IP マルチキャスト：PIM コンフィギュレーション ガイド、Cisco IOS XE Release 3S（Cisco ASR 1000）

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

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

目 次

第 1 章

IP マルチキャスト テクノロジーの概要

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

この章では、IP マルチキャストの技術的概要を説明します。 IP マルチキャストは、ネットワーク リソース（特に、音声やビデオなどの帯域幅集約型サービス）を効率的に使用する方法です。IP マルチキャストの設定を開始する前に、このモジュールに示す情報を理解することが重要です。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

IP マルチキャスト テクノロジーに関する情報

情報配信における IP マルチキャストの役割

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

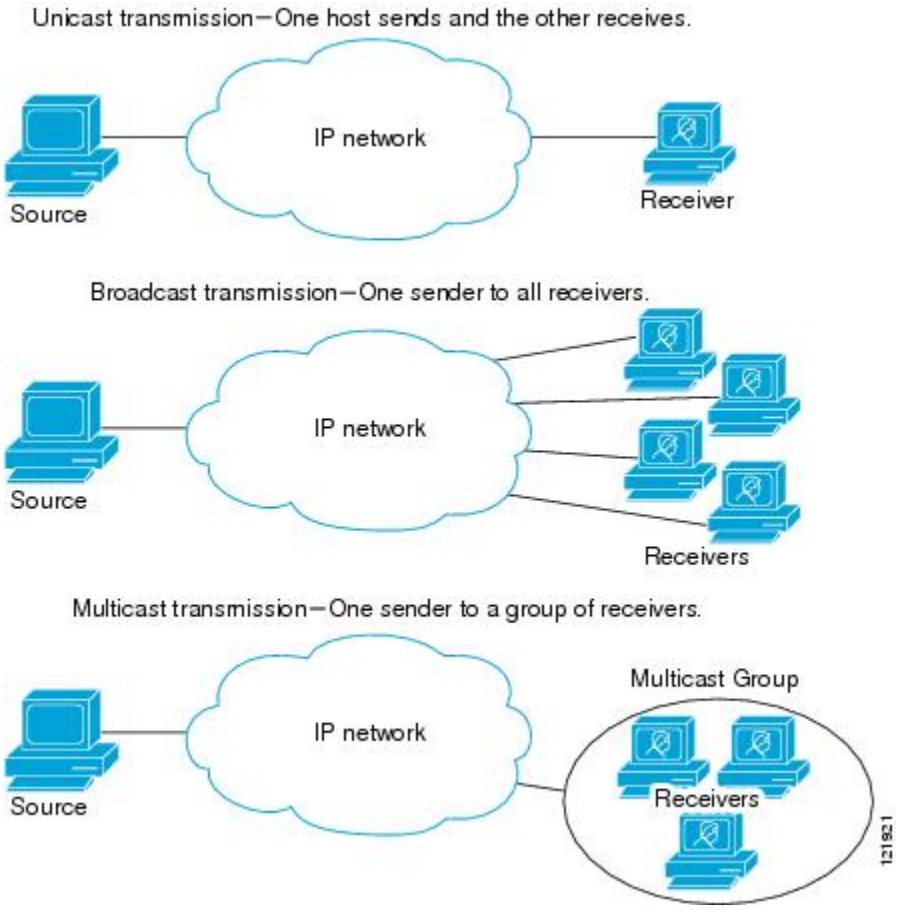
IP マルチキャスト ルーティングを使用すると、ホスト（送信元）は IP「マルチキャスト グループ アドレス」と呼ばれる特殊な形式の IP アドレスを使用し、IP ネットワーク内の任意の場所にあるホスト（レシーバー）のグループにパケットを送信できます。 ソースのホストは、マルチキャスト グループ アドレスをパケットの宛先 IP アドレス フィールドに挿入します。IP マルチキャスト ルータおよびマルチレイヤ スイッチは、受信した IP マルチキャスト パケットを、マルチキャスト グループのメンバにつながるすべてのインターフェイスから転送します。 どのホストも、グループのメンバであるかどうかにか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

マルチキャスト グループの転送方式

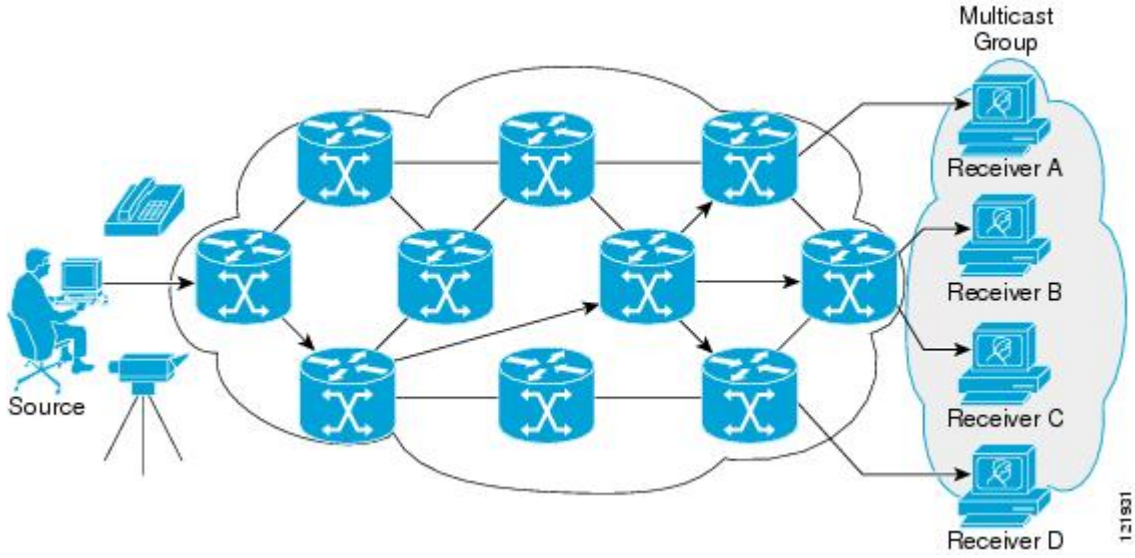
IP 通信は、最初の図に示すように、トラフィックの送信側と受信側として機能するホストで構成されます。 送信側をソースと呼びます。 従来の IP 通信は、別の単一ホスト（ユニキャスト転送）またはすべてのホスト（ブロードキャスト転送）に送信する単一ホストによって実現されます。IP マルチキャストは、1 つのホストがすべてのホストのサブセットにパケットを送信できる 3 番目の方式（マルチキャスト転送）を提供します。 この受信側ホストのサブセットは、マルチキャスト グループと呼ばれます。 マルチキャスト グループに属するホストは、グループ メンバと呼ばれます。

マルチキャストは、このグループの概念に基づいています。マルチキャスト グループは、特定のデータ ストリームを受信するためにグループに加入する任意の数のレシーバです。 このマルチキャスト グループには、物理的境界または地理的境界はありません。ホストは、インターネット上または任意のプライベート インターネットワーク内の任意の場所に配置できます。 ソースから特定のグループへのデータの受信に関与するホストは、そのグループに加入する必要があります。グループへの加入は、インターネット グループ管理プロトコル（IGMP）を介してホスト レシーバによって行われます。

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



次の図では、レシーバ（指定されたマルチキャスト グループ）はソースからビデオ データ ストリームを受信します。 これらのレシーバは、ネットワーク内のルータに IGMP ホスト レポートを送信することによってその意思を示します。 ルータは、ソースからレシーバへのデータ配信を行います。 ルータは、Protocol Independent Multicast（PIM）を使用して、マルチキャスト配信ツリーを動的に作成します。 ビデオ データ ストリームは、ソースとレシーバの間のパスにあるネットワーク セグメントだけに配信されます。



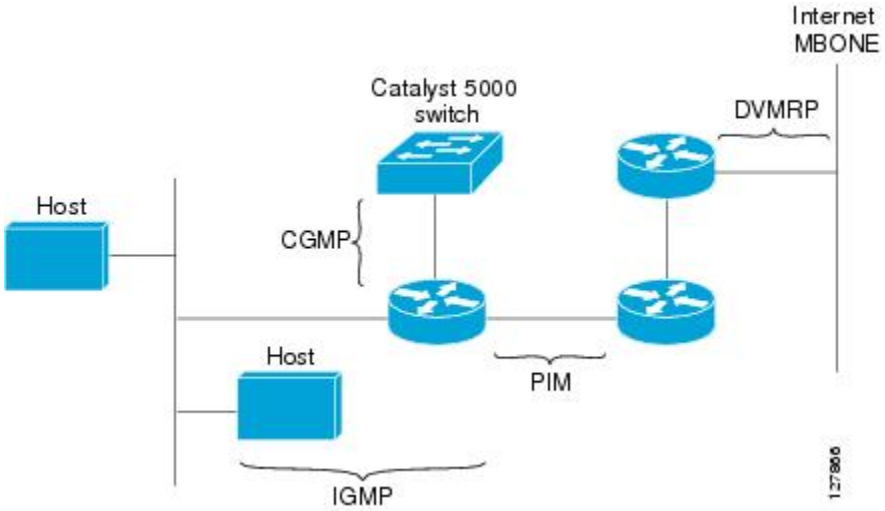
IP マルチキャスト ルーティング プロトコル

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

- IGMP は、ホストがメンバになっているマルチキャスト グループを追跡するために LAN 上のホストと LAN 上のルータ間で使用されます。
- プロトコル独立マルチキャスト（PIM）は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにルータ間で使用されます。
- ディスタンス ベクトル マルチキャスト ルーティング プロトコル（DVMRP）は、MBONE（インターネットのマルチキャスト バックボーン）に使用されます。 ソフトウェアは PIM と DVMRP の相互作用をサポートします。
- Cisco グループ管理プロトコル（CGMP）は、IGMP によって実行される作業と同様の作業を実行するために、Catalyst スイッチに接続されたルータ上で使用されます。

図に、これらのプロトコルが動作する IP マルチキャスト環境内の位置を示します。

図 *1*：*IP* マルチキャスト ルーティング プロトコル



IP マルチキャスト グループ アドレッシング

マルチキャスト グループは、マルチキャスト グループ アドレスによって識別されます。 マルチキャスト パケットは、そのマルチキャスト グループ アドレスに送信されます。 単一のホストを一意に識別するユニキャストアドレスとは異なり、マルチキャストIPアドレスは、特定のホストを識別しません。マルチキャストアドレスに送信されたデータを受信するには、ホストは、そのアドレスによって識別されるグループに加入する必要があります。データは、マルチキャストアドレスに送信され、そのグループに送信されたトラフィックを受信する意思を示してグループに加入しているすべてのホストによって受信されます。マルチキャストグループアドレスは、ソースでグループに割り当てられます。 マルチキャスト グループ アドレスを割り当てるネットワーク管理者は、アドレスが、インターネット割り当て番号局（IANA）によって予約されているマルチキャスト アドレス範囲の割り当てに準拠していることを確認する必要があります。

IP クラス D アドレス

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

（注） クラス D アドレス範囲は、IP マルチキャスト トラフィックのグループ アドレスまたは宛先アドレスだけに使用されます。 マルチキャスト データグラムのソース アドレスは、常にユニキャスト ソースアドレスです。

IP マルチキャスト アドレスのスコーピング

マルチキャスト アドレス範囲は、さまざまなアドレス範囲に対して、およびより小さなドメイン内でアドレスを再使用する場合に、予測可能な動作を提供するために細分化されています。 表に、マルチキャスト アドレス範囲の概要を示します。 それに続いて、各範囲について簡単に説明します。

表 *1*：マルチキャスト アドレス範囲の割り当て

名前	範囲	説明
予約済みリンク ローカル アドレス	224.0.0.0 ～ 224.0.0.255	ローカル ネットワーク セグメント上のネットワーク プロトコル用に予約されています。
グローバル スコープ アドレス	224.0.1.0 ～ 238.255.255.255	組織間およびインターネット上でのマルチキャスト データの送信用に予約されています。
Source Specific Multicast	232.0.0.0 ～ 232.255.255.255	明示的にグループに加入している受信側のみにデータを転送する SSM データグラム配信モデル用に予約されています。
GLOP アドレス	233.0.0.0 ～ 233.255.255.255	割り当て済みの自律システム（AS）ドメイン番号をすでに持つ組織によって静的に定義されるアドレス用に予約されています。
限定スコープ アドレス	239.0.0.0 ～ 239.255.255.255	プライベート マルチキャスト ドメイン用の管理スコープアドレスまたは限定スコープアドレスとして予約されています。

予約済みリンク ローカル アドレス

224.0.0.0 ～ 224.0.0.255 の範囲は、IANA によってローカル ネットワーク セグメント上のネットワーク プロトコル用に予約されています。 この範囲のアドレスを持つパケットのスコープはローカルであり、IP ルータによって転送されません。 通常、リンク ローカル宛先アドレスを持つパケットは存続可能時間（TTL）値 1 を使用して送信されるため、ルータによって転送されません。

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

IANA は、アドレス範囲 224.0.1.xxx からネットワーク プロトコルまたはネットワーク アプリケーションに 1 つのマルチキャスト アドレス要求を割り当てます。 マルチキャスト ルータは、これらのマルチキャスト アドレスを転送します。

グローバル スコープ アドレス

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

Source Specific Multicast アドレス

232.0.0.0/8 のアドレス範囲は、Source Specific Multicast（SSM）用に予約されています。 Cisco IOS ソフトウェアでは、**ip pim ssm** コマンドを使用して任意の IP マルチキャスト アドレスに SSM を設定することもできます。 SSM は、1 対多の通信で効率的なデータ配信メカニズムを可能にする Protocol Independent Multicast（PIM）の拡張です。 SSM については、IP マルチキャスト配信モード, （8 ページ）を参照してください。

GLOP アドレス

RFC 2770『GLOP Addressing in 233/8』で提唱されている GLOP アドレッシングでは、予約済みの AS 番号をすでに持つ組織は、静的に定義するアドレス用に 233.0.0.0/8 の範囲を予約することを推奨しています。 これは、GLOP アドレッシングと呼ばれます。 ドメインの AS 番号は、233.0.0.0/8 アドレス範囲の 2 番目と 3 番目のオクテットに組み込まれます。 たとえば、AS62010 は 16 進形式では F23A と記述します。 この 2 つのオクテット F2 および 3A を分割すると、結果は 10 進数でそれぞれ 242 および 58 となります。 これらの値から 233.242.58.0/24 のサブネットが得られ、AS62010 用にグローバルに予約されます。

限定スコープ アドレス

239.0.0.0 ～ 239.255.255.255 の範囲のアドレスは、プライベート マルチキャスト ドメイン用の限定スコープアドレスまたは管理スコープ アドレスとして予約されています。 これらのアドレスは、ローカル グループまたは組織に使用するように制限されています。 会社、大学、およびその他の組織は、ドメインの外に転送されないローカルマルチキャストアプリケーション用に、限定スコープ アドレスを使用できます。 通常、このアドレス範囲内のマルチキャスト トラフィックが自律システム（AS）またはユーザ定義のドメイン外に流出することを防ぐため、ルータにフィルタを設定します。 AS またはドメイン内では、ローカル マルチキャスト境界を定義できるように、限定スコープ アドレス範囲を細分化することもできます。

（注） ネットワーク管理者は、インターネット上の他のユーザと競合することなく、この範囲のマルチキャスト アドレスをドメイン内で使用できます。

レイヤ 2 マルチキャスト アドレス

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

Cisco グループ管理プロトコル（CGMP）は、IGMP によって実行される作業と同様の作業を実行するために、Catalyst スイッチに接続されたルータ上で使用されます。 IP マルチキャスト データ パケットと IGMP レポート メッセージ（いずれも MAC レベルで同じグループ アドレスにアドレス指定されます）を区別できない Catalyst スイッチの場合、CGMP が必要になります。

IP マルチキャスト配信モード

IP マルチキャスト配信モードは、レシーバ ホストでのみ異なり、ソース ホストでは異なりません。 ソース ホストは、自身の IP アドレスをパケットの IP ソース アドレスとして、グループ アドレスをパケットの IP 宛先アドレスとして、IP マルチキャスト パケットを送信します。

Any Source Multicast（ASM）

Any Source Multicast（ASM）配信モードでは、IP マルチキャストのレシーバ ホストは、任意のバージョンの IGMP を使用してマルチキャスト グループに加入できます。 ルーティング テーブル ステート表記では、このグループは G として表記されます。 レシーバ ホストは、このグループに加入することにより、任意のソースからグループ G に送信された IP マルチキャスト トラフィックを受信する意思を示します。 ネットワークは、宛先アドレス G を持つ任意のソース ホストから送信された IP マルチキャスト パケットを、グループ G に加入しているネットワーク内のすべてのレシーバ ホストに配信します。

ASM では、ネットワーク内でグループ アドレスを割り当てる必要があります。 常に、ASM グループは、1 つのアプリケーションでのみ使用される必要があります。 2 つのアプリケーションが同じ ASM グループを同時に使用する場合は、両方のアプリケーションのレシーバ ホストが両方のアプリケーション ソースからトラフィックを受信します。その結果、ネットワーク内で予期しない過剰なトラフィックが生成される場合があります。この状況では、ネットワーク リンクの輻輳およびアプリケーションのレシーバ ホストの誤動作が発生する可能性があります。

Source Specific Multicast

Source Specific Multicast（SSM）は、ブロードキャスト アプリケーションとしても知られる 1 対多アプリケーションをサポートする最善のデータグラム配信モデルです。 SSMは、オーディオおよ

びビデオのブロードキャストアプリケーション環境を対象としたシスコのIPマルチキャスト実装の中核的なネットワーク テクノロジーです。

SSM配信モードでは、IPマルチキャストのレシーバホストは、IGMPバージョン3（IGMPv3）を使用してチャネル（S, G）にサブスクライブする必要があります。 レシーバ ホストは、このチャネルにサブスクライブすることにより、ソース ホストSからグループGに送信されたIP マルチキャストトラフィックを受信する意思を示します。 ネットワークは、ソースホストSからグループGに送信されたIPマルチキャストパケットを、チャネル(S, G)にサブスクライブしているネットワーク内のすべてのホストに配信します。

SSM では、ネットワーク内でグループ アドレスを割り当てる必要はありません。各ソース ホスト内で割り当てるだけです。 同じソースホストで実行されている異なるアプリケーションは、異なる SSM グループを使用する必要があります。 異なるソース ホストで実行されている異なるアプリケーションは、ネットワーク上で過剰なトラフィックを発生させることなく、任意にSSMグループ アドレスを再利用できます。

プロトコル独立マルチキャスト

プロトコル独立マルチキャスト（PIM）プロトコルは、レシーバによって開始されたメンバーシップの現在の IP マルチキャスト サービス モードを維持します。 PIM は、特定のユニキャスト ルーティング プロトコルには依存しません。これは、IPルーティングプロトコルに依存せず、Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、Border Gateway Protocol（BGP）、スタティック ルートなど、ユニキャスト ルーティング テーブルに入力するために使用されるユニキャストルーティングプロトコルをすべて利用できます。 PIMは、ユニキャスト ルーティング情報を使用してマルチキャスト転送機能を実行します。

PIMはマルチキャストルーティングプロトコルと呼ばれますが、実際は完全な非依存型のマルチキャスト ルーティング テーブルを構築するのではなく、ユニキャスト ルーティング テーブルを使用してリバース パス転送（RPF）チェック機能を実行します。 他のルーティング プロトコルとは異なり、PIM は、ルータ間のルーティング アップデートを送受信しません。

PIM は、RFC 2362『Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification』で定義されています。

PIM は、デンス モードまたはスパース モードで動作できます。 ルータは、スパース グループとデンス グループの両方を同時に処理できます。 これらのモードは、ルータによるマルチキャストルーティングテーブルの書き込み方法と、ルータが直接接続されたLANから受信したマルチキャスト パケットの転送方法を決定します。

PIM の転送（インターフェイス）モードについては、次の項を参照してください。

PIM デンス モード（PIM-DM）

PIM デンス モード（PIM-DM）は、プッシュ モデルを使用してマルチキャスト トラフィックをネットワークの隅々にまでフラッディングします。 このプッシュ モデルは、データを要求するレシーバを使用せずにデータをレシーバに配信するための方式です。 この方式は、ネットワークのあらゆるサブネットにアクティブなレシーバが存在する特定の配置には効率的です。

デンスモードでは、ルータは、他のすべてのルータが特定のグループのマルチキャストパケットの転送を求めていると想定します。あるルータがマルチキャストパケットを受信した場合、直接接続されたメンバまたはPIMネイバーが存在しないときは、ソースにプルーニング メッセージが返送されます。 後続のマルチキャスト パケットは、このプルーニングされたブランチ上のこのルータにはフラッディングされません。 PIMは、ソース ベースのマルチキャスト配信ツリーを構築します。

PIM-DM は最初に、ネットワーク全体にマルチキャスト トラフィックをフラッディングします。ダウンストリーム ネイバーを持たないルータは、不要なトラフィックをプルーニングします。このプロセスは 3 分ごとに繰り返されます。

ルータはフラッディングおよびプルーニング メカニズムを通じてデータ ストリームを受信することにより、ステート情報を蓄積します。 これらのデータ ストリームには、ダウンストリーム ルータがマルチキャスト転送テーブルを構築できるように、ソースおよびグループの情報が含まれます。 PIM-DM ではソース ツリー、つまり（S, G）エントリしかサポートされないので、共有配信ツリーは作成できません。

（注） デンス モードはあまり使用されないため、使用は推奨されていません。 このため、関連モジュールの設定作業では指定しません。

PIM スパース モード

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

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

PIM-SM は、共有ツリー上のデータ パケットを転送することによって、アクティブな送信元に関する情報を配布します。 PIM-SM は少なくとも最初は共有ツリーを使用するので、ランデブー ポイント（RP）を使用する必要があります。 RP は管理上メットワークで設定されている必要があります。 詳細については、ランデブー ポイント，（14 ページ）を参照してください。

スパース モードでは、ルータは、トラフィックに対する明示的な要求がない限り、他のルータはグループのマルチキャストパケットを転送しないと見なします。 ホストがマルチキャスト グループに加入すると、直接接続されたルータは RP に PIM 加入メッセージを送信します。 RP はマルチキャスト グループを追跡します。 マルチキャスト パケットを送信するホストは、そのホストのファーストホップルータによってRPに登録されます。その後、RPは、ソースに加入メッセージを送信します。 この時点で、パケットが共有配信ツリー上で転送されます。 特定のソースから

のマルチキャスト トラフィックが十分である場合、ホストのファースト ホップ ルータは、ソース ベースのマルチキャスト配信ツリーを構築するために加入メッセージをソースに向けて送信できます。

ソースが RP に登録すると、データは共有ツリーを下方向に転送され、レシーバに到達します。エッジ ルータは、RP を介してソースから共有ツリーでデータ パケットを受信するときに、そのソースについて学習します。 次に、エッジ ルータは、そのソースに向けて PIM (S, G)加入メッセージを送信します。 リバース パスに沿った各ルータは、RP アドレスのユニキャスト ルーティング メトリックをソース アドレスのメトリックと比較します。 ソース アドレスのメトリックの方が良い場合は、ソースに向けて PIM（S, G）加入メッセージを転送します。 RP のメトリックと同じ、または RP のメトリックの方が良い場合は、RP と同じ方向に PIM (S, G)加入メッセージが送信されます。 この場合、共有ツリーとソース ツリーは一致すると見なされます。

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

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

スパース-デンス モード

インターフェイス上でスパース モードまたはデンス モードを設定すると、そのインターフェイス全体にスパース性またはデンス性が適用されます。 ただし、環境によっては、単一リージョン内の一部のグループについては PIM をスパース モードで実行し、残りのグループについてはデンス モードで実行しなければならない場合があります。

デンス モードだけ、またはスパース モードだけをイネーブルにする代わりに、スパース-デンス モードをイネーブルにできます。この場合、グループがデンス モードであればインターフェイスはデンス モードとして処理され、グループがスパース モードであればインターフェイスはスパース モードとして処理されます。 インターフェイスがスパース-デンス モードである場合にグループをスパース グループとして処理するには、RP が必要です。

スパース-デンス モードを設定すると、ルータがメンバになっているグループにスパース性またはデンス性の概念が適用されます。

スパース-デンス モードのもう 1 つの利点は、Auto-RP 情報をデンス モードで配信しながら、ユーザ グループのマルチキャスト グループをスパース モード方式で使用できることです。 したがって、リーフ ルータ上にデフォルト RP を設定する必要はありません。

インターフェイスがデンス モードで処理される場合、次のいずれかの条件が満たされると、そのインターフェイスはマルチキャスト ルーティング テーブルの発信インターフェイス リストに追加されます。

- インターフェイス上にメンバまたは DVMRP ネイバーが存在する。
- PIM ネイバーが存在し、グループがプルーニングされていない。

インターフェイスがスパース モードで処理される場合、次のいずれかの条件が満たされると、そのインターフェイスはマルチキャスト ルーティング テーブルの発信インターフェイス リストに追加されます。

- インターフェイス上にメンバまたは DVMRP ネイバーが存在する。
- インターフェイス上の PIM ネイバーが明示的な加入メッセージを受信した。

双方向 PIM

双方向 PIM（Bidir-PIM）は、個々の PIM ドメイン内での効率的な多対多通信用に設計された PIM プロトコルの拡張機能です。双方向モードのマルチキャスト グループは、追加オーバーヘッドを最小限に抑えながら、任意の数のソースに対応できます。

PIM スパース モードで作成される共有ツリーは単方向性です。 これは、データ ストリームが RP（共有ツリーのルート）にもたらされるようにソース ツリーを作成する必要があることを意味します。これにより、データ ストリームはブランチを下方向に転送され、レシーバに到達できます。 ソースのデータは、共有ツリーの上方向にある RP に向かって流れることはできません。これは、双方向共有ツリーと見なされます。

双方向モードでは、トラフィックは、グループの RP をルートとする双方向共有ツリーに沿ってのみ、ルーティングされます。 Bidir-PIM では、RP の IP アドレスは、すべてのルータがその IP アドレスをルートとするループフリーのスパニングツリー トポロジを確立するうえで重要な役割を果たします。 この IP アドレスはルータ アドレスである必要はなく、PIM ドメイン内のどこからでも到達可能なネットワーク上の任意の未割り当て IP アドレスを使用できます。

Bidir-PIM は PIM スパース モード（PIM-SM）のメカニズムから派生しており、共有ツリー動作の多くを共有します。 Bidir-PIM にも、共有ツリーのアップストリームにある RP に向けてソース トラフィックを無条件に転送する機能がありますが、PIM-SM のようなソースの登録プロセスはありません。 これらの変更は、すべてのルータで (*, G) マルチキャスト ルーティング エントリだけに基づいてトラフィックを転送できるようにするには、必要にして十分なものです。 この機能では、ソース固有のステートは不要であり、スケーリング機能を使用して任意の数のソースに対応できます。

マルチキャスト グループ モード

PIM では、マルチキャスト グループのパケット トラフィックは、そのマルチキャスト グループのために設定されたモードのルールに従ってルーティングされます。 PIM の Cisco 実装は、マルチキャスト グループ用に次の 4 つのモードをサポートしています。

- PIM 双方向モード
- PIM スパース モード
- PIM デンス モード
- PIM Source Specific Multicast（SSM）モード

ルータは、異なるマルチキャスト グループに対して、4 つのモードすべて、またはそれらの任意の組み合わせを同時にサポートできます。

双方向モード

双方向モードでは、トラフィックは、グループのランデブー ポイント（RP）をルートとする双方向共有ツリーに沿ってのみ、ルーティングされます。 Bidir-PIM では、RP の IP アドレスは、すべてのルータがその IP アドレスをルートとするループフリーのスパニングツリー トポロジを確立するうえで重要な役割を果たします。 この IP アドレスはルータである必要はなく、PIM ドメイン内のどこからでも到達可能なネットワーク上の任意の未割り当て IP アドレスを使用できます。 この技術は、Bidir-PIM の冗長 RP 設定を確立するための優先設定方式です。

双方向グループに対するメンバーシップは、明示的な加入メッセージを通じて伝えられます。ソースからのトラフィックは、無条件で、共有ツリーの上方向にある RP に向けて送信され、ツリーの下方向にある各ブランチ上のレシーバに渡されます。

スパース モード

スパース モード動作は 1 つの単方向共有ツリーを中心としており、そのルート ノードは Rendezvous Point（RP）と呼ばれます。 マルチキャスト トラフィックが RP 経由で共有ツリーを下方向に流れるためには、ソースが RP に登録する必要があります。 この登録プロセスでは、ネットワーク内のグループにアクティブなレシーバが存在すると、実際に RP によって最短パス ツリー（SPT）加入がソースに向けてトリガーされます。

スパース モード グループは、明示的な相互運用加入モデルを使用します。 レシーバ ホストは、ランデブー ポイント（RP）でグループに加入します。 異なるグループは、異なる RP を持つ可能性があります。

マルチキャスト トラフィック パケットは、共有ツリーを下方向へ流れ、トラフィックの受信を明示的に求めたレシーバだけに到達します。

デンス モード

デンス モードは、ブロードキャスト（フラッディング）およびプルーニング モデルを使用して動作します。

マルチキャスト ルーティング テーブルに値を入力する際には、デンス モード インターフェイスが常にテーブルに追加されます。 マルチキャスト トラフィックは、発信インターフェイス リスト内のすべてのインターフェイスからすべてのレシーバへ転送されます。 インターフェイスは、プルーニングと呼ばれるプロセスで発信インターフェイス リストから削除されます。 デンス モードでは、直接接続されたレシーバが存在しないなど、さまざまな理由でインターフェイスがプルーニングされます。

プルーニングされたインターフェイスは再構築が可能です。つまり、マルチキャスト トラフィックのフローを最小限の遅延で再開できるように再接合できます。

ランデブー ポイント

ランデブー ポイント（RP）は、デバイスが Protocol Independent Multicast（PIM）のスパース モード（SM）で動作しているときに実行する役割です。 RP が必要になるのは、PIM SM を実行しているネットワークだけです。 PIM SM モデルでは、マルチキャスト データを明示的に要求したアクティブなレシーバを含むネットワーク セグメントだけにトラフィックが転送されます。 マルチキャスト データを配信するこの方法は、PIM デンス モード（PIM-DM）とは対照的です。 PIM DM では、マルチキャスト トラフィックは、最初にネットワークのすべてのセグメントにフラッディングされます。 ダウンストリーム ネイバーを持たないルータやレシーバに直接接続されたルータは、不要なトラフィックをプルーニングします。

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

ほとんどの場合、ネットワークにおける RP の配置は複雑な判断を必要としません。 デフォルトでは、RP が必要になるのは、ソースおよびレシーバとの新しいセッションを開始する場合だけです。 その結果、RP では、トラフィックのフローまたは処理によるオーバーヘッドはほとんど発生しません。 PIM バージョン 2 では、ステートを作成する RP にソースが定期的に登録するだけなので、RP が実行する処理は PIM バージョン 1 より少なくなります。

Auto-RP

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

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

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

複数の RP を使用して、異なるグループ範囲にサービスを提供したり、互いにバックアップとしての役割を果たしたりできます。 Auto-RP が機能するためには、RP 通知メッセージを RP から受信して競合を解決する RP マッピング エージェントとしてルータが指定されている必要があります。 その後、RP マッピング エージェントは、グループから RP への一貫したマッピングを他のす

べてのルータに送信するようになります。 これにより、すべてのルータは、サポート対象のグループに使用する RP を自動的に検出します。

（注） PIM をスパース モードまたはデンス モードに設定し、Auto-RP を設定しない場合は、RP を静的に設定する必要があります。

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

Auto-RP が機能するためには、RP 通知メッセージを RP から受信して競合を解決する RP マッピング エージェントとしてルータが指定されている必要があります。 その後、RP マッピング エージェントは、デンス モード フラッディングにより、グループから RP への一貫したマッピングを他のすべてのルータに送信するようになります。 これにより、すべてのルータは、サポート対象のグループに使用する RP を自動的に検出します。 インターネット割り当て番号局（IANA）は、224.0.1.39 と 224.0.1.40 という 2 つのグループ アドレスを Auto-RP 用に割り当てています。 Auto-RP の利点の 1 つは、指定した RP に対するすべての変更は、RP であるルータ上で設定するだけで、リーフ ルータ上で設定する必要がないことです。 Auto-RP のもう 1 つの利点は、ドメイン内で RP アドレスのスコープを設定する機能を提供することです。 スコーピングを設定するには、Auto-RP アドバタイズメントに許容されている存続可能時間（TTL）値を定義します。

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

Auto-RP のスパース-デンス モード

Auto-RP の前提条件は、**ip pim sparse-dense-mode** インターフェイス コンフィギュレーション コマンドを使用して、すべてのインターフェイスをスパース - デンス モードで設定する必要があることです。 スパース-デンス モードで設定されたインターフェイスは、マルチキャスト グループの動作モードに応じてスパース モードまたはデンス モードで処理されます。 マルチキャスト グループ内に既知の RP が存在する場合、インターフェイスはスパース モードで処理されます。 グループ内に既知の RP が存在しない場合、デフォルトでは、インターフェイスはデンス モードで処理され、このインターフェイス上にデータがフラッディングされます（デンス モード フォールバックを回避することもできます。「基本的な IP マルチキャスト設定」モジュールを参照してください）。

Auto-RP を正常に実装し、224.0.1.39 および 224.0.1.40 以外のグループがデンス モードで動作することを回避するには、「シンク RP」（「ラスト リゾート RP」とも呼ばれます）を設定することを推奨します。 シンク RP は、ネットワーク内に実際に存在するかどうかわからない静的に設定された RP です。 デフォルトでは、Auto-RP メッセージはスタティック RP 設定よりも優先される

ため、シンク RP の設定は Auto-RP の動作と干渉しません。 未知のソースや予期しないソースをアクティブにできるため、ネットワーク内の可能なすべてのマルチキャスト グループにシンク RP を設定することを推奨します。 ソースの登録を制限するように設定された RP がない場合は、グループがデンス モードに戻り、データがフラッディングされる可能性があります。

BSR

PIM-SM バージョン 2 では、Auto-RP に続いてブートストラップ ルータ（BSP）と呼ばれるもう 1 つの RP 選択モデルが導入されました。 BSR は、RP 機能およびグループの RP 情報のリレーに候補ルータを使用するという点において Auto-RP と同様に動作します。 RP 情報は、PIM メッセージ内で伝送される BSR メッセージを通じて配信されます。 PIM メッセージは、PIM ルータから PIM ルータに送信されるリンクローカル マルチキャスト メッセージです。 RP 情報を広めるこのシングル ホップ方式のために、TTL スコーピングは BSR と一緒に使用できません。 デンス モード動作に戻るというリスクを冒さないこと、およびドメイン内でスコープ設定機能を提供しないことを除いて、BSR は RP と同様に動作します。

Multicast Source Discovery Protocol

PIM スパース モード モデルでは、マルチキャスト ソースおよびレシーバはローカルのランデブー ポイント（RP）に登録する必要があります。 実際には、ソースまたはレシーバに最も近いルータが RP に登録しますが、注目すべき重要点は、RP が特定のグループのすべてのソースおよびレシーバを認識していることです。 他のドメインの RP が他のドメインに存在するソースについて知る方法はありません。 Multicast Source Discovery Protocol（MSDP）は、この問題を解決するための洗練された手段です。

MSDP は、アクティブなソースに関する情報を RP が共有できるようにするメカニズムです。 RP は、ローカル ドメイン内のレシーバを認識しています。 リモート ドメインの RP は、アクティブなソースについてヒアリングすると、その情報をそれぞれのローカル レシーバに渡すことができます。 その後、ドメイン間でマルチキャスト データを転送できるようになります。 MSDP の便利な機能は、他のドメインに依存しない独自の RP を各ドメインが維持することは許可するが、RP がドメイン間でトラフィックを転送することは許可しないことです。 マルチキャスト ドメイン間でのトラフィックの転送には、PIM-SM が使用されます。

各ドメインの RP は、TCP 接続を使用して、他のドメインの RP または他のドメインに接続する境界ルータとの MSDP ピアリング セッションを確立します。 RP は、（正規の PIM 登録メカニズムを通じて）自身のドメイン内にある新しいマルチキャスト ソースについて知ると、Source-Active（SA）メッセージの最初のデータ パケットをカプセル化し、その SA をすべての MSDP ピアに送信します。 各受信側ピアは、相互接続されたネットワーク（理論的には、マルチキャスト インターネット全体）内のすべての MSDP ルータに SA が到達するまで、修正されたリバース パス転送（RPF）チェックを使用して SA を転送します。 受信側の MSDP ピアが RP であり、その RP に SA 内のグループに対する (*, G) エントリがある（該当する受信先が存在する）場合、RP はソースに対して (S, G) ステートを作成し、ソースの最短パス ツリーに加入します。 このカプセル化されたデータはカプセル化解除され、その RP の共有ツリーを下方向に転送されます。 ラスト ホップ ルータ（レシーバに最も近いルータ）は、マルチキャスト パケットを受信すると、ソースへの最短パス ツリーに加入できるようになります。 MSDP スピーカーは、その RP のドメイン内のすべてのソースを含む SA を定期的に送信します。

MSDP は、インターネット サービス プロバイダー（ISP）間のピアリングを実現するために開発されました。 ISP は、競合する ISP によって管理された RP に依存して顧客にサービスを提供することを望んでいませんでした。 MSDP により、各 ISP は独自のローカル RP を持ちながら、インターネットに対してマルチキャスト トラフィックを送受信できます。

エニーキャスト RP

エニーキャスト RP は、MSDP の有益な応用です。 本来、MSDP は、ドメイン間マルチキャスト アプリケーション用に開発されたものですが、冗長性および負荷分散機能を提供するドメイン間機能としてエニーキャスト RP にも使用されます。 エンタープライズ カスタマーは、通常、単一のマルチキャスト ドメイン内の耐障害性要件を満たすために、エニーキャスト RP を使用して Protocol Independent Multicast スパース モード（PIM-SM）ネットワークを設定します。

エニーキャスト RP では、ループバック インターフェイス上で同じ IP アドレスを使用して複数の RP を設定します。 エニーキャスト RP ループバック アドレスは、32 ビット マスクを使用して設定し、ホストアドレスにする必要があります。 すべてのダウンストリーム ルータは、このエニーキャスト RP ループバック アドレスがローカル RP の IP アドレスであることを認識するように設定する必要があります。 IP ルーティングでは、トポロジ的に最も近い RP が各ソースおよびレシーバに自動的に選択されます。 ソースはネットワークの周囲に等間隔に配置されていると仮定すると、各 RP には同数のソースが登録されます。 つまり、ソースを登録するプロセスは、ネットワーク内のすべての RP によって均等に共有されます。

ソースは 1 つの RP に登録でき、レシーバは異なる RP に加入できるため、RP にはアクティブなソースに関する情報を交換するための手段が必要です。 この情報の交換は、MSDP を使用して行われます。

エニーキャスト RP では、すべての RP が互いに MSDP ピアになるように設定されます。 ソースが 1 つの RP に登録すると、特定のマルチキャスト グループにアクティブなソースが存在することを通知する SA メッセージが他の RP に送信されます。 その結果、各 RP は、他の RP のエリア内に存在するアクティブなソースを認識します。 いずれかの RP で障害が発生すると、IP ルーティングが収束し、他の RP のいずれかが複数のエリアのアクティブ RP になります。 新しいソースは、バックアップ RP に登録します。 レシーバはこれらの新しい RP に加入し、接続が維持されます。

（注） RP は、通常、ソースおよびレシーバとの新しいセッションを開始するためだけに必要になります。 RP は、ソースとレシーバがマルチキャスト データ フローを直接確立できるように、共有ツリーを支援します。 すでにソースとレシーバの間にマルチキャスト データ フローが確立されている場合、そのセッションは RP 障害による影響を受けません。 エニーキャスト RP を使用すると、いつでもソースおよびレシーバとの新しいセッションを開始できます。

マルチキャスト転送

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

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

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

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

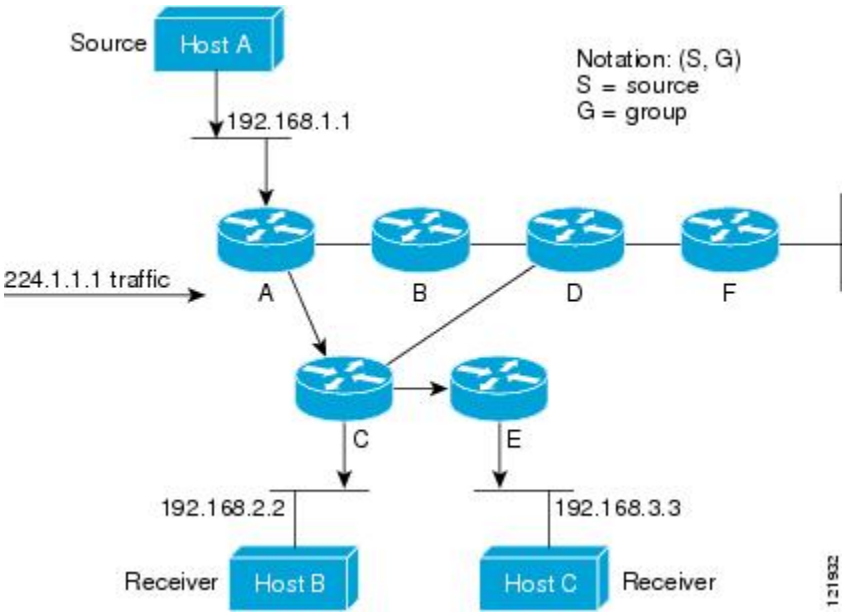
(S, G) という表記（「S カンマ G」と読みます）は、最短パス ツリーの列挙です。S はソースの IP アドレス、G はマルチキャスト グループ アドレスを表します。

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

マルチキャスト配信のソース ツリー

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

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



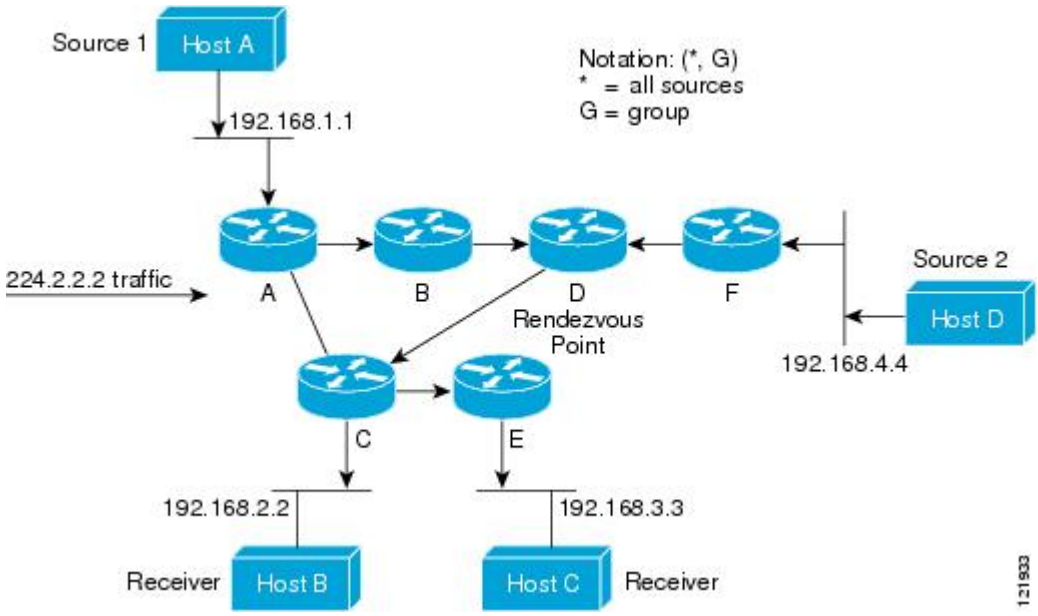
標準表記を使用すると、図の例の SPT は（192.168.1.1, 224.1.1.1）となります。

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

マルチキャスト配信の共有ツリー

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

マルチキャスト配信の共有ツリー に、ルータ D にルートが配置されたグループ 224.2.2.2 の共有ツリーを示します。この共有ツリーは一方向です。ソース トラフィックは、ソース ツリー上の RP に向けて送信されます。このトラフィックは、次に RP から共有ツリーを下方向に転送され、すべてのレシーバに到達します（レシーバがソースと RP の間に配置されていない場合は、直接サービスが提供されます）。



この例では、ソース（ホスト A およびホスト D）からのマルチキャスト トラフィックは、ルート（ルータ D）に送信された後、共有ツリーを下方向に転送され、2 つのレシーバ（ホスト B およびホスト C）に到達します。 マルチキャスト グループ内のすべてのソースが同じ共有ツリーを使用するため、このツリーは、（*, G）というワイルドカード表記（「スター カンマ G」と読みます）を使用して表されます。 この場合、* はすべてのソースを意味し、G はマルチキャスト グループを表します。 したがって、マルチキャスト配信の共有ツリーの共有ツリーは（*, 224.2.2.2）と表記します。

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

ソース ツリーの利点

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

共有ツリーの利点

共有ツリーには、各ルータにおいて要求されるステートの量が最小限に抑えられるという利点があります。 この利点により、共有ツリーだけが許容されるネットワークの全体的なメモリ要件が緩和されます。 共有ツリーの欠点は、特定の状況でソースとレシーバの間のパスが最適パスではなくなり、パケット配信に遅延を生じる可能性があることです。 たとえば、上の図の場合、ホスト A（ソース 1）とホスト B（レシーバ）の間の最短パスは、ルータ A およびルータ C であると考えられます。 ここでは、ルータ D を共有ツリーのルートとして使用しているため、トラフィックは、ルータ A、ルータ B、ルータ D、ルータ C の順に通過する必要があります。 共有ツリーだけの環境を実装する場合、ネットワーク設計者は、Rendezvous Point（RP）の配置を慎重に検討する必要があります。

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

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

リバース パス転送

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

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

Protocol Independent Multicast（PIM）は、ユニキャスト ルーティング情報を使用して、レシーバからソースへ向かうリバース パスに沿って配信ツリーを作成します。 その後、マルチキャスト ルー

