることによる MRIB 接続のリセット

	コマンドまたはアクション	目的
	Device> enable	
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	clear ipv6 pim traffic 例： Device# clear ipv6 pim traffic	PIM トラフィック カウンタをリセットします。
ステップ 4	show ipv6 pim traffic 例： Device# show ipv6 pim traffic	PIM トラフィック カウンタを表示します。
ステップ 5	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

PIM トポジテーブルをクリアすることによる MRIB 接続のリセット

MRIB を使用するのに設定は不要です。ただし、特定の状況においては、ユーザーは PIM トポジテーブルをクリアして MRIB 接続をリセットし、MRIB 情報を確認する必要がある場合があります。

PIM トポジテーブルをクリアして MRIB 接続をリセットするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	clear ipv6 pim topology [<i>group-name</i> <i>group-address</i>] 例 : Device# clear ipv6 pim topology FF04::10	PIM トポロジテーブルをクリアします。
ステップ 4	show ipv6 mrib client [<i>filter</i>] [<i>name</i> { <i>client-name</i> <i>client-name</i> : <i>client-id</i> }] 例 : Device# show ipv6 mrib client	インターフェイスのマルチキャスト関連情報を表示します。
ステップ 5	show ipv6 mrib route { <i>link-local</i> <i>summary</i> } [<i>sourceaddress-or-name</i> *] [<i>groupname-or-address</i> [<i>prefix-length</i>]] 例 : Device# show ipv6 mrib route	MRIB ルート情報を表示します。
ステップ 6	show ipv6 pim topology [<i>groupname-or-address</i> [<i>sourceaddress-or-name</i>] <i>link-local</i> <i>route-count</i> [<i>detail</i>]] 例 : Device# show ipv6 pim topology	特定のグループまたはすべてのグループの PIM トポロジテーブル情報を表示します。
ステップ 7	debug ipv6 mrib client 例 : Device# debug ipv6 mrib client	MRIB クライアント管理アクティビティに対するデバッグをイネーブルにします。
ステップ 8	debug ipv6 mrib io 例 : Device# debug ipv6 mrib io	MRIB I/O イベントに対するデバッグをイネーブルにします。
ステップ 9	debug ipv6 mrib proxy 例 : Device# debug ipv6 mrib proxy	分散型スイッチプラットフォームにおけるスイッチプロセッサとラインカード間の MRIB プロキシアクティビティに対するデバッグをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 10	debug ipv6 mrib route [<i>group-name</i> <i>group-address</i>] 例 : Device# debug ipv6 mrib route	MRIB ルーティング エントリ関連のアクティビティに関する情報を表示します。
ステップ 11	debug ipv6 mrib table 例 : Device# debug ipv6 mrib table	MRIB テーブル管理アクティビティに対するデバッグをイネーブルにします。
ステップ 12	copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

PIM IPv6 スタブルルーティングの設定

PIM スタブルルーティング機能は、ディストリビューションレイヤとアクセスレイヤの間のマルチキャストルーティングをサポートします。サポート対象のPIMインターフェイスは、アプリケーション PIM インターフェイスと PIM パッシブ インターフェイスの 2 種類です。PIM パッシブ モードに設定されているルーテッドインターフェイスは、PIM 制御トラフィックの通過も転送も行いません。通過させたり転送したりするのは MLD トラフィックだけです。

PIM IPv6 スタブルルーティングの設定時の注意事項

- PIM スタブルルーティングを設定する前に、スタブルータと中央のルータの両方に IPv6 マルチキャストルーティングが設定されている必要があります。また、スタブルータのアプリケーション インターフェイス上に、PIM モード (スパースモード) が設定されている必要があります。
- PIM スタブルータは、ディストリビューションルータ間の伝送トラフィックのルーティングは行いません。ユニキャスト (EIGRP) スタブルルーティングではこの動作が強制されます。PIM スタブルータの動作を支援するためにユニキャスト スタブルルーティングを設定する必要があります。詳細については、「EIGRP スタブルルーティング」の項を参照してください。
- 直接接続されたマルチキャスト (MLD) レシーバおよび送信元だけが、レイヤ 2 アクセスドメインで許可されます。アクセスドメインでは、PIM プロトコルはサポートされません。
- 冗長 PIM スタブルータ トポロジはサポートされません。

IPv6 PIM ルーティングのデフォルト設定

次の表に、デバイスの IPv6 PIM ルーティングのデフォルト設定を示します。

表 20: マルチキャストルーティングのデフォルト設定

機能	デフォルト設定
マルチキャストルーティング	すべてのインターフェイスで
PIM のバージョン	バージョン 2
PIM モード	モードは未定義
PIM スタブルーティング	未設定
PIM RP アドレス	未設定
PIM ドメイン境界	ディセーブル。
PIM マルチキャスト境界	なし
候補 BSR	ディセーブル。
候補 RP	ディセーブル。
SPT しきい値レート	0 kb/s
PIM ルータ クエリー メッセージ インターバル	30 秒

IPv6 PIM スタブルーティングのイネーブル化

IPv6 PIM スタブルーティングをイネーブルにするには、次の手順を実行します。

始める前に

PIM スタブルーティングは IPv6 ではデフォルトでディセーブルです。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例：	グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
	Device# <code>configure terminal</code>	
ステップ 3	ipv6 multicast pim-passive-enable 例 : Device(config-if)# <code>ipv6 multicast pim-passive-enable</code>	スイッチで IPv6 マルチキャスト PIM ルーティングをイネーブルにします。
ステップ 4	interface interface-id 例 : Device(config)# <code>interface gigabitethernet 9/0/6</code>	<p>PIM スタブルルーティングをイネーブルにするインターフェイスを指定し、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。</p> <p>次のいずれかのインターフェイスを指定する必要があります。</p> <ul style="list-style-type: none"> • ルーテッドポート : レイヤ3ポートとして no switchport インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。また、インターフェイスの IP PIM スパース モードをイネーブルにして、静的に接続されたメンバーとしてインターフェイスを MLD スタティック グループに結合する必要があります。 • SVI : interface vlan vlan-id グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。また、VLAN 上で IP PIM スパース モードをイネーブルにして、静的に接続されたメンバーとして VLAN を MLD スタティック グループに結合し、VLAN、MLD スタティック グループ、および物理インターフェイスで MLD スヌーピングをイネーブルにする必要があります。 <p>これらのインターフェイスには、IPv6 アドレスを割り当てる必要があります。</p>

	コマンドまたはアクション	目的
ステップ 5	ipv6 pim 例 : Device(config-if) # ipv6 pim	インターフェイスで PIM をイネーブルにします。
ステップ 6	ipv6 pim {bsr} {dr-priority value} {hello-interval seconds} {join-prune-interval seconds} {passive} 例 : Device(config-if) # ipv6 pim bsr dr-priority hello-interval join-prune-interval passive	インターフェイスでさまざまな PIM スタブ機能を設定します。 bsr を入力して PIM スイッチの BSR を設定します。 dr-priority を入力して、PIM スイッチの DR 優先順位を設定します。 hello-interval を入力して、インターフェイスの PIM hello メッセージの頻度を設定します。 join-prune-interval を入力して、指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。 passive を入力して、パッシブモードの PIM を設定します。
ステップ 7	end 例 : Device(config-if) # end	特権 EXEC モードに戻ります。

IPv6 PIM スタブルーティングのモニター

表 21: PIM スタブ設定の show コマンド

コマンド	目的
show ipv6 pim interface	各インターフェイスで有効になっている PIM スタブを表示します。
show ipv6 mld groups	特定のマルチキャストグループを結合した対象クライアントを表示します。
show ipv6 mroute	ソースから対象クライアントへのマルチキャストストリーム転送を確認します。

IPv6 PIM での組み込み RP サポートのディセーブル化

ドメイン内のすべてのデバイスが組み込み RP をサポートしていない場合、必要に応じて、インターフェイスで組み込み RP サポートを無効化できます。



(注) この作業では、IPv6 PIM での組み込み RP サポートだけでなく、PIM を完全にディセーブルにします。

IPv6 PIM の組み込み RP サポートを無効化するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	no ipv6 pim [vrf vrf-name] rp embedded 例： Device(config)# no ipv6 pim rp embedded	IPv6 PIM での組み込み RP サポートをディセーブルにします。
ステップ 4	interface type number 例： Device(config)# interface FastEthernet 1/0	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 5	no ipv6 pim 例： Device(config-if)# no ipv6 pim	指定したインターフェイスで IPv6 PIM をオフにします。

BSR の設定

ここでの作業について、以下に説明します。

BSR の設定および BSR 情報の確認

BSR 情報を設定および確認するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipv6 pim bsr candidate bsr <i>ipv6-address[hash-mask-length] [priority priority-value]</i> 例： Device (config)# ipv6 pim bsr candidate bsr 2001:DB8:3000:3000::42 124 priority 10	候補 BSR になるようにスイッチを設定します。
ステップ 4	interface type number 例： Device (config)# interface GigabitEthernet 1/0/1	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 5	ipv6 pim bsr border 例： Device (config-if)# ipv6 pim bsr border	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 6	exit 例： Device (config-if)# exit	このコマンドを2回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 7	show ipv6 pim bsr {election rp-cache candidate-rp} 例：	PIM BSR プロトコル処理に関連する情報を表示します。

	コマンドまたはアクション	目的
	Device(config-if)# show ipv6 pim bsr election	
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BSR への PIM RP アドバタイズメントの送信

BSR に PIM RP アドバタイズメントを送信するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipv6 pim bsr candidate rp ipv6-address [group-list access-list-name] [priority priority-value] [interval seconds] 例： Device(config)# ipv6 pim bsr candidate rp 2001:DB8:3000:3000::42 priority 0	BSR に PIM RP アドバタイズメントを送信します。
ステップ 4	interface type number 例： Device(config)# interface GigabitEthernet 1/0/1	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーション モードにします。
ステップ 5	ipv6 pim bsr border 例： Device(config-if)# ipv6 pim bsr border	指定したインターフェイスの任意のスコープの全 BSM に対して境界を設定します。
ステップ 6	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

限定スコープゾーン内で BSR を使用できるようにするための設定

スコープゾーン内で使用する BSR を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	ipv6 pim bsr candidate rp ipv6-address [hash-mask-length] [priority priority-value] 例： Device (config)# ipv6 pim bsr candidate bsr 2001:DB8:1:1:4	候補 BSR になるようにスイッチを設定します。
ステップ 4	ipv6 pim bsr candidate rp ipv6-address [group-list access-list-name] [priority priority-value] [interval seconds] 例： Device (config)# ipv6 pim bsr candidate rp 2001:DB8:1:1:1 group-list list scope 6	BSR に PIM RP アドバタイズメントを送信するように候補 RP を設定します。
ステップ 5	interface type number 例： Device (config-if)# interface GigabitEthernet 1/0/1	インターフェイスのタイプと番号を指定し、スイッチをインターフェイス コンフィギュレーションモードにします。
ステップ 6	ipv6 multicast boundary scope scope-value 例： Device (config-if)# ipv6 multicast boundary scope 6	指定されたスコープのインターフェイスでマルチキャスト境界を設定します。
ステップ 7	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

BSR スイッチにスコープと RP のマッピングをアナウンスさせるための設定

IPv6 BSR スイッチは、スコープと RP のマッピングを候補 RP メッセージから学習するのではなく、直接アナウンスするようにスタティックに設定できます。ユーザーは、スコープと RP のマッピングをアナウンスするように BSR スイッチを設定して、BSR をサポートしていない RP がその BSR にインポートされるように設定できます。この機能をイネーブルにすると、ローカルの候補 BSR スイッチの既知のリモート RP が、企業の BSR ドメインの外部に配置されている RP を学習できるようになります。

スコープと RP のマッピングをアナウンスするように BSR スイッチを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipv6 pim bsr announced rp <i>ipv6-address</i> [<i>group-list access-list-name</i>] [<i>priority priority-value</i>] 例： Device(config)# ipv6 pim bsr announced rp 2001:DB8:3000:3000::42 priority 0	指定した候補 RP の BSR からスコープと RP のマッピングを直接アナウンスします。
ステップ 4	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

SSM マッピングの設定

SSM マッピング機能をイネーブルにすると、DNS ベースの SSM マッピングが自動的にイネーブルになります。つまり、スイッチは、マルチキャスト MLD バージョン 1 レポートの送信元を DNS サーバーから検索するようになります。

スイッチ設定に応じて、DNS ベースのマッピングまたはスタティック SSM マッピングのいずれかを使用できます。スタティック SSM マッピングを使用する場合は、複数のスタティック

SSM マッピングを設定できます。複数のスタティック SSM マッピングを設定すると、一致するすべてのアクセスリストの送信元アドレスが使用されるようになります。



- (注) DNS ベースの SSM マッピングを使用するには、スイッチは正しく設定されている DNS サーバーを少なくとも 1 つ見つける必要があります。スイッチは、その DNS サーバーに直接接続される可能性があります。

SSM マッピングを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipv6 mld ssm-map enable 例 : Device(config)# ipv6 mld ssm-map enable	設定済みの SSM 範囲内のグループに対して SSM マッピング機能をイネーブルにします。
ステップ 4	no ipv6 mld ssm-map query dns 例 : Device(config)# no ipv6 mld ssm-map query dns	DNS ベースの SSM マッピングをディセーブルにします。
ステップ 5	ipv6 mld ssm-map static access-list source-address 例 : Device(config-if)# ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1	スタティック SSM マッピングを設定します。

	コマンドまたはアクション	目的
ステップ 6	exit 例： Device(config-if)# exit	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 7	show ipv6 mld ssm-map [source-address] 例： Device(config-if)# show ipv6 mld ssm-map	SSM マッピング情報を表示します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

スタティック mroute の設定

IPv6 のスタティック マルチキャスト ルート (mroute) は、IPv6 スタティック ルートの拡張として実装できます。スイッチを設定する際には、ユニキャスト ルーティング専用としてスタティック ルートを使用するか、マルチキャスト RPF 選択専用としてスタティック マルチキャスト ルートを使用するか、またはユニキャスト ルーティングとマルチキャスト RPF 選択の両方にスタティック ルートを使用するように設定できます。

静的 mroute を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipv6 route {ipv6-prefix / prefix-length ipv6-address interface-type interface-number ipv6-address} [administrative-distance] [administrative-multicast-distance unicast multicast] [tag tag]	スタティック IPv6 ルートを確立します。 この例は、ユニキャスト ルーティングとマルチキャスト RPF 選択の両方に使用されるスタティック ルートを示しています。

	コマンドまたはアクション	目的
	例 : Device(config)# ipv6 route 2001:DB8::/64 6::6 100	
ステップ 4	exit 例 : Device# exit	グローバル コンフィギュレーション モードを終了し、スイッチを特権 EXEC モードに戻します。
ステップ 5	show ipv6 mroute [<i>link-local</i> [<i>group-name</i> <i>group-address</i> [<i>source-address</i> <i>source-name</i>]]] [summary] [count] 例 : Device# show ipv6 mroute ff07::1	IPv6 マルチキャストルーティング テーブルの内容を表示します。
ステップ 6	show ipv6 mroute [link-local <i>group-name</i> <i>group-address</i>] active [<i>kbits</i>] 例 : Device(config-if)# show ipv6 mroute active	スイッチ上のアクティブなマルチキャスト ストリームを表示します。
ステップ 7	show ipv6 rpf [<i>ipv6-prefix</i>] 例 : Device(config-if)# show ipv6 rpf 2001::1:1:2	特定のユニキャスト ホスト アドレスおよびプレフィックスの RPF 情報を確認します。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

IPv6 マルチキャストでの MFIB の使用

IPv6 マルチキャストルーティングをイネーブルにすると、マルチキャスト転送が自動的にイネーブルになります。

IPv6 マルチキャストでの MFIB の動作の確認

IPv6 マルチキャストで MFIB の動作を確認するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	show ipv6 mfib [verbose <i>group-address-name</i> <i>ipv6-prefix / prefix-length</i> <i>source-address-name</i> count interface status summary] 例： Device# show ipv6 mfib	IPv6 MFIB での転送エントリおよびインターフェイスを表示します。
ステップ 3	show ipv6 mfib [all linkscope <i>group-name</i> <i>group-address</i> [<i>source-name</i> <i>source-address</i>]] count 例： Device# show ipv6 mfib ff07::1	IPv6 マルチキャストルーティングテーブルの内容を表示します。
ステップ 4	show ipv6 mfib interface 例： Device# show ipv6 mfib interface	IPv6 マルチキャスト対応インターフェイスとその転送ステータスに関する情報を表示します。
ステップ 5	show ipv6 mfib status 例： Device# show ipv6 mfib status	一般的な MFIB 設定と動作ステータスを表示します。
ステップ 6	show ipv6 mfib summary 例： Device# show ipv6 mfib summary	IPv6 MFIB エントリおよびインターフェイスの数に関するサマリー情報を表示します。
ステップ 7	debug ipv6 mfib [<i>group-name</i> <i>group-address</i>] [adjacency db fs init interface mrrib [detail] nat pak platform ppr ps signal table] 例： Device# debug ipv6 mfib FF04::10 pak	IPv6 MFIB に対するデバッグ出力をイネーブルにします。

