



H3C S5560X-EI スイッチシリーズ

IPマルチキャストコンフィギュレーションガイド

新h3cテクノロジー株式会社<http://www.h3c.com>

ソフトウェアバージョン:Release 1118、Release
1118P07ドキュメントバージョン:6W101-20180821

無断複写・転載を禁ず

本取扱説明書の内容の一部または全部を無断転載することは禁止されています。

商標について

H3C、**H3C**、H3CS、H3CIE、H3CNE、Aolynk、、H3Care、、IRF、NetPilot、Netflow、SecEngine、SecPath、SecCenter、SecBlade、Comware、ITCMM および HUASAN は、New H3C Technologies Co.,Ltd.の商標です。

このマニュアルに記載されているその他すべての商標は、それぞれの所有者の所有物です。

注意事項

このドキュメントの情報は、予告なしに変更されることがあります。記述、情報、および推奨事項を含むこのドキュメントのすべての内容は正確であると考えられますが、それらは明示的または黙示的を問わず、いかなる種類の保証もなしに提示されます。H3Cは、ここに含まれる技術的または編集上の誤りまたは脱落に対して責任を負わないものとします。

はじめに

このコンフィギュレーションガイドでは、IPマルチキャストの基礎と設定手順について説明します。IPv4マルチキャスト設定とIPv6マルチキャスト設定についても説明します。マルチキャストを使用すると、効率的なポイントツーマルチポイントデータ伝送をネットワークに実装できます。

ここでは、マニュアルに関する次の内容について説明します。

- 対象読者
- 表記規則
- マニュアルに関するフィードバック

対象読者

本書の対象読者は、次のとおりです。

- ネットワークプランナー。
- フィールドテクニカルサポートおよびサービスエンジニア。
- L3スイッチシリーズでマルチキャストを使用するネットワーク管理者。

表記規則

ここでは、マニュアルで使用されている表記規則について説明します。

コマンドの表記法

表記法	説明
太字	太字は、記載されているとおりに入力したコマンドおよびキーワードを表します。
イタリック	イタリックのテキストは、実際の値に置き換える引数を表します。
()	省略可能な構文の選択肢(キーワードまたは引数)は、角カッコで囲みます。
{ x y ... }	波カッコで囲まれた一連の必須構文を縦棒で区切って、その中から1つを選択します。
[x y ...]	角カッコは、縦棒で区切られたオプションの構文の選択肢のセットを囲み、その中から1つまたは何も選択しません。
x y ... } *	アスタリスクの付いた中カッコは、必要な構文の選択肢のセットを縦棒で囲んだもので、その中から最低1つを選択します。
[x y ...] *	角カッコで囲まれたアスタリスクは、省略可能な構文の選択肢を縦棒で区切ったものです。この中から、1つの選択肢を選択するか、複数の選択肢を選択するか、または何も選択しません。
&<1-n>	アンパサンド(&)記号の前の引数またはキーワードと引数の組み合わせは、1～n回入力できます。
#	シャープ記号(#)で始まる行はコメントです。

GUIの表記法

表記法	説明
太字	ウィンドウ名、ボタン名、フィールド名およびメニュー項目は太字で表示されます。たとえば、 New User ウィンドウがオープンしたら、 OK をクリックします。
>	複数レベルのメニューは、 File > Create > Folder のように、山括弧で区切られています。

記号

表記法	説明
 警告:	けがの原因となる重要な情報への注意を促す警告。
 注意:	データの消失、データの破損、ハードウェアまたはソフトウェアの損傷を引き起こす可能性のある重要な情報への注意を喚起する警告。
 重要:	重要な情報への注意を促す警告。
注:	追加情報または補足情報を含むアラート。
 ヒント:	有用な情報を提供する警告。

ネットワークポロジのアイコン

表記法	説明
	ルータ、スイッチ、ファイアウォールなどの汎用ネットワークデバイスを表します。
	ルータやレイヤ3スイッチなどのルーティング対応デバイスを表します。
	レイヤ2スイッチやレイヤ3スイッチなどの汎用スイッチ、またはレイヤ2フォワーディングやその他のレイヤ2機能をサポートするルータを表します。
	アクセスコントローラ、統合有線WLANモジュール、または統合有線WLANスイッチ上のアクセスコントローラエンジンを表します。
	アクセスポイントを表します。
	無線ターミネータユニットを表します。
	無線ターミネータを表します。
	メッシュアクセスポイントを表します。
	全方向性信号を表します。

	方向信号を表します。
	ファイアウォール、UTM、マルチサービスセキュリティゲートウェイ、ロードバランシングデバイスなどのセキュリティ製品を表します。
	ファイアウォール、ロードバランシング、NetStream、SSL VPN、IPS、ACGモジュールなどのセキュリティモジュールを表します。

本書で提供される例

このドキュメントの例では、ご使用のデバイスとハードウェアモデル、設定、またはソフトウェアバージョンが異なるデバイスが使用されている場合があります。通常、例のポート番号、出力例、スクリーンショット、およびその他の情報は、ご使用のデバイスのものとは異なります。

マニュアルに関するフィードバック

製品ドキュメントに関するご意見は、info@h3c.comまで電子メールでお寄せください。ご意見に感謝いたします。

内容

マルチキャストの概要	15
マルチキャストの概要	15
情報伝達技術	15
マルチキャスト機能	17
マルチキャストの利点と用途	18
マルチキャストモデル	18
ASMモデル	19
SFMモデル	19
SSMモデル	19
マルチキャストアドレス	19
IPマルチキャストアドレス	19
EthernetマルチキャストMACアドレス	23
マルチキャストプロトコル	24
レイヤ3マルチキャストプロトコル	24
レイヤ2マルチキャストプロトコル	26
マルチキャストパケット転送メカニズム	27
IPマルチキャストアーキテクチャ	27
マルチキャストにおける共通の表記法	28
IGMPスヌーピングの設定	29
IGMPスヌーピングの概要	29
IGMPスヌーピングの基礎	29
GMPスヌーピングポート	30
IGMPスヌーピングの動作	31
IGMPスヌーピングプロキシ	34
プロトコルと標準	35
制約事項および注意事項:IGMPスヌーピング設定	35
VLANベースのIGMPスヌーピングタスクの概要	36
VSIベースのIGMPスヌーピングタスクの概要	37
IGMPスヌーピング機能の有効化	38
IGMPスヌーピングの有効化	38
IGMPスヌーピングのグローバルな有効化	38
VLANのIGMPスヌーピングの有効化	40
VSIのIGMPスヌーピングの有効化	40
基本的なIGMPスヌーピング機能の設定	41
IGMPスヌーピングバージョンの指定	41
IGMPスヌーピングフォワーディングエントリの最大数の設定	42
スタティックマルチキャストMACアドレスエントリの設定	42
IGMP最終メンバークエリーインターバルの設定	43
IGMPスヌーピングポート機能の設定	44
ダイナミックポートのエージングタイマーの設定	44
スタティックメンバーポートの設定	46
スタティックルータポートの設定	46
シミュレートメンバーホストとしてのポートの構成	47
高速脱退処理の有効化	47
ポートがダイナミックルータポートになることを無効にする	48
IGMPスヌーピングクエリーアの設定	50
IGMPスヌーピングクエリーアの有効化	50
IGMPスヌーピングクエリーア選定の有効化	51
IGMP一般クエリーおよび応答のパラメータの設定	52
IGMPスヌーピングプロキシの有効化	54
IGMPメッセージのパラメータの設定	54
IGMPメッセージの送信元IPアドレスの設定	54
IGMPメッセージの802.1pプライオリティの設定	57

IGMPスヌーピングポリシーの設定	57
マルチキャストグループポリシーの設定	57
マルチキャスト送信元ポートフィルタリングの有効化	58
不明なマルチキャストデータの破棄の有効化	59
IGMPレポート抑制の有効化	60
ポート上のマルチキャストグループの最大数の設定	60
マルチキャストグループ置換の有効化	62
ホストトラッキングの有効化	62
発信IGMPスヌーピングプロトコルパケットのDSCP値の設定	63
IGMPスヌーピングの表示およびメンテナンスコマンド	64
IGMPスヌーピングの設定例	66
例:VLANベースのIGMPスヌーピンググループポリシーおよびシミュレートされた加入の設定	66
例:VLANベースのIGMPスヌーピングスタティックポートの設定	68
例:VLANベースのIGMPスヌーピングクエリーの設定	71
例:VLANベースのIGMPスヌーピングプロキシの設定	74
例:VXLANベースのIGMPスヌーピングの設定	76
IGMPスヌーピングのトラブルシューティング	82
レイヤ2マルチキャストフォワーディングが機能しない	82
マルチキャストグループポリシーが機能しない	82
PIMスヌーピングの設定	83
PIMスヌーピングの概要	83
制約事項および注意事項:PIMスヌーピング設定	84
PIMスヌーピングタスクの概要	85
PIMスヌーピングの有効化	85
マスター/下位スイッチオーバー後のグローバルポートのエージングタイムの設定	86
グローバルポートについて	86
グローバルネイバーポートのエージングタイムの設定	86
グローバルダウンストリームポートおよびグローバルルータポートのエージングタイムの設定	87
PIMスヌーピングの表示およびメンテナンスコマンド	87
PIMスヌーピングの設定例	88
例:PIMスヌーピングの設定	88
PIMスヌーピングのトラブルシューティング	91
PIMスヌーピングがレイヤ2デバイスで動作しない	91
マルチキャストVLANの設定	92
マルチキャストVLAN機能	92
マルチキャストVLAN方式	92
サブVLANベースのマルチキャストVLAN	92
ポートベースのマルチキャストVLAN	93
制約事項および注意事項:マルチキャストVLANの設定	94
サブVLANベースのマルチキャストVLANの設定	94
ポートベースマルチキャストVLANの設定	95
マルチキャストVLANフォワーディングエントリの最大数の設定	97
マルチキャストVLANの表示およびメンテナンスコマンド	97
マルチキャストVLANの設定例	98
例:サブVLANベースのマルチキャストVLANの設定	98
例:ポートベースのマルチキャストVLANの設定	101
マルチキャストルーティングおよびフォワーディングの設定	105
マルチキャストルーティングおよびフォワーディングについて	105
RPFチェックメカニズム	105
スタティックマルチキャストルートの使用	107
ユニキャストサブネット間のマルチキャスト転送	109
Mtrace	110
制約事項および注意事項: マルチキャストルーティングおよび転送の設定	111
マルチキャストルーティングおよび転送タスクの概要	112
マルチキャストルーティングおよび転送の前提条件	112

IPマルチキャストルーティングの有効化	112
スタティックマルチキャストルートの設定	112
最長プレフィクス一致原則の指定	113
マルチキャストロードスプリットの設定	113
マルチキャストフォワーディング境界の設定	115
スーパーVLANのサブVLAN間のマルチキャストフォワーディングの有効化	115
mtraceを使用してマルチキャストパスをトレースする	116
mtrace1を使用してマルチキャストパスをトレースする	116
mtrace2を使用してマルチキャストパスをトレースする	116
マルチキャストルーティングおよびフォワーディング用の表示およびメンテナンスコマンド	117
マルチキャストルーティングおよびフォワーディングの設定例	119
例:RPFルートの変更	119
例:RPFルートの作成	121
マルチキャストルーティングおよびフォワーディングのトラブルシューティング	124
スタティックマルチキャストルートの障害	124
IGMPの設定	125
IGMPの概要	125
IGMPのバージョン	125
IGMPv1の概要	125
IGMPv2の機能拡張	127
IGMPv3の機能拡張	128
IGMP SSMマッピング	130
IGMPプロキシ	131
プロトコルと標準	132
IGMPタスクの概要	132
IGMPの前提条件	132
IGMPの有効化	132
基本的なIGMP機能の設定	134
IGMPバージョンの指定	134
スタティックグループメンバーの設定	134
マルチキャストグループポリシーの設定	135
IGMPパフォーマンスの調整	136
IGMPクエリーおよび応答パラメータの設定	136
高速脱退処理の有効化	139
IGMP SSMマッピングの設定	139
IGMPプロキシの設定	140
IGMPプロキシ設定の前提条件	140
IGMPプロキシの有効化	140
非クエリーアインターフェイス上のマルチキャストフォワーディングの有効化	140
IGMPプロキシインターフェイスのマルチキャストロードスプリットの設定	141
IGMP NSRの有効化	142
発信IGMPプロトコルパケットのDSCP値の設定	142
IGMPの表示およびメンテナンスコマンド	142
IGMPの設定例	144
例:基本的なIGMP機能の設定	144
例:IGMP SSMマッピングの設定	146
例:IGMPプロキシの設定	150
IGMPのトラブルシューティング	151
受信側機器にメンバーシップ情報が無い	151
同一サブネット上のデバイスの一貫性のないメンバーシップ情報	152
PIMの設定	153
PIMの概要	153
PIMモード	153
PIM-DM	153
PIM-SM	156
管理者の権限適用範囲	163

PIM-SSM	165
プロトコルと標準	166
制約事項および注意事項:PIMの設定	167
PIM-DMの設定	168
PIM-DMタスクの概要	168
PIM-DMの前提条件	168
PIM-DMの有効化	168
状態更新機能の構成	170
PIM-DMグラフトリタイマーの設定	171
PIM-SMの設定	171
PIM-SMタスクの概要	171
PIM-SMの前提条件	173
PIM-SMの有効化	173
スタティックRPの設定	173
C-RPの設定	174
C-BSRの設定	175
PIMドメイン境界の設定	175
BSMセマンティックフラグメンテーションの無効化	176
デバイスが着信インターフェイスからBSMを転送できないようにする	177
Auto-RPリスニングの有効化	177
エニーキャストRPの設定	177
マルチキャスト送信元登録の設定	178
SPTへのスイッチオーバーの設定	180
PIM-SSMの設定	180
PIM-SSMタスクの概要	180
PIM-SSMの前提条件	180
PIM-SMの有効化	180
SSMグループ範囲の設定	181
一般的なPIM機能の設定	182
一般的なPIM機能のタスクの概要	182
マルチキャスト送信元ポリシーの設定	182
PIMハローポリシーの設定	183
PIMハローメッセージオプションの設定	183
Generation IDオプションを使用しないhelloメッセージのドロップ	185
一般的なPIMタイマーの設定	186
ジョインまたはプルーンメッセージの最大サイズの設定	187
発信PIMプロトコルパケットのDSCP値の設定	188
PIMのBFDの有効化	188
PIMパッシブモードの有効化	189
PIM NSRの有効化	189
PIMのSNMP通知の有効化	190
PIMの表示およびメンテナンスコマンド	191
PIMの設定例	192
例:PIM-DMの設定	192
例:非スコープPIM-SMの設定	195
例:管理スコープPIM-SMの設定	199
例:PIM-SSMの設定	204
PIMのトラブルシューティング	207
マルチキャスト配信ツリーを正しく構築できない	207
マルチキャストデータが中間デバイスで異常終了する	208
RPがPIM-SMのSPTに加入できない	208
PIM-SMでRPTを構築できない、またはマルチキャスト送信元登録が失敗する	209
MSDPの設定	209
MSDPの概要	209
MSDPの機能	209
MSDPを介したエニーキャストRP	214

プロトコルと標準	215
MSDPタスクの概要	215
MSDPの前提条件	215
MSDPの有効化	216
MSDPピアの作成	216
スタティックRPFピアの設定	217
MSDPメッシュグループの設定	218
MSDPピアリング接続の制御	218
MSDPピアリング接続の終了	218
MSDPセッションのキープアライブタイマーおよびピアホールドタイマーの設定	219
MSDP接続リトライ間隔の設定	219
TCP接続確立のためのMD5認証の有効化	220
SAメッセージ関連パラメータの設定	221
SAメッセージでのマルチキャストデータカプセル化の有効化	221
SAメッセージの発信元RPの設定	221
SA要求メッセージの設定	222
SAメッセージポリシーの設定	222
SAキャッシュメカニズムの設定	223
MSDPベースのエニーキャストRPの設定	225
MSDP NSRの有効化	225
発信MSDPプロトコルパケットのDSCP値の設定	225
MSDPの表示およびメンテナンスコマンド	226
MSDPの設定例	227
例:PIM-SMDメイン間マルチキャストの設定	227
例:スタティックRPFピアを利用したAS間マルチキャストの設定	232
例:エニーキャストRPの設定	237
例:SAメッセージフィルタリングの設定	241
MSDPのトラブルシューティング	244
MSDPピアが無効ステートのままになる	244
デバイスのSAメッセージキャッシュにSAエントリが存在しない	245
RP間でローカルに登録された(S, G)エントリの交換なし	245
MLDスヌーピングの設定	246
MLDスヌーピングの概要	246
MLDスヌーピングの基礎	246
MLDスヌーピングポート	246
MLDスヌーピングの動作	248
MLDスヌーピングプロキシ	250
プロトコルと標準	251
制約事項および注意事項:MLDスヌーピング設定	251
VLANベースのMLDスヌーピングタスクの概要	252
VSIベースのMLDスヌーピングタスクの概要	253
MLDスヌーピング機能の有効化	254
MLDスヌーピングの有効化	254
MLDスヌーピングのグローバルな有効化	254
VLANのMLDスヌーピングの有効化	255
VSIのMLDスヌーピングの有効化	255
基本的なMLDスヌーピング機能の設定	256
MLDスヌーピングバージョンの指定	256
MLDスヌーピングフォワーディングエントリの最大数の設定	257
スタティックIPv6マルチキャストMACアドレスエントリの設定	257
MLD最終リスナー クエリー インターバルの設定	258
MLDスヌーピングポート機能の設定	259
ダイナミックポートのエージングタイマーの設定	259
スタティックメンバーポートの設定	261
スタティックルータポートの設定	261
シミュレートメンバーホストとしてのポートの構成	262

高速脱退処理の有効化	262
ポートがダイナミックルータポートになることを無効にする	263
MLDスヌーピングクエリアの設定	264
MLDスヌーピングクエリアの有効化	264
MLDスヌーピングクエリア選択の有効化	265
MLD一般クエリおよび応答のパラメータの設定	266
MLDスヌーピングプロキシの有効化	267
MLDメッセージのパラメータの設定	267
MLDメッセージの送信元IPv6アドレスの設定	267
MLDメッセージの802.1pプライオリティの設定	269
MLDスヌーピングポリシーの設定	270
IPv6マルチキャストグループポリシーの設定	270
IPv6マルチキャスト送信元ポートフィルタリングの有効化	272
不明なIPv6マルチキャストデータの破棄の有効化	272
MLDレポート抑制の有効化	273
ポート上の最大IPv6マルチキャストグループ数の設定	274
IPv6マルチキャストグループ置換の有効化	274
ホストトラッキングの有効化	275
発信MLDスヌーピングプロトコルパケットのDSCP値の設定	276
MLDスヌーピングの表示およびメンテナンスコマンド	276
MLDスヌーピングの設定例	279
例:VLANベースIPv6グループポリシーおよびシミュレートされた加入の設定	279
例:VLANベースのスタティックポートの設定	281
例:VLANベースMLDスヌーピングクエリアの設定	284
例:VLANベースのMLDスヌーピングプロキシの設定	286
例:VXLANベースのMLDスヌーピングの設定	289
MLDスヌーピングのトラブルシューティング	294
レイヤ2マルチキャストフォワーディングが機能しない	294
IPv6マルチキャストグループポリシーが機能しない	294
IPv6 PIMスヌーピングの設定	295
IPv6 PIMスヌーピングの概要	295
制約事項および注意事項:IPv6 PIMスヌーピング設定	296
IPv6 PIMスヌーピングタスクの概要	297
IPv6 PIMスヌーピングの有効化	297
マスター/下位スイッチオーバー後のグローバルポートのエージングタイムの設定	298
グローバルポートについて	298
グローバルネイバーポートのエージングタイムの設定	298
グローバルダウンストリームポートおよびグローバルルータポートのエージングタイムの設定	299
IPv6 PIMスヌーピングの表示およびメンテナンスコマンド	299
IPv6 PIMスヌーピングの設定例	300
例:IPv6 PIMスヌーピングの設定	300
IPv6 PIMスヌーピングのトラブルシューティング	303
IPv6 PIMスヌーピングがレイヤ2デバイスで動作しない	303
IPv6マルチキャストVLANの設定	304
IPv6マルチキャストVLAN機能	304
IPv6マルチキャストVLAN方式	304
サブVLANベースのIPv6マルチキャストVLAN	304
ポートベースのIPv6マルチキャストVLAN	305
制約事項および注意事項:IPv6マルチキャストVLAN設定	306
サブVLANベースのIPv6マルチキャストVLANの設定	307
ポートベースIPv6マルチキャストVLANの設定	308
IPv6マルチキャストVLANフォワーディングエントリの最大数の設定	309
IPv6マルチキャストVLANの表示およびメンテナンスコマンド	309
IPv6マルチキャストVLANの設定例	311
例:サブVLANベースのIPv6マルチキャストVLANの設定	311
例:ポートベースIPv6マルチキャストVLANの設定	314

IPv6マルチキャストルーティングおよびフォワーディングの設定	317
IPv6マルチキャストルーティングおよび転送について	317
RPFチェックメカニズム	317
IPv6ユニキャストサブネット間のIPv6マルチキャスト転送	320
IPv6のmtrace	320
IPv6マルチキャストルーティングおよび転送タスクの概要	321
IPv6マルチキャストルーティングおよび転送の前提条件	321
IPv6マルチキャストルーティングの有効化	321
最長プレフィクス一致原則の指定	322
IPv6マルチキャストロードスプリットの設定	322
IPv6マルチキャストフォワーディング境界の設定	322
スーパーVLANのサブVLAN間のIPv6マルチキャストフォワーディングの有効化	323
mtrace2を使用したIPv6マルチキャストパスのトレース	324
IPv6マルチキャストルーティングおよびフォワーディングの表示およびメンテナンスコマンド	325
MLDの設定	327
MLDの概要	327
MLDバージョン	327
MLDv1の機能	327
MLDv2拡張機能	329
MLD SSMマッピング	330
MLDプロキシ	332
プロトコルと標準	333
MLDタスクの概要	333
MLDの前提条件	333
MLDの有効化	333
基本的なMLD機能の設定	335
MLDバージョンの指定	335
スタティックグループメンバーの設定	335
IPv6マルチキャストグループポリシーの設定	336
MLDパフォーマンスの調整	336
MLDクエリーおよび応答パラメータの設定	336
高速脱退処理の有効化	339
MLD SSMマッピングの設定	340
MLDプロキシの設定	340
MLDプロキシの前提条件	340
MLDプロキシの有効化	340
非クエリーインターフェイス上のIPv6マルチキャストフォワーディングの有効化	341
MLDプロキシインターフェイスのIPv6マルチキャストロードスプリットの有効化	341
MLD NSRの有効化	342
発信MLDプロトコルパケットのDSCP値の設定	342
MLDの表示およびメンテナンスコマンド	343
MLDの設定例	344
例:基本的なMLD機能の設定	344
例:MLD SSMマッピングの設定	346
例:MLDプロキシの設定	349
MLDのトラブルシューティング	350
受信側の機器にメンバー情報が存在しない	350
同一サブネット上のデバイスの一貫性のないメンバーシップ情報	352
IPv6 PIMの設定	353
IPv6 PIMの概要	353
IPv6 PIMモード	353
IPv6 PIM-DM	353
IPv6 PIM-SM	356
IPv6管理スコープ	363
IPv6 PIM-SSM	365
プロトコルと標準	367

制約事項および注意事項:IPv6 PIMの設定	367
IPv6 PIM-DMの設定	367
IPv6 PIM-DMタスクの概要	367
IPv6 PIM-DMの前提条件	367
IPv6 PIM-DMの有効化	367
状態更新機能の構成	368
IPv6 PIM-DMグラフトリタイマーの設定	369
IPv6 PIM-SMの設定	370
IPv6 PIM-SMタスクの概要	370
IPv6 PIM-SMの前提条件	370
IPv6 PIM-SMの有効化	370
スタティックRPの設定	371
C-RPの設定	372
C-BSRの設定	373
IPv6 PIMドメイン境界の設定	373
BSMセマンティックフラグメンテーションの無効化	374
デバイスが着信インターフェイスからBSMを転送できないようにする	374
エニーキャストRPの設定	376
IPv6マルチキャスト送信元登録の設定	376
SPTへのスイッチオーバーの設定	378
IPv6 PIM-SSMの設定	378
IPv6 PIM-SSMタスクの概要	378
IPv6 PIM-SSMの前提条件	378
IPv6 PIM-SMの有効化	379
IPv6 SSMグループ範囲の指定	379
一般的なIPv6 PIM機能の設定	380
一般的なIPv6 PIM機能のタスクの概要	380
IPv6マルチキャスト送信元ポリシーの設定	380
IPv6 PIMハローポリシーの設定	381
IPv6 PIMハローメッセージオプションの設定	381
Generation IDオプションを使用しないhelloメッセージのドロップ	383
共通IPv6 PIMタイマーの設定	384
ジョインまたはプルーンメッセージの最大サイズの設定	386
発信IPv6 PIMプロトコルパケットのDSCP値の設定	386
IPv6 PIMのBFDの有効化	386
IPv6 PIMパッシブモードの有効化	387
IPv6 PIM NSRの有効化	387
IPv6 PIMのSNMP通知の有効化	388
IPv6 PIMの表示およびメンテナンスコマンド	388
IPv6 PIMの設定例	390
例:IPv6 PIM-DMの設定	390
例:非スコープIPv6 PIM-SMの設定	394
例:管理スコープのIPv6 PIM-SMの設定	397
例:IPv6 PIM-SSMの設定	404
IPv6 PIMのトラブルシューティング	407
マルチキャスト配信ツリーを正しく構築できない	407
IPv6マルチキャストデータが中間デバイスで異常終了する	407
RPがIPv6 PIM-SMのSPTに加入できない	408
IPv6 PIM-SMでRPTを構築できない、またはIPv6マルチキャスト送信元登録が失敗する	408

マルチキャストの概要

マルチキャストの概要

マルチキャストは、ユニキャストやブロードキャストと共存する技術として、ポイントツーマルチポイントのデータ伝送に有効であり、ネットワーク上で効率的なポイントツーマルチポイントのデータ伝送を可能にすることで、ネットワーク帯域の大幅な節約とネットワーク負荷の軽減を実現します。

マルチキャスト技術を使用することにより、ネットワークオペレータは、帯域幅が重要で時間が重要な情報サービスを容易に提供することができる。これらのサービスには、ライブウェブ放送、ウェブTV、遠隔教育、遠隔医療、ウェブラジオ、およびリアルタイムビデオ会議が含まれる。

情報伝達技術

ユニキャスト

情報伝送技術には、ユニキャスト、ブロードキャスト、およびマルチキャストが含まれる。

ユニキャスト送信では、情報ソースは、情報を必要とする各ホストに情報の個別のコピーを送信する必要があります。

図1 ユニキャスト送信

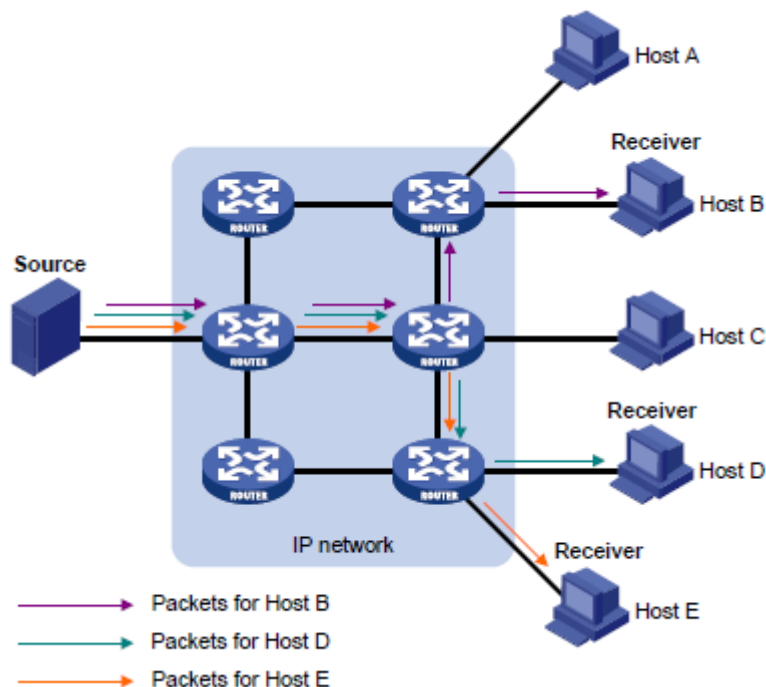


図1では、ホストB、ホストD、およびホストEが情報を必要とします。情報源からこれらの各ホストへの個別の伝送チャネルを確立する必要があります。

ユニキャスト送信では、ネットワークを介して送信されるトラフィックは、情報を必要とするホストの数に比

例します。多数のホストが情報を必要とする場合、情報ソースはこれらの各ホストに同じ情報の個別のコピーを送信する必要があります。多数のコピーを送信すると、情報ソースおよびネットワーク帯域幅に多大な負荷がかかります。

ユニキャストは、情報のバッチ送信には適していません。

ブロードキャスト

ブロードキャスト送信では、一部のホストが情報を必要としない場合でも、情報ソースはサブネット上のすべてのホストに情報を送信します。

図2 ブロードキャスト送信

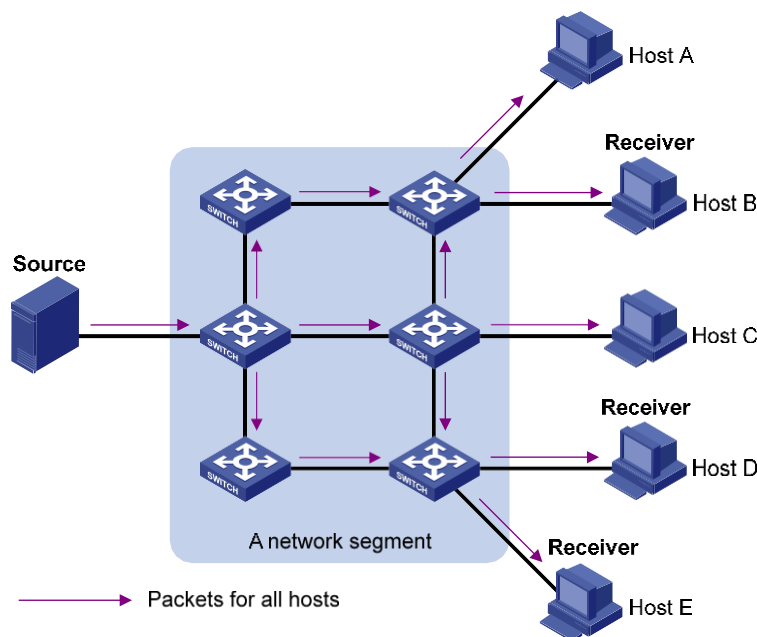


図2では、情報を必要とするのはホストB、ホストD、およびホストEだけです。情報がサブネットにブロードキャストされる場合、ホストAおよびホストCもそれを受信します。情報セキュリティの問題に加えて、情報を必要としないホストにブロードキャストすると、同じサブネット上でトラフィックのフラッディングが発生します。

ブロードキャストは、特定のホストにデータを送信する場合に不利である。さらに、ブロードキャスト送信は、ネットワークリソースの著しい浪費である。

マルチキャスト

マルチキャストは、ネットワーク消費を最小限に抑えたポイントツーマルチポイントデータ伝送を提供します。ネットワーク上の一部のホストがマルチキャスト情報を必要とする場合、情報送信者またはマルチキャスト送信元は、情報のコピーを1つだけ送信します。マルチキャスト配信ツリーは、マルチキャストルーティングプロトコルによって構築され、パケットはツリーが分岐するノードにのみ複製されます。

図3 マルチキャスト送信

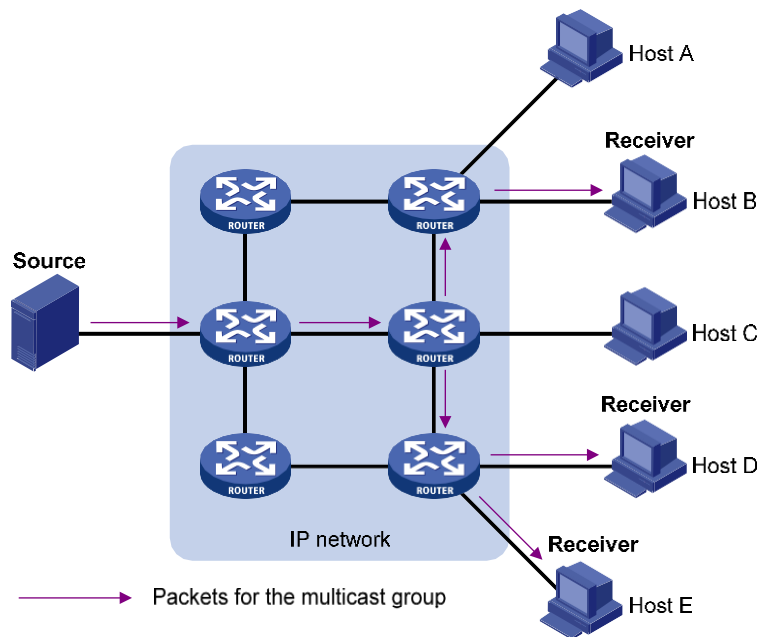


図3では、マルチキャストソースは情報の1つのコピーだけをマルチキャストグループに送信します。情報レシーバであるホストB、ホストD、およびホストEは、マルチキャストグループに参加する必要があります。ネットワーク上のルータは、グループメンバーの配信に基づいて情報を複製し、転送します。最後に、情報はホストB、ホストD、およびホストEに正しく配信されます。

要約すると、マルチキャストには次の利点があります。

- ユニキャストに対する利点マルチキャストデータは、送信元から最も遠いノードに流れるまで複製され、分散されます。受信側ホストの増加によって、送信元の負荷やネットワークリソースの使用量が大幅に増加することはありません。
- ブロードキャストに対する利点マルチキャストデータは、それを必要とする受信者にのみ送信されます。これにより、ネットワーク帯域幅が節約され、ネットワークセキュリティが強化されます。また、マルチキャストデータは同じサブネットに限定されません。

マルチキャスト機能

- マルチキャストグループは、IPマルチキャストアドレスで識別されるマルチキャスト受信者セットです。ホストがマルチキャストグループのメンバーになるには、そのマルチキャストグループにアドレス指定されたマルチキャストデータを受信する前に、マルチキャストグループに加入する必要があります。通常、マルチキャスト送信元がマルチキャストグループに加入する必要はありません。
- マルチキャストソースは情報送信者です。複数のマルチキャストグループに同時にデータを送信できます。複数のマルチキャストソースが同じマルチキャストグループに同時にデータを送信できます。

- グループメンバーシップは動的です。ホストはいつでもマルチキャストグループに参加または脱退できます。マルチキャストグループは地理的制限の対象ではありません。
- マルチキャストルータまたはレイヤ3マルチキャストデバイスは、レイヤ3マルチキャストをサポートするルータまたはレイヤ3スイッチです。マルチキャストルーティングを提供し、グループメンバーが接続されたスタブサブネット上のマルチキャストグループメンバーシップを管理します。マルチキャストルータ自体をマルチキャストグループメンバーにすることができます。

マルチキャストの概念をよりよく理解するために、マルチキャスト伝送をテレビ番組の伝送と比較することができます。

表1 TV番組伝送とマルチキャスト伝送の比較

テレビ番組送出	マルチキャスト送信
テレビ局は、チャンネルを通じてテレビ番組を放送します。	マルチキャスト送信元は、マルチキャストグループにマルチキャストデータを送信します。
ユーザーは、テレビをそのチャンネルに合わせる。	レシーバがマルチキャストグループに加入します。
ユーザーは、そのチャンネルのTV局から送信されたTV番組の視聴を開始する。	レシーバは、ソースによってマルチキャストグループに送信されたマルチキャストデータの受信を開始します。
ユーザーはテレビの電源を切るか、別のチャンネルに合わせます。	受信者は、マルチキャストグループから脱退するか、別のグループに参加します。

マルチキャストの利点と用途

マルチキャストの利点

- 情報発信元サーバやネットワーク機器のプロセッサ負荷を軽減します。
- 最適なパフォーマンス冗長トラフィックを削減します。
- 分散アプリケーション:最小限のネットワークリソースのコストでポイントツーマルチポイントアプリケーションを有効にします。

マルチキャストアプリケーション

- Web TV、Webラジオ、リアルタイムのビデオ/音声会議などのマルチメディアおよびストリーミングアプリケーション
- 遠隔教育や遠隔医療などの訓練や協力活動のためのコミュニケーション
- データウェアハウスおよび財務アプリケーション(株価情報)
- データ配信用のその他のポイントツーマルチポイントアプリケーション

マルチキャストモデル

受信者がマルチキャストソースを処理する方法に基づいて、マルチキャストモデルには、Any-Source

Multicast(ASM)、Source-Filtered Multicast(SFM)、およびSource-Specific Multicast(SSM)が含まれます。

ASMモデル

ASMモデルでは、任意のマルチキャストソースがマルチキャストグループに情報を送信できます。受信者は、マルチキャストグループに参加し、そのマルチキャストグループにアドレス指定されたマルチキャスト情報を任意のマルチキャストソースから取得できます。このモデルでは、受信者はマルチキャストソースの位置を事前に認識しません。

SFMモデル

SFMモデルはASMモデルから派生したものである。マルチキャストソースにとって、2つのモデルは同じマルチキャストメンバーシップアーキテクチャを持つように見える。

SFMモデルは、ASMモデルを機能的に拡張したものである。上位層のソフトウェアは、受信したマルチキャストパケットの送信元アドレスをチェックし、特定の送信元からのマルチキャストトラフィックを許可または拒否します。レシーバは、マルチキャストソースの一部だけからマルチキャストデータを取得します。レシーバにとって、マルチキャストソースはすべて有効ではありませんが、フィルタリングされます。

SSMモデル

SSMモデルは、マルチキャストレシーバが関与するマルチキャストソースを指定できるようにする送信サービスを提供します。

SSMモデルでは、レシーバはすでにマルチキャストソースの場所を決定しています。これがSSMモデルとASMモデルの主な違いです。さらに、SSMモデルはASM/SFMモデルとは異なるマルチキャストアドレス範囲を使用します。レシーバと指定されたマルチキャストソースの間には、専用のマルチキャスト転送パスが確立されます。

マルチキャストアドレス

IPマルチキャストアドレス

IPv4マルチキャストアドレス

IANAはIPv4マルチキャストにクラスDアドレスブロック(224.0.0.0から239.255.255.255)を割り当てました。

表2 クラスDのIPアドレスブロックおよび説明

アドレスブロック	説明
224.0.0.0から224.0.0.255	予約された永続的なグループアドレス。IPアドレス224.0.0.0は予約されています。他のIPアドレスは、ルーティングプロトコルやトポロジ検索、プロトコルメンテナンスなどに使用できます。 表3に、一般的な永続グループアドレスを示します。このブロック内のアドレス宛てのパケットは、IPヘッダー内のTTL値に関係なく、ローカルサブネットを越えて転送されることはありません。
224.0.1.0から238.255.255.255	グローバルにスコープされたグループアドレス。このブロックには、次のタイプの指定グループアドレスが含まれます。 ● 232.0.0.0/8: SSMグループアドレス。 ● 233.0.0.0/8: Glopグループアドレス。
239.0.0.0から239.255.255.255	管理用スコープのマルチキャストアドレス。これらのアドレスは、グローバルに一意ではなく、ローカルに一意であると見なされます。異なる組織によって管理されているドメイン内で、競合を引き起こすことなく再利用できます。詳細については、RFC 2365を参照してください。

注:

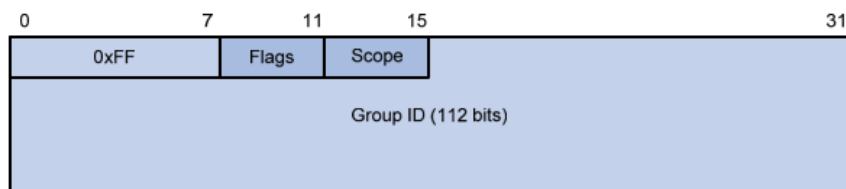
Glopは、異なるAS間でマルチキャストアドレスを割り当てるためのメカニズムです。233.0.0.0の中央の2バイトにAS番号を入力すると、そのASに255のマルチキャストアドレスが割り当てられます。詳細については、RFC 2770を参照してください。

表3共通パーマネントマルチキャストグループアドレス

アドレス	説明
224.0.0.1	ホストおよびルータを含む、このサブネット上のすべてのシステム。
224.0.0.2	このサブネット上のすべてのマルチキャストルータ。
224.0.0.3	未割り当て。
224.0.0.4	DVMRPルータ。
224.0.0.5	OSPFルータ。
224.0.0.6	OSPF代表ルータおよびバックアップ代表ルータ。
224.0.0.7	Shared Tree(ST)ルータ。
224.0.0.8	STホスト。
224.0.0.9	RIPv2ルータ。
224.0.0.11	モバイルエージェント。
224.0.0.12	DHCPサーバリレーエージェント。
224.0.0.13	すべてのProtocol Independent Multicast(PIM)ルータ。
224.0.0.14	RSVPカプセル化。
224.0.0.15	すべてのCore-Based Tree(CBT)ルータ。
224.0.0.16	指定SBM。
224.0.0.17	全てのSBM
224.0.0.18	VRRP

IPv6マルチキャストアドレス

図4 IPv6マルチキャスト形式



次に、IPv6マルチキャストアドレスのフィールドについて説明します。

- **0 xFF**-上位8ビットは11111111です。
- **Flags**-Flagsフィールドには4ビットが含まれます。

図5 Flagsフィールドの形式



表4 Flagsフィールドの説明

ビット	説明
0	予約済み。0に設定されます。
R	0に設定すると、このアドレスはRPアドレスが埋め込まれていないIPv6マルチキャストアドレスになります。 1に設定されている場合、このアドレスはRPアドレスが埋め込まれたIPv6マルチキャストアドレスです(PおよびTビットも1に設定する必要があります)。
P	0に設定される時、このアドレスはユニキャストプレフィックスに基づかないIPv6マルチキャストアドレスです。 1に設定されている場合、このアドレスはユニキャストプレフィックスに基づくIPv6マルチキャストアドレスです(Tビットも1に設定する必要があります)。
T	0に設定すると、このアドレスはIANAによって永続的に割り当てられたIPv6マルチキャストアドレスになります。 1に設定すると、このアドレスは一時的または動的に割り当てられたIPv6マルチキャストアドレスになります。

- **Scope:** Scopeフィールドには、マルチキャストトラフィックが対象とするIPv6インターネットワークのスコープを表す4ビットが含まれます。

表5 Scopeフィールドの値

値	意味
0、	予約済み。
1	インターフェイスローカルスコープ。
2	リンクローカルスコープ。
3	サブネットローカルスコープ。
4	管理者ローカルスコープ。
5	サイトローカルスコープ。
6、7、9～D	未割り当て。
8	組織ローカルスコープ。
E	グローバルスコープ。

- グループID-グループIDフィールドには、112ビットが含まれます。スコープフィールドで定義されたスコープ内のIPv6マルチキャストグループを一意に識別します。

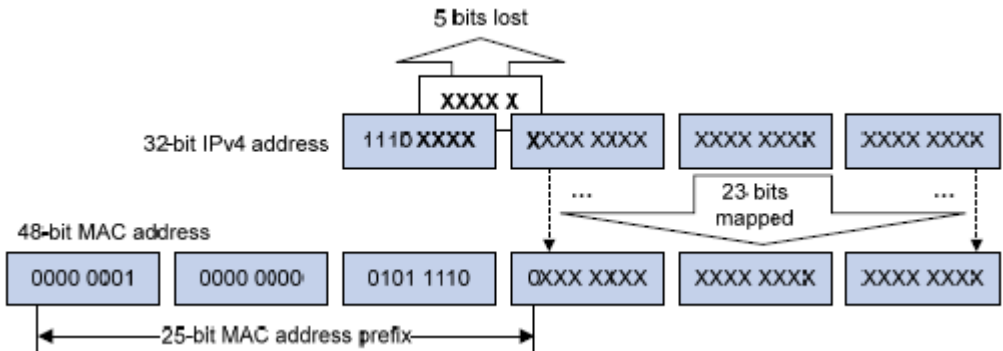
EthernetマルチキャストMACアドレス

イーサネットマルチキャストMACアドレスは、データリンク層の同じマルチキャストグループに属するレシーバを識別します。

IPv4マルチキャストMACアドレス

IANAによって定義されているように、IPv4マルチキャストMACアドレスの最上位24ビットは0x01005Eです。ビット25は0で、残りの23ビットはIPv4マルチキャストアドレスの最下位23ビットです。

図6 IPv4からMACアドレスへのマッピング

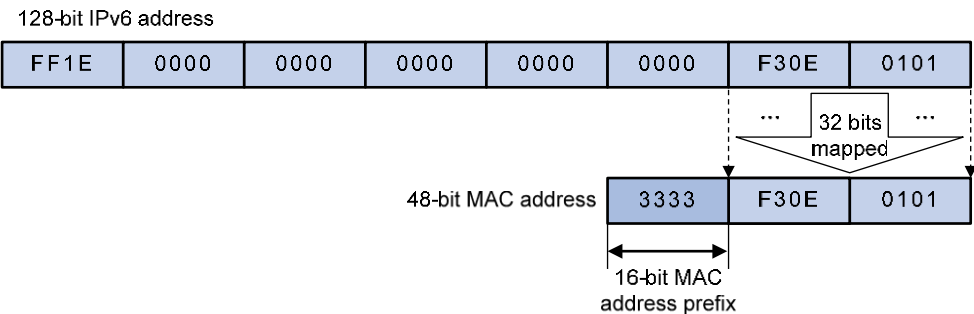


IPv4マルチキャストアドレスの上位4ビットは1110に固定されています。IPv4からMACへのアドレスマッピングでは、IPv4マルチキャストアドレスの5ビットが失われます。その結果、32個のIPv4マルチキャストアドレスが同じIPv4マルチキャストMACアドレスにマッピングされます。デバイスは、レイヤ2処理で不要なマルチキャストデータを受信する場合があります。これは、上位レイヤでフィルタリングする必要があります。

IPv6マルチキャストMACアドレス

IANAで定義されているように、IPv6マルチキャストMACアドレスの最上位16ビットは0x3333です。最下位32ビットは、IPv6マルチキャストアドレスの最下位32ビットからマッピングされます。したがって、IPv4からMACアドレスへのマッピングと同様に、IPv6からMACアドレスへの重複マッピングの問題も発生します。

図7 IPv6からMACアドレスへのマッピング



マルチキャストプロトコル

マルチキャストプロトコルには、次のカテゴリがあります。

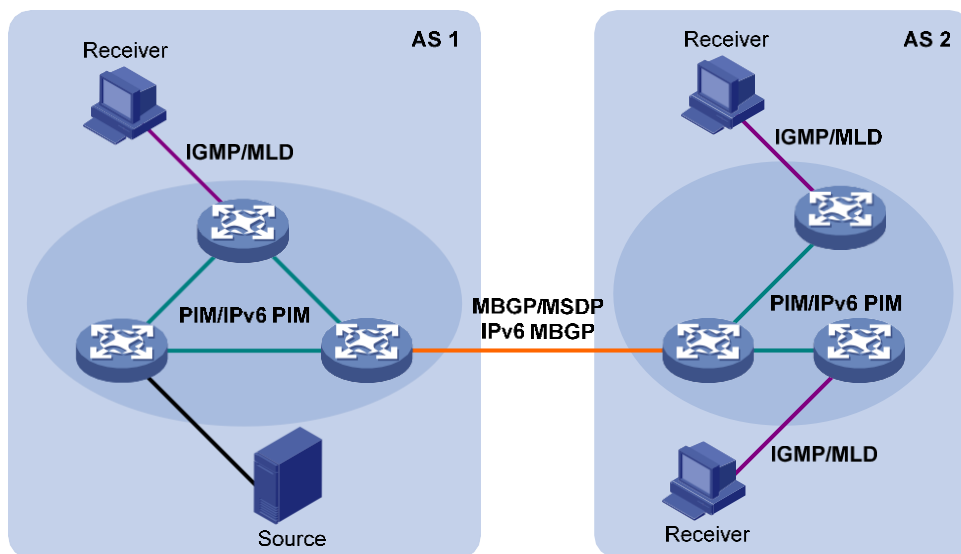
- レイヤ3およびレイヤ2マルチキャストプロトコル:
 - レイヤ3マルチキャストは、ネットワーク層で動作するIPマルチキャストを指します。
Layer 3 multicast protocols: IGMP、MLD、PIM、IPv6 PIM、MSDP、MBGP、およびIPv6 MBGP。
 - レイヤ2マルチキャストは、データリンク層で動作するIPマルチキャストを指します。
Layer 2 multicast protocols: IGMPスヌーピング、MLDスヌーピング、PIMスヌーピング、IPv6 PIMスヌーピング、マルチキャストVLAN、およびIPv6 マルチキャストVLAN。
- IPv4およびIPv6マルチキャストプロトコル:
 - IPv4 networks**の場合、IGMPスヌーピング、PIMスヌーピング、マルチキャストVLAN、IGMP、PIM、MSDP、およびMBGP。
 - IPv6 networks**の場合、MLDスヌーピング、IPv6 PIMスヌーピング、IPv6マルチキャストVLAN、MLD、IPv6 PIM、およびIPv6 MBGP。

ここでは、ネットワークにおけるレイヤ2およびレイヤ3マルチキャストプロトコルのアプリケーションと機能についての一般的な説明だけを示します。これらのプロトコルの詳細については、関連する章を参照してください。

レイヤ3マルチキャストプロトコル

図8において、レイヤ3マルチキャストプロトコルは、マルチキャストグループ管理プロトコルおよびマルチキャストルーティングプロトコルを含む。

図8 レイヤ3マルチキャストプロトコルの位置

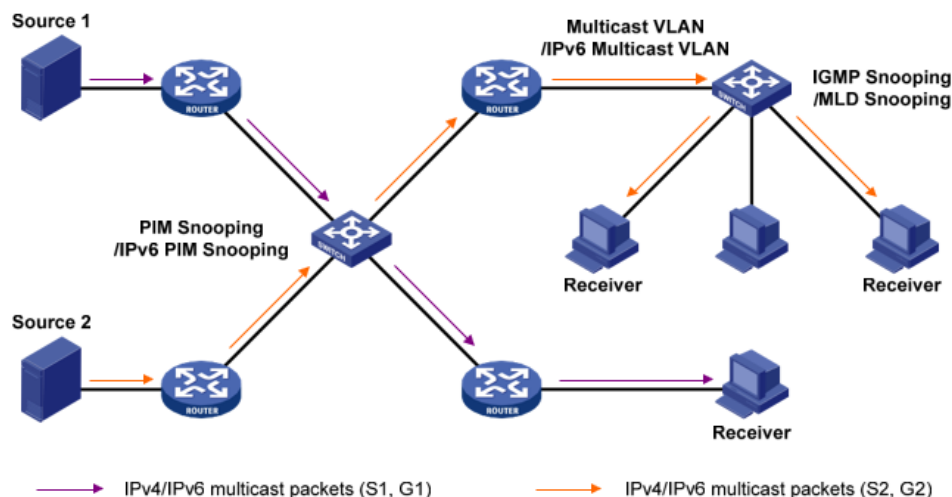


- マルチキャストグループ管理プロトコル:
Internet Group Management Protocol(IGMP)およびMulticast Listener Discovery(MLD)プロトコルは、マルチキャストグループ管理プロトコルです。通常は、ホストと、ホストに直接接続してマルチキャストグループメンバーシップを確立および維持するレイヤ3マルチキャストデバイスとの間で実行されます。
- マルチキャストルーティングプロトコル:
マルチキャストルーティングプロトコルは、レイヤ3マルチキャストデバイス上で実行され、マルチキャストルートを確認および維持し、マルチキャストパケットを正しく効率的に転送します。マルチキャストルートは、データソースから複数のレシーバへのループのないデータ伝送パス(マルチキャスト配信ツリーとも呼ばれます)を構成します。
ASMモデルでは、マルチキャストルートにはドメイン内ルートとドメイン間ルートが含まれる。
 - ドメイン内マルチキャストルーティングプロトコルは、マルチキャストソースを検出し、AS内にマルチキャスト配信ツリーを構築して、マルチキャストデータを受信者に配信します。さまざまな成熟したドメイン内マルチキャストルーティングプロトコルの中で、PIMが最も広く使用されています。PIMには、転送メカニズムに基づいて、デンスモード(PIM-DMと呼ばれることが多い)とスパスモード(PIM-SMと呼ばれることが多い)があります。
 - ドメイン間マルチキャストルーティングプロトコルは、2つのAS間でマルチキャスト情報を配信するために使用されます。これまでのところ、成熟したソリューションには、Multicast Source Discovery Protocol(MSDP)とMBGPがあります。MSDPは、異なるAS間でマルチキャストソース情報を伝播します。MBGPは、異なるAS間でマルチキャストルーティング情報を交換するためのMP-BGPの拡張です。
 SSMモデルでは、マルチキャストルートはドメイン内ルートとドメイン間ルートに分割されません。レシーバはマルチキャストソースの位置を認識しているため、マルチキャスト情報の転送にはPIM-SMを介して確立されたチャンネルで十分です。

レイヤ2マルチキャストプロトコル

図9において、レイヤ2マルチキャストプロトコルは、IGMPスヌーピング、MLDスヌーピング、PIMスヌーピング、IPv6 PIMスヌーピング、マルチキャストVLANおよびIPv6マルチキャストVLANを含みます。

図9 レイヤ2マルチキャストプロトコルの位置



- IGMPスヌーピングおよびMLDスヌーピング:
IGMPスヌーピングおよびMLDスヌーピングは、レイヤ2デバイス上で動作するマルチキャスト抑制メカニズムです。ホストとレイヤ3マルチキャストデバイス間で交換されるIGMPまたはMLDメッセージを監視および分析することにより、マルチキャストグループを管理および制御します。これにより、レイヤ2ネットワークでのマルチキャストデータのフラッディングが効果的に制御されます。
- PIMスヌーピングおよびIPv6 PIMスヌーピング:
PIMスヌーピングおよびIPv6 PIMスヌーピングは、レイヤ2デバイス上で動作します。IGMPスヌーピングまたはMLDスヌーピングと連携して、受信したPIMメッセージを分析します。次に、特定のマルチキャストデータに関係するポートをPIMスヌーピングルーティングエントリまたはIPv6 PIMスヌーピングルーティングエントリに追加します。このようにして、マルチキャストデータは、そのデータに関係するポートだけに転送できます。
- マルチキャストVLANおよびIPv6マルチキャストVLAN:
マルチキャストVLANまたはIPv6マルチキャストVLANは、同じグループのマルチキャストレシーバが異なるVLANに存在するマルチキャストネットワーク内のレイヤ2デバイス上で動作します。これらのプロトコルを使用すると、レイヤ3マルチキャストデバイスは、レイヤ2デバイス上のマルチキャストVLANまたはIPv6マルチキャストVLANにマルチキャストのコピーを1つだけ送信します。この方法により、ネットワーク帯域幅の浪費やレイヤ3デバイスへの余分な負荷が回避されます。

マルチキャストパケット転送メカニズム

マルチキャストモデルでは、マルチキャストグループの受信側ホストは通常、ネットワーク上の異なる領域に配置されます。これらのホストは、同じ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をこれらの受信者に配信するために、マルチキャスト送信元は、宛先アドレスとしてマルチキャストグループアドレスを使用して、マルチキャストデータをIPパケットにカプセル化します。転送パス上のマルチキャストルータは、着信インターフェイスが複数の発信インターフェイスを介して受信するマルチキャストパケットを転送します。ユニキャストモデルと比較すると、マルチキャストモデルは次の点でより複雑です。

- ネットワーク上でマルチキャストパケットを確実に転送するには、さまざまなルーティングテーブルを使用してマルチキャスト転送をガイドします。これらのルーティングテーブルには、ユニキャストルーティングテーブル、マルチキャスト用ルーティングテーブル(MBGPルーティングテーブルなど)、およびスタティックマルチキャストルーティングテーブルが含まれます。
- 異なるインターフェイスで受信された異なるピアからの同じマルチキャスト情報を処理するために、マルチキャストデバイスは各マルチキャストパケットに対してRPFチェックを実行します。RPFチェックの結果によって、パケットが転送されるか廃棄されるかが決まります。RPFチェックメカニズムは、マルチキャスト転送を実装するためのほとんどのマルチキャストルーティングプロトコルの基礎です。

RPFメカニズムの詳細については、「マルチキャストルーティングおよびフォワーディングの設定」および「IPv6マルチキャストルーティングおよびフォワーディングの設定」を参照してください。

IPマルチキャストアーキテクチャ

IPマルチキャストは、次の問題に対処します。

- マルチキャスト送信元はどこに情報を送信すべきですか?(マルチキャストアドレス指定。)
- ネットワーク上に存在するレシーバ(ホスト登録)
- データをレシーバに提供するマルチキャストソースはどこにありますか(マルチキャストソースディスカバリ)。
- 情報はどのようにしてレシーバに送信されますか?(マルチキャストルーティング。)

IPマルチキャストは、エンドツーエンドのサービスです。マルチキャストアーキテクチャには、次の部分が含まれます。

- **Addressing mechanism:** マルチキャスト送信元は、マルチキャストアドレスを通じて受信者のグループに情報を送信します。
- **Host registration:** 受信側ホストは、マルチキャストグループに動的に加入および脱退できます。このメカニズムは、グループメンバーシップの管理の基礎となります。

- **Multicast routing:** マルチキャスト配信ツリー(ネットワーク上のマルチキャストデータの転送パスツリー)は、マルチキャストソースから受信者にマルチキャストデータを配信するために構築されます。
- **Multicast applications:** ビデオ会議などのマルチキャストアプリケーションをサポートするソフトウェアシステムを、マルチキャストソースおよびレシーバホストにインストールする必要があります。TCP/IPスタックは、マルチキャストデータの受信と送信をサポートする必要があります。

マルチキャストにおける共通の表記法

次の表記法は、マルチキャスト転送で一般的に使用されます。

- **(*,G):**Rendezvous Point Tree(RPT)、または任意のマルチキャスト送信元がマルチキャストグループGに送信するマルチキャストパケット。アスタリスク(*)は任意のマルチキャスト送信元を表し、「G」は特定のマルチキャストグループを表します。
- **(S, G):**Shortest Path Tree(SPT)、またはマルチキャスト送信元「S」がマルチキャストグループ「G」に送信するマルチキャストパケット。「S」は特定のマルチキャスト送信元を表し、「G」は特定のマルチキャストグループを表します。

RPTおよびSPTの概念の詳細については、「PIMの設定」および「IPv6 PIMの設定」を参照してください。

IGMPスヌーピングの設定

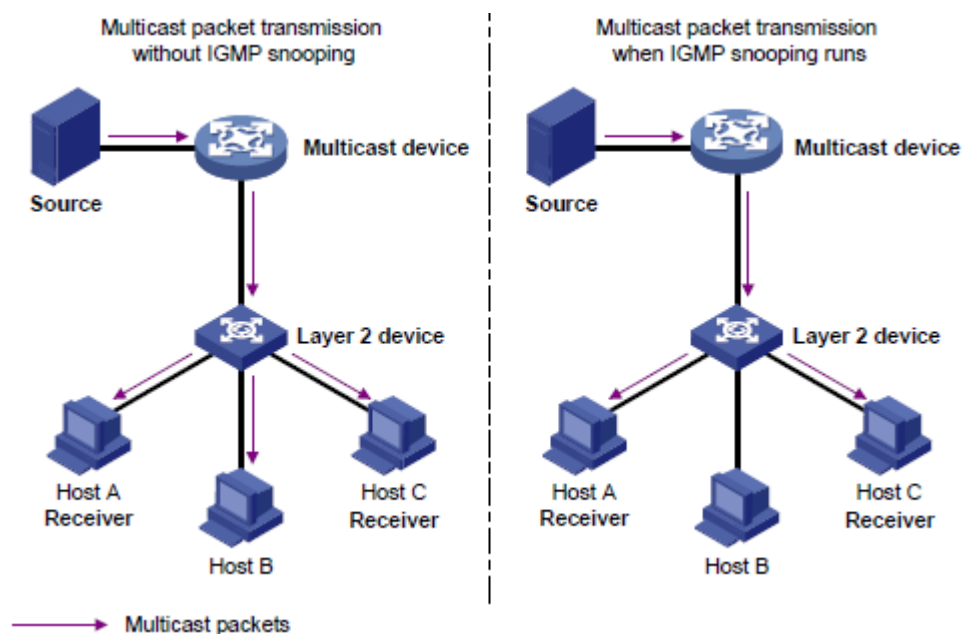
IGMPスヌーピングの概要

IGMPスヌーピングは、マルチキャスト転送効率を向上させるためのマルチキャスト抑制メカニズムとしてレイヤ2デバイス上で動作します。IGMPスヌーピングは、ホストとレイヤ3デバイス間で交換されるIGMP packets からレイヤ2マルチキャスト転送エントリを作成します。

IGMPスヌーピングの基礎

図10に示されるように、IGMPスヌーピングが有効でない場合、レイヤ2スイッチはVLANまたはVSIのすべてのホストにマルチキャストパケットをフラッディングします。IGMPスヌーピングが有効な場合、レイヤ2スイッチは既知のマルチキャストグループのマルチキャストパケットをレシーバだけに転送します。

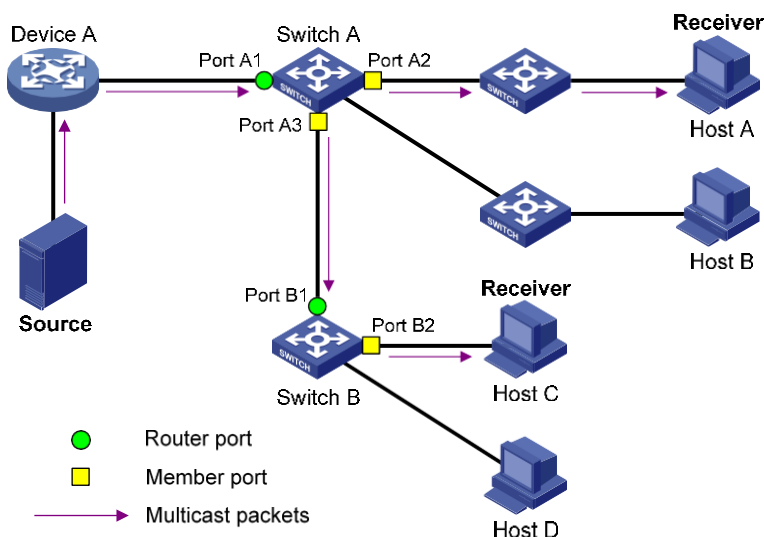
図10 IGMPスヌーピングを使用しない場合と使用した場合のマルチキャストパケット送信



GMPスヌーピングポート

図11に示すように、IGMPスヌーピングはスイッチAとスイッチBで動作し、ホストAとホストCはマルチキャストグループのレシーバです。IGMPスヌーピングポートは、メンバーポートとルータポートに分割されます。

図11 IGMPスヌーピングポート



ルータポート

IGMPスヌーピングレイヤ2デバイスでは、レイヤ3マルチキャストデバイスへのポートはルータポートと呼ばれます。図11では、スイッチAのポートA1およびスイッチBのポートB1はルータポートです。

ルータポートには、次のタイプがあります。

- **Dynamic router port:** 送信元アドレスが0.0.0.0ではないIGMP一般クエリーを受信したポート、またはPIM helloメッセージを受信したポートは、ダイナミックルータポートリストに追加されます。同時に、ポートのエイジングタイマーが開始されます。タイマーの期限が切れる前にポートがいずれかのメッセージを受信した場合、タイマーはリセットされます。タイマーの期限が切れたときにポートがいずれのメッセージも受信しなかった場合、ポートはダイナミックルータポートリストから削除されます。
- **Static router port:** ポートがルータポートとしてスタティックに設定されると、スタティックルータポートリストに追加されます。スタティックルータポートは期限切れにならず、手動でのみ削除できます。

IGMPスヌーピングの「ルータポート」を、一般に「レイヤ3インターフェイス」と呼ばれる「ルーテッドインターフェイス」と混同しないでください。IGMPスヌーピングのルータポートは、レイヤ2インターフェイスです。

メンバーポート

IGMPスヌーピングレイヤ2デバイスでは、レシーバホストへのポートはメンバーポートと呼ばれます。図11では、スイッチAのポートA2とポートA3、およびスイッチBのポートB2がメンバーポートです。

メンバーポートには、次のタイプがあります。

- **Dynamic member port:** ポートがIGMPレポートを受信すると、関連付けられたダイナミックIGMPスヌーピング転送エントリに発信インターフェイスとして追加されます。同時に、ポートのエージングタイマーが開始されます。タイマーの期限が切れる前にポートがIGMPレポートを受信した場合、タイマーはリセットされます。タイマーの期限が切れたときにポートがIGMPレポートを受信しなかった場合、ポートは関連付けられたダイナミックフォワーディングエントリから削除されます。
- **Static member port:** ポートがメンバーポートとしてスタティックに設定されている場合、関連付けられたスタティックIGMPスヌーピング転送エントリに発信インターフェイスとして追加されます。スタティックメンバーポートは期限切れにならず、手動でのみ削除できます。

特に指定のない限り、このマニュアルのルータポートおよびメンバーポートには、スタティックルータポートとダイナミックルータポートの両方が含まれます。

IGMPスヌーピングの動作

このセクションのポートは、ダイナミックポートです。スタティックポートの設定および削除の方法については、「スタティックメンバーポートの設定」および「スタティックルータポートの設定」を参照してください。IGMPメッセージタイプには、一般的なクエリー、IGMPレポート、およびリーブメッセージが含まれます。IGMPスヌーピング対応レイヤ2デバイスの動作は、メッセージタイプによって異なります。

一般的なクエリー

IGMPクエリーは、IGMP一般クエリーをローカルサブネット上のすべてのホストおよびデバイスに定期的に送信して、マルチキャストグループメンバーの存在を確認します。

IGMP一般クエリーを受信した後、レイヤ2デバイスは、受信ポートを除くVLANまたはVSIのすべてのポートにクエリーを転送します。レイヤ2デバイスは、次のいずれかのアクションも実行します:

- 受信ポートがダイナミックルータポートリスト内のダイナミックルータポートである場合、レイヤ2デバイスはそのポートのエージングタイマーを再開します。
- 受信ポートがダイナミックルータポートリストに存在しない場合、レイヤ2デバイスはそのポートをダイナミックルータポートリストに追加します。また、ポートのエージングタイマーを開始します。

IGMPレポート

ホストは、次の目的でIGMPクエリーにIGMPレポートを送信します。

- ホストがマルチキャストグループメンバーである場合、クエリーに応答します。
- マルチキャストグループメンバーシップを申請します。

ホストからIGMPレポートを受信すると、レイヤ2デバイスはVLANまたはVSI内のすべてのルータポートを介してレポートを転送します。また、レポートされたマルチキャストグループのアドレスを解決し、次のように転送テーブルで一致するエントリを検索します。

- 一致するものが見つからない場合、レイヤ2デバイスは受信ポートを発信インターフェイスとしてフォワーディングエントリを作成します。また、受信ポートをダイナミックメンバーポートとしてマークし、ポートのエージングタイマーを開始します。
- 一致が見つかったが、一致するフォワーディングエントリに受信ポートが含まれていない場合、レイ

レイヤ2デバイスは受信ポートを発信インターフェイスリストに追加します。また、受信ポートをダイナミックメンバーポートとしてマークし、そのポートのエージングタイマーを開始します。

- 一致が検出され、一致するフォワーディングエントリに受信ポートが含まれている場合、レイヤ2デバイスはそのポートのエージングタイマーを再開します。

注.

レイヤ2デバイスは、ホストIGMPレポート抑制メカニズムのため、非ルータポートを介してIGMPレポートを転送しません。非ルータポートにメンバーホストが接続されている場合、メンバーホストは、非ルータポートによって転送されたIGMPレポートを受信すると、IGMPレポートを抑制します。レイヤ2デバイスは、非ルータポートに接続されたメンバーホストの存在を認識できません。

IGMPレポート抑制メカニズムの詳細については、「IGMPの設定」を参照してください。

メッセージを残す

IGMPv1レシーバホストは、マルチキャストグループを脱退するときにLeaveメッセージを送信しません。レイヤ2デバイスは、レシーバホストに接続されているポートのステータスをすぐに更新することはできません。レイヤ2デバイスは、グループのエージングタイムが満了するまで、関連する転送エントリの発信インターフェイスリストからポートを削除しません。

IGMPv2またはIGMPv3ホストは、マルチキャストグループを脱退するときにIGMP Leaveメッセージを送信します。

レイヤ2デバイスは、ダイナミックメンバーポート上でIGMP Leaveメッセージを受信すると、まずフォワーディングエントリがメッセージ内のグループアドレスと一致するかどうかを確認します。

- 一致が見つからない場合、レイヤ2デバイスはIGMP Leaveメッセージを破棄します。
- 一致が検出されても、受信ポートが転送エントリの発信インターフェイスではない場合、レイヤ2デバイスはIGMP Leaveメッセージを廃棄します。
- 一致が検出され、受信ポートが転送エントリ内の唯一の発信インターフェイスではない場合、レイヤ2デバイスは次のアクションを実行します。
 - IGMP Leaveメッセージを廃棄します。
 - IGMPグループ固有クエリーを送信して、受信ポートに接続されたアクティブレシーバがグループに存在するかどうかを識別します。
 - 受信ポートのエージングタイマーを、IGMP最終メンバークエリーインターバルの2倍に設定します。
- 一致が検出され、受信ポートが転送エントリ内の唯一の発信インターフェイスである場合、レイヤ2デバイスは次の処理を実行します。
 - VLANまたはVSIのすべてのルータポートにIGMP Leaveメッセージを転送します。
 - IGMPグループ固有クエリーを送信して、受信ポートに接続されたアクティブレシーバがグループに存在するかどうかを識別します。

- 受信ポートのエージングタイマーを、IGMP最終メンバークエリーインターバルの2倍に設定します。

ポート上でIGMP Leaveメッセージを受信すると、IGMPクエリアはメッセージ内のマルチキャストグループアドレスを解決します。次に、受信ポートを介してIGMPグループ固有のクエリーをマルチキャストグループに送信します。

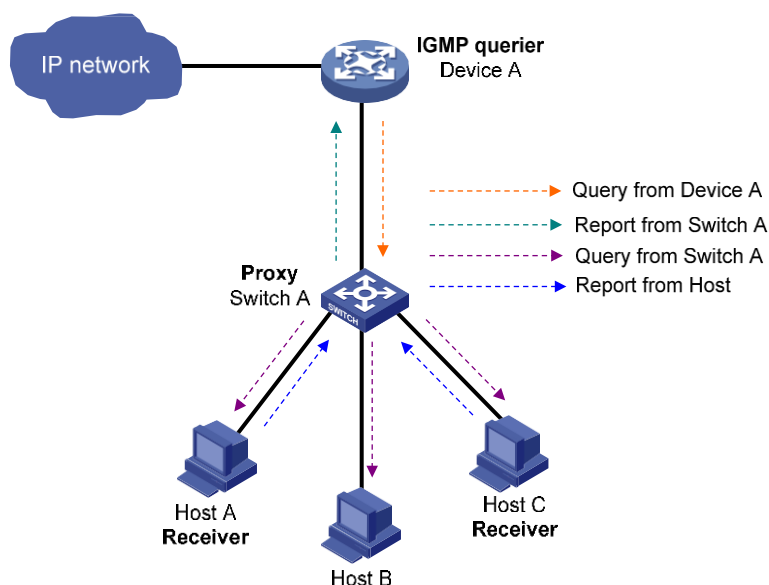
IGMPグループ固有クエリーを受信した後、レイヤ2デバイスは、VLANまたはVSI内のグループのすべてのルータポートおよびメンバーポートを介してクエリーを転送します。次に、直接接続されたホストからの応答IGMPレポートを待ちます。リーブメッセージを受信したダイナミックメンバーポートに対して、レイヤ2デバイスは次のいずれかのアクションも実行します。

- エージングタイマーが満了する前にポートがIGMPレポートを受信した場合、レイヤ2デバイスはエージングタイマーをリセットします。
- エージングタイマーが満了する時、ポートがIGMPレポートを受信しない場合、レイヤ2デバイスは、マルチキャストグループのフォワーディングエントリからポートを削除します。

IGMPスヌーピングプロキシ

図12に示されるように、上流のデバイスによって受信されるIGMPレポートおよびリーブメッセージの数を減らすために、エッジデバイス上でIGMPスヌーピングプロキシングを有効にすることができます。IGMPスヌーピングプロキシングが有効な状態で、エッジデバイスは、上流のIGMPスヌーピングクエリアのホストとして動作し、IGMPレポートおよびリーブメッセージをデバイスAに送信します。エッジデバイス上のホストIGMPレポート抑制メカニズムは、有効ではありません。IGMPレポート抑制メカニズムの詳細については、「IGMPの設定」を参照してください。

図12 IGMPスヌーピングプロキシ



IGMPスヌーピングプロキシデバイスは、さまざまなIGMPメッセージを次のように処理します。

- 一般クエリー
IGMP一般クエリーを受信した後、デバイスは受信ポートを除くVLAN内のすべてのポートにクエリーを転送します。デバイスはまた、ローカルメンバーシップ情報に基づいてIGMPレポートを生成し、そのレポートをすべてのルータポートに送信します。
- グループ固有クエリーまたはグループ/ソース固有クエリー
IGMPグループ特定クエリーまたはグループおよび送信元特定クエリーを受信した後、デバイスは受信ポートを除くVLAN内のすべてのポートにクエリーを転送します。フォワーディングエントリにメンバーポートがある場合、デバイスはVLAN内のすべてのルータポートにレポートを送信します。
- レポート
ホストからIGMPレポートを受信した後、デバイスは次のように転送テーブルで一致するエントリを検索します。
 - 一致が検出され、一致するフォワーディングエントリに受信ポートが含まれている場合、デバイスはそのポートのエージングタイマーをリセットします。

- 一致するものが見つかったも、一致するフォワーディングエントリに受信ポートが含まれていない場合、デバイスは受信ポートを発信インターフェイスリストに追加します。また、受信ポートをダイナミックメンバーポートとしてマークし、ポートのエージングタイマーを開始します。
- 一致するものが見つからない場合、デバイスは受信ポートを発信インターフェイスとする転送エントリを作成します。また、受信ポートをダイナミックメンバーポートとしてマークし、ポートのエージングタイマーを開始します。次に、レポートをすべてのルータポートに送信します。
- メッセージを残す
ポートでIGMP Leaveメッセージを受信すると、デバイスは受信ポートを介してIGMPグループ固有のクエリを送信します。最後のメンバーポートが転送エントリから削除された場合にのみ、デバイスはすべてのルータポートにIGMP Leaveメッセージを送信します。

プロトコルと標準

RFC 4541『Considerations for Internet Group Management Protocol(IGMP)and Multicast Listener Discovery(MLD)Snooping Switch es』

制約事項および注意事項:IGMPスヌーピング設定

セカンダリVLANから受信したIGMPレポートの場合、関連付けられたIGMPスヌーピング転送エントリはプライマリVLANによって維持されます。したがって、プライマリVLANに対してだけIGMPスヌーピングを有効にする必要があります。セカンダリVLANで作成されたIGMPスヌーピング設定は有効になりません。プライマリVLANおよびセカンダリVLANの詳細については、『Layer 2 LAN Configuration Guide』を参照してください。

レイヤ2集約インターフェイスで行われたIGMPスヌーピング設定は、メンバーポートで行われた設定と干渉しません。また、レイヤ2集約インターフェイスで行われた設定は、集約計算には関与しません。集約グループのメンバーポートで行われた設定は、そのポートが集約グループから脱退した後に有効になります。

一部の機能は、VLANビュー内の1つのVLANまたはIGMPスヌーピングビュー内の複数のVLANに対して設定できます。VLANビュー内の設定とIGMPスヌーピングビュー内の設定は同じプライオリティを持ち、最新の設定が有効になります。

一部の機能は、VLANビューで1つのVLANに対して設定するか、IGMPスヌーピングビューですべてのVLANに対してグローバルに設定できます。VLAN固有の設定は、グローバル設定よりも優先されます。

一部の機能は、VSIビューでVSIに対して設定するか、IGMPスヌーピングビューですべてのVSIに対してグローバルに設定できます。VSI固有の設定は、グローバル設定よりも優先されます。

一部の機能は、インターフェイスビューで1つのインターフェイスに対して設定することも、IGMPスヌーピ

ングビューで指定されたVLANのすべてのインターフェイスに対して設定することもできます。インターフェイス固有の設定は、IGMPスヌーピングビューでの設定よりも優先されます。

VLANベースのIGMPスヌーピングタスクの概要

VLANにIGMPスヌーピングを設定するには、次の作業を実行します。

1. IGMPスヌーピング機能の有効化
2. IGMPスヌーピングの有効化
必要に応じて、次のタスクを選択します。
 - IGMPスヌーピングのグローバルな有効化
 - VLANのIGMPスヌーピングの有効化
3. (任意)基本的なIGMPスヌーピング機能の設定
 - IGMPスヌーピングバージョンの指定
 - IGMPスヌーピングフォワーディングエントリの最大数の設定
 - スタティックマルチキャストMACアドレスエントリの設定
 - IGMP最終メンバークエリーインターバルの設定
4. (任意)IGMPスヌーピングポート機能の設定
 - ダイナミックポートのエージングタイマーの設定
 - スタティックメンバーポートの設定
 - スタティックルータポートの設定
 - シミュレートメンバーホストとしてのポートの構成
 - 高速脱退処理の有効化
 - ポートがダイナミックルータポートになることを無効にする
5. (任意)IGMPスヌーピングクエリーアの設定
 - IGMPスヌーピングクエリーアの有効化
 - IGMPスヌーピングクエリーア選定の有効化
 - IGMP一般クエリーおよび応答のパラメータの設定
6. (任意)IGMPスヌーピングプロキシの有効化
7. (任意)IGMPメッセージのパラメータの設定
 - IGMPメッセージの送信元IPアドレスの設定
 - IGMPメッセージの802.1pプライオリティの設定
8. (任意)IGMPスヌーピングポリシーの設定
 - マルチキャストグループポリシーの設定
 - マルチキャスト送信元ポートフィルタリングの有効化
 - 不明なマルチキャストデータの破棄の有効化
 - IGMPレポート抑制の有効化

- ポート上のマルチキャストグループの最大数の設定
 - マルチキャストグループ置換の有効化
 - ホストトラッキングの有効化
9. (任意)発信IGMPスヌーピングプロトコルパケットのDSCP値の設定

VSIベースのIGMPスヌーピングタスクの概要

VSIのIGMPスヌーピングを設定するには、次の作業を実行します。

1. IGMPスヌーピング機能の有効化
2. IGMPスヌーピングの有効化
必要に応じて、次のタスクを選択します。
 - IGMPスヌーピングのグローバルな有効化
 - VSIのIGMPスヌーピングの有効化
3. (任意)基本的なIGMPスヌーピング機能の設定
 - IGMPスヌーピングバージョンの指定
 - IGMPスヌーピングフォワーディングエントリの最大数の設定
 - IGMP最終メンバークエリーインターバルの設定
4. (任意)ダイナミックポートのエージングタイマーの設定
5. (任意)IGMPスヌーピングクエリーアの設定
 - IGMPスヌーピングクエリーアの有効化
 - IGMPスヌーピングクエリーア選定の有効化
 - IGMP一般クエリーおよび応答のパラメータの設定
6. (任意)IGMPスヌーピングプロキシの有効化
7. (任意)IGMPメッセージのパラメータの設定
 - IGMPメッセージの送信元IPアドレスの設定
 - IGMPメッセージの802.1pプライオリティの設定
8. (任意)IGMPスヌーピングポリシーの設定
 - 不明なマルチキャストデータの破棄の有効化
 - IGMPレポート抑制の有効化
9. (任意)発信IGMPスヌーピングプロトコルパケットのDSCP値の設定

IGMPスヌーピング機能の有効化

IGMPスヌーピング機能の有効化について

他のIGMPスヌーピング機能を設定する前に、IGMPスヌーピング機能を有効にする必要があります。

手順

1. システムビューに入ります。

System-view

2. IGMPスヌーピング機能を有効にし、IGMPスヌーピングビューを開始します。

igmp-snooping

デフォルトでは、IGMPスヌーピング機能は無効です。

IGMPスヌーピングの有効化

IGMPスヌーピングのグローバルな有効化

IGMPスヌーピングのグローバルな有効化について

IGMPスヌーピングをグローバルに有効にすると、すべてのVLANまたはVSIでIGMPスヌーピングが有効になります。IGMPスヌーピングがグローバルに有効の場合、VLANまたはVSIのIGMPスヌーピングを無効にできます。

制約事項とガイドライン

VLANまたはVSIに他のIGMPスヌーピング機能を設定するには、IGMPスヌーピングがグローバルに有効になっている場合でも、特定のVLANまたはVSIに対してIGMPスヌーピングを有効にする必要があります。

VLAN固有またはVSI固有のIGMPスヌーピング設定は、グローバルなIGMPスヌーピング設定よりも優先されます。たとえば、IGMPスヌーピングをグローバルに有効にしてから、**igmp-snooping disable** コマンドを使用してVLANのIGMPスヌーピングを無効にすると、VLANのIGMPスヌーピングは無効になります。

手順

1. System-viewに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. IGMPスヌーピングをグローバルに有効にします。

global-enable

デフォルトでは、IGMPスヌーピングはグローバルに無効です。

4. (任意)VLANまたはVSIのIGMPスヌーピングを無効にします。

- a. システムビューに戻ります。

quit

- b. VLANまたはVSIビューを入力します。

vlan *vlan-id*

vsi *vsi-name*

- c. VLANまたはVSIのIGMPスヌーピングを無効にします。

igmp-snooping disable

デフォルトでは、VLANまたはVSIのIGMPスヌーピングステータスは、グローバルなIGMPスヌーピングステータスと一致します。

VLANのIGMPスヌーピングの有効化

制約事項とガイドライン

複数のVLANに対してIGMPスヌーピングを有効にするには、IGMPスヌーピングビューでenable vlanコマンドを使用します。VLANに対してIGMPスヌーピングを有効にするには、VLANビューでIGMP-snooping enableコマンドを使用します。VLANビューでの設定は、IGMPスヌーピングビューでの設定と同じプライオリティになります。

VLANのIGMPスヌーピング設定は、VLANのメンバーポートだけで有効になります。

複数のVLANに対するIGMPスヌーピングの有効化

1. システムビューに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. 指定されたVLANのIGMPスヌーピングを有効にします。

enable vlan *vlan-list*

デフォルトでは、VLANのIGMPスヌーピングステータスは、グローバルなIGMPスヌーピングステータスと一致します。

VLANのIGMPスヌーピングの有効化

1. システムビューに入ります。

System-view

2. VLANビューを開始します。

vlan *vlan-id*

3. VLANのIGMPスヌーピングを有効にします。

igmp-snooping enable

デフォルトでは、VLANのIGMPスヌーピングステータスは、グローバルなIGMPスヌーピングステータスと一致します。

VSIのIGMPスヌーピングの有効化

制約事項とガイドライン

VSIの場合、igmp-snooping enableコマンドを使用して、VSIのIGMPスヌーピングだけを有効にできます。コマンドを使用します。

VSIのIGMPスヌーピング設定は、VSIのメンバーポートだけで有効です。

手順

1. システムビューに入ります。

System-view

2. VSIビューを入力します。

vsi vsi-name

3. VSIのIGMPスヌーピングを有効にします。

igmp-snooping enable

デフォルトでは、VSIのIGMPスヌーピングステータスは、グローバルIGMPスヌーピングステータスと一致します。

基本的なIGMPスヌーピング機能の設定

IGMPスヌーピングバージョンの指定

IGMPスヌーピングのバージョンについて

IGMPスヌーピングのバージョンが異なると、処理するIGMPメッセージのバージョンも異なります。

- IGMPv2スヌーピングはIGMPv1メッセージ、IGMPv2メッセージ、およびIGMPv3クエリーを処理しますが、VLANまたはVSI内のIGMPv3レポートを処理せずにフラッディングします。
- IGMPv3スヌーピングは、IGMPv1、IGMPv2、およびIGMPv3メッセージを処理します。

制約事項とガイドライン

IGMPスヌーピングバージョンを2から3に変更すると、デバイスは次のアクションを実行します。

- ダイナミックに作成されたすべてのIGMPスヌーピング転送エントリをクリアします。
- スタティックIGMPv3スヌーピング転送エントリ(*,G)を保持します。
- スタティックIGMPv3スヌーピング転送エントリ(S, G)をクリアします。これは、IGMPスヌーピングバージョンが3に戻されたときに復元されます。

スタティックIGMPスヌーピングフォワーディングエントリの詳細については、「スタティックメンバーポートの設定」を参照してください。

複数のVLANに対するIGMPスヌーピングバージョンの指定

1. システムビューに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. 複数のVLANに対してIGMPスヌーピングバージョンを指定します。

version version-number vlan vlan-list

デフォルトでは、VLANのIGMPスヌーピングバージョンは2です。

VLANのIGMPスヌーピングバージョンの指定

1. システムビューに入ります。

System-view

2. VLANビューを開始します。

3. **vlan vlan-id**

4. VLANのIGMPスヌーピングバージョンを指定します。

igmp-snooping version version-number

デフォルトでは、VLANのIGMPスヌーピングバージョンは2です。

VSIのIGMPスヌーピングバージョンの指定

1. システムビューに入ります。

System-view

2. VSIビューを入力します。

vsi vsi-name

3. VSIのIGMPスヌーピングバージョンを指定します。

igmp-snooping version version-number

デフォルトでは、VSIのIGMPスヌーピングバージョンは2です。

IGMPスヌーピングフォワーディングエントリの最大数の設定

IGMPスヌーピングフォワーディングエントリの最大数の設定について

ダイナミックエントリおよびスタティックエントリを含む、IGMPスヌーピング転送エントリの最大数を変更できます。デバイス上の転送エントリ数が上限に達すると、デバイスは既存のエントリを自動的に削除しません。新しいエントリを作成できるようにするには、一部のエントリを手動で削除します。

手順

1. システムビューに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. IGMPスヌーピングフォワーディングエントリの最大数を設定します。

entry-limit limit

デフォルトでは、IGMPスヌーピングフォワーディングエントリの最大数は4294967295です。

スタティックマルチキャストMACアドレスエントリの設定

スタティックマルチキャストMACアドレスエントリについて

レイヤ2マルチキャストでは、レイヤ2マルチキャストプロトコル(IGMPスヌーピングなど)を使用して、マルチキャストMACアドレスエントリをダイナミックに作成できます。マルチキャストMACアドレスおよびポートをバインドしてマルチキャストデータの宛先ポートを制御することにより、スタティックマルチキャストMACアドレスエントリを手動で設定することもできます。

制約事項とガイドライン

スタティックマルチキャストMACアドレスエントリを設定する場合は、未使用のマルチキャストMACアドレスを指定する必要があります。マルチキャストMACアドレスは、最上位オクテットの最下位ビットが1であるMACアドレスです。

システムビューでのスタティックマルチキャストMACアドレスエントリの設定

1. システムビューに入ります。

System-view

2. スタティックマルチキャストMACアドレスエントリを設定します。

mac-address multicast *mac-address* **interface** *interface-list* **vlan** *vlan-id*

インターフェイスビューでのスタティックマルチキャストMACアドレスエントリの設定

1. システムビューに入ります。

System-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface *interface-type* *interface-number*

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation *interface-number*

3. スタティックマルチキャストMACアドレスエントリを設定します。

mac-address multicast *mac-address* **vlan** *vlan-id*

IGMP最終メンバークエリインターバルの設定

IGMP最終メンバークエリインターバルについて

レシーバホストは、マルチキャストグループに対するIGMPグループ固有クエリを受信すると、そのグループのレポート遅延タイマーを開始します。このタイマーは、0からクエリでアドバタイズされる最大応答時間までの範囲のランダム値に設定されます。タイマー値が0に減少すると、ホストはグループにIGMPレポートを送信します。

IGMP最終メンバークエリインターバルは、IGMPグループ固有のクエリでアドバタイズされる最大応答時間を定義します。IGMPグループ固有のクエリに対するホストの応答を高速化し、IGMPレポートトラフィックのバーストを回避するには、IGMP最終メンバークエリインターバルに適切な値を設定します。

IGMP最終メンバークエリインターバルのグローバルな設定

1. システムビューに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. IGMP最終メンバークエリインターバルをグローバルに設定します。

last-member-query-interval *interval*

デフォルトでは、グローバルなIGMP最終メンバークエリインターバルは1秒です。

VLANのIGMP最終メンバークエリインターバルの設定

1. システムビューに入ります。

System-view

2. VLANビューを開始します。

```
vlan vlan-id
```

3. VLANのIGMP最終メンバークエリインターバルを設定します。

```
igmp-snooping last-member-query-interval interval
```

デフォルトでは、VLANのIGMP最終メンバークエリインターバルは1秒です。

VSIのIGMP最終メンバークエリインターバルの設定

1. システムビューに入ります。

System-view

2. VSIビューを入力します。

```
vsi vsi-name
```

3. VSIのIGMP最終メンバークエリインターバルを設定します。

```
igmp-snooping last-member-query-interval interval
```

デフォルトでは、VSIのIGMP最終メンバークエリインターバルは1秒です。

IGMPスヌーピングポート機能の設定

ダイナミックポートのエージングタイマーの設定

ダイナミックポートのエージングタイマーについて

ダイナミックルータポートは、エージングタイマーが満了したときにIGMP一般クエリまたはPIM helloメッセージを受信しない場合、ダイナミックルータポートリストから削除されます。

ダイナミックメンバーポートは、エージングタイマーが満了したときにIGMPレポートを受信しない場合、ダイナミックメンバーポートから削除されます。

制約事項とガイドライン

ダイナミックポートのエージングタイマーに適切な値を設定します。たとえば、マルチキャストグループのメンバーシップが頻繁に変更される場合は、ダイナミックメンバーポートのエージングタイマーに比較的小さい値を設定します。マルチキャストグループのメンバーシップがほとんど変更されない場合は、比較的大きな値を設定します。

ダイナミックルータポートがPIMv2 helloメッセージを受信した場合、そのポートのエージングタイマーはhelloメッセージで指定されます。この場合、**router-aging-time**または**igmp-snooping router-aging-time**コマンドは、ポート上で有効になりません。

レイヤ2デバイスによって生成されたIGMPグループ固有のクエリは、ダイナミックメンバーポートのエージングタイマーの調整を開始します。ダイナミックメンバーポートがこのようなクエリを受信した場合、エージングタイマーはIGMP最終メンバークエリインターバルの2倍に設定されます。レイヤ2デバイスのIGMP最終メンバークエリインターバルの設定についての詳細は、「IGMP最終メンバークエリインターバルの設定」を参照してください。

ダイナミックポートのエージングタイマーのグローバルな設定

1. システムビューに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. ダイナミックルータポートのエージングタイマーをグローバルに設定します。

router-aging-time seconds

デフォルトでは、ダイナミックルータポートのエージングタイマーは260秒です。

4. ダイナミックメンバーポートのグローバルエージングタイマーをグローバルに設定します。

host-aging-time seconds

デフォルトでは、ダイナミックメンバーポートのエージングタイマーは260秒です。

VLANにおけるダイナミックポートのためのエージングタイマーの設定

1. システムビューに入ります。

System-view

2. VLANビューを開始します。

vlan vlan-id

3. VLAN内のダイナミックルータポートのエージングタイマーを設定します。

igmp-snooping router-aging-time seconds

デフォルトでは、ダイナミックルータポートのエージングタイマーは260秒です。

4. VLAN内のダイナミックメンバーポートのエージングタイマーを設定します。

igmp-snooping host-aging-time seconds

デフォルトでは、ダイナミックメンバーポートのエージングタイマーは260秒です。

VSIでのダイナミックポートのエージングタイマーの設定

1. システムビューに入ります。

System-view

2. VSIビューを入力します。

vsi vsi-name

3. VSIでダイナミックルータポートのエージングタイマーを設定します。

igmp-snooping router-aging-time seconds

デフォルトでは、ダイナミックルータポートのエージングタイマーは260秒です。

4. VSIのダイナミックメンバーポートのエージングタイマーを設定します。

igmp-snooping host-aging-time seconds

デフォルトでは、ダイナミックメンバーポートのエージングタイマーは260秒です。

スタティックメンバーポートの設定

スタティックメンバーポートについて

ポートに接続されたホストが常にグループのマルチキャストを受信できるように、ポートをマルチキャストグループのスタティックメンバーポートとして設定できます。スタティックメンバーポートは、IGMPクエリーに応答しません。ポート上でこの設定を完了またはキャンセルすると、ポートは非送信請求IGMPレポートまたはLeaveメッセージを送信しません。

手順

1. システムビューに入ります。

System-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface *interface-type interface-number*

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation *interface-number*

3. ポートをスタティックメンバーポートとして設定します。

```
igmp-snooping static-group group-address [ source-ip source-address ] vlan vlan-id
```

デフォルトでは、ポートはスタティックメンバーポートではありません。

スタティックルータポートの設定

スタティックルータポートについて

ポートで受信したグループのすべてのマルチキャストデータが転送されるように、ポートをマルチキャストグループのスタティックルータポートとして設定できます。

手順

1. システムビューに入ります。

System-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface *interface-type interface-number*

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation *interface-number*

3. ポートをスタティックルータポートとして設定します。

igmp-snooping static-router-port **vlan** *vlan-id*

デフォルトでは、ポートはスタティックルータポートではありません。

シミュレートメンバーホストとしてのポートの構成

シミュレートされたメンバーホストについて

ポートをシミュレートメンバーホストとして設定すると、次の点で独立ホストと同等になります。

- 設定が完了すると、非送信請求IGMPレポートが送信されます。
- IGMP一般クエリーには、IGMPレポートで応答します。
- 設定をキャンセルすると、IGMP Leaveメッセージが送信されます。

シミュレートされたメンバーホストで動作しているIGMPのバージョンは、ポートで動作しているIGMPスヌーピングのバージョンと同じです。ポートは、ダイナミックメンバーポートと同じ方法で期限切れになります。

手順

1. システムビューに入ります。

System-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface *interface-type* *interface-number*

- レイヤ2集約インターフェイスビューを開始します。

interface **bridge-aggregation** *interface-number*

3. ポートをシミュレートメンバーホストとして設定します。

igmp-snooping **host-join** *group-address* [**source-ip** *source-address*] **vlan**
vlan-id

デフォルトでは、ポートはシミュレートされるメンバーホストではありません。

高速脱退処理の有効化

高速脱退処理について

この機能は、ポートがリーブメッセージを受信した際に、レイヤ2デバイスがマルチキャストグループのフォワーディングエントリからポートを即座に削除することを可能にします。レイヤ2デバイスは、グループに対するIGMPグループ固有のクエリーをポートに送信または転送しなくなります。

制約事項とガイドライン

VLAN内に複数のレシーバホストがあるポートでは、高速脱退処理を有効にしないでください。この場合、レシーバがグループを脱退すると、残りのレシーバはグループのマルチキャストデータを受信できなくなります。

高速脱退処理のグローバルな有効化

1. システムビューに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. 高速脱退処理をグローバルに有効にします。

fast-leave [vlan vlan-list]

デフォルトでは、高速脱退処理はグローバルに無効です。

ポート上での高速脱退処理の有効化

1. システムビューに入ります。

System-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface interface-type interface-number

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation interface-number

3. ポート上で高速脱退処理を有効にします。

igmp-snoopingfast-leave [vlan vlan-list]

デフォルトでは、高速脱退処理はポート上で無効です。

ポートがダイナミックルータポートになることを無効にする

ポートがダイナミックルータポートになることを無効にする方法

レシーバホストは、テスト目的でIGMP一般クエリーまたはPIM helloメッセージを送信する場合があります。レイヤ2デバイスでは、いずれかのメッセージを受信するポートはダイナミックルータポートになります。ポートのエージングタイマーが期限切れになる前に、次の問題が発生する可能性があります。

- ポートが属するVLANのすべてのマルチキャストデータは、ポートに送信されます。その後、ポートは接続されたレシーバホストにデータを転送します。レシーバホストは、受信したくないマルチキャストデータを受信します。
- ポートは、IGMP一般クエリーまたはPIM helloメッセージをアップストリームレイヤ3デバイスに転送します。これらのメッセージは、レイヤ3デバイス上のマルチキャストルーティングプロトコルステート(IGMPクエリーアまたはDR選定など)に影響を与える可能性があります。これにより、ネットワークがさらに中断される可能性があります。

これらの問題を解決するために、ポートがダイナミックルータポートにならないようにすることができます。

これにより、ネットワークセキュリティと受信ホストの制御も向上します。

制約事項とガイドライン

この設定とスタティックルータポート設定は、相互に干渉しません。

手順

1. システムビューに入ります。

System-view

2. レイヤ2インターフェイスビューを開始します。
 - レイヤ2イーサネットインターフェイスビューを開始します。
interface *interface-type interface-number*
 - レイヤ2集約インターフェイスビューを開始します。
interface bridge-aggregation *interface-number*
3. ポートがダイナミックルータポートになることを無効にします。
igmp-snooping router-port-deny [**vlan** *vlan-list*]
デフォルトでは、ポートはダイナミックルータポートになることができます。

IGMPスヌーピングクエリーの設定

IGMPスヌーピングクエリーの有効化

IGMPスヌーピングクエリーについて

この機能を使用すると、レイヤ2デバイスは定期的にIGMP一般クエリーを送信して、データリンクレイヤでマルチキャスト転送エントリを確立および維持できます。レイヤ3マルチキャストデバイスのないネットワーク上でIGMPスヌーピングクエリーを設定できます。

制約事項とガイドライン

IGMPを実行するマルチキャストネットワークでは、IGMPスヌーピングクエリーを有効にしないでください。IGMPスヌーピングクエリーは、IGMPクエリーの選定には参加しません。ただし、低い送信元IPアドレスを持つIGMP一般クエリーを送信する場合は、IGMPクエリーの選定に影響する可能性があります。IGMPクエリーの詳細については、「IGMPの設定」を参照してください。

VXLANネットワークでは、VSIのIGMPスヌーピングクエリーは、IGMP一般クエリーにVLANタグを含めません。ベストプラクティスとして、VSIでIGMPスヌーピングクエリーを有効にしないでください。

イーサネットアクセスモード。イーサネットアクセスモードの詳細については、「VXLAN設定ガイド」を参照してください。

VLANのIGMPスヌーピングクエリーの有効化

1. システムビューに入ります。

System-view

2. VLANビューを開始します。

vlan *vlan-id*

3. VLANのIGMPスヌーピングクエリーを有効にします。

igmp-snooping querier

デフォルトでは、VLANのIGMPスヌーピングクエリーは無効です。

VSIのIGMPスヌーピングクエリーの有効化

1. システムビューに入ります。

System-view

2. VSIビューを入力します。

vsi *vsi-name*

3. VSIのIGMPスヌーピングクエリーを有効にします。

igmp-snooping querier

デフォルトでは、VSIのIGMPスヌーピングクエリーは無効です。

IGMPスヌーピングクエリーア選定の有効化

IGMPスヌーピングクエリーアの選定について

VLANまたはVSI内の1つのクエリーアの障害によるトラフィックの中断を回避するには、VLANまたはVSI内に複数のクエリーアを設定し、クエリーアの選定を有効にします。選定されたクエリーアに障害が発生すると、デバイスはマルチキャスト転送を保証するために新しいクエリーアの選定を開始します。IGMPスヌーピングクエリーアの選定メカニズムは、IGMPクエリーアの選定メカニズムと同じです。IGMPクエリーアの選定の詳細については、「IGMPの設定」を参照してください。

IGMPスヌーピングクエリーア選定を有効にするための前提条件

IGMPスヌーピングクエリーア選定を有効にする前に、次の作業を完了する必要があります。

- VLANまたはVSIのIGMPスヌーピングクエリーアを有効にします。IGMPスヌーピングクエリーアの有効化の詳細については、「IGMPスヌーピングクエリーアの有効化」を参照してください。
- IGMPの一般的なクエリーの送信元IPアドレスを0.0.0.0およびローカルクエリーアのIPアドレス。IGMPスヌーピングクエリーアは、受信したIGMP一般クエリーの送信元IPアドレスが0.0.0.0または自身のIPアドレスでない場合にだけ、クエリーア選定を実行します。
- 候補IGMPスヌーピングクエリーアが同じIGMPスヌーピングバージョンを実行していることを確認します。IGMPスヌーピングバージョンを指定するには、**igmp-snooping version**コマンドを使用します。

VLANのIGMPスヌーピングクエリーア選定の有効化

1. システムビューに入ります。

System-view

2. VLANビューを開始します。

vlan *vlan-id*

3. VLANのIGMPスヌーピングクエリーア選定を有効にします。

igmp-snooping querier-election

デフォルトでは、VLANのIGMPスヌーピングクエリーア選定は無効です。

VSIのIGMPスヌーピングクエリーア選定の有効化

1. システムビューに入ります。

System-view

2. VSIビューを入力します。

vsi *vsi-name*

3. VSIのIGMPスヌーピングクエリーアの選択を有効にします。

igmp-snooping querier-election

デフォルトでは、VSIのIGMPスヌーピングクエリーア選択は無効です。

IGMP一般クエリーおよび応答のパラメータの設定

IGMP一般クエリーおよび応答のパラメータの概要

ネットワークの実際の状態に基づいて、IGMP一般クエリーインターバルを変更できます。

レシーバホストは、IGMP一般クエリーを受信すると、加入しているマルチキャストグループごとにレポート遅延タイマーを開始します。このタイマーは、0からクエリーでアドバタイズされる最大応答時間までの範囲のランダム値に設定されます。タイマー値が0に減少すると、ホストは対応するマルチキャストグループにIGMPレポートを送信します。

IGMP一般クエリーの最大応答時間に適切な値を設定して、IGMP一般クエリーに対するホストの応答を高速化し、IGMPレポートトラフィックのバーストを回避します。

制約事項とガイドライン

マルチキャストグループメンバーを誤って削除しないようにするには、IGMP一般クエリーインターバルをIGMP一般クエリーの最大応答時間よりも長くします。

IGMP一般クエリーおよび応答のグローバルなパラメータ設定

1. システムビューに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. IGMP一般クエリーの最大応答時間を設定します。

max-response-time seconds

デフォルトでは、IGMP一般クエリーの最大応答時間は10秒です。

VLAN上でのIGMP一般クエリーおよびレスポンスのパラメータ設定

1. システムビューに入ります。

System-view

2. VLANビューを開始します。

vlan vlan-id

3. VLANのIGMP一般クエリーインターバルを設定します。

igmp-snooping query-interval interval

デフォルトでは、VLANのIGMP一般クエリーインターバルは125秒です。

4. VLAN内のIGMP一般クエリーの最大応答時間を設定します。

igmp-snooping max-response-time seconds

デフォルトでは、VLANのIGMP一般クエリーの最大応答時間は10秒です。

VSIでのIGMP一般クエリーおよび応答のパラメータ設定

1. システムビューに入ります。

System-view

2. VSIビューを入力します。

vsivsi-name

3. VSIでIGMP一般クエリー間隔を設定します。

igmp-snooping query-interval interval

デフォルトでは、VSIのIGMP一般クエリー間隔は125秒です。

4. VSIでのIGMP一般クエリーの最大応答時間を設定します。

igmp-snooping max-response-time seconds

デフォルトでは、VSIのIGMP一般クエリーの最大応答時間は10秒です。

IGMPスヌーピングプロキシの有効化

1. システムビューに入ります。

System-view

2. VLANビューを開始します。

vlan vlan-id

3. VLANのIGMPスヌーピングプロキシを有効にします。

igmp-snoopingproxy enable

デフォルトでは、VLANのIGMPスヌーピングプロキシは無効です。

IGMPメッセージのパラメータの設定

IGMPメッセージの送信元IPアドレスの設定

IGMPメッセージの送信元IPアドレスの設定について

IGMPスヌーピングクエリは、送信元IPアドレス0. 0. 0. 0を使用してIGMP一般クエリを送信する場合があります。このようなクエリを受信するポートは、ダイナミックルータポートとして維持されません。これにより、関連付けられたダイナミックIGMPスヌーピング転送エントリがデータリンク層で正しく作成されなくなり、最終的にマルチキャストトラフィックの転送が失敗する可能性があります。この問題を回避するには、IGMPスヌーピングクエリアでIGMPクエリの送信元IPアドレスとしてすべてゼロ以外のIPアドレスを設定します。この設定は、サブネット内のIGMPクエリアの選定に影響する場合があります。