タは、その配信ツリーに沿ってソースからレシーバにパケットを転送します。 RPF は、マルチキャスト転送における重要な概念です。 RPF により、ルータは、配信ツリーの下方向へ正しくマルチキャスト トラフィックを転送できます。 RPF は、既存のユニキャスト ルーティング テーブルを使用して、アップストリーム ネイバーとダウンストリーム ネイバーを決定します。 ルータは、アップストリームインターフェイスで受信した場合にのみ、マルチキャストパケットを転送します。 この RPF チェックにより、配信ツリーがループフリーであることを保証できます。

RPF チェック

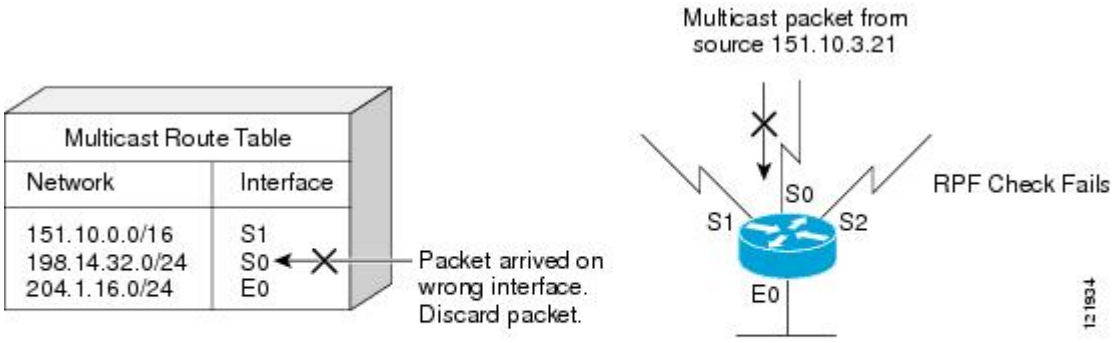
マルチキャストパケットがルータに到達すると、ルータはそのパケットに対してRPFチェックを実行します。 RPFチェックが成功すると、パケットが転送されます。 そうでない場合、パケットはドロップされます。

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

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

図に、RPF チェックの失敗例を示します。

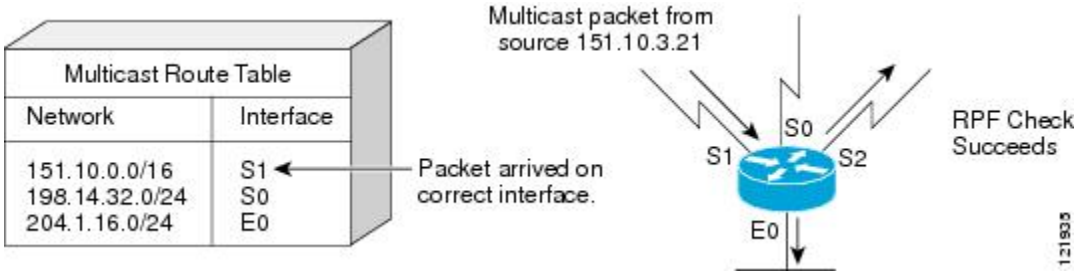
図 *2*：*RPF* チェックの失敗



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

図に、RPF チェックの成功例を示します。

図 *3*：*RPF* チェックの成功



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

PIM デンス モード フォールバック

ミッション クリティカルなネットワークで IP マルチキャストを使用する場合は、PIM-DM（デンス モード）の使用を回避する必要があります。

デンス モード フォール バックとは、（RP が必要になる）スパース モードから（RP を使用しない）デンス モードに PIM モードを変更（フォールバック）するイベントです。 デンス モード フォールバックは、RP 情報が失われると発生します。

スパース モード用に設定されたインターフェイス上ではデンス モード グループを作成できないため、**ip pim sparse-mode** コマンドを使用してすべてのインターフェイスを設定している場合はデンス モード フォールバックは発生しません。

デンス モード フォールバックの原因と結果

PIM は、マルチキャスト グループが PIM-DM モードで動作するか、PIM-SM モードで動作するかを、グループから RP へのマッピング キャッシュ内の RP 情報の存在だけに基づいて決定します。Auto-RP を設定している場合やブートストラップ ルータ（BSR）を使用して RP 情報を配信する場合には、ネットワークの輻輳が原因ですべての RP、Auto-RP、またはグループの BSR に障害が発生すると RP 情報が失われる可能性があります。 この障害により、ネットワークの一部または全部が PIM-DM にフォールバックすることがあります。

ネットワークが PIM-DM にフォールバックした場合、AutoRP または BSR が使用されているときは、デンス モード フラッディングが発生します。 RP 情報が失われたルータがデンス モードにフォールバックし、障害が発生したグループに対して作成される必要がある新しいステートがデンス モードで作成されます。

デンス モード フォールバックを回避することによる効果

PIM-DM フォールバックを回避するまでは、グループから RP へのマッピングを使用しないすべてのマルチキャスト グループはデンス モードで処理されます。

PIM-DM フォールバックを回避すると、デンス モード フラッディングを回避するように PIM-DM フォールバック動作が変更されます。 デフォルトでは、（**ip pim sparse-mode** コマンドを使用して）すべてのインターフェイスが PIM スパース モードで動作するように設定する場合は、**no ip pim dm-fallback** コマンドを設定する必要はありません（つまり、PIM-DM フォールバック動作がデフォルトでイネーブルになります）。 **ip pim sparse-mode** コマンド（たとえば、**ip pim sparse-dense-mode** コマンド）を使用して設定したインターフェイスがない場合は、**no ip pim dm-fallback** コマンドを使用して PIM-DM フォールバック動作を明示的にディセーブルにできます。

no ip pim dm-fallback コマンドを設定している場合、またはすべてのインターフェイス上で **ip pim sparse-mode** を設定している場合、スパース モードで実行されている既存のグループは引き続きスパース モードで動作しますが、0.0.0.0 に設定された RP を使用します。 RP アドレスが 0.0.0.0 に設定されたマルチキャスト エントリは、次のように動作します。

- 既存の (S, G) ステートを維持します。
- (*, G) または (S, G, RPbit) の PIM 加入またはプルーニング メッセージは送信しません。
- 受信した (*, G) または (S, G, RPbit) 加入またはプルーニング メッセージは無視します。
- 登録は送信せず、ファースト ホップのトラフィックはドロップします。
- 受信した登録には、登録停止で応答します。
- 資産は変更しません。
- (*, G) 発信インターフェイス リスト（olist）は、インターネット グループ管理プロトコル（IGMP）ステートに対してのみ維持します。
- RP 0.0.0.0 グループに対する Multicast Source Discovery Protocol（MSDP）Source-Active（SA）メッセージは、引き続き受信して転送します。

PIM モードの選択に関するガイドライン

設定プロセスを開始する前に、どの PIM モードを使用する必要があるかを決定する必要があります。 この決定は、ネットワーク上でサポートするアプリケーションによって異なります。

基本的なガイドラインには次のものが含まれます。

- 一般に、本質的な 1 対多または多対多アプリケーションでは PIM-SM を正常に使用できます。
- 1 対多アプリケーションで最適なパフォーマンスを得るには、SSM が適しています。ただし、IGMP バージョン 3 サポートが必要です。
- 多対多アプリケーションで最適なパフォーマンスを得るには、双方向 PIM が適しています。ただし、ハードウェア サポートは、シスコ デバイスおよび Sup720 を搭載した Catalyst 6000 シリーズ スイッチに制限されます。

次の作業

- 基本 IP マルチキャストの設定については、「基本的な IP マルチキャスト設定」モジュールを参照してください。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『*Cisco IOS IP Multicast Command Reference*』

標準

標準	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
CISCO-PIM-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2934	『*Protocol Independent Multicast MIB for IPv4*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP マルチキャスト テクノロジーの機能情報の概要

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *2* : *IP* マルチキャスト テクノロジーの機能情報の概要

機能名	リリース	機能の設定情報
ネットワークにおける RP 情報損失後の PIM デンス モード フォールバック回避	12.3(4)T	ネットワークにおける RP 情報損失後の PIM デンス モード フォールバック回避機能は、すべての RP で障害が発生したときに PIM-DM のフォールバックを回避できるようにします。信頼性が重大な意味を持つマルチキャストネットワークにとって、デンス モードの使用を回避することは非常に重要です。この機能は、スパース モードでマルチキャスト グループを保持するためのメカニズムを提供し、それによってデンスモード フラッディングを回避します。

用語集

基本マルチキャスト：インタラクティブなドメイン内マルチキャスト。 企業キャンパス内でマルチキャストアプリケーションをサポートします。 信頼性の高いマルチキャスト転送である Pragmatic General Multicast（PGM）を含めることにより、ネットワークに追加の完全性を提供できます。

bidir PIM：双方向 PIM は、双方向のデータ フローを提供する共有スパース ツリーを実装するプロトコルの PIM スイートに対する拡張機能です。 PIM-SM とは対照的に、Bidir-PIM ではソース固有のステートをルータに保持することを回避できるため、ツリーを拡張して任意の数のソースに対応できます。

ブロードキャスト：ノードが受信することを求めているかどうかに関係なく、すべてのノードに対してメッセージのコピーを 1 つ送信する 1 対全の通信。

Cisco グループ管理プロトコル（CGMP）：レイヤ 2 スイッチが Cisco ルータ上の IGMP 情報を利用してレイヤ 2 転送の決定を行うことを可能にする、シスコによって開発されたプロトコル。 これにより、スイッチは、トラフィックを必要としているポートだけにマルチキャスト トラフィックを転送できます。

デンス モード（DM）（インターネット ドラフト仕様）：すべての潜在的なレシーバに対してマルチキャスト データの送信をアクティブに試行し（フラッディング）、セルフプルーニング（グループからの削除）に依存して目的の配信を行います。

指定ルータ（DR）：IGMP ホストから受信した IGMP メンバーシップ情報に応えて、加入/プルーニング メッセージのカスケードをアップストリームの RP にルーティングする、PIM-SM ツリー上のルータ。

配信ツリー：マルチキャスト トラフィックは、すべてのソースをグループ内のすべてのレシーバに接続する配信ツリー上で、ソースからマルチキャスト グループに流れます。 このツリーをすべてのソース（共有ツリー）で共有したり、ソース（ソース ツリー）ごとに個別の配信ツリーを構築したりできます。 共有ツリーは一方向または双方向です。

IGMP メッセージ：IGMP メッセージは、IP プロトコル番号 2 および IP ルータ アラート オプション（RFC 2113）を使用して標準 IP データグラムにカプセル化されます。

IGMP スヌーピング：IGMP スヌーピングは、LAN スイッチに対して、ホストからルータに送信された IGMP パケットに含まれるレイヤ 3 情報を検査（「スヌーピング」）することを要求します。 特定のマルチキャスト グループのホストからの IGMP レポートをヒアリングすると、スイッチは、そのホストのポート番号を関連するマルチキャスト テーブル エントリに追加します。 ホストからの IGMP グループ脱退メッセージをヒアリングすると、スイッチは、そのホストのポートをテーブル エントリから削除します。

IGMP 単方向リンク ルーティング（UDLR）：シスコの他の UDLR ソリューションでは、IP マルチキャスト ルーティングを、UDLR に対応するように強化された IGMP と組み合わせて使用します。 このソリューションは、多くの衛星リンクに対する優れた拡張性を備えています。

インターネット グループ管理プロトコル（IGMP）v2：IP ルータおよびそれらに直接接続されたホストがマルチキャスト グループ メンバーシップ ステートをやりとりするために使用します。

インターネット グループ管理プロトコル（IGMP）v3：IGMP は、隣接するマルチキャスト ルータに IP マルチキャスト グループ メンバーシップを報告するために IPv4 システムが使用するプロトコルです。 IGMP バージョン 3 では、「ソース フィルタリング」のサポートが追加されています。これは、特定のマルチキャストアドレスに送信された特定のソースアドレスからのみ（または、特定のソース アドレスを除くすべてのアドレスから）パケットを受信するかどうかを報告するためのシステム機能です。

マルチキャスト：IP トラフィックを 1 つのソースまたは複数のソースから送信し、複数の宛先に配信できるルーティング手法。 各宛先に、個々のパケットを送信する代わりに、マルチキャスト グループと呼ばれる宛先のグループに 1 つのパケットが送信されます。このグループは 1 つの IP 宛先グループ アドレスで識別されます。 マルチキャスト アドレッシングは、複数ホストへの 1 つの IP データグラムの転送をサポートします。

Multicast Routing Monitor（MRM）：大規模マルチキャスト ルーティング インフラストラクチャにおいてネットワーク障害検出および分離機能を提供する管理診断ツール。マルチキャスト ルーティングの問題をほぼリアルタイムでネットワーク管理者に通知するように設計されています。

Multicast Source Discovery Protocol（MSDP）：複数の PIM スパース モード（PIM-SM）ドメインを接続するためのメカニズム。 MSDP により、異なるドメインのすべての Rendezvous Point（RP）がマルチキャスト グループのソースを認識できます。 各 PIM-SM ドメインは自身の RP を使用するため、他のドメインの RP に依存する必要はありません。 RP は、MSDP を TCP 上で実行して他のドメインのマルチキャスト ソースを検出します。 MSDP は、グループを送信する送信元のアナウンスにも使用されます。 これらのアナウンスは、ドメイン RP で発信する必要があります。 MSDP は、ドメイン間の動作に関して Multicast BGP（マルチキャスト BGP）に大きく依存しています。

Protocol Independent Multicast（PIM）：既存の IP ネットワークでの IP マルチキャスト ルーティングを可能にする、IETF によって規定されたマルチキャスト ルーティング アーキテクチャ。 OSPF や BGP などの基礎となるユニキャスト プロトコルから独立している点が重要です。

プルーニング：マルチキャスト対応ルータが適切なマルチキャスト メッセージを送信して、特定のマルチキャスト グループのマルチキャスト ツリーから自身を削除することを意味するマルチキャスト ルーティング用語。 そのグループにアドレス指定されたマルチキャスト データの受信を停止するため、グループに再加入するまで、接続先のホストにデータを配信できません。

クエリー：接続先のホストからマルチキャスト グループ メンバーシップ情報を引き出すためにルータから送信される IGMP メッセージ。

ランデブー ポイント（RP）：PIM-SM 共有マルチキャスト配信ツリーのルートとなるマルチキャスト ルータ。

レポート：マルチキャスト グループにおいてメンバーシップの加入、維持、または脱退を行うホストから送信される IGMP メッセージ。

ソース ツリー：ソースとレシーバの指定ルータ（またはランデブー ポイント）を直接接続し、ネットワークの最短パスを取得するマルチキャスト配信パス。 ソースとレシーバの間で最も効率的にデータをルーティングできますが、RP 以外のデバイスで構築されると、ネットワーク全体で不要なデータ重複が発生する可能性があります。

スパース モード（SM）（RFC 2362）：マルチキャスト グループのレシーバへのマルチキャスト データの送信を試行するまで、明示的な加入方式に依存します。

UDLR トンネル：バック チャネル（別のリンク）を使用して、ルーティング プロトコルが一方向のリンクを双方向として認識するようにします。バック チャネル自体は、特殊な単方向総称ルーティング カプセル化（GRE）トンネルであり、これによってユーザ データ フローの反対方向のトラフィック フローを制御します。 この機能により、IP および関連するユニキャスト/マルチキャスト ルーティング プロトコルは、単方向リンクを論理的な双方向リンクとして認識できます。 このソリューションでは、プロトコルを変更せずに、すべての IP ユニキャストおよびマルチキャスト ルーティング プロトコルに対応できます。 ただし、拡張性がないため、20 を超えるトンネルをアップストリーム ルータにフィードできません。 単方向 GRE トンネルの目的は、制御パケットをダウンストリーム ノードからアップストリーム ノードに移動することです。

ユニキャスト：各要求者に個別にメッセージのコピーを送信するようにソースに要求するポイントツーポイント送信。

単方向リンク ルーティング プロトコル（UDLR）：物理的な単方向インターフェイス（広帯域幅の衛星リンクなど）上で、バック チャネルを持つスタブ ネットワークにマルチキャスト パケットを転送するための手段を提供するルーティング プロトコル。

URL Rendezvous Directory（URD）：URD は、コンテンツ ストリームの特定のソースに関する情報をネットワークに直接提供する Multicast-Lite ソリューションです。 これにより、ネットワークは、ソースからレシーバへの最も直接的な配信パスをすばやく確立できるため、ストリーミング メディアの受信に必要な時間と労力が大幅に削減されます。 URD により、アプリケーションは、Web ページ リンクまたは Web を介してコンテンツ ストリームのソースを直接識別できます。 この情報は、アプリケーションに戻された後、URD を使用して再びネットワークに伝送されます。

この機能では、URD 対応の Web ページは、Web ページ上のソース、グループ、およびアプリケーションに関する情報を（media-type 経由で）提供します。 関心のあるホストは、Web ページをク

リックして HTTP トランザクション内の情報をプルします。 レシーバへのラスト ホップ ルータは、このトランザクションを代行受信し、IANA によって割り当てられた特別なポートに送信します。 ラスト ホップ ルータも URD に対応し、この情報を使用して、PIM ソースであるグループ (S, G) 加入をホストに代わって開始します。

第 2 章

基本的な IP マルチキャスト設定

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

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

基本的な IP マルチキャスト設定の前提条件

- このモジュールに含まれているどの作業を実行する必要があるかを判断するには、使用する Protocol Independent Multicast（PIM）モードを決定する必要があります。 この決定は、ネットワーク上でサポートするアプリケーションによって異なります。
- このモジュールの作業で使用するアクセス リストはすべて、設定作業を開始する前に設定しておく必要があります。 アクセス リストの設定方法については、『*Security Configuration Guide: Access Control Lists*』の「Creating an IP Access List and Applying It to an Interface」モジュールを参照してください。

基本的な IP マルチキャスト設定に関する情報

Auto-RP の概要

PIM ネットワークでの AutoRP の役割

AutoRP は、PIM ネットワークにおけるグループからランデブー ポイント（RP）へのマッピングの配信を自動化します。 AutoRP が機能するためには、RP アナウンスメント メッセージを RP から受信して競合を解決する RP マッピング エージェントとしてデバイスが指定されている必要があります。 その後、RP マッピング エージェントは、デンス モード フラッディングにより、グループから RP への一貫したマッピングを他のすべてのデバイスに送信するようになります。

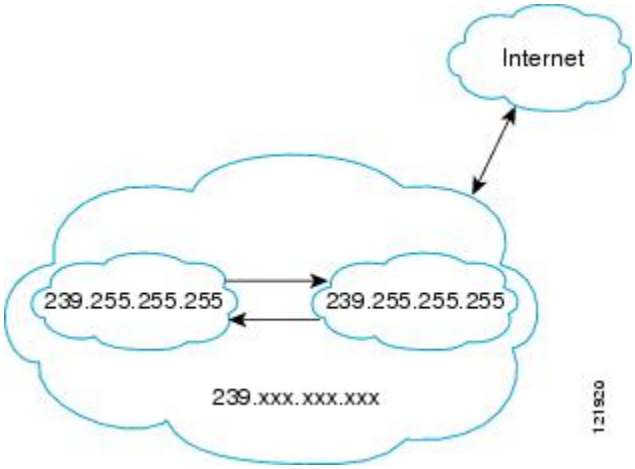
これにより、すべてのルータは、サポート対象のグループに使用する RP を自動的に検出します。インターネット割り当て番号局（IANA）は、224.0.1.39 と 224.0.1.40 という 2 つのグループ アドレスを AutoRP 用に割り当てています。

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

IP マルチキャスト境界

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

図 *4*：境界でのアドレス スコーピング



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

インターネット割り当て番号局（IANA）は、マルチキャスト アドレス範囲 239.0.0.0 ～ 239.255.255.255 を管理用スコープのアドレスとして指定しました。 この範囲のアドレスは、さまざまな組織で管理されるドメイン内で再使用されます。 これらは、グローバルに一意ではなくローカルとみなされます。

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

PIM ネットワークでの Auto-RP の利点

- Auto-RP では、指定した RP に対するすべての変更は、RP であるデバイス上で設定することができ、リーフ ルータ上で設定する必要がありません。
- Auto-RP では、ドメイン内で RP アドレスをスコーピングできます。

エニーキャスト RP の概要

エニーキャスト RP は、MSDP の有益な応用です。 本来、MSDP は、ドメイン間マルチキャスト アプリケーション用に開発されたものですが、冗長性および負荷分散機能を提供するドメイン間機能としてエニーキャスト RP にも使用されます。 エンタープライズ カスタマーは、通常、単一のマルチキャスト ドメイン内の耐障害性要件を満たすために、エニーキャスト RP を使用して Protocol Independent Multicast スパース モード（PIM-SM）ネットワークを設定します。

エニーキャスト RP では、ループバック インターフェイス上で同じ IP アドレスを使用して複数の RP を設定します。 エニーキャスト RP ループバック アドレスは、32 ビット マスクを使用して設定し、ホストアドレスにする必要があります。すべてのダウンストリームルータは、このエニーキャスト RP ループバック アドレスがローカル RP の IP アドレスであるように設定する必要があります。 IP ルーティングでは、トポロジ的に最も近い RP が各ソースおよびレシーバに自動的に選択されます。 ソースはネットワークの周囲に等間隔に配置されていると仮定すると、各 RP には同数のソースが登録されます。 つまり、ソースを登録するプロセスは、ネットワーク内のすべての RP によって均等に共有されます。

ソースは 1 つの RP に登録でき、レシーバは異なる RP に加入できるため、RP にはアクティブなソースに関する情報を交換するための手段が必要です。 この情報の交換は、MSDP を使用して行われます。

エニーキャスト RP では、すべての RP が互いに MSDP ピアになるように設定されます。 ソースが 1 つの RP に登録すると、特定のマルチキャスト グループにアクティブなソースが存在することを通知する SA メッセージが他の RP に送信されます。 その結果、各 RP は、他の RP のエリア内に存在するアクティブなソースを認識します。いずれかの RP で障害が発生すると、IP ルーティングが収束し、他の RP のいずれかが複数のエリアのアクティブ RP になります。 新しいソースは、バックアップ RP に登録します。 レシーバはこれらの新しい RP に加入し、接続が維持されます。

RP は、通常、ソースおよびレシーバとの新しいセッションを開始するためだけに必要になります。 RP は、ソースとレシーバが直接マルチキャスト データ フローを確立できるように、共有ツリーを支援します。 すでにソースとレシーバの間にマルチキャスト データ フローが確立されている場合、そのセッションは RP 障害による影響を受けません。 エニーキャスト RP を使用すると、いつでもソースおよびレシーバとの新しいセッションを開始できます。

BSR の概要

BSR の選定と機能

PIM は BSR を使用して各グループ プレフィックスの RP 設定情報を検出し、PIM ドメイン内のすべてのルータにアナウンスします。 これは、Auto-RP によって行われるのと同じ機能ですが、BSR は PIM バージョン 2 仕様の一部です。 BSR メカニズムは、Cisco ルータ上の Auto-RP と相互運用します。

シングル ポイント障害を回避するために、1 つの PIM ドメインに複数の候補 BSR を設定できます。 BSR は候補 BSR の中から自動的に選定されます。これらはブートストラップ メッセージを使用して、最も優先度の高い BSR を検出します。 その後、このルータが BSR であると PIM ドメイン内のすべての PIM ルータに通知します。

BSR の選定の後、候補 RP はユニキャストを使用して RP になりたいという要求を BSR に通知します。 BSR は、グループと RP のマッピングセット全体をルータ リンク ローカル アドレス 224.0.0.13 にアドバタイズします。 RP を選択するために Auto-RP によって使用される Auto-RP の RP マッピング エージェントとは異なり、BSR ネットワークのすべてのルータが、RP の選択を行います。

BSR には RP アドバタイズメントをスコーピングする機能が欠けていますが、BSR はベンダー相互運用性またはオープン スタンダードの遵守が必要な場合に使用されます。

BSR 境界インターフェイス

PIM スパース モードのドメインの境界インターフェイスには、特にそのインターフェイスによって到達可能な隣接ドメインも PIM スパース モードを実行している場合、そのドメインとの特定のトラフィックのやりとりを阻止する防止策が必要です。 一方のドメインにあるルータは他方のドメインにある RP を選択し、その結果ドメイン間でプロトコルが誤動作したり分離が行われない可能性があるため、BSR および Auto-RP メッセージを異なるドメイン間で交換しないでください。インターフェイスでの BSR メッセージの送受信を防ぐために BSR 境界インターフェイスを設定します。

スタティック RP の概要

PIM スパース モードを設定している場合、マルチキャスト グループに PIM RP を設定する必要があります。 RP は各デバイスで静的に設定するか、ダイナミック メカニズムによって学習できます。 この作業は、Auto-RP のようにダイナミック メカニズムによってルータが RP を学習するのではなく、RP を静的に設定する方法を説明しています。

PIM 指定ルータ（DR）は共有ツリーに分散するために、直接接続されたマルチキャスト ソースから RP にデータを転送します。 データは次の 2 つの方法のいずれかを使用して RP に転送されます。 データは登録パケットにカプセル化され、直接 RP にユニキャストされます。または、RP がソース ツリーに参加している場合は、RPF 転送アルゴリズムによってマルチキャスト転送されます。 レシーバに直接接続されたラスト ホップ ルータは、それぞれの判断でソース ツリーに参加し、共有ツリーから自身をプルーニングできます。

アクセス リストによって定義された複数のグループに単一の RP を設定できます。 グループに RP が設定されていない場合、ルータは PIM デンス モード技術を使用してグループをデンスとして処理します（**no ip pim dm-fallback** コマンドを設定するとこれを防げます）。

ダイナミックとスタティックのグループと RP のマッピングが共に使用され、RP アドレスが競合している場合、スタティックのグループと RP のマッピングに設定された RP アドレスが（**ip pim rp-address override** コマンドによって）優先されます。

（注） **override** キーワードが指定されておらず、RP アドレスが競合している場合、ダイナミックのグループと RP のマッピングがスタティックのグループと RP のマッピングに優先されます。

SSM の概要

Source Specific Multicast（SSM）。 SSM は、レシーバが明示的に参加したマルチキャスト ソースからのみデータグラム トラフィックがレシーバに転送されるIPマルチキャストの拡張機能です。SSM 用に設定されたマルチキャスト グループは、（共有ツリーではなく）ソース固有のマルチキャスト配信ツリーのみが作成されます。

SSM のコンポーネント

Source Specific Multicast（SSM）は、ブロードキャスト アプリケーションとしても知られる 1 対多アプリケーションをサポートする最善のデータグラム配信モデルです。 SSMは、オーディオおよびビデオ ブロードキャスト アプリケーション環境を対象とした IP マルチキャスト ソリューションの Cisco 実装のコア ネットワーキング テクノロジーで、RFC 3569 に説明されています。 次の 2 つのコンポーネントは共に SSM の実装をサポートします。

- Protocol Independent Multicast Source-Specific Mode（PIM-SSM）
- インターネット グループ管理プロトコル バージョン 3（IGMPv3）

Protocol Independent Multicast（PIM）SSM（PIM-SSM）は、SSM の実装をサポートするルーティング プロトコルで、PIM スパース モード（PIM-SM）から派生しました。 IGMP は、ホストがルータにマルチキャスト グループ メンバーシップを伝えるために使用するインターネット技術特別調査委員会（IETF）標準トラック プロトコルです。 IGMP バージョン 3 は、SSM に必要なソース フィルタリングをサポートします。 SSM を IGMPv3 と共に実行するには、SSM がデバイス、アプリケーションが実行されるホスト、およびアプリケーション自体でサポートされる必要があります。

Internet Standard Multicast と SSM の違い

インターネットと多くの企業イントラネットの標準IPマルチキャストインフラストラクチャは、PIM-SM プロトコルと Multicast Source Discovery Protocol（MSDP）に基づいています。 これらのプロトコルは信頼でき、広範で、効率的であることが証明されています。 しかし、インターネット標準マルチキャスト（ISM）サービス モデルの複雑さと機能性の制限があります。 たとえば、ISM では、ネットワークは、実際にマルチキャスト トラフィックを送信しているホストについての情報を維持する必要があります。 SSM では、この情報は IGMPv3 によってラスト ホップ デバイスにリレーされるソース アドレスを通してレシーバによって提供されます。 SSM は、ISM に関連付けられた問題への対応を強化し、ネットワーク内で ISM 用に開発されたプロトコルと共存することを目的としています。 一般に、SSM は SSM を使用するアプリケーションに IP マルチキャスト サービスを提供します。

ISM サービスについては RFC 1112 で説明されています。 このサービスは、任意のソースからマルチキャスト ホスト グループと呼ばれるレシーバのグループへの IP データグラムの配信によって構成されています。 マルチキャスト ホスト グループのデータグラム トラフィックは、任意の IP ユニキャスト送信元アドレス S と IP 宛先アドレスとしてのマルチキャスト グループ アドレス G のデータグラムで構成されます。 システムはホスト グループのメンバになることによってこのトラフィックを受信します。 ホスト グループのメンバーシップには IGMP バージョン 1、2、または 3 によるホスト グループのシグナリングが必要です。

SSM では、データグラムは（S, G）チャネルに基づいて配信されます。 1 つの (S, G) チャネルのトラフィックは、IP 宛先アドレスとして IP ユニキャスト ソース アドレス S とマルチキャスト グループ アドレス G を持つデータグラムで構成されています。 システムは、（S, G）チャネルのメンバになることによって、このトラフィックを受信します。 SSM と ISM のどちらでも、ソースになるためにシグナリングは必要ありません。ただし、SSM では、レシーバーは特定の送信元からのトラフィックの受信または非受信を決めるために（S, G）への加入または脱退を行う必要があります。 つまり、レシーバーは加入した（S, G）チャネルからだけトラフィックを受信できます。一方、ISM では、レシーバーは受信するトラフィックの送信元の IP アドレスを知る必要はありません。 提案されているチャネル加入シグナリングの標準的な方法では、IGMP INCLUDE モード メンバーシップ レポートを使用します。これは、IGMP バージョン 3 でのみサポートされています。

IP マルチキャスト グループ アドレス範囲の設定済みのサブセットに SSM 配信モデルを適用することにより、SSM と ISM サービスを一緒に使用できます。インターネット割り当て番号局（IANA）は、SSM アプリケーションおよびプロトコル用に 232.0.0.0 ～ 232.255.255.255 のアドレス範囲を確保しています。 ソフトウェアでは、224.0.0.0 ～ 239.255.255.255 の IP マルチキャスト アドレス範囲の任意のサブセットの SSM 設定を許可します。 SSM 範囲が定義されると、（アプリケーションが明示的な（S, G）チャネル加入を使用するように変更されているか、URL Rendezvous Directory（URD）によって SSM に対応していない限り）SSM 範囲内でアドレスを使用しようとする場合に既存の IP マルチキャスト レシーバ アプリケーションはトラフィックを受信しません。

SSM の動作

確立されているネットワークは、IP マルチキャスト サービスが PIM SM に基づいているので、SSM サービスをサポートできます。 SSM は、ドメイン間の PIM-SM に必要なプロトコルがすべて揃っていないネットワークで単独で配備することもできます。 つまり、SSM には RP が必要ではないため、Auto-RP、MSDP、ブートストラップ ルータ（BSR）などの RP メカニズムは必要ありません。

SSM がすでに PIM-SM 用に設定済みのネットワークで配備されている場合、ラスト ホップ デバイスのみを、SSM をサポートするソフトウェア イメージにアップグレードする必要があります。 レシーバに直接接続されていないルータを SSM をサポートするソフトウェア イメージにアップグレードする必要はありません。 一般的に、これらのラスト ホップではないデバイスは、SSM 範囲で PIM-SM のみを実行する必要があります。 これらは、MSDP シグナリング、登録、または PIM-SM 共有ツリー動作が SSM 範囲内で発生することを抑制するために、追加のアクセス コントロール設定を必要とする場合もあります。

SSM モードの動作は、**ip pim ssm** グローバル コンフィギュレーション コマンドを使用して SSM 範囲を設定することによってイネーブルにできます。 この設定による影響は次のとおりです。

- SSM 範囲内のグループの場合、(S, G) チャネル加入は IGMPv3 INCLUDE モード メンバーシップ レポートによって受け入れられます。
- SSM 範囲のアドレスの PIM 動作は、PIM-SM の派生モードである PIM-SSM に変更されます。このモードでは、PIM（S, G）加入およびプルーニング メッセージのみがデバイスによって生成されます。 ランデブー ポイント ツリー（RPT）動作に関連した着信メッセージは無視されるか、拒否され、着信 PIM 登録メッセージは登録停止メッセージによってただちに応答されます。 ラストホップ デバイス以外のデバイスでは、PIM-SSM は PIM-SM と下位互換性を保ちます。 したがって、ラストホップ デバイス以外のデバイスは SSM グループに PIM-SM を使用できます（SSM をサポートしていない場合など）。
- SSM 範囲内のグループの場合、SSM 範囲内の MSDP Source-Active（SA）メッセージは受け入れ、生成、または転送されません。

IGMPv3 ホスト シグナリング

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

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

Source Specific Multicast の利点

IP マルチキャスト アドレス管理が不要

ISM サービスで、トラフィック ディストリビューションは使用する IP マルチキャスト グループ アドレスにのみ基づくため、アプリケーションは一意の IP マルチキャスト グループ アドレスを取得する必要があります。 異なるソースとレシーバを持つ 2 つのアプリケーションが同じ IP マルチキャスト グループ アドレスを使用すると、両方のアプリケーションのレシーバが両方のアプリケーションのソースからトラフィックを受信します。 適切にプログラムしている場合、レシーバは不要なトラフィックをフィルタできますが、この状態は一般的に許容できないレベルの不要なトラフィックを生み出します。

アプリケーションへの一意の IP マルチキャスト グループ アドレスの割り当ては問題となります。最も短期のアプリケーションはセッション記述プロトコル（SDP）やセッション通知プロトコル（SAP）のようなメカニズムを使用して、ランダム アドレスを取得します。これは、インターネット内のアプリケーションの増加によってうまく機能しないソリューションです。 長期アプリケーションの現在のベスト ソリューションは、RFC 2770 に説明されていますが、このソリューションは各自律システムが 255 の使用可能な IP マルチキャスト アドレスのみに限定される制限の影響を受けます。

SSM で、他のソースからのトラフィックとは関係なく、各ソースからのトラフィックはネットワーク内のデバイス間で転送されます。 このため、異なるソースが SSM 範囲のマルチキャスト グループ アドレスを再利用できます。

望ましくないソースからのサービス拒否攻撃の阻止

SSM で、個別の各ソースからのマルチキャスト トラフィックは、（IGMPv3、IGMP v3lite、またはURD メンバーシップによって）レシーバから要求された場合にのみネットワーク中に転送されます。 これに対し、ISM はマルチキャスト グループに送信するアクティブなソースからそのマルチキャスト グループを要求するすべてのレシーバにトラフィックを転送します。インターネット ブロードキャスト アプリケーションで、トラフィックを同じマルチキャスト グループにただ送信するだけで、望ましくないソースが実際のインターネット ブロードキャスト ソースを簡単に妨害できるため、この ISM の動作は非常に望ましくありません。 この状況は、レシーバ側で不要なトラフィックによって帯域幅を消耗させるため、インターネット ブロードキャストの無停止の受信を妨害します。 SSM では、トラフィックをマルチキャスト グループにただ送信するだけでは、このような種類の DoS 攻撃は行えません。

インストールと管理が容易

ネットワークがマルチキャスト グループに送信しているアクティブ ソースについての情報を維持する必要がないため、SSM は簡単にインストールし、ネットワークでプロビジョニングできます。 この要件は、（IGMPv1、IGMPv2、または IGMPv3 を使用する）ISM でのみ存在します。

ISM サービスの現在の標準ソリューションは PIM-SM と MSDP です。 PIM-SM（Auto-RP または BSR の必要性を含む）および MSDP での Rendezvous Point（RP）管理は、ネットワークがアクティブ ソースについて学習するためにのみ必要です。 この管理は SSM では必要ありません。このため、SSM は ISM よりインストールや管理が簡単で、配備での動作面の拡張も ISM より簡単です。SSM のインストールが簡単であるその他の要素は、既存の PIM-SM ネットワークを活用でき、ラスト ホップ デバイスをアップグレードするだけで IGMPv3、IGMP v3lite、または URD をサポートできる点です。

インターネット ブロードキャスト アプリケーションに最適

上記の 3 つの利点により、次の理由で SSM はインターネット ブロードキャスト スタイルのアプリケーションに理想的です。

- 一意の IP マルチキャスト アドレスなしで SSM によって、インターネット ブロードキャスト サービスを提供できるため、コンテンツ プロバイダーはサービスを簡単に提供できます（コンテンツ プロバイダーにとって、IP マルチキャスト アドレス割り当てはこれまで深刻な問題でした）。
- インターネット ブロードキャスト サービスは多数のレシーバに公開されることにより、DoS 攻撃の最も一般的な対象となるため、このような攻撃の阻止はインターネット ブロードキャスト サービスの重要な要素です。
- SSM はインストールや動作が簡単なため、特に、コンテンツを複数の独立した PIM ドメイン間で転送する必要のある場合（SSM のために PIM ドメイン間で MSDP を管理する必要がないため）、ネットワーク オペレータにとって理想的です。

Bidir-PIM の概要

Bidir-PIM は最短パス ツリー（SPT）動作の多くを PIM-SM と共有します。 Bidir-PIM にも、共有ツリーのアップストリームにある RP に向けてソース トラフィックを無条件に転送する機能がありますが、PIM-SM のようなソースの登録プロセスはありません。 これらの変更によって、(*, G) マルチキャスト ルーティング エントリのみに基づいてすべてのルータでトラフィックを転送できます。 この転送形式では、ソース固有のステートは不要であり、スケーリング機能を使用して任意の数のソースに対応できます。

マルチキャスト グループ モード

PIM では、マルチキャスト グループのパケット トラフィックは、そのマルチキャスト グループのために設定されたモードのルールに従ってルーティングされます。 PIM の Cisco 実装は、マルチキャスト グループ用に次の 4 つのモードをサポートしています。

- PIM 双方向モード
- PIM デンス モード
- PIM スパース モード
- PIM Source Specific Mode（SSM）

ルータは、異なるマルチキャスト グループに対して、4 つのモードすべて、またはそれらの任意の組み合わせを同時にサポートできます。

双方向共有ツリー

双方向モードでは、トラフィックは、グループのランデブーポイント（RP）をルートとする双方向共有ツリーに沿ってのみ、ルーティングされます。 Bidir-PIM では、RP の IP アドレスは、すべてのルータがその IP アドレスをルートとするループフリーのスパニングツリートポロジを確立するうえで重要な役割を果たします。 この IP アドレスはルータである必要はなく、PIM ドメイン内のどこからでも到達可能なネットワーク上の任意の未割り当て IP アドレスを使用できます。 この技術は、Bidir-PIM の冗長 RP 設定を確立するための優先設定方式です。

双方向グループのメンバーシップは、明示的な加入メッセージによって伝えられます。 ソースからのトラフィックは、無条件で、共有ツリーの上方向にある RP に向けて送信され、ツリーの下方向にある各ブランチ上のレシーバに渡されます。

下の図は、単方向共有ツリーおよびソース ツリーに対する双方向共有ツリーのルータごとの状態の違いを示しています。

図 *5*：単方向共有ツリーおよびソース ツリー

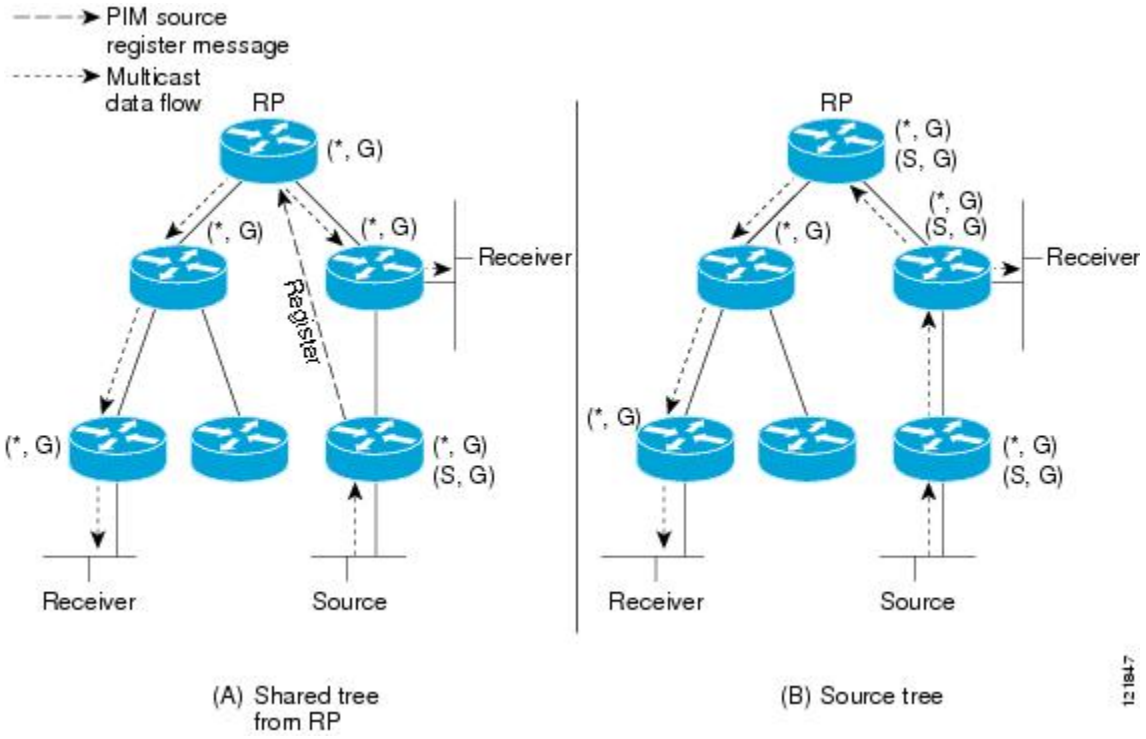
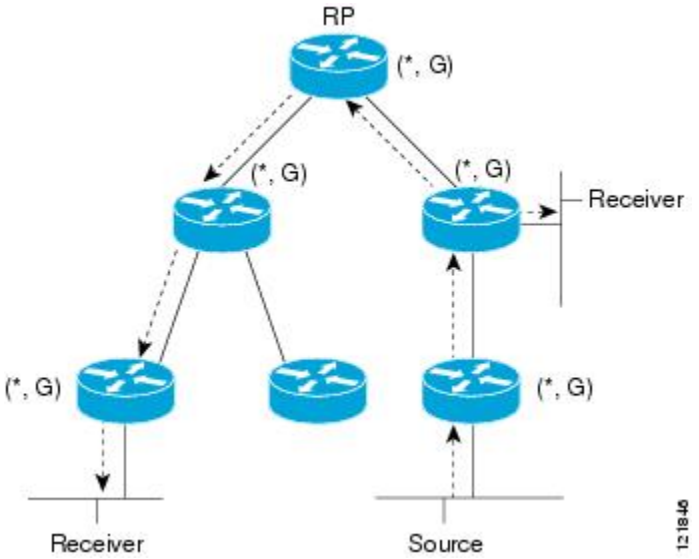


図 *6*：双方向共有ツリー



RP からレシーバ方向へダウンストリームで転送されるパケットの場合、Bidir-PIM と PIM-SM 間の基本的な違いはありません。 ソースからアップストリームで RP 方向に渡されるトラフィックの場合、Bidir-PIM は実質的に PIM-SM から逸脱します。

PIM-SM は、トラフィックを 1 つのリバース パス転送（RPF）インターフェイスからのみ受け入れるため、ツリーのアップストリーム方向にトラフィックを転送できません。 （共有ツリーの）このインターフェイスは RP 方向を指し、そのため、ダウンストリーム トラフィック フローのみを許可します。アップストリーム トラフィックはまずユニキャスト登録メッセージにカプセル化され、これがソースの指定ルータ（DR）から RP に渡されます。 次に、RP がソースをルートとする SPT に参加します。 このため、PIM-SM で RP 方向のソースからのトラフィックは共有ツリーでアップストリームにはフローせず、RP に達するまで、ソースの SPT に沿ってダウンストリームにフローします。 RP から、トラフィックは共有ツリーに沿ってすべてのレシーバに向けてフローします。

Bidir-PIM では、パケット転送ルールが PIM-SM から改善され、トラフィックを共有ツリーで RP 方向にアップストリームに渡せるようになりました。 マルチキャスト パケット ルーピングを避けるために、Bidir-PIM は指定フォワーダ（DF）選定と呼ばれる新しいメカニズムを導入します。これは、RP をルートとするループフリー SPT を確立します。

DF 選定

すべてのネットワーク セグメントとポイントツーポイント リンクで、PIM ルータはすべて指定フォワーダ（DF）選定と呼ばれる手順に参加します。 この手順では、双方向グループのすべての RP で DF としてルータを 1 つ選定します。 このルータは、そのネットワークで受信されたマルチキャスト パケットの転送を担当します。

DF 選定は、ユニキャスト ルーティング メトリックに基づきます。 RP への最も望ましいユニキャスト ルーティング メトリックを持つルータが DF になります。 この方法を使用することによって、RP へのパラレル等コスト パスがある場合にも、すべてのパケットのコピー 1 つだけが RP に送信されます。

DF は双方向グループのすべての RP に対して選定されます。 結果として、ネットワーク セグメント上で各 RP に 1 つずつ複数のルータが DF として選定されます。 複数のインターフェイスで特定のルータが DF として選定される場合があります。

双方向グループ ツリー ビルディング

双方向グループの共有ツリーに参加する手順は、PIM-SM での手順とほとんど同じです。 1 つ大きな違いは、双方向グループの場合、DR のロールが RP の DF によって仮定される点です。

ローカル レシーバを持つネットワークでは、DF として選定されたルータのみがインターネット グループ管理プロトコル（IGMP）加入メッセージの受信時に発信インターフェイス リスト（olist）を読み込み、(*, G) 加入および脱退メッセージを RP 方向にアップストリームに送信します。 ダウンストリーム ルータが共有ツリーに参加したい場合、PIM 加入および脱退メッセージの RPF ネイバーが常に RP に向かうインターフェイスの DF に選定されます。