MFIB トラフィック カウンタのリセット

MFIB トラフィックカウンタをリセットするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	clear ipv6 mfib counters [<i>group-name</i> <i>group-address</i> [<i>source-address</i> <i>source-name</i>]] 例 : Device# clear ipv6 mfib counters FF04::10	アクティブなすべての MFIB トラフィック カウンタをリセットします。

その他の参考資料

標準および RFC

標準/RFC	タイトル
RFC 4292	IP 転送テーブル
RFC 4293	『 <i>Management Information Base for the Internet Protocol (IP)</i> 』

IPv6 マルチキャストの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	IPv6 マルチキャスト	IPv6 マルチキャストでは、ホストから単一データストリームをすべてのホストのサブネットに同時に送信（グループ伝送）できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 11 章

MLD スヌーピングの設定

このモジュールには、MLD スヌーピングの設定の詳細が含まれています。

- [IPv6 MLD スヌーピングの設定に関する情報 \(261 ページ\)](#)
- [IPv6 MLD スヌーピングの設定方法 \(265 ページ\)](#)
- [MLD スヌーピング情報の表示 \(275 ページ\)](#)
- [MLD スヌーピングの設定例 \(276 ページ\)](#)
- [その他の参考資料 \(277 ページ\)](#)
- [MLD スヌーピングの機能履歴 \(277 ページ\)](#)

IPv6 MLD スヌーピングの設定に関する情報

スイッチ上で Multicast Listener Discovery (MLD) スヌーピングを使用して、スイッチドネットワーク内のクライアントおよびルータに IP Version 6 (IPv6) マルチキャストデータを効率的に配信することができます。特に指示がないかぎり、スイッチという用語は、スタンドアロンスイッチおよびスイッチ スタックを指します。

IPv6 を使用するには、IPv6 スイッチデータベース管理 (SDM) テンプレートがスイッチに設定されている必要があります。

MLD スヌーピングの概要

IP Version 4 (IPv4) では、レイヤ 2 スイッチはインターネットグループ管理プロトコル (IGMP) スヌーピングを使用して、動的にレイヤ 2 インターフェイスを設定することにより、マルチキャストトラフィックのフラッドを抑制します。そのため、マルチキャストトラフィックは IP マルチキャストデバイスに対応付けられたインターフェイスにだけ転送されます。IPv6 では、MLD スヌーピングが同様の機能を実行します。MLD スヌーピングを使用すると、IPv6 マルチキャストデータは VLAN (仮想 LAN) 内のすべてのポートにフラッドされるのではなく、データを受信するポートのリストに選択的に転送されます。このリストは、IPv6 マルチキャスト制御パケットをスヌーピングすることにより構築されます。

MLD は IPv6 マルチキャストルータで使用されるプロトコルで、ルータに直接接続されたリンク上のマルチキャストリスナー (IPv6 マルチキャストパケットを受信するノード) の存在、

および隣接ノードを対象とするマルチキャストパケットを検出します。MLD は IGMP から派生しています。MLD バージョン 1 (MLDv1) は IGMPv2 と、MLD バージョン 2 (MLDv2) は IGMPv3 とそれぞれ同等です。MLD は Internet Control Message Protocol バージョン 6 (ICMPv6) のサブプロトコルです。MLD メッセージは ICMPv6 メッセージのサブセットで、IPv6 パケット内で先頭の Next Header 値 58 により識別されます。

スイッチは、次の 2 つのバージョンの MLD スヌーピングをサポートします。

- MLDv1 スヌーピング : MLDv1 制御パケットを検出し、IPv6 宛先マルチキャストアドレスに基づいてトラフィックのブリッジングを設定します。
- MLDv2 基本スヌーピング (MBSS) : MLDv2 制御パケットを使用して、IPv6 宛先マルチキャストアドレスに基づいてトラフィックの転送を設定します。

スイッチは MLDv1 プロトコルパケットと MLDv2 プロトコルパケットの両方でスヌーピングでき、IPv6 宛先マルチキャストアドレスに基づいて IPv6 マルチキャストデータをブリッジングします。



- (注) スイッチは、IPv6 送信元および宛先マルチキャストアドレスベースの転送を設定する MLDv2 拡張スヌーピングをサポートしません。

MLD スヌーピングは、グローバルまたは VLAN 単位でイネーブルまたはディセーブルに設定できます。MLD スヌーピングがイネーブルの場合、VLAN 単位の IPv6 マルチキャストアドレステーブルはソフトウェアおよびハードウェアで構築されます。その後、スイッチはハードウェアで IPv6 マルチキャストアドレスに基づくブリッジングを実行します。

MLD メッセージ

MLDv1 は、次の 3 種類のメッセージをサポートします。

- Listener Query : IGMPv2 クエリーと同等で、General Query または Multicast-Address-Specific Query (MASQ) のいずれかになります。
- Multicast Listener Report : IGMPv2 レポートと同等です。
- Multicast Listener Done メッセージ : IGMPv2 Leave メッセージと同等です。

MLDv2 では、MLDv1 レポートおよび Done メッセージに加えて、MLDv2 クエリーおよび MLDv2 レポートもサポートします。

メッセージの送受信の結果生じるメッセージタイマーおよびステート移行は、IGMPv2 メッセージの場合と同じです。リンクに対してローカルで有効な IPv6 送信元アドレスを持たない MLD メッセージは、MLD ルータおよび MLD スイッチで無視されます。

MLD クエリー

スイッチは MLD クエリーを送信し、IPv6 マルチキャストアドレスデータベースを構築し、MLD グループ固有クエリー、MLD グループおよび送信元固有クエリーを生成して、MLD Done

メッセージに応答します。また、スイッチはレポート抑制、レポートプロキシング、即時脱退機能、およびスタティックな IPv6 マルチキャスト グループ アドレス設定もサポートします。

MLD スヌーピングがディセーブルの場合、すべての MLD クエリーが入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合、受信された MLD クエリーが入力 VLAN でフラッディングされ、クエリーのコピーは CPU に送信され、処理されます。MLD スヌーピングでは、受信されたクエリーから IPv6 マルチキャスト アドレス データベースを構築します。MLD スヌーピングは、マルチキャスト ルータ ポートを検出して、タイマーを維持し、レポート応答時間を設定します。また、VLAN のクエリア IP 送信元アドレス、VLAN 内のクエリア ポートを学習して、マルチキャスト アドレス エージングを維持します。

グループが MLD スヌーピング データベースに存在する場合、スイッチは MLDv1 レポートを送信して、グループ固有のクエリーに回答します。このグループが不明の場合、グループ固有のクエリーは入力 VLAN にフラッディングされます。

ホストがマルチキャスト グループから脱退する場合、MLD Done メッセージ (IGMP Leave メッセージと同等) を送信できます。スイッチが MLDv1 Done メッセージを受信した際に、即時脱退がイネーブルでなければ、スイッチはメッセージを受信したポートに MASQ を送信して、ポートに接続する他のデバイスがマルチキャスト グループに残る必要があるかどうか判断します。

マルチキャスト クライアント エージングの堅牢性

クエリー数に基づいて、アドレスからのポートメンバーシップの削除を設定できます。1つのアドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対するレポートがない場合のみです。デフォルトの回数は2回です。

マルチキャスト ルータ 検出

IGMP スヌーピングと同様に、MLD スヌーピングでは次の特性を持つマルチキャスト ルータ検出を行います。

- ユーザにより設定されたポートには、期限切れがありません。
- ダイナミックなポート学習は、MLDv1 スヌーピング クエリーおよび IPv6 PIMv2 パケットにより行われます。
- 複数のルータが同じレイヤ2 インターフェイス上にある場合、MLD スヌーピングではポート上の単一のマルチキャスト ルータ (直前にルータ制御パケットを送信したルータ) を追跡します。
- マルチキャスト ルータ ポートのダイナミックなエージングは、デフォルト タイマーの5分に基づきます。ポート上で制御パケットが5分間受信されない場合、マルチキャスト ルータはルータのポート リストから削除されます。
- IPv6 マルチキャスト ルータ検出が実行されるのは、MLD スヌーピングがスイッチでイネーブルの場合のみです。

- 受信された IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネーブルかどうかにかかわらず、常に入力 VLAN にフラッディングされます。
- 最初の IPv6 マルチキャスト ルータ ポートが検出された後は、不明の IPv6 マルチキャスト データは、検出されたルータ ポートに対してのみ転送されます（それまでは、すべての IPv6 マルチキャスト データは入力 VLAN にフラッディングされます）。

MLD レポート

MLDv1 join メッセージは、本質的には IGMPv2 と同じように処理されます。IPv6 マルチキャスト ルータが VLAN で検出されない場合は、レポートが処理されないか、またはスイッチから転送されません。IPv6 マルチキャスト ルータが検出され、MLDv1 レポートが受信されると、IPv6 マルチキャスト グループ アドレスが VLAN の MLD データベースに入力されます。その後、VLAN 内のグループに対するすべての IPv6 マルチキャスト トラフィックが、このアドレスを使用して転送されます。MLD スヌーピングがディセーブルの場合、レポートは入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合は、MLD レポート抑制（リスナーメッセージ抑制）は自動的にイネーブルになります。レポート抑制により、スイッチはグループで受信された最初の MLDv1 レポートを IPv6 マルチキャスト ルータに転送します。グループのそれ以降のレポートはルータに送信されません。MLD スヌーピングがディセーブルの場合は、レポート抑制がディセーブルになり、すべての MLDv1 レポートは入力 VLAN にフラッディングされます。

スイッチは、MLDv1 プロキシ レポーティングもサポートします。MLDv1 MASQ が受信されると、スイッチに他のポートのグループが存在する場合、およびクエリーを受信したポートとアドレスの最後のメンバポートが異なる場合は、スイッチはクエリーを受信したアドレスに関する MLDv1 レポートで応答します。

MLD Done メッセージおよび即時脱退

即時脱退機能がイネーブルの場合にホストが MLDv1 Done メッセージ（IGMP Leave メッセージと同等）を送信すると、Done メッセージを受信したポートはグループからただちに削除されます。VLAN で即時脱退をイネーブルにする場合は（IGMP スヌーピングと同様に）、ポートに単一のホストが接続されている VLAN でのみこの機能を使用します。ポートがグループの最後のメンバである場合、グループも削除され、検出された IPv6 マルチキャスト ルータに脱退情報が転送されます。

VLAN で即時脱退がイネーブルでない場合に（1つのポート上にグループのクライアントが複数ある場合）、Done メッセージがポートで受信されると、このポートで MASQ が生成されます。ユーザは、既存アドレスのポート メンバシップが削除される時期を MASQ 数の観点から制御できます。アドレスに対するメンバシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対する MLDv1 レポートがない場合です。

生成される MASQ 数は、**ipv6 mld snooping last-listener-query count** グローバル コンフィギュレーション コマンドにより設定されます。デフォルトの回数は 2 回です。

MASQ は、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信されます。スイッチの最大応答時間内に MASQ で指定された IPv6 マルチキャスト アドレスにレポートが送信されなければ、MASQ が送信されたポートは IPv6 マルチキャスト アドレス データベースから

ら削除されます。最大応答時間は、**ipv6 mld snooping last-listener-query-interval** グローバルコンフィギュレーション コマンドにより設定します。削除されたポートがマルチキャストアドレスの最後のメンバである場合は、マルチキャストアドレスも削除され、スイッチは検出されたマルチキャスト ルータすべてにアドレス脱退情報を送信します。

TCN 処理

ipv6 mld snooping tcn query solicit グローバル コンフィギュレーション コマンドを使用して、トポロジ変更通知 (TCN) 送信要求を有効にすると、MLDv1 スヌーピングは、設定された数の MLDv1 クエリによりすべての IPv6 マルチキャストトラフィックをフラッディングするよう VLAN に設定してから、選択されたポートにのみマルチキャストデータの送信を開始します。この値は、**ipv6 mld snooping tcn flood query count** グローバルコンフィギュレーションコマンドを使用して設定します。デフォルトでは、2つのクエリーが送信されます。スイッチが VLAN 内の STP ルートになる場合、またはスイッチがユーザにより設定された場合は、リンクに対してローカルで有効な IPv6 送信元アドレスを持つ MLDv1 グローバル Done メッセージも生成されます。これは IGMP スヌーピングの場合と同じです。

IPv6 MLD スヌーピングの設定方法

MLD スヌーピングのデフォルト設定

表 22: MLD スヌーピングのデフォルト設定

機能	デフォルト設定
MLD スヌーピング (グローバル)	ディセーブル。
MLD スヌーピング (VLAN 単位)	イネーブルVLAN MLD スヌーピングが実行されるためには、MLD スヌーピングがグローバルにイネーブルである必要があります。
IPv6 マルチキャストアドレス	未設定
IPv6 マルチキャスト ルータ ポート	未設定
MLD スヌーピング即時脱退	ディセーブル。
MLD スヌーピングの堅牢性変数	グローバル : 2、VLAN 単位 : 0 (注) VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。

機能	デフォルト設定
最後のリスナー クエリー カウント	グローバル : 2、VLAN 単位 : 0 (注) VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー インターバル	グローバル : 1000 (1 秒)、VLAN : 0 (注) VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバルのインターバルを使用します。
TCN クエリー送信請求	ディセーブル。
TCN クエリー カウント	2
MLD リスナー抑制	ディセーブル

MLD スヌーピング設定時の注意事項

MLD スヌーピングの設定時は、次の注意事項に従ってください。

- MLD スヌーピングの特性はいつでも設定できますが、設定を有効にする場合は、**ipv6 mld snooping** グローバル コンフィギュレーション コマンドを使用して MLD 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。
- MLD スヌーピングと IGMP スヌーピングは相互に独立して動作します。スイッチで両方の機能を同時にイネーブルにできます。
- スイッチまたはスイッチスタックに保持可能なマルチキャストエントリの最大数は 1024 です。

スイッチでの MLD スヌーピングのイネーブル化またはディセーブル化

デフォルトでは、IPv6 MLD スヌーピングはスイッチではグローバルにディセーブルで、すべての VLAN ではイネーブルです。MLD スヌーピングがグローバルにディセーブルの場合は、すべての VLAN でもディセーブルです。MLD スヌーピングをグローバルにイネーブルにすると、VLAN 設定はグローバル設定を上書きします。つまり、MLD スヌーピングはデフォルトステート (イネーブル) の VLAN インターフェイスでのみイネーブルになります。

VLAN 単位または VLAN 範囲で MLD スヌーピングをイネーブルおよびディセーブルにできますが、MLD スヌーピングをグローバルにディセーブルにした場合は、すべての VLAN でディセーブルになります。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

スイッチでグローバルにMLD スヌーピングをイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipv6 mld snooping 例： Device(config)# ipv6 mld snooping	スイッチで MLD スヌーピングをイネーブルにします。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config 例： Device(config)# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ 6	reload 例： Device(config)# reload	OS (オペレーティング システム) をリロードします。

VLAN に対する MLD スヌーピングのイネーブル化またはディセーブル化

VLAN で MLD スヌーピングをイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipv6 mld snooping 例： Device(config)# ipv6 mld snooping	スイッチで MLD スヌーピングをイネーブルにします。
ステップ 4	ipv6 mld snooping vlan <i>vlan-id</i> 例： Device(config)# ipv6 mld snooping vlan 1	VLAN で MLD スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 (注) VLAN スヌーピングをイネーブルにするには、MLD スヌーピングがグローバルにイネーブルである必要があります。
ステップ 5	end 例： Device(config)# end	特権 EXEC モードに戻ります。

スタティックなマルチキャストグループの設定

ホストまたはレイヤ 2 ポートは、通常マルチキャストグループにダイナミックに加入しますが、VLAN に IPv6 マルチキャストアドレスおよびメンバポートをスタティックに設定することもできます。

マルチキャストグループのメンバとしてレイヤ 2 ポートを追加するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	ipv6 mld snooping vlan <i>vlan-id</i> static <i>ipv6_multicast_address</i> interface <i>interface-id</i> 例 : Device (config)# ipv6 mld snooping vlan 1 static 3333.0000.1111 interface gigabitethernet 1/1/0/1	マルチキャストグループのメンバとしてレイヤ 2 ポートにマルチキャストグループを設定します。 <ul style="list-style-type: none"> • <i>vlan-id</i> は、マルチキャストグループの VLAN ID です。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 • <i>ipv6_multicast_address</i> は、128 ビットのグループ IPv6 アドレスです。このアドレスは RFC 2373 で指定された形式でなければなりません。 • <i>interface-id</i> は、メンバポートです。物理インターフェイスまたはポートチャネル (1 ~ 48) に設定できます。
ステップ 4	end 例 : Device (config)# end	特権 EXEC モードに戻ります。
ステップ 5	次のいずれかを使用します。 <ul style="list-style-type: none"> • show ipv6 mld snooping address • show ipv6 mld snooping address vlan <i>vlan-id</i> 例 :	スタティックメンバポートおよび IPv6 アドレスを確認します。

	コマンドまたはアクション	目的
	Device# <code>show ipv6 mld snooping address</code> または Device# <code>show ipv6 mld snooping vlan 1</code>	