IGMPレポートの送信元IPアドレスを変更したり、シミュレートされたメンバーホストまたはIGMPスヌーピングプロキシから送信されたメッセージを残したりすることもできます。

VLANにおけるIGMPメッセージの送信元IPアドレスの設定

1. システムビューに入ります。

System-view

2. VLANビューを開始します。

vlan vlan-id

3. IGMP一般クエリの送信元IPアドレスを設定します。

igmp-snooping general-query source-ip ip-address

デフォルトでは、IGMP一般クエリの送信元IPアドレスは、現在のVLANインターフェイスのIPアドレスです。現在のVLANインターフェイスにIPアドレスがない場合、送信元IPアドレスは0.0.0.0になります。

4. IGMPグループ固有クエリの送信元IPアドレスを設定します。

igmp-snooping special-query source-ip ip-address

デフォルトでは、IGMPグループ固有クエリーの送信元IPアドレスは次のいずれかです。

- VLANのIGMPスヌーピングクエリアがIGMP一般クエリーを受信した場合のIGMPグループ固有クエリーの送信元アドレス。
- IGMPスヌーピングクエリアがIGMP一般クエリーを受信しない場合の、現在のVLANインターフェイスのIPアドレス。
- IGMPスヌーピングクエリアがIGMP一般クエリーを受信せず、現在のVLANインターフェイスにIPアドレスがない場合は、0.0.0.0。

5. IGMPレポートの送信元IPアドレスを設定します。

igmp-snooping report source-ip *ip-address*

デフォルトでは、IGMPレポートの送信元IPアドレスは、現在のVLANインターフェイスのIPアドレスです。現在のVLANインターフェイスにIPアドレスが設定されていない場合、送信元IPアドレスは0.0.0.0になります。

6. IGMP Leaveメッセージの送信元IPアドレスを設定します。

igmp-snooping leave source-ip *ip-address*

デフォルトでは、IGMP Leaveメッセージの送信元IPアドレスは、現在のVLANインターフェイスのIPアドレスです。現在のVLANインターフェイスにIPアドレスがない場合、送信元IPアドレスは0.0.0.0になります。

VSIIにおけるIGMPメッセージの送信元IPアドレスの設定

1. システムビューに入ります。

System-view

2. VSIビューを入力します。

vsi *vsi-name*

3. IGMP一般クエリーの送信元IPアドレスを設定します。

igmp-snooping general-query source-ip *ip-address*

デフォルトでは、IGMP一般クエリーの送信元IPアドレスは、VSIのゲートウェイインターフェイスのIPアドレスです。ゲートウェイインターフェイスにIPアドレスがない場合、送信元IPアドレスは0.0.0.0になります。

4. IGMPグループ固有クエリーの送信元IPアドレスを設定します。

igmp-snooping special-query source-ip *ip-address*

デフォルトでは、IGMPグループ固有クエリーの送信元IPアドレスは次のいずれかです。

- VSIのIGMPスヌーピングクエリアがIGMP一般クエリーを受信した場合のIGMP一般クエリーの送信元IPアドレス。
- IGMPスヌーピングクエリアがIGMP一般クエリーを受信しない場合のVSIのゲートウェイインターフェイスのIPアドレス。
- VSIのゲートウェイインターフェイスにIPアドレスがない場合は0.0.0.0。

5. IGMPレポートの送信元IPアドレスを設定します。

igmp-snooping report source-ip *ip-address*

デフォルトでは、IGMPレポートの送信元IPアドレスは、VSIのゲートウェイインターフェイスのIPアドレスです。ゲートウェイインターフェイスにIPアドレスがない場合、送信元IPアドレスは0.0.0.0になります。

6. IGMP Leaveメッセージの送信元IPアドレスを設定します。

igmp-snooping leave source-ip *ip-address*

デフォルトでは、IGMP Leaveメッセージの送信元IPアドレスは、VSIのゲートウェイインターフェイスのIPアドレスです。ゲートウェイインターフェイスにIPアドレスがない場合、送信元IPアドレスは0.0.0.0です。

IGMPメッセージの802.1pプライオリティの設定

IGMPメッセージの802.1pプライオリティについて

レイヤ2デバイスの出力ポートで輻輳が発生した場合、レイヤ2デバイスは802.1pプライオリティの高い順にIGMPメッセージをフォワーディングします。デバイスによって作成またはフォワーディングされたIGMPメッセージにより高い802.1pプライオリティを割り当てることができます。

制約事項とガイドライン

IGMPスヌーピングビューの設定は、すべてのVLANに対してのみ有効です。VSIの場合、VSIビューでのみIGMPメッセージの802.1pプライオリティを設定できます。

IGMPメッセージのグローバルな802.1pプライオリティの設定

1. システムビューに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. IGMPメッセージの802.1pプライオリティを設定します。

dot1p-priority priority

VLAN内のIGMPメッセージの802.1pプライオリティの設定

1. システムビューに入ります。

System-view

2. VLANビューを開始します。

vlan vlan-id

3. VLAN内のIGMPメッセージに802.1pプライオリティを設定します。

igmp-snooping dot1p-priority priority

IGMPスヌーピングポリシーの設定

マルチキャストグループポリシーの設定

マルチキャストグループポリシーについて

この機能により、レイヤ2デバイスは、マルチキャストグループとオプションの送信元を指定するACLを使用して、IGMPレポートをフィルタリングできます。これは、ホストが加入できるマルチキャストグループを制御するために使用されます。この設定は、ポートが動的に加入するマルチキャストグループに対してのみ有効です。

マルチキャストアプリケーションでは、ユーザーがマルチキャストプログラムを要求すると、ホストは非送信請求IGMPレポートを送信します。レイヤ2デバイスは、マルチキャストグループポリシーを使用してIGMPレポートをフィルタリングします。ホストがマルチキャストグループに加入できるのは、IGMPレポー

トがマルチキャストグループポリシーによって許可されている場合だけです。

マルチキャストグループポリシーのグローバルな設定

1. システムビューに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. マルチキャストグループポリシーをグローバルに設定します。

group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

デフォルトでは、マルチキャストグループポリシーは設定されておらず、ホストはどのマルチキャストグループにも加入できません。

ポート上のマルチキャストグループポリシーの設定

1. システムビューに入ります。

System-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface *interface-type interface-number*

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation *interface-number*

3. ポート上でマルチキャストグループポリシーを設定します。

igmp-snooping group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

デフォルトでは、ポート上にマルチキャストグループポリシーは設定されておらず、ポートに接続されたホストは任意のマルチキャストグループに加入できます。

マルチキャスト送信元ポートフィルタリングの有効化

マルチキャスト送信元ポートフィルタリングについて

この機能により、レイヤ2デバイスはすべてのマルチキャストデータパケットを廃棄し、マルチキャストプロトコルパケットを受け入れることができます。この機能は、マルチキャストレシーバだけに接続するポートで有効にできます。

制約事項とガイドライン

マルチキャスト送信元ポートフィルタリングが有効の場合、システムは自動的にIPv6マルチキャスト送信元ポートフィルタリングを有効にします。

IGMPスヌーピングビューで複数のインターフェイスに対して作成された設定は、インターフェイス固有の設定と同じプライオリティを持ち、最新の設定が有効になります。

IGMPスヌーピングビューでのマルチキャスト送信元ポートフィルタリングの有効化

1. システムビューに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. マルチキャスト送信元ポートフィルタリングを有効にします。

source-deny port *interface-list*

デフォルトでは、マルチキャスト送信元ポートのフィルタリングは無効です。

インターフェイスビューでのマルチキャスト送信元ポートフィルタリングの有効化

1. システムビューに入ります。

System-view

2. レイヤ2イーサネットインターフェイスビューを開始します。

interface *interface-type interface-number*

3. マルチキャスト送信元ポートフィルタリングを有効にします。

igmp-snooping source-deny

デフォルトでは、マルチキャスト送信元ポートのフィルタリングは無効です。

不明なマルチキャストデータの破棄の有効化

不明なマルチキャストデータのドロップについて

不明なマルチキャストデータとは、IGMPスヌーピング転送テーブルに転送エントリが存在しないマルチキャストデータのことです。この機能を使用すると、デバイスは不明なマルチキャストデータをルータポートだけに転送できます。デバイスにルータポートがない場合、不明なマルチキャストデータはドロップされます。

この機能を有効にしない場合、不明なマルチキャストデータは、データが属するVLANまたはVSIでフラグディングされます。

制約事項とガイドライン

不明なIPv4マルチキャストデータのドロップが有効の場合、デバイスは不明なIPv6マルチキャストデータもドロップします。

不明なマルチキャストデータの廃棄が有効の場合、デバイスは、受信側ルータポート以外のルータポートから不明なマルチキャストデータを転送します。

VLANの不明なマルチキャストデータの破棄の有効化

1. システムビューに入ります。

System-view

2. VLANビューを開始します。

vlan *vlan-id*

3. VLANの不明なマルチキャストデータの廃棄を有効にします。

igmp-snooping drop-unknown

デフォルトでは、VLANの不明なマルチキャストデータの廃棄は無効です。不明なマルチキャストデータはVLANでフラッディングされます。

VSIの不明なマルチキャストデータのドロップの有効化

1. システムビューに入ります。

System-view

2. VSIビューを入力します。

vsi vsi-name

3. VSIの不明なマルチキャストデータのドロップを有効にします。

igmp-snooping drop-unknown

デフォルトでは、VSIの不明なマルチキャストデータのドロップは無効です。不明なマルチキャストデータは、VSIでフラッディングされます。

IGMPレポート抑制の有効化

IGMPレポート抑制の概要

この機能を使用すると、レイヤ2デバイスは、マルチキャストグループの最初のIGMPレポートだけを、直接接続されたレイヤ3デバイスに転送できます。同じクエリーテーブル内の同じグループの他のレポートは廃棄されます。この機能は、マルチキャストトラフィックを削減するために使用します。

手順

1. システムビューに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. IGMPレポート抑制を有効にします。

report-aggregation

デフォルトでは、IGMPレポート抑制は有効です。

ポート上のマルチキャストグループの最大数の設定

ポート上のマルチキャストグループの最大数の設定について

ポート上のマルチキャストグループの最大数を設定して、ポートトラフィックを制御できます。この設定は、ポートがダイナミックに加入するマルチキャストグループに対してだけ有効です。

ポート上のマルチキャストグループの数が制限を超えると、システムはそのポートに関連付けられたすべての転送エントリを削除します。そのポートに接続されたレシーバホストは、ポート上のマルチキャストグループの数が制限に達する前に、再びマルチキャストグループに参加できます。

手順

1. システムビューに入ります。

System-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface *interface-type interface-number*

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation *interface-number*

3. ポート上のマルチキャストグループの最大数を設定します。

igmp-snooping group-limit *limit* [**vlan** *vlan-list*]

デフォルトでは、ポート上のマルチキャストグループの最大数に制限はありません。

マルチキャストグループ置換の有効化

マルチキャストグループの置換について

この機能を使用すると、レイヤ2デバイスは、グループ番号が上限を超えた場合に、最小のIPアドレスを持つ既存のグループを新しく加入したグループに置き換えることができます。この機能は通常、チャンネルスイッチングアプリケーションで使用されます。この機能がない場合、デバイスは新しいグループのIGMPレポートを破棄し、ユーザーは新しいチャンネルに変更できません。

制約事項とガイドライン

この設定は、ポートがダイナミックに加入するマルチキャストグループに対してだけ有効です。

マルチキャストグループ置換のグローバルな有効化

1. システムビューに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. マルチキャストグループ置換をグローバルに有効にします。

overflow-replace [vlan vlan-list]

デフォルトでは、マルチキャストグループ置換はグローバルに無効になっています。

ポート上のマルチキャストグループ置換の有効化

1. システムビューに入ります。

System-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface interface-type interface-number

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation interface-number

3. ポート上でマルチキャストグループ置換を有効にします。

igmp-snooping overflow-replace [vlan vlan-list]

デフォルトでは、マルチキャストグループ置換はポートで無効になっています。

ホストトラッキングの有効化

ホストトラッキングについて

この機能を使用すると、レイヤ2デバイスは、マルチキャストデータを受信しているメンバーホストに関する情報を記録できます。この情報には、ホストのIPアドレス、ホストがマルチキャストグループに加入してから経過時間、およびホストの残りのタイムアウト時間が含まれます。この機能により、メンバーホストの監視と管理が容易になります。

制約事項とガイドライン

グローバル設定は、VSIでは有効になりません。

ホストトラッキングのグローバルな有効化

1. システムビューに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. ホストトラッキングをグローバルに有効にします。

host-tracking

デフォルトでは、ホストトラッキングはグローバルに無効です。

VLANのホストトラッキングの有効化

1. システムビューに入ります。

System-view

2. VLANビューを開始します。

vlan vlan-id

3. VLANのホストトラッキングを有効にします。

igmp-snooping host-tracking

デフォルトでは、VLANのホストトラッキングは無効です。

発信IGMPスヌーピングプロトコルパケットのDSCP値の設定

発信IGMPスヌーピングプロトコルパケットのDSCP値について

DSCP値は、パケット送信の優先順位を決定します。DSCP値が大きいほど、優先順位が高くなります。

手順

1. システムビューに入ります。

System-view

2. IGMPスヌーピングビューを開始します。

igmp-snooping

3. 発信IGMPスヌーピングプロトコルパケットのDSCP値を設定します。

dscp dscp-value

デフォルトでは、発信IGMPスヌーピングプロトコルパケットのDSCP値は48です。

IGMPスヌーピングの表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
IGMPスヌーピングステータスを表示します。	display igmp-snooping [global vlan <i>vlan-id</i> vsi <i>vsi-name</i>]
ダイナミックIGMPスヌーピンググループエントリを表示します。	display igmp-snooping group [<i>group-address</i> <i>source-address</i>] * [vlan <i>vlan-id</i> vsi <i>vsi-name</i>] [interface <i>interface-type</i> <i>interface-number</i> [verbose] [slot <i>slot-number</i>]]
ホストトラッキング情報を表示します。	display igmp-snooping host-tracking vlan <i>vlan-id</i> group <i>group-address</i> [source <i>source-address</i>] [slot <i>slot-number</i>]
ダイナミックルータポート情報を表示します。	display igmp-snooping router-port [vlan <i>vlan-id</i> vsi <i>vsi-name</i>] [verbose] [slot <i>slot-number</i>]
スタティックIGMPスヌーピンググループエントリを表示します。	display igmp-snooping static-group [<i>group-address</i> <i>source-address</i>] * [vlan <i>vlan-id</i>] [verbose] [slot <i>slot-number</i>]
スタティックルータポート情報を表示します。	display igmp-snooping static-router-port [vlan <i>vlan-id</i>] [verbose] [slot <i>slot-number</i>]
IGMPスヌーピングによって学習されたIGMPメッセージおよびPIMv2 helloメッセージの統計情報を表示します。	display igmp-snooping statistics
レイヤ2マルチキャスト高速フォワーディングエントリを表示します。	display l2-multicast fast-forwarding cache [vlan <i>vlan-id</i>] [<i>source-address</i> <i>group-address</i>] * [slot <i>slot-number</i>]
レイヤ2 IPマルチキャストグループに関する情報を表示します。	display l2-multicast ip [group <i>group-address</i> source <i>source-address</i>] * [vlan <i>vlan-id</i> vsi <i>vsi-name</i>] [slot <i>slot-number</i>]
レイヤ2 IPマルチキャストグループエントリを表示します。	display l2-multicast ip forwarding [group <i>group-address</i> source <i>source-address</i>] * [vlan <i>vlan-id</i> vsi <i>vsi-name</i>] [slot <i>slot-number</i>]

レイヤ2 MACマルチキャストグループに関する情報を表示します。	display l2-multicast mac [<i>mac-address</i>] [vlan <i>vlan-id</i> vsi <i>vsi-name</i>] [slot <i>slot-number</i>]
レイヤ2 MACマルチキャストグループエントリを表示します。	display l2-multicast mac forwarding [<i>mac-address</i>] [vlan <i>vlan-id</i> vsi <i>vsi-name</i>] [slot <i>slot-number</i>]
スタティックマルチキャストMACアドレスエントリを表示します。	display mac-address [<i>mac-address</i> [vlan <i>vlan-id</i>] [multicast] [vlan <i>vlan-id</i>] [count]]
ダイナミックIGMPスヌーピンググループエントリをクリアします。	reset igmp-snooping group { <i>group-address</i> [<i>source-address</i>] all } [vlan <i>vlan-id</i> vsi <i>vsi-name</i>]
ダイナミックルータのポート情報をクリアします。	reset igmp-snooping router-port { all vlan <i>vlan-id</i> vsi <i>vsi-name</i> }
IGMPスヌーピングによって学習されたIGMPメッセージおよびPIMv2 helloメッセージの統計情報をクリアします。	reset igmp-snooping statistics
レイヤ2マルチキャスト高速フォワーディングエントリをクリアします。	reset l2-multicast fast-forwarding cache [vlan <i>vlan-id</i>] { { <i>source-address</i> <i>group-address</i> } * all } [slot <i>slot-number</i>]

IGMPスヌーピングの設定例

例:VLANベースのIGMPスヌーピンググループポリシーおよびシミュレートされた加入の設定

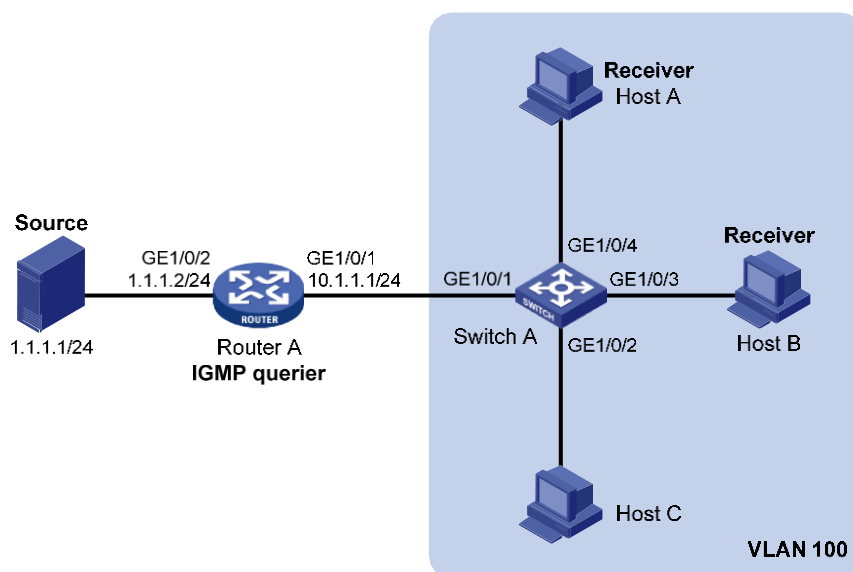
ネットワークの設定

図13に示すように、ルータAはIGMPv2を実行し、IGMPクエリャーとして機能します。スイッチAはIGMPv2スヌーピングを実行します。

次の要件を満たすように、マルチキャストグループポリシーとシミュレートされた参加を設定します。

- ホストAおよびホストBは、マルチキャストグループ224.1.1.1宛てのマルチキャストデータだけを受信します。ホストAおよびホストBがマルチキャストデータの受信に失敗した場合でも、スイッチAのGigabitEthernet 1/0/3およびGigabitEthernet 1/0/4を介して、マルチキャストデータを継続的に転送できます。
- スイッチAは、不明なマルチキャストデータをVLAN 100にフラッディングせずに廃棄します。

図13 ネットワークダイアグラム



手順

1. 図13に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
2. ルータAを設定します。

```
# Enable IP multicast routing.  
<RouterA> system-view  
[RouterA] multicast routing  
[RouterA-mrib] quit
```

Enable IGMP on GigabitEthernet 1/0/1.

```
[RouterA] interface gigabitethernet 1/0/1
```

```
[RouterA-GigabitEthernet1/0/1] igmp enable
```

```
[RouterA-GigabitEthernet1/0/1] quit
```

Enable PIM-DM on GigabitEthernet 1/0/2.

```
[RouterA] interface gigabitethernet 1/0/2
```

```
[RouterA-GigabitEthernet1/0/2] pim dm
```

```
[RouterA-GigabitEthernet1/0/2] quit
```

3. スイッチAを設定します。

Enable the IGMP snooping feature.

```
<SwitchA> system-view
```

```
[SwitchA] igmp-snooping
```

```
[SwitchA-igmp-snooping] quit
```

Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the VLAN.

```
[SwitchA] vlan 100
```

```
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Enable IGMP snooping, and enable dropping unknown multicast data for VLAN 100.

```
[SwitchA-vlan100] igmp-snooping enable
```

```
[SwitchA-vlan100] igmp-snooping drop-unknown
```

```
[SwitchA-vlan100] quit
```

Configure a multicast group policy so that hosts in VLAN 100 can join only multicast group 224.1.1.1.

```
[SwitchA] acl basic 2001
```

```
[SwitchA-acl-ipv4-basic-2001] rule permit source 224.1.1.1 0
```

```
[SwitchA-acl-ipv4-basic-2001] quit
```

```
[SwitchA] igmp-snooping
```

```
[SwitchA-igmp-snooping] group-policy 2001 vlan 100
```

```
[SwitchA-igmp-snooping] quit
```

Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 as simulated member hosts of multicast group 224.1.1.1.

```
[SwitchA] interface gigabitethernet 1/0/3
```

```
[SwitchA-GigabitEthernet1/0/3] igmp-snooping host-join 224.1.1.1 vlan 100
```

```
[SwitchA-GigabitEthernet1/0/3] quit
```

```
[SwitchA] interface gigabitethernet 1/0/4
```

```
[SwitchA-GigabitEthernet1/0/4] igmp-snooping host-join 224.1.1.1 vlan 100
```

```
[SwitchA-GigabitEthernet1/0/4] quit
```

設定の確認

#ホストAおよびホストBからIGMPレポートを送信し、マルチキャストグループ224.1.1.1および224.2.2.2に参加します(詳細は省略)。

#スイッチA上のVLAN 100のダイナミックIGMPスヌーピンググループエントリを表示します。

```
[SwitchA] display igmp-snooping group vlan 100
```

```
Total 1 entries.
```

VLAN 100: Total 1 entries.

(0.0.0.0, 224.1.1.1)

Host ports (2 in total):

GE1/0/3

(00:03:23)

GE1/0/4

(00:04:10)

出力には次の情報が表示されます。

- ホストAおよびホストBは、それぞれスイッチA上のメンバーポートGigabitEthernet 1/0/4およびGigabitEthernet 1/0/3を介して、マルチキャストグループ224.1.1.1に加入しています。
- ホストAおよびホストBは、マルチキャストグループ224.2.2.2への加入に失敗しました。

例:VLANベースのIGMPスヌーピングスタティックポートの設定

ネットワークの設定

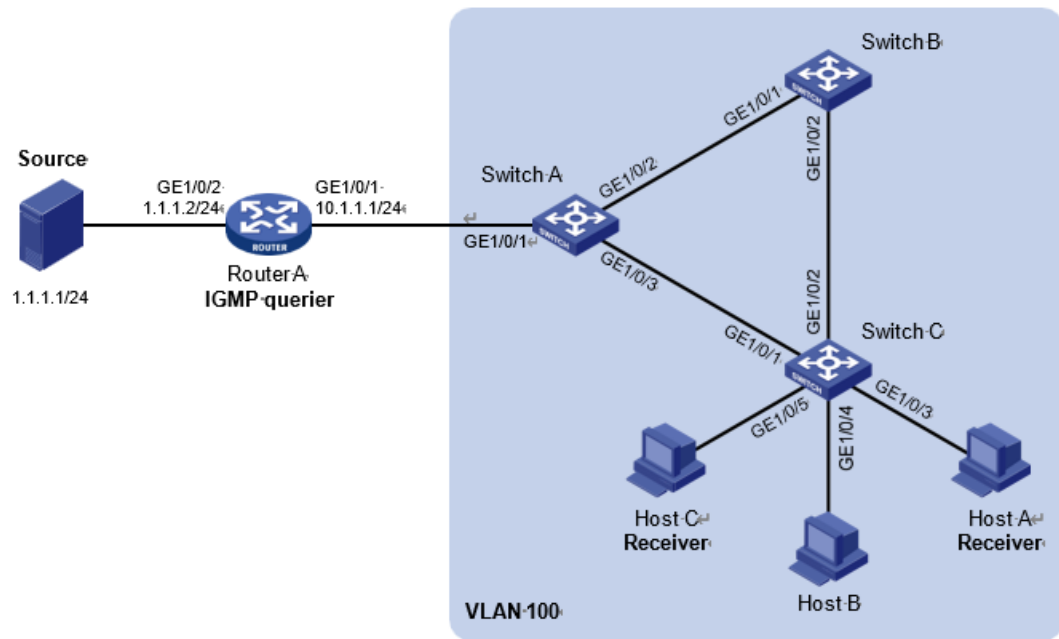
図14に示します。

- ルータAはIGMPv2を実行し、IGMPクエリアとして動作します。スイッチA、スイッチB、およびスイッチCは、IGMPv2スヌーピングを実行します。
- ホストAとホストCは、マルチキャストグループ224.1.1.1の永続的なレシーバです。次の要件を満たすようにスタティックポートを設定します。
- マルチキャストトラフィック伝送の信頼性を高めるには、GigabitEthernet 1/0/3およびスイッチC上のGigabitEthernet 1/0/5をマルチキャストグループ224.1.1.1のスタティックメンバーポートとして設定します。
- STPがネットワーク上で動作していると仮定します。データループを回避するために、スイッチAからスイッチCへの転送パスはブロックされます。マルチキャストデータは、スイッチA、スイッチB、スイッチCのパスに沿ってのみ、スイッチCに接続されたレシーバに流れます。このパスがブロックされると、少なくとも1つのIGMP

マルチキャストデータがスイッチAスイッチCのパスに沿ってレシーバに流れる前に、query-responseサイクルが完了する必要があります。この場合、マルチキャスト配信はプロセス中に中断されます。STPの詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

スイッチAのGigabitEthernet 1/0/3をスタティックルータポートとして設定します。これにより、スイッチAスイッチBスイッチCのパスがブロックされた場合でも、マルチキャストデータをスイッチAスイッチCのパスに沿ってほぼ中断なくレシーバに流すことができます。

図14 ネットワークダイアグラム



手順

1. 図14に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)

2. ルータAを設定します。

Enable IP multicast routing.

```
<RouterA> system-view
```

```
[RouterA] multicast routing
```

```
[RouterA-mrib] quit
```

Enable IGMP on GigabitEthernet 1/0/1.

```
[RouterA] interface gigabitethernet 1/0/1
```

```
[RouterA-GigabitEthernet1/0/1] igmp enable
```

```
[RouterA-GigabitEthernet1/0/1] quit
```

Enable PIM-DM on GigabitEthernet 1/0/2.

```
[RouterA] interface gigabitethernet 1/0/2
```

```
[RouterA-GigabitEthernet1/0/2] pim dm
```

```
[RouterA-GigabitEthernet1/0/2] quit
```

3. スイッチAを設定します。

Enable the IGMP snooping feature.

```
<SwitchA> system-view
```

```
[SwitchA] igmp-snooping
```

```
[SwitchA-igmp-snooping] quit
```

Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet1/0/3 to the VLAN.

```
[SwitchA] vlan 100
```

```
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

```
# Enable IGMP snooping for VLAN 100.
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit
# Configure GigabitEthernet 1/0/3 as a static router port.
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

4. スイッチBを構成します。

```
# Enable the IGMP snooping feature.
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
# Create VLAN 100, and assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the VLAN.
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
# Enable IGMP snooping for VLAN 100
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

5. スイッチCを設定します。

```
# Enable the IGMP snooping feature.
<SwitchC> system-view
[SwitchC] igmp-snooping
[SwitchC-igmp-snooping] quit
# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to the VLAN.
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
# Enable IGMP snooping for VLAN 100.
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] quit
# Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 as static member ports for multicast group 224.1.1.1.
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
[SwitchC] interface gigabitethernet 1/0/5
[SwitchC-GigabitEthernet1/0/5] igmp-snooping static-group 224.1.1.1 vlan 100
[SwitchC-GigabitEthernet1/0/5] quit
```

設定の確認

#スイッチAのVLAN 100のスタティックルータポート情報を表示します。

```
[SwitchA] display igmp-snooping static-router-port vlan 100
VLAN 100:
```

Router ports (1 in total):

GE1/0/3

The output shows that GigabitEthernet 1/0/3 on Switch A has become a static router port. # Display static IGMP snooping group entries for VLAN 100 on Switch C.
[SwitchC] display igmp-snooping static-group vlan 100
Total 1 entries.

VLAN 100: Total 1 entries.
(0.0.0.0, 224.1.1.1)
Host ports (2 in total):
GE1/0/3
GE1/0/5

この出力は、スイッチCのGigabitEthernet 1/0/3およびGigabitEthernet 1/0/5がマルチキャストグループ 224.1.1.1のスタティックメンバーポートになったことを示しています。

例:VLANベースのIGMPスヌーピングクエリアの設定

ネットワークの設定

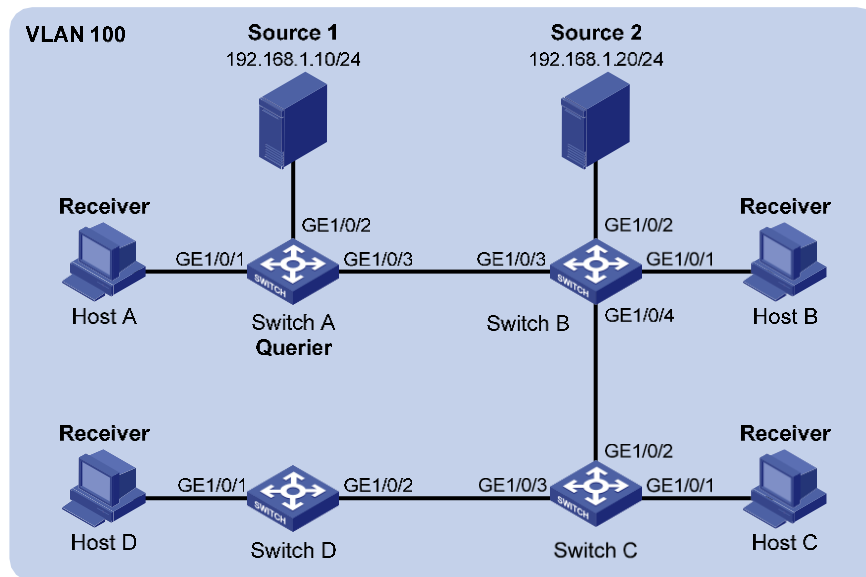
図15に示します。

- ネットワークはレイヤ2だけのネットワークです。
- 送信元1および送信元2は、それぞれマルチキャストグループ224.1.1.1および225.1.1.1にマルチキャストデータを送信します。
- ホストAとホストCはマルチキャストグループ224.1.1.1のレシーバであり、ホストBとホストDはマルチキャストグループ225.1.1.1のレシーバです。
- すべてのホストレシーバはIGMPv2を実行し、すべてのスイッチはIGMPv2スヌーピングを実行します。スイッチA(マルチキャスト送信元に近い)は、IGMPスヌーピングクエリアとして機能します。

次の要件を満たすようにスイッチを設定します。

- スイッチがVLAN内の不明なデータをフラッディングしないようにするには、すべてのスイッチで不明なマルチキャストデータを廃棄できるようにします。
- スイッチは、送信元IPアドレス0.0.0.0のIGMPクエリーを受信したポートをダイナミックルータポートとしてマークしません。これは、レイヤ2転送エントリの確立とマルチキャストトラフィック転送に悪影響を及ぼします。これを回避するには、IGMPクエリーの送信元IPアドレスを0以外のIPアドレスとして設定します。

図15 ネットワークダイアグラム



手順

1. スイッチAを設定します。

Enable the IGMP snooping feature.

```
<SwitchA> system-view
```

```
[SwitchA] igmp-snooping
```

```
[SwitchA-igmp-snooping] quit
```

Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to the VLAN.

```
[SwitchA] vlan 100
```

```
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

Enable IGMP snooping, and enable dropping unknown multicast data for VLAN 100.

```
[SwitchA-vlan100] igmp-snooping enable
```

```
[SwitchA-vlan100] igmp-snooping drop-unknown
```

Configure Switch A as the IGMP snooping querier.

```
[SwitchA-vlan100] igmp-snooping querier
```

```
[SwitchA-vlan100] quit
```

In VLAN 100, specify 192.168.1.1 as the source IP address of IGMP general queries.

```
[SwitchA-vlan100] igmp-snooping general-query source-ip 192.168.1.1
```

In VLAN 100, specify 192.168.1.1 as the source IP address of IGMP group-specific queries.

```
[SwitchA-vlan100] igmp-snooping special-query source-ip 192.168.1.1
```

```
[SwitchA-vlan100] quit
```

2. スイッチBを構成します。

Enable the IGMP snooping feature.

```
<SwitchB> system-view
```

```
[SwitchB] igmp-snooping
```

```
[SwitchB-igmp-snooping] quit
```

Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the VLAN.


```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
# Enable IGMP snooping, and enable dropping unknown multicast data for VLAN 100.
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] igmp-snooping drop-unknown
[SwitchB-vlan100] quit
```

3. スイッチCを設定します。

```
# Enable the IGMP snooping feature.
<SwitchC> system-view
[SwitchC] igmp-snooping
[SwitchC-igmp-snooping] quit
# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to the
VLAN.
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
# Enable IGMP snooping, and enable dropping unknown multicast data for VLAN 100.
[SwitchC-vlan100] igmp-snooping enable
[SwitchC-vlan100] igmp-snooping drop-unknown
[SwitchC-vlan100] quit
```

4. スイッチDを構成します。

```
# Enable the IGMP snooping feature.
<SwitchD> system-view
[SwitchD] igmp-snooping
[SwitchD-igmp-snooping] quit
# Create VLAN 100, and assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the VLAN.
[SwitchD] vlan 100
[SwitchD-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
# Enable IGMP snooping, and enable dropping unknown multicast data for VLAN 100.
[SwitchD-vlan100] igmp-snooping enable
[SwitchD-vlan100] igmp-snooping drop-unknown
[SwitchD-vlan100] quit
```

設定の確認

#スイッチBのIGMPスヌーピングを通じて学習されたIGMPメッセージおよびPIMv2 helloメッセージの統計情報を表示します。

```
[SwitchB] display igmp-snooping statistics
Received IGMP general queries: 3
Received IGMPv1 reports: 0
Received IGMPv2 reports: 12
Received IGMP leaves: 0
Received IGMPv2 specific queries: 0
Sent IGMPv2 specific queries: 0
Received IGMPv3 reports: 0
Received IGMPv3 reports with right and wrong records:0
Received IGMPv3 specific queries: 0
```

Received IGMPv3 specific sg queries: 0
Sent IGMPv3 specific queries: 0
Sent IGMPv3 specific sg queries: 0
Received PIMv2 hello: 0
Received error IGMP messages: 0

この出力は、スイッチAがIGMPスヌーピングクエリアとして動作した後、スイッチAを除くすべてのスイッチがIGMP一般クエリーを受信できることを示しています。

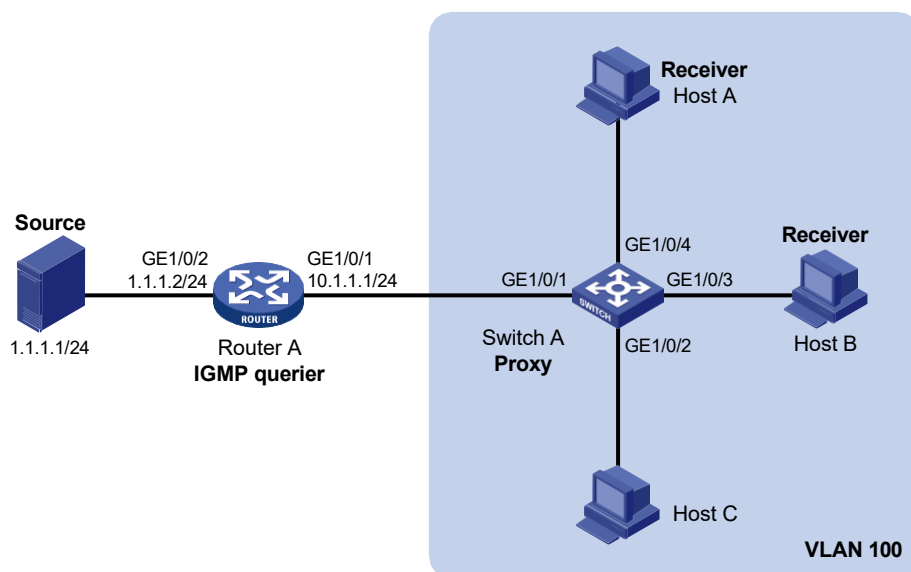
例:VLANベースのIGMPスヌーピングプロキシの設定

ネットワークの設定

図16に示すように、ルータAはIGMPv2を実行し、IGMPクエリアとして動作します。スイッチAはIGMPv2スヌーピングを実行します。スイッチAが次のアクションを実行できるように、IGMPスヌーピングプロキシを設定します。

- IGMPレポートおよびリーブメッセージをルータAに転送します。
- ルータAから送信されたIGMPクエリーに応答し、そのクエリーをダウンストリームホストに転送します。

図16 ネットワークダイアグラム



手順

1. 図16に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)

2. ルータAを設定します。

```
# Enable IP multicast routing.
```

```
<RouterA> system-view
```

```
[RouterA] multicast routing
```

```
[RouterA-mrib] quit
```

Enable IGMP and PIM-DM on GigabitEthernet 1/0/1.

```
[RouterA] interface gigabitethernet 1/0/1
```

```
[RouterA-GigabitEthernet1/0/1] igmp enable
```

```
[RouterA-GigabitEthernet1/0/1] pim dm
```

```
[RouterA-GigabitEthernet1/0/1] quit
```

Enable PIM-DM on GigabitEthernet 1/0/2.

```
[RouterA] interface gigabitethernet 1/0/2
```

```
[RouterA-GigabitEthernet1/0/2] pim dm
```

```
[RouterA-GigabitEthernet1/0/2] quit
```

3. スイッチAを設定します。

Enable the IGMP snooping feature.

```
<SwitchA> system-view
```

```
[SwitchA] igmp-snooping
```

```
[SwitchA-igmp-snooping] quit
```

Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the VLAN.

```
[SwitchA] vlan 100
```

```
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Enable IGMP snooping and IGMP snooping proxying for the VLAN.

```
[SwitchA-vlan100] igmp-snooping enable
```

```
[SwitchA-vlan100] igmp-snooping proxy enable
```

```
[SwitchA-vlan100] quit
```

設定の確認

#ホストAおよびホストBからIGMPレポートを送信し、マルチキャストグループ224.1. 1. 1および224.1. 1. 1に参加します(詳細は省略)。

#スイッチA上のIGMPスヌーピンググループエントリに関する要約情報を表示します。

```
[SwitchA] display igmp-snooping group
```

Total 1 entries.

VLAN 100: Total 1 entries.

(0.0.0.0, 224.1.1.1)

Host ports (2 in total):

GE1/0/3	(00:04:00)

GE1/0/4	(00:04:04)

この出力は、GigabitEthernet 1/0/3およびGigabitEthernet 1/0/4がマルチキャストグループ224.1. 1. 1のメンバーポートであることを示しています。ホストAおよびホストBがグループのレシーバになります。

#ルータAのIGMPグループメンバーシップ情報を表示します。

```
[RouterA] display igmp group
```

IGMP groups in total: 1

GigabitEthernet1/0/1(10.1.1.1):

IGMP groups reported in total: 1

Group address	Last reporter	Uptime	Expires
224.1.1.1	0.0.0.0	00:00:31	00:02:03

#ホストAからIGMP Leaveメッセージを送信して、マルチキャストグループ224.1. 1. 1を脱退させます。

(詳細は省略)#スイッチA上のIGMPスヌーピンググループエントリに関する簡単な情報を表示します。

```
[SwitchA] display igmp-snooping group
```

Total 1 entries.

VLAN 100: Total 1 entries.

(0.0.0.0, 224.1.1.1)

Host ports (1 in total):

GE1/0/3

(00:01:23)

この出力は、GigabitEthernet 1/0/3がマルチキャストグループ224.1. 1. 1の唯一のメンバーポートであることを示しています。ホストBだけがグループのレシーバとして残ります。

例:VXLANベースのIGMPスヌーピングの設定

ネットワークの設定

図17に示します。

- VXLAN 10は、ネットワークサイト間でVM 1、VM 2、およびVM 3にレイヤ2接続を提供します。
- VXLAN 10は、トラフィックのフラッディングにユニキャストモードを使用します。

レイヤ2マルチキャスト転送を実装し、VXLAN 10のVTEPに既知のマルチキャストトラフィックを複製する負荷を軽減するには、スイッチにIGMPスヌーピングを設定します。

図17 ネットワーク図

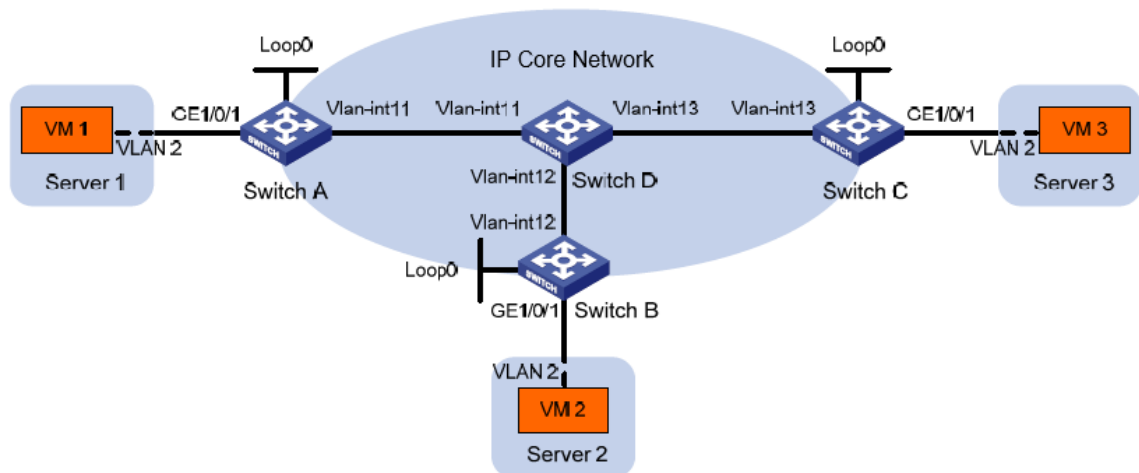


表6インターフェイスとIPアドレスの割り当て

デバイス	インターフェイス	IPアドレス	デバイス	インターフェイス	IPアドレス
Switch A	VLAN- int11	11.1.1.1/24	Switch C	VLAN- int13	13.1.1.3/24
Switch A	Loop0	1.1.1.1/32	Switch C	Loop0	3.3.3.3/32
Switch B	VLAN- int12	12.1.1.2/24	Switch D	VLAN- int11	11.1.1.4/24
Switch B	Loop0	2.2.2.2/32	Switch D	VLAN- int12	12.1.1.4/24
			Switch D	VLAN-int13	13.1.1.4/24

手順

1. 表6に示すように、トランスポートネットワーク上の各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
2. 転送ネットワーク内のすべてのスイッチにOSPFを設定します(詳細は省略)。
3. スイッチAを設定します。

Enable L2VPN.

```
<SwitchA> system-view
```

```
[SwitchA] l2vpn enable
```

Enable Layer 2 forwarding for VXLANs.

```
[SwitchA] undo vxlan ip-forwarding
```

Create a VSI named **vpna**, and create VXLAN 10.

```
[SwitchA] vsi vpna
```

```
[SwitchA-vsi-vpna] vxlan 10
```

```
[SwitchA-vsi-vpna-vxlan-10] quit
```

```
[SwitchA-vsi-vpna] quit
```

Enable the IGMP snooping feature.

```
[SwitchA] igmp-snooping
```

```
[SwitchA-igmp-snooping] quit
```

Enable IGMP snooping and dropping unknown multicast data packets for VSI **vpna**.

```
[SwitchA] vsi vpna
```

```
[SwitchA-vsi-vpna] igmp-snooping enable
```

```
[SwitchA-vsi-vpna] igmp-snooping drop-unknown
```

```
[SwitchA-vsi-vpna] quit
```

Assign an IP address to Loopback 0. This IP address will be used as the source address of the VXLAN tunnels to Switch B and Switch C.

```
[SwitchA] interface loopback 0
```

```
[SwitchA-Loopback0] ip address 1.1.1.1 255.255.255.255
```

```
[SwitchA-Loopback0] quit
```

Create a VXLAN tunnel to Switch B.

- The tunnel interface name is **Tunnel 1**.

- The source address and destination address of the tunnel interface are 1.1.1.1 and 2.2.2.2, respectively.

```
[SwitchA] interface tunnel 1 mode vxlan
```

```
[SwitchA-Tunnel1] source 1.1.1.1
```

```
[SwitchA-Tunnel1] destination 2.2.2.2
```

```
[SwitchA-Tunnel1] quit
```

Create a VXLAN tunnel to Switch C.

- The tunnel interface name is **Tunnel 2**.

- The source address and destination address of the tunnel interface are 1.1.1.1 and 3.3.3.3, respectively.

```
[SwitchA] interface tunnel 2 mode vxlan
```

```
[SwitchA-Tunnel2] source 1.1.1.1
```

```
[SwitchA-Tunnel2] destination 3.3.3.3
```

```
[SwitchA-Tunnel2] quit
# Assign Tunnel 1 and Tunnel 2 to VXLAN 10.
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] vxlan 10
[SwitchA-vsi-vpna-vxlan-10] tunnel 1
[SwitchA-vsi-vpna-vxlan-10] tunnel 2
[SwitchA-vsi-vpna-vxlan-10] quit
[SwitchA-vsi-vpna] quit
# On GigabitEthernet 1/0/1, create Ethernet service instance 1000 to match VLAN 2.
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] service-instance 1000
[SwitchA-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 2
# Map Ethernet service instance 1000 to VSI vpna.
[SwitchA-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna
[SwitchA-GigabitEthernet1/0/1-srv1000] quit
[SwitchA-GigabitEthernet1/0/1] quit
```

4. スイッチBを構成します。

```
# Enable L2VPN.
<SwitchB> system-view
[SwitchB] l2vpn enable
# Enable Layer 2 forwarding for VXLANs.
[SwitchB] undo vxlan ip-forwarding
# Create a VSI named vpna, and create VXLAN 10.
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] vxlan 10
[SwitchB-vsi-vpna-vxlan-10] quit
[SwitchB-vsi-vpna] quit
# Enable the IGMP snooping feature.
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
# Enable IGMP snooping and dropping unknown multicast data packets for VSI vpna.
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] igmp-snooping enable
[SwitchB-vsi-vpna] igmp-snooping drop-unknown
[SwitchB-vsi-vpna] quit
# Assign an IP address to Loopback 0. This IP address will be used as the source address of
the VXLAN tunnels to Switch A and Switch C.
[SwitchB] interface loopback 0
[SwitchB-Loopback0] ip address 2.2.2.2 255.255.255.255
[SwitchB-Loopback0] quit
# Create a VXLAN tunnel to Switch A.
o The tunnel interface name is Tunnel 2.
o The source address and destination address of the tunnel interface are 2.2.2.2 and
1.1.1.1, respectively.
[SwitchB] interface tunnel 2 mode vxlan
```

```
[SwitchB-Tunnel2] source 2.2.2.2
[SwitchB-Tunnel2] destination 1.1.1.1
[SwitchB-Tunnel2] quit
```

Create a VXLAN tunnel to Switch C.

- The tunnel interface name is **Tunnel 3**.
- The source address and destination address of the tunnel interface are 2.2.2.2 and 3.3.3.3, respectively.

```
[SwitchB] interface tunnel 3 mode vxlan
[SwitchB-Tunnel3] source 2.2.2.2
[SwitchB-Tunnel3] destination 3.3.3.3
[SwitchB-Tunnel3] quit
```

Assign Tunnel 2 and Tunnel 3 to VXLAN 10.

```
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] vxlan 10
[SwitchB-vsi-vpna-vxlan-10] tunnel 2
[SwitchB-vsi-vpna-vxlan-10] tunnel 3
[SwitchB-vsi-vpna-vxlan-10] quit
[SwitchB-vsi-vpna] quit
```

On GigabitEthernet 1/0/1, create Ethernet service instance 1000 to match VLAN 2.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] service-instance 1000
[SwitchB-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 2
# Map Ethernet service instance 1000 to VSI vpna.
[SwitchB-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna
[SwitchB-GigabitEthernet1/0/1-srv1000] quit
[SwitchB-GigabitEthernet1/0/1] quit
```

5. スイッチCを設定します。

Enable L2VPN.

```
<SwitchC> system-view
[SwitchC] l2vpn enable
```

Enable Layer 2 forwarding for VXLANs.

```
[SwitchC] undo vxlan ip-forwarding
```

Create a VSI named **vpna**, and create VXLAN 10.

```
[SwitchC] vsi vpna
[SwitchC-vsi-vpna] vxlan 10
[SwitchC-vsi-vpna-vxlan-10] quit
[SwitchC-vsi-vpna] quit
```

Enable the IGMP snooping feature.

```
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

Enable IGMP snooping for VSI **vpna**.

```
[SwitchC] vsi vpna
[SwitchC-vsi-vpna] igmp-snooping enable
```

Enable dropping unknown multicast data packets for VSI **vpna**.

```
[SwitchC-vsi-vpna] igmp-snooping drop-unknown
```

```

# Specify 3.3.3.3 as the source IP address of IGMP general queries in VSI vpna.
[SwitchC-vsi-vpna] igmp-snooping general-query source-ip 3.3.3.3
# Enable the IGMP snooping querier.
[SwitchC-vsi-vpna] igmp-snooping querier
[SwitchC-vsi-vpna] quit
# Assign an IP address to Loopback 0. This address will be used as the source address of the
VXLAN tunnels to Switch A and Switch B.
[SwitchC] interface loopback 0
[SwitchC-Loopback0] ip address 3.3.3.3 255.255.255.255
[SwitchC-Loopback0] quit
# Create a VXLAN tunnel to Switch A.
  ○ The tunnel interface name is Tunnel 1.
  ○ The source address and destination address of the tunnel interface are 3.3.3.3 and
    1.1.1.1, respectively.
[SwitchC] interface tunnel 1 mode vxlan
[SwitchC-Tunnel1] source 3.3.3.3
[SwitchC-Tunnel1] destination 1.1.1.1
[SwitchC-Tunnel1] quit
# Create a VXLAN tunnel to Switch B.
  ○ The tunnel interface name is Tunnel 3.
  ○ The source address and destination address of the tunnel interface are 3.3.3.3 and
    2.2.2.2, respectively.
[SwitchC] interface tunnel 3 mode vxlan
[SwitchC-Tunnel3] source 3.3.3.3
[SwitchC-Tunnel3] destination 2.2.2.2
[SwitchC-Tunnel3] quit
# Assign Tunnel 1 and Tunnel 3 to VSI vpna.
[SwitchC] vsi vpna
[SwitchC-vsi-vpna] vxlan 10
[SwitchC-vsi-vpna-vxlan-10] tunnel 1
[SwitchC-vsi-vpna-vxlan-10] tunnel 3
[SwitchC-vsi-vpna-vxlan-10] quit
[SwitchC-vsi-vpna] quit
# On GigabitEthernet 1/0/1, create Ethernet service instance 1000 to match VLAN 2.
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] service-instance 1000
[SwitchC-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 2
# Map Ethernet service instance 1000 to VSI vpna.
[SwitchC-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna
[SwitchC-GigabitEthernet1/0/1-srv1000] quit
[SwitchC-GigabitEthernet1/0/1] quit

```

設定の確認

#スイッチA上のVSI **vpna**のダイナミックルータポートに関する簡単な情報を表示します。

```
[SwitchA] display igmp-snooping router-port vsi vpna
```


VSI vpna:

Router ports (1 in total):

Tun2 (VXLAN ID 10)

(00:04:17)

#スイッチB上のVSI vpnaのダイナミックルータポートに関する簡単な情報を表示します。

[SwitchB] display igmp-snooping router-port vsi vpna

VSI vpna:

Router ports (1 in total):

Tun3 (VXLAN ID 10)

(00:04:07)

IGMPスヌーピングのトラブルシューティング

レイヤ2マルチキャストフォワーディングが機能しない

症状

レイヤ2マルチキャストフォワーディングは、レイヤ2デバイス上では機能しません。

解決方法

この問題を解決するには、次の手順を実行し

1. IGMPスヌーピングステータスを表示するには、**display igmp-snooping**コマンドを使用します。
2. IGMPスヌーピングが有効でない場合、システムビューで**igmp-snooping**コマンドを使用して、IGMPスヌーピング機能を有効にします。次に、VLANビューまたはVSIビューで**igmp-snooping enable**コマンドを使用して、VLANまたはVSIのIGMPスヌーピングを有効にします。
3. IGMPスヌーピングがグローバルに有効になっているが、VLANまたはVSIに対して有効になっていない場合は、VLANビューまたはVSIビューで**igmp-snooping enable**コマンドを使用して、VLANまたはVSIに対してIGMPスヌーピングを有効にします。
4. 問題が解決しない場合は、H3Cサポートに連絡してください。

マルチキャストグループポリシーが機能しない

症状

ホストは、マルチキャストグループポリシーで許可されていないマルチキャストグループのマルチキャストデータを受信できます。

解決方法

この問題を解決するには、次の手順を実行し

1. 設定されたACLがマルチキャストグループポリシーの要件を満たしていることを確認するには、**display acl**コマンドを使用します。
2. IGMPスヌーピングビューまたは対応するインターフェイスビューで**display this**コマンドを表示して、正しいマルチキャストグループポリシーが適用されていることを確認します。適用されたポリシーが正しくない場合は、**group-policy**または **igmp-snooping group-policy**コマンドを使用して、正しいマルチキャストグループポリシーを適用します。
3. 不明なマルチキャストデータの廃棄が有効であることを確認するには、**display igmp-snooping**コマンドを使用します。そうでない場合は、**igmp-snooping drop-unknown**コマンドを使用して、不明なマルチキャストデータの廃棄を有効にします。
4. 問題が解決しない場合は、H3Cサポートに連絡してください。

PIMスヌーピングの設定

PIMスヌーピングの概要

PIMスヌーピングはレイヤ2デバイス上で動作します。IGMPスヌーピングとともに動作して、受信したPIMメッセージを分析し、特定のマルチキャストデータに関するポートをPIMスヌーピングのルーティングエントリに追加します。このようにして、マルチキャストデータは、そのデータに関するポートだけに転送できます。

図18 PIMスヌーピングがある場合とない場合のマルチキャストパケット送信

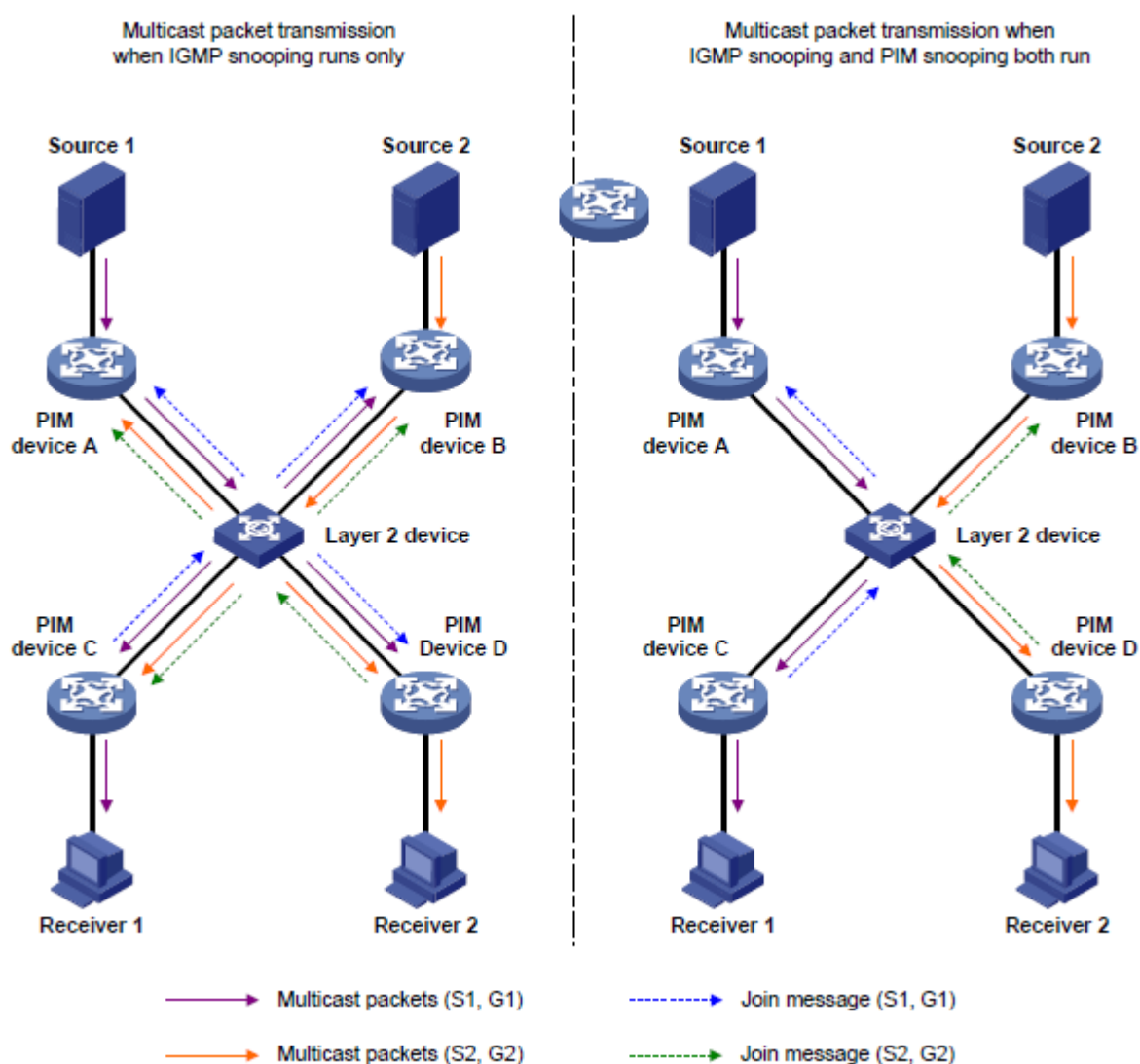


図18に示すように、Source 1はマルチキャストグループG1にマルチキャストデータを送信し、Source 2はマルチキャストグループG2にマルチキャストデータを送信します。Receiver 1はG1に属し、Receiver 2はG2に属します。PIMルータに接続するレイヤ2スイッチのインターフェイスは、同じVLAN内にあります。

- レイヤ2スイッチがIGMPスヌーピングだけを実行する場合、次のアクションを実行します。

- a. PIMルータが送信する受信PIM helloメッセージに従って、ルータポートを維持します。
 - b. VLAN内のPIM helloメッセージを除く、受信した他のすべてのタイプのPIMメッセージをフラグディングします。
 - c. すべてのマルチキャストデータをVLAN内のすべてのルータポートに転送します。
- VLAN内の各PIMルータは、マルチキャストデータに関係するかどうかに関係なく、すべてのマルチキャストデータと、PIM helloメッセージを除くすべてのPIMメッセージを受信できます。
- レイヤ2スイッチがIGMPスヌーピングとPIMスヌーピングの両方を実行する時、次のアクションを実行します。
 - a. ルータが送信する受信PIMメッセージに従って、PIMルータがマルチキャストグループにアドレス指定されたマルチキャストデータに関心があるかどうかを調べます。
 - b. ルータに接続され、データに関係するポートだけをPIMスヌーピングルーティングエントリに追加します。
 - c. PIMメッセージおよびマルチキャストデータを、そのデータに関係するルータだけに転送します。これにより、ネットワーク帯域幅が節約されます。

IGMPスヌーピングおよびルータポートの詳細については、「IGMPスヌーピングの設定」を参照してください。

PIMスヌーピングは、PIM-SMおよびPIM-SSMネットワークで実行できます。PIM-DMまたはBIDIR-PIMネットワークでは、PIMスヌーピングを設定しないでください。PIMの詳細については、「PIMの設定」を参照してください。

制約事項および注意事項:PIMスヌーピング設定

PIMスヌーピングはセカンダリVLANでは有効になりません。ベストプラクティスとして、セカンダリVLANにはPIMスヌーピングを設定しないでください。セカンダリVLANの詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

PIM加入またはプルーニングメッセージの最大サイズが、PIMスヌーピングデバイスに接続されているデバイスのパスMTUよりも小さいことを確認してください。そうでない場合、フラグメント化されたPIM加入またはプルーニングメッセージにより、PIMスヌーピングはマルチキャストデータを正しく転送できなくなります。加入またはプルーニングメッセージの最大サイズの設定の詳細については、「PIMの設定」を参照してください。

VLANにPIMスヌーピングを設定すると、PIMスヌーピングはそのVLANに属するポートだけで有効になります。

PIMスヌーピングタスクの概要

PIMスヌーピングを設定するには、次の作業を実行します。

1. PIMスヌーピングの有効化
2. (任意)マスター/下位スイッチオーバー後のグローバルポートのエージングタイムの設定
 - グローバルネイバーポートのエージングタイムの設定
 - グローバルダウンストリームポートおよびグローバルルータポートのエージングタイムの設定

PIMスヌーピングの有効化

1. システムビューに入ります。

System-view

2. IGMPスヌーピング機能を有効にし、IGMPスヌーピングビューを開始します。

igmp-snooping

デフォルトでは、IGMPスヌーピングは無効です。

このコマンドの詳細については、『IP Multicast Command Reference』の「IGMPスヌーピングコマンド」を参照してください。

3. システムビューに戻ります。

quit

4. VLANビューを開始します。

vlan *vlan-id*

5. VLANのIGMPスヌーピングを有効にします。

igmp-snooping enable

デフォルトでは、VLANのIGMPスヌーピングは無効です。

このコマンドの詳細については、『IP Multicast Command Reference』を参照してください。

6. VLANのPIMスヌーピングを有効にします。

pim-snooping enable

デフォルトでは、VLANのPIMスヌーピングは無効です。

マスター/下位スイッチオーバー後のグローバルポートのエイジングタイムの設定

グローバルポートについて

グローバルポートは、レイヤ2集約インターフェイスなどのマスターデバイス上の仮想ポートです。ネイバーポート、ダウンストリームポート、またはルータポートとして動作するグローバルポートは、それぞれグローバルネイバーポート、グローバルダウンストリームポート、およびグローバルルータポートと呼ばれます。

マスター/下位スイッチオーバー後のPIMスヌーピングエントリのエイジングによって発生するレイヤ2マルチキャストデータの中断を減らすには、次の作業を実行します。

制約事項とガイドライン

グローバルネイバーポートの場合、マスター/下位スイッチオーバー後にポートがPIM helloメッセージを受信しても、設定されたエイジングタイムは有効になりません。ポートのエイジングタイムは、PIM helloメッセージのエイジングタイムによって決定されます。

グローバルルータポートまたはグローバルダウンストリームポートの場合、マスター/下位スイッチオーバー後にポートがPIM加入メッセージを受信しても、設定されたエイジングタイムは有効になりません。ポートのエイジングタイムは、PIM加入メッセージのエイジングタイムによって決定されます。

グローバルネイバーポートのエイジングタイムの設定

1. システムビューに入ります。

System-view

2. VLANビューを開始します。

vlan *vlan-id*

3. マスター/下位スイッチオーバー後のグローバルネイバーポートのエイジングタイムを設定します。

pim-snooping graceful-restart neighbor-aging-time *seconds*

デフォルトでは、マスター/下位スイッチオーバー後のグローバルネイバーポートのエイジングタイムは105秒です。

グローバルダウンストリームポートおよびグローバルルータポートのエイジングタイムの設定

1. システムビューに入ります。

System-view

2. VLANビューを開始します。

vlan *vlan-id*

3. マスター/下位スイッチオーバー後のグローバルダウンストリームポートおよびグローバルルータポートのエイジングタイムを設定します。

pim-snooping graceful-restart join-aging-time *seconds*

デフォルトでは、マスター/下位スイッチオーバー後のダウンストリームポートおよびグローバルルータポートのエイジングタイムは210秒です。

PIMスヌーピングの表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
PIMスヌーピングネイバー情報を表示します。	display pim-snooping neighbor [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [verbose]
PIMスヌーピングルータポート情報を表示します。	display pim-snooping router-port [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [verbose]
PIMスヌーピングルーティングエントリを表示します。	display pim-snooping routing-table [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [verbose]
PIMスヌーピングを通じて学習されたPIMメッセージの統計情報を表示します。	display pim-snooping statistics
PIMスヌーピングによって学習されたPIMメッセージの統計情報をクリアします。	reset pim-snooping statistics

PIMスヌーピングの設定例

例:PIMスヌーピングの設定

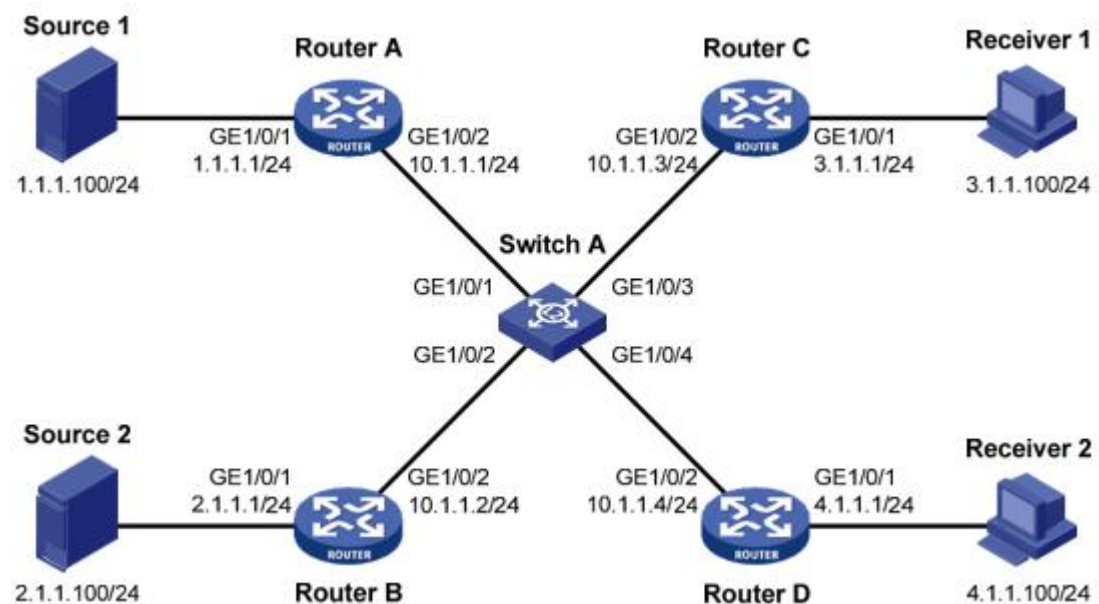
ネットワークの設定

図19に示します。

- OSPFはネットワーク上で動作します。
- 送信元1および送信元2は、それぞれマルチキャストグループ224.1.1.1および225.1.1.1にマルチキャストデータを送信します。
- レシーバ1とレシーバ2は、それぞれマルチキャストグループ224.1.1.1と225.1.1.1に属しています。
- ルータCとルータDではGigabitEthernet 1/0/1上でIGMPが動作しています。ルータA、ルータB、ルータC、およびルータDではPIM-SMが動作しています。
- ルータAのGigabitEthernet 1/0/2は、C-BSRおよびC-RPとして機能します。

スイッチAにIGMPスヌーピングおよびPIMスヌーピングを設定します。その後、スイッチAはPIMプロトコルパケットおよびマルチキャストデータパケットを、レシーバに接続されたルータだけに転送します。

図19 ネットワークダイアグラム



手順

1. 図19に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
2. ルータでOSPFを設定します(詳細は省略)。
3. ルータAを設定します。

```
# Enable IP multicast routing.
```

```
<RouterA> system-view
```



```

[RouterA] multicast routing
[RouterA-mrib] quit
# Enable PIM-SM on each interface.
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pim sm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim sm
[RouterA-GigabitEthernet1/0/2] quit
# Configure GigabitEthernet 1/0/2 as a C-BSR and a C-RP.
[RouterA] pim
[RouterA-pim] c-bsr 10.1.1.1
[RouterA-pim] c-rp 10.1.1.1
[RouterA-pim] quit

```

4. ルータBを設定します。

```

# Enable IP multicast routing.
<RouterB> system-view
[RouterB] multicast routing
[RouterB-mrib] quit
# Enable PIM-SM on each interface.
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] pim sm
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] pim sm
[RouterB-GigabitEthernet1/0/2] quit

```

5. ルータCを設定します。

```

# Enable IP multicast routing.
<RouterC> system-view
[RouterC] multicast routing
[RouterC-mrib] quit
# Enable IGMP on GigabitEthernet 1/0/1.
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] igmp enable
[RouterC-GigabitEthernet1/0/1] quit
# Enable PIM-SM on GigabitEthernet 1/0/2.
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] pim sm
[RouterC-GigabitEthernet1/0/2] quit

```

6. ルータDを設定します。

```

# Enable IP multicast routing.
<RouterD> system-view
[RouterD] multicast routing
[RouterD-mrib] quit
# Enable IGMP on GigabitEthernet 1/0/1.

```

```
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] igmp enable
[RouterD-GigabitEthernet1/0/1] quit
# Enable PIM-SM on GigabitEthernet 1/0/2.
[RouterD] interface gigabitethernet 1/0/2
[RouterD-GigabitEthernet1/0/2] pim sm
[RouterD-GigabitEthernet1/0/2] quit
```

7. スイッチAを設定します。

```
# Enable the IGMP snooping feature.
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the
VLAN.
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
# Enable IGMP snooping and PIM snooping for VLAN 100.
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] pim-snooping enable
[SwitchA-vlan100] quit
```

設定の確認

#スイッチAでは、VLAN 100のPIMスヌーピングネイバー情報を表示します。

```
[SwitchA] display pim-snooping neighbor vlan 100
Total 4 neighbors.
```

VLAN 100: Total 4 neighbors.

```
10.1.1.1
Ports (1 in total):
  GE1/0/1          (00:32:43)
10.1.1.2
Ports (1 in total):
  GE1/0/2          (00:32:43)
10.1.1.3
Ports (1 in total):
  GE1/0/3          (00:32:43)
10.1.1.4
Ports (1 in total):
  GE1/0/4          (00:32:43)
```

この出力は、ルータA、ルータB、ルータC、およびルータDがPIMスヌーピングネイバーであることを示しています。#スイッチAで、VLAN 100のPIMスヌーピングルーティングエントリを表示します。

```
[SwitchA] display pim-snooping routing-table vlan 100
Total 2 entries.
FSM Flag: NI-no info, J-join, PP-prune pending
```

VLAN 100: Total 2 entries.

```
(* , 224.1.1.1)
Upstream neighbor: 10.1.1.1
Upstream Ports (1 in total):
GE1/0/1
Downstream Ports (1 in total): GE1/0/3
Expires: 00:03:01, FSM: J (* ,
225.1.1.1)
Upstream neighbor: 10.1.1.2
Upstream Ports (1 in total):
GE1/0/2
Downstream Ports (1 in total): GE1/0/4
Expires: 00:03:11, FSM: J
```

出力には次の情報が表示されます。

- スイッチAは、マルチキャストグループ224.1.1.1宛てのマルチキャストデータをルータCだけに転送します。
- スイッチAは、マルチキャストグループ225.1.1.1宛てのマルチキャストデータをルータDだけに転送します。

PIMスヌーピングのトラブルシューティング

PIMスヌーピングがレイヤ2デバイスで動作しない

症状

PIMスヌーピングは、レイヤ2デバイスでは動作しません。

解決方法

この問題を解決するには、次の手順を実行し

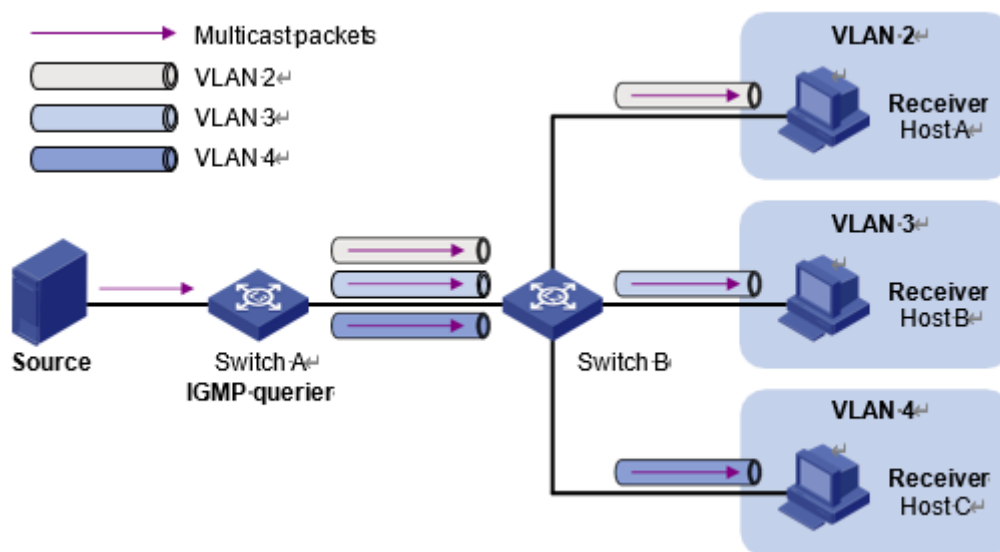
1. IGMPスヌーピングおよびPIMスヌーピングに関する情報を表示するには、**display current-configuration**コマンドを使用します。
2. IGMPスヌーピングが有効でない場合は、IGMPスヌーピング機能を有効にしてから、VLANのIGMPスヌーピングおよびPIMスヌーピングを有効にします。
3. PIMスヌーピングが有効でない場合は、VLANのPIMスヌーピングを有効にします。
4. 問題が解決しない場合は、H3Cサポートに連絡してください。

マルチキャストVLANの設定

マルチキャストVLAN機能

図20に示すように、ホストA、ホストB、およびホストCは、3つの異なるVLANおよび同じマルチキャストグループ内にあります。スイッチA(レイヤ3デバイス)は、そのグループのマルチキャストデータを受信すると、マルチキャストデータの3つのコピーをスイッチB(レイヤ2デバイス)に送信します。これは、大量の帯域幅を占有し、レイヤ3デバイスの負荷を増加させます。

図20 マルチキャストVLAN機能を使用しないマルチキャスト送信



スイッチBにマルチキャストVLANが設定されると、スイッチAはマルチキャストデータの1つのコピーだけをスイッチBのマルチキャストVLANに送信します。この方法は、ネットワーク帯域幅を節約し、レイヤ3デバイスの負荷を軽減します。

マルチキャストVLAN方式

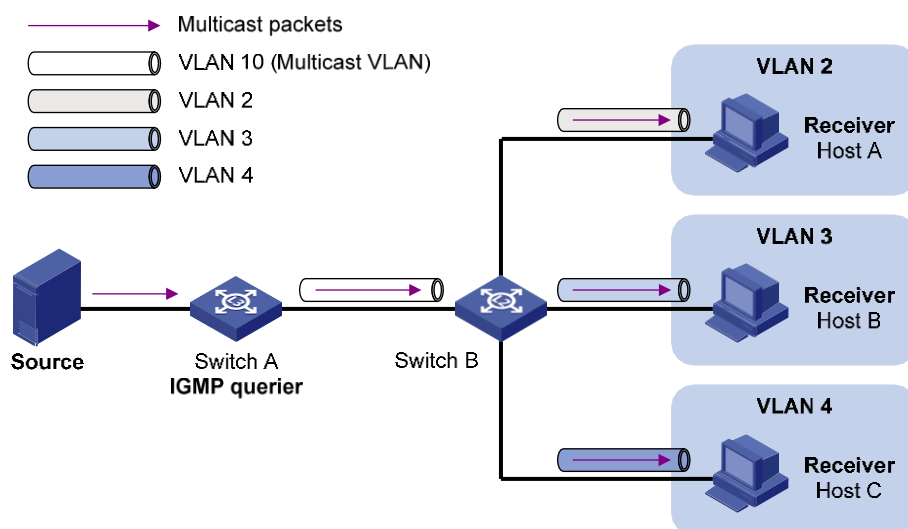
マルチキャストVLANには、サブVLANベースのマルチキャストVLANとポートベースのマルチキャストVLANが含まれます。

サブVLANベースのマルチキャストVLAN

図21に示します。

- ホストA、ホストB、およびホストCは、それぞれVLAN 2～VLAN 4にあります。
- スイッチBでは、VLAN 10はマルチキャストVLANです。VLAN 2～VLAN 4は、VLAN 10のサブVLANです。
- IGMPスヌーピングは、マルチキャストVLANおよびそのサブVLANに対して有効です。

図21 サブVLANベースのマルチキャストVLAN



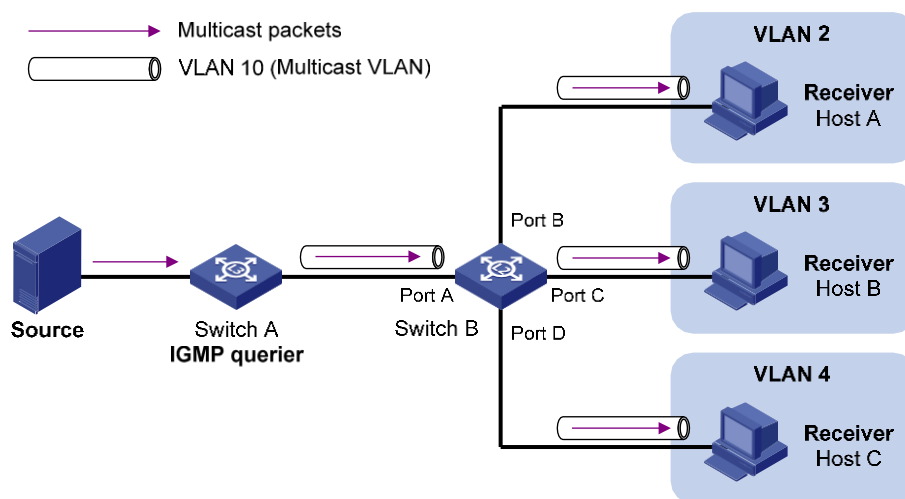
IGMPスヌーピングは、マルチキャストVLANのルータポートと各サブVLANのメンバーポートを管理します。スイッチAがマルチキャスト送信元からマルチキャストデータを受信すると、スイッチBのマルチキャストVLANにマルチキャストデータのコピーを1つだけ送信します。次に、スイッチBはマルチキャストVLANの各サブVLANに個別のコピーを送信します。

ポートベースのマルチキャストVLAN

図22に示します。

- ホストA、ホストB、およびホストCは、それぞれVLAN 2～VLAN 4にあります。
- スイッチBでは、VLAN 10はマルチキャストVLANです。すべてのユーザーポートはハイブリッドポートであり、VLAN 10に割り当てられます。
- IGMPスヌーピングは、マルチキャストVLANおよびVLAN 2～VLAN 4に対して有効です。

図22 ポートベースマルチキャストVLAN



IGMPスヌーピングは、マルチキャストVLANのルータポートおよびメンバーポートを管理します。スイッチ

Aがマルチキャスト送信元からマルチキャストデータを受信すると、スイッチBのマルチキャストVLANにマルチキャストデータのコピーを1つだけ送信します。スイッチBは、マルチキャストVLANの各ユーザーポートに個別のコピーを送信します。

制約事項および注意事項:マルチキャストVLANの設定

マルチキャストVLANとして設定するVLANが存在している必要があります。

サブVLANベースマルチキャストVLANとポートベースマルチキャストVLANの両方を設定した場合、ポートベースマルチキャストVLANの設定が有効になります。

IPマルチキャストルーティングが有効になっているデバイスでは、マルチキャストVLANを設定しないでください。設定すると、エラーが表示されます。マルチキャストVLANが設定されているデバイスでは、IPマルチキャストルーティングを有効にしないでください。有効にしないと、マルチキャスト転送の例外が発生します。

VLANインターフェイスでPIMまたはIGMPが有効になっている場合は、VLANをマルチキャストVLANまたはマルチキャストサブVLANとして設定しないでください。設定すると、エラーが表示されます。VLANインターフェイスがマルチキャストVLANまたはマルチキャストサブVLANに属している場合は、VLANインターフェイスでPIMまたはIGMPを有効にしないでください。有効にしないと、マルチキャスト転送例外が発生します。

マルチキャストVLAN機能は、セカンダリVLANでは有効になりません。ベストプラクティスとして、セカンダリVLANにはマルチキャストVLAN機能を設定しないでください。セカンダリVLANの詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

サブVLANベースのマルチキャストVLANの設定

制約事項とガイドライン

マルチキャストVLANのサブVLANとして設定されるVLANは存在している必要があり、マルチキャストVLANまたは他のマルチキャストVLANのサブVLANにすることはできません。

必要条件

サブVLANベースのマルチキャストVLANを設定する前に、次の作業を完了する必要があります。

- 必要に応じてVLANを作成します。
- VLANをマルチキャストVLANとして設定し、VLANをサブVLANとして設定するには、IGMPスヌーピングを有効にします。

手順

1. システムビューに入ります。

System-view

2. VLANをマルチキャストVLANとして設定し、マルチキャストVLANビューを開始します。

multicast-vlan *vlan-id*

デフォルトでは、VLANはマルチキャストVLANではありません。

3. VLANをマルチキャストVLANにサブVLANとして割り当てます。

subvlan *vlan-list*

ポートベースマルチキャストVLANの設定

制約事項とガイドライン

マルチキャストVLANビューでユーザーポートをマルチキャストVLANに割り当てても、インターフェイスビューでユーザーポートをマルチキャストVLANに割り当ててもできます。これらの設定のプライオリティは同じです。

ユーザーポートは、1つのマルチキャストVLANだけに属することができます。

必要条件

ポートベースのマルチキャストVLANを設定する前に、次の作業を完了する必要があります。

- 必要に応じてVLANを作成します。
- マルチキャストVLANとして設定するVLANのIGMPスヌーピングを有効にします。
- マルチキャストレシーバを含むすべてのVLANに対してIGMPスヌーピングを有効にします。
- ユーザーポートのアトリビュートを設定します。ポートが、マルチキャストVLANとして設定されるVLANからのパケットを転送でき、VLANタグを削除したパケットを送信できることを確認します。ポートアトリビュートの設定の詳細については、『Layer 2 LAN Switching Configuration Guide』の「VLAN configuration」を参照してください。

マルチキャストVLANビューでのマルチキャストVLANへのユーザーポートの割り当て

1. システムビューに入ります。

System-view

2. VLANをマルチキャストVLANとして設定し、マルチキャストVLANビューを開始します。

multicast-vlan *vlan-id*

デフォルトでは、VLANはマルチキャストVLANではありません。

3. マルチキャストVLANにポートを割り当てます。

port *interface-list*

インターフェイスビューでのマルチキャストVLANへのユーザーポートの割り当て

1. システムビューに入ります。

System-view

2. VLANをマルチキャストVLANとして設定し、マルチキャストVLANビューを開始します。

multicast-vlan *vlan-id*

デフォルトでは、VLANはマルチキャストVLANではありません。

3. システムビューに戻ります。

quit

4. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface *interface-type interface-number*

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation *interface-number*

5. ポートをマルチキャストVLANに割り当てます。

port multicast-vlan *vlan-id*

デフォルトでは、ポートはどのマルチキャストVLANにも所属しません。

マルチキャストVLANフォワーディングエントリの最大数の設定

マルチキャストVLANフォワーディングエントリの最大数の設定について

デバイス上のマルチキャストVLANフォワーディングエントリの最大数を設定できます。上限に達すると、一部のエントリが期限切れになるか、手動で削除されるまで、デバイスはマルチキャストVLANフォワーディングエントリを作成しません。

手順

1. システムビューに入ります。

System-view

2. マルチキャストVLANフォワーディングエントリの最大数を設定します。

multicast-vlan entry-limit *limit*

デフォルトでは、マルチキャストVLANフォワーディングエントリの最大数は4000です。

マルチキャストVLANの表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
マルチキャストVLANに関する情報を表示します。	display multicast-vlan [<i>vlan-id</i>]
マルチキャストVLANフォワーディングエントリに関する情報を表示します。	display multicast-vlan forwarding-table [<i>group-address</i> [mask { <i>mask-length</i> <i>mask</i> }] <i>source-address</i> [mask { <i>mask-length</i> <i>mask</i> }] slot <i>slot-number</i> subvlan <i>vlan-id</i> vlan <i>vlan-id</i>] *
マルチキャストVLAN内のマルチキャストグループに関する情報を表示します。	display multicast-vlan group [<i>source-address</i> <i>group-address</i> slot <i>slot-number</i> verbose vlan <i>vlan-id</i>] *
マルチキャストVLAN内のマルチキャストグループをクリアします。	reset multicast-vlan group [<i>source-address</i> [mask { <i>mask-length</i> <i>mask</i> }] <i>group-address</i> [mask { <i>mask-length</i> <i>mask</i> }] vlan <i>vlan-id</i>] *

マルチキャストVLANの設定例

例:サブVLANベースのマルチキャストVLANの設定

ネットワークの設定

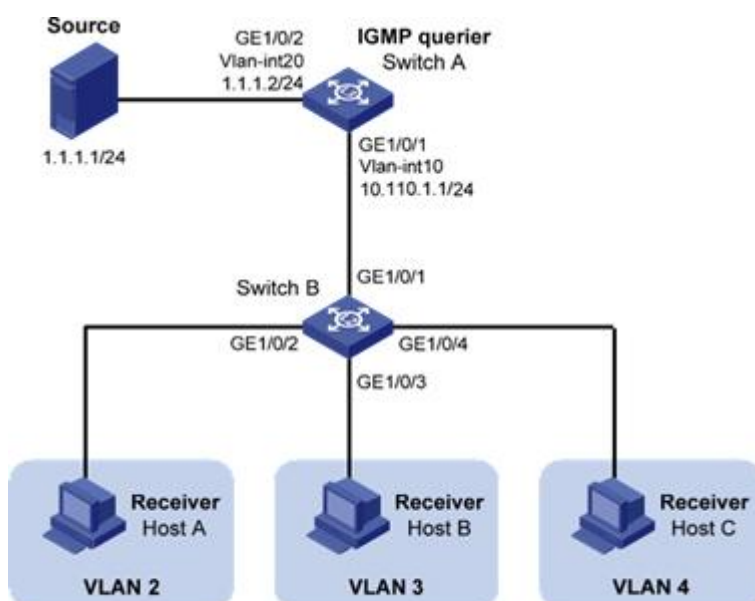
図23に示します。

- レイヤ3デバイスのスイッチAはIGMPv2を実行し、IGMPクエリャーとして動作します。レイヤ2デバイスのスイッチBはIGMPv2スヌーピングを実行します。
- マルチキャスト送信元は、マルチキャストグループ224.1.1.1にマルチキャストデータを送信します。レシーバのホストA、ホストB、およびホストCは、それぞれVLAN 2、VLAN 3、およびVLAN 4に属します。

次の要件を満たすように、スイッチBにサブVLANベースのマルチキャストVLANを設定します。

- スイッチAは、マルチキャストVLANを介してスイッチBにマルチキャストデータを送信します。
- スイッチBは、異なるユーザーVLAN内のレシーバにマルチキャストデータを転送します。

図23 ネットワークダイアグラム



手順

1. スイッチAを設定します。

```
# Enable IP multicast routing.
```

```
<SwitchA> system-view
```

```
[SwitchA] multicast routing
```

```
[SwitchA-mrib] quit
```

```
# Create VLAN 20, and assign GigabitEthernet 1/0/2 to the VLAN.
```

```
[SwitchA] vlan 20
```

```

[SwitchA-vlan20] port gigabitethernet 1/0/2
[SwitchA-vlan20] quit
# Assign an IP address to VLAN-interface 20, and enable PIM-DM on the interface.
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ip address 1.1.1.2 24
[SwitchA-Vlan-interface20] pim dm
[SwitchA-Vlan-interface20] quit
# Create VLAN 10.
[SwitchA] vlan 10
[SwitchA-vlan10] quit
# Configure GigabitEthernet 1/0/1 as a hybrid port, and assign the port to VLAN 10 as a tagged
VLAN member.
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type hybrid
[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 10 tagged
[SwitchA-GigabitEthernet1/0/1] quit
# Assign an IP address to VLAN-interface 10, and enable IGMP on the interface.
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 10.110.1.1 24
[SwitchA-Vlan-interface10] igmp enable
[SwitchA-Vlan-interface10] quit

```

2. スイッチBを構成します。

```

# Enable the IGMP snooping feature.
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
# Create VLAN 2, assign GigabitEthernet 1/0/2 to the VLAN, and enable IGMP snooping for the
VLAN.
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/2
[SwitchB-vlan2] igmp-snooping enable
[SwitchB-vlan2] quit
# Create VLAN 3, assign GigabitEthernet 1/0/3 to the VLAN, and enable IGMP snooping in the
VLAN.
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/3
[SwitchB-vlan3] igmp-snooping enable
[SwitchB-vlan3] quit
# Create VLAN 4, assign GigabitEthernet 1/0/4 to the VLAN, and enable IGMP snooping in the
VLAN.
[SwitchB] vlan 4
[SwitchB-vlan4] port gigabitethernet 1/0/4
[SwitchB-vlan4] igmp-snooping enable
[SwitchB-vlan4] quit
# Create VLAN 10, and enable IGMP snooping for the VLAN.

```

```
[SwitchB] vlan 10
[SwitchB-vlan10] igmp-snooping enable
[SwitchB-vlan10] quit
# Configure GigabitEthernet 1/0/1 as a hybrid port, and assign the port to VLAN 10 as a tagged
VLAN member.
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type hybrid
[SwitchB-GigabitEthernet1/0/1] port hybrid vlan 10 tagged
[SwitchB-GigabitEthernet1/0/1] quit
# Configure VLAN 10 as a multicast VLAN, and assign VLAN 2 through VLAN 4 as sub-VLANs
to multicast VLAN 10.
[SwitchB] multicast-vlan 10
[SwitchB-mvlan-10] subvlan 2 to 4
[SwitchB-mvlan-10] quit
```

設定の確認

#スイッチB上のすべてのマルチキャストVLANに関する情報を表示します。

```
[SwitchB] display multicast-vlan
Total 1 multicast VLANs.
```

```
Multicast VLAN 10:
  Sub-VLAN list(3 in total):
    2-4
  Port list(0 in total):
```

#スイッチB上のマルチキャストVLAN内のマルチキャストグループに関する情報を表示します。

```
[SwitchB] display multicast-vlan group
Total 1 entries.
```

```
Multicast VLAN 10: Total 1 entries.
(0.0.0.0, 224.1.1.1)
  Sub-VLANs (3 in total):
    VLAN 2
    VLAN 3
    VLAN 4
```

この出力は、マルチキャストグループ224.1.1.1がマルチキャストVLAN 10に属していることを示しています。マルチキャストVLAN 10には、VLAN 2～VLAN 4のサブVLANが含まれています。スイッチBは、VLAN 10のマルチキャストデータをVLAN 4経由でVLAN 2に複製します。

例:ポートベースのマルチキャストVLANの設定

ネットワークの設定

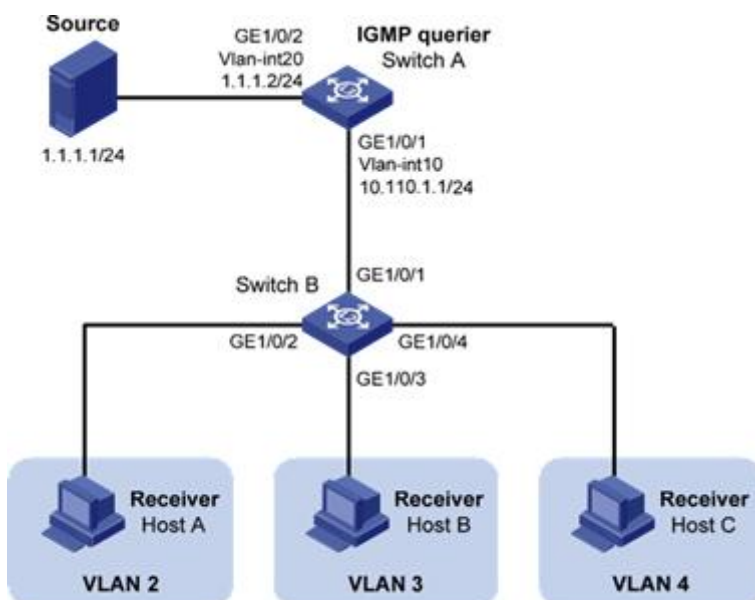
図24に示します。

- レイヤ3デバイスのスイッチAはIGMPv2を実行し、IGMPクエリアーとして動作します。レイヤ2デバイスのスイッチBはIGMPv2スヌーピングを実行します。
- マルチキャスト送信元は、マルチキャストグループ224.1.1.1にマルチキャストデータを送信します。レシーバのホストA、ホストB、およびホストCは、それぞれVLAN 2、VLAN 3、およびVLAN 4に属します。

次の要件を満たすように、スイッチBでポートベースのマルチキャストVLANを設定します。

- スイッチAは、マルチキャストVLANを介してスイッチBにマルチキャストデータを送信します。
- スイッチBは、異なるユーザーVLAN内のレシーバにマルチキャストデータを転送します。

図24 ネットワークダイアグラム



手順

1. スイッチAを設定します。

```
# Enable IP multicast routing.
```

```
<SwitchA> system-view
```

```
[SwitchA] multicast routing
```

```
[SwitchA-mrib] quit
```

```
# Create VLAN 20, and assign GigabitEthernet 1/0/2 to the VLAN.
```

```
[SwitchA] vlan 20
```

```
[SwitchA-vlan20] port gigabitethernet 1/0/2
```

```
[SwitchA-vlan20] quit
```

```
# Assign an IP address to VLAN-interface 20, and enable PIM-DM on the interface.
```

```
[SwitchA] interface vlan-interface 20
```

```
[SwitchA-Vlan-interface20] ip address 1.1.1.2 24
[SwitchA-Vlan-interface20] pim dm
[SwitchA-Vlan-interface20] quit
# Create VLAN 10, and assign GigabitEthernet 1/0/1 to the VLAN.
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/1
[SwitchA-vlan10] quit
# Assign an IP address to VLAN-interface 10, and enable IGMP on the interface.
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 10.110.1.1 24
[SwitchA-Vlan-interface10] igmp enable
[SwitchA-Vlan-interface10] quit
```

2. スイッチBを構成します。

```
# Enable the IGMP snooping feature.
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
# Create VLAN 10, assign GigabitEthernet 1/0/1 to the VLAN, and enable IGMP snooping for the VLAN.
[SwitchB] vlan 10
[SwitchB-vlan10] port gigabitethernet 1/0/1
[SwitchB-vlan10] igmp-snooping enable
[SwitchB-vlan10] quit
# Create VLAN 2, and enable IGMP snooping for the VLAN.
[SwitchB] vlan 2
[SwitchB-vlan2] igmp-snooping enable
[SwitchB-vlan2] quit
# Create VLAN 3, and enable IGMP snooping for the VLAN.
[SwitchB] vlan 3
[SwitchB-vlan3] igmp-snooping enable
[SwitchB-vlan3] quit
# Create VLAN 4, and enable IGMP snooping for the VLAN.
[SwitchB] vlan 4
[SwitchB-vlan4] igmp-snooping enable
[SwitchB-vlan4] quit
# Configure GigabitEthernet 1/0/2 as a hybrid port, and configure VLAN 2 as the PVID of the hybrid port.
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type hybrid
[SwitchB-GigabitEthernet1/0/2] port hybrid pvid vlan 2
# Assign GigabitEthernet 1/0/2 to VLAN 2 and VLAN 10 as an untagged VLAN member.
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 2 untagged
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 as a hybrid port, and configure VLAN 3 as the PVID of the hybrid port.

```
[SwitchB] interface gigabitethernet 1/0/3
```

```
[SwitchB-GigabitEthernet1/0/3] port link-type hybrid
```

```
[SwitchB-GigabitEthernet1/0/3] port hybrid pvid vlan 3
```

Assign GigabitEthernet 1/0/3 to VLAN 3 and VLAN 10 as an untagged VLAN member.

```
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 3 untagged
```

```
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 10 untagged
```

```
[SwitchB-GigabitEthernet1/0/3] quit
```

Configure GigabitEthernet 1/0/4 as a hybrid port, and configure VLAN 4 as the PVID of the hybrid port.

```
[SwitchB] interface gigabitethernet 1/0/4
```

```
[SwitchB-GigabitEthernet1/0/4] port link-type hybrid
```

```
[SwitchB-GigabitEthernet1/0/4] port hybrid pvid vlan 4
```

Assign GigabitEthernet 1/0/4 to VLAN 4 and VLAN 10 as an untagged VLAN member.

```
[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 4 untagged
```

```
[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 10 untagged
```

```
[SwitchB-GigabitEthernet1/0/4] quit
```

Configure VLAN 10 as a multicast VLAN.

```
[SwitchB] multicast-vlan 10
```

Assign GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to VLAN 10.

```
[SwitchB-mvlan-10] port gigabitethernet 1/0/2 to gigabitethernet 1/0/3
```

```
[SwitchB-mvlan-10] quit
```

Assign GigabitEthernet 1/0/4 to VLAN 10.