ルータが加入または脱退メッセージを受け取り、ルータが受信インターフェイスの DF でない場合、メッセージは無視されます。そうでない場合、ルータは共有ツリーをスパースモードと同じように更新します。

ルータがすべて双方向共有ツリーをサポートしているネットワークでは、(S, G) 加入および脱退メッセージは無視されます。 DF 選定手順は RP からパラレル ダウンストリーム パスをなくすため、PIM アサート メッセージを送信する必要もありません。 RP はソースへのパスに参加することなく、登録停止も送信しません。

パケット転送

ルータは双方向グループに対してのみ (*, G) エントリを作成します。 (*, G) エントリの olist には、ルータが選定された DF であり、IGMP または PIM 加入メッセージを受信したインターフェイスがすべて含まれます。 ルータが送信者専用ブランチにある場合、(*, G) ステートも作成されますが、olist にはいずれのインターフェイスも含まれません。

パケットを RP 方向の RPF インターフェイスから受信した場合、(*, G) エントリの olist に従って、パケットはダウンストリームに転送されます。 それ以外の場合、受信インターフェイスの DF であるルータのみがパケットを RP 方向にアップストリームに転送します。その他のルータはすべてパケットを廃棄する必要があります。

双方向 PIM の利点

- Bidir-PIM は、多数のソースのルーティング ステート テーブルを維持するパフォーマンス コストをなくします。
- Bidir-PIM は、各 PM ドメイン内の多対多のアプリケーションで使用するよう設計されています。 双方向 PIM モードのマルチキャスト グループは、ソースの数によりオーバーヘッドを引き起こすことなく、任意の数のソースに拡張できます。

基本的な IP マルチキャストの設定方法

この項で説明する作業では、基本的な IP マルチキャスト モードを設定します。 ここでの作業はどれも必須ではありません。しかし、ネットワーク内の IP マルチキャストを設定するためには、少なくとも 1 つは作業を実行する必要があります。 複数の作業が必要な場合もあります。

自動ランデブー ポイント（AutoRP）でのスパース モードの設定

はじめる前に

- スパース-デンス モードで設定されたインターフェイスは、マルチキャスト グループの動作モードに応じてスパース モードまたはデンス モードで処理されます。 インターフェイスを設定する方法を決定する必要があります。

- AutoRP の設定時に必要なアクセス リストすべてを、設定作業の開始前に設定する必要があります。

（注）

- グループ内に既知の RP が存在せず、インターフェイスがスパース-デンス モードに設定される場合、インターフェイスはデンス モードであるかのように処理され、データがインターフェイスにフラッディングされます。 このデータのフラッディングを回避するには、AutoRP リスナーを設定し、スパース モードとしてインターフェイスを設定します。
- AutoRP を設定する場合は、AutoRP リスナー機能を設定し（ステップ 5）、スパース モードを指定する（ステップ 7）か、デンス モードを指定する（ステップ 8）必要があります。
- スパース-デンス モードを指定する場合、デンス モードのフェールオーバーがネットワークのデンス モードのフラッディングを引き起こす可能性があります。 この状態を回避するために、AutoRP リスナー機能では PIM スパース モードを使用します。

自動ランデブー ポイント（AutoRP）を設定するには、次の手順に従ってください。 AutoRP は、任意でエニーキャスト RP で使用することもできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. ステップ 5～7 またはステップ 6 ～ 8 を実行します。
5. **ip pim autorp listener**
6. **interface** *type number*
7. **ip pim sparse-mode**
8. **ip pim sparse-dense-mode**
9. **exit**
10. すべての PIM インターフェイス上でステップ 1 ～ 9 を繰り返します。
11. **ip pim send-rp-announce** {*interface-type interface-number* | *ip-address*} **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**]
12. **ip pim send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value* [**interval** *seconds*]
13. **ip pim rp-announce-filter rp-list** *access-list* **group-list** *access-list*
14. **no ip pim dm-fallback**
15. **interface** *type number*
16. **ip multicast boundary** *access-list* [**filter-autorp**]
17. **end**
18. **show ip pim autorp**
19. **show ip pim rp** [**mapping**] [*rp-address*]
20. **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]
21. **show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*]

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip multicast-routing** [**distributed**] 例： `Device(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。 • **distributed** キーワードを使用して、マルチキャスト分散スイッチングをイネーブルにします。
ステップ 4	ステップ 5～7 またはステップ 6 ～ 8 を実行します。	--
ステップ 5	**ip pim autorp listener** 例： `Device(config)# ip pim autorp listener`	2 つの AutoRP グループ 224.0.1.39 と 224.0.1.40 の IP マルチキャスト トラフィックを PIM スパース モードで動作しているインターフェイスでフラッディングされる PIM デンス モードにします。 • ステップ 8 でスパース-デンス モードを設定している場合、このステップはスキップします。
ステップ 6	**interface** *type number* 例： `Device(config)# interface Gigabitethernet 1/0/0`	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 7	**ip pim sparse-mode** 例： `Device(config-if)# ip pim sparse-mode`	インターフェイスで PIM スパース モードをイネーブルにします。スパース モードで AutoRP を設定している場合、次のステップで AutoRP リスナーも設定する必要があります。 • ステップ 8 でスパース-デンス モードを設定している場合、このステップはスキップします。
ステップ 8	**ip pim sparse-dense-mode** 例： `Device(config-if)# ip pim sparse-dense-mode`	インターフェイスで PIM スパース-デンス モードをイネーブルにします。 • ステップ 7 でスパース モードを設定した場合、このステップはスキップします。
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	すべての PIM インターフェイス上でステップ 1 ～ 9 を繰り返します。	--

	コマンドまたはアクション	目的
ステップ 11	**ip pim send-rp-announce** {*interface-type interface-number* | *ip-address*} **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**] 例： `Device(config)# ip pim send-rp-announce loopback0 scope 31 group-list 5`	RP アナウンスメントをすべての PIM 対応インターフェイスに送信します。 • RP デバイスでのみこのステップを実行します。 • RP アドレスとして使用する IP アドレスを定義するには、*interface-type* 引数と *interface-number* 引数を使用します。 • 直接接続されている IP アドレスを RP アドレスとして指定するには、*ip-address* 引数を使用します。 （注） このコマンドに *ip-address* 引数が設定されている場合、RP 通知メッセージがこのアドレスが接続されているインターフェイスによって送信されます（つまり、RP 通知メッセージの IP ヘッダーのソース アドレスがそのインターフェイスの IP アドレスです）。 • この例は、最大ホップ数が 31 でインターフェイスがイネーブルであることを示します。 デバイスを RP として識別するために使用される IP アドレスは、ループバック インターフェイス 0 に関連付けられた IP アドレスです。 アクセス リスト 5 はこのデバイスが RP として機能しているグループを示しています。
ステップ 12	**ip pim send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value* [**interval** *seconds*] 例： `Device(config)# ip pim send-rp-discovery loopback 1 scope 31`	デバイスを RP マッピング エージェントとして設定します。 • RP マッピング エージェント デバイスまたは複合 RP/RP マッピング エージェント デバイスでこのステップを実行します。 （注） AutoRP により、RP 機能を 1 台のデバイスで別々に実行できるようになり、RP マッピング エージェントを 1 台または複数のデバイスで実行できるようになります。 複合 RP/RP マッピング エージェント デバイスに、RP および RP マッピング エージェントを展開することができます。 • RP マッピング エージェントのソース アドレスとして使用する IP アドレスを定義するには、オプションの *interface-type* 引数と *interface-number* 引数を使用します。 • AutoRP 検出メッセージの IP ヘッダーで存続可能時間（TTL）値を指定するには、**scope** キーワードと *ttl-value* 引数を使用します。 • AutoRP 検出メッセージが送信される間隔を指定するには、オプションの **interval** キーワードと *seconds* 引数を使用します。

	コマンドまたはアクション	目的
		（注） AutoRP 検出メッセージが送信される間隔をデフォルト値の 60 秒から減らすと、group-to-RP マッピングのより頻繁なフラッディングが発生します。一部のネットワーク環境では、間隔を短縮する欠点（コントロールパケット オーバーヘッドの増加）が利点（グループと RP のマッピングのより頻繁な更新）を上回る場合があります。 • 例では、ループバック インターフェイス 1 で AutoRP 検出メッセージを 31 ホップに制限していることを示しています。
ステップ 13	**ip pim rp-announce-filter rp-list** *access-list* **group-list** *access-list* 例： `Device(config)# ip pim rp-announce-filter rp-list 1 group-list 2`	候補 RP（C-RP）から RP マッピング エージェントに送信される着信 RP 通知メッセージをフィルタリングします。 • RP マッピング エージェントでのみこのステップを実行します。
ステップ 14	**no ip pim dm-fallback** 例： `Device(config)# no ip pim dm-fallback`	（任意）PIM デンス モードのフォールバックを防ぎます。 • すべてのインターフェイスが PIM スパース モードで動作するよう設定されている場合、このステップはスキップします。 （注） （**ip pim sparse-mode** コマンドを使用して）すべてのインターフェイスが PIM スパース モードで動作するよう設定されている場合、**no ip pim dm-fallback** コマンド動作はデフォルトでイネーブルになります。
ステップ 15	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/0`	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 16	**ip multicast boundary** *access-list* [**filter-autorp**] 例： `Device(config-if)# ip multicast boundary 10 filter-autorp`	管理用スコープの境界を設定します。 • このステップは、他のデバイスとの境界であるインターフェイス上で実行します。 • この作業ではアクセス リストは表示されません。 • **deny** キーワードを使用するアクセス リスト エントリはそのエントリに一致するパケットのマルチキャスト境界を作成します。

	コマンドまたはアクション	目的
ステップ 17	**end** 例： `Device(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 18	**show ip pim autorp** 例： `Device# show ip pim autorp`	（任意）AutoRP 情報を表示します。
ステップ 19	**show ip pim rp** [**mapping**] [*rp-address*] 例： `Device# show ip pim rp mapping`	（任意）ネットワークで既知の RP を表示し、デバイスが各 RP について学習する方法を示します。
ステップ 20	**show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**] 例： `Device# show ip igmp groups`	（任意）デバイスに直接接続されている、インターネット グループ管理プロトコル（IGMP）を通じて学習されたレシーバを持つマルチキャスト グループを表示します。 • レシーバ情報が結果の画面に表示されるには、レシーバがこのコマンドが発行された時点でネットワーク上でアクティブである必要があります。
ステップ 21	**show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*] 例： `Device# show ip mroute cbone-audio`	（任意）IP マルチキャスト ルーティング（mroute）テーブルの内容を表示します。

次の作業

「IP マルチキャスト オペレーションの確認」モジュールに進みます。

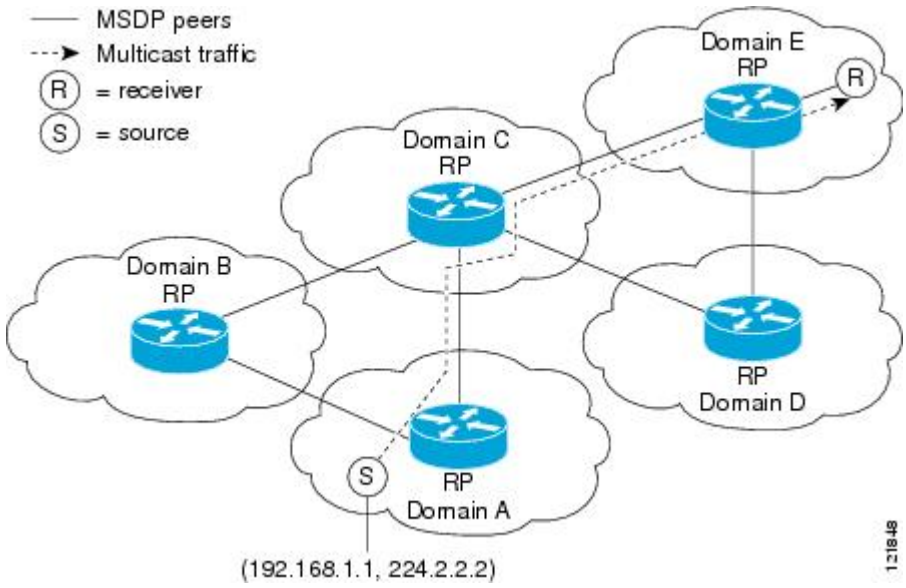
エニーキャスト RP でのスパース モードの設定

ここでは、RP 冗長性のためにエニーキャスト RP でスパース モードを設定する手順について説明します。

エニーキャスト RP は静的に設定され、インターフェイスは Protocol Independent Multicast スパース モード（PIM-SM）で動作するように設定されます。 エニーキャスト RP 設定では、ループバック インターフェイス上で同じ IP アドレスを使用して複数の RP を設定します。 エニーキャスト RP ループバック アドレスは、32 ビット マスクを使用して設定し、ホスト アドレスにする必要があります。 エニーキャスト RP 設定は、設定されているルータに関係なく、同じホスト アドレスが RP アドレスとして使用されるため、設定やトラブルシューティングが容易です。

エニーキャスト RP では、ソース登録のための負荷を複数の Rendezvous Point（RP）で共有でき、互いのホット バックアップ ルータとして機能できます。 Multicast Source Discovery Protocol（MSDP）は、エニーキャスト RP を可能にするキー プロトコルです。

図 *7*：各ドメインの *RP* 間でソース情報を共有する *MSDP*



手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **interface** *type number*
5. **ip pim sparse-mode**
6. **ip pim rp-address** *rp-address*
7. それぞれに同じ RP アドレスを割り当てる複数のルータでステップ 1 ～ 6 を繰り返します。
8. **interface loopback** [*interface-number*] **ip address** [*ip-address*] [*mask*]
9. **interface loopback** [*interface-number*] **ip address** [*ip-address*] [*mask*]
10. **exit**
11. **ip msdp peer** {*peer-name* | *peer-address*} [**connect-source** *interface-type* **interface-number**] [**remote-as** *as-number*]
12. **ip msdp originator-id loopback** [*interface*]
13. 冗長 RP 上でステップ 8 ～ 12 を繰り返します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip multicast-routing** [**distributed**] 例： `Router(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。 • **distributed** キーワードを使用して、マルチキャスト分散スイッチングをイネーブルにします。
ステップ 4	**interface** *type number* 例： `Router(config)# interface gigabitethernet 1/0/0`	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。

	コマンドまたはアクション	目的
ステップ 5	**ip pim sparse-mode** 例： `Router(config-if)# ip pim sparse-mode`	スパース モードをイネーブルにします。
ステップ 6	**ip pim rp-address** *rp-address* 例： `Router(config-if)# ip pim rp-address 10.0.0.1`	特定のグループの PIM RP のアドレスを設定します。
ステップ 7	それぞれに同じ RP アドレスを割り当てる複数のルータでステップ 1 ～ 6 を繰り返します。	--

ステップ 8	**interface loopback** [*interface-number*] **ip address** [*ip-address*] [*mask*]
	例：
	`Router(config-if)# interface loopback 0`
	例：
	`ip address 10.0.0.1 255.255.255.255`
		RP ルータにインターフェイス ループバック IP アドレスを設定します。
		• RP ルータでこのステップを実行します。

ステップ 9	**interface loopback** [*interface-number*] **ip address** [*ip-address*] [*mask*]
	例：
	`Router(config-if)# interface loopback 1`
	例：
	`ip address 10.1.1.1 255.255.255.255`
		MSDP ピアリングにインターフェイス ループバック IP アドレスを設定します。

ステップ 10	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**ip msdp peer** {*peer-name* | *peer-address*} [**connect-source** *interface-type* **interface-number**] [**remote-as** *as-number*]	MSDP ピアを設定します。 • RP ルータでこのステップを実行します。

	コマンドまたはアクション	目的
	例： `Router(config)# ip msdp peer 10.1.1.2 connect-source loopback 1`	
ステップ 12	**ip msdp originator-id loopback** [*interface*] 例： `Router(config)# ip msdp originator-id loopback 1`	SA メッセージのソースの MSDP スピーカーがインターフェイスの IP アドレスを SA メッセージ内で RP アドレスとして使用できるようにします。 • RP ルータでこのステップを実行します。
ステップ 13	冗長 RP 上でステップ 8 ～ 12 を繰り返します。	--

次の作業

「IP マルチキャスト オペレーションの確認」モジュールに進みます。

ブートストラップ ルータでのスパース モードの設定

ここでは、ルータがグループと RP のマッピングを動的に学習するように、耐障害性、自動 RP 検出、および配布メカニズム備えたブートストラップ ルータ（BSR）を設定する方法について説明します。

（注） Auto-RP と BSR の同時配備はサポートされていません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **interface** *type number*
5. **ip pim sparse-mode**
6. **end**
7. すべてのルータのすべてのマルチキャスト対応インターフェイス上でステップ 1 ～ 6 を繰り返します。
8. **ip pim bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority*]]
9. **ip pim rp-candidate** *interface-type interface-number* [group-list *access-list*] [**interval** seconds] [**priority** *value*]
10. すべての RP および BSR ルータ上でステップ 8 ～ 9 を繰り返します。
11. **interface** *type number*
12. **ip pim bsr-border**
13. **end**
14. メッセージを送受信すべきではない境界インターフェイスを持つすべてのルータでステップ 11 から 13 を繰り返します。
15. **show ip pim rp** [**mapping**] [*rp-address*]
16. **show ip pim rp-hash** [*group-address*] [*group-name*]
17. **show ip pim bsr-router**
18. **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]
19. **show ip mroute**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip multicast-routing** [**distributed**] 例： `Router(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。 • **distributed** キーワードを使用して、マルチキャスト分散スイッチングをイネーブルにします。
ステップ 4	**interface** *type number* 例： `Router(config)# interface gigabitethernet 1/0/0`	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 5	**ip pim sparse-mode** 例： `Router(config-if)# ip pim sparse-mode`	スパース モードをイネーブルにします。
ステップ 6	**end** 例： `Router(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	すべてのルータのすべてのマルチキャスト対応インターフェイス上でステップ 1 ～ 6 を繰り返します。	--
ステップ 8	**ip pim bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority*]] 例： `Router(config)# ip pim bsr-candidate gigibitethernet 0/0/0 0 192`	ルータがブートストラップ ルータ（BSR）として候補であることをアナウンスするよう設定します。 • RP または複合 RP/BSR ルータでこのステップを実行します。 （注） BSR により、RP 機能を 1 つのルータで別々に実行できるようになり、BSR を 1 つまたは複数のルータで実行できるようになります。 複合 RP/BSR ルータに、RP および BSR を展開することができます。 • このコマンドは、（*interface-type* および *interface-number* 引数に設定された）BSR アドレスとして指定されたインターフェイスのアドレスで、すべての PIM ネイバーに BSR メッセージを送信するようにルータを設定します。 • PIMv2 ハッシュ関数が呼び出される前にグループ アドレスと AND 連結されるマスクの長さ（最大 32 ビット）を設定するには、オプションの *hash-mask-length* 引数を使用します。 ハッ

	コマンドまたはアクション	目的
		シュ元が同じであるすべてのグループは、同じ RP に（対応）します。 たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。 ハッシュ マスク長により、1 つの RP を複数のグループで使用できるようになります。 デフォルトのハッシュ マスク長は 0 です。 • BSR の C-RP としてのプライオリティを指定するには、オプションの *priority* 引数を（ハッシュ マスク長を設定した後に）使用します。 プライオリティの範囲は 0 ～ 255 です。 最もプライオリティの高い（プライオリティ値が最も小さい）BSR C-RP がより優先されます。 プライオリティ値が同じ場合は、IP アドレスがより高位であるルータが優先されます。 デフォルトのプライオリティ値は 0 です。 （注） Cisco IOS および Cisco IOS XE に PIM BSR を実装する場合は、候補 RP および BSR のデフォルト プライオリティとして値 0 が使用されます。 この実装は、デフォルト優先値として 192 を指定する最初の IETF ドラフトである draft-ietf-pim-sm-bsr IETF ドラフト以前から存在します。 このため、Cisco IOS および Cisco IOS XE の実装は IETF ドラフトに反します。 ドラフトで指定されたデフォルトのプライオリティに準拠するには、プライオリティ値を明示的に 192 に設定する必要があります。
ステップ 9	**ip pim rp-candidate** *interface-type interface-number* [group-list *access-list*] [**interval** seconds] [**priority** *value*] 例： `Router(config)# ip pim rp-candidate gigabitethernet 2/0/0 group-list 4 priority 192`	ルータが自身を PIM バージョン 2 の候補 RP として BSR にアドバタイズするよう設定します。 • RP または複合 RP/BSR ルータでこのステップを実行します。 （注） BSR により、RP 機能を 1 つのルータで別々に実行できるようになり、BSR を 1 つまたは複数のルータで実行できるようになります。 複合 RP/BSR ルータに、RP および BSR を展開することができます。 • 間隔が指定されている場合、候補 RP アドバタイズメント間隔は指定された秒数に設定されます。 デフォルト インターバルは 60 秒です。 この間隔を短くすると、PIMv2 メッセージの発生を増加させて、セカンダリ RP へのフェールオーバーに必要な時間が短縮できます。 • Cisco IOS および Cisco IOS XE に PIM BSR を実装する場合は、RFC 2362 の仕様に準拠しない方法を使用して、1 組の候補 RP から RP を選択します。 設定の回避策については、BSR および RFC 2362 の相互利用可能な候補 RP の例, （69 ページ）を参

	コマンドまたはアクション	目的
		照してください。 詳細については、Cisco Bug Toolkit を使用して CSCdy56806 を参照してください。 （注） Cisco IOS および Cisco IOS XE に PIM BSR を実装する場合は、候補 RP および BSR のデフォルト プライオリティとして値 0 が使用されます。 この実装は、デフォルト優先値として 192 を指定する最初の IETF ドラフトである draft-ietf-pim-sm-bsr IETF ドラフト以前から存在します。このため、Cisco IOS および Cisco IOS XE の実装は IETF ドラフトに反します。 ドラフトで指定されたデフォルトのプライオリティに準拠するには、プライオリティ値を明示的に 192 に設定する必要があります。
ステップ 10	すべての RP および BSR ルータ上でステップ 8 ～ 9 を繰り返します。	--
ステップ 11	**interface** *type number* 例： `Router(config)# interface gigabitethernet 1/0/0`	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 12	**ip pim bsr-border** 例： `Router(config-if)# ip pim bsr-border`	インターフェイスでのブートストラップルータ（BSP）メッセージの送受信を防ぎます。 • 詳細については、BSR 境界インターフェイス，（35 ページ）を参照してください。
ステップ 13	**end** 例： `Router(config-if)# end`	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。
ステップ 14	メッセージを送受信すべきではない境界インターフェイスを持つすべてのルータでステップ 11 から 13 を繰り返します。	--
ステップ 15	**show ip pim rp** [**mapping**] [*rp-address*] 例： `Router# show ip pim rp`	（任意）関連付けられたマルチキャスト ルーティング エントリでキャッシュされたアクティブなランデブー ポイント（RP）を表示します。

	コマンドまたはアクション	目的
ステップ 16	**show ip pim rp-hash** [*group-address*] [*group-name*] 例： `Router# show ip pim rp-hash 239.1.1.1`	（任意）指定されたグループに対して選択されたランデブー ポイント（RP）を表示します。
ステップ 17	**show ip pim bsr-router** 例： `Router# show ip pim bsr-router`	（任意）ブートストラップ ルータ（BSP）情報を表示します。
ステップ 18	**show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**] 例： `Router# show ip igmp groups`	（任意）ルータに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャスト グループを表示します。 • レシーバ情報が結果の画面に表示されるには、レシーバがこのコマンドが発行された時点でネットワーク上でアクティブである必要があります。
ステップ 19	**show ip mroute** 例： `Router# show ip mroute cbone-audio`	（任意）IP mroute テーブルの内容を表示します。

次の作業

「IP マルチキャスト オペレーションの確認」モジュールに進みます。

単一のスタティック RP でのスパース モードの設定

ランデブー ポイント（RP）は Protocol Independent Multicast Sparse Mode（PIM-SM）を実行しているネットワークで必要です。 PIM-SM でトラフィックは、明示的にマルチキャスト データを要求したアクティブなレシーバを持つネットワーク セグメントにのみ転送されます。

ここでは、単一のスタティック RP でスパース モードを設定する手順について説明します。

はじめる前に

単一のスタティック RP でのスパース モードの設定時に必要なアクセス リストすべてを、設定作業の開始前に設定する必要があります。

（注） 双方向とスパース モード PIM グループの両方に同じ RP アドレスは使用できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **interface** *type number*
5. **ip pim sparse-mode**
6. IP マルチキャストを使用するすべてのインターフェイスでステップ 1 ～ 5 を繰り返します。
7. **exit**
8. **ip pim rp-address** *rp-address* [*access-list*] [**override**]
9. **end**
10. **show ip pim rp** [**mapping**] [*rp-address*]
11. **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]
12. **show ip mroute**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip multicast-routing** [**distributed**] 例： `Router(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。 • **distributed** キーワードを使用して、マルチキャスト分散スイッチングをイネーブルにします。
ステップ 4	**interface** *type number* 例： `Router(config)# interface gigabitethernet 1/0/0`	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。

	コマンドまたはアクション	目的
ステップ 5	**ip pim sparse-mode** 例： `Router(config-if)# ip pim sparse-mode`	インターフェイス上の PIM をイネーブルにします。 スパース モードを使用する必要があります。
ステップ 6	IP マルチキャストを使用するすべてのインターフェイスでステップ 1 ～ 5 を繰り返します。	--
ステップ 7	**exit** 例： `Router(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**ip pim rp-address** *rp-address* [*access-list*] [**override**] 例： `Router(config)# ip pim rp-address 192.168.0.0`	特定のグループの PIM RP のアドレスを設定します。 • マルチキャスト グループを RP に静的にマッピングされるよう定義する標準アクセス リストに名前を付けたり、番号を指定するために、オプションの *access-list* 引数が使用されます。 （注） アクセス リストが定義されていない場合、RP がすべてのマルチキャスト グループ 224/4 にマッピングされます。 • ダイナミックとスタティックのグループと RP のマッピングが共に使用され、RP アドレスが競合している場合、スタティックのグループと RP のマッピングに設定された RP アドレスが優先されるよう指定するには、オプションの **override** キーワードを使用します。 （注） **override** キーワードが指定されておらず、RP アドレスが競合している場合、ダイナミックのグループと RP のマッピングがスタティックのグループと RP のマッピングに優先されます。
ステップ 9	**end** 例： `Router(config)# end`	現在のコンフィギュレーション セッションを終了して、EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**show ip pim rp** [**mapping**] [*rp-address*] 例： `Router# show ip pim rp mapping`	（任意）ネットワークで既知の RP を表示し、ルータが各 RP について学習する方法を示します。
ステップ 11	**show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**] 例： `Router# show ip igmp groups`	（任意）ルータに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャスト グループを表示します。 • レシーバ情報が結果の画面に表示されるには、レシーバがこのコマンドが発行された時点でネットワーク上でアクティブである必要があります。
ステップ 12	**show ip mroute** 例： `Router# show ip mroute`	（任意）IP mroute テーブルの内容を表示します。

次の作業

「IP マルチキャスト オペレーションの確認」モジュールに進みます。

Source Specific Multicast の設定

ここでは、Source Specific Multicast（SSM）の設定方法を説明します。

はじめる前に

SSM 範囲の定義にアクセス リストを使用したい場合、**ip pim ssm** コマンドでアクセス リストを参照する前にアクセス リストを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **ip pim ssm** {**default** | **range** *access-list*}
5. **interface** *type number*
6. **ip pim sparse-mode**
7. IP マルチキャストを使用するすべてのインターフェイスでステップ 1 ～ 6 を繰り返します。
8. **ip igmp version 3**
9. ホスト方向のインターフェイスすべてでステップ 8 を繰り返します。
10. **end**
11. **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]
12. **show ip mroute**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip multicast-routing** [**distributed**] 例： `Device(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。 • **distributed** キーワードを使用して、マルチキャスト分散スイッチングをイネーブルにします。
ステップ 4	**ip pim ssm** {**default**	**range** *access-list*} 例： `Device(config)# ip pim ssm default`	SSM サービスを設定します。 • **default** キーワードは SSM 範囲のアクセス リストを 232/8 と定義します。 • **range** キーワードは標準の IP アクセス リスト番号または SSM 範囲を定義する名前を指定します。

	コマンドまたはアクション	目的
ステップ 5	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/0`	IGMPv3 をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 6	**ip pim sparse-mode** 例： `Device(config-if)# ip pim sparse-mode`	インターフェイス上の PIM をイネーブルにします。 スパース モードを使用する必要があります。
ステップ 7	IP マルチキャストを使用するすべてのインターフェイスでステップ 1 ～ 6 を繰り返します。	--
ステップ 8	**ip igmp version 3** 例： `Device(config-if)# ip igmp version 3`	このインターフェイス上で IGMPv3 をイネーブルにします。 デフォルトでは、IGMP のバージョン 2 が設定されます。 SSM にはバージョン 3 が必要です。
ステップ 9	ホスト方向のインターフェイスすべてでステップ 8 を繰り返します。	--
ステップ 10	**end** 例： `Device(config-if)# end`	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。
ステップ 11	**show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**] 例： `Device# show ip igmp groups`	（任意）デバイスに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャスト グループを表示します。 • レシーバ情報が結果の画面に表示されるには、レシーバがこのコマンドが発行された時点でネットワーク上でアクティブである必要があります。
ステップ 12	**show ip mroute** 例： `Device# show ip mroute`	（任意）IP mroute テーブルの内容を表示します。 • このコマンドは、マルチキャスト グループが SSM サービス用に設定されているのか、ソース固有のホスト レポートを受信しているのかを示します。

次の作業

「IP マルチキャスト オペレーションの確認」モジュールに進みます。

双方向 PIM（Bidir-PIM）の設定

ここでは、双方向 PIM（Bidir-PIM）の設定方法について説明します。

はじめる前に

双方向 PIM の設定時に必要なアクセス リストすべてを、設定作業の開始前に設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **interface** *type number*
5. **ip pim sparse-mode**
6. **exit**
7. **ip pim bidir-enable**
8. **ip pim rp-address** *rp-address* [*access-list*] [**override**] **bidir**
9. **end**
10. すべてのルータのすべてのマルチキャスト対応インターフェイス上でステップ 2 ～ 9 を繰り返します。
11. **show ip pim rp** [**mapping**] [*rp-address*]
12. **show ip mroute**
13. **show ip pim interface** [*type number*] [**df** | **count**] [*rp-address*]

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip multicast-routing** [**distributed**] 例： `Router(config)# ip multicast-routing`	IP マルチキャスト ルーティングをイネーブルにします。 • **distributed** キーワードを使用して、マルチキャスト分散スイッチングをイネーブルにします。
ステップ 4	**interface** *type number* 例： `Router(config)# interface gigabitethernet 1/0/0`	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 5	**ip pim sparse-mode** 例： `Router(config-if)# ip pim sparse-mode`	スパース モードをイネーブルにします。
ステップ 6	**exit** 例： `Router(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**ip pim bidir-enable** 例： `Router(config)# ip pim bidir-enable`	ルータの Bidir-PIM をイネーブルにします。 • すべてのルータでこのステップを実行します。
ステップ 8	**ip pim rp-address** *rp-address* [*access-list*] [**override**] **bidir** 例： `Router(config)# ip pim rp-address 10.0.1.1 45 bidir`	特定のグループの PIM RP のアドレスを設定します。 • すべてのルータでこのステップを実行します。 • このコマンドは、RP を双方向に定義し、アクセス リストの方法で双方向グループを定義します。 • ダイナミックとスタティックのグループと RP のマッピングが共に使用され、RP アドレスが競合している場合、スタティックのグループと RP のマッピングに設定された RP アドレスが優先されるよう指定するには、オプションの **override** キーワードを使用します。 （注） **override** キーワードが指定されておらず、RP アドレスが競合している場合、ダイナミックのグループと RP のマッピングがスタティックのグループと RP のマッピングに優先されます。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 10	すべてのルータのすべてのマルチキャスト対応インターフェイス上でステップ 2 ～ 9 を繰り返します。	--
ステップ 11	**show ip pim rp** [**mapping**] [*rp-address*] 例： `Router# show ip pim rp`	（任意）関連付けられたマルチキャスト ルーティング エントリでキャッシュされたアクティブな RP を表示します。
ステップ 12	**show ip mroute** 例： `Router# show ip mroute`	（任意）IP mroute テーブルの内容を表示します。
ステップ 13	**show ip pim interface** [*type number*] [**df** | **count**] [*rp-address*] 例： `Router# show ip pim interface`	（任意）DF に関連付けられたユニキャスト ルーティング メトリックと共に、インターフェイスの各 RP の選定された DF についての情報を表示します。

基本的な IP マルチキャストの設定例

例：AutoRP でのスパース モード

次の例では、AutoRP でスパース モードを設定しています。

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

```
access-list 10 permit 239.254.2.0 0.0.0.255
access-list 10 permit 239.254.3.0 0.0.0.255
```

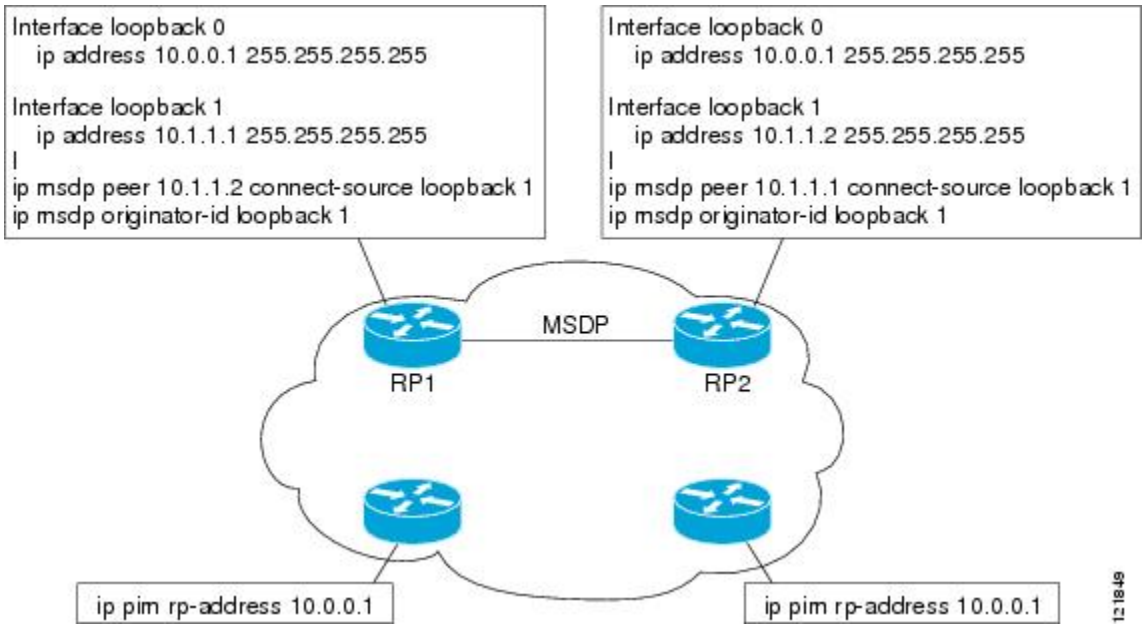
エニーキャスト RP でのスパース モードの例

エニーキャスト RP 実装の主な目的は、ダウンストリーム マルチキャスト ルータが RP に対してアドレスを 1 つだけ持つことです。 下の図の例は、RP（RP1 および RP2）のループバック インターフェイス 0 が 10.0.0.1 IP アドレスで設定される方法を示しています。 この 10.0.0.1 アドレスがすべての RP でループバック インターフェイス 0 のアドレスとして設定され、RP アドレスとして設定される場合、IP ルーティングが最も近い RP 上で収束します。 このアドレスは、ホスト ルートである必要があります。255.255.255.255 サブネット マスクです。

ダウンストリーム ルータは 10.0.0.1 RP アドレスについて通知される必要があります。 下の図で、ルータは **ip pim rp-address 10.0.0.1** グローバル コンフィギュレーション コマンドによって静的に設定されます。 この設定は、Auto-RP またはブートストラップ ルータ（BSR）機能を使用して行うこともできます。

図の RP は MSDP を使用してソース情報を共有する必要もあります。 この例で、RP（RP1 および RP2）のループバック インターフェイス 1 は MSDP ピアリング用に設定されています。 MSDP ピアリング 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。

図 *8*：エニーキャスト *RP* の設定



多くのルーティング プロトコルがルータ ID に対してループバック インターフェイス上で最も高い IP アドレスを選択します。 ルータがルータ ID に対してエニーキャスト RP アドレスを選択すると、問題が発生する場合があります。 RP 上でルータ ID を MSDP ピアリング アドレスと同じアドレスに手動で設定して、この問題を回避することを推奨します（たとえば、上の図のループバック 1 アドレス）。 Open Shortest Path First（OSPF）では、ルータ ID は **router-id** ルータ コン

フィギュレーションコマンドを使用して設定されます。ボーダーゲートウェイプロトコル（BGP）では、ルータ ID は **bgp router-id** ルータ コンフィギュレーション コマンドを使用して設定されます。 多くの BGP トポロジでは、RPF チェックをパスするために、MSDP ピアリング アドレスと BGP ピアリング アドレスが同じである必要があります。 BGP ピアリング アドレスは、**neighbor update-source** ルータ コンフィギュレーション コマンドを使用して設定できます。

上記のエニーキャスト RP の例は、RFC 1918 からの IP アドレスを使用します。 これらの IP アドレスは通常ドメイン間の境界でブロックされ、このため、他の ISP にはアクセスできません。 RP に他のドメインから到達できるようにするには、有効な IP アドレスを使用する必要があります。

次の例は、エニーキャスト RP 設定の実行方法を示しています。

RP 1 上で

```
ip pim rp-address 10.0.0.1
interface loopback 0
 ip address 10.0.0.1 255.255.255.255
!
interface loopback 1
 ip address 10.1.1.1. 255.255.255.255
!
 ip msdp peer 10.1.1.2 connect-source loopback 1
 ip msdp originator-id loopback 1
```

RP 2 上で

```
ip pim rp-address 10.0.0.1
interface loopback 0
 ip address 10.0.0.1 255.255.255.255
interface loopback 1
 ip address 10.1.1.2. 255.255.255.255
!
 ip msdp peer 10.1.1.1 connect-source loopback 1
 ip msdp originator-id loopback 1
```

その他のすべてのルータ

```
ip pim rp-address 10.0.0.1
```

ブートストラップ ルータでのスパース モードの例

次の例は、候補 BSR の設定です。これは、候補 RP の場合も同様です。

```
!
ip multicast-routing
!
interface GigabitEthernet0/0/0
 ip address 172.69.62.35 255.255.255.240
 ip pim sparse-mode
!
interface GigabitEthernet1/0/0
 ip address 172.21.24.18 255.255.255.248
 ip pim sparse-mode
!
interface GigabitEthernet2/0/0
 ip address 172.21.24.12 255.255.255.248
 ip pim sparse-mode
!
```

```
ip pim bsr-candidate GigabitEthernet2/0/0 30 10
ip pim rp-candidate GigabitEthernet2/0/0 group-list 5
access-list 5 permit 239.255.2.0 0.0.0.255
```

BSR および RFC 2362 の相互利用可能な候補 RP の例

シスコ製およびシスコ製以外のルータが PIM バージョン 2 BSR を備えた単一の PIM ドメイン内で動作している場合、BSR RP 選択の Cisco 実装は RFC 2362 と完全には互換性がないため候補 RP の設定時には注意が必要です。

RFC 2362 は BSR RP が次のように選択されるよう指定しています（RFC 2362, 3.7）。

1. 最も高い優先度（最も低く設定された優先値）の候補 RP を選択します。
2. 優先度が同点の場合、ハッシュ関数値が最も高い候補 RP を選択します。
3. ハッシュ関数値が同点の場合、IP アドレスが最も高い候補 RP を選択します。

Cisco ルータは、優先度、ハッシュ関数、IP アドレスに基づいて RP を選択する前に、常に通知されたグループ アドレス プレフィックスの最長一致に基づいて候補 RP を選択します。

部分的に重複するグループ アドレス範囲で複数の候補 RP が設定されると、同じドメイン内のシスコ製およびシスコ製以外の RFC 2362 互換ルータ間で候補 RP 選択が矛盾する可能性があります。 候補 RP 選択の矛盾は、PIM ドメイン内のソースとレシーバ間の接続を妨げる可能性があります。 ソースがある候補 RP を登録し、レシーバが同じグループ内であっても別の候補 RP に接続する可能性があります。

次の例は、PIM バージョン 2 BSR を備えた単一の PIM ドメイン内のシスコ製およびシスコ製以外のルータ間で RP 選択の矛盾を招く可能性のある設定を示しています。

```
access-list 10 permit 224.0.0.0  7.255.255.255
ip pim rp-candidate gigabitethernet1/0/0 group-list 10 priority 20
access-list 20 permit 224.0.0.0 15.255.255.255
ip pim rp-candidate gigabitethernet2/0/0 group-list 20 priority 10
```

この例では、GigabitEthernet インターフェイス 1/0/0 の候補 RP がより低い優先度 20 を持つより長いグループ プレフィックス 224.0.0.0/5 を通知します。 GigabitEthernet インターフェイス 2/0/0 の候補 RP がより高い優先度 10 を持つより短いグループ プレフィックス 224.0.0.0/4 を通知します。両方の範囲に一致するすべてのグループで、イーサネット インターフェイス 1 の候補 RP はより長いグループ プレフィックスを通知するため、Cisco ルータは常にこれを選択します。GigabitEthernet インターフェイス 2/0/0 の候補 RP はより高い優先度で設定されているため、シスコ製以外の RFC 2362 に完全準拠したルータは常にこれを選択します。

この相互運用性の問題を避けるには、部分的に重複するグループアドレスプレフィックスを通知する別の候補 RP を設定しないでください。 同じグループ プレフィックス長を持つ複数の候補 RP から通知する場合は、任意のグループ プレフィックスを設定します。

次の例は、PIM バージョン 2 BSR を備えた単一の PIM ドメイン内の Cisco ルータとシスコ製以外のルータの間に互換性が生じるように以前の例を設定する方法を示します。

```
access-list 10 permit 224.0.0.0  7.255.255.255
ip pim rp-candidate gigabitethernet1/0/0 group-list 10 priority 20
access-list 20 permit 224.0.0.0  7.255.255.255
```

```
access-list 20 permit 232.0.0.0  7.255.255.255
ip pim rp-candidate gigabitethernet2/0/0 group-list 20 priority 10
```

この設定では、イーサネット インターフェイス 2 の候補 RP がグループ アドレス 224.0.0.0/5 と 224.0.0.0/4 に等しい 232.0.0.0/5 を通知しますが、インターフェイスにイーサネット 1 の候補 RP と同じグループ プレフィックス長（5）を与えます。 結果として、Cisco ルータと RFC 2362 互換ルータの両方が RP イーサネット インターフェイス 2 を選択します。

例：単一のスタティック RP でのスパース モード

次に、すべてのマルチキャスト グループの PIM RP アドレスを 192.168.1.1 に設定し、すべてのグループがスパース モードで動作するように定義する例を示します。

```
ip multicast-routing
interface gigiabitethernet 1/0/0
 ip pim sparse-mode
ip pim rp-address 192.168.1.1
```

（注） 双方向モードおよびスパース モードの両方のグループに対して同じ RP は使用できません。

次に、マルチキャスト グループ 225.2.2.2 についてのみ PIM RP アドレスを 172.16.1.1 に設定する例を示します。

```
access list 1 225.2.2.2 0.0.0.0
 ip pim rp-address 172.17.1.1
```

IGMPv3 を使用した SSM の例

次の例は、SSM 用に（IGMPv3 を実行する）デバイスを設定する方法を示しています。

```
ip multicast-routing
!
interface GigabitEthernet3/1/0
 ip address 172.21.200.203 255.255.255.0
 description backbone interface
 ip pim sparse-mode
!
interface GigabitEthernet3/2/0
 ip address 131.108.1.2 255.255.255.0
 ip pim sparse-mode
 description ethernet connected to hosts
 ip igmp version 3
!
ip pim ssm default
```

SSM フィルタリング例

次の例は、SSM ルーティングをサポートしないソフトウェア リリースを実行しているレガシー RP ルータでフィルタリングを設定する方法を示しています。 このフィルタリングは SSM 範囲で不要な PIM-SM および MSDP トラフィックをすべて抑制します。 このフィルタリングがなくても

SSM は動作しますが、レガシーのファースト ホップ ルータとラスト ホップ ルータがネットワークに存在する場合、追加の RPT トラフィックがある場合があります。

```
ip access-list extended  no-ssm-range
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM range
  permit ip any any
! Deny registering in SSM range
ip pim accept-register list no-ssm-range
ip access-list extended msdp-nono-list
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM Range
  ! .
  ! .
  ! .
  ! See ftp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt for other SA
  ! messages that typically need to be filtered.
  permit ip any any
! Filter generated SA messages in SSM range. This configuration is only needed if there
! are directly connected sources to this router. The "ip pim accept-register" command
! filters remote sources.
ip msdp redistribute list msdp-nono-list
! Filter received SA messages in SSM range. "Filtered on receipt" means messages are
! neither processed or forwarded. Needs to be configured for each MSDP peer.
ip msdp sa-filter in msdp-peer1 list msdp-nono-list
! .
! .
! .
ip msdp sa-filter in msdp-peerN list msdp-nono-list
```

Bidir-PIM の例

デフォルトで、双方向 RP はすべてのグループを双方向としてアドバタイズします。 RP 上のアクセス リストは、双方向とアドバタイズされるグループのリストを指定するために使用できます。 **deny** キーワードを持つグループはデンス モードで動作します。 単一のアクセス リストでは、**permit** キーワードまたは **deny** キーワードのどちらかだけを使用できるため、スパースモードで動作するグループには、非双方向の異なる RP アドレスが必要です。