マルチキャスト ルータ ポートの設定



(注) マルチキャストルータへのスタティック接続は、スイッチポートに限りサポートされます。

VLAN にマルチキャスト ルータ ポートを追加するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> <code>enable</code>	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipv6 mld snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i> 例 : Device(config)# <code>ipv6 mld snooping vlan 1 mrouter interface gigabitethernet 1/0/2</code>	マルチキャストルータの VLAN ID を指定して、マルチキャストルータにインターフェイスを指定します。 <ul style="list-style-type: none"> 指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 このインターフェイスには物理インターフェイスまたはポートチャネルを指定できます。指定できるポートチャネルの範囲は 1 ~ 48 です。
ステップ 4	end 例 : Device(config)# <code>end</code>	特権 EXEC 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 5	show ipv6 mld snooping mrouter [vlan <i>vlan-id</i>] 例 : Device# show ipv6 mld snooping mrouter vlan 1	VLAN インターフェイスで IPv6 MLD スヌーピングがイネーブルになっていることを確認します。

MLD 即時脱退のイネーブル化

MLDv1 即時脱退をイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipv6 mld snooping vlan <i>vlan-id</i> immediate-leave 例 : Device (config)# ipv6 mld snooping vlan 1 immediate-leave	VLAN インターフェイスで MLD 即時脱退をイネーブルにします。
ステップ 4	end 例 : Device (config)# end	特権 EXEC モードに戻ります。
ステップ 5	show ipv6 mld snooping vlan <i>vlan-id</i> 例 : Device# show ipv6 mld snooping vlan 1	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。

MLD スヌーピングクエリーの設定

スイッチまたはVLANにMLD スヌーピングクエリの特性を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ipv6 mld snooping robustness-variable value 例： Device(config)# ipv6 mld snooping robustness-variable 3	（任意）スイッチが一般クエリーに 응답しないリスナー（ポート）を削除する前に、送信されるクエリー数を設定します。指定できる範囲は1～3です。デフォルトは2です。
ステップ 4	ipv6 mld snooping vlan vlan-id robustness-variable value 例： Device(config)# ipv6 mld snooping vlan 1 robustness-variable 3	（任意）VLAN 単位でロバストネス変数を設定します。これにより、MLD レポート応答がない場合にマルチキャストアドレスがエージングアウトされるまでに、MLD スヌーピングが送信する一般クエリー数が決定されます。指定できる範囲は1～3です。デフォルトは0です。0に設定すると、使用される数はグローバルな堅牢性変数の値になります。
ステップ 5	ipv6 mld snooping last-listener-query-count count 例： Device(config)# ipv6 mld snooping last-listener-query-count 7	（任意）MLD クライアントがエージングアウトされる前にスイッチが送信するMASQ数を設定します。指定できる範囲は1～7です。デフォルトは2です。クエリーは1秒後に送信されます。
ステップ 6	ipv6 mld snooping vlan vlan-id last-listener-query-count count 例：	（任意）VLAN 単位でラストリスナークエリーカウントを設定します。この値はグローバルに設定された値を上書

	コマンドまたはアクション	目的
	Device (config) # ipv6 mld snooping vlan 1 last-listener-query-count 7	きします。指定できる範囲は 1 ～ 7 です。デフォルトは 0 です。0 に設定すると、グローバルなカウント値が使用されます。クエリーは 1 秒後に送信されます。
ステップ 7	ipv6 mld snooping last-listener-query-interval interval 例 : Device (config) # ipv6 mld snooping last-listener-query-interval 2000	(任意) スイッチが MASQ を送信したあと、マルチキャスト グループからポートを削除するまで待機する最大応答時間を設定します。指定できる範囲は、100 ～ 32,768 ミリ秒です。デフォルト値は 1000 (1 秒) です。
ステップ 8	ipv6 mld snooping vlan vlan-id last-listener-query-interval interval 例 : Device (config) # ipv6 mld snooping vlan 1 last-listener-query-interval 2000	(任意) VLAN 単位で last-listener クエリーインターバルを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は、0 ～ 32,768 ミリ秒です。デフォルトは 0 です。0 に設定すると、グローバルな最後のリスナークエリーインターバルが使用されます。
ステップ 9	ipv6 mld snooping tcn query solicit 例 : Device (config) # ipv6 mld snooping tcn query solicit	(任意) トポロジ変更通知 (TCN) をイネーブルにします。これにより、VLAN は設定された数のクエリーに関する IPv6 マルチキャストトラフィックすべてをフラッドイングしてから、マルチキャストデータをマルチキャストデータの受信を要求するポートに対してのみ送信します。デフォルトでは、TCN はディセーブルに設定されています。
ステップ 10	ipv6 mld snooping tcn flood query count count 例 : Device (config) # ipv6 mld snooping tcn flood query count 5	(任意) TCN がイネーブルの場合、送信される TCN クエリー数を指定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 11	end	特権 EXEC モードに戻ります。
ステップ 12	show ipv6 mld snooping querier [vlan vlan-id] 例 :	(任意) スイッチまたは VLAN の MLD スヌーピングクエリア情報を確認します。

	コマンドまたはアクション	目的
	Device (config) # show ipv6 mld snooping querier vlan 1	

MLD リスナーメッセージ抑制のディセーブル化

デフォルトでは、MLD スヌーピングリスナーメッセージ抑制はイネーブルに設定されています。この機能がイネーブルの場合、スイッチはマルチキャストルータクエリーごとに1つのMLDレポートのみを転送します。メッセージ抑制がディセーブルの場合は、複数のマルチキャストルータにMLDレポートが転送されます。

MLD リスナーメッセージ抑制をディセーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	no ipv6 mld snooping listener-message-suppression 例： Device (config) # no ipv6 mld snooping listener-message-suppression	MLD メッセージ抑制をディセーブルにします。
ステップ 4	end 例： Device (config) # end	特権 EXEC モードに戻ります。
ステップ 5	show ipv6 mld snooping 例： Device# show ipv6 mld snooping	IPv6 MLD スヌーピングレポート抑制がディセーブルであることを確認します。

MLD スヌーピング情報の表示

ダイナミックに学習された、あるいはスタティックに設定されたルータ ポートおよび VLAN インターフェイスの MLD スヌーピング情報を表示できます。また、MLD スヌーピング用に設定された VLAN の IPv6 グループ アドレス マルチキャスト エントリを表示することもできます。

表 23: MLD スヌーピング情報表示用のコマンド

コマンド	目的
<code>show ipv6 mld snooping [vlan vlan-id]</code>	<p>スイッチのすべての VLAN または指定された VLAN の MLD スヌーピング設定情報を表示します。</p> <p>(任意) 個々の VLAN に関する情報を表示するには、vlan vlan-id を入力します。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。</p>
<code>show ipv6 mld snooping mrouter [vlan vlan-id]</code>	<p>ダイナミックに学習され、手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。MLD スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先であるインターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。</p> <p>(任意) 個々の VLAN に関する情報を表示するには、vlan vlan-id を入力します。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。</p>
<code>show ipv6 mld snooping querier [vlan vlan-id]</code>	<p>VLAN 内で直前に受信した MLD クエリー メッセージの IPv6 アドレスおよび着信ポートに関する情報を表示します。</p> <p>(任意) vlan vlan-id を入力して、単一の VLAN 情報を表示します。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。</p>
<code>show ipv6 mld snooping address [vlan vlan-id] [count dynamic user]</code>	<p>すべての IPv6 マルチキャスト アドレス情報あるいはスイッチまたは VLAN の特定の IPv6 マルチキャスト アドレス情報を表示します。</p> <ul style="list-style-type: none"> • count を入力して、スイッチまたは VLAN のグループ数を表示します。 • dynamic を入力して、スイッチまたは VLAN の MLD スヌーピング学習済みグループ情報を表示します。 • user を入力して、スイッチまたは VLAN の MLD スヌーピングユーザ設定グループ情報を表示します。

コマンド	目的
show ipv6 mld snooping address vlan <i>vlan-id</i> [ipv6-multicast-address]	指定の VLAN および IPv6 マルチキャスト アドレスの MLD スヌーピングを表示します。

MLD スヌーピングの設定例

スタティックなマルチキャスト グループの設定：例

次に、IPv6 マルチキャスト グループをスタティックに設定する例を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping vlan 2 static 3333.0000.1111 interface
gigabitethernet1/0/1
Device(config)# end
```

マルチキャスト ルータ ポートの設定：例

次に、VLAN 200 にマルチキャスト ルータ ポートを追加する例を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping vlan 200 mrouter interface gigabitethernet
1/0/2
Device(config)# exit
```

MLD 即時脱退のイネーブル化：例

次に、VLAN 130 で MLD 即時脱退をイネーブルにする例を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping vlan 130 immediate-leave
Device(config)# exit
```

MLD スヌーピング クエリーの設定：例

次に、MLD スヌーピングのグローバルな堅牢性変数を 3 に設定する例を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping robustness-variable 3
Device(config)# exit
```

次に、VLAN の MLD スヌーピングの最後のリスナー クエリー カウントを 3 に設定する例を示します。

```
Device# configure terminal
```

```
Device(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
Device(config)# exit
```

次に、MLD スヌーピングの最後のリスナー クエリー インターバル（最大応答時間）を 2000（2 秒）に設定する例を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping last-listener-query-interval 2000
Device(config)# exit
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9200 Series Switches)</i>

MLD スヌーピングの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能名	機能情報
Cisco IOS XE Fuji 16.9.2	MLD スヌーピング	MLD スヌーピングにより、スイッチで MLD パケットを調べ、パケットの内容に基づいて転送先を決定できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfmng.cisco.com/> にアクセスします。



第 12 章

IP マルチキャストの最適化：大規模な IP マルチキャスト展開での PIM スパースモードの最適化

- [大規模な IP マルチキャスト展開での PIM スパースモードの最適化の前提条件 \(279 ページ\)](#)
- [大規模な IP マルチキャスト展開での PIM スパースモードの最適化について \(280 ページ\)](#)
- [大規模な IP マルチキャスト展開で PIM スパースモードを最適化する方法 \(283 ページ\)](#)
- [大規模なマルチキャスト展開での PIM スパースモードの最適化の設定例 \(286 ページ\)](#)
- [IP マルチキャストの最適化：大規模な IP マルチキャスト展開での PIM スパースモードの最適化に関するその他の関連資料 \(287 ページ\)](#)
- [IP マルチキャストの最適化の機能履歴：大規模な IP マルチキャスト展開での PIM スパースモードの最適化 \(287 ページ\)](#)

大規模な IP マルチキャスト展開での PIM スパースモードの最適化の前提条件

- PIM スパースモードがネットワークで実行されている必要があります。
- どのグループに最短パスツリー (SPT) しきい値を適用するかを制御するのにグループリストを使用することを計画している場合は、この作業を実行する前にアクセスリストを設定する必要があります。

大規模な IP マルチキャスト展開での PIM スパース モードの最適化について

PIM 登録プロセス

IP マルチキャスト ソースは、その存在をアナウンスするのにシグナリング メカニズムを使用しません。送信元は接続ネットワークにデータを送信するだけなのに対し、受信者は Internet Group Management Protocol (IGMP) を使用して、自身の在席状態を示します。ソースが PIM スパースモード (PIM-SM) で設定されているマルチキャストグループにトラフィックを送信すると、ソースにつながる指定ルータ (DR) は、このソースの存在についてランデブー ポイント (RP) に知らせなければなりません。この送信元からマルチキャストトラフィックを (ネイティブに) 受信するダウンストリーム受信者が RP にいて、RP が送信元につながる最短パスに加入していない場合、DR はトラフィックを送信元から RP に送信する必要があります。PIM 登録プロセスは、各 (S, G) エントリに対し個別に実行されますが、DR と RP 間のこれらのタスクを実行します。

登録プロセスは、DR が新しい (S, G) ステートを作成すると開始されます。DR は、(S, G) ステートに一致するすべてのデータ パケットを PIM 登録メッセージにカプセル化し、それらの登録メッセージを RP にユニキャストします。

RP が新しいソースからの登録メッセージを受信したいダウンストリーム レシーバを持っている場合は、RP は、登録メッセージを DR を通じて受信し続けることも、ソースにつながる最短パスに加入することもできます。デフォルトでは、ネイティブ マルチキャストトラフィックの配信が最も高いスループットを実現するため、RP は最短パスに加入します。最短パス経由でネイティブに到着した最初のパケットを受信後、RP は DR に登録停止メッセージを送り返します。DR は、この登録停止メッセージを受信したら、RP への登録メッセージの送信を停止します。

RP に新しい送信元からの登録メッセージを受信するダウンストリーム受信者がいない場合、RP は最短パスに加入しません。その代わりに、RP は、ただちに DR に登録停止メッセージを送り返します。DR は、この登録停止メッセージを受信したら、RP への登録メッセージの送信を停止します。

いったんソースへのルーティング エントリが確立されたら、DR と RP の間で定期的な再登録が発生します。DR が RP から登録停止メッセージを受信するまでは、ソースがアクティブであれば、マルチキャストルーティング テーブル ステートがタイムアウトする 1 分前に DR が 1 つのデータのない登録メッセージを RP に送信します。このアクションがマルチキャストルーティング テーブル エントリのタイムアウト時間をリスタートさせ、通常は、2 分ごとに 1 つの登録交換が行われることとなります。登録は、ステートを維持するため、ステート損失から回復するため、および RP 上でソースを追跡するために必要です。これは、RP の最短パスへの加入からは独立して発生します。

PIM バージョン 1 の互換性

RP が PIM バージョン 1 を実行している場合、それはデータのない登録メッセージは理解しません。この場合、DR は RP にデータのない登録メッセージを送信しません。代わりに、RP から登録停止メッセージを受信後約 3 分おきに、DR は送信元からの着信データ パケットを登録メッセージにカプセル化し、それを RP に送信します。DR は RP から別の登録停止メッセージを受信するまで、登録メッセージを送信し続けます。DR が PIM バージョン 1 を実行している場合、同じ動作が起こります。

PIM バージョン 1 を実行している DR が特定の (S, G) エントリ向けの登録メッセージにデータ パケットをカプセル化すると、エントリではプロセススイッチングが行われます（高速スイッチングやハードウェアスイッチングではない）。これらの高速パスをサポートしているプラットフォームでは、PIM バージョン 1 を実行している RP または DR の PIM 登録プロセスが、定期的で不適切なパケット配信の原因となる可能性があります。そのため、ネットワークを PIM バージョン 1 から PIM バージョン 2 にアップグレードすることを推奨しています。

PIM 指定ルータ

IP マルチキャスト用に設定されているデバイスは、PIM ハロー メッセージを送信して、どのデバイスが各 LAN セグメント（サブネット）の指定ルータ（DR）であるかを調べます。ハローメッセージにはデバイスの IP アドレスが含まれており、最も大きい IP アドレスを持つデバイスが DR になります。

DR は、直接接続された LAN 上のすべてのホストに Internet Group Management Protocol (IGMP) ホストクエリメッセージを送信します。スパースモードで稼働している場合は、DR は、ソース登録メッセージをランデブーポイント（RP）に送信します。

デフォルトでは、マルチキャスト デバイスは、30 秒ごとに PIM ルータ クエリ メッセージを送信します。デバイスがより頻繁に PIM ハロー メッセージを送信できるようにすることにより、デバイスは、応答しないネイバーをより迅速に検出できるようになります。その結果、デバイスは、より効率的なフェールオーバー手順または回復手順を実装できます。この変更は、ネットワークのエッジ上の冗長デバイスに対してのみ行うことが推奨されます。

PIM スパース モード登録メッセージ

データのない登録メッセージは、1 秒に 1 メッセージのレートで送信されます。DR が集中的なソース（データ レートの高いソース）を登録しており、RP が PIM バージョン 2 を実行していない場合は、連続的に高いレートの登録メッセージが発生する可能性があります。

デフォルトでは、PIM スパース モード登録メッセージは、レート制限なしで送信されます。登録メッセージのレートを制限すると、設定された制限を超えた登録メッセージはドロップされるという代償を伴いますが、DR および RP にかかる負荷が制限されます。レシーバは、パケットが集中的なソースから送信されてから最初の 1 秒間に、データ パケット損失を経験する可能性があります。