```
[SwitchB] interface gigabitethernet 1/0/4
```

```
[SwitchB-GigabitEthernet1/0/4] port multicast-vlan 10
```

```
[SwitchB-GigabitEthernet1/0/4] quit
```

設定の確認

#スイッチB上のマルチキャストVLANIに関する情報を表示します。

```
[SwitchB] display multicast-vlan
```

Total 1 multicast VLANs.

Multicast VLAN 10:

Sub-VLAN list(0 in total):

Port list(3 in total):

GE1/0/2

GE1/0/3

GE1/0/4

#スイッチBのダイナミックIGMPスヌーピングフォワーディングエントリを表示します。

```
[SwitchB] display igmp-snooping group
```

Total 1 entries.

VLAN 10: Total 1 entries.

(0.0.0.0, 224.1.1.1)

Host slots (0 in total):

Host ports (3 in total):

GE1/0/2	(00:03:23)
GE1/0/3	(00:04:07)
GE1/0/4	(00:04:16)

この出力は、IGMPスヌーピングがマルチキャストVLAN(VLAN 10)内のユーザーポートを維持していることを示しています。スイッチBは、これらのユーザーポートを介してVLAN 10のマルチキャストデータを転送します。

マルチキャストルーティングおよびフォワーディングの設定

マルチキャストルーティングおよびフォワーディングについて

各マルチキャストルーティングプロトコルには、独自のルーティングテーブルがあります。マルチキャストルーティングプロトコルによって生成されたルーティングエントリおよび静的に設定されたマルチキャストルーティングエントリ内のマルチキャストルーティング情報は、(S, G)および(*,G)エントリのセットに要約されます。すべての(S, G)および(*,G)エントリは、一般的なマルチキャストルーティングテーブルを形成します。一般的なマルチキャストルーティングテーブル内の最適なマルチキャストルーティングエントリは、マルチキャスト転送テーブルに追加され、マルチキャストデータの転送をガイドします。

RPFチェックメカニズム

マルチキャストルーティングプロトコルは、Reverse Path Forwarding(RPF)チェックを使用して、正しいパスに沿ったマルチキャストデータ配信を保証し、データループを回避します。

RPFチェックプロセス

マルチキャストデバイスは、マルチキャストパケットに対して次のようにRPFチェックを実行します。

1. ユニキャスト、MBGP、およびスタティックマルチキャストルーティングテーブルとは別に、パケット送信元に戻る最適ルートを選択します。

「パケット送信元」という用語は、状況によって異なるものを意味します。

- SPTに沿って送信されるパケットの場合、パケット送信元はマルチキャスト送信元です。
- RPTに沿って送信されるパケットの場合、パケットの送信元はRPです。
- BSRから発信されたブートストラップメッセージの場合、パケットの送信元はBSRです。

SPT、RPT、送信元側RPT、RP、およびBSRの概念の詳細については、「PIMの設定」を参照してください。

2. 次のように、3つの最適ルートのいずれかをRPFルートとして選択します。

- デバイスが最長プレフィクス一致の原則を使用する場合、サブネットマスクが最大のルートがRPFルートになります。ルートのマスクが同じ場合、ルートプリファレンスが最大のルートがRPFルートになります。ルートのルートプリファレンスが同じ場合、ユニキャストルートがRPFルートになります。

ルートプリファレンスの詳細については、『Layer 3 IP Routing Configuration Guide』を参照してください。

- デバイスが最長プレフィクス一致の原則を使用しない場合、ルートプリファレンスが最も高いルートがRPFルートになります。ルートが同じプリファレンスを持つ場合、ユニキャストルートがRPFルートになります。

RPFルートには、RPFインターフェイスおよびRPFネイバー情報が含まれます。

- RPFルートがユニキャストルートまたはMBGPルートの場合、発信インターフェイスはRPFインターフェイスであり、ネクストホップはRPFネイバーです。
- RPFルートがスタティックマルチキャストルートの場合、RPFインターフェイスとRPFネイバーがルートに指定されます。

3. パケットがRPFインターフェイスに到着したかどうかを判別します。

- パケットがRPFインターフェイスに到達した場合、RPFチェックは成功し、パケットは転送されます。
- パケットが非RPFインターフェイスに到達した場合、RPFチェックは失敗し、パケットは廃棄されます。

マルチキャストにおけるRPFチェックの実装

受信した各マルチキャストパケットにRPFチェックを実装すると、デバイスに大きな負荷がかかります。この問題を解決するには、マルチキャスト転送テーブルを使用します。デバイスは、(S, G)パケットのマルチキャスト転送エントリを作成するときに、パケットのRPFインターフェイスを(S, G)エントリの着信インターフェイスとして設定します。デバイスは、別の(S, G)パケットを受信した後、一致する(S, G)エントリをマルチキャスト転送テーブルで検索します。

- 一致するものが見つからない場合、デバイスは最初にパケット送信元とRPFインターフェイスに戻るRPFルートを決定します。次に、RPFインターフェイスを着信インターフェイスとする転送エントリを作成し、次の判断を行います。
 - 受信インターフェイスがRPFインターフェイスの場合、RPFチェックは成功し、デバイスはすべての発信インターフェイスからパケットを転送します。
 - 受信インターフェイスがRPFインターフェイスでない場合、RPFチェックは失敗し、デバイスはパケットを廃棄します。
- 一致が見つかり、一致する転送エントリに受信インターフェイスが含まれている場合、デバイスはすべての発信インターフェイスからパケットを転送します。
- 一致が検出されても、一致する転送エントリに受信インターフェイスが含まれていない場合、デバイスはパケット送信元に戻るRPFルートを決定します。その後、デバイスは次のいずれかのアクションを実行します。
 - RPFインターフェイスが着信インターフェイスの場合は、転送エントリは正しいが、パケットが誤ったパスを通過したことを意味します。パケットはRPFチェックに失敗し、デバイスはパケットを廃棄します。
 - RPFインターフェイスが着信インターフェイスでない場合は、転送エントリが期限切れになったことを意味します。デバイスは着信インターフェイスをRPFインターフェイスに置き換え、受信イ

ンターフェイスをRPFインターフェイスと照合します。受信インターフェイスがRPFインターフェイスの場合、デバイスはすべての発信インターフェイスからパケットを転送します。それ以外の場合、パケットは廃棄されます。

図25 RPFチェックプロセス

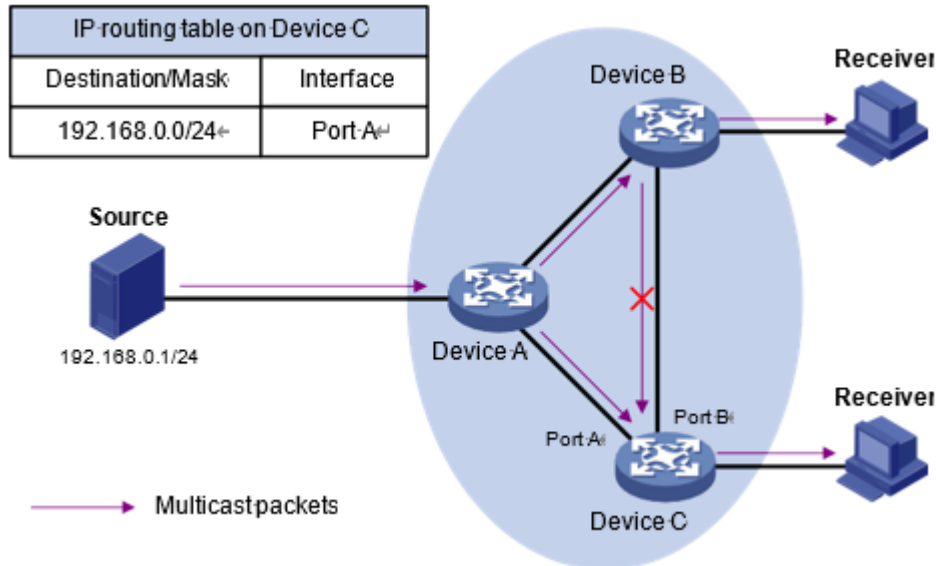


図25に示すように、ネットワーク上でユニキャストルートが使用可能であり、MBGPが設定されておらず、デバイスCにスタティックマルチキャストルートが設定されていないとします。マルチキャストパケットは、SPTに従ってマルチキャスト送信元からレシーバに送信されます。デバイスCのマルチキャスト転送テーブルには(S, G)エントリが含まれ、ポートAが着信インターフェイスになります。

- ポートAのデバイスCにマルチキャストパケットが到着した場合、受信インターフェイスは(S, G)エントリの着信インターフェイスです。デバイスCは、すべての発信インターフェイスからパケットを転送します。
- マルチキャストパケットがデバイスCのポートBに到着した場合、受信インターフェイスは(S, G)エントリの着信インターフェイスではありません。デバイスCはユニキャストルーティングテーブルを検索し、送信元(RPFインターフェイス)への発信インターフェイスがポートAであることを検出します。この場合、(S, G)エントリは正しいのですが、パケットが誤ったパスを通過しました。パケットはRPFチェックに失敗し、デバイスCはパケットを廃棄します。

スタティックマルチキャストルートの使用

スタティックマルチキャストルートは、RPFルートを変更したり、RPFルートを作成したりできます。

RPFルートの変更

通常、マルチキャストネットワークのトポロジ構造はユニキャストネットワークのトポロジ構造と同じであり、

マルチキャストトラフィックはユニキャストトラフィックと同じ伝送パスに従います。マルチキャスト送信元にスタティックマルチキャストルートを設定して、RPFルートを変更できます。その結果、デバイスはユニキャストトラフィック用の伝送パスとは異なるマルチキャストトラフィック用の伝送パスを作成します。

図26 RPFルートの変更

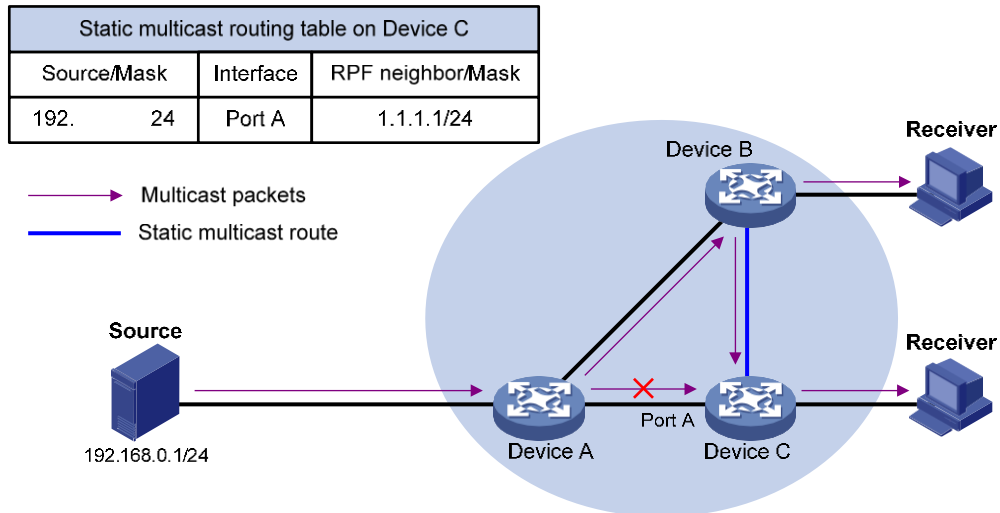


図26に示すように、スタティックマルチキャストルートが設定されていない場合、送信元に戻るパス上のデバイスCのRPFネイバーはデバイスAです。送信元からのマルチキャストデータは、デバイスAを経由してデバイスCに送信されます。デバイスCにスタティックマルチキャストルートを設定し、送信元に戻るパス上のデバイスCのRPFネイバーとしてデバイスBを指定できます。送信元からのマルチキャストデータは、デバイスA、デバイスB、デバイスCというパスに沿って送信されます。

RPFルートの作成

ユニキャストルートがブロックされると、RPFルートがないためにマルチキャスト転送が停止する場合があります。スタティックマルチキャストルートを設定して、RPFルートを作成できます。このようにして、マルチキャスト転送をガイドするマルチキャストルーティングエントリが作成されます。

図27 RPFルートの作成

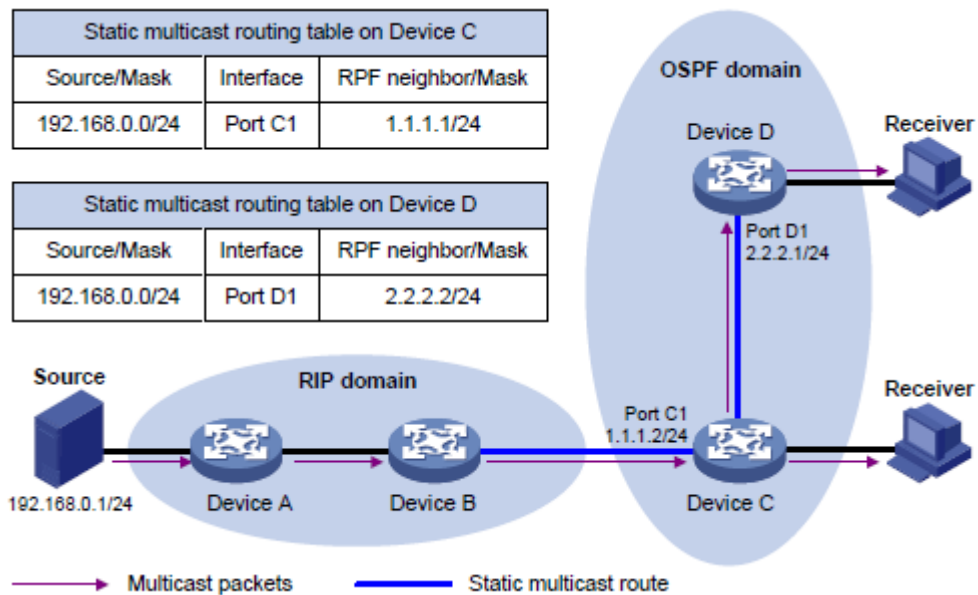


図27に示すように、RIPドメインとOSPFドメインは互いにユニキャストで分離されています。OSPFドメイン内のレシーバホストがRIPドメイン内のマルチキャスト送信元からマルチキャストパケットを受信するには、デバイスCとデバイスDを次のように設定する必要があります。

- デバイスCでは、マルチキャスト送信元にスタティックマルチキャストルートを設定し、RPFネイバーとしてデバイスBを指定します。
- デバイスDでは、マルチキャスト送信元にスタティックマルチキャストルートを設定し、RPFネイバーとしてデバイスCを指定します。

ユニキャストサブネット間のマルチキャスト転送

デバイスは、マルチキャストソースからのマルチキャストデータを転送ツリーに沿ってホップバイホップで転送しますが、一部のデバイスはネットワーク内でマルチキャストプロトコルをサポートしない場合があります。マルチキャストデータがIPマルチキャストをサポートしないデバイスに転送されると、転送パスがブロックされます。この場合、2つのユニキャストサブネットのエッジにあるデバイス間にトンネルを確立することによって、2つのユニキャストサブネット間でのマルチキャスト転送を有効にできます。

図28 トンネルを介したマルチキャストデータの送信

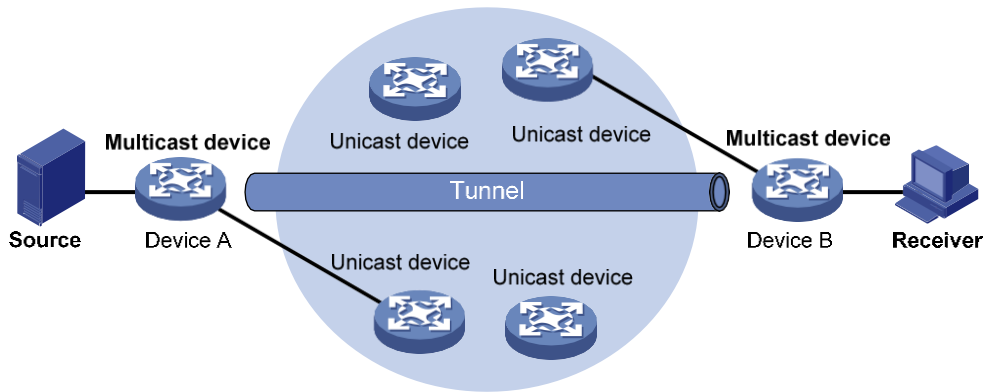


図28に示すように、デバイスAとデバイスBの間にトンネルが確立されます。デバイスAはマルチキャストデータをユニキャストIPパケットにカプセル化し、トンネルを介してユニキャストデバイス経由でデバイスBに転送します。次に、デバイスBはユニキャストIPヘッダーを取り除き、マルチキャストデータを受信側に転送し続けます。

このトンネルをマルチキャストトラフィック専用を使用するには、トンネルをマルチキャストルート専用の発信インターフェイスとして設定します。

Mtrace

mtraceは、マルチキャストグループデータが送信元から宛先に移動するパスをトレースするために使用されるtraceroute機能です。

デバイスの役割

mtraceには、次の役割があります。

- **Last-Hop Router(LHR):** LHRは、宛先と同じサブネット上にマルチキャスト対応インターフェイスがあり、特定のマルチキャストデータをサブネットに転送できるルータです。
- **First-Hop Router(FHR):** FHRは、マルチキャスト送信元に直接接続されているルータです。
- **Client:** クライアントは、mtraceを開始するルータです。

プロセス

mtraceのプロセスは次のとおりです。

1. クライアントは、mtrace Queryメッセージ(トレースする最大ホップ数を示すhopsフィールドを含む)を宛先に送信します。
2. LHRは、ローカル転送情報を追加して、受信したQueryメッセージをmtrace Requestメッセージに変換し、そのRequestメッセージを上流のネイバーに送信します。
3. トレースされたパスに沿った各ルータは、受信した要求メッセージにローカル転送情報を追加し、その要求メッセージを上流のネイバーに送信します。
4. FHRは、受信した要求メッセージにローカル転送情報を追加します。次に、要求メッセージをmtrace

応答メッセージに変換し、応答メッセージをクライアントに送信します。

5. クライアントは、Replyメッセージ内の転送情報を解釈し、その情報を表示します。

クライアントが待機時間内にReplyメッセージを受信しなかった場合、クライアントはパス上のどのデバイスでエラーが発生したかを判別するhop-by-hopトレース。hopsフィールドを1に設定してQueryメッセージを送信し、Replyメッセージを待機します。待機時間内にReplyメッセージを受信しなかった場合、クライアントはこのホップでエラーが発生したと判断します。待機時間内にReplyメッセージを受信した場合、クライアントはhopsフィールドの値を1増やしてQueryメッセージを送信し、Replyメッセージを待機します。このプロセスは、待機時間内にReplyメッセージを受信しなくなるまで続きます。

制約事項および注意事項: マルチキャストルーティングおよび転送の設定

デバイスは、セカンダリアドレスまたはアンナナードIPアドレスではなく、インターフェイスのプライマリIPアドレスを介してのみ、マルチキャストデータをルーティングおよび転送できます。プライマリおよびセカンダリIPアドレスとIPアンナナードの詳細については、『Layer 3 IP Services Configuration Guide』を参照してください。

マルチキャストルーティングおよび転送タスクの概要

マルチキャストルーティングおよび転送を設定するには、次の作業を実行します。

1. IPマルチキャストルーティングの有効化
2. (任意)スタティックマルチキャストルートの設定
3. (任意)最長プレフィクス一致原則の指定
4. (任意)マルチキャストロードスプリットの設定
5. (任意)マルチキャスト転送境界の設定
6. (任意)スーパーVLANのサブVLAN間のマルチキャスト転送の有効化
7. (省略可能) mtraceを使用したマルチキャストパスのトレース

マルチキャストルーティングおよび転送の前提条件

マルチキャストルーティングおよび転送を設定する前に、ドメイン内のすべてのデバイスがネットワーク層で相互運用できるように、ユニキャストルーティングプロトコルを設定します。

IPマルチキャストルーティングの有効化

IPマルチキャストルーティングの概要

レイヤ3マルチキャスト機能を設定する前に、IPマルチキャストルーティングを有効にします。

手順

1. システムビューに入ります。
System-view
2. IPマルチキャストルーティングを有効にし、MRIBビューを開始します。
multicast routing
デフォルトでは、IPマルチキャストルーティングは無効になっています。

スタティックマルチキャストルートの設定

スタティックマルチキャストルートについて

マルチキャスト送信元のスタティックマルチキャストルートを設定するには、その送信元からのマルチキャストトラフィックのRPFインターフェイスまたはRPFネイバーを指定します。

制約事項とガイドライン

スタティックマルチキャストルートは、そのルートが設定されているマルチキャストデバイス上でだけ有効になり、ネットワーク全体にアドバタイズされたり、他のデバイスに再配布されたりすることはありません。

手順

1. システムビューに入ります。

System-view

2. スタティックマルチキャストルートを設定します。

```
ip rpf-route-static source-address { mask-length | mask } { rpf-nbr-address | interface-type interface-number } [ preference preference ]
```

(任意)すべてのスタティックマルチキャストルートを削除します。

delete ip rpf-route-static

特定のスタティックマルチキャストルートを削除するには、`undo ip rpf-route-static`コマンドを使用します。すべてのスタティックマルチキャストルートを削除するには、`delete ip rpf-route-static`コマンドを使用します。

最長プレフィクス一致原則の指定

最長一致検索の原則について

RPFルート選択のための最長プレフィクス一致原則を使用するために、デバイスを有効にすることができます。RPFルート選択の詳細については、「RPFチェックプロセス」を参照してください。

手順

1. システムビューに入ります。

System-view

2. MRIBビューに入ります。

multicast routing

3. 最長プレフィクス照合方式を指定します。

longest-match

デフォルトでは、ルートプリファレンスの原則が使用されます。

マルチキャストロードスプリットの設定

マルチキャストロードスプリットについて

デバイスが複数のデータフローを送信元単位または送信元およびグループ単位で分割するように設定できます。これにより、トラフィック配信が最適化されます。

手順

1. システムビューに入ります。

System-view

2. MRIBビューに入ります。

multicast routing

3. マルチキャストロードスプリットを設定します。

```
load-splitting { source | source-group }
```

デフォルトでは、マルチキャストロードスプリットは無効になっています。

マルチキャストフォワーディング境界の設定

マルチキャスト転送境界について

インターフェイスを、マルチキャストグループ範囲のマルチキャスト転送境界として設定できます。インターフェイスは、グループ範囲のマルチキャストパケットを受信または転送できません。

制約事項とガイドライン

この設定の前にIPマルチキャストを有効にする必要はありません。

手順

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

```
interface interface-type interface-number
```

3. インターフェイスをマルチキャストグループ範囲のマルチキャスト転送境界として設定します。

```
multicast boundary group-address { mask-length | mask }  
デフォルトでは、インターフェイスはマルチキャスト転送境界ではありません。
```

スーパーVLANのサブVLAN間のマルチキャストフォワーディングの有効化

スーパーVLANのサブVLAN間のマルチキャストフォワーディングについて

スーパーVLANは、複数のサブVLANに関連付けられます。サブVLANはレイヤ2で相互に分離されます。スーパーVLANおよびサブVLANの詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

手順

1. システムビューに入ります。

System-view

2. VLANインターフェイスビューを開始します。

```
interface vlan-interface interface-number
```

3. スーパーVLANに関連付けられたサブVLAN間のマルチキャスト転送を有効にします。

```
multicast forwarding supervlan community
```

デフォルトでは、マルチキャストデータは、スーパーVLANに関連付けられたサブVLAN間で転送できません。

4. システムビューに戻ります。

```
quit
```

5. ユーザービューに戻ります。

quit

6. スーパーVLANインターフェイスを着信インターフェイスとするすべてのマルチキャスト転送エントリをクリアします。

```
reset multicast forwarding-table incoming-interface { interface-type interface-number }
```

multicast forwarding supervlan communityコマンドが有効になるのは、このステップを実行した後だけです。

mtraceを使用してマルチキャストパスをトレースする

mtrace1を使用してマルチキャストパスをトレースする

mtraceバージョン1(mtrace1)を使用してマルチキャストパスをトレースするには、任意のビューで次のコマンドを実行します。

```
mtrace [ v1 ] { source-address | group-address } * [ destination address ]  
[ verbose ]
```

mtrace2を使用してマルチキャストパスをトレースする

制約事項とガイドライン

mtraceを正常に実行するには、他のモジュールで使用されているUDPポート番号を指定しないでください。トレースパス上のすべてのデバイスで同じUDPポート番号を指定する必要があります。

手順

1. システムビューに入ります。

System-view

2. (任意)mtraceが使用するUDPポート番号を指定します。

```
mtrace-service port number
```

デフォルトでは、mtraceはUDPポート番号10240を使用します。

3. マルチキャストパスをトレースするには、mtrace version 2(mtrace2)を使用します。

```
mtrace v2 { source-address | group-address } * [ destination address |  
port number | wait-time time | max-hop count ] * [ verbose ]
```

任意のビューでこのコマンドを実行します。

このコマンドで指定するUDPポート番号は、**mtrace-service port**コマンドで指定するポート番号と同じでなければなりません。

マルチキャストルーティングおよびフォワーディング 用の表示およびメンテナンスコマンド

△注意:

リセットコマンドは、マルチキャストデータ送信障害を引き起こす可能性があります。

任意のビューで**display**コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
MRIBで管理されるインターフェイスに関する情報を表示します。	display mrib interface [<i>interface-type interface-number</i>]
マルチキャスト境界情報を表示します。	display multicast boundary [<i>group-address [mask-length mask]</i>] [interface interface-type interface-number]
マルチキャスト高速フォワーディングエントリを表示します。	display multicast fast-forwarding cache [<i>source-address group-address</i>] * [slot slot-number]
マルチキャスト転送イベントの統計情報を表示します。	display multicast forwarding event [slot slot-number]
マルチキャストフォワーディングエントリを表示します。	display multicast forwarding-table [<i>source-address [mask { mask-length mask }] group-address [mask { mask-length mask }] incoming-interface interface-type interface-number outgoing-interface { exclude include match } interface-type interface-number slot slot-number statistics</i>] *
マルチキャストルーティングエントリを表示します。	display multicast routing-table [<i>source-address [mask { mask-length mask }] group-address [mask { mask-length mask }] incoming-interface interface-type interface-number outgoing-interface { exclude include match } interface-type interface-number</i>] *
スタティックマルチキャストルーティングエントリを表示します。	display multicast routing-table static [<i>source-address { mask-length mask }</i>]

マルチキャスト送信元のRPF情報を表示します。	display multicast rpf-info <i>source-address</i> [<i>group-address</i>]
マルチキャスト高速フォワーディングエントリをクリアします。	reset multicast fast-forwarding cache { { <i>source-address</i> <i>group-address</i> } * all } [slot <i>slot-number</i>]
マルチキャスト転送イベントの統計情報をクリアします。	reset multicast forwarding event
マルチキャストフォワーディングエントリをクリアします。	reset multicast forwarding-table { { <i>source-address</i> [mask { <i>mask-length</i> <i>mask</i> }] <i>group-address</i> [mask { <i>mask-length</i> <i>mask</i> }] incoming-interface { <i>interface-type</i> <i>interface-number</i> } } * all }
マルチキャストルーティングエントリをクリアします。	reset multicast routing-table { { <i>source-address</i> [mask { <i>mask-length</i> <i>mask</i> }] <i>group-address</i> [mask { <i>mask-length</i> <i>mask</i> }] incoming-interface <i>interface-type</i> <i>interface-number</i> } * all }

注:

- マルチキャストルーティングエントリをクリアすると、関連するマルチキャストフォワーディングエントリもクリアされます。
 - マルチキャストフォワーディングエントリをクリアすると、関連するマルチキャストルーティングエントリもクリアされます。
-

マルチキャストルーティングおよびフォワーディング の設定例

例:RPFルートの変更

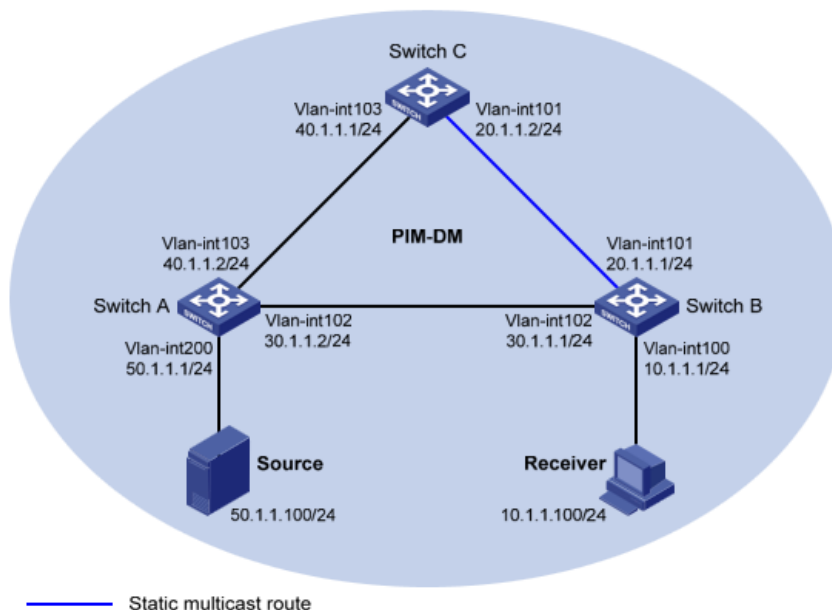
ネットワークの設定

図29に示します。

- PIM-DMはネットワーク上で動作します。
- ネットワーク上のすべてのスイッチは、マルチキャストをサポートします。
- スイッチA、スイッチB、およびスイッチCはOSPFを実行します。
- 通常、レシーバホストは、スイッチAからスイッチBへのパス(ユニキャストルートと同じ)を介して、送信元からマルチキャストデータを受信できます。

送信元からのマルチキャストデータがパス(スイッチA～スイッチC～スイッチB)を介して受信側に送信されるようにスイッチを設定します。これはユニキャストルートとは異なります。

図29 ネットワークダイアグラム



手順

1. 図29に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
2. PIM-DMドメイン内のスイッチにOSPFを設定します(詳細は省略)。
3. IPマルチキャストルーティングを有効にし、IGMPとPIM-DMを有効にします。

On Switch B, enable IP multicast routing.

```
<SwitchB> system-view
```

```
[SwitchB] multicast routing
```

```
[SwitchB-mrib] quit
# Enable IGMP on the receiver-side interface VLAN-interface 100.
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] igmp enable
[SwitchB-Vlan-interface100] quit
# Enable PIM-DM on other interfaces.
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim dm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] pim dm
[SwitchB-Vlan-interface102] quit
# On Switch A, enable IP multicast routing.
<SwitchA> system-view
[SwitchA] multicast routing
[SwitchA-mrib] quit
# Enable PIM-DM on each interface.
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] pim dm
[SwitchA-Vlan-interface200] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim dm
[SwitchA-Vlan-interface102] quit
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim dm
[SwitchA-Vlan-interface103] quit
# Enable IP multicast routing and PIM-DM on Switch C in the same way Switch A is configured.
(Details not shown.)
```

4. スイッチBの送信元のRPF情報を表示します。

```
[SwitchB] display multicast rpf-info 50.1.1.100
RPF information about source 50.1.1.100:
  RPF interface: Vlan-interface102, RPF neighbor: 30.1.1.2
  Referenced route/mask: 50.1.1.0/24
  Referenced route type: igp
  Route selection rule: preference-preferred
  Load splitting rule: disable
```

この出力は、スイッチB上の現在のRPFルートがユニキャストルーティングによって提供されていることを示しています。

RPFネイバーはスイッチAです。

5. スイッチBにスタティックマルチキャストルートを設定し、送信元へのルート上のRPFネイバーとしてスイッチCを指定します。

```
[SwitchB] ip rpf-route-static 50.1.1.0 24 20.1.1.2
```

設定の確認

#スイッチBの送信元のRPF情報を表示します。

[SwitchB] display multicast rpf-info 50.1.1.100

RPF information about source 50.1.1.100:

RPF interface: Vlan-interface101, RPF neighbor: 20.1.1.2

Referenced route/mask: 50.1.1.0/24

Referenced route type: multicast static

Route selection rule: preference-preferred

Load splitting rule: disable

出力には次の情報が表示されます。

- スイッチBのRPFルートは、設定済みのスタティックマルチキャストルートです。
- スイッチBのRPFネイバーはスイッチCです。

例:RPFルートの作成

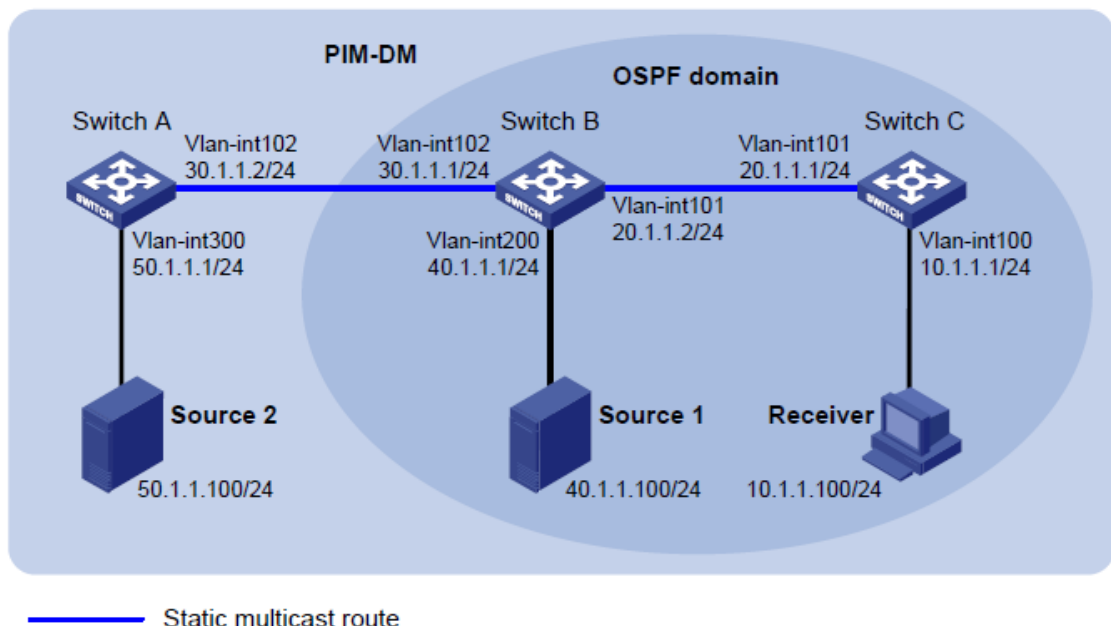
ネットワークの設定

図30に示します。

- PIM-DMはネットワーク上で動作します。
- ネットワーク上のすべてのスイッチは、IPマルチキャストをサポートします。
- スイッチBとスイッチCはOSPFを実行し、スイッチAへのユニキャストルートはありません。
- 通常、レシーバホストは、OSPFドメインのSource 1からマルチキャストデータを受信します。

レシーバホストがOSPFドメインの外部にあるSource 2からマルチキャストデータを受信するように、スイッチを設定します。

図30 ネットワークダイアグラム



手順

1. 図30に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)

2. スイッチBとスイッチCにOSPFを設定します(詳細は省略)。
3. IPマルチキャストルーティングを有効にし、IGMPとPIM-DMを有効にします。

On Switch C, enable IP multicast routing.

```
<SwitchC> system-view
[SwitchC] multicast routing
[SwitchC-mrib] quit
```

Enable IGMP on the receiver-side interface VLAN-interface 100.

```
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] igmp enable
[SwitchC-Vlan-interface100] quit
```

Enable PIM-DM on VLAN-interface 101.

```
[SwitchC] interface vlan-interface 101
[SwitchC-Vlan-interface101] pim dm
[SwitchC-Vlan-interface101] quit
```

On Switch A, enable IP multicast routing.

```
<SwitchA> system-view
[SwitchA] multicast routing
[SwitchA-mrib] quit
```

Enable PIM-DM on each interface.

```
[SwitchA] interface vlan-interface 300
[SwitchA-Vlan-interface300] pim dm
[SwitchA-Vlan-interface300] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim dm
[SwitchA-Vlan-interface102] quit
```

Enable IP multicast routing and PIM-DM on Switch B in the same way Switch A is configured.
(Details not shown.)

4. スイッチBおよびスイッチCの送信元2のRPF情報を表示します。

```
[SwitchB] display multicast rpf-info 50.1.1.100
[SwitchC] display multicast rpf-info 50.1.1.100
```

スイッチBまたはスイッチCにはSource 2へのRPFルートが存在しないため、出力は表示されません。

5. スタティックマルチキャストルートを設定します。

#スイッチBにスタティックマルチキャストルートを設定し、スイッチAをSource 2へのルート上のRPFネイバーとして指定します。

```
[SwitchB] ip rpf-route-static 50.1.1.0 24 30.1.1.2
```

#スイッチCにスタティックマルチキャストルートを設定し、スイッチBをSource 2へのルート上のRPFネイバーとして指定します。

```
[SwitchC] ip rpf-route-static 10.1.1.0 24 20.1.1.2
```

設定の確認

#スイッチB上のソース2のRPF情報を表示します。

```
[SwitchB] display multicast rpf-info 50.1.1.100
```

RPF information about source 50.1.1.100:

RPF interface: Vlan-interface102, RPF neighbor: 30.1.1.2

Referenced route/mask: 50.1.1.0/24

Referenced route type: multicast static

Route selection rule: preference-preferred

Load splitting rule: disable

#スイッチCの送信元2のRPF情報を表示します。

[SwitchC] display multicast rpf-info 50.1.1.100

RPF information about source 50.1.1.100:

RPF interface: Vlan-interface101, RPF neighbor: 20.1.1.2

Referenced route/mask: 50.1.1.0/24

Referenced route type: multicast static

Route selection rule: preference-preferred

Load splitting rule: disable

この出力は、Source 2へのRPFルートがスイッチBおよびスイッチCに存在することを示しています。これらのルートは、設定済みのスタティックルートです。

マルチキャストルーティングおよびフォワーディング のトラブルシューティング

スタティックマルチキャストルートの障害

症状

ルータ上で有効になっているダイナミックルーティングプロトコルはなく、インターフェイスの物理ステータスとリンクレイヤステータスは両方ともアップですが、スタティックマルチキャストルートに障害が発生します。

解決方法

この問題を解決するには、次の手順を実行し

1. スタティックマルチキャストルートに関する情報を表示するには、**display multicast routing-table static**コマンドを使用します。スタティックマルチキャストルートが正しく設定されていること、およびスタティックマルチキャストルーティングテーブルにルートエントリが存在することを確認します。
2. スタティックマルチキャストルートをRPFネイバーに接続するインターフェイスのタイプを確認します。インターフェイスがポイントツーポイントインターフェイスでない場合は、必ずRPFネイバーのアドレスを指定してください。
3. 問題が解決しない場合は、H3Cサポートに連絡してください。

IGMPの設定

IGMPの概要

Internet Group Management Protocol(IGMP)は、レイヤ3マルチキャストデバイスと、直接接続されたサブネット上のホストとの間のマルチキャストグループメンバーシップを確立し、維持します。

IGMPのバージョン

IGMPには次のバージョンがあります。

- IGMPv1(RFC 1112で定義)
- IGMPv2(RFC 2236で定義)
- IGMPv3(RFC 3376で定義)

すべてのIGMPバージョンはASMモデルをサポートしています。IGMPv3はSSMモデルを直接実装できます。SSMモデルを実装するには、IGMPv1およびIGMPv2がIGMP SSMマッピング機能と連携する必要があります。ASMおよびSSMモデルの詳細については、「マルチキャストの概要」を参照してください。

IGMPv1の概要

IGMPv1は、クエリーおよび応答メカニズムに基づいて、マルチキャストグループメンバーシップを管理します。

同じサブネット上でIGMPを実行するすべてのデバイスは、ホストからIGMPメンバーシップレポートメッセージ(レポートと呼ばれる)を取得できます。ただし、IGMPクエリーメッセージ(クエリーと呼ばれる)を送信するためにIGMPクエリーアとして機能できるのは、1つのデバイスだけです。クエリーア選択メカニズムは、サブネット上でIGMPクエリーアとして機能するデバイスを決定します。

IGMPv1では、マルチキャストルーティングプロトコル(PIMなど)によって選択されたDRがIGMPクエリーアとして動作します。DRの詳細については、「PIMの設定」を参照してください。

図31 IGMPクエリーおよびレポート

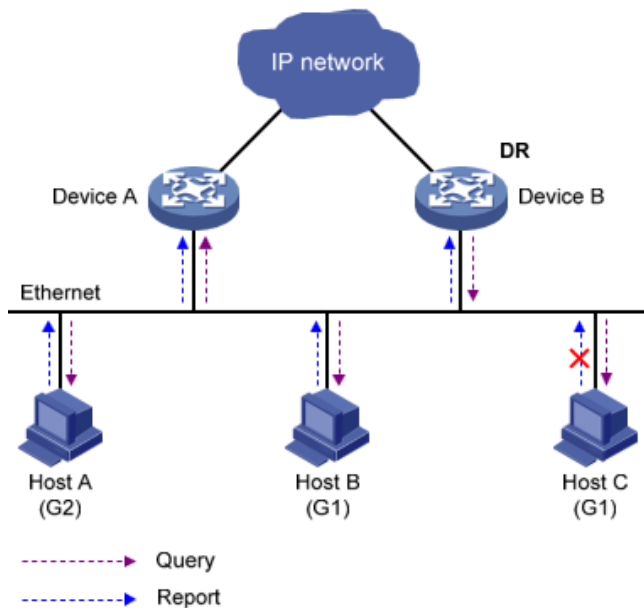


図31に示すように、ホストBおよびホストCは、マルチキャストグループG1宛てのマルチキャストデータに関心があります。ホストAは、G2宛てのマルチキャストデータに関心があります。次のプロセス

に、ホストがマルチキャストグループに加入する方法、およびIGMPクエリア(図31のデバイスB)がマルチキャストグループメンバーシップを維持する方法を示します。

1. ホストは、IGMPクエリーを待たずに、参加したいマルチキャストグループに非送信請求IGMPレポートを送信します。
2. IGMPクエリアは、定期的にIGMPクエリー(宛先アドレス224.0.0.1)をローカルサブネット上のすべてのホストおよびデバイスにマルチキャストします。
3. クエリーメッセージを受信した後、レポート遅延タイマーの期限が切れたホストは、まずマルチキャストグループG1にIGMPレポートを送信して、G1のメンバーシップをアナウンスします。この例では、ホストBがレポートメッセージを送信します。ホストBからレポートを受信した後、ホストCはG1のレポートを抑制します。

IGMPデバイスは、G1に最低1つのメンバーがあることをすでに認識しているため、他のメンバーは自分のメンバーシップを報告する必要はありません。ホストIGMPレポート抑制と呼ばれるこのメカニズムは、ローカルサブネット上のトラフィックを削減するのに役立ちます。

4. 同時に、ホストAはクエリーを受信した後、マルチキャストグループG2にレポートを送信します。
5. クエリーおよび応答プロセスを通じて、IGMPデバイス(デバイスAおよびデバイスB)は、ローカルサブネットにG1およびG2のメンバーがあることを判別します。デバイス上のマルチキャストルーティングプロトコル(PIMなど)は、(*,G1)および(*,G2)マルチキャスト転送エントリを生成します。アスタリスク(*)は任意のマルチキャスト送信元を表します。これらのエントリは、後続のマルチキャスト転送の基礎となります。
6. G1またはG2にアドレス指定されたマルチキャストデータがIGMPデバイスに到達すると、デバイス

はマルチキャスト転送テーブルを検索します。(*,G1)または(*,G2)エントリに基づいて、デバイスはマルチキャストデータをローカルサブネットに転送します。その後、サブネット上のレシーバはデータを受信できます。

IGMPv1では、Leaveグループメッセージ(Leaveメッセージと呼ばれることが多い)は定義されていません。IGMPv1ホストは、マルチキャストグループを脱退するときに、そのマルチキャストグループへのレポートの送信を停止します。サブネットにマルチキャストグループのメンバーがない場合、IGMPデバイスはそのマルチキャストグループ宛てのレポートを受信しません。この場合、デバイスは一定期間後にそのマルチキャストグループの情報をクリアします。

IGMPv2の機能拡張

IGMPv2はIGMPv1と下位互換性があり、クエリーア選定メカニズムと脱退グループメカニズムが導入されました。

クエリーア選定メカニズム

IGMPv1では、レイヤ3マルチキャストルーティングプロトコル(PIMなど)によって選定されたDRがクエリーアとして機能します。

IGMPv2では、独立したクエリーア選定メカニズムが導入されました。クエリーア選定プロセスは次のとおりです。

1. 最初は、すべてのIGMPv2デバイスが自身をクエリーアと見なします。各デバイスは、IGMP一般クエリーメッセージ(一般クエリーと呼ばれる)をローカルサブネット上のすべてのホストおよびデバイスに送信します。宛先アドレスは224.0.0.1です。
2. 一般的なクエリーを受信すると、すべてのIGMPv2デバイスは、クエリーの送信元IPアドレスを自身のインターフェイスアドレスと比較します。最小のIPアドレスを持つデバイスがクエリーアになります。他のすべてのIGMPv2デバイスは非クエリーアになります。
3. すべての非クエリーアは、他のクエリーアの存在タイマーを開始します。タイマーが切れる前にデバイスがクエリーアからIGMPクエリーを受信した場合、このタイマーをリセットします。そうでない場合、デバイスはクエリーアがタイムアウトしたと見なします。この場合、デバイスは新しいクエリーアの選定プロセスを開始します。

“脱退グループ”メカニズム

IGMPv1では、ホストがマルチキャストグループを脱退する場合、マルチキャストデバイスに通知を送信しません。マルチキャストデバイスは、最大応答時間を使用して、グループにメンバーがいるかどうかを判断します。これにより、脱退の遅延が増加します。

IGMPv2では、ホストがマルチキャストグループから脱退する場合、次のプロセスが発生します。

1. ホストは、ローカルサブネット上のすべてのデバイスにリーブメッセージを送信します。リーブメッセージの宛先アドレスは224.0.0.2です。
2. Leaveメッセージを受信した後、クエリーアは設定可能な数のIGMPホストが脱退するグループへのグループ固有のクエリー。メッセージの宛先アドレスフィールドとグル

ープアドレスフィールドの両方が、クエリーされるマルチキャストグループのアドレスです。

3. グループ内の残りのメンバーの1つ(サブネット上に存在する場合)は、グループ固有のクエリーでアドバタイズされる最大応答時間内にレポートを送信する必要があります。
4. 最大応答タイマーの期限が切れる前にクエリーアがグループのレポートを受信した場合、クエリーアはグループのメンバーシップを維持します。それ以外の場合、クエリーアはローカルサブネットにグループのメンバーホストがないと見なし、グループのメンバーシップの維持を停止します。

IGMPv3の機能拡張

IGMPv3は、IGMPv1およびIGMPv2に基づいており、これらと互換性があります。ホストの制御機能と、IGMPデバイスのクエリーおよびレポート機能を拡張します。

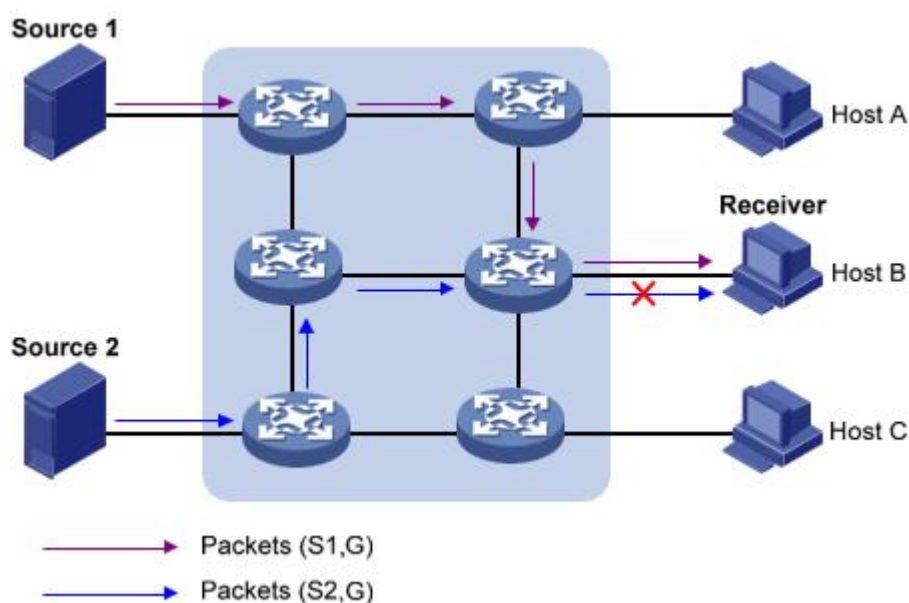
ホストの制御能力の強化

IGMPv3では、2つの送信元フィルタリングモード(IncludeおよびExclude)が導入されました。これらのモードにより、ホストは、指定されたマルチキャスト送信元からのマルチキャストデータを受信または拒否できます。ホストがマルチキャストグループに加入すると、次のいずれかが発生します。

- ホストがS1、S2、...のような特定のソースからマルチキャストデータを受信することを期待する場合、「Include Sources(S1, S2, ...)」として示されるフィルターモードでレポートを送信します。
- もしホストがS1、S2、...のような特定のソースからのマルチキャストデータを拒否することを期待するのなら、「Exclude Sources(S1, S2, ...)」として示されるフィルターモードで報告を送ります。

図32に示すように、ネットワークにはSource 1(S1)とSource 2(S2)の2つのマルチキャストソースがあります。これらのソースは両方ともマルチキャストグループGにマルチキャストデータを送信できます。ホストBは、Source 2からではなく、Source 1からG宛てのマルチキャストデータを受信したいと考えています。

図32 送信元およびグループ固有のマルチキャストトラフィックのフローパス



IGMPv1またはIGMPv2では、ホストBはマルチキャストグループGに加入するときにマルチキャストソースを選択できません。ソース1とソース2の両方からのマルチキャストストリームは、必要であるかどうかにかかわらず、ホストBに流れます。

IGMPv3では、ホストBは、マルチキャストグループG宛てのマルチキャストデータをSource 1から受信する必要があるが、Source 2からは受信しないことを明示的に表現できます。

クエリー機能とレポート機能の強化

IGMPv3では、グループレコードを伝送するIGMPグループ/ソースクエリーおよびIGMPレポートが導入されました。

- ソースアドレスを運ぶ問合せメッセージ

IGMPv3はIGMPv1およびIGMPv2と互換性があり、IGMP一般クエリーおよびIGMPグループ固有クエリーをサポートします。また、IGMPグループおよび送信元固有クエリーも導入されています。

- 一般的な問合せはグループアドレスやソースアドレスを運びません。
- グループ特定問合せはグループアドレスを運びますが、ソースアドレスを運びません。
- グループおよびソース特定問合せはグループアドレスと1つ以上のソースアドレスを運びます。

- 複数のグループレコードを含むレポート

IGMPv1またはIGMPv2レポートとは異なり、IGMPv3レポートは224.0.0.22を宛先とし、1つ以上のグループレコードを含みます。各グループレコードには、マルチキャストグループアドレスとマルチキャスト送信元アドレスリストが含まれます。

グループレコードには、次のカテゴリが含まれます。

- **IS_IN**: 現在のフィルタリングモードはIncludeです。レポート送信者は、Source Addressフィールドで指定された送信元からのマルチキャストデータだけを要求します。
- **IS_EX**: 現在のフィルタリングモードはExcludeです。レポート送信者は、Source Addressフィールドで指定されたソースを除く任意のソースからのマルチキャストデータを要求します。
- **TO_IN**: フィルタリングモードがExcludeからIncludeに変更されました。
- **TO_EX**: フィルタリングモードがIncludeからExcludeに変更されました。
- **ALLOW**: Source Addressフィールドには、受信者がデータの取得を希望する追加ソースのリストが含まれます。現行のフィルターモードがIncludeの場合、これらのソースはマルチキャストソースリストに追加されます。現行のフィルターモードがExcludeの場合、これらのソースはマルチキャストソースリストから削除されます。
- **BLOCK**: Source Addressフィールドには、受信者がデータの取得を希望しないソースのリストが含まれます。現行のフィルターモードがIncludeの場合、これらのソースはマルチキャストソースリストから削除されます。現行のフィルターモードがExcludeの場合、これらのソースはマルチキャストソースリストに追加されます。

IGMP SSMマッピング

IGMPv3ホストは、IGMPv3レポートでマルチキャスト送信元を明示的に指定できます。レポートから、IGMPデバイスはマルチキャスト送信元アドレスを取得し、SSMサービスを直接提供できます。ただし、IGMPv1またはIGMPv2ホストは、IGMPv1またはIGMPv2レポートでマルチキャスト送信元を指定できません。

IGMP SSMマッピング機能により、IGMPデバイスはIGMPv1またはIGMPv2ホストにSSMサポートを提供できます。デバイスは、設定されたIGMP SSMマッピングに基づいて、IGMPv1またはIGMPv2レポートの(*,G)を(G, INCLUDE, (S1, S2.))に変換します。

図33 IGMP SSMマッピング

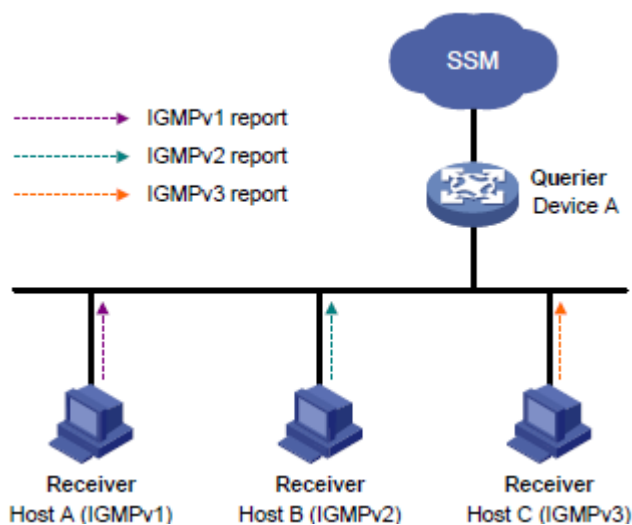


図33に示すように、SSMネットワークでは、ホストA、ホストB、およびホストCがそれぞれIGMPv1、IGMPv2、およびIGMPv3を実行します。ホストAおよびホストBにSSMサービスを提供するには、デバイスAでIGMP SSMマッピング機能を設定する必要があります。

IGMP SSMマッピングが設定されると、デバイスAは受信したIGMPv1またはIGMPv2レポートのマルチキャストグループアドレスGをチェックし、次の処理を実行します。

- GがSSMグループ範囲にない場合は、デバイスAがASMサービスを提供します。
- GがSSMグループ範囲内にあるが、どのIGMP SSMマッピングとも一致しない場合、デバイスAはレポートをドロップします。
- GがSSMグループ範囲内にあり、IGMP SSMマッピングと一致する場合、デバイスAはレポートの(*,G)を(G, INCLUDE, (S1, S2.))に変換してSSMサービスを提供します。

注:

IGMP SSMマッピング機能は、IGMPv3レポートを処理しません。

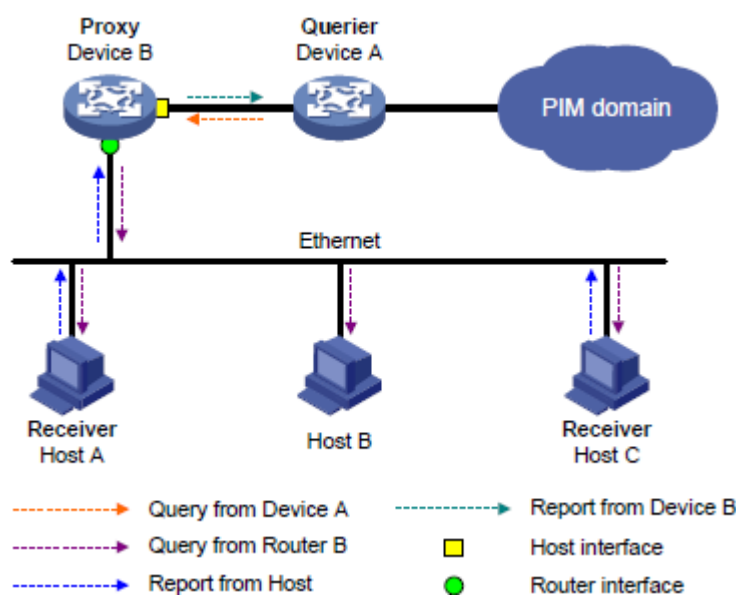
SSMグループ範囲の詳細については、「PIMの設定」を参照してください。

IGMPプロキシ

図34に示すように、単純なツリー型トポロジでは、エッジデバイス上でPIMなどのマルチキャストルーティングプロトコルを実行する必要はありません。代わりに、これらのデバイス上でIGMPプロキシを設定できます。IGMPプロキシを設定すると、エッジデバイスはIGMPプロキシとして機能します。

- アップストリームIGMPクエリアの場合、IGMPプロキシデバイスはホストとして動作します。
- ダウンストリームレシーバホストの場合、IGMPプロキシデバイスはIGMPクエリアとして機能します。

図34 IGMPプロキシ



IGMPプロキシでは、次のタイプのインターフェイスが定義されています。

- **Host interface:** マルチキャスト転送ツリーのルート方向にあるインターフェイス。ホストインターフェイスは、IGMPを実行するレシーバホストとして機能します。このインターフェイスでは、IGMPプロキシを有効にする必要があります。このインターフェイスは「プロキシインターフェイス」とも呼ばれます。
- **Router interface:** マルチキャスト転送ツリーのリーフ方向のインターフェイス。ルータインターフェイスは、IGMPを実行しているルータとして動作します。このインターフェイスでは、IGMPを設定する必要があります。

IGMPプロキシデバイスは、すべてのルータインターフェイスのグループメンバーシップを保存するグループメンバーシップデータベースを維持します。ホストインターフェイスとルータインターフェイスは、このメンバーシップデータベースに基づいてアクションを実行します。

- ホストインターフェイスは、メンバーシップデータベースに従ってクエリーに応答するか、データベースが変更されたときにJoin/Leaveメッセージを送信します。
- ルータインターフェイスは、受信したIGMPレポートに基づいてクエリア選定に参加し、クエリーを送信し、メンバーシップを維持します。

プロトコルと標準

- RFC 1112『Host Extensions for IP Multicasting』
- RFC 2236『Internet Group Management Protocol, Version 2』(インターネットグループ管理プロトコル、バージョン2)
- RFC 3376『Internet Group Management Protocol, Version 3』(インターネットグループ管理プロトコル、バージョン3)

IGMPタスクの概要

IGMPを設定するには、次の作業を実行します。

1. IGMPの有効化
2. (任意)基本的なIGMP機能の設定
 - IGMPバージョンの指定
 - スタティックグループメンバーの設定
 - マルチキャストグループポリシーの設定
3. (任意)IGMPパフォーマンスの調整
 - IGMPクエリーおよび応答パラメータの設定
 - 高速脱退処理の有効化
4. (任意)IGMP SSMマッピングの設定
5. (任意)IGMPプロキシの設定
 - IGMPプロキシの有効化
 - 非クエリーアインターフェイス上のマルチキャストフォワーディングの有効化
 - IGMPプロキシインターフェイスのマルチキャストロードスプリットの設定
6. (任意)IGMP NSRの有効化
7. (任意)発信IGMPプロトコルパケットのDSCP値の設定

IGMPの前提条件

IGMPを設定する前に、すべてのデバイスがネットワーク層で相互運用できるように、ユニキャストルーティングプロトコルを設定する必要があります。

IGMPの有効化

制約事項とガイドライン

マルチキャストグループメンバーシップが確立され、維持されるインターフェイスでIGMPを有効にします。

手順

1. システムビューに入ります。

System-view

2. IPマルチキャストルーティングを有効にし、MRIBビューを開始します。

multicast routing

デフォルトでは、IPマルチキャストルーティングは無効になっています。

このコマンドの詳細については、『IP Multicast Command Reference』を参照してください。

3. システムビューに戻ります。

quit

4. インターフェイスビューに入ります。

interface *interface-type interface-number*

5. IGMPを有効にします。

igmp enable

デフォルトでは、IGMPは無効です。

基本的なIGMP機能の設定

IGMPバージョンの指定

制約事項とガイドライン

IGMPを正しく動作させるには、同じサブネット上のすべてのデバイスに同じIGMPバージョンを指定します。

手順

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

interface *interface-type* *interface-number*

3. インターフェイスのIGMPバージョンを指定します。

igmp version *version-number*

デフォルトでは、インターフェイスのIGMPバージョンはIGMPv2です。

スタティックグループメンバーの設定

スタティックグループメンバーについて

インターフェイスをマルチキャストグループのスタティックグループメンバーとして設定できます。これにより、インターフェイスは常に、指定されたマルチキャストグループ宛てのマルチキャストデータを受信できます。

スタティックグループメンバーは、IGMPクエリーに応答しません。インターフェイス上でこの設定を完了またはキャンセルした場合、インターフェイスは非送信請求IGMPレポートまたはLeaveメッセージを送信しません。

制約事項とガイドライン

スタティックグループメンバーとして設定されるインターフェイスには、以下の制限があります。

- インターフェイスでIGMPとPIM-SMが有効になっている場合、そのインターフェイスはPIM-SM DRである必要があります。
- インターフェイスがIGMP対応であってもPIM-SM対応でない場合は、IGMPクエリーアである必要があります。PIM-SMおよびDRの詳細については、「PIMの設定」を参照してください。

手順

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

interface *interface-type interface-number*

3. インターフェイスをスタティックグループメンバーとして設定します。

igmp static-group *group-address* [**source** *source-address*]

マルチキャストグループポリシーの設定

マルチキャストグループポリシーについて

この機能は、マルチキャストグループとオプションの送信元を指定するACLを使用して、インターフェイスがIGMPレポートをフィルタリングできるようにします。これは、インターフェイスに接続されたホストが加入できるマルチキャストグループを制御するために使用されます。

制約事項とガイドライン

スタティックグループメンバーはIGMPレポートを送信しないので、このコンフィギュレーションはスタティックグループメンバーに影響を与えません。

手順

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

interface *interface-type interface-number*

3. マルチキャストグループポリシーを設定します。

igmp group-policy *ipv4-acl-number* [*version-number*]

IGMPパフォーマンスの調整

IGMPクエリーおよび応答パラメータの設定

IGMPクエリーおよび応答パラメータについて

IGMPクエリーおよび応答パラメータは、次のとおりです。

- **IGMP querier's robustness variable:** パケット損失時にIGMPクエリーを再送信する回数。ロバストネス変数が高いほどIGMPクエリーはより堅牢になりますが、マルチキャストグループのタイムアウト時間が長くなります。
- **IGMP startup query interval:** IGMPクエリーが起動時にIGMP一般クエリーを送信する間隔。
- **IGMP startup query count:** IGMPクエリーが起動時に送信するIGMP一般クエリーの数。
- **IGMP general query interval:** IGMPクエリーがIGMP一般クエリーを送信してネットワーク上のマルチキャストグループメンバーをチェックする間隔。
- **IGMP last member query interval:** IGMPv2では、クエリーがLeaveメッセージを受信した後にグループ固有のクエリーを送信するインターバルを設定します。IGMPv3では、マルチキャスト送信元およびグループマッピングを変更するレポートを受信した後に、クエリーがグループおよび送信元固有のクエリーを送信するインターバルを設定します。
- **IGMP last member query count:** IGMPv2では、クエリーがLeaveメッセージを受信した後に送信するグループ固有クエリーの数を設定します。IGMPv3ではマルチキャスト送信元およびグループマッピングを変更するレポートを受信した後に、クエリーが送信するグループ/送信元固有のクエリー。
- **IGMP maximum response time:** レシーバがIGMP一般クエリーにレポートで応答するまでの最大時間。このグループ単位のタイマーは、0からIGMPクエリーで指定された最大応答時間までの範囲のランダム値に初期化されます。グループのタイマー値が0に減少すると、レシーバはグループにIGMPレポートを送信します。
- **IGMP other querier present timer:** 非クエリーがIGMP一般クエリーを受信した後のIGMPクエリーのIGMP他クエリー存在タイマーの寿命。このタイマーが切れたときに非クエリーが新しいクエリーを受信しない場合、非クエリーはクエリーが失敗したと見なし、新しいクエリーの選択を開始します。

制約事項とガイドライン

IGMPクエリーが頻繁に変更されないようにするには、IGMP一般クエリー間隔よりも大きいIGMP他クエリー存在タイマーを設定します。さらに、同じサブネット上のすべてのIGMPデバイスに対して同じIGMP他クエリー存在タイマーを設定します。

マルチキャストレシーバを誤って削除しないようにするには、IGMP一般クエリー間隔をIGMP一般クエリーの最大応答時間よりも長く設定します。

IGMPクエリーへの応答を高速化し、IGMPレポートトラフィックバーストの原因となる同時タイマーの期限

切れを回避するには、適切な最大応答時間を設定します。

- IGMP一般クエリーの場合、最大応答時間はmax-response-timeで指定します。
- IGMPグループ固有クエリーおよびIGMPグループ/送信元固有クエリーの場合、最大応答時間はIGMP最終メンバークエリーインターバルと等しくなります。

次の設定は、IGMPv2およびIGMPv3を実行するデバイスでだけ有効です。

- IGMP一般クエリーの最大応答時間。
- IGMP最終メンバークエリーインターバル。
- IGMP最終メンバークエリー数。
- IGMPの他のクエリーアの存在間隔。

IGMPクエリーおよび応答パラメータは、IGMPビューのすべてのインターフェイスに対してグローバルに設定することも、インターフェイスビューのインターフェイスに対して設定することもできます。インターフェイス固有の設定は、グローバル設定よりも優先されます。

IGMPクエリーおよび応答パラメータのグローバルな設定

1. システムビューに入ります。

System-view

2. IGMPビューに入ります。

igmp

3. IGMPクエリーアのロバストネス変数を設定します。

robust-count *count*

デフォルトでは、IGMPクエリーアのロバストネス変数は2です。

4. IGMPスタートアップクエリーインターバルを設定します。

startup-query-interval *interval*

デフォルトでは、IGMPスタートアップクエリーインターバルは、IGMP一般クエリーインターバルの4分の1に等しくなります。

5. IGMPスタートアップクエリーカウントを設定します。

startup-query-count *count*

デフォルトでは、IGMP起動クエリーカウントはIGMPクエリーアのロバストネス変数と同じです。

6. IGMP一般クエリーインターバルを設定します。

query-interval *interval*

デフォルトでは、IGMP一般クエリーインターバルは125秒です。

7. IGMP最終メンバークエリーインターバルを設定します。

last-member-query-interval *interval*

デフォルトでは、IGMP最終メンバークエリーインターバルは1秒です。

8. IGMP最終メンバークエリーカウントを設定します。

last-member-query-count *count*

デフォルトでは、IGMP最終メンバークエリーカウントは、IGMPクエリーアのロバストネス変数と同じ

です。

9. IGMP一般クエリーの最大応答時間を設定します。

max-response-time *time*

デフォルトでは、IGMP一般クエリーの最大応答時間は10秒です。

10. IGMPの他のクエリーアの存在タイマーを設定します。

other-querier-present-interval *interval*

デフォルトでは、IGMPの他のクエリーアの存在タイマーは、[IGMP一般クエリーインターバル] ×

[IGMPロバストネス変数] + [IGMP一般クエリーの最大応答時間] / 2という式を使用して計算されます。

インターフェイス上でのIGMPクエリーおよび応答パラメータの設定

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

interface*interface-type interface-number*

3. IGMPクエリーアのロバストネス変数を設定します。

igmp robust-count *count*

デフォルトでは、IGMPクエリーアのロバストネス変数は2です。

4. IGMPスタートアップクエリーインターバルを設定します。

igmp startup-query-interval *interval*

デフォルトでは、IGMPスタートアップクエリーインターバルは、IGMP一般クエリーインターバルの4分の1に等しくなります。

5. IGMPスタートアップクエリーカウントを設定します。

igmp startup-query-count *count*

デフォルトでは、IGMP起動クエリーカウントはIGMPクエリーアのロバストネス変数と同じです。

6. IGMP一般クエリーインターバルを設定します。

igmp query-interval *interval*

デフォルトでは、IGMP一般クエリーインターバルは125秒です。

7. IGMP最終メンバークエリーインターバルを設定します。

igmp last-member-query-interval *interval*

デフォルトでは、IGMP最終メンバークエリーインターバルは1秒です。

8. IGMP最終メンバークエリーカウントを設定します。

igmp last-member-query-count *count*

デフォルトでは、IGMP最終メンバークエリーカウントは、IGMPクエリーアのロバストネス変数と同じです。

9. IGMP一般クエリーの最大応答時間を設定します。

igmp max-response-time *time*

デフォルトでは、IGMP一般クエリーの最大応答時間は10秒です。

10. IGMPの他のクエリーアの有存在タイマーを設定します。

igmp other-querier-present-interval *interval*

デフォルトでは、IGMPの他のクエリーアの有存在タイマーは、IGMP一般クエリーインターバル×IGMP

ロバストネス変数+IGMP一般クエリーの最大応答時間/2という式を使用して計算されます。

高速脱退処理の有効化

高速脱退処理について

この機能を使用すると、IGMPクエリーアは、Leaveメッセージの受信後にグループ固有またはグループ/ソース固有のクエリーを送信せずに、アップストリームにLeave通知を送信できます。この機能を使用して、脱退遅延を短縮し、ネットワーク帯域幅を確保します。

制約事項とガイドライン

高速脱退処理の設定は、デバイスでIGMPv2またはIGMPv3が実行されている場合にだけ有効です。

手順

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

interface *interface-type interface-number*

3. 高速脱退処理を有効にします。

igmp fast-leave [**group-policy** *ipv4-acl-number*]

デフォルトでは、高速脱退処理は無効です。

IGMP SSMマッピングの設定

IGMP SSMマッピングの概要

この機能により、デバイスはIGMPv1またはIGMPv2ホストにSSMサービスを提供できます。

制約事項とガイドライン

この機能では、IGMPv3メッセージは処理されません。IGMPv3レポートを確実に処理するには、受信側インターフェイスでIGMPv3を有効にします。

手順

1. システムビューに入ります。

System-view

2. IGMPビューに入ります。

igmp

3. IGMP SSMマッピングを設定します。

ssm-mapping *source-address ipv4-acl-number*

IGMPプロキシの設定

IGMPプロキシ設定の前提条件

IGMPプロキシを設定する前に、ネットワークポロジに基づいてルータインターフェイスとホストインターフェイスを決定し、ルータインターフェイスでIGMPを有効にします。

IGMPプロキシの有効化

制約事項とガイドライン

受信側インターフェイスでIGMPプロキシを有効にします。

IGMPプロキシを有効にしたインターフェイスでは、**igmp version** コマンドだけが有効になり、他のIGMPコマンドは有効になりません。

同じデバイス上でIGMPプロキシとマルチキャストルーティングプロトコル(PIMやMSDPなど)の両方を有効にした場合、マルチキャストルーティングプロトコルは有効になりません。

IGMPv1では、DRはPIMによって選択され、IGMPクエリアとして動作します。PIMはプロキシデバイスでは有効にならないため、IGMPv1を実行しているルータインターフェイスはDRとして選択できません。ルータインターフェイス上のダウンストリームレシーバホストがマルチキャストデータを受信できるようにするには、そのインターフェイス上でマルチキャスト転送を有効にする必要があります。詳細については、「非クエリーアインターフェイスでのマルチキャスト転送の有効化」を参照してください。

手順

1. システムビューに入ります。
System-view
2. インターフェイスビューに入ります。
interface interface-type interface-number
3. IGMPプロキシを有効にします。
igmp proxying enable
デフォルトでは、IGMPプロキシは無効です。

非クエリーアインターフェイス上のマルチキャストフォワーディングの有効化

非クエリーアインターフェイスのマルチキャストフォワーディング機能について

通常、マルチキャストトラフィックを転送できるのはIGMPクエリーアのみで、非クエリーアは転送できません。これにより、マルチキャストデータが繰り返し転送されるのを防ぎます。IGMPプロキシデバイス上

のルータインターフェイスがクエリーアを選択に失敗した場合、接続されたレシーバホストにマルチキャストデータを転送するには、そのインターフェイス上でマルチキャスト転送を有効にします。

制約事項とガイドライン

共有メディアネットワークには、クエリーアとして動作する1つのプロキシを含む、複数のMLDプロキシが存在する場合があります。マルチキャストトラフィックの重複を避けるために、ネットワークの非クエリーアMLDプロキシではマルチキャスト転送を有効にしないでください。

手順

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

interface *interface-type* *interface-number*

3. インターフェイスでマルチキャスト転送を有効にします。

igmp proxy forwarding

デフォルトでは、マルチキャストフォワーディングは、非クエリーアインターフェイスで無効です。

IGMPプロキシインターフェイスのマルチキャストロードスプリットの設定

IGMPプロキシインターフェイスのマルチキャストロードスプリットについて

デバイス上に複数のIGMPプロキシインターフェイスが存在する場合、最も大きいIPアドレスを持つプロキシインターフェイスだけがマルチキャストトラフィックを転送します。すべてのプロキシインターフェイスがマルチキャストトラフィックを共有できるように、MLDプロキシインターフェイスのマルチキャストロードスプリットを有効にできます。

手順

1. システムビューに入ります。

System-view

2. IGMPビューに入ります。

igmp

3. IGMPプロキシインターフェイスのマルチキャストロードスプリットを有効にします。

proxy multipath

デフォルトでは、IGMPプロキシインターフェイスのマルチキャストロードスプリットは無効です。

IGMP NSRの有効化

IGMP NSRの概要

この機能は、IGMPインターフェイスおよびIGMPマルチキャストグループに関する情報をスタンバイプロセスにバックアップします。アクティブ/スタンバイスイッチオーバーが発生した場合、デバイスは他のデバイスの協力なしに情報を回復します。この機能を使用して、アクティブ/スタンバイスイッチオーバーがマルチキャストサービスに影響を与えないようにします。

手順

1. システムビューに入ります。

System-view

2. IGMP NSRを有効にします。

igmp non-stop-routing

デフォルトでは、IGMP NSRは無効になっています。

発信IGMPプロトコルパケットのDSCP値の設定

発信IGMPプロトコルパケットのDSCP値について

DSCP値は、パケット送信の優先順位を決定します。DSCP値が大きいほど、優先順位が高くなります。

手順

1. システムビューに入ります。

System-view

2. IGMPビューに入ります。

igmp

3. 発信IGMPプロトコルパケットのDSCP値を設定します。

dscp dscp-value

デフォルトでは、発信IGMPプロトコルパケットのDSCP値は48です。

IGMPの表示およびメンテナンスコマンド

注意:

reset igmp groupコマンドを使用すると、マルチキャストデータの転送が失敗する場合があります。

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
IGMPマルチキャストグループに関する情報を表示します。	display igmp group [<i>group-address</i> interface <i>interface-type</i> <i>interface-number</i>] [static verbose]
インターフェイスのIGMP情報を表示します。	display igmp interface [<i>interface-type</i> <i>interface-number</i>] [host proxy] [verbose]
IGMPプロキシによって保持されるマルチキャストグループメンバーシップ情報を表示します。	display igmp proxy group [<i>group-address</i> interface <i>interface-type</i> <i>interface-number</i>] [verbose]
IGMPプロキシによって維持されるマルチキャストルーティングエントリを表示します。	display igmp proxy routing-table [<i>source-address</i> [mask { <i>mask-length</i> <i>mask</i> }] <i>group-address</i> [mask { <i>mask-length</i> <i>mask</i> }]] * [verbose]
IGMP SSMマッピングを表示します。	display igmp ssm-mapping <i>group-address</i>
ダイナミックIGMPマルチキャストグループエントリをクリアします。	reset igmp group { all interface <i>interface-type</i> <i>interface-number</i> } { all <i>group-address</i> [mask { <i>mask</i> <i>mask-length</i> }] [<i>source-address</i> [mask { <i>mask</i> <i>mask-length</i> }]] } }

IGMPの設定例

例:基本的なIGMP機能の設定

ネットワークの設定

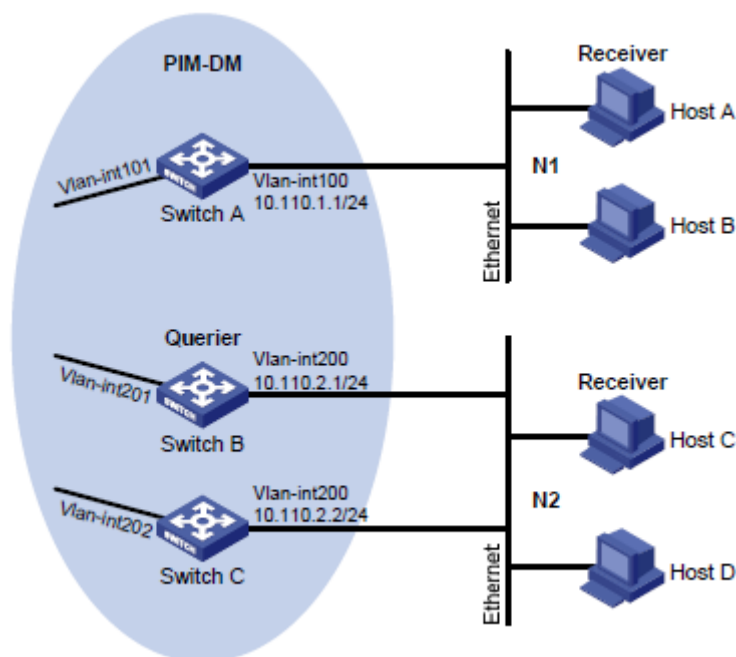
図35に示します。

- OSPFとPIM-DMはネットワーク上で動作します。
- VODストリームは、マルチキャストでレシーバホストに送信されます。異なる組織のレシーバホストは、スタブネットワークN1およびN2を形成します。ホストAおよびホストCは、それぞれN1およびN2のレシーバホストです。
- IGMPv2は、スイッチAとN1の間、および他の2つのスイッチとN2の間で動作します。スイッチAは、N1のIGMPクエリアーとして動作します。スイッチBは、より小さいIPアドレスを持つため、N2のIGMPクエリアーとして動作します。

次の要件を満たすようにルータを設定します。

- N1内のホストは、マルチキャストグループ224.1.1.1だけに加入できます。
- N2内のホストは、任意のマルチキャストグループに加入できます。

図35 ネットワークダイアグラム



手順

1. 図35に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
2. PIM-DMドメイン内のスイッチにOSPFを設定します(詳細は省略)。
3. IPマルチキャストルーティング、IGMP、およびPIM-DMを有効にします。
On Switch A, enable IP multicast routing.


```

<SwitchA> system-view
[SwitchA] multicast routing
[SwitchA-mrib] quit
# Enable IGMP on VLAN-interface 100.
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] quit
# Enable PIM-DM on VLAN-interface 101.
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim dm
[SwitchA-Vlan-interface101] quit
# On Switch B, enable IP multicast routing.
<SwitchB> system-view
[SwitchB] multicast routing
[SwitchB-mrib] quit
# Enable IGMP on VLAN-interface 200.
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp enable
[SwitchB-Vlan-interface200] quit
# Enable PIM-DM on VLAN-interface 201.
[SwitchB] interface vlan-interface 201
[SwitchB-Vlan-interface201] pim dm
[SwitchB-Vlan-interface201] quit
# On Switch C, enable IP multicast routing.
<SwitchC> system-view
[SwitchC] multicast routing
[SwitchC-mrib] quit
# Enable IGMP on VLAN-interface 200.
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] igmp enable
[SwitchC-Vlan-interface200] quit
# Enable PIM-DM on VLAN-interface 202.
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] pim dm
[SwitchC-Vlan-interface202] quit

```

4. スイッチ A でマルチキャスト グループ ポリシーを設定し、VLAN インターフェース 100 に接続されているホストがマルチキャスト グループ 224.1.1.1 にのみ参加できるようにします。

```

[SwitchA] acl basic 2001
[SwitchA-acl-ipv4-basic-2001] rule permit source 224.1.1.1 0
[SwitchA-acl-ipv4-basic-2001] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp group-policy 2001
[SwitchA-Vlan-interface100] quit

```

設定の確認

#スイッチB上のVLANインターフェイス200のIGMP情報を表示します。

```
[SwitchB] display igmp interface vlan-interface 200
Vlan-interface200(10.110.2.1):
  IGMP is enabled.
  IGMP version: 2
  Query interval for IGMP: 125s
  Other querier present time for IGMP: 255s Maximum
  query response time for IGMP: 10s Querier for IGMP:
  10.110.2.1 (This router)
  IGMP groups reported in total: 1
```

例:IGMP SSMマッピングの設定

ネットワークの設定

図36に示します。

- OSPFはネットワーク上で動作します。
- PIM-SMドメインは、マルチキャスト配信にSSMモデルを使用します。SSMグループの範囲は232.1.1.0/24です。
- IGMPv3は、スイッチDのVLANインターフェイス400で動作します。レシーバホストはIGMPv2を実行し、IGMPv3をサポートしません。レシーバホストは、メンバーシップレポートでマルチキャスト送信元を指定できません。
- Source 1、Source 2、およびSource 3は、SSMグループ範囲232.1.1.0/24のマルチキャストグループにマルチキャストパケットを送信します。

レシーバホストが送信元1および送信元3からだけマルチキャストデータを受信できるように、スイッチDでIGMP SSMマッピング機能を設定します。

図36 ネットワークダイアグラム

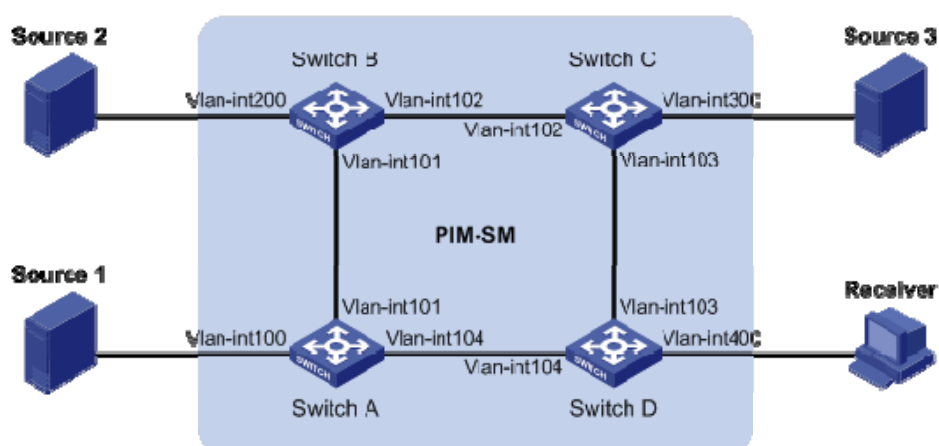


表7インターフェイスとIPアドレスの割り当て

デバイス	インターフェイス	IPアドレス	デバイス	インターフェイス	IPアドレス
Source 1	-	133.133.1.1/24	Spurce 3	-	133.133.3.1/24
Source 2	-	133.133.2.1/24	Receiver	-	133.133.4.1/24
Switch A	Vlan-int100	133.133.1.2/24	Switch C	Vlan-int300	133.133.3.2/24
Switch A	Vlan-int101	192.168.1.1/24	Switch C	Vlan-int103	192.168.3.1/24
Switch A	Vlan-int104	192.168.4.2/24	Switch C	Vlan-int102	192.168.2.2/24
Switch B	Vlan-int200	133.133.2.2/24	Switch D	Vlan-int400	133.133.4.2/24
Switch B	Vlan-int101	192.168.1.2/24	Switch D	Vlan-int103	192.168.3.2/24
Switch B	Vlan-int102	192.168.2.1/24	Switch D	Vlan-int104	192.168.4.1/24

手順

1. 図36に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
2. PIM-SMドメイン内のスイッチにOSPFを設定します(詳細は省略)。
3. IPマルチキャストルーティング、PIM-SM、およびIGMPを有効にします。

On Switch D, enable IP multicast routing.

```
<SwitchD> system-view
```

```
[SwitchD] multicast routing
```

```
[SwitchD-mrib] quit
```

Enable IGMPv3 on the receiver-side interface (VLAN-interface 400).

```
[SwitchD] interface vlan-interface 400
```

```
[SwitchD-Vlan-interface400] igmp enable
```

```
[SwitchD-Vlan-interface400] igmp version 3
```

```
[SwitchD-Vlan-interface400] quit
```

Enable PIM-SM on the other interfaces.

```
[SwitchD] interface vlan-interface 103
```

```
[SwitchD-Vlan-interface103] pim sm
```

```
[SwitchD-Vlan-interface103] quit
```

```
[SwitchD] interface vlan-interface 104
```

```
[SwitchD-Vlan-interface104] pim sm
```

```
[SwitchD-Vlan-interface104] quit
```

On Switch A, enable IP multicast routing.

```
<SwitchA> system-view
```

```
[SwitchA] multicast routing
```

```
[SwitchA-mrib] quit
```

Enable PIM-SM on each interface.

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] pim sm
```

```
[SwitchA-Vlan-interface100] quit
```

```
[SwitchA] interface vlan-interface 101
```

```
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 104
[SwitchA-Vlan-interface104] pim sm
[SwitchA-Vlan-interface104] quit
```

Configure Switch B and Switch C in the same way Switch A is configured. (Details not shown.)

4. SSMグループ範囲を設定します。

On Switch D, specify 232.1.1.0/24 as the SSM group range.

```
[SwitchD] acl basic 2000
[SwitchD-acl-ipv4-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[SwitchD-acl-ipv4-basic-2000] quit
[SwitchD] pim
[SwitchD-pim] ssm-policy 2000
[SwitchD-pim] quit
```

#スイッチDの設定と同じ方法で、スイッチA、スイッチB、およびスイッチCのSSMグループ範囲を設定します(詳細は省略)。

5. スイッチDにIGMP SSMマッピングを設定します。

```
[SwitchD] igmp
[SwitchD-igmp] ssm-mapping 133.133.1.1 2000
[SwitchD-igmp] ssm-mapping 133.133.3.1 2000
[SwitchD-igmp] quit
```

設定の確認

#スイッチD上のマルチキャストグループ232.1.1.1のIGMP SSMマッピングを表示します。

```
[SwitchD] display igmp ssm-mapping 232.1.1.1
Group: 232.1.1.1
Source list:
    133.133.1.1
    133.133.3.1
```

#スイッチDで、ホストがダイナミックに加入したIGMPマルチキャストグループに関する情報を表示します。

```
[SwitchD] display igmp group
IGMP groups in total: 1
Vlan-interface400(133.133.4.2):
IGMP groups reported in total: 1
  Group address      Last reporter      Uptime      Expires
  232.1.1.1          133.133.4.1        00:02:04    off
```

#スイッチDのPIMルーティングエントリを表示します。

```
[SwitchD] display pim routing-table
Total 0 (*, G) entry; 2 (S, G) entry

(133.133.1.1, 232.1.1.1)
  Protocol: pim-ssm, Flag:
  UpTime: 00:13:25
  Upstream interface: Vlan-interface104
  Upstream neighbor: 192.168.4.2 RPF
```

prime neighbor: 192.168.4.2

Downstream interface(s) information:

Total number of downstreams: 1

1: Vlan-interface400

Protocol: igmp, UpTime: 00:13:25, Expires: -

(133.133.3.1, 232.1.1.1)

Protocol: pim-ssm, Flag:

UpTime: 00:13:25

Upstream interface: Vlan-interface103

Upstream neighbor: 192.168.3.1

RPF prime neighbor: 192.168.3.1

Downstream interface(s) information:

Total number of downstreams: 1

1: Vlan-interface400

Protocol: igmp, UpTime: 00:13:25, Expires: -

例:IGMPプロキシの設定

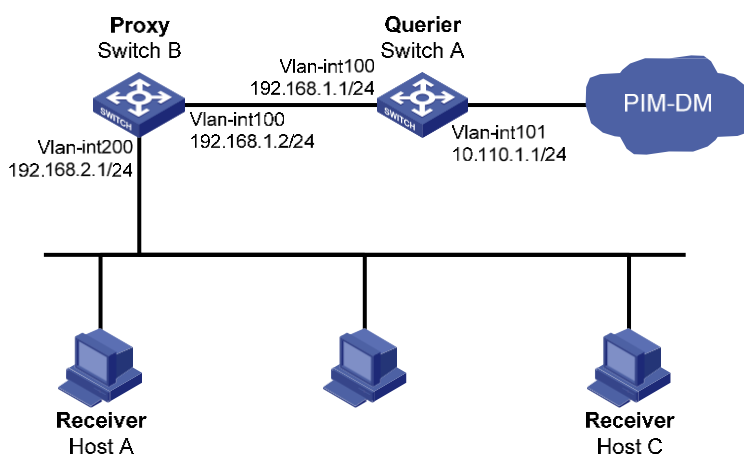
ネットワークの設定

図37に示します。

- PIM-DMはコアネットワーク上で動作します。
- スタブネットワーク上のホストAとホストCは、マルチキャストグループ224.1.1.1に送信されたビデオオンデマンド情報を受信します。

スイッチBがグループメンバーシップを維持し、PIM-DMを実行せずにマルチキャストトラフィックを転送できるように、スイッチBにIGMPプロキシ機能を設定します。

図37 ネットワークダイアグラム



手順

1. 図37に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
2. IPマルチキャストルーティング、PIM-DM、IGMP、およびIGMPプロキシを有効にします。

On Switch A, enable IP multicast routing.

```
<SwitchA> system-view
```

```
[SwitchA] multicast routing
```

```
[SwitchA-mrib] quit
```

Enable PIM-DM on VLAN-interface 101.

```
[SwitchA] interface vlan-interface 101
```

```
[SwitchA-Vlan-interface101] pim dm
```

```
[SwitchA-Vlan-interface101] quit
```

Enable IGMP on VLAN-interface 100.

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] igmp enable
```

```
[SwitchA-Vlan-interface100] quit
```

On Switch B, enable IP multicast routing.

```
<SwitchB> system-view
```

```
[SwitchB] multicast routing
```

```
[SwitchB-mrib] quit
# Enable IGMP proxying on VLAN-interface 100.
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] igmp proxy enable
[SwitchB-Vlan-interface100] quit
# Enable IGMP on VLAN-interface 200.
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp enable
[SwitchB-Vlan-interface200] quit
```

設定の確認

#スイッチB上のIGMPプロキシが保持するマルチキャストグループメンバーシップ情報を表示します。