次の例は、スパース モードと双方向モードの両方のグループで RP を設定する方法を示しています。 224/8 および 227/8 と特定されたグループは双方向グループで、226/8 はスパース モード グループです。 RP は、スパース モード動作と双方向モード動作に異なる IP アドレスを使用するよう必要があります。 2 つのループバック インターフェイスはこの設定を許可するよう使用します。 これらのループバック インターフェイスのアドレスは、PIM ドメイン内の他のルータが RP と通信できる方法で、PIM ドメイン中にルーティングする必要があります。

```
ip multicast-routing
!
.
.
.
!
interface loopback 0
 description One loopback address for this router's Bidir Mode RP function
 ip address 10.0.1.1 255.255.255.0
!
interface loopback 1
description One loopback address for this router's Sparse Mode RP function
 ip address 10.0.2.1 255.255.255.0
!
.
.
.
!
```

```
ip pim bidir-enable
ip pim rp-address 10.0.1.1 45 bidir
ip pim rp-address 10.0.2.1 46
!
access-list 45 permit 224.0.0.0 0.255.255.255
access-list 45 permit 227.0.0.0 0.255.255.255
access-list 46 permit 226.0.0.0 0.255.255.255
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』

標準および RFC

標準/RFC	タイトル
draft-kouvelas-pim-bidir-new-00.txt	『A New Proposal for Bi-directional PIM』
RFC 1112	『Host Extensions for IP Multicasting』
RFC 1918	『Address Allocation for Private Internets』
RFC 2770	『GLOP Addressing in 233/8』
RFC 3569	『An Overview of Source-Specific Multicast (SSM)』

MIB

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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv4 ネットワークでの基本的な IP マルチキャスト設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *3*：*IPv4* ネットワークでの基本的な *IP* マルチキャスト設定の機能情報

機能名	リリース	機能情報
Auto RP の拡張機能	Cisco IOS XE Release 2.1	Auto-RP は、PIM ネットワークにおけるグループからランデブー ポイント（RP）へのマッピングの配信を自動化します。Auto-RP が機能するためには、RP 通知メッセージを RP から受信して競合を解決する RP マッピング エージェントとしてルータが指定されている必要があります。

機能名	リリース	機能情報
双方向 PIM	Cisco IOS XE Release 2.2	双方向 PIM は、双方向のデータ フローを提供する共有スパース ツリーを実装するプロトコルの PIM スイートに対する拡張機能です。 PIM スパース モードとは対照的に、双方向 PIM ではソース固有のステートをルータに保持することを回避できるため、ツリーを拡張して任意の数のソースに対応できます。
ネットワークにおける RP 情報損失後の PIM デンス モード フォールバック回避	12.3(4)T 12.0(28)S 12.2(33)SRA 12.2(33)SXH Cisco IOS XE Release 2.1 15.0(1)S	ネットワークにおける RP 情報損失後の PIM デンス モード フォールバック回避機能は、すべての RP で障害が発生したときに PIM-DM のフォールバックを回避できるようにします。信頼性が重大な意味を持つマルチキャスト ネットワークにとって、デンス モードの使用を回避することは非常に重要です。この機能は、スパース モードでマルチキャスト グループを保持するためのメカニズムを提供し、それによってデンスモード フラッディングを回避します。 次のコマンドがこの機能により導入されました。**ip pim dm-fallback**。
Source Specific Multicast（SSM）	12.3(4)T 12.2(25)S 12.0(28)S 12.2(33)SXH 12.2(33)SRA 15.0(1)S Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0SG	SSM は、レシーバが明示的に参加したマルチキャスト ソースからのみデータグラム トラフィックがレシーバに転送される IP マルチキャストの拡張機能です。 SSM 用に設定されたマルチキャスト グループは、（共有ツリーではなく）ソース固有のマルチキャスト配信ツリーのみが作成されます。

第 3 章

IPv6 ネットワークでの基本的な IP マルチキャスト設定

このモジュールでは、IPv6 ネットワークで基本的な IP マルチキャストを設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

基本的な IP マルチキャスト設定の前提条件

- このモジュールに含まれているどの作業を実行する必要があるかを判断するには、使用する Protocol Independent Multicast（PIM）モードを決定する必要があります。 この決定は、ネットワーク上でサポートするアプリケーションによって異なります。
- このモジュールの作業で使用するアクセス リストはすべて、設定作業を開始する前に設定しておく必要があります。 アクセス リストの設定方法については、『*Security Configuration Guide: Access Control Lists*』の「Creating an IP Access List and Applying It to an Interface」モジュールを参照してください。

IPv6 ネットワークでの基本的な IP マルチキャスト設定に関する情報

IPv6 マルチキャスト

IPv6 マルチキャストの概要

IPv6マルチキャスト グループは、特定のデータ ストリームを受信する受信側の任意のグループです。 このグループには、物理的境界または地理的境界はありません。受信側は、インターネット上または任意のプライベート ネットワーク内の任意の場所に配置できます。 特定のグループへのデータ フローの受信に関与する受信側は、ローカル デバイスに対してシグナリングすることによってそのグループに加入する必要があります。 このシグナリングは、MLD プロトコルを使用して行われます。

デバイスは、MLDプロトコルを使用して、直接接続されているサブネットにグループのメンバが存在するかどうかを学習します。 ホストは、MLD レポート メッセージを送信することによってマルチキャスト グループに加入します。 ネットワークでは、各サブネットでマルチキャスト データのコピーを 1 つだけ使用して、潜在的に無制限の受信側にデータが伝送されます。 トラフィックの受信を希望する IPv6 ホストはグループ メンバと呼ばれます。

グループ メンバに伝送されるパケットは、単一のマルチキャスト グループ アドレスによって識別されます。 マルチキャスト パケットは、IPv6ユニキャスト パケットと同様に、ベストエフォート型の信頼性を使用してグループに伝送されます。

マルチキャスト環境は、送信側と受信側で構成されます。 どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。 ただし、グループのメンバだけがメッセージを受信します。

マルチキャスト アドレスがマルチキャスト グループの受信先として選択されます。 送信者は、データグラムの宛先アドレスとしてグループのすべてのメンバに到達するためにそのアドレスを使用します。

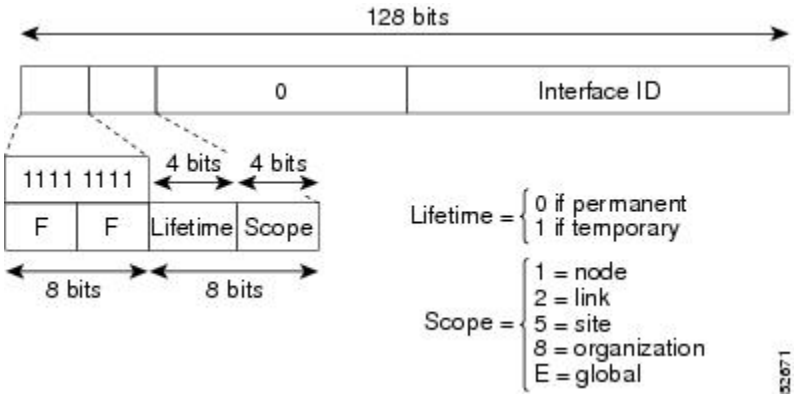
マルチキャスト グループ内のメンバーシップはダイナミックです。ホストはいつでも加入および脱退できます。 マルチキャスト グループ内のメンバの場所または数に制約はありません。 ホストは、一度に複数のマルチキャスト グループのメンバにすることができます。

マルチキャスト グループがどの程度アクティブであるか、その期間、およびメンバーシップはグループおよび状況によって異なります。 メンバを含むグループにアクティビティがない場合もあります。

IPv6 マルチキャスト アドレッシング

IPv6 マルチキャスト アドレスは、FF00::/8（1111 1111）というプレフィックスを持つ IPv6 アドレスです。 IPv6 マルチキャスト アドレスは、通常は異なるノードに属するインターフェイス セットの識別子です。 マルチキャスト アドレスに送信されたパケットは、マルチキャスト アドレスが示すすべてのインターフェイスに配信されます。 プレフィックスに続く 2 番めのオクテットで、マルチキャスト アドレスのライフタイムとスコープが定義されます。 永久マルチキャスト アドレスはライフタイム パラメータが 0 に等しく、一時マルチキャスト アドレスのライフタイム パラメータは 1 に等しくなっています。 ノード、リンク、サイト、組織のスコープ、またはグローバル スコープを持つマルチキャスト アドレスのスコープ パラメータは、それぞれ 1、2、5、8、または E です。 たとえば、プレフィックスが FF02::/16 のマルチキャスト アドレスは、リンク スコープを持つ永続マルチキャスト アドレスです。 下の図は、IPv6 マルチキャスト アドレスの形式を示しています。

図 *9*：*IPv6* マルチキャスト アドレス形式



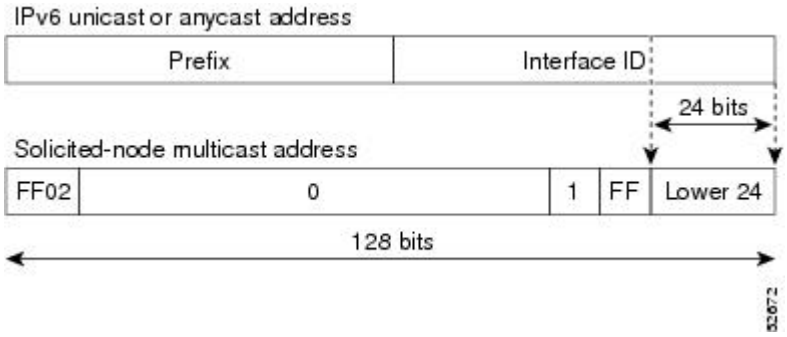
IPv6 ノード（ホストとルータ）は、（受信パケットの宛先となる）次のマルチキャスト グループに加入する必要があります。

- 全ノード マルチキャスト グループ FF02:0:0:0:0:0:0:1（スコープはリンクローカル）
- 割り当てられたユニキャスト アドレスおよびエニーキャスト アドレスごとの送信要求ノード マルチキャスト グループ FF02:0:0:0:0:1:FF00:0000/104

IPv6 ルータは、全ルータ マルチキャスト グループ FF02:0:0:0:0:0:0:2（スコープはリンクローカル）にも加入する必要があります。

送信要求ノード マルチキャスト アドレスは、IPv6 ユニキャスト アドレスまたはエニーキャスト アドレスに対応するマルチキャスト グループです。IPv6 ノードは、割り当てられているユニキャスト アドレスおよびエニーキャスト アドレスごとに、関連付けられた送信要求ノード マルチキャスト グループに加入する必要があります。 IPv6 送信要求ノード マルチキャスト アドレスには、対応する IPv6 ユニキャスト アドレスまたは IPv6 エニーキャスト アドレスの下位 24 ビットに連結されたプレフィックス FF02:0:0:0:0:1:FF00:0000/104 があります（下の図を参照）。 たとえば、IPv6 アドレス 2037::01:800:200E:8C6C に対応する請求ノード マルチキャスト アドレスは FF02::1:FF0E:8C6C です。 送信要求ノード アドレスは、ネイバー送信要求メッセージで使用されます。

図 *10*：*IPv6* 送信要求ノード マルチキャスト アドレス形式



（注） IPv6 にはブロードキャスト アドレスはありません。 ブロードキャスト アドレスの代わりに IPv6 マルチキャスト アドレスが使用されます。

IPv6 マルチキャスト グループ

インターフェイスで IPv6 トラフィックを転送できるようにするには、そのインターフェイスで IPv6 アドレスを設定する必要があります。インターフェイスでサイトローカルまたはグローバル IPv6 アドレスを設定すると、リンクローカル アドレスが自動的に設定され、そのインターフェイスに対して IPv6 がアクティブになります。また、設定されたインターフェイスは、そのリンクに必要な次のマルチキャスト グループに自動的に加入します。

- インターフェイスに割り当てられたユニキャスト アドレスおよびエニーキャスト アドレスごとの請求ノード マルチキャスト グループ FF02:0:0:0:0:1:FF00::/104

  （注） 送信要求ノード マルチキャスト アドレスは、ネイバー探索プロセスで使用されます。

- 全ノード リンクローカル マルチキャスト グループ FF02::1
- 全ルータ リンクローカル マルチキャスト グループ FF02::2

IPv6 マルチキャスト アドレス グループ範囲のサポート

この機能は、IPv6 マルチキャスト エッジ ルーティングにアクセス コントロール メカニズムを提供します。 ACL では、許可または拒否されるマルチキャスト グループまたはチャネルを指定します。拒否されたグループまたはチャネルについて、デバイスはプロトコル トラフィックおよびアクションを無視し（たとえば、MLD ステートは作成されず、mroute ステートは作成されず、PIM join は転送されません）、システムのすべてのインターフェイス上でデータ トラフィックをドロップし、ACL によって拒否されたグループまたはチャネルのマルチキャストをディセーブルにします。

限定スコープ アドレス アーキテクチャ

IPv6 では、グローバル アドレスと非グローバル アドレスがサポートされています。 ここでは、異なるスコープの IPv6 アドレスの使用方法について説明します。

スコープ ゾーン（簡単にはゾーン）とは、特定のスコープのトポロジの、接続されているリージョンです。 たとえば、特定のサイト内のデバイスが接続しているリンクのセット、およびこれらのリンクに接続されているインターフェイスは、サイトローカル スコープの単一のゾーンを構成します。

ゾーンはトポロジ リージョンの特定のインスタンス（たとえば、ゾーン 1 のサイトまたはゾーン 2 のサイト）であるのに対し、スコープはトポロジ リージョンの規模（たとえば、サイトまたはリンク）です。特定の非グローバルアドレスに関連するゾーンは、アドレス自体では符号化されません。ただし、その代わりに、その送受信を行うインターフェイスなどのコンテキストによって判別されます。 したがって、特定の非グローバル スコープのアドレスは、そのスコープの別々のゾーンで再利用される場合があります。 たとえば、ゾーン 1 のサイトとゾーン 2 のサイトのそれぞれに、サイトローカル アドレス FEC0::1 を持つノードが含まれている場合があります。

異なるスコープのゾーンは、次のようにインスタンス化されます。

- 各リンク、およびそのリンクに接続されているインターフェイスは、リンクローカル スコープの単一のゾーン（ユニキャストおよびマルチキャストの両方に使用）を構成します。
- インターネットのすべてのリンクおよびインターフェイスで構成されるグローバル スコープの単一のゾーン（ユニキャストおよびマルチキャストの両方に使用）もあります。
- インターフェイスローカル、リンクローカル、およびグローバル以外のスコープのゾーンの境界については、ネットワーク管理者が定義および設定する必要があります。ユニキャストおよびマルチキャストの両方で、サイト境界が境界として機能します。

ゾーン境界は、比較的スタティックな機能であり、トポロジにおける短期的な変更に応じて変化することはありません。 したがって、ゾーン内のトポロジが「接続されている必要がある」という要件は、一時的にだけ接続されることがあるリンクとインターフェイスを含めるためのものです。 たとえば、ダイヤルアップにより従業員のサイトへのインターネットアクセスを取得するレジデンシャル ノードまたはネットワークは、ダイヤルアップ リンクが切断された場合でも、従業員のサイトローカル ゾーンの一部として扱われることがあります。 同様に、ゾーンのパーティション化を引き起こすデバイス、インターフェイス、またはリンクの障害が発生しても、そのゾー

ンが複数のゾーンに分割されることはありません。厳密には、別個のパーティションが引き続き同じゾーンに属しているものと見なされます。

ゾーンには、他にも次の特性があります。

- ゾーン境界はリンクではなくノードを横断します（グローバルゾーンには境界はなく、インターフェイスローカル ゾーンの境界には1つのインターフェイスだけが含まれています）。
- 同じスコープのゾーンは重なることができません。つまり、共通のリンクまたはインターフェイスを持つことはできません。
- （グローバルより小さい）特定のスコープのゾーンは、それより大きいスコープのゾーン内に完全に含まれます。つまり、小さいスコープのゾーンには、リンクまたはインターフェイスを共有する大きいスコープのゾーンを超えるトポロジを含めることはできません。
- 各インターフェイスは、それぞれのスコープの 1 つのゾーンに厳密に属しています。

MRIB

マルチキャストルーティング情報ベース（MRIB）は、マルチキャスト ルーティング プロトコル（ルーティング クライアント）によってインスタンス化されるマルチキャスト ルーティング エントリのプロトコル非依存リポジトリです。その主要機能は、ルーティングプロトコルとマルチキャスト転送情報ベース（MFIB）間の非依存性を実現することです。また、クライアント間の調整および通信ポイントとしても機能します。

ルーティング クライアントは、MRIB が提供するサービスを使用して、ルーティング エントリをインスタンス化し、他のクライアントによってルーティング エントリに加えられた変更を取得します。 MRIB では、ルーティング クライアント以外に、転送クライアント（MFIB インスタンス）や特別なクライアント（MLD など）も扱われます。 MFIB は、MRIB からその転送エントリを取得し、パケットの受信に関連するイベントについて MRIB に通知します。 これらの通知は、ルーティング クライアントによって明示的に要求されることも、MFIB によって自発的に生成されることもあります。

MRIB のもう 1 つの重要な機能は、同じマルチキャスト セッション内でマルチキャスト接続を確立する際に、複数のルーティング クライアントの調整を可能にすることです。 また、MRIB では、MLD とルーティング プロトコル間の調整も可能です。

IPv6 マルチキャストのプロセス スイッチングおよび高速スイッチング

統合 MFIB は、IPv6 マルチキャストでの PIM-SM および PIM-SSM に対するファスト スイッチングおよびプロセス スイッチングの両サポートを提供するために使用されます。 プロセス スイッチングでは、ルート プロセッサが各パケットの調査、書き換え、および転送を行う必要があります。 最初にパケットが受信され、システム メモリにコピーされます。次に、デバイスがルーティング テーブル内でレイヤ 3 ネットワーク アドレスを検索します。 そのあと、レイヤ 2 フレームがネクストホップの宛先アドレスで書き換えられ、発信インターフェイスに送信されます。 また、RP は、巡回冗長検査（CRC）も計算します。 このスイッチング方式は、IPv6 パケットをスイッチングする方式の中でスケーラビリティが最も低い方式です。

IPv6 マルチキャストの高速スイッチングを使用すると、デバイスはプロセス スイッチングよりも高いパケット転送パフォーマンスを実現できます。 従来ルート キャッシュに格納される情報は、IPv6 マルチキャスト スイッチング用にいくつかのデータ構造に格納されます。 これらのデータ構造では、ルックアップが最適化され、パケット転送を効率的に行えるようになっています。

IPv6 マルチキャスト転送では、PIM プロトコル ロジックで許可されていれば、最初のパケットのファスト スイッチングが行われます。 IPv6 マルチキャストの高速スイッチングでは、MAC カプセル化ヘッダーが事前に計算されます。 IPv6 マルチキャストの高速スイッチングでは、MFIB を使用して、IPv6 送信先プレフィックス ベースのスイッチング判定が行われます。 IPv6 マルチキャストの高速スイッチングでは、MFIB に加えて、隣接関係テーブルを使用して、レイヤ 2 アドレッシング情報が付加されます。 隣接関係テーブルでは、すべての MFIB エントリのレイヤ 2 ネクストホップ アドレスが管理されます。

隣接が検出されると、隣接関係テーブルにそのデータが入力されます。（ARP などを使用して）隣接エントリが作成されるたびに、その隣接ノードのリンク層ヘッダーが事前に計算され、隣接関係テーブルに格納されます。ルートが決定されると、そのヘッダーはネクストホップおよび対応する隣接エントリを指します。そのあと、そのヘッダーはパケット スイッチング時のカプセル化に使用されます。

ロード バランシングと冗長性の両方に対応するようにデバイスが設定されている場合など、ルートには送信先プレフィックスへの複数のパスが存在することがあります。 解決されたパスごとに、そのパスのネクストホップ インターフェイスに対応する隣接へのポインタが追加されます。このメカニズムは、複数のパスでのロード バランシングに使用されます。

IPv6 エニーキャスト RP ソリューション

PIMv6 エニーキャスト RP ソリューションの概要

IPv6 PIM のエニーキャスト RP ソリューションは、IPv6 ネットワークによる PIM-SM RP のエニーキャスト サービスのサポートを可能にします。 これにより、PIM のみを実行するドメイン内でエニーキャスト RP を使用できるようになります。 エニーキャスト RP は、IPv4 および IPv6 で使用できますが、IPv4 だけで動作する Multicast Source Discovery Protocol（MSDP）には依存しません。この機能は、ドメイン間接続が不要な場合に便利です。

エニーキャスト RP は、PIM RP のデバイスに障害が発生した場合に、高速コンバージェンスを取得するために ISP ベースのバックボーンが使用するメカニズムです。 受信側および送信元が最も近くの RP にランデブーできるようにするには、送信元からのパケットがすべての RP に到達して、加入している受信側を検出する必要があります。

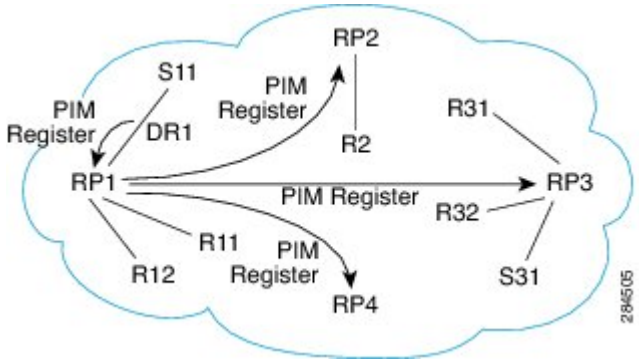
ユニキャスト IP アドレスは RP アドレスとして選択されます。 このアドレスは、静的に設定されるか、またはダイナミック プロトコルを使用して、ドメイン全体のすべての PIM デバイスに配信されます。 ドメイン内の一連のデバイスが、この RP アドレスの RP として動作するように選択されます。これらのデバイスは、エニーキャスト RP セットと呼ばれます。 エニーキャスト RP セット内の各デバイスは、RP アドレスを使用してループバック インターフェイスで設定されます。また、エニーキャスト RP セット内の各デバイスには、RP 間の通信に使用する別の物理 IP アドレスも必要です。

RP アドレス、または RP アドレスに対応するプレフィックスは、ドメイン内部のユニキャスト ルーティング システムに挿入されます。 エニーキャスト RP セット内の各デバイスは、エニーキャスト RP セット内のその他すべてのデバイスのアドレスで設定されます。また、この設定は、セット内のすべての RP で一致している必要があります。

PIMv6 エニーキャスト RP の通常の動作

次の図に、PIMv6 エニーキャスト RP の通常の動作を示し、次のように想定します。

- RP1、RP2、RP3、および RP4 は同じエニーキャスト RP グループのメンバです。
- S11 と S31 は、ユニキャスト ルーティング メトリックに基づいて RP1 と RP3 をそれぞれ使用するソースです。
- R11、R12、R2、R31 および R32 はレシーバです。 ユニキャスト ルーティング メトリックに基づいて、R11 と R12 は RP1 に加入し、R2 は RP2 と R31 に加入し、R32 は RP3 にそれぞれ加入します。

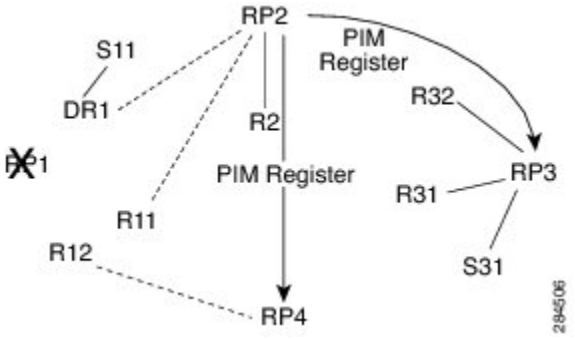


S11 がパケットの送信を開始すると、次のイベント シーケンスが発生します。

1. DR1 は（S, G）ステートを作成し、RP1 へ register を送信します。 DR1 はデータ パケットを register にカプセル化する場合もあります。
2. register を受信すると、RP1 は通常の PIM-SM RP 機能を実行し、パケットを R11 と R12 へ転送します。
3. RP1 は、register（データ パケットをカプセル化する場合もあります）を RP2、RP3、RP4 にも送信します。
4. RP2、RP3、RP4 がさらに register を相互に転送することはありません。
5. RP2、RP3、RP4 は通常の PIM-SM RP 機能を実行し、カプセル化されたデータ パケットがある場合、RP2 はデータ パケットを R2 に転送し、RP3 はデータ パケットを R31 と R32 にそれぞれ転送します。
6. DR1 から送信された null registers に対して上記の 5 ステップが繰り返されます。

PIMv6 エニーキャスト RP フェールオーバー

次の図は、PIM エニーキャスト RP フェールオーバーを示しています。



フェールオーバーでは、RP1 が到達可能な場合、次のことが実行されます。

- DR1 からの register は RP2 にトランスペアレントにルーティングされます。
- R11 は RP として RP2 を使用し、R12 は、RP として RP4 を使用します。
- DR1 からの register は RP2 から RP3 および RP4 にルーティングされます。

このように、RP の損失（この場合は RP1）は DR1、R11、および R12 に対してトランスペアレントであり、ネットワークは、IGP が収束するとすぐに収束します。

IPv6 BSR

IPv6 BSR

ドメイン内の PIM デバイスは、各マルチキャスト グループを正しい RP アドレスにマッピングできる必要があります。 PIM-SM 対応の BSR プロトコルは、グループと RP のマッピング情報をドメイン全体に迅速に配布するためのダイナミック適応メカニズムを備えています。 IPv6 BSR 機能を使用すると、到達不能になった RP が検出され、マッピング テーブルが変更されます。これにより、到達不能な RP が今後使用されなくなり、新しいテーブルがドメイン全体に迅速に配布されるようになります。

すべての PIM-SM マルチキャスト グループを RP の IP または IPv6 アドレスに関連付ける必要があります。 新しいマルチキャスト送信側が送信を開始すると、そのローカル DR がこれらのデータ パケットを PIM register メッセージにカプセル化し、そのマルチキャスト グループの RP に送信します。 新しいマルチキャスト受信側が加入すると、そのローカル DR がそのマルチキャスト グループの RP に PIM join メッセージを送信します。 PIM デバイスは、（*, G）join メッセージを送信するとき、RP 方向への次のデバイスを認識して、G（グループ）がそのデバイスにメッセージを送信できるようにする必要があります。 また、PIM デバイスは、（*, G）ステートを使用してデータ パケットを転送するとき、G を宛先としたパケットの正しい着信インターフェイスを認識する必要があります。これは、他のインターフェイスに着信するパケットを拒否する必要があるためです。

ドメイン内の少数のデバイスが候補ブートストラップ ルータ（C-BSR）として設定され、単一の BSR がそのドメイン用に選択されます。 また、ドメイン内の一連のデバイスが候補 RP（C-RP）として設定されます。通常、これらのデバイスは、C-BSR として設定されているものと同じデバイスです。 候補 RP は、候補 RP アドバタイズメント（C-RP-Adv）メッセージをそのドメインの BSR に定期的にユニキャストし、RP になる意思をアドバタイズします。 C-RP-Adv メッセージには、アドバタイズを行っている C-RP のアドレス、およびグループ アドレスとマスク長のフィールドの任意のリストが含まれています。これらのフィールドは、立候補のアドバタイズの対象となるグループ プレフィックスを示します。 BSR は、定期的に発信するブートストラップ メッセージ（BSM）にこれらの一連の C-RP とそれに対応するグループ プレフィックスを含めます。 BSM は、ドメイン全体にホップバイホップで配布されます。

双方向 BSR がサポートされているため、双方向 RP を C-RP メッセージおよび BSM の双方向範囲でアドバタイズできます。 システム内のすべてのデバイスは、BSM で双方向範囲を使用できる必要があります。使用できない場合は、双方向 RP 機能が機能しません。

IPv6 BSR：RP マッピングの設定

RP マッピングを設定するための IPv6 BSR 機能を使用すると、スコープと RP のマッピングを候補 RP メッセージから学習する代わりに、BSR から直接アナウンスするように、IPv6 マルチキャスト デバイスをスタティックに設定できます。 BSR から RP マッピングをアナウンスすると、次のいくつかの状況で役立ちます。

- RP が 1 つしか存在しないか、またはグループ範囲でエニーキャスト RP が使用されているために、RP アドレスが変わらない場合、候補 BSR で RP アドレス通知をスタティックに設定することは容易になります。
- RP アドレスが仮想 RP アドレスである場合（双方向 PIM を使用している場合など）、BSR はそのアドレスを候補 RP から学習できません。 その代わりに、候補 BSR で仮想 RP アドレスをアナウンス対象 RP として設定する必要があります。

IPv6 BSR：スコープ ゾーン サポート

BSR では、管理用スコープのマルチキャストを使用してネットワークでグループと RP のマッピングを配布することによって、限定スコープゾーンをサポートしています。ユーザは、ドメイン内の管理用スコープ領域ごとに候補 BSR と一連の候補 RP を設定できます。

BSR が管理用スコープで正しく機能するためには、BSR および少なくとも 1 つの C-RP がすべての管理用スコープ領域内に存在している必要があります。管理用スコープ ゾーンの境界は、ゾーン境界デバイスで設定する必要があります。これは、エラー条件が原因で境界を間違って越える可能性がある PIM join メッセージをフィルタリングする必要があるためです。 また、管理用スコープ ゾーン内の少なくとも 1 つの C-BSR が、管理用スコープ ゾーンのアドレス範囲の C-BSR になるように設定する必要があります。

BSR 選択は、（BSM を使用して）管理用スコープ範囲ごとに 1 回、およびグローバル範囲に対して 1 回行われるようになります。 管理用スコープ範囲は BSM で識別されます。これは、特定の RP セットで処理するように設定されている範囲だけでなく、管理用スコープ範囲であることを示すように、グループ範囲がマーク付けされているためです。

C-RP にスコープが設定されていない場合、その C-RP は、スコープ ゾーンのグループ範囲を含む選択 BSR から BSM を受信することによって、管理用スコープ ゾーンの有無およびそのグループ範囲を検出します。 C-RP には、各選択 BSR のアドレスとその BSM に含まれる管理用スコープ範囲が格納されます。 C-RPは、RPとして動作する意思のある管理用スコープ範囲ごとにC-RP-Advメッセージを適切な BSR に個別にユニキャストします。

管理用スコープ範囲が使用中の PIM ブートストラップ ドメイン内のすべての PIM デバイスが、BSM を受信し、該当するすべての管理用スコープ ゾーンに対する選択 BSR と RP のセットを格納できる必要があります。

IPv6 マルチキャスト：BSR パケットの RPF フラッディング

シスコの IPv6 デバイスでは、BSM のフローを妨げることがないように、BSR パケットの RPF フラッディングがサポートされています。 デバイスは、BSM を十分に認識および解析して、BSR アドレスを識別します。 デバイスは、このBSRアドレスのRPFチェックを実行し、RPFインターフェイスで受信したパケットだけを転送します。 また、RPF 情報を含むBSRエントリを作成し、同じ BSR からの今後の BSM に使用できるようにします。 特定の BSR から BSM を今後受信しなくなると、BSR エントリはタイムアウトします。

IPv6 マルチキャスト グループ

インターフェイスで IPv6 トラフィックを転送できるようにするには、そのインターフェイスで IPv6アドレスを設定する必要があります。 インターフェイスでサイトローカルまたはグローバル IPv6アドレスを設定すると、リンクローカル アドレスが自動的に設定され、そのインターフェイスに対してIPv6がアクティブになります。また、設定されたインターフェイスは、そのリンクに必要な次のマルチキャスト グループに自動的に加入します。

- インターフェイスに割り当てられたユニキャスト アドレスおよびエニーキャスト アドレスごとの請求ノード マルチキャスト グループ FF02:0:0:0:0:1:FF00::/104

（注） 送信要求ノード マルチキャスト アドレスは、ネイバー探索プロセスで使用されます。

- 全ノード リンクローカル マルチキャスト グループ FF02::1
- 全ルータ リンクローカル マルチキャスト グループ FF02::2

IPv6 マルチキャスト アドレス グループ範囲のサポート

この機能は、IPv6 マルチキャスト エッジ ルーティングにアクセス コントロール メカニズムを提供します。 ACL では、許可または拒否されるマルチキャスト グループまたはチャネルを指定します。 拒否されたグループまたはチャネルについて、デバイスはプロトコル トラフィックおよびアクションを無視し（たとえば、MLD ステートは作成されず、mroute ステートは作成されず、PIM join は転送されません）、システムのすべてのインターフェイス上でデータ トラフィックを

ドロップし、ACL によって拒否されたグループまたはチャネルのマルチキャストをディセーブルにします。

IPv6 ネットワークでの基本的な IP マルチキャストの設定方法

IPv6 マルチキャスト ルーティングのイネーブル化

IPv6 マルチキャストは、MLD バージョン 2 を使用します。 このバージョンの MLD には、MLD バージョン 1 との完全な下位互換性があります（*RFC 2710* で規定）。 MLD バージョン 1 だけをサポートするホストは、MLD バージョン 2 を実行しているデバイスと相互運用します。 MLD バージョン 1 ホストと MLD バージョン 2 ホストの両方が混在する LAN もサポートされています。

はじめる前に

最初に、IPv6 マルチキャスト ルーティングをイネーブルにするデバイスのすべてのインターフェイスで、IPv6 ユニキャスト ルーティングをイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 multicast-routing** [**vrf** *vrf-name*]

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ipv6 multicast-routing** [**vrf** *vrf-name*] 例： `Device(config)# ipv6 multicast-routing`	すべての IPv6 対応インターフェイスでマルチキャスト ルーティングをイネーブルにし、イネーブルになっているすべてのデバイス インターフェイスで PIM および MLD に対してマルチキャスト転送をイネーブルにします。 • IPv6 マルチキャスト ルーティングは、IPv6 ユニキャスト ルーティングがイネーブルの場合、デフォルトでディセーブルです。 特定のデバイスでは、IPv6 ユニキャスト ルーティングを使用するには、IPv6 マルチキャスト ルーティングもイネーブルにする必要があります。

デバイスでの未認証マルチキャストトラフィックの受信のディセーブル化

状況によっては、アクセスコントロールプロファイルに従って加入者の認証とチャネルの許可が行われていないかぎり、マルチキャスト トラフィックの受信を防止することが必要となる場合があります。 つまり、アクセス コントロール プロファイルで特に指定がなければ、トラフィックを完全になくす必要があります。

未認証グループまたは未許可チャネルからマルチキャスト トラフィックをデバイスが受信しないようにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 multicast** [**vrf** *vrf-name*] **group-range**[*access-list-name*]

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 multicast** [**vrf** *vrf-name*] **group-range**[*access-list-name*] 例： `Device(config)# ipv6 multicast group-range`	デバイスのすべてのインターフェイスで未許可グループまたはチャネルのマルチキャスト プロトコル アクションおよびトラフィック転送をディセーブルにします。

IPv6 マルチキャストのトラブルシューティング

手順の概要

1. **enable**
2. **debug ipv6 mfib** *group-name* | *group-address*] [**adjacency** | **signal** | **db** | **init** | **mrib** | **pak** | **ps**
3. debug ipv6 mld [group-name | group-address | interface-type]
4. **debug ipv6 mld explicit** [*group-name* | *group-address*
5. **debug ipv6 pim** [*group-name* | *group-address* | *interface-type* | **neighbor** | **bsr**
6. **debug bgp ipv6** {**unicast** | **multicast**} **dampening** [**prefix-list** *prefix-list-name*
7. **debug bgp ipv6** {**unicast** | **multicast**} **updates** [*ipv6-address*] [**prefix-list** *prefix-list-name*] [**in** | **out**
8. **debug ipv6 mrib client**
9. **debug ipv6 mrib io**
10. **debug ipv6 mrib issu**
11. **debug ipv6 mrib proxy**
12. **debug ipv6 mrib route** [*group-name* | *group-address*
13. **debug ipv6 mrib table**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**debug ipv6 mfib** *group-name* | *group-address*] [**adjacency** | **signal** | **db** | **init** | **mrib** | **pak** | **ps** 例： `Device# debug ipv6 mfib pak FF04::10`	IPv6 MFIB に対するデバッグ出力をイネーブルにします。
ステップ 3	debug ipv6 mld [group-name | group-address | interface-type] 例： `Device# debug ipv6 mld`	MLD プロトコル アクティビティに対するデバッグをイネーブルにします。
ステップ 4	**debug ipv6 mld explicit** [*group-name* | *group-address* 例： `Device# debug ipv6 mld explicit`	ホストの明示的トラッキングに関連する情報を表示します。
ステップ 5	**debug ipv6 pim** [*group-name* | *group-address* | *interface-type* | **neighbor** | **bsr** 例： `Device# debug ipv6 pim`	PIM プロトコル アクティビティに対するデバッグをイネーブルにします。
ステップ 6	**debug bgp ipv6** {**unicast** | **multicast**} **dampening** [**prefix-list** *prefix-list-name* 例： `Device# debug bgp ipv6 multicast`	IPv6 BGP 減衰のデバッグ メッセージを表示します。
ステップ 7	**debug bgp ipv6** {**unicast** | **multicast**} **updates** [*ipv6-address*] [**prefix-list** *prefix-list-name*] [**in** | **out** 例： `Device# debug bgp ipv6 multicast updates`	IPv6 BGP アップデート パケットのデバッグ メッセージを表示します。
ステップ 8	**debug ipv6 mrib client** 例： `Device# debug ipv6 mrib client`	MRIB クライアント管理アクティビティに対するデバッグをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 9	**debug ipv6 mrib io** 例： `Device# debug ipv6 mrib io`	MRIB I/O イベントに対するデバッグをイネーブルにします。
ステップ 10	**debug ipv6 mrib issu** 例： `Device# debug ipv6 mrib issu`	MRIB 稼働中ソフトウェア アップデートに対するデバッグをイネーブルにします。
ステップ 11	**debug ipv6 mrib proxy** 例： `Device# debug ipv6 mrib proxy`	分散型デバイスにおけるルート プロセッサとラインカード間の MRIB プロキシ アクティビティに対するデバッグをイネーブルにします。
ステップ 12	**debug ipv6 mrib route** [*group-name* | *group-address* 例： `Device# debug ipv6 mrib route`	MRIB ルーティング エントリ関連のアクティビティに関する情報を表示します。
ステップ 13	**debug ipv6 mrib table** 例： `Device# debug ipv6 mrib table`	MRIB テーブル管理アクティビティに対するデバッグをイネーブルにします。

PIMv6 エニーキャスト RP の設定

このタスクでは、2 つの PIMv6 RP ピアをイネーブル化する方法について説明します。 ステップ 3～11 は RP1 の設定を示し、ステップ 12～19 は RP2 の設定を示しています。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*] [**bidir**]
4. **interface** *type number*
5. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*}
6. **no shut**
7. **interface** *type number*
8. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*}
9. **no shut**
10. **exit**
11. **ipv6 pim anycast-RP** *rp-address peer-address*
12. **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*] [**bidir**]
13. **interface** *type number*
14. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*}
15. **no shut**
16. **interface** *type number*
17. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*}
18. **no shut**
19. **ipv6 pim anycast-RP** *rp-address peer-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*] [**bidir**] 例： `Device(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1`	特定のグループ範囲の PIM RP のアドレスを設定します。

	コマンドまたはアクション	目的
ステップ 4	**interface** *type number* 例： `Device(config)# interface Loopback4`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 5	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*} 例： `Device(config-if)# ipv6 address 2001:DB8::4:4/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 6	**no shut** 例： `Device(config-if)# no shut`	インターフェイスをイネーブルにします。
ステップ 7	**interface** *type number* 例： `Device(config-if)# interface Loopback5`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 8	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*} 例： `Device(config-if)# ipv6 address 2001:DB8:0:ABCD::1/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 9	**no shut** 例： `Device(config-if)# no shut`	インターフェイスをイネーブルにします。
ステップ 10	**exit** 例： `Device(config-if)# exit`	このコマンドを入力してインターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 11	**ipv6 pim anycast-RP** *rp-address peer-address* 例： `Device(config)# ipv6 pim anycast-rp 2001:DB8:0:ABCD::1 2001:DB8::3:3`	このコマンドを使用して、エニーキャスト グループ範囲の PIM RP のアドレスを設定します。

	コマンドまたはアクション	目的
ステップ 12	**ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*] [**bidir**] 例： `Device(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1`	特定のグループ範囲の PIM RP のアドレスを設定します。
ステップ 13	**interface** *type number* 例： `Device(config)# interface Loopback4`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 14	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*} 例： `Device(config-if)# ipv6 address 2001:DB8::3:3/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 15	**no shut** 例： `Device(config-if)# no shut`	インターフェイスをイネーブルにします。
ステップ 16	**interface** *type number* 例： `Device(config-if)# interface Loopback5`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 17	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*} 例： `Device(config-if)# ipv6 address 2001:DB8:0:ABCD::1/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 18	**no shut** 例： `Device(config-if)# no shut`	インターフェイスをイネーブルにします
ステップ 19	**ipv6 pim anycast-RP** *rp-address peer-address* 例： `Device(config-if)# ipv6 pim anycast-rp 2001:DB8::1:1 2001:DB8::4:4`	このコマンドを使用して、エニーキャスト グループ範囲の PIM RP のアドレスを設定します。

BSR の設定および BSR 情報の確認

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address*[*hash-mask-length*] [**priority** *priority-value*]
4. **interface** *type number*
5. **ipv6 pim bsr border**
6. **end**
7. **show ipv6 pim** [**vrf** *vrf-name*] **bsr** {**election** | **rp-cache** | **candidate-rp**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 pim** [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address*[*hash-mask-length*] [**priority** *priority-value*] 例： `Device(config)# ipv6 pim bsr candidate bsr 2001:DB8:3000:3000::42 124 priority 10`	候補 BSR になるようにデバイスを設定します。
ステップ 4	**interface** *type number* 例： `Device(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 5	**ipv6 pim bsr border** 例： `Device(config-if)# ipv6 pim bsr border`	指定したインターフェイスの任意のスコープの全 BSM に対して境界を設定します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ipv6 pim** [**vrf** *vrf-name*] **bsr** {**election** | **rp-cache** | **candidate-rp**} 例： `Device# show ipv6 pim bsr election`	PIM BSR プロトコル処理に関連する情報を表示します。

BSR への PIM RP アドバタイズメントの送信

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]
4. **interface** *type number*
5. **ipv6 pim bsr border**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 pim** [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority**	BSR に PIM RP アドバタイズメントを送信します。

	コマンドまたはアクション	目的
	priority-value] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**] 例： `Device(config)# ipv6 pim bsr candidate rp 2001:DB8:3000:3000::42 priority 0`	
ステップ 4	**interface** *type number* 例： `Device(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 5	**ipv6 pim bsr border** 例： `Device(config-if)# ipv6 pim bsr border`	指定したインターフェイスの任意のスコープの全 BSM に対して境界を設定します。

限定スコープ ゾーン内で BSR を使用できるようにするための設定

ユーザは、ドメイン内の管理用スコープ領域ごとに候補 BSR と一連の候補 RP を設定できます。

候補 RP でスコープが指定されている場合、このデバイスは指定されたスコープの BSR に自身を C-RP 専用としてアドバタイズします。 スコープとともにグループ リストが指定されている場合は、そのグループ リストと同じスコープが指定されたアクセス リスト内のプレフィックスだけがアドバタイズされます。

ブートストラップ デバイスでスコープが指定されている場合、その BSR はそのスコープに関連付けられているグループ範囲を含む BSM の起点となり、指定されたスコープに属するグループに対する C-RP 通知を受け入れます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*]
4. **ipv6 pim** [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]
5. **interface** *type number*
6. **ipv6 multicast boundary scope** *scope-value*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 pim** [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] 例： `Device(config)# ipv6 pim bsr candidate bsr 2001:DB8:1:1:4`	候補BSRになるようにデバイスを設定します。
ステップ 4	**ipv6 pim** [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**] 例： `Device(config)# ipv6 pim bsr candidate rp 2001:DB8:1:1:1 group-list list scope 6`	BSR に PIM RP アドバタイズメントを送信するように候補 RP を設定します。
ステップ 5	**interface** *type number* 例： `Device(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 6	**ipv6 multicast boundary scope** *scope-value* 例： `Device(config-if)# ipv6 multicast boundary scope 6`	指定されたスコープのインターフェイスでマルチキャスト境界を設定します。

BSR デバイスにスコープと RP のマッピングをアナウンスさせるための設定

IPv6 BSR デバイスは、スコープと RP のマッピングを候補 RP メッセージから学習するのではなく、直接アナウンスするようにスタティックに設定できます。 ユーザは、スコープと RP のマッピングをアナウンスするように BSR デバイスを設定して、BSR をサポートしていない RP がその BSR にインポートされるように設定できます。 この機能をイネーブルにすると、ローカルの候補 BSR デバイスの既知のリモート RP が、企業の BSR ドメインの外部に配置されている RP を学習できるようになります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **bsr announced rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**bidir**] [**scope** *scope-value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 pim** [**vrf** *vrf-name*] **bsr announced rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**bidir**] [**scope** *scope-value*] 例： `Device(config)# ipv6 pim bsr announced rp 2001:DB8:3000:3000::42 priority 0`	指定した候補 RP の BSR からスコープと RP のマッピングを直接アナウンスします。

IPv6 ネットワークでの基本的な IP マルチキャストの設定例

例：IPv6 マルチキャスト ルーティングのイネーブル化

次に、すべてのインターフェイスでマルチキャスト ルーティングをイネーブルにし、イネーブルになっているすべてのデバイス インターフェイスで PIM および MLD に対してマルチキャスト転送をイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 multicast-routing
```

例：IPv6マルチキャストアドレスグループ範囲のサポートのディセーブル化

次の例では、list2 という名前のアクセス リストによって拒否されたグループまたはチャネルのマルチキャストをデバイスでディセーブルにできます。

```
ipv6 multicast group-range list2
```

次に、上記の例のコマンドが int2 で指定されたインターフェイス上で上書きされる例を示します。int2 で、MLD ステートは int-list2 によって許可されるグループまたはチャネルに対して作成されますが、int-list2 によって拒否されるグループまたはチャネルに対しては作成されません。他のすべてのインターフェイスでは、list2 という名前のアクセスリストがアクセス コントロールに使用されます。

この例では、すべてあるいはほとんどのマルチキャスト グループまたはチャネルを拒否するように list2 を指定でき、インターフェイス int2 に対してのみ許可グループまたはチャネルを許可するように int-list2 を指定できます。

```
Device(config)# interface int2
Device(config-if)# ipv6 mld access-group int-list2
```