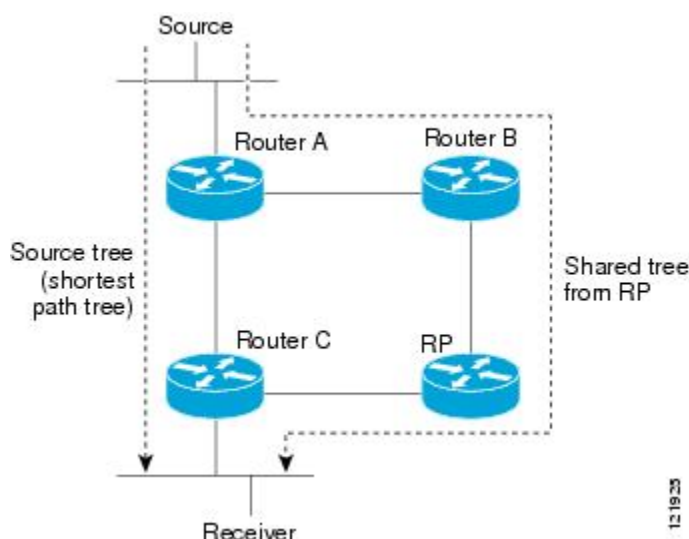
メモリ要件を減らすために最短パス ツリーの使用を回避する

PIM 共有ツリーとソース ツリーを理解しておく、最短パス ツリーの使用を回避することでどのようにメモリ要件を減らせるかについて理解しやすくなります。

PIM 共有ツリーおよびソース ツリー（最短パス ツリー）

デフォルトでは、ランデブー ポイント（RP）がルートになる単一のデータ配信ツリー全体にわたって、マルチキャストグループのメンバが送信者からグループへのデータを受信します。このタイプの配布ツリーは、図に示すように、共有ツリーと呼ばれます。送信側からのデータは、RP に配信され、その共有ツリーに加入しているグループ メンバに配布されます。

図 18: 共有ツリーとソース ツリー（最短パス ツリー）



データレートで保証される場合、共有ツリー上のリーフルータは、送信元をルートとするデータ配信ツリーへの切り替えを開始できます。このタイプの配信ツリーは、最短パス ツリー（SPT）またはソースツリーと呼ばれます。デフォルトでは、ソフトウェアが送信元から最初のデータ パケットを受信すると、送信元ツリーに切り替わります。

次に、共有ツリーから送信元ツリーに切り替わるプロセスの詳細を示します。

1. レシーバがグループに加入します。リーフルータであるルータ C が、RP に向けて加入メッセージを送信します。
2. RP がルータ C へのリンクを発信インターフェイス リストに登録します。
3. 送信元がデータを送信します。ルータ A はデータをカプセル化して登録メッセージに格納し、RP に送信します。
4. RP が、データを共有ツリーの下流に向けて、ルータ C に転送し、ソースに向けて加入メッセージを送信します。この時点で、データはルータ C に 2 回（カプセル化された状態で 1 回、ネイティブの状態ですべて 1 回）着信する可能性があります。

5. データがネイティブに（マルチキャストを通じて）RP に到着すると、RP は、ルータ A に登録停止メッセージを送信します。
6. デフォルトでは、最初のデータパケットの受信で、ルータ C のソースへの加入メッセージ送信が促されます。
7. ルータ C は、(S, G) でデータを受信すると、共有ツリーの上流に向けて、ソースのプルーニングメッセージを送信します。
8. RP が (S, G) の発信インターフェイスからルータ C へのリンクを削除します。RP は、ソースに向けてプルーニングメッセージをトリガーします。

加入メッセージとプルーニングメッセージが、ソースと RP に送信されます。これらのメッセージはホップバイホップで送信され、送信元または RP に向かうパス上の各 PIM ルータによって処理されます。register および register-stop メッセージは、ホップバイホップで送信されません。これらのメッセージは、送信元に直接接続されている指定ルータによって送信され、グループの RP によって受信されます。

グループへ送信する複数の送信元で、共有ツリーが使用されます。

最短パスツリーの使用を回避または延期する利点

共有ツリーからソースツリーへのスイッチは、最初のデータパケットのラストホップデバイス（PIM 共有ツリーおよびソースツリー（最短パスツリー）（282 ページ）でのルータ C）への到着によって発生します。このスイッチが発生するのは、`ip pim spt-threshold` コマンドがタイミングを制御しているためで、そのデフォルト設定は 0 kbps です。

最短パスツリーは共有ツリーより多くのメモリを必要としますが、遅延は低減します。この使用を回避または延期して、メモリの要件を減らすことができます。リーフデバイスがただちに最短パスツリーに移動できるようにする代わりに、SPT の使用を防止したり、まずトラフィックがしきい値に到達しなければならないように指定したりできます。

PIM リーフデバイスが、指定グループの SPT に加入する時期を設定できます。送信元の送信速度が指定速度（キロビット/秒）以上の場合、デバイスは PIM Join メッセージを送信元に向けて送信し、ソースツリー（SPT）を構築します。`infinity` キーワードを指定すると、指定されたグループのすべての送信元で共有ツリーが使用され、送信元ツリーに切り替わらなくなります。

大規模な IP マルチキャスト展開で PIM スパース モードを最適化する方法

大規模な展開での PIM スパース モードの最適化

IP マルチキャストの展開が大規模な場合には、この作業を行うことを検討してください。

このタスクのステップ 3、5、および 6 は相互に依存せず、オプションと見なされます。これらの手順はいずれも、PIM スパース モードの最適化に役立ちます。ステップ 5 または 6 を実行する場合は、ステップ 4 を実行する必要があります。ステップ 6 は、指定ルータにしか適用されません。PIM クエリーの間隔の変更は、PIM ドメインのエッジにある冗長ルータに対してしか適切ではありません。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip pim register-rate-limit rate 例： Router(config)# ip pim register-rate-limit 10	(任意) 各 (S, G) ルーティング エントリについて、1 秒当たりに送信される PIM スパース モード登録メッセージの最大数の制限を設定します。 • このコマンドは、指定ルータ (DR) が各 (S, G) エントリに許可する登録メッセージ数を制限する場合に使用します。 • デフォルトでは、最大レートは設定されていません。 • このコマンドを設定すると、設定された制限を超えた登録メッセージはドロップされるという代償を伴いますが、DR および RP への負荷は制限されます。 • レシーバは、登録メッセージが集中的なソースから送信されてから最初の 1 秒間に、データ パケット損失を経験する可能性があります。
ステップ 4	ip pim spt-threshold {kpbs infinity}[group-list access-list] 例：	(任意) 最短パス ツリーに移行するには超えなければならないしきい値を指定します。

	コマンドまたはアクション	目的
	<pre>Router(config)# ip pim spt-threshold infinity group-list 5</pre>	<ul style="list-style-type: none"> デフォルト値は0です。この場合、ルータは、最初のデータパケットを受信するとただちに SPT に加入します。 infinity キーワードを指定すると、最短パスツリーへの移行は一切行われなくなり、共有ツリーのままとなります。このキーワードは、「多対多」通信のマルチキャスト環境に適用されます。 グループリストは、SPT のしきい値がどのグループに適用されるかを制御する標準アクセスリストです。0 の値を指定するか、またはグループリストを指定しなかった場合、しきい値はすべてのグループに適用されます。 この例では、グループリスト 5 は、すでにマルチキャスト グループ 239.254.2.0 および 239.254.3.0 を許可するように設定されています (access-list 5 permit 239.254.2.0 0.0.0.255 access-list 5 permit 239.254.3.0 0.0.0.255)。
ステップ 5	<p>interface <i>type number</i></p> <p>例 :</p> <pre>Router(config)# interface GigabitEthernet 1/0/1</pre>	<p>インターフェイスを設定します。</p> <ul style="list-style-type: none"> PIM SPT しきい値または PIM クエリー間隔のデフォルト値を変更したくない場合は、このステップは実行しないでください。このステップで変更が行われます。
ステップ 6	<p>ip pim query-interval <i>period</i> [msec]</p> <p>例 :</p> <pre>Router(config-if)# ip pim query-interval 1</pre>	<p>(任意) マルチキャスト ルータが PIM ルータ クエリー メッセージを送信する頻度を設定します。</p> <ul style="list-style-type: none"> この手順は、PIM ドメインのエッジにある冗長ルータに対してだけ実行してください。 デフォルトのクエリー間隔は 30 秒です。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • msec キーワードを指定しない限り、<i>period</i> 引数の単位は秒です。 • クエリー間隔を少ない秒数に設定するとコンバージェンスを高速化できますが、コンバージェンスの高速化と引き換えに CPU と帯域幅の使用量が大きくなります。

大規模なマルチキャスト展開での PIM スパース モードの最適化の設定例

大規模な IP マルチキャスト展開での PIM スパース モードの最適化の例

次の例は、下記のことを行う方法を示します。

- クエリー間隔を 1 秒に設定して、コンバージェンスを高速化する。
- ルータが一切 SPT に移行せず、共有ツリーに留まるように設定する。
- 各 (S, G) ルーティング エントリについて、1 秒あたりに送信される PIM スパース モード登録メッセージの制限を 10 個に設定する。

```
interface GigabitEthernet 1/0/1
 ip pim query-interval 1
 .
 .
 .
 !
 ip pim spt-threshold infinity
 ip pim register-rate-limit 10
 !
```

IP マルチキャストの最適化：大規模な IP マルチキャスト展開での PIM スパース モードの最適化に関するその他の関連資料

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャストルーティングのコマンド」の項を参照してください。 <i>Command Reference (Catalyst 9200 Series Switches)</i>

IP マルチキャストの最適化の機能履歴：大規模な IP マルチキャスト展開での PIM スパースモードの最適化

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	IP マルチキャストの最適化：大規模な IP マルチキャスト展開での PIM スパースモードの最適化	Protocol Independent Multicast (PIM) には、スパースモードとデンスモードの2つの基本的な動作モードがあり、多様なリンクやデバイスが混在する大規模なネットワークに適しています。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfmng.cisco.com/> にアクセスします。



第 13 章

IP マルチキャストの最適化：マルチキャストサブセカンドコンバージェンス

- [マルチキャストサブセカンドコンバージェンスの前提条件 \(289 ページ\)](#)
- [マルチキャストサブセカンドコンバージェンスの制約事項 \(289 ページ\)](#)
- [マルチキャストサブセカンドコンバージェンスについて \(290 ページ\)](#)
- [マルチキャストサブセカンドコンバージェンスの設定方法 \(291 ページ\)](#)
- [マルチキャストサブセカンドコンバージェンスの設定例 \(293 ページ\)](#)
- [IP マルチキャストの最適化：マルチキャストサブセカンドコンバージェンスに関するその他の参考資料 \(294 ページ\)](#)
- [IP マルチキャストの最適化：マルチキャストサブセカンドコンバージェンスの機能情報 \(294 ページ\)](#)

マルチキャストサブセカンドコンバージェンスの前提条件

サービスプロバイダは、シスコマルチキャストサブセカンドコンバージェンス機能を使用するには、マルチキャスト対応コアが必要です。

マルチキャストサブセカンドコンバージェンスの制約事項

サブセカンド指定ルータ (DR) フェールオーバー拡張機能を使用するデバイスは、到着した Hello インターバル情報をミリ秒単位で処理できる必要があります。輻輳しているデバイス、または Hello インターバルを処理するための十分な CPU サイクルがないデバイスは、それが事実でない可能性があっても、Protocol Independent Multicast (PIM) ネイバーが切断されていると見なす可能性があります。

マルチキャストサブセカンドコンバージェンスについて

マルチキャストサブセカンドコンバージェンスの利点

- スケーラビリティ コンポーネントは、サービスユーザー（レシーバ）とサービス負荷（ソースまたはコンテンツ）の増加（または減少）を処理する際の効率を向上させます。
- 新しいアルゴリズムとプロセス（最大 1000 個の個別メッセージを 1 つのパケットに入れて配信する、集約された加入メッセージなど）が、コンバージェンスに達するまでの時間を 10 分の 1 にも低減します。
- マルチキャストサブセカンドコンバージェンスが、大規模なマルチキャストネットワークのサービス可用性を向上させます。
- マルチキャスト機能は以前に必要とした何分の 1 かの時間で元に戻せるため、金融サービス会社や証券会社などのマルチキャストユーザーは、Quality of Service (QoS) の向上が得られます。

マルチキャストサブセカンドコンバージェンス スケーラビリティ拡張機能

マルチキャストサブセカンドコンバージェンス機能は、サービスユーザー（レシーバ）とサービス負荷（ソースまたはコンテンツ）の増加（または減少）を処理する際の効率を向上させるスケーラビリティ拡張機能を提供します。このリリースのスケーラビリティ拡張機能に含まれているものは次のとおりです。

- 新しいタイマー管理テクニックによる、インターネットグループ管理プロトコル (IGMP) と PIM ステート メンテナンスの向上
- Multicast Source Discovery Protocol (MSDP) Source-Active (SA) キャッシュの規模拡張の向上

スケーラビリティ拡張機能には、以下のメリットがあります。

- 可能な PIM マルチキャストルート (mroute)、IGMP、および MSDP SA キャッシュステート容量の増加
- CPU 使用率の減少

PIM ルータ クエリ メッセージ

マルチキャストサブセカンドコンバージェンスによって、PIM ルータ クエリ メッセージ (PIM hello) を数ミリ秒ごとに送信できます。PIM hello メッセージは、隣接する PIM デバイスを探すために使用されます。この機能の導入前は、デバイスは PIM hello を数秒単位でしか送信で

きませんでした。デバイスがより頻繁に PIM ハロー メッセージを送信できるようにすることにより、デバイスは、この機能を使用して応答しないネイバーをより迅速に検出できるようになります。その結果、デバイスは、より効率的なフェールオーバー手順または回復手順を実装できます。

Reverse Path Forwarding

ユニキャストリバースパス転送 (RPF) 機能は、裏付けのない IP ソースアドレスを持つ IP パケットを廃棄することにより、ネットワークに変形または偽造 (スプーフィング) された IP ソースアドレスが注入されて引き起こされる問題の緩和に役立ちます。変形または偽造 (スプーフィング) された送信元アドレスは、送信元 IP アドレスのスプーフィングに基づいたサービス拒絶 (DoS) 攻撃を示す場合があります。

RPF はアクセスコントロールリスト (ACL) を使用して、不正なまたは偽造の IP 送信元アドレスを持つデータパケットをドロップまたは転送するかどうかを判断します。ACL コマンドのオプションを使用して、システム管理者は、ドロップまたは転送されたパケットに関する情報をログに記録できます。偽装パケットに関する情報をログに記録しておくこと、可能性のあるネットワーク攻撃に関する情報の発見に役立てることができます。

インターフェイスごとの統計情報を使用して、システム管理者は、ネットワーク攻撃のエントリーポイントとなっているインターフェイスを迅速に検出できます。

トポロジの変更とマルチキャストルーティングのリカバリ

マルチキャストサブセカンドコンバージェンスフィーチャセットは、ユニキャストルーティングのリカバリの後にほぼ瞬時に完了するマルチキャストパスリカバリを提供することにより、企業とサービスプロバイダ両方のネットワークバックボーンを強化します。

ネットワークトポロジの変更が発生すると、PIM は RPF の計算をユニキャストルーティングテーブルに依存するため、ユニキャストプロトコルは最初にトラフィックのベストパスのオプションを計算する必要があり、その後、マルチキャストはベストパスを決定できるようになります。

マルチキャストサブセカンドコンバージェンスは、ユニキャストの計算が完了した後の、ほぼ瞬時のマルチキャストプロトコル計算完了を可能にします。その結果、トポロジの変更後、マルチキャストトラフィックの転送は大幅に速く復元されます。

マルチキャストサブセカンドコンバージェンスの設定方法

PIM ルータクエリメッセージ間隔の変更

PIM ルータクエリメッセージ間隔を変更するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface type slot / subslot / port 例： Device(config)# interface gigabitethernet 1/0/0	インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 4	ip pim query-interval period [msec] 例： Device(config-if)# ip pim query-interval 45	マルチキャストルータが PIM ルータ クエリーメッセージを送信する頻度を設定します。

マルチキャストサブセカンドコンバージェンス設定の確認

マルチキャストサブセカンドコンバージェンス機能に関する詳細情報を表示し、確認するには、次のタスクを実行します。

手順

ステップ 1 enable

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 show ip pim interface type number

このコマンドを使用して、PIM に設定されているインターフェイスに関する情報を表示します。

次に、**show ip pim interface** コマンドの出力例を示します。

例 :

```
Device# show ip pim interface GigabitEthernet 1/0/0
Address          Interface          Ver/   Nbr   Query  DR    DR
                  Interface          Mode  Count Intvl  Prior
172.16.1.4       GigabitEthernet1/0/0 v2/S  1     100 ms 1     172.16.1.4
```

ステップ3 show ip pim neighbor

Cisco IOS XE ソフトウェアによって検出された PIM ネイバーを表示するには、このコマンドを使用します。

次に、**show ip pim neighbor** コマンドの出力例を示します。

例 :

```
Device# show ip pim neighbor
PIM Neighbor Table
Neighbor          Interface          Uptime/Expires   Ver  DR
Address           Address           Address           Ver  Prio/Mode
172.16.1.3        GigabitEthernet1/0/0 00:03:41/250 msec v2   1 / S
```

マルチキャストサブセカンドコンバージェンスの設定例

PIM ルータ クエリ メッセージ インターバルの変更例

次の例では、**ip pim query-interval** コマンドが 100 ミリ秒に設定されています。このコマンドは、間隔値がデフォルト以外の値になるように設定されていない限り、**show running-config** コマンド出力に表示されません。

```
!
interface gigabitethernet 1/0/1
 ip address 172.16.2.1 255.255.255.0
 ip pim query-interval 100 msec
 ip pim sparse-mode
```

IP マルチキャストの最適化：マルチキャストサブセカンドコンバージェンスに関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャストルーティングのコマンド」の項を参照してください。 <i>Command Reference (Catalyst 9200 Series Switches)</i>