```
[SwitchB] display igmp proxy group
IGMP proxy group records in total: 1
Vlan-interface100(192.168.1.2):
IGMP proxy group records in total: 1
```

Group address	Member state	Expires
224.1.1.1	Delay	00:00:02

IGMPのトラブルシューティング

受信側機器にメンバーシップ情報がない

症状

ホストがマルチキャストグループGに参加するためのレポートを送信する場合、そのホストに最も近いデバイスにはマルチキャストグループGのメンバーシップ情報は存在しません。

解決方法

この問題を解決するには、次の手順を実行し

1. ネットワーク、インターフェイス接続、およびIPアドレスの設定が正しいことを確認するには、**display igmp interface**コマンドを使用します。
2. マルチキャストルーティングが有効になっていることを確認するには、**display current-configuration**コマンドを使用します。有効になっていない場合は、システムビューで**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ます。さらに、関連するインターフェイスでIGMPが有効になっていることを確認します。
3. **display igmp interface**コマンドを使用して、インターフェイスのIGMPバージョンがホストのIGMPバージョンよりも低いことを確認します。
4. マルチキャストグループGのIGMPレポートをフィルタリングするマルチキャストグループポリシーが設定されていないことを確認するには、**display current-configuration interface**コマンドを使用します。
5. 問題が解決しない場合は、H3Cサポートに連絡してください。

同一サブネット上のデバイスの一貫性のないメンバーシップ情報

症状

同じサブネット上の異なるIGMP機器で異なるメンバーシップが維持されます。

解決方法

この問題を解決するには、次の手順を実行し

1. インターフェイス上のIGMP情報を確認するには、**display current-configuration**コマンドを使用します。サブネット上のデバイスのインターフェイスに同じIGMP設定があることを確認します。
2. IGMP関連のタイマー設定を確認するには、同じサブネット上のすべてのデバイスで**display igmp interface**コマンドを使用します。設定がすべてのデバイスで一貫していることを確認してください。
3. 同じサブネット上のすべてのデバイスが同じIGMPバージョンを実行していることを確認するには、**display igmp interface**コマンドを使用します。
4. 問題が解決しない場合は、H3Cサポートに連絡してください。

PIMの設定

PIMの概要

Protocol Independent Multicast(PIM)は、ユニキャストルーティングプロトコルによって生成されたユニキャストスタティックルートまたはユニキャストルーティングテーブルを利用して、IPマルチキャストフォワーディングを提供します。PIMは、基礎となるユニキャストルーティングを使用して、特定のユニキャストルーティングプロトコルに依存しないマルチキャストルーティングテーブルを生成します。PIMは、RPFメカニズムを使用して、マルチキャストフォワーディングを実装します。RPFの詳細については、「マルチキャストルーティングおよびフォワーディングの設定」を参照してください。

PIMモード

実装メカニズムに基づいて、PIMには次のモードがあります。

- Protocol Independent Multicast Dense Mode(PIM-DM)。
- Protocol Independent Multicast: Sparse Mode(PIM-SM)。
- Protocol Independent Multicast Source-Specific Multicast(PIM-SSM)。

このマニュアルでは、PIMドメインとは、PIMデバイスを含むネットワークを指します。

PIM-DM

PIM-DMは、マルチキャスト転送にプッシュモードを使用し、マルチキャストメンバーが密に分散している小規模なネットワークに適しています。

PIM-DMでは、すべてのダウンストリームノードがソースからマルチキャストデータを受信することを想定しているため、マルチキャストデータはネットワーク上のすべてのダウンストリームノードにフラッディングされます。ダウンストリームレシーバのないブランチは、フォワーディングツリーからプルーニングされます。プルーニングされたブランチに新しいレシーバがある場合、グラフトメカニズムは、プルーニングされたブランチをフォワーディングブランチに変換します。

PIM-DMでは、マルチキャストグループのマルチキャスト転送パスによって、転送ツリーが構成されます。転送ツリーは、マルチキャスト送信元をルートとし、その「リーフ」としてマルチキャストグループメンバーを持ちます。転送ツリーは、マルチキャスト送信元から受信者への最短パスで構成されるため、Shortest Path Tree(SPT)とも呼ばれます。

PIM-DMメカニズムには、ネイバー探索、SPT構築、グラフト、およびアサートが含まれます。

近隣探索

PIMドメインでは、デバイス上の各PIMインターフェイスが定期的にPIM helloメッセージをローカルサブネット上の他のすべてのPIMデバイス(アドレス224.0.0.13で識別される)にマルチキャストします。hello

メッセージの交換を通じて、サブネット上のすべてのPIMデバイスは、そのPIMネイバーを決定し、他のデバイスとのPIMネイバー関係を維持し、SPTを構築および維持します。

SPTの構築

SPTを構築するプロセスは、flood-and-pruneプロセスです。

1. PIM-DMドメインでは、マルチキャスト送信元SからマルチキャストグループGへのマルチキャストデータがドメイン全体にフラッディングされます。デバイスは、マルチキャストデータに対してRPFチェックを実行します。RPFチェックが成功すると、デバイスは(S, G)エントリを作成し、ネットワーク上のすべてのダウンストリームノードにデータを転送します。フラッディングプロセスでは、PIM-DMドメイン内のすべてのデバイスが(S, G)エントリを作成します。
2. ダウンストリームレシーバのないノードはプルーンングされます。ダウンストリームレシーバを持たないデバイスは、サブネット上のすべてのPIMデバイスにプルーンングメッセージをマルチキャストします。アップストリームノードがプルーンングメッセージを受信すると、(S, G)エントリから受信インターフェイスを削除します。

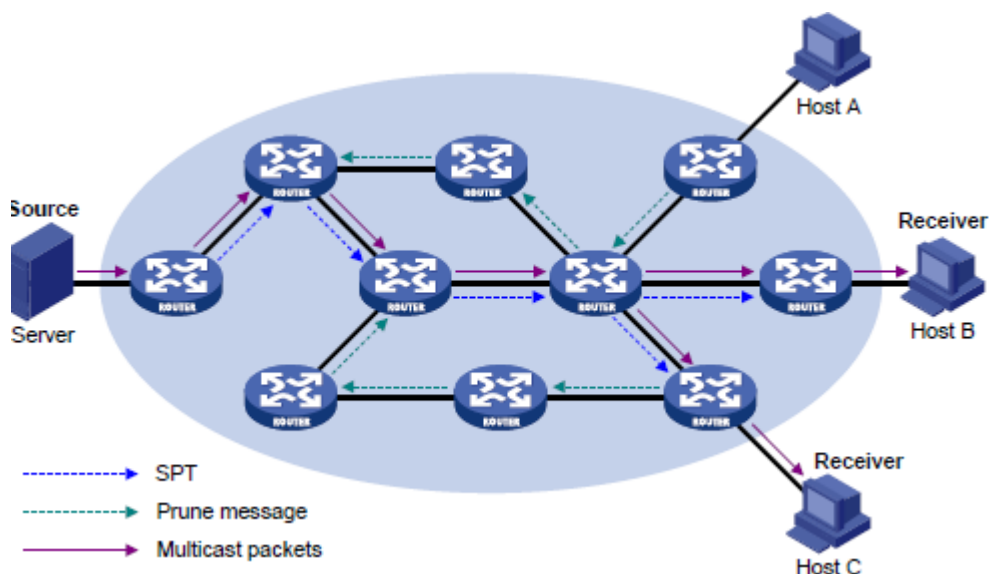
このようにして、アップストリームノードは、そのマルチキャストグループ宛ての後続のパケットをこのノードに転送するのを停止します。

注:

(S, G)エントリには、マルチキャスト送信元アドレスS、マルチキャストグループアドレスG、発信インターフェイスリスト、および着信インターフェイスが含まれます。

プルーンングプロセスは、リーフデバイスによって開始されます。図38に示すように、ダウンストリームレシーバを持たないデバイスインターフェイスは、マルチキャスト送信元に向けてプルーンングメッセージを送信することによって、プルーンングプロセスを開始します。このプルーンングプロセスは、必要なブランチだけがPIM-DMドメインに残され、これらの必要なブランチがSPTを構成するまで続行されます。

図38 SPTの構築



ブランチのプルーニングされた状態には、有限のホールドタイムタイマーがあります。タイマーが期限切れになると、マルチキャストデータはプルーニングされたブランチに再び転送されます。フラッディングとプルーニングのサイクルは、転送するブランチを維持するために定期的に行われます。

Graft

以前にプルーニングされたブランチには、新しいダウンストリームレシーバが存在する場合があります。このブランチの転送機能を再開するための遅延を短縮するために、次のようなグラフトメカニズムが使用されます。

1. マルチキャストデータを受信する必要があるノードは、上流ノードにGraftメッセージを送信し、SPTに再加入するように指示します。
2. インターフェイス上でこのグラフトメッセージを受信した後、アップストリームノードは受信インターフェイスを(S, G)エントリの発信インターフェイスリストに追加します。また、graft-ackメッセージをグラフト送信者に送信します。
3. グラフト送信者がgraft-ackメッセージを受信した場合、グラフトプロセスは終了します。それ以外の場合、グラフト送信者は、上流ノードから確認応答を受信するまで、グラフト再試行間隔でグラフトメッセージを送信し続けます。

Assert

複数のマルチキャストデバイスがあるサブネットでは、アサートメカニズムによって、ネットワークへの重複したマルチキャストフローが遮断されます。これは、サブネットに固有のマルチキャストフォワーダを選択することによって行われます。

図39 アサートメカニズム

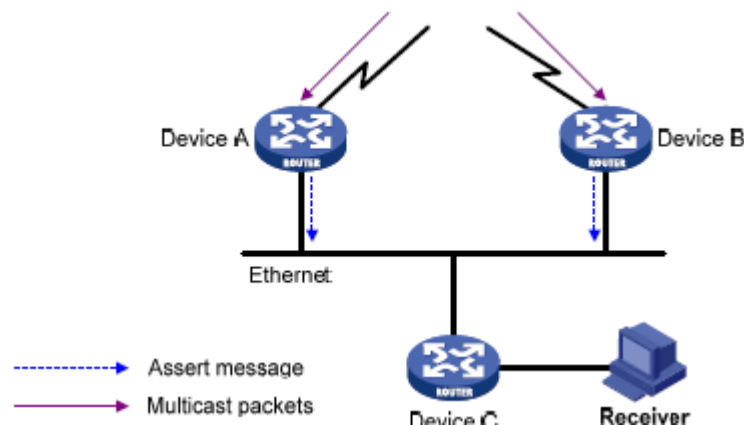


図39に示すように、デバイスAとデバイスBは、アップストリームノードから(S, G)パケットを受信した後、両方ともそのパケットをローカルサブネットに転送します。その結果、ダウンストリームノードのデバイスCは、2つの同一のマルチキャストパケットを受信します。さらに、ダウンストリームインターフェイス上のデバイスAとデバイスBは、もう一方から転送された重複パケットを受信します。この状態を検出すると、両

方のデバイスは、パケットを受信したインターフェイスを介して、ローカルサブネット上のすべてのPIMデバイス(224.0.0.13)にアサートメッセージを送信します。アサートメッセージには、マルチキャスト送信元アドレス(S)、マルチキャストグループアドレス(G)、およびマルチキャスト送信元へのユニキャストルート/MBGPルート/スタティックマルチキャストルートのメトリックプリファレンスとメトリックが含まれます。これらのパラメータを比較することにより、デバイスAまたはデバイスBのいずれかが、共有メディアLAN上の後続の(S, G)パケットの一意のフォワーダになります。比較プロセスは次のとおりです。

1. マルチキャスト送信元よりも高いメトリックプリファレンスを持つデバイスが勝ちます。
2. 両方のデバイスのメトリックプリファレンスが同じ場合は、メトリックが小さい方のデバイスが優先されます。
3. 両方のデバイスのメトリックが同じ場合は、ダウンストリームインターフェイス上でより大きいIPアドレスを持つデバイスが優先されます。

PIM-SM

PIM-DMは、フラッディング/プルニングサイクルを使用して、マルチキャストデータ転送用のSPTを構築します。SPTは、マルチキャストソースからレシーバへの最短パスを持ちますが、効率性は低くなります。したがって、PIM-DMは、大規模および中規模のネットワークには適していません。PIM-SMは、マルチキャスト転送にプルモードを使用し、マルチキャストグループメンバーがまばらに広く分散している大規模および中規模のネットワークに適しています。

PIM-SMは、ホストがマルチキャストデータを必要としないことを前提としています。マルチキャストレシーバは、データが転送される前に、マルチキャストグループのマルチキャストデータへの関心を表明する必要があります。Rendezvous Point(RP)は、PIM-SMドメインのコアです。RPに依存して、SPTおよびRendezvous Point Tree(RPT)が確立され、マルチキャストデータ転送を実装するために維持されます。SPTはマルチキャストソースをルートとし、そのリーフとしてRPを持ちます。RPTはRPをルートとし、そのリーフとしてレシーバホストを持ちます。

PIM-SMメカニズムには、ネイバーディスカバリ、DR選定、RPディスカバリ、エニーキャストRP、RPT構築、マルチキャスト送信元登録、SPTへのスイッチオーバー、およびアサートが含まれます。

近隣探索

PIM-SMは、PIM-DMと同じ近傍検索メカニズムを使用します。詳細については、「近傍検索」を参照してください。

DR選定

ソース側のネットワークとレシーバ側のネットワークの両方に、代表ルータ(DR)が必要です。ソース側のDRは、マルチキャストソースの代わりに動作して、登録メッセージをRPに送信します。レシーバ側のDRは、マルチキャストレシーバの代わりに動作して、加入メッセージをRPに送信します。

PIM-DMにはDRは必要ありません。ただし、IGMPv1がPIM-DMドメイン内の共有メディアLANで実行される場合は、LANのIGMPv1クエリアとして動作するDRを選択する必要があります。IGMPの詳細については、「IGMPの設定」を参照してください。

❗重要:

受信側DRとして機能するデバイスでは、IGMPを有効にする必要があります。そうしないと、DRに接続された受信ホストはマルチキャストグループに参加できません。

図40 DRの選択

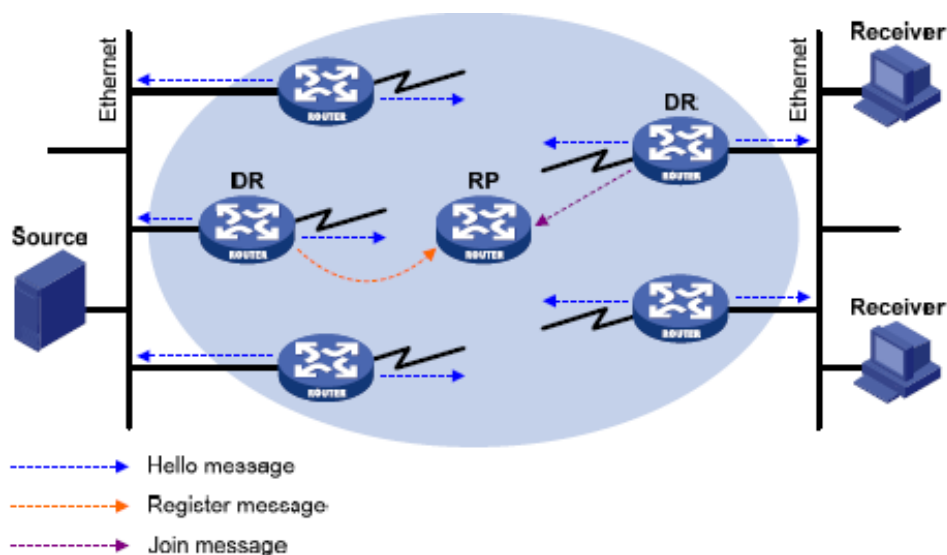


図40に示すように、DR選定プロセスは次のとおりです。

1. 共有メディアLAN上のデバイスは、相互にhelloメッセージを送信します。helloメッセージには、DR選出のためのDRプライオリティが含まれています。DRプライオリティが最も高いデバイスがDRとして選出されます。
2. 次のいずれかの条件下では、最大のIPアドレスを持つデバイスがDR選定に勝ちます。
 - すべてのデバイスは、同じDR選定優先順位を持ちます。
 - デバイスは、helloメッセージでのDRプライオリティの伝送をサポートしていません。

DRに障害が発生すると、そのPIMネイバーのライフタイムが期限切れになり、他のデバイスは新しいDRの選定を開始します。

RPディスカバリ

RPは、PIM-SMドメインのコアです。マルチキャストグループは、マルチキャスト転送用に1つのRPだけを持つことができ、1つのRPを複数のマルチキャストグループに指定できます。RPは、Bootstrap Router(BSR)メカニズムを使用して静的に設定することも、動的に選択することもできます。BSMメカニズムは、RPの負荷を軽減し、RPTのトポロジ構造を最適化します。

BSRメカニズムには、次のロールがあります。

- **Candidate-RPs (C-RPs):** マルチキャストグループにサービスを提供するために、RPがC-RPから動的に選択されます。
- **BSR:** BSRは、PIM-SMドメインの管理コアのコアです。ドメイン全体のRP情報の収集とアドバタイ

ズを担当します。PIM-SMドメインにはBSRが1つだけあり、BSRはC-BSRから選択されます。

- **Candidate-BSRs (C-BSRs):** PIM-SMドメイン内の任意のデバイスがC-BSRとして動作でき、BSRはC-BSRから選出されます。BSRに障害が発生すると、新しいBSRがC-BSRから
- マルチキャストトラフィックの中断を回避します。マルチキャストトラフィックの中断を回避するためにC-BSRから選択されます。

図41 C-RPとBSR間の情報交換

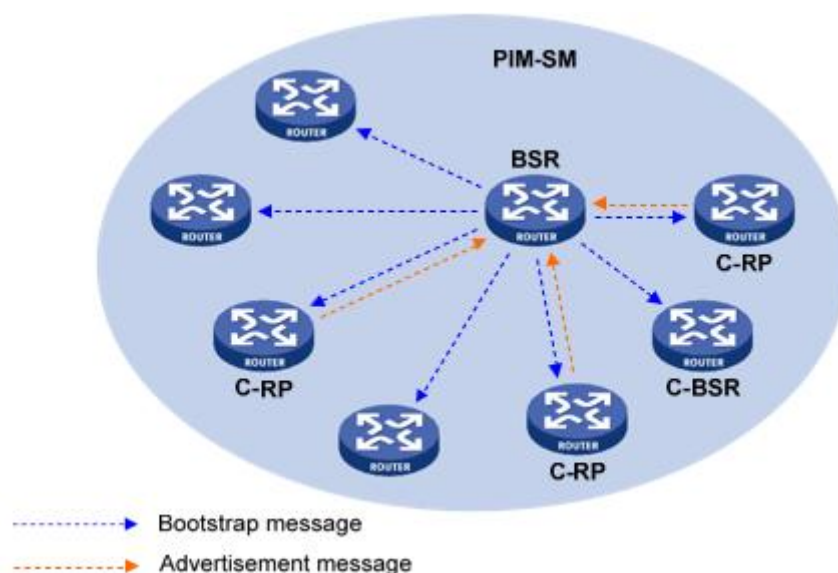


図41に示すように、RPは次のように選出されます。

1. 各C-BSRは、PIM-SMドメイン内の他のデバイスにブートストラップメッセージ(BSM)を送信します。
2. C-BSRは、別のC-BSRからBSMを受信すると、自身のプライオリティとメッセージに含まれるプライオリティを比較します。プライオリティが高いC-BSRがBSRとして選出されます。プライオリティが同じ場合は、IPアドレスが大きいC-BSRが選出されます。敗者は、勝者のBSRアドレスを使用して自身のBSRアドレスを置き換え、自身をBSRと見なさなくなります。勝者は自身のBSRアドレスを保持し、自身をBSRと見なし続けます。
3. 各C-RPは、定期的にアドバタイズメントメッセージをBSRにユニキャストします。アドバタイズメントメッセージには、アドバタイジングC-RPのアドレスと、それが指定されているマルチキャストグループ範囲が含まれます。
4. BSRはこれらのアドバタイズメントメッセージを収集し、C-RP情報をRPセットにまとめます。RPセットは、マルチキャストグループとRP間のマッピングのデータベースです。BSRはRPセット情報をBootstrap Message(BSM)にカプセル化し、BSMをPIM-SMドメイン全体にフラッディングします。
5. PIM-SMドメイン内のすべてのデバイスは、次のルールに基づいてマルチキャストグループのRPを選択します。
 - a. 最小のマルチキャストグループ範囲に指定されているC-RPが優先されます。
 - b. 複数のC-RPが同じグループ範囲に指定されている場合は、プライオリティの最も高いC-RP

が優先されます。

- c. 複数のC-RPのプライオリティが同じ場合は、ハッシュ値が最大のC-RPが優先されます。ハッシュ値は、ハッシュアルゴリズムによって計算されます。
- d. 複数のC-RPのハッシュ値が同じ場合は、IPアドレスが最も大きいC-RPが採用されます。

エニーキャストRP

PIM-SMでは、各マルチキャストグループを処理するために1つのアクティブRPだけが必要です。アクティブRPに障害が発生すると、マルチキャストトラフィックが中断される可能性があります。エニーキャストRPメカニズムでは、同じIPアドレスを持つ複数のRPを設定することで、RP間の冗長性バックアップが可能になります。マルチキャスト送信元が最も近いRPに登録されるか、受信者が最も近いRPに加入して、送信元情報の同期が実装されます。

エニーキャストRPには次の利点があります。

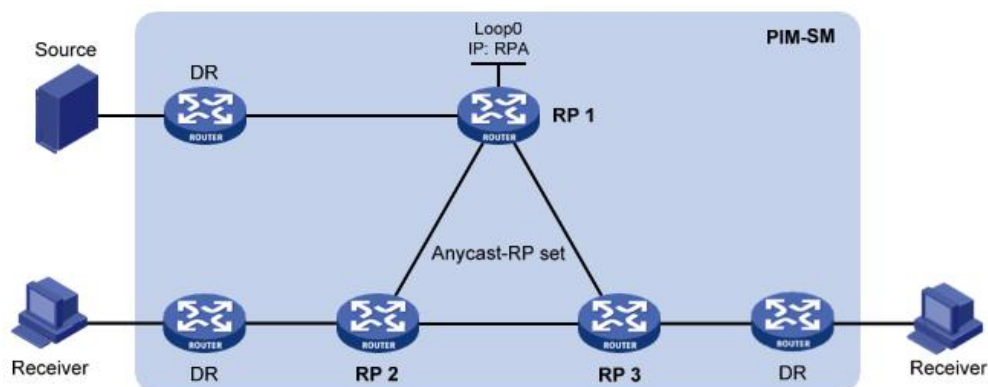
- **Optimal RP path:** マルチキャスト送信元は、最も近いRPに登録して、最適なSPTを構築します。レシーバは、最も近いRPに加入して、最適なRPTを構築します。
- **Redundancy backup among RPs :** RPに障害が発生すると、RP関連の送信元は利用可能な最も近いRPに登録され、受信側のDRは利用可能な最も近いRPに加入します。これにより、RP間の冗長バックアップが提供されます。

エニーキャストRPは、次のいずれかの方法で実装されます。

- **Anycast RP through MSDP:** MSDPを介したエニーキャストRPこの方式では、1つのマルチキャストグループに対して同じIPアドレスを持つ複数のRPを設定し、それらのRP間にMSDPピアリング関係を設定できます。MSDPを介したエニーキャストRPの詳細については、「MSDPの設定」を参照してください。
- **Anycast RP through PIM-SM:** PIM-SMを介したエニーキャストRPこの方式では、1つのマルチキャストグループに対して複数のRPを設定し、それらをエニーキャストRPセットに追加できます。この方式では、次の概念が導入されます。
 - **Anycast RP set:** 同じマルチキャストグループに指定されたRPのセット。
 - **Anycast RP member:** Anycast RPセット内の各RP。
 - **Anycast RP member address:** RPメンバー間の通信に使用される各エニーキャストRPメンバーのIPアドレス。
 - **Anycast RP address:** PIM-SMドメイン内の通信用に設定されたAnycast RPのIPアドレス。RPAとも呼ばれます。

図42に示されるように、RP 1、RP 2およびRP 3はエニーキャストRPセットのメンバーです。

図42 PIM-SMを介したエニーキャストRP



次に、PIM-SMを介したエニーキャストRPの実装方法について説明します。

- a. RP 1はRPA宛ての登録メッセージを受信します。このメッセージは他のエニーキャストRPメンバー(RP 2またはRP 3)からのメッセージではないため、RP 1は登録メッセージがDR RP 1からのものであると見なし、登録メッセージの送信元IPアドレスを自身のアドレスに変更し、他のメンバー(RP 2およびRP 3)にメッセージを送信します。

デバイスがDRとRPの両方として動作する場合、デバイスは登録メッセージを作成し、そのメッセージを他のRPメンバーに転送します。

- b. 登録メッセージを受信した後、RP 2およびRP 3は、登録メッセージの送信元アドレスがエニーキャストRPメンバードレスであることを確認し、他のデバイスへのメッセージの転送を停止します。

エニーキャストRP実装では、マルチキャスト送信元情報を同期するために、RPはDRからの登録メッセージを他のエニーキャストRPメンバーに転送する必要があります。

RPT構築

図43 PIM-SMドメインでのRPT構築

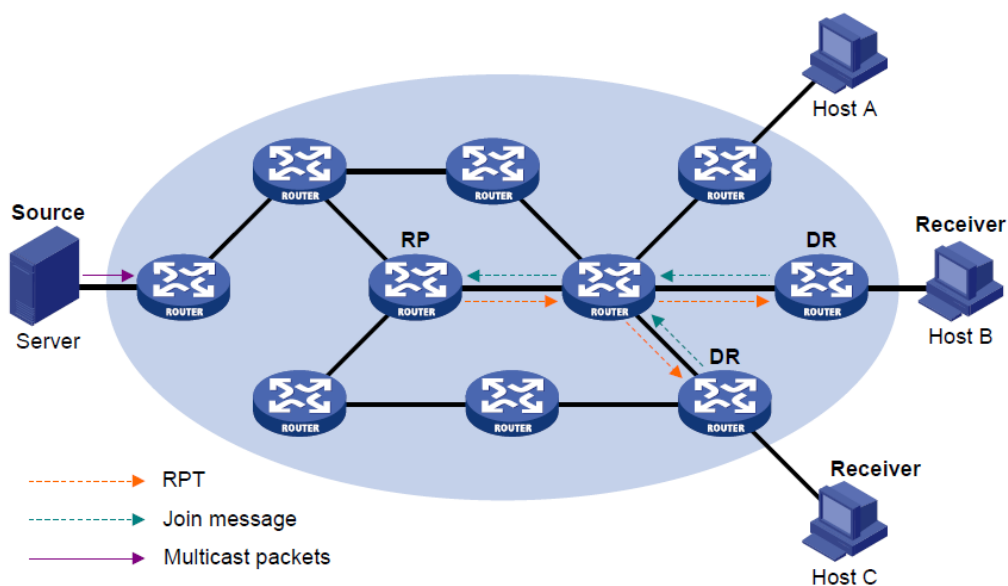


図43に示すように、RPTを構築するプロセスは次のとおりです。

1. レシーバは、マルチキャストグループGに加入する場合、IGMPメッセージを使用してレシーバ側のDRに通知します。
2. レシーバ情報を取得した後、DRはJoinメッセージを送信します。このメッセージは、マルチキャストグループのRPにホップバイホップで送信されます。
3. DRからRPへのパス上のデバイスは、RPTブランチを形成します。このブランチ上の各デバイスは、転送テーブルに(*,G)エントリを追加します。アスタリスク(*)は、任意のマルチキャストソースを表します。RPはRPTのルートであり、DRはRPTのリーフです。

マルチキャストグループG宛てのマルチキャストデータがRPに到達すると、RPは確立されたRPTに沿ってデータをDRに転送し、最終的に受信者に転送します。

受信者がマルチキャストグループG宛てのマルチキャストデータに興味を失った場合、受信者側DRはプルーンメッセージを送信します。プルーンメッセージは、RPTに沿ってRPまでホップバイホップで送信されます。プルーンメッセージを受信した後、アップストリームノードは、このダウンストリームノードに接続しているインターフェイスを発信インターフェイスリストから削除します。同時に、アップストリームデバイスは、そのマルチキャストグループの受信者の存在を確認します。マルチキャストグループの受信者が存在しない場合、デバイスはプルーンメッセージをアップストリームデバイスに転送し続けます。

マルチキャスト送信元登録

マルチキャスト送信元は、登録プロセスを使用して、その存在をRPに通知します。

図44 マルチキャスト送信元登録

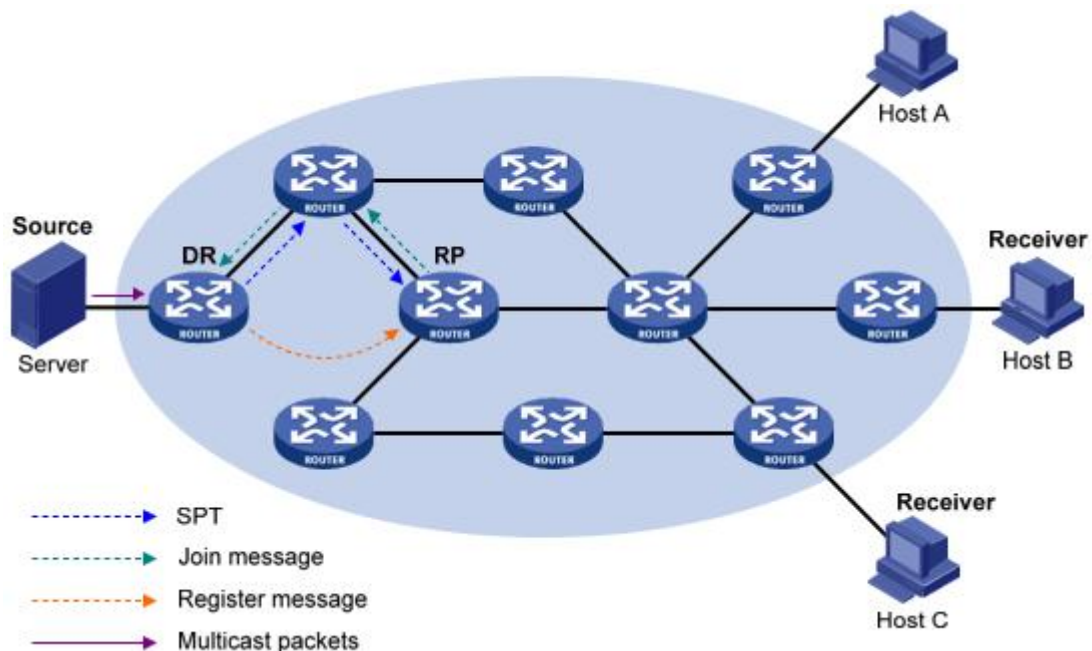


図44に示されるように、マルチキャスト送信元は次のようにRPに登録されます。

1. マルチキャストソースSは、最初のマルチキャストパケットをマルチキャストグループGに送信します。ソース側のDRは、マルチキャストパケットを受信すると、そのパケットをPIM Registerメッセー

ジにカプセル化し、RPにユニキャストします。

2. RPは、登録メッセージを受信すると、登録メッセージのカプセル化を解除し、登録メッセージをRPTに転送します。同時に、(S, G)送信元固有のJoinメッセージをマルチキャスト送信元に向けて送信します。RPからマルチキャスト送信元へのパス上のデバイスは、SPTブランチを構成します。このブランチ上の各デバイスは、転送テーブルに(S, G)エントリを作成します。
3. マルチキャストソースからの後続のマルチキャストデータは、確立されたSPTに沿ってRPに転送されます。マルチキャストデータがSPTに沿ってRPに到達すると、RPはRPTに沿ってデータをレシーバに転送します。一方、ソース側のDRに登録停止メッセージをユニキャストして、DRがデータを不必要にカプセル化しないようにします。

SPTへのスイッチオーバー

このセクションでは、ルータを例として取り上げます。ルータでのSPTへの切り替えと比較して、SPTへの切り替えはスイッチでより簡単な方法で実装されます。

PIM-SMドメインでは、1つのRPと1つのRPTだけが特定のマルチキャストグループにサービスを提供します。SPTへのスイッチオーバーが発生する前に、ソース側のDRはすべてのマルチキャストデータを登録メッセージにカプセル化し、RPに送信します。これらの登録メッセージを受信した後、RPはそれらのカプセル化を解除し、RPTに沿って受信側のDRに転送します。

RPTに沿ったマルチキャスト転送には、次の弱点があります。

- カプセル化とカプセル化解除は、ソース側のDRとRPでは複雑です。
- マルチキャストパケットのパスが最短パスではない可能性があります。
- RPは、マルチキャストトラフィックバーストによって過負荷になる可能性があります。

これらの弱点を排除するために、PIM-SMでは、RPまたはDRがマルチキャストトラフィックを受信したときに、RPまたはDRがSPTへのスイッチオーバーを開始できるようにしています。

- RPはSPTへのスイッチオーバーを開始します。

RPは、マルチキャストトラフィックを受信すると、(S, G)送信元固有のJoinメッセージをマルチキャスト送信元に向けて送信します。RPからマルチキャスト送信元へのパス上のルータは、SPTを構成します。後続のマルチキャストデータは、登録メッセージにカプセル化されることなく、SPTに沿ってRPに転送されます。

Assert

RPによって開始されるSPTへのスイッチオーバーの詳細については、「マルチキャスト送信元登録」を参照してください。

- レシーバ側のDRは、SPTへのスイッチオーバーを開始します。
レシーバ側のDRは、マルチキャストトラフィックを受信すると、次のようにSPTへのスイッチオーバーを開始します。
 - a. レシーバ側のDRは、(S, G)送信元固有の加入メッセージをマルチキャスト送信元に向けて送信します。パス上のルータは、転送テーブルに(S, G)エントリを作成して、SPTブランチを構成します。
 - b. マルチキャストパケットがRPTとSPTが分岐しているルータに到達すると、ルータはRPTに沿って移動す

るマルチキャストパケットをドロップします。次に、RPビットを含むプルーニングメッセージをRPIに向けて送信します。

- c. プルーニングメッセージを受信した後、RPIはそれをマルチキャストソースに転送します(1つのレシーバだけが存在すると仮定します)。このようにして、SPTへのスイッチオーバーが完了します。後続のマルチキャストパケットは、マルチキャストソースからレシーバホストまでSPTに沿って移動します。

SPTへの切り替えにより、PIM-SMはPIM-DMよりも経済的にSPTを構築します。

PIM-SMは、PIM-DMと同様のアサートメカニズムを使用します。詳細については、「アサート」を参照してください。

管理者の権限適用範囲

通常、PIM-SMDメインには、ドメイン全体でRPセット情報をアドバタイズする役割を持つBSRが1つだけ含まれています。すべてのマルチキャストグループに関する情報は、BSRが管理するネットワーク内で転送されます。これは、「非スコープBSRメカニズム」と呼ばれます。

管理上のスコープ設定メカニズム

洗練された管理を実装するには、PIM-SMDメインをグローバルスコープゾーンと複数の管理スコープゾーン(管理スコープゾーン)に分割します。これは「管理スコープメカニズム」と呼ばれます。

管理スコーピングメカニズムは、シングルBSRドメインの管理にかかる負荷を効果的に軽減し、プライベートグループアドレスを使用してゾーン固有のサービスを提供できるようにします。

管理スコープゾーンは、マルチキャストグループ用に分割されます。Zone Border Device(ZBR)は、管理スコープゾーンの境界を形成します。各管理スコープゾーンは、特定の範囲内のマルチキャストグループに対して1つのBSRを維持します。特定のグループ範囲のアサートメッセージやBSMなどのマルチキャストプロトコルパケットは、そのグループ範囲の管理スコープゾーンの境界を越えることはできません。異なる管理スコープゾーンに関連付けられたマルチキャストグループ範囲は、交差を持つことができます。ただし、管理スコープゾーン内のマルチキャストグループはローカルゾーン内でのみ有効であり、これらのマルチキャストグループはプライベートグループアドレスと見なされます。

グローバルスコープゾーンは、どの管理スコープゾーンにも属さないマルチキャストグループのBSRを維持します。

管理者スコープのゾーンと大域スコープのゾーンの関係

グローバルスコープゾーンと各管理スコープゾーンには、独自のC-RPとBSRがあります。これらのデバイスはそれぞれのゾーンでのみ有効であり、BSR選定とRP選定は独立して実装されます。各管理スコープゾーンには独自の境界があります。ゾーン内のマルチキャスト情報は、どちらの方向にもこの境界を越えることはできません。地理的な場所とマルチキャストグループアドレス範囲に基づいて、グローバルスコープゾーンと管理スコープゾーンをよりよく理解できます。

- 地理的な位置を考慮して:

管理スコープゾーンは、特定のマルチキャストグループの論理ゾーンです。このようなマルチキャストグループのマルチキャストパケットは、ローカルの管理スコープゾーン内に限定され、ゾーンの境

界を越えることはできません。

図45 地理的な位置関係

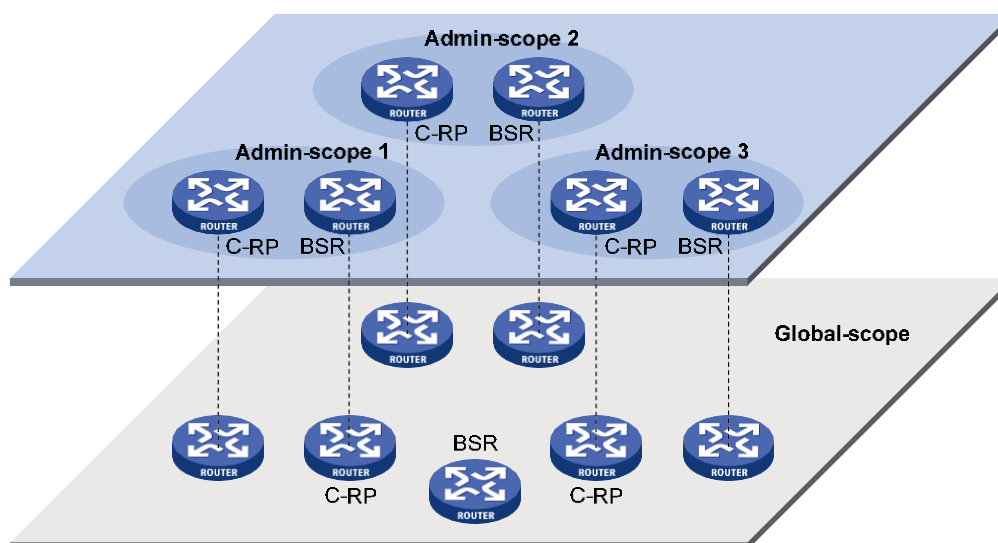


図45に示されるように、特定のグループアドレス範囲のマルチキャストグループに対して管理スコープゾーンは、地理的に分離されている必要があります。デバイスは、複数の管理スコープゾーンに属することはできません。管理スコープゾーンには、他の管理スコープゾーンに属するデバイスを含めることはできません。ただし、グローバルスコープゾーンには、PIM-SMDメイン内のすべてのデバイスが含まれます。管理スコープゾーンに属さないマルチキャストパケットは、PIM-SMDメイン全体で転送されます。

- マルチキャストグループアドレス範囲を考慮すると、次のようになります。
各管理スコープゾーンは、特定のマルチキャストグループに指定されます。そのマルチキャストグループのアドレスは、ローカルゾーン内でのみ有効です。
管理スコープのゾーンには共通部分がある場合があります。管理スコープのゾーン以外のすべてのマルチキャストグループは、グローバルスコープのゾーンを使用します。

図46 マルチキャストグループアドレス範囲を考慮した関係

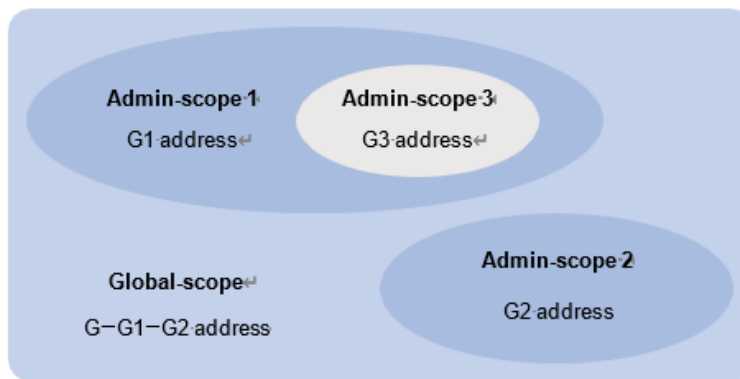


図46に示すように、管理スコープゾーン1と2には共通部分がありませんが、管理スコープゾーン3は管理スコープゾーン1のサブセットです。
は、管理スコープゾーン1および2(この場合はG-G1-G2)でカバーされないすべてのマルチキャストグループにサービスを提供します。

PIM-SSM

ASMモデルには、PIM-DMとPIM-SMが含まれます。SSMモデルは、PIM-SM技術の一部を利用して実装できます。「PIM-SSM」とも呼ばれます。

SSMモデルは、送信元固有のマルチキャストに対するソリューションを提供します。IGMPv3を介してホストとデバイス間の関係を維持します。

実際のアプリケーションでは、IGMPv3およびPIM-SM技術の一部を採用してSSMモデルを実装します。SSMモデルでは、レシーバがマルチキャスト送信元を特定しているため、RPまたはRPTは必要ありません。マルチキャスト送信元はRPに登録されず、他のPIMドメイン内のマルチキャスト送信元を検出するためにMSDPは必要ありません。

PIM-SSMメカニズムには、ネイバー探索、DR選定、およびSPT構築が含まれます。

近隣探索

PIM-SSMは、PIM-SMと同じネイバー探索メカニズムを使用します。詳細については、「ネイバー探索」を参照してください。

DR選定

PIM-SSMは、PIM-SMと同じDR選定メカニズムを使用します。詳細については、「DR選定」を参照してください。

SPT構築

PIM-SM用のRPTまたはPIM-SSM用のSPTを構築するかどうかは、受信者が加入するマルチキャストグループがSSMグループの範囲内にあるかどうかによって決まります。IANAによって予約されているSSMグループの範囲は232.0.0.0/8です。

図47 PIM-SSMでのSPT構築

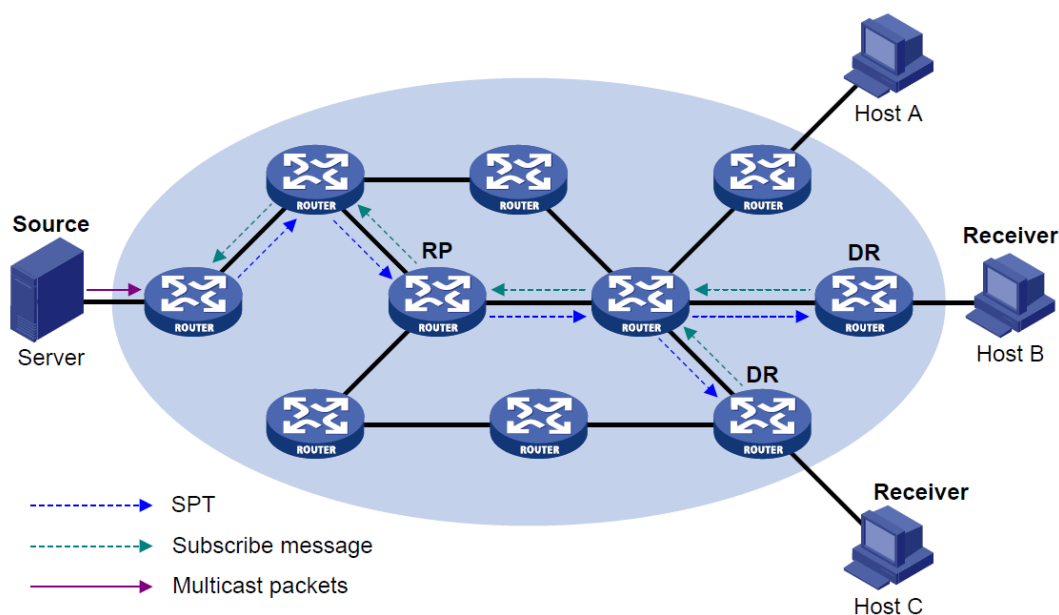


図47に示すように、ホストBおよびホストCはレシーバです。これらは、IGMPv3レポートメッセージをDRに送信して、マルチキャスト送信元SがマルチキャストグループGに送信するマルチキャスト情報への関心を表明します。

レポートメッセージを受信すると、DRはまず、このメッセージ内のグループアドレスがSSMグループ範囲内にあるかどうかを確認し、次の処理を実行します。

- グループアドレスがSSMグループ範囲内にある場合、DRはマルチキャストソースSに向けてホップバイホップで加入メッセージを送信します。DRからソースへのパス上のすべてのデバイスは、SPTを構築するために(S, G)エントリを作成します。SPTはマルチキャストソースSをルートとし、そのリーフとしてレシーバを持ちます。このSPTは、PIM-SSMの送信チャンネルです。
- グループアドレスがSSMグループ範囲内でない場合、レシーバ側のDRは(*,G)JoinメッセージをRPに送信します。マルチキャスト送信元は、送信元側のDRに登録されます。

PIM-SSMでは、「加入メッセージ」という用語は加入メッセージを意味します。

プロトコルと標準

- RFC 3973『Protocol Independent Multicast-Dense Mode(PIM-DM):Protocol Specification(Revised)』
- RFC 4601『Protocol Independent Multicast-Sparse Mode(PIM-SM):Protocol Specification(Revised)』
- RFC 4610『Anycast-RP Using Protocol Independent Multicast(PIM)』
- RFC 5059『Bootstrap Router(BSR)Mechanism for Protocol Independent Multicast(PIM)』
- RFC 4607『Source-Specific Multicast for IP』
- Draft-ietf-ssm-overview-05、Source-Specific Multicast(SSM)の概要

制約事項および注意事項:PIMの設定

デバイス上のすべてのインターフェイスは、同じPIMモードで動作する必要があります。

PIM-DMの設定

PIM-DMタスクの概要

PIM-DMを設定するには、次の作業を実行します。

1. PIM-DMの有効化
2. (オプション)状態更新機能の設定
3. (任意)PIM-DMグラフトリタイマーの設定
4. (任意)一般的なPIMタイマーの設定

PIM-DMの前提条件

PIM-DMを設定する前に、次の作業を実行します。

- ドメイン内のすべてのデバイスがネットワーク層で相互運用できるように、ユニキャストルーティングプロトコルを設定します。
- IPマルチキャストルーティングを有効にします。

PIM-DMの有効化

PIM-DMの有効化について

インターフェイス上でPIM-DMを有効にすると、デバイスはPIMネイバー関係を確立し、PIMネイバーからのPIMメッセージを処理できます。

制約事項とガイドライン

ベストプラクティスとして、PIM-DMドメインを展開する場合は、デバイスのすべての非境界インターフェイスでPIM-DMを有効にします。

手順

1. システムビューに入ります。

System-view

2. IPマルチキャストルーティングを有効にし、MRIBビューを開始します。

multicast routing

デフォルトでは、IPマルチキャストルーティングは無効になっています。

このコマンドの詳細については、『IP Multicast Command Reference』を参照してください。

3. システムビューに戻ります。

quit

4. インターフェイスビューに入ります。

interface interface-type interface-number

5. PIM-DMを有効にします。

pim dm

デフォルトでは、PIM-DMは無効です。

状態更新機能の構成

状態更新機能について

- **State refresh capability:** 送信元に直接接続されたPIMデバイスが定期的に状態更新メッセージを送信できるようにします。また、他のPIMデバイスが状態更新メッセージを受信した後に、プルニングされた状態タイマーを更新できるようにします。これにより、プルニングされたインターフェイスがマルチキャスト転送を再開できなくなります。
- **State refresh interval:** デバイスが状態更新メッセージを送信する間隔を決定します。
- **Wait time before accepting a new state refresh message:** デバイスが短時間に重複した状態更新メッセージを受信する場合があります。この状況を回避するために、デバイスが新しい状態更新メッセージを受け入れるまで待機する時間を設定できます。デバイスがタイマーの期限が切れる前に新しい状態更新メッセージを受信した場合は、メッセージを廃棄します。デバイスがタイマーの期限が切れた後に新しい状態更新メッセージを受信した場合は、メッセージを受け入れ、自身のPIM-DM状態を更新し、待機タイマーをリセットします。
- **TTL value of state refresh messages:** 状態更新メッセージのTTL値は、ダウンストリームノードに転送される前にデバイスを通過するたびに1ずつ減少します。TTL値が0になると、状態更新メッセージは転送されません。TTL値が大きい状態更新メッセージは、小規模なネットワークで循環する場合があります。
ステートリフレッシュメッセージの伝播範囲を効果的に制御するには、マルチキャスト送信元に直接接続されているデバイスのネットワークサイズに基づいて、適切なTTL値を設定します。

制約事項とガイドライン

この作業は、PIM-DMドメイン内のすべてのデバイスで実行します。

手順

1. システムビューに入ります。
System-view
2. インターフェイスビューに入ります。
interface interface-type interface-number
3. 状態更新機能を有効にします。
pim state-refresh-capable
デフォルトでは、状態更新機能は有効になっています。
4. システムビューに戻ります。
quit
5. PIMビューを開始します。
pim
6. 状態更新間隔を設定します。
state-refresh-interval interval

デフォルト設定は60秒です。

この作業は、マルチキャスト送信元に直接接続されているデバイスで実行します。

7. デバイスが新しい状態更新メッセージを受け入れるまで待機する時間を設定します。

```
state-refresh-rate-limit time
```

デフォルト設定は30秒です。

8. 状態更新メッセージのTTL値を設定します。

```
state-refresh-ttl ttl-value
```

デフォルト設定は255です。

PIM-DMグラフトリタイマーの設定

PIM-DMグラフトリタイマーの設定について

デバイスが上流のデバイスからgraft-ackメッセージを受信しない場合に、デバイスがグラフトメッセージを再送信する間隔を調整するには、次の作業を実行します。

手順

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

```
interface interface-type interface-number
```

3. グラフトリタイマーを設定します。

```
pim timer graft-retry interval
```

デフォルト設定は3秒です。

PIM-SMの設定

PIM-SMタスクの概要

PIM-SMを設定するには、次の作業を実行します。

1. PIM-SMの有効化

2. スタティックRPの設定

ベストプラクティスとして、ネットワークにダイナミックRPが1つしか存在しない場合は、スタティックRPを設定します。

3. ダイナミックRPの設定

- C-RPの設定
- C-BSRの設定
- (任意)PIMドメイン境界の設定
- (任意)BSMセマンティックフラグメンテーションの無効化

○ (任意)デバイスが着信インターフェイスからBSMを転送できないようにする。ネットワークに複数のPIMデバイスが存在する場合は、ダイナミックRPを設定することをお勧めします。スタティックRP、ダイナミックRP、またはその両方を設定できます。

4. (任意)Auto-RPリスニングの有効化
5. (任意)エニーキャストRPの設定
6. (任意)マルチキャスト送信元登録の設定
7. (任意)SPTへのスイッチオーバーの設定
8. (任意)一般的なPIM機能の設定

PIM-SMの前提条件

PIM-SMを設定する前に、次の作業を実行します。

- ドメイン内のすべてのデバイスがネットワーク層で相互運用できるように、ユニキャストルーティングプロトコルを設定します。
- IPマルチキャストルーティングを有効にします。

PIM-SMの有効化

PIM-SMの有効化について

インターフェイス上でPIM-SMを有効にすると、デバイスはPIMネイバー関係を確立し、PIMネイバーからのPIMメッセージを処理できます。

制約事項とガイドライン

PIM-SMドメインを展開する場合は、デバイスのすべての非境界インターフェイスでPIM-SMを有効にすることを推奨します。

手順

1. システムビューに入ります。

System-view

2. IPマルチキャストルーティングを有効にし、MRIBビューを開始します。

multicast routing

デフォルトでは、IPマルチキャストルーティングは無効になっています。

このコマンドの詳細については、『IP Multicast Command Reference』を参照してください。

3. システムビューに戻ります。

quit

4. インターフェイスビューに入ります。

interface interface-type interface-number

5. PIM-SMを有効にします。

Pim sm

デフォルトでは、PIM-SMは無効になっています。

スタティックRPの設定

スタティックRPについて

ネットワーク上にダイナミックRPが1つしか存在しない場合は、シングルポイント障害による通信の中断を避けるために、スタティックRPを設定できます。また、スタティックRPでは、C-RPとBSRの間で頻繁にメッセージ交換が行われるため、帯域幅の浪費を避けることもできます。

制約事項とガイドライン

PIM-SMDメインでは、同じRPアドレスと異なるACLを使用することで、異なるマルチキャストグループに同じスタティックRPを設定できます。

インターフェイスをスタティックRPとして設定する場合は、PIMを有効にする必要はありません。

1つのマルチキャストグループに複数のスタティックRPを設定した場合、最も大きいIPアドレスを持つスタティックRPだけが有効になります。

スタティックRPの設定は、PIM-SMDメイン内のすべてのデバイスで同じである必要があります。

手順

1. システムビューに入ります。

System-view

2. PIMビューを開始します。

pim

3. スタティックRPを設定します。

```
static-rp rp-address [ ipv4-acl-number | preferred ] *
```

C-RPの設定

C-RPの設定について

C-RPスプーフィングを回避するには、パケット送信元アドレス範囲とマルチキャストグループアドレスを指定するACLを使用して、C-RPアドバタイズメントメッセージをフィルタリングするようにC-RPポリシーを設定します。

制約事項とガイドライン

バックボーンネットワークに存在するデバイスにC-RPを設定します。

RPと他のデバイスはPIM-SMDメインで大量の情報を交換するため、C-RPと他のデバイス間で大きな帯域幅を予約します。

すべてのC-BSRがBSRになる可能性があるため、PIM-SMDメイン内のすべてのC-BSRに同じC-RPポリシーを設定する必要があります。

手順

1. システムビューに入ります。

System-view

2. PIMビューを開始します。

pim

3. C-RPを設定します。

```
c-rp ip-address [ advertisement-interval adv-interval | group-policy  
ipv4-acl-number | holdtime hold-time | priority priority ] *
```

4. (任意)C-RPポリシーを設定します。

crp-policy ipv4-acl-number

デフォルトでは、C-RPポリシーは設定されていません。すべてのC-RPアドバタイズメントメッセージ

は、合法と見なされます。

C-BSRの設定

C-BSRについて

ダイナミックRP選定を設定する場合は、C-BSRを設定する必要があります。

正当なBSRが悪意のあるホストによって置き換えられないようにするには、正当なBSRアドレスを指定するACLを使用してBSRメッセージをフィルタリングするようにBSRポリシーを設定します。これは、正当なBSRが悪意のあるホストによって置き換えられないようにするために使用されます。

制約事項とガイドライン

バックボーンネットワークに存在するデバイスにC-BSRを設定します。

BSRと他のデバイスはPIM-SMDメイン内で大量の情報を交換するため、C-BSRと他のデバイス間で大きな帯域幅を予約します。

PIM-SMDメイン内のデバイス上のC-BSR設定は同じである必要があります。

RPFチェックを正常に行うには、C-BSRがトンネルを介して他のPIMデバイスに接続するときに、C-BSRへのネクストホップがトンネルインターフェイスになるようにスタティックマルチキャストルートを設定します。スタティックマルチキャストルートの詳細については、「マルチキャストルーティングおよび転送の設定」を参照してください。

手順

1. システムビューに入ります。

System-view

2. PIMビューを開始します。

pim

3. C-BSRを設定します。

```
c-bsr ip-address [ scope group-address { mask-length | mask } ] [ hash-length hash-length | priority priority ] *
```

4. (任意)BSRポリシーを設定します。

```
bsr-policy ipv4-acl-number
```

デフォルトでは、BSRポリシーは設定されていません。すべてのブートストラップメッセージは、有効と見なされます。

PIMドメイン境界の設定

PIMドメイン境界について

PIMドメイン境界は、ブートストラップメッセージの転送境界を決定します。ブートストラップメッセージは、どちらの方向にもドメイン境界を越えることはできません。多数のPIMドメイン境界インターフェイスは、ネットワークを異なるPIM-SMDメインに分割します。

手順

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

interface *interface-type interface-number*

3. PIMドメイン境界を設定します。

pim bsr-boundary

デフォルトでは、インターフェイスはPIMドメイン境界ではありません。

BSMセマンティックフラグメンテーションの無効化

BSMセマンティックフラグメンテーションについて

BSMセマンティックフラグメンテーションを使用すると、BSMがMTUを超過した場合に、BSRでBSMを複数のBSM Fragment(BSMFs)に分割できます。このように、非BSRデバイスは、グループ範囲のすべてのBSMFsを受信した後で、その範囲のRPセット情報を更新できます。1つのBSMFの損失は、フラグメントに含まれるグループ範囲のRPセット情報にだけ影響します。

制約事項とガイドライン

デバイスがBSMセマンティックフラグメンテーションをサポートしていない場合、デバイスはBSMFをBSMと見なし、BSMFを受信するたびにRPセット情報を更新します。デバイスはRPセット情報の一部だけを学習するため、RP選定にさらに影響を与えます。したがって、このようなデバイスがPIM-SMドメイン内に存在する場合は、すべてのC-BSRでBSMセマンティックフラグメンテーションを無効にする必要があります。

手順

1. システムビューに入ります。

System-view

2. PIMビューを開始します。

pim

3. BSMセマンティックフラグメンテーションを無効にします。

undo bsm-fragment enable

デフォルトでは、BSMセマンティックフラグメンテーションは有効です。

デバイスが着信インターフェイスからBSMを転送できないようにする

デバイスが着信インターフェイスからBSMを転送できないようにする方法

デフォルトでは、デバイスは着信インターフェイスからBSMを転送します。このデフォルト設定により、サブネット上のすべてのデバイスは、ルーティング情報に矛盾がある場合でもBSMを受信できます。ただし、このデフォルト設定では、マルチキャストトラフィックが重複します。サブネット上のすべてのデバイスのルーティング情報に矛盾がないことが確実な場合は、デバイスが着信インターフェイスからBSMを転送しないように設定できます。

手順

1. システムビューに入ります。

System-view

2. PIMビューを開始します。

pim

3. デバイスが着信インターフェイスからBSMを転送できないようにします。

undo bsm-reflection enable

デフォルトでは、デバイスは着信インターフェイスからBSMを転送します。

Auto-RPリスニングの有効化

Auto-RPリスニングの概要

この機能により、デバイスはAuto-RP AnnouncementおよびDiscoveryメッセージを受信し、RP情報を学習できます。Auto-RP AnnouncementおよびDiscoveryメッセージの宛先IPアドレスは、それぞれ224.0.1.39および224.0.1.40です。

手順

1. システムビューに入ります。

System-view

2. PIMビューを開始します。

pim

3. Auto-RPリスニングを有効にします。

auto-rp enable

デフォルトでは、Auto-RPリスニングは無効です。

エニーキャストRPの設定

制約事項とガイドライン

他のエニーキャストRPメンバーデバイスがBSRから送信されたBSMを廃棄しないようにするには、エニーキャストRPアドレスがBSRアドレスと異なることを確認します。

ネットワークパフォーマンスを確保するベストプラクティスとして、1つのAnycast RPセットに最大16のAnycast RPメンバーを設定します。

ベストプラクティスとして、ループバックインターフェイスのIPアドレスをRPメンバードレスとして設定します。同じデバイス上の複数のインターフェイスのIPアドレスをRPメンバードレスとして設定する場合、最も小さいIPアドレスが有効になります。残りのインターフェイスアドレスは、バックアップRPメンバードレスになります。

エニーキャストRPアドレスは、サブネットマスクが255.255.255.255のホストアドレスである必要があります。

エニーキャストRPがRPメンバーとして常駐するデバイスを、エニーキャストRPセットに追加する必要があります。

必要条件

エニーキャストRPを設定する前に、PIM-SMDメイン内にスタティックRPまたはC-RPを設定する必要があります。スタティックRPまたはダイナミックに選択されたRPのアドレスをエニーキャストRPアドレスとして使用します。

手順

1. システムビューに入ります。

System-view

2. PIMビューを開始します。

pim

3. エニーキャストRPを設定します。

`anycast-rp` *anycast-rp-address member-rp-address*

デフォルトでは、エニーキャストRPは設定されていません。

このコマンドを繰り返して、複数のRPメンバードレスをエニーキャストRPセットに追加できます。

マルチキャスト送信元登録の設定

マルチキャスト送信元登録について

- **PIM register policy:** PIM登録ポリシーを使用すると、マルチキャスト送信元およびグループを指定するACLを使用して、RPが登録メッセージをフィルタリングできるようになります。このポリシーは、RPが指定されているマルチキャストグループを制限します。登録メッセージがACLによって拒否された場合、またはACLと一致しない場合、RPは登録メッセージを廃棄し、登録停止メッセージをソース側DR登録プロセスが停止します。
- **Checksum computing method for register messages:** 登録メッセージの情報整合性のため

に、登録メッセージ全体に基づいてチェックサムを計算するようにデバイスを設定できます。デバイスが登録メッセージ全体に基づいてチェックサムを計算できない場合は、登録メッセージヘッダーに基づいてチェックサムを計算するようにデバイスを設定できます。

- **Register suppression time:** 送信元側のDRは、RPから登録停止メッセージを受信すると、IPv6マルチキャストデータでカプセル化された登録メッセージの送信を停止し、登録停止タイマーを開始します。登録停止タイマーの期限が切れる前に、DRはヌル登録メッセージ(カプセル化されたマルチキャストデータを含まない登録メッセージ)をRPに送信し、登録プローブタイマーを開始します。登録プローブタイマーの期限が切れる前にDRが登録停止メッセージを受信すると、登録停止タイマーがリセットされます。それ以外の場合、DRはカプセル化されたデータを含む登録メッセージの送信を再開します。

register-stopタイマーは、 $(0.5 \times \text{register\_suppression\_time} - \text{register\_probe\_time})$ から $(1.5 \times \text{register\_suppression\_time} - \text{register\_probe\_time})$ の間で一様選択されるランダムな値に設定されます。register_probe_timeは5秒に固定されています。registerの抑え込みの時間は調整できます。

制約事項とガイドライン

すべてのC-RPデバイス上で、PIM登録ポリシーおよび登録メッセージのチェックサム計算方式を設定します。

ソース側のDRになる可能性のあるすべてのデバイスで、レジスタの抑え込みの時間を設定します。

手順

1. システムビューに入ります。

System-view

2. PIMビューを開始します。

pim

3. PIM登録ポリシーを設定します。

register-policy *ipv4-acl-number*

デフォルトでは、PIM Registerポリシーは設定されていません。すべてのPIM Registerメッセージは合法と見なされます。

4. 登録メッセージ全体に基づいてチェックサムを計算するようにデバイスを設定します。

register-whole-checksum

デフォルトでは、デバイスは登録メッセージのヘッダーに基づいてチェックサムを計算します。

5. レジスタの抑え込みの時間を設定します。

register-suppression-timeout *interval*

デフォルト設定は60秒です。

SPTへのスイッチオーバーの設定

制約事項とガイドライン

一部のデバイスは、RP宛ての登録メッセージ内のマルチキャストデータをカプセル化できません。マルチキャストデータの転送障害を回避するためのベストプラクティスとして、RPになる可能性のあるC-RP上でSPTへのスイッチオーバーを無効にしないでください。

手順

1. システムビューに入ります。

System-view

2. PIMビューを開始します。

pim

3. RPTからSPTへのスイッチオーバーを設定します。

```
spt-switch-threshold { immediacy | infinity } [ group-policy ipv4-acl-number ]
```

デフォルトでは、最初のマルチキャストデータパケットによってRPTからSPTへのスイッチオーバーがトリガーされます。

PIM-SSMの設定

PIM-SSMタスクの概要

PIM-SSMを設定するには、次の作業を実行します。

1. PIM-SMの有効化
2. (任意)SSMグループ範囲の設定
3. (任意)一般的なPIM機能の設定

PIM-SSMの前提条件

PIM-SSMを設定する前に、次の作業を実行します。

- ドメイン内のすべてのデバイスがネットワーク層で相互運用できるように、ユニキャストルーティングプロトコルを設定します。
- PIM-SMを有効にします。
- マルチキャストレシーバに接続するPIMデバイスでIGMPv3を有効にします。

PIM-SMの有効化

制約事項とガイドライン

ベストプラクティスとして、IPv6 PIM-SSMDメインを展開する場合は、デバイスのすべての非境界インタ

ーフェイスでIPv6 PIM-SMを有効にします。

手順

1. システムビューに入ります。

System-view

2. マルチキャストルーティングを有効にし、MRIBビューを開始します。

multicast routing

デフォルトでは、マルチキャストルーティングは無効になっています。

このコマンドの詳細については、『IP Multicast Command Reference』を参照してください。

3. システムビューに戻ります。

quit

4. インターフェイスビューに入ります。

interface interface-type interface-number

5. PIM-SMを有効にします。

Pim sm

デフォルトでは、PIM-SMは無効になっています。

SSMグループ範囲の設定

SSM-group範囲について

PIM-SM対応のインターフェイスは、マルチキャストパケットを受信すると、そのパケットのマルチキャストグループアドレスがSSMグループ範囲内にあるかどうかを確認します。マルチキャストグループアドレスがこの範囲内にある場合、このパケットのPIMモードはPIM-SSMです。マルチキャストグループアドレスがこの範囲内でない場合、PIMモードはPIM-SMです。

制約事項とガイドライン

PIM-SSMドメイン全体のすべてのデバイスで同じSSMグループ範囲を設定します。そうしないと、SSMモデルを介してマルチキャスト情報を配信できません。

SSMグループ範囲内のマルチキャストグループのメンバーがIGMPv1またはIGMPv2レポートメッセージを送信する場合、デバイスは(*,G)加入をトリガーしません。

手順

1. システムビューに入ります。

System-view

2. PIMビューを開始します。

pim

3. SSMグループ範囲を設定します。

ssm-policy ipv4-acl-number

デフォルトでは、SSMグループ範囲は232.0.0.0/8です。

一般的なPIM機能の設定

一般的なPIM機能のタスクの概要

次の作業はすべてオプションです。

- マルチキャスト送信元ポリシーの設定
- PIMハローポリシーの設定
- PIMハローメッセージオプションの設定
- Generation IDオプションを使用しないhelloメッセージのドロップ
- 一般的なPIMタイマーの設定
- ジョインまたはプルーンメッセージの最大サイズの設定
- 発信PIMプロトコルパケットのDSCP値の設定
- PIMのBFDの有効化
- PIMパッシブモードの有効化
- PIM NSRの有効化
- PIMのSNMP通知の有効化

マルチキャスト送信元ポリシーの設定

マルチキャスト送信元ポリシーについて

この機能により、デバイスは、マルチキャスト送信元とオプションのグループを指定するACLを使用して、マルチキャストデータをフィルタリングできます。データパケットをフィルタリングするだけでなく、マルチキャストデータがカプセル化されたメッセージも登録します。ダウンストリームの受信者が利用できる情報を制御します。

手順

1. システムビューに入ります。

System-view

2. PIMビューを開始します。

pim

3. マルチキャスト送信元ポリシーを設定します。

source-policy ipv4-acl-number

デフォルトでは、マルチキャスト送信元ポリシーは設定されていません。デバイスはマルチキャストデータパケットをフィルタリングしません。

PIMハローポリシーの設定

PIM helloポリシーについて

この機能は、パケット送信元アドレスを指定するACLを使用して、デバイスがPIMハローメッセージをフィルタリングできるようにします。これは、PIMメッセージ攻撃から保護し、正しいPIM隣接関係を確立するために使用されます。

既存のPIMネイバーのhelloメッセージがポリシーによってフィルタリングされた場合、そのネイバーはエージングタイマーの期限が切れると自動的に削除されます。

手順

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

interface *interface-type interface-number*

3. PIM helloポリシーを設定します。

pim neighbor-policy *ipv4-acl-number*

デフォルトでは、PIM Helloポリシーはインターフェイスに設定されません。すべてのPIM Helloメッセージは合法と見なされます。

PIMハローメッセージオプションの設定

PIMハローメッセージオプションについて

PIM-DMドメインまたはPIM-SMドメインのいずれかで、デバイス間で交換されるhelloメッセージには、次の設定可能なオプションが含まれます。

- **DR_Priority** (PIM-SMの場合のみ): DR選定のプライオリティ。プライオリティが最も高いデバイスがDR選定されます。このオプションは、マルチキャスト送信元またはレシーバに直接接続する共有メディアLAN内のすべてのデバイスに対して設定できます。
- **Holdtime**: PIMネイバーのライフタイム。ネイバーのライフタイムが期限切れになったときに、デバイスがネイバーからhelloメッセージを受信しなかった場合、そのネイバーは障害が発生したか到達不能であると見なされます。
- **LAN_Prune_Delay**: 共有メディアLAN上のダウンストリームインターフェイスのプルーンングの遅延。このオプションには、LAN遅延フィールド、Override Intervalフィールド、およびTビットがあります。

LAN遅延は、PIMメッセージの伝搬遅延を定義します。上書き間隔は、デバイスがプルーンメッセージを上書きする期間を定義します。Tビットは、アップストリームデバイス上のダウンストリームデバイスステータスを追跡する機能を指定します。

共有メディアLANでは、伝搬遅延とオーバーライド間隔は次のように使用されます。

- デバイスがアップストリームインターフェイスでPruneメッセージを受信した場合、それは共有メディアLAN上にダウンストリームデバイスがあることを意味します。このデバイスがまだマルチキャストデータを受信する必要がある場合、上書き間隔内にJoinメッセージを送信してPruneメッセージを上書きする必要があります。
- デバイスがダウンストリームインターフェイスからプルーンメッセージを受信する時、すぐにこのインターフェイスをプルーンしません。代わりに、タイマー(伝播遅延+オーバーライド間隔)を開始します。タイマーが切れる前にインターフェイスがジョインメッセージを受信した場合、デバイスはインターフェイスをプルーンしません。それ以外の場合、デバイスはインターフェイスをプルーンします。
- **Neighbor tracking:** アップストリームデバイスでネイバートラッキングを有効にした場合、このデバイスは、加入状態保持時間タイマーが期限切れになっていないダウンストリームノードの状態を追跡できます。ダウンストリームデバイスからのすべてのJoinメッセージが受け入れられます。

制約事項とガイドライン

共有メディアLAN上の異なるPIMデバイス上の伝搬遅延またはオーバーライド間隔が異なる場合、最大のもので適用されます。

ネイバートラッキングを有効にする場合は、共有メディアLAN上のすべてのPIMデバイスで有効にする必要があります。そうしないと、アップストリームデバイスは、すべてのダウンストリームデバイスからのJoinメッセージを追跡できません。

PIMビューのすべてのインターフェイス、またはインターフェイスビューの現在のインターフェイスに対して、helloメッセージオプションを設定できます。インターフェイスビューで行った設定は、PIMビューで行った設定よりも優先されます。

helloメッセージオプションのグローバルな設定

1. システムビューに入ります。

System-view

2. PIMビューを開始します。

pim

3. DRプライオリティを設定します。

hello-option dr-priority *priority*

既定の設定は1です。

4. ネイバーのライフタイムを設定します。

hello-option holdtime *time*

デフォルト設定は105秒です。

5. 共有メディアLANのPIMメッセージ伝搬遅延を設定します。

hello-option lan-delay *delay*

デフォルト設定は500ミリ秒です。

6. 上書き間隔を設定します。
hello-option override-interval *interval*
デフォルト設定は2500ミリ秒です。
7. ネイバートラッキングを有効にします。
hello-option neighbor-tracking
デフォルトでは、ネイバートラッキングは無効です。

インターフェイスでのhelloメッセージオプションの設定

1. システムビューに入ります。
System-view
2. インターフェイスビューに入ります。
interface *interface-type* *interface-number*
3. DRプライオリティを設定します。
pim hello-option dr-priority *priority*
既定の設定は1です。
4. ネイバーのライフタイムを設定します。
pim hello-option holdtime *time*
デフォルト設定は105秒です。
5. PIMメッセージの伝搬遅延を設定します
pim hello-option lan-delay *delay*
設定は500ミリ秒です。
6. 上書き間隔を設定します。
pim hello-option override-interval *interval*
デフォルト設定は2500ミリ秒です。
7. ネイバートラッキングを有効にします。
pim hello-option neighbor-tracking
デフォルトでは、ネイバートラッキングは無効です。

Generation IDオプションを使用しないhelloメッセージのドロップ

Generation IDオプションを使用しないhelloメッセージのドロップについて

インターフェイスでPIMが有効になっている場合、デバイスはhelloメッセージの生成IDを生成します。生成IDはランダムな値ですが、デバイスのステータスが変更された場合にだけ変更されます。PIMデバイスは、アップストリームデバイスからのhelloメッセージ内の生成IDが変更されたことを検出すると、アップストリームデバイスのステータスが変更されたと見なします。この場合、ステータス更新のためにJoinメッセージをアップストリームデバイスに送信します。アップストリームデバイスのステータスを迅速に知るために、生成IDオプションを使用せずにhelloメッセージをドロップするようにインターフェイスを設定できます。

手順

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

interface *interface-type interface-number*

3. Generation IDオプションを使用せずにhelloメッセージをドロップするようにインターフェイスを有効にします。

pim require-genid

デフォルトでは、インターフェイスはGeneration IDオプションのないhelloメッセージを受け入れません。

一般的なPIMタイマーの設定

一般的なPIMタイマーについて

次に、一般的なPIMタイマーを示します。

- **Hello interval:** PIMデバイスがhelloメッセージを送信してPIMネイバーを検出し、PIMネイバー関係を維持する間隔。
- **Triggered hello delay:** 同時に発生するhelloメッセージによって引き起こされる衝突を回避するための、helloメッセージ送信の最大遅延。helloメッセージを受信した後、PIMデバイスは、helloメッセージを送信する前にランダムな時間待機します。このランダムな時間は、0からトリガーされたhello遅延までの範囲です。
- **Join/Prune interval:** PIMデバイスが状態更新のために加入/プルーニングメッセージをアップストリームデバイスに送信する間隔。
- **Joined/Pruned state holdtime:** PIMデバイスがダウンストリームインターフェイスの加入/プルーニング状態を保持する時間。この加入/プルーニング状態保持時間は、Join/Pruneメッセージで指定されます。
- **Multicast source lifetime:** PIMデバイスがマルチキャスト送信元に対して保持するライフタイム。タイマーの期限が切れたときに、デバイスがマルチキャスト送信元Sから後続のマルチキャストデータを受信しない場合、マルチキャスト送信元の(S, G)エントリが削除されます。

制約事項とガイドライン

アップストリームネイバーがエージングアウトしないようにするには、Join/Prune間隔をJoin/Pruneステート保持時間よりも短く設定します。

PIMビュー内のすべてのインターフェイス、またはインターフェイスビュー内の現在のインターフェイスに対して、共通のPIMタイマーを設定できます。インターフェイスビューで行った設定は、PIMビューで行った設定よりも優先されます。

ベストプラクティスとして、特別な要件のないネットワークにはデフォルトを使用します。

共通PIMタイマーのグローバルな設定

1. システムビューに入ります。

System-view

2. PIMビューを開始します。

pim

3. hello間隔を設定します。

```
timer hello interval
```

デフォルト設定は30秒です。

4. ジョイン/プルーンインターバルを設定します。

```
timer join-prune interval
```

デフォルト設定は60秒です。

この設定は、現在のインターバルの終了後に有効になります。

5. 参加/プルーニング状態の保持時間を設定します。

```
holdtime join-prune time
```

デフォルト設定は210秒です。

6. マルチキャスト送信元ライフタイムを設定します。

```
source-lifetime time
```

デフォルト設定は210秒です。

インターフェイス上の一般的なPIMタイマーの設定

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

```
interface interface-type interface-number
```

3. hello間隔を設定します。

```
pim timer hello interval
```

デフォルト設定は30秒です。

4. triggered hello delayを設定します。

```
pim triggered-hello-delay delay
```

デフォルト設定は5秒です。

5. ジョイン/プルーンインターバルを設定します。

```
pim timer join-prune interval
```

デフォルト設定は60秒です。

この設定は、現在のインターバルの終了後に有効になります。

6. 加入/プルーニング状態の保持時間を設定します。

```
pim holdtime join-prune time
```

デフォルト設定は210秒です。

ジョインまたはプルーンメッセージの最大サイズの設定

ジョインまたはプルーンメッセージの最大サイズの設定について

大きすぎるジョインまたはプルーンメッセージが失われると、大量の情報が失われる可能性があります。ジョインまたはプルーンメッセージのサイズに小さい値を設定すると、影響を軽減できます。

手順

1. システムビューに入ります。
System-view
2. PIMビューを開始します。
pim
3. join/pruneメッセージの最大サイズを設定します。
jp-pkt-size size
リリース1118P07以降では、デフォルト設定は1200バイトです。

発信PIMプロトコルパケットのDSCP値の設定

発信PIMプロトコルパケットのDSCP値について

DSCP値は、パケット送信の優先順位を決定します。DSCP値が大きいほど、優先順位が高くなります。

手順

1. システムビューに入ります。
System-view
2. PIMビューを開始します。
pim
3. 発信PIMプロトコルパケットのDSCP値を設定します。
dscp dscp-value
デフォルトでは、発信PIMプロトコルパケットのDSCP値は48です。

PIMのBFDの有効化

PIMのBFDの有効化の概要

共有メディアネットワーク上のDRに障害が発生した場合、新しいDR選定プロセスは、DRが期限切れになるまで開始されません。また、他のデバイスがリンク障害を検出して新しいDR選定をトリガーするまでに長い時間がかかる場合があります。元のDRに障害が発生した直後に新しいDR選定プロセスを開始するには、PIMのBFDを有効にして、PIMネイバー間のリンク障害を検出します。

共有メディアネットワーク上のすべてのPIMデバイスでPIMのBFDを有効にする必要があります。BFDの詳細については、『High Availability Configuration Guide』を参照してください。

手順

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

interface *interface-type interface-number*

3. PIMのBFDを有効にします。

pim bfd enable

デフォルトでは、PIMのBFDは無効です。

PIMパッシブモードの有効化

PIMパッシブモードについて

PIM helloスプーフィングを防止するために、受信側インターフェイスでPIMパッシブモードを有効にできます。PIMパッシブインターフェイスは、PIMプロトコルメッセージ(register、register-stop、およびC-RP-Advメッセージを除く)を送受信できず、サブネット上のDRとして動作します。

制約事項とガイドライン

重複したマルチキャストデータ送信およびフローラップを回避するために、複数のPIMデバイスがある共有メディアLANでこの機能を有効にしないでください。

手順

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

interface *interface-type interface-number*

3. インターフェイス上でPIMパッシブモードを有効にします。

pim passive

デフォルトでは、PIMパッシブモードはインターフェイス上で無効です。

PIM NSRの有効化

PIM NSRの概要

この機能を使用すると、PIMはプロトコルステート情報およびデータ(PIMネイバー情報およびルートを含む)をアクティブプロセスからスタンバイプロセスにバックアップできます。アクティブプロセスに障害が発生すると、スタンバイプロセスがただちに処理を引き継ぎます。この機能を使用して、アクティブ/スタンバイスイッチオーバーが発生した場合のPIMのルートフラッピングおよび転送の中断を回避します。

手順

1. システムビューに入ります。

System-view

2. PIM NSRを有効にします。

pim non-stop-routing

デフォルトでは、PIM NSRは無効です。

PIMのSNMP通知の有効化

PIMのSNMP通知について

重要なPIMイベントをNMSに報告するには、PIMのSNMP通知を有効にします。PIMイベント通知が正しく送信されるように、『Network Management and Monitoring Configuration Guide』の説明に従ってSNMPを設定する必要もあります。

手順

1. システムビューに入ります。

System-view

2. PIMのSNMP通知を有効にします。

```
snmp-agent trap enable pim [ candidate-bsr-win-election | elected-bsr-lost-election | neighbor-loss ] *
```

デフォルトでは、PIMのSNMP通知は有効になっています。

PIMの表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
レジスタトンネルインターフェイス情報を表示します。	display interface [register-tunnel [<i>interface-number</i>]] [brief [description down]]
PIM-SMDメインのBSR情報を表示します。	display pim bsr-info
PIMで使用するルートに関する情報を表示します。	display pim claimed-route [<i>source-address</i>]
PIM-SMDメイン内のC-RP情報を表示します。	display pim c-rp [local]
インターフェイスのPIM情報を表示します。	display pim interface [<i>interface-type</i> <i>interface-number</i>] [verbose]
PIMネイバー情報を表示します。	display pim neighbor [<i>neighbor-address</i> interface <i>interface-type</i> <i>interface-number</i> verbose] *
PIMルーティングエントリを表示します。	display pim routing-table [<i>group-address</i> [mask { <i>mask-length</i> <i>mask</i> }] <i>source-address</i> [mask { <i>mask-length</i> <i>mask</i> }] flags <i>flag-value</i> fsm incoming-interface <i>interface-type</i> <i>interface-number</i> mode <i>mode-type</i> outgoing-interface { exclude include match } <i>interface-type</i> <i>interface-number</i> proxy] *
PIM-SMDメイン内のRP情報を表示します。	display pim rp-info [<i>group-address</i>]
PIMパケットの統計情報を表示します。	display pim statistics

PIMの設定例

例:PIM-DMの設定

ネットワークの設定

図48に示します。

- OSPFはネットワーク上で動作します。
- VoDストリームはマルチキャストでレシーバホストに送信されます。異なる組織のレシーバグループはスタブネットワークを形成し、各スタブネットワーク上に1つ以上のレシーバホストが存在します。
- PIMドメイン全体がデンスモードで動作します。
- ホストAとホストCは、2つのスタブネットワーク上のマルチキャストレシーバです。
- IGMPv2は、スイッチAとN1の間、およびスイッチB、スイッチC、N2の間で動作します。

図48 ネットワークダイアグラム

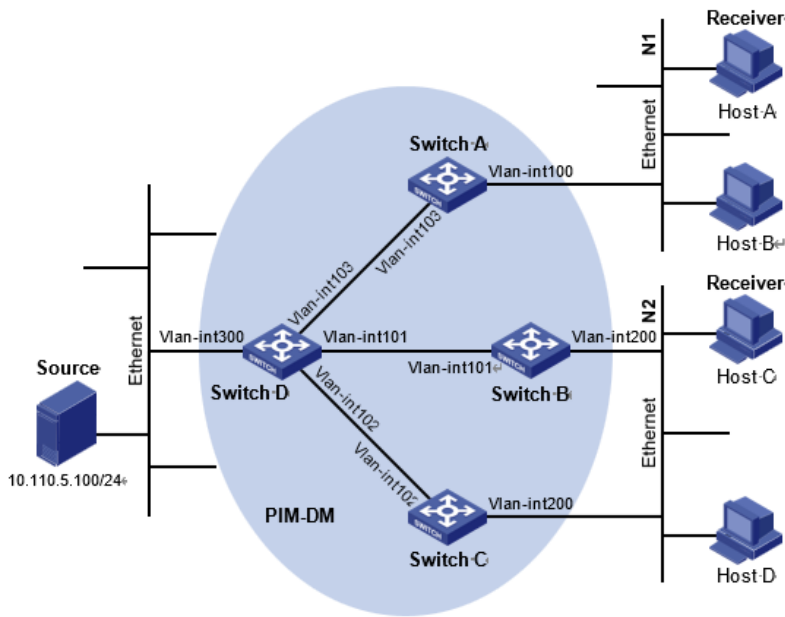


表8 インターフェイスとIPアドレスの割り当て

デバイス	インターフェイス	IPアドレス	デバイス	インターフェイス	IPアドレス
Switch A	VLAN-int100	10.110.1.1/24	Switch C	Vlan-int102	192.168.3.1/24
Switch A	Vlan-int103	192.168.1.1/24	Switch D	Vlan-int300	10.110.5.1/24
Switch B	Vlan-int200	10.110.2.1/24	Switch D	Vlan-int103	192.168.1.2/24
Switch B	Vlan-int101	192.168.2.1/24	Switch D	Vlan-int101	192.168.2.2/24
Switch C	Vlan-int200	10.110.2.2/24	Switch D	Vlan-int102	192.168.3.2/24

手順

1. 図48に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
2. PIM-DMドメイン内のスイッチにOSPFを設定します(詳細は省略)。
3. IPマルチキャストルーティング、IGMP、およびPIM-DMを有効にします。

On Switch A, enable IP multicast routing.

```
<SwitchA> system-view
```

```
[SwitchA] multicast routing
```

```
[SwitchA-mrib] quit
```

Enable IGMP on VLAN-interface 100 (the interface that connects to the stub network).

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] igmp enable
```

```
[SwitchA-Vlan-interface100] quit
```

Enable PIM-DM on VLAN-interface 103.

```
[SwitchA] interface vlan-interface 103
```

```
[SwitchA-Vlan-interface103] pim dm
```

```
[SwitchA-Vlan-interface103] quit
```

Enable IP multicast routing, IGMP, and PIM-DM on Switch B and Switch C in the same way Switch A is configured. (Details not shown.)

On Switch D, enable IP multicast routing, and enable PIM-DM on each interface.

```
<SwitchD> system-view
```

```
[SwitchD] multicast routing
```

```
[SwitchD-mrib] quit
```

```
[SwitchD] interface vlan-interface 300
```

```
[SwitchD-Vlan-interface300] pim dm
```

```
[SwitchD-Vlan-interface300] quit
```

```
[SwitchD] interface vlan-interface 103
```

```
[SwitchD-Vlan-interface103] pim dm
```

```
[SwitchD-Vlan-interface103] quit
```

```
[SwitchD] interface vlan-interface 101
```

```
[SwitchD-Vlan-interface101] pim dm
```

```
[SwitchD-Vlan-interface101] quit
```

```
[SwitchD] interface vlan-interface 102
```

```
[SwitchD-Vlan-interface102] pim dm
```

```
[SwitchD-Vlan-interface102] quit
```

設定の確認

#スイッチDのPIM情報を表示します。

```
[SwitchD] display pim interface
```

Interface	NbrCnt	HelloInt	DR-Pri	DR-Address	
Vlan300	0	30	1	10.110.5.1	(local)
Vlan103	1	30	1	192.168.1.2	(local)
Vlan101	1	30	1	192.168.2.2	(local)
Vlan102	1	30	1	192.168.3.2	(local)

#スイッチDのPIMネイバー関係を表示します。

[SwitchD] display pim neighbor

Total Number of Neighbors = 3

Neighbor	Interface	Uptime	Expires	Dr-Priority Mode
192.168.1.1	Vlan103	00:02:22	00:01:27	1
192.168.2.1	Vlan101	00:00:22	00:01:29	3
192.168.3.1	Vlan102	00:00:23	00:01:31	5

#ホストAからIGMPレポートを送信して、マルチキャストグループ225.1.1.1に参加します(詳細は省略)。

#マルチキャストソース10.110.5.100/24からマルチキャストグループ225.1.1.1にマルチキャストデータを送信します(詳細は省略)。

#スイッチAのPIMルーティングエントリを表示します。

[SwitchA] display pim routing-table

Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)

Protocol: pim-dm, Flag: WC

UpTime: 00:04:25

Upstream interface: NULL Upstream

neighbor: NULL RPF prime

neighbor: NULL

Downstream interface(s) information:

Total number of downstreams: 1 1: Vlan-
interface100

Protocol: igmp, UpTime: 00:04:25, Expires: -

(10.110.5.100, 225.1.1.1)

Protocol: pim-dm, Flag: ACT

UpTime: 00:06:14

Upstream interface: Vlan-interface103

Upstream neighbor: 192.168.1.2 RPF

prime neighbor: 192.168.1.2

Downstream interface(s) information:

Total number of downstreams: 1 1: Vlan-
interface100

Protocol: pim-dm, UpTime: 00:04:25, Expires: -

#スイッチDのPIMルーティングエントリを表示します。

[SwitchD] display pim routing-table

Total 0 (*, G) entry; 1 (S, G) entry

(10.110.5.100, 225.1.1.1)

Protocol: pim-dm, Flag: LOC ACT

UpTime: 00:03:27

Upstream interface: Vlan-interface30

Upstream neighbor: NULL

RPF prime neighbor: NULL

Downstream interface(s) information:

Total number of downstreams: 2

1: Vlan-interface103

Protocol: pim-dm, UpTime: 00:03:27, Expires: -

2: Vlan-interface102

Protocol: pim-dm, UpTime: 00:03:27, Expires: -

出力には次の情報が表示されます。

- SPTパス上のスイッチ(スイッチAおよびスイッチD)には、正しい(S, G)エントリがあります。
- スイッチAには正しい(*, G)エントリがあります。

例:非スコープPIM-SMの設定

ネットワークの設定

図49に示します。

- OSPFはネットワーク上で動作します。
- VODストリームはマルチキャストでレシーバホストに送信されます。異なるサブネットのレシーバはスタブネットワークを形成し、各スタブネットワーク上に少なくとも1つのレシーバホストが存在します。
- PIM-SMDメイン全体に含まれるBSRは1つだけです。
- ホストAおよびホストCは、2つのスタブネットワークN1およびN2上のマルチキャストレシーバです。
- スイッチEのVLANインターフェイス102をC-BSRおよびC-RPとして指定します。C-RPは、マルチキャストグループ範囲225.1.1.0/24に指定されます。ダイナミックRPをバックアップするには、すべてのスイッチでスイッチDのVLANインターフェイス101をスタティックRPとして指定します。
- IGMPv2は、スイッチAとN1の間、およびスイッチB、スイッチC、N2の間で動作します。

図49 ネットワークダイアグラム

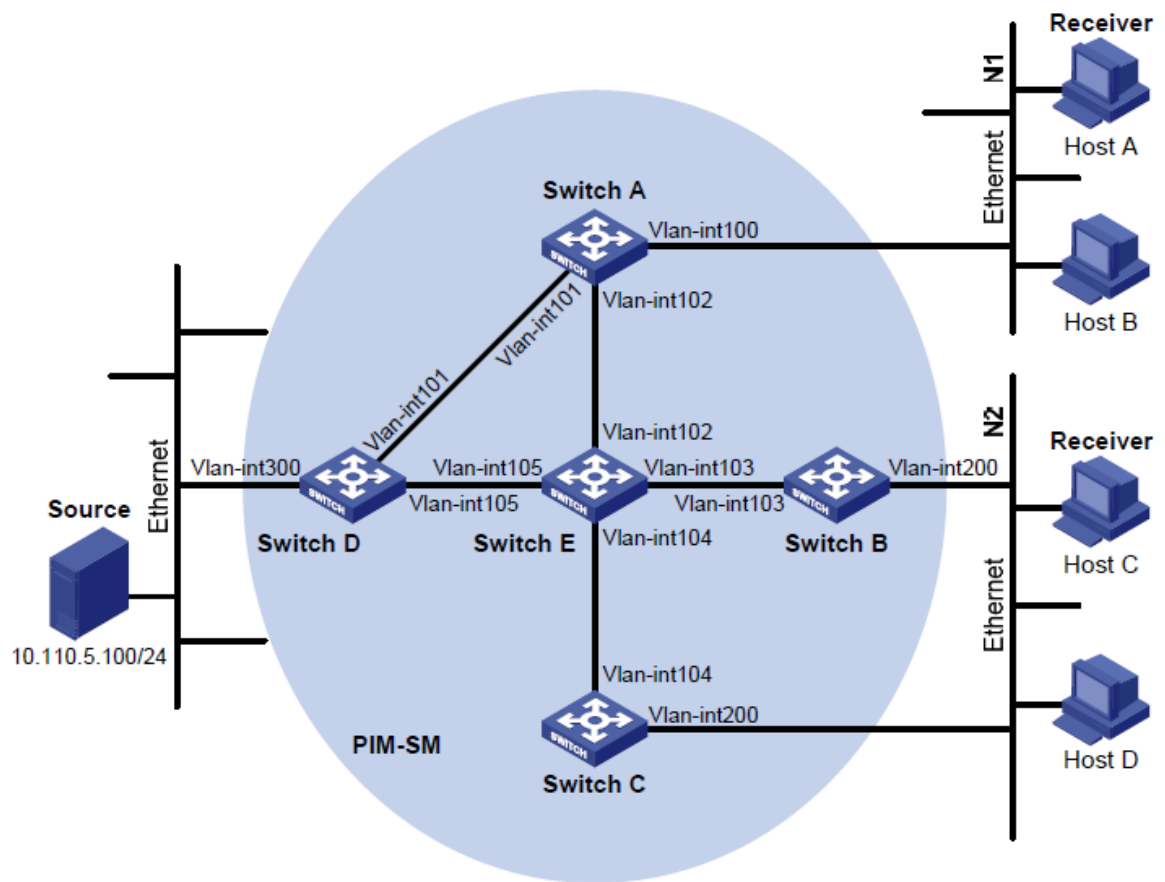


表9インターフェイスとIPアドレスの割り当て

デバイス	インターフェイス	IPアドレス	デバイス	インターフェイス	IPアドレス
Switch A	Vlan-int100	10.110.1.1/24	Switch D	Vlan-int300	10.110.5.1/24
Switch A	Vlan-int101	192.168.1.1/24	Switch D	Vlan-int101	192.168.1.2/24
Switch A	Vlan-int102	192.168.9.1/24	Switch D	Vlan-int105	192.168.4.2/24
Switch B	Vlan-int200	10.110.2.1/24	Switch E	Vlan-int104	192.168.3.2/24
Switch B	Vlan-int103	192.168.2.1/24	Switch E	Vlan-int103	192.168.2.2/24
Switch C	Vlan-int200	10.110.2.2/24	Switch E	Vlan-int102	192.168.9.2/24
Switch C	Vlan-int104	192.168.3.1/24	Switch E	Vlan-int105	192.168.4.1/24

手順

1. 図49に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
2. PIM-SMドメイン内のすべてのスイッチにOSPFを設定します(詳細は省略)。
3. IPマルチキャストルーティングを有効にし、IGMPとPIM-SMを有効にします。

On Switch A, enable IP multicast routing.

```
<SwitchA> system-view
```

```
[SwitchA] multicast routing
```

```
[SwitchA-mrib] quit
```

Enable IGMP on VLAN-interface 100 (the interface that connects to the stub network).

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] igmp enable
```

```
[SwitchA-Vlan-interface100] quit
```

Enable PIM-SM on the other interfaces.

```
[SwitchA] interface vlan-interface 101
```

```
[SwitchA-Vlan-interface101] pim sm
```

```
[SwitchA-Vlan-interface101] quit
```

```
[SwitchA] interface vlan-interface 102
```

```
[SwitchA-Vlan-interface102] pim sm
```

```
[SwitchA-Vlan-interface102] quit
```

#スイッチAの設定と同じ方法で、スイッチBとスイッチCのIPマルチキャストルーティング、IGMP、およびPIM-SMを有効にします(詳細は省略)。

#スイッチAの設定と同じ方法で、スイッチDとスイッチEのIPマルチキャストルーティングとPIM-SMを有効にします(詳細は省略)。

4. C-BSR、C-RP、およびスタティックRPを設定します。

On Switch E, configure the service scope of RP advertisements.

```
<SwitchE> system-view
```

```
[SwitchE] acl basic 2005
```

```
[SwitchE-acl-ipv4-basic-2005] rule permit source 225.1.1.0 0.0.0.255
```

```
[SwitchE-acl-ipv4-basic-2005] quit
```

Configure VLAN-interface 102 as a C-BSR and a C-RP.

```
[SwitchE] pim
```

```
[SwitchE-pim] c-bsr 192.168.9.2
```

```
[SwitchE-pim] c-rp 192.168.9.2 group-policy 2005
```

Configure VLAN-interface 101 of Switch D as the static RP.

```
[SwitchE-pim] static-rp 192.168.1.2
```

```
[SwitchE-pim] quit
```

On Switch A, configure VLAN-interface 101 of Switch D as the static RP.

```
[SwitchA] pim
```

```
[SwitchA-pim] static-rp 192.168.1.2
```

```
[SwitchA-pim] quit
```

#スイッチAの設定と同じ方法で、スイッチB、スイッチC、およびスイッチDにスタティックRPを設定します(詳細は省略)。

設定の確認

#スイッチAのPIM情報を表示します。

```
[SwitchA] display pim interface
```

Interface	NbrCnt	HelloInt	DR-Pri	DR-Address
Vlan101	1	30	1	192.168.1.2
Vlan102	1	30	1	192.168.9.2

#スイッチAのBSR情報を表示します。

```
[SwitchA] display pim bsr-info
```

Scope: non-scoped
State: Accept Preferred
Bootstrap timer: 00:01:44
Elected BSR address: 192.168.9.2
Priority: 64
Hash mask length: 30
Uptime: 00:11:18

#スイッチEのBSR情報を表示します。

[SwitchE] display pim bsr-info

Scope: non-scoped
State: Elected
Bootstrap timer: 00:01:44
Elected BSR address: 192.168.9.2
Priority: 64
Hash mask length: 30
Uptime: 00:11:18
Candidate BSR address: 192.168.9.
Priority: 64
Hash mask length: 30

#スイッチAのRP情報を表示します。

[SwitchA] display pim rp-info

BSR RP information:

Scope: non-scoped Group/MaskLen:

225.1.1.0/24

RP address	Priority	HoldTime	Uptime	Expires
192.168.9.2	192	180	00:51:45	00:02:22

Static RP information:

RP address	ACL	Mode	Preferred
192.168.1.2	---	pim-sm	No

例:管理スコープPIM-SMの設定

ネットワークの設定

図50に示します。

- OSPFはネットワーク上で動作します。
- VODストリームは、マルチキャストで受信側ホストに送信されます。PIM-SMドメイン全体は、管理スコープゾーン1、管理スコープゾーン2、およびグローバルスコープゾーンに分割されます。スイッチB、スイッチC、およびスイッチDは、それぞれ3つのゾーンのZBRです。
- ソース1とソース2は、マルチキャストグループ239.1. 1. 1に異なるマルチキャストデータを送信します。ホストAはソース1からのみマルチキャストデータを受信し、ホストBはソース2からのみマルチキャストデータを受信します。ソース3はマルチキャストグループ224.1. 1. 1にマルチキャストデータを送信します。ホストCはマルチキャストグループ224.1. 1. 1のマルチキャストレシーバです。
- スイッチBのVLANインターフェイス101は、管理スコープゾーン1のC-BSRおよびC-RPとして機能し、スイッチDのVLANインターフェイス105は、管理スコープゾーン2のC-BSRおよびC-RPとして機能します。2つのインターフェイスは両方とも、マルチキャストグループ範囲239.0.0.0/8に指定されています。スイッチFのVLANインターフェイス109は、グローバルスコープゾーンのC-BSRおよびC-RPとして機能し、範囲239.0.0.0/8にないすべてのマルチキャストグループに指定されています。
- IGMPv2は、スイッチA、スイッチE、スイッチI、およびこれらに直接接続するレシーバの間でそれぞれ実行されます。

図50 ネットワークダイアグラム

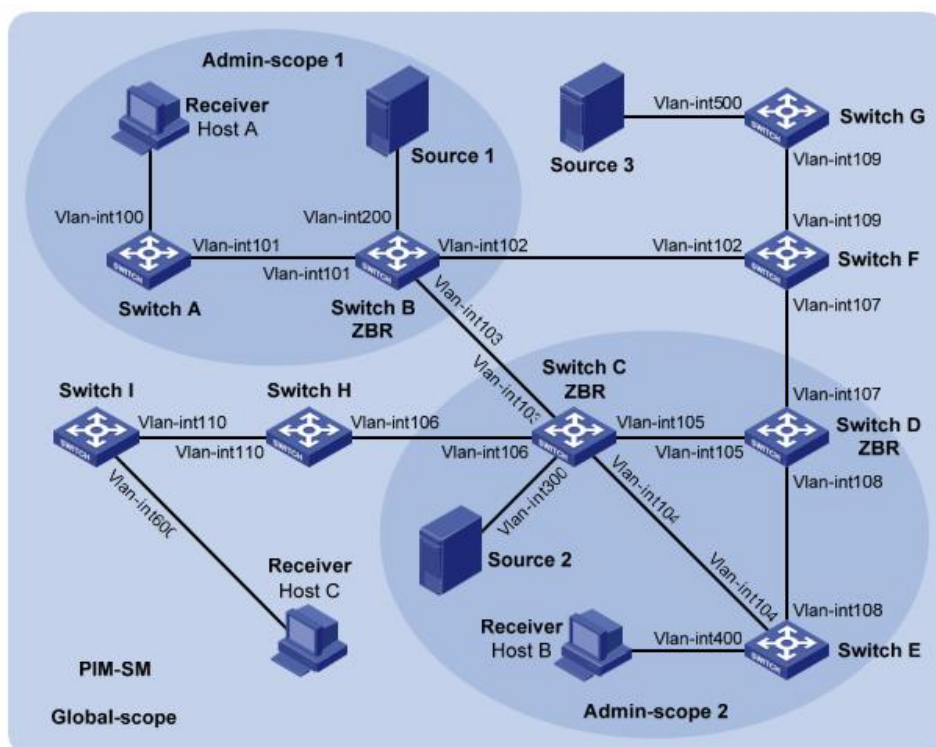


表10インターフェイスとIPアドレスの割り当て

デバイス	インターフェイス	IPアドレス	デバイス	インターフェイス	IPアドレス
Switch A	VLAN-int100	192.168.1.1/24	Switch D	Vlan-int105	10.110.5.2/24
Switch A	Vlan-int101	10.110.1.1/24	Switch D	Vlan-int108	10.110.7.1/24
Switch B	Vlan-int200	192.168.2.1/24	Switch D	Vlan-int107	10.110.8.1/24
Switch B	Vlan-int101	10.110.1.2/24	Switch E	Vlan-int400	192.168.4.1/24
Switch B	Vlan-int103	10.110.2.1/24	Switch E	Vlan-int104	10.110.4.2/24
Switch B	Vlan-int102	10.110.3.1/24	Switch E	Vlan-int108	10.110.7.2/24
Switch C	Vlan-int300	192.168.3.1/24	Switch F	Vlan-int109	10.110.9.1/24
Switch C	Vlan-int104	10.110.4.1/24	Switch F	Vlan-int107	10.110.8.2/24
Switch C	Vlan-int105	10.110.5.1/24	Switch F	Vlan-int102	10.110.3.2/24
Switch C	Vlan-int103	10.110.2.2/24	Switch G	Vlan-int500	192.168.5.1/24
Switch C	Vlan-int106	10.110.6.1/24	Switch G	Vlan-int109	10.110.9.2/24
Switch H	Vlan-int110	10.110.10.1/24	Source 1	-	192.168.2.10/24
Switch H	Vlan-int106	10.110.6.2/24	Source 2	-	192.168.3.10/24
Switch I	Vlan-int600	192.168.6.1/24	Source 3	-	192.168.5.10/24
Switch I	Vlan-int110	10.110.10.2/24			

手順

1. 図50に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)

2. PIM-SMドメイン内のすべてのスイッチにOSPFを設定します(詳細は省略)。
3. IPマルチキャストルーティングを有効にし、IGMPとPIM-SMを有効にします。

On Switch A, enable IP multicast routing.

```
<SwitchA> system-view
[SwitchA] multicast routing
[SwitchA-mrib] quit
```

Enable IGMP on the receiver-side interface (VLAN-interface 100).

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] quit
```

Enable PIM-SM on VLAN-interface 101.

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
```

#スイッチEとスイッチIで、同じ方法でIPマルチキャストルーティング、IGMP、およびPIM-SMを有効にします。

スイッチAが設定されます(詳細は省略)。

#スイッチBで、IPマルチキャストルーティングを有効にし、各インターフェイスでPIM-SMを有効にします。

```
<SwitchB> system-view
[SwitchB] multicast routing
[SwitchB-mrib] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] pim sm
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim sm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] pim sm
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] pim sm
[SwitchB-Vlan-interface103] quit
```

#スイッチBの設定と同じ方法で、スイッチC、スイッチD、スイッチF、スイッチG、およびスイッチHのIPマルチキャストルーティングとPIM-SMを有効にします(詳細は省略)。

4. 管理スコープのゾーン境界を設定します。

#スイッチBで、VLAN-interface 102およびVLAN-interface 103を管理スコープゾーン1の境界として設定します。

```
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] multicast boundary 239.0.0.0 8
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 103
```

```
[SwitchB-Vlan-interface103] multicast boundary 239.0.0.0 8
[SwitchB-Vlan-interface103] quit
```

#スイッチCで、VLAN-interface 103およびVLAN-interface 106を管理スコープゾーン2の境界として設定します。

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 103
[SwitchC-Vlan-interface103] multicast boundary 239.0.0.0 8
[SwitchC-Vlan-interface103] quit
[SwitchC] interface vlan-interface 106
[SwitchC-Vlan-interface106] multicast boundary 239.0.0.0 8
[SwitchC-Vlan-interface106] quit
```

#スイッチDで、VLANインターフェイス107を管理スコープゾーン2の境界として設定します。

```
<SwitchD> system-view
[SwitchD] interface vlan-interface 107
[SwitchD-Vlan-interface107] multicast boundary 239.0.0.0 8
[SwitchD-Vlan-interface107] quit
```

5. C-BSRおよびC-RPを設定します。

#スイッチBで、RPアドバタイズメントのサービス範囲を設定します。

```
[SwitchB] acl basic 2001
[SwitchB-acl-ipv4-basic-2001] rule permit source 239.0.0.0 0.255.255.255 [SwitchB-acl-ipv4-basic-2001] quit
```

#管理スコープゾーン1のC-BSRおよびC-RPとしてVLANインターフェイス101を設定します。

```
[SwitchB] pim
[SwitchB-pim] c-bsr 10.110.1.2 scope 239.0.0.0 8
[SwitchB-pim] c-rp 10.110.1.2 group-policy 2001
[SwitchB-pim] quit
```

#スイッチDで、RPアドバタイズメントのサービス範囲を設定します。

```
[SwitchD] acl basic 2001
[SwitchD-acl-ipv4-basic-2001] rule permit source 239.0.0.0 0.255.255.255
[SwitchD-acl-ipv4-basic-2001] quit
```

#VLANインターフェイス105を、管理スコープゾーン2のC-BSRおよびC-RPとして設定します。

```
[SwitchD] pim
[SwitchD-pim] c-bsr 10.110.5.2 scope 239.0.0.0 8
[SwitchD-pim] c-rp 10.110.5.2 group-policy 2001
[SwitchD-pim] quit
```

#スイッチFで、VLANインターフェイス109をグローバルスコープゾーンのC-BSRおよびC-RPとして設定します。

```
<SwitchF> system-view
[SwitchF] pim
[SwitchF-pim] c-bsr 10.110.9.1
[SwitchF-pim] c-rp 10.110.9.1
[SwitchF-pim] quit
```

設定の確認

#スイッチBのBSR情報を表示します。

[SwitchB] display pim bsr-info

Scope: non-scoped

State: Accept Preferred Bootstrap timer:

00:01:44 Elected BSR address:

10.110.9.1

Priority: 64

Hash mask length: 30

Uptime: 00:01:45

Scope: 239.0.0.0/8

State: Elected

Bootstrap timer: 00:00:06 Elected BSR

address: 10.110.1.2

Priority: 64

Hash mask length: 30 Uptime:

00:04:54

Candidate BSR address: 10.110.1.2 Priority: 64

Hash mask length: 30

#スイッチDのBSR情報を表示します。

[SwitchD] display pim bsr-info

Scope: non-scoped

State: Accept Preferred Bootstrap timer:

00:01:44 Elected BSR address:

10.110.9.1

Priority: 64

Hash mask length: 30 Uptime:

00:01:45

Scope: 239.0.0.0/8

State: Elected

Bootstrap timer: 00:01:12 Elected BSR

address: 10.110.5.2

Priority: 64

Hash mask length: 30 Uptime:

00:03:48

Candidate BSR address: 10.110.5.2 Priority: 64

Hash mask length: 30

#スイッチFのBSR情報を表示します。

[SwitchF] display pim bsr-info

Scope: non-scoped

State: Elected

Bootstrap timer: 00:00:49 Elected BSR

address: 10.110.9.1

Priority: 64

Hash mask length: 30 Uptime:

00:11:11

Candidate BSR address: 10.110.9.1 Priority: 64

Hash mask length: 30

#スイッチBのRP情報を表示します。

[SwitchB] display pim rp-info

BSR RP information:

Scope: non-scoped

Group/MaskLen: 224.0.0.0/4

RP address	Priority	HoldTime	Uptime	Expires
10.110.9.1	192	180	00:03:39	00:01:51

Scope: 239.0.0.0/8

Group/MaskLen: 239.0.0.0/8

RP address	Priority	HoldTime	Uptime	Expires
10.110.1.2 (local)	192	180	00:07:44	00:01:51

#スイッチDのRP情報を表示します。

[SwitchD] display pim rp-info

BSR RP information:

Scope: non-scoped

Group/MaskLen: 224.0.0.0/4

RP address	Priority	HoldTime	Uptime	Expires
10.110.9.1	192	180	00:03:42	00:01:48

Scope: 239.0.0.0/8

Group/MaskLen: 239.0.0.0/8

RP address	Priority	HoldTime	Uptime	Expires
10.110.5.2 (local)	192	180	00:06:54	00:02:41

#スイッチFのRP情報を表示します。

[SwitchF] display pim rp-info

BSR RP information:

Scope: non-scoped

Group/MaskLen: 224.0.0.0/4

RP address	Priority	HoldTime	Uptime	Expires
10.110.9.1 (local)	192	180	00:00:32	00:01:58

例:PIM-SSMの設定

ネットワークの設定

図51に示します。

- OSPFはネットワーク上で動作します。
- 受信機は、マルチキャストを介してビデオオンデマンド情報を受信します。異なる組織の受信機グループはスタブネットワークを形成し、各スタブネットワーク上に1つ以上の受信機ホストが存在します。
- PIMドメイン全体がSSMモードで動作します。
- ホストAとホストCは、2つのスタブネットワーク上のマルチキャストレシーバです。
- SSMグループの範囲は232.1.1.0/24です。
- IGMPv3は、スイッチAとN1の間、およびスイッチB、スイッチC、N2の間で動作します。

図51 ネットワークダイアグラム

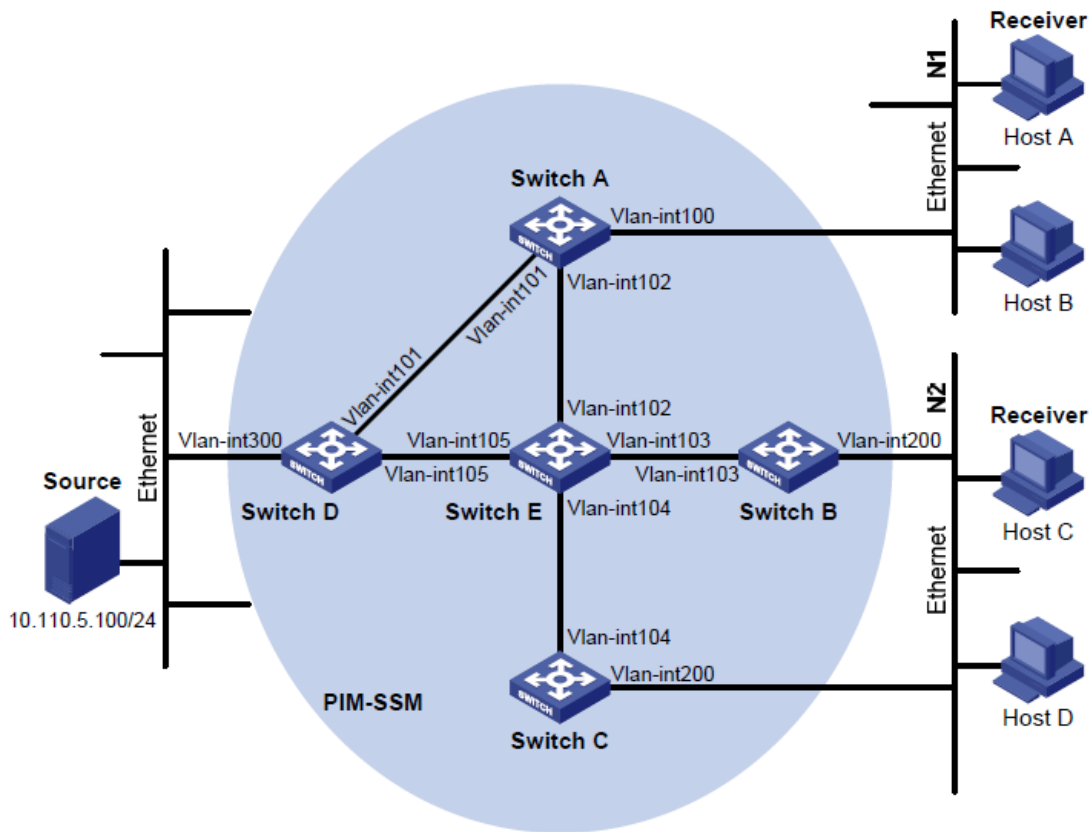


表11インターフェイスとIPアドレスの割り当て

デバイス	インターフェイス	IPアドレス	デバイス	インターフェイス	IPアドレス
Switch A	Vlan-int100	10.110.1.1/24	Switch D	Vlan-int300	10.110.5.1/24
Switch A	Vlan-int101	192.168.1.1/24	Switch D	Vlan-int101	192.168.1.2/24
Switch A	Vlan-int102	192.168.9.1/24	Switch D	Vlan-int105	192.168.4.2/24
Switch B	Vlan-int200	10.110.2.1/24	Switch E	Vlan-int104	192.168.3.2/24
Switch B	Vlan-int103	192.168.2.1/24	Switch E	Vlan-int103	192.168.2.2/24
Switch C	Vlan-int200	10.110.2.2/24	Switch E	Vlan-int102	192.168.9.2/24
Switch C	Vlan-int104	192.168.3.1/24	Switch E	Vlan-int105	192.168.4.1/24

手順

1. 図51に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
2. PIM-SSMドメイン内のスイッチにOSPFを設定します(詳細は省略)。
3. IPマルチキャストルーティング、IGMP、およびPIM-SMを有効にします。

#スイッチAで、IPマルチキャストルーティングを有効にします。

```
<SwitchA> system-view
[SwitchA] multicast routing
[SwitchA-mrib] quit
```

#VLAN-interface 100(スタブネットワークに接続するインターフェイス)でIGMPv3を有効にします。

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] igmp version 3
[SwitchA-Vlan-interface100] quit
```

#他のインターフェイスでPIM-SMを有効にします。

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim sm
[SwitchA-Vlan-interface102] quit
```

#スイッチBとスイッチCで、同じ方法でIPマルチキャストルーティング、IGMP、およびPIM-SMを有効にします。

スイッチAが設定されます(詳細は省略)。

#スイッチAの設定と同じ方法で、スイッチDとスイッチEのIPマルチキャストルーティングとPIM-SMを有効にします(詳細は省略)。

4. SSMグループ範囲を設定します。

#スイッチAでSSMグループ範囲232.1.1.0/24を設定します。

```
[SwitchA] acl basic 2000
[SwitchA-acl-ipv4-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[SwitchA-acl-ipv4-basic-2000] quit
[SwitchA] pim
[SwitchA-pim] ssm-policy 2000
[SwitchA-pim] quit
```

#スイッチB、スイッチC、スイッチD、およびスイッチEのSSMグループ範囲を同じ

スイッチAの設定方法(詳細は省略)

設定の確認

#スイッチAのPIM情報を表示します。

```
[SwitchA] display pim interface
```

Interface	NbrCnt	HelloInt	DR-Pri	DR-Address
Vlan101	1	30	1	192.168.1.2
Vlan102	1	30	1	192.168.9.2

#ホストAからIGMPv3レポートを送信して、マルチキャスト送信元およびグループ(10.110.5.100/24、232.1.1.1)に参加します(詳細は省略)。

#スイッチAのPIMルーティングテーブルを表示します。

```
[SwitchA] display pim routing-table
```

Total 0 (*, G) entry; 1 (S, G) entry

(10.110.5.100, 232.1.1.1)

Protocol: pim-ssm, Flag: ACT

UpTime: 00:13:25

```
Upstream interface: Vlan-interface10
Upstream neighbor: 192.168.1.2
RPF prime neighbor: 192.168.1.2
Downstream interface(s) information:
Total number of downstreams: 1
  1: Vlan-interface100
    Protocol: igmp, UpTime: 00:13:25, Expires: 00:03:25
```

#スイッチDのPIMルーティングテーブルを表示します。

```
[SwitchD] display pim routing-table
Total 0 (*, G) entry; 1 (S, G) entry
(10.110.5.100, 232.1.1.1)
  Protocol: pim-ssm, Flag: LOC
  UpTime: 00:12:05
  Upstream interface: Vlan-interface300
  Upstream neighbor: NULL
  RPF prime neighbor: NULL
  Downstream interface(s) information:
Total number of downstreams: 1
  1: Vlan-interface105
    Protocol: pim-ssm, UpTime: 00:12:05, Expires: 00:03:25
```

この出力は、SPTパス上のスイッチ(スイッチAおよびスイッチD)が正しい(S, G)エントリを生成したことを示しています。

PIMのトラブルシューティング

マルチキャスト配信ツリーを正しく構築できない

症状

PIMネットワーク内のデバイス(マルチキャスト送信元または受信者に直接接続されているデバイスを含む)では、マルチキャスト転送エントリは確立されません。これは、マルチキャスト配信ツリーを正しく構築できないことを意味します。

解決方法

この問題を解決するには、次の手順を実行し

1. マルチキャスト送信元またはRPへのユニキャストルートが使用可能であることを確認するには、**display ip routing-table**を使用します。
2. 各インターフェイス、特にRPFインターフェイスのPIM情報を確認するには、**display pim interface**を使用します。インターフェイスでPIMが有効になっていない場合は、**pim dm**または**pim sm**を使用して、そのインターフェイスのPIM-DMまたはPIM-SMを有効にします。
3. RPFネイバーがPIMネイバーであることを確認するには、**display pim neighbor**を使用します。
4. マルチキャスト送信元またはレシーバに直接接続されているインターフェイスで、PIMおよび

IGMPが有効になっていることを確認します。

5. **display pim interface verbose**を使用して、デバイスのRPFインターフェイスと、デバイスのRPFネイバーの接続インターフェイスで同じPIMモードが有効になっていることを確認します。
6. すべてのデバイスで同じPIMモードが有効になっていることを確認するには、**display current-configuration**を使用します。PIM-SMの場合は、BSRおよびC-RPが正しく設定されていることを確認します。
7. 問題が解決しない場合は、H3Cサポートに連絡してください。

マルチキャストデータが中間デバイスで異常終了する

症状

中間デバイスはマルチキャストデータを正常に受信できますが、データはラストホップデバイスに到達できません。中間デバイス上のインターフェイスはマルチキャストデータを受信しますが、PIMルーティングテーブルに(S, G)エントリを作成しません。

解決方法

この問題を解決するには、次の手順を実行し

1. マルチキャスト転送境界設定を確認するには、**display current-configuration**を使用します。
multicast boundaryを使用して、マルチキャスト転送境界設定を変更し、マルチキャストパケットが境界を通過できるようにします。
2. マルチキャスト送信元ポリシーを確認するには、**display current-configuration**を使用します。
マルチキャストデータの送信元/グループアドレスがACLフィルタリングを通過できるように、**source-policy**コマンドで定義されたACLルールを変更します。
3. 問題が解決しない場合は、H3Cサポートに連絡してください。

RPがPIM-SMのSPTに加入できない

症状

RPTを正しく構築できないか、RPがマルチキャスト送信元に向けてSPTに加入できません。

解決方法

この問題を解決するには、次の手順を実行し

1. 各デバイスでRPへのユニキャストルートが使用可能であることを確認するには、**display ip routing-table**を使用します。
2. ダイナミックRP情報がすべてのデバイスで一貫していることを確認するには、**display pim rp-info**を使用します。
3. **display pim rp-info**を使用して、同じスタティックRPがネットワーク上のすべてのデバイスに設定されていることを確認します。

4. 問題が解決しない場合は、H3Cサポートに連絡してください。

PIM-SMでRPTを構築できない、またはマルチキャスト送信元登録が失敗する

症状

C-RPは、BSRにアドバタイズメントメッセージをユニキャストできません。BSRは、C-RP情報を含むBSMをアドバタイズせず、C-RPへのユニキャストルートを持ちません。RPTを正しく確立できないか、ソース側のDRがマルチキャストソースをRPに登録できません。

解決方法

この問題を解決するには、次の手順を実行し

1. 各デバイスで**display ip routing-table**を使用して、ルーティングテーブル情報を表示します。
C-RPおよびBSRへのユニキャストルートが各デバイスで使用可能であること、および各C-RPとBSRの間でルートが使用可能であることを確認します。
2. 各デバイスにBSR情報が存在することを確認するには、**display pim bsr-info**を使用します。
3. 各デバイスのRP情報が正しいことを確認するには、**display pim rp-info**を使用します。
4. **display pim neighbor**を使用して、PIMネイバー関係がデバイス間で正しく確立されていることを確認します。
5. 問題が解決しない場合は、H3Cサポートに連絡してください。

MSDPの設定

MSDPの概要

Multicast Source Discovery Protocol(MSDP)は、PIM-SMドメインの相互接続に対応するドメイン間マルチキャストソリューションです。他のPIM-SMドメイン内のマルチキャスト送信元情報を検出します。

MSDPは、ASMモデルだけに適用できます。

MSDPの機能

注:

DR、BSR、C-BSR、RP、C-RP、SPT、およびRPTの詳細については、「PIMの設定」を参照してください。

異なるPIM-SMドメインのRPが相互に相互接続されるように、ネットワーク上の適切なデバイス間で

MSDPピア関係が確立されます。これらのMSDPピアはSource Active(SA)メッセージを交換するため、マルチキャスト送信元情報はこれらのドメイン間で共有されます。

MSDPピア

ネットワーク上の1つまたは複数のMSDPピアのペアが、MSDP相互接続マップを形成します。

図52 ネットワーク上のMSDPピアの位置

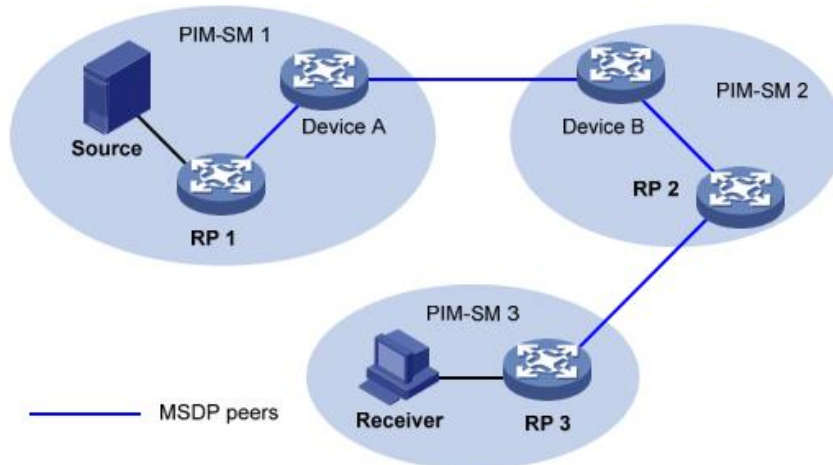


図52に示すように、MSDPピアは任意のPIM-SMデバイス上に作成できます。異なる役割を担うPIM-SMデバイス上に作成されたMSDPピアは、異なる機能を果たします。