例：IPv6 MRIB 情報の確認

次の例では、IPv6 MRIB クライアントに関する情報を示します。

```
Device# show ipv6 mrib client

IP MRIB client-connections
igmp:145        (connection id 0)
pim:146 (connection id 1)
mfib ipv6:3     (connection id 2)
slot 3  mfib ipv6 rp agent:16   (connection id 3)
slot 1  mfib ipv6 rp agent:16   (connection id 4)
slot 0  mfib ipv6 rp agent:16   (connection id 5)
```

```
slot 4  mfib ipv6 rp agent:16   (connection id 6)
slot 2  mfib ipv6 rp agent:16   (connection id 7)
```

次の例では、IPv6 MRIB ルートに関するサマリー情報を示します。

```
Device# show ipv6 mrib route summary

MRIB Route-DB Summary
  No. of (*,G) routes = 52
  No. of (S,G) routes = 0
  No. of Route x Interfaces (RxI) = 10
```

例：PIMv6 エニーキャスト RP の設定

```
RP1
Device1(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1
Device1(config)# interface Loopback4
Device1(config-if)# ipv6 address 2001:DB8::4:4/64
Device1(config-if)# no shut

Device1(config)# interface Loopback5
Device1(config-if)# ipv6 address 2001:DB8:0:ABCD::1/64
Device1(config-if)# no shut
Device1(config-if)# exit
Device1(config)# ipv6 pim anycast-rp 2001:DB8:0:ABCD::1 2001:DB8::3:3

RP2 (Anycast RP Peer)
Device2(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1
Device2(config)# interface Loopback4
Device2(config-if)# ipv6 address 2001:DB8::3:3/64
Device2(config-if)# no shut

Device2(config)# interface Loopback5
Device2(config-if)# ipv6 address 2001:DB8:0:ABCD::1/64
Device2(config-if)# no shut
Device2(config)# ipv6 pim anycast-rp 2001:DB8::1:1 2001:DB8::4:4
```

```
Device2 show ipv6 pim anycast-rp 2001:DB8::1:1

Anycast RP Peers For 2001:DB8::1:1   Last Register/Register-Stop received
  2001:DB8::3:3 00:00:00/00:00:00
  2001:DB8::4:4 00:00:00/00:00:00
```

例：BSR の設定

```
Device# show ipv6 pim bsr election

PIMv2 BSR information
BSR Election Information
Scope Range List: ff00::/8
This system is the Bootstrap Router (BSR)
BSR Address: 60::1:1:4
Uptime: 00:11:55, BSR Priority: 0, Hash mask length: 126
RPF: FE80::A8BB:CCFF:FE03:C400,Ethernet0/0
BS Timer: 00:00:07
This system is candidate BSR
Candidate BSR address: 60::1:1:4, priority: 0, hash mask length: 126
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 用 RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 ネットワークでの基本的な IP マルチキャスト設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *4* : *IPv6* ネットワークでの基本的な *IP* マルチキャスト設定の機能情報

機能名	リリース	機能情報
IPv6 マルチキャスト	12.0(26)S 12.2(25)SG 12.2(33)SRA 12.2(18)SXE 12.3(2)T 12.4 12.4(2)T 15.0(2)SE Cisco IOS XE Release 2.1	IPv6マルチキャストを使用すると、ホストがすべてのホストのサブセットに同時に単一のデータ ストリームを送信できるようになります。 次のコマンドが導入または変更されました。**clear ipv6 pim topology**、**debug ipv6 mld**、**debug ipv6 mrib**、**debug ipv6 pim**、**debug ipv6 pim neighbor**、**ipv6 mld join-group**、 **ipv6 mld query-interval**、**ipv6 mld query-max-response-time**、**ipv6 mld query-timeout**、**ipv6 mld router**、**ipv6 mld static-group**、**ipv6 multicast-routing** 、**ipv6 pim**、**ipv6 pim dr-priority**、**ipv6 pim hello-interval**、**ipv6 pim rp-address** 、**ipv6 pim spt-threshold infinity** 、**show ipv6 mld groups**、**show ipv6 mld groups summary**、**show ipv6 mld interface**、**show ipv6 mrib client**、**show ipv6 mrib route**、**show ipv6 mroute**、**show ipv6 pim group-map**、**show ipv6 pim interface**、**show ipv6 pim neighbor**、**show ipv6 pim range-list**、**show ipv6 pim topology**、**show ipv6 pim tunnel**。

機能名	リリース	機能情報
IPv6 マルチキャスト アドレス グループ範囲のサポート	15.0(1)M 12.2(40)SG 3.2.0SG 15.0(2)SG 12.2(33)SRE 12.2(33)SXI Cisco IOS XE Release 2.6	この機能は、グループ範囲のディセーブル化とも呼ばれます。 この機能は、IPv6マルチキャスト エッジ ルーティングにアクセス コントロール メカニズムを提供します。 次のコマンドが導入または変更されました。**ipv6 mld access-group**、**ipv6 multicast boundary scope**、**ipv6 multicast group-range**。
IPv6マルチキャスト：スコープ境界	12.0(26)S 12.2(18)S 12.2(25)SG 12.2(33)SRA 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IPv6 では、グローバル アドレスと非グローバル アドレスがサポートされています。 ここでは、異なるスコープの IPv6 アドレスの使用方法について説明します。
PIMv6：エニーキャスト RP ソリューション	15.1(3)S Cisco IOS XE Release 3.4S 15.2(3)T	IPv6 PIM のエニーキャスト RP ソリューションでは、IPv6ネットワークで PIM-SM RP に対するエニーキャスト サービスのサポートが可能になり、PIMのみを実行しているドメイン内でエニーキャスト RP を使用できます。 次のコマンドが導入または変更されました。**ipv6 pim anycast-RP**、**show ipv6 pim anycast-RP**。

機能名	リリース	機能情報
IPv6マルチキャスト：ブートストラップ ルータ	12.0(28)S 12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.3(11)T 12.4 12.4(2)T Cisco IOS XE Release 2.4 15.0(1)S	この機能を使用すると、到達不能になった RP が検出され、マッピング テーブルが変更されます。これにより、到達不能な RP が今後使用されなくなり、新しいテーブルがドメイン全体に迅速に配布されるようになります。 次のコマンドが導入または変更されました。**debug ipv6 pim bsr**、**ipv6 pim bsr border**、**ipv6 pim bsr candidate bsr**、**ipv6 pim bsr candidate rp**、**show ipv6 pim bsr**、**show ipv6 pim group-map**。
IPv6 BSR：RP マッピングの設定	12.2(33)SRE 12.2(50)SY 12.4(2)T Cisco IOS XE Release 2.4 15.0(1)S	この機能を使用すると、スコープとRPのマッピングを候補RPメッセージから学習する代わりに、BSRから直接アナウンスするように、IPv6マルチキャストデバイスをスタティックに設定できます。 次のコマンドが導入または変更されました。**ipv6 multicast-routing**、**ipv6 pim bsr announced rp**、**ipv6 pim bsr candidate bsr**。
IPv6 マルチキャスト：BSR パケットの RPF フラッディング	Cisco IOS XE Release 2.1	BSR パケット機能の RPF フラッディングを使用すると、Cisco IPv6 デバイスが BSM のフローを妨げることがなくなります。 次のコマンドが導入されました。**show ipv6 pim bsr**。

機能名	リリース	機能情報
IPv6 マルチキャスト VRF Lite	15.1(4)M Cisco IOS XE Release 3.4S	この機能は、複数の仮想ルーティング/転送コンテキスト（VRF）に対する IPv6 マルチキャスト サポートを提供します（これらの VRF のスコープは、VRF が定義されているデバイスに制限されています）。

第 4 章

MSDPを使用しての複数のPIM-SMドメインの相互接続

このモジュールでは、Multicast Source Discovery Protocol（MSDP）を使用した複数の PIM-SM ドメインの相互接続に関連する作業について説明します。 作業では、MSDP のピア、メッシュ グループ、およびデフォルト ピアを設定する方法、フィルタを使用して MSDP のアクティビティを制御し、範囲を設定する方法、およびMSDPをモニタリングし、維持する方法を説明します。 MSDP を PIM-SM と併用することで、複数の PIM-SM ドメインを簡単に接続できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

MSDP を使用して複数の PIM-SM ドメインを相互接続する前提条件

MSDP を設定する前に、すべての MSDP ピアのアドレスがボーダー ゲートウェイ プロトコル（BGP）で認識されている必要があります。

MSDP を使用して複数の PIM-SM ドメインを相互接続するための情報

MSDP を使用して複数の PIM-SM ドメインを相互接続することの利点

- ランデブー ポイント（RP）でドメイン外のアクティブなソースを動的に検出できます。
- 複数のドメイン間でマルチキャスト配信ツリーを構築するためのさらに管理しやすいアプローチを導入できます。

複数の PIM-SM ドメインを相互接続するための MSDP の使用

MSDP は、複数の PIM-SM ドメインを接続するメカニズムです。 MSDP の目的は、他の PIM ドメイン内のマルチキャスト ソースを検出することです。 MSDP の主な利点は、PIM-SM ドメインで（共通の共有ツリーではなく）ドメイン間ソース ツリーを使用することで、複数の PIM-SM ドメインを簡単に相互接続できることです。 MSDP がネットワークで設定されている場合、RP は他のドメインの RP とソース情報を交換します。 RP は、レシーバがいるグループに送信するソースのドメイン間ソース ツリーに参加できます。 これができるのは、RP が、アクティブなレシーバが存在するドメイン内のすべてのポイントへのブランチがある、ドメイン内の共有ツリーのルートであるためです。 ラスト ホップ ルータは（共有ツリー下のソースからのマルチキャスト パケットの着信によって）PIM-SM ドメイン外の新しいソースを学習すると、ソースに加入を送信し、ドメイン間ソース ツリーに参加できます。

（注） RP に特定のグループの共有ツリーがないか、または RP の共有ツリーの発信インターフェイス リストが空の場合は、別のドメイン内のソースに加入を送信しません。

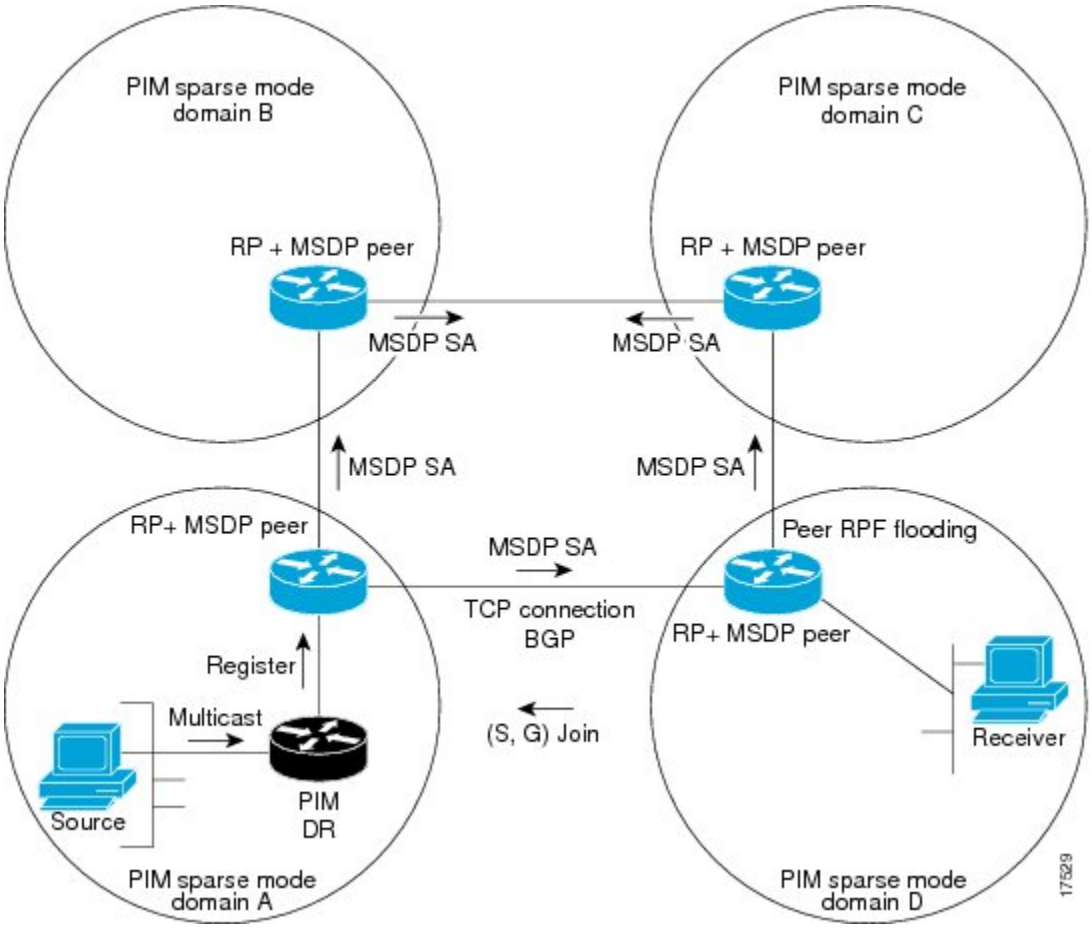
MSDP がイネーブルになっている場合、PIM-SM ドメインの RP は、他のドメインの MSDP 対応ルータとの MSDP ピアリング関係を維持します。 このピアリング関係は TCP 接続を通じて発生し、主にマルチキャスト グループに送信するソースのリストが交換されます。 MSDP は、ピアリング接続に TCP（ポート 639）を使用します。 BGP と同様に、ポイントツーポイント TCP ピアリングを使用することは、各ピアを明示的に設定する必要があることを意味します。 また、RP 間

の TCP 接続は、基本的なルーティング システムによって実現されます。 受信側の RP では、送信元リストを使用して送信元のパスが確立されます。 マルチキャスト ソースがレシーバがいるドメインの対象である場合、マルチキャスト データは PIM-SM で提供される通常のソース ツリー構築メカニズムを使用して配信されます。 MSDP は、グループを送信する送信元のアナウンスにも使用されます。 これらのアナウンスは、ドメインの RP で発信する必要があります。

（注） MSDP は、ドメイン間の動作に関して BGP またはマルチプロトコル BGP（MBGP）に依存しています。 グローバル マルチキャスト グループに送信する RP で MSDP を実行することを推奨します。

図に、2 つの MSDP ピア間で動作する MSDP を示します。 PIM では、ドメインの RP に送信元を登録するための標準メカニズムとして、MSDP が使用されます。

図 *11*：*RP* ピア間で動作する *MSDP*



MSDP が実装されている場合、次のイベント シーケンスが発生します。

1 図に示すように、PIM 指定ルータ（DR）が RP にソースを登録すると、RP はその MSDP ピアすべてに Source-Active（SA）メッセージを送信します。

（注） DR は、（ソースがアクティブになると）カプセル化されたデータをソースごとに 1 回だけ RP に送信します。 ソースがタイムアウトした場合、ソースが再度アクティブになるとこのプロセスが実行されます。 この状況は、発信側の RP に登録されたすべてのソースを含む定期的な SA メッセージとは異なります。 これらの SA メッセージは MSDP の制御パケットで、そのため、アクティブなソースからのカプセル化されたデータは含まれません。

1. SA メッセージでは、ソース アドレス、ソースの送信先グループ、および RP のアドレスまたは発信者 ID が識別されます（設定されている場合）。
2. SA メッセージを受信する各 MSDP ピアは、発信者からのダウンストリームのすべてのピアに SA メッセージをフラッディングします。 場合によっては（図のように PIM-SM ドメイン B および C に RP がある場合など）、RP は複数の MSDP ピアから SA メッセージのコピーを受信することがあります。 ループが作成されないように、RP は BGP ネクスト ホップ データベースに問い合わせて、SA メッセージの発信者へのネクスト ホップを識別します。 MBGP とユニキャスト BGP の両方が設定されている場合、最初に MBGP がチェックされ、次にユニキャスト BGP がチェックされます。 そのネクスト ホップ ネイバーは発信者の RPF ピアです。 RPF ピアとのインターフェイス以外のインターフェイスの発信者から受信した SA メッセージはドロップされます。 そのため、SA メッセージ フラッディング プロセスはピア RPF フラッディングと呼ばれます。 ピア RPF フラッディング メカニズムにより、BGP または MBGP は MSDP とともに実行する必要があります。

（注） （M）BGP は、MSDP メッシュ グループのシナリオでは必要ありません。 MSDP メッシュ グループの詳細については、MSDP メッシュ グループの設定, （137 ページ）のセクションを参照してください。

（注） （M）BGP は、デフォルト MSDP ピアのシナリオまたは MSDP ピアが 1 つだけ設定されているシナリオでは必要ありません。 詳細については、デフォルトの MSDP ピアの設定, （136 ページ）のセクションを参照してください。

1. RP は SA メッセージを受信すると、グループ（*, G）の発信インターフェイス リストにインターフェイスがあるかどうかを確認して、アドバタイズされたグループのメンバがドメイン内にあるかどうかを確認します。 グループ メンバが存在しない場合、RP は何も実行しません。 グループ メンバが存在する場合、RP はソースに対して（S,G）加入を送信します。 その結果、RP へのドメイン間のブランチが自律システムの境界を越えて構築されます。 マルチキャスト パケットは、RP に着信すると、その共有ツリーを経由して RP のドメイン内のグループ メンバに転送されます。 メンバの DR は、標準的な PIM-SM 手順を使用してソースへのランデブー ポイント ツリー（RPT）に加入することもできます。
2. 発信側の RP は、ソースがグループにパケットを送信している限り、（S, G）ステートの定期的な SA メッセージを 60 秒ごとに送信し続けます。 RP は SA メッセージを受信すると、SA

メッセージをキャッシュします。 たとえば、RP が発信側の RP 10.5.4.3 から（172.16.5.4、228.1.2.3）の SA メッセージを受信するとします。 RP は mroute テーブルに問い合わせて、グループ 228.1.2.3 にアクティブ メンバがないことを検出するため、10.5.4.3 のダウンストリームのピアに SA メッセージを渡します。 ドメイン内のホストがグループ 228.1.2.3 の RP に加入を送信すると、RP はホストへのインターフェイスを（*, 224.1.2.3）エントリの発信インターフェイス リストに追加します。 RP は SA メッセージをキャッシュするため、ルータは (172.16.5.4, 228.1.2.3) のエントリを持ち、ホストが加入を要求するとすぐにソース ツリーに加入できます。

（注） 現行のすべてのサポートされているソフトウェア リリースでは、MSDP SA メッセージのキャッシュは必須であり、手動でイネーブルまたはディセーブルにすることはできません。 デフォルトでは、MSDP ピアが設定されると、**ip multicast cache-sa-state** コマンドが自動的に実行コンフィギュレーションに追加されます。

MSDP メッセージ タイプ

それぞれ独自のタイプ、長さ、値（TLV）データ形式で符号化された 4 つの基本的な MSDP メッセージ タイプがあります。

SA メッセージ

SA メッセージは、ドメイン内のアクティブなソースをアドバタイズするために使用されます。また、これらの SA メッセージには、ソースから送信された初期マルチキャスト データ パケットが含まれる場合があります。

SA メッセージには、発信側の RP の IP アドレスおよびアドバタイズされる 1 つまたは複数の（S, G）ペアが含まれます。 また、SA メッセージにはカプセル化されたデータ パケットが含まれることがあります。

（注） SA メッセージの詳細については、SA メッセージの発信、受信、および処理, （112 ページ）を参照してください。

SA 要求メッセージ

SA 要求メッセージは、特定のグループのアクティブなソースのリストを要求するために使用されます。 これらのメッセージは、SA キャッシュにアクティブな（S, G）ペアのリストを保持する MSDP SA キャッシュに送信されます。 参加遅延は、発信側の RP によって再度アドバタイズされるグループ内のすべてのアクティブなソースに対して最大 60 秒待機するのではなく、SA 要求メッセージを使用してグループのアクティブなソースのリストを要求することで低減できます。

（注） SA 要求メッセージの詳細については、MSDP ピアへのソース情報の要求，（143 ページ）を参照してください。

SA 応答メッセージ

SA 応答メッセージは、SA 要求メッセージに応じて MSDP ピアによって送信されます。 SA 応答メッセージには、発信側 RP の IP アドレス、およびキャッシュに格納されている発信側 RP のドメイン内のアクティブなソースの（S, G）ペアが 1 つまたは複数含まれます。

（注） SA 応答メッセージの詳細については、SA 要求フィルタを使用した MSDP ピアからの発信 SA 要求メッセージに対する応答の制御，（145 ページ）を参照してください。

キープアライブ メッセージ

キープアライブ メッセージは、MSDP セッションをアクティブにしておくために 60 秒ごとに送信されます。 キープアライブ メッセージまたは SA メッセージが 75 秒間受信されない場合、MSDP セッションはリセットされます。

（注） キープアライブ メッセージの詳細については、MSDP キープアライブ インターバルおよび保留時間インターバルの調整，（133 ページ）を参照してください。

SA メッセージの発信、受信、および処理

ここでは SA メッセージの発信、受信、および処理について詳しく説明します。

SA メッセージの発信

SA メッセージは、ローカル PIM-SM ドメイン内で新しいソースがアクティブになると、RP によってトリガーされます（MSDP が設定されている場合）。 ローカル ソースは、RP に直接接続されているソース、または登録されているファースト ホップ DR です。 RP は、PIM-SM ドメイン内のローカル ソース、つまり RP に登録されているローカル ソースの SA メッセージだけを発信します。

（注） ローカル ソースは、RP の（S, G）mroute エントリに設定されている A フラグによって示されます（**show ip mroute** コマンドの出力で確認できます）。 このフラグは、ソースが、RP が他の MSDP ピアにアドバタイズする候補であることを示します。

ソースがローカル PIM-SM ドメイン内にある場合、RP に（S, G）ステートが作成されます。 新しいソースは、登録メッセージを受信するか、直接接続されているソースから最初の（S,G）パケットが着信することによって RP で検出されます。 ソースから送信された最初のマルチキャスト パケット（登録メッセージにカプセル化されるか、直接接続されているソースから受信します）は、最初の SA メッセージにカプセル化されます。

SA メッセージの受信

SA メッセージは、発信者への最良パスにある MSDP RPF ピアからに限り受け入れられます。 他の MSDP ピアから着信する同じ SA メッセージは無視する必要があり、無視しないと、SA ループが発生することがあります。 着信 SA メッセージの MSDP RPF ピアを選択するには、MSDP トポロジの知識が必要です。 ただし、MSDP はルーティング アップデートの形式でトポロジ情報を送信しません。 MSDP は、SA RPF チェック メカニズムに（M）BGP ルーティング データを MSDP トポロジの最適な近似データとして使用して、この情報を推測します。 したがって、MSDP トポロジは BGP ピア トポロジと同じ汎用トポロジに従う必要があります。 いくつかの例外（デフォルト MSDP ピア、MSDP メッシュ グループの MSDP ピアなど）を除いて、MSDP ピアは、一般に（M）BGP ピアにする必要があります。

RPF チェック ルールを SA メッセージに適用する方法

SA メッセージの RPF チェックに適用されるルールは、MSDP ピア間の BGP ピアリングによって異なります。

- ルール 1：送信側の MSDP ピアが Interior (M)BGP（i（M）BGP）ピアでもある場合に適用されます。
- ルール 2：送信側の MSDP ピアが Exterior（M）BGP（e（M）BGP）ピアでもある場合に適用されます。
- ルール 3：送信側の MSDP ピアが（M）BGP ピアでない場合に適用されます。

RPF チェックは次の場合は実行されません。

- 送信側の MSDP ピアが唯一の MSDP ピアである場合。これは、MSDP ピアが 1 つだけまたはデフォルト MSDP ピアだけが設定されている場合です。
- 送信側の MSDP ピアがメッシュ グループのメンバである場合。
- 送信側の MSDP ピアのアドレスが SA メッセージに含まれる RP アドレスである場合

ソフトウェアが RPF チェックに適用するルールを決定する方法

ソフトウェアは、次の論理で RPF チェックに適用する RPF ルールを決定します。

- 送信側の MSDP ピアと同じ IP アドレスを持つ（M）BGP ネイバーを検索します。
  - 一致した（M）BGP ネイバーが Internal BGP（iBGP）ピアである場合、ルール 1 を適用します。
  - 一致した（M）BGP ネイバーが External BGP（eBGP）ピアである場合、ルール 2 を適用します。
  - 一致するネイバーが見つからなかった場合、ルール 3 を適用します。

RPF チェックのルールの選択では、デバイスの MSDP ピアを設定するために使用される IP アドレスが同じデバイスの（M）BGP ピアを設定するために使用される IP アドレスと一致していることが前提になっています。

MSDP の SA メッセージの RPF チェックのルール 1

送信側の MSDP ピアが i（M）BGP ピアでもある場合、MSDP の RPF チェックのルール 1 が適用されます。 ルール 1 が適用されると、RPF チェックは次のように行われます。

1. ピアは、BGP マルチキャスト ルーティング情報ベース（MRIB）を検索して SA メッセージを発信した RP への最適パスを探します。 MRIB でパスが検出されなかった場合、ピアはユニキャスト ルーティング情報ベース（URIB）を検索します。 それでもパスが検出されなかった場合は、RPF チェックは失敗します。
2. 検索が成功した場合（最適パスが検出された場合）、ピアはこの最適パスの BGP ネイバーのアドレスを決定します。このアドレスは、ピアに BGP アップデート メッセージでパスを送信した BGP ネイバーのアドレスになります。

（注） BGP ネイバー アドレスは、パス内のネクスト ホップ アドレスと同じではありません。i（M）BGP ピアはパスのネクスト ホップ属性を更新しないため、ネクスト ホップ アドレスは通常、パスを送信した BGP ピアのアドレスと同じではありません。

（注） BGP ネイバー アドレスは、ピアにパスを送信したピアの BGP ID と同じでなくても構いません。

1. 送信側の MSDP ピアの IP アドレスが BGP ネイバー アドレス（ピアにパスを送信した BGP ピアのアドレス）と同じである場合、RPF チェックは正常に終了します。同じでない場合は、RPF チェックは失敗します。

RPF チェックのルール 1 の MSDP への影響

MSDP トポロジでは、（M）BGP トポロジをミラーリングする必要があります。 一般に、2 台のデバイス間に i（M）BGP ピア接続がある場合は、必ず MSDP ピア接続を設定する必要があります。 つまり、遠端 MSDP ピア接続の IP アドレスは、遠端 i（M）BGP ピア接続と同じにする必要があります。 自律システム内の i（M）BGP ピア間の BGP トポロジは AS パスでは記述されないため、アドレスを同じにする必要があります。 別の i（M）BGP ピアへのアップデートの送信時に i（M）BGP ピアがパス内のネクスト ホップ アドレスをアップデートした場合、ピアはネクスト ホップ アドレスを使用して i（M）BGP トポロジ（したがって MSDP トポロジ）を表すことができます。ただし、i（M）BGP ピアのデフォルトの動作はネクストホップアドレスをアップデートしないため、ピアはネクスト ホップ アドレスを使用して（M）BGP トポロジ（MSDP トポロジ）を表すことはできません。 その代わりに、i（M）BGP ピアは、パスを送信した i（M）BGP ピアのアドレスを使用して、自律システム内の i（M）BGP トポロジ（MSDP トポロジ）を表します。

ヒント MSDP ピアを設定する場合は、i（M）BGP ピア アドレスと MSDP ピア アドレスの両方に同じアドレスが使用されるように注意する必要があります。

MSDP の SA メッセージの RPF チェックのルール 2

送信側の MSDP ピアが e（M）BGP ピアでもある場合、MSDP の RPF チェックのルール 2 が適用されます。 ルール 2 が適用されると、RPF チェックは次のように行われます。

1. ピアは、BGP MRIB を検索して SA メッセージを発信した RP への最適パスを探します。 MRIB でパスが検出されなかった場合、ピアは URIB を検索します。 それでもパスが検出されなかった場合は、RPF チェックは失敗します。
2. 検索が成功した場合（最適パスが検出された場合）、ピアはパスを検査します。 RP への最適パス内の最初の自律システムが e（M）BGP ピア（送信側の MSDP ピアでもある）の自律システムと同じである場合、RPF チェックは正常に終了します。同じでない場合は、RPF チェックは失敗します。

RPF チェックのルール 2 の MSDP への影響

MSDP トポロジでは、（M）BGP トポロジをミラーリングする必要があります。 一般に、2 台のデバイス間に e（M）BGP ピア接続がある場合は、必ず MSDP ピア接続を設定する必要があります。 ルール 1 とは対照的に、遠端 MSDP ピア接続の IP アドレスは遠端 e（M）BGP ピア接続と同じである必要はありません。その理由は、2 つの e（M）BGP ピア間の BGP トポロジが AS パスで記述されないためです。

MSDP の SA メッセージの RPF チェックのルール 3

送信側の MSDP ピアが（M）BGP ピアではない場合、RPF チェックのルール 3 が適用されます。 ルール 3 が適用されると、RPF チェックは次のように行われます。

1. ピアは、BGP MRIB を検索して SA メッセージを発信した RP への最適パスを探します。 MRIB でパスが検出されなかった場合、ピアは URIB を検索します。 それでもパスが検出されなかった場合は、RPF チェックは失敗します。
2. 検索が成功した場合（つまり、SA メッセージを発信した RP への最適パスが検出された場合）、ピアは BGP MRIB を検索して SA メッセージを送信した MSDP ピアへの最適パスを探します。 MRIB でパスが検出されなかった場合、ピアは URIB を検索します。 それでもパスが検出されなかった場合は、RPF チェックは失敗します。

（注） SA メッセージを送信した MSDP ピアの自律システムは発信元自律システムで、これは MSDP ピアへの AS パス内にある最後の自律システムです。

1. RP への最適パス内の最初の自律システムが送信側の MSDP ピアの自律システムと同じである場合、RPF チェックは正常に終了します。同じでない場合は、RPF チェックは失敗します。

SA メッセージの処理

MSDP ピアは、SA メッセージを処理するたびに次の手順を実行します。

1. ピアは SA メッセージの（S, G）ペアのグループ アドレス G を使用して、mroute テーブル内の関連する（*, G）エントリを見つけます。 （*, G）エントリが検出され、発信インターフェイス リストが空でない場合、SA メッセージでアドバタイズされたソースのアクティブなレシーバが PIM-SM ドメインにあります。
2. MSDP ピアは、アドバタイズされたソースの（S, G）エントリを作成します。
3. (S, G) エントリがない場合、MSDP ピアはソース ツリーに加入するためにソースへの (S, G) 加入をただちにトリガーします。
4. ピアは SA メッセージをその他のすべての MSDP ピアにフラッディングします。ただし、次を除きます。
   - SA メッセージを受信した MSDP ピア。
   - このデバイスと同じ MSDP メッシュ グループ内の MSDP ピア（ピアがメッシュ グループのメンバである場合）。

（注） SA メッセージは、デバイス SA キャッシュにローカルに保存されます。

MSDP ピア

BGP と同様に、MSDP は他の MSDP ピアとのネイバー関係を確立します。 MSDP ピアは TCP ポート 639 を使用して接続します。 IP アドレスが小さい方のピアは、TCP 接続を開くアクティブなロールを担います。 IP アドレスが大きい方のピアは、他方が接続を確立するのを LISTEN ステートで待機します。 MSDP ピアは、60 秒ごとにキープアライブ メッセージを送信します。 データが着信すると、キープアライブ メッセージと同じ機能が実行され、セッションがタイムアウトにならないようにします。 キープアライブ メッセージまたはデータが 75 秒間受信されない場合、TCP 接続はリセットされます。

MSDP MD5 パスワード認証

MSDP MD5 パスワード認証機能は、2 つの MSDP ピア間の TCP 接続上で Message Digest 5（MD5）シグネチャの保護を提供するための拡張です。 この機能は、TCP 接続ストリームに導入されるスプーフィングされた TCP セグメントの脅威に対して MSDP を保護することにより、追加のセキュリティを提供します。

MSDP MD5 パスワード認証の動作

RFC 2385 に準拠して開発された MSDP MD5 パスワード認証機能は、MSDP ピア間の TCP 接続で送信された各セグメントを確認するために使用されます。 **ip msdp password peer** コマンドは、2 つの MSDP ピア間の TCP 接続の MD5 認証をイネーブルにするために使用されます。 2 つの MSDP ピア間で MD5 認証がイネーブルになると、ピア間の TCP 接続で送信された各セグメントが確認されます。 どちらの MSDP ピアでも同じパスワードを使用して MD5 認証を設定する必要があります。そうしない場合は、これらの間の接続が確立されません。 MD5 認証を設定すると、Cisco IOS ソフトウェアにより、TCP 接続上で送信される各セグメントについて MD5 ダイジェストが生成され、検証されるようになります。

MSDP MD5 パスワード認証の利点

- TCP 接続ストリームに入り込むスプーフィングされた TCP セグメントの脅威に対して MSDP を保護します。
- 業界標準の MD5 アルゴリズムを使用して信頼性およびセキュリティを向上させます。

SA メッセージの制限

デバイスが特定の MSDP ピアから受け入れることができる SA メッセージの総数を制限するには、**ip msdp sa-limit** コマンドを使用します。 **ip msdp sa-limit** コマンドを設定すると、そのピア用に設定された SA メッセージの制限に到達した場合、デバイスは SA キャッシュに格納されている SA メッセージのピアごとの数を維持し、ピアからの新規メッセージを無視します。

MSDP 対応デバイスをサービス拒否（DoS）攻撃から保護するための手段として、**ip msdp sa-limit** コマンドが導入されました。 デバイス上のすべての MSDP ピアリングに対して SA メッセージの制限を設定することを推奨します。 適度に低い SA 制限をスタブ MSDP リージョンとのピアリングに設定する必要があります（たとえば、さらにダウンストリーム ピアを持つが、インターネットの残りの部分で SA メッセージの中継として動作しないピアなど）。 インターネット上の SA メッセージの中継として動作するすべての MSDP ピアリングに高い SA 制限を設定する必要があります。

MSDP キープアライブ インターバルおよび保留時間インターバル

MSDP ピアがキープアライブ メッセージを送信する間隔、および MSDP ピアがダウンしたと宣言するまでに他のピアからのキープアライブ メッセージを待機する間隔を調整するには、**ip msdp keepalive** コマンドを使用します。

MSDP ピアリング セッションが確立されると、接続の各側はキープアライブ メッセージを送信し、キープアライブ タイマーを設定します。 キープアライブ タイマーの期限が切れると、ローカル MSDP ピアはキープアライブ メッセージを送信し、キープアライブ タイマーを再開します。この間隔をキープアライブ インターバルといいます。 *keepalive-interval* 引数がキープアライブ メッセージの送信間隔を調整するために使用されます。キープアライブ タイマーは、ピアがアップ状態のときに *keepalive-interval* 引数に指定された値に設定されます。 キープアライブ タイマーは、MSDP キープアライブ メッセージがピアに送信されるたびに *keepalive-interval* 引数の値にリセットされ、タイマーの期限が切れるとリセットされます。 キープアライブ タイマーは、MSDP ピアリング セッションが終了したときに削除されます。 デフォルトでは、keepalive タイマーは 60 秒に設定されます。

（注） *keepalive-interval* 引数に指定される値は、*holdtime-interval* 引数に指定される値未満にしなければならず、また、1 秒以上に設定する必要があります。

保留時間タイマーは、MSDP ピアリング接続が確立されると *hold-time-interval* 引数の値に初期化され、MSDP キープアライブ メッセージが受信されると *hold-time-interval* 引数の値にリセットされます。 保留時間タイマーは、MSDP ピアリング接続が閉じられると削除されます。 デフォルトでは、保留時間インターバルは 75 秒に設定されています。

MSDP ピアが他のピアがダウンしたと宣言するまで他のピアからのキープアライブ メッセージを待機する間隔を調整するには、*hold-time-interval* 引数を使用します。

MSDP 接続再試行インターバル

ピアリングセッションがリセットされてからピアリングセッションの再確立が試行されるまですべての MSDP ピアが待機する間隔を調整できます。 この間隔は、接続再試行インターバルと呼ばれます。デフォルトでは、ピアリングセッションがリセットされてから他のピアとのピアリングセッションの再確立が試行されるまで MSDP ピアは 30 秒間待機します。 変更された設定済み接続再試行インターバルは、デバイス上のすべての MSDP ピアリング セッションに適用されます。

MSDP の IETF RFC 3618 準拠

MSDP の IETF RFC 3618 準拠機能が設定されている場合は、IETF RFC 3618 で定義されているピア RPF 転送ルールが MSDP ピアに適用されます。 IETF RFC 3618 では、MSDP が使用可能なインターネット全体で SA メッセージを転送するために使用されるピア RPF 転送ルールが規定されています。 データ パケットの転送時に使用される RPF チェックではパケットのソース アドレスをパケットを受信したインターフェイスと比較しますが、ピア RPF チェックでは SA メッセージで送信される RP アドレスをメッセージを受信した MSDP ピアと比較します。 MSDP メッシュ グループを使用されている場合を除き、SA メッセージのループを避けるために RP アドレスからの SA メッセージは 1 つの MSDP ピアからだけ受け入れます。

（注） RFC 3618 で定義されている MSDP ピア転送ルールの詳細については、RFC 3618『Multicast Source Discovery Protocol（MSDP）』を参照してください。

MSDP の RFC 3618 準拠の利点

- BGP ルート リフレクタ（RR）で MSDP を実行しなくても、BGP RR を使用できます。 この機能は、RR の負荷を軽減する必要があるサービス プロバイダーに役立ちます。
- リバース パス転送（RPF）のチェックに Interior Gateway Protocol（IGP）を使用でき、そのため（M）BGP なしでピアリングを実行できます。 この機能は、（M）BGP を実行せず、メッシュ グループが提供できるものより大規模なトポロジを必要とする企業に役立ちます。

（注） IGP ピアリングは直接接続された MSDP ピア間に常に存在する必要があります。そうしないと、RPF チェックは失敗します。

- 直接接続されていない自律システム（つまり、1 つまたは複数の自律システムがその間に存在する）のルータ間でピアリングを設定できます。 この機能は、連合設定および冗長性に役立ちます。

デフォルト MSDP ピア

ほとんどのシナリオでは、MSDP ピアは BGP ピアでもあります。 自律システムがスタブまたは非中継自律システムであり、特に自律システムがマルチホーム化されてない場合、中継自律システムに BGP を実行する理由は、ほとんどまたはまったくありません。 一般に、スタブ自律システムのスタティックなデフォルト ルート、および中継自律システムのスタブ プレフィックスに接続するスタティックなルートで十分です。 ただし、スタブ自律システムがマルチキャスト ドメインでもあり、RP が隣接ドメイン内の RP とピアリングする必要がある場合は、MSDP は BGP ネクスト ホップ データベースを使用してピア RPF チェックを行います。 **ip msdp default-peer** コマンドを

使用して、ピア RPF チェックを実行せずにすべての SA メッセージを受け入れるデフォルト ピアを定義することにより、この BGP への依存をディセーブルにできます。 デフォルトの MSDP ピアは、事前に設定しておく必要があります。

スタブ自律システムには、冗長性を実現するために複数の RP との MSDP ピアリングが必要な場合もあります。 たとえば、RPF チェック メカニズムがないため、SA メッセージは複数のデフォルト ピアから受け入れられません。 代わりに、SA メッセージは 1 つのピアからのみ受け入れられます。 そのピアに障害が発生した場合、SA メッセージは別のピアから受け入れられます。 ここでの基本的な前提は、両方のデフォルト ピアが同じ SA メッセージを送信していることです。

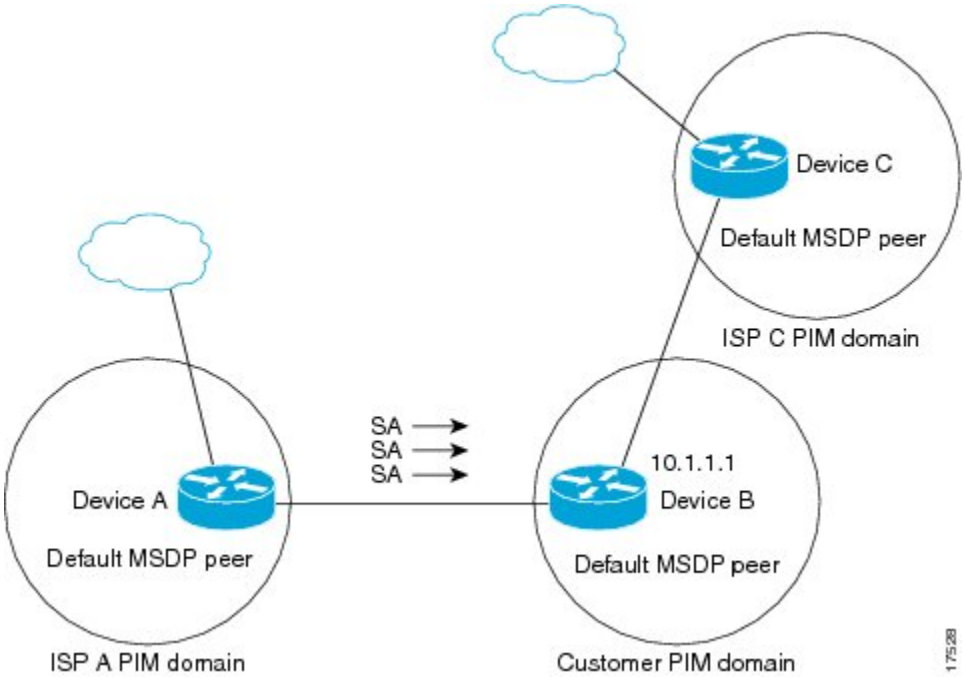
図に、デフォルト MSDP ピアが使用されるシナリオを示します。 この図では、ルータ B を所有するカスタマーが 2 つのインターネット サービス プロバイダー（ISP）を介してインターネットに接続されています。一方の ISP はルータ A を所有し、もう一方の ISP はルータ C を所有しています。 これらの ISP 間で、BGP または MBGP は動作していません。 カスタマーが ISP ドメインまたは他のドメイン内のソースについて学習するために、ルータ B はルータ A をデフォルト MSDP ピアとして識別します。 ルータ B はルータ A とルータ C の両方に SA メッセージをアドバタイズしますが、ルータ A だけまたはルータ C だけから SA メッセージを受け入れます。 ルータ A が設定内の最初のデフォルト ピアである場合、ルータ A が稼働していればルータ A が使用されます。ルータ A が稼働していない場合に限り、ルータ B がルータ C からの SA メッセージを受け入れます。

ISP は、プレフィックス リストを使用して、カスタマーのルータから受け入れるプレフィックスを定義する場合もあります。 カスタマーは、複数のデフォルト ピアを定義します。各ピアには関連するプレフィックスを 1 つまたは複数設定します。

カスタマーは 2 つの ISP を使用しています。 カスタマーはこの 2 つの ISP をデフォルト ピアとして定義します。 設定内で最初のデフォルト ピアとして特定されているピアが稼働している限り、

このピアがデフォルト ピアになり、カスタマーはそのピアから受信するすべての SA メッセージを受け入れます。

図 *12*：デフォルト *MSDP* ピアのシナリオ



ルータ B はルータ A およびルータ C に SA をアドバタイズしますが、ルータ A またはルータ C だけを使用して SA メッセージを受け入れます。 ルータ A が設定内の最初のルータである場合、ルータ A が稼働していればルータ A が使用されます。 ルータ A が稼働していない場合に限り、ルータ B がルータ C から SA メッセージを受け入れます。 これは、プレフィックス リストがない場合の動作です。

プレフィックス リストを指定すると、リスト内のプレフィックスに対してだけピアはデフォルト ピアになります。プレフィックスリストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。 プレフィックス リストがない場合も、複数のデフォルト ピアを設定できますが、アクティブなデフォルト ピアになるのは最初のピアだけです（このピアにルータが接続されていて、ピアがアクティブの場合に限ります）。 最初に設定されたピアがダウンするか、このピアとの接続がダウンした場合、2 番目に設定されたピアがアクティブなデフォルト ピアになります。以下同様です。

MSDP メッシュ グループ

MSDP メッシュ グループは、MSDP によってフル メッシュ型に相互接続された MSDP スピーカーのグループです。 つまり、グループの各 MSDP ピアには、グループ内の他のすべての MSDP ピアとの MSDP ピアリング関係（MSDP 接続）が必要です。 MSDP メッシュ グループが MSDP ピアのグループ間に設定されている場合、SA メッセージのフラッディングが削減されます。 グループ内の MSDP ピアがグループ内の別の MSDP ピアから SA メッセージを受信すると、この SA メッ

セージはグループ内のその他のすべての MSDP ピアに送信されたとみなされるためです。 その結果、受信側の MSDP ピアがグループ内の他の MSDP ピアに SA メッセージをフラッディングする必要はありません。

MSDP メッシュ グループの利点

- SA フラッディングの最適化：グループ内に複数のピアがある場合、SA フラッディングを最適化するために MSDP メッシュ グループは特に有用です。
- インターネットを通過する SA トラフィック量の削減：MSDP メッシュ グループを使用すると、SA メッセージは他のメッシュ グループ ピアにフラッディングされません。
- 着信 SA メッセージの RPF チェックの省略：MSDP メッシュ グループが設定されていると、メッシュ グループ ピアからの SA メッセージは常に受け入れられます。

SA 発信フィルタ

デフォルトでは、MSDP を実行するように設定されている RP は、それが RP であるすべてのローカル ソースの SA メッセージを発信します。 そのため、RP に登録されているローカル ソースは SA メッセージでアドバタイズされますが、これが望ましくない場合もあります。 たとえば、PIM-SM ドメイン内のソースがプライベート アドレス（たとえば、ネットワーク 10.0.0.0/8）を使用している場合、SA 発信フィルタを設定してこれらのアドレスがインターネット上の他の MSDP ピアにアドバタイズされないようにする必要があります。

どのソースが SA メッセージでアドバタイズされるかを制御するには、RP に SA 発信フィルタを設定します。 SA 発信フィルタを作成すると、SA メッセージでアドバタイズされるソースを次のように制御できます。

- デバイスが SA メッセージのローカル ソースをアドバタイズしないように、RP を設定できます。 デバイスは引き続き通常の方法で他の MSDP ピアからの SA メッセージを転送し、ローカル ソースの SA メッセージは送信しません。
- 拡張アクセス リストで定義されている（S, G）ペアと一致する、特定のグループに送信するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。 その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。
- AS パス アクセス リストで定義されている AS パスと一致する、特定のグループに送信するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。 その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。
- ルート マップで定義されている基準と一致するローカル ソースの SA メッセージだけを発信するようにデバイスを設定できます。 その他のすべてのローカル ソースは SA メッセージでアドバタイズされません。
- 拡張アクセス リスト、AS パス アクセス リスト、およびルート マップ、またはその組み合わせを含む SA 発信フィルタを設定します。 この場合、ローカル ソースが SA メッセージでアドバタイズされる前に、すべての条件を満たしている必要があります。

MSDP での発信フィルタ リストの使用

デフォルトでは、MSDP 対応デバイスは、受信したすべての SA メッセージをその MSDP ピアすべてに転送します。 ただし、発信フィルタ リストを作成することで、SA メッセージが MSDP ピアに転送されないようにすることができます。発信フィルタリストは、ローカルに発信されたか別の MSDP ピアから受信したかに関係なくすべての SA メッセージに適用されますが、SA 発信フィルタはローカルに発信された SA メッセージだけに適用されます。 ローカル デバイスから発信される MSDP SA メッセージのフィルタを有効にする方法の詳細については、ローカル ソースの RP によって発信された SA メッセージの制御, （139 ページ）を参照してください。

発信フィルタ リストを作成すると、デバイスがピアに転送する SA メッセージを次のように制御できます。

- MSDP ピアへの SA メッセージの転送を停止するようにデバイスを設定することにより、特定の MSDP ピアに転送されたすべての発信 SA メッセージをフィルタリングできます。
- 拡張アクセス リストで許可された（S, G）ペアと一致する SA メッセージだけを MSDP ピアに転送するようにデバイスを設定することにより、拡張アクセス リストで定義されている（S, G）ペアに基づいて、特定の MSDP ピアに転送された発信 SA メッセージのサブセットをフィルタリングできます。 その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。
- ルート マップで定義されている基準と一致する SA メッセージだけを転送するようにデバイスを設定することにより、ルートマップで定義されている一致基準に基づいて、特定の MSDP ピアに転送された発信 SA メッセージのサブセットをフィルタリングできます。 その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。
- SA メッセージが 1 つまたは複数の MSDP ピアに転送された後でも、発信元に基づいて発信 SA メッセージをフィルタリングするようにデバイスを設定することにより、SA メッセージに含まれる、アナウンスする RP アドレスに基づいて、特定のピアからの発信 SA メッセージのサブセットをフィルタリングできます。 その他のすべての SA メッセージの MSDP ピアへの転送は停止されます。
- 拡張アクセス リスト、ルート マップ、および RP アクセス リストまたは RP ルート マップのいずれかを含む発信フィルタ リストを設定できます。 その場合、MSDP ピアで発信 SA メッセージを転送するにはすべての条件を満たしている必要があります。

注意 SA メッセージの任意のフィルタリングを実行すると、ダウンストリーム MSDP ピアで正当なアクティブソースの SA メッセージを受信できなくなることがあります。 そのため、このタイプのフィルタを使用する場合は注意が必要です。 通常、発信フィルタ リストは、プライベート アドレスを使用するソースなど、望ましくないソースを拒否するためだけに使用します。

MSDP での着信フィルタ リストの使用

デフォルトでは、MSDP 対応デバイスは MSDP ピアからそのデバイスに送信されたすべての SA メッセージを受信します。 ただし、着信フィルタ リストを作成して、デバイスが MSDP ピアから受信するソース情報を制御できます。

着信フィルタ リストを作成すると、デバイスがピアから受信する着信 SA メッセージを次のように制御できます。

- 特定の MSDP ピアから送信されたすべての SA メッセージを無視するようにデバイスを設定することにより、特定の MSDP ピアからのすべての着信 SA メッセージをフィルタリングできます。
- 拡張アクセス リストで定義されている（S, G）ペアと一致する MSDP ピアからの SA メッセージだけを受信するようにデバイスを設定することにより、拡張アクセス リストで定義されている（S,G）ペアに基づいて、特定のピアからの着信 SA メッセージのサブセットをフィルタリングできます。 MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- ルート マップで定義されている基準と一致する SA メッセージだけを受信するようにデバイスを設定することにより、ルートマップで定義されている一致基準に基づいて、特定のピアからの着信 SA 要求メッセージのサブセットをフィルタリングできます。 MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- 拡張アクセス リストで定義されている（S,G）ペアおよびルート マップで定義されている基準の両方と一致する着信 SA メッセージだけを受信するようにデバイスを設定することにより、拡張アクセス リストで定義されている（S,G）ペアおよびルート マップで定義されている一致基準の両方に基づいて、特定のピアからの着信 SA メッセージのサブセットをフィルタリングできます。 MSDP ピアからのその他のすべての着信 SA メッセージは無視されます。
- SA メッセージが 1 つまたは複数の MSDP ピアに転送された後でも、発信元に基づいて着信 SA メッセージをフィルタリングするようにデバイスを設定することにより、SA メッセージに含まれる、アナウンスする RP アドレスに基づいて、特定のピアからの着信 SA メッセージのサブセットをフィルタリングできます。
- 拡張アクセス リスト、ルート マップ、および RP アクセス リストまたは RP ルート マップのいずれかを含む着信フィルタ リストを設定できます。 その場合、MSDP ピアで着信 SA メッセージを受信するにはすべての条件を満たしている必要があります。

注意 SA メッセージの任意のフィルタリングを実行すると、ダウンストリーム MSDP ピアで正当なアクティブソースの SA メッセージを受信できなくなることがあります。 そのため、このタイプのフィルタを使用する場合は注意が必要です。 通常、着信フィルタ リストは、プライベートアドレスを使用するソースなど、望ましくないソースを拒否するためだけに使用されます。

MSDP の TTL しきい値

存続可能時間（TTL）値を使用して、ドロップされる前にパケットが取得できるホップの数を制限できます。 特定の MSDP ピアに送信された、データがカプセル化された SA メッセージの TTL を指定するには、**ip multicast ttl-threshold** コマンドを使用します。 デフォルトでは、パケットの TTL 値が 0（標準 TTL 動作）より大きい場合は、SA メッセージのマルチキャスト データ パケットは MSDP ピアに送信されます。

一般に、TTL しきい値の問題は、SA メッセージ内でソースの初期マルチキャスト パケットがカプセル化されることによって発生することがあります。マルチキャストパケットはユニキャスト SA メッセージ内部でカプセル化されるため（TTL は 255）、SA メッセージが MSDP ピアに送信されるときに TTL は減少しません。 さらに、マルチキャスト トラフィックおよびユニキャスト トラフィックは MSDP ピアへのまったく異なるパスと、その結果としてリモート PIM-SM ドメインへのまったく異なるパスに従うため、SA メッセージが通過するホップの総数は、通常のマルチキャスト パケットとは大きく異なります。 その結果、カプセル化されたパケットは TTL しきい値に違反することになります。 この問題を解決するには、**ip multicast ttl-threshold** コマンドを使用して、特定の MSDP ピアに送信された SA メッセージにカプセル化されているマルチキャスト パケットに関連付けられた TTL しきい値を設定します。 **ip msdp ttl-threshold** コマンドを使用すると、IP ヘッダーの TTL が *ttl-value* 引数に指定されている TTL 値未満であるマルチキャスト パケットが、ピアに送信される SA メッセージにカプセル化されないようにすることができます。

SA 要求メッセージ

非キャッシュ デバイスが 1 つ以上の特定の MSDP ピアに SA 要求メッセージを送信するように設定できます。

非キャッシュ RP に SA をキャッシュする MSDP ピアがある場合、非キャッシュ ピアが SA 要求メッセージを送信できるようにすると非キャッシュ ピアの参加遅延を低減できます。 ホストが特定のグループに対して加入を要求すると、非キャッシュ RP は SA 要求メッセージをキャッシュ ピアに送信します。 ピアがこの特定のグループのソース情報をキャッシュしている場合、SA 応答メッセージで要求側の RP に情報を送信します。 要求側の RP は SA 応答内の情報を使用しますが、他のピアにメッセージを転送しません。 非キャッシュ RP が SA 要求を受信すると、要求者にエラー メッセージを返します。

（注） 現行のすべてのサポートされているソフトウェア リリースでは、MSDP SA メッセージのキャッシュは必須であり、手動でイネーブルまたはディセーブルにすることはできません。 デフォルトでは、MSDP ピアが設定されると、設定済みコマンドが自動的に実行コンフィギュレーションに追加されます。

SA 要求フィルタ

デフォルトでは、デバイスはその MSDP ピアからのすべての発信 SA 要求メッセージを受け入れます。つまり、ルータはキャッシュされたソース情報を要求側の MSDP ピアに SA 応答メッセージで送信します。 SA 要求フィルタを作成すると、デバイスが特定のピアから受け入れる発信 SA 要求メッセージを制御できます。 SA 要求フィルタは、デバイスが MSDP ピアから受け入れる発信 SA 要求を次のように制御します。

- 特定の MSDP ピアからのすべての SA 要求メッセージを無視するようにデバイスを設定することにより、特定のピアからのすべての SA 要求メッセージをフィルタリングできます。
- 標準アクセス リストで定義されているグループと一致する MSDP ピアからの SA 要求メッセージだけを受け入れるようにデバイスを設定することにより、標準アクセス リストで定義されているグループに基づいて、特定のピアからの SA 要求メッセージのサブセットをフィルタリングできます。 その他のグループの指定されたピアからの SA 要求メッセージは無視されます。

MSDP MIB

MSDP MIB には、SNMP を介して MSDP スピーカーのリモート モニタリングを行う際に使用できる管理対象オブジェクトが規定されています。 MSDP MIB モジュールには、スカラ オブジェクトが 4 つとテーブルが 3 つあります。 このテーブルは、要求テーブル、ピア テーブル、および Source-Active（SA）キャッシュ テーブルです。 シスコの実装では、ピア テーブルと SA キャッシュ テーブルだけがサポートされています。 要求テーブルには、SA 要求の送信先のピアを決定するために使用される情報が含まれています。 ただし、Cisco IOS ソフトウェアで使用される MSDP 実装では、ピアへの SA 要求の送信はグループ アドレス（またはグループ アドレス マスク）に関連付けられていません。

（注） MSDP-MIB.my ファイルは、次の URL にある Cisco.com の Cisco MIB Web サイトからダウンロードできます。http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml。

MSDP を使用して複数の PIM-SM ドメインを相互接続する方法

最初の作業は必須で、他の作業はすべて任意です。

MSDP ピアの設定

（注） MSDP ピアをイネーブルにすることで、MSDP は暗黙的にイネーブルになります。

はじめる前に

- IP マルチキャスト ルーティングをイネーブルにし、PIM-SM を設定する必要があります。
- 単一の MSDP ピア、デフォルト MSDP ピア、および MSDP メッシュ グループのシナリオを除いて、すべての MSDP ピアは、MSDP 用に設定する前に BGP を実行するように設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp peer** {*peer-name*| *peer-address*} [*connect-source type number*] [**remote-as** *as-number*]
4. **ip msdp description** {*peer-name*| *peer-address*} *text*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp peer** {*peer-name*| *peer-address*} [*connect-source type number*] [**remote-as** *as-number*]	MSDP をイネーブルにし、DNS 名または IP アドレスによって指定された MSDP ピアを設定します。 （注） MSDP ピアとして設定するように選択されたデバイスは、通常 BGP ネイバーでもあります。 そうでない場合は、デフォルトの MSDP ピアの設定, （136 ページ）またはMSDP メッシュ グループの設定, （137 ページ）を参照してください。

	コマンドまたはアクション	目的
	例： `Device(config)# ip msdp peer 192.168.1.2 connect-source loopback0`	• **connect-source** キーワードを指定した場合、指定したローカル インターフェイスの *type* および *number* の値のプライマリ アドレスは TCP 接続のソース IP アドレスとして使用されます。 特にリモート ドメイン内のデバイスとピアリングする境界上の MSDP ピアに対しては、**connect-source** キーワードが推奨されます。
ステップ 4	**ip msdp description** {*peer-name*| *peer-address*} *text* 例： `Device(config)# ip msdp description 192.168.1.2 router at customer a`	（任意）設定内で、または **show** コマンド出力内で簡単に識別できるように、指定されたピアの説明を設定します。
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP ピアのシャットダウン

MSDP ピアをシャットダウンするには、次の任意の作業を実行します。

複数の MSDP ピアを設定していて、すべてのピアの設定が完了するまでいずれのピアもアクティブにしない場合は、各ピアをシャット ダウンし、各ピアを設定した後で起動することができます。 MSDP ピアの設定を失わずに、MSDP セッションをシャットダウンすることもできます。

（注） MSDP ピアがシャット ダウンされると、TCP 接続は終了し、（指定されたピアに対して）**no ip msdp shutdown** コマンドを使用してピアを再起動するまで再開されません。

はじめる前に

MSDP を実行していること、および MSDP ピアを設定することが必要です。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp shutdown** {*peer-name* | *peer-address*}
4. 別の MSDP ピアをシャットダウンするには、ステップ 3 を繰り返します。
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp shutdown** {*peer-name* | *peer-address*} 例： `Device(config)# ip msdp shutdown 192.168.1.3`	指定された MSDP ピアを管理上シャットダウンします。
ステップ 4	別の MSDP ピアをシャットダウンするには、ステップ 3 を繰り返します。	--
ステップ 5	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP ピア間の MSDP MD5 パスワード認証の設定

MSDP ピア間の MSDP Message Digest 5（MD5）パスワード認証を設定するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string*
4. **exit**
5. **show ip msdp peer** [peer-address | peer-name]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string* 例： `Device(config)# ip msdp password peer 10.32.43.144 0 test`	2 つの MSDP ピア間の TCP 接続で MD5 パスワード暗号化をイネーブルにします。 （注） どちらの MSDP ピアでも同じパスワードを使用して MD5 認証を設定する必要があります。そうしない場合は、これらの間の接続が確立されません。 • 2 つの MSDP ピア間の MD5 認証で使用するパスワードやキーを設定または変更する場合、パスワードを設定した後、ローカル デバイスは既存のセッションを解放しません。 ローカル デバイスは、キープアライブ期間が期限切れになるまで新しいパスワードを使用してピアリング セッションを維持しようとします。 キープアライブ期間が期限切れになるまでにリモート デバイスでパスワードが入力または変更されなかった場合、セッションはタイムアウトし、MSDP セッションはリセットされます。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show ip msdp peer** [peer-address | peer-name] 例： `Device# show ip msdp peer`	（任意）MSDP ピアに関する詳細情報を表示します。 （注） このコマンドを使用して、MSDP ピアで MD5 パスワード認証がイネーブルになっているかどうかを確認します。

トラブルシューティングのヒント

デバイスに MSDP ピアのパスワードが設定されており、MSDP ピアに設定されていない場合、デバイスが MSDP ピアとの間にセッションを確立しようとすると、次のようなメッセージがコンソールに表示されます。

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's
IP address]:179
```