IP マルチキャストの最適化：マルチキャストサブセカンドコンバージェンスの機能情報

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	IP マルチキャストの最適化：マルチキャストサブセカンドコンバージェンス	マルチキャストサブセカンドコンバージェンス機能は、サービスユーザー（レシーバ）とサービス負荷（ソースまたはコンテンツ）の増加（または減少）を処理する際の効率を向上させるスケラビリティ拡張機能を提供します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfnnng.cisco.com/> にアクセスします。



第 14 章

IP マルチキャストの最適化：等コストパス間での IP マルチキャストロードスプリッティング

- 等コストパス間での IP マルチキャストロードスプリットの前提条件 (295 ページ)
- 等コストパス間での IP マルチキャストロードスプリッティングについて (296 ページ)
- ECMP を介して IP マルチキャストトラフィックをロードスプリットする方法 (305 ページ)
- ECMP を介した IP マルチキャストトラフィックのロードスプリットの設定例 (313 ページ)
- IP マルチキャストの最適化に関するその他の関連情報：等コストパス間での IP マルチキャストロードスプリッティング (314 ページ)
- IP マルチキャストの最適化の機能履歴：等コストパス間での IP マルチキャストロードスプリッティング (315 ページ)

等コストパス間での IP マルチキャストロードスプリットの前提条件

IP マルチキャストをデバイスで有効にするには、『*IP Multicast Routing Configuration Guide*』の「Configuring Basic IP Multicast」モジュールに記載されているタスクを使用します。

等コストパス間での IP マルチキャスト ロードスプリッティングについて

ロードスプリットとロードバランシング

ロードスプリットとロードバランシングは同じではありません。ロードスプリットでは、複数の等コストリバースパスフォワーディング (RPF) パスを介して (*, G) および (S, G) トラフィックストリームをランダムに分散する手段が提供され、必ずしもそれらの等コスト RPF パス上で平衡のとれた IP マルチキャストトラフィック負荷が得られるわけではありません。IP マルチキャストトラフィックのロードスプリットに使用される方法は、(*, G) および (S, G) トラフィックストリームをランダムに分散させることによって、フローをカウントしてではなく、むしろ疑似乱数判定を作成して、使用可能な各 RPF パスに等価な量のトラフィックフローを分散させようとしています。これらの方法は総称して等コストマルチパス (ECMP) マルチキャストロードスプリットと呼ばれ、ほぼ同量の帯域幅を使用する多くのトラフィックストリームがあるネットワークでのロードシェアリングを向上させます。

一連の等コストリンクにわたってわずか 2、3 の (S, G) または (*, G) ステートフローしかない場合は、それらの良好なバランスが得られる可能性は非常に低くなります。この制限を克服するため、(S, G) ステートの場合は事前に計算された発信元アドレス、または (*, G) ステートの場合はランデブーポイント (RP) アドレスを使用して、合理的な形式のロードバランシングを実現できます。この制限は、Cisco Express Forwarding (CEF) または EtherChannel でのフロー単位のロードスプリットに同様に適用されます。わずかなフローがある限り、それらの方法でロードスプリットを行っても、何らかの形式の手動によるエンジニアリングなしでは良好なロード分散は得られません。

複数の等コストパスが存在する場合の IP マルチキャストのデフォルト動作

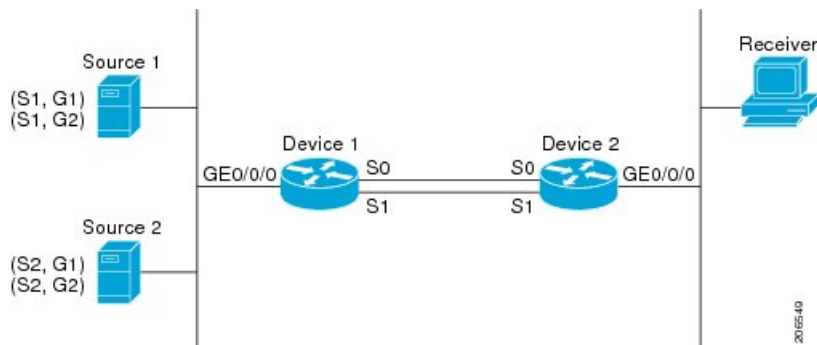
デフォルトでは、Protocol Independent Multicast スパースモード (PIM-SM)、Source Specific Multicast (PIM-SSM)、双方向 PIM (Bidir-PIM)、グループについては、複数の等コストパスが使用可能な場合、IPv4 マルチキャストトラフィック向けのリバースパスフォワーディング (RPF) は、最も大きい IP アドレスを持つ PIM ネイバーに基づきます。この方法は、最高 PIM ネイバー動作と呼ばれます。この動作は、PIM-SM の RFC2362 に基づいていますが、PIM-SSM、および Bidir-PIM にも適用されます。

次の図に、複数の等コストパスが存在する場合の IP マルチキャストのデフォルト動作を説明するためにここで使用するサンプルトポロジを示します。



(注) 次の図および例では設定内のルータを使用していますが、任意のデバイス (ルータやコントローラ) を使用できます。

図 19: 複数の等コストパスが存在する場合の IP マルチキャストのデフォルト動作



この図では、2つの送信元 S1 および S2 が、トラフィックを IPv4 マルチキャストグループ G1 および G2 に送信しています。PIM-SM、PIM-SSM、PIM-DM のいずれかをこのトポロジに使用できます。PIM-SM を使用する場合は、`ip pim spt-threshold` コマンドのデフォルト 0 がデバイス 2 で使用中であること、内部ゲートウェイプロトコル (IGP) が実行中であること、S1 および S2 (デバイス 2 で入力した場合) で `show ip route` コマンドの出力に、デバイス 1 のシリアルインターフェイス 0 とシリアルインターフェイス 1 が、デバイス 2 の等コストネクストホップ PIM ネイバーとして表示されることを前提としています。

追加の設定を行うことなく、図に示すトポロジ内の IPv4 マルチキャストトラフィックは、どちらのインターフェイスがより高い IP アドレスを持っているかに応じて、常に 1 つのシリアルインターフェイス (シリアルインターフェイス 0 またはシリアルインターフェイス 1) を経由して移動します。たとえば、デバイス 1 上のシリアルインターフェイス 0 とシリアルインターフェイス 1 で設定されている IP アドレスが、それぞれ 10.1.1.1 と 10.1.2.1 であるものとします。このシナリオが与えられているとして、PIM-SM と PIM-SSM の場合、デバイス 2 は、図に示されるすべてのソースおよびグループについて、常に PIM 加入メッセージを 10.1.2.1 に送信し、常にシリアルインターフェイス 1 上で IPv4 マルチキャストトラフィックを受信します。

IPv4 RPF ルックアップが中継マルチキャストデバイスによって実行され、IPv4 (*,G) および (S,G) マルチキャストルート (ツリー) のための RPF インターフェイスと RPF ネイバーが決定されます。RPF ルックアップは、RPF ルート選択とルートパス選択によって構成されます。RPF ルート選択は、マルチキャストツリーのルートを特定するために、IP ユニキャストアドレスだけで動作します。(*,G) ルート (PIM-SM および Bidir-PIM) の場合、マルチキャストツリーのルートはグループ G の RP アドレスです。(S,G) ツリー (PIM-SM、PIM-SSM) の場合、マルチキャストツリーのルートは送信元 S です。RPF ルート選択では、ルーティング情報ベース (RIB) で、また設定済みの場合 (または使用可能な場合) は、ディスタンスベクターマルチキャストルーティングプロトコル (DVMRP) ルーティングテーブルまたは設定済みの静的マルチキャストルーターで、RP または送信元に対する最適なルートが検索されます。得られたルートが使用可能な 1 つのパスだけだった場合は、RPF ルックアップが完了し、ルートのネクストホップデバイスおよびインターフェイスが、このマルチキャストツリーの RPF ネイバーと RPF インターフェイスになります。そのルートに使用可能な複数のパスがある場合は、ルートパス選択を使用して、どのパスを選択するかが決定されます。

IP マルチキャストでは、ルートパス選択に次の方法が使用できます。



(注) IP マルチキャストで使用可能なルートパス選択のデフォルトの方法以外のすべての方法で、いくつかの形式の ECMP マルチキャストロードスプリッティングが可能です。

- 最も高い PIM ネイバー：これはデフォルトの方法です。したがって、設定は不要です。複数の等コストパスが使用できる場合は、RPF for IPv4 マルチキャストトラフィックは、最も大きい IP アドレスを持つ PIM ネイバーに基づき、その結果、設定しなければ、ECMP マルチキャストロードスプリットはデフォルトでディセーブルになります。
- ECMP マルチキャストロードスプリットの送信元アドレスに基づいた方法：**ip multicast multipath** コマンドを使用して、ECMP マルチキャストロードスプリットを設定できます。この形式の **ip multicast multipath** コマンドを入力すると、S ハッシュアルゴリズムを使用した送信元アドレスに基づく ECMP マルチキャストロードスプリットがイネーブルになります。詳細については、「S ハッシュアルゴリズムを使用した、送信元アドレスに基づく ECMP マルチキャストロードスプリット」の項を参照してください。
- ECMP マルチキャストロードスプリットの送信元アドレスとグループアドレスに基づいた方法：**ip multicast multipath** コマンドに **s-g-hash** キーワードと **basic** キーワードを指定して、ECMP マルチキャストロードスプリットを設定できます。この形式の **ip multicast multipath** コマンドを入力すると、基本 S-G ハッシュアルゴリズムを使用した送信元アドレスとグループアドレスに基づく ECMP マルチキャストロードスプリットがイネーブルになります。詳細については、「基本 S-G ハッシュアルゴリズムを使用した、送信元アドレスとグループアドレスに基づく ECMP マルチキャストロードスプリット」の項を参照してください。
- ECMP マルチキャストロードスプリットの送信元アドレス、グループアドレス、ネクストホップアドレスに基づいた方法：**ip multicast multipath** コマンドに **s-g-hash** キーワードと **next-hop-based** キーワードを指定して、ECMP マルチキャストロードスプリットを設定できます。この形式のコマンドを入力すると、ネクストホップベースの S-G ハッシュアルゴリズムを使用した、ソースアドレス、グループアドレス、およびネクストホップアドレスに基づく ECMP マルチキャストロードスプリットが可能になります。詳細については、「送信元アドレス、グループアドレス、およびネクストホップアドレスに基づく ECMP マルチキャストロードスプリットのイネーブル化」の項を参照してください。

デフォルト動作（最高 PIM ネイバー動作）は、IP マルチキャストでのどのような形の ECMP ロードスプリットにもならず、使用可能なパスのネクストホップ PIM ネイバーの中から最も大きい IP アドレスを持つ PIM ネイバーを選択します。ネクストホップが **show ip pim neighbor** コマンドの出力に表示された場合、PIM ネイバーとみなされます。これは、PIM Hello メッセージがネクストホップから受信され、タイムアウトしていない場合です。使用可能なネクストホップのいずれも PIM ネイバーでない場合は、そのまま最も高い IP アドレスを持つネクストホップが選択されます。

IP マルチキャストトラフィックをロードスプリットする方法

一般に、IP マルチキャストトラフィックのロードスプリットには、次の方法が使用できます。

- ソースアドレス、ソースアドレスとグループアドレス、またはソースアドレスとグループアドレスとネクストホップアドレスに基づいて、ECMP マルチキャストロードスプリッティングをイネーブルにできます。等コストパスが認識された後、ECMP マルチキャストロードスプリットは、ユニキャストトラフィックと同様に、パケットごとではなく、(S, G) ごとに動作します。
- IP マルチキャストをロードスプリットする別の方法としては、2つ以上の等コストパスを Generic Routing Encapsulation (GRE) トンネルに統合して、ユニキャストルーティングプロトコルがロードスプリットを実行できるようにするか、または Fast または Gigabit EtherChannel インターフェイス、マルチリンク PPP (MLPPP) リンクバンドル、またはマルチリンクフレームリレー (FR.16) リンクバンドルなどのバンドルインターフェイスを介してロードスプリットできるようにします。

ECMP マルチキャストロードスプリットの概要

デフォルトでは、IPv4 マルチキャストトラフィックの ECMP マルチキャストロードスプリットはディセーブルになっています。ECMP マルチキャストロードスプリットは、**ip multicast multipath** コマンドを使用してイネーブルにできます。

S ハッシュアルゴリズムを使用した、ソースアドレスに基づく ECMP マルチキャストロードスプリット

発信元アドレスに基づく ECMP マルチキャストロードスプリットのトラフィックは、S ハッシュアルゴリズムを使用して、各 (*, G) または (S, G) ステートの RPF インターフェイスが、ステートの解決される RPF アドレスに応じて、使用可能な等コストパスの中から選択されるようにします。(S, G) ステートの場合、RPF アドレスはステートの発信元アドレスです。(*, G) ステートの場合、RPF アドレスはステートのグループアドレスに関連付けられた RP のアドレスです。

発信元アドレスに基づいて ECMP マルチキャストロードスプリットを設定すると、さまざまなステートのマルチキャストトラフィックを等コストインターフェイスのうち複数を経由して受信できます。原則として、IPv4 マルチキャストによって適用される方法は、IPv4 CEF でのデフォルトのフロー単位のロードスプリットまたは Fast および Gigabit EtherChannel で使用されるロードスプリットとかなり似ています。しかし、ECMP マルチキャストロードスプリットのこの方法は、局在化の影響を受けます。

基本 S-G ハッシュアルゴリズムを使用した、ソースアドレスとグループアドレスに基づく ECMP マルチキャストロードスプリット

送信元アドレスとグループアドレスに基づく ECMP マルチキャストロードスプリットでは、送信元アドレスとグループアドレスに基づいた基本 S-G ハッシュアルゴリズムと呼ばれる、単純なハッシュが使用されます。基本 S-G ハッシュアルゴリズムは、ハッシュ値を出すためにランダム化を一切使用しないため、予測可能です。ただし、S-G ハッシュアルゴリズムは、特定のソースとグループについて、どのデバイス上でそのハッシュが計算されたかに関係なく常に同じハッシュが得られるため、局在化する傾向があります。



(注) 基本の S-G ハッシュ アルゴリズムでは、Bidir-PIM グループは無視されます。

S ハッシュおよび基本 S-G ハッシュ アルゴリズムを使用した場合の副産物としての予測可能性

IPv4 マルチキャストの ECMP マルチキャスト ロードスプリットで使用される方法では、同じ数の等コストパスがトポロジ内の複数の場所に存在するネットワークにおいて、一貫したロードスプリットが可能です。フローを N パスを通して分割させるために RP アドレスまたは送信元アドレスが計算されると、フローはトポロジ内のすべての場所で同じようにそれらの N パスを通して分割されます。一貫したロードスプリットによって予測可能性を考慮でき、それにより、IPv4 マルチキャスト トラフィックのロードスプリットを手動で操作できるようになります。

S ハッシュおよび基本 S-G ハッシュ アルゴリズムを使用した場合の副産物としての局在化

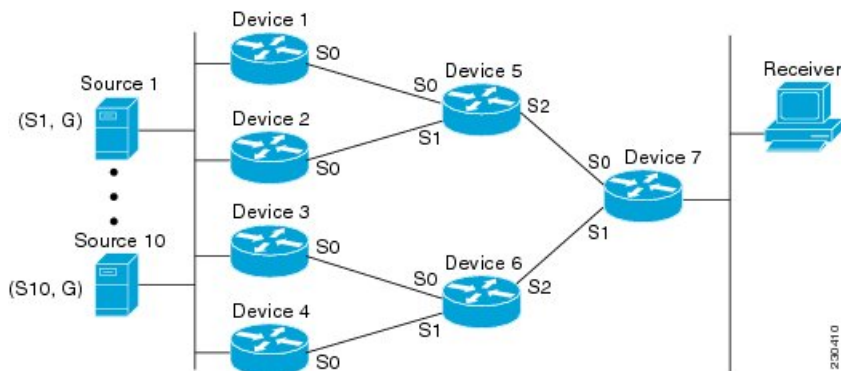
ソース アドレスまたはソースおよびグループ アドレスによってマルチキャスト トラフィックをロードスプリットするために IPv4 マルチキャストで使用されるハッシュ機能には通常、局在化と呼ばれる問題があります。ソース アドレスまたはソースおよびグループ アドレスに基づく ECMP マルチキャスト ロードスプリットの副産物として、局在化は、一部のトポロジ内のルータがロードスプリットに使用可能なすべてのパスを効果的に使用できないという問題です。

次の図に、ソース アドレスに基づく、またはソース アドレスとグループ アドレスに基づく ECMP マルチキャスト ロードスプリットを設定した場合の局在化の問題を説明するために、ここで使用するトポロジを示します。