- RP上に作成されたMSDPピア:
 - **Source-side MSDP peer:** RP 1など、マルチキャストソースに最も近いMSDPピア。ソース側RPは、SAメッセージを作成してリモートMSDPピアに送信し、ローカルに登録されたマルチキャストソース情報をMSDPピアに通知します。
ソース側のMSDPピアは、ソース側のRP上に作成する必要があります。そうしないと、PIM-SMドメインからマルチキャスト送信元情報をアドバタイズできません。
 - **Receiver-side MSDP peer:** レシーバに最も近いMSDPピアで、通常はRP 3などのレシーバ側のRPです。SAメッセージを受信した後、レシーバ側のMSDPピアはメッセージに含まれるマルチキャストソース情報。次に、PIM-SMドメイン間でマルチキャストソースをルートとするSPTに加入します。マルチキャストソースからマルチキャストデータが着信すると、レシーバ側のMSDPピアはRPTに沿ってデータをレシーバに転送します。
 - **Intermediate MSDP peer:** RP 2などの複数のリモートMSDPピアを持つ中間MSDPピア。中間MSDPピアは、1つのリモートMSDPピアから受信したSAメッセージを他のリモートMSDPピアに転送します。マルチキャスト送信元情報を転送するためのリレーとして機能します。
- RPではないPIM-SMデバイスで作成されたMSDPピア:
デバイスAとデバイスBは、RPではないマルチキャストデバイス上のMSDPピアです。このようなMSDPピアは、SAメッセージだけを転送します。

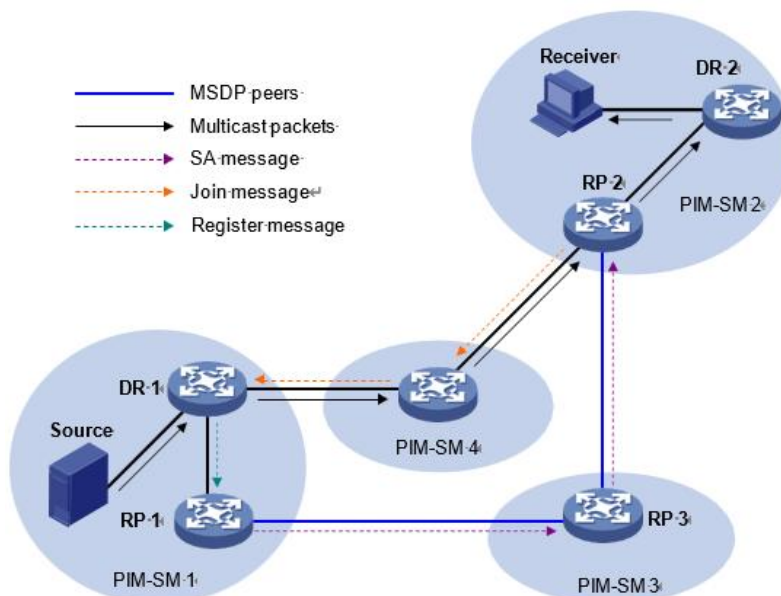
BSRメカニズムを使用するPIM-SMネットワークでは、RPはC-RPから動的に選出されます。PIM-SMネ

ネットワークには通常、ネットワークの堅牢性を確保するために複数のC-RPがあります。RPの選出結果は予測できないため、MSDP相互接続マップ上で常に優勢なC-RPを維持するために、すべてのC-RP間でMSDPピアリング関係を構築する必要があります。C-RPが失われると、このマップ上の共通のPIM-SMデバイスの役割が想定されます。

MSDPによるドメイン間マルチキャスト配信

図53に示すように、アクティブなソース(Source)はドメインPIM-SM 1に存在し、RP 1はマルチキャストソース登録を通じてSourceの存在を学習しています。PIM-SM 2およびPIM-SM 3のRPも、Sourceからのマルチキャストトラフィックをレシーバに送信できるように、Sourceのロケーションを検索します。RP 1とRP 3の間、およびRP 3とRP 2の間で、MSDPピアリング関係を確立する必要があります。

図53 MSDPを介したドメイン間マルチキャスト配信



MSDPピアを利用してPIM-SMDメイン間マルチキャスト配信を実装するプロセスは、次のとおりです。

1. PIM-SM 1内のマルチキャスト送信元が最初のマルチキャストパケットをマルチキャストグループGに送信すると、DR 1は登録メッセージ内にデータをカプセル化します。DR 1は登録メッセージをRP 1に送信し、RP 1はマルチキャスト送信元に関する情報を取得します。
2. 送信元側RPとして、RP 1はSAメッセージを作成し、定期的にMSDPピアに送信します。
SAメッセージには、マルチキャスト送信元のアドレス(S)、マルチキャストグループアドレス(G)、およびこのSAメッセージを作成したRPのアドレス(この例ではRP 1)が含まれます。
3. MSDPピアでは、各SAメッセージはRPFチェックとマルチキャストポリシーベースのフィルタリングを受けます。正しいパスに沿って到着し、フィルタリングを通過したSAメッセージだけが受信および転送されます。これにより、SAメッセージの配信ループが回避されます。さらに、MSDPピアをMSDPメッシュグループに設定して、MSDPピア間のSAメッセージフラッドを回避できます。
MSDPメッシュグループとは、相互にMSDPピアリング関係を確立し、同じグループ名を共有する

MSDPピアのグループを指します。

4. SAメッセージは、あるMSDPピアから別のMSDPピアに転送されます。最後に、マルチキャスト送信に関する情報は、MSDPピア(この例ではPIM-SM 2およびPIM-SM 3)を持つすべてのPIM-SMDメインを通過します。
5. RP 1が作成したSAメッセージを受信した後、PIM-SM 2のRP 2は、マルチキャストグループのレシーバがドメイン内に存在するかどうかを調べます。
 - レシーバがドメイン内に存在する場合、マルチキャストグループGのRPTはRP 2とレシーバの間で維持されます。RP 2は(S, G)エントリを作成し、(S, G)Joinメッセージを送信します。Joinメッセージはマルチキャストソースに向かってホップ単位で送信され、SPTはPIM-SMDメイン間で確立されます。

以降のマルチキャストデータは、SPTに従ってRP 2に送信され、RPTに従ってRP 2からレシーバ側のDRに送信されます。マルチキャストデータを受信したレシーバ側のDRは、設定に基づいてRPTからSPTへのスイッチオーバープロセスを開始するかどうかを決定します。
 - ドメイン内にレシーバが存在しない場合、RP 2は(S, G)エントリを作成せず、マルチキャスト送信元にJoinメッセージを送信しません。

MSDPを使用したドメイン間マルチキャストでは、RPは、別のPIM-SMDメイン内のマルチキャスト送信元に関する情報を取得すると、他のPIM-SMDメイン内のRPに依存なくなります。レシーバは、他のドメイン内のRPを上書きして、送信元をルートとするマルチキャストSPTに直接加入できます。

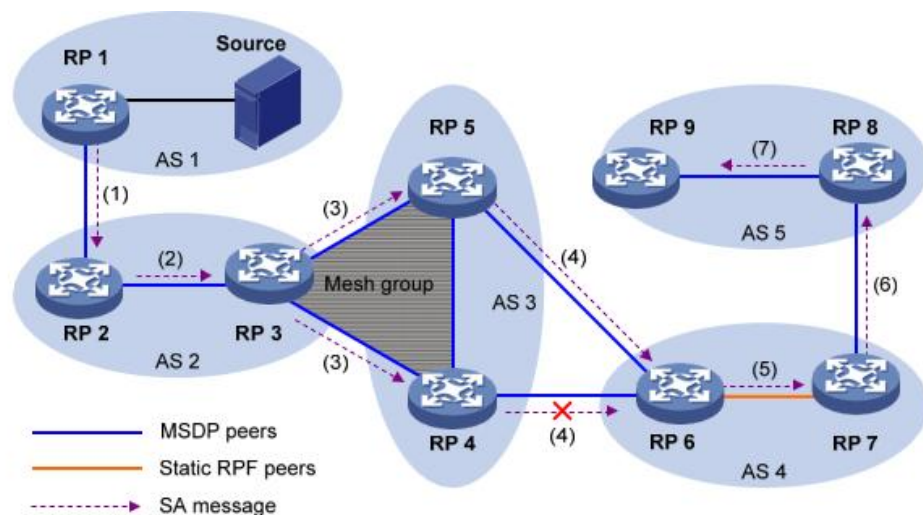
MSDPピア - RPFフォワーディング

MSDPピアRPFチェックは、MSDPを実行するネットワーク上でSAメッセージを転送するために使用されます。ピアRPFチェックが成功した場合、SAメッセージは受け入れられ、転送されます。それ以外の場合、SAメッセージは廃棄されます。

図54に示します。

- ネットワーク上には5つのASがあります。IGPは各AS内で実行され、BGPまたはMBGPはこれらのAS間で実行されます。
- 各ASには最低1つのPIM-SMDメインが含まれ、各PIM-SMDメインには最低1つのRPが含まれます。
- これらのRP間では、MSDPピアリング関係が確立されています。RP 3、RP 4、およびRP 5は、同じMSDPメッシュグループ内にあります。RP 6は、RP 7のスタティックRPFピアとして設定されます。

図54 MSDPピア - RPFフォワーディング



ピアRPFフォワーディングのプロセスは次のとおりです。

1. RP 1はSAメッセージを作成し、ピアRP 2に転送します。
2. SAメッセージ内のRPアドレスがRP 1のアドレスと同じであるため、RP 2はRP 1がSAメッセージを作成したRPであると判断します。その後、RP 2はSAメッセージを受け入れて転送します。
3. RP 2とRP 3は同じASに存在し、RP 2はRP 3からRP 1へのネクストホップであるため、RP 3はSAメッセージを受け入れて転送します。
4. RP 4およびRP 5はSAメッセージを受け入れます。これは、RP 3がRP 4およびRP 5と同じメッシュグループ内にあるためです。次に、RP 4およびRP 5は、メッシュグループの他のメンバーではなく、ピアRP 6にSAメッセージを転送します。
5. RP 4とRP 5は、RP 1へのルート内で最も近いASに存在します。ただし、RP 5のIPアドレスはRP 4のIPアドレスよりも高いため、RP 6はRP 5からのSAメッセージだけを受け入れて転送します。
6. RP 6はスタティックRPFピアであるため、RP 7はSAメッセージを受け入れて転送します。
7. RP 7はRP 1へのピアRPFルートのEBGPまたはMBGPネクストホップであるため、RP 8はSAメッセージを受け入れて転送します。
8. RP 8はRP 9の唯一のRPであるため、RP 9はSAメッセージを受け入れます。

MSDPを介したエニーキャストRP

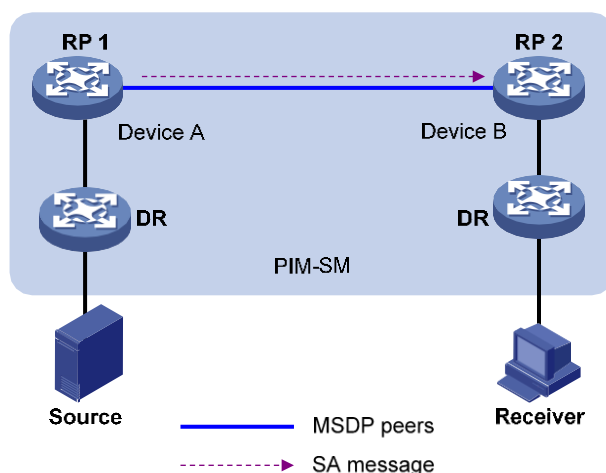
PIM-SMでは、各マルチキャストグループを処理するためにアクティブなRPが1つだけ必要です。アクティブなRPに障害が発生すると、マルチキャストトラフィックが中断される可能性があります。エニーキャストRPメカニズムでは、1つのマルチキャストグループに対して同じIPアドレスを持つ複数のRPを設定することで、2つ以上のRP間の冗長バックアップが可能になります。マルチキャスト送信元が最も近いRPに登録されるか、受信者が最も近いRPに加入して、送信元情報の同期が実装されます。

MSDPを介して実装されたエニーキャストRPの場合、エニーキャストRPセット内のすべてのメンバーRPが同じIPアドレスを持ち、RP間でMSDPピアリング接続が確立されます。

図55に示すように、PIM-SMドメイン内では、マルチキャスト送信元はマルチキャストグループGにマルチキャストデータを送信し、受信者はマルチキャストグループに加入します。MSDPを介してエニーキャストRPを実装するには、次の作業を実行します。

1. 同じIPアドレス(エニーキャストRPアドレス、通常はプライベートアドレス)をデバイスAとデバイスBのインターフェイスに割り当てます。
2. インターフェイスをC-RPとして設定します。
3. デバイスAとデバイスBの間にMSDPピアリング関係を確立します。

図55 MSDPを介したエニーキャストRP



次に、MSDPを介したエニーキャストRPの実装方法について説明します。

1. ソースからマルチキャストデータを受信した後、ソース側のDRは最も近いRP(この例ではRP 1)に登録します。
2. レシーバ側のDRは、レシーバからIGMPレポートメッセージを受信した後、最も近いRP(この例ではRP 2)にJoinメッセージを送信します。このRPをルートとするRPTが確立されます。
3. RP1は、SAメッセージを介して登録されたマルチキャスト送信元情報を共有します。マルチキャスト送信元情報を取得した後、RP 2は(S, G)送信元固有のJoinメッセージを送信元に送信し、SPTを作成します。
4. マルチキャストデータがSPTに沿ってRP 2に到達すると、RP1はRPTに沿ってデータをレシーバに

転送します。マルチキャストデータを受信した後、レシーバ側のDRは、設定に基づいてRPTからSPTへのスイッチオーバープロセスを開始するかどうかを決定します。

プロトコルと標準

- RFC 3618『Multicast Source Discovery Protocol(MSDP)』
- RFC 3446『Anycast Rendezvous Point(RP)mechanism using Protocol Independent Multicast(PIM)and Multicast Source Discovery Protocol(MSDP)』

MSDPタスクの概要

1. MSDPの有効化
2. MSDPピアの作成
3. (任意)スタティックRPFピアの設定
4. (任意)MSDPメッシュグループの設定
5. (任意)MSDPピアリング接続の制御
 - MSDPピアリング接続の終了
 - MSDPセッションのキープアライブタイマーおよびピアホールドタイマーの設定
 - MSDP接続リトライ間隔の設定
 - TCP接続確立のためのMD5認証の有効化
6. (任意)SAメッセージ関連パラメータの設定
 - SAメッセージでのマルチキャストデータカプセル化の有効化
 - SAメッセージの発信元RPの設定
 - SA要求メッセージの設定
 - SAメッセージポリシーの設定
 - SAキャッシュメカニズムの設定
7. (任意)MSDPベースのエニーキャストRPの設定
8. (任意)MSDP NSRの有効化
9. (任意)発信MSDPプロトコルパケットのDSCP値の設定

MSDPの前提条件

MSDPを設定する前に、次の作業を実行します。

- ドメイン内のすべてのデバイスがネットワーク層で相互運用できるように、ユニキャストルーティングプロトコルを設定します。
- ドメイン内マルチキャストを有効にするようにPIM-SMを設定します。

MSDPの有効化

1. システムビューに入ります。

System-view

2. IPマルチキャストルーティングを有効にし、MRIBビューを開始します。

multicast routing

デフォルトでは、IPマルチキャストルーティングは無効になっています。

このコマンドの詳細については、『IP Multicast Command Reference』を参照してください。

3. システムビューに戻ります。

quit

4. MSDPを有効にし、MSDPビューを開始します。

msdp

デフォルトでは、MSDPは無効です。

MSDPピアの作成

MSDPピアの概要

MSDPピアリング関係は、アドレスペア(ローカルMSDPピアとリモートMSDPピアのアドレス)によって識別されます。MSDPピアリング接続を作成するには、MSDPピアのペアである両方のデバイスで次の操作を実行する必要があります。

MSDPピアの説明を設定すると、MSDPピアを他のMSDPピアと簡単に区別できます。

制約事項とガイドライン

MSDPピアとBGPまたはMBGPピアが同じインターフェイスを共有する場合は、同じIPアドレスを使用してMSDPピアとBGPまたはMBGPピアを指定します。

手順

1. システムビューに入ります。

System-view

2. MSDPビューを入力します。

msdp

3. MSDPピアを作成します。

peer *peer-address* **connect-interface** *interface-type interface-number*
4. (任意)MSDPピアの説明を設定します。

peer *peer-address* **description** *text*

スタティックRPFピアの設定

スタティックRPFピアについて

受信したSAメッセージに対してRPFチェックを実行しないように、スタティックRPFピアを設定できます。これにより、SAメッセージのRPFチェックメカニズムが簡素化されます。

制約事項とガイドライン

1つのMSDPピアだけがデバイスに設定されている場合、このMSDPピアはスタティックRPFピアと見なされます。

手順

1. システムビューに入ります。

System-view

2. MSDPビューを入力します。

msdp

3. スタティックRPFピアを設定します。

```
static-rpf-peer peer-address [ rp-policy ip-prefix-name ]
```

MSDPメッシュグループの設定

MSDPメッシュグループの概要

この機能は、AS内のMSDPピア間でのSAメッセージのフラッディングを回避します。また、これらのMSDPピア間でBGPまたはMBGPを実行する必要がないため、RPFチェックメカニズムが簡素化されます。

メッシュグループ外からSAメッセージを受信すると、メンバーMSDPピアはSAメッセージに対してRPFチェックを実行します。SAメッセージがRPFチェックに合格すると、メンバーMSDPピアはメッシュグループ内の他のメンバーにメッセージをフラッディングします。別のメンバーからSAメッセージを受信すると、MSDPピアはメッセージに対してRPFチェックを実行せず、メッセージを他のメンバーに転送しません。複数のMSDPピアを1つのメッシュグループにまとめるには、これらのMSDPピアに同じメッシュグループ名を割り当てます。

制約事項とガイドライン

MSDPメッシュグループを設定する前に、デバイスが相互に相互接続されていることを確認してください。1つのMSDPピアを複数のMSDPメッシュグループに割り当てると、最新の設定が有効になります。

手順

1. システムビューに入ります。

System-view

2. MSDPビューを入力します。

msdp

3. MSDPメッシュグループを設定します。

peer peer-address mesh-group name

デフォルトでは、MSDPピアはどのメッシュグループにも属しません。

MSDPピアリング接続の制御

MSDPピアリング接続の終了

MSDPピアリング接続の終了について

MSDPピアは、TCP(ポート番号639)を介して相互接続されます。MSDPピアリング接続をティアダウンまたは再確立して、MSDPピア間のSAメッセージ交換を制御できます。2つのMSDPピア間の接続がティアダウンすると、SAメッセージはピア間で配信されなくなります。接続の再確立は試行されません。ピアの設定情報は変更されません。

手順

1. システムビューに入ります。

System-view

2. MSDPビューを入力します。

msdp

3. MSDPピアリング接続をティアダウンします。

shutdown peer-address

デフォルトでは、MSDPピアリング接続はアクティブです。

MSDPセッションのキープアライブタイマーおよびピアホールドタイマーの設定

MSDPセッションのキープアライブタイマーおよびピアホールドタイマーについて

MSDPピアは定期的に相互にキープアライブメッセージを送信して、セッションを存続させます。セッションが確立されると、MSDPピアはピアにキープアライブメッセージを送信し、キープアライブタイマーとピアホールドタイマーを開始します。キープアライブタイマーが期限切れになると、MSDPピアは新しいキープアライブメッセージを送信します。MSDPピアは、ピアホールドタイマーが期限切れになる前にピアからMSDPメッセージを受信すると、ピアホールドタイマーをリセットします。それ以外の場合、MSDPピアはセッションを切断します。

MSDPピアはキープアライブタイマーとピアホールドタイマーをネゴシエートできないため、セッションのMSDPピアには同じキープアライブタイマーとピアホールドタイマーを設定する必要があります。キープアライブタイマーは、ピアホールドタイマーよりも小さくする必要があります。

手順

1. システムビューに入ります。

System-view

2. MSDPビューを入力します。

msdp

3. MSDPセッションのキープアライブタイマーおよびピアホールドタイマーを設定します。

timer keepalive keepalive holdtime

デフォルトでは、キープアライブタイマーとピアホールドタイマーはそれぞれ60秒と75秒です。

このコマンドは、確立されたセッションでただちに有効になります。

MSDP接続リトライ間隔の設定

MSDP接続リトライ間隔について

TCP接続は、次のいずれかの条件が存在する場合に必要です。

- 新しいMSDPピアが作成されます。
- 以前に非アクティブ化されたMSDPピアリング接続が再度アクティブ化されます。

- 以前に障害が発生したMSDPピアは、動作を再開しようとします。

MSDPピアリング接続試行の間隔を調整するには、次の作業を実行します。

手順

1. システムビューに入ります。

System-view

2. MSDPビューを入力します。

msdp

3. MSDP接続リトライ間隔を設定します。

timer retry interval

デフォルト設定は30秒です。

TCP接続確立のためのMD5認証の有効化

TCPコネクション確立時のMD5認証について

MSDPセキュリティを強化するには、両方のMSDPピアでMD5認証を有効にして、TCP接続を確立します。MD5認証に失敗すると、TCP接続を確立できません。

制約事項とガイドライン

認証およびTCP接続の障害を回避するために、MD5認証に関与するMSDPピアに対して同じ認証方式およびキーを設定します。

手順

1. システムビューに入ります。

System-view

2. MSDPビューを入力します。

msdp

3. MSDPピアとのTCP接続の確立時にMD5認証を実行するようにデバイスを設定します。

peer peer-address password { cipher | simple } password

デフォルトでは、デバイスは、MSDPピアとTCP接続を確立する時、MD5認証を実行しません。

SAメッセージ関連パラメータの設定

SAメッセージでのマルチキャストデータカプセル化の有効化

SAメッセージのマルチキャストデータカプセル化の概要

一部のマルチキャスト送信元は、(S, G)エントリのエージングタイムよりも長い間隔でマルチキャストデータを送信します。この場合、送信元側のDRは、マルチキャストデータを登録メッセージにパケット単位でカプセル化し、送信元側のRPに送信する必要があります。送信元側のRPは、SAメッセージを使用して(S, G)情報をリモートRPに送信します。次に、リモートRPはJoinメッセージを送信元側のDRに送信し、SPTを構築します。(S, G)エントリがタイムアウトしたため、リモートレシーバはマルチキャスト送信元からマルチキャストデータを受信できません。

この問題を回避するには、ソース側RPを有効にして、マルチキャストデータをSAメッセージにカプセル化します。その結果、ソース側RPは、SAメッセージ内のマルチキャストデータをリモートMSDPピアに転送できます。SAメッセージを受信したリモートRPは、SAメッセージのカプセル化を解除し、マルチキャストデータをRPTに沿ってローカルドメイン内のレシーバに転送します。

手順

1. システムビューに入ります。

System-view

2. MSDPビューを入力します。

msdp

3. SAメッセージのマルチキャストデータカプセル化を有効にします。

encap-data-enable

デフォルトでは、SAメッセージには(S, G)エントリだけが含まれ、マルチキャストデータは含まれません。

SAメッセージの発信元RPの設定

SAメッセージの発信元RPの設定について

この機能を使用すると、インターフェイスでSAメッセージを発信し、そのIPアドレスをSAメッセージ内のRPアドレスとして使用できます。通常は、Anycast-RPアプリケーションで使用されます。

デフォルトでは、メンバーAnycast-RPによって発信されたSAメッセージ内のRPアドレスはAnycast-RPアドレスです。SAメッセージ内のRPアドレスはローカルRPアドレスと同じであるため、SAメッセージは他のメンバーでのRPFチェックに失敗します。この場合、Anycast-RP内で送信元情報を交換できません。この問題を解決するには、メンバーAnycast-RPがSAメッセージの発信元RPとして存在するインターフェイス以外のインターフェイスを指定する必要があります。

手順

1. システムビューに入ります。

System-view

2. MSDPビューを入力します。

msdp

3. インターフェイスをSAメッセージの発信元RPとして設定します。

originating-rp *interface-type interface-number*

デフォルトでは、SAメッセージは実際のRPによって発信されます。

SA要求メッセージの設定

SA要求メッセージの設定について

デフォルトでは、新しい加入メッセージを受信したあと、マルチキャスト送信元情報を取得してSPTに加入するために、デバイスはSAメッセージを待ちます。SA要求メッセージをMSDPピアに送信することで、デバイスが送信元情報を要求できるようにすることができます。これにより、加入遅延が減少します。SA要求ポリシーを使用すると、デバイスは、マルチキャストグループを指定するACLを使用して、MSDPピアからのSA要求メッセージをフィルタリングできます。

必要条件

デバイスによるSA要求の送信を有効にする前に、**undocache-sa-enable**コマンドによってSAメッセージキャッシュメカニズムが無効になっていることを確認してください。

手順

1. システムビューに入ります。

System-view

2. MSDPビューを入力します。

msdp

3. デバイスがSA要求メッセージをMSDPピアに送信できるようにします。

peer *peer-address* **request-sa-enable**

デフォルトでは、新しいJoinメッセージを受信したあと、デバイスはどのMSDPピアにもSA要求メッセージを送信せず、MSDPピアからの次のSAメッセージを待ちます。

4. MSDPピアのSA要求ポリシーを設定します。

peer *peer-address* **sa-request-policy** [**acl** *ipv4-acl-number*]

デフォルトでは、SA要求ポリシーは存在せず、MSDPピアからのすべてのSA要求が許可されます。

SAメッセージポリシーの設定

SAメッセージポリシーについて

マルチキャスト送信元情報の伝播を制御するには、次のポリシーを設定します。

- **SA creation policy:** SAメッセージでアドバタイズされるマルチキャスト送信元情報を制限します。このポリシーにより、デバイスは、マルチキャスト送信元およびグループを指定する使用ACLに基

づいて(S, G)エントリをアドバタイズできます。

- **SA incoming or outgoing policy:** SAメッセージの受信または転送を制限します。このポリシーにより、デバイスは、マルチキャスト送信元およびグループを指定するACLに基づいてSAメッセージを受信または転送できます。
- **The lower TTL threshold for multicast data packets encapsulated in SA messages:** デフォルトでは、マルチキャストデータパケットはSAメッセージにカプセル化され、パケットのTTL値がゼロより大きい場合にだけMSDPピアに転送されます。MSDPピアに送信されるSAメッセージにカプセル化されたマルチキャストデータパケットの下限TTLしきい値を設定できます。次に、TTL値が設定値以上であるマルチキャストデータパケットだけがSAメッセージにカプセル化されます。TTL値が設定値以上であるSAメッセージだけが、指定されたMSDPピアに転送されます。これにより、マルチキャストデータパケットのカプセル化が制御され、SAメッセージの伝播範囲が制限されます。

手順

1. システムビューに入ります。

System-view

2. MSDPビューを入力します。

msdp

3. SA作成ポリシーを設定します。

```
import-source [ acl ipv4-acl-number ]
```

4. SA着信ポリシーまたは発信ポリシーを設定します。

```
peer peer-address sa-policy { export | import } [ acl ipv4-acl-number ]
```

デフォルトでは、SA着信または発信ポリシーは設定されていません。デバイスは、着信または発信SAメッセージをフィルタリングしません。

5. SAメッセージにカプセル化されたマルチキャストデータパケットの下限TTLしきい値を設定します。

```
peer peer-address minimum-ttl ttl-value
```

既定の設定は0です。

SAキャッシュメカニズムの設定

SAキャッシュメカニズムについて

SAキャッシュメカニズムを使用すると、デバイスはSAメッセージに含まれる(S, G)エントリをローカルにキャッシュできます。これにより、マルチキャスト送信元情報を取得する時間が短縮されますが、メモリの占有量が増加します。

SAキャッシュメカニズムが有効の場合、デバイスは新しい(*,G)Joinメッセージを受信すると、最初にSAメッセージキャッシュを検索します。

- 一致する(S, G)エントリが見つからない場合、デバイスは、MSDPピアが次のサイクルで送信するSAメッセージを待ちます。

- 一致する(S, G)エントリがキャッシュ内で見つかった場合、デバイスはSをルートとするSPTに加入します。

DoS攻撃からデバイスを保護するために、MSDPピアからのSAキャッシュ内の(S, G)エントリ数に制限を設定できます。

手順

1. システムビューに入ります。

System-view

2. MSDPビューを入力します。

msdp

3. SAキャッシュメカニズムを有効にします。

cache-sa-enable

デフォルトでは、SAメッセージキャッシュメカニズムは有効になっています。デバイスは、受信したSAメッセージに含まれる(S, G)エントリをキャッシュします。

4. (任意)MSDPピアからのSAキャッシュ内の(S, G)エントリの最大数を設定します。

peer *peer-address* **sa-cache-maximum** *sa-limit*

デフォルト設定は4294967295です。

MSDPベースのエニーキャストRPの設定

1. 複数のデバイスで同じRPを設定します。

RPの設定の詳細については、「PIMの設定」を参照してください。

2. デバイス間のMSDPピア関係を確立します。RPアドレスは、MSDPピアアドレスとは異なる必要があります。

MSDPピア関係の確立の詳細については、「MSDPピアの作成」を参照してください。

MSDPピア関係を確立するためのIPアドレスは、エニーキャストRPアドレスとは異なる必要があります。

MSDP NSRの有効化

MSDP NSRの概要

この機能により、MSDPはプロトコルステート情報およびデータ(MSDPピアおよびリモートマルチキャスト送信元情報など)をアクティブプロセスからスタンバイプロセスにバックアップできます。アクティブプロセスに障害が発生すると、スタンバイプロセスがシームレスに引き継ぎます。この機能を使用して、アクティブ/スタンバイスイッチオーバーが発生したときにMSDPの転送が中断されないようにします。

手順

1. システムビューに入ります。

System-view

2. MSDP NSRを有効にします。

msdp non-stop-routing

デフォルトでは、MSDP NSRは無効です。

発信MSDPプロトコルパケットのDSCP値の設定

発信MSDPプロトコルパケットのDSCP値について

DSCP値は、パケット送信の優先順位を決定します。DSCP値が大きいほど、優先順位が高くなります。

手順

1. システムビューに入ります。

System-view

2. MSDPビューを入力します。

msdp

3. 発信MSDPプロトコルパケットのDSCP値を設定します。

dscp *dscp-value*

デフォルトでは、発信MSDPプロトコルパケットのDSCP値は48です。

MSDPの表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
MSDPピアに関する要約情報を表示します。	display msdpbrief [state{connect disabled established listen shutdown}]
MSDP NSRステータス情報を表示します。	display msdp non-stop-routing status
MSDPピアの詳細なステータスを表示します。	display msdppeer-status [peer-address]
SAキャッシュ内の(S, G)エントリを表示します。	display msdpsa-cache [group-address source-address as-number]*
SAキャッシュ内の(S, G)エントリ数を表示します。	display msdpsa-count [as-number]
MSDPピアとのTCP接続をリセットし、MSDPピアの統計情報をクリアします。	reset msdppeer [peer-address]
SAキャッシュ内の(S, G)エントリを削除します。	reset msdpsa-cache [group-address]
MSDPピアとのTCP接続をリセットせずに、MSDPピアの統計情報をクリアします。	reset msdpstatistics [peer-address]

MSDPの設定例

例:PIM-SMドメイン間マルチキャストの設定

ネットワークの設定

図56に示します。

- OSPFはAS 100およびAS 200内で動作し、BGPはこれらの間で動作します。
- 各PIM-SMドメインには、少なくとも1つのマルチキャスト送信元または受信者があります。

PIM-SMドメイン内のRP間でMSDPピアリング関係を設定して、PIM-SMドメイン間でマルチキャスト送信元情報を共有します。

図56 ネットワークダイアグラム

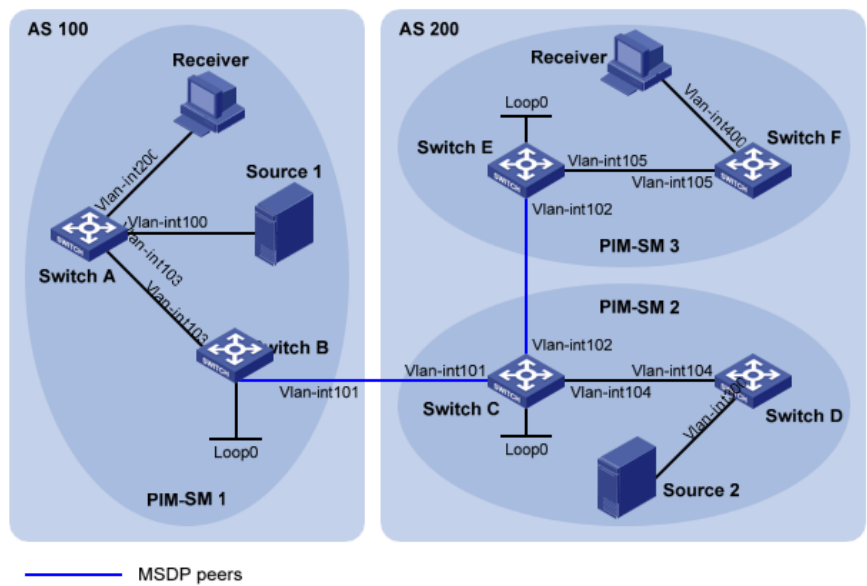


表12 インターフェイスとIPアドレスの割り当て

デバイス	インターフェイス	IPアドレス	デバイス	インターフェイス	IPアドレス
Switch A	Vlan-int103	10.110.1.2/24	Switch D	Vlan-int104	10.110.4.2/24
Switch A	Vlan-int100	10.110.2.1/24	Switch D	Vlan-int300	10.110.5.1/24
Switch A	Vlan-int200	10.110.3.1/24	Switch E	Vlan-int105	10.110.6.1/24
Switch B	Vlan-int103	10.110.1.1/24	Switch E	Vlan-int102	192.168.3.2/24
Switch B	Vlan-int101	192.168.1.1/24	Switch E	Loop0	3.3.3.3/32
Switch B	Loop0	1.1.1.1/32	Switch F	Vlan-int105	10.110.6.2/24
Switch C	Vlan-int104	10.110.4.1/24	Switch F	Vlan-int400	10.110.7.1/24
Switch C	Vlan-int102	192.168.3.1/24	Source 1	-	10.110.2.100/24
Switch C	Vlan-int101	192.168.1.2/24	Source 2	-	10.110.5.100/24
Switch C	Loop0	2.2.2.2/32	Switch D	Vlan-int104	10.110.4.2/24

手順

1. 図56に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
2. AS内のスイッチにOSPFを設定します(詳細は省略)。
3. IPマルチキャストルーティングとPIM-SMを有効にし、PIM-SMドメイン境界を設定します。

#スイッチAで、IPマルチキャストルーティングを有効にします。

```
<SwitchA> system-view
```

```
[SwitchA] multicast routing
```

```
[SwitchA-mrib] quit
```

#VLAN-interface 103およびVLAN-interface 100でPIM-SMを有効にします。

```
[SwitchA] interface vlan-interface 103
```

```
[SwitchA-Vlan-interface103] pim sm
```

```
[SwitchA-Vlan-interface103] quit
```

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] pim sm
```

```
[SwitchA-Vlan-interface100] quit
```

#受信側のインターフェイス(VLAN-インターフェイス200)でIGMPを有効にします。

```
[SwitchA] interface vlan-interface 200
```

```
[SwitchA-Vlan-interface200] igmp enable
```

```
[SwitchA-Vlan-interface200] quit
```

#スイッチB、スイッチC、スイッチD、スイッチEでIPマルチキャストルーティングおよびPIM-SMを有効にします。スイッチAと同じ方法でスイッチFを設定します。(詳細は省略)

#スイッチBにPIMドメイン境界を設定します。

```
[SwitchB] interface vlan-interface 101
```

```
[SwitchB-Vlan-interface101] pim bsr-boundary
```

```
[SwitchB-Vlan-interface101] quit
```

#スイッチBと同じ方法で、スイッチCとスイッチEにPIMドメイン境界を設定します。(詳細は省略)。

4. C-BSRおよびC-RPを設定します。

#スイッチBでLoopback 0をC-BSRおよびC-RPとして設定します。

```
[SwitchB] pim
```

```
[SwitchB-pim] c-bsr 1.1.1.1
```

```
[SwitchB-pim] c-rp 1.1.1.1
```

```
[SwitchB-pim] quit
```

#スイッチBと同様に、スイッチCおよびスイッチEでC-BSRおよびC-RPを設定します。(詳細は省略)。

5. BGPとOSPFの間で相互にルートを再配布するようにBGPを設定します。

#スイッチBでEBGPピアを設定し、OSPFルートを再配布します。

```
[SwitchB] bgp 100
```

```
[SwitchB-bgp] router-id 1.1.1.1
```

```
[SwitchB-bgp] peer 192.168.1.2 as-number 200
```

```
[SwitchB-bgp] address-family ipv4 unicast
```

```
[SwitchB-bgp-ipv4] import-route ospf 1
```

```
[SwitchB-bgp-ipv4] peer 192.168.1.2 enable
```

```
[SwitchB-bgp-ipv4] quit
```

#スイッチCで、EBGPピアを設定し、OSPFルートを再配布します。

```
[SwitchC] bgp 200
```

```
[SwitchC-bgp] router-id 2.2.2.2
```

```
[SwitchC-bgp] peer 192.168.1.1 as-number 100
```

```
[SwitchC-bgp] address-family ipv4 unicast
```

```
[SwitchC-bgp-ipv4] import-route ospf 1
```

```
[SwitchC-bgp-ipv4] peer 192.168.1.1 enable
```

```
[SwitchC-bgp-ipv4] quit
```

#スイッチBのOSPFにBGPルートを再配布します。

```
[SwitchB] ospf 1
```

```
[SwitchB-ospf-1] import-route bgp
```

```
[SwitchB-ospf-1] quit
```

#スイッチCのOSPFにBGPルートを再配布します。

```
[SwitchB] ospf 1
```

```
[SwitchB-ospf-1] import-route bgp
```

```
[SwitchB-ospf-1] quit
```

6. MSDPピアを設定します。

#スイッチBでMSDPピアを設定します。

```
[SwitchB] msdp
```

```
[SwitchB-msdp] peer 192.168.1.2 connect-interface vlan-interface 101
```

```
[SwitchB-msdp] quit
```

#スイッチCでMSDPピアを設定します。

```
[SwitchC] msdp
```

```
[SwitchC-msdp] peer 192.168.1.1 connect-interface vlan-interface 101
```

```
[SwitchC-msdp] peer 192.168.3.2 connect-interface vlan-interface 102
```

```
[SwitchC-msdp] quit
```

#スイッチEでMSDPピアを設定します。

```
[SwitchE] msdp
```

```
[SwitchE-msdp] peer 192.168.3.1 connect-interface vlan-interface 102
```

```
[SwitchE-msdp] quit
```

設定の確認

#スイッチBのBGPピアグループに関する情報を表示します。

```
[SwitchB] display bgp peer ipv4
```

BGP local router ID: 1.1.1.1

Local AS number: 100

Total number of peers: 1

Peers in established state: 1 Peer

	AS	MsgRcvd	MsgSent	OutQ	PrefRcv	Up/Down	State
192.168.1.2	200	24	21	0	6	00:20:07	Established

#スイッチCのBGPピアグループに関する情報を表示します。

```
[SwitchC] display bgp peer ipv4
```

BGP local router ID: 2.2.2.2

Local AS number: 1

Total number of peers: 1

Peers in established state: 1 Peer

	AS	MsgRcvd	MsgSent	OutQ	PrefRcv	Up/Down	State
192.168.1.1	100	18	16	0	1	00:20:07	Established

#スイッチCのBGPルーティングテーブルを表示します。

[SwitchC] display bgp routing-table ipv4

Total number of routes: 5

BGP local router ID is 2.2.2.2

Status codes: * - valid, > - best, d - dampened, h - history,

s - suppressed, S - stale, i - internal, e - external

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* >	1.1.1.1/32	192.168.1.1	0		0	100?
* >i	2.2.2.2/32	0.0.0.0	0		0	?
* >	192.168.1.0	0.0.0.0	0		0	?
* >	192.168.1.1/32	0.0.0.0	0		0	?
* >	192.168.1.2/32	0.0.0.0	0		0	?

#PIM-SM 1およびPIM-SM 3のホストが、PIM-SM 1のSource 1およびPIM-SM 2のSource 2からのマルチキャストデータを受信できることを確認します(詳細は省略)。

[SwitchB] display msdp brief

Configured	Established	Listen	Connect	Shutdown	Disabled
1	1	0	0	0	0

Peer address	State	Up/Down time	AS	SA count	Reset count
192.168.1.2	Established	00:12:57	200	13	0

#スイッチCのMSDPピアグループに関する要約情報を表示します。

[SwitchC] display msdp brief

Configured	Established	Listen	Connect	Shutdown	Disabled
1	1	0	0	0	0

Peer address	State	Up/Down time	AS	SA count	Reset count
192.168.3.2	Established	01:43:57	?	8	0
192.168.1.1	Established	01:43:57	?	13	0

Switch E に MSDP ピアグループに関する簡単な情報を表示する。

[SwitchE] display msdp brief

Configured	Established	Listen	Connect	Shutdown	Disabled
1	1	0	0	0	0

Peer address	State	Up/Down time	AS	SA count	Reset count
192.168.3.1	Established	01:07:57	200	8	0

#スイッチBの詳細なMSDPピア情報を表示します。

[SwitchB] display msdp peer-status

MSDP Peer 192.168.1.2; AS 200

Description:

Information about connection status:

State: Established

Up/down time: 00:15:47

Resets: 0

Connection interface: Vlan-interface101 (192.168.1.1)
 Received/sent messages: 16/16
 Discarded input messages: 0
 Discarded output messages: 0
 Elapsed time since last connection or counters clear: 00:17:40
 Mesh group peer joined: momo
 Last disconnect reason: Hold timer expired with truncated message
 Truncated packet: 5 bytes in buffer, type: 1, length: 20, without packet time: 75sn
 Information about (Source, Group)-based SA filtering policy:
 Import policy: None
 Export policy: None
 Information about SA-Requests:
 Policy to accept SA-Requests: None
 Sending SA-Requests status: Disable
 Minimum TTL to forward SA with encapsulated data: 0
 SAs learned from this peer: 0, SA cache maximum for the peer: 4294967295
 Input queue size: 0, Output queue size: 0
 Counters for MSDP messages:
 RPF check failure: 0
 Incoming/outgoing SA: 0/0
 Incoming/outgoing SA-Request: 0/0
 Incoming/outgoing SA-Response: 0/0
 Incoming/outgoing Keepalive: 867/867
 Incoming/outgoing Notification: 0/0
 Incoming/outgoing Traceroutes in progress: 0/0
 Incoming/outgoing Traceroute reply: 0/0
 Incoming/outgoing Unknown: 0/0
 Incoming/outgoing data packet: 0/0

例:スタティックRPFピアを利用したAS間マルチキャストの設定

ネットワークの設定

図57に示します。

- このネットワークには、AS 100とAS 200の2つのASがあります。OSPFは各AS内で実行されます。BGPは2つのAS間で実行されます。
- PIM-SM 1はAS 100に属し、PIM-SM 2およびPIM-SM 3はAS 200に属します。各PIM-SMDメインには、少なくとも1つのマルチキャスト送信元または受信者があります。
inter-ASマルチキャストを次のように設定します。
- スイッチA、スイッチD、およびスイッチGで、ループバック0を関連するPIM-SMDメインのC-BSRおよびC-RPとして設定します。
- ピアRPF転送ルールに従って、スイッチはスタティックRPFピアからのフィルタリングポリシーを通過するSAメッセージを受け入れます。ユニキャストトポロジ構造を変更せずにPIM-SMDメイン間でマルチキャスト送信元情報を共有するには、PIM-SMDメインのRPIにMSDPピアリング関係を設定し、スタティックRPFピアリング関係を設定します。

図57 ネットワーク図

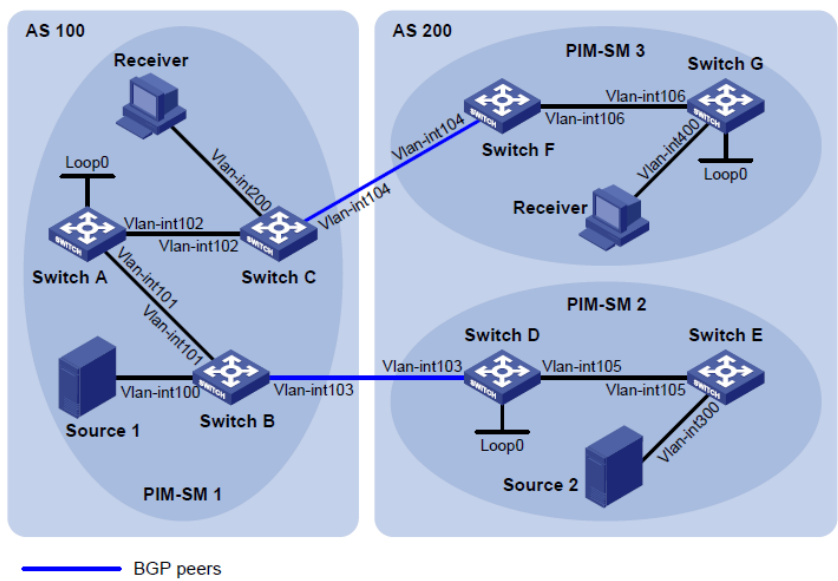


表13 インターフェイスとIPアドレスの割り当て

デバイス	インターフェイス	IPアドレス	デバイス	インターフェイス	IPアドレス
source1	-	192.168.1.100/24	Switch D	Vlan-int105	10.110.5.1/24
Source2	-	192.168.3.100/24	Switch D	Vlan-int103	10.110.3.2/24
Switch A	Vlan-int101	10.110.1.1/24	Switch D	Loop0	2.2.2.2/32
Switch A	Vlan-int102	10.110.2.1/24	Switch E	Vlan-int105	10.110.5.2/24
Switch A	Loop0	1.1.1.1/32	Switch E	Vlan-int300	192.168.3.1/24

Switch B	Vlan-int101	10.110.1.2/24	Switch F	Vlan-int106	10.110.6.1/24
Switch B	Vlan-int100	192.168.1.1/24	Switch F	Vlan-int104	10.110.4.2/24
Switch B	Vlan-int103	10.110.3.1/24	Switch G	Vlan-int106	10.110.6.2/24
Switch C	Vlan-int102	10.110.2.2/24	Switch G	Vlan-int400	192.168.4.1/24
Switch C	Vlan-int200	192.168.2.1/24	Switch G	Loop0	3.3.3.3/32
Switch C	Vlan-int104	10.110.4.1/24			

手順

1. 表13に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
2. AS内のスイッチにOSPFを設定します(詳細は省略)。
3. IPマルチキャストルーティング、PIM-SM、およびIGMPを有効にし、PIM-SMドメイン境界を設定します。

#スイッチCで、IPマルチキャストルーティングを有効にします。

```
<SwitchC> system-view
```

```
[SwitchC] multicast routing
```

```
[SwitchC-mrib] quit
```

#各インターフェイスでPIM-SMを有効にし、受信側インターフェイスでIGMPを有効にします。

(VLAN-インターフェイス200)。

```
[SwitchC] interface vlan-interface 102
```

```
[SwitchC-Vlan-interface102] pim sm
```

```
[SwitchC-Vlan-interface102] quit
```

```
[SwitchC] interface vlan-interface 200
```

```
[SwitchC-Vlan-interface200] igmp enable
```

```
[SwitchC-Vlan-interface200] quit
```

```
[SwitchC] interface vlan-interface 104
```

```
[SwitchC-Vlan-interface104] pim sm
```

```
[SwitchC-Vlan-interface104] quit
```

#スイッチCを設定するのと同じ方法で、スイッチA、スイッチB、スイッチD、スイッチE、スイッチF、およびスイッチGを設定します(詳細は省略)。

#スイッチBで、PIMドメイン境界を設定します。

```
[SwitchB] interface vlan-interface 103
```

```
[SwitchB-Vlan-interface103] pim bsr-boundary
```

```
[SwitchB-Vlan-interface103] quit
```

#同じ方法で、スイッチC、スイッチD、およびスイッチFのPIMドメイン境界を設定します。

スイッチBが設定されます(詳細は省略)。

4. C-BSRおよびC-RPを設定します。

#スイッチAで、Loopback 0をC-BSRおよびC-RPとして設定します。

```
[SwitchA] pim
```

```
[SwitchA-pim] c-bsr 1.1.1.1
```

```
[SwitchA-pim] c-rp 1.1.1.1
```

```
[SwitchA-pim] quit
```

#スイッチAと同様に、スイッチDおよびスイッチGでC-BSRおよびC-RPを設定します。
(詳細は省略)。

5. BGPを設定し、BGPルーティング情報をOSPFに再配布し、OSPFルーティング情報をBGPに再配布します。

#スイッチBで、EBGPピアを設定し、OSPFルーティング情報を再配布します。

```
[SwitchB] bgp 100
[SwitchB-bgp] router-id 1.1.1.2
[SwitchB-bgp] peer 10.110.3.2 as-number 200
[SwitchB-bgp] address-family ipv4 unicast
[SwitchB-bgp-ipv4] peer 10.110.3.2 enable
[SwitchB-bgp-ipv4] import-route ospf 1
[SwitchB-bgp-ipv4] quit
[SwitchB-bgp] quit
```

#スイッチDで、EBGPピアを設定し、OSPFルーティング情報を再配布します。

```
[SwitchD] bgp 200
[SwitchD-bgp] router-id 2.2.2.2
[SwitchD-bgp] peer 10.110.3.1 as-number 100
[SwitchD-bgp] address-family ipv4 unicast
[SwitchD-bgp-ipv4] peer 10.110.3.1 enable
[SwitchD-bgp-ipv4] import-route ospf 1
[SwitchD-bgp-ipv4] quit
[SwitchD-bgp] quit
```

#スイッチCで、EBGPピアを設定し、OSPFルーティング情報を再配布します。

```
[SwitchC] bgp 100
[SwitchC-bgp] router-id 1.1.1.3
[SwitchC-bgp] peer 10.110.4.2 as-number 200
[SwitchC-bgp] address-family ipv4 unicast
[SwitchC-bgp-ipv4] peer 10.110.4.2 enable
[SwitchC-bgp-ipv4] import-route ospf 1
[SwitchC-bgp-ipv4] quit
[SwitchC-bgp] quit
```

#スイッチFで、EBGPピアを設定し、OSPFルーティング情報を再配布します。

```
[SwitchF] bgp 200
[SwitchF-bgp] router-id 3.3.3.1
[SwitchF-bgp] peer 10.110.4.1 as-number 100
[SwitchF-bgp] address-family ipv4 unicast
[SwitchF-bgp-ipv4] peer 10.110.4.1 enable
[SwitchF-bgp-ipv4] import-route ospf 1
[SwitchF-bgp-ipv4] quit
[SwitchF-bgp] quit
```

#スイッチBでは、BGPルーティング情報をOSPFに再配布します。

```
[SwitchB] ospf 1
[SwitchB-ospf-1] import-route bgp
[SwitchB-ospf-1] quit
```

#スイッチDでは、BGPルーティング情報をOSPFに再配布します。

```
[SwitchD] ospf 1
[SwitchD-ospf-1] import-route bgp
[SwitchD-ospf-1] quit
```

#スイッチCでは、BGPルーティング情報をOSPFに再配布します。

```
[SwitchC] ospf 1
[SwitchC-ospf-1] import-route bgp
[SwitchC-ospf-1] quit
```

#スイッチFでは、BGPルーティング情報をOSPFに再配布します。

```
[SwitchF] ospf 1
[SwitchF-ospf-1] import-route bgp
[SwitchF-ospf-1] quit
```

6. MSDPピアおよびスタティックRPFピアを設定します。

#スイッチAで、スイッチDとスイッチGをMSDPピアおよびスタティックRPFピアとして設定します。

```
[SwitchA] ip prefix-list list-dg permit 10.110.0.0 16 greater-equal 16 less-equal 32
[SwitchA] msdp
[SwitchA-msdp] peer 10.110.3.2 connect-interface vlan-interface 101
[SwitchA-msdp] peer 10.110.6.2 connect-interface vlan-interface 102
[SwitchA-msdp] static-rpf-peer 10.110.3.2 rp-policy list-dg
[SwitchA-msdp] static-rpf-peer 10.110.6.2 rp-policy list-dg
[SwitchA-msdp] quit
```

#スイッチDで、スイッチAをMSDPピアおよびスタティックRPFピアとして設定します。

```
[SwitchD] ip prefix-list list-a permit 10.110.0.0 16 greater-equal 16 less-equal 32
[SwitchD] msdp
[SwitchD-msdp] peer 10.110.1.1 connect-interface vlan-interface 103
[SwitchD-msdp] static-rpf-peer 10.110.1.1 rp-policy list-a
[SwitchD-msdp] quit
```

#スイッチGで、スイッチAをMSDPピアおよびスタティックRPFピアとして設定します。

```
[SwitchG] ip prefix-list list-a permit 10.110.0.0 16 greater-equal 16 less-equal 32
[SwitchG] msdp
[SwitchG-msdp] peer 10.110.2.1 connect-interface vlan-interface 106
[SwitchG-msdp] static-rpf-peer 10.110.2.1 rp-policy list-a
[SwitchG-msdp] quit
```

設定の確認

#スイッチA上のBGPピアリング関係を表示します。

```
[SwitchA] display bgp peer
```

スイッチAとスイッチDの間、またはスイッチAとスイッチGの間にBGPピアリング関係が確立されていないため、情報は出力されません。つまり、ユニキャストトポロジは変更されません。

#スイッチA上のMSDPピアに関する要約情報を表示します。

```
[SwitchA] display msdp brief
```

Configured	Established	Listen	Connect	Shutdown	Disabled
2	2	0	0	0	0

Peer address	State	Up/Down time	AS	SA count	Reset count
10.110.3.2	Established	01:07:08	?	8	0
10.110.6.2	Established	00:16:39	?	13	0

#スイッチD上のMSDPピアに関する要約情報を表示します。

[SwitchD] display msdp brief

Configured	Established	Listen	Connect	Shutdown	Disabled
1	1	0	0	0	0
Peer address	State	Up/Down time	AS	SA count	Reset count
10.110.1.1	Established	01:07:09	?	8	0

#スイッチG上のMSDPピアに関する要約情報を表示します。

[SwitchG] display msdp brief

Configured	Established	Listen	Connect	Shutdown	Disabled
1	1	0	0	0	0
Peer address	State	Up/Down time	AS	SA count	Reset count
10.110.2.1	Established	00:16:40	?	13	0

#PIM-SM 1およびPIM-SM 3のレシーバが、Source 1およびSource 2からマルチキャストグループへのマルチキャストデータを受信できることを確認します(詳細は省略)。

例:エニーキャストRPの設定

ネットワークの設定

図58に示すように、OSPFはドメイン内で実行され、ユニキャストルートを提供します。

レシーバ側DRとソース側DRが、トポロジ的に最も近いそれぞれのRPへの加入プロセスを開始できるように、エニーキャストRPアプリケーションを設定します。

スイッチBとスイッチDのルータIDをそれぞれ1.1.1.1と2.2.2.2に設定します。スイッチBとスイッチDの間にMSDPピアリング関係を設定します。

図58 ネットワークダイアグラム

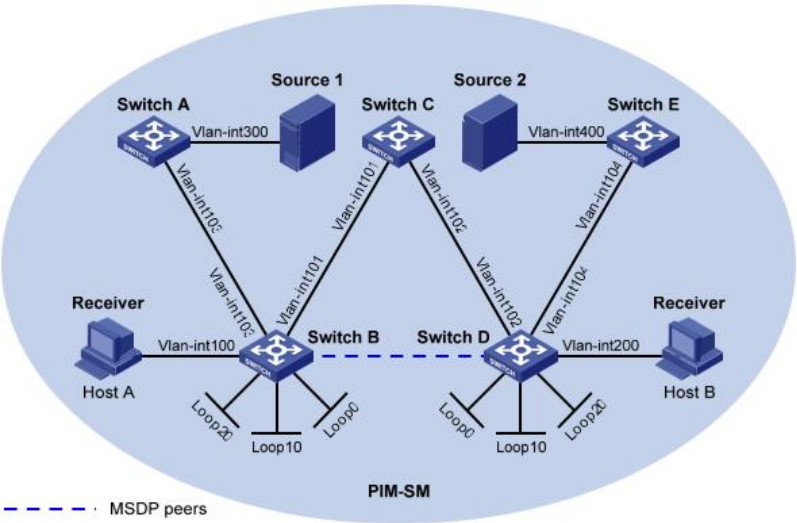


表14インターフェイスとIPアドレスの割り当て

デバイス	インターフェイス	IPアドレス	デバイス	インターフェイス	IPアドレス
Source1	-	10.110.5.100/24	Switch C	Vlan-int101	192.168.1.2/24
Source2	-	10.110.6.100/24	Switch C	Vlan-int102	192.168.2.2/24
Switch A	Vlan-int300	10.110.5.1/24	Switch D	Vlan-int200	10.110.3.1/24
Switch A	Vlan-int103	10.110.2.2/24	Switch D	Vlan-int104	10.110.4.1/24
Switch B	Vlan-int100	10.110.1.1/24	Switch D	Vlan-int102	192.168.2.1/24
Switch B	Vlan-int103	10.110.2.1/24	Switch D	Loop0	2.2.2.2/32
Switch B	Vlan-int101	192.168.1.1/24	Switch D	Loop10	4.4.4.4/32
Switch B	Loop0	1.1.1.1/32	Switch D	Loop20	10.1.1.1/32
Switch B	Loop10	3.3.3.3/32	Switch E	Vlan-int400	10.110.6.1/24
Switch B	Loop20	10.1.1.1/32	Switch E	Vlan-int104	10.110.4.2/24

手順

- 図58に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
- スイッチにOSPFを設定します(詳細は省略)。

3. IPマルチキャストルーティング、IGMP、およびPIM-SMを有効にします。

#スイッチBで、IPマルチキャストルーティングを有効にします。

```
<SwitchB> system-view
[SwitchB] multicast routing
[SwitchB-mrib] quit
```

#受信側のインターフェイス(VLANインターフェイス100)でIGMPを有効にします。

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] igmp enable
[SwitchB-Vlan-interface100] quit
```

#他のインターフェイスでPIM-SMを有効にします。

```
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] pim sm
[SwitchB-Vlan-interface103] quit
[SwitchB] interface Vlan-interface 101
[SwitchB-Vlan-interface101] pim sm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface loopback 0
[SwitchB-LoopBack0] pim sm
[SwitchB-LoopBack0] quit
[SwitchB] interface loopback 10
[SwitchB-LoopBack10] pim sm
[SwitchB-LoopBack10] quit
[SwitchB] interface loopback 20
[SwitchB-LoopBack20] pim sm
[SwitchB-LoopBack20] quit
```

#スイッチBの設定と同じ方法で、スイッチA、スイッチC、スイッチD、およびスイッチEのIPマルチキャストルーティング、IGMP、およびPIM-SMを有効にします(詳細は省略)。

4. C-BSRおよびC-RPを設定します。

#スイッチBでLoopback 10をC-BSRとして、Loopback 20をC-RPとして設定します。

```
[SwitchB] pim
[SwitchB-pim] c-bsr 3.3.3.3
[SwitchB-pim] c-rp 10.1.1.1
[SwitchB-pim] quit
```

#スイッチBを設定するのと同じ方法で、スイッチDにC-BSRとC-RPを設定します。(詳細は省略)。

5. MSDPピアを設定します。

#スイッチBのループバック0にMSDPピアを設定します。

```
[SwitchB] msdp
[SwitchB-msdp] originating-rp loopback 0
[SwitchB-msdp] peer 2.2.2.2 connect-interface loopback 0
[SwitchB-msdp] quit
```

#スイッチDのループバック0にMSDPピアを設定します。

```
[SwitchD] msdp
[SwitchD-msdp] originating-rp loopback 0
[SwitchD-msdp] peer 1.1.1.1 connect-interface loopback 0
```

[SwitchD-msdp] quit

設定の確認

#スイッチB上のMSDPピアに関する要約情報を表示します。

[SwitchB] display msdp brief

Configured	Established	Listen	Connect	Shutdown	Disabled
1	1	0	0	0	0

Peer address	State	Up/Down time	AS	SA count	Reset count
2.2.2.2	Established	00:10:57	?	0	0

#スイッチD上のMSDPピアに関する要約情報を表示します。

[SwitchD] display msdp brief

Configured	Established	Listen	Connect	Shutdown	Disabled
1	1	0	0	0	0

Peer address	State	Up/Down time	AS	SA count	Reset count
1.1.1.1	Established	00:10:57	?	0	0

ホストAからIGMPレポートを送信してマルチキャストグループ225.1.1.1に参加します。(詳細は省略)

ソース1からマルチキャストデータをマルチキャストグループ225.1.1.1に送信します。(詳細は省略)

スイッチDでPIMルーティングテーブルを表示します。

[SwitchD] display pim routing-table

スイッチDでは何も出力されません。

スイッチBでPIMルーティングテーブルを表示します。

[SwitchB] display pim routing-table

Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)

RP: 10.1.1.1 (local)

Protocol: pim-sm, Flag: WC

UpTime: 00:15:04

Upstream interface: Register

Upstream neighbor: NULL

RPF prime neighbor: NULL

Downstream interface(s) information:

Total number of downstreams: 1

1: Vlan-interface100

Protocol: igmp, UpTime: 00:15:04, Expires: -

(10.110.5.100, 225.1.1.1)

RP: 10.1.1.1 (local)

Protocol: pim-sm, Flag: SPT 2MSDP ACT

UpTime: 00:46:28

Upstream interface: Vlan-interface103

Upstream neighbor: 10.110.2.2

RPF prime neighbor: 10.110.2.2

Downstream interface(s) information:

Total number of downstreams: 1

1: Vlan-interface100

Protocol: pim-sm, UpTime: - , Expires: -

出力結果から、スイッチBがソース1とホストAのRP(リライティングプロバイダ)として動作していることがわかります。

ホストAからIGMP離脱メッセージを送信して、マルチキャストグループ225.1.1.1から離脱します。(詳細は省略)

#ホストBからIGMP レポートを送信し、マルチキャストグループ225.1. 1. 1にJoinします(詳細は省略)。

#Source 2からマルチキャストグループ225.1. 1. 1にマルチキャストデータを送信します(詳細は省略)。

#スイッチBのPIMルーティングテーブルを表示します。

[SwitchB] display pim routing-table

スイッチBからは情報が出力されません。

#スイッチDのPIMルーティングテーブルを表示します。

[SwitchD] display pim routing-table

Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.1)

RP: 10.1.1.1 (local)

Protocol: pim-sm, Flag: WC

UpTime: 00:12:07

Upstream interface: Register

Upstream neighbor: NULL RPF

prime neighbor: NULL

Downstream interface(s) information:

Total number of downstreams: 1 1: Vlan-
interface200

Protocol: igmp, UpTime: 00:12:07, Expires: -

(10.110.6.100, 225.1.1.1)

RP: 10.1.1.1 (local)

Protocol: pim-sm, Flag: SPT 2MSDP ACT UpTime:
00:40:22

Upstream interface: Vlan-interface104 Upstream

neighbor: 10.110.4.2

RPF prime neighbor: 10.110.4.2 Downstream

interface(s) information:

Total number of downstreams: 1 1: Vlan-
interface200

Protocol: pim-sm, UpTime: - , Expires: -

この出力は、スイッチDがソース2およびホストBのRPとして動作していることを示しています。

例:SAメッセージフィルタリングの設定

ネットワークの設定

図59に示します。

- OSPFは、PIM-SMDメイン内およびドメイン間で動作し、ユニキャストルーティングを提供します。
- スイッチAとスイッチCの間、およびスイッチCとスイッチDの間にMSDPピアリング関係を設定します。
- 送信元1はマルチキャストグループ225.1.1.0/30および226.1.1.0/30にマルチキャストデータを送信し、送信元2はマルチキャストグループ227.1.1.0/30にマルチキャストデータを送信します。

次のようにSAメッセージポリシーを設定します。

- ホストAおよびホストBは、マルチキャストグループ225.1.1.0/30および226.1.1.0/30宛てのマルチキャストデータだけを受信します。
- ホストCは、マルチキャストグループ226.1.1.0/30および227.1.1.0/30だけを宛先とするマルチキャストデータを受信します。

図59 ネットワークダイアグラム

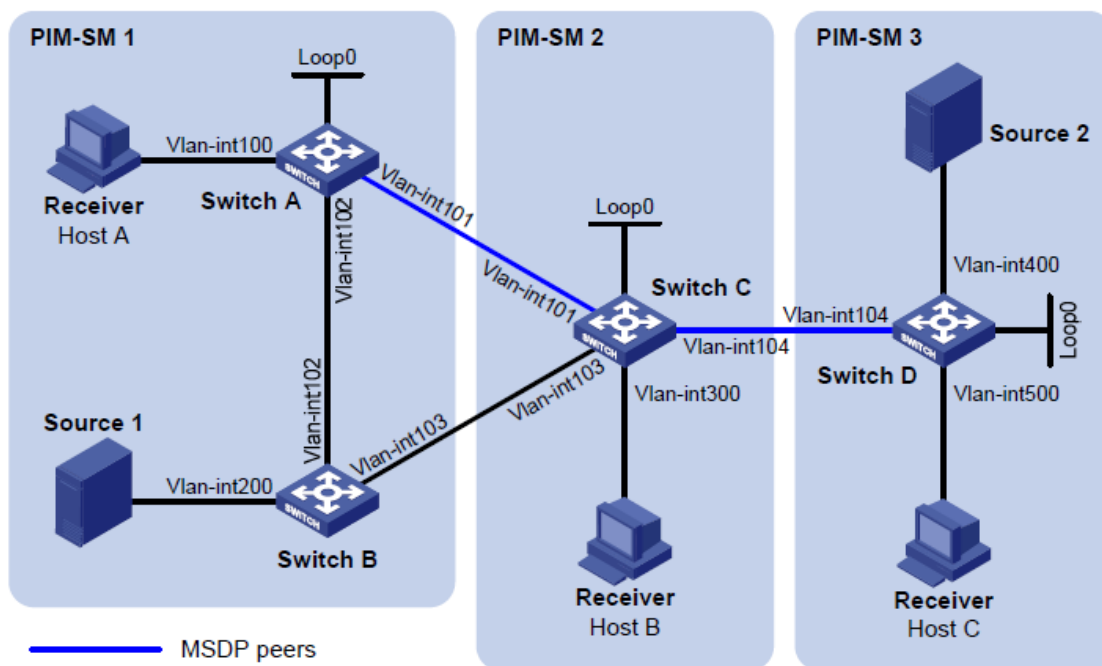


表15インターフェイスとIPアドレスの割り当て

デバイス	インターフェイス	IPアドレス	デバイス	インターフェイス	IPアドレス
Source1	-	10.110.3.100/24	Switch C	Vlan-int300	10.110.4.1/24
Source2	-	10.110.6.100/24	Switch C	Vlan-int104	10.110.5.1/24
Switch A	Vlan-int100	10.110.1.1/24	Switch C	Vlan-int101	192.168.1.2/24
Switch A	Vlan-int102	10.110.2.1/24	Switch C	Vlan-int103	192.168.2.2/24
Switch A	Vlan-int101	192.168.1.1/24	Switch C	Loop0	2.2.2.2/32
Switch A	Loop0	1.1.1.132/	Switch D	Vlan-int400	10.110.6.1/24
Switch B	Vlan-int200	10.110.3.1/24	Switch D	Vlan-int500	10.110.7.1/24
Switch B	Vlan-int102	10.110.2.2/24	Switch D	Vlan-int104	10.110.5.2/24
Switch B	Vlan-int103	192.168.2.1/24	Switch D	Loop0	3.3.3.3/32

手順

1. 図59に示すように、各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
2. PIM-SMドメイン内のスイッチにOSPFを設定します(詳細は省略)。
3. IPマルチキャストルーティング、IGMP、およびPIM-SMを有効にし、PIMドメイン境界を設定します。

#スイッチAで、IPマルチキャストルーティングを有効にします。

```
<SwitchA> system-view
[SwitchA] multicast routing
[SwitchA-mrib] quit
```

#受信側のインターフェイス(VLANインターフェイス100)でIGMPを有効にします。

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] quit
```

#他のインターフェイスでPIM-SMを有効にします。

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim sm
[SwitchA-Vlan-interface102] quit
[SwitchA] interface loopback 0
[SwitchA-LoopBack0] pim sm
[SwitchA-LoopBack0] quit
```

#スイッチAの設定と同じ方法で、スイッチB、スイッチC、およびスイッチDのIPマルチキャストルーティング、IGMP、およびPIM-SMを有効にします(詳細は省略)。

#スイッチCにPIMドメイン境界を設定します。

```
[SwitchC] interface vlan-interface 101
[SwitchC-Vlan-interface101] pim bsr-boundary
```

```
[SwitchC-Vlan-interface101] quit
[SwitchC] interface vlan-interface 103
[SwitchC-Vlan-interface103] pim bsr-boundary
[SwitchC-Vlan-interface103] quit
[SwitchC] interface vlan-interface 104
[SwitchC-Vlan-interface104] pim bsr-boundary
[SwitchC-Vlan-interface104] quit
```

#スイッチA、スイッチB、およびスイッチDのPIMドメイン境界を、スイッチCと同様の方法で設定してください。(詳細は省略)

4. C-BSRおよびC-RPを設定します。

#Loopback 0をスイッチAのC-BSRおよびC-RPとして設定します。

```
[SwitchA] pim
[SwitchA-pim] c-bsr 1.1.1.1
[SwitchA-pim] c-rp 1.1.1.1
[SwitchA-pim] quit
```

#スイッチAと同様に、スイッチCおよびスイッチDでC-BSRおよびC-RPを設定します。

(詳細は省略)。

5. MSDPピアを設定します。

#スイッチAでMSDPピアを設定します。

```
[SwitchA] msdp
[SwitchA-msdp] peer 192.168.1.2 connect-interface vlan-interface 101
[SwitchA-msdp] quit
```

#スイッチCにMSDPピアを設定します。

```
[SwitchC] msdp
[SwitchC-msdp] peer 192.168.1.1 connect-interface vlan-interface 101
[SwitchC-msdp] peer 10.110.5.2 connect-interface vlan-interface 104
[SwitchC-msdp] quit
```

#スイッチDでMSDPピアを設定します。

```
[SwitchD] msdp
[SwitchD-msdp] peer 10.110.5.1 connect-interface vlan-interface 104
[SwitchD-msdp] quit
```

6. SAメッセージポリシーを設定します。

#スイッチCが(Source 1、225.1.1.0/30)のSAメッセージをスイッチDに転送しないように、スイッチCでSAの受け入れおよび転送ポリシーを設定します。

```
[SwitchC] acl advanced 3001
[SwitchC-acl-ipv4-adv-3001] rule deny ip source 10.110.3.100 0 destination 225.1.1.0 0.0.0.3
[SwitchC-acl-ipv4-adv-3001] rule permit ip source any destination any
[SwitchC-acl-ipv4-adv-3001] quit
[SwitchC] msdp
[SwitchC-msdp] peer 10.110.5.2 sa-policy export acl 3001
[SwitchC-msdp] quit
```

#スイッチDでSA作成ポリシーを設定して、スイッチDがSource 2のSAメッセージを作成しないようにします。

```
[SwitchD] acl basic 2001
[SwitchD-acl-ipv4-basic-2001] rule deny source 10.110.6.100 0
[SwitchD-acl-ipv4-basic-2001] quit
[SwitchD] msdp
[SwitchD-msdp] import-source acl 2001
[SwitchD-msdp] quit
```

設定の確認

#スイッチCのSAメッセージキャッシュ内の(S, G)エントリを表示します。

```
[SwitchC] display msdp sa-cache
MSDP Total Source-Active Cache - 8 entries
Matched 8 entries
```

Source	Group	Origin	RP	Pro	AS	Uptime	Expires
10.110.3.100		225.1.1.0	1.1.1.1	?	?	02:03:30	00:05:31
10.110.3.100		225.1.1.1	1.1.1.1	?	?	02:03:30	00:05:31
10.110.3.100		225.1.1.2	1.1.1.1	?	?	02:03:30	00:05:31
10.110.3.100		225.1.1.3	1.1.1.1	?	?	02:03:30	00:05:31
10.110.3.100		226.1.1.0	1.1.1.1	?	?	02:03:30	00:05:31
10.110.3.100		226.1.1.1	1.1.1.1	?	?	02:03:30	00:05:31
10.110.3.100		226.1.1.2	1.1.1.1	?	?	02:03:30	00:05:31
10.110.3.100		226.1.1.3	1.1.1.1	?	?	02:03:30	00:05:31

#スイッチDのSAメッセージキャッシュ内の(S, G)エントリを表示します。

```
[SwitchD] display msdp sa-cache
MSDP Total Source-Active Cache - 4 entries
Matched 4 entries
```

Source	Group	Origin	RP	Pro	AS	Uptime	Expires
10.110.3.100		226.1.1.0	1.1.1.1	?	?	00:32:53	00:05:07
10.110.3.100		226.1.1.1	1.1.1.1	?	?	00:32:53	00:05:07
10.110.3.100		226.1.1.2	1.1.1.1	?	?	00:32:53	00:05:07
10.110.3.100		226.1.1.3	1.1.1.1	?	?	00:32:53	00:05:07

MSDPのトラブルシューティング

ここでは、一般的なMSDPの問題とそのトラブルシューティング方法について説明します。

MSDPピアが無効状態のままになる

症状

設定されたMSDPピアは無効状態のままです。

解決方法

この問題を解決するには、次の手順を実行し

1. **display ip routing-table**コマンドを使用して、デバイス間のユニキャストルートが到達可能であることを確認します。
2. 相互にMSDPピアとなる2つのデバイス間でユニキャストルートが使用できることを確認します。

3. リモートデバイスのローカルインターフェイスアドレスとMSDPピアアドレスが同じであることを確認するには、**display current-configuration**コマンドを使用します。
4. 問題が解決しない場合は、H3Cサポートに連絡してください。

デバイスのSAメッセージキャッシュにSAエントリが存在しない

症状

MSDPは、SAメッセージを介した(S, G)エントリの送信に失敗します。

解決方法

この問題を解決するには、次の手順を実行し

1. **display ip routing-table**コマンドを使用して、デバイス間のユニキャストルートが到達可能であることを確認します。
2. 相互にMSDPピアとなる2つのデバイス間でユニキャストルートが使用できることを確認します。
3. **import-source**コマンドとその *ipv4-acl-number* の設定を確認します。
引数を使用して、ACLルールが適切な(S, G)エントリをフィルタリングするようにします。
4. 問題が解決しない場合は、H3Cサポートに連絡してください。

RP間でローカルに登録された(S, G)エントリの交換なし

症状

RPIは、Anycast RPアプリケーション内のローカルに登録された(S, G)エントリを相互に交換できません。

解決方法

この問題を解決するには、次の手順を実行し

1. **display ip routing-table**コマンドを使用して、デバイス間のユニキャストルートが到達可能であることを確認します。
2. MSDPピアリング関係を確立する2つのデバイス間でユニキャストルートが使用できることを確認します。
3. **originating-rp**コマンドの設定を確認します。エニーキャストRPアプリケーション環境では、**originating-rp**コマンドを使用して、SAメッセージ内のRPアドレスを設定します。このアドレスは、ローカルインターフェイスアドレスである必要があります。
4. C-BSRアドレスがエニーキャストRPアドレスと異なることを確認します。
5. 問題が解決しない場合は、H3Cサポートに連絡してください。

MLDスヌーピングの設定

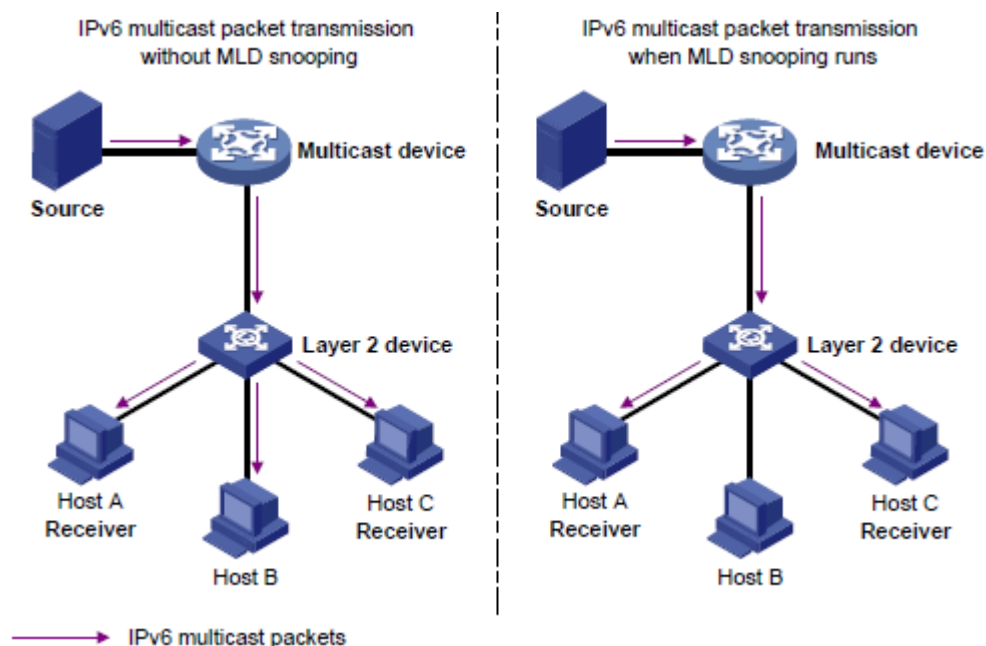
MLDスヌーピングの概要

MLDスヌーピングは、IPv6マルチキャスト抑制メカニズムとしてレイヤ2デバイス上で動作し、マルチキャスト転送効率を向上させます。ホストとレイヤ3デバイス間で交換されるMLDメッセージから、レイヤ2マルチキャスト転送エントリを作成します。

MLDスヌーピングの基礎

図60に示されるように、MLDスヌーピングが有効でない時、レイヤ2スイッチは、VLANまたはVSIのすべてのホストにIPv6マルチキャストパケットをフラッディングします。MLDスヌーピングが有効な時、レイヤ2スイッチは、レシーバのみに既知のIPv6マルチキャストグループのマルチキャストパケットを転送します。

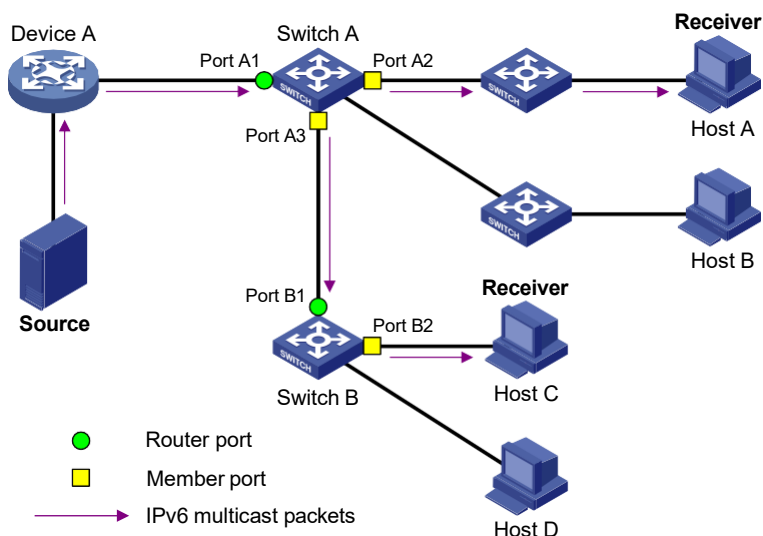
図60 MLDスヌーピングを使用しない場合と使用した場合のマルチキャストパケット送信プロセス



MLDスヌーピングポート

図61に示されるように、MLDスヌーピングはスイッチAとスイッチBで動作し、ホストAとホストCはIPv6マルチキャストグループのレシーバホストです。MLDスヌーピングポートは、メンバーポートとルータポートに分けられます。

図61 MLDスヌーピングポート



ルータポート

MLDスヌーピングレイヤ2デバイスでは、レイヤ3マルチキャストデバイスへのポートはルータポートと呼ばれます。図61では、スイッチAのポートA1とスイッチBのポートB1はルータポートです。

ルータポートには、次のタイプがあります。

- **Dynamic router port:** ポートが送信元アドレスが0::0でないMLD一般クエリーを受信した場合、またはIPv6 PIM helloメッセージを受信した場合、ポートはダイナミックルータポートリストに追加されます。同時に、ポートのエージングタイマーが開始されます。タイマーの期限が切れる前にポートがいずれかのメッセージを受信した場合、タイマーはリセットされます。タイマーの期限が切れたときにポートがいずれのメッセージも受信しなかった場合、ポートはダイナミックルータポートリストから削除されます。
- **Static router port:** ポートがルータポートとしてスタティックに設定されると、スタティックルータポートリストに追加されます。スタティックルータポートは期限切れにならず、手動でのみ削除されます。

MLDスヌーピングの「ルータポート」を、一般に「レイヤ3インターフェイス」として知られる「ルーテッドインターフェイス」と混同しないでください。MLDスヌーピングのルータポートは、レイヤ2インターフェイスです。

メンバーポート

MLDスヌーピングレイヤ2デバイスでは、レシーバホストへのポートは、メンバーポートと呼ばれます。図61では、スイッチAのポートA2とポートA3およびスイッチBのポートB2は、メンバーポートです。

メンバーポートには、次のタイプがあります。

- Dynamic member port:** ポートがMLDレポートを受信すると、関連付けられたダイナミックMLDスヌーピング転送エントリに発信インターフェイスとして追加されます。同時に、ポートのエージングタイマーが開始されます。タイマーの期限が切れる前にポートがMLDレポートを受信した場合、タ

イマーはリセットされます。タイマーの期限が切れたときにポートがMLDレポートを受信しなかった場合、ポートは関連付けられたダイナミックフォワーディングエントリから削除されます。

- **Static member port:** ポートがメンバーポートとしてスタティックに設定されている場合、関連付けられたスタティックMLDスヌーピング転送エントリに発信インターフェイスとして追加されます。スタティックメンバーポートは期限切れにならず、手動でのみ削除できます。

特に指定のない限り、このマニュアルのルータポートおよびメンバーポートには、スタティックルータポートとダイナミックルータポートの両方が含まれます。

MLDスヌーピングの動作

このセクションのポートは、ダイナミックポートです。スタティックポートの設定および削除の方法については、「スタティックメンバーポートの設定」および「スタティックルータポートの設定」を参照してください。

MLDメッセージには、一般クエリー、MLDレポート、およびDoneメッセージが含まれます。MLDスヌーピングが有効になっているレイヤ2デバイスの動作は、MLDメッセージタイプによって異なります。

一般的なクエリー

MLDクエリーは、ローカルサブネット上のすべてのホストおよびデバイスにMLD一般クエリーを定期的に変送して、IPv6マルチキャストグループメンバーの存在を確認します。

MLD一般クエリーを受信した後、レイヤ2デバイスは受信ポートを除くVLANまたはVSIのすべてのポートにクエリーを転送します。また、レイヤ2デバイスは次のいずれかのアクションを実行します。

- 受信ポートがダイナミックルータポートリスト内のダイナミックルータポートである場合、レイヤ2デバイスはルータポートのエージングタイマーを再起動します。
- 受信ポートがダイナミックルータポートリストに存在しない場合、レイヤ2デバイはそのポートをダイナミックルータポートリストに追加します。また、ポートのエージングタイマーを開始します。

MLDレポート

ホストは、次の目的でMLDレポートをMLDクエリーに送信します。

- ホストがIPv6マルチキャストグループメンバーである場合、クエリーに応答します。
- IPv6マルチキャストグループメンバーシップを申請します。

ホストからMLDレポートを受信した後、レイヤ2デバイスはVLANまたはVSIのすべてのルータポートを介してレポートを転送します。また、レポートされたIPv6マルチキャストグループのIPv6アドレスを解決し、次のように転送テーブルで一致するエントリを検索します。

- 一致するものが見つからない場合、レイヤ2デバイスは受信ポートを発信インターフェイスとして、グループのフォワーディングエントリを作成します。また、受信ポートをダイナミックメンバーポートとしてマークし、ポートのエージングタイマーを開始します。
- 一致が見つかったが、一致するフォワーディングエントリに受信ポートが含まれていない場合、レイヤ2デバイスは受信ポートを発信インターフェイスリストに追加します。また、ポートをフォワーディングエントリのダイナミックメンバーポートとしてマークし、ポートのエージングタイマーを開始します。

- 一致が検出され、一致するフォワーディングエントリに受信ポートが含まれている場合、レイヤ2 デバイスはそのポートのエージングタイマーを再開します。

注:

レイヤ 2 デバイスは、ホストの MLD レポート抑制メカニズムにより、非ルータ ポートを介して MLD レポートを転送しません。非ルータ ポートにメンバー ホストが接続されている場合、メンバー ホストは、非ルータ ポートから転送された MLD レポートを受信すると、自身の MLD レポートを抑制します。レイヤ 2 デバイスは、非ルータ ポートに接続されているメンバー ホストの存在を知ることができません。MLD レポート抑制メカニズムの詳細については、「MLD の設定」を参照してください。

完了メッセージ

ホストがIPv6マルチキャストグループから脱退する場合、ホストはレイヤ3デバイスにMLD Doneメッセージを送信します。レイヤ2デバイスがダイナミックメンバーポートでMLD Doneメッセージを受信すると、レイヤ2デバイスはまず、転送エントリがメッセージ内のIPv6マルチキャストグループアドレスと一致するかどうかを調べます。

- 一致が見つからない場合、レイヤ2デバイスはMLD doneメッセージを破棄します。
 - 一致が検出されても、受信ポートが転送エントリ内の発信インターフェイスでない場合、レイヤ2デバイスはMLD doneメッセージを廃棄します。
 - 一致が検出され、受信ポートが転送エントリ内の唯一の発信インターフェイスではない場合、レイヤ2デバイスは次のアクションを実行します。
 - MLD doneメッセージを廃棄します。
 - MLDマルチキャストアドレス固有クエリーを送信して、受信ポートに接続されたアクティブなリスナーがグループにあるかどうかを確認します。
 - 受信ポートのエージングタイマーを、MLD最終リスナークエリーインターバルの2倍に設定します。
 - 一致が検出され、受信ポートが転送エントリ内の唯一の発信インターフェイスである場合、レイヤ2デバイスは次の処理を実行します。
 - MLD doneメッセージをVLANまたはVSI内のすべてのルータポートに転送します。
 - MLDマルチキャストアドレス固有クエリーを送信して、受信ポートに接続されたアクティブなリスナーがグループにあるかどうかを確認します。
 - 受信ポートのエージングタイマーを、MLD最終リスナークエリーインターバルの2倍に設定します。
- ポートでMLD doneメッセージを受信すると、MLDクエリーはメッセージ内のIPv6マルチキャストグループアドレスを解決します。次に、MLDマルチキャストアドレス固有のクエリーを、受信ポートを介してIPv6マルチキャストグループに送信します。

MLDマルチキャストアドレス固有クエリーを受信した後、レイヤ2デバイスは、VLANまたはVSI内のグループのすべてのルータポートおよびメンバーポートを介してクエリーを転送します。次に、直接接続されたホストからの応答MLDレポートを待ちます。Doneメッセージを受信したダイ

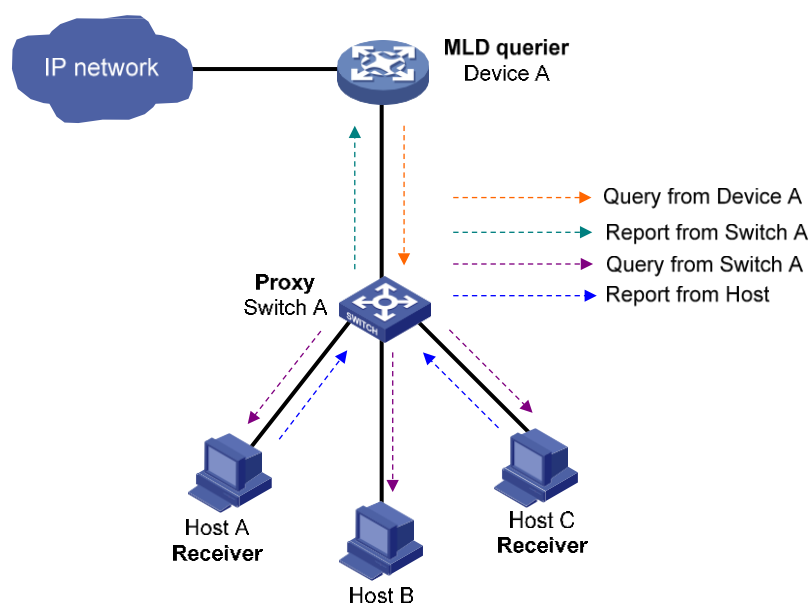
ナミックメンバーポートに対して、レイヤ2デバイスは次のいずれかのアクションも実行します。

- エージングタイマーが満了する前にポートがMLDレポートを受信した場合、レイヤ2デバイスは、ポートのエージングタイマーをリセットします。
- エージングタイマーが満了したときにポートがMLDレポートメッセージを受信しなかった場合、レイヤ2デバイスはIPv6マルチキャストグループのフォワーディングエントリからポートを削除します。

MLDスヌーピングプロキシ

図62に示されるように、上流のデバイスによって受信されるMLDレポートおよびDoneメッセージの数を減らすために、エッジデバイス上でMLDスヌーピングプロキシングを有効にすることができます。MLDスヌーピングプロキシングが有効な状態で、エッジデバイスは上流のMLDスヌーピングクエリアのホストとして動作し、MLDレポートおよびDoneメッセージをデバイスAに送信します。エッジデバイス上のホストMLDレポート抑制メカニズムは、有効ではありません。MLDレポート抑制メカニズムの詳細については、「MLDの設定」を参照してください。

図62 MLDスヌーピングプロキシ



MLDスヌーピングプロキシデバイスは、さまざまなMLDメッセージを次のように処理します。

- General query.
MLD一般クエリーを受信した後、デバイスは受信ポートを除くVLAN内のすべてのポートにクエリーを転送します。デバイスはまた、ローカルメンバーシップ情報に基づいてMLDレポートを生成し、レポートをすべてのルータポートに送信します。
- multicast-address-specific queryまたはmulticast-address-and-source-specific query。
MLDマルチキャストアドレス固有のクエリーを受信した後、または
multicast-address-and-source-specific queryを使用すると、デバイスは受信ポートを除く

VLAN内のすべてのポートにクエリーを転送します。転送エントリにメンバーポートがある場合、デバイスはVLAN内のすべてのルータポートに応答を送信します。

- Report

ホストからMLDレポートを受信した後、デバイスは次のようにフォワーディングテーブルで一致するエントリを検索します。

- 一致が検出され、一致するフォワーディングエントリに受信ポートが含まれている場合、デバイスはそのポートのエージングタイマーをリセットします。
- 一致するものが見つかったも、一致するフォワーディングエントリに受信ポートが含まれていない場合、デバイスは受信ポートを発信インターフェイスリストに追加します。また、受信ポートをダイナミックメンバーポートとしてマークし、ポートのエージングタイマーを開始します。
- 一致するものが見つからない場合、デバイスは受信ポートを発信インターフェイスとする転送エントリを作成します。また、受信ポートをダイナミックメンバーポートとしてマークし、ポートのエージングタイマーを開始します。次に、レポートをすべてのルータポートに送信します。

- Done message

ポートでMLD doneメッセージを受信した後、デバイスはMLDを送信します。

受信ポートを経由するマルチキャストアドレス固有のクエリー。最後のメンバーポートが転送エントリから削除された場合に限り、デバイスはすべてのルータポートにMLD doneメッセージを送信します。

プロトコルと標準

RFC 4541『Considerations for Internet Group Management Protocol(IGMP)and Multicast Listener Discovery(MLD)Snooping Switch es』

制約事項および注意事項:MLDスヌーピング設定

セカンダリVLANから受信したMLDレポートの場合、関連するMLDスヌーピング転送エントリはプライマリVLANによって維持されます。したがって、プライマリVLANに対してだけMLDスヌーピングを有効にする必要があります。セカンダリVLANで行った設定は有効になりません。プライマリVLANおよびセカンダリVLANの詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

レイヤ2集約インターフェイスで行われたMLDスヌーピング設定は、メンバーポートで行われた設定と干渉しません。また、レイヤ2集約インターフェイスで行われた設定は、集約計算には関与しません。集約グループのメンバーポートで行われた設定は、ポートが集約グループから脱退した後有効になります。

一部の機能は、VLANビュー内の1つのVLAN、またはMLDスヌーピングビュー内の複数のVLANに対して設定できます。VLAN固有の設定とMLDスヌーピングビュー内の設定は同じプライオリティを持ち、最新の設定が有効になります。

一部の機能は、VLANビュー内のVLANに対して、またはMLDスヌーピングビュー内のすべてのVLANに

対してグローバルに設定できます。VLAN固有の設定は、グローバル設定よりも優先されます。

一部の機能は、VSIビューでVSIに対して設定するか、MLDスヌーピングビューですべてのVSIに対してグローバルに設定できます。VSI固有の設定は、グローバル設定よりも優先されます。

一部の機能は、インターフェイスビューで特定のインターフェイスに対して設定することも、MLDスヌーピングビューで指定されたVLANのすべてのインターフェイスに対して設定することもできます。インターフェイス固有の設定は、MLDスヌーピングビューでの設定よりも優先されます。

VLANベースのMLDスヌーピングタスクの概要

VLANのMLDスヌーピングを設定するには、次の作業を実行します。

1. MLDスヌーピング機能の有効化
2. MLDスヌーピングの有効化
必要に応じて、次のタスクを選択します。
 - MLDスヌーピングのグローバルな有効化
 - VLANのMLDスヌーピングの有効化
3. (任意)基本的なMLDスヌーピング機能の設定
 - MLDスヌーピングバージョンの指定
 - MLDスヌーピングフォワーディングエントリの最大数の設定
 - スタティックIPv6マルチキャストMACアドレスエントリの設定
 - MLD最終リスナークエリインターバルの設定
4. (任意)MLDスヌーピングポート機能の設定
 - ダイナミックポートのエージングタイマーの設定
 - スタティックメンバーポートの設定
 - スタティックルータポートの設定
 - シミュレートメンバーホストとしてのポートの構成
 - 高速脱退処理の有効化
 - ポートがダイナミックルータポートになることを無効にする
5. (任意)MLDスヌーピングクエリアの設定
 - MLDスヌーピングクエリアの有効化
 - MLDスヌーピングクエリア選択の有効化
 - MLD一般クエリおよび応答のパラメータの設定
6. (任意)MLDスヌーピングプロキシの有効化
7. (任意)MLDメッセージのパラメータの設定
 - MLDメッセージの送信元IPv6アドレスの設定
 - MLDメッセージの802.1pプライオリティの設定
8. (任意)MLDスヌーピングポリシーの設定

- IPv6マルチキャストグループポリシーの設定
 - IPv6マルチキャスト送信元ポートフィルタリングの有効化
 - 不明なIPv6マルチキャストデータの破棄の有効化
 - MLDレポート抑制の有効化
 - ポート上の最大IPv6マルチキャストグループ数の設定
 - IPv6マルチキャストグループ置換の有効化
 - ホストトラッキングの有効化
9. (任意)発信MLDスヌーピングプロトコルパケットのDSCP値の設定

VSIベースのMLDスヌーピングタスクの概要

VSIにMLDスヌーピングを設定するには、次の作業を実行します。

1. MLDスヌーピング機能の有効化
2. MLDスヌーピングの有効化
必要に応じて、次のタスクを選択します。
 - MLDスヌーピングのグローバルな有効化
 - VSIのMLDスヌーピングの有効化
3. (任意)基本的なMLDスヌーピング機能の設定
 - MLDスヌーピングバージョンの指定
 - MLDスヌーピングフォワーディングエントリの最大数の設定
 - MLD最終リスナークエリーインターバルの設定
4. (任意)ダイナミックポートのエージングタイマーの設定
5. (任意)MLDスヌーピングクエリーアの設定
 - MLDスヌーピングクエリーアの有効化
 - MLDスヌーピングクエリーア選択の有効化
 - MLD一般クエリーおよび応答のパラメータの設定
6. (任意)MLDメッセージのパラメータの設定
 - MLDメッセージの送信元IPv6アドレスの設定
 - MLDメッセージの802.1pプライオリティの設定
7. (任意)MLDスヌーピングポリシーの設定
 - 不明なIPv6マルチキャストデータの破棄の有効化
 - MLDレポート抑制の有効化
8. (任意)発信MLDスヌーピングプロトコルパケットのDSCP値の設定

MLDスヌーピング機能の有効化

MLDスヌーピング機能の有効化について

他のMLDスヌーピング機能を設定する前に、MLDスヌーピング機能を有効にする必要があります。

手順

1. システムビューに入ります。

system-view

2. MLDスヌーピング機能を有効にし、MLDスヌーピングビューを開始します。

mld-snooping

デフォルトでは、MLDスヌーピング機能は無効です。

MLDスヌーピングの有効化

MLDスヌーピングのグローバルな有効化

MLDスヌーピングのグローバルな有効化について

MLDスヌーピングをグローバルに有効にすると、すべてのVLANまたはVSIでMLDスヌーピングが有効になります。MLDスヌーピングがグローバルに有効の場合、VLANまたはVSIのMLDスヌーピングを無効にできません。

制約事項とガイドライン

VLANまたはVSIに対して他のMLDスヌーピング機能を設定するには、MLDスヌーピングがグローバルに有効であっても、特定のVLANまたはVSIに対してMLDスヌーピングを有効にする必要があります。

VLAN固有またはVSI固有のMLDスヌーピング設定は、グローバルなMLDスヌーピング設定よりも優先されます。たとえば、MLDスヌーピングをグローバルに有効にしてから、**mld-snooping disable**コマンドを使用してVLANのMLDスヌーピングを無効にすると、VLANのMLDスヌーピングは無効になります。

手順

1. システムビューに入ります。

system-view

2. MLDスヌーピングビューを入力します。

mld-snooping

3. MLDスヌーピングをグローバルに有効にします。

global-enable

デフォルトでは、MLDスヌーピングはグローバルに無効です。

4. (任意)VLANまたはVSIのMLDスヌーピングを無効にします。

- a. システムビューに戻ります。

quit

- b. VLANまたはVSIビューを入力します。

vlan *vlan-id*

vsi *vsi-name*

- c. VLANまたはVSIのMLDスヌーピングを無効にします。

mld-snooping disable

デフォルトでは、VLANまたはVSIのMLDスヌーピングステータスは、グローバルMLDスヌーピングステータスと一致します。

VLANのMLDスヌーピングの有効化

制約事項とガイドライン

MLDスヌーピングビューで**enable vlan**コマンドを使用して複数のVLANに対してMLDスヌーピングを有効にするか、VLANビューで**mld-snooping enable**コマンドを使用してVLANに対してMLDスヌーピングを有効にすることができます。VLANビューの設定は、MLDスヌーピングビューの設定と同じプライオリティを持ちます。

VLANのMLDスヌーピング設定は、VLANのメンバーポートだけで有効になります。

複数VLANのMLDスヌーピングの有効化

1. システムビューに入ります。

system-view

2. MLDスヌーピングビューを入力します。

mld-snooping

3. 複数のVLANに対してMLDスヌーピングを有効にします。

enable vlan *vlan-list*

デフォルトでは、VLANのMLDスヌーピングステータスは、グローバルMLDスヌーピングステータスと一致します。

VLANのMLDスヌーピングの有効化

1. システムビューに入ります。

system-view

2. VLANビューを開始します。

vlan *vlan-id*

3. VLANのMLDスヌーピングを有効にします。

mld-snooping enable

デフォルトでは、VLANのMLDスヌーピングステータスは、グローバルMLDスヌーピングステータスと一致します。

VSIのMLDスヌーピングの有効化

制約事項とガイドライン

VSIの場合、VSIビューでmld-snooping enableコマンドを使用することによってのみ、VSIのMLDスヌーピングを有効にできます。

VSIのMLDスヌーピング設定は、VSIのメンバーポートでのみ有効です。

手順

1. システムビューに入ります。

system-view

2. VSIビューを入力します。

vsi *vsi-name*

3. VSIのMLDスヌーピングを有効にします。

mld-snooping enable

デフォルトでは、VSIのMLDスヌーピングステータスは、グローバルMLDスヌーピングステータスと一致します。

基本的なMLDスヌーピング機能の設定

MLDスヌーピングバージョンの指定

MLDスヌーピングバージョンについて

MLDスヌーピングのバージョンが異なると、処理できるMLDメッセージのバージョンも異なります。

- MLDv1スヌーピングはMLDv1メッセージおよびMLDv2クエリーを処理できますが、VLANまたはVSI内のMLDv2レポートを処理せずにフラッディングします。
- MLDv2スヌーピングは、MLDv1およびMLDv2メッセージを処理できます。

制約事項とガイドライン

MLDスヌーピングのバージョンを2から1に変更する場合、システムは次のアクションを実行します。

- ダイナミックに作成されたすべてのMLDスヌーピング転送エントリをクリアします。
- スタティックMLDv2スヌーピング転送エントリ(*,G)を保持します。
- スタティックMLDv2スヌーピング転送エントリ(S, G)をクリアします。これは、MLDスヌーピングがMLDv2スヌーピングにスイッチバックされたときに復元されます。

スタティックMLDスヌーピングフォワーディングエントリの詳細については、「スタティックメンバーポートの設定」を参照してください。

複数のVLANに対するMLDスヌーピングバージョンの指定

1. システムビューに入ります。

system-view

2. MLDスヌーピングビューを入力します。

mld-snooping

3. 複数のVLANに対してMLDスヌーピングバージョンを指定します。

```
version version-number vlan vlan-list
```

デフォルトでは、VLANのMLDスヌーピングバージョンは1です。

VLANのMLDスヌーピングバージョンの指定

1. システムビューに入ります。

```
system-view
```

2. VLANビューを開始します。

```
vlan vlan-id
```

3. VLANのMLDスヌーピングバージョンを指定します。

```
mld-snooping version version-number
```

デフォルトでは、VLANのMLDスヌーピングバージョンは1です。

VSIのMLDスヌーピングバージョンの指定

1. システムビューに入ります。

```
system-view
```

2. VSIビューを入力します。

```
vsi vsi-name
```

3. VSIのMLDスヌーピングバージョンを指定します。

```
mld-snooping version version-number
```

デフォルトでは、VSIのMLDスヌーピングバージョンは1です。

MLDスヌーピングフォワーディングエントリの最大数の設定

MLDスヌーピングフォワーディングエントリの最大数の設定について

ダイナミックエントリおよびスタティックエントリを含む、MLDスヌーピングフォワーディングエントリの最大数を変更できます。デバイス上のフォワーディングエントリの数が増え、上限に達すると、デバイスは既存のエントリを自動的に削除しません。新しいエントリを作成できるようにするには、一部のエントリを手動で削除します。

手順

1. システムビューに入ります。

```
system-view
```

2. MLDスヌーピングビューを入力します。

```
mld-snooping
```

3. MLDスヌーピングフォワーディングエントリの最大数を設定します。

```
entry-limit limit
```

デフォルトでは、MLDスヌーピングフォワーディングエントリの最大数は4294967295です。

スタティックIPv6マルチキャストMACアドレスエントリの設定

スタティックIPv6マルチキャストMACアドレスエントリについて

レイヤ2 IPv6マルチキャストでは、IPv6マルチキャストMACアドレスエントリは、レイヤ2マルチキャストプロトコル(MLDスヌーピングなど)を介してダイナミックに作成できます。また、IPv6マルチキャストMACアドレスおよびポートをバインドしてIPv6マルチキャストデータの宛先ポートを制御することにより、スタティックIPv6マルチキャストMACアドレスエントリを手動で設定することもできます。

制約事項とガイドライン

スタティックIPv6マルチキャストMACアドレスエントリを設定する場合は、未使用のマルチキャストMACアドレスを指定する必要があります。マルチキャストMACアドレスは、最上位オクテットの最下位ビットが1であるMACアドレスです。

システムビューでのスタティックIPv6マルチキャストMACアドレスエントリの設定

1. システムビューに入ります。

system-view

スタティックIPv6マルチキャストMACアドレスエントリを設定します。

```
mac-address multicast mac-address interface interface-list vlan  
vlan-id
```

インターフェイスビューでのスタティックIPv6マルチキャストMACアドレスエントリの設定

1. システムビューに入ります。

system-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

```
interface interface-type interface-number
```

- レイヤ2集約インターフェイスビューを開始します。

```
interface bridge-aggregation interface-number
```