同様に、2 台のデバイスに異なるパスワードが設定されている場合、次のようなメッセージがコンソールに表示されます。

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's
IP address]:179
```

debug ip tcp transactions コマンドを使用すると、ステートの変更、再送、重複するパケットなどの重要な TCP トランザクションに関する情報が表示されます。 MSDP MD5 パスワード認証のモニタリングやトラブルシューティングでは、**debug ip tcp transactions** コマンドを使用して、MD5 パスワードがイネーブルになっていること、およびキープアライブ メッセージが MSDP ピアによって受信されたことを確認します。

SA キャッシュ内で許可される特定の MSDP ピアからの SA メッセージ数の制限によるサービス拒絶（DoS）攻撃の防止

デバイスが特定の MSDP ピアから受け入れることができる SA メッセージの総数を制限するには、この任意の作業（ただし強く推奨されます）を実行します。 この作業を実行することで、分散型サービス拒否攻撃（DoS）から MSDP 対応デバイスを保護します。

（注） デバイス上のすべての MSDP ピアリングに対してこの作業を実行することを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp sa-limit** {*peer-address* | *peer-name*} *sa-limit*
4. 別の MSDP ピアの SA 制限を設定するには、ステップ 3 を繰り返します。
5. **exit**
6. **show ip msdp count** [*as-number*]
7. **show ip msdp peer** [*peer-address* | *peer-name*]
8. **show ip msdp summary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp sa-limit** {*peer-address* | *peer-name*} *sa-limit* 例： `Device(config)# ip msdp sa-limit 192.168.10.1 100`	SA キャッシュ内で許可される特定の MSDP ピアからの SA メッセージの数を制限します。
ステップ 4	別の MSDP ピアの SA 制限を設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show ip msdp count** [*as-number*] 例： `Device# show ip msdp count`	（任意）MSDP SA メッセージ内で発信されたソースおよびグループの数、および SA キャッシュ内の MSDP ピアからの SA メッセージの数を表示します。

	コマンドまたはアクション	目的
ステップ 7	**show ip msdp peer** [*peer-address* | *peer-name*] 例： `Device# show ip msdp peer`	（任意）MSDP ピアに関する詳細情報を表示します。 （注） このコマンドの出力には、キャッシュに格納されている MSDP ピアから受信した SA メッセージの数が表示されます。
ステップ 8	**show ip msdp summary** 例： `Device# show ip msdp summary`	（任意）MSDP ピアのステータスを表示します。 （注） このコマンドの出力には、キャッシュに格納されている SA の数を表示するピアごとの「SA Count」フィールドが表示されます。

MSDP キープアライブ インターバルおよび保留時間インターバルの調整

MSDP ピアがキープアライブ メッセージを送信する間隔、および MSDP ピアが他のピアがダウンしたと宣言するまでに他のピアからのキープアライブ メッセージを待機する間隔を調整するには、次の任意の作業を実行します。 デフォルトでは、MSDP ピアが別の MSDP ピアとのピアリング セッションが停止したことを検出するために 75 秒かかる場合があります。 冗長 MSDP ピアがあるネットワーク環境では、保留時間インターバルを短くすると、MSDP ピアに障害が発生した場合に MSDP ピアの再コンバージェンス時間を短縮できます。

（注） **ip msdp keepalive** コマンドのデフォルト値は RFC 3618『*Multicast Source Discovery Protocol*』に準拠しているため、コマンドのデフォルト値を変更しないことを推奨します。 ネットワーク環境でデフォルト値を変更する必要がある場合は、MSDP ピアリング セッションの両端で *keepalive-interval* および *hold-time-interval* 引数に同じ時間値を設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp keepalive** {*peer-address* | *peer-name*} *keepalive-interval hold-time-interval*
4. 別の MSDP ピアのキープアライブ メッセージの間隔を調整するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp keepalive** {*peer-address* | *peer-name*} *keepalive-interval hold-time-interval* 例： `Device(config)# ip msdp keepalive 10.1.1.3 40 55`	MSDP ピアがキープアライブ メッセージを送信する間隔、および MSDP ピアが他のピアがダウンしたと宣言するまでに他のピアからのキープアライブ メッセージを待機する間隔を設定します。
ステップ 4	別の MSDP ピアのキープアライブ メッセージの間隔を調整するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP 接続再試行インターバルの調整

ピアリングセッションがリセットされてからピアリングセッションの再確立が試行されるまですべての MSDP ピアが待機する間隔を調整するには、次の任意の作業を実行します。 SA メッセージの迅速なリカバリが必要なネットワーク環境（金融機関の取引フロアのネットワーク環境など）では、接続再試行インターバルをデフォルト値の 30 秒未満に短縮することが必要な場合があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp timer** *connection-retry-interval*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバルコンフィギュレーションモードを開始します。
ステップ 3	**ip msdp timer** *connection-retry-interval* 例： `Device# ip msdp timer 45`	ピアリング セッションがリセットされてからピアリング セッションの再確立が試行されるまで MSDP ピアが待機する間隔を設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP の IETF RFC 3618 準拠の設定

インターネット技術特別調査委員会（IETF）RFC 3618 の MSDP の仕様に準拠するように MSDP ピアを設定するには、次の任意作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp rpf rfc3618**
4. **end**
5. **show ip msdp rpf-peer** *rp-address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp rpf rfc3618** 例： `Router(config)# ip msdp rpf rfc3618`	IETF RFC 3618 で指定されているピア RPF 転送ルールに準拠するようにします。
ステップ 4	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ip msdp rpf-peer** *rp-address* 例： `Router# show ip msdp rpf-peer 192.168.1.5`	（任意）指定された RP から発信される SA メッセージをルータが受け入れる固有の MSDP ピア情報を表示します。

デフォルトの MSDP ピアの設定

デフォルト MSDP ピアを設定するには、次の任意の作業を実行します。

はじめる前に

デフォルト MSDP ピアは、事前に設定されている MSDP ピアでなければなりません。デフォルト MSDP ピアを設定する前に、まず MSDP ピアを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp default-peer** {*peer-address* | *peer-name*} [**prefix-list** *list*]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp default-peer** {*peer-address* | *peer-name*} [**prefix-list** *list*] 例： `Device(config)# ip msdp default-peer 192.168.1.3`	すべての MSDP SA メッセージの受信元となるデフォルト ピアを設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP メッシュ グループの設定

MSDP メッシュ グループを設定するには、次の任意の作業を実行します。

（注） デバイスごとに複数のメッシュ グループを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp mesh-group** *mesh-name* {*peer-address* | *peer-name*}
4. MSDP ピアをメッシュ グループのメンバとして追加するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp mesh-group** *mesh-name* {*peer-address* | *peer-name*} 例： `Device(config)# ip msdp mesh-group peermesh`	MSDP メッシュ グループを設定し、MSDP ピアがそのメッシュ グループに属することを指定します。 （注） メッシュ グループに参加するデバイスのすべての MSDP ピアは、グループ内の他のすべての MSDP ピアと完全にメッシュ化されている必要があります。 各デバイスの各 MSDP ピアは、**ip msdp peer** コマンドを使用してピアとして設定する必要があり、また、**ip msdp mesh-group** コマンドを使用してメッシュ グループのメンバとしても設定する必要があります。
ステップ 4	MSDP ピアをメッシュ グループのメンバとして追加するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ローカル ソースの RP によって発信された SA メッセージの制御

SA メッセージでアドバタイズされる登録ソースを制限するフィルタをイネーブルにして、RP によって発信された SA メッセージを制御するには、次の作業を実行します。

（注） MSDP SA メッセージ フィルタの設定に関するベスト プラクティス情報については、テクニカル ノート『Multicast Source Discovery Protocol SA Filter Recommendations』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp redistribute** [**list** *access-list*] [**asn** *as-access-list*] [**route-map** *map-name*]
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp redistribute** [**list** *access-list*] [**asn** *as-access-list*] [**route-map** *map-name*] 例： `Device(config)# ip msdp redistribute route-map customer-sources`	ローカル デバイスによって発信される MSDP SA メッセージのフィルタをイネーブルにします。 （注） **ip msdp redistribute** コマンドは、RP で認識されているが登録されていないソースをアドバタイズするために使用することもできます。 ただし、RP に登録されていないソースのアドバタイズメントは発信しないことを強く推奨します。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

発信フィルタ リストを使用した SA メッセージの MSDP ピアへの転送の制御

発信フィルタ リストを設定して SA メッセージの MSDP ピアへの転送を制御するには、次の任意の作業を実行します。

（注） MSDP SA メッセージ フィルタの設定に関するベスト プラクティス情報については、テクニカル ノート『Multicast Source Discovery Protocol SA Filter Recommendations』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*]
4. 別の MSDP ピアの発信フィルタ リストを設定するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip msdp sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*] 例： `Device(config)# ip msdp sa-filter out 192.168.1.5 peerone`	発信 MSDP メッセージのフィルタをイネーブルにします。
ステップ 4	別の MSDP ピアの発信フィルタ リストを設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

着信フィルタ リストを使用した MSDP ピアからの SA メッセージの受信の制御

MSDP ピアからの着信 SA メッセージの受信を制御するには、次の任意の作業を実行します。

（注） MSDP SA メッセージ フィルタの設定に関するベスト プラクティス情報については、テクニカル ノート『Multicast Source Discovery Protocol SA Filter Recommendations』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*]
4. 別の MSDP ピアの着信フィルタ リストを設定するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*] 例： `Device(config)# ip msdp sa-filter in 192.168.1.3`	着信 MSDP SA メッセージのフィルタをイネーブルにします。
ステップ 4	別の MSDP ピアの着信フィルタ リストを設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

TTL しきい値を使用した SA メッセージで送信されたマルチキャスト データの制限

存続可能時間（TTL）しきい値を設定して、SA メッセージで送信されるマルチキャスト データを制限するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp ttl-threshold** {*peer-address* | *peer-name*} *ttl-value*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp ttl-threshold** {*peer-address* | *peer-name*} *ttl-value* 例： 例： `Device(config)# ip msdp ttl-threshold 192.168.1.5 8`	ローカル デバイスにより発信される MSDP メッセージの TTL 値を設定します。 • デフォルトでは、パケットの TTL 値が 0（標準 TTL 動作）より大きい場合は、SA メッセージのマルチキャスト データ パケットは MSDP ピアに送信されます。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP ピアへのソース情報の要求

デバイスが MSDP ピアにソース情報を要求できるようにするには、次の任意の作業を実行します。

（注） SA キャッシングはデフォルトでイネーブルになっており、以前の Cisco ソフトウェア リリースでは明示的にイネーブルまたはディセーブルにすることができないため、この作業を実行する必要はほとんどありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp sa-request** {*peer-address* | *peer-name*}
4. デバイスが別の MSDP キャッシュ ピアに SA 要求メッセージを送信するように指定するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp sa-request** {*peer-address* | *peer-name*} 例： `Device(config)# ip msdp sa-request 192.168.10.1`	デバイスが指定された MSDP ピアに SA 要求メッセージを送信するように指定します。
ステップ 4	デバイスが別の MSDP キャッシュ ピアに SA 要求メッセージを送信するように指定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SA 要求フィルタを使用した MSDP ピアからの発信 SA 要求メッセージに対する応答の制御

デバイスが MSDP ピアから受け入れる発信 SA 要求メッセージを制御するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp filter-sa-request** {*peer-address* | *peer-name*} [**list** *access-list*]
4. 別の MSDP ピアの SA 要求フィルタを設定するには、ステップ 3 を繰り返します。
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp filter-sa-request** {*peer-address* | *peer-name*} [**list** *access-list*] 例： `Device(config)# ip msdp filter sa-request 172.31.2.2 list 1`	発信 SA 要求メッセージのフィルタをイネーブルにします。 （注） MSDP ピアには SA 要求フィルタを 1 つだけ設定できます。
ステップ 4	別の MSDP ピアの SA 要求フィルタを設定するには、ステップ 3 を繰り返します。	--
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

境界 PIM デンス モード リージョンの MSDP への包含

PIM デンス モード（PIM-DM）リージョンでアクティブなソースの SA メッセージを送信するように境界デバイスを設定するには、次の任意作業を実行します。

PIM-SM リージョンと PIM-DM リージョンの境界にデバイスを設定できます。 デフォルトでは、PIM-DM ドメインのソースは MSDP に含まれません。 PIM-DM ドメインでアクティブなソースの SA メッセージを送信するようにこの境界デバイスを設定できます。 その場合、**ip msdp redistribute** コマンドを設定してアドバタイズする PIM-DM ドメインのローカル ソースを制御することも非常に重要です。 このコマンドを設定しないと、PIM-DM ドメインのソースが送信を停止した後も長時間 (S, G) ステートのままになります。 設定の詳細については、ローカル ソースの RP によって発信された SA メッセージの制御, （139 ページ）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp border sa-address** *type number*
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp border sa-address** *type number* 例： `Device(config)# ip msdp border sa-address gigabitethernet0/0/0`	PIM-DM ドメインでアクティブなソースの SA メッセージを発信するように、PIM-SM および PIM-DM ドメイン間の境界にデバイスを設定します。 • インターフェイスの IP アドレスは、SA メッセージの RP フィールドに示されるソース ID として使用されます。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

RP アドレス以外のソース アドレスの設定

SA メッセージを発信する MSDP スピーカーがそのインターフェイスの 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るようにするには、次の任意の作業を実行します。

また、次のいずれかの理由から、発信 ID を変更できます。

- Anycast RP の MSDP メッシュ グループに複数のデバイスを設定する場合。
- デバイスが PIM-SM ドメインと PIM-DM ドメインの境界にある場合。 デバイスが PIM-SM ドメインと PIM-DM ドメインの境界にあり、PIM-DM ドメイン内のアクティブなソースをアドバタイズする場合は、SA メッセージ内の RP アドレスがソース デバイスのインターフェイスのアドレスとなるように設定します。

はじめる前に

MSDP がイネーブルであり、MSDP ピアが設定されている必要があります。 MSDP ピアの設定の詳細については、MSDP ピアの設定, （127 ページ）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip msdp originator-id** *type number*
4. **exit**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip msdp originator-id** *type number* 例： `Device(config)# ip msdp originator-id ethernet 1`	SA メッセージ内の RP アドレスをソース デバイスのインターフェイスのアドレスになるように設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MSDP のモニタリング

MSDP の SA メッセージ、ピア、ステート、およびピアのステータスをモニタリングするには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **debug ip msdp** [*peer-address* | *peer-name*] [**detail**] [**routes**]
3. **debug ip msdp resets**
4. **show ip msdp count** [*as-number*]
5. **show ip msdp peer** [*peer-address* | *peer-name*]
6. **show ip msdp sa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*]
7. **show ip msdp summary**

手順の詳細

ステップ 1 **enable**

例：

```
Device# enable
```

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

ステップ 2 **debug ip msdp** [*peer-address* | *peer-name*] [**detail**] [**routes**]
このコマンドを使用して、MSDP アクティビティをデバッグします。

オプションの *peer-address* 引数または *peer-name* 引数を使用して、デバッグ イベントをログに記録するピアを指定します。

次に、**debug ip msdp** コマンドの出力例を示します。

例：

```
Device# debug ip msdp
MSDP debugging is on
Device#
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.254: Received 1028-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1028, ec: 85, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1028-byte SA to peer
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.250: Received 56-byte message from peer
MSDP: 224.150.44.250: SA TLV, len: 56, ec: 4, RP: 192.168.76.241
MSDP: 224.150.44.250: Peer RPF check passed for 192.168.76.241, used EMBGP peer
MSDP: 224.150.44.254: Forward 56-byte SA to peer
MSDP: 224.150.44.254: Received 116-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 116, ec: 9, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.250: Forward 116-byte SA to peer
MSDP: 224.150.44.254: Received 32-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 32, ec: 2, RP: 172.31.3.78
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.78, used EMBGP peer
MSDP: 224.150.44.250: Forward 32-byte SA to peer
```

ステップ 3 **debug ip msdp resets**
このコマンドを使用して、MSDP ピアのリセット理由をデバッグします。

例：

```
Device# debug ip msdp resets
```

ステップ 4 **show ip msdp count** [*as-number*]
このコマンドを使用して、MSDP SA メッセージ内で発信したソースおよびグループの数、および SA キャッシュ内の MSDP ピアからの SA メッセージの数を表示します。 何らかの出力を得るためには、このコマンドに **ip msdp cache-sa-state** コマンドを設定しておく必要があります。

次に、**show ip msdp count** コマンドの出力例を示します。

例：

```
Device# show ip msdp count
SA State per Peer Counters, <Peer>: <# SA learned>
    192.168.4.4: 8
```

```
SA State per ASN Counters, <asn>: <# sources>/<# groups>
    Total entries: 8
    ?: 8/8
```

ステップ 5 **show ip msdp peer** [*peer-address* | *peer-name*]

このコマンドを使用して、MSDP ピアに関する詳細情報を表示します。

オプションの *peer-address* 引数または *peer-name* 引数を使用して、特定のピアに関する情報を表示します。

次に、**show ip msdp peer** コマンドの出力例を示します。

例：

```
Device# show ip msdp peer 192.168.4.4
MSDP Peer 192.168.4.4 (?), AS 64512 (configured AS)
  Connection status:
    State: Up, Resets: 0, Connection source: Loopback0 (2.2.2.2)
    Uptime(Downtime): 00:07:55, Messages sent/received: 8/18
    Output messages discarded: 0
    Connection and counters cleared 00:08:55 ago
  SA Filtering:
    Input (S,G) filter: none, route-map: none
    Input RP filter: none, route-map: none
    Output (S,G) filter: none, route-map: none
    Output RP filter: none, route-map: none
  SA-Requests:
    Input filter: none
  Peer ttl threshold: 0
  SAs learned from this peer: 8
  Input queue size: 0, Output queue size: 0
  MD5 signature protection on MSDP TCP connection: not enabled
```

ステップ 6 **show ip msdp sa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*]

このコマンドを使用して、MSDP ピアから学習した (S, G) ステートを表示します。

次に、**show ip msdp sa-cache** コマンドの出力例を示します。

例：

```
Device# show ip msdp sa-cache
MSDP Source-Active Cache - 8 entries
(10.44.44.5, 239.232.1.0), RP 192.168.4.4, BGP/AS 64512, 00:01:20/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.1), RP 192.168.4.4, BGP/AS 64512, 00:01:20/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.2), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.3), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.4), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.5), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.6), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.7), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
```

ステップ 7 **show ip msdp summary**

このコマンドを使用して、MSDP ピアのステータスを表示します。

次に、**show ip msdp summary** コマンドの出力例を示します。

例：

```
Device# show ip msdp summary
MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
```

```
                                Downtime Count Count
192.168.4.4       4     Up      00:08:05 0     8     ?
```

MSDP 接続、統計情報、および SA キャッシュ エントリの消去

MSDP 接続、統計情報、および SA キャッシュ エントリを消去するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **clear ip msdp peer** [*peer-address* | *peer-name*]
3. **clear ip msdp statistics** [*peer-address* | peer-name]
4. **clear ip msdp sa-cache** [*group-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear ip msdp peer** [*peer-address* | *peer-name*] 例： `Device# clear ip msdp peer`	指定された MSDP ピアへの TCP 接続をクリアし、すべての MSDP メッセージ カウンタをリセットします。
ステップ 3	**clear ip msdp statistics** [*peer-address* | peer-name] 例： `Device# clear ip msdp statistics`	指定された MSDP ピアの統計情報カウンタをクリアし、すべての MSDP メッセージ カウンタをリセットします。
ステップ 4	**clear ip msdp sa-cache** [*group-address*] 例： `Device# clear ip msdp sa-cache`	SA キャッシュ エントリを消去します。 • **clear ip msdp sa-cache** コマンドにオプションの *group-address* 引数または *source-address* 引数を指定した場合、すべての SA キャッシュ エントリは消去されます。

	コマンドまたはアクション	目的
		• 特定のグループに関連付けられたすべてのSA キャッシュエントリを消去するには、オプションの *group-address* 引数を使用します。

MSDPの簡易ネットワーク管理プロトコル（SNMP）モニタリングのイネーブル化

MSDP の簡易ネットワーク管理プロトコル（SNMP）モニタリングをイネーブルにするには、次の任意の作業を実行します。

はじめる前に

- SNMP および MSDP がデバイスに設定されています。
- 各 PIM-SM ドメインには、MSDP スピーカーとして設定されているデバイスが必要です。 このデバイスは、SNMP と MSDP MIB がイネーブルに設定されている必要があります。

（注）
- すべての MSDP-MIB オブジェクトは読み取り専用として実装されます。
- 要求テーブルは、シスコの MSDP MIB の実装ではサポートされていません。
- msdpEstablished 通知は、シスコの MSDP MIB の実装ではサポートされていません。

手順の概要

1. **enable**
2. **snmp-server enable traps msdp**
3. **snmp-server host** *host* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth**| **priv** | **noauth**]}] *community-string* [**udp-port** *port-number*] **msdp**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**snmp-server enable traps msdp** 例： `Device# snmp-server enable traps msdp`	SNMP で使用される MSDP 通知の送信をイネーブルにします。 （注） **snmp-server enable traps msdp** コマンドは、トラップと応答要求の両方をイネーブルにします。
ステップ 3	**snmp-server host** *host* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth**| **priv** | **noauth**]}] *community-string* [**udp-port** *port-number*] **msdp** 例： `Device# snmp-server host examplehost msdp`	MSDP トラップまたは応答要求の受信者（ホスト）を指定します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

MSDP MIB 通知の結果とソフトウェアの出力を比較するには、適切なデバイスで **show ip msdp summary** コマンドおよび **show ip msdp peer** コマンドを使用します。 また、これらのコマンドの結果と SNMP GET 操作の結果を比較することもできます。 SA キャッシュ テーブル エントリを確認するには、**show ip msdp sa-cache** コマンドを使用します。 接続のローカル アドレス、ローカル ポート、リモート ポートなどのその他のトラブルシューティング情報は、**debug ip msdp** コマンドの出力を使用して取得できます。

MSDP を使用して複数の PIM-SM ドメインを相互接続する設定例

例：MSDP ピアの設定

次に、3 つの MSDP ピア間で MSDP ピアリング接続を確立する例を示します。

デバイス A

```
!
interface Loopback 0
 ip address 10.220.8.1 255.255.255.255
!
ip msdp peer 10.220.16.1 connect-source Loopback0
ip msdp peer 10.220.32.1 connect-source Loopback0
!
```

デバイス B

```
!
interface Loopback 0
 ip address 10.220.16.1 255.255.255.255
!
ip msdp peer 10.220.8.1 connect connect-source Loopback0
ip msdp peer 10.220.32.1 connect connect-source Loopback0
!
```

デバイス C

```
!
interface Loopback 0
 ip address 10.220.32.1 255.255.255.255
!
ip msdp peer 10.220.8.1 connect 10.220.8.1 connect-source Loopback0
ip msdp peer 10.220.16.1 connect 10.220.16.1 connect-source Loopback0
!
```

例：MSDP MD5 パスワード認証の設定

次に、2 つの MSDP ピア間の TCP 接続の MD5 パスワード認証をイネーブルにする例を示します。

デバイス A

```
!
ip msdp peer 10.3.32.154
ip msdp password peer 10.3.32.154 0 test
!
```

デバイス B

```
!
ip msdp peer 10.3.32.153
ip msdp password peer 10.3.32.153 0 test
!
```

MSDP の IETF RFC 3618 準拠の設定の例

次に、10.10.2.4 および 10.20.1.2 の MSDP ピアを IETF RFC 3618 で指定されているピア RPF 転送ルールに準拠するように設定する例を示します。

```
ip msdp peer 10.10.2.4
ip msdp peer 10.20.1.2
ip msdp rpf rfc3618
```

デフォルト MSDP ピアの設定の例

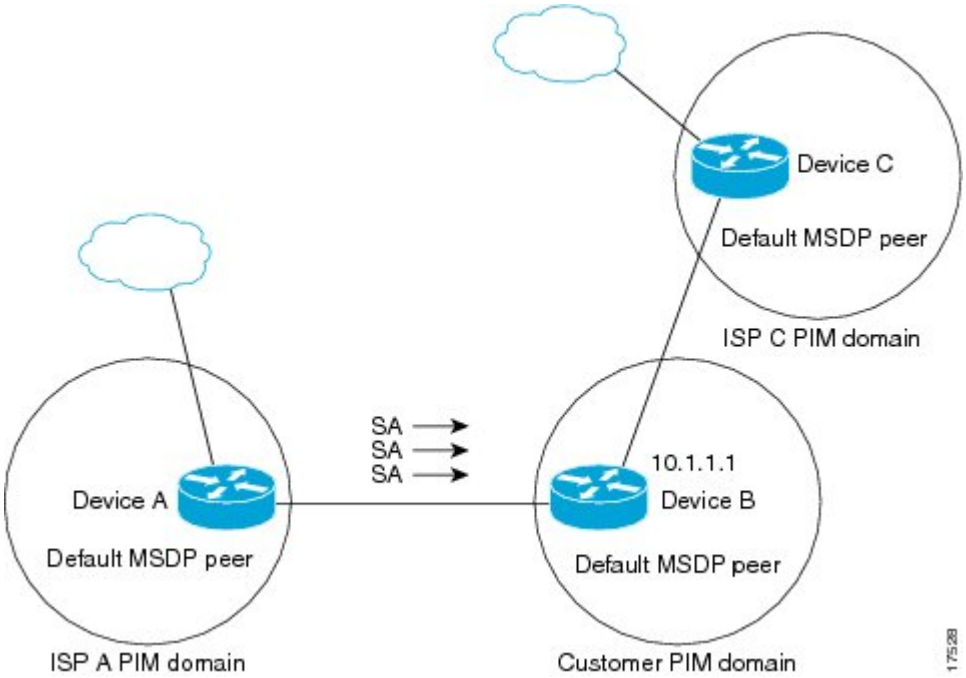
図に、デフォルト MSDP ピアが使用されるシナリオを示します。 この図では、ルータ B を所有するカスタマーが 2 つの ISP を介してインターネットに接続されています。一方の ISP はルータ A を所有し、もう一方の ISP はルータ C を所有しています。 これらの ISP 間で、（M）BGP は動作していません。 カスタマーが ISP ドメインまたは他のドメイン内のソースについて学習するために、ルータ B はルータ A をデフォルト MSDP ピアとして識別します。 ルータ B はルータ A とルータ C の両方に SA メッセージをアドバタイズしますが、ルータ A だけまたはルータ C だけから SA メッセージを受け入れます。 ルータ A が設定内の最初のデフォルト ピアである場合、ルータ A が稼働していればルータ A が使用されます。 ルータ A が稼働していない場合に限り、ルータ B がルータ C からの SA メッセージを受け入れます。

ISP は、プレフィックス リストを使用して、カスタマーのルータから受け入れるプレフィックスを定義する場合もあります。カスタマーは、複数のデフォルト ピアを定義します。各ピアには関連するプレフィックスを 1 つまたは複数設定します。

カスタマーは 2 つの ISP を使用しています。 カスタマーはこの 2 つの ISP をデフォルト ピアとして定義します。 設定内で最初のデフォルト ピアとして特定されているピアが稼働している限り、

このピアがデフォルト ピアになり、カスタマーはそのピアから受信するすべての SA メッセージを受け入れます。

図 *13*：デフォルト *MSDP* ピアのシナリオ



ルータ B はルータ A およびルータ C に SA をアドバタイズしますが、ルータ A またはルータ C だけを使用して SA メッセージを受け入れます。 ルータ A が設定ファイル内の最初のルータである場合、ルータ A が稼働していればルータ A が使用されます。 ルータ A が稼働していない場合に限り、ルータ B がルータ C から SA メッセージを受け入れます。 これは、プレフィックス リストがない場合の動作です。

プレフィックス リストを指定すると、リスト内のプレフィックスに対してだけピアはデフォルト ピアになります。プレフィックスリストがそれぞれ関連付けられている場合は、複数のアクティブなデフォルト ピアを設定できます。 プレフィックス リストがない場合も、複数のデフォルト ピアを設定できますが、アクティブなデフォルト ピアになるのは最初のピアだけです（このピアにルータが接続されていて、ピアがアクティブの場合に限ります）。 最初に設定されたピアがダウンするか、このピアとの接続がダウンした場合、2 番目に設定されたピアがアクティブなデフォルト ピアになります。以下同様です。

次に、図に示されているルータ A およびルータ C の部分的な設定例を示します。 これらの ISP にはそれぞれ、図に示すデフォルト ピアリングを使用するカスタマーのような複数のカスタマーがある場合があります。 そのようなカスタマーの設定は類似しています。 つまり、SA が対応するプレフィックス リストによって許可される場合、デフォルト ピアからの SA だけを受け入れます。

ルータ A の設定

```
ip msdp default-peer 10.1.1.1
ip msdp default-peer 10.1.1.1 prefix-list site-b ge 32
ip prefix-list site-b permit 10.0.0.0/8
```

ルータ C の設定

```
ip msdp default-peer 10.1.1.1 prefix-list site-b ge 32
ip prefix-list site-b permit 10.0.0.0/8
```

例：MSDP メッシュ グループの設定

次に、3 台のデバイスを MSDP メッシュ グループのフル メッシュ メンバになるように設定する例を示します。

デバイス A の設定

```
ip msdp peer 10.2.2.2
ip msdp peer 10.3.3.3
ip msdp mesh-group test-mesh-group 10.2.2.2
ip msdp mesh-group test-mesh-group 10.3.3.3
```

デバイス B の設定

```
ip msdp peer 10.1.1.1
ip msdp peer 10.3.3.3
ip msdp mesh-group test-mesh-group 10.1.1.1
ip msdp mesh-group test-mesh-group 10.3.3.3
```

デバイス C の設定

```
ip msdp peer 10.1.1.1
ip msdp peer 10.2.2.2
ip msdp mesh-group test-mesh-group 10.1.1.1
ip msdp mesh-group test-mesh-group 10.2.2.2
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 2385	『Protection of BGP Sessions via the TCP MD5 Signature Option』
RFC 2858	『Multiprotocol Extensions for BGP-4』
RFC 3618	『Multicast Source Discovery Protocol』

MIB

MIB	MIB のリンク
MSDP-MIB.my	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

MSDP を使用して複数の PIM-SM ドメインを相互接続するための機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *5*：*MSDP* を使用して複数の *PIM-SM* ドメインを相互接続するための機能情報

機能名	リリース	機能情報
Multicast Source Discovery Protocol（MSDP）	Cisco IOS XE Release 2.1 Cisco IOS Xe Release 3.5S	Multicast Source Discovery Protocol（MSDP）は、複数の PIM スパース モード（SM）ドメインを接続するためのメカニズムです。 MSDP を使用すると、さまざまなドメイン内のすべてのランデブー ポイント（RP）に、グループのマルチキャスト送信元を通知できます。 各 PIM-SM ドメインは自身の RP を使用するため、他のドメインの RP に依存する必要はありません。 RP は、MSDP を TCP 上で実行して他のドメインのマルチキャスト ソースを検出します。 Cisco IOS XE Release 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。