(注) 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 20: 局在化トポロジ



図に示すトポロジでは、ルータ 7 がルータ 5 およびルータ 6 を経由してソース S1 ~ S10 に向かう 2 つの等コストパスがあることに注目してください。このトポロジでは、トポロジ内のすべてのルータで ECMP マルチキャストロードスプリッティングが `ip multicast multipath` コマンドを使用して有効になっていると仮定します。このシナリオでは、ルータ 7 は、10 個の (S, G) ステートに等コストロードスプリットを適用します。このシナリオにおける局在化の問題は、ルータ 7 に影響します。そのルータがソース S1 ~ S5 についてはルータ 5 でシリアルインターフェイス 0 を選択し、ソース S6 ~ S10 についてはルータ 6 でシリアルインターフェイス 1 を選択することになるからです。さらに、このトポロジでは、局在化の問題による影響はルータ 5 とルータ 6 にも及びます。ルータ 5 には、ルータ 1 上のシリアルインターフェイス 0 およびルータ 2 上のシリアルインターフェイス 1 を経由する S1 ~ S5 への 2 つの等コストパスがあります。ルータ 5 は、2 つのパスのどちらを使用するかを選択に同じハッシュアルゴリズムを適用するため、ソース S1 ~ S5 には 2 つのアップストリームパスのうちの片方だけを使用することになります。つまり、すべてのトラフィックがルータ 1 とルータ 5 を流れるか、またはルータ 2 とルータ 5 を流れるかのいずれかになります。このトポロジでは、ロードスプリットにルータ 1 とルータ 5 およびルータ 2 とルータ 5 を使用することはできません。同様に、局在化問題は、ルータ 3 とルータ 6 およびルータ 4 とルータ 6 に当てはまります。つまり、このトポロジでは、ロードスプリットにルータ 3 とルータ 6 およびルータ 4 とルータ 6 の両方を使用することはできません。

ソースグループとネクストホップアドレスに基づく ECMP マルチキャストロードスプリッティング

ソース、グループ、およびネクストホップアドレスに基づいて ECMP マルチキャストロードスプリットを設定すると、ソース、グループ、およびネクストホップアドレスに基づくより複雑なハッシュ、ネクストホップベースの S-G ハッシュアルゴリズムが有効になります。ネクストホップベースの S-G ハッシュアルゴリズムは、ハッシュ値の計算にランダム化を一切使用しないため、予測可能です。S ハッシュアルゴリズムや基本 S-G ハッシュアルゴリズムと違って、ネクストホップベースの S-G ハッシュアルゴリズムに使用されるハッシュメカニズムは、局在化の傾向がありません。



- (注) IPv4 マルチキャストにおけるネクストホップベースの S-G ハッシュアルゴリズムは、IPv6 ECMP マルチキャストロードスプリットで使用されるものと同じアルゴリズムであり、PIM-SM ブートストラップデバイス (BSR) に使用されるものと同じハッシュ機能を活用できます。

ネクストホップベースのハッシュ機能では局在化は生成されず、パスで障害が発生した場合により良い RPF の安定性が維持されます。これらの利点には、ソースアドレスまたは RP IP アドレスを使用して信頼性を持って予測したり、ネクストホップベースの S-G ハッシュアルゴリズムを使用した場合にロードスプリットの成果をエンジニアリングしたりすることができないという代償が伴います。多くのカスタマーネットワークは等コストマルチパストポロジを実装しているため、ロードスプリットの手動操作は多くの場合必須ではありません。むしろ、IP マルチキャストのデフォルトの動作が IP ユニキャストと類似している必要があります。つまり、IP マルチキャストはベストエフォートベースで複数の等コストパスを使用すると期待されます。そのため、局在化の異常により、IPv4 マルチキャストのロードスプリットはデフォルトで有効にできません。



- (注) また、CEF ユニキャストのロードスプリットは局在化を示さない方法を使用し、同様にロードスプリットの結果を予測したりロードスプリットの結果を操作するために使用することはできません。

ネクストホップ ベースのハッシュ機能では、PIM ネイバーの実際のネクストホップ IP アドレスが計算に取り込まれるため、局在化を回避できます。そのため、ハッシュの結果は各デバイスで異なり、実質的に局在化の問題はありません。局在化の回避に加えて、このハッシュ機能は、パスの障害に直面して選択された RPF パスの安定性も向上させます。4つの等コストパスを持つデバイスと、これらのパス間でロードスプリットされる多数のステートを考えます。これらのパスの1つに障害が発生し、残りの3つのパスが使用可能な状態になったとします。ハッシュ機能の二極化によって使用されるハッシュ機能（S ハッシュおよび基本の S-G ハッシュ アルゴリズムによって使用されるハッシュ機能）を使用して、すべてのステートの RPF パスは再コンバージェンスされるため、それら3つのパスの間（特にそれら3つのパスのいずれかをすでに使用していたパス）で変更される可能性があります。したがって、これらのステートは、その RPF インターフェイスとネクストホップ ネイバーが不必要に変更されることとなります。この問題が発生するのは、このアルゴリズムでは、選択されるパスが、考慮できるすべてのパスの総数を取ることでより決定されるためです。このため、いったんパスが変わると、すべてのステートの RPF 選択も変更の対象となります。ネクストホップ ベースのハッシュ アルゴリズムでは、RPF の変更されたパスを使用していたステートだけが、残る3つのパスのいずれかへと再コンバージェンスする必要があります。すでにこれらのパスのいずれかを使用しているステートは、変更されません。4つ目のパスが再び稼働し始めると、最初はそれを使用していたステートが、ただちに再コンバージェンスしてそのパスに戻ります。他のステートは、一切影響を受けません。



- (注) ネクストホップ ベースの S-G ハッシュ アルゴリズムでは、Bidir-PIM グループは無視されます。

RPF パス選択のための PIM ネイバー クエリおよびハロー メッセージへの ECMP マルチキャスト ロードスプリットの影響

ECMP を介する IP マルチキャスト トラフィックのロードスプリットがイネーブルになっておらず、RP またはソースに向けて複数の等コストパスが存在する場合、IPv4 マルチキャストは、まず最も大きい IP アドレスの PIM ネイバーを選択します。PIM ネイバーとは、受信した PIM ハロー（または PIMv1 クエリ）メッセージのソース デバイスです。たとえば、IGP で学習された、または2つのスタティック ルート経路で設定された2つの等コストパスを持つデバイスを考えてみます。これら2つのパスのネクストホップは、10.1.1.1 と 10.1.2.1 です。これらのネクストホップ デバイスの両方が PIM ハロー メッセージを送信した場合、10.1.2.1 が最も IP アドレスの大きい PIM ネイバーとして選択されます。10.1.1.1 だけが PIM ハロー メッセージを送信した場合は、10.1.1.1 が選択されます。これらのデバイスのどちらも PIM ハロー メッセージを送信しない場合は、10.1.2.1 が選択されます。PIM ハロー メッセージへのこの違いが、スタティック マルチキャスト ルート（mrout）しか持たない特定のタイプのダイナミック

ク フェールオーバー シナリオの構築を可能にします。それ以外では、これはあまり有用ではありません。



- (注) スタティック mroute の設定の詳細については、<ftp://ftpeng.cisco.com/ipmulticast/config-notes/static-mroutes.txt> で Cisco IOS IP マルチキャスト FTP サイトにある『*Configuring Multiple Static Mroutes in Cisco IOS*』設定ノートを参照してください。

ECMP を介する IP マルチキャストトラフィックのロードスプリットがイネーブルになっている場合、ネイバーからの PIM ハローメッセージの存在は考慮されません。つまり、選択される RPF ネイバーは、そのネイバーからの PIM ハローメッセージを受信したかどうかには左右されません。選択は、等コストルート エントリの有無にだけ依存します。

PIM-SM および PIM-SSM での PIM アサート処理に対する ECMP マルチキャストロードスプリットの影響

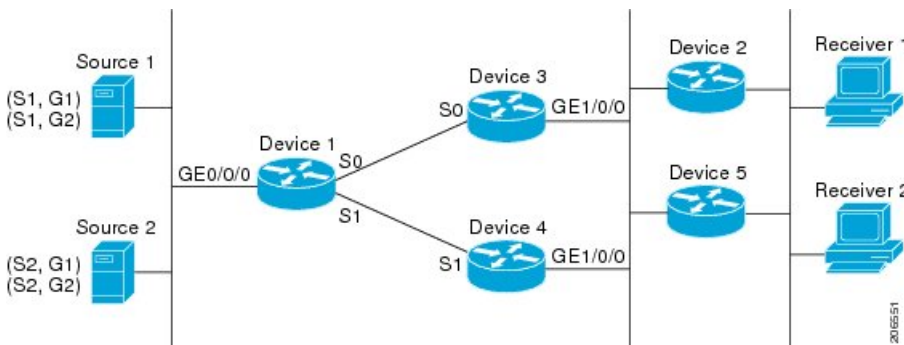
PIM-SM を (*, G) または (S, G) 転送で使用していた場合、または PIM-SSM を (S, G) 転送で使用していた場合でも、PIM アサート処理が発生したことが原因で **ip multicast multipath** コマンドでの ECMP マルチキャストロードスプリットが有効でなくなる場合もあります。

次の図に、PIM-SM および PIM-SSM での ECMP マルチキャストロードスプリットの PIM アサート処理への影響を説明するためにここで使用するサンプルトポロジを示します。



- (注) 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやコントローラ）を使用できます。

図 21: PIM-SM および PIM-SSM での ECMP マルチキャストロードスプリットと PIM アサート処理



図に示すトポロジでは、デバイス 2 とデバイス 5 の両方がシスコデバイスで、**ip multicast multipath** コマンドを使用して ECMP マルチキャストロードスプリット用に一貫性を持って設定されており、ロードスプリットが期待どおりに動作し続けるようになっています。つまり、両方のデバイスがデバイス 3 とデバイス 4 を等コストネクストホップとして持ち、等コストパスのリストを同じ方法で (IP アドレスにより) ソートします。各 (S, G) ステートまたは (*, G) ステートに対してマルチパスハッシュ関数を適用すると、それらは同じ RPF ネイバー (デバ

イス 3 またはデバイス 4) を選択し、その PIM 加入をこのネイバーに送信するようになります。

デバイス 5 とデバイス 2 が `ip multicast multipath` コマンドで一貫性のないように設定されている場合、またはデバイス 5 がサードパーティ製デバイスの場合は、デバイス 2 とデバイス 5 が、一部の (*, G) ステートまたは (S, G) ステートに対して異なる RPF ネイバーを選択する可能性があります。たとえば、デバイス 2 は、特定の (S, G) ステートに対してデバイス 3 を選択し、デバイス 5 は特定の (S, G) ステートに対してデバイス 4 を選択したりします。このシナリオでは、デバイス 3 とデバイス 4 が両方ともそのステートのトラフィックのギガビットイーサネットインターフェイス 1/0/0 への転送を開始し、お互いの転送したトラフィックを見て、トラフィックの重複を回避するためにアサート処理を開始します。その結果、その (S, G) ステートについては、ギガビットイーサネットインターフェイス 1/0/0 に最も大きい IP アドレスを持つデバイスがトラフィックを転送します。ところが、デバイス 2 とデバイス 5 は両方ともアサート選定での選択結果を追跡し、このアサートで選択されたデバイスが自分がその RPF 選択で計算して得たデバイスと同じでなくても、そのステートのための PIM 加入をこのアサートで選択されたデバイスに送信します。このため、PIM-SM と PIM-SSM では、ECMP マルチキャストロードスプリットの動作が保証されるのは、LAN 上のすべてのダウンストリームデバイスが一貫性を持って設定されたシスコ デバイスである場合だけです。

ユニキャストルーティングが変わった場合の ECMP マルチキャストロードスプリットと再コンバージェンス

ユニキャストルーティングが変わると、すべての IP マルチキャストルーティング ステートが、利用可能なユニキャストルーティング情報を元にしてただちに再コンバージェンスされません。特に、1つのパスが停止した場合、残りのパスがただちに再コンバージェンスされ、そのパスが再び稼働し始めた場合、それ以降は、マルチキャスト転送は、そのパスが停止する前に使用されていた同じ RPF パスに再コンバージェンスされます。再コンバージェンスは、ECMP 上の IP マルチキャストトラフィックのロードスプリットが設定されているかどうかにかかわらず発生します。

スタティック mroute での ECMP マルチキャストロードスプリットの使用

特定のソースまたは RP に対して IGP を使用して等コストルートをインストールすることが可能でない場合、スタティックルートを設定して、ロードスプリットのための等コストパスを指定することができます。ソフトウェアは、プレフィックスに対し1つのスタティック mroute という設定をサポートしていないため、等コストパスの設定にスタティック mroute は使用できません。再帰的なルートルックアップを使用した場合のこの制限にはいくつかの回避策がありますが、その回避策は等コストマルチパスルーティングには適用できません。



(注) スタティック mroute の設定の詳細については、[ftp://ftpeng.cisco.com/ipmulticast/config-notes/static-mroutes.txt](http://ftpeng.cisco.com/ipmulticast/config-notes/static-mroutes.txt) で Cisco IOS IP マルチキャスト FTP サイトにある『*Configuring Multiple Static Mroutes in Cisco IOS*』設定ノートを参照してください。

IPv4 マルチキャストでは等コスト マルチパスにスタティック `mroute` のみを指定できます。しかし、それらのスタティック `mroute` はマルチキャストにのみ適用できます。または、等コスト マルチパスがユニキャストおよびマルチキャストルーティングの両方に適用されるように指定できます。IPv6 マルチキャストでは、このような制限はありません。等コスト マルチパス `mroute` を、ユニキャストルーティングのみ、マルチキャストルーティングのみ、またはこの双方に適用するスタティック IPv6 `mroute` に設定することができます。

IP マルチキャスト トラフィックのロードスプリッティングの代替方法

IP マルチキャスト トラフィックのロードスプリットは、複数のパラレルリンクを単一のトンネルに統合し、マルチキャストトラフィックがそのトンネルを介してルーティングされるようにすることによっても達成できます。ロードスプリッティングのこの方法は、ECMP マルチキャストロードスプリッティングよりも設定が複雑です。GRE リンクを使用した等コストパスを介したロードスプリットを設定するのが有利である例として、(S, G) ステートまたは (*, G) ステートの合計数が非常に小さく、各ステートによって伝送される帯域幅の変動が大きい場合、ソースまたは RP アドレスの手動でのエンジニアリングでさえトラフィックの適切なロードスプリットを保証できない場合が挙げられます。



(注) ECMP マルチキャストロードスプリットの可用性があるため、通常は、パケットごとのロードシェアリングが必要な場合にしかトンネルを使用する必要はありません。

IP マルチキャスト トラフィックは、ファストまたはギガビット EtherChannel インターフェイス、MLPPP リンクバンドル、マルチリンク フレームリレー (FRF.16) バンドルなどのバンドルインターフェイスを介したロードスプリットにも使用できます。GRE またはその他のタイプのトンネルも、このような形態のレイヤ2 リンクバンドルを構成できます。このようなレイヤ2 メカニズムを使用する場合は、ユニキャストとマルチキャストのトラフィックがどのようにロードスプリットされるかを理解しておく必要があります。

トンネルを介した等コストパス間で IP マルチキャスト トラフィックをロードスプリットするには、その前に CEF のパケットごとのロードバランシングを設定しておく必要があります。これをしなければ、GRE パケットにパケットごとのロードバランシングが行われません。

ECMP を介して IP マルチキャスト トラフィックをロードスプリットする方法

ECMP マルチキャストロードスプリットのイネーブル化

発信元アドレスに基づいて複数の等コストパス間で IP マルチキャスト トラフィックの負荷を分割するには、次のタスクを実行します。

ソースから 2 つ以上の等コストパスが使用できる場合は、ユニキャスト トラフィックはそれらのパスの間でロードスプリットされます。一方、マルチキャスト トラフィックは、デフォ

ルトでは、複数の等コストパスの間でロードスプリットすることはありません。一般に、マルチキャストトラフィックは、RPF ネイバーから下流に流れます。PIM 仕様によると、複数のネイバーが同じメトリックを持つ場合、このネイバーは最も大きい IP アドレスを持っていない限りなりません。

ip multicast multipath コマンドでロードスプリットを設定すると、システムは送信元アドレスに基づき、S ハッシュアルゴリズムを使用して複数の等コストパスの間でマルチキャストトラフィックをロードスプリットします。**ip multicast multipath** コマンドを設定して、複数の等コストパスが存在する場合、マルチキャストトラフィックを伝送するパスは、送信元 IP アドレスに基づいて選択されます。異なる複数のソースからのマルチキャストトラフィックが、異なる複数の等コストパスの間でロードスプリットされます。同一ソースから異なる複数のマルチキャストグループに送信されたマルチキャストトラフィックについては、複数の等コストパスの間でロードスプリットは行われません。



- (注) **ip multicast multipath** コマンドは、トラフィックのロードバランシングではなくロードスプリットを行います。ソースからのトラフィックは、そのトラフィックがその他のソースからのトラフィックよりはるかに多い場合でも、1つのパスしか使用しません。

IP マルチキャスト ロードスプリットの前提条件：ECMP

- 送信元アドレスに基づいて ECMP マルチキャスト ロードスプリットを有効にするには、十分な数の送信元（少なくとも 3 つの送信元）が必要です。
- ECMP マルチキャスト ロードスプリットを設定するには、RP が使用できる複数のパスが必要です。