3. スタティックIPv6マルチキャストMACアドレスエントリを設定します。

```
mac-address multicast mac-address vlan vlan-id
```

MLD最終リスナー クエリー インターバルの設定

MLD最終リスナークエリーインターバルについて

レシーバホストは、グループのMLDマルチキャストアドレス固有のクエリーを受信すると、IPv6マルチキャストグループのレポート遅延タイマーを開始します。このタイマーは、0からクエリーでアドバタイズされる最大応答時間までの範囲のランダム値に設定されます。タイマー値が0に減少すると、ホストはグループにMLDレポートを送信します。

MLD Last Listener Query Intervalは、MLDマルチキャストアドレス固有のクエリーでアドバタイズされる最大応答時間を定義します。MLD Multicast-address-specificクエリーに対するホストの応答を高速化し、MLDレポートトラフィックバーストを回避するには、MLD Last Listener Query Intervalに適切な値を設定します。

MLD最終リスナークエリー間隔のグローバルな設定

1. システムビューに入ります。
system-view
2. MLDスヌーピングビューを入力します。
mld-snooping
3. MLD最終リスナークエリー間隔をグローバルに設定します。
last-listener-query-interval interval
デフォルトでは、MLD最終リスナークエリー間隔は1秒です。

VLANのMLD最終リスナークエリー間隔の設定

1. システムビューに入ります。
system-view
2. VLANビューを開始します。
vlan vlan-id
3. VLANのMLD最終リスナークエリー間隔を設定します。
mld-snooping last-listener-query-interval interval
デフォルトでは、VLANのMLD最終リスナークエリー間隔は1秒です。

VSIのMLD最終リスナークエリー間隔の設定

1. システムビューに入ります。
system-view
2. VSIビューを入力します。
vsi vsi-name
3. VSIのMLD最終リスナークエリー間隔を設定します。
mld-snooping last-listener-query-interval interval
デフォルトでは、VSIのMLD最終リスナークエリー間隔は1秒です。

MLDスヌーピングポート機能の設定

ダイナミックポートのエージングタイマーの設定

ダイナミックポートのエージングタイマーについて

ダイナミックルータポートは、エージングタイマーが満了したときにMLD一般クエリーまたはIPv6 PIM helloメッセージを受信しなかった場合、ダイナミックルータポートリストから削除されます。

ダイナミックメンバーポートは、エージングタイマーが満了したときにMLDレポートを受信しなかった場合、ダイナミックメンバーポートから削除されます。

制約事項とガイドライン

実際のネットワーク要件に基づいて、ダイナミックポートのエージングタイマーに適切な値を設定します。
たとえば、IPv6マルチキャストグループのメンバーシップが頻繁に変更される場合は、ダイナミックメンバ

ーポートのエージングタイマーに比較的小さい値を設定します。

ダイナミックルータポートがIPv6 PIMv2 helloメッセージを受信した場合、ポートのエージングタイマーはhelloメッセージによって指定されます。この場合、`mld-snooping router-aging-time`コマンドはポート上で有効になりません。

レイヤ2デバイスによって生成されたMLDマルチキャストアドレス固有のクエリーは、ダイナミックメンバーポートのエージングタイマーの調整をトリガーします。ダイナミックメンバーポートがこのようなクエリーを受信した場合、エージングタイマーはMLD最終リスナークエリーインターバルの2倍に設定されます。レイヤ2デバイス上でのMLD最終リスナークエリーインターバルの設定についての詳細は、「MLD最終リスナークエリーインターバルの設定」を参照してください。

ダイナミックポートのエージングタイマーのグローバルな設定

1. システムビューに入ります。

system-view

2. MLDスヌーピングビューを入力します。

mld-snooping

3. ダイナミックルータポートのエージングタイマーをグローバルに設定します。

router-aging-time *seconds*

デフォルトでは、ダイナミックルータポートのエージングタイマーは260秒です。

4. ダイナミックメンバーポートのエージングタイマーをグローバルに設定します。

host-aging-time *seconds*

デフォルトでは、ダイナミックメンバーポートのエージングタイマーは260秒です。

VLANにおけるダイナミックポートのためのエージングタイマーの設定

1. システムビューに入ります。

system-view

2. VLANビューを開始します。

vlan *vlan-id*

3. VLAN内のダイナミックルータポートのエージングタイマーを設定します。

mld-snooping router-aging-time *seconds*

デフォルトでは、VLANのダイナミックルータポートのエージングタイマーは260秒です。

4. VLAN内のダイナミックメンバーポートのエージングタイマーを設定します。

mld-snooping host-aging-time *seconds*

デフォルトでは、VLANのダイナミックメンバーポートのエージングタイマーは260秒です。

VSIでのダイナミックポートのエージングタイマーの設定

1. システムビューに入ります。

system-view

2. VSIビューを入力します。

vsi *vsi-name*

3. VSIでダイナミックルータポートのエージングタイマーを設定します。

```
mld-snooping router-aging-time seconds
```

デフォルトでは、VSIのダイナミックルータポートのエージングタイマーは260秒です。

4. VSIのダイナミックメンバーポートのエージングタイマーを設定します。

```
mld-snooping host-aging-time seconds
```

デフォルトでは、VSIのダイナミックメンバーポートのエージングタイマーは260秒です。

スタティックメンバーポートの設定

スタティックメンバーポートについて

ポートに接続されたすべてのホストが常にグループのIPv6マルチキャストデータを受信できるように、ポートをIPv6マルチキャストグループのスタティックメンバーポートとして設定できます。スタティックメンバーポートはMLDクエリーに応答しません。この設定を完了またはキャンセルすると、ポートは非送信請求レポートまたはDoneメッセージを送信しなくなります。

手順

1. システムビューに入ります。

```
system-view
```

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

```
interface interface-type interface-number
```

- レイヤ2集約インターフェイスビューを開始します。

```
interface bridge-aggregation interface-number
```

3. ポートをスタティックメンバーポートとして設定します。

```
mld-snooping static-group ipv6-group-address [ source-ip ipv6-source-address ] vlan vlan-id
```

デフォルトでは、ポートはスタティックメンバーポートではありません。

スタティックルータポートの設定

スタティックルータポートについて

ポートで受信したグループのすべてのIPv6マルチキャストデータが転送されるように、ポートをIPv6マルチキャストグループのスタティックルータポートとして設定できます。

手順

1. システムビューに入ります。

```
system-view
```

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

```
interface interface-type interface-number
```

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation interface-number

3. ポートをスタティックルータポートとして設定します。

mld-snooping static-router-port vlan vlan-id

デフォルトでは、ポートはスタティックルータポートではありません。

シミュレートメンバーホストとしてのポートの構成

シミュレートされたメンバーホストについて

ポートをシミュレートメンバーホストとして設定すると、次の点で独立ホストと同等になります。

- 設定が完了すると、非送信請求MLDレポートが送信されます。
- MLD一般クエリーには、MLDレポートで応答します。
- 設定を削除すると、MLD doneメッセージが送信されます。

シミュレートされたメンバーホスト上で動作するMLDのバージョンは、ポート上で動作するMLDスヌーピングのバージョンと同じです。ポートは、ダイナミックメンバーポートと同じ方法で期限切れになります。

手順

1. システムビューに入ります。

system-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface interface-type interface-number

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation interface-number

3. ポートをシミュレートメンバーホストとして設定します。

mld-snooping host-join ipv6-group-address [source-ip ipv6-source-address] vlan vlan-id

デフォルトでは、ポートはシミュレートされるメンバーホストではありません。

高速脱退処理の有効化

高速脱退処理について

この機能により、ポートがdoneメッセージを受信した場合、レイヤ2デバイスはIPv6マルチキャストグループのフォワーディングエントリからポートを即座に削除することができます。デバイスは、グループのMLDマルチキャストアドレス固有のクエリーをポートに送信または転送しなくなります。

制約事項とガイドライン

1つのVLANに複数のレシーバホストが接続されているポートでは、高速脱退処理を有効にしないでください。この場合、レシーバがグループを脱退すると、残りのレシーバはグループのIPv6マルチキャストデータを受信できなくなります。

高速脱退処理のグローバルな有効化

1. システムビューに入ります。

system-view

2. MLDスヌーピングビューを入力します。

mld-snooping

3. 高速脱退処理をグローバルに有効にします。

fast-leave [vlan vlan-list]

デフォルトでは、高速脱退処理はグローバルに無効です。

ポート上での高速脱退処理の有効化

1. システムビューに入ります。

system-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface interface-type interface-number

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation interface-number

3. ポート上で高速脱退処理を有効にします。

mld-snooping fast-leave [vlan vlan-list]

デフォルトでは、高速脱退処理はポート上で無効です。

ポートがダイナミックルータポートになることを無効にする

ポートがダイナミックルータポートになることを無効にする方法

レシーバホストは、テスト目的でMLD一般クエリーまたはIPv6 PIM helloメッセージを送信する場合があります。レイヤ2デバイスでは、いずれかのメッセージを受信するポートはダイナミックルータポートになります。ポートのエージングタイマーが期限切れになる前に、次の問題が発生する可能性があります。

- ポートが属するVLANのすべてのIPv6マルチキャストデータは、ポートに送信されます。その後、ポートは接続されたレシーバホストにデータを転送します。レシーバホストは、予期しないIPv6マルチキャストデータを受信します。
- ポートは、MLD一般クエリーまたはIPv6 PIMハローメッセージを上流のレイヤ3デバイスに転送します。これらのメッセージは、レイヤ3デバイス上のマルチキャストルーティングプロトコルの状態(MLDクエリーアまたはDR選定など)に影響を与える可能性があります。これにより、ネットワークがさらに中断される可能性があります。

これらの問題を解決するには、いずれかのメッセージを受信したときにポートがダイナミックルータポートにならないようにします。これにより、ネットワークのセキュリティと受信側ホストの制御も向上します。

制約事項とガイドライン

この設定とスタティックルータポート設定は、相互に干渉しません。

手順

1. システムビューに入ります。

system-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface interface-type interface-number

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation interface-number

3. ポートがダイナミックルータポートになることを無効にします。

mld-snooping router-port-deny [vlan vlan-list]

デフォルトでは、ポートはダイナミックルータポートになることができます。

MLDスヌーピングクエリアの設定

MLDスヌーピングクエリアの有効化

MLDスヌーピングクエリアの概要

この機能により、レイヤ2デバイスは定期的にMLD一般クエリーを送信して、データリンクレイヤでマルチキャスト転送エントリを確立および維持できます。レイヤ3マルチキャストデバイスのないネットワーク上でMLDスヌーピングクエリアを設定できます。

制約事項とガイドライン

MLDを実行するIPv6マルチキャストネットワークでは、MLDスヌーピングクエリアを有効にしないでください。MLDスヌーピングクエリアは、MLDクエリアの選定には参加しません。ただし、低い送信元IPv6アドレスでMLD一般クエリーを送信する場合は、MLDクエリアの選定に影響を与える可能性があります。MLDクエリーの詳細については、「MLDの設定」を参照してください。

VXLANネットワークでは、VSIのMLDスヌーピングクエリアは、MLD一般クエリーにVLANタグを含めません。ベストプラクティスとして、VSIがイーサネットアクセスモードを使用する場合は、VSIのMLDスヌーピングクエリアを有効にしないでください。イーサネットアクセスモードの詳細については、『VXLAN Configuration Guide』を参照してください。

VLANのMLDスヌーピングクエリアの有効化

1. システムビューに入ります。

system-view

2. VLANビューを開始します。

vlan vlan-id

3. VLANのMLDスヌーピングクエリーアを有効にします。

mld-snooping querier

デフォルトでは、VLANのMLDスヌーピングクエリーアは無効です。

VSIのMLDスヌーピングクエリーアの有効化

1. システムビューに入ります。

system-view

2. VSIビューを入力します。

vsi *vsi-name*

3. VSIのMLDスヌーピングクエリーアを有効にします。

mld-snooping querier

デフォルトでは、VSIのMLDスヌーピングクエリーアは無効です。

MLDスヌーピングクエリーア選択の有効化

MLDスヌーピングクエリーア選定の概要

VLANまたはVSI内の単一クエリーアの障害によるトラフィックの中断を回避するには、VLANまたはVSI内に複数のクエリーアを設定し、クエリーアの選定を有効にします。選定されたクエリーアに障害が発生すると、デバイスは新しいクエリーアの選定を開始して、マルチキャスト転送を保証します。MLDスヌーピングクエリーアの選定メカニズムは、MLDクエリーアの選定メカニズムと同じです。MLDクエリーアの選定の詳細については、「MLDの設定」を参照してください。

必要条件

MLDスヌーピングクエリーア選択を有効にする前に、次の作業を実行する必要があります。

- VLANまたはVSIのMLDスヌーピングクエリーアを有効にします。MLDスヌーピングクエリーアの有効化の詳細については、「MLDスヌーピングクエリーアの有効化」を参照してください。
- MLD一般クエリーの送信元IPv6アドレスを、::およびローカルクエリーアIPv6アドレスとは異なるIPv6アドレスとして設定します。MLDスヌーピングクエリーアは、受信したMLD一般クエリーの送信元IPv6アドレスが::または自身のIPv6アドレスでない場合に限り、クエリーア選定を実行します。
- 候補MLDスヌーピングクエリーアが同じMLDスヌーピングバージョンを実行していることを確認します。MLDスヌーピングバージョンを指定するには、**mld-snooping version**コマンドを使用します。

VLANのMLDスヌーピングクエリーア選定の有効化

1. システムビューに入ります。

system-view

2. VLANビューを開始します。

vlan *vlan-id*

3. VLANのMLDスヌーピングクエリーア選定を有効にします。

mld-snooping querier-election

デフォルトでは、VLANのMLDスヌーピングクエリア選定は無効です。

VSIのMLDスヌーピング クエリア選定の有効化

1. システムビューに入ります。

system-view

2. VSIビューを入力します。

vsi *vsi-name*

3. VSIのMLDスヌーピングクエリアの選択を有効にします。

mld-snooping querier-election

デフォルトでは、VSIのMLDスヌーピングクエリアの選択は無効です。

MLD一般クエリーおよび応答のパラメータの設定

MLD一般クエリーおよび応答のパラメータの概要

実際のネットワーク状態に基づいて、MLD一般クエリーインターバルを変更できます。

レシーバホストは、MLD一般クエリーを受信すると、加入している各IPv6マルチキャストグループのレポート遅延タイマーを開始します。このタイマーは、0から最大値までの範囲のランダム値に設定されます。

タイマー値が0に減少すると、ホストは対応するIPv6マルチキャストグループにMLDレポートを送信します。

MLD一般クエリーの最大応答時間に適切な値を設定して、MLD一般クエリーに対するホストの応答を高速化し、MLDレポートトラフィックのバーストを回避します。

制約事項とガイドライン

IPv6マルチキャストグループメンバーを誤って削除しないようにするには、MLD一般クエリーインターバルをMLD一般クエリーの最大応答時間よりも長くします。

MLD一般クエリーおよび応答のグローバルなパラメータ設定

1. システムビューに入ります。

system-view

2. MLDスヌーピングビューを入力します。

mld-snooping

3. MLD一般クエリーの最大応答時間を設定します。

max-response-time *seconds*

デフォルトでは、MLD一般クエリーの最大応答時間は10秒です。

VLANのMLD一般的なクエリーおよび応答のパラメータ設定

1. システムビューに入ります。

system-view

2. VLANビューを開始します。

vlan *vlan-id*

3. VLANでMLD一般クエリーインターバルを設定します。

```
mld-snooping query-interval interval
```

デフォルトでは、VLANのMLD一般クエリーインターバルは125秒です。

4. VLANのMLD一般クエリーの最大応答時間を設定します。

```
mld-snooping max-response-time seconds
```

デフォルトでは、VLANのMLD一般クエリーの最大応答時間は10秒です。

VSIのMLD一般クエリーおよび応答のパラメータの設定

1. システムビューに入ります。

```
system-view
```

2. VSIビューを入力します。

```
vsi vsi-name
```

3. VSIでMLD一般クエリーインターバルを設定します。

```
mld-snooping query-interval interval
```

デフォルトでは、VSIのMLD一般クエリーインターバルは125秒です。

4. VSIでMLD一般クエリーの最大応答時間を設定します。

```
mld-snooping max-response-time seconds
```

デフォルトでは、VSIのMLD一般クエリーの最大応答時間は10秒です。

MLDスヌーピングプロキシの有効化

1. システムビューに入ります。

```
system-view
```

2. VLANビューを開始します。

```
vlan vlan-id
```

3. VLANのMLDスヌーピングプロキシを有効にします。

```
mld-snooping proxy enable
```

デフォルトでは、VLANのMLDスヌーピングプロキシは無効です。

MLDメッセージのパラメータの設定

MLDメッセージの送信元IPv6アドレスの設定

MLDメッセージの送信元IPv6アドレスの設定について

MLDスヌーピングクエリアによって送信されるMLDクエリーの送信元IPv6アドレスを変更できます。この設定は、サブネット内のMLDクエリア選定に影響を与える場合があります。

また、シミュレートされたメンバーホストまたはMLDスヌーピングプロキシによって送信されるMLDレポートまたはDoneメッセージの送信元IPv6アドレスを変更することもできます。

VLANに対するMLDメッセージの送信元IPv6アドレスの設定

1. システムビューに入ります。

system-view

2. VLANビューを開始します。

vlan *vlan-id*

3. MLD一般クエリーの送信元IPv6アドレスを設定します。

mld-snooping general-query source-ip *ipv6-address*

デフォルトでは、MLD一般クエリーの送信元IPv6アドレスは、現在のVLANインターフェイスのIPv6リンクローカルアドレスです。現在のVLANインターフェイスにIPv6リンクローカルアドレスがない場合、送信元IPv6アドレスはFE80::02FF:FFFF:FE00:0001になります。

4. MLDマルチキャストアドレス固有クエリーの送信元IPv6アドレスを設定します。

mld-snooping special-query source-ip *ipv6-address*

デフォルトでは、MLDマルチキャストアドレス固有クエリーの送信元IPv6アドレスは、次のいずれかです。

- VLANのMLDスヌーピングクエリアがMLD一般クエリーを受信した場合、MLD一般クエリーの送信元アドレス。
- MLDスヌーピングクエリアがMLD一般クエリーを受信しない場合の、現在のVLANインターフェイスのIPv6リンクローカルアドレス。
- FE80::02FF:FFFF:FE00:0001:MLDスヌーピングクエリアがMLD一般クエリーを受信せず、現在のVLANインターフェイスにIPv6リンクローカルアドレスがない場合。

5. MLDレポートの送信元IPv6アドレスを設定します。

mld-snooping report source-ip *ipv6-address*

デフォルトでは、MLDレポートの送信元IPv6アドレスは、現在のVLANインターフェイスのIPv6リンクローカルアドレスです。現在のVLANインターフェイスにIPv6リンクローカルアドレスがない場合、送信元IPv6アドレスはFE80::02FF:FFFF:FE00:0001になります。

6. MLD doneメッセージの送信元IPv6アドレスを設定します。

mld-snooping done source-ip *ipv6-address*

デフォルトでは、MLD doneメッセージの送信元IPv6アドレスは、現在のVLANインターフェイスのIPv6リンクローカルアドレスです。現在のVLANインターフェイスにIPv6リンクローカルアドレスがない場合、送信元IPv6アドレスはFE80::02FF:FFFF:FE00:0001になります。

VSIのMLDメッセージの送信元IPv6アドレスの設定

1. システムビューに入ります。

system-view

2. VLANビューを開始します。

vsi *vsi-name*

3. MLD一般クエリーの送信元IPv6アドレスを設定します。

mld-snooping general-query source-ip *ipv6-address*

デフォルトでは、MLD一般クエリーの送信元IPv6アドレスは、VSIのゲートウェイインターフェイスのIPv6リンクローカルアドレスです。ゲートウェイインターフェイスにIPv6リンクローカルアドレスがない場合、送信元IPv6アドレスはFE80::02FF:FFFF:FE00:0001になります。

4. MLDマルチキャストアドレス固有クエリーの送信元IPv6アドレスを設定します。

mld-snooping special-query source-ip *ipv6-address*

デフォルトでは、MLDマルチキャストアドレス固有クエリーの送信元IPv6アドレスは、次のいずれかです。

- MLD一般クエリーの送信元アドレス(VSIのMLDスヌーピングクエリアがMLD一般クエリーを受信した場合)。
- MLDスヌーピングクエリアがMLD一般クエリーを受信しない場合の、VSIのゲートウェイインターフェイスのIPv6リンクローカルアドレス。
- FE80::02FF:FFFF:FE00:0001ゲートウェイインターフェイスにIPv6リンクローカルアドレスがない場合。

5. MLDレポートの送信元IPv6アドレスを設定します。

mld-snooping report source-ip *ipv6-address*

デフォルトでは、MLDレポートの送信元IPv6アドレスは、VSIのゲートウェイインターフェイスのIPv6リンクローカルアドレスです。ゲートウェイインターフェイスにIPv6リンクローカルアドレスがない場合、送信元IPv6アドレスはFE80::02FF:FFFF:FE00:0001になります。

6. MLD doneメッセージの送信元IPv6アドレスを設定します。

mld-snooping done source-ip *ipv6-address*

デフォルトでは、MLD doneメッセージの送信元IPv6アドレスは、VSIのゲートウェイインターフェイスのIPv6リンクローカルアドレスです。ゲートウェイインターフェイスにIPv6リンクローカルアドレスがない場合、送信元IPv6アドレスはFE80::02FF:FFFF:FE00:0001になります。

MLDメッセージの802.1pプライオリティの設定

MLDメッセージの802.1pプライオリティについて

レイヤ2デバイスの出力ポートで輻輳が発生すると、レイヤ2デバイスは802.1pプライオリティの高い順にMLDメッセージを転送します。デバイスによって作成または転送されたMLDメッセージにより高い802.1pプライオリティを割り当てることができます。

制約事項とガイドライン

MLDスヌーピングビューのコンフィグレーションは、VLANに対してのみ有効です。VSIについては、VSIビューでのみ、MLDメッセージの802.1pプライオリティを設定できます。

MLDメッセージのグローバルな802.1pプライオリティの設定

1. システムビューに入ります。

system-view

2. MLDスヌーピングビューを入力します。

mld-snooping

3. MLDメッセージの802.1pプライオリティを設定します。

dot1p-priority *priority*

VLANのMLDメッセージの802.1pプライオリティの設定

1. システムビューに入ります。

system-view

2. VLANビューを開始します。

vlan *vlan-id*

3. VLAN内のMLDメッセージの802.1pプライオリティを設定します。

mld-snooping dot1p-priority *priority*

MLDスヌーピングポリシーの設定

IPv6マルチキャストグループポリシーの設定

IPv6マルチキャストグループポリシーについて

この機能により、レイヤ2デバイスは、IPv6マルチキャストグループおよび任意の送信元を指定するACLを使用して、MLDレポートをフィルタリングできます。これは、レシーバホストが加入できるIPv6マルチキャストグループを制御するために使用されます。この設定は、ポートがダイナミックに加入するIPv6マルチキャストグループに対して有効になります。

IPv6マルチキャストアプリケーションでは、ユーザーがIPv6マルチキャストプログラムを要求すると、ホストは非送信請求MLDレポートを送信します。レイヤ2デバイスは、IPv6マルチキャストグループポリシーを使用してMLDレポートをフィルタリングします。MLDレポートがIPv6マルチキャストグループポリシーによって許可されている場合に限り、ホストはIPv6マルチキャストグループに加入できます。

IPv6マルチキャストグループポリシーのグローバルな設定

1. システムビューに入ります。

system-view

2. MLDスヌーピングビューを入力します。

mld-snooping

3. IPv6マルチキャストグループポリシーをグローバルに設定します。

group-policy *ipv6-acl-number* [**vlan** *vlan-list*]

デフォルトでは、IPv6マルチキャストグループポリシーは存在しません。ホストは任意のIPv6マルチキャストグループに加入できます。

ポート上でのIPv6マルチキャストグループポリシーの設定

1. システムビューに入ります。

system-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface *interface-type interface-number*

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation *interface-number*

3. ポート上でIPv6マルチキャストグループポリシーを設定します。

mld-snooping group-policy *ipv6-acl-number* [**vlan** *vlan-list*]

デフォルトでは、IPv6マルチキャストグループポリシーはポートに存在しません。ポートに接続されたホストは、任意のIPv6マルチキャストグループに加入できます。

IPv6マルチキャスト送信元ポートフィルタリングの有効化

IPv6マルチキャスト送信元ポートフィルタリングについて

この機能により、レイヤ2デバイスはすべてのIPv6マルチキャストデータパケットを廃棄し、IPv6マルチキャストプロトコルパケットを受け入れることができます。この機能は、IPv6マルチキャストレシーバだけに接続するポートで有効にできます。

MLDスヌーピングビューで行われたコンフィグレーションは、インターフェイス特有のコンフィグレーションよりも同じプライオリティを持っています。

制約事項とガイドライン

IPv6マルチキャスト送信元ポートフィルタリングが有効の場合、デバイスは自動的にIPv4マルチキャスト送信元ポートフィルタリングを有効にします。

MLDスヌーピングビューで行われたコンフィグレーションは、インターフェイス特有のコンフィグレーションと同じプライオリティを持ち、最新のコンフィグレーションが有効になります。

MLDスヌーピングビューでのIPv6マルチキャスト送信元ポートフィルタリングの有効化

1. システムビューに入ります。

system-view

2. MLDスヌーピングビューを入力します。

mld-snooping

3. IPv6マルチキャスト送信元ポートフィルタリングをグローバルに有効にします。

source-deny port interface-list

デフォルトでは、IPv6マルチキャスト送信元ポートフィルタリングはグローバルに無効です。

インターフェイスビューでのIPv6マルチキャスト送信元ポートフィルタリングの有効化

1. システムビューに入ります。

system-view

2. レイヤ2イーサネットインターフェイスビューを開始します。

interface interface-type interface-number

3. ポート上でIPv6マルチキャスト送信元ポートフィルタリングを有効にします。

mld-snooping source-deny

デフォルトでは、IPv6マルチキャスト送信元ポートフィルタリングはポート上で無効です。

不明なIPv6マルチキャストデータの破棄の有効化

不明なIPv6マルチキャストデータのドロップについて

不明なIPv6マルチキャストデータとは、MLDスヌーピング転送テーブルに転送エントリが存在しないIPv6マルチキャストデータを指します。この機能により、デバイスは不明なIPv6マルチキャストデータをルータポートだけに転送できます。デバイスにルータポートがない場合、不明なIPv6マルチキャストデータはドロ

ップされます。

この機能を有効にしない場合、不明なIPv6マルチキャストデータは、データが属するVLANまたはVSIでフラッディングされます。

制約事項とガイドライン

不明なIPv6マルチキャストデータのドロップが有効の場合、デバイスは不明なIPv4マルチキャストデータもドロップします。

不明なIPv6マルチキャストデータのドロップを有効にしても、デバイスは不明なIPv6マルチキャストデータをルータポート(受信側ルータポートを除く)から転送します。

VLANの不明なIPv6マルチキャストデータの廃棄の有効化

1. システムビューに入ります。

system-view

2. VLANビューを開始します。

vlan *vlan-id*

3. VLANの不明なIPv6マルチキャストデータのドロップを有効にします。

mld-snooping drop-unknown

デフォルトでは、不明なIPv6マルチキャストデータのドロップは無効になっています。不明なIPv6マルチキャストデータはフラッディングされます。

VSIの不明なIPv6マルチキャストデータのドロップの有効化

1. システムビューに入ります。

system-view

2. VSIビューを入力します。

vsi *vsi-name*

3. VSIの不明なIPv6マルチキャストデータのドロップを有効にします。

mld-snooping drop-unknown

デフォルトでは、不明なIPv6マルチキャストデータのドロップは無効になっています。不明なIPv6マルチキャストデータはフラッディングされます。

MLDレポート抑制の有効化

MLDレポート抑制の概要

この機能により、レイヤ2デバイスは、IPv6マルチキャストグループの最初のMLDレポートだけを直接接続されたレイヤ3デバイスに転送できます。同じクエリーテーブル内の同じグループの他のレポートは廃棄されます。この機能を使用して、マルチキャストトラフィックを軽減します。

手順

1. システムビューに入ります。

system-view

2. MLDスヌーピングビューを入力します。

mld-snooping

3. MLDレポート抑制を有効にします。

report-aggregation

デフォルトでは、MLDレポート抑制は有効です。

ポート上の最大IPv6マルチキャストグループ数の設定

ポート上のIPv6マルチキャストグループの最大数の設定について

ポート上のIPv6マルチキャストグループの最大数を設定して、ポートトラフィックを制御できます。この設定は、ポートがダイナミックに加入するIPv6マルチキャストグループ上だけで有効です。

ポート上のIPv6マルチキャストグループの数が制限を超えると、システムはそのポートに関連するすべての転送エントリを削除します。この場合、そのポートに接続されているレシーバホストは、ポート上のIPv6マルチキャストグループの数が制限に達する前に、IPv6マルチキャストグループに再度加入できます。

手順

1. システムビューに入ります。

system-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface interface-type interface-number

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation interface-number

3. ポート上のIPv6マルチキャストグループの最大数を設定します。

mld-snooping group-limit limit [vlan vlan-list]

デフォルトでは、ポート上のIPv6マルチキャストグループの最大数に制限はありません。

IPv6マルチキャストグループ置換の有効化

IPv6マルチキャストグループ置換の概要

この機能を使用すると、グループの数が上限を超えた場合に、レイヤ2デバイスは既存のグループを新しく参加したグループに置き換えることができます。この機能は通常、チャンネルスイッチングアプリケーションで使用されます。この機能がない場合、デバイスは新しいグループのMLDレポートを廃棄し、ユーザーは新しいチャンネルに変更できません。

制約事項とガイドライン

この設定は、ポートがダイナミックに加入するマルチキャストグループに対してだけ有効です。

IPv6マルチキャストグループ置換のグローバルな有効化

1. システムビューに入ります。

system-view

2. MLDスヌーピングビューを入力します。

mld-snooping

3. IPv6マルチキャストグループ置換をグローバルに有効にします。

overflow-replace [vlan vlan-list]

デフォルトでは、IPv6マルチキャストグループ置換はグローバルに無効になっています。

ポート上でのIPv6マルチキャストグループ置換の有効化

1. システムビューに入ります。

system-view

2. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface interface-type interface-number

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation interface-number

3. ポート上でIPv6マルチキャストグループ置換を有効にします。

mld-snooping overflow-replace [vlan vlan-list]

マルチキャストグループ置換はポート上で無効です。

ホストラッキングの有効化

ホストラッキングについて

この機能を使用すると、レイヤ2デバイスは、IPv6マルチキャストデータを受信するメンバーホストに関する情報を記録できます。この情報には、ホストのIPv6アドレス、ホストがIPv6マルチキャストグループに加入してからの経過時間、およびホストの残りのタイムアウト時間が含まれます。この機能により、メンバーホストの監視と管理が容易になります。

制約事項とガイドライン

MLDスヌーピングビューで行われた設定は、VSIでは有効になりません。

ホストラッキングのグローバルな有効化

1. システムビューに入ります。

system-view

2. MLDスヌーピングビューを入力します。

mld-snooping

3. ホストラッキングをグローバルに有効にします。

host-tracking

デフォルトでは、ホストラッキングはグローバルに無効です。

VLANでのホストトラッキングの有効化

1. システムビューに入ります。

system-view

2. VLANビューを開始します。

vlan vlan-id

3. VLANのホストトラッキングを有効にします。

mld-snooping host-tracking

デフォルトでは、VLANでのホストトラッキングは無効です。

発信MLDスヌーピングプロトコルパケットのDSCP値の設定

発信MLDスヌーピングプロトコルパケットのDSCP値について

DSCP値は、パケット送信の優先順位を決定します。DSCP値が大きいほど、優先順位が高くなります。

手順

1. システムビューに入ります。

system-view

2. MLDスヌーピングビューを入力します。

mld-snooping

3. 発信MLDスヌーピングプロトコルパケットのDSCP値を設定します。

dscp dscp-value

デフォルトでは、発信MLDスヌーピングプロトコルパケットのDSCP値は48です。

MLDスヌーピングの表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
レイヤ2 IPv6マルチキャスト高速フォワーディングエントリを表示します。	display ipv6 l2-multicast fast-forwarding cache [vlan vlan-id] [ipv6-source-address ipv6-group-address] * [slot slot-number]
レイヤ2 IPv6マルチキャストグループに関する情報を表示します。	display ipv6 l2-multicast ip [group ipv6-group-address source ipv6-source-address] * [vlan vlan-id vsi vsi-name] [slot slot-number]

レイヤ2 IPv6マルチキャストグループエントリを表示します。	display ipv6 l2-multicast ip forwarding [group <i>ipv6-group-address</i> source <i>ipv6-source-address</i>] * [vlan <i>vlan-id</i> vsi <i>vsi-name</i>] [slot <i>slot-number</i>]
レイヤ2 IPv6 MACマルチキャストグループに関する情報を表示します。	display ipv6 l2-multicast mac [<i>mac-address</i>] [vlan <i>vlan-id</i> vsi <i>vsi-name</i>] [slot <i>slot-number</i>]
レイヤ2 IPv6 MACマルチキャストグループエントリを表示します。	display ipv6 l2-multicast mac forwarding [<i>mac-address</i>] [vlan <i>vlan-id</i> vsi <i>vsi-name</i>] [slot <i>slot-number</i>]
スタティックIPv6マルチキャストMACアドレスエントリを表示します。	display mac-address [<i>mac-address</i> [vlan <i>vlan-id</i>] [multicast] [vlan <i>vlan-id</i>] [count]]
MLDスヌーピングステータスを表示します。	display mld-snooping [global vlan <i>vlan-id</i> vsi <i>vsi-name</i>]
ダイナミックMLDスヌーピンググループエントリを表示します。	display mld-snooping group [<i>ipv6-group-address</i> <i>ipv6-source-address</i>] * [vlan <i>vlan-id</i> vsi <i>vsi-name</i>] [interface <i>interface-type interface-number</i> [verbose] [slot <i>slot-number</i>]]
ホストトラッキング情報を表示します。	display mld-snooping host-tracking vlan <i>vlan-id</i> group <i>ipv6-group-address</i> [source <i>ipv6-source-address</i>] [slot <i>slot-number</i>]
ダイナミックルータポート情報を表示します。	display mld-snooping router-port [vlan <i>vlan-id</i> vsi <i>vsi-name</i>] [verbose] [slot <i>slot-number</i>]
スタティックMLDスヌーピンググループエントリを表示します。	display mld-snooping static-group [<i>ipv6-group-address</i> <i>ipv6-source-address</i>] * [vlan <i>vlan-id</i>] [verbose] [slot <i>slot-number</i>]
スタティックルータポート情報を表示します。	display mld-snooping static-router-port [vlan <i>vlan-id</i>] [verbose] [slot <i>slot-number</i>]
MLDスヌーピングによって取得されたMLDメッセージおよびIPv6 PIMハローメッセージの統計情報を表示します。	display mld-snooping statistics
レイヤ2 IPv6マルチキャスト高速フォワーディングエントリをクリアします。	reset ipv6 l2-multicast fast-forwarding cache [vlan <i>vlan-id</i>] { { <i>ipv6-source-address</i> <i>ipv6-group-address</i> } * all } [slot <i>slot-number</i>]

ダイナミックMLDスヌーピンググループエントリをクリアします。	reset mld-snooping group { <i>ipv6-group-address</i> [<i>ipv6-source-address</i>] all } [vlan <i>vlan-id</i> vsi <i>vsi-name</i>]
ダイナミックルータのポート情報をクリアします。	reset mld-snooping router-port { all vlan <i>vlan-id</i> vsi <i>vsi-name</i> }
MLDスヌーピングによって学習されたMLDメッセージおよびIPv6 PIM helloメッセージの統計情報をクリアします。	reset mld-snooping statistics

MLDスヌーピングの設定例

例:VLANベースIPv6グループポリシーおよびシミュレートされた加入の設定

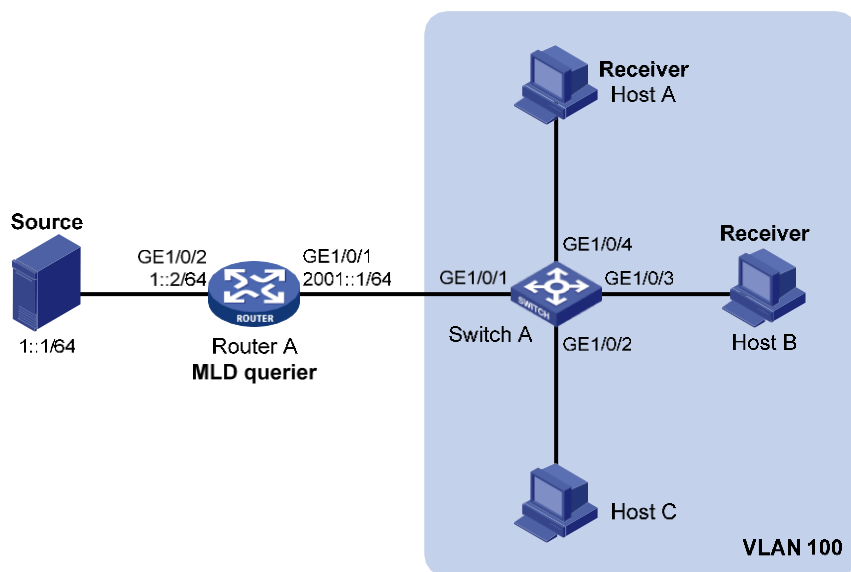
ネットワークの設定

図63に示されるように、ルータAはMLDv1を実行し、MLDクエリアとして動作し、スイッチAはMLDv1スヌーピングを実行します。

次の要件を満たすようにグループポリシーを設定し、参加をシミュレートします。

- ホストAおよびホストBは、IPv6マルチキャストグループFF1E::101宛てのIPv6マルチキャストデータだけを受信します。ホストAおよびホストBがマルチキャストデータの受信に失敗した場合でも、スイッチAのGigabitEthernet 1/0/3およびGigabitEthernet 1/0/4を介してIPv6マルチキャストデータを継続的に転送できます。
- スイッチAは、不明なIPv6マルチキャストデータをVLAN 100にフラッディングせずに廃棄します。

図63 ネットワークダイアグラム



手順図63に示すように、各インターフェイスにIPv6アドレスとプレフィクス長を割り当てます。(詳細は省略)

1. ルータAを設定します。

```
# Enable IPv6 multicast routing.
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
# Enable MLD on GigabitEthernet 1/0/1.
[RouterA] interface gigabitethernet 1/0/1
```

```
[RouterA-GigabitEthernet1/0/1] mld enable
```

```
[RouterA-GigabitEthernet1/0/1] quit
```

```
# Enable IPv6 PIM-DM on GigabitEthernet 1/0/2.
```

```
[RouterA] interface gigabitethernet 1/0/2
```

```
[RouterA-GigabitEthernet1/0/2] ipv6 pim dm
```

```
[RouterA-GigabitEthernet1/0/2] quit
```

2. スイッチAを設定します。

```
# Enable the MLD snooping feature.
```

```
<SwitchA> system-view
```

```
[SwitchA] mld-snooping
```

```
[SwitchA-mld-snooping] quit
```

```
# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the VLAN.
```

```
[SwitchA] vlan 100
```

```
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

```
# Enable MLD snooping, and enable dropping IPv6 unknown multicast data for VLAN 100.
```

```
[SwitchA-vlan100] mld-snooping enable
```

```
[SwitchA-vlan100] mld-snooping drop-unknown
```

```
[SwitchA-vlan100] quit
```

```
# Configure an IPv6 multicast group policy so that hosts in VLAN 100 can join only IPv6 multicast group FF1E::101.
```

```
[SwitchA] acl ipv6 basic 2001
```

```
[SwitchA-acl-ipv6-basic-2001] rule permit source ff1e::101 128
```

```
[SwitchA-acl-ipv6-basic-2001] quit
```

```
[SwitchA] mld-snooping
```

```
[SwitchA-mld-snooping] group-policy 2001 vlan 100
```

```
[SwitchA-mld-snooping] quit
```

```
# Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4 as simulated member hosts to join IPv6 multicast group FF1E::101.
```

```
[SwitchA] interface gigabitethernet 1/0/3
```

```
[SwitchA-GigabitEthernet1/0/3] mld-snooping host-join ff1e::101 vlan 100
```

```
[SwitchA-GigabitEthernet1/0/3] quit
```

```
[SwitchA] interface gigabitethernet 1/0/4
```

```
[SwitchA-GigabitEthernet1/0/4] mld-snooping host-join ff1e::101 vlan 100
```

```
[SwitchA-GigabitEthernet1/0/4] quit
```

設定の確認

#ホストAおよびホストBからMLDレポートを送信して、IPv6マルチキャストグループFF1E::101およびFF1E::202に参加します(詳細は省略)。

#スイッチA上のVLAN 100のダイナミックMLDスヌーピンググループエントリを表示します。

```
[SwitchA] display mld-snooping group vlan 100
```

```
Total 1 entries.
```

```
VLAN 100: Total 1 entries.
```

```
(::, FF1E::101)
```


Host ports (2 in total):

GE1/0/3	(00:03:23)
GE1/0/4	(00:04:10)

出力には次の情報が表示されます。

- ホストAおよびホストBは、それぞれスイッチA上のメンバーポートGigabitEthernet 1/0/4およびGigabitEthernet 1/0/3を介してIPv6マルチキャストグループFF1E::101に加入しています。
- ホストAとホストBは、マルチキャストグループFF1E::202に参加できませんでした。

例:VLANベースのスタティックポートの設定

ネットワークの設定

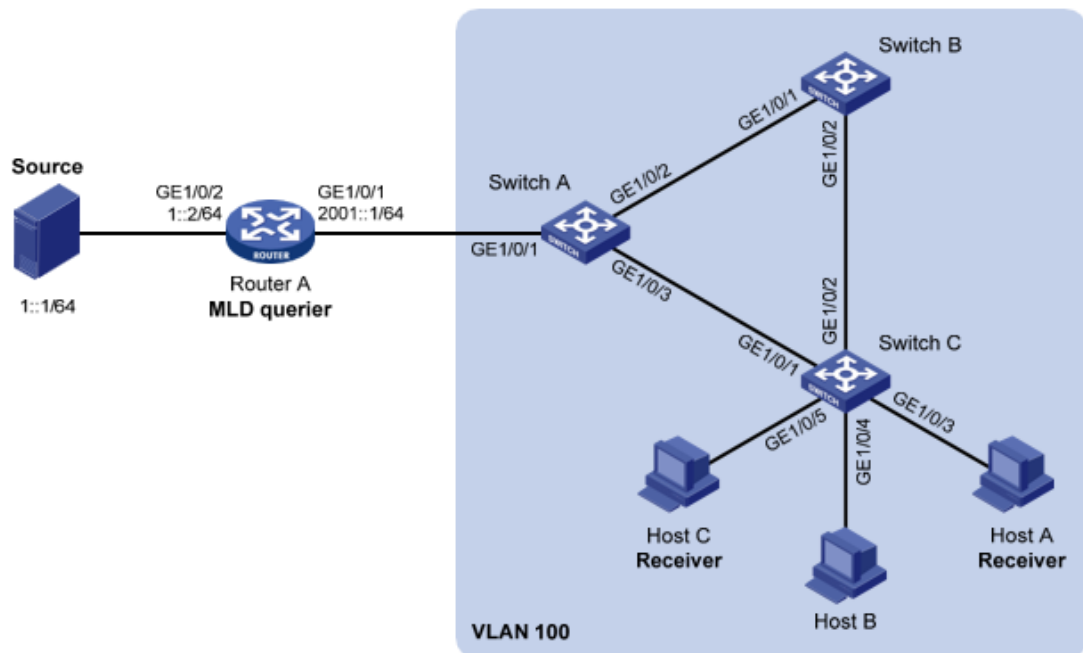
図64に示します。

- ルータAはMLDv1を実行し、MLDクエリーアとして動作します。スイッチA、スイッチB、およびスイッチCは、MLDv1スヌーピングを実行します。
- ホストAとホストCは、IPv6マルチキャストグループFF1E::101のパーマネントレシーバです。次の要件を満たすようにスタティックポートを設定します。
 - IPv6マルチキャストトラフィック伝送の信頼性を高めるには、GigabitEthernet 1/0/3を設定します。およびGigabitEthernet 1/0/5をIPv6マルチキャストグループFF1E::101のスタティックメンバーポートとして設定します。
- STPがネットワーク上で動作していると仮定します。データループを回避するために、スイッチAからスイッチCへの転送パスはブロックされます。IPv6マルチキャストデータは、スイッチA、スイッチB、スイッチCのパスに沿ってだけ、スイッチCに接続されたレシーバに流れます。このパスがブロックされると、IPv6マルチキャストデータがレシーバに流れる前に、少なくとも1つのMLDクエリー応答サイクルが完了する必要があります。

スイッチAスイッチCのパスに沿って。この場合、マルチキャスト配信はプロセス中に中断されます。STPの詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

スイッチAのGigabitEthernet 1/0/3をスタティックルータポートとして設定します。これにより、スイッチAスイッチBスイッチCのパスがブロックされた場合でも、IPv6マルチキャストデータをスイッチAスイッチCのパスに沿ってほぼ中断なくレシーバに流すことができます。

図64 ネットワークダイアグラム



手順

1. 図64に示すように、各インターフェイスにIPv6アドレスとプレフィクス長を割り当てます。(詳細は省略)

2. ルータAを設定します。

```
# Enable IPv6 multicast routing.
<RouterA> system-view
[RouterA] ipv6 multicast routing
[RouterA-mrib6] quit
# Enable MLD on GigabitEthernet 1/0/1.
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] quit
# Enable IPv6 PIM-DM on GigabitEthernet 1/0/2.
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ipv6 pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

3. スイッチAを設定します。

```
# Enable the MLD snooping feature.
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to the VLAN.
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

```
# Enable MLD snooping for VLAN 100.
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] quit
# Configure GigabitEthernet 1/0/3 as a static router port.
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

4. スイッチBを構成します。

```
# Enable the MLD snooping feature.
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
# Create VLAN 100, and assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the VLAN.
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
# Enable MLD snooping for VLAN 100.
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] quit
```

5. スイッチCを設定します。

```
# Enable the MLD snooping feature.
<SwitchC> system-view
[SwitchC] mld-snooping
[SwitchC-mld-snooping] quit
# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to the VLAN.
[SwitchC] vlan 100
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/5
# Enable MLD snooping for VLAN 100.
[SwitchC-vlan100] mld-snooping enable
[SwitchC-vlan100] quit
# Configure GigabitEthernet 1/0/3 and GigabitEthernet 1/0/5 as static member ports for IPv6 multicast group FF1E::101.
[SwitchC] interface gigabitethernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet1/0/3] quit
[SwitchC] interface gigabitethernet 1/0/5
[SwitchC-GigabitEthernet1/0/5] mld-snooping static-group ff1e::101 vlan 100
[SwitchC-GigabitEthernet1/0/5] quit
```

設定の確認

#スイッチA上のVLAN 100のスタティックルータポート情報を表示します。

```
[SwitchA] display mld-snooping static-group vlan 100
VLAN 100:
```

Router ports (1 in total):

```
GE1/0/3
```

#スイッチC上のVLAN 100における静的MLDスヌーピンググループエントリを表示します。

```
[SwitchC] display mld-snooping static-group vlan 100  
Total 1 entries).
```

VLAN 100: Total 1 entries)

(::, FF1E::101)

Host ports (2 in total):

GE1/0/3

GE1/0/5

この出力は、スイッチCのGigabitEthernet 1/0/3およびGigabitEthernet 1/0/5がIPv6マルチキャストグループFF1E::101のスタティックメンバーポートになったことを示しています。

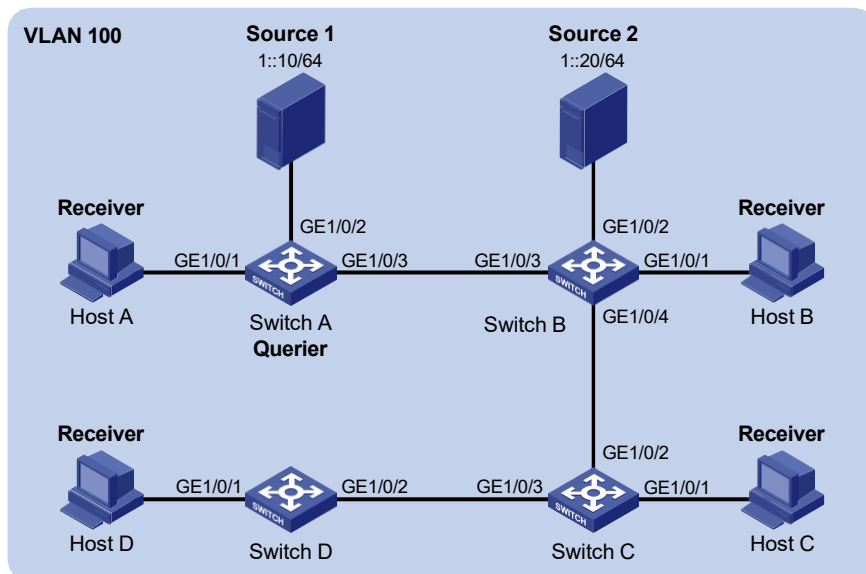
例:VLANベースMLDスヌーピングクエリアーの設定

ネットワークの設定

図65に示します。

- ネットワークはレイヤ2だけのネットワークです。
- Source 1とSource 2は、それぞれIPv6マルチキャストグループFF1E::101とFF1E::102にマルチキャストデータを送信します。
- ホストAとホストCはIPv6マルチキャストグループFF1E::101のレシーバであり、ホストBとホストDはIPv6マルチキャストグループFF1E::102のレシーバです。
- すべてのホストレシーバはMLDv1を実行し、すべてのスイッチはMLDv1スヌーピングを実行します。スイッチA(マルチキャスト送信元に近い)は、MLDスヌーピングクエリアーとして機能します。スイッチがVLAN内で不明なIPv6パケットをフラッディングしないようにするには、すべてのスイッチが不明なIPv6マルチキャストパケットをドロップできるようにします。

図65 ネットワークダイアグラム



手順

1. スイッチAを設定します。

Enable the MLD snooping feature.

```
<SwitchA> system-view
```

```
[SwitchA] mld-snooping
```

```
[SwitchA-mld-snooping] quit
```

Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to the VLAN.

```
[SwitchA] vlan 100
```

```
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

Enable MLD snooping, and enable dropping unknown IPv6 multicast data for VLAN 100.

```
[SwitchA-vlan100] mld-snooping enable
```

```
[SwitchA-vlan100] mld-snooping drop-unknown
```

Configure Switch A as the MLD snooping querier.

```
[SwitchA-vlan100] MLD-snooping querier
```

```
[SwitchA-vlan100] quit
```

2. スイッチBを構成します。

Enable the MLD snooping feature.

```
<SwitchB> system-view
```

```
[SwitchB] mld-snooping
```

```
[SwitchB-mld-snooping] quit
```

Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the VLAN.

```
[SwitchB] vlan 100
```

```
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

Enable MLD snooping, and enable dropping unknown IPv6 multicast data for VLAN 100.

```
[SwitchB-vlan100] mld-snooping enable
```

```
[SwitchB-vlan100] mld-snooping drop-unknown
```

```
[SwitchB-vlan100] quit
```

3. スイッチCを設定します。

Enable the MLD snooping feature.

```
<SwitchC> system-view
```

```
[SwitchC] mld-snooping
```

```
[SwitchC-mld-snooping] quit
```

Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to the VLAN.

```
[SwitchC] vlan 100
```

```
[SwitchC-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

Enable MLD snooping, and enable dropping unknown IPv6 multicast data for VLAN 100.

```
[SwitchC-vlan100] mld-snooping enable
```

```
[SwitchC-vlan100] mld-snooping drop-unknown
```

```
[SwitchC-vlan100] quit
```

4. スイッチDを構成します。

```
# Enable the MLD snooping feature.
<SwitchD> system-view
[SwitchD] mld-snooping
[SwitchD-mld-snooping] quit
# Create VLAN 100, and assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to the VLAN.
[SwitchD] vlan 100
[SwitchD-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
# Enable MLD snooping, and enable dropping unknown IPv6 multicast data for VLAN 100.
[SwitchD-vlan100] mld-snooping enable
[SwitchD-vlan100] mld-snooping drop-unknown
[SwitchD-vlan100] quit
```

設定の確認

#スイッチBのMLDスヌーピングを通じて学習されたMLDメッセージおよびIPv6 PIM helloメッセージの統計情報を表示します。

```
[SwitchB] display mld-snooping statistics
Received MLD general queries: 3
Received MLDv1 specific queries: 0
Received MLDv1 reports: 12
Received MLD done: 0
Sent MLDv1 specific queries: 0
Received MLDv2 reports: 0
Received MLDv2 reports with right and wrong records: 0
Received MLDv2 specific queries: 0
Received MLDv2 specific sg queries: 0
Sent MLDv2 specific queries: 0
Sent MLDv2 specific sg queries: 0
Received IPv6 PIM hello: 0
Received error MLD messages: 0
```

この出力は、スイッチAがMLDスヌーピングクエリーアとして動作したあと、スイッチAを除くすべてのスイッチがMLD一般クエリーを受信できることを示しています。

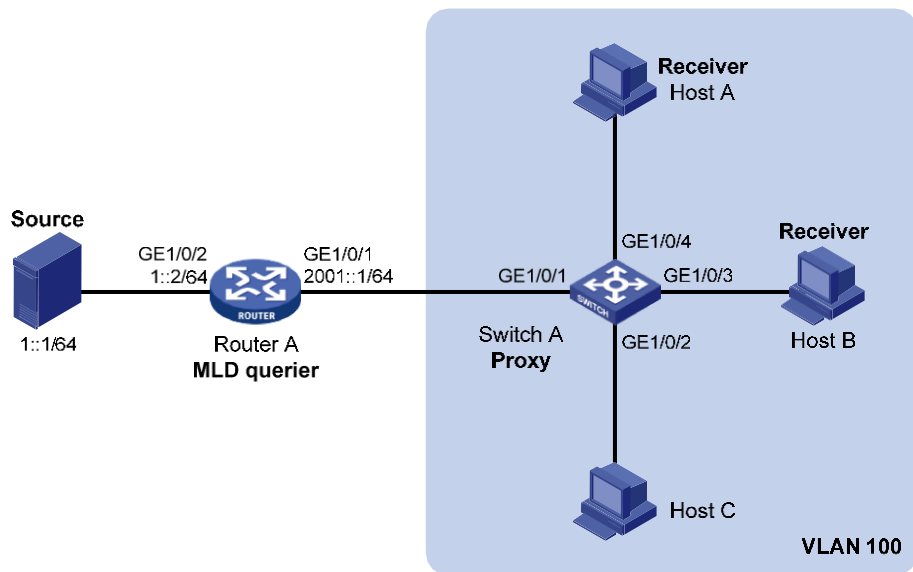
例:VLANベースのMLDスヌーピングプロキシの設定

ネットワークの設定

図66に示すように、ルータAはMLDv1を実行し、MLDクエリーアとして動作します。スイッチAはMLDv1スヌーピングを実行します。スイッチAが次のアクションを実行できるように、MLDスヌーピングプロキシを設定します。

- MLDレポートと完了メッセージをルータAに転送します。
- ルータAによって送信されたMLDクエリーに応答し、そのクエリーをダウンストリームホストに転送します。

図66 ネットワークダイアグラム



手順

1. 図66に示すように、各インターフェイスにIPv6アドレスとサブネットマスクを割り当てます。(詳細は省略)

2. ルータAを設定します。

Enable IPv6 multicast routing.

```
<RouterA> system-view
```

```
[RouterA] ipv6 multicast routing
```

```
[RouterA-mrib6] quit
```

Enable MLD and IPv6 PIM-DM on GigabitEthernet 1/0/1.

```
[RouterA] interface gigabitethernet 1/0/1
```

```
[RouterA-GigabitEthernet1/0/1] mld enable
```

```
[RouterA-GigabitEthernet1/0/1] ipv6 pim dm
```

```
[RouterA-GigabitEthernet1/0/1] quit
```

Enable IPv6 PIM-DM on GigabitEthernet 1/0/2.

```
[RouterA] interface gigabitethernet 1/0/2
```

```
[RouterA-GigabitEthernet1/0/2] ipv6 pim dm
```

```
[RouterA-GigabitEthernet1/0/2] quit
```

3. スイッチAを設定します。

Enable the MLD snooping feature.

```
<SwitchA> system-view
```

```
[SwitchA] mld-snooping
```

```
[SwitchA-mld-snooping] quit
```

Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the VLAN.

```
[SwitchA] vlan 100
```

```
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
# Enable MLD snooping and MLD snooping proxying for the VLAN.
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping proxy enable
[SwitchA-vlan100] quit
```

設定の確認

#ホストAとホストBからMLDレポートを送信して、IPv6マルチキャストグループFF1E::101に参加します
(詳細は省略)。

Display MLD snooping group entries on Switch A.

```
[SwitchA] display mld-snooping group
Total 1 entries.
```

VLAN 100: Total 1 entries.

(::, FF1E::101)

Host ports (2 in total):

GE1/0/3	(00:04:09)
GE1/0/4	(00:03:06)

この出力は、GigabitEthernet 1/0/3およびGigabitEthernet 1/0/4がIPv6マルチキャストグループFF1E::101のメンバーポートであることを示しています。ホストAおよびホストBは、グループのIPv6マルチキャストデータを受信します。

#ルータA上のMLDグループメンバーシップ情報を表示します。

```
[RouterA] display mld grou
MLD groups in total: 1
GigabitEthernet1/0/1(2001::1):
MLD groups reported in total:
Group address: FF1E::101
Last reporter: FE80::2FF:FFFF:FE00:1
Uptime: 00:00:31
Expires: 00:03:48
```

#MLD doneメッセージをホストAから送信し、IPv6マルチキャストグループFF1E::101から脱退します(詳細は省略)。

#スイッチA上のMLDスヌーピンググループエントリを表示します。

```
[SwitchA] display mld-snooping group
Total 1 entries.
```

VLAN 100: Total 1 entries.

(::, FF1E::101)

Host ports (1 in total):

GE1/0/3	(00:01:23)

この出力は、GigabitEthernet 1/0/3がIPv6マルチキャストグループFF1E::101の唯一のメンバーポートであることを示しています。ホストBだけがグループのIPv6マルチキャストデータを受信します。

例:VXLANベースのMLDスヌーピングの設定

ネットワークの設定

図67に示します。

- VXLAN 10は、ネットワークサイト間でVM 1、VM 2、およびVM 3にレイヤ2接続を提供します。
- VXLAN 10は、トラフィックのフラッディングにユニキャストモードを使用します。

IPv6レイヤ2マルチキャスト転送を実装し、VXLAN 10のVTEPの既知のマルチキャストトラフィックを複製する負荷を軽減するには、スイッチにMLDスヌーピングを設定します。

図67 ネットワークダイアグラム

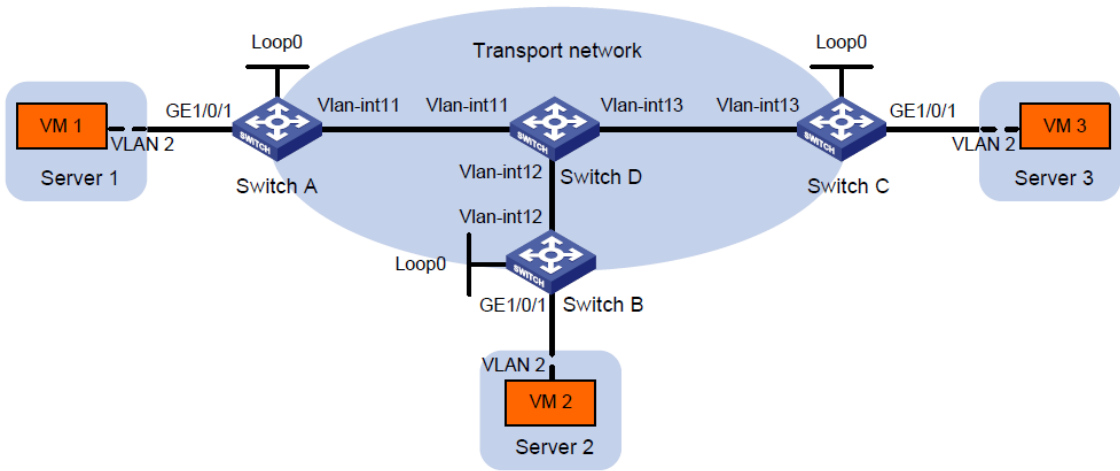


表16インターフェイスとIPアドレスの割り当て

デバイス	インターフェイス	IPアドレス	デバイス	インターフェイス	IPアドレス
Switch A	Vlan-int11	11.1.1.1/24	Switch C	Vlan-int13	13.1.1.3/24
Switch A	Loop0	1.1.1.1/32	Switch C	Loop0	3.3.3.3/32
Switch B	Vlan-int12	12.1.1.2/24	Switch D	Vlan-int11	11.1.1.4/24
Switch B	Loop0	2.2.2.2/32	Switch D	Vlan-int12	12.1.1.4/24
			Switch D	Vlan-int13	13.1.1.4/24

手順

1. 表16に示すように、トランスポートネットワーク上の各インターフェイスにIPアドレスとサブネットマスクを割り当てます。(詳細は省略)
2. 転送ネットワーク内のすべてのスイッチにOSPFを設定します(詳細は省略)。
3. スイッチAを設定します。

```
# Enable L2VPN.  
<SwitchA> system-view  
[SwitchA] l2vpn enable  
# Enable Layer 2 forwarding for VXLANs.
```

```

[SwitchA] undo vxlan ip-forwarding
# Create a VSI named vpna, and create VXLAN 10.
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] vxlan 10
[SwitchA-vsi-vpna-vxlan-10] quit
[SwitchA-vsi-vpna] quit
# Enable the MLD snooping feature.
[SwitchA] mld-snooping
[SwitchA -mld-snooping] quit
# Enable MLD snooping and dropping unknown IPv6 multicast data packets for VSI vpna.
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] mld-snooping enable
[SwitchA-vsi-vpna] mld-snooping drop-unknown
[SwitchA-vsi-vpna] quit
# Assign an IP address to Loopback 0. This address will be used as the source address of
the VXLAN tunnels to Switch B and Switch C.
[SwitchA] interface loopback 0
[SwitchA-Loopback0] ip address 1.1.1.1 255.255.255.255
[SwitchA-Loopback0] quit
# Create a VXLAN tunnel to Switch B.


- The tunnel interface name is Tunnel 1.
- The source address and destination address of the tunnel interface are 1.1.1.1 and 2.2.2.2, respectively.


[SwitchA] interface tunnel 1 mode vxlan
[SwitchA-Tunnel1] source 1.1.1.1
[SwitchA-Tunnel1] destination 2.2.2.2
[SwitchA-Tunnel1] quit
# Create a VXLAN tunnel to Switch C.


- The tunnel interface name is Tunnel 2.
- The source address and destination address of the tunnel interface are 1.1.1.1 and 3.3.3.3, respectively.


[SwitchA] interface tunnel 2 mode vxlan
[SwitchA-Tunnel2] source 1.1.1.1
[SwitchA-Tunnel2] destination 3.3.3.3
[SwitchA-Tunnel2] quit
# Assign Tunnel 1 and Tunnel 2 to VXLAN 10.
[SwitchA] vsi vpna
[SwitchA-vsi-vpna] vxlan 10
[SwitchA-vsi-vpna-vxlan-10] tunnel 1
[SwitchA-vsi-vpna-vxlan-10] tunnel 2
[SwitchA-vsi-vpna-vxlan-10] quit
[SwitchA-vsi-vpna] quit
# On GigabitEthernet 1/0/1, create Ethernet service instance 1000 to match VLAN 2.
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] service-instance 1000

```

```
[SwitchA-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 2
# Map Ethernet service instance 1000 to VSI vpna.
[SwitchA-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna
[SwitchA-GigabitEthernet1/0/1-srv1000] quit
[SwitchA-GigabitEthernet1/0/1] quit
```

4. スイッチBを設定します。#L2VPNを有効にします。

```
<SwitchB> system-view
[SwitchB] l2vpn enable
# Enable Layer 2 forwarding for VXLANs.
[SwitchB] undo vxlan ip-forwarding
# Create a VSI named vpna, and create VXLAN 10.
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] vxlan 10
[SwitchB-vsi-vpna-vxlan-10] quit
[SwitchB-vsi-vpna] quit
# Enable the MLD snooping feature.
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
# Enable MLD snooping and dropping unknown IPv6 multicast data packets for VSI vpna.
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] mld-snooping enable
[SwitchB-vsi-vpna] mld-snooping drop-unknown
[SwitchB-vsi-vpna] quit
# Assign an IP address to Loopback 0. This address will be used as the source address of
the
VXLAN tunnels to Switch A and Switch C.
[SwitchB] interface loopback 0
[SwitchB-Loopback0] ip address 2.2.2.2 255.255.255.255
[SwitchB-Loopback0] quit
# Create a VXLAN tunnel to Switch A.


- The tunnel interface name is Tunnel 2.
- The source address and destination address of the tunnel interface are 2.2.2.2 and 1.1.1.1, respectively.



```
[SwitchB] interface tunnel 2 mode vxlan
[SwitchB-Tunnel2] source 2.2.2.2
[SwitchB-Tunnel2] destination 1.1.1.1
[SwitchB-Tunnel2] quit
Create a VXLAN tunnel to Switch C.

- The tunnel interface name is Tunnel 3.
- The source address and destination address of the tunnel interface are 2.2.2.2 and 3.3.3.3, respectively.


```
[SwitchB] interface tunnel 3 mode vxlan
[SwitchB-Tunnel3] source 2.2.2.2
[SwitchB-Tunnel3] destination 3.3.3.3
```


```


```

```
[SwitchB-Tunnel3] quit
# Assign Tunnel 2 and Tunnel 3 to VXLAN 10.
[SwitchB] vsi vpna
[SwitchB-vsi-vpna] vxlan 10
[SwitchB-vsi-vpna-vxlan-10] tunnel 2
[SwitchB-vsi-vpna-vxlan-10] tunnel 3
[SwitchB-vsi-vpna-vxlan-10] quit
[SwitchB-vsi-vpna] quit
# On GigabitEthernet 1/0/1, create Ethernet service instance 1000 to match VLAN 2.
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] service-instance 1000
[SwitchB-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 2
# Map Ethernet service instance 1000 to VSI vpna.
[SwitchB-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna
[SwitchB-GigabitEthernet1/0/1-srv1000] quit
[SwitchB-GigabitEthernet1/0/1] quit
```

5. スイッチCを設定します。#L2VPNを有効にします。

```
<SwitchC> system-view
[SwitchC] l2vpn enable
# Enable Layer 2 forwarding for VXLANs.
[SwitchC] undo vxlan ip-forwarding
# Create a VSI named vpna, and create VXLAN 10.
[SwitchC] vsi vpna
[SwitchC-vsi-vpna] vxlan 10
[SwitchC-vsi-vpna-vxlan-10] quit
[SwitchC-vsi-vpna] quit
# Enable the MLD snooping feature.
[SwitchB] mld-snooping
[SwitchB -mld-snooping] quit
# Enable MLD snooping for VSI vpna.
[SwitchC] vsi vpna
[SwitchC-vsi-vpna] mld-snooping enable
# Enable dropping unknown IPv6 multicast data packets for VSI vpna.
[SwitchC-vsi-vpna] mld-snooping drop-unknown
# Specify FE80::3 as the source IPv6 address of MLD general queries in VSI vpna.
[SwitchC-vsi-vpna] mld-snooping general-query source-ip fe80::3
# Enable the MLD snooping querier for VSI vpna.
[SwitchC-vsi-vpna] mld-snooping querier
[SwitchC-vsi-vpna] quit
# Assign an IP address to Loopback 0. This address will be used as the source address of
the VXLAN tunnels to Switch A and Switch B.
[SwitchC] interface loopback 0
[SwitchC-Loopback0] ip address 3.3.3.3 255.255.255.255
[SwitchC-Loopback0] quit
# Create a VXLAN tunnel to Switch A.
```

- The tunnel interface name is **Tunnel 1**.
- The source address and destination address of the tunnel interface are 3.3.3.3 and 1.1.1.1, respectively.

```
[SwitchC] interface tunnel 1 mode vxlan
```

```
[SwitchC-Tunnel1] source 3.3.3.3
```

```
[SwitchC-Tunnel1] destination 1.1.1.1
```

```
[SwitchC-Tunnel1] quit
```

Create a VXLAN tunnel to Switch B.

- The tunnel interface name is **Tunnel 3**.
- The source address and destination address of the tunnel interface are 3.3.3.3 and 2.2.2.2, respectively.

```
[SwitchC] interface tunnel 3 mode vxlan
```

```
[SwitchC-Tunnel3] source 3.3.3.3
```

```
[SwitchC-Tunnel3] destination 2.2.2.2
```

```
[SwitchC-Tunnel3] quit
```

Assign Tunnel 1 and Tunnel 3 to VXLAN 10.

```
[SwitchC] vsi vpna
```

```
[SwitchC-vsi-vpna] vxlan 10
```

```
[SwitchC-vsi-vpna-vxlan-10] tunnel 1
```

```
[SwitchC-vsi-vpna-vxlan-10] tunnel 3
```

```
[SwitchC-vsi-vpna-vxlan-10] quit
```

```
[SwitchC-vsi-vpna] quit
```

On GigabitEthernet 1/0/1, create Ethernet service instance 1000 to map VLAN 2.

```
[SwitchC] interface gigabitethernet 1/0/1
```

```
[SwitchC-GigabitEthernet1/0/1] service-instance 1000
```

```
[SwitchC-GigabitEthernet1/0/1-srv1000] encapsulation s-vid 2
```

Map Ethernet service instance 1000 to VSI **vpna**.

```
[SwitchC-GigabitEthernet1/0/1-srv1000] xconnect vsi vpna
```

```
[SwitchC-GigabitEthernet1/0/1-srv1000] quit
```

```
[SwitchC-GigabitEthernet1/0/1] quit
```

設定の確認

#スイッチA上のVSI vpnaのダイナミックルータポート情報を表示します。

```
[SwitchA] display mld-snooping router-port vsi vpna
```

VSI vpna:

Router ports (1 in total):

Tun2 (VXLAN ID 10) (00:04:17)

#スイッチB上のVSI vpnaのダイナミックルータポート情報を表示します。

```
[SwitchB] display mld-snooping router-port vsi vpna
```

VSI vpna:

Router ports (1 in total):

Tun3 (VXLAN ID 10) (00:04:07)

MLDスヌーピングのトラブルシューティング

レイヤ2マルチキャストフォワーディングが機能しない

症状

レイヤ2マルチキャストフォワーディングは、MLDスヌーピングを介して機能できません。

解決方法

この問題を解決するには、次の手順を実行し

1. MLDスヌーピングステータスを表示するには、**display mld-snooping**コマンドを使用します。
2. MLDスヌーピングが有効でない場合は、システムビューで**mld-snooping**コマンドを使用して、MLDスヌーピング機能を有効にします。次に、VLANビューまたはVSIビューで**mld-snooping enable**コマンドを使用して、VLANまたはVSIのMLDスヌーピングを有効にします。
3. MLDスヌーピングがグローバルに有効になっていて、VLANまたはVSIに対して有効になっていない場合は
VLANまたはVSIのMLDスヌーピングを有効にするには、VLANビューまたはVSIビューで**mld-snooping enable**コマンドを使用します。
4. 問題が解決しない場合は、H3Cサポートに連絡してください。

IPv6マルチキャストグループポリシーが機能しない

症状

ホストは、IPv6マルチキャストグループポリシーで許可されていないIPv6マルチキャストグループのIPv6マルチキャストデータを受信できます。

解決方法

この問題を解決するには、次の手順を実行し

1. 設定されたipv6 ACLがipv6マルチキャストグループポリシー要件を満たしていることを確認するには、**display acl ipv6**コマンドを使用します。
2. 正しいIPv6マルチキャストグループポリシーが適用されたことを確認するには、MLDスヌーピングビューまたはインターフェイスビューで**display this**コマンドを使用します。適用されたポリシーが正しくない場合は、**group-policy**または **group-policy**コマンドを使用して、正しいIPv6マルチキャストグループポリシーを適用します。
3. 不明なIPv6マルチキャストデータのドロップが有効であることを確認するには、**display mld-snooping**コマンドを使用します。そうでない場合は、**mld-snooping drop-unknown**コマンドを使用して、不明なIPv6マルチキャストデータのドロップを有効にします。
4. 問題が解決しない場合は、H3Cサポートに連絡してください。

IPv6 PIMスヌーピングの設定

IPv6 PIMスヌーピングの概要

IPv6 PIMスヌーピングはレイヤ2デバイス上で動作します。MLDスヌーピングとともに動作して、受信したIPv6 PIMメッセージを分析し、特定のマルチキャストデータに関するポートをIPv6 PIMスヌーピングルーティングエントリに追加します。このようにして、マルチキャストデータは、そのデータに関するポートだけに転送できます。

図68 IPv6 PIMスヌーピングを使用した、または使用しないマルチキャストパケット送信

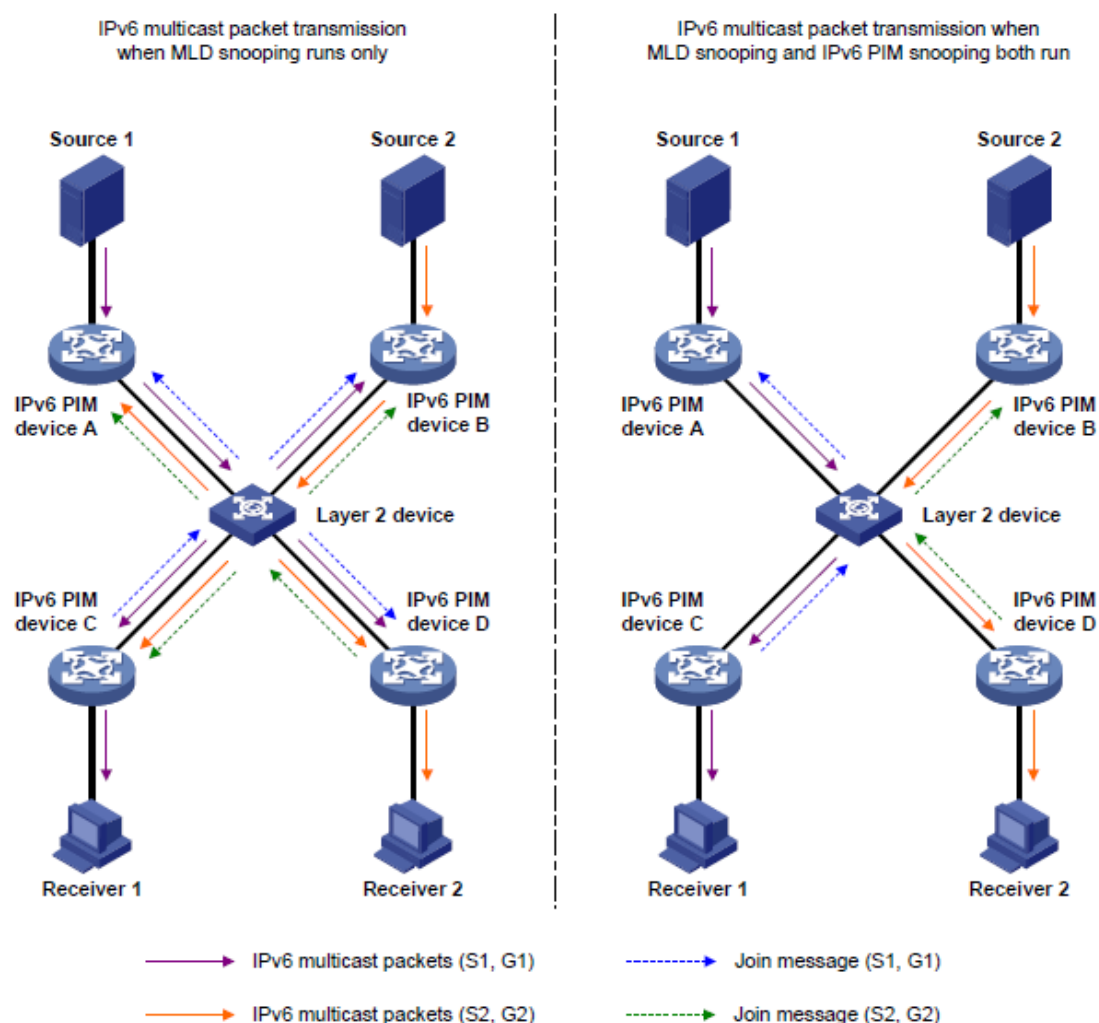


図68に示すように、送信元1はマルチキャストグループG1にマルチキャストデータを送信し、送信元2はマルチキャストグループG2にマルチキャストデータを送信します。レシーバ1はG1に属し、レシーバ2はG2に属します。IPv6 PIM対応ルータに接続するレイヤ2スイッチのインターフェイスは、同じVLAN内にあります。

- レイヤ2スイッチがMLDスヌーピングのみを実行する時、次のアクションを実行します。

- a. IPv6 PIM対応ルータが送信する受信IPv6 PIM helloメッセージに従って、ルータポートを維持します。
 - b. VLAN内のPIM helloメッセージを除く、受信した他のすべてのタイプのIPv6 PIMメッセージをフラッディングします。
 - c. すべてのマルチキャストデータをVLAN内のすべてのルータポートに転送します。
VLAN内の各IPv6 PIM対応ルータは、マルチキャストデータに関係するかどうかに関係なく、すべてのマルチキャストデータと、IPv6 PIM helloメッセージを除くすべてのIPv6 PIMメッセージを受信できます。
- レイヤ2スイッチがMLDスヌーピングとIPv6 PIMスヌーピングの両方を実行する時、次のアクションを実行します。
 - a. ルータが送信する受信IPv6 PIMメッセージに従って、IPv6 PIMルータがマルチキャストグループ宛てのマルチキャストデータに関心があるかどうかを調べます。
 - b. ルータに接続され、データに関係するポートだけをIPv6 PIMスヌーピングルーティングエントリに追加します。
 - c. マルチキャスト転送エントリに従って、IPv6 PIMメッセージおよびマルチキャストデータだけをルータに転送します。これにより、ネットワーク帯域幅が節約されます。

MLDスヌーピングおよびルータポートの詳細については、「MLDスヌーピングの設定」を参照してください。

IPv6 PIMスヌーピングは、IPv6 PIM-SMおよびIPv6 PIM-SSMネットワークで実行できます。IPv6 PIM-DMまたはIPv6 BIDIR-PIMネットワークでは、IPv6 PIMスヌーピングを設定しないでください。IPv6 PIMの詳細については、「IPv6 PIMの設定」を参照してください。

制約事項および注意事項:IPv6 PIMスヌーピング設定

ベストプラクティスとして、セカンダリVLANにはIPv6 PIMスヌーピングを設定しないでください。IPv6 PIMスヌーピングはセカンダリVLANでは有効になりません。セカンダリVLANの詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

IPv6 PIM join/pruneメッセージの最大サイズが、IPv6 PIMスヌーピングデバイスに接続されているデバイスのパスMTUよりも小さいことを確認してください。そうでない場合、フラグメント化されたIPv6 PIM join/pruneメッセージは、IPv6 PIMスヌーピングがIPv6マルチキャストデータを正しく転送することを妨げます。join/pruneメッセージの最大サイズの設定の詳細については、「IPv6 PIMの設定」を参照してください。

VLANでIPv6 PIMスヌーピングを有効にすると、IPv6 PIMスヌーピングはそのVLANに属するポートだけで有効になります。

IPv6 PIMスヌーピングタスクの概要

IPv6 PIMスヌーピングを設定するには、次の作業を実行します。

1. IPv6 PIMスヌーピングの有効化
2. (任意)マスター/下位スイッチオーバー後のグローバルポートのエージングタイムの設定
 - グローバルネイバーポートのエージングタイムの設定
 - グローバルダウンストリームポートおよびグローバルルータポートのエージングタイムの設定

IPv6 PIMスヌーピングの有効化

1. システムビューに入ります。
system-view
2. MLDスヌーピング機能を有効にし、MLDスヌーピングビューを開始します。
mld-snooping
デフォルトでは、MLDスヌーピングは無効です。
このコマンドの詳細については、『IP Multicast Command Reference』を参照してください。
3. システムビューに戻ります。
quit
4. VLANビューを開始します。
vlan *vlan-id*
5. VLANのMLDスヌーピングを有効にします。
mld-snooping enable
デフォルトでは、VLANのMLDスヌーピングは無効です。
このコマンドの詳細については、『IP Multicast Command Reference』を参照してください。
6. VLANのIPv6 PIMスヌーピングを有効にします。
ipv6 pim-snooping enable
デフォルトでは、IPv6 PIMスヌーピングはVLANで無効になっています。

マスター/下位スイッチオーバー後のグローバルポートのエージングタイムの設定

グローバルポートについて

グローバルポートは、レイヤ2集約インターフェイスなどのマスターデバイス上の仮想ポートです。ネイバーポート、ダウンストリームポート、またはルータポートとして動作するグローバルポートは、それぞれグローバルネイバーポート、グローバルダウンストリームポート、およびグローバルルータポートと呼ばれます。

マスター/下位スイッチオーバー後のIPv6 PIMスヌーピングエントリのエージングによって発生するレイヤ2 IPv6マルチキャストデータの中断を減らすには、次の作業を実行します。

制約事項とガイドライン

グローバルネイバーポートの場合、マスター/下位スイッチオーバー後にポートがIPv6 PIM helloメッセージを受信しても、設定されたエージングタイムは有効になりません。ポートのエージングタイムは、IPv6 PIM helloメッセージのエージングタイムによって決まります。

グローバルルータポートまたはグローバルダウンストリームポートの場合、設定されたエージングタイムは、マスター/下位スイッチオーバー後にポートがIPv6 PIM Joinメッセージを受信したときには有効になりません。ポートのエージングタイムは、IPv6 PIM Joinメッセージのエージングタイムによって決まります。

グローバルネイバーポートのエージングタイムの設定

1. システムビューに入ります。

system-view

2. VLANビューを開始します。

vlan *vlan-id*

3. マスター/下位スイッチオーバー後のグローバルネイバーポートのエージングタイムを設定します。

pim-snooping graceful-restart neighbor-aging-time *seconds*

デフォルトでは、マスター/下位スイッチオーバー後のグローバルネイバーポートのエージングタイムは105秒です。

グローバルダウンストリームポートおよびグローバルルータポートのエージングタイムの設定

1. システムビューに入ります。

system-view

2. VLANビューを開始します。

vlan *vlan-id*

3. マスター/下位スイッチオーバー後のグローバルダウンストリームポートおよびグローバルルータポートのエージングタイムを設定します。

pim-snooping graceful-restart join-aging-time *seconds*

デフォルトでは、マスター/下位スイッチオーバー後のダウンストリームポートおよびグローバルルータポートのエージングタイムは210秒です。

IPv6 PIMスヌーピングの表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
IPv6 PIMスヌーピングネイバー情報を表示します。	display ipv6 pim-snooping neighbor [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [verbose]
IPv6 PIMスヌーピングルータポート情報を表示します。	display ipv6 pim-snooping router-port [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [verbose]
IPv6 PIMスヌーピングルーティングエントリを表示します。	display ipv6 pim-snooping routing-table [vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [verbose]
IPv6 PIMスヌーピングによって学習されたIPv6 PIMメッセージの統計情報を表示します。	display ipv6 pim-snooping statistics
IPv6 PIMスヌーピングによって学習されたIPv6 PIMメッセージの統計情報をクリアします。	reset ipv6 pim-snooping statistics

IPv6 PIMスヌーピングの設定例

例:IPv6 PIMスヌーピングの設定

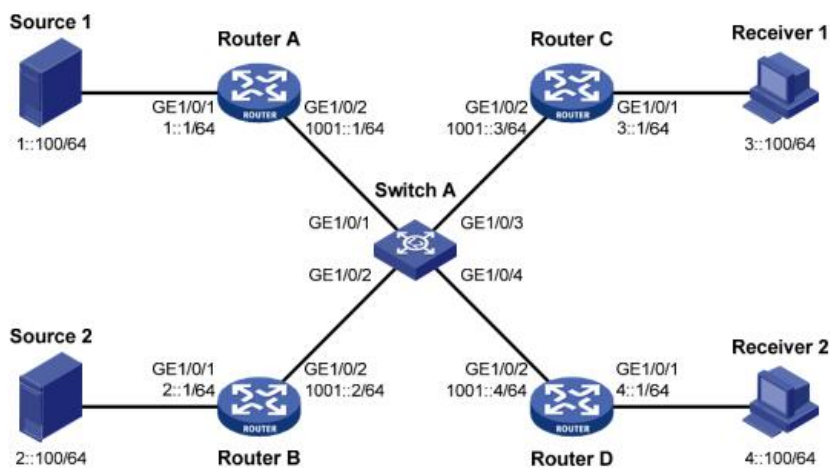
ネットワークの設定

図69に示します。

- OSPFv3はネットワーク上で動作します。
- 送信元1と送信元2は、それぞれIPv6マルチキャストグループFF1E::101とFF2E::101にIPv6マルチキャストデータを送信します。
- Receiver 1とReceiver 2は、それぞれIPv6マルチキャストグループFF1E::101とFF2E::101に属しています。
- ルータCおよびルータDは、GigabitEthernet 1/0/1上でMLDを実行します。
- ルータA、ルータB、ルータC、およびルータDは、IPv6 PIM-SMを実行しています。ルータAのGigabitEthernet 1/0/2は、C-BSRおよびC-RPとして動作します。

スイッチAでMLDスヌーピングおよびIPv6 PIMスヌーピングを設定します。次に、スイッチAは、レシーバに接続されたルータだけにIPv6 PIMプロトコルパケットおよびIPv6マルチキャストデータパケットを転送します。

図69 ネットワークダイアグラム



手順

1. 図69に示すように、各インターフェイスにIPv6アドレスとプレフィクス長を割り当てます。(詳細は省略)
2. ルータにOSPFv3を設定します(詳細は省略)。
3. ルータAを設定します。

#IPv6マルチキャストルーティングを有効にします。

```
<RouterA> system-view
```

```
[RouterA] ipv6 multicast routing
```

```
[RouterA-mrib6] quit
# Enable IPv6 PIM-SM on each interface.
[RouterA] interface gigabitethernet 1/0/1
[RouterA-GigabitEthernet1/0/1] ipv6 pim sm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface gigabitethernet 1/0/2
[RouterA-GigabitEthernet1/0/2] ipv6 pim sm
[RouterA-GigabitEthernet1/0/2] quit
# Configure GigabitEthernet 1/0/2 as a C-BSR and a C-RP.
[RouterA] ipv6 pim
[RouterA-pim6] c-bsr 1001::1
[RouterA-pim6] c-rp 1001::1
[RouterA-pim6] quit
```

4. ルータBを設定します。

#IPv6マルチキャストルーティングを有効にします。

```
<RouterB> system-view
[RouterB] ipv6 multicast routing
[RouterB-mrib6] quit
# Enable IPv6 PIM-SM on each interface.
[RouterB] interface gigabitethernet 1/0/1
[RouterB-GigabitEthernet1/0/1] ipv6 pim sm
[RouterB-GigabitEthernet1/0/1] quit
[RouterB] interface gigabitethernet 1/0/2
[RouterB-GigabitEthernet1/0/2] ipv6 pim sm
[RouterB-GigabitEthernet1/0/2] quit
```

5. ルータCを設定します。

#IPv6マルチキャストルーティングを有効にします。

```
<RouterC> system-view
[RouterC] ipv6 multicast routing
[RouterC-mrib6] quit
# Enable MLD on GigabitEthernet 1/0/1.
[RouterC] interface gigabitethernet 1/0/1
[RouterC-GigabitEthernet1/0/1] mld enable
[RouterC-GigabitEthernet1/0/1] quit
# Enable IPv6 PIM-SM on GigabitEthernet 1/0/2.
[RouterC] interface gigabitethernet 1/0/2
[RouterC-GigabitEthernet1/0/2] ipv6 pim sm
[RouterC-GigabitEthernet1/0/2] quit
```

6. ルータDを設定します。

#IPv6マルチキャストルーティングを有効にします。

```
<RouterD> system-view
[RouterD] ipv6 multicast routing
[RouterD-mrib6] quit
# Enable MLD on GigabitEthernet 1/0/1.
```

```
[RouterD] interface gigabitethernet 1/0/1
[RouterD-GigabitEthernet1/0/1] mld enable
[RouterD-GigabitEthernet1/0/1] quit
# Enable IPv6 PIM-SM on GigabitEthernet 1/0/2.
[RouterD] interface gigabitethernet 1/0/2
[RouterD-GigabitEthernet1/0/2] ipv6 pim sm
[RouterD-GigabitEthernet1/0/2] quit
```

7. スイッチAを設定します。

```
#MLDスヌーピング機能を有効にします。
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
# Create VLAN 100, and assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/4 to the
VLAN.
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
# Enable MLD snooping and IPv6 PIM snooping for VLAN 100.
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] ipv6 pim-snooping enable
[SwitchA-vlan100] quit
```

設定の確認

#スイッチAで、VLAN 100のIPv6 PIMスヌーピングネイバー情報を表示します。

```
[SwitchA] display ipv6 pim-snooping neighbor vlan 100
Total 4 neighbors.
```

VLAN 100: Total 4 neighbors.