機能名	リリース	機能情報
MSDP の IETF RFC 3618 準拠	Cisco IOS XE Release 2.1	MSDP の IETF RFC 3618 準拠機能は、IETF RFC 3618 仕様で規定されているピアと RPF 間の転送ルールに準拠するように MSDP を設定できるようにします。 MSDP の IETF RFC 3618 準拠機能をイネーブルにすると、SA メッセージのループを防止できます。 また、MSDP の IETF RFC 3618 準拠機能をイネーブルにすることで、BGP RR で MSDP を実行する必要がなくなり、RPF チェックに IGP を使用でき、直接接続されていない自律システムのルータ間で MSDP ピアリングが可能になります。 この機能により、**ip msdp rpf rfc3618** コマンドおよび **show ip msdp rpf-peer** コマンドが導入または変更されました。
MSDP MD5 パスワード認証	Cisco IOS XE Release 2.5	MSDP MD5 パスワード認証機能は、2 つの MSDP ピア間の TCP 接続上で MD5 シグネチャの保護を提供するための拡張です。 この機能は、TCP 接続ストリームに導入されるスプーフィングされた TCP セグメントの脅威に対して MSDP を保護することにより、追加のセキュリティを提供します。 この機能により、**ip msdp password peer** コマンドおよび **show ip msdp peer** コマンドが導入または変更されました。

第 5 章

PIM Allow RP

このモジュールでは、IPv4 または IPv6 ネットワークで Protocol Independent Multicast（PIM）スパース モード（SM）ドメインを異なるランデブー ポイントで相互接続するための PIM Allow RP 機能を設定する方法について説明します。 PIM Allow RP では、着信（*, G）加入が処理され、異なる RP が識別されたときに、受信側デバイスで独自の RP を使用してステートを作成し、共有ツリーを構築することができます。 これにより、受信側デバイスは異なる RP からの（*, G）加入を受け入れることができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

PIM Allow RP の制約事項

- PIM Allow RP では、PIM SM ドメインの接続のみがサポートされます。
- PIM Allow RP はダウンストリーム トラフィックだけに適用可能です。つまり、共有ツリーの構築だけに適用できます。
- PIM Allow RP は、Auto-RP やブート ストラップ ルータ（BSR）では機能しません。 スタティック設定だけがサポートされています。 ただし、コンシューマ ネットワークの組み込み RP が、サービス プロバイダー ネットワークに静的に設定されているものと異なることは可能です。

PIM Allow RP について

ランデブー ポイント

ランデブー ポイント（RP）は、デバイスが Protocol Independent Multicast（PIM）のスパース モード（SM）で動作しているときに実行する役割です。 RP が必要になるのは、PIM SM を実行しているネットワークだけです。 PIM SM モデルでは、マルチキャスト データを明示的に要求したアクティブなレシーバを含むネットワーク セグメントだけにトラフィックが転送されます。マルチキャスト データを配信するこの方法は、PIM デンス モード（PIM-DM）とは対照的です。 PIM DM では、マルチキャスト トラフィックは、最初にネットワークのすべてのセグメントにフラッディングされます。 ダウンストリーム ネイバーを持たないルータやレシーバに直接接続されたルータは、不要なトラフィックをプルーニングします。

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

ほとんどの場合、ネットワークにおける RP の配置は複雑な判断を必要としません。 デフォルトでは、RP が必要になるのは、ソースおよびレシーバとの新しいセッションを開始する場合だけです。 その結果、RP では、トラフィックのフローまたは処理によるオーバーヘッドはほとんど発生しません。 PIM バージョン 2 では、ステートを作成する RP にソースが定期的に登録するだけなので、RP が実行する処理は PIM バージョン 1 より少なくなります。

PIM Allow RP

パブリッシャ、コンシューマ、転送の 3 種類のネットワークがあります。 多くのパブリッシャ ネットワークは、コンテンツを発信することができ、多くのコンシューマ ネットワークはコンテ

ンツに関心がある場合があります。サービスプロバイダーが所有および運用する転送ネットワークは、パブリッシャ ネットワークとコンシューマ ネットワークを接続します。

コンシューマ ネットワークと転送ネットワークは次のように接続されます。

特定のグループ範囲、または全グループ範囲（デフォルトルートと同様）について、サービスプロバイダーは、RP-A などのランデブー ポイント（RP）を定義します。 コンシューマ デバイスから RP-A のリバース パス転送により、（*,G）加入が転送ネットワークに向けて送信されます。

同じグループに対して、サービス プロバイダーは、G の転送ネットワーク内で共有ツリーを構築するために使用される異なる RP（RP-B など）を定義することができます。 RP-A と RP-B は、通常異なる RP であり、各 RP は、異なるグループ範囲に対して定義されます。

RFC 4601 では、デバイスが（*, G）加入を受信し、（*, G）加入で指定されている RP が受信側デバイスが予想する RP と異なる（不明な RP）場合、着信（*, G）加入を無視する必要があることを規定しています。 PIM Allow RP 機能では、着信（*, G）加入が処理され、異なる RP が識別されたときに、受信側デバイスで独自の RP を使用してステートを作成し、共有ツリーを構築することができます。 これにより、受信側デバイスは異なる RP からの（*, G）加入を受け入れることができます。

PIM Allow RP は、共有ツリーを構築するためのダウンストリーム トラフィックだけに適用できます。 Auto-RP や BSR では機能しません。 スタティック設定だけがサポートされています。 ただし、PIM Allow RP では、コンシューマ ネットワークの組み込み RP が転送ネットワークに静的に設定されているものと異なる場合は補正されます。

PIM Allow RP の設定方法

PIM-SM への RP 設定

はじめる前に

すべてのアクセス リストを設定作業の開始前に設定する必要があります。 アクセス リストの設定方法については、『*Security Configuration Guide: Access Control Lists*』の「Creating an IP Access List and Applying It to an Interface」モジュールを参照してください。

IPv6 ネットワーク デバイスの場合は、最初に IPv6 マルチキャスト ルーティングをイネーブルにするデバイスのすべてのインターフェイスで、IPv6 ユニキャスト ルーティングをイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. • **ip multicast-routing** [**vrf** *vrf-name*] **distributed**
   • **ipv6 multicast-routing** [**vrf** *vrf-name*]
4. **interface** *type number*
5. • **ip pim sparse-mode**
   • **ipv6 pim enable**
6. **ipv6 address** {*ipv6-address* | *prefix-length* | *prefix-name sub-bits* | *prefix-length*}
7. **no shut**
8. **exit**
9. IP マルチキャストを使用するすべてのインターフェイスでステップ 4 ～ 8 を繰り返します。
10. • **ip pim** [**vrf** *vrf-name*] **rp-address** *rp-address* [*access-list*] [**override**]
    • **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*]
11. **exit**
12. **show ip pim rp** [**mapping**] [*rp-address*]
13. **show ip mroute**

手順の詳細

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

ステップ 3	• **ip multicast-routing** [**vrf** *vrf-name*] **distributed**
	• **ipv6 multicast-routing** [**vrf** *vrf-name*]
	
	例：
	`Device(config)# ip multicast-routing`
	`Device(config)# ipv6 multicast-routing`
		• IPv4 の場合：デバイスのすべてのインターフェイスでマルチキャスト ルーティングをイネーブルにします。Cisco IOS XE Release 3.2S 以前のリリースでは、**distributed** キーワードは任意選択です。
		• IPv6 の場合：デバイスのすべてのインターフェイスでマルチキャスト ルーティングをイネーブルにし、デバイスのすべてのマルチキャスト対応インターフェイス

	コマンドまたはアクション	目的
		で PIM および MLD に対してマルチキャスト転送をイネーブルにします。 （注） IPv6 マルチキャスト ルーティングは、IPv6 ユニキャスト ルーティングがイネーブルの場合、デフォルトでディセーブルです。 特定のデバイスでは、IPv6 ユニキャスト ルーティングを使用するには、IPv6 マルチキャスト ルーティングもイネーブルにする必要があります。
ステップ 4	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/0`	PIMをイネーブルにできるホストに接続されているインターフェイスを選択します。

ステップ 5	• **ip pim sparse-mode**
	• **ipv6 pim enable**
	
	例：
	`Device(config-if)# ip pim sparse-mode`
	`Device(config-if)# ipv6 pim enable`
		• IPv4 の場合：PIM をイネーブルにします。 スパースモードを使用する必要があります。
		• IPv6 の場合：IPv6 およびデフォルトで、IPv6 PIM をイネーブルにします。

ステップ 6	**ipv6 address** {*ipv6-address* | *prefix-length* | *prefix-name sub-bits* | *prefix-length*} 例： `Device(config-if)# ipv6 address 2001:DB8::4:4/64`	IPv6 の場合のみ：IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 7	**no shut** 例： `Device(config-if)# no shut`	インターフェイスをイネーブルにします。
ステップ 8	**exit** 例： `Device(config-if)# exit`	— グローバル コンフィギュレーション モードに戻ります。
ステップ 9	IPマルチキャストを使用するすべてのインターフェイスでステップ 4 ～ 8 を繰り返します。	

	コマンドまたはアクション	目的

ステップ 10	• **ip pim** [**vrf** *vrf-name*] **rp-address** *rp-address* [*access-list*] [**override**]
	• **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*]
	
	例：
	`Device(config)# ip pim rp-address 192.0.2.1 acl-sparse`
	
	`Device(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1`
		• IPv4 の場合：PIM RP のアドレスを設定します。 アクセス リストを指定しなかった場合、RP アドレスはすべてのマルチキャスト グループ 224/4 に適用されます。
		• IPv6 の場合：PIM RP のアドレスを設定します。 グループ アドレス リストを指定しなかった場合、FFX[3-f]::/8 から FF3X::/96 の範囲の SSM を除く、ルーティング可能な IPv6 マルチキャスト グループ範囲全体に RP アドレスが適用されます。

ステップ 11	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 12	**show ip pim rp** [**mapping**] [*rp-address*] 例： `Device# show ip pim rp mapping`	（任意）ネットワークで既知の RP を表示し、ルータが各 RP について学習する方法を示します。
ステップ 13	**show ip mroute** 例： `Device# show ip mroute`	（任意）IP mroute テーブルの内容を表示します。

PIM Allow RP のイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. • **ip pim allow-rp** [**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]]
   • **ipv6 pim allow-rp** [**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]]
4. **exit**

手順の詳細

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

ステップ 3	• **ip pim allow-rp** [**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]]
	• **ipv6 pim allow-rp** [**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]]
	
	例：
	`Device(config)# ip pim allow-rp`
	`Device(config)# ipv6 pim allow-rp`
		PIM Allow RP をイネーブルにします。

ステップ 4	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。

PIM-SM および RP に関する情報の表示

手順の概要

1. **enable**
2. • **show ip pim** [**vrf** *vrf-name*] **rp** [**metric**] [*rp-address*]
   • **show ipv6 pim** [**vrf** *vrf-name*] **interface** [**state-on**] [**state-off**] [*type number*]
3. • **show ip pim** [**vrf** *vrf-name*] **rp mapping** [*rp-address*]
   • **show ipv6 pim** [**vrf** *vrf-name*] **group-map** [*group-name* | *group-address*] | [*group-range* | *group-mask*] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}]

手順の詳細

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

ステップ 2	• **show ip pim** [**vrf** *vrf-name*] **rp** [**metric**] [*rp-address*]
	• **show ipv6 pim** [**vrf** *vrf-name*] **interface** [**state-on**] [**state-off**] [*type number*]
	
	例：
	`Device# show ip pim interface`
	`Device# show ipv6 pim interface`
		PIM に対して設定されたインターフェイスに関する情報を表示します。

ステップ 3	• **show ip pim** [**vrf** *vrf-name*] **rp mapping** [*rp-address*]
	• **show ipv6 pim** [**vrf** *vrf-name*] **group-map** [*group-name* | *group-address*] | [*group-range* | *group-mask*] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}]
	
	例：
	`Device# show ipv6 pim rp mapping`
	`Device# show ipv6 pim group-map static`
		PIM グループとアクティブ ランデブー ポイントのマッピングを表示します。

PIM Allow RP の設定例

例：IPv4 PIM Allow RP

次の例で、

1. ダウンストリーム デバイスのループバック（Loopback100）で、存在しない RP（11.30.3.3）に対してスタティック（*,239.1.2.3）加入が作成されます。
2. スタティック ルートでは、デバイスがこの RP は 11.10.2.1 経由でアップストリーム デバイスを介して到達可能であると認識するため、ダウンストリームデバイスはRPアドレス（11.30.3.3）を持つ（*,239.1.2.3）PIM 加入をアップストリーム ルータに送信します。

3 アップストリーム デバイスは（* 239.1.2.3）PIM 加入を受信すると、加入（11.30.3.3）内の RP アドレスが既知の（設定済みの）インターフェイスから RP へのアドレス（11.10.3.3）と異なることを認識します。

4 アップストリーム デバイス上の PIM Allow RP 設定により（*,239.1.2.3）が処理され、RP（11.10.3.3）への（239.1.2.3）加入が作成されます。

（注） アップストリーム デバイスで **pim allow-rp** コマンドが設定されていない場合、アップストリーム デバイスは異なる RP の加入を無視する必要があります。

```
##################
#   Downstream
##################
!
hostname downstream-router
!
!
ip multicast-routing distributed
!
!
interface Loopback100
ip address 101.10.1.2 255.255.255.0
ip igmp static-group 239.1.2.3
ip pim sparse-dense-mode
no shut
!
interface Ethernet1/2
ip address 11.10.2.2 255.255.255.0
ip pim sparse-dense-mode
no shut
!
router ospf 200
network 11.0.0.0 0.255.255.255 area 1
network 101.0.0.0 0.255.255.255 area 1
!
ip pim rp-address 11.30.3.3
ip mroute 11.30.3.3 255.255.255.255 11.10.2.1
!
end


##################
#   Upstream
##################
!
hostname Upstream-router
!
!
ip multicast-routing distributed
!
!
interface FastEthernet0/0/2
ip address 11.10.2.1 255.255.255.0
ip pim sparse-dense-mode
no shut
!
interface FastEthernet0/0/4
! interface to RP (11.10.3.3)
ip address 10.10.4.1 255.255.255.0
ip pim sparse-dense-mode
no shut
!
router ospf 200
network 10.0.0.0 0.255.255.255 area 1
network 11.0.0.0 0.255.255.255 area 1
```

```
!
ip pim rp-address 11.10.3.3
ip pim allow-rp
!
end
```

例：IPv6 PIM Allow RP

次の例で、

1. ダウンストリーム デバイスのループバックで、存在しない RP（80::1:1:3）へのスタティック（*,FF03::1）加入が作成されます。
2. スタティック ルートでは、デバイスがこの RP は 10::1:1:1 経由でアップストリーム デバイスを介して到達可能であると認識するため、ダウンストリームデバイスはRPアドレス（80::1:1:3）を持つ（*,FF03::1）PIM 加入をアップストリーム デバイスへ送信します。
3. アップストリーム デバイスは（*,FF03::1）PIM 加入を受信すると、加入（80::1:1:3）内の RP アドレスが（既知の）設定されたアドレス（20::1:1:3）とは異なることを認識します。
4. アップストリーム デバイス上の PIM Allow RP 設定により（*,FF03::1）が処理され、RP（20::1:1:3）への（*,FF03::1）加入が作成されます。

（注） アップストリームデバイスで**pim allow-rp** コマンドが設定されていない場合、アップストリーム デバイスは異なる RP の加入を無視する必要があります。

```
##################
# Downstream
##################

!
hostname downstream-router
!
!
ipv6 unicast-routing
ipv6 multicast-routing
!
!
interface Loopback100
ipv6 address FE80::50:1:2 link-local
ipv6 address 50::1:1:2/64
ipv6 enable
ipv6 ospf 1 area 0
ipv6 mld join-group FF03::1
!
interface Ethernet1/2
ipv6 address FE80::10:1:2 link-local
ipv6 address 10::1:1:2/64
ipv6 enable
ipv6 ospf 1 area 0
no keepalive
!
!
ipv6 pim rp-address 80::1:1:3
ipv6 route 80::1:1:3/128 10::1:1:1 multicast
!
ipv6 router ospf 1
router-id 205.2.0.2
```

```
!
!
end


###################
#  Upstream
###################
!
hostname Upstream-router
!
!
ipv6 unicast-routing
ipv6 multicast-routing
!
!
interface FastEthernet0/0/2
ipv6 address FE80::10:1:1 link-local
ipv6 address 10::1:1:1/64
ipv6 enable
ipv6 ospf 1 area 0
!
interface FastEthernet0/0/3
! interface to the RP (20::1:1:3)
ipv6 address FE80::20:1:1 link-local
ipv6 address 20::1:1:1/64
ipv6 enable
ipv6 ospf 1 area 0
!
!
ipv6 pim rp-address 20::1:1:3
ipv6 pim allow-rp
!
ipv6 router ospf 1
router-id 205.1.0.1
!
!
end
```

PIM Allow RP の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 4601	『*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

PIM Allow RP に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *6*：***PIM Allow RP*** に関する機能情報

機能名	リリース	機能情報
PIM Allow RP	15.2(4)T Cisco IOS XE Release 3.7S 15.3(1)T	PIM Allow RP 機能では、着信（*, G）加入が処理され、異なる RP が識別されたときに、受信側デバイスで独自の RP を使用してステートを作成し、共有ツリーを構築することができます。 このプロセスにより、受信側デバイスは異なる RP からの（*, G）加入を受け入れることができます。 次のコマンドが導入または変更されました。**ip pim allow-rp**、**ipv6 pim allow-rp**。

第 6 章

Source Specific Multicast の設定

このモジュールでは、Source Specific Multicast（SSM）の設定方法を説明します。 Source Specific Multicast 機能は、レシーバが明示的に参加したマルチキャスト ソースからのみデータグラム トラフィックがレシーバに転送される IP マルチキャストの拡張機能です。 SSM 用に設定されたマルチキャスト グループは、（共有ツリーではなく）ソース固有のマルチキャスト配信ツリーのみが作成されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

Source Specific Multicast の制約事項

SSM 範囲のレガシー アプリケーションに関する制約

SSM にまだ対応していない、ネットワーク内の既存のアプリケーションは、（S, G）チャネル加入をサポートするように変更されているか、URD によってイネーブルになっていない限り、SSM 範囲内では機能しません。 そのため、既存のアプリケーションが指定の SSM 範囲内のアドレスを使用する場合、ネットワークで SSM をイネーブルにすると問題が発生することがあります。

IGMP v3lite および URD には Cisco ラスト ホップ ルータが必要

SSM および IGMPv3 は IETF で標準化されたソリューションです。 しかし、IGMP v3lite と URD はシスコが開発したソリューションです。 ホストの IGMP v3lite と URD が正しく動作するには、そのホスト方向のラスト ホップ ルータが IGMP v3lite または URD がイネーブルになった Cisco ルータである必要があります。

（注） ホストが IGMPv3 のカーネル サポートを備えている場合、HSIL は IGMP v3lite の代わりにカーネル IGMPv3 を使用するため、この制約は HSIL を使用しているアプリケーションには適用されません。

アドレス管理に関する制約

SSM をレイヤ 2 スイッチング メカニズムとともに使用する場合は、ある程度のアドレス管理が必要となります。 Cisco Group Management Protocol（CGMP）、IGMP スヌーピング、または Router-Port Group Management Protocol（RGMP）は現在、（S, G）チャネル固有のフィルタリングではなく、グループ固有のフィルタリングのみをサポートしています。 スイッチド ネットワークの別のレシーバが、同じグループを共有している別の（S, G）チャネルを要求すると、これらの既存のメカニズムの利点は活用できません。 代わりに、両方のレシーバが (S, G) チャネル トラフィックをすべて受信（入力で不要なトラフィックをフィルタリング）します。 SSM は SSM 範囲のグループ アドレスを多くの独立したアプリケーションに再利用できるため、この状況により、スイッチド ネットワークでトラフィック フィルタリングが予想を下回る可能性があります。 このため、SSM の IETF ドラフトに記載されている推奨事項に従い、SSM 範囲外のランダム IP アドレスをアプリケーションに使用し、SSM 範囲内で異なるアプリケーションが 1 つのアドレスを再利用する可能性を最小限に抑えることが重要です。 たとえば、TV チャネル セットを提供するアプリケーション サービスで、SSM を使用する場合は、各 TV（S, G）チャネルに異なるグループを使用する必要があります。 この設定によって、同じアプリケーション サービス内の異なるチャネルの複数のレシーバがレイヤ 2 スイッチを含むネットワーク内でトラフィックのエイリアスを経験することがなくなります。

IGMP スヌーピングおよび CGMP の制限

IGMPv3 は、古い IGMP スヌーピング スイッチに正しく認識されない可能性のある新しいメンバーシップ レポート メッセージを使用します。この場合、ホストがトラフックを正しく受信しませ

ん。 IGMP v3lite と URD は IGMPv1 または IGMPv2 メンバーシップ レポートのみに依存するため、この状況は、URD または IGMP v3lite がオペレーティング システムが IGMPv3 用にアップグレードされていないホストで使用されている場合は問題ではありません。

URD インターセプト URL の制約事項

URD インターセプト URL の文字列は 256 バイト未満で、*/path* 引数で始まる必要があります。 HTTP/TCP 接続では、この文字列は単一の TCP/IP パケット内に含まれている必要もあります。 たとえば、256 バイトの文字列の場合、ホストと代行受信ルータ間のリンク最大伝送単位（MTU）が 128 バイトでは、URD が正しく動作しません。

ステート管理の制限事項

PIM-SSM で、適切な（S, G）加入がインターフェイス上にある場合、ラスト ホップ ルータは（S, G）加入メッセージを定期的に送り続けます。 このため、レシーバが（S, G）加入を送信する限り、ソースが長時間（または二度と）トラフィックを送信しなくてもレシーバからソースへの最短パス ツリー（SPT）状態が維持されます。

これは、送信元がトラフィックを送信し、レシーバーがグループに加入している場合にだけ（S, G）ステートが維持される PIM-SM とは対照的です。 PIM-SM では、送信元がトラフィックの送信を 3 分間停止すると、（S, G）ステートは削除され、再確立されるのは、その送信元からのパケットが RPT を通じて再度到達した場合だけです。 PI-SSM では、送信元がアクティブであることをレシーバに通知するメカニズムがないので、レシーバが（S, G）チャネルの受信を要求している限り、（S, G）ステートを維持する必要があります。

HSIL の制限事項

IGMP v3lite ホスト シグナリング, （182 ページ）の概要で説明されているように、HSIL はホスト オペレーティング システムが IGMPv3 をサポートするかどうかを判別しようとします。 このチェックは、オペレーティング システムが IGMPv3 にアップグレードされているホストとオペレーティング システムが IGMPv1 または IGMPv2 のみをサポートするホストの両方で単一のアプリケーションが使用できるように行われます。

HSIL が提供された時点でこのオペレーティング システムの少なくとも 1 つのバージョンに対して IGMPv3 カーネル サポートが存在する場合、ホスト オペレーティング システムでの IGMPv3 のアベイラビリティのチェックは、HSIL でのみ実行できます。 このような IGMPv3 カーネル実装が最近まで使用できなかった場合、HSIL でコンパイルされたアプリケーションが動的に最新バージョンの HSIL にバインドされるように、ユーザはホストで HSIL もアップグレードする必要のある場合があります。最新バージョンの HSIL は、オペレーティング システム カーネルで IGMPv3 のチェックをサポートしています。 HSIL のアップグレードは、アプリケーション自体のアップグレードとは別に実行できます。

Source Specific Multicast について

SSM の概要

Source Specific Multicast（SSM）。 SSM は、レシーバが明示的に参加したマルチキャスト ソースからのみデータグラム トラフィックがレシーバに転送されるIPマルチキャストの拡張機能です。 SSM 用に設定されたマルチキャスト グループは、（共有ツリーではなく）ソース固有のマルチキャスト配信ツリーのみが作成されます。

SSM のコンポーネント

SSM は、1 対多のアプリケーション（ブロードキャスト アプリケーション）に最適なデータグラム配信モデルです。 SSM は、オーディオおよびビデオ ブロードキャスト アプリケーション環境を対象とした IP マルチキャスト ソリューションの Cisco 実装のコア ネットワーキング テクノロジーで、RFC 3569 に説明されています。 次の 2 つのコンポーネントは共に SSM の実装をサポートします。

- Protocol Independent Multicast Source-Specific Mode（PIM-SSM）
- インターネット グループ管理プロトコル バージョン 3（IGMPv3）

Protocol Independent Multicast（PIM）SSM（PIM-SSM）は、SSM の実装をサポートするルーティング プロトコルで、PIM スパース モード（PIM-SM）から派生しました。 IGMP は、ホストがルータにマルチキャスト グループ メンバーシップを伝えるために使用するインターネット技術特別調査委員会（IETF）標準トラック プロトコルです。 IGMP バージョン 3 は、SSM に必要なソース フィルタリングをサポートします。 SSM を IGMPv3 と共に実行するには、SSM がルータ、アプリケーションが実行されるホスト、およびアプリケーション自体でサポートされる必要があります。

Internet Standard Multicast と SSM の違い

インターネットと多くの企業イントラネットの標準IPマルチキャストインフラストラクチャは、PIM-SM プロトコルと Multicast Source Discovery Protocol（MSDP）に基づいています。 これらのプロトコルは信頼でき、広範で、効率的であることが証明されています。 しかし、インターネット標準マルチキャスト（ISM）サービス モデルの複雑さと機能性の制限があります。 たとえば、ISM では、ネットワークは、実際にマルチキャスト トラフィックを送信しているホストについての情報を維持する必要があります。 SSM では、この情報は IGMPv3 によってラスト ホップ デバイスにリレーされるソース アドレスを通してレシーバによって提供されます。 SSM は、ISM に関連付けられた問題への対応を強化し、ネットワーク内で ISM 用に開発されたプロトコルと共存することを目的としています。 一般に、SSM は SSM を使用するアプリケーションに IP マルチキャスト サービスを提供します。

ISM サービスについては RFC 1112 で説明されています。 このサービスは、任意のソースからマルチキャスト ホスト グループと呼ばれるレシーバのグループへの IP データグラムの配信によって構成されています。 マルチキャスト ホスト グループのデータグラム トラフィックは、任意の IP ユニキャスト送信元アドレス S と IP 宛先アドレスとしてのマルチキャスト グループ アドレス G のデータグラムで構成されます。 システムはホスト グループのメンバになることによってこのトラフィックを受信します。 ホスト グループのメンバーシップには IGMP バージョン 1、2、または 3 によるホスト グループのシグナリングが必要です。

SSM では、データグラムは（S, G）チャネルに基づいて配信されます。 1 つの (S, G) チャネルのトラフィックは、IP 宛先アドレスとして IP ユニキャスト ソース アドレス S とマルチキャスト グループ アドレス G を持つデータグラムで構成されています。 システムは、（S, G）チャネルのメンバになることによって、このトラフィックを受信します。 SSM と ISM のどちらでも、ソースになるためにシグナリングは必要ありません。ただし、SSM では、レシーバーは特定の送信元からのトラフィックの受信または非受信を決めるために（S, G）への加入または脱退を行う必要があります。 つまり、レシーバーは加入した（S, G）チャネルからだけトラフィックを受信できます。一方、ISM では、レシーバーは受信するトラフィックの送信元の IP アドレスを知る必要はありません。 提案されているチャネル加入シグナリングの標準的な方法では、IGMP INCLUDE モード メンバーシップ レポートを使用します。これは、IGMP バージョン 3 でのみサポートされています。

IP マルチキャスト グループ アドレス範囲の設定済みのサブセットに SSM 配信モデルを適用することにより、SSM と ISM サービスを一緒に使用できます。インターネット割り当て番号局（IANA）は、SSM アプリケーションおよびプロトコル用に 232.0.0.0 ～ 232.255.255.255 のアドレス範囲を確保しています。 ソフトウェアでは、224.0.0.0 ～ 239.255.255.255 の IP マルチキャスト アドレス範囲の任意のサブセットの SSM 設定を許可します。 SSM 範囲が定義されると、（アプリケーションが明示的な（S, G）チャネル加入を使用するように変更されているか、URL Rendezvous Directory（URD）によって SSM に対応していない限り）SSM 範囲内でアドレスを使用しようとする場合に既存の IP マルチキャスト レシーバ アプリケーションはトラフィックを受信しません。

SSM の動作

確立されているネットワークは、IP マルチキャスト サービスが PIM SM に基づいているので、SSM サービスをサポートできます。 SSM は、ドメイン間の PIM-SM に必要なプロトコルがすべて揃っていないネットワークで単独で配備することもできます。 つまり、SSM には RP が必要ではないため、Auto-RP、MSDP、ブートストラップ ルータ（BSR）などの RP メカニズムは必要ありません。

SSM がすでに PIM-SM 用に設定済みのネットワークで配備されている場合、ラスト ホップ ルータのみを、SSM をサポートするソフトウェア イメージにアップグレードする必要があります。 レシーバに直接接続されていないルータを SSM をサポートするソフトウェア イメージにアップグレードする必要はありません。 一般的に、これらのラスト ホップではないルータは、SSM 範囲で PIM-SM のみを実行する必要があります。 これらは、MSDP シグナリング、登録、または PIM-SM 共有ツリー動作が SSM 範囲内で発生することを抑制するために、追加のアクセス コントロール設定を必要とする場合もあります。

SSM モードの動作は、**ip pim ssm** グローバル コンフィギュレーション コマンドを使用して SSM 範囲を設定することによってイネーブルにできます。 この設定による影響は次のとおりです。

- SSM 範囲内のグループの場合、(S, G) チャネル加入は IGMPv3 INCLUDE モード メンバーシップ レポートによって受け入れられます。
- SSM 範囲のアドレスの PIM 動作は、PIM-SM の派生モードである PIM-SSM に変更されます。このモードでは、PIM (S, G) 加入およびプルーニング メッセージのみがルータによって生成されます。 ランデブー ポイント ツリー（RPT）動作に関連した着信メッセージは無視されるか、拒否され、着信 PIM 登録メッセージは登録停止メッセージによってただちに応答されます。 ラストホップ ルータ以外のルータでは、PIM-SSM は PIM-SM と下位互換性を保ちます。 したがって、ラストホップ ルータ以外のルータは SSM グループに PIM-SM を使用できます（SSM をサポートしていない場合など）。
- SSM 範囲内のグループの場合、SSM 範囲内の MSDP Source-Active（SA）メッセージは受け入れ、生成、または転送されません。

IGMPv3 ホスト シグナリング

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

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

Source Specific Multicast の利点

IP マルチキャスト アドレス管理が不要

ISM サービスで、トラフィック ディストリビューションは使用する IP マルチキャスト グループ アドレスにのみ基づくため、アプリケーションは一意の IP マルチキャスト グループ アドレスを取得する必要があります。 異なるソースとレシーバを持つ 2 つのアプリケーションが同じ IP マルチキャスト グループ アドレスを使用すると、両方のアプリケーションのレシーバが両方のアプリケーションのソースからトラフィックを受信します。 適切にプログラムしている場合、レシーバは不要なトラフィックをフィルタできますが、この状態は一般的に許容できないレベルの不要なトラフィックを生み出します。

アプリケーションへの一意の IP マルチキャスト グループ アドレスの割り当ては問題となります。最も短期のアプリケーションはセッション記述プロトコル（SDP）やセッション通知プロトコル（SAP）のようなメカニズムを使用して、ランダム アドレスを取得します。これは、インターネット内のアプリケーションの増加によってうまく機能しないソリューションです。 長期アプリケーションの現在のベスト ソリューションは、RFC 2770 に説明されていますが、このソリューションは各自律システムが 255 の使用可能な IP マルチキャスト アドレスのみに限定される制限の影響を受けます。

SSM で、他のソースからのトラフィックとは関係なく、各ソースからのトラフィックはネットワーク内のルータ間で転送されます。 このため、異なるソースが SSM 範囲のマルチキャスト グループ アドレスを再利用できます。

望ましくないソースからのサービス拒否攻撃の阻止

SSM で、個別の各ソースからのマルチキャスト トラフィックは、（IGMPv3、IGMP v3lite、またはURD メンバーシップによって）レシーバから要求された場合にのみネットワーク中に転送されます。 これに対し、ISM はマルチキャスト グループに送信するアクティブなソースからそのマルチキャスト グループを要求するすべてのレシーバにトラフィックを転送します。インターネット ブロードキャスト アプリケーションで、トラフィックを同じマルチキャスト グループにただ送信するだけで、望ましくないソースが実際のインターネット ブロードキャスト ソースを簡単に妨害できるため、この ISM の動作は非常に望ましくありません。 この状況は、レシーバ側で不要なトラフィックによって帯域幅を消耗させるため、インターネット ブロードキャストの無停止の受信を妨害します。 SSM では、トラフィックをマルチキャスト グループにただ送信するだけでは、このような種類の DoS 攻撃は行えません。

インストールと管理が容易

ネットワークがマルチキャスト グループに送信しているアクティブ ソースについての情報を維持する必要がないため、SSM は簡単にインストールし、ネットワークでプロビジョニングできます。 この要件は、（IGMPv1、IGMPv2、または IGMPv3 を使用する）ISM でのみ存在します。

ISM サービスの現在の標準ソリューションは PIM-SM と MSDP です。 PIM-SM（Auto-RP または BSR の必要性を含む）および MSDP での Rendezvous Point（RP）管理は、ネットワークがアクティブ ソースについて学習するためにのみ必要です。 この管理は SSM では必要ありません。このため、SSM は ISM よりインストールや管理が簡単で、配備での動作面の拡張も ISM より簡単です。SSM のインストールが簡単であるその他の要素は、既存の PIM-SM ネットワークを活用でき、ラスト ホップ ルータをアップグレードするだけで IGMPv3、IGMP v3lite、または URD をサポートできる点です。

インターネット ブロードキャスト アプリケーションに最適

上記の 3 つの利点により、次の理由で SSM はインターネット ブロードキャスト スタイルのアプリケーションに理想的です。

- 一意の IP マルチキャスト アドレスなしで SSM によって、インターネット ブロードキャスト サービスを提供できるため、コンテンツ プロバイダーはサービスを簡単に提供できます（コンテンツ プロバイダーにとって、IP マルチキャスト アドレス割り当てはこれまで深刻な問題でした）。
- インターネット ブロードキャスト サービスは多数のレシーバに公開されることにより、DoS 攻撃の最も一般的な対象となるため、このような攻撃の阻止はインターネット ブロードキャスト サービスの重要な要素です。
- SSM はインストールや動作が簡単なため、特に、コンテンツを複数の独立した PIM ドメイン間で転送する必要のある場合（SSM のために PIM ドメイン間で MSDP を管理する必要がないため）、ネットワーク オペレータにとって理想的です。

IGMP v3lite ホスト シグナリング

IGMP v3liteは、SSMアプリケーションのプログラミングをすぐに開始できるように、アプリケーション開発者向けにシスコが開発した移行ソリューションです。 これによって、オペレーティング システム カーネルでIGMPv3をサポートしていないホストでSSMアプリケーションを記述し、実行できます。

IGMP v3liteの場合、アプリケーションはHost Side IGMP Library（HSIL）でコンパイルする必要があります。 このソフトウェアは、SSMアプリケーションの記述に必要なIGMPv3アプリケーション プログラミング インターフェイス（API）のサブセットをアプリケーションに提供します。 HSIL は Talarian によってシスコ用に開発され、次の Web ページで入手できます。

http://www.talarianmulticast.com/cgi-bin/igmpdownld

HSIL の一部は SSM アプリケーションにリンクされているクライアント ライブラリです。 これは、IGMPv3 API の SSM のサブセットを SSM アプリケーションに提供します。 可能な場合は、オペレーティング システム カーネルがIGMPv3をサポートしているかどうかをライブラリがチェックします。 サポートしている場合、API コールはそのままカーネルに渡されます。 カーネルが IGMPv3 をサポートしない場合、ライブラリは、IGMP v3lite メカニズムを使用します。

IGMP v3lite メカニズムを使用している場合、ライブラリはオペレーティング システム カーネルにマルチキャスト グループ全体に参加するように呼びかけます。これは、（オペレーティング システム カーネルが IGMPv1 または IGMPv2 のみをサポートしている場合）グループ全体に参加することが、アプリケーションがそのマルチキャスト グループのトラフィックを受信する唯一の方法であるためです。 また、ライブラリは IGMP v3lite サーバ プロセスに（S, G）チャネル加入を伝えます。これはHSILの一部でもあります。 複数のSSMアプリケーションが同じホスト上にある場合があるため、サーバ プロセスが必要です。 このサーバ プロセスは、その後、IGMP v3lite 固有の（S, G）チャネル加入をラスト ホップCisco IOSルータに送信します。これは、IGMP v3lite用にイネーブルにする必要があります。 このルータは、オペレーティング システム カーネルから IGMPv1 または IGMPv2 グループ メンバーシップ レポートを参照し、HSIL デーモンから（S, G）チャネル加入も参照します。 ルータが両方のメッセージを参照すると、これらをSSM（S, G）チャネル加入と解釈して、PIM-SSMによってチャネルに参加します。お使いのアプリケーションでの IGMP v3lite の使用方法の詳細については、HSIL ソフトウェアに付属しているマニュアルを参照することを推奨します。

IGMP v3liteは、HSILから独立したルータの機能としてではなく、HSILによるAPIを通してのみシスコからサポートされます。 デフォルトでは、IGMP v3liteはディセーブルになっています。 IGMP v3liteがインターフェイス上で **ip igmp v3lite** インターフェイス コンフィギュレーション コマンドによって設定されている場合、SSM範囲のIPマルチキャスト アドレスに対してのみアクティブになります。

URD ホスト シグナリング

URDはシスコが開発した移行ソリューションで、アプリケーションを変更したり、アプリケーションを実行しているレシーバ ホスト上のソフトウェアを変更または追加することなく、既存のIPマルチキャスト レシーバ アプリケーションをSSMと共に使用できます。 URDは、Webブラ

ウザからレシーバ アプリケーションを開始したり制御できるコンテンツ プロバイダー ソリューションです。

URD は、特殊な URL を Web ブラウザからラスト ホップ ルータに渡すことによって機能します。この URL は、URD インターセプト URL と呼ばれます。 URD インターセプト URL は、（S, G）チャネル加入で符号化され、ラストホップルータが簡単に代行受信できる形式になっています。

アプリケーションがマルチキャスト グループ G のメンバーシップを維持する限り、ラスト ホップ ルータが URD インターセプト URL で符号化された (S, G) チャネル加入を代行受信し、レシーバ アプリケーションから同じマルチキャスト グループの IGMP グループ メンバーシップ レポートを参照するとただちに、ラスト ホップ ルータが PIM-SSM を使用して (S, G) チャネルに参加します。 URD インターセプト URL は、当初、参加のためにソースのアドレスをラスト ホップ ルータに提供するためにのみ必要です。

URD インターセプト URL の構文は、次のとおりです。

```
http://
webserver
:465/
path
?group=
group
&source=
source1
&...source=
sourceN
&
```

webserver ストリングは、URL がターゲットとする名前または IP アドレスです。 ラスト ホップ ルータが URD メカニズムをサポートできないことを Web サーバが確認する場合以外は、このターゲットは既存の Web サーバの IP アドレスである必要はありません。 465 という番号は URD ポートを示します。 ポート 465 は、URD メカニズムのために IANA によってシスコ用に確保されています。このため、他のアプリケーションはこのポートを使用できません。

ホストのブラウザが URD インターセプト URL を検出すると、ポート 465 上で Web サーバへの TCP 接続を開こうとします。 ルータがホストから TCP パケットを受信するインターフェイスで URD 用にラスト ホップ ルータがイネーブルの場合、（Web サーバのアドレスとは関係のない）TCP 接続の実際の宛先アドレスから独立したポート 465 への TCP 接続のすべてのパケットを代行受信します。 代行受信すると、ラスト ホップ ルータはこの TCP 接続で HTTP の非常に単純なサブセットを伝え、Web サーバをエミュレートします。 ラスト ホップ ルータが理解し、応答する唯一の HTTP 要求は、次の GET 要求です。

```
GET
argument
 HTTP/1.0
argument
 = /
path
?group=
group
&source=
source1
&...source=
sourceN
&
```

GET コマンドを受信すると、ルータはこの構文に従って引数を解析し、1 つまたは複数の (S, G) チャネル メンバーシップを取得しようとします。 引数の *path* ストリングは、最初の疑問符まで

（最初の疑問符を含まない）で無視されます。 *group* と *source1* から *sourceN* までのストリングは、この引数が加入要求であるチャネルのIPアドレスまたは完全修飾ドメイン名です。引数が表示された構文に一致する場合、ルータは（*source1*、*group*）から（*sourceN*、*group*）チャネルに加入する引数を解釈します。

次の条件が満たされると、ルータはチャネル加入を受け入れます。

- マルチキャスト グループの IP アドレスは SSM 範囲内です。
- TCP 接続の元となるホストの IP アドレスはルータに直接接続されます。

チャネル加入が受け入れられると、ルータは次の HTML ページ形式で TCP 接続に応答します。

```
HTTP/1.1 200 OK
Server:cisco IOS
Content-Type:text/html
<html>
<body>
Retrieved URL string successfully
</body>
</html>
```

エラー状態が発生すると、返信 HTML ページの <body> 部分が適切なエラー メッセージを表示します。 HTML ページは URD メカニズムの副産物です。 URD インターセプト URL を表示する Web ページの設計方法に応じて、この返信テキストはユーザに表示されるか、または、実際の返信 HTML ページが表示されないようにサイズが決定されます。

URDメカニズムの主な影響は、ルータが受信したチャネル加入を記憶し、ホストによって受信された IGMP グループ メンバーシップ レポートと一致させます。 ルータは、IGMP グループ メンバーシップ レポートと一致させずに、URD (S, G) チャネル加入を 3 分まで記憶します。 ルータは、マルチキャスト グループ G の IGMP グループ メンバーシップ レポートと、同じグループ G のURD（S, G）チャネル加入の両方を受信したことを確認すると、すぐにPIM-SSMを介して（S, G）チャネルに参加します。 ルータは、ホストからの継続中の IGMP メンバーシップの存在だけに基づいて（S,G）チャネルへの参加を続けます。 このため、当初のURDチャネル加入は、URD で SSM をイネーブルにするために Web ページ経由で唯一追加される必要があります。

レシーバ ホストからのラスト ホップ ルータが URD に対してイネーブルでない場合、ポート 465 の Web サーバへの HTTP 接続は代行受信されません。 この状況により、Web サーバ上でポート 465 への TCP 接続が発生します。 Web サーバ上でさらにプロビジョニングが行われない場合、URD インターセプト URL を表示するための Web ページのエリアに（この出力を表示するように Web ページが設計されている場合）通知（「Connection refused」など）が表示される場合があります。 ポート 465 で Web サーバに要求を「リッスン」させ、Web サーバがチャネル加入が失敗したかどうかを知る（たとえば、後でより複雑なエラー説明をユーザに返信する）ことができる Common Gateway Interface（CGI）スクリプトをインストールすることもできます。

ルータはテキストと HTML のコンテンツタイプを返すため、URD インターセプト URL を Web ページに含める最善の方法は、フレームを使用する方法です。 フレームのサイズを定義することによって、表示されているページで URD インターセプト URL を非表示にすることもできます。

デフォルトでは、URDはすべてのインターフェイス上でディセーブルです。URDがインターフェイス上で **ip urd** インターフェイス コンフィギュレーション コマンドによって設定されている場合、SSM 範囲の IP マルチキャスト アドレスに対してのみアクティブになります。

Source Specific Multicast の設定方法

SSM の設定

SSM を設定するには、グローバル コンフィギュレーション モードを開始して次のコマンドを使用します。

手順の概要

1. Router(config)# **ip pim ssm** [**default** | **range***access-list*]
2. Router(config)# **interface** type number
3. Router(config-if)# **ip pim** {**sparse-mode** | **sparse-dense-mode**}
4. 次のいずれかを実行します。
   - Router(config-if)# **ip igmp version 3**
   -
   -
   -
   - Router(config-if)# **ip igmp v3lite**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **ip pim ssm** [**default** | **range***access-list*]	IP マルチキャスト アドレスの SSM 範囲を定義します。
ステップ 2	Router(config)# **interface** type number	IGMPv3、IGMP v3lite、および URD をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 3	Router(config-if)# **ip pim** {**sparse-mode** | **sparse-dense-mode**}	インターフェイス上の PIM をイネーブルにします。 sparse mode と sparse-dense mode のどちらかを使用する必要があります。
ステップ 4	次のいずれかを実行します。 • Router(config-if)# **ip igmp version 3** • • • • Router(config-if)# **ip igmp v3lite**	このインターフェイス上で IGMPv3 をイネーブルにします。デフォルトでは、IGMP のバージョン 2 が設定されます。 または インターフェイスで IGMP v3lite メンバーシップ レポートの受け入れと処理をイネーブルにします。 または

	コマンドまたはアクション	目的
	例： 例： 例： 例： `Router(config-if)# ip urd`	インターフェイスで確保された URD ポート 465 に送信された TCP パケットの代行受信と URD チャネル加入レポートの処理をイネーブルにします。

SSM のモニタリング

SSM をモニタするには、必要に応じて特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# show ip igmp groups detail`	IGMPv3、IGMP v3lite、または URD で (S, G) チャネル加入を表示します。
`Router# show ip mroute`	マルチキャスト グループが SSM サービスをサポートしているかどうか、またはソース固有のホスト レポートが受信されたかどうかを表示します。

Source Specific Multicast の設定例

IGMPv3 を使用した SSM の例

次の例は、SSM 用に（IGMPv3 を実行する）ルータを設定する方法を示しています。

```
ip multicast-routing
!
interface GigabitEthernet3/1/0
 ip address 172.21.200.203 255.255.255.0
```

```
 description backbone interface
 ip pim sparse-mode
!
interface GigabitEthernet3/2/0
 ip address 131.108.1.2 255.255.255.0
 ip pim sparse-mode
 description ethernet connected to hosts
 ip igmp version 3
!
ip pim ssm default
```