- (注) 送信元または RP がそれぞれ使用できるパスが複数あることを確認するには、*ip-address* 引数に送信元の IP アドレスまたは RP の IP アドレスを指定して、**show ip route** コマンドを使用します。コマンドの出力に複数のパスが表示されない場合は、ECMP マルチキャストロードスプリットを設定することはできません。
- 最短パス ツリー (SPT) フォワーディングで PIM-SM を使用する場合は、すべての (S, G) ステートのフォワーディングに T ビットを設定する必要があります。
 - ECMP マルチキャスト ロードスプリットを設定する前に、**show ip rpf** コマンドを使用して、送信元が IP マルチキャストマルチパス機能を利用できるかどうかを確認しておくことをベストプラクティスとして推奨します。

IP マルチキャスト ロードスプリッティング ECMP の制約事項

- ソースから 2 つ以上の等コストパスが使用できる場合は、ユニキャストトラフィックはそれらのパスの間でロードスプリットされます。一方、マルチキャストトラフィックは、

デフォルトでは、複数の等コストパスの間でロードスプリットすることはありません。一般に、マルチキャストトラフィックは、RPF ネイバーから下流に流れます。PIM 仕様によると、複数のネイバーが同じメトリックを持つ場合、このネイバーは最も大きい IP アドレスを持っていないければなりません。

- **ip multicast multipath** コマンドは、同一の PIM ネイバー IP アドレスに複数の等コストパスを介して到達できるような設定はサポートしていません。この状況は、通常、番号付けされていないインターフェイスを使用している場合に発生します。**ip multicast multipath** コマンドを設定する際は、すべてのインターフェイスに異なる IP アドレスを使用します。
- **ip multicast multipath** コマンドは、トラフィックのロードバランシングではなくロードスプリットを行います。ソースからのトラフィックは、そのトラフィックがその他のソースからのトラフィックよりはるかに多い場合でも、1つのパスしか使用しません。

ソースアドレスに基づく ECMP マルチキャストロードスプリットのイネーブル化

ソースアドレスに基づいたマルチキャストトラフィックの ECMP マルチキャストロードスプリット (Sハッシュアルゴリズムを使用) をイネーブルにして、ネットワーク上にある複数のパスの利点を活かすには、次の作業を実行します。Sハッシュアルゴリズムは、ハッシュ値の計算にランダム化を一切使用しないため、予測可能です。ただし、Sハッシュアルゴリズムは、特定のソースについて、ハッシュが計算されたデバイスに関係なく常に同じハッシュが得られるため、局在化する傾向があります。



- (注) 複数の着信インターフェイスからのトラフィックのレシーバになるデバイスで ECMP マルチキャストロードスプリットをイネーブルにします。これは、ユニキャストルーティングと反対です。ユニキャストの視点からすると、複数の発信インターフェイスに接続されている送信デバイス上でマルチキャストがアクティブになっています。

始める前に

- 発信元アドレスに基づいて ECMP マルチキャストロードスプリットを有効にするには、十分な数の送信元 (少なくとも 3 つの送信元) が必要です。
- ECMP マルチキャストロードスプリットを設定するには、RP が使用できる複数のパスが必要です。



- (注) 送信元または RP がそれぞれ使用できるパスが複数あることを確認するには、**ip-address** 引数に送信元の IP アドレスまたは RP の IP アドレスを指定して、**show ip route** コマンドを使用します。コマンドの出力に複数のパスが表示されない場合は、ECMP マルチキャストロードスプリットを設定することはできません。

- 最短パス ツリー (SPT) フォワーディングで PIM-SM を使用する場合は、すべての (S, G) ステートのフォワーディングに T ビットを設定する必要があります。
- ECMP マルチキャスト ロード スプリットを設定する前に、**show ip rpf** コマンドを使用して、送信元が IP マルチキャストマルチパス機能を利用できるかどうかを確認しておくことをベストプラクティスとして推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： <pre>Device> enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： <pre>Device# configure terminal</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 3	ip multicast multipath 例： <pre>Device(config)# ip multicast multipath</pre>	S ハッシュ アルゴリズムを使用した、ソース アドレスに基づく ECMP マルチキャスト ロードスプリットをイネーブルにします。 <ul style="list-style-type: none"> • このコマンドは RPF ネイバーが選択される方法を変更するため、ループを回避するために、冗長トポロジ内のすべてのデバイスに一貫性を持たせて設定しなければなりません。 • このコマンドは、同一の PIM ネイバー IP アドレスに複数の等コストパスを介して到達できるような設定はサポートしていません。この状況は、通常、番号付けされていないインターフェイスを使用している場合に発生します。このコマンドが設定されるデバイスでは、各インターフェイスに異なる IP アドレスを使用します。 • このコマンドは、トラフィックのロード バランシングではなくロードスプリットを行います。ソースからのトラフィックは、そのトラ

	コマンドまたはアクション	目的
		フィックがその他のソースからのトラフィックよりはるかに多い場合でも、1つのパスしか使用しません。
ステップ 4	冗長トポロジ内のすべてのデバイスで、ステップ 3 を繰り返します。	--
ステップ 5	exit 例 : Device(config)# exit	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	show ip rpf source-address [group-address] 例 : Device# show ip rpf 10.1.1.2	(任意) IP マルチキャストルーティングが RPF チェックの実行に使用する情報を表示します。 <ul style="list-style-type: none"> IP マルチキャストトラフィックが正常にロードスプリットされるようにするために、このコマンドを使用して RPF 選択を確認します。
ステップ 7	show ip route ip-address 例 : Device# show ip route 10.1.1.2	(任意) IP ルーティングテーブルの現在のステータスを表示します。 <ul style="list-style-type: none"> このコマンドを使用して、ECMP マルチキャストロードスプリットのために、ソースまたは RP までに複数のパスが使用できることを確認します。 <i>ip-address</i> 引数については、ソースまでに複数のパスが使用できることを確認するにはソースの IP アドレスを入力し (最短パスツリーの場合)、RP までに複数のパスが使用できることを確認するには RP の IP アドレスを入力します (共有ツリーの場合)。

ソースアドレスおよびグループアドレスに基づく ECMP マルチキャストロードスプリットのイネーブル化

ソースアドレスとグループアドレスに基づいたマルチキャストトラフィックの ECMP マルチキャストロードスプリット (基本 S-G ハッシュアルゴリズムを使用) をイネーブルにして、ネットワーク上にある複数のパスの利点を活かすには、次の作業を実行します。基本 S-G ハッ

シチュアルゴリズムは、ハッシュ値の計算にランダム化を一切しようしないため、予測可能です。ただし、基本 S-G ハッシュアルゴリズムは、特定のソースとグループについて、ハッシュが計算されているデバイスに関係なく常に同じハッシュが得られるため、局在化する傾向があります。

基本 S-G ハッシュアルゴリズムは、ECMP マルチキャストロードスプリットに対して、S ハッシュアルゴリズムよりも柔軟なサポートを提供します。ロードスプリットに基本 S-G ハッシュアルゴリズムを使用すると、特に、グループに多数のストリームを送信するデバイスや、IPTV サーバーや MPEG ビデオサーバーのように多くのチャンネルをブロードキャストするデバイスからのマルチキャストトラフィックを、複数の等コストパスの間でより効果的にロードスプリットすることが可能になります。



- (注) 複数の着信インターフェイスからのトラフィックのレシーバになるデバイスで ECMP マルチキャストロードスプリットをイネーブルにします。これは、ユニキャストルーティングと反対です。ユニキャストの視点からすると、複数の発信インターフェイスに接続されている送信デバイス上でマルチキャストがアクティブになっています。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： <code>Device> enable</code>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： <code>Device# configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip multicast multipath s-g-hash basic 例： <code>Device(config)# ip multicast multipath s-g-hash basic</code>	基本 S-G ハッシュアルゴリズムを使用した、ソース アドレスとグループ アドレスに基づく ECMP マルチキャストロードスプリットをイネーブルにします。 <ul style="list-style-type: none">このコマンドは RPF ネイバーが選択される方法を変更するため、ループを回避するために、冗長トポロジ内のすべてのデバイスに一貫性を持たせて設定しなければなりません。
ステップ 4	冗長トポロジ内のすべてのデバイスで、ステップ 3 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 5	exit 例： Device(config)# exit	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	show ip rpf source-address [group-address] 例： Device# show ip rpf 10.1.1.2	(任意) IP マルチキャストルーティングが RPF チェックの実行に使用する情報を表示します。 <ul style="list-style-type: none"> IP マルチキャストトラフィックが正常にロードスプリットされるようにするために、このコマンドを使用して RPF 選択を確認します。
ステップ 7	show ip route ip-address 例： Device# show ip route 10.1.1.2	(任意) IP ルーティングテーブルの現在のステータスを表示します。 <ul style="list-style-type: none"> このコマンドを使用して、ECMP マルチキャストロードスプリットのために、ソースまたは RP までに複数のパスが使用できることを確認します。 ip-address 引数については、ソースまでに複数のパスが使用できることを確認するにはソースの IP アドレスを入力し（最短パスツリーの場合）、RP までに複数のパスが使用できることを確認するには RP の IP アドレスを入力します（共有ツリーの場合）。

ソースグループおよびネクストホップアドレスに基づく ECMP マルチキャストロードスプリットのイネーブル化

ソースアドレス、グループアドレス、およびネクストホップアドレスに基づいたマルチキャストトラフィックの ECMP マルチキャストロードスプリット（ネクストホップベースの S-G ハッシュアルゴリズムを使用）をイネーブルにして、ネットワーク上にある複数のパスの利点を活かすには、次の作業を実行します。ネクストホップベースの S-G ハッシュアルゴリズムは、ハッシュ値の計算にランダム化を一切使用しないため、予測可能です。S ハッシュアルゴリズムや基本 S-G ハッシュアルゴリズムと違って、ネクストホップベースの S-G ハッシュアルゴリズムに使用されるハッシュメカニズムは、局在化の傾向がありません。

ネクストホップベースの S-G ハッシュアルゴリズムは、ECMP マルチキャストロードスプリットに対して、S ハッシュアルゴリズムよりも柔軟なサポートを提供し、局在化の問題をな

くします。ECMP マルチキャスト ロードスプリットにネクストホップベースの S-G ハッシュ アルゴリズムを使用すると、グループに多数のストリームを送信するデバイスや、IPTV サーバーや MPEG ビデオ サーバーのように多くのチャンネルをブロードキャストするデバイスからのマルチキャストトラフィックを、複数の等コストパスの間でより効果的にロードスプリットすることが可能になります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip multicast multipath s-g-hash next-hop-based 例： Device(config)# ip multicast multipath s-g-hash next-hop-based	ネクストホップベースの S-G ハッシュ アルゴリズムを使用した、ソース アドレス、グループ アドレス、およびネクストホップアドレスに基づく ECMP マルチキャスト ロードスプリットをイネーブル化します。 <ul style="list-style-type: none"> このコマンドは RPF ネイバーが選択される方法を変更するため、ループを回避するために、冗長トポロジ内のすべてのルータに一貫性を持たせて設定しなければなりません。 (注) 複数の着信インターフェイスからのトラフィックの受信先になると想定されるルータ上で、 ip multicast multipath コマンドをイネーブルにします。これは、ユニキャストルーティングと反対です。ユニキャストの視点からすると、複数の発信インターフェイスに接続されている送信ルータ上でマルチキャストがアクティブになっています。
ステップ 4	冗長トポロジ内のすべてのルータについて、ステップ 1～3 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 5	end 例： Device(config)# end	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	show ip rpf source-address [group-address] 例： Device# show ip rpf 10.1.1.2	(任意) IP マルチキャストルーティングが RPF チェックの実行に使用する情報を表示します。 <ul style="list-style-type: none"> IP マルチキャストトラフィックが正常にロードスプリットされるようにするために、このコマンドを使用して RPF 選択を確認します。
ステップ 7	show ip route ip-address 例： Device# show ip route 10.1.1.2	(任意) IP ルーティングテーブルの現在のステータスを表示します。 <ul style="list-style-type: none"> このコマンドを使用して、ECMP マルチキャストロードスプリットのために、ソースまたは RP までに複数のパスが使用できることを確認します。 <i>ip-address</i> 引数については、ソースまでに複数のパスが使用できることを確認するにはソースの IP アドレスを入力し（最短パスツリーの場合）、RP までに複数のパスが使用できることを確認するには RP の IP アドレスを入力します（共有ツリーの場合）。

ECMP を介した IP マルチキャストトラフィックのロードスプリットの設定例

例：ソースアドレスに基づく ECMP マルチキャストロードスプリットのイネーブル化

次の例は、S ハッシュ アルゴリズムを使用した、ソースアドレスに基づく ECMP マルチキャストロードスプリットをルータ上でイネーブルにする方法を示します。

```
ip multicast multipath
```

ソース アドレスおよびグループ アドレスに基づく ECMP マルチキャスト ロードスプリットのイネーブル化の例

次の例は、基本 S-G ハッシュ アルゴリズムを使用した、ソース アドレスとグループ アドレスに基づく ECMP マルチキャスト ロードスプリットをルータ上でイネーブルにする方法を示します。

```
ip multicast multipath s-g-hash basic
```

ソース グループおよびネクストホップ アドレスに基づく ECMP マルチキャスト ロードスプリットのイネーブル化の例

次の例は、ネクストホップ ベースの S-G ハッシュ アルゴリズムを使用した、ソース アドレス、グループ アドレス、およびネクストホップ アドレスに基づく ECMP マルチキャスト ロードスプリットをルータ上でイネーブルにする方法を示します。

```
ip multicast multipath s-g-hash next-hop-based
```

IP マルチキャストの最適化に関するその他の関連情報： 等コストパス間での IP マルチキャスト ロードスプリッ ティング

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。 <i>Command Reference (Catalyst 9200 Series Switches)</i>

標準および RFC

標準/RFC	タイトル
RFC 4601	『Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification』

IP マルチキャストの最適化の機能履歴：等コストパス間での IP マルチキャストロードスプリッティング

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	IP マルチキャストの最適化：ECMP を介した IP マルチキャストトラフィックのロードスプリット	ロードスプリットとロードバランシングは同じではありません。ロードスプリットでは、複数の等コストリバーパスフォワーディング (RPF) パスを介して (*,G) および (S,G) トラフィックストリームをランダムに分散する手段が提供され、必ずしもそれらの等コスト RPF パス上で平衡のとれた IP マルチキャストトラフィック負荷が得られるわけではありません。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfmng.cisco.com/> にアクセスします。



第 15 章

IP マルチキャストの最適化：マルチキャスト向け SSM チャンネルベースフィルタリング

- [マルチキャスト境界向け SSM チャンネルベースフィルタリングの前提条件 \(317 ページ\)](#)
- [マルチキャスト境界向け SSM チャンネルベースフィルタリングについて \(317 ページ\)](#)
- [マルチキャスト境界向け SSM チャンネルベースフィルタリングの設定方法 \(318 ページ\)](#)
- [マルチキャスト境界向け SSM チャンネルベースフィルタリングの設定例 \(320 ページ\)](#)
- [IP マルチキャストの最適化：マルチキャスト向け SSM チャンネルベースフィルタリングに関するその他の参考資料 \(321 ページ\)](#)
- [IP マルチキャストの最適化の機能履歴：マルチキャスト向け SSM チャンネルベースフィルタリング \(321 ページ\)](#)

マルチキャスト境界向け SSM チャンネルベースフィルタリングの前提条件

IP マルチキャストをデバイスで有効にするには、『*IP Multicast: PIM Configuration Guide*』の「Configuring Basic IP Multicast」モジュールに記載されているタスクを使用します。

マルチキャスト境界向け SSM チャンネルベースフィルタリングについて

ここでは、マルチキャスト境界向けの SSM チャンネルベースフィルタリング機能について説明します。

マルチキャスト境界のルール

マルチキャスト境界向けの SSM チャンネルベース フィルタリング機能は、**ip multicast boundary** コマンドを拡張して、コントロールプレーン フィルタリングをサポートします。1つのインターフェイスに複数の **ip multicast boundary** コマンドを適用できます。

次のルールで **ip multicast boundary** コマンドは制御されます。

- 1つのインターフェイスに設定できるのは、**in** および **out** キーワードの一方のインスタンスです。
- **in** および **out** キーワードは、標準アクセスリストまたは拡張アクセスリストに使用できません。
- **filter-autorp** キーワードまたは **no** キーワードを使用する場合、標準のアクセスリストだけが許可されます。
- コマンドの最大3つのインスタンスが1つのインターフェイスで許可されます。**in** の1つのインスタンス、**out** の1つのインスタンス、および **filter-autorp** または **no** キーワードの1つのインスタンスです。
- コマンドの複数のインスタンスを使用すると、フィルタリングは累積的になります。キーワードなしの境界ステートメントが、**in** キーワードが含まれる境界ステートメントと存在する場合、両方のアクセスリストが入力方向に適用され、どちらか一方での一致で十分です。
- コマンドのすべてのインスタンスは、制御トラフィックおよびデータプレーントラフィックの両方に適用されます。
- 拡張アクセスリストのプロトコル情報は解析され、一貫性の再利用とフィルタリングが許可されます。アクセスリストがすべてのプロトコルの (S,G) トラフィックをフィルタリングする場合、(S,G) オペレーションは、キーワードについて記述されたすべての条件で拡張アクセスリストによってフィルタリングされます。