```
FE80::1
  Ports (1 in total):
    GE1/0/1                (00:32:43)
FE80::2
  Ports (1 in total):
    GE1/0/2                (00:32:43)
FE80::3
  Ports (1 in total):
    GE1/0/3                (00:32:43)
FE80::4
  Ports (1 in total):
    GE1/0/4                (00:32:43)
```

この出力は、ルータA、ルータB、ルータC、およびルータDがIPv6 PIMスヌーピングネイバーであることを示しています。

#スイッチAで、VLAN 100のIPv6 PIMスヌーピングルーティングエントリを表示します。

```
[SwitchA] display ipv6 pim-snooping routing-table vlan 100
Total 2 entries.
FSM flag: NI-no info, J-join, PP-prune pending
```

VLAN 100: Total 2 entries.

(*, FF1E::101)

Upstream neighbor: FE80::1

Upstream ports (1 in total):

GE1/0/1

Downstream ports (1 in total):

GE1/0/3

Expires: 00:03:01, FSM: J

(*, FF2E::101)

Upstream neighbor: FE80::2

Upstream ports (1 in total):

GE1/0/2

Downstream ports (1 in total):

GE1/0/4

Expires: 00:03:01, FSM: J

出力には次の情報が表示されます。

- スイッチAは、IPv6マルチキャストグループFF1E::101宛てのマルチキャストデータをルータCだけに転送します。
- スイッチAは、IPv6マルチキャストグループFF2E::101宛てのマルチキャストデータをルータDだけに転送します。

IPv6 PIMスヌーピングのトラブルシューティング

ここでは、IPv6 PIMスヌーピングの一般的な問題とそのトラブルシューティング方法について説明します。

IPv6 PIMスヌーピングがレイヤ2デバイスで動作しない

症状

IPv6 PIMスヌーピングは、レイヤ2デバイスでは動作しません。

解決方法

この問題を解決するには、次の手順を実行し

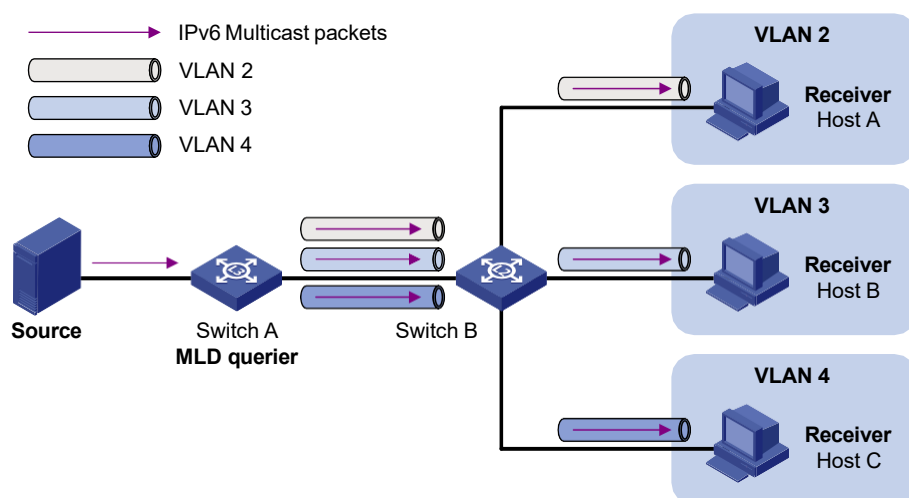
1. MLDスヌーピングおよびIPv6 PIMスヌーピングに関する情報を表示するには、display current-configurationコマンドを使用します。
2. MLDスヌーピングが有効でない場合は、MLDスヌーピング機能を有効にしてから、VLANのMLDスヌーピングおよびIPv6 PIMスヌーピングを有効にします。
3. IPv6 PIMスヌーピングが有効でない場合は、VLANのIPv6 PIMスヌーピングを有効にします。
4. 問題が解決しない場合は、H3Cサポートに連絡してください。

IPv6マルチキャストVLANの設定

IPv6マルチキャストVLAN機能

図70に示すように、ホストA、ホストB、およびホストCは異なるVLANにあり、同じIPv6マルチキャストグループに属しています。スイッチA(レイヤ3デバイス)は、そのグループのIPv6マルチキャストデータを受信すると、データの3つのコピーをスイッチB(レイヤ2デバイス)に転送します。これは大量の帯域幅を占有し、レイヤ3デバイスの負荷を増加させます。

図70 IPv6マルチキャストVLAN機能を使用しないマルチキャスト送信



IPv6マルチキャストVLANがスイッチBに設定されると、スイッチAはIPv6マルチキャストデータの1つのコピーをスイッチBのIPv6マルチキャストVLANに送信します。これにより、ネットワーク帯域幅が節約され、レイヤ3デバイスの負荷が軽減されます。

IPv6マルチキャストVLAN方式

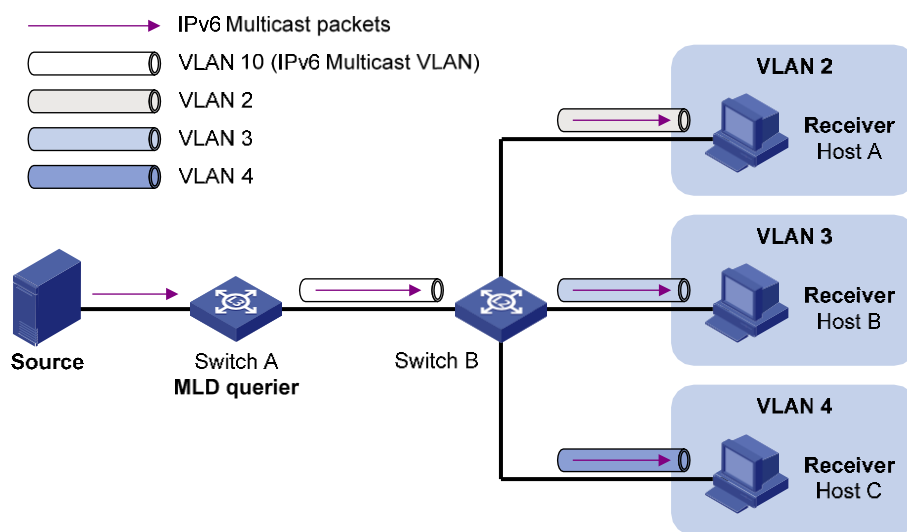
IPv6マルチキャストVLANは、サブVLANベースのIPv6マルチキャストVLANおよびポートベースのIPv6マルチキャストVLANをサポートします。

サブVLANベースのIPv6マルチキャストVLAN

図71に示します。

- ホストA、ホストB、およびホストCは、それぞれVLAN 2～VLAN 4にあります。
- スイッチBでは、VLAN 10はIPv6マルチキャストVLANです。VLAN 2～VLAN 4は、VLAN 10のサブVLANです。
- MLDスヌーピングは、マルチキャストVLANおよびそのサブVLANに対して有効です。

図71 サブVLANベースのマルチキャストVLAN



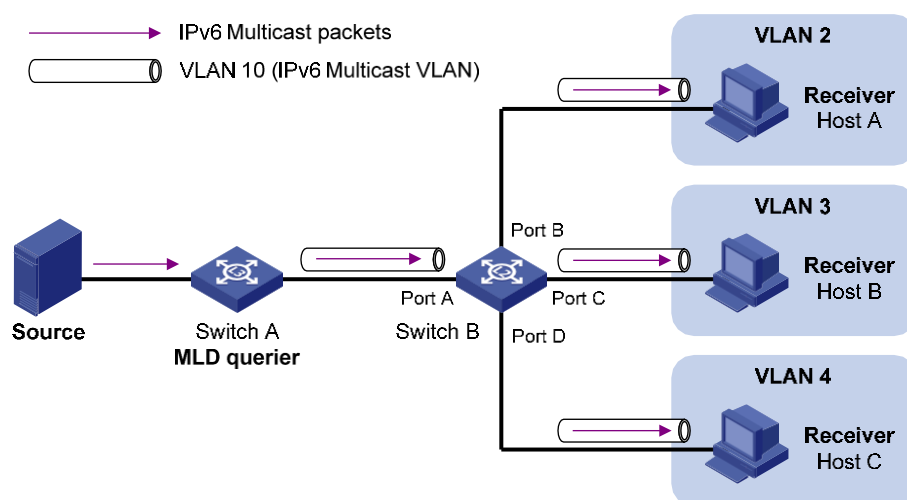
MLDスヌーピングは、IPv6マルチキャストVLANのルータポートおよび各サブVLANのメンバーポートを管理します。スイッチAは、IPv6マルチキャスト送信元からIPv6マルチキャストデータを受信すると、IPv6マルチキャストデータの1つのコピーだけをスイッチBのIPv6マルチキャストVLANに送信します。次に、スイッチBはIPv6マルチキャストVLANの各サブVLANに個別のコピーを送信します。

ポートベースのIPv6マルチキャストVLAN

図72に示します。

- ホストA、ホストB、およびホストCは、それぞれVLAN 2～VLAN 4内にあります。スイッチBのすべてのユーザーポート(ホストが接続されたポート)はハイブリッドポートです。
- スイッチBでは、VLAN 10はIPv6マルチキャストVLANです。すべてのユーザーポートはVLAN 10に割り当てられます。
- MLDスヌーピングは、IPv6マルチキャストVLANおよびそのサブVLANに対して有効です。

図72 ポートベースIPv6マルチキャストVLAN



MLDスヌーピングは、IPv6マルチキャストVLANのルータポートおよびメンバーポートを管理します。スイッチAは、IPv6マルチキャスト送信元からIPv6マルチキャストデータを受信すると、IPv6マルチキャストデータの1つのコピーだけをスイッチBのIPv6マルチキャストVLANに送信します。次に、スイッチBはIPv6マルチキャストVLANの各ユーザーポートに個別のコピーを送信します。

制約事項および注意事項:IPv6マルチキャストVLAN設定

IPv6マルチキャストVLANとして設定されるVLANが存在する必要があります。

デバイスにサブVLANベースIPv6マルチキャストVLANとポートベースIPv6マルチキャストVLANの両方を設定した場合、ポートベースIPv6マルチキャストVLAN設定が有効になります。

IPv6マルチキャストルーティングが有効になっているデバイスでは、IPv6マルチキャストVLANを設定しないでください。設定した場合、エラーが表示されます。IPv6マルチキャストVLANが設定されているデバイスでは、IPv6マルチキャストルーティングを有効にしないでください。有効にしないと、IPv6マルチキャスト転送例外が発生します。

VLANインターフェイスでIPv6 PIMまたはMLDが有効になっている場合は、VLANをIPv6マルチキャストVLANまたはIPv6サブVLANとして設定しないでください。設定すると、エラーが表示されます。VLANインターフェイスがIPv6マルチキャストVLANまたはIPv6マルチキャストサブVLANに属する場合は、VLANインターフェイスでIPv6 PIMまたはMLDを有効にしないでください。有効にしないと、IPv6マルチキャスト転送例外が発生します。

IPv6マルチキャストVLAN機能は、セカンダリVLANでは有効になりません。ベストプラクティスとして、セカンダリVLANにはIPv6マルチキャストVLAN機能を設定しないでください。セカンダリVLANの詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

サブVLANベースのIPv6マルチキャストVLANの設定

制約事項とガイドライン

IPv6マルチキャストVLANのサブVLANとして設定されるVLANが存在する必要があります。IPv6マルチキャストVLANまたは他のIPv6マルチキャストVLANのサブVLANは設定できません。

必要条件

サブVLANベースのIPv6マルチキャストVLANを設定する前に、次の作業を完了する必要があります。

- 必要に応じてVLANを作成します。
- VLANをIPv6マルチキャストVLANとして設定し、VLANをサブVLANとして設定するには、MLDスヌーピングを有効にします。

手順

1. システムビューに入ります。

system-view

2. IPv6マルチキャストVLANとしてVLANを設定し、IPv6マルチキャストVLANビューを開始します。

ipv6 multicast-vlan *vlan-id*

デフォルトでは、VLANはIPv6マルチキャストVLANではありません。

3. VLANをサブVLANとしてIPv6マルチキャストVLANに割り当てます。

subvlan *vlan-list*

デフォルトでは、IPv6マルチキャストVLANにはサブVLANはありません。

ポートベースIPv6マルチキャストVLANの設定

制約事項とガイドライン

IPv6マルチキャストVLANビューでIPv6マルチキャストVLANにユーザーポートを割り当てるか、またはインターフェイスビューでIPv6マルチキャストVLANにユーザーポートを割り当てることができます。

ユーザーポートは、1つのIPv6マルチキャストVLANだけに属することができます。

必要条件

ポートベースIPv6マルチキャストVLANを設定する前に、次の作業を完了する必要があります。

- 必要に応じてVLANを作成します。
- IPv6マルチキャストVLANとして設定するVLANのMLDスヌーピングを有効にします。
- マルチキャストレシーバを含むすべてのVLANに対してMLDスヌーピングを有効にします。
- ユーザーポートの属性を設定します。ポートが、IPv6マルチキャストVLANとして設定されるVLANからのパケットを転送でき、VLANタグが削除されたパケットを送信できることを確認します。ポート属性の設定の詳細については、『Layer 2 LAN Switching Configuration Guide』の「VLAN configuration」を参照してください。

IPv6マルチキャストVLANビューでのIPv6マルチキャストVLANへのユーザーポートの割り当て

1. システムビューに入ります。

system-view

2. IPv6 VLANをIPv6マルチキャストVLANとして設定し、IPv6マルチキャストVLANビューを開始します。

ipv6 multicast-vlan *vlan-id*

デフォルトでは、VLANはIPv6マルチキャストVLANではありません。

3. IPv6マルチキャストVLANにユーザーポートとしてポートを割り当てます。

port *interface-list*

インターフェイスビューでのIPv6マルチキャストVLANへのユーザーポートの割り当て

1. システムビューに入ります。

system-view

2. IPv6 VLANをIPv6マルチキャストVLANとして設定し、IPv6マルチキャストVLANビューを開始します。

ipv6 multicast-vlan *vlan-id*

デフォルトでは、VLANはIPv6マルチキャストVLANではありません。

3. システムビューに戻ります。

quit

4. レイヤ2インターフェイスビューを開始します。

- レイヤ2イーサネットインターフェイスビューを開始します。

interface*interface-type interface-number*

- レイヤ2集約インターフェイスビューを開始します。

interface bridge-aggregation interface-number

5. IPv6マルチキャストVLANにポートをユーザーポートとして割り当てます。

ipv6 port multicast-vlan vlan-id

デフォルトでは、ポートはどのIPv6マルチキャストVLANにも属しません。

IPv6マルチキャストVLANフォワーディングエントリの最大数の設定

IPv6マルチキャストVLANフォワーディングエントリの最大数の設定について

デバイス上のIPv6マルチキャストVLANフォワーディングエントリの最大数を設定できます。上限に達すると、一部のエントリが期限切れになるか、手動で削除されるまで、デバイスはIPv6マルチキャストVLANフォワーディングエントリを作成しません。

手順

1. システムビューに入ります。

system-view

2. IPv6マルチキャストVLAN転送エントリの最大数を設定します。

ipv6 multicast-vlan entry-limit limit

デフォルトでは、IPv6マルチキャストVLAN転送エントリの最大数は4000です。

IPv6マルチキャストVLANの表示およびメンテナンス コマンド

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
IPv6マルチキャストVLANに関する情報を表示します。	display ipv6 multicast-vlan [<i>vlan-id</i>]
IPv6マルチキャストVLANフォワーディングエントリを表示します。	display ipv6 multicast-vlan forwarding-table [<i>ipv6-source-address</i> [<i>prefix-length</i>] <i>ipv6-group-address</i> [<i>prefix-length</i>] slot <i>slot-number</i> subvlan <i>vlan-id</i> vlan <i>vlan-id</i>] *
IPv6マルチキャストVLAN内のIPv6マルチキャストグループエントリに関する情報	display ipv6 multicast-vlan group [<i>ipv6-source-address</i> <i>ipv6-group-address</i>

を表示します。	slot <i>slot-number</i> verbose vlan <i>vlan-id</i>] *
IPv6マルチキャストVLANのIPv6マルチキャストグループエントリをクリアします。	reset ipv6 multicast-vlan group [<i>ipv6-group-address</i> [<i>prefix-length</i>] <i>ipv6-source-address</i> [<i>prefix-length</i>] vlan <i>vlan-id</i>] *

IPv6マルチキャストVLANの設定例

例:サブVLANベースのIPv6マルチキャストVLANの設定

ネットワークの設定

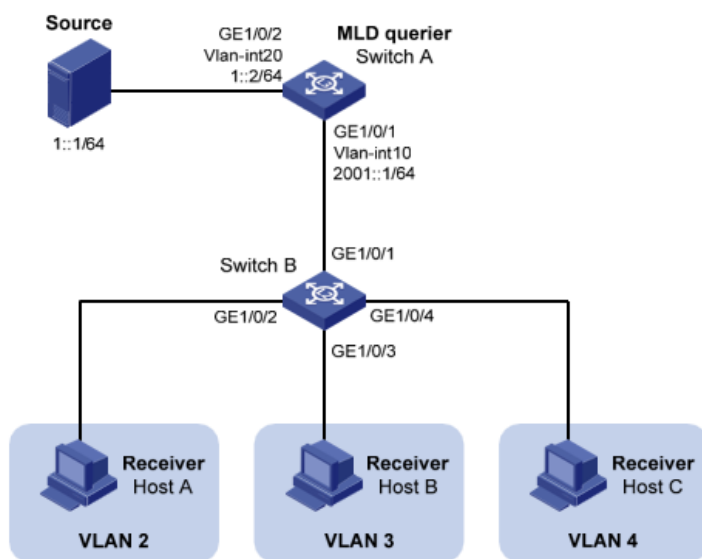
図73に示します。

- レイヤ3デバイスのスイッチAはMLDを実行し、MLDクエリアとして動作します。レイヤ2デバイスのスイッチBはMLDv1スヌーピングを実行します。
- IPv6マルチキャスト送信元は、IPv6マルチキャストデータをIPv6マルチキャストグループ FF1E::101に送信します。レシーバHost A、Host B、およびHost Cは、それぞれVLAN 2、VLAN 3、およびVLAN 4に属します。

次の要件を満たすように、スイッチBにサブVLANベースのIPv6マルチキャストVLANを設定します。

- スイッチAは、IPv6マルチキャストVLAN経由でIPv6マルチキャストデータをスイッチBに送信します。
- スイッチBは、IPv6マルチキャストデータを異なるユーザーVLANのレシーバに転送します。

図73 ネットワークダイアグラム



手順

1. スイッチAを設定します。

```
# Enable IPv6 multicast routing.
```

```
<SwitchA> system-view
```

```
[SwitchA] ipv6 multicast routing
```

```
[SwitchA-mrib6] quit
```

```
# Create VLAN 20, and assign GigabitEthernet 1/0/2 to the VLAN.
```

```
[SwitchA] vlan 20
```

```
[SwitchA-vlan20] port gigabitethernet 1/0/2
```

```
[SwitchA-vlan20] quit
```

```
# Assign an IPv6 address to VLAN-interface 20, and enable IPv6 PIM-DM on the interface.
```

```
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ipv6 address 1::2 64
[SwitchA-Vlan-interface20] ipv6 pim dm
[SwitchA-Vlan-interface20] quit
# Create VLAN 10.
[SwitchA] vlan 10
[SwitchA-vlan10] quit
# Configure GigabitEthernet 1/0/1 as a hybrid port, and assign the port to VLAN 10 as a tagged
VLAN member.
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type hybrid
[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 10 tagged
[SwitchA-GigabitEthernet1/0/1] quit
# Assign an IPv6 address to VLAN-interface 10, and enable MLD on the interface.
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ipv6 address 2001::1 64
[SwitchA-Vlan-interface10] mld enable
[SwitchA-Vlan-interface10] quit
```

2. スイッチBを構成します。

```
# Enable the MLD snooping feature.
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
# Create VLAN 2, assign GigabitEthernet 1/0/2 to the VLAN, and enable MLD snooping for the
VLAN.
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/2
[SwitchB-vlan2] mld-snooping enable
[SwitchB-vlan2] quit
# Create VLAN 3, assign GigabitEthernet 1/0/3 to the VLAN, and enable MLD snooping for the
VLAN.
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/3
[SwitchB-vlan3] mld-snooping enable
[SwitchB-vlan3] quit
# Create VLAN 4, assign GigabitEthernet 1/0/4 to the VLAN, and enable MLD snooping for the
VLAN.
[SwitchB] vlan 4
[SwitchB-vlan4] port gigabitethernet 1/0/4
[SwitchB-vlan4] mld-snooping enable
[SwitchB-vlan4] quit
# Create VLAN 10, and enable MLD snooping for the VLAN.
[SwitchB] vlan 10
[SwitchB-vlan10] mld-snooping enable
[SwitchB-vlan10] quit
```


Configure GigabitEthernet 1/0/1 as a hybrid port, and assign the port to VLAN 10 as a tagged VLAN member.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type hybrid
[SwitchB-GigabitEthernet1/0/1] port hybrid vlan 10 tagged
[SwitchB-GigabitEthernet1/0/1] quit
```

Configure VLAN 10 as an IPv6 multicast VLAN, and assign VLAN 2 through VLAN 4 as sub-VLANs to multicast VLAN 10.

```
[SwitchB] ipv6 multicast-vlan 10
[SwitchB-ipv6-mvlan-10] subvlan 2 to 4
[SwitchB-ipv6-mvlan-10] quit
```

設定の確認

#スイッチB上のすべてのIPv6マルチキャストVLANに関する情報を表示します。

```
[SwitchB] display ipv6 multicast-vlan
Total 1 IPv6 multicast VLANs.
```

```
IPv6 multicast VLAN 10:
  Sub-VLAN list(3 in total):
    2-4
  Port list(0 in total):
```

#スイッチB上のIPv6マルチキャストVLAN内のIPv6マルチキャストグループに関する情報を表示します。

```
[SwitchB] display ipv6 multicast-vlan group
Total 1 entries.
```

```
IPv6 multicast VLAN 10: Total 1 entries.
  (::, FF1E::101)
  Sub-VLANs (3 in total):
    VLAN 2
    VLAN 3
    VLAN 4
```

この出力は、IPv6マルチキャストグループFF1E::101がIPv6マルチキャストVLAN 10に属していることを示しています。IPv6マルチキャストVLAN 10には、VLAN 2～VLAN 4のサブVLAN VLANが含まれています。スイッチBは、VLAN 10のIPv6マルチキャストデータをVLAN 4～VLAN 2に複製します。

例:ポートベースIPv6マルチキャストVLANの設定

ネットワークの設定

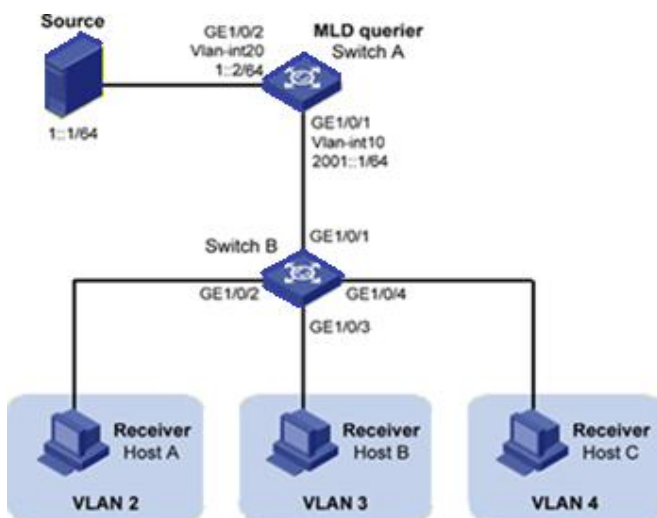
図74に示します。

- レイヤ3デバイスのスイッチAはMLDv1を実行し、MLDクエリアーとして動作します。レイヤ2デバイスのスイッチBはMLDv1スヌーピングを実行します。
- IPv6マルチキャスト送信元は、IPv6マルチキャストデータをIPv6マルチキャストグループ FF1E::101に送信します。レシーバHost A、Host B、およびHost Cは、それぞれVLAN 2、VLAN 3、およびVLAN 4に属します。

次の要件を満たすように、スイッチBでポートベースのIPv6マルチキャストVLANを設定します。

- スイッチAは、IPv6マルチキャストVLAN経由でIPv6マルチキャストデータをスイッチBに送信します。
- スイッチBは、IPv6マルチキャストデータを異なるユーザーVLANのレシーバに転送します。

図74 ネットワークダイアグラム



手順

1. スイッチAを設定します。

```
# Enable IPv6 multicast routing.
```

```
<SwitchA> system-view
```

```
[SwitchA] ipv6 multicast routing
```

```
[SwitchA-mrib6] quit
```

```
# Create VLAN 20, and assign GigabitEthernet 1/0/2 to the VLAN.
```

```
[SwitchA] vlan 20
```

```
[SwitchA-vlan20] port gigabitethernet 1/0/2
```

```
[SwitchA-vlan20] quit
```

```
# Assign an IPv6 address to VLAN-interface 20, and enable IPv6 PIM-DM on the interface.
```

```
[SwitchA] interface vlan-interface 20
```

```
[SwitchA-Vlan-interface20] ipv6 address 1::2 64
```

```
[SwitchA-Vlan-interface20] ipv6 pim dm
```

```
[SwitchA-Vlan-interface20] quit
# Create VLAN 10, and assign GigabitEthernet 1/0/1 to the VLAN.
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 1/0/1
[SwitchA-vlan10] quit
# Assign an IPv6 address to VLAN-interface 10, and enable MLD on the interface.
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ipv6 address 2001::1 64
[SwitchA-Vlan-interface10] mld enable
[SwitchA-Vlan-interface10] quit
```

2. スイッチBを構成します。

```
# Enable the MLD snooping feature.
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
# Create VLAN 10, assign GigabitEthernet 1/0/1 to the VLAN, and enable MLD snooping for the VLAN.
[SwitchB] vlan 10
[SwitchB-vlan10] port gigabitethernet 1/0/1
[SwitchB-vlan10] mld-snooping enable
[SwitchB-vlan10] quit
# Create VLAN 2, and enable MLD snooping for the VLAN.
[SwitchB] vlan 2
[SwitchB-vlan2] mld-snooping enable
[SwitchB-vlan2] quit
# Create VLAN 3, and enable MLD snooping for the VLAN.
[SwitchB] vlan 3
[SwitchB-vlan3] mld-snooping enable
[SwitchB-vlan3] quit
# Create VLAN 4, and enable MLD snooping for the VLAN.
[SwitchB] vlan 4
[SwitchB-vlan4] mld-snooping enable
[SwitchB-vlan4] quit
# Configure GigabitEthernet 1/0/2 as a hybrid port, and configure VLAN 2 as the PVID of the hybrid port.
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type hybrid
[SwitchB-GigabitEthernet1/0/2] port hybrid pvid vlan 2
# Assign GigabitEthernet 1/0/2 to VLAN 2 and VLAN 10 as an untagged VLAN member.
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 2 untagged
[SwitchB-GigabitEthernet1/0/2] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/2] quit
# Configure GigabitEthernet 1/0/3 as a hybrid port, and configure VLAN 3 as the PVID of the hybrid port.
[SwitchB] interface gigabitethernet 1/0/3
```

```

[SwitchB-GigabitEthernet1/0/3] port link-type hybrid
[SwitchB-GigabitEthernet1/0/3] port hybrid pvid vlan 3
# Assign GigabitEthernet 1/0/3 to VLAN 3 and VLAN 10 as an untagged VLAN member.
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 3 untagged
[SwitchB-GigabitEthernet1/0/3] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/3] quit
# Configure GigabitEthernet 1/0/4 as a hybrid port, and configure VLAN 4 as the PVID of the
hybrid port.
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] port link-type hybrid
[SwitchB-GigabitEthernet1/0/4] port hybrid pvid vlan 4
# Assign GigabitEthernet 1/0/4 to VLAN 4 and VLAN 10 as an untagged VLAN member.
[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 4 untagged
[SwitchB-GigabitEthernet1/0/4] port hybrid vlan 10 untagged
[SwitchB-GigabitEthernet1/0/4] quit
# Configure VLAN 10 as an IPv6 multicast VLAN.
[SwitchB] ipv6 multicast-vlan 10
# Assign GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to VLAN 10.
[SwitchB-ipv6-mvlan-10] port gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[SwitchB-ipv6-mvlan-10] quit
# Assign GigabitEthernet 1/0/4 to VLAN 10.
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] ipv6 port multicast-vlan 10
[SwitchB-GigabitEthernet1/0/4] quit

```

設定の確認

#スイッチB上のIPv6マルチキャストVLANに関する情報を表示します。

```

[SwitchB] display ipv6 multicast-vlan
Total 1 IPv6 multicast VLANs.
IPv6 multicast VLAN 10:
  Sub-VLAN list(0 in total):
  Port list(3 in total):
    GE1/0/2
    GE1/0/3
    GE1/0/4

```

#スイッチBのダイナミックMLDスヌーピングフォワーディングエントリを表示します。

```

[SwitchB] display mld-snooping group
Total 1 entries.
VLAN 10: Total 1 entries.
  (::, FF1E::101)
  Host slots (0 in total):
  Host ports (3 in total):
    GE1/0/2      (00:03:23)
    GE1/0/3      (00:04:07)
    GE1/0/4      (00:04:16)

```

この出力は、MLDスヌーピングがマルチキャストVLAN(VLAN 10)内のユーザーポートを維持してい

ることを示しています。スイッチBは、これらのユーザーポートを介してVLAN 10のIPv6マルチキャストデータを転送します。

IPv6マルチキャストルーティングおよびフォワーディングの設定

IPv6マルチキャストルーティングおよび転送について

各IPv6マルチキャストルーティングプロトコルには、独自のルーティングテーブルがあります。IPv6マルチキャストルーティングプロトコルによって生成されたルーティングエントリ内のマルチキャストルーティング情報は、(S, G)および(*,G)エントリのセットに要約されます。すべての(S, G)および(*,G)エントリは、一般的なIPv6マルチキャストルーティングテーブルを形成します。一般的なIPv6マルチキャストルーティングテーブル内の最適なIPv6マルチキャストルーティングエントリは、IPv6マルチキャストデータ転送をガイドするためにIPv6マルチキャスト転送テーブルに追加されます。

RPFチェックメカニズム

IPv6マルチキャストルーティングプロトコルは、Reverse Path Forwarding(RPF)チェックメカニズムを使用して、IPv6マルチキャストデータが正しいパスに沿って配信されるようにし、データループを回避します。

RPFチェックプロセス

IPv6マルチキャストデバイスは、IPv6マルチキャストパケットに対してRPFチェックを次のように実行します。

1. IPv6ユニキャストおよびIPv6 MBGPルーティングテーブルとは別に、パケット送信元に戻る最適ルートを選択します。

RPFチェックでは、「パケット送信元」は異なる状況で異なるものを意味します。

- SPTに沿って送信されるパケットの場合、パケット送信元はIPv6マルチキャスト送信元です。
- RPTに沿って送信されるパケットの場合、パケットの送信元はRPです。
- BSRから発信されたブートストラップメッセージの場合、パケットの送信元はBSRです。

SPT、RPT、送信元側RPT、RP、およびBSRの概念の詳細については、「IPv6 PIMの設定」を参照してください。

2. 次のように、最適ルートの1つをRPFルートとして選択します。

- デバイスが最長プレフィクス一致原則を使用する場合、プレフィクス長が長いルートがRPFルートになります。ルートのプレフィクス長が同じ場合、ルートプリファレンスが高いルートがRPF

ルートになります。ルートのルートプリファレンスが同じ場合、IPv6 MBGPルートがRPFルートになります。

ルートプリファレンスの詳細については、『Layer 3 IP Routing Configuration Guide』を参照してください。

- デバイスが最長プレフィクス一致原則を使用しない場合、より高いルートプリファレンスを持つルートがRPFルートになります。ルートが同じルートプリファレンスを持つ場合、IPv6 MBGPルートがRPFルートになります。

RPFルートでは、発信インターフェイスはRPFインターフェイスであり、ネクストホップはRPFネイバーです。

3. パケットがRPFインターフェイスに到着したかどうかを判別します。

- パケットがRPFインターフェイスに到達した場合、RPFチェックは成功し、パケットは転送されます。
- パケットが非RPFインターフェイスに到達した場合、RPFチェックは失敗し、パケットは廃棄されます。

IPv6マルチキャストでのRPFチェックの実装

受信した各IPv6マルチキャストパケットにRPFチェックを実装すると、デバイスに大きな負荷がかかります。IPv6マルチキャスト転送テーブルを使用することで、この問題を解決できます。デバイスは、IPv6(S, G)パケットのIPv6マルチキャスト転送エントリを作成するときに

パケットを(S, G)エントリの着信インターフェイスとして送信します。デバイスは、別の(S, G)パケットを受信すると、IPv6マルチキャスト転送テーブルで一致する(S, G)エントリを検索します。

- 一致するものが見つからない場合、デバイスはまずパケット送信元に戻るRPFルートを決定します。次に、RPFインターフェイスを着信インターフェイスとする転送エントリを作成し、次のいずれかのタスクを実行します。
 - 受信インターフェイスがRPFインターフェイスの場合、RPFチェックは成功し、デバイスはすべての発信インターフェイスからパケットを転送します。
 - 受信インターフェイスがRPFインターフェイスでない場合、RPFチェックは失敗し、デバイスはパケットを廃棄します。
- 一致が見つかり、一致する転送エントリに受信インターフェイスが含まれている場合、デバイスはすべての発信インターフェイスからパケットを転送します。
- 一致が見つかったものの、一致する転送エントリに受信インターフェイスが含まれていない場合、デバイスはパケット送信元に戻るRPFルートを決定します。その後、デバイスは次のいずれかのタスクを実行します。
 - RPFインターフェイスが着信インターフェイスの場合は、転送エントリは正しいが、パケットが誤ったパスを通過したことを意味します。パケットはRPFチェックに失敗し、デバイスはパケットを廃棄します。
 - RPFインターフェイスが着信インターフェイスでない場合は、転送エントリが期限切れになった

ことを意味します。デバイスは着信インターフェイスをRPFインターフェイスに置き換え、受信インターフェイスをRPFインターフェイスと照合します。受信インターフェイスがRPFインターフェイスの場合、デバイスはすべての発信インターフェイスからパケットを転送します。それ以外の場合、パケットは廃棄されます。

図75 RPFチェックプロセス

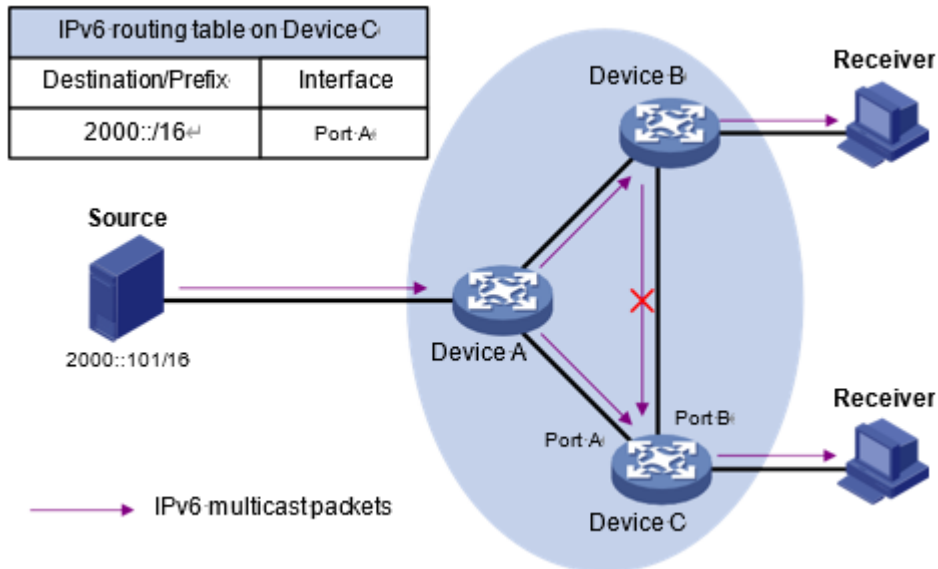


図75に示されるように、IPv6ユニキャストルートがネットワーク上で利用可能であると想定します。IPv6 MBGPは設定されていません。IPv6マルチキャストパケットは、SPTに沿ってマルチキャスト送信元からレシーバに送信されます。デバイスCのIPv6マルチキャスト転送テーブルには(S, G)エントリが含まれ、ポートAはRPFインターフェイスです。

- IPv6マルチキャストパケットがデバイスCのポートAに到着した場合、受信インターフェイスは(S, G)エントリの着信インターフェイスです。デバイスCは、すべての発信インターフェイスからパケットを転送します。
- IPv6マルチキャストパケットがデバイスCのポートBに到着した場合、受信インターフェイスは(S, G)エントリの着信インターフェイスではありません。デバイスCは自身のIPv6ユニキャストルーティングテーブルを検索し、送信元(RPFインターフェイス)への発信インターフェイスがポートAであることを検出します。これは、(S, G)エントリは正しいが、パケットが誤ったパスを通過したことを意味します。パケットはRPFチェックに失敗し、デバイスCはパケットを廃棄します。

IPv6ユニキャストサブネット間のIPv6マルチキャスト転送

デバイスは、転送ツリーに沿ってホップバイホップでIPv6マルチキャストソースからIPv6マルチキャストデータを転送しますが、一部のデバイスはネットワーク内でIPv6マルチキャストプロトコルをサポートしない場合があります。IPv6マルチキャストデータがIPv6マルチキャストをサポートしないデバイスに転送されると、転送パスがブロックされます。この場合、IPv6ユニキャストサブネットの両端にあるデバイス間にトンネルを確立することによって、IPv6ユニキャストサブネット間でのIPv6マルチキャストデータの転送を有効にできます。

図76 トンネルを介したIPv6マルチキャストデータ送信

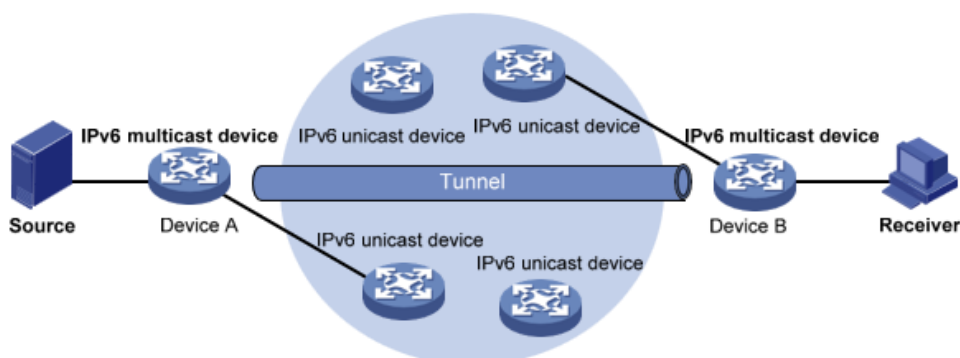


図76に示すように、デバイスAとデバイスBの間にトンネルが確立されます。デバイスAはIPv6マルチキャストデータをユニキャストIPv6パケットにカプセル化し、ユニキャストデバイスを経由してトンネル経由でデバイスBに転送します。次に、デバイスBはユニキャストIPv6ヘッダーを取り除き、IPv6マルチキャストデータをレシーバに向けて転送し続けます。

IPv6のmtrace

IPv6 mtraceは、mtrace2を使用して、IPv6マルチキャストグループデータが送信元から宛先に移動するパスをトレースします。

デバイスの役割

IPv6 mtraceには、次の役割があります。

- **Last-Hop Router(LHR):**LHRは、宛先と同じサブネット上にIPv6マルチキャスト対応インターフェイスがあり、特定のIPv6マルチキャストデータをサブネットに転送できるルータです。
- **First-Hop Router(FHR):**FHRは、IPv6マルチキャスト送信元に直接接続されているルータです。
- **Client:**クライアントは、mtrace2を開始するルータです。

プロセス

IPv6 mtraceプロセスは、次のとおりです。

1. クライアントは、mtrace2 Queryメッセージ(トレースする最大ホップ数を示すhopsフィールドを含む)

を宛先に送信します。

2. LHRは、ローカル転送情報を追加して、受信したQueryメッセージをmtrace2 Requestメッセージに変換し、そのRequestメッセージを上流のネイバーに送信します。
3. トレースされたパスに沿った各ルータは、受信した要求メッセージにローカル転送情報を追加し、その要求メッセージを上流のネイバーに送信します。
4. FHRは、受信した要求メッセージにローカル転送情報を追加します。次に、要求メッセージをmtrace2応答メッセージに変換し、その応答メッセージをクライアントに送信します。
5. クライアントは、Replyメッセージ内の転送情報を解釈し、その情報を表示します。

IPv6マルチキャストルーティングおよび転送タスクの概要

IPv6マルチキャストルーティングおよび転送を設定するには、次の作業を実行します。

1. IPv6マルチキャストルーティングの有効化
2. (任意)最長プレフィクス一致原則の指定
3. (任意)IPv6マルチキャストロードスプリットの設定
4. (任意)IPv6マルチキャスト転送境界の設定
5. (任意)スーパーVLANのサブVLAN間でのIPv6マルチキャスト転送の有効化
6. (省略可能)mtrace2を使用したIPv6マルチキャストパスのトレース

IPv6マルチキャストルーティングおよび転送の前提条件

マルチキャストルーティングおよび転送を設定する前に、IPv6ユニキャストルーティングプロトコルを設定して、ドメイン内のすべてのデバイスがネットワーク層で相互運用できるようにします。

IPv6マルチキャストルーティングの有効化

IPv6マルチキャストルーティングについて

レイヤ3 IPv6マルチキャスト機能を設定する前に、IPv6マルチキャストルーティングを有効にします。

手順

1. システムビューに入ります。

system-view

2. IPv6マルチキャストルーティングを有効にし、IPv6 MRIBビューを開始します。

```
ipv6 multicast routing
```

デフォルトでは、IPv6マルチキャストルーティングは無効になっています。

最長プレフィクス一致原則の指定

最長一致検索の原則について

RPFルート選択のための最長プレフィクス一致原則を使用するために、デバイスを有効にすることができます。RPFルート選択の詳細については、「RPFチェックプロセス」を参照してください。

手順

1. システムビューに入ります。
system-view
2. IPv6 MRIBビューを入力します。
ipv6 multicast routing
3. RPFルート選択の最長プレフィクス一致原則を指定します。

```
longest-match
```

デフォルトでは、ルートプリファレンスの原則が使用されます。

IPv6マルチキャストロードスプリットの設定

IPv6マルチキャストロードスプリットについて

デバイスを有効にして、複数のIPv6マルチキャストデータフローを送信元単位または送信元およびグループ単位で分割できます。

手順

1. システムビューに入ります。
system-view
2. IPv6 MRIBビューを入力します。
ipv6 multicast routing
3. IPv6マルチキャストロードスプリットを設定します。

```
load-splitting { source | source-group }
```

デフォルトでは、IPv6マルチキャストロードスプリットは無効になっています。

IPv6マルチキャストフォワーディング境界の設定

IPv6マルチキャスト転送境界について

インターフェイスを、IPv6マルチキャストグループ範囲のIPv6マルチキャスト転送境界として設定できます。インターフェイスは、範囲内のグループのIPv6マルチキャストパケットを受信または転送できません。

制約事項とガイドライン

この設定の前に、IPv6マルチキャストルーティングを有効にする必要はありません。

手順

1. システムビューに入ります。

system-view

2. インターフェイスビューに入ります。

interface *interface-type* *interface-number*

3. IPv6マルチキャスト転送境界を設定します。

```
ipv6 multicast boundary { ipv6-group-address prefix-length | scope
{ scope-id | admin-local | global | organization-local | site-local } }
```

デフォルトでは、インターフェイスはIPv6マルチキャストグループのIPv6マルチキャスト転送境界ではありません。

スーパーVLANのサブVLAN間のIPv6マルチキャスト トフォワーディングの有効化

スーパーVLANのサブVLAN間のIPv6マルチキャストトフォワーディングについて

スーパーVLANは、複数のサブVLANに関連付けられます。サブVLANは、レイヤ2で相互に分離されます。スーパーVLANおよびサブVLANの詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

手順

1. システムビューに入ります。

system-view

2. VLANインターフェイスビューを開始します。

interface **vlan-interface** *interface-number*

3. スーパーVLANに関連付けられたサブVLAN間のIPv6マルチキャスト転送を有効にします。

```
ipv6 multicast forwarding supervlan community
```

デフォルトでは、IPv6マルチキャストデータは、スーパーVLANに関連付けられたサブVLAN間で転送できません。

4. システムビューに戻ります。

quit

5. ユーザービューに戻ります。

quit

6. スーパーVLANインターフェイスを着信インターフェイスとして持つすべてのIPv6マルチキャストトフォワーディングエントリをクリアします。

```
reset ipv6 multicast forwarding-table incoming-interface  
{ interface-type interface-number }
```

ipv6 multicast forwarding supervlanコマンドが有効になるのは、この手順を実行した後だけです。

mtrace2を使用したIPv6マルチキャストパスのトレース

制約事項とガイドライン

IPv6 mtraceを正常に実行するには、他のモジュールで使用されているUDPポート番号を使用しないでください。トレースパス上のすべてのデバイスで、同じUDPポート番号を指定する必要があります。

手順

1. システムビューに入ります。

system-view

2. (任意)IPv6 mtraceが使用するUDPポート番号を指定します。

```
ipv6 mtrace-service port number
```

デフォルトでは、IPv6 mtraceはUDPポート番号10240を使用します。

3. IPv6マルチキャストパスをトレースするには、mtrace2を使用します。

4. **mtrace v2 ipv6 { *source-address* | *group-address* } * [**destination address** | **port number** | **wait-time time** | **max-hop count**] * [**verbose**]**
このコマンドで指定するUDPポート番号は、**mtrace-service port**コマンドで指定するポート番号と同じでなければなりません。

IPv6マルチキャストルーティングおよびフォワーディングの表示およびメンテナンスコマンド

△注意:

resetコマンドを使用すると、IPv6マルチキャストデータ送信が失敗する場合があります。

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
インターフェイス情報を表示するIPv6 MRIBによって維持されます。	display ipv6 mrib interface [<i>interface-type interface-number</i>]
IPv6マルチキャスト境界情報を表示します。	display ipv6 multicast boundary { group [<i>ipv6-group-address</i> [<i>prefix-length</i>]] scope [<i>scope-id</i>] } [interface <i>interface-type interface-number</i>]
IPv6マルチキャスト高速フォワーディングエントリを表示します。	display ipv6 multicast fast-forwarding cache [<i>ipv6-source-address</i> <i>ipv6-group-address</i>] * [slot <i>slot-number</i>]
IPv6マルチキャスト転送イベントの統計情報を表示します。	display ipv6 multicast forwarding event [slot <i>slot-number</i>]
IPv6マルチキャストフォワーディングエントリを表示します。	display ipv6 multicast forwarding-table [<i>ipv6-source-address</i> [<i>prefix-length</i>] <i>ipv6-group-address</i> [<i>prefix-length</i>] incoming-interface <i>interface-type interface-number</i> outgoing-interface { exclude include match } <i>interface-type interface-number</i> slot <i>slot-number</i> statistics] *
IPv6マルチキャストルーティングエントリを表示します。	display ipv6 multicast routing-table [<i>ipv6-source-address</i> [<i>prefix-length</i>] <i>ipv6-group-address</i> [<i>prefix-length</i>] incoming-interface <i>interface-type interface-number</i> outgoing-interface { exclude include match } <i>interface-type interface-number</i>] *
IPv6マルチキャスト送信元のRPF情報を表示します。	display ipv6 multicast rpf-info <i>ipv6-source-address</i> [<i>ipv6-group-address</i>]

IPv6マルチキャスト高速フォワーディングエントリをクリアします。	reset ipv6 multicast fast-forwarding cache { { <i>ipv6-source-address</i> <i>ipv6-group-address</i> } * all } [slot <i>slot-number</i>]
IPv6マルチキャスト転送イベントの統計情報をクリアします。	reset ipv6 multicast forwarding event
IPv6マルチキャストフォワーディングエントリをクリアします。	reset ipv6 multicast forwarding-table { { <i>ipv6-source-address</i> [<i>prefix-length</i>] <i>ipv6-group-address</i> [<i>prefix-length</i>] incoming-interface { <i>interface-type</i> <i>interface-number</i> } } * all }
IPv6マルチキャストルーティングエントリをクリアします。	reset ipv6 multicast routing-table { { <i>ipv6-source-address</i> [<i>prefix-length</i>] <i>ipv6-group-address</i> [<i>prefix-length</i>] incoming-interface <i>interface-type</i> <i>interface-number</i> } * all }

注:

- IPv6マルチキャストルーティングエントリをクリアすると、関連するIPv6マルチキャストフォワーディングエントリもクリアされます。
 - IPv6マルチキャストフォワーディングエントリをクリアすると、関連するIPv6マルチキャストルーティングエントリもクリアされます。
-

MLDの設定

MLDの概要

Multicast Listener Discovery(MLD)は、レイヤ3マルチキャストデバイスと直接接続されたサブネット上のホストとの間にIPv6マルチキャストグループメンバーシップを確立し、維持します。

MLDバージョン

MLDには次のバージョンがあります。

- IGMPv2から派生したMLDv1(RFC 2710で定義)。
- IGMPv3から派生したMLDv2(RFC 3810で定義)。

MLDv1およびMLDv2は、ASMモデルをサポートします。MLDv2はSSMモデルを直接実装できますが、MLDv1はMLD SSMマッピング機能と連携してSSMモデルを実装する必要があります。ASMおよびSSMモデルの詳細については、「マルチキャストの概要」を参照してください。

MLDv1の機能

MLDv1は、クエリーおよび応答メカニズムに基づいてIPv6マルチキャストリスナー管理を実装します。

MLDクエリーアの選択

同じサブネット上でMLDを実行するすべてのIPv6マルチキャストデバイスは、ホストからのMLDリスナーレポートメッセージ(しばしばレポートと呼ばれます)を監視できます。ただし、MLDクエリーメッセージ(しばしばクエリーと呼ばれます)を送信するためにMLDクエリーアとして動作できるのは、1つのデバイスだけです。クエリーア選択メカニズムは、サブネット上でMLDクエリーアとして動作するデバイスを決定します。

1. 最初は、すべてのMLDデバイスが自身をクエリーアと見なします。各デバイスは、ローカルサブネット上のすべてのホストおよびデバイスにMLD一般クエリーメッセージ(一般クエリーと呼ばれることもあります)を送信します。一般クエリーの宛先アドレスはFF02::1です。
2. 一般的なクエリーを受信した後、すべてのMLDデバイスは、クエリーの送信元IPv6アドレスを自身のリンクローカルインターフェイスアドレスと比較します。最も低いIPv6アドレスを持つデバイスがクエリーアの選択に勝ち、クエリーアになります。他のすべてのデバイスは非クエリーアになります。
3. すべての非クエリーアは、「他のクエリーア存在タイマー」と呼ばれるタイマーを開始します。タイマーが切れる前にデバイスがクエリーアからMLDクエリーを受信した場合、このタイマーをリセットします。そうでない場合、デバイスはクエリーアがタイムアウトしたと見なします。この場合、デバイスは新しいクエリーア選択プロセスを開始します。

IPv6マルチキャストグループへの参加

図77 MLDクエリーおよびレポート

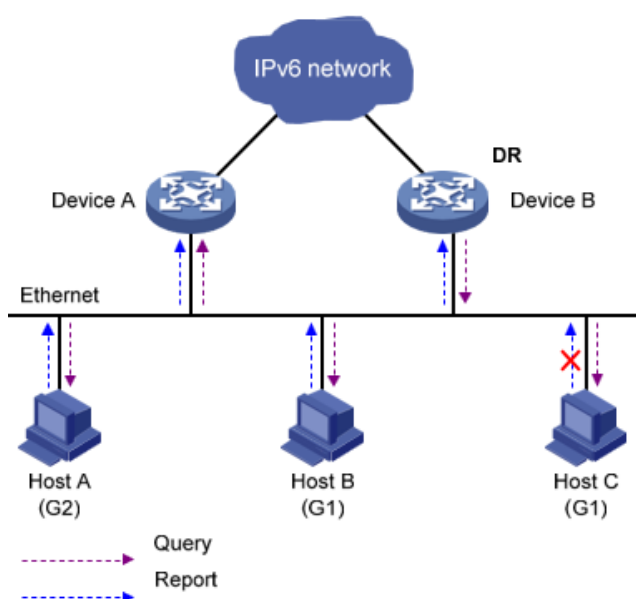


図77に示すように、ホストBとホストCは、IPv6マルチキャストグループG1宛てのIPv6マルチキャストデータを受信します。ホストAは、G2宛てのIPv6マルチキャストデータを受信します。次のプロセスでは、ホストがIPv6マルチキャストグループに加入する方法と、MLDクエリー(図77のデバイスB)がIPv6マルチキャストグループメンバーシップを維持する方法について説明します。

1. ホストは、MLDクエリーを待つことなく、加入するIPv6マルチキャストグループに非送信請求MLDレポートを送信します。
2. MLDクエリーは、定期的にMLDクエリー(宛先アドレスFF02::1)をローカルサブネット上のすべてのホストおよびデバイスにマルチキャストします。
3. クエリーを受信したあと、レポート遅延タイマーが期限切れになったホストは、まずMLDレポートをIPv6マルチキャストグループG1に送信して、G1のメンバーシップをアナウンスします。この例では、ホストBがレポートを送信します。ホストBと同じサブネット上にあるホストCは、ホストBからレポートを受信したあと、G1のレポートを抑制します。

MLDデバイスは、G1に最低1つのメンバーがあることをすでに認識しているため、他のメンバーは自分のメンバーシップを報告する必要がありません。ホストMLDレポート抑制と呼ばれるこのメカニズムは、ローカルサブネット上のトラフィックを削減するのに役立ちます。

4. 同時に、ホストAはG2に関心があるため、IPv6マルチキャストグループG2にレポートを送信します。
5. 照会/報告プロセスを通して、MLDデバイスは、G1およびG2がローカルサブネット上にメンバーを持っていることを決定します。デバイス上で動作しているIPv6マルチキャストルーティングプロトコル(例えば、IPv6 PIM)は、(*,G1)および(*,G2)マルチキャストフォワーディングエントリを生成します。これらのエントリは、後続のIPv6マルチキャストフォワーディングの基礎となります。アスタリスク(*)は、任意のIPv6マルチキャストソースを表します。
6. G1またはG2宛てのIPv6マルチキャストデータがMLDデバイスに到達すると、デバイスはIPv6マ

マルチキャスト転送テーブルを検索します。(*,G1)および(*,G2)エントリに基づいて、デバイスはIPv6マルチキャストデータをローカルサブネットに転送します。その後、サブネット上のレシーバがデータを受信します。

IPv6マルチキャストグループからの脱退

ホストがIPv6マルチキャストグループから脱退する場合、次のプロセスが発生します。

1. ホストは、ローカルサブネット上のすべてのIPv6マルチキャストデバイスにMLD doneメッセージを送信します。doneメッセージの宛先アドレスはFF02::2です。
2. MLD完了メッセージを受信した後、クエリーは、ホストが離脱するグループに対して、設定可能な数のマルチキャストアドレス固有のクエリーを送信します。クエリーされるIPv6マルチキャストアドレスには、メッセージの宛先アドレスフィールドとグループアドレスフィールドの両方が含まれます。
3. グループ内の残りのメンバー(サブネット上に存在する場合)の1つが、マルチキャストアドレス固有のクエリーでアドバタイズされた最大応答時間の時間内にレポートを送信します。
4. クエリーアは、最大応答時間内にグループのレポートを受信した場合、IPv6マルチキャストグループのメンバーシップを維持します。それ以外の場合、クエリーアは、サブネット上のどのホストもそのグループにアドレス指定されたIPv6マルチキャストトラフィックに関係がないと見なし、グループのメンバーシップの維持を停止します。

MLDv2拡張機能

MLDv2はMLDv1をベースにしており、MLDv1と下位互換性があります。MLDv2はホストに拡張制御機能を提供し、MLDステートを拡張します。

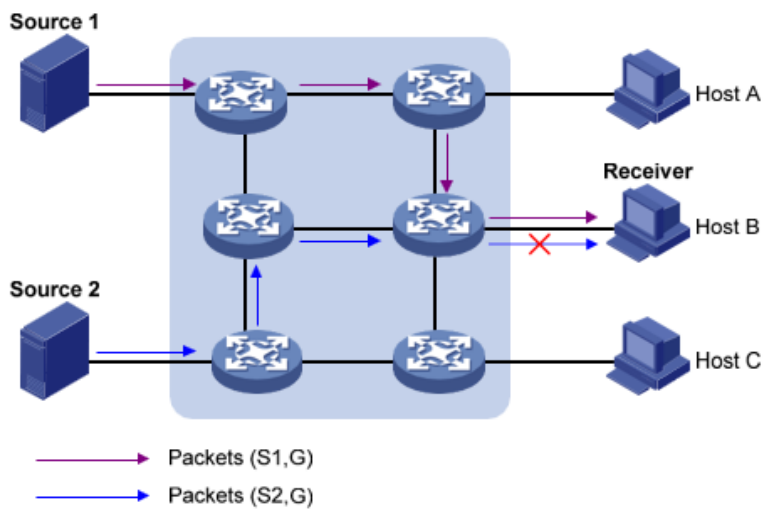
ホストの制御能力の強化

MLDv2では、IPv6マルチキャスト送信元フィルタリングモード(IncludeおよびExclude)が導入されています。これらのモードを使用すると、ホストは、指定されたIPv6マルチキャスト送信元からのマルチキャストデータを受信または拒否できます。ホストがIPv6マルチキャストグループに加入すると、次のいずれかが発生します。

- もしホストがS1, S2, ...のような特定のIPv6マルチキャストソースからのIPv6マルチキャストデータを期待するなら、「ソースを含む(S1, S2, ...)」としてFilter-Modeで報告を送ります。
- もしホストがS1, S2, ...のような特定のIPv6マルチキャストソースからのIPv6マルチキャストデータを期待しないなら、「Exclude Sources(S1, S2, ...)」のFilter-Modeで報告を送ります。

図78に示すように、ネットワークには2つのIPv6マルチキャスト送信元、Source 1(S1)とSource 2(S2)があります。どちらの送信元もIPv6マルチキャストデータをIPv6マルチキャストグループGに送信できます。ホストBは、Source 1からG宛てのIPv6マルチキャストデータを受信しますが、Source 2からは受信しません。

図78マルチキャストアドレスおよび送信元固有のマルチキャストトラフィックのフローパス



MLDv1では、ホストBはIPv6マルチキャストグループGに加入するときにIPv6マルチキャストソースを選択できません。Source 1とSource 2の両方からのIPv6マルチキャストストリームは、必要かどうかに関係なくホストBに流れます。

MLDv2では、ホストBは、Source 1からG宛てのIPv6マルチキャストデータに対する関心を明示的に表明できますが、Source 2からの関心は表明できません。したがって、ホストBはSource 1からのIPv6マルチキャストデータだけを受信します。

MLD状態での機能拡張

MLDv2を実行しているマルチキャストデバイスは、接続されている各サブネット上の各マルチキャストアドレスのマルチキャストアドレスステートを維持します。マルチキャストアドレスステートは、次の情報で構成されます。

- **Filter mode:** デバイスは、IncludeまたはExclude状態をトレースし続けます。
- **ソースのリストデバイス:** 新しく追加または削除されたIPv6マルチキャストソースを追跡し続けます。
- **Timers:** IPv6マルチキャストアドレスのタイムアウト後にIncludeモードに切り替わるまでデバイスが待機する時間を含むフィルタタイマー、およびソース録音のソースタイマー。

MLD SSMマッピング

MLDv2ホストは、MLDv2レポートでマルチキャスト送信元を明示的に指定できます。レポートから、MLDデバイスはマルチキャスト送信元アドレスを取得し、SSMサービスを直接提供できます。ただし、MLDv1ホストは、MLDv1レポートでマルチキャスト送信元を指定できません。

MLD SSMマッピング機能を使用すると、MLDデバイスはMLDv1レシーバホストのSSMをサポートできます。デバイスは、設定されたMLD SSMマッピングに基づいて、MLDv1レポートの(*,G)を(G, INCLUDE, (S1, S2.))に変換します。

図79 ネットワークダイアグラム

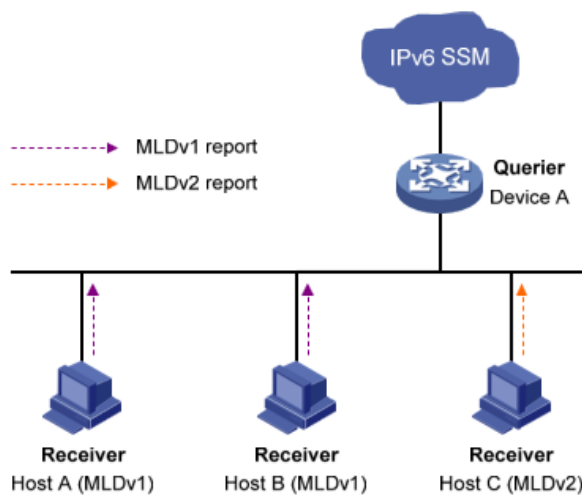


図79に示すように、IPv6 SSMネットワーク上のホストAおよびホストBはMLDv1を実行し、ホストCはMLDv2を実行します。ホストAおよびホストBにSSMサービスを提供するには、デバイスAでMLD SSMマッピング機能を設定する必要があります。

MLD SSMマッピングの設定後、デバイスAはメッセージで伝送されたIPv6マルチキャストグループアドレスGをチェックし、次の動作を実行します。

- GがIPv6 SSMグループ範囲にない場合は、デバイスAがASMサービスを提供します。
- GがIPv6 SSMグループ範囲内にあり、どのMLD SSMマッピングとも一致しない場合、デバイスAはレポートをドロップします。
- GがIPv6 SSMグループ範囲内にあり、MLD SSMマッピングと一致する場合、デバイスAはレポートの(*,G)を(G, INCLUDE, (S1, S2.))に変換してSSMサービスを提供します。

注:

MLD SSMマッピング機能は、MLDv2レポートを処理しません。

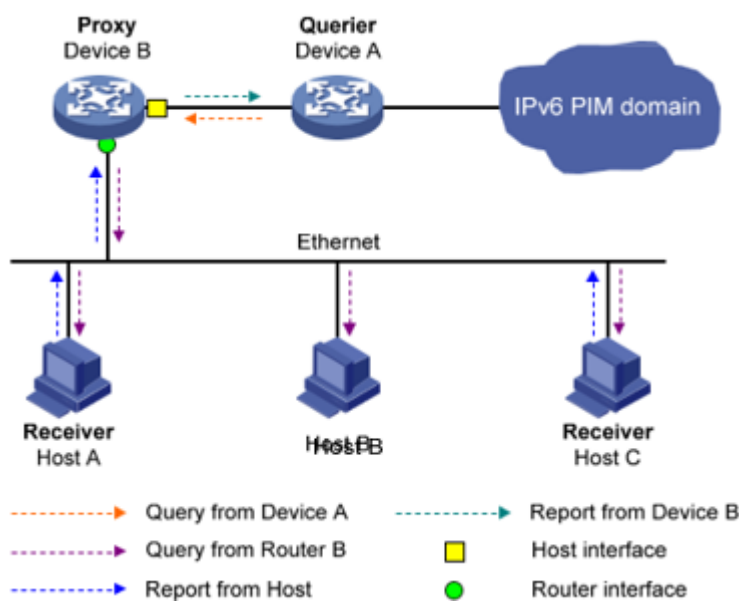
IPv6 SSMグループ範囲の詳細については、「IPv6 PIMの設定」を参照してください。

MLDプロキシ

図80に示されるように、単純なツリー型トポロジでは、IPv6 PIMのようなIPv6マルチキャストルーティングプロトコルをエッジデバイスに設定する必要はありません。代わりに、これらのデバイスにMLDプロキシを設定できます。MLDプロキシが設定されると、エッジデバイスはMLDプロキシとして動作します。

- アップストリームMLDクエリーアの場合、MLDプロキシデバイスはホストとして動作します。
- ダウンストリームレシーバホストの場合、MLDプロキシデバイスはMLDクエリーアとして機能します。

図80 ネットワークダイアグラム



次のインターフェイスは、MLDプロキシで定義されます。

- ホストインターフェイス:マルチキャスト転送ツリーのルート方向にあるインターフェイス。ホストインターフェイスは、MLDを実行するレシーバホストとして機能します。MLDプロキシは、このインターフェイスで有効にする必要があります。このインターフェイスは「プロキシインターフェイス」とも呼ばれます。
- ルータインターフェイス:マルチキャスト転送ツリーのリーフ方向のインターフェイス。ルータインターフェイスは、MLDを実行するルータとして動作します。MLDは、このインターフェイスで設定する必要があります。

MLDプロキシデバイスは、すべてのルータインターフェイス上のグループメンバーシップを保存するグループメンバーシップデータベースを維持します。ホストインターフェイスとルータインターフェイスは、このメンバーシップデータベースに基づいてアクションを実行します。

- ホストインターフェイスは、メンバーシップデータベースに従ってクエリーに応答するか、データベースが変更されたときにjoin/doneメッセージを送信します。
- ルータインターフェイスは、受信したMLDレポートに基づいてクエリーア選定に参加し、クエリーを送信し、メンバーシップを維持します。

プロトコルと標準

- RFC 2710『Multicast Listener Discovery(MLD)for IPv6』
- RFC 3810『Multicast Listener Discovery Version 2(MLDv2)for IPv6』

MLDタスクの概要

MLDを設定するには、次の作業を実行します。

1. MLDの有効化
2. (任意)基本的なMLD機能の設定
 - MLDバージョンの指定
 - スタティックグループメンバーの設定
 - IPv6マルチキャストグループポリシーの設定
3. (任意)MLDパフォーマンスの調整
 - MLDクエリーおよび応答パラメータの設定
 - 高速脱退処理の有効化
4. (任意)MLD SSMマッピングの設定
5. (任意)MLDプロキシの設定
 - MLDプロキシの有効化
 - 非クエリーインターフェイス上のIPv6マルチキャストフォワーディングの有効化
 - MLDプロキシインターフェイスのIPv6マルチキャストロードスプリットの有効化
6. (任意)MLD NSRの有効化
7. (任意)発信MLDプロトコルパケットのDSCP値の設定

MLDの前提条件

MLDを設定する前に、すべてのデバイスがネットワーク層で相互運用できるように、IPv6ユニキャストルーティングプロトコルを設定する必要があります。

MLDの有効化

制約事項とガイドライン

この作業は、IPv6マルチキャストグループメンバーシップが作成および維持されるインターフェイスで行います。

手順

1. システムビューに入ります。

system-view

2. IPv6マルチキャストルーティングを有効にし、IPv6 MRIBビューを開始します。

ipv6 multicast routing

デフォルトでは、IPv6マルチキャストルーティングは無効になっています。

このコマンドの詳細については、『IP Multicast Command Reference』を参照してください。

3. システムビューに戻ります。

quit

4. インターフェイスビューに入ります。

interface *interface-type interface-number*

5. MLDを有効にします。

mld enable

デフォルトでは、MLDは無効です。

基本的なMLD機能の設定

MLDバージョンの指定

制約事項とガイドライン

MLDを正しく動作させるには、同じサブネット上のすべてのデバイスに同じMLDバージョンを指定します。

手順

1. システムビューに入ります。

system-view

2. インターフェイスビューに入ります。

interface *interface-type* *interface-number*

3. インターフェイスのMLDバージョンを指定します。

mld version *version-number*

デフォルトでは、インターフェイスのMLDバージョンはMLDv1です。

スタティックグループメンバーの設定

スタティックグループメンバーについて

インターフェイスをIPv6マルチキャストグループのスタティックメンバーとして設定できます。その後、インターフェイスは常にグループのIPv6マルチキャストデータを受信できます。

スタティックグループメンバーは、MLDクエリーに応答しません。インターフェイス上でこの設定を完了またはキャンセルすると、インターフェイスは非送信請求MLDレポートまたはdoneメッセージを送信しません。

制約事項とガイドライン

IPv6マルチキャストグループのスタティックメンバーとして設定されるインターフェイスには、次の制約事項があります。

- インターフェイスがMLDで、IPv6 PIM-SMが有効の場合、そのインターフェイスはIPv6 PIM-SM DRである必要があります。
- インターフェイスでMLDが有効で、IPv6 PIM-SMが有効でない場合、MLDクエリーアである必要があります。IPv6 PIM-SMおよびDRの詳細については、「IPv6 PIMの設定」を参照してください。

手順

1. システムビューに入ります。

system-view

2. インターフェイスビューに入ります。

interface *interface-type* *interface-number*

3. スタティックグループメンバーを設定します。

```
mld static-group ipv6-group-address [ source ipv6-source-address ]
```

IPv6マルチキャストグループポリシーの設定

IPv6マルチキャストグループポリシーについて

この機能により、インターフェイスは、IPv6マルチキャストグループとオプションの送信元を指定するACLを使用して、MLDレポートをフィルタリングできます。これは、インターフェイスに接続されたホストが加入できるIPv6マルチキャストグループを制御するために使用されます。

制約事項とガイドライン

スタティックグループメンバーはMLDレポートを送信しないので、このコンフィグレーションは、スタティックグループメンバーに影響を与えません。

手順(

1. システムビューに入ります。

```
system-view
```

2. インターフェイスビューに入ります。

```
interface interface-type interface-number
```

3. インターフェイス上でIPv6マルチキャストグループポリシーを設定します。

```
mld group-policy ipv6-acl-number [ version-number ]
```

MLDパフォーマンスの調整

MLDクエリーおよび応答パラメータの設定

MLDクエリーおよび応答パラメータの概要

次に、MLDクエリーおよび応答パラメータを示します。

- **MLD querier's robustness variable:** パケット損失時にMLDクエリーを再送信する回数。ロバストネス変数が高いほどMLDクエリーはより堅牢になりますが、IPv6マルチキャストグループのタイムアウト時間が長くなります。
- **MLD startup query interval:** MLDクエリーが起動時にMLD一般クエリーを送信する間隔。
- **MLD startup query count:** MLDクエリーが起動時に送信するMLD一般クエリーの数。
- **MLD general query interval:** MLDクエリーがネットワーク上のIPv6マルチキャストグループメンバーをチェックするためにMLD一般クエリーを送信する間隔。
- **MLD last listener query interval:** MLDv1では、クエリーがdoneメッセージを受信した後にマルチキャストアドレス固有のクエリーを送信する間隔を設定します。MLDv2では、クエリーがIPv6マルチキャスト送信元およびグループマッピングを変更するレポートを受信した後にマルチキャストアドレスおよび送信元固有のクエリーを送信する間隔を設定します。

- **MLD last listener query count:** MLDv1では、クエリーがdoneメッセージを受信した後に送信するマルチキャストアドレス固有のクエリー数を設定します。MLDv2では、クエリーがIPv6マルチキャストグループおよび送信元マッピングを変更するレポートを受信した後に送信するマルチキャストアドレスおよび送信元固有のクエリー数を設定します。
- **MLD maximum response time:** レシーバがMLD一般クエリーにレポートで応答するまでの最大時間。このグループ単位のタイマーは、0からMLDクエリーで指定された最大応答時間までの範囲のランダム値に初期化されます。タイマー値が0に減少すると、レシーバはMLDレポートをグループに送信します。
- **MLD other querier present timer:** 非クエリーがMLD一般クエリーを受信した後のMLDクエリーのMLD Other Querier present timer。このタイマーが満了したときに非クエリーが新しいクエリーを受信しなかった場合、非クエリーはクエリーが失敗したと見なし、新しいクエリーの選択を開始します。

制約事項とガイドライン

- MLDクエリーが頻繁に変更されないようにするには、MLD一般クエリーインターバルよりも大きいMLD他クエリー存在タイマーを設定します。さらに、同じサブネット上のすべてのMLDデバイスに対して、同じMLD他クエリー存在タイマーを設定します。
- MLDクエリーへの応答を高速化し、MLDレポートトラフィックバーストの原因となる同時タイマー時間切れを回避するには、適切な最大応答時間を設定する必要があります。
MLDの一般的なクエリーの場合、最大応答時間は**max-response-time**コマンドによって設定されます。
 - MLDマルチキャストアドレス固有のクエリーまたはMLDマルチキャストアドレスおよび送信元固有のクエリーの場合、最大応答時間はMLD最終リスナークエリーインターバルと等しくなります。
- MLDビューのすべてのインターフェイスに対してグローバルに、またはインターフェイスビューのインターフェイスに対してMLDクエリーおよび応答パラメータを設定できます。インターフェイス固有の設定は、グローバル設定よりも優先されます。

MLDクエリーおよび応答パラメータのグローバルな設定

1. システムビューに入ります。
system-view
2. MLDビューを入力します。
mld
3. MLDクエリーのロバストネス変数を設定します。
robust-count count
デフォルトでは、MLDクエリーのロバストネス変数は2です。
4. MLDスタートアップクエリーインターバルを設定します。
startup-query-interval interval

デフォルトでは、MLDスタートアップクエリインターバルは、MLD一般クエリインターバルの4分の1に等しくなります。

5. MLDスタートアップクエリカウントを設定します。

startup-query-count *count*

デフォルトでは、MLDスタートアップクエリカウントは、MLDクエリアのロバストネス変数と同じです。

6. MLD一般クエリインターバルを設定します。

query-interval *interval*

デフォルトでは、MLD一般クエリインターバルは125秒です。

7. MLD最終リスナークエリインターバルを設定します。

last-listener-query-interval *interval*

デフォルトでは、MLD最終リスナークエリインターバルは1秒です。

8. MLD最終リスナークエリカウントを設定します。

last-listener-query-count *count*

デフォルトでは、MLD最終リスナークエリカウントは、MLDクエリアのロバストネス変数と同じです。

9. MLD一般クエリの最大応答時間を設定します。

max-response-time *time*

デフォルトでは、MLD一般クエリの最大応答時間は10秒です。

10. MLD Other Querier presentタイマーを設定します。

other-querier-present-timeout *time*

デフォルトでは、 $[\text{MLD general query interval}] \times [\text{MLD robustness variable}] + [\text{MLD general queriesのmaximum response time}] / 2$ という式を使用して、MLDの他のクエリアの存在タイマーが計算されます。

インターフェイス上のMLDクエリおよびレスポンスパラメータの設定

1. システムビューに入ります。

system-view

2. インターフェイスビューに入ります。

interface*interface-type interface-number*

3. MLDクエリアのロバストネス変数を設定します。

mld robust-count *count*

デフォルトでは、MLDクエリアのロバストネス変数は2です。

4. MLDスタートアップクエリインターバルを設定します。

mld startup-query-interval *interval*

デフォルトでは、MLDスタートアップクエリインターバルは、MLD一般クエリインターバルの4分の1に等しくなります。

5. MLDスタートアップクエリーカウントを設定します。

mld startup-query-count *count*

デフォルトでは、MLDスタートアップクエリーカウントは、MLDクエリーアのロバストネス変数と同じです。

6. MLD一般クエリーインターバルを設定します。

mld query-interval *interval*

デフォルトでは、MLD一般クエリーインターバルは125秒です。

7. MLD最終リスナークエリーインターバルを設定します。

mld last-listener-query-interval *interval*

デフォルトでは、MLD最終リスナークエリーインターバルは1秒です。

8. MLD最終リスナークエリーカウントを設定します。

mld last-listener-query-count *count*

デフォルトでは、MLD最終リスナークエリーカウントは、MLDクエリーアのロバストネス変数と同じです。

9. MLD一般クエリーの最大応答時間を設定します。

mld max-response-time *time*

デフォルトでは、MLD一般クエリーの最大応答時間は10秒です。

10. MLD Other Querier presentタイマーを設定します。

mld other-querier-present-timeout *time*

デフォルトでは、 $[\text{MLD general query interval}] \times [\text{MLD robustness variable}] + [\text{MLD general queriesの最大応答時間}] / 2$ という式を使用して、MLDの他のクエリーアの存在タイマーが計算されます。

高速脱退処理の有効化

高速脱退処理について

この機能を使用すると、MLDクエリーアは、doneメッセージの受信後にマルチキャストアドレス固有のクエリーまたはマルチキャストアドレスおよび送信元固有のクエリーを送信せずに、アップストリームにLeave通知を送信できます。この機能を使用して、脱退遅延を短縮し、ネットワーク帯域幅を確保します。

手順

1. システムビューに入ります。

system-view

2. インターフェイスビューに入ります。

interface *interface-type interface-number*

3. 高速脱退処理を有効にします。

mld fast-leave [**group-policy** *ipv6-acl-number*]

デフォルトでは、高速脱退処理は無効です。

MLD SSMマッピングの設定

MLD SSMマッピングの概要

この機能により、デバイスはMLDv1ホストにSSMサービスを提供できます。

制約事項とガイドライン

この機能はMLDv2メッセージを処理しません。MLDv2レシーバホストからのMLDv2レポートを処理できるようにするには、レシーバ側インターフェイスでMLDv2を有効にします。

手順

1. システムビューに入ります。
system-view
2. MLDビューを入力します。
mld
3. MLD SSMマッピングを設定します。
mld fast-leave [group-policy ipv6-acl-number]

MLDプロキシの設定

MLDプロキシの前提条件

MLDプロキシを設定する前に、ネットワークポロジに基づいてルータインターフェイスとホストインターフェイスを決定します。次に、ルータインターフェイスでMLDを有効にします。

MLDプロキシの有効化

制約事項とガイドライン

- 受信側インターフェイスでMLDプロキシを有効にします。
- MLDプロキシを有効にしたインターフェイスでは、**mldversion**コマンドだけが有効になり、他のMLDコマンドは有効になりません。
- 同じデバイス上でMLDプロキシとIPv6マルチキャストルーティングプロトコルの両方を有効にした場合、IPv6マルチキャストルーティングプロトコルは有効になりません。

手順

1. システムビューに入ります。
system-view
2. インターフェイスビューに入ります。
interface interface-type interface-number
3. MLDプロキシを有効にします。

mld proxy enable

デフォルトでは、MLDプロキシは無効です。

非クエリーインターフェイス上のIPv6マルチキャストフォワーディングの有効化

非クエリーインターフェイスのIPv6マルチキャストフォワーディング機能について

通常、IPv6マルチキャストトラフィックを転送できるのはMLDクエリーアだけで、非クエリーアは転送できません。これにより、IPv6マルチキャストデータが繰り返し転送されることがなくなります。MLDプロキシのルータインターフェイスがクエリーアの選択に失敗した場合、IPv6マルチキャストデータをダウンストリームレシーバに転送するには、インターフェイスでIPv6マルチキャスト転送を有効にします。

制約事項とガイドライン

共有メディアネットワークには、クエリーアとして動作する1つのプロキシを含む、複数のMLDプロキシが存在する場合があります。重複したIPv6マルチキャストトラフィックを回避するには、ネットワークの非クエリーアMLDプロキシでIPv6マルチキャスト転送を有効にしないでください。

手順

1. システムビューに入ります。

system-view

2. インターフェイスビューに入ります。

interface *interface-type* *interface-number*

3. 非クエリーアインターフェイスでIPv6マルチキャストフォワーディングを有効にしてください。

mld proxy forwarding

デフォルトでは、IPv6マルチキャストフォワーディングは、非クエリーアインターフェイスで無効です。

MLDプロキシインターフェイスのIPv6マルチキャストロードスプリットの有効化

MLDプロキシインターフェイスのIPv6マルチキャストロードスプリットの有効化の概要

デバイス上に複数のMLDプロキシインターフェイスが存在する場合、最上位のIPアドレスを持つプロキシインターフェイスだけがIPv6マルチキャストトラフィックを転送します。すべてのプロキシインターフェイスがIPv6マルチキャストトラフィックを共有できるように、デバイス上でIPv6マルチキャストロードスプリットを有効にできます。

手順

1. システムビューに入ります。

system-view

2. MLDビューを入力します。

mld

3. MLDプロキシインターフェイスのIPv6マルチキャストロードスプリットを有効にします。

proxy multipath

デフォルトでは、IPv6マルチキャストロードスプリットはMLDプロキシインターフェイスに対して無効です。

MLD NSRの有効化

MLD NSRの概要

この機能は、MLDインターフェイスおよびMLDマルチキャストグループに関する情報をスタンバイプロセスにバックアップします。アクティブ/スタンバイスイッチオーバーが発生した場合、デバイスは他のデバイスの協力なしに情報を回復します。この機能を使用して、アクティブ/スタンバイスイッチオーバーがIPv6マルチキャストサービスに影響を与えないようにします。

手順

1. システムビューに入ります。

system-view

2. MLD NSRを有効にします。

mld non-stop-routing

デフォルトでは、MLD NSRは無効です。

発信MLDプロトコルパケットのDSCP値の設定

発信MLDプロトコルパケットのDSCP値について

DSCP値は、パケット送信の優先順位を決定します。DSCP値が大きいほど、優先順位が高くなります。

手順

1. システムビューに入ります。

system-view

2. MLDビューを入力します。

mld

3. 発信MLDプロトコルパケットのDSCP値を設定します。

dscp dscp-value

デフォルトでは、発信MLDプロトコルパケットのDSCP値は48です。

MLDの表示およびメンテナンスコマンド

△注意:

reset mld groupコマンドを使用すると、IPv6マルチキャストデータ送信が失敗する場合があります。

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
MLDマルチキャストグループに関する情報を表示します。	display mld group [<i>ipv6-group-address</i> interface <i>interface-type interface-number</i>] [static verbose]
インターフェイスのMLD情報を表示します。	display mld interface [<i>interface-type interface-number</i>] [proxy] [verbose]
MLDプロキシによって保持されるIPv6マルチキャストルーティングエントリを表示します。	display mld proxy group [<i>ipv6-group-address</i> interface interface-type interface-number] [verbose]
MLDプロキシルーティングテーブルに関する情報を表示します。	display mld proxy routing-table [<i>ipv6-source-address</i> [<i>prefix-length</i>] <i>ipv6-group-address</i> [<i>prefix-length</i>]] * [verbose]
MLD SSMマッピングを表示します。	display mld ssm-mapping ipv6-group-address
ダイナミックMLDマルチキャストグループエントリをクリアします。	reset mld group { all interface interface-type interface-number { all <i>ipv6-group-address</i> [<i>prefix-length</i>] [<i>ipv6-source-address</i> [<i>prefix-length</i>]] } }

MLDの設定例

例:基本的なMLD機能の設定

ネットワークの設定

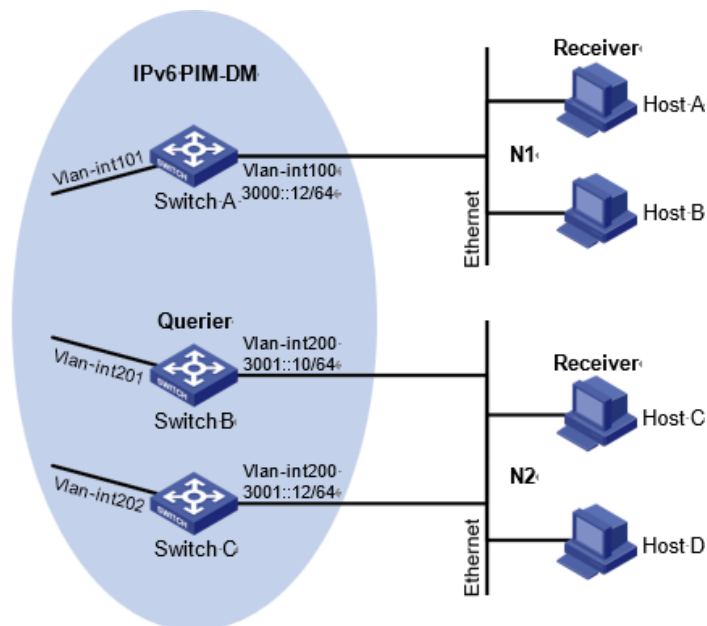
図81に示します。

- OSPFv3およびIPv6 PIM-DMはネットワーク上で動作します。
- VODストリームは、マルチキャストでレシーバホストに送信されます。異なる組織のレシーバホストは、スタブネットワークN1およびN2を形成します。ホストAおよびホストCは、それぞれN1およびN2のマルチキャストレシーバホストです。
- MLDv1は、スイッチAとN1の間、および他の2つのスイッチ(スイッチBとスイッチC)とN2の間で動作します。
- スwitch AはN1でMLDクエリアとして動作します。スイッチBはIPv6アドレスが小さいため、N2でMLDクエリアとして動作します。

次の要件を満たすようにスイッチを設定します。

- N1のホストは、IPv6マルチキャストグループFF1E::101だけに加入できます。
- N2のホストは、任意のIPv6マルチキャストグループに加入できます。

図81 ネットワークダイアグラム



手順

1. 図81に示すように、各インターフェイスにIPv6アドレスとプレフィクス長を割り当てます。(詳細は省略)
2. IPv6 PIM-DMドメイン内のスイッチにOSPFv3を設定します(詳細は省略)。
3. IPv6マルチキャストルーティング、MLD、およびIPv6 PIM-DMを有効にします。

#スイッチAで、IPv6マルチキャストルーティングを有効にします。

```
<SwitchA> system-view
[SwitchA] ipv6 multicast routing
[SwitchA-mrib6] quit
# Enable MLD on VLAN-interface 100.
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] quit
# Enable IPv6 PIM-DM on VLAN-interface 101.
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ipv6 pim dm
[SwitchA-Vlan-interface101] quit
# On Switch B, enable IPv6 multicast routing.
```

```
<SwitchB> system-view
[SwitchB] ipv6 multicast routing
[SwitchB-mrib6] quit
# Enable MLD on VLAN-interface 200.
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] mld enable
[SwitchB-Vlan-interface200] quit
# Enable IPv6 PIM-DM on VLAN-interface 201.
[SwitchB] interface vlan-interface 201
[SwitchB-Vlan-interface201] ipv6 pim dm
[SwitchB-Vlan-interface201] quit
# On Switch C, enable IPv6 multicast routing.
```

```
<SwitchC> system-view
[SwitchC] ipv6 multicast routing
[SwitchC-mrib6] quit
# Enable MLD on VLAN-interface 200.
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] mld enable
[SwitchC-Vlan-interface200] quit
# Enable IPv6 PIM-DM on VLAN-interface 202.
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] ipv6 pim dm
[SwitchC-Vlan-interface202] quit
```

4. スイッチ A 上で IPv6 マルチキャスト グループ ポリシーを設定し、VLAN インターフェース 100 に接続されているホストが IPv6 マルチキャスト グループ FF1E::101 にのみ参加できるようにします。

```
[SwitchA] acl ipv6 basic 2001
[SwitchA-acl-ipv6-basic-2001] rule permit source ff1e::101 128
[SwitchA-acl-ipv6-basic-2001] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld group-policy 2001
[SwitchA-Vlan-interface100] quit
```

設定の確認

#スイッチBのVLANインターフェイス200のMLD情報を表示します。

```
[SwitchB] display mld interface vlan-interface 200
Vlan-interface200(FE80::200:5EFF:FE66:5100):
  MLD is enabled.
  MLD version: 1
  Query interval for MLD: 125s
  Other querier present time for MLD: 255s
  Maximum query response time for MLD: 10s
  Querier for MLD: FE80::200:5EFF:FE66:5100 (This router)
  MLD groups reported in total: 1
```

例:MLD SSMマッピングの設定

ネットワークの設定

図82に示します。

- OSPFv3はネットワーク上で動作します。
- IPv6 PIM-SMドメインは、IPv6マルチキャスト配信にSSMモデルを使用します。SSMグループの範囲はFF3E::/64です。
- MLDv2はルータDのVLANインターフェイス400上で動作します。レシーバホストはMLDv1を実行し、MLDv2をサポートしません。レシーバホストは、メンバーシップレポートでIPv6マルチキャストソースを指定できません。
- 送信元1、送信元2、および送信元3は、IPv6 SSMグループ範囲FF3E::/64のマルチキャストグループにIPv6マルチキャストパケットを送信します。

レシーバホストがSource 1およびSource 3からだけIPv6マルチキャストデータを受信するように、スイッチDでMLD SSMマッピング機能を設定します。

図82 ネットワークダイアグラム

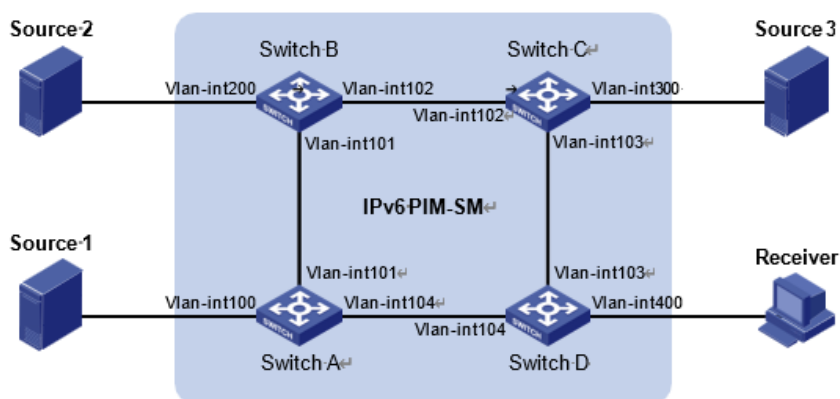


表17 インターフェイスおよびIPv6アドレス割り当て

デバイス	インターフェイス	IPv6アドレス	デバイス	インターフェイス	IPv6アドレス
Source1	-	1001::1/64	Source3	-	3001::1/64
Source2	-	2001::1/64	Receiver	-	4001::1/64

Switch A	VLAN-int100	1001::2/64	Switch C	Vlan-int300	3001::2/64
Switch A	Vlan-int101	1002::1/64	Switch C	Vlan-int103	3002::1/64
Switch A	Vlan-int104	1003::1/64	Switch C	Vlan-int102	2002::2/64
Switch B	Vlan-int200	2001::2/64	Switch D	Vlan-int400	4001::2/64
Switch B	Vlan-int101	1002::2/64	Switch D	Vlan-int103	3002::2/64
Switch B	Vlan-int102	2002::1/64	Switch D	Vlan-int104	1003::2/64

手順

1. 表17に示すように、各インターフェイスにIPv6アドレスとプレフィク長を割り当てます。(詳細は省略)
2. IPv6 PIM-SMドメイン内のスイッチにOSPFv3を設定します(詳細は省略)。
3. IPv6マルチキャストルーティングを有効にし、IPv6 PIM-SMおよびMLDを有効にします。

On Switch D, enable IPv6 multicast routing.

```
<SwitchD> system-view
```

```
[SwitchD] ipv6 multicast routing
```

```
[SwitchD-mrib6] quit
```

Enable MLDv2 on the receiver-side interface (VLAN-interface 400).

```
[SwitchD] interface vlan-interface 400
```

```
[SwitchD-Vlan-interface400] mld enable
```

```
[SwitchD-Vlan-interface400] mld version 2
```

```
[SwitchD-Vlan-interface400] quit
```

Enable IPv6 PIM-SM on the other interfaces.

```
[SwitchD] interface vlan-interface 103
```

```
[SwitchD-Vlan-interface103] ipv6 pim sm
```

```
[SwitchD-Vlan-interface103] quit
```

```
[SwitchD] interface vlan-interface 104
```

```
[SwitchD-Vlan-interface104] ipv6 pim sm
```

```
[SwitchD-Vlan-interface104] quit
```

On Switch A, enable IPv6 multicast routing.

```
<SwitchA> system-view
```

```
[SwitchA] ipv6 multicast routing
```

```
[SwitchA-mrib6] quit
```

Enable IPv6 PIM-SM on each interface.

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] ipv6 pim sm
```

```
[SwitchA-Vlan-interface100] quit
```

```
[SwitchA] interface vlan-interface 101
```

```
[SwitchA-Vlan-interface101] ipv6 pim sm
```

```
[SwitchA-Vlan-interface101] quit
```

```
[SwitchA] interface vlan-interface 104
```

```
[SwitchA-Vlan-interface104] ipv6 pim sm
```

```
[SwitchA-Vlan-interface104] quit
```

#スイッチAを設定するのと同じ方法で、スイッチBとスイッチCを設定します(詳細は省略)。

4. IPv6 SSMグループ範囲を設定します。

```
[SwitchD] acl ipv6 basic 2000
[SwitchD-acl-ipv6-basic-2000] rule permit source ff3e:: 64
[SwitchD-acl-ipv6-basic-2000] quit
[SwitchD] pim ipv6
[SwitchD-pim6] ssm-policy 2000
[SwitchD-pim6] quit
```

#スイッチDを設定するのと同じ方法で、スイッチA、スイッチB、およびスイッチCを設定します。(詳細は省略)。

5. スイッチDでMLD SSMマッピングを設定します。

```
[SwitchD] mld
[SwitchD-mld] ssm-mapping 1001::1 2000
[SwitchD-mld] ssm-mapping 3001::1 2000
[SwitchD-mld] quit
```

設定の確認

#スイッチD上のIPv6マルチキャストグループFF3E::101に対するMLD SSMマッピングを表示します。

```
[SwitchD] display mld ssm-mapping ff3e::101
Group: FF3E::101
Source list:
  1001::1
  3001::1
```

On Switch D, display information about MLD multicast groups that hosts have dynamically joined.

```
[SwitchD] display mld group
MLD groups in total: 1
Vlan-interface400(FE80::101):
  MLD groups reported in total: 1
  Group address: FF3E::101
  Last reporter: FE80::1
  Uptime: 00:02:04
  Expires: Off
```

Display IPv6 PIM routing entries on Switch D.

```
[SwitchD] display ipv6 pim routing-table
Total 0 (*, G) entry; 2 (S, G) entry
```

```
(1001::1, FF3E::101)
  Protocol: pim-ssm, Flag:
  UpTime: 00:13:25
  Upstream interface: Vlan-interface104
    Upstream neighbor: 1003::1
    RPF prime neighbor: 1003::1
  Downstream interface(s) information: Total
  number of downstreams: 1
    1: Vlan-interface400
      Protocol: mld, UpTime: 00:13:25, Expires: -
```

```
(3001::1, FF3E::101)
```

Protocol: pim-ssm, Flag:
 UpTime: 00:13:25
 Upstream interface: Vlan-interface103
 Upstream neighbor: 3002::1
 RPF prime neighbor: 3002::1
 Downstream interface(s) information:
 Total number of downstreams: 1
 1:Vlan-interface400
 Protocol: mld, UpTime: 00:13:25, Expires: -

例:MLDプロキシの設定

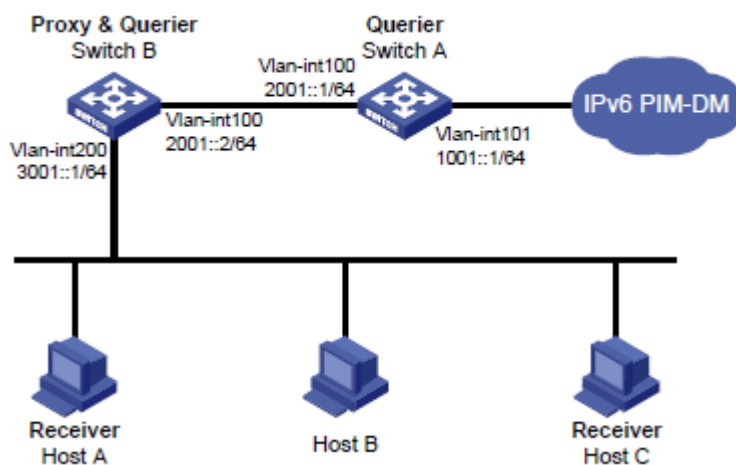
ネットワークの設定

図83に示します。

- IPv6 PIM-DMはコアネットワーク上で動作します。
- スタブネットワーク上のホストAとホストCは、IPv6マルチキャストグループFF3E::101宛てのビデオオンデマンド情報を受信します。

スイッチBがグループメンバーシップを維持し、IPv6 PIM-DMを実行せずにIPv6マルチキャストトラフィックを転送できるように、スイッチBでMLDプロキシ機能を設定します。

図83 ネットワークダイアグラム



手順

1. 図83に示すように、各インターフェイスにIPv6アドレスとプレフィクス長を割り当てます(詳細は省略)。

2. IPv6マルチキャストルーティング、IPv6 PIM-DM、MLD、およびMLDプロキシを有効にします。

On Switch A, enable IPv6 multicast routing.

```
<SwitchA> system-view
```

```
[SwitchA] ipv6 multicast routing
```

```
[SwitchA-mrib6] quit
```

Enable IPv6 PIM-DM on VLAN-interface 101.

```
[SwitchA] interface vlan-interface 101
```

```
[SwitchA-Vlan-interface101] ipv6 pim dm
[SwitchA-Vlan-interface101] quit
# Enable MLD on VLAN-interface 100.
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] quit
# On Switch B, enable IPv6 multicast routing.
<SwitchB> system-view
[SwitchB] multicast ipv6 routing-enable
[SwitchB-mrib6] quit
# Enable MLD proxying on VLAN-interface 100.
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] mld proxying enable
[SwitchB-Vlan-interface100] quit
# Enable MLD on VLAN-interface 200.
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] mld enable
[SwitchB-Vlan-interface200] quit
```

設定の確認

#スイッチB上のMLDプロキシが保持するIPv6マルチキャストグループメンバーシップ情報を表示します。

```
[SwitchB] display mld proxy group
MLD proxy group records in total: 1
Vlan-interface100(FE80::16:1):
MLD proxy group records in total: 1
Group address: FF1E::1
Member state: Delay
Expires: 00:00:02
```

MLDのトラブルシューティング

受信側の機器にメンバー情報が存在しない

症状

ホストがIPv6マルチキャストグループGに参加することをアナウンスするメッセージを送信する場合、直接のデバイスにはマルチキャストグループGのメンバー情報は存在しません。

解決方法

この問題を解決するには、次の手順を実行し

1. ネットワーク、インターフェイス接続、およびIPアドレス設定が正しいことを確認するには、**display mld interface**コマンドを使用します。
2. ipv6マルチキャストルーティングが有効になっていることを確認するには、**display current-configuration**コマンドを使用します。有効になっていない場合は、システムビ

ユーで**ipv6 multicast routing**コマンドを使用して、ipv6マルチキャストルーティングを有効にします。さらに、関連するインターフェイスでMLDが有効になっていることを確認します。

3. インターフェイス上のMLDバージョンがホスト上のバージョンよりも低いことを確認するには、**display mld interface**コマンドを使用します。
4. IPv6マルチキャストグループGのMLDレポートをフィルタリングするIPv6マルチキャストグループポリシーが設定されていないことを確認するには、**display current-configuration interface**コマンドを使用します。
5. 問題が解決しない場合は、H3Cサポートに連絡してください。

同一サブネット上のデバイスの一貫性のないメンバーシップ情報

症状

同一サブネット上の異なるMLDデバイスで異なるメンバーシップが維持されます。

解決方法

この問題を解決するには、次の手順を実行し

1. インターフェイスのMLD情報を確認するには、**display current-configuration**コマンドを使用します。サブネット上のデバイスのインターフェイスに同じMLD設定があることを確認します。
2. MLDタイマーに矛盾した設定がないかチェックするには、同じサブネット上のすべてのデバイスで**display mld interface**コマンドを使用します。
3. すべてのデバイスが同じMLDバージョンを実行していることを確認するには、**display mld interface**コマンドを使用します。
4. 問題が解決しない場合は、H3Cサポートに連絡してください。

IPv6 PIMの設定

IPv6 PIMの概要

IPv6 Protocol Independent Multicast(IPv6 PIM)は、任意のIPv6ユニキャストルーティングプロトコルによって生成されたIPv6ユニキャストスタティックルートまたはIPv6ユニキャストルーティングテーブルを利用して、IPv6マルチキャスト転送を提供します。IPv6 PIMは、基礎となるIPv6ユニキャストルーティングを使用して、特定のIPv6ユニキャストルーティングプロトコルに依存せずにIPv6マルチキャストルーティングテーブルを生成します。

IPv6 PIMは、RPFメカニズムを使用してIPv6マルチキャストフォワーディングを実装します。RPFの詳細については、「IPv6マルチキャストルーティングおよびフォワーディングの設定」を参照してください。

IPv6 PIMモード

実装メカニズムに基づいて、IPv6 PIMには次のモードがあります。

- IPv6 Protocol Independent Multicast Dense Mode(IPv6 PIM-DM)。
- IPv6 Protocol Independent Multicast:スパースモード(IPv6 PIM-SM)。
- IPv6 Protocol Independent Multicast Source-Specific Multicast(IPv6 PIM-SSM)。

このマニュアルでは、IPv6 PIMドメインとは、IPv6 PIMデバイスで構成されるネットワークを指します。

IPv6 PIM-DM

IPv6 PIM-DMは、マルチキャスト転送にプッシュモードを使用し、IPv6マルチキャストメンバーが密集して分散している小規模ネットワークに適しています。

IPv6 PIM-DMは、すべてのダウンストリームノードが送信元からIPv6マルチキャストデータを受信することを想定しているため、IPv6マルチキャストデータはネットワーク上のすべてのダウンストリームノードにフラッディングされます。ダウンストリームレシーバのないブランチは、フォワーディングツリーからプルーニングされ、レシーバを含むブランチだけが残される。プルーニングされたブランチに新しいレシーバがある場合、グラフトメカニズムは、プルーニングされたブランチをフォワーディングブランチに変換する。

IPv6 PIM-DMでは、IPv6マルチキャストグループのマルチキャスト転送パスによって転送ツリーが構成されます。転送ツリーはIPv6マルチキャスト送信元をルートとし、その「リーフ」としてマルチキャストグループメンバーを持ちます。転送ツリーは、IPv6マルチキャスト送信元から受信者への最短パスで構成されるため、「Shortest Path Tree(SPT)」とも呼ばれます。

IPv6 PIM-DMメカニズムには、ネイバー探索、SPT構築、グラフト、およびアサートが含まれます。

近隣探索

IPv6 PIMドメインでは、各IPv6 PIMインターフェイスが定期的にIPv6 PIM helloメッセージをローカルサブネット上の他のすべてのIPv6 PIMデバイスにマルチキャストします。helloメッセージの交換を通じて、すべてのIPv6 PIMデバイスはIPv6 PIMネイバーを決定し、他のデバイスとのIPv6 PIMネイバー関係を維持し、SPTを構築して維持します。

SPT構築

SPTを構築するプロセスは、flood-and-pruneプロセスです。

1. IPv6 PIM-DMドメインでは、IPv6マルチキャスト送信元SからIPv6マルチキャストグループGへのIPv6マルチキャストデータがドメイン全体にフラッディングされます。デバイスは、IPv6マルチキャストデータに対してRPFチェックを実行します。チェックが成功すると、デバイスは(S, G)エントリを作成し、ネットワーク内のすべてのダウンストリームノードにデータを転送します。フラッディングプロセスでは、IPv6 PIM-DMドメイン内のすべてのデバイスが(S, G)エントリを作成します。
2. ダウンストリームレシーバを持たないノードはプルーンングされます。ダウンストリームレシーバを持たないデバイスは、サブネット上のすべてのIPv6 PIMデバイスにプルーンングメッセージをマルチキャストします。

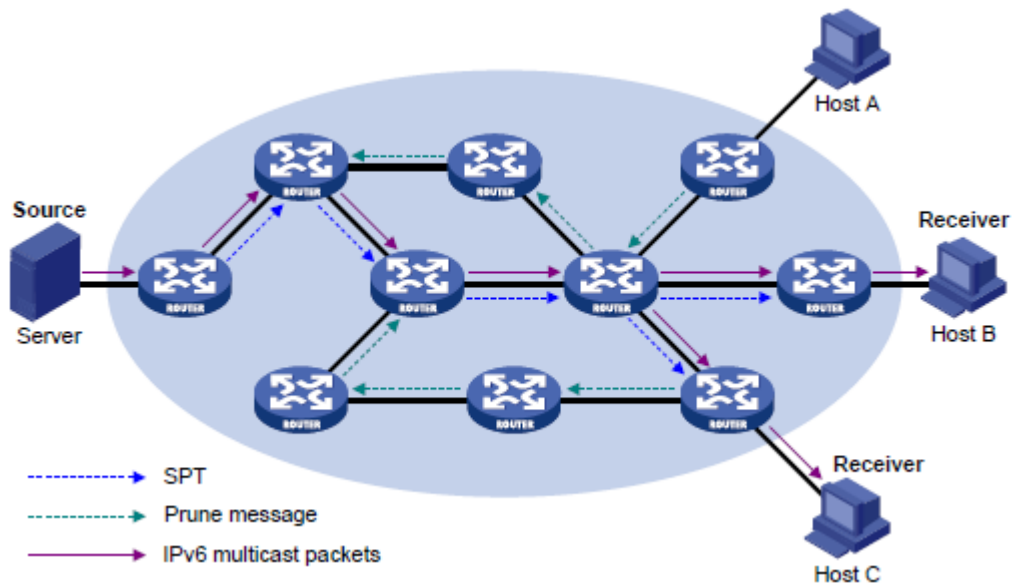
アップストリームノードはプルーンメッセージを受信すると、(S, G)エントリから受信インターフェイスを削除します。このようにして、アップストリームストリームノードは、そのIPv6マルチキャストグループ宛ての後続のパケットをこのノードに転送するのを停止します。

注:

(S, G)エントリには、IPv6マルチキャスト送信元アドレスS、IPv6マルチキャストグループアドレスG、送信インターフェースリスト、および受信インターフェースが含まれます。

プルーンプロセスは、リーフデバイスによって開始されます。図84に示されるように、ダウンストリームレシーバを持たないデバイスインターフェイスは、IPv6マルチキャスト送信元に向けてプルーンメッセージを送信することによって、プルーンプロセスを開始します。このプルーンプロセスは、必要なブランチだけがIPv6 PIM-DMドメインに残され、これらの必要なブランチがSPTを構成するまで続きます。

図84 SPT構築



ブランチのプルーニングされた状態には、有限のホールドタイムタイマーがあります。タイマーが期限切れになると、IPv6マルチキャストデータはプルーニングされたブランチに再び転送されます。フラッディングとプルーニングのサイクルは、転送ブランチを維持するために定期的に行われます。

Graft

以前にプルーニングされたブランチには、新しいダウンストリームレシーバが存在する場合があります。このブランチの転送機能を再開するための遅延を短縮するために、次のようなグラフトメカニズムが使用されます。

1. IPv6マルチキャストデータを受信する必要があるノードは、上流ノードにSPTへの再加入を指示するグラフトメッセージを送信します。
2. インターフェイス上でこのグラフトメッセージを受信した後、アップストリームノードは受信インターフェイスを(S, G)エントリの発信インターフェイスリストに追加します。また、graft-ackメッセージをグラフト送信者に送信します。
3. グラフト送信者がgraft-ackメッセージを受信した場合、グラフトプロセスは終了します。それ以外の場合、グラフト送信者は、上流ノードから確認応答を受信するまで、グラフト再試行間隔でグラフトメッセージを送信し続けます。

Assert

複数のマルチキャストデバイスがあるサブネットでは、アサートメカニズムによって、ネットワークへの重複したマルチキャストフローが遮断されます。これは、サブネットに固有のマルチキャストフォワーダを選択することによって行われます。

図85 アサートメカニズム

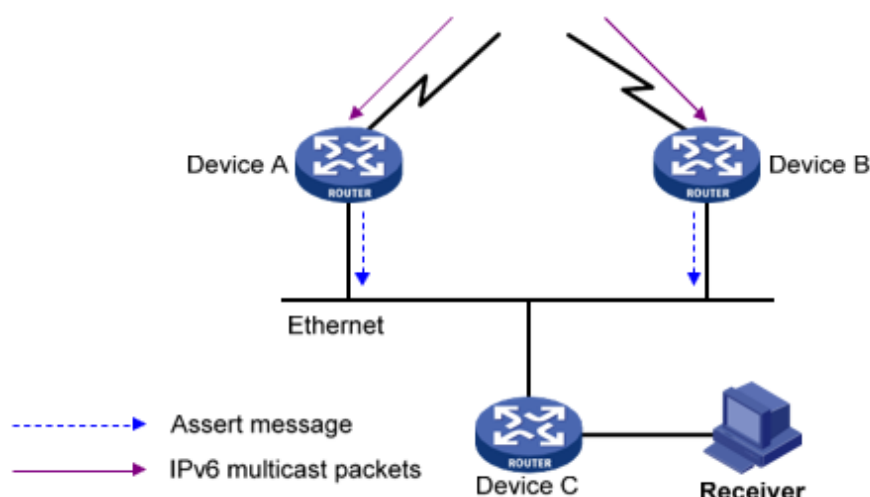


図85に示すように、デバイスAとデバイスBは、アップストリームノードから(S, G)パケットを受信した後、両方ともパケットをローカルサブネットに転送します。その結果、ダウンストリームノードのデバイスCは、2つの同一のマルチキャストパケットを受信します。さらに、ダウンストリームインターフェイス上のデバイスAとデバイスBは、もう一方から転送された重複パケットを受信します。この状態を検出すると、両方のデバイスは、パケットを受信したインターフェイスを介して、ローカルサブネット上のすべてのIPv6 PIMデバイスにアサートメッセージを送信します。アサートメッセージには、IPv6マルチキャスト送信元アドレス(S)、IPv6マルチキャストグループアドレス(G)、およびIPv6マルチキャスト送信元へのIPv6ユニキャストルート/MBGPルート/スタティックマルチキャストルートのメトリックプリファレンスとメトリックが含まれます。これらのパラメータを比較することにより、デバイスAまたはデバイスBのいずれかが、サブネット上の後続の(S, G)パケットの一意のフォワーダになります。比較プロセスは次のとおりです。

1. IPv6マルチキャスト送信元に対してより高いメトリック優先度を持つデバイスが勝ちます。
2. 両方のデバイスがIPv6マルチキャスト送信元に対して同じメトリックプリファレンスを持つ場合、IPv6マルチキャスト送信元に対してより小さいメトリックを持つデバイスが優先されます。
3. 両方のデバイスのメトリックが同じである場合、ダウンストリームインターフェイス上で上位のIPv6リンクローカルアドレスを持つデバイスが優先されます。

IPv6 PIM-SM

IPv6 PIM-DMは、flood-and-pruneサイクルを使用して、IPv6マルチキャストデータフォワーディング用のSPTを構築します。SPTは、IPv6マルチキャスト送信元から受信側への最短パスを持ちますが、低い効率で構築されます。そのため、IPv6 PIM-DMは、大規模および中規模のネットワークには適していません。IPv6 PIM-SMは、IPv6マルチキャスト転送にブルモードを使用します。これは、IPv6マルチキャストグループメンバーがまばらに広く分散している大規模および中規模のネットワークに適しています。

IPv6 PIM-SMは、ホストがIPv6マルチキャストデータを必要としないことを前提としています。マルチキャストレシーバは、データが転送される前に、IPv6マルチキャストグループのIPv6マルチキャストデータへの

関心を示す必要があります。Rendezvous Point(RP)は、IPv6 PIM-SMドメインのコアです。RPに依存して、SPTおよびRendezvous Point Tree(RPT)が確立され、IPv6マルチキャストデータフォワーディングを実装するために維持されます。SPTはIPv6マルチキャストソースをルートとし、そのリーフとしてRPを持ちます。RPTはRPをルートとし、そのリーフとしてレシーバホストを持ちます。

IPv6 PIM-SMメカニズムには、ネイバーディスカバリ、DR選定、RPディスカバリ、エニーキャストRP、RPT構築、マルチキャスト送信元登録、SPTへのスイッチオーバー、およびアサートが含まれます。

近隣探索

IPv6 PIM-SMは、IPv6 PIM-DMと同じネイバー探索メカニズムを使用します。詳細については、「ネイバー探索」を参照してください。

DR選定

Designated Router(DR)は、ソース側のネットワークとレシーバ側のネットワークの両方で必要です。ソース側のDRは、IPv6マルチキャストソースに代わって動作し、登録メッセージをRPに送信します。レシーバ側のDRは、レシーバホストに代わって動作し、JoinメッセージをRPに送信します。

❗重要:

MLDは、レシーバ側のDRとして動作するデバイス上で有効にする必要があります。そうしないと、DRに接続されたレシーバホストはIPv6マルチキャストグループに加入できません。MLDの詳細については、「MLDの設定」を参照してください。

図86 DRの選択

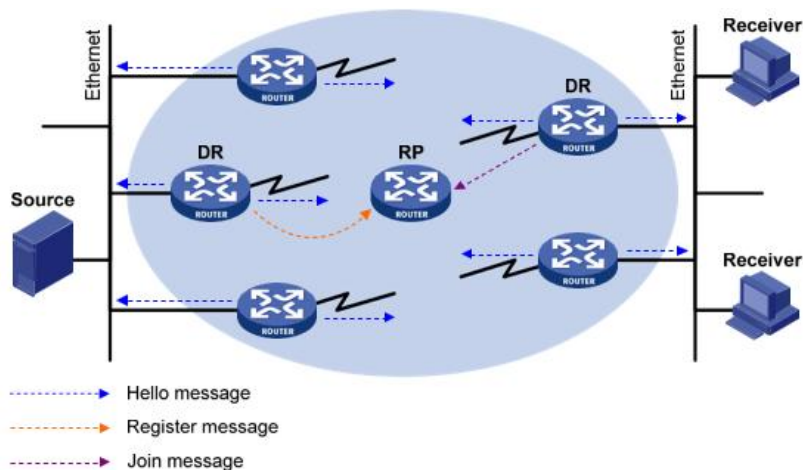


図86に示すように、DRの選定プロセスは次のとおりです。

1. 共有メディアLAN上のデバイスは、相互にhelloメッセージを送信します。helloメッセージには、DR選出のためのDRプライオリティが含まれています。DRプライオリティが最も高いデバイスがDRとして選出されます。
2. 次のいずれかの条件下では、最も大きいIPv6リンクローカルアドレスを持つデバイスがDR選定に勝ちます。
 - すべてのデバイスは、同じDR選定優先順位を持ちます。

- デバイスは、helloメッセージでのDRプライオリティの伝送をサポートしていません。

DRに障害が発生すると、そのIPv6 PIMネイバーのライフタイムが期限切れになり、他のデバイスが新しいDR選定を開始します。

RPディスカバリ

RPは、IPv6 PIM-SMドメインのコアです。IPv6マルチキャストグループは、IPv6マルチキャスト転送用に1つのRPだけを持つことができ、1つのRPを複数のIPv6マルチキャストグループに指定できます。RPは、Bootstrap Router(BSR)メカニズムを使用して、スタティックに設定することも、ダイナミックに選択することもできます。BSMメカニズムは、RPの負荷を軽減し、RPTのトポロジ構造を最適化します。

BSRメカニズムには、次のルールがあります。

- **Candidate-RP(C-RP)**: IPv6マルチキャストグループにサービスを提供するために、RPがC-RPから動的に選択されます。
- **BSR**: BSRは、IPv6 PIM-SMドメインの管理コアのコアです。ドメイン全体のRP情報の収集とアドバタイズを担当します。IPv6 PIM-SMドメインにはBSRが1つだけあり、BSRはC-BSRから選択されます。
- **Candidate-BSR(C-BSR)**: IPv6 PIM-SMドメイン内の任意のデバイスがC-BSRとして動作でき、BSRはC-BSRから選定されます。BSRに障害が発生すると、新しいBSRがマルチキャストトラフィックの中断を回避するためのC-BSR。

図87 C-RPとBSR間の情報交換

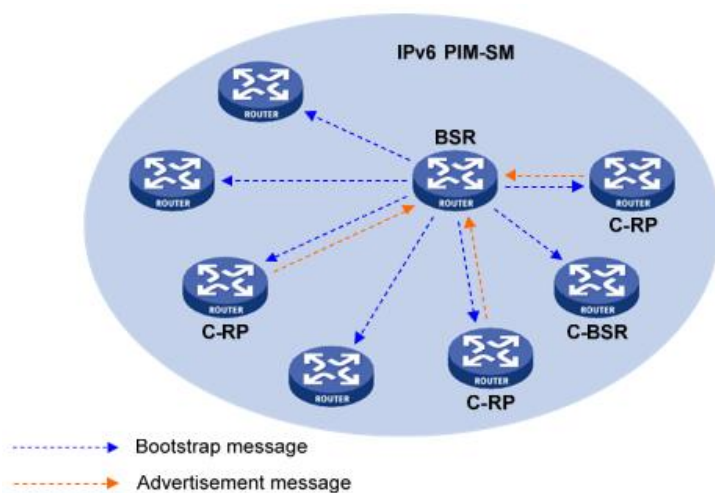


図87に示すように、RPは次のように選出されます。

1. 各C-BSRは、IPv6 PIM-SMドメイン内の他のデバイスにBootstrap Message(BSM)を送信します。
2. C-BSRは、別のC-BSRからBSMを受信すると、自身のプライオリティとメッセージで伝送されたプライオリティを比較します。プライオリティが高いC-BSRがBSRの選択に勝ちます。プライオリティが同じ場合は、IPv6アドレスが大きいC-BSRが選択されます。負けた方は、勝った方のBSRアドレスを使用して自身のBSRアドレスを置き換え、自身をBSRと見なさなくなります。勝った方は自身のBSRアドレスを保持し、自身をBSRと見なし続けます。
3. 各C-RPは、定期的アドバタイズメントメッセージをBSRにユニキャストします。アドバタイズメン

トメッセージには、アドバタイジングC-RPのアドレスと、それが指定されているIPv6マルチキャストグループ範囲が含まれます。

4. BSRはこれらのアドバタイズメントメッセージを収集し、C-RP情報をRPセットに編成します。RPセットは、IPv6マルチキャストグループとRP間のマッピングのデータベースです。BSRはRPセット情報をBootstrap Message(BSM)にカプセル化し、BSMをIPv6 PIM-SMドメイン全体にフラッディングします。
5. IPv6 PIM-SMドメイン内のすべてのデバイスは、次のルールに基づいてIPv6マルチキャストグループのRPを選択します。
 - a. 最小のIPv6マルチキャストグループ範囲に指定されたC-RPが勝利します。
 - b. 複数のC-RPが同じグループ範囲に指定されている場合は、プライオリティの最も高いC-RPが優先されます。
 - c. 複数のC-RPのプライオリティが同じ場合は、ハッシュ値が最大のC-RPが優先されます。ハッシュ値は、ハッシュアルゴリズムによって計算されます。
 - d. 複数のC-RPのハッシュ値が同じ場合は、IPアドレスが最も大きいC-RPが採用されます。

組み込みRP

組み込みRPメカニズムにより、デバイスはIPv6マルチキャストグループアドレスからRPアドレスを解決して、IPv6マルチキャストグループをRPにマッピングできます。このRPは、設定済みのステイックRPまたはブートストラップメカニズムによってダイナミックに選択されたRPの代わりに使用できます。DRは、事前にRPアドレスを学習する必要はありません。プロセスは次のとおりです。

- 受信側:
 - a. レシーバホストはMLDレポートを開始して、IPv6マルチキャストグループへの関係を示します。
 - b. MLDレポートを受信すると、レシーバ側のDRはIPv6マルチキャストグループアドレスに埋め込まれたRPアドレスを解決し、JoinメッセージをRPに送信します。
- IPv6マルチキャスト送信元側:
 - c. IPv6マルチキャスト送信元は、IPv6マルチキャストトラフィックをIPv6マルチキャストグループに送信します。
 - d. ソース側のDRは、IPv6マルチキャストアドレスに埋め込まれたRPアドレスを解決し、登録メッセージをRPに送信します。

エニーキャストRP

IPv6 PIM-SMでは、各IPv6マルチキャストグループにサービスを提供するアクティブRPが1つだけ必要です。アクティブRPに障害が発生すると、マルチキャストトラフィックが中断される可能性があります。エニーキャストRPメカニズムでは、1つのマルチキャストグループに対して同じIPv6アドレスを持つ複数のRPを設定することで、RP間の冗長バックアップが可能になります。IPv6マルチキャスト送信元は、最も近いRPに登録するか、受信側のDRが最も近いRPに加入して、送信元情報の同期を実装します。

エニーキャストRPには次の利点があります。

- **Optimal RP path:** IPv6マルチキャスト送信元は、最も近いRPに登録して、最適なSPTを構築し

ます。レシーバは、最も近いRPに加入して、最適なRPTを構築します。

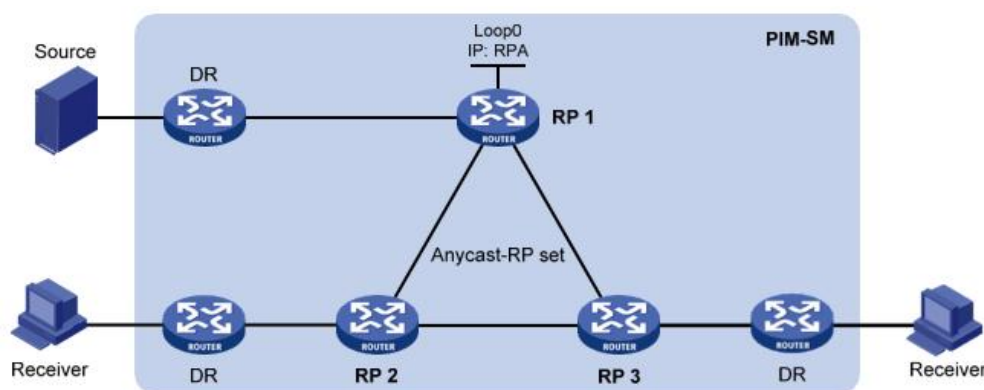
- **Redundancy backup among RPs** :RPに障害が発生すると、RP関連の送信元は利用可能な最も近いRPに登録され、受信側のDRは利用可能な最も近いRPに加入します。これにより、RP間の冗長バックアップが提供されます。

エニーキャストRPは、次のいずれかの方法を使用して実装されます。

- **Anycast RP through MSDP**: この方式では、1つのマルチキャストグループに対して同じIPアドレスを持つ複数のRPを設定し、それらのRP間にMSDPピアリング関係を設定できます。MSDPを介したエニーキャストRPの詳細については、「MSDPの設定」を参照してください。
- **Anycast RP through IPv6 PIM-SM**: この方式では、1つのIPv6マルチキャストグループに対して複数のRPを設定し、それらをエニーキャストRPセットに追加できます。この方式では、次の概念が導入されます。
 - **Anycast RP set**: 同じIPv6マルチキャストグループに指定されたRPのセット。
 - **Anycast RP member**: Anycast RPセット内の各RP。
 - **Anycast RP member address**: RPメンバー間の通信に使用される各エニーキャストRPメンバーのIPv6アドレス。
 - **Anycast RP address**: IPv6 PIM-SMドメイン内の通信用に設定されたエニーキャストRPのIPv6アドレス。RPAとも呼ばれます。

図88に示されるように、RP 1、RP 2およびRP 3は、エニーキャストRPセットのメンバーです。

図88 IPv6 PIM-SMを介したエニーキャストRP



次に、IPv6 PIM-SMを介したエニーキャストRPの実装方法について説明します。

- RP 1はRPA宛ての登録メッセージを受信します。このメッセージは他のエニーキャストRPメンバー(RP 2またはRP 3)からのものではないため、RP 1は登録メッセージがDR RP 1は、登録メッセージの送信元IPv6アドレスを自身のIPv6アドレスに変更し、他のメンバー(RP 2およびRP 3)にメッセージを送信します。
デバイスがDRとRPの両方として動作する場合、デバイスは登録メッセージを作成し、そのメッセージを他のRPメンバーに転送します。
- 登録メッセージを受信した後、RP 2およびRP 3は、登録メッセージの送信元アドレスがエニーキャストRPメンバーアドレスであることを確認し、他のデバイスへのメッセージの転送を停止しま

す。

エニーキャストRP実装では、RPはDRからの登録メッセージを他のエニーキャストRPメンバーに転送して、IPv6マルチキャスト送信元情報を同期化する必要があります。

RPT構築

図89 IPv6 PIM-SMドメインでのRPT構築

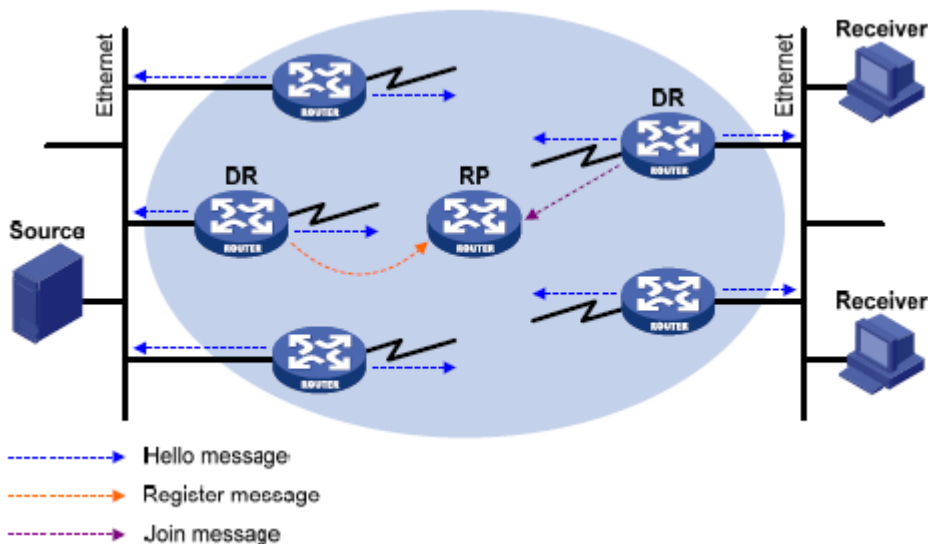


図89に示すように、RPTを構築するプロセスは次のとおりです。

1. レシーバは、IPv6マルチキャストグループGに加入する場合、MLDメッセージを使用してレシーバ側のDRに通知します。
2. レシーバ情報を取得した後、DRはJoinメッセージを送信します。このメッセージは、IPv6マルチキャストグループのRPにホップバイホップで送信されます。
3. DRからRPへのパス上のデバイスは、RPTブランチを形成します。このブランチ上の各デバイスは、転送テーブルに(*,G)エントリを追加します。アスタリスク(*)は任意のIPv6マルチキャストソースを表します。RPTはRPをルートとし、そのリーフとしてDRを持ちます。

IPv6マルチキャストグループG宛てのIPv6マルチキャストデータがRPに到達すると、RPは確立されたRPTに沿ってデータをDRに転送します。最後に、DRはIPv6マルチキャストデータをレシーバホストに転送します。

受信者がIPv6マルチキャストグループG宛てのIPv6マルチキャストデータを必要としなくなると、受信者側のDRはプルーンメッセージを送信します。プルーンメッセージは、RPTに沿ってRPまでホップバイホップで送信されます。プルーンメッセージを受信した後、アップストリームノードは、このダウンストリームノードに接続しているインターフェイスを発信インターフェイスリストから削除します。同時に、アップストリームデバイスは、そのIPv6マルチキャストグループの受信者の存在を確認します。IPv6マルチキャストグループの受信者が存在しない場合、デバイスはプルーンメッセージをアップストリームデバイスに転送し続けます。

IPv6マルチキャスト送信元登録

IPv6マルチキャスト送信元は、登録プロセスを使用して自身の存在をRPに通知します。

図90 IPv6マルチキャスト送信元登録

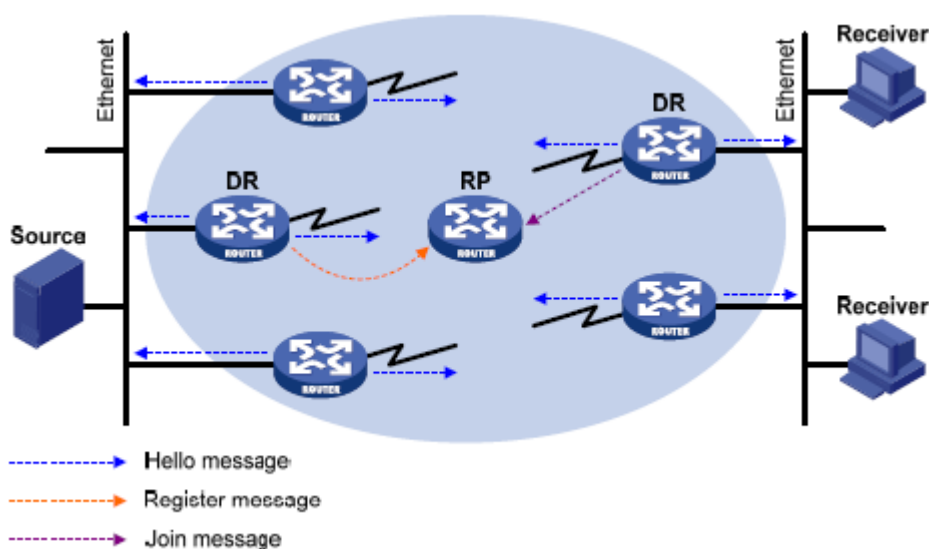


図90に示すように、IPv6マルチキャスト送信元は、次のようにRPに登録されます。

1. IPv6マルチキャストソースSは、最初のマルチキャストパケットをIPv6マルチキャストグループGに送信します。マルチキャストパケットを受信すると、IPv6マルチキャストソースに直接接続しているソース側のDRは、そのパケットを登録メッセージにカプセル化し、RPにユニキャストします。
2. RPは登録メッセージを受信すると、カプセル化を解除してRPTに転送します。同時に、(S, G)送信元固有の加入メッセージをIPv6マルチキャスト送信元に向けて送信します。RPからIPv6マルチキャスト送信元へのパス上のデバイスは、SPTブランチを構成します。このブランチ上の各デバイスは、転送テーブルに(S, G)エントリを作成します。
3. IPv6マルチキャスト送信元からの後続のIPv6マルチキャストデータは、SPTに従ってRPに転送されます。IPv6マルチキャストデータがSPTに従ってRPに到達すると、RPはデータをRPTに従ってレシーバに転送します。一方、登録停止メッセージをソース側のDRにユニキャストして、DRが不必要にデータをカプセル化ないようにします。

SPTへのスイッチオーバー

IPv6 PIM-SMドメインでは、1つのRPと1つのRPTだけが特定のIPv6マルチキャストグループにサービスを提供します。SPTへのスイッチオーバーが発生する前に、ソース側のDRはすべてのIPv6マルチキャストデータを登録メッセージにカプセル化し、RPに送信します。これらの登録メッセージを受信した後、RPはカプセル化を解除し、RPTに沿って受信側のDRに転送します。

RPTに沿ったIPv6マルチキャスト転送には、次の弱点があります。

- カプセル化とカプセル化解除は、ソース側のDRとRPでは複雑です。
- IPv6マルチキャストパケットのパスは、最短パスではない場合があります。
- RPは、IPv6マルチキャストトラフィックバーストによって過負荷になる可能性があります。

これらの弱点を排除するために、IPv6 PIM-SMでは、RPまたは受信側DRがIPv6マルチキャストトラフィックを受信したときに、RPまたはDRがSPTへのスイッチオーバーを開始できるようにします。

- RPはSPTへのスイッチオーバーを開始します。

RPは、IPv6マルチキャストトラフィックを受信すると、(S, G)送信元固有のJoinメッセージをIPv6マルチキャスト送信元に向けて送信します。RPからIPv6マルチキャスト送信元へのパス上のデバイスは、SPTブランチを構成します。後続のIPv6マルチキャストデータは、登録メッセージにカプセル化されずに、SPTに沿ってRPに転送されます。

RPによって開始されるSPTへのスイッチオーバーの詳細については、「IPv6マルチキャスト送信元登録」を参照してください。

- レシーバ側のDRは、SPTへのスイッチオーバーを開始します。
レシーバ側のDRは、IPv6マルチキャストトラフィックを受信すると、次のようにSPTへのスイッチオーバーを開始します。
 - a. レシーバ側のDRは、(S, G)送信元固有のJoinメッセージをIPv6マルチキャスト送信元に向けて送信します。パス上のデバイスは、転送テーブルに(S, G)エントリを作成して、SPTブランチを構成します。
 - b. マルチキャストパケットがRPTとSPTの分岐があるデバイスに到達すると、デバイスはRPTに沿って移動するマルチキャストパケットをドロップします。次に、RPビットを含むプルーンングメッセージをRPに向けて送信します。
 - c. プルーンメッセージを受信した後、RPはそれをIPv6マルチキャストソースに転送します(1つのレシーバだけが存在すると仮定します)。このようにして、SPTへのスイッチオーバーが完了します。IPv6マルチキャストグループの後続のIPv6マルチキャストパケットは、IPv6マルチキャストソースからレシーバホストまでSPTに沿って移動します。

SPTへのスイッチオーバーにより、IPv6 PIM-SMはIPv6 PIM-DMよりも経済的にSPTを構築します。

Assert

IPv6 PIM-SMは、IPv6 PIM-DMと同様のアサートメカニズムを使用します。詳細については、「アサート」を参照してください。

IPv6管理スコープ

通常、IPv6 PIM-SMDメインには、ドメイン全体でRPセット情報をアドバタイズする役割を持つBSRが1つだけ含まれています。すべてのIPv6マルチキャストグループに関する情報は、BSRが管理するネットワーク内で転送されます。これは、「IPv6非スコープBSRメカニズム」と呼ばれます。

IPv6管理用スコープ機構

洗練された管理を実装するには、IPv6 PIM-SMDメインをIPv6グローバルスコープゾーンと複数のIPv6管理スコープゾーン(管理スコープゾーン)に分割します。これは、「IPv6管理スコープメカニズム」と呼ばれます。

管理スコーピングメカニズムは、シングルBSRドメインの管理にかかる負荷を効果的に軽減し、プライベートグループアドレスを使用してゾーン固有のサービスを提供できるようにします。

IPv6管理スコープゾーンは、グループアドレスに同じスコープフィールド値を持つ特定のIPv6マルチキャストグループに指定されます。Zone Border Router(ZBR)は、IPv6管理スコープゾーンの境界を形成します。各IPv6管理スコープゾーンは、同じスコープフィールド値を持つIPv6マルチキャストグループに対して1つのBSRを維持します。これらのIPv6マルチキャストグループのアサートメッセージやBSMなどのIPv6マルチキャストプロトコルパケットは、グループ範囲のIPv6管理スコープゾーンの境界を越えることはできません。異なるIPv6管理スコープゾーンが指定されているIPv6マルチキャストグループ範囲は、交差を持つことができます。ただし、IPv6管理スコープゾーン内のIPv6マルチキャストグループは、そのローカルゾーン内でのみ有効であり、これらのIPv6マルチキャストグループはプライベートグループアドレスと見なされます。

IPv6グローバルスコープゾーンは、特別なIPv6管理スコープゾーンと見なすことができ、スコープフィールド値が14のIPv6マルチキャストグループのBSRを維持します。

IPv6管理スコープゾーンとIPv6グローバルスコープゾーンの関係

IPv6グローバルスコープゾーンと各IPv6管理スコープゾーンには、独自のC-RPとBSRがあります。これらのデバイスはそれぞれのゾーンでのみ有効であり、BSR選定とRP選定は独立して実装されます。各IPv6管理スコープゾーンには、独自の境界があります。ゾーン内のIPv6マルチキャスト情報は、この境界をどちらの方向にも越えることはできません。地理的な場所とスコープフィールドの値に基づいて、IPv6グローバルスコープゾーンとIPv6管理スコープゾーンをよりよく理解できます。

- 地理的な位置を考慮して:

IPv6管理スコープゾーンは、同じスコープフィールド値を持つ特定のIPv6マルチキャストグループ用の論理ゾーンです。このようなIPv6マルチキャストグループのIPv6マルチキャストパケットは、ローカルIPv6管理スコープゾーン内に限定され、ゾーンの境界を越えることはできません。

図91 地理的な位置関係

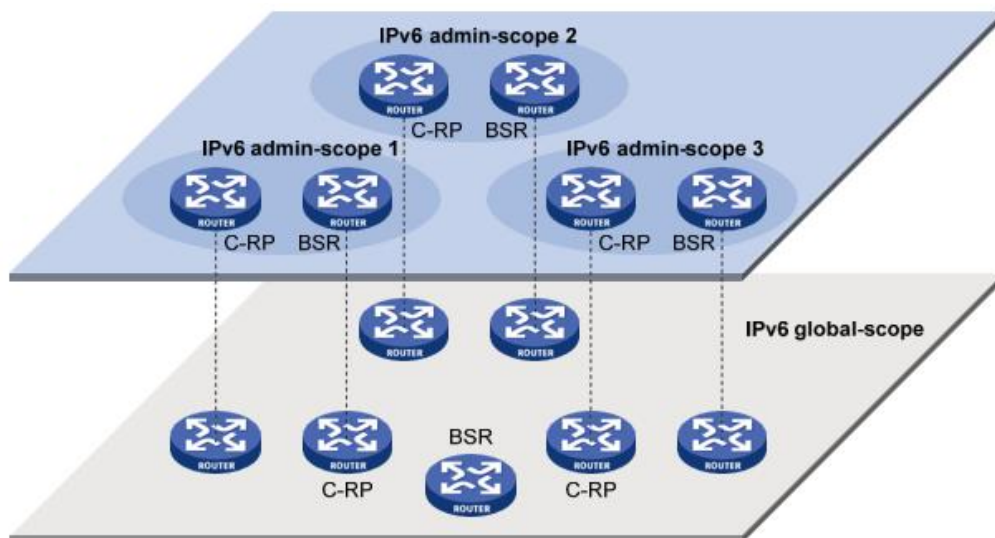


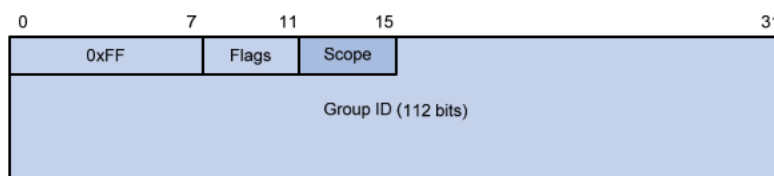
図91に示すように、同じスコープフィールド値を持つIPv6マルチキャストグループの場合、IPv6管理スコープゾーンは地理的に分離されている必要があります。IPv6グローバルスコープゾーンには、IPv6 PIM-SMドメイン内のすべてのデバイスが含まれます。どのIPv6管理スコープゾーンにも属さないIPv6

マルチキャストパケットは、IPv6 PIM-SMドメイン全体で転送されます。

- scopeフィールドの値を考慮すると、次のようになります。

スコープフィールド値に関しては、IPv6マルチキャストグループアドレスのスコープフィールドは、IPv6マルチキャストグループが属するゾーンを示します。

図92 IPv6マルチキャストアドレスフォーマット



スコープフィールド値が大きいIPv6管理者スコープゾーンには、スコープフィールド値が小さいIPv6管理者スコープゾーンが含まれます。スコープフィールド値がEのゾーンは、IPv6グローバルスコープゾーンです。表18に、スコープフィールドの使用可能な値を示します。

表18 Scopeフィールドの値

値	意味	備考:
0、F	予約済み	N/A
1	インターフェイスローカルスコープ	N/A
2	リンクローカルスコープ	N/A
3	サブネットローカルスコープ	IPv6管理スコープゾーン。
4	管理者-ローカルスコープ	IPv6管理スコープゾーン。
5	サイトローカルスコープ	IPv6管理スコープゾーン。
6、7、9～D	未割り当て	IPv6管理スコープゾーン。
8	組織のローカル範囲	IPv6管理スコープゾーン。
E	グローバルスコープ	IPv6グローバルスコープゾーン。

IPv6 PIM-SSM

ASMモデルには、IPv6 PIM-DMとIPv6 PIM-SMが含まれています。SSMモデルは、IPv6 PIM-SM技術の一部を利用して実装できます。「IPv6 PIM-SSM」とも呼ばれます。

SSMモデルは、送信元固有のマルチキャストに対するソリューションを提供します。SSMモデルは、MLDv2を介してホストとデバイス間の関係を維持します。

実際のアプリケーションでは、SSMモデルを実装するために、MLDv2およびIPv6 PIM-SM技術の一部が採用されています。SSMモデルでは、レシーバがIPv6マルチキャスト送信元を特定しているため、RPまたはRPTは必要ありません。他のIPv6 PIMドメイン内のIPv6マルチキャスト送信元を検出するために、送信元登録プロセスは必要ありません。

IPv6 PIM-SSMメカニズムには、ネイバー探索、DR選定、およびSPT構築が含まれます。

近隣探索

IPv6 PIM-SSMは、IPv6 PIM-SMと同じネイバー探索メカニズムを使用します。詳細については、「ネイバー探索」を参照してください。

DR選定

IPv6 PIM-SSMは、IPv6 PIM-SMと同じDR選定メカニズムを使用します。詳細については、「DR選定」を参照してください。

SPT構築

IPv6 PIM-SM用のRPTまたはIPv6 PIM-SSM用のSPTを作成するかどうかは、受信側ホストが加入するIPv6マルチキャストグループがIPv6 SSMグループ範囲内にあるかどうかによって決まります。IANAによって予約されているIPv6 SSMグループ範囲はFF3x::/32です。「x」は有効なアドレス範囲を表します。

図93 IPv6 PIM-SSMでのSPT構築

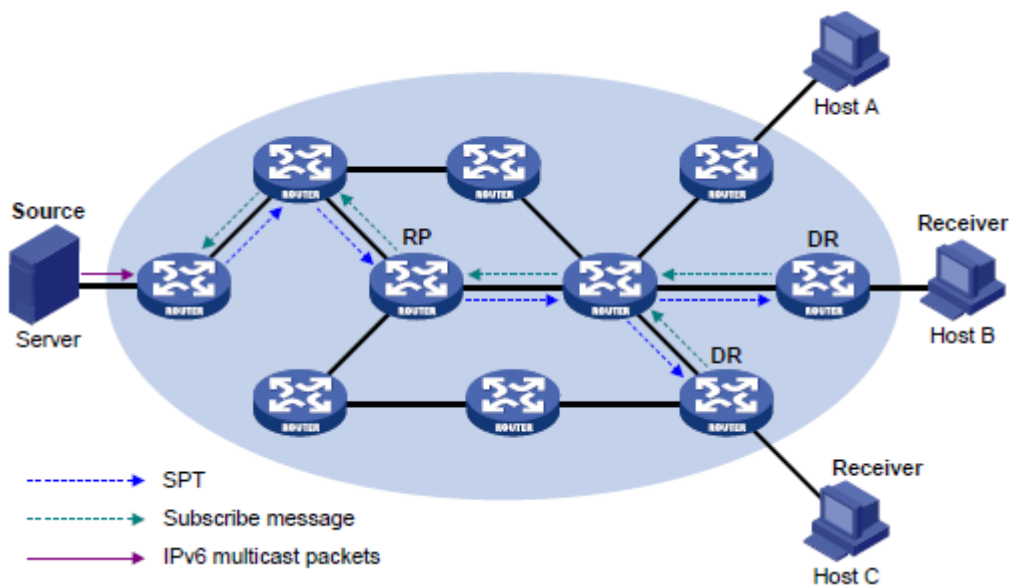


図93に示すように、ホストBとホストCはレシーバです。これらは、MLDv2レポートメッセージをDRに送信して、IPv6マルチキャスト送信元SがIPv6マルチキャストグループGに送信するマルチキャスト情報への関心を表明します。

レポートメッセージを受信した後、DRはまずメッセージ内のグループアドレスがIPv6 SSMグループ範囲内にあるかどうかを確認し、次の処理を実行します。

- グループアドレスがIPv6 SSMグループ範囲内にある場合、DRは加入メッセージをIPv6マルチキャストソースSにホップバイホップで送信します。DRからIPv6マルチキャストソースへのパス上のすべてのデバイスは、SPTを構築するために(S, G)エントリを作成します。SPTはIPv6マルチキャストソースSをルートとし、そのリーフとしてレシーバを持ちます。このSPTは、IPv6 PIM-SSMの送信チャネルです。
- グループアドレスがIPv6 SSMグループ範囲内でない場合、レシーバ側のDRは(*, G)JoinメッセージをRPに送信します。IPv6マルチキャスト送信元は、送信元側のDRに登録されます。

IPv6 PIM-SSMでは、「加入メッセージ」という用語は加入メッセージを意味します。

プロトコルと標準

- RFC 3973『Protocol Independent Multicast-Dense Mode(PIM-DM):Protocol Specification(Revised)』
- RFC 4601『Protocol Independent Multicast-Sparse Mode(PIM-SM):Protocol Specification(Revised)』
- RFC 4610『Anycast-RP Using Protocol Independent Multicast(PIM)』
- RFC 3956『Embedding the Rendezvous Point(RP)Address in a IPv6 Multicast Address』
- RFC 5059『Bootstrap Router(BSR)Mechanism for Protocol Independent Multicast(PIM)』
- RFC 4607『Source-Specific Multicast for IP』
- Draft-ietf-ssm-overview-05、*An Overview of Source-Specific Multicast(SSM)*

制約事項および注意事項:IPv6 PIMの設定

デバイス上のすべてのインターフェイスは、同じIPv6 PIMモードで動作する必要があります。

IPv6 PIM-DMの設定

IPv6 PIM-DMタスクの概要

IPv6 PIM-DMを設定するには、次の作業を実行します。

1. IPv6 PIM-DMの有効化
2. (オプション)状態更新機能の設定
3. (任意)IPv6 PIM-DMグラフトリタイマーの設定
4. (任意)一般的なIPv6 PIM機能の設定

IPv6 PIM-DMの前提条件

IPv6 PIM-DMを設定する前に、次の作業を完了する必要があります。

- ドメイン内のすべてのデバイスがネットワーク層で相互運用できるように、IPv6ユニキャストルーティングプロトコルを設定します。
- IPv6マルチキャストルーティングを有効にします。

IPv6 PIM-DMの有効化

IPv6 PIM-DMの有効化について

インターフェイス上でIPv6 PIM-DMを有効にすると、デバイスはIPv6 PIMネイバー関係を確立し、IPv6

PIMネイバーからのIPv6 PIMメッセージを処理できます。

制約事項とガイドライン

ベストプラクティスとして、IPv6 PIM-DMドメインを展開する場合は、デバイスのすべての非境界インターフェイスでIPv6 PIM-DMを有効にします。

手順

1. システムビューに入ります。

system-view

2. IPv6マルチキャストルーティングを有効にし、IPv6 MRIBビューを開始します。

ipv6 multicast routing

デフォルトでは、IPv6マルチキャストルーティングは無効になっています。

このコマンドの詳細については、『IP Multicast Command Reference』を参照してください。

3. システムビューに戻ります。

quit

4. インターフェイスビューに入ります。

interface interface-type interface-number

5. IPv6 PIM-DMを有効にします。

ipv6 pim dm

デフォルトでは、IPv6 PIM-DMは無効です。

状態更新機能の構成

状態更新機能について

- **An Overview of:** 送信元に直接接続されたIPv6 PIMデバイスが定期的に状態更新メッセージを送信できるようにします。また、他のPIMデバイスが状態更新メッセージを受信した後、プルーニングされた状態タイマーを更新できるようにします。この機能を使用して、プルーニングされたインターフェイスがマルチキャスト転送を再開しないようにします。
- **State refresh interval:** デバイスが状態更新メッセージを送信する間隔を決定します。
- **Wait time before accepting a new state refresh message:** デバイスが短時間に重複した状態更新メッセージを受信する場合があります。この状況を防ぐために、デバイスが新しい状態更新メッセージを受け入れるまでの待機時間を調整できます。タイマーが切れる前に新しい状態更新メッセージを受信した場合、デバイスはメッセージを廃棄します。タイマーが切れた後に新しい状態更新メッセージを受信した場合、デバイスはメッセージを受け入れ、自身のIPv6 PIM-DM状態をリフレッシュし、待機タイマーをリセットします。
- **Hop limit value of state refresh messages:** 状態更新メッセージのホップ制限値は、ダウンストリームノードに転送される前にデバイスを通過するたびに1ずつ減少します。ホップ制限が0になると、状態更新メッセージは転送されません。大きいホップ制限値を持つ状態更新メッセージは、

小規模なネットワークで循環する場合があります。状態更新メッセージの伝播範囲を制御するには、IPv6マルチキャスト送信元に直接接続されたデバイス上で、ネットワークサイズに基づいて適切なホップ制限値を設定します。

制約事項とガイドライン

この作業は、IPv6 PIM-DMドメイン内のすべてのデバイスで実行します。

手順

1. システムビューに入ります。
system-view
2. インターフェイスビューに入ります。
interface interface-type interface-number
3. 状態更新機能を有効にします。
ipv6 pim state-refresh-capable
デフォルトでは、状態更新機能は有効になっています。
4. システムビューに戻ります。
quit
5. IPv6 PIMビューを開始します。
ipv6 pim
6. 状態更新間隔を設定します。
state-refresh-interval interval
デフォルト設定は60秒です。
7. デバイスが新しい状態更新メッセージを受け入れるまで待機する時間を設定します。
state-refresh-rate-limit time
デフォルト設定は30秒です。
8. 状態更新メッセージのホップ制限値を設定します。
state-refresh-hoplimit hoplimit-value
デフォルト設定は255です。

IPv6 PIM-DMグラフトリトライタイマーの設定

IPv6 PIM-DMグラフトリトライタイマーの概要

デバイスが上流のデバイスからgraft-ackメッセージを受信しない場合に、デバイスがグラフトメッセージを再送信する間隔を調整するには、次の作業を実行します。

手順

1. システムビューに入ります。
system-view
2. インターフェイスビューに入ります。
interface interface-type interface-number

3. IPv6 PIM-DMグラフトリタイマーを設定します。

ipv6 pim timer graft-retry interval

デフォルトでは、IPv6 PIM-DMグラフトリタイマーは3秒です。

IPv6 PIM-SMの設定

IPv6 PIM-SMタスクの概要

IPv6 PIM-SMを設定するには、次の作業を実行します。

1. IPv6 PIM-SMの有効化
2. スタティックRPの設定
ベストプラクティスとして、ネットワークにダイナミックRPが1つしか存在しない場合は、スタティックRPを設定します。
3. C-RPの設定
4. C-BSRの設定
 - (任意)IPv6 PIMドメイン境界の設定
 - (任意)BSMセマンティックフラグメンテーションの無効化
 - (任意)デバイスが着信インターフェイスからBSMを転送できないようにする。
ネットワークに複数のIPv6 PIMデバイスが存在する場合は、ダイナミックRPを設定することを推奨します。スタティックRP、ダイナミックRP、またはその両方を設定できます。
5. (任意)エニーキャストRPの設定
6. (任意)IPv6マルチキャスト送信元登録の設定
7. (任意)SPTへのスイッチオーバーの設定
8. (任意)一般的なIPv6 PIM機能の設定

IPv6 PIM-SMの前提条件

IPv6 PIM-SMを設定する前に、次の作業を完了する必要があります。

- ドメイン内のすべてのデバイスがネットワーク層で相互運用できるように、IPv6ユニキャストルーティングプロトコルを設定します。
- IPv6マルチキャストルーティングを有効にします。

IPv6 PIM-SMの有効化

IPv6 PIM-SMの有効化について

インターフェイス上でIPv6 PIM-SMを有効にすると、デバイスはIPv6 PIMネイバー関係を確立し、IPv6

PIMネイバーからのIPv6 PIMメッセージを処理できます。

制約事項とガイドライン

ベストプラクティスとして、IPv6 PIM-SMドメインを展開する場合は、デバイスのすべての非境界インターフェイスでIPv6 PIM-SMを有効にします。

手順

1. システムビューに入ります。

system-view

2. IPv6マルチキャストルーティングを有効にし、IPv6 MRIBビューを開始します。

ipv6 multicast routing

デフォルトでは、IPv6マルチキャストルーティングは無効になっています。

このコマンドの詳細については、『IP Multicast Command Reference』を参照してください。

3. システムビューに戻ります。

quit

4. インターフェイスビューに入ります。

interface interface-type interface-number

5. IPv6 PIM-SMを有効にします。

ipv6 pim sm

デフォルトでは、IPv6 PIM-SMは無効です。

スタティックRPの設定

スタティックRPについて

ネットワーク上にダイナミックRPが1つしか存在しない場合は、シングルポイント障害による通信の中断を避けるためにスタティックRPを設定できます。また、スタティックRPを使用すると、C-RPとBSRの間で頻繁に行われるメッセージ交換による帯域幅の浪費を避けることもできます。

制約事項とガイドライン

IPv6 PIM-SMドメインでは、同じRPアドレスで異なるACLを使用することにより、複数のIPv6マルチキャストグループに同じスタティックRPを設定できます。

インターフェイスをスタティックRPとして設定する場合は、IPv6 PIMを有効にする必要はありません。

IPv6マルチキャストグループに対して複数のスタティックRPを設定した場合は、IPv6アドレスが最も大きいスタティックRPだけが有効になります。

スタティックRP設定は、IPv6 PIM-SMドメイン内のすべてのデバイスで同じである必要があります。

手順

1. システムビューに入ります。

system-view

2. IPv6 PIMビューを開始します。

ipv6 pim

3. IPv6 PIM-SM用のスタティックRPを設定します。

```
static-rp ipv6-rp-address [ ipv6-acl-number | preferred ] *
```

C-RPの設定

C-RPの設定について

C-RPスプーフィングを回避するには、パケット送信元アドレス範囲とマルチキャストグループアドレスを指定するACLを使用して、C-RPアドバタイズメントメッセージをフィルタリングするようにC-RPポリシーを設定します。

制約事項とガイドライン

バックボーンネットワークに存在するデバイスにC-RPを設定します。

RPと他のデバイスはIPv6 PIM-SMDメインで大量の情報を交換するため、C-RPと他のデバイス間で大きな帯域幅を予約します。

すべてのC-BSRがBSRになる可能性があるため、IPv6 PIM-SMDメイン内のすべてのC-BSRに同じC-RPポリシーを設定する必要があります。

デバイスは、RFC 4601またはRFC 2362に記載されているBSR RPハッシュアルゴリズムを使用して、マルチキャストグループのRPを計算できます。IPv6 PIM-SMDメイン内のすべてのPIMデバイスでグループからRPへのマッピングの一貫性を確保するには、デバイス上で同じBSR RPハッシュアルゴリズムを指定します。

手順

1. システムビューに入ります。

```
system-view
```

2. IPv6 PIMビューを開始します。

```
ipv6 pim
```

3. C-RPを設定します。

```
c-rp ipv6-address [ advertisement-interval adv-interval | { group-policy ipv6-acl-number | scope scope-id } | holdtime hold-time | priority priority ] *
```

4. (任意)C-RPポリシーを設定します。

```
crp-policy ipv6-acl-number
```

デフォルトでは、C-RPポリシーは設定されていません。すべてのC-RPアドバタイズメントメッセージは、合法と見なされます。

5. (任意)RFC 2362に記述されているBSR RPハッシュアルゴリズムを使用するようにデバイスを設定します。

```
bsr-rp-mapping rfc2362
```

デフォルトでは、デバイスはRFC 4601に記述されているBSR RPハッシュアルゴリズムを使用しま

す。

C-BSRの設定

C-BSRについて

ダイナミックRP選定を設定する場合は、C-BSRを設定する必要があります。

正当なBSRが悪意のあるホストによって置き換えられないようにするには、正当なBSRアドレスを指定するACLを使用してBSRメッセージをフィルタリングするようにBSRポリシーを設定します。

制約事項とガイドライン

バックボーンネットワークに存在するデバイスにC-BSRを設定します。

BSRと他のデバイスはIPv6 PIM-SMDメインで大量の情報を交換するため、C-BSRと他のデバイス間で大きい帯域幅を予約します。

IPv6 PIM-SMDメイン内のデバイス上のC-BSR設定は、同じである必要があります。

手順

1. システムビューに入ります。

system-view

2. IPv6 PIMビューを開始します。

ipv6 pim

3. C-BSRを設定します。

c-bsr *ipv6-address* [**scope** *scope-id*] [**hash-length** *hash-length* | **priority** *priority*] *

4. (任意)BSRポリシーを設定します。

bsr-policy *ipv6-acl-number*

デフォルトでは、BSRポリシーは設定されていません。すべてのブートストラップメッセージは、有効と見なされます。

IPv6 PIMドメイン境界の設定

IPv6 PIMドメイン境界について

IPv6 PIMドメイン境界は、ブートストラップメッセージの送信境界を決定します。ブートストラップメッセージは、どちらの方向にもドメイン境界を越えることはできません。多数のIPv6 PIMドメイン境界インターフェイスによって、ネットワークが異なるIPv6 PIM-SMDメインに分割されます。

手順

1. システムビューに入ります。

system-view

2. インターフェイスビューに入ります。

interface *interface-type interface-number*

3. IPv6 PIMドメイン境界を設定します。

ipv6 pim bsr-boundary

デフォルトでは、インターフェイスはIPv6 PIMドメイン境界ではありません。

BSMセマンティックフラグメンテーションの無効化

BSMセマンティックフラグメンテーションについて

BSMセマンティックフラグメンテーションを使用すると、BSMがMTUを超過した場合に、BSRでBSMを複数のBSM Fragment(BSMFs)に分割できます。このように、非BSRデバイスは、グループ範囲のすべてのBSMFsを受信した後で、そのグループ範囲のRPセット情報を更新できます。1つのBSMFの損失は、フラグメントに含まれるグループ範囲のRPセット情報にだけ影響します。

制約事項とガイドライン

デバイスがBSMセマンティックフラグメンテーションをサポートしていない場合、デバイスはBSMFをBSMと見なし、BSMFを受信するたびにRPセット情報を更新します。デバイスはRPセット情報の一部だけを学習し、RP選定にさらに影響を与えます。したがって、このようなデバイスがIPv6 PIM-SMドメインに存在する場合は、すべてのC-BSRでBSMセマンティックフラグメンテーションを無効にする必要があります。

手順

1. システムビューに入ります。
system-view
2. IPv6 PIMビューを開始します。
ipv6 pim
3. BSMセマンティックフラグメンテーションを無効にします。

undo bsm-fragmentenable

デフォルトでは、BSMセマンティックフラグメンテーションは有効です。

デバイスが着信インターフェイスからBSMを転送できないようにする

デバイスが着信インターフェイスからBSMを転送できないようにする方法

デフォルトでは、デバイスは着信インターフェイスからBSMを転送します。このデフォルト設定により、サブネット上のすべてのデバイスは、ルーティング情報に一貫性がない場合でも、BSMを受信できます。ただし、このデフォルト設定では、IPv6マルチキャストトラフィックが重複します。サブネット上のすべてのデバイスのルーティング情報に一貫性がある場合は、デバイスが着信インターフェイスからBSMを転送しないように設定できます。

手順

1. システムビューに入ります。

system-view

2. IPv6 PIMビューを開始します。

ipv6 pim

3. デバイスが着信インターフェイスからBSMを転送できないようにします。

undo bsm-reflection enable

デフォルトでは、デバイスは着信インターフェイスからBSMを転送します。

エニーキャストRPの設定

制約事項とガイドライン

他のエニーキャストRPメンバーデバイスがBSRから送信されたBSMを廃棄しないようにするには、エニーキャストRPアドレスがBSRアドレスと異なることを確認します。

ネットワークパフォーマンスを確保するベストプラクティスとして、1つのAnycast RPセットに最大16のAnycast RPメンバーを設定します。

ベストプラクティスとして、ループバックインターフェイスのIPv6アドレスをRPメンバードレスとして設定します。

同じデバイス上の複数のインターフェイスのIPv6アドレスをRPメンバードレスとして設定する場合、最も小さいIPv6アドレスが有効になります。残りのインターフェイスアドレスは、バックアップRPメンバードレスになります。

エニーキャストRPがRPメンバーとして常駐するデバイスを、エニーキャストRPセットに追加する必要があります。

必要条件

エニーキャストRPを設定する前に、IPv6 PIM-SMドメイン内にスタティックRPまたはC-RPを設定する必要があります。スタティックRPまたはダイナミックに選択されたRPのアドレスをエニーキャストRPアドレスとして使用します。

手順

1. システムビューに入ります。

system-view

2. IPv6 PIMビューを開始します。

ipv6 pim

3. エニーキャストRPを設定します。

anycast-rp *ipv6-anycast-rp-address ipv6-member-address*

このコマンドを繰り返して、複数のRPメンバードレスをエニーキャストRPセットに追加できます。

IPv6マルチキャスト送信元登録の設定

IPv6マルチキャスト送信元登録について

- **IPv6 PIM register policy:** IPv6 PIM登録ポリシーを使用すると、RPは、IPv6マルチキャスト送信元およびグループを指定するACLを使用して登録メッセージをフィルタリングできます。このポリシーは、RPが指定されているマルチキャストグループを制限します。登録メッセージがACLによって拒否されるか、ACLと一致しない場合、RPは登録メッセージを廃棄し
ソース側のDRへのregister-stopメッセージ。登録プロセスが停止します。
- **Checksum computing method for register messages:** 登録メッセージの情報整合性のため

に、登録メッセージ全体に基づいてチェックサムを計算するようにデバイスを設定できます。デバイスが登録メッセージ全体に基づいてチェックサムを計算できない場合は、登録メッセージヘッダーに基づいてチェックサムを計算するようにデバイスを設定できます。

- **Register suppression tim:** 送信元側のDRは、RPから登録停止メッセージを受信すると、IPv6マルチキャストデータでカプセル化された登録メッセージの送信を停止し、登録停止タイマーを開始します。登録停止タイマーの期限が切れる前に、DRはヌル登録メッセージ(カプセル化されたIPv6マルチキャストデータを含まない登録メッセージ)をRPに送信し、登録プローブタイマーを開始します。登録プローブタイマーの期限が切れる前にDRが登録停止メッセージを受信すると、登録停止タイマーがリセットされます。登録プローブタイマーの期限が切れたときにDRが登録停止メッセージを受信しなかった場合、DRはカプセル化されたデータを含む登録メッセージの送信を再開します。

register-stopタイマーは、 $(0.5 \times \text{register\_suppression\_time} - \text{register\_probe\_time})$ から $(1.5 \times \text{register\_suppression\_time} - \text{register\_probe\_time})$ までの間で一様に選択されるランダムな値に設定されます。register_probe_timeは(5秒)です。registerの抑え込みの時間は調整できます。

制約事項とガイドライン

すべてのC-RPデバイス上で、IPv6 PIM登録ポリシーおよび登録メッセージのチェックサム計算方式を設定します。

ソース側のDRになる可能性のあるすべてのデバイスで、レジスタの抑え込みの時間を設定します。

手順

1. システムビューに入ります。

system-view

2. IPv6 PIMビューを開始します。

ipv6 pim

3. IPv6 PIM登録ポリシーを設定します。

register-policy *ipv6-acl-number*

デフォルトでは、IPv6登録ポリシーは設定されていません。すべてのIPv6登録メッセージは有効と見なされます。

4. 登録メッセージ全体に基づいてチェックサムを計算するようにデバイスを設定します。

register-whole-checksum

デフォルトでは、デバイスは登録メッセージのヘッダーに基づいてチェックサムを計算します。

5. レジスタの抑え込みの時間を設定します。

register-suppression-timeout *interval*

デフォルト設定は60秒です。

SPTへのスイッチオーバーの設定

制約事項とガイドライン

一部のデバイスでは、RP宛ての登録メッセージ内のIPv6マルチキャストデータをカプセル化できません。IPv6マルチキャストデータの転送障害を回避するためのベストプラクティスとして、RPIになる可能性のあるC-RP上でSPTへのスイッチオーバーを無効にしないでください。

手順

1. システムビューに入ります。

system-view

2. IPv6 PIMビューを開始します。

ipv6 pim

3. SPTへのスイッチオーバーを設定します。

register-policy *ipv6-acl-number*

デフォルトでは、最初のIPv6マルチキャストデータパケットによってRPTからSPTへのスイッチオーバーがトリガーされます。

IPv6 PIM-SSMの設定

IPv6 PIM-SSMタスクの概要

IPv6 PIM-SSMを設定するには、次の作業を実行します。

1. IPv6 PIM-SMの有効化
2. (任意)IPv6 PIM helloポリシーの設定
3. (任意)一般的なIPv6 PIM機能の設定

IPv6 PIM-SSMの前提条件

IPv6 PIM-SSMを設定する前に、次の作業を完了する必要があります。

- ドメイン内のすべてのデバイスがネットワーク層で相互運用できるように、IPv6ユニキャストIPv6ルーティングプロトコルを設定します。
- IPv6 PIM-SMを有効にします。
- IPv6マルチキャストレシーバに接続するIPv6 PIMデバイスでMLDv2を有効にします。

IPv6 PIM-SMの有効化

制約事項とガイドライン

ベストプラクティスとして、IPv6 PIM-SSMドメインを展開する場合は、デバイスのすべての非境界インターフェイスでIPv6 PIM-SMを有効にします。

手順

1. システムビューに入ります。

system-view

2. IPv6マルチキャストルーティングを有効にし、IPv6 MRIBビューを開始します。

ipv6 multicast routing

デフォルトでは、IPv6マルチキャストルーティングは無効になっています。

このコマンドの詳細については、『IP Multicast Command Reference』を参照してください。

3. システムビューに戻ります。

quit

4. インターフェイスビューに入ります。

interface *interface-type* *interface-number*

5. IPv6 PIM-SMを有効にします。

ipv6 pim sm

デフォルトでは、IPv6 PIM-SMは無効です。

IPv6 SSMグループ範囲の指定

SSM-group範囲について

IPv6 PIM-SM対応インターフェイスは、IPv6マルチキャストパケットを受信すると、そのパケットのIPv6マルチキャストグループアドレスがIPv6 SSMグループ範囲内にあるかどうかを確認します。IPv6マルチキャストグループアドレスがこの範囲内にある場合、このパケットのIPv6 PIMモードはIPv6 PIM-SSMになります。IPv6マルチキャストグループアドレスがこの範囲内でない場合、IPv6 PIMモードはIPv6 PIM-SMになります。

制約事項とガイドライン

IPv6 PIM-SMドメイン全体のすべてのデバイスに同じIPv6 SSMグループ範囲を設定します。そうしないと、IPv6マルチキャスト情報をIPv6 SSMモデルを介して配信できません。

IPv6 SSMグループ範囲内のIPv6マルチキャストグループのメンバーがMLDv1レポートメッセージを送信する場合、デバイスは(*,G)加入をトリガーしません。

手順

1. システムビューに入ります。

system-view

2. IPv6 PIMビューを開始します。

ipv6 pim

3. IPv6 SSMグループ範囲を設定します。

ssm-policy ipv6-acl-number

デフォルトの範囲はFF3x::/32です。xには有効なスコープを指定できます。

一般的なIPv6 PIM機能の設定

一般的なIPv6 PIM機能のタスクの概要

次の作業はすべてオプションです。

- IPv6 PIMハローポリシーの設定
- IPv6 PIMハローメッセージオプションの設定
- Generation IDオプションを使用しないhelloメッセージのドロップ
- 共通IPv6 PIMタイマーの設定
- ジョインまたはプルーンメッセージの最大サイズの設定
- 発信IPv6 PIMプロトコルパケットのDSCP値の設定
- IPv6 PIMのBFDの有効化
- IPv6 PIMパッシブモードの有効化
- IPv6 PIM NSRの有効化
- IPv6 PIMのSNMP通知の有効化

IPv6マルチキャスト送信元ポリシーの設定

IPv6マルチキャスト送信元ポリシーについて

この機能により、デバイスは、IPv6マルチキャストソースおよびオプションのグループを指定するACLを使用して、IPv6マルチキャストデータをフィルタリングできます。IPv6マルチキャストデータパケットだけでなく、IPv6マルチキャストデータがカプセル化されたIPv6 PIM Registerメッセージもフィルタリングされます。これにより、ネットワーク上のIPv6マルチキャストトラフィックも削減されます。

手順

1. システムビューに入ります。

system-view

2. IPv6 PIMビューを開始します。

ipv6 pim

3. IPv6マルチキャスト送信元ポリシーを設定します。

source-policy ipv6-acl-number

デフォルトでは、IPv6マルチキャスト送信元ポリシーは設定されていません。デバイスはIPv6マルチキャストデータパケットをフィルタリングしません。

IPv6 PIMハローポリシーの設定

IPv6 PIM helloポリシーの概要

この機能は、パケット送信元アドレスを指定するACLを使用して、デバイスがIPv6 PIMハローメッセージをフィルタリングできるようにします。これは、IPv6 PIMメッセージ攻撃から保護し、正しいIPv6 PIMネイバー関係を確立するために使用されます。

既存のIPv6 PIMネイバーのhelloメッセージがポリシーによってフィルタリングされた場合、このネイバーはエージングタイマーの期限が切れると自動的に削除されます。

手順

1. システムビューに入ります。

system-view

2. インターフェイスビューに入ります。

interface *interface-type* *interface-number*

3. IPv6 PIM helloポリシーを設定します。

ipv6 pim neighbor-policy *ipv6-acl-number*

デフォルトでは、IPv6 PIM helloポリシーはインターフェイスに設定されません。すべてのIPv6 PIM helloメッセージは合法と見なされます。

IPv6 PIMハローメッセージオプションの設定

IPv6 PIMハローメッセージオプションについて

IPv6 PIM-DMドメインまたはIPv6 PIM-SMドメインのいずれかで、デバイス間で交換されるhelloメッセージには、次の設定可能なオプションが含まれます。

- **DR_Priority** (IPv6 PIM-SMのみ): DR選定のプライオリティ。最も高いプライオリティを持つデバイスがDR選定を勝ち取ります。このオプションは、IPv6マルチキャストソースまたはレシーバに直接接続する共有メディアLAN内のすべてのデバイスに対して設定できます。
- **Holdtime**: IPv6 PIMネイバーのライフタイム。ネイバーのライフタイムが期限切れになったときに、デバイスがネイバーからhelloメッセージを受信しなかった場合、そのネイバーは障害が発生したか到達不能であると見なされます。
- **LAN_Prune_Delay**: 共有メディアLAN上のダウストリームインターフェイスのプルーニングの遅延。このオプションには、LAN遅延フィールド、Override Intervalフィールド、およびTビットがあります。

LAN遅延は、IPv6 PIMメッセージの伝搬遅延を定義します。上書き間隔は、ダウストリームデバイスがプルーニングメッセージを上書きする期間を定義します。Tビットは、アップストリームデ

バース上のダウンストリームデバイスステータスを追跡する機能を指定します。

共有メディアLANでは、伝搬遅延とオーバーライド間隔は次のように使用されます。

- デバイスがアップストリームインターフェイスでPruneメッセージを受信した場合、それは共有メディアLAN上にダウンストリームデバイスがあることを意味します。このデバイスがまだマルチキャストデータを受信する必要がある場合、上書き間隔内にJoinメッセージを送信してPruneメッセージを上書きする必要があります。
- デバイスがダウンストリームインターフェイスからプルーンメッセージを受信する時、すぐにこのインターフェイスをプルーンしません。代わりに、タイマー(伝播遅延+オーバーライド間隔)を開始します。タイマーが切れる前にインターフェイスがジョインメッセージを受信した場合、デバイスはインターフェイスをプルーンしません。それ以外の場合、デバイスはインターフェイスをプルーンします。
- ネイバートラッキング:アップストリームデバイスでネイバートラッキングを有効にした場合、このデバイスは、加入状態保持時間タイマーが期限切れになっていないダウンストリームノードの状態を追跡できます。ダウンストリームデバイスからのすべてのJoinメッセージが受け入れられます。

制約事項とガイドライン

共有メディアLAN上の異なるIPv6 PIMデバイス上の伝搬遅延またはオーバーライド間隔が異なる場合、最も大きいものが適用されます。

ネイバートラッキングを有効にした場合、すべてのダウンストリームデバイスからのJoinメッセージを追跡するには、共有メディアLANまたはアップストリームデバイス上のすべてのIPv6 PIMデバイスでネイバートラッキングを有効にする必要があります。

IPv6 PIMビューのすべてのインターフェイス、またはインターフェイスビューの現在のインターフェイスに対して、helloメッセージオプションを設定できます。インターフェイスビューで行った設定は、IPv6 PIMビューで行った設定よりも優先されます。

helloメッセージオプションのグローバルな設定

1. システムビューに入ります。
system-view
2. IPv6 PIMビューを開始します。
ipv6 pim
3. DRプライオリティを設定します。
hello-option dr-priority *priority*
既定の設定は1です。
4. ネイバーのライフタイムを設定します。
hello-option holdtime *time*
デフォルト設定は105秒です。
5. 共有メディアLANのIPv6 PIMメッセージ伝搬遅延を設定します。
hello-option lan-delay *delay*

デフォルト設定は500ミリ秒です。

6. 上書き間隔を設定します。

```
hello-option override-interval interval
```

デフォルト設定は2500ミリ秒です。

7. ネイバートラッキングを有効にします。

```
hello-option neighbor-tracking
```

デフォルトでは、ネイバートラッキングは無効です。

インターフェイスでのhelloメッセージオプションの設定

1. システムビューに入ります。

System-view

2. インターフェイスビューに入ります。

```
interface interface-type interface-number
```

3. DRプライオリティを設定します。

```
ipv6 pim hello-option dr-priority priority
```

既定の設定は1です。

4. ネイバーのライフタイムを設定します。

```
ipv6 pim hello-option holdtime time
```

デフォルト設定は105秒です。

5. IPv6 PIMメッセージの伝搬遅延を設定します。

```
ipv6 pim hello-option lan-delay delay
```

デフォルト設定は500ミリ秒です。

6. 上書き間隔を設定します。

```
ipv6 pim hello-option override-interval interval
```

デフォルト設定は2500ミリ秒です。

7. ネイバートラッキングを有効にします。

```
ipv6 pim hello-option neighbor-tracking
```

デフォルトでは、ネイバートラッキングは無効です。

Generation IDオプションを使用しないhelloメッセージのドロップ

Generation IDオプションを使用しないhelloメッセージのドロップについて

インターフェイスでIPv6 PIMが有効になっている場合、デバイスはhelloメッセージの生成IDを生成します。生成IDはランダムな値ですが、デバイスのステータスが変更された場合にだけ変更されます。IPv6 PIMデバイスは、アップストリームデバイスからのhelloメッセージ内の生成IDが変更されたことを検出すると、アップストリームデバイスのステータスが変更されたと見なします。この場合、ステータスアップデートのためにJoinメッセージをアップストリームデバイスに送信します。アップストリームデバイスのステータスを迅速に把握するために、生成IDオプションを使用せずにhelloメッセージをドロップするようにインターフェイスを設定できます。

手順

1. システムビューに入ります。

system-view

2. インターフェイスビューに入ります。

interface *interface-type* *interface-number*

3. Generation IDオプションを使用せずにhelloメッセージをドロップするようにインターフェイスを有効にします。

ipv6 pim require-genid

デフォルトでは、インターフェイスはGeneration IDオプションのないhelloメッセージを受け入れません。

共通IPv6 PIMタイマーの設定

一般的なIPv6 PIMタイマーについて

次に、一般的なIPv6 PIMタイマーを示します。

- **Hello interval:** IPv6 PIMデバイスがhelloメッセージを送信して、IPv6 PIMネイバーを検出し、IPv6 PIMネイバー関係を維持する間隔。
- **Triggered hello delay:** 同時のhelloメッセージによって引き起こされる衝突を回避するための、helloメッセージ送信の最大遅延。helloメッセージを受信した後、IPv6 PIMデバイスは、helloメッセージを送信する前に、ランダムな時間待機します。このランダムな時間は、0からトリガーされたhello遅延までの範囲です。
- **Join/Prune interval:** IPv6 PIMデバイスが状態更新のためにJoin/Pruneメッセージをアップストリームデバイスに送信する間隔。
- **Joined/Pruned state holdtime:** IPv6 PIMデバイスがダウンストリームインターフェイスの加入/プルーニング状態を保持する時間。この加入/プルーニング状態保持時間は、Join/Pruneメッセージに含まれます。
- **IPv6 multicast source lifetime:** IPv6 PIMデバイスがIPv6マルチキャスト送信元に対して維持するライフタイム。タイマーの期限が切れたときに、デバイスがIPv6マルチキャスト送信元Sから後続のIPv6マルチキャストデータを受信しない場合、デバイスはIPv6マルチキャスト送信元の(S, G)エントリを削除します。

制約事項とガイドライン

アップストリームネイバーがエージングアウトしないようにするには、Join/Prune間隔をJoin/Pruneステート保持時間よりも短く設定します。

IPv6 PIMビューのすべてのインターフェイス、またはインターフェイスビューの現在のインターフェイスに対して、共通のIPv6 PIMタイマーを設定できます。インターフェイスビューで行った設定は、IPv6 PIMビューで行った設定よりも優先されます。

ベストプラクティスとして、特別な要件のないネットワークにはデフォルトを使用します。

共通IPv6 PIMタイマーのグローバルな設定

1. システムビューに入ります。

system-view

2. IPv6 PIMビューを開始します。

ipv6 pim

3. hello間隔を設定します。

timer hello *interval*

デフォルトでは、helloメッセージを送信する間隔は30秒です。

4. ジョイン/プルーンインターバルを設定します。

timer join-prune *interval*

デフォルトでは、join/pruneメッセージを送信する間隔は60秒です。この

設定は、現在の間隔が終了した後には有効になります。

5. 参加/プルーニング状態の保持時間を設定します。

holdtime join-prune *time*

デフォルトでは、join/pruneステートのホールドタイムタイマーは210秒です。

6. IPv6マルチキャスト送信元ライフタイムを設定します。

source-lifetime *time*

デフォルトでは、IPv6マルチキャスト送信元ライフタイムは210秒です。

インターフェイス上の共通IPv6 PIMタイマーの設定

1. システムビューに入ります。

system-view

2. インターフェイスビューに入ります。

interface *interface-type interface-number*

3. hello間隔を設定します。

ipv6 pim timer hello *interval*

デフォルト設定は30秒です。

4. triggered hello delayを設定します。

ipv6 pim triggered-hello-delay *delay*

デフォルト設定は5秒です。

5. ジョイン/プルーンインターバルを設定します。

ipv6 pim timer join-prune *interval*

デフォルト設定は60秒です。

この設定は、現在のインターバルの終了後に有効になります。

6. 参加/プルーニング状態の保持時間を設定します。

ipv6 pim holdtime join-prune *time*

デフォルト設定は210秒です。

ジョインまたはプルーンメッセージの最大サイズの設定

制約事項とガイドライン

大きすぎるジョインまたはプルーンメッセージが失われると、大量の情報が失われる可能性があります。
ジョインまたはプルーンメッセージのサイズに小さい値を設定すると、影響を軽減できます。

手順

1. システムビューに入ります。
system-view
2. IPv6 PIMビューを開始します。
ipv6 pim
3. join/pruneメッセージの最大サイズを設定します。
jp-pkt-size size
リリース1118P07以降では、デフォルト設定は1200バイトです。

発信IPv6 PIMプロトコルパケットのDSCP値の設定

発信IPv6 PIMプロトコルパケットのDSCP値について

DSCP値は、パケット送信の優先順位を決定します。DSCP値が大きいほど、優先順位が高くなります。

手順

1. システムビューに入ります。
system-view
2. IPv6 PIMビューを開始します。
ipv6 pim
3. 発信IPv6 PIMプロトコルパケットのDSCP値を設定します。
dscp dscp-value
デフォルトでは、発信IPv6 PIMプロトコルパケットのDSCP値は48です。

IPv6 PIMのBFDの有効化

IPv6 PIMのBFDの有効化の概要

共有メディアネットワーク上のDRに障害が発生した場合、DRが期限切れになった後、新しいDR選定プロセスが開始されます。ただし、他のデバイスがリンク障害を検出し、新しいDR選定をトリガーするまでに長い時間がかかる場合があります。元のDRに障害が発生した直後に新しいDR選定プロセスを開始するには、IPv6 PIMのBFDを有効にして、IPv6 PIMネイバー間のリンク障害を検出できます。
共有メディアネットワーク上のすべてのIPv6 PIMデバイスでIPv6 PIMのBFDを有効にする必要があります。BFDの詳細については、『High Availability Configuration Guide』を参照してください。

インターフェイス上でこの機能を設定する前に、インターフェイス上でIPv6 PIM-DMまたはIPv6 PIM-SMを有効にする必要があります。

手順

1. システムビューに入ります。
system-view
2. インターフェイスビューに入ります。
interface interface-type interface-number
3. IPv6 PIMのBFDを有効にします。
ipv6 pim bfd enable
デフォルトでは、IPv6 PIMのBFDは無効です。

IPv6 PIMパッシブモードの有効化

IPv6 PIMパッシブモードの概要

IPv6 PIM helloスプーフィングから保護するには、受信側インターフェイスでIPv6 PIMパッシブモードを有効にします。インターフェイスはIPv6 PIMプロトコルメッセージ(register、register-stop、およびC-RP-Advメッセージを除く)を受信または転送できず、サブネット上のDRとして動作します。

制約事項とガイドライン

この機能は、IPv6 PIM-DMまたはIPv6 PIM-SMがインターフェイスで有効になっている場合にだけ有効です。

重複したマルチキャストデータ送信およびフローループを回避するために、複数のIPv6 PIMデバイスがある共有メディアLANでこの機能を有効にしないでください。

手順

1. システムビューに入ります。
system-view
2. インターフェイスビューに入ります。
interface interface-type interface-number
3. インターフェイス上でIPv6 PIMパッシブモードを有効にします。
ipv6 pim passive
デフォルトでは、IPv6 PIMパッシブモードはインターフェイスで無効になっています。

IPv6 PIM NSRの有効化

PIM NSRの概要

この機能を使用すると、IPv6 PIMは、IPv6 PIMネイバー情報およびルートなどのプロトコルステート情報を、アクティブプロセスからスタンバイプロセスにバックアップできます。アクティブプロセスに障害が発生すると、スタンバイプロセスがただちに引き継ぎます。この機能を使用して、アクティブ/スタンバイ

スイッチオーバーが発生した場合にIPv6 PIMのルートフラッピングおよび転送が中断されないようにします。

手順

1. システムビューに入ります。
system-view
2. IPv6 PIM NSRを有効にします。
ipv6 pim non-stop-routing
デフォルトでは、IPv6 PIM NSRは無効です。

IPv6 PIMのSNMP通知の有効化

IPv6 PIMのSNMP通知の有効化について

重要なIPv6 PIMイベントをNMSに報告するには、IPv6 PIMのSNMP通知を有効にします。PIMイベント通知を正しく送信するには、『Network Management and Monitoring Configuration Guide』の説明に従って、SNMPも設定する必要があります。

手順

1. システムビューに入ります。
system-view
2. IPv6 PIMのSNMP通知を有効にします。
snmp-agent trap enable pim6 [candidate-bsr-win-election | elected-bsr-lost-election | neighbor-loss]*
デフォルトでは、IPv6 PIMのSNMP通知は有効になっています。

IPv6 PIMの表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行します。

タスク	コマンド
レジスタトンネルインターフェイス情報を表示します。	display interface [register-tunnel [interface-number]] [brief [description down]]
IPv6 PIM-SMドメインのBSR情報を表示します。	display ipv6 pim bsr-info
IPv6 PIMで使用するルートに関する情報を表示します。	display ipv6 pim claimed-route [ipv6-source-address]
IPv6 PIM-SMドメインのC-RP情報を表示します。	display ipv6 pim c-rp [local]

インターフェイスのIPv6 PIM情報を表示します。	display ipv6 pim interface [<i>interface-type</i> <i>interface-number</i>] [verbose]
IPv6 PIMネイバー情報を表示します。	display ipv6 pim neighbor [<i>ipv6-neighbor-address</i> interface <i>interface-type</i> <i>interface-number</i> verbose] *
IPv6 PIMルーティングエントリを表示します。	display ipv6 pim routing-table [<i>ipv6-group-address</i> [<i>prefix-length</i>] <i>ipv6-source-address</i> [<i>prefix-length</i>] flags <i>flag-value</i> fsm incoming-interface <i>interface-type</i> <i>interface-number</i> mode <i>mode-type</i> outgoing-interface { exclude include match } <i>interface-type</i> <i>interface-number</i>] *
IPv6 PIM-SMドメインのRP情報を表示します。	display ipv6 pim rp-info [<i>ipv6-group-address</i>]
IPv6 PIMパケットの統計情報を表示します。	display ipv6 pim statistics

IPv6 PIMの設定例

例:IPv6 PIM-DMの設定

ネットワークの設定

図94に示します。

- OSPFv3はネットワーク上で動作します。
- VoDストリームはマルチキャストでレシーバホストに送信されます。異なる組織のレシーバグループはスタブネットワークを形成し、各スタブネットワークには1つ以上のレシーバホストが存在します。IPv6 PIMドメイン全体がデンスモードで動作しています。
- ホストAとホストCは、2つのスタブネットワークN1とN2のマルチキャストレシーバです。
- MLDv1は、スイッチAとN1の間、およびスイッチB、スイッチC、N2の間で動作します。

図94 ネットワークダイアグラム

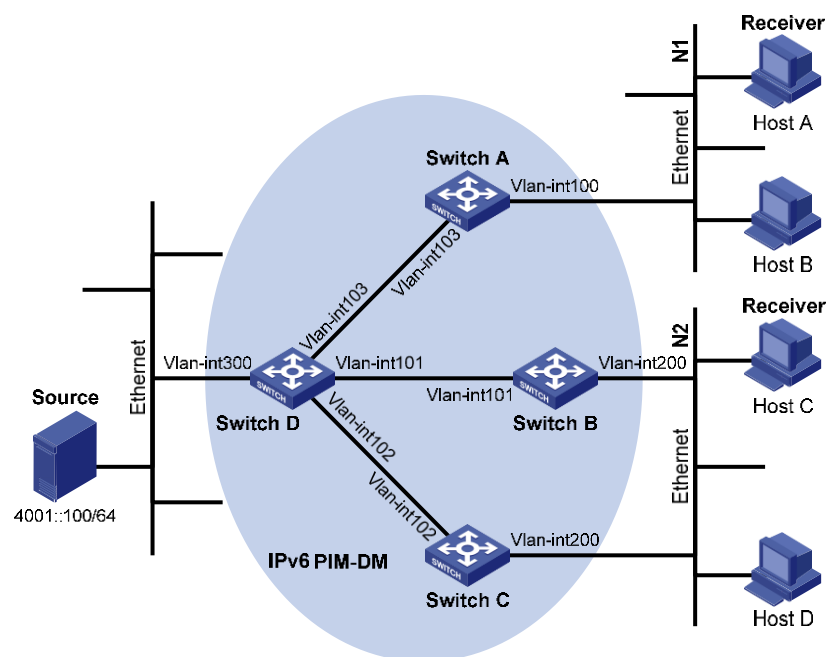


表19インターフェイスおよびIPv6アドレス割り当て

デバイス	インターフェイス	IPv6アドレス	デバイス	インターフェイス	IPv6アドレス
Switch A	Vlan-int100	1001::1/64	Switch D	Vlan-int300	4001::1/64
Switch A	Vlan-int103	1002::1/64	Switch D	Vlan-int103	1002::2/64
Switch B	Vlan-int200	2001::1/64	Switch D	Vlan-int101	2002::2/64
Switch B	Vlan-int101	2002::1/64	Switch D	Vlan-int102	3001::2/64
Switch C	Vlan-int200	2001::2/64	Switch D	Vlan-int300	4001::1/64
Switch C	Vlan-int102	3001::1/64	Switch D	Vlan-int103	1002::2/64

手順

1. 図94に示すように、各インターフェイスにIPv6アドレスとプレフィクス長を割り当てます(詳細は省略)。
2. IPv6 PIM-DMドメイン内のスイッチにOSPFv3を設定します(詳細は省略)。
3. IPv6マルチキャストルーティング、MLD、およびIPv6 PIM-DMを有効にします。

On Switch A, enable IPv6 multicast routing.

```
<SwitchA> system-view
```

```
[SwitchA] ipv6 multicast routing
```

```
[SwitchA-mrib6] quit
```

Enable MLD on VLAN-interface 100 (the interface that is connected to the stub network).

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] mld enable
```

```
[SwitchA-Vlan-interface100] quit
```

Enable IPv6 PIM-DM on VLAN-interface 103.

```
[SwitchA] interface vlan-interface 103
```

```
[SwitchA-Vlan-interface103] ipv6 pim dm
```

```
[SwitchA-Vlan-interface103] quit
```

Enable IPv6 multicast routing, MLD, and IPv6 PIM-DM on Switch B and Switch C in the same way Switch A is configured. (Details not shown.)

On Switch D, enable IPv6 multicast routing, and enable IPv6 PIM-DM on each interface.

```
<SwitchD> system-view
```

```
[SwitchD] ipv6 multicast routing
```

```
[SwitchD-mrib6] quit
```

```
[SwitchD] interface vlan-interface 300
```

```
[SwitchD-Vlan-interface300] ipv6 pim dm
```

```
[SwitchD-Vlan-interface300] quit
```

```
[SwitchD] interface vlan-interface 103
```

```
[SwitchD-Vlan-interface103] ipv6 pim dm
```

```
[SwitchD-Vlan-interface103] quit
```

```
[SwitchD] interface vlan-interface 101
```

```
[SwitchD-Vlan-interface101] ipv6 pim dm
```

```
[SwitchD-Vlan-interface101] quit
```

```
[SwitchD] interface vlan-interface 102
```

```
[SwitchD-Vlan-interface102] ipv6 pim dm
```

```
[SwitchD-Vlan-interface102] quit
```

設定の確認

#スイッチDのIPv6 PIM情報を表示します。

```
[SwitchD] display ipv6 pim interface
```

Interface	NbrCnt	HelloInt	DR-Pri	DR-Address
Vlan300	0	30	1	FE80::A01:201:1 (local)
Vlan103	0	30	1	FE80::A01:201:2 (local)

```
Vlan101    1    30    1    FE80::A01:201:3
            (local)
Vlan102    1    30    1    FE80::A01:201:4
            (local)
```

#スイッチD上のIPv6 PIMネイバー関係を表示します。

```
[SwitchD] display ipv6 pim neighbor
```

Total Number of Neighbors = 3

Neighbor	Interface	Uptime	Expires	Dr-
Priority FE80::A01:101:1	Vlan103	00:04:00	00:01:29	1
FE80::B01:102:2	Vlan101	00:04:16	00:01:29	3
FE80::C01:103:3	Vlan102	00:03:54	00:01:17	5

#IPv6マルチキャストグループFF0E::101に参加するために、ホストAからMLDレポートを送信します(詳細は省略)。

#IPv6マルチキャスト送信元4001::100/64からIPv6マルチキャストグループFF0E::101にIPv6マルチキャストデータを送信します(詳細は省略)。

#スイッチA上のIPv6 PIMマルチキャストルーティングテーブル情報を表示します。

```
[SwitchA] display ipv6 pim routing-table
```

Total 1 (*, G) entry; 1 (S, G) entry

(*, FF0E::101)

Protocol: pim-dm, Flag: WC

UpTime: 00:01:24

Upstream interface: NULL

Upstream neighbor: NULL

RPF prime neighbor: NULL

Downstream interface(s) information:

Total number of downstreams: 1

1:Vlan-interface100

Protocol: mld, UpTime: 00:01:20, Expires: -

(4001::100, FF0E::101)

Protocol: pim-dm, Flag: ACT

UpTime: 00:01:20

Upstream interface: Vlan-interface103

Upstream neighbor: 1002::2

RPF prime neighbor: 1002::2

Downstream interface(s) information:

Total number of downstreams: 1

1: Vlan-interface100

Protocol: pim-dm, UpTime: 00:01:20, Expires: -

#スイッチD上のIPv6 PIMマルチキャストルーティングテーブル情報を表示します。

```
[SwitchD] display ipv6 pim routing-table
```

Total 0 (*, G) entry; 1 (S, G) entry

(4001::100, FF0E::101)

Protocol: pim-dm, Flag: LOC ACT

UpTime: 00:02:19

Upstream interface: Vlan-interface300

Upstream neighbor: NULL

RPF prime neighbor: NULL

Downstream interface(s) information:

Total number of downstreams: 2

1: Vlan-interface103

Protocol: pim-dm, UpTime: 00:02:19, Expires: -

2: Vlan-interface102

Protocol: pim-dm, UpTime: 00:02:19, Expires: -

出力には次の情報が表示されます。

- SPTパス上のスイッチ(スイッチAおよびスイッチD)には、正しい(S, G)エントリがあります。
- スイッチAには正しい(*,G)エントリがあります。

例:非スコープIPv6 PIM-SMの設定

ネットワークの設定

図95に示します。

- OSPFv3はネットワーク上で動作します。
- VODストリームは、マルチキャストでレシーバホストに送信されます。異なるサブネットのレシーバはスタブネットワークを形成し、各スタブネットワークには少なくとも1つのレシーバホストが存在します。IPv6 PIM-SMドメイン全体に含まれるBSRは1つだけです。
- ホストAおよびホストCは、スタブネットワークN1およびN2のマルチキャストレシーバです。
- スイッチEのVLANインターフェイス102をC-BSRおよびC-RPとして指定します。C-RPは、IPv6マルチキャストグループ範囲FF0E::101/64に指定されます。ダイナミックRPをバックアップするには、すべてのスイッチでスイッチDのVLANインターフェイス101をスタティックRPとして指定します。
- MLDv1は、スイッチAとN1の間、およびスイッチB、スイッチC、N2の間で動作します。

図95 ネットワークダイアグラム

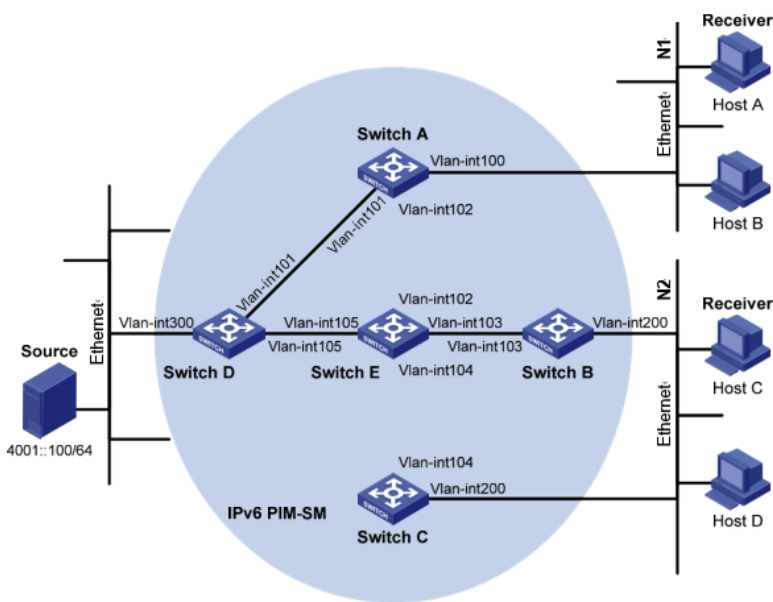


表20 インターフェイスおよびIPv6アドレスの割り当て

デバイス	インターフェイス	IPv6アドレス	デバイス	インターフェイス	IPv6アドレス
Switch A	Vlan-int100	1001::1/64	Switch D	Vlan-int300	4001::1/64
Switch A	Vlan-int101	1002::1/64	Switch D	Vlan-int101	1002::2/64
Switch A	Vlan-int102	1003::1/64	Switch D	Vlan-int105	4002::1/64
Switch B	Vlan-int200	2001::1/64	Switch E	Vlan-int104	3001::2/64
Switch B	Vlan-int103	200::1/64	Switch E	Vlan-int103	2002::2/64
Switch C	Vlan-int200	2001::2/64	Switch E	Vlan-int102	1003::2/64
Switch C	Vlan-int104	3001::1/64	Switch E	Vlan-int105	4002::2/64

手順

1. 図95に示すように、IPv6アドレスとプレフィックス長を各インターフェイスに割り当てます。(詳細は省略)
2. IPv6 PIM-SMドメイン内のすべてのスイッチにOSPFv3を設定します。(詳細は省略)。
3. IPv6マルチキャストルーティング、MLD、およびIPv6 PIM-SMの有効化

On Switch A, enable IPv6 multicast routing.

```
<SwitchA> system-view
```

```
[SwitchA] ipv6 multicast routing
```

```
[SwitchA-mrib6] quit
```

Enable MLD on VLAN-interface 100 (the interface that is connected to the stub network).

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] mld enable
```

```
[SwitchA-Vlan-interface100] quit
```

Enable IPv6 PIM-SM on other interfaces.

```
[SwitchA] interface vlan-interface 101
```

```
[SwitchA-Vlan-interface101] ipv6 pim sm
```

```
[SwitchA-Vlan-interface101] quit
```

```
[SwitchA] interface vlan-interface 102
```

```
[SwitchA-Vlan-interface102] ipv6 pim sm
```

```
[SwitchA-Vlan-interface102] quit
```

#スイッチAを設定するのと同じ方法で、スイッチBとスイッチCでIPv6マルチキャストルーティング、MLD、およびIPv6 PIM-SMを有効にします(詳細は省略)。

#スイッチAを設定するのと同じ方法で、スイッチDとスイッチEでIPv6マルチキャストルーティングとIPv6 PIM-SMを有効にします(詳細は省略)。

4. C-BSR、C-RP、およびスタティックRPを設定します。

On Switch E, configure the service scope of RP advertisements.

```
<SwitchE> system-view
```

```
[SwitchE] acl ipv6 basic 2005
```

```
[SwitchE-acl-ipv6-basic-2005] rule permit source ff0e::101 64
```

```
[SwitchE-acl-ipv6-basic-2005] quit
```

Configure VLAN-interface 102 as a C-BSR and a C-RP, and configure VLAN-interface 101 of Switch D as the static RP.

```
[SwitchE] ipv6 pim
```

```
[SwitchE-pim6] c-bsr 1003::2
```

```
[SwitchE-pim6] c-rp 1003::2 group-policy 2005
```

```
[SwitchE-pim6] static-rp 1002::2
```

```
[SwitchE-pim6] quit
```

On Switch A, configure VLAN-interface 101 of Switch D as a static RP.

```
[SwitchA] ipv6 pim
```

```
[SwitchA-pim6] static-rp 1002::2
```

```
[SwitchA-pim6] quit
```

#スイッチAと同じ方法で、スイッチB、スイッチC、およびスイッチDにスタティックRPを設定します。

(詳細は省略)。

設定の確認

#スイッチAのIPv6 PIM情報を表示します。

```
[SwitchA] display ipv6 pim interface
```

Interface	NbrCnt	HelloInt	DR-Pri	DR-Address
Vlan101	1	30	1	FE80::A01:201:2
Vlan102	1	30	1	FE80::A01:201:3

#スイッチAのBSR情報を表示します。

```
[SwitchA] display ipv6 pim bsr-info
```

Scope: non-scoped

State: Accept Preferred Bootstrap timer:
00:01:44 Elected BSR address: 1003::2

Priority: 64

Hash mask length: 126

Uptime: 00:11:18

#スイッチEのBSR情報を表示します。

```
[SwitchE] display ipv6 pim bsr-info
```

Scope: non-scoped

State: Elected

Bootstrap timer: 00:01:44

Elected BSR address: 1003::2

Priority: 64

Hash mask length: 126

Uptime: 00:11:18

Candidate BSR address: 1003::2

Priority: 64

Hash mask length: 126

Display RP information on Switch A.

```
[SwitchA] display ipv6 pim rp-info
```

BSR RP information:

Scope: non-scoped

Group/MaskLen: FF0E::101/64

RP address	Priority	HoldTime	Uptime	Expires
1003::2	192	180	00:05:19	00:02:11

Static RP information:

RP address	ACL	Mode	Preferred
1002::2	----	pim-sm	No

例:管理スコープのIPv6 PIM-SMの設定

ネットワークの設定

図96に示します。

- OSPFv3はネットワーク上で動作します。
 - VODストリームは、マルチキャストで受信ホストに送信されます。IPv6 PIM-SMドメイン全体は、IPv6管理スコープゾーン1、IPv6管理スコープゾーン2、およびIPv6グローバルスコープゾーンに分割されます。スイッチB、スイッチC、およびスイッチDは、それぞれ3つのゾーンのZBRです。
 - 送信元1と送信元2は異なるIPv6マルチキャストデータをIPv6マルチキャストグループFF14::101に送信します。ホストAはIPv6マルチキャストデータを送信元1からだけ受信し、ホストBはIPv6マルチキャストデータを送信元2からだけ受信します。送信元3はIPv6マルチキャストデータをIPv6マルチキャストグループFF1E::202に送信します。ホストCはIPv6マルチキャストグループFF1E::202のIPv6マルチキャストレシーバです。
 - スイッチBのVLANインターフェイス101は、IPv6管理スコープゾーン1のC-BSRおよびC-RPとして動作し、スイッチDのVLANインターフェイス105は、IPv6管理スコープゾーンのC-BSRおよびC-RPとして動作します。
2. 2つのインターフェイスは両方とも、スコープフィールド値が4のIPv6マルチキャストグループに指定されています。スイッチFのVLANインターフェイス109は、IPv6のC-BSRおよびC-RPとして機能します。
- グローバルスコープゾーンであり、スコープフィールド値14でIPv6マルチキャストグループに指定されます。
- MLDv1は、スイッチA、スイッチE、スイッチI、およびこれらに直接接続されたレシーバの間でそれぞれ動作します。

図96 ネットワークダイアグラム

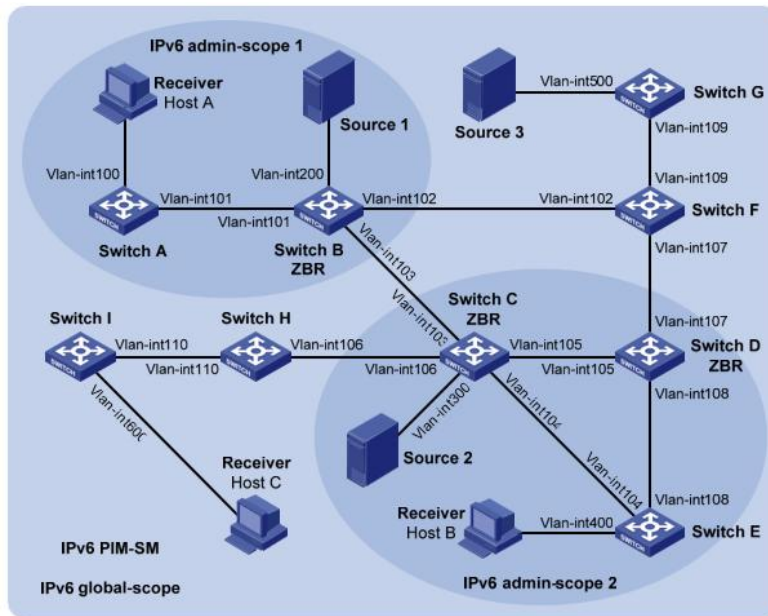


表21 インターフェイスおよびIPv6アドレス割り当て

デバイス	インターフェイス	IPv6アドレス	デバイス	インターフェイス	IPv6アドレス
Switch A	Vlan-int100	1001::1/64	Switch E	Vlan-int104	3002::2/64
Switch A	Vlan-int101	1002::1/64	Switch E	Vlan-int108	6001::2/64
Switch B	Vlan-int200	2001::1/64	Switch F	Vlan-int109	8001::1/64
Switch B	Vlan-int101	1002::2/64	Switch F	Vlan-int107	6002::2/64
Switch B	Vlan-int103	2002::1/64	Switch F	Vlan-int102	2003::2/64
Switch B	Vlan-int102	2003::1/64	Switch G	Vlan-int500>	9001::1/64
Switch C	Vlan-int300	3001::1/64	Switch G	Vlan-int109	8001::2/64
Switch C	Vlan-int104	3002::1/64	Switch H	Vlan-int110	4001::1/64
Switch C	Vlan-int105	3003::1/64	Switch H	Vlan-int106	3004::2/64
Switch C	Vlan-int103	2002::2/64	Switch I	Vlan-int600	5001::1/64
Switch C	Vlan-int106	3004::1/64	Switch I	Vlan-int110	4001::2/64
Switch D	Vlan-int105	3003::2/64	Source1	-	2001::100/64
Switch D	Vlan-int108	6001::1/64	Source2	-	3001::100/64
Switch D	Vlan-int107	6002::1/64	Source3	-	9001::100/64
Switch E	Vlan-int400	7001::1/64			

手順

1. 図96に示すように、IPv6アドレスとプレフィックス長を各インターフェイスに割り当てます。(詳細は省略)
2. IPv6 PIM-SMDメイン内のすべてのスイッチにOSPFv3を設定します。(詳細は省略)。
3. IPv6マルチキャストルーティング、MLD、およびIPv6 PIM-SMを有効にします。

On Switch A, enable IPv6 multicast routing.

```
<SwitchA> system-view
```

```
[SwitchA] ipv6 multicast routing
```

```
[SwitchA-mrib6] quit
```

Enable MLD on the receiver-side interface (VLAN-interface 100).

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] mld enable
```

```
[SwitchA-Vlan-interface100] quit
```

Enable IPv6 PIM-SM on VLAN-interface 101.

```
[SwitchA] interface vlan-interface 101
```

```
[SwitchA-Vlan-interface101] ipv6 pim sm
```

```
[SwitchA-Vlan-interface101] quit
```

Enable IPv6 multicast routing, MLD, and IPv6 PIM-SM on Switch E and Switch I in the same way Switch A is configured. (Details not shown.)

On Switch B, enable IPv6 multicast routing, and enable IPv6 PIM-SM on each interface.

```
<SwitchB> system-view
```

```
[SwitchB] ipv6 multicast routing
```

```
[SwitchB-mrib6] quit
```

```
[SwitchB] interface vlan-interface 200
```

```
[SwitchB-Vlan-interface200] ipv6 pim sm
```

```
[SwitchB-Vlan-interface200] quit
```

```
[SwitchB] interface vlan-interface 101
```

```
[SwitchB-Vlan-interface101] ipv6 pim sm
```

```
[SwitchB-Vlan-interface101] quit
```

```
[SwitchB] interface vlan-interface 102
```

```
[SwitchB-Vlan-interface102] ipv6 pim sm
```

```
[SwitchB-Vlan-interface102] quit
```

```
[SwitchB] interface vlan-interface 103
```

```
[SwitchB-Vlan-interface103] ipv6 pim sm
```

```
[SwitchB-Vlan-interface103] quit
```

#スイッチBの設定と同じ方法で、スイッチC、スイッチD、スイッチF、スイッチG、およびスイッチHでIPv6マルチキャストルーティングとIPv6 PIM-SMを有効にします(詳細は省略)。

4. IPv6管理スコープゾーン境界を設定します。

On Switch B, configure VLAN-interface 102 and VLAN-interface 103 as the boundaries of IPv6 admin-scoped zone 1.

```
[SwitchB] interface vlan-interface 102
```

```
[SwitchB-Vlan-interface102] ipv6 multicast boundary scope 4
```

```
[SwitchB-Vlan-interface102] quit
```

```
[SwitchB] interface vlan-interface 103
```

```
[SwitchB-Vlan-interface103] ipv6 multicast boundary scope 4
```

```
[SwitchB-Vlan-interface103] quit
```

On Switch C, configure VLAN-interface 103 and VLAN-interface 106 as the boundaries of IPv6 admin-scoped zone 2.

```
<SwitchC> system-view
```

```
[SwitchC] interface vlan-interface 103
```

```
[SwitchC-Vlan-interface103] ipv6 multicast boundary scope 4
[SwitchC-Vlan-interface103] quit
[SwitchC] interface vlan-interface 106
[SwitchC-Vlan-interface106] ipv6 multicast boundary scope 4
[SwitchC-Vlan-interface106] quit
```

On Switch D, configure VLAN-interface 107 as the boundary of IPv6 admin-scoped zone 2.

```
<SwitchD> system-view
[SwitchD] interface vlan-interface 107
[SwitchD-Vlan-interface107] ipv6 multicast boundary scope 4
[SwitchD-Vlan-interface107] quit
```

5. C-BSRおよびC-RPを設定します。

#スイッチBで、VLANインターフェイス101をIPv6管理スコープゾーン1のC-BSRおよびC-RPとして設定します。

```
[SwitchB] ipv6 pim
[SwitchB-pim6] c-bsr 1002::2 scope 4
[SwitchB-pim6] c-rp 1002::2 scope 4
[SwitchB-pim6] quit
```

#スイッチDで、VLANインターフェイス105をIPv6管理スコープゾーン2のC-BSRおよびC-RPとして設定します。

```
[SwitchD] ipv6 pim
[SwitchD-pim6] c-bsr 3003::2 scope 4
[SwitchD-pim6] c-rp 3003::2 scope 4
[SwitchD-pim6] quit
```

#スイッチFで、VLANインターフェイス109をIPv6のC-BSRおよびC-RPとして設定します。

```
<SwitchF> system-view
[SwitchF] ipv6 pim
[SwitchF-pim6] c-bsr 8001::1
[SwitchF-pim6] c-rp 8001::1
[SwitchF-pim6] quit
```

設定の確認

#スイッチBのBSR情報を表示します。

```
[SwitchB] display ipv6 pim bsr-info
Scope: non-scoped
  State: Accept Preferred
  Bootstrap timer: 00:01:25
  Elected BSR address: 8001::1
  Priority: 64
  Hash mask length: 126
  Uptime: 00:01:45
```

```
Scope: 4
  State: Elected
  Bootstrap timer: 00:00:0
  Elected BSR address: 1002::2
  Priority: 64
```


Hash mask length: 126
Uptime: 00:04:54
Candidate BSR address: 1002::2
Priority: 64
Hash mask length: 126

#スイッチDのBSR情報を表示します。

[SwitchD] display ipv6 pim bsr-info
Scope: non-scoped
State: Accept Preferred
Bootstrap timer: 00:01:25
Elected BSR address: 8001::1
Priority: 64
Hash mask length: 126
Uptime: 00:01:45

Scope: 4
State: Elected
Bootstrap timer: 00:01:25
Elected BSR address: 3003::2
Priority: 64
Hash mask length: 126
Uptime: 00:01:45
Candidate BSR address: 3003::
Priority: 64
Hash mask length: 126

#スイッチFのBSR情報を表示します。

[SwitchF] display ipv6 pim bsr-info
Scope: non-scoped
State: Elected
Bootstrap timer: 00:00:49
Elected BSR address: 8001::1
Priority: 64
Hash mask length: 126
Uptime: 00:01:11
Candidate BSR address: 8001::1
Priority: 64
Hash mask length: 126

#スイッチBのRP情報を表示します。

[SwitchB] display ipv6 pim rp-info
BSR RP information:
Scope: non-scoped

Group/MaskLen: FF00::/8

RP address	Priority	HoldTime	Uptime	Expires
8001::1	192	180	00:01:14	00:02:46

Scope: 4

Group/MaskLen: FF04::/16

RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FF14::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FF24::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FF34::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FF44::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FF54::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FF64::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FF74::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FF84::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FF94::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FFA4::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FFB4::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FFC4::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FFD4::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FFE4::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FFF4::/16				
RP address	Priority	HoldTime	Uptime	Expires

1002::2 (local)	192	180	00:02:03	00:02:56
Group/MaskLen: FF04::/16				
RP address	Priority	HoldTime	Uptime	Expires
1002::2 (local)	192	180	00:02:03	00:02:56

#スイッチFのRP情報を表示します。

[SwitchF] display ipv6 pim rp-info

BSR RP information:

Scope: non-scoped

Group/MaskLen: FF00::/8

RP address	Priority	HoldTime	Uptime	Expires
8001::1 (local)	192	180	00:10:28	00:02:31

例:IPv6 PIM-SSMの設定

ネットワークの設定

図97に示します。

- OSPFv3はネットワーク上で動作します。
- レシーバはマルチキャストを介してビデオオンデマンド情報を受信します。異なる組織のレシーバグループはスタブネットワークを形成し、各スタブネットワークには1つ以上のレシーバホストが存在します。IPv6 PIMドメイン全体がSSMモードで動作します。
- ホストAとホストCは、2つのスタブネットワークN1とN2上のIPv6マルチキャストレシーバです。
- SSMグループの範囲はFF3E::/64です。
- MLDv2は、スイッチAとN1の間、およびスイッチB、スイッチC、N2の間で動作します。

図97 ネットワークダイアグラム

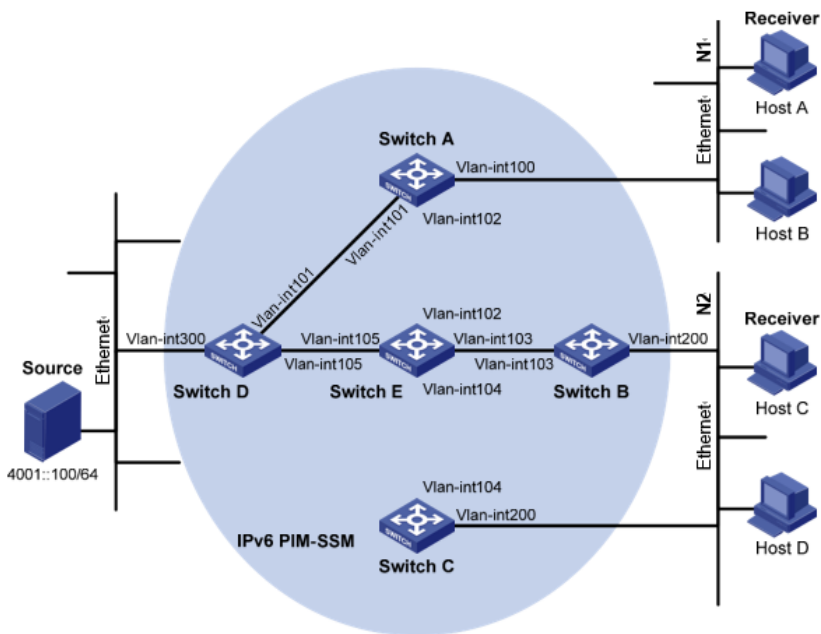


表22 インターフェイスおよびIPv6アドレス割り当て

デバイス	インターフェイス	IPv6アドレス	デバイス	インターフェイス	IPv6アドレス
Switch A	Vlan-int100	1001::1/64	Switch D	Vlan-int300	4001::1/64
Switch A	Vlan-int101	1002::1/64	Switch D	Vlan-int101	1002::2/64
Switch A	Vlan-int102	1003::1/64	Switch D	Vlan-int105	4002::1/64
Switch B	Vlan-int200	2001::1/64	Switch E	Vlan-int104	3001::2/64
Switch B	Vlan-int103	2002::1/64	Switch E	Vlan-int103	2002::2/64
Switch C	Vlan-int200	2001::2/64	Switch E	Vlan-int102	1003::2/64
Switch C	Vlan-int104	3001::1/64	Switch E	Vlan-int105	4002::2/64

手順

1. 図97に示すように、IPv6アドレスとプレフィックス長を各インターフェイスに割り当てます。(詳細は

省略)

2. IPv6 PIM-SSMドメイン内のスイッチにOSPFv3を設定します。(詳細は省略)。
3. IPv6マルチキャストルーティング、MLD、およびIPv6 PIM-SMを有効にします。

#スイッチAで、IPv6マルチキャストルーティングを有効にします。

```
<SwitchA> system-view
```

```
[SwitchA] ipv6 multicast routing
```

```
[SwitchA-mrib6] quit
```

Enable MLDv2 on VLAN-interface 100 (the interface that connects to the stub network).

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] mld enable
```

```
[SwitchA-Vlan-interface100] mld version 2
```

```
[SwitchA-Vlan-interface100] quit
```

Enable IPv6 PIM-SM on the other interfaces.

```
[SwitchA] interface vlan-interface 101
```

```
[SwitchA-Vlan-interface101] ipv6 pim sm
```

```
[SwitchA-Vlan-interface101] quit
```

```
[SwitchA] interface vlan-interface 102
```

```
[SwitchA-Vlan-interface102] ipv6 pim sm
```

```
[SwitchA-Vlan-interface102] quit
```

#スイッチBとスイッチCでIPv6マルチキャストルーティング、MLD、およびIPv6 PIM-SMを有効にします。スイッチAの設定方法(詳細は省略)

#スイッチAを設定するのと同じ方法で、スイッチDとスイッチEでIPv6マルチキャストルーティングとIPv6 PIM-SMを有効にします(詳細は省略)。

4. スイッチAでIPv6 SSMグループ範囲FF3E::/64を設定します。

```
[SwitchA] acl ipv6 basic 2000
```

```
[SwitchA-acl-ipv6-basic-2000] rule permit source ff3e:: 64
```

```
[SwitchA-acl-ipv6-basic-2000] quit
```

```
[SwitchA] ipv6 pim
```

```
[SwitchA-pim6] ssm-policy 2000
```

```
[SwitchA-pim6] quit
```

5. スイッチB、スイッチC、スイッチD、およびスイッチEのIPv6 SSMグループ範囲を、スイッチBと同様の方法で設定します。(詳細は省略)。

設定の確認

#スイッチAのIPv6 PIM情報を表示します。

```
[SwitchA] display          ipv6    pim interface
```

Interface	NbrCnt	HelloInt	DR-Pri	DR-Address
Vlan101	1	30	1	FE80::A01:201:2
Vlan102	1	30	1	FE80::A01:201:3

#ホストAからMLDv2レポートを送信して、IPv6マルチキャストソースおよびグループ(4001::100/64, FF3E::101)に参加します(詳細は省略)。

#スイッチA上のIPv6 PIMマルチキャストルーティングテーブル情報を表示します。

```
[SwitchA] display ipv6 pim routing-table
Total 0 (*, G) entry; 1 (S, G) entry
```

```
(4001::100, FF3E::101)
  Protocol: pim-ssm, Flag: ACT
  UpTime: 00:00:11
  Upstream interface: Vlan-interface101
    Upstream neighbor: 1002::2
    RPF prime neighbor: 1002::2
  Downstream interface(s) information:
    Total number of downstreams: 1
      1: Vlan-interface100
        Protocol: mld, UpTime: 00:00:11, Expires: 00:03:25
```

#スイッチB上のIPv6 PIMマルチキャストルーティングテーブル情報を表示します。

```
[SwitchD] display ipv6 pim routing-table
Total 0 (*, G) entry; 1 (S, G) entry
```

```
(4001::100, FF3E::101)
  Protocol: pim-ssm, Flag: LOC
  UpTime: 00:08:02
  Upstream interface: Vlan-interface300
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
  Downstream interface(s) information:
    Total number of downstreams: 1
      1: Vlan-interface105
        Protocol: pim-ssm, UpTime: 00:08:02, Expires: 00:03:25
```

この出力は、SPTパス上のスイッチ(スイッチAおよびスイッチD)が正しい(S, G)エントリを生成したことを示しています。

IPv6 PIMのトラブルシューティング

マルチキャスト配信ツリーを正しく構築できない

症状

IPv6マルチキャストフォワーディングエントリは、IPv6 PIMネットワーク内のデバイス(マルチキャスト送信元または受信者に直接接続されているデバイスを含む)では確立されません。これは、IPv6マルチキャスト配信ツリーを正しく構築できないことを意味します。

解決方法

この問題を解決するには、次の手順を実行し

1. **display ipv6 routing-table**を使用して、IPv6マルチキャスト送信元またはRPへのIPv6ユニキャストルートが使用可能であることを確認します。
2. 各インターフェイス、特にRPFインターフェイスでipv6 PIM情報を確認するには、**display ipv6 pim interface**を使用します。インターフェイスでipv6 PIMが有効になっていない場合は、**pv6 pim dm** または **ipv6 pim sm**を使用して、インターフェイスでipv6 PIM-DMまたはipv6 PIM-SMを有効にします。
3. RPFネイバーがIPv6 PIMネイバーであることを確認するには、**display ipv6 pim neighbor**を使用します。
4. IPv6マルチキャスト送信元またはレシーバに直接接続されているインターフェイスで、IPv6 PIMおよびMLDが有効になっていることを確認します。
5. **display ipv6 pim interface verbose**を使用して、同じipv6 PIMモードがデバイス上のRPFインターフェイスおよびデバイスのRPFネイバーの接続インターフェイスで有効になっていることを確認します。
6. **display current-configuration**を使用して、同じIPv6 PIMモードがネットワーク上のすべてのデバイスで有効になっていることを確認します。IPv6 PIM-SMの場合は、BSRおよびC-RPが正しく設定されていることを確認します。
7. 問題が解決しない場合は、H3Cサポートに連絡してください。

IPv6マルチキャストデータが中間デバイスで異常終了する

症状

中間デバイスはIPv6マルチキャストデータを正常に受信できますが、データはラストホップデバイスに到達できません。中間デバイスのインターフェイスはIPv6マルチキャストデータを受信しますが、IPv6 PIMルーティングテーブルに(S, G)エントリを作成しません。

解決方法

この問題を解決するには、次の手順を実行し

1. ipv6マルチキャスト転送境界設定を確認するには、`display current-configuration`を使用します。マルチキャスト転送境界設定を変更して、ipv6マルチキャストパケットが境界を通過できるようにするには、ipv6マルチキャスト境界を使用します。
2. IPv6マルチキャスト送信元ポリシーを確認するには、`display current-configuration`を使用します。source-policyコマンドで定義されたACLルールを変更して、IPv6マルチキャストデータの送信元/グループアドレスがACLフィルタリングを通過できるようにします。
3. 問題が解決しない場合は、H3Cサポートに連絡してください。

RPがIPv6 PIM-SMのSPTに加入できない

症状

RPTを正しく構築できないか、RPがIPv6マルチキャスト送信元に向けてSPTに加入できません。

解決方法

この問題を解決するには、次の手順を実行し

1. 各デバイスでRPへのIPv6ユニキャストルートが使用可能であることを確認するには、`display ipv6 routing-table`を使用します。
2. ダイナミックRP情報がすべてのデバイスで一貫していることを確認するには、`display ipv6 pim rp-info`を使用します。
3. `display ipv6 pim rp-info`を使用して、同じスタティックRPがネットワーク上のすべてのデバイスに設定されていることを確認します。
4. 問題が解決しない場合は、H3Cサポートに連絡してください。

IPv6 PIM-SMでRPTを構築できない、またはIPv6マルチキャスト送信元登録が失敗する

症状

C-RPはBSRにアドバタイズメントメッセージをユニキャストできません。BSRはC-RP情報を含むBSMをアドバタイズせず、C-RPへのIPv6ユニキャストルートを持ちません。RPTを正しく確立できないか、またはソース側のDRがIPv6マルチキャストソースをRPに登録できません。

解決方法

この問題を解決するには、次の手順を実行し

1. ルーティングテーブル情報を表示するには、各デバイスで`display ipv6 routing-table`を使用します。C-RPおよびBSRへのipv6ユニキャストルートが各デバイスで使用可能であり、各C-RPとBSRの間でルートが使用可能であることを確認します。

2. 各デバイスにBSR情報が存在することを確認するには、**display ipv6 pim bsr-info**を使用します。
3. 各デバイスのRP情報が正しいことを確認するには、**display ipv6 pim rp-info**を使用します。
4. **display ipv6 pim neighbor**を使用して、ipv6 PIMネイバー関係がデバイス間で正しく確立されていることを確認します。
5. 問題が解決しない場合は、H3Cサポートに連絡してください。