IGMP v3lite と URD を使用した SSM の例

次の例は、SSM 用にホストに接続されたインターフェイス上で IGMP v3lite と URD を設定する方法を示しています。 IGMP v3lite と URD の設定は、バックボーン インターフェイスでは必須でも推奨事項でもありません。

```
interface gigabitethernet 3/1/1
 ip address 172.21.200.203 255.255.255.0
 ip pim sparse-dense-mode
 description gigabitethernet connected to hosts
!
interface gigabitethernet 1/1/1
description gigabitethernet connected to hosts
 ip address 131.108.1.2 255.255.255.0
 ip pim sparse-dense-mode
 ip urd
 ip igmp v3lite
```

SSM フィルタリング例

次の例は、SSM ルーティングをサポートしないソフトウェア リリースを実行しているレガシー RP ルータでフィルタリングを設定する方法を示しています。 このフィルタリングは SSM 範囲で不要な PIM-SM および MSDP トラフィックをすべて抑制します。 このフィルタリングがなくても SSM は動作しますが、レガシーのファースト ホップ ルータとラスト ホップ ルータがネットワークに存在する場合、追加の RPT トラフィックがある場合があります。

```
ip access-list extended  no-ssm-range
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM range
  permit ip any any
! Deny registering in SSM range
ip pim accept-register list no-ssm-range
ip access-list extended msdp-nono-list
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM Range
  ! .
  ! .
  ! .
  ! See ftp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt for other SA
  ! messages that typically need to be filtered.
  permit ip any any
! Filter generated SA messages in SSM range. This configuration is only needed if there
! are directly connected sources to this router. The "ip pim accept-register" command
! filters remote sources.
ip msdp redistribute list msdp-nono-list
! Filter received SA messages in SSM range. "Filtered on receipt" means messages are
! neither processed or forwarded. Needs to be configured for each MSDP peer.
ip msdp sa-filter in msdp-peer1 list msdp-nono-list
! .
! .
! .
ip msdp sa-filter in msdp-peerN list msdp-nono-list
```

その他の関連資料

ここでは、Source Specific Multicast に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
PIM-SM と SSM の概念および設定例	「基本的な IP マルチキャスト設定」モジュール
IP マルチキャスト コマンド：コマンド構文の詳細、コマンドモード、デフォルト設定、コマンド履歴、使用に関する注意事項、および例	『*Cisco IOS IP Multicast Command Reference*』

標準

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

MIB

MIB	MIB のリンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能がサポートする新しい RFC または変更された RFC はありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

Source Specific Multicast の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *7*：***Source Specific Multicast*** の機能情報

機能名	リリース	機能情報
Source Specific Multicast（SSM）	12.3(4)T 12.2(25)S 12.0(28)S 12.2(33)SXH 12.2(33)SRA 15.0(1)S Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.1.0SG Cisco IOS XE Release 3.5S	SSM は、レシーバが明示的に参加したマルチキャスト ソースからのみデータグラム トラフィックがレシーバに転送される IP マルチキャストの拡張機能です。 SSM 用に設定されたマルチキャスト グループは、（共有ツリーではなく）ソース固有のマルチキャスト配信ツリーのみが作成されます。 Cisco IOS XE Release 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。

第 7 章

非IPマルチキャストエリアを接続するトンネリング

このモジュールでは、非 IP マルチキャスト エリア間で IP マルチキャスト パケットをトンネリングするための総称ルーティング カプセル化（GRE）トンネルの設定方法について説明します。その利点は、IP マルチキャストをサポートしないエリアを経由して、IP マルチキャスト トラフィックをソースからマルチキャスト グループに送信できることです。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

非IPマルチキャストエリアを接続するトンネリングの前提条件

このモジュールでは、「IPマルチキャストテクノロジーの概要」モジュールの概念を理解していることを前提としています。

非IPマルチキャストエリアを接続するトンネリングについて

非 IP マルチキャスト エリアを接続するトンネリングの利点

- ソースとグループ メンバ（宛先）間のパスで IP マルチキャストがサポートされていない場合、それらの間のトンネルで IP マルチキャスト パケットを転送できます。
- パケットごとのロード バランシングを使用できます。 IP マルチキャストのロード バランシングは、通常 (S, G) ごとです。 したがって、X と Y がパラレル リンクである場合、（S1, G）がリンク X を通過し、（S2, G）がリンク Y を通過します。 ルータ間にトンネルを作成すると、ロード バランシングはトンネル ユニキャスト パケットで行われるため、ロード バランシングをパケットごとにすることができます。

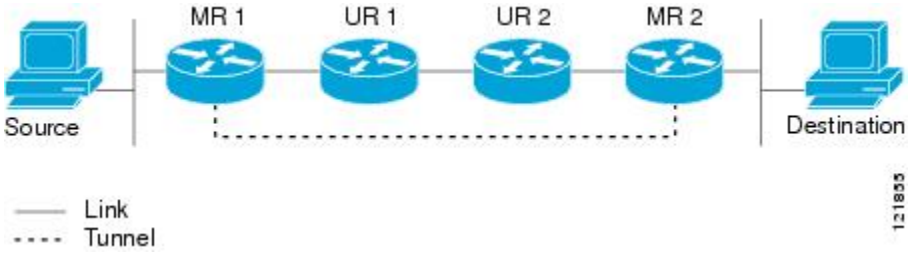
IP マルチキャスト スタティック ルート

IP マルチキャスト スタティック ルート（mroute）により、ユニキャスト パスを迂回するマルチキャスト パスを使用できます。 Protocol Independent Multicast（PIM）を使用する場合、ルータはユニキャスト パケットを発信元に返送するときと同じインターフェイスでパケットを受信することを想定しています。 この予測は、マルチキャスト トポロジとユニキャスト トポロジが一致する場合は有益です。しかし、ユニキャストパケットに使用するパスとは別のパスをマルチキャストに使用することも考えられます。

別々のユニキャストパスおよびマルチキャストパスを使用する最も一般的な理由はトンネリングです。 ソースと宛先の間のパスでマルチキャストルーティングがサポートされていない場合、解決策はこれらの間に 2 つのルータと GRE トンネルを設定することです。 図では、各ユニキャス

トルータ（UR）は、ユニキャストパケットだけをサポートし、各マルチキャストルータ（MR）はマルチキャスト パケットをサポートします。

図 *14*：マルチキャスト パケット用のトンネル



図では、Source は MR 1 および MR 2 を使用してマルチキャスト パケットを Destination に伝送します。 MR 2 は、トンネルを経由して Source に到達できることを確信している場合だけ、マルチキャスト パケットを受け取ります。 この状態では、Destination が Source にユニキャスト パケットを送信すると、MR2 はトンネルを経由してユニキャスト パケットを送信します。 MR2 がトンネルを経由して Source に到達できることのチェックは、リバース パス転送（RPF）チェックです。マルチキャストパケットが到着するインターフェイスがソースへのユニキャストパスでない場合、スタティック mroute によってこのチェックが成功します。 トンネル経由のパケット送信は、本来の UR 2、UR 1、および MR 1 を経由した送信よりも遅くなることがあります。

スタティック マルチキャスト ルートでは、スタティック マルチキャスト ソースを設定して、図の設定を使用することができます。 システムは、ユニキャスト ルーティング テーブルの代わりに設定情報を使用してトラフィックをルーティングします。 したがって、ユニキャストパケットにトンネルを使用させることなく、マルチキャスト パケットがトンネルを使用できます。 スタティック mroute は設定されたルータに対してローカルであり、その他のルータにアドバタイズまたは再配布されることはありません。

非 IP マルチキャスト エリアの接続方法

非 IP マルチキャスト エリアを接続するトンネリングの設定

マルチキャスト パスをユニキャスト パスとは異なるものにする場合は、マルチキャスト スタティック ルートを設定します。 たとえば、ソースと宛先間のユニキャスト パスでマルチキャスト ルーティングがサポートされていないために、2 台のルータ間にトンネルを設定する場合があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip unnumbered** *type number*
5. **ip pim sparse-mode**
6. **tunnel source** {*ip-address* | *type number*}
7. **tunnel destination** {*hostname* | *ip-address*}
8. トンネルの送信元アドレスとトンネルの宛先アドレスを逆にして、トンネルの反対側のルータでステップ 1～7 を繰り返します。
9. **end**
10. **ip mroute** *source-address mask* **tunnel** *number* [*distance*]
11. **ip mroute** *source-address mask* **tunnel** *number* [*distance*]
12. **end**
13. **show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*]
14. **show ip rpf** {*source-address* | *source-name*} [**metric**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface tunnel** *number* 例： `Router(config)# interface tunnel 0`	トンネル インターフェイスを設定します。
ステップ 4	**ip unnumbered** *type number* 例： `Router(config-if)# ip unnumbered gigabitethernet 0/0/0`	インターフェイスに IP アドレスを割り当てないで、IP 処理をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**ip pim sparse-mode** 例： `Router(config-if)# ip pim sparse-mode`	トンネル インターフェイスで PIM スパース モードをイネーブルにします。
ステップ 6	**tunnel source** {*ip-address* | *type number*} 例： `Router(config-if)# tunnel source 100.1.1.1`	トンネル送信元を設定します。
ステップ 7	**tunnel destination** {*hostname* | *ip-address*} 例： `Router(config-if)# tunnel destination 100.1.5.3`	トンネル宛先を設定します。
ステップ 8	トンネルの送信元アドレスとトンネルの宛先アドレスを逆にして、トンネルの反対側のルータでステップ1～7を繰り返します。	ルータ A のトンネルの送信元アドレスは、ルータ B のトンネルの宛先アドレスに一致します。 ルータ A のトンネルの宛先アドレスは、ルータ B のトンネルの送信元アドレスに一致します。
ステップ 9	**end** 例： `Router(config-if)# end`	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 10	**ip mroute** *source-address mask* **tunnel** *number* [*distance*] 例： `Router(config)# ip mroute 0.0.0.0 0.0.0.0 tunnel 0`	トンネルの反対側にリバース パス転送するために、スタティック マルチキャスト ルートを設定します。 • トンネルの使用によって、マルチキャスト トポロジがユニキャスト トポロジと一致しなくなり、マルチキャスト トラフィックだけがトンネルを通過できるため、トンネルを正しくリバース パス転送するようにルータを設定する必要があります。 • 送信元範囲が指定されている場合、mroute はこれらの送信元にだけ適用されます。 • この例では、*source-address* および *mask* は 0.0.0.0、0.0.0.0 であり、これは任意のアドレスを意味します。 • より短い距離が優先されます。 • デフォルトの距離は、0 です。

	コマンドまたはアクション	目的
ステップ 11	**ip mroute** *source-address mask* **tunnel** *number* [*distance*] 例： `Router(config)# ip mroute 0.0.0.0 0.0.0.0 tunnel 0`	アクセス ルータからトンネルの反対側にリバース パス転送するために、スタティック ルートを設定します。
ステップ 12	**end** 例： `Router(config)# end`	（任意）現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 13	**show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*] 例： `Router# show ip mroute`	（任意）IP マルチキャスト ルーティング（mroute）テーブルの内容を表示します。
ステップ 14	**show ip rpf** {*source-address* | *source-name*} [**metric**] 例： `Router# show ip rpf 10.2.3.4`	（任意）IP マルチキャスト ルーティングが RPF を行う方法を表示します。

非IPマルチキャストエリアを接続するトンネリングの設定例

非 IP マルチキャスト エリアを接続するトンネリングの例

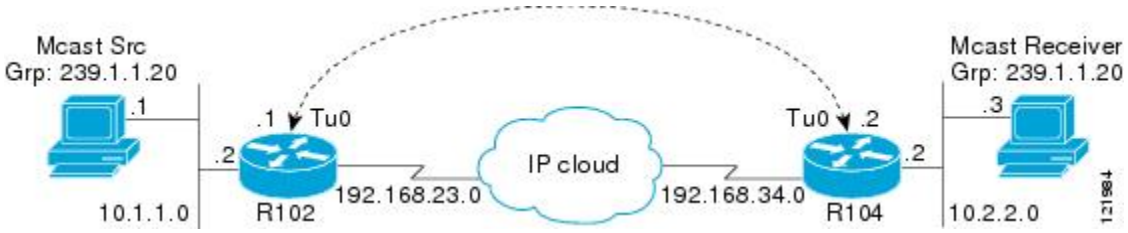
次の例は、次のオンラインでも表示されます。

http://www.cisco.com/en/US/tech/tk828/tk363/technologies_configuration_example09186a00801a5aa2.shtml

下の図では、マルチキャスト ソース（10.1.1.1）は R102 に接続され、マルチキャスト グループ 239.1.1.20 に対して設定されています。 マルチキャスト レシーバ（10.2.2.3）は R104 に接続され、

グループ 239.1.1.20 のマルチキャスト パケットを受信するように設定されています。 R102 と R104 は、マルチキャスト ルーティング用に設定されていない IP クラウドで分離されています。

図 *15*：非 *IP* マルチキャスト エリアを接続するトンネル



ループバック インターフェイスによって、R102 と R104 の間にトンネルが設定されています。 トンネル インターフェイス上で **ip pim sparse-dense-mode** コマンドが設定されており、R102 と R104 でマルチキャスト ルーティングがイネーブルになっています。 トンネル インターフェイスの sparse-dense-mode 設定により、スパース モード パケットまたはデンス モード パケットをグループのランデブー ポイント（RP）設定に応じて、トンネルを経由して転送できます。

（注） デンス モードの場合：トンネルに PIM デンス モードを設定し、R104 で **ip mroute 10.1.1.0 255.255.255.0 tunnel 0** コマンドを設定すると、マルチキャスト ソース アドレス 10.1.1.1 の RPF の正常終了が確実になります。 Tunnel0（Tu0）を経由した着信（10.1.1.1、239.1.1.20）マルチキャスト パケットは、この mroute ステートメントを使用して、リバース パス転送（RPF）がチェックされます。 チェックが正常終了すると、発信インターフェイス リスト（OIL）インターフェイスにマルチキャスト パケットが転送されます。

（注） スパース モードの場合：トンネルに PIM スパース モードを設定し、次の点に確実に対処します。

- RP からの共有ツリー（*,G）上のマルチキャスト トラフィックに対する RPF 確認の正常終了には、トンネル インターフェイスに接続する RP アドレスに対して **ip mroute rp-address nexthop** コマンドの設定が必要です。

この例では、R102 が RP（RP アドレス 2.2.2.2）であることが前提となっており、mroute には、**ip mroute 2.2.2.2 255.255.255.255 tunnel 0** コマンドが設定されています。これによって、共有ツリー上のトラフィックに対して RPF チェックの正常終了が確実になります。

- 最短パス ツリー（SPT）上のマルチキャスト（S, G）トラフィックに対する RPF 確認の正常終了には、トンネル インターフェイスに接続するマルチキャスト ソースに対して **ip mroute source-address nexthop** コマンドの設定が必要です。

この例では、SPT トラフィックがトンネル インターフェイスを経由する場合、R104 に **ip mroute 10.1.1.0 255.255.255.0 tunnel 0** コマンドが設定されます。これによって、Tunnel 0 インターフェイ

スを経由する着信（10.1.1.1, 239.1.1.20）マルチキャスト パケットに対する RPF 確認の正常終了が確実になります。

R102#

```
version 12.2
hostname r102
ip subnet-zero
no ip domain-lookup
!--- It stops IP domain lookup, which improves the show command response time.
!
ip multicast-routing
!--- Enables IP multicast routing.
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!--- Tunnel Source interface.
!
interface Tunnel0
!--- Tunnel interface configured for PIM and carrying multicast packets to R104.
 ip address 192.168.24.1 255.255.255.252
 ip pim sparse-dense-mode
 tunnel source Loopback0
 tunnel destination 4.4.4.4
!
interface Ethernet0/0
!--- Interface connected to Source.
ip address 10.1.1.2 255.255.255.0
 ip pim sparse-dense-mode
!
interface Serial8/0
 ip address 192.168.23.1 255.255.255.252
!--- Note IP PIM sparse-dense mode is not configured on Serial interface.
!
router ospf 1
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 10.1.1.0 0.0.0.255 area 0
 network 192.168.23.0 0.0.0.255 area 0
!
ip classless
ip pim bidir-enable
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

R104#

```
version 12.2
!
hostname r104
!
ip subnet-zero
no ip domain-lookup
!--- It stops IP domain lookup, which improves the show command response time.
!
ip multicast-routing
!--- Enables IP multicast routing.
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
!--- Tunnel Source interface.
!
interface Tunnel0
```

```
 ip address 192.168.24.2 255.255.255.252
!--- Tunnel interface configured for PIM and carrying multicast packets.
ip pim sparse-dense-mode
 tunnel source Loopback0
 tunnel destination 2.2.2.2
!
interface Ethernet0/0
 ip address 10.2.2.2 255.255.255.0
 ip pim sparse-dense-mode
!
interface Serial9/0
 ip address 192.168.34.1 255.255.255.252
!--- Note IP PIM sparse-dense mode is not configured on Serial interface.
!
!
router ospf 1
 log-adjacency-changes
 network 4.4.4.4 0.0.0.0 area 0
 network 10.2.2.0 0.0.0.255 area 0
 network 192.168.34.0 0.0.0.255 area 0
!
ip classless
no ip http server
ip pim bidir-enable
ip mroute 10.1.1.0 255.255.255.0 Tunnel0
!--- This Mroute ensures a successful RPF check for packets flowing from the source.
!--- 10.1.1.1 over Shared tree in case of Dense more and SPT in case of Sparse mode.
!
ip mroute 2.2.2.2 255.255.255.255 tunnel 0
!--- This Mroute is required for RPF check when Sparse mode multicast traffic is
!--- flowing from RP (assuming R102 with 2.2.2.2 as RP)  towards receiver via tunnel
!--- before the SPT switchover.
line con 0
line aux 0
line vty 0 4
 login
!
end
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IP マルチキャスト コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用に関する注意事項、および例	『*Cisco IOS IP Multicast Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
この機能がサポートする新しい MIB または変更された MIB はありません。また、この機能で変更された既存規格のサポートはありません。	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

非IPマルチキャストエリアを接続するトンネリングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを

示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *8*：非 *IP* マルチキャスト エリアを接続するトンネリングの機能情報

機能名	リリース	機能の設定情報
Cisco IOS XE Release 2.1 以降で導入または修正された機能がないため、この表は意図的に空白にしてあります。 この表は、このモジュールに機能情報が追加されると更新されます。	--	--

第 8 章

マルチキャスト（PIM）の BFD サポート

このモジュールには、IPv4 および IPv6 ネットワークの Protocol Independent Multicast（PIM）インターフェイスで双方向フォワーディング検出（BFD）の検出プロトコルをイネーブルにするための情報が含まれています。 PIM BFD をイネーブルにすると、PIM で BFD の迅速な隣接システム障害検出を使用し、独自の検出メカニズムの低速なクエリー間隔を回避できます。

マルチキャスト（PIM）の BFD サポートの制限事項

- この機能は、Multicast VPN（MVPN）ではサポートされません。
- この機能は、PIM と BFD の両方がサポートされるインターフェイス上でのみサポートされます。

マルチキャスト（PIM）の BFD サポートに関する情報

PIM BFD

双方向フォワーディング検出（BFD）は、すべてのメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルのために短時間での転送パス障害検出を提供するために設計された検出プロトコルで、上位層のプロトコルに依存しません。 高速転送パス障害検出に加えて、BFD

はネットワーク管理者に整合性のある障害検出方法を提供します。ネットワーク管理者はBFDを使用することで、さまざまなルーティング プロトコルの HELLO メカニズムにより、変動速度ではなく一定速度で転送パス障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再収束時間の整合性が保たれ、予測可能になります。

Protocol Independent Multicast（PIM）では、新しいネイバーを検出するため、および隣接ノード間のエラーを検出するために hello メカニズムが使用されます。 PIM の最小障害検出時間は、PIM クエリー間隔の3倍です。迅速な障害検出を有効にするには、インターフェイスでPIM Helloメッセージが送信されるレートを設定できます。 ただし、間隔が短いとプロトコルの負荷が増大し、CPU およびメモリ使用率が増加して、システム全体のパフォーマンスに悪影響を及ぼす可能性があります。 また、間隔が短いと、ネイバーから受信した hello メッセージの処理前にネイバーの期限切れが発生することがあるため、PIM ネイバーが頻繁に期限切れになる可能性もあります。

マルチキャスト（PIM）の BFD サポート機能は PIM BFD とも呼ばれ、PIM は BFD のクライアントとして登録されます。 PIMはBFDを使用して隣接するPIMのノードとのセッションを開始し、プロトコル層で BFD の高速な隣接障害検出をサポートできます。 PIM は PIM と IPv6 PIM の両方に一度だけに登録されます。

（BFD クライアントとしての）PIM 要求で、BFD は、活性を維持し、隣接ノードへの転送パス障害を検出するために、隣接ノードとのセッションを確立し、維持します。 PIM hello は、BFD がネイバーとの BFD セッションを確立し、維持した後も、ネイバー間で引き続き交換されます。 PIM hello メカニズムの動作は、この機能の導入によって変更されません。

PIM は内部ゲートウェイ プロトコル（IGP）に依存し、BFD は IGP でサポートされていますが、PIM BFD は IGP の BFD に依存しません。

マルチキャスト（PIM）の BFD サポートの設定方法

インターフェイスでの BFD PIM のイネーブル化

はじめる前に

- IPv4 ネットワークでは、IP マルチキャストをイネーブルにし、Protocol Independent Multicast（PIM）をインターフェイス上で設定する必要があります。詳細については、『*IP Multicast*：*PIM* コンフィギュレーション ガイド』の「IPv4 ネットワークでの基本的な IP マルチキャスト設定」モジュールを参照してください。
- IPv6 ネットワークでは、IPv6 マルチキャストをイネーブルにし、Protocol Independent Multicast（PIM）をインターフェイス上で設定する必要があります。詳細については、『*IP Multicast*：*PIM* コンフィギュレーション ガイド』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***type number*
4. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
5. 次のいずれかを使用します。
   - **ip pim bfd**
   - **ipv6 pim bfd**
6. BFD PIM をイネーブルにする各インターフェイスに対して上記のステップを繰り返します。
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***type number* 例： `Device(config)# interface fastethernet 1/6`	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* 例： `Device(config-if)# bfd interval 500 min_rx 500 multiplier 5`	インターフェイスで BFD をイネーブルにします。
ステップ 5	次のいずれかを使用します。 • **ip pim bfd** • **ipv6 pim bfd**	インターフェイス上で PIM BFD をイネーブルにします。

	コマンドまたはアクション	目的

	例：
	`Device(config-if)# ip pim bfd`
	`Device(config-if)# ipv6 pim bfd`	

ステップ 6	BFD PIM をイネーブルにする各インターフェイスに対して上記のステップを繰り返します。	
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

マルチキャスト（PIM）の BFD サポートの設定例

マルチキャスト（PIM）の BFD サポートのその他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』
双方向フォワーディング検出（BFD）検出プロトコル	『*IP Routing BFD Configuration Guide*』
IPv4 ネットワークの Protocol Independent Multicast（PIM）	『*IP Multicast*：*PIM* コンフィギュレーション ガイド』の「IPv4 ネットワークでの基本的な IP マルチキャスト設定」モジュール
IPv6 ネットワークの PIM	『*IP Multicast*：*PIM* コンフィギュレーション ガイド』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

マルチキャスト（PIM）の BFD サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *9*：マルチキャスト（*PIM*）の *BFD* サポートの機能情報

機能名	リリース	機能情報
マルチキャスト（PIM）の BFD サポート	15.3(2)S Cisco IOS XE Release 3.9S	この機能を使用すると、マルチキャスト PIM で BFD の迅速な隣接システム障害検出を使用し、独自の検出メカニズムの低速なクエリー間隔を回避できます。 次のコマンドが導入または変更されました。**ip pim bfd**、**ipv6 pim bfd**、**show ip pim**、**show ipv6 pim interface**。

第 9 章

HSRP Aware PIM

このモジュールでは、ホットスタンバイ ルータ プロトコル（HSRP）アクティブ ルータ（AR）経由でマルチキャスト トラフィックを転送するための HSRP Aware PIM を設定し、Protocol Independent Multicast（PIM）で HSRP 冗長性を活用して潜在的な重複トラフィックを回避し、フェールオーバーをイネーブルにする方法を説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

HSRP Aware PIM の制約事項

- HSRP IPv6 はサポートされていません。
- ステートフル フェールオーバーはサポートされていません。PIM ステートレス フェールオーバー中は、HSRP グループの仮想 IP アドレスがスタンバイ ルータへ転送されますが、mrouting ステート情報は転送されません。PIM は、状態変更イベントをリッスンして応答し、フェールオーバーの際に mroute ステートを作成します。
- 各インターフェイスの PIM によって追跡できる HSRP グループの最大数は 16 です。
- PIM DR の冗長性のプライオリティは、同じ HSRP グループがイネーブルになっているデバイス上の PIM DR プライオリティの設定済みまたはデフォルトの値（1）より大きくする必要があります。そうしないと、HSRP アクティブは DR 選択に失敗します。

HSRP Aware PIM について

HSRP

ホットスタンバイ ルータ プロトコル（HSRP）は、フォールトトレラント デフォルト ゲートウェイを確立するためのシスコ独自の冗長プロトコルです。

プロトコルは、プライマリ ゲートウェイがアクセス不能になると、デフォルト ゲートウェイのフェールオーバーを実施するためにネットワーク デバイス間のフレームワークを確立します。IP アドレスと MAC（レイヤ 2）アドレスを共有することによって、2 台以上のルータが 1 つの仮想ルータとして動作できます。 仮想ルータ グループのメンバは、継続的にステータス メッセージを交換し、1 台のデバイスは、別のデバイスが計画的または計画外の理由から動作しなくなった場合、ルーティング引き継ぐことができます。 ホストは同じ IP および MAC アドレスに IP パケットを転送し続け、ルーティングを行うデバイスの切り替えは透過的です。

HSRP は、ホストがルータ ディスカバリ プロトコルをサポートしておらず、選択されたデバイスのリロードや電源故障時に新しいデバイスに切り替えることができない場合に有効です。 また、既存の TCP セッションはフェールオーバーが発生しても存続するため、このプロトコルでは IP トラフィックをルーティングするためにネクスト ホップを動的に選択するホストの回復をさらに透過的に実行できます。

HSRP をネットワーク セグメントに設定すると、HSRP が動作するデバイスのグループで仮想 MAC アドレスと IP アドレスを共有できるようになります。 この HSRP ルータ グループのアドレスが仮想 IP アドレスと呼ばれます。 このようなデバイスの 1 つが、アクティブ ルータ（AR）としてプロトコルによって選択されます。 AR は、グループの MAC アドレス宛てのパケットを受信してルーティングします。

HSRP では、プライオリティ メカニズムを使用して、デフォルトの AR にする HSRP 設定済みデバイスを決定します。 デバイスを AR として設定するには、他のすべての HSRP 設定済みデバイスのプライオリティよりも高いプライオリティをそのルータに割り当てます。 デフォルトのプラ

イオリティは 100 です。したがって、100 よりも高いプライオリティを持つデバイスを 1 つだけ設定した場合、そのデバイスがデフォルトの AR になります。

HSRP を実行しているデバイスは、ユーザ データグラム プロトコル（UDP）ベースのマルチキャストhelloメッセージを送信および受信して、デバイスの障害を検出したり、アクティブおよびスタンバイ デバイスを割り当てたりします。 AR が設定された時間内に hello メッセージを送信できなかった場合は、最高のプライオリティのスタンバイ デバイスが AR になります。 このようにパケット転送機能が別のデバイスに移行しても、ネットワークのいずれのホストにもまったく影響はありません。

複数のホット スタンバイ グループをインターフェイスに設定できるので、冗長デバイスおよびロード シェアリングを余すところなく活用できるようになっています。

HSRPは、IPルートをアドバタイズせず、ルーティング テーブルに影響を与えないため、ルーティング プロトコルではありません。

HSRP は、デバイス上の 1 つ以上のインターフェイスに障害が発生した場合にフェールオーバーをトリガーすることができます。 これは、それぞれがヘッド エンドへの単一のシリアル リンクを備えたデュアル ブランチ デバイスに役立つことがあります。 プライマリ デバイスのシリアル リンクがダウンすると、バックアップデバイスはプライマリ機能を引き継ぎ、ヘッドエンドへの接続を維持します。

HSRP Aware PIM

Protocol Independent Multicast（PIM）には固有の冗長性機能がなく、その動作は、ホットスタンバイ ルータ プロトコル（HSRP）グループの状態から完全に独立しています。 その結果、IP マルチキャスト トラフィックは、必ずしも HSRP によって選択されたデバイスと同じデバイスによって転送されるわけではありません。 HSRP Aware PIM 機能は、仮想ルーティング グループがイネーブルの冗長ネットワークで一貫した IP マルチキャスト転送を提供します。

HSRP Aware PIM により、HSRP アクティブ ルータ（AR）を通じてマルチキャスト トラフィックを転送し、PIM でHSRP冗長性を活用し、潜在的な重複トラフィックを回避し、デバイスのHSRPステートに応じてフェールオーバーをイネーブルにすることができます。 PIM指定ルータ（DR）は、HSRP AR と同じゲートウェイ上で実行され、mroute ステートを維持します。

マルチアクセス セグメント（LAN など）では、PIM DR 選択で冗長構成が認識されず、選択されたDR と HSRP AR が同じルータでない場合があります。 PIM DR が RP または FHR へ PIM Join/Prune メッセージを常に転送できるようにするため、HSRP AR が PIM DR になります（HSRP グループが 1 つだけの場合）。 PIM により、グループの状態に基づいて DR プライオリティが調整されます。 フェールオーバーが発生すると、HSRP グループで選択された新しい AR にマルチキャスト ステートが作成され、AR は HSRP 仮想 IP アドレス宛てのすべてのトラフィックのルーティングと転送を行います。

HSRP Aware PIM がイネーブルの場合、デバイスが HSRP アクティブになると、PIM は各アクティブ HSRP グループのソース アドレスとして HSRP 仮想 IP アドレスを使用して、追加の PIM Hello メッセージを送信します。 PIM Helloは、他のルータによるフェールオーバーへの応答をトリガーするために新しい GenID を送信します。 ダウンストリーム デバイスは、この PIM Hello を受信すると、PIM ネイバー リストに仮想アドレスを追加します。 PIM Hello で送信される新しい GenID は、ダウンストリーム ルータによる仮想アドレスへの PIM Join メッセージの再送信をトリガーし

ます。 アップストリーム ルータは、HSRP グループの状態に基づいて PIM Join/Prune を処理します（J/P）。

J/P 宛先が HSRP グループの仮想アドレスに一致し、宛先デバイスが HSRP アクティブ状態の場合、新しい AR が動作中の PIM DR であるため、PIM Join を処理します。 これにより、すべての PIM Join/Prune が HSRP グループの仮想アドレスに到達することができ、ダウンストリーム ルータ側での変更および設定が最小限に抑えられます。

IP ルーティング サービスは既存の仮想ルーティング プロトコルを使用して、PIM などのクライアント アプリケーションに基本的なステートレス フェールオーバー サービスを提供します。 ローカル HSRP グループの状態およびスタンバイ ルータ役割の変更は、関与するクライアント アプリケーションに伝達されます。 クライアント アプリケーションは、ステートフルまたはステートレス フェールオーバーを提供するために IRS 上に構築されることがあります。 PIM は HSRP クライアントとして HSRP から状態変更通知をリッスンし、HSRP ステートに基づいて PIM DR のプライオリティを自動的に調整します。 PIM クライアントは、新しい AR に mroute ステートを作成するために、フェールオーバーの際にアップストリーム デバイスとダウンストリーム デバイス間の通信もトリガーします。

HSRP Aware PIM の設定方法

インターフェイスでの HSRP グループの設定

はじめる前に

- IP マルチキャストがすでにデバイスで設定されている必要があります。
- PIM がすでにインターフェイスで設定されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **ip** [*ip-address* [*secondary*]]
6. **standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*
7. **standby** [*group-number*] **priority** *priority*
8. **standby** [*group-number*] **name** *group-name*
9. **end**
10. **show standby** [*type number* [*group*]] [**all** | **brief**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* [*name-tag*] 例： `Device(config)# interface ethernet 0/0`	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.0.0.2 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 5	**standby** [*group-number*] **ip** [*ip-address* [*secondary*]] 例： `Device(config-if)# standby 1 ip 192.0.2.99`	HSRP をアクティブにし、HSRP グループを定義します。
ステップ 6	**standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime* 例： `Device(config-if)# standby 1 timers 5 15`	（任意）hello パケット間の時間と、他のデバイスによって HSRP アクティブ ルータまたはスタンバイ ルータの停止が宣言されるまでの時間を設定します。
ステップ 7	**standby** [*group-number*] **priority** *priority* 例： `Device(config-if)# standby 1 priority 120`	（任意）HSRP アクティブ ルータとスタンバイ ルータを選択するために使用される HSRP プライオリティを割り当てます。
ステップ 8	**standby** [*group-number*] **name** *group-name* 例： `Device(config-if)# standby 1 name HSRP1`	（任意）HSRP グループの名前を定義します。 （注） HSRP Aware PIM で使用するように HSRP グループを設定する場合は、常に **standby ip name** コマンドを設定することを推奨します。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show standby** [*type number* [*group*]] [**all** | **brief**] 例： `Device# show standby`	設定を確認するために HSRP グループ情報を表示します。

PIM の冗長性の設定

はじめる前に

HSRP グループがすでにインターフェイスで設定されている必要があります。「インターフェイスでの HSRP グループの設定」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip address** *ip-address mask*
5. **ip pim redundancy** *group* **dr-priority** *priority*
6. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* [*name-tag*] 例： `Device(config)# interface ethernet 0/0`	設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.0.0.2 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 5	**ip pim redundancy** *group* **dr-priority** *priority* 例： `Device(config-if)# ip pim redundancy HSRP1 dr-priority 60`	PIM 冗長性をイネーブルにし、アクティブな PIM 指定ルータ（DR）に冗長性のプライオリティ値を割り当てます。 • HSRP グループ名では大文字と小文字が区別されるため、*group* 引数の値は **standby ip name** コマンドを使用して設定されたグループ名と一致している必要があります。 • PIM DR の冗長性のプライオリティは、同じ HSRP グループがイネーブルになっているデバイス上の PIM DR プライオリティの設定済みの値またはデフォルト値（1）より大きくする必要があります。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

HSRP Aware PIM の設定例

例：HSRP Aware PIM

HSRP Aware PIM の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』
HSRP コマンド	『First Hop Redundancy Protocol Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 2281	『*Cisco Hot Standby Router Protocol (HSRP)*』

MIB

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

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

HSRP Aware PIM に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *10*：*HSRP Aware PIM* に関する機能情報

機能名	リリース	機能情報
HSRP Aware PIM	15.2(4)S Cisco IOS XE Release 3.7S 15.3(1)T 15.3(1)SY1	HSRP Aware PIM 機能は、マルチキャストトラフィックをホットスタンバイ ルータ プロトコル（HSRP）アクティブ ルータ経由で転送できるようにすることによって、仮想ルーティング グループを含む冗長ネットワークで一貫した IP マルチキャスト転送を提供します。これにより、PIM では、HSRP 冗長性を活用し、潜在的な重複トラフィックを回避し、デバイスの HSRP ステートに応じてフェールオーバーをイネーブルにすることができます。 **ip pim redundancy** コマンドが導入または変更されました。

第 10 章

IP マルチキャスト オペレーションの確認

このモジュールでは、Protocol Independent Multicast（PIM）スパース モード（PIM-SM）または Source Specific Multicast（PIM-SSM）の実装後に、ネットワークで IP マルチキャスト オペレーションを確認する方法を説明します。 このモジュールの作業では、IP マルチキャストの到達可能性をテストし、IP マルチキャスト ネットワークでレシーバとソースが想定どおりに動作していることを確認できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

IP マルチキャスト オペレーションの確認の前提条件

- このモジュールの作業を実行する前に、「IP マルチキャスト テクノロジーの概要」モジュールで説明している概念をよく理解しておく必要があります。
- このモジュールの作業は、IP マルチキャストがイネーブルに設定され、PIM-SM または SSM が「基本的な IP マルチキャスト設定」モジュールで説明されている関連タスクを使用して設定されていることを前提としています。

IP マルチキャスト オペレーションの確認における制限

- PIM-SM については、このモジュールでは、PIM 対応ルータで最短パス ツリー（SPT）しきい値が値ゼロ（デフォルト）に設定され、無限大ではないことが前提となります。 SPT しきい値の詳細については、『*Cisco IOS IP Multicast Command Reference*』の **ip pim spt-threshold** コマンド ページを参照してください。
- 双方向 PIM（Bidir-PIM）ネットワーク、または有限あるいは無限の SPT しきい値が使用されている PIM-SM ネットワークでの IP マルチキャスト オペレーションの確認は、このモジュールの範囲外です。

IP マルチキャスト オペレーションに関する情報

PIM-SM ネットワーク環境および PIM-SSM ネットワーク環境での IP マルチキャスト オペレーションの確認に関するガイドライン

PIM-SM ネットワーク環境または PIM-SSM ネットワーク環境で IP マルチキャストのオペレーションを確認するときに、効果的なアプローチは、ラスト ホップ ルータで確認プロセスを開始し、ファースト ホップ ルータに到達するまで、SPT が使用されているルータ上で確認プロセスを続行することです。 この確認の目的は、IP マルチキャスト ネットワークを介して IP マルチキャスト トラフィックが適切にルーティングされていることを確認することです。

ラスト ホップ ルータでの IP マルチキャスト オペレーションの確認に使用される一般的なコマンド（PIM-SM および PIM-SSM）

表に、PIM-SM ネットワーク環境および PIM-SSM ネットワーク環境のラスト ホップ ルータで IP マルチキャスト オペレーションの確認に使用される一般的なコマンドについて説明します。

表 *11*：一般的な *IP* マルチキャスト確認コマンド（ラスト ホップ ルータ）

コマンド	説明および目的
show ip igmp groups	ルータに直接接続されているレシーバとインターネット グループ管理プロトコル（IGMP）によって学習されたレシーバを持つマルチキャスト グループを表示します。 • LAN 上のレシーバが加入したグループのラスト ホップ ルータ上で、IGMP キャッシュが適切に生成されていることを確認するには、このコマンドを使用します。
show ip pim rp mapping	（設定、あるいは Auto-RP または BSR からの学習により）ルータが認識しているグループ-RP マッピングをすべて表示します。 • グループ-RP 間のマッピングがラスト ホップ ルータで正しく生成されていることを確認する場合は、このコマンドを使用します。 （注） PIM-SSM ではランデブー ポイント（RP）が使用されないため、**show ip pim rp mapping** コマンドは PIM-SSM ネットワーク内のルータでは動作しません。
show ip mroute	マルチキャスト ルーティング（mroute）テーブルの内容を表示します。 • mroute テーブルがラスト ホップ ルータで正しく生成されていることを確認する場合は、このコマンドを使用します。
show ip interface	設定されているインターフェイスについて、情報および統計情報を表示します。 • IP マルチキャスト高速スイッチングがラスト ホップ ルータの発信インターフェイスでイネーブルになっていることを確認するには、このコマンドを使用します。
show ip mfib	IP マルチキャスト転送情報ベース（MFIB）の転送エントリおよびインターフェイスを表示します。

コマンド	説明および目的
show ip pim interface count	PIM 対応インターフェイスで送受信されたマルチキャスト パケットの数に関連する統計情報を表示します。 • マルチキャスト トラフィックがラスト ホップ ルータに転送されていることを、ラスト ホップ ルータ上で確認する場合は、このコマンドを使用します。
show ip mroute active	アクティブなソースがマルチキャスト グループに送信しているレートを、キロビット/秒（kb/s）単位で表示します。 • ラスト ホップ ルータ上のグループに送信を実行しているアクティブなソースのマルチキャスト パケット レートに関する情報を表示する場合は、このコマンドを使用します。
show ip mroute count	mroute テーブルの mroute に関連する統計情報を表示します。 • マルチキャスト トラフィックがラスト ホップ ルータに転送されていることを、ラスト ホップ ルータ上で確認する場合は、このコマンドを使用します。

SPT が使用されているルータでの IP マルチキャスト オペレーションの確認に使用される一般的なコマンド（PIM-SM および PIM-SSM）

表に、PIM-SM ネットワーク環境および PIM-SSM ネットワーク環境の SPT が使用されているルータで IP マルチキャスト オペレーションの確認に使用される一般的なコマンドについて説明します。

表 *12*：一般的な *IP* マルチキャスト確認コマンド（*SPT* が使用されているルータ）

コマンド	説明および目的
show ip mroute	mroute テーブルの内容を表示します。 • ソースへのリバース パス転送（RPF）ネイバーが、SPT が使用されている各ルータの想定 RPF ネイバーであることを確認するには、このコマンドを使用します。
show ip mroute active	アクティブなソースがマルチキャスト グループに送信しているレートを、kb/s 単位で表示します。 • SPT が使用されているルータ上のグループに送信を実行しているアクティブなソースのマルチキャスト パケット レートに関する情報を表示する場合は、このコマンドを使用します。

ファースト ホップ ルータでの IP マルチキャスト オペレーションの確認に使用される一般的なコマンド（PIM-SM および PIM-SSM）

表に、PIM-SM ネットワーク環境および PIM-SSM ネットワーク環境のファースト ホップ ルータで IP マルチキャスト オペレーションの確認に使用される一般的なコマンドについて説明します。

表 *13*：一般的な *IP* マルチキャスト確認コマンド（ファースト ホップ ルータ）

コマンド	説明および目的
show ip mroute	mroute テーブルの内容を表示します。 • F フラグがファースト ホップ ルータの mroute に設定されていることを確認するには、このコマンドを使用します。

コマンド	説明および目的
show ip mroute active	アクティブなソースがマルチキャスト グループに送信しているレートを、kb/s 単位で表示します。 • ファースト ホップ ルータ上のグループに送信を実行しているアクティブなソースのマルチキャスト パケット レートに関する情報を表示する場合は、このコマンドを使用します。

IP マルチキャスト オペレーションを確認する方法

PIM 対応ルータを使用して IP マルチキャストの到達可能性をテストする方法

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

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

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

マルチキャスト ping に応答するルータの設定

ルータをマルチキャスト ping に応答するように設定するには、次の作業を実行します。 この作業の実行によって、指定されたグループに加入するよう、ルータ上のインターフェイスが設定されます。 この作業は、マルチキャスト ネットワークに加入しているルータ上の各インターフェイス、およびマルチキャスト ネットワークに加入しているすべてのルータで実行する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip igmp join-group** *group-address*
5. マルチキャスト ネットワークに加入しているルータ上のインターフェイスで、ステップ 3 とステップ 4 を繰り返します。
6. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 5	マルチキャスト ネットワークに加入しているルータ上のインターフェイスで、ステップ 3 とステップ 4 を繰り返します。	--
ステップ 6	**end** 例： `Router(config-if)# end`	現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。

マルチキャスト ping に応答するように設定されているルータの ping

マルチキャスト ping に応答するように設定されているルータをテストするために、ルータ上で ping を開始するには、次の作業を実行します。 この作業は、ネットワークの IP マルチキャストの到達可能性をテストするために使用します。

手順の概要

1. **enable**
2. **ping** *group-address*

手順の詳細

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

PIM-SM ネットワークまたは PIM-SSM ネットワークでの IP マルチキャスト オペレーションの確認

PIM-SM ネットワークまたは PIM-SSM ネットワークで IP マルチキャスト オペレーションを確認するには、次の任意の作業を実行します。 ソースとレシーバが期待どおりに動作していない場合、これらの作業の手順を実行すると、障害が発生したホップの場所を特定できます。

（注） パケットが想定された宛先に到達していない場合、IP マルチキャスト高速スイッチングをディセーブルにすることを検討する必要が生じることがあります。これによって、ルータはプロセス スイッチング モードになります。 IP マルチキャスト高速スイッチングがディセーブルされた後で、パケットが適切な宛先に到達し始めた場合、問題は IP マルチキャスト高速スイッチングに関連していた可能性が非常に高くなります。IP マルチキャスト高速スイッチングをディセーブルにする方法の詳細については、「IP マルチキャストのモニタリングおよび保持」モジュールを参照してください。

PIM-SM マルチキャスト ネットワークまたは PIM-SSM マルチキャスト ネットワークで IP マルチキャスト オペレーションを確認するには、次の確認作業を実行します。

ラスト ホップ ルータでの IP マルチキャスト オペレーションの確認

ラスト ホップ ルータで IP マルチキャストのオペレーションを確認するには、次の作業を実行します。

（注） PIM-SSM ネットワークのラスト ホップ ルータを確認する場合は、ステップ 3 を無視します。

手順の概要

1. **enable**
2. **show ip igmp groups**
3. **show ip pim rp mapping**
4. **show ip mroute**
5. **show ip interface** [*type number*]
6. **show ip mfib**
7. **show ip pim interface count**
8. **show ip mroute count**
9. **show ip mroute active** [*kb/s*]

手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

```
Router> enable
```

ステップ 2 **show ip igmp groups**

ラスト ホップ ルータで IGMP メンバーシップを確認するには、このコマンドを使用します。 この情報によって、ラストホップルータに直接接続され、IGMPを介して認識されるレシーバが使用されているマルチキャスト グループが確認されます。

次に、**show ip igmp groups** コマンドの出力例を示します。

例：

```
Router# show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
239.1.2.3        GigabitEthernet1/0/0     00:05:14  00:02:14  10.1.0.6
224.0.1.39       GigabitEthernet0/0/0     00:09:11  00:02:08  172.31.100.1
```

ステップ 3 **show ip pim rp mapping**

グループ-RP 間のマッピングがラスト ホップ ルータで正しく生成されていることを確認する場合は、このコマンドを使用します。

（注） PIM-SSM ネットワークのラスト ホップ ルータを確認する場合は、この手順を無視します。 PIM-SSM では RP が使用されないため、**show ip pim rp mapping** コマンドは PIM-SSM ネットワーク内のルータでは動作しません。 さらに、正しく設定されている場合、**show ip pim rp mapping** コマンドの出力には PIM-SSM グループは表示されません。

次に、**show ip pim rp mapping** コマンドの出力例を示します。

例：

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 172.16.0.1 (?), v2v1
    Info source: 172.16.0.1 (?), elected via Auto-RP
         Uptime: 00:09:11, expires: 00:02:47
```

ステップ 4 **show ip mroute**

mroute テーブルがラスト ホップ ルータで正