マルチキャスト境界向け SSM チャンネル ベース フィルタリングの利点

- この機能によって、送信元インターフェイスでの入力が可能になります。
- アクセス制御機能は、SSM および Any Source Multicast (ASM) の場合と同じです。

マルチキャスト境界向け SSM チャンネル ベース フィルタリングの設定方法

ここでは、マルチキャスト境界に SSM チャンネルベースのフィルタリングを設定する手順について説明します。

マルチキャスト境界の設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip access-list {standard extended} access-list-name 例 : Device(config)# ip access-list 101	標準または拡張のアクセス リストを設定します。
ステップ 4	permit protocol host address host address 例 : Device(config-ext-nacl)# permit ip host 181.1.2.201 host 232.1.1.11	指定された ip ホスト トラフィックを許可します。
ステップ 5	deny protocol host address host address 例 : Device(config-acl-nacl)# deny ip host 181.1.2.203 host 232.1.1.1	指定されたマルチキャスト ip グループ および送信元 トラフィックを拒否します。
ステップ 6	必要に応じて、ステップ 4 または ステップ 5 を繰り返します。	指定されたホスト および送信元 トラフィックを許可 および 拒否 します。
ステップ 7	interface type interface-number port -number 例 : Device(config)# interface gigabitethernet 2/3/0	インターフェイス コンフィギュレーション モードをイネーブルにします。
ステップ 8	ip multicast boundary access-list-name [in out filter-autorp]	マルチキャスト境界を設定します。 (注)

	コマンドまたはアクション	目的
	例： Device(config-if)# ip multicast boundary acc_grp1 out	filter-autorp キーワードは、拡張アクセスリストをサポートしていません。

マルチキャスト境界向け SSM チャンネル ベース フィルタリングの設定例

ここでは、マルチキャスト境界向け SSM チャンネル ベースフィルタリング機能の設定例を紹介します。

トラフィックを許可および拒否するマルチキャスト境界の設定例

次の例では、(181.1.2.201, 232.1.1.1) および (181.1.2.202, 232.1.1.1) への発信トラフィックを許可し、他のすべての (S,G) を拒否します。

```
configure terminal
ip access-list extended acc_grp1
permit ip host 0.0.0.0 232.1.1.1 0.0.0.255
permit ip host 181.1.2.201 host 232.1.1.1
permit udp host 181.1.2.202 host 232.1.1.1
permit ip host 181.1.2.202 host 232.1.1.1
deny igmp host 181.2.3.303 host 232.1.1.1
interface gigabitethernet 1/0/1
ip multicast boundary acc_grp1 out
```

トラフィックを許可するマルチキャスト境界の設定例

次の例では、(192.168.2.201, 232.1.1.5) および (192.168.2.202, 232.1.1.5) への発信トラフィックを許可します。

```
configure terminal
ip access-list extended acc_grp6
permit ip host 0.0.0.0 232.1.1.1 5.0.0.255
deny udp host 192.168.2.201 host 232.1.1.5
permit ip host 192.168.2.201 host 232.1.1.5
deny pim host 192.168.2.201 host 232.1.1.5
permit ip host 192.168.2.202 host 232.1.1.5
deny igmp host 192.2.3.303 host 232.1.1.1
interface gigabitethernet 1/0/1
ip multicast boundary acc_grp6 out
```

トラフィックを拒否するマルチキャスト境界の設定例

次に、候補 RP でアナウンスされるグループ範囲を拒否する例を示します。グループ範囲が拒否されるため、pim auto-rp マッピングは作成されません。

```
configure terminal
ip access-list standard acc_grp10
deny 225.0.0.0 0.255.255.255
permit any
access-list extended acc_grp12
permit pim host 181.1.2.201 host 232.1.1.8
deny udp host 181.1.2.201 host 232.1.1.8
permit pim host 181.1.2.203 0.0.0.255 host 227.7.7.7
permit ip host 0.0.0.0 host 227.7.7.7
permit ip 181.1.2.203 0.0.0.255 host 227.7.7.7
permit ip host 181.1.2.201 host 232.1.1.7
ip access-list extended acc_grp13
deny ip host 181.1.2.201 host 232.1.1.8
permit ip any any
interface gigabitethernet 1/0/1
ip multicast boundary acc_grp10 filter-autorp
ip multicast boundary acc_grp12 out
ip multicast boundary acc_grp13 in
```

IP マルチキャストの最適化：マルチキャスト向け SSM チャンネルベース フィルタリングに関するその他の参考資料

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9200 Series Switches)</i> の「IP マルチキャストルーティング コマンド」の項を参照してください。

IP マルチキャストの最適化の機能履歴：マルチキャスト向け SSM チャンネルベース フィルタリング

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	IP マルチキャストの最適化：マルチキャスト向け SSM チャンネル ベース フィルタリング	マルチキャスト境界のための SSM チャンネル ベース フィルタリング機能は、 <code>ip multicast boundary</code> コマンドを拡張して、コントロールプレーン フィルタリングをサポートします。複数の <code>ip multicast boundary</code> コマンドをインターフェイスに適用できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfng.cisco.com/> にアクセスします。



第 16 章

IP マルチキャストの最適化：IGMP ステート制限

- [IGMP ステート制限の前提条件 \(323 ページ\)](#)
- [IGMP ステート制限の制約事項 \(323 ページ\)](#)
- [IGMP ステート制限に関する情報 \(323 ページ\)](#)
- [IGMP ステート制限の設定方法 \(325 ページ\)](#)
- [IGMP ステート制限の設定例 \(327 ページ\)](#)
- [その他の参考資料 \(329 ページ\)](#)
- [IP マルチキャストの最適化の機能履歴：IGMP ステート制限 \(329 ページ\)](#)

IGMP ステート制限の前提条件

- IP マルチキャストを有効にして、Protocol Independent Multicast (PIM) インターフェイスを設定するには、『*IP Multicast: PIM Configuration Guide*』の「Configuring Basic IP Multicast」モジュールに記載されているタスクを使用します。
- すべての ACL を設定する必要があります。詳細については、『*Security Configuration Guide: Access Control Lists*』ガイドの「Creating an IP Access List and Applying It to an Interface」モジュールを参照してください。

IGMP ステート制限の制約事項

デバイスごとに1つのグローバル制限と、インターフェイスごとに1つの制限を設定できません。

IGMP ステート制限に関する情報

ここでは、IGMP ステート制限について説明します。

IGMP ステート制限

IGMP ステート制限機能を使用すると、IGMP ステートリミッタの設定が可能になり、この設定により、IGMP メンバーシップレポート (IGMP 加入) により生成される mroute ステートの数がグローバルに、またはインターフェイスごとに制限されます。設定されている制限を超えたメンバーシップレポートは、IGMP キャッシュに入れられません。この機能により、DoS (サービス拒絶) 攻撃を防止したり、すべてのマルチキャストフローがほぼ同量の帯域幅を使用するネットワーク環境でマルチキャスト CAC メカニズムを提供したりできます。



(注) IGMP ステートリミッタは、IGMP、IGMP v3lite、および URL Rendezvous Directory (URD) メンバーシップレポートから生じる route ステートの数に、グローバルまたはインターフェイスごとに制限をかけます。

IGMP ステート制限機能の設計

- グローバル コンフィギュレーション モードで IGMP ステートリミッタを設定すると、キャッシュに格納できる IGMP メンバーシップレポートの数に対してグローバルな制限を指定できます。
- インターフェイス コンフィギュレーション モードで IGMP ステートリミッタを設定すると、IGMP メンバーシップレポートの数に対してインターフェイスごとの制限を指定できます。
- ACL を使用すれば、グループまたはチャンネルがインターフェイス制限に対してカウントされることがなくなります。標準 ACL または拡張 ACL を指定できます。標準 ACL は、(*, G) ステートがインターフェイスへの制限から除外されるように定義するのに使用できます。拡張 ACL は、(S,G) ステートがインターフェイスへの制限から除外されるように定義するのに使用できます。拡張 ACL は、拡張アクセス リストを構成する許可文または拒否文の中でソースアドレスとソースワイルドカードに 0.0.0.0 を指定することにより ((0, G) とみなされます) インターフェイスへの制限から除外される (*, G) ステートを定義するのにも使用できます。
- デバイスごとに 1 つのグローバル制限と、インターフェイスごとに 1 つの制限を設定できます。

IGMP ステートリミッタのメカニズム

IGMP ステートリミッタのメカニズムは、次のとおりです。

- ルータが特定のグループまたはチャンネルに関する IGMP メンバーシップレポートを受信するたびに、Cisco IOS ソフトウェアは、グローバル IGMP ステートリミッタまたはインターフェイスごとの IGMP ステートリミッタが制限に達したかどうかを確認します。
- グローバル IGMP ステートリミッタだけが設定されていて、その制限に達していない場合は、IGMP メンバーシップレポートは受け入れられます。設定されている制限に達した場

合は、以降の IGMP メンバーシップ レポートは無視され（ドロップされ）、次のいずれかの形式の警告メッセージが生成されます。

- ```
%IGMP-6-IGMP_GROUP_LIMIT: IGMP limit exceeded for <group (*, group address)> on
<interface type number> by host <ip address>
```
  - ```
%IGMP-6-IGMP_CHANNEL_LIMIT: IGMP limit exceeded for <channel (source address,
group address)> on <interface type number> by host <ip address>
```
- インターフェイスごとの IGMP ステートリミッタだけに達した場合、各制限はそれが設定されているインターフェイスに対してだけカウントされます。
 - グローバル IGMP ステートリミッタとインターフェイスごとの IGMP ステートリミッタの両方が設定されている場合、インターフェイスごとの IGMP ステートリミッタに設定されている制限も実施されますが、グローバル制限により制約されます。

IGMP ステート制限の設定方法

ここでは、IGMP ステート制限を設定する方法について説明します。

IGMP ステート リミッタの設定

IGMP ステートリミッタは、IGMP、IGMP v3lite、および URD メンバーシップ レポートから生じる route ステートの数に、グローバルにかまたはインターフェイスごとに制限をかけます。

グローバルな IGMP ステート リミッタの設定

デバイスごとに1つのグローバルな IGMP ステートリミッタを設定するには、次の任意作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	ip igmp limit <i>number</i> 例： Device(config)# ip igmp limit 150	IGMP メンバーシップ レポート (IGMP 加入) から生じる mroute ステートの数に対するグローバルな制限を設定します。
ステップ 4	end 例： Device(config-if)# end	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 5	show ip igmp groups 例： Device# show ip igmp groups	(任意) デバイスに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャスト グループを表示します。

インターフェイスごとの IGMP ステート リミッタの設定

インターフェイスごとの IGMP ステート リミッタを設定するには、次の任意作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface <i>type number</i> 例： Device(config)# interface GigabitEthernet 1/0/0	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。 <ul style="list-style-type: none"> ホストに接続されているインターフェイスを指定します。
ステップ 4	ip igmp limit <i>number</i> [except <i>access-list</i>] 例： Device(config-if)# ip igmp limit 100	IGMP メンバーシップ レポート (IGMP 加入) の結果として作成される mroute ステートの数に対するインターフェイスごとの制限を設定します。

	コマンドまたはアクション	目的
ステップ 5	次のいずれかを実行します。 <ul style="list-style-type: none"> • exit • end 例 : <pre>Device(config-if)# exit Device(config-if)# end</pre>	<ul style="list-style-type: none"> • (任意) 現在のコンフィギュレーションセッションを終了して、グローバルコンフィギュレーションモードに戻ります。別のインターフェイスでインターフェイスごとのリミッタを設定するには、ステップ 3 および 4 を繰り返します。 • 現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 6	show ip igmp interface [type number] 例 : <pre>Device# show ip igmp interface</pre>	(任意) インターフェイス上の IGMP のステータスと設定およびマルチキャストルーティングに関する情報を表示します。
ステップ 7	show ip igmp groups 例 : <pre>Device# show ip igmp groups</pre>	(任意) デバイスに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャストグループを表示します。

IGMP ステート制限の設定例

ここでは、IGMP ステート制限の設定例を紹介します。

IGMP ステート リミッタの設定例

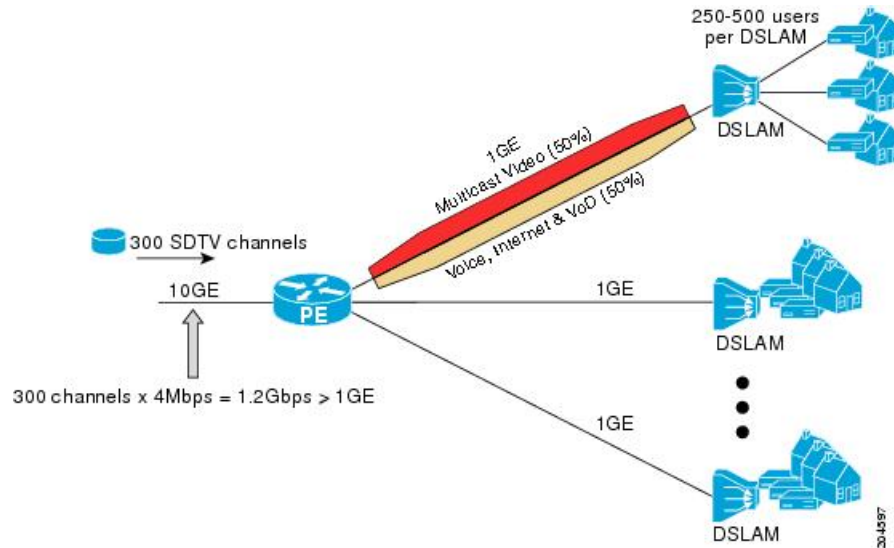
次の例は、すべてのマルチキャストフローがほぼ同量の帯域幅を使用するネットワーク環境でマルチキャスト CAC を提供するために、IGMP ステートリミッタを設定する方法を示します。

この例では、図に示すトポロジを使用します。



(注) 次の図および例では設定内のルータを使用していますが、任意のデバイス（ルータやスイッチ）を使用できます。

図 22: IGMP ステート制限のサンプル トポロジ



この例では、サービスプロバイダーは、300の標準画質（SD）TVチャンネルを提供しています。各SDチャンネルが、約4Mbpsを使用します。

このサービスプロバイダーは、デジタル加入者回線アクセスマルチプレクサ（DSLAM）に接続されているPEルータ上のギガビットイーサネットインターフェイスを、リンクの帯域幅の50%（500Mbps）をインターネット、音声、およびビデオオンデマンド（VoD）サービス提供の加入者が利用できるようにしたうえで、リンクの帯域幅の残りの50%（500Mbps）はSDチャンネル提供の加入者が利用できるようにプロビジョニングしなければなりません。

各SDチャンネルが同量の帯域幅（4Mbps）を使用するため、このサービスプロバイダーが提供するサービスのプロビジョニングに必要なCACは、インターフェイスごとのIGMPステートリミッタを使用して提供できます。インターフェイスごとに必要な必須CACを調べるために、チャンネルの総数を4で割ります（各チャンネルが4Mbpsの帯域幅を使用するため）。したがって、インターフェイスごとに必要な必須CACは、次のようになります。

$$500\text{Mbps} / 4\text{Mbps} = 125 \text{ mroute}$$

必須CACがわかったら、サービスプロバイダーは、その結果を使用して、PEルータ上でギガビットイーサネットインターフェイスをプロビジョニングするのに必要なIGMPごとのステートリミッタを設定します。このサービスプロバイダーは、ネットワークのCAC要件に基づいて、ギガビットイーサネットインターフェイスから外部へ転送できるSDチャンネルを（常時）125に制限しなければなりません。SDチャンネルのプロビジョンのためのインターフェイスごとのIGMPステート制限を125に設定すると、リンクの帯域幅の50%は常にSDチャンネルの提供に確保しなければならない（しかし使用が50%を超えてはならない）500Mbpsの帯域幅にインターフェイスをプロビジョニングできます。

次の設定は、サービスプロバイダーがインターフェイスごとのmrouteステートリミッタを使用して、加入者に提供するSDチャンネルとインターネット、音声、およびVoDサービス用にインターフェイスギガビットイーサネット0/0/0をプロビジョニングする方法を示します。

```
interface GigabitEthernet0/0/0
```

```
description --- Interface towards the DSLAM ---  
.  
.  
ip igmp limit 125
```

その他の参考資料

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャストルーティングのコマンド」の項を参照してください。 <i>Command Reference (Catalyst 9200 Series Switches)</i>

IP マルチキャストの最適化の機能履歴 : IGMP ステート制限

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	IP マルチキャストの最適化 : IGMP ステート制限	IGMP ステート制限機能を使用すると、IGMP ステートリミッタの設定が可能になり、この設定により、IGMP メンバーシップレポート (IGMP 加入) により生成される mroute ステートの数がグローバルに、またはインターフェイスごとに制限されます。設定されている制限を超えたメンバーシップレポートは、IGMP キャッシュに入れられません。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfngn.cisco.com/> にアクセスします。

翻訳について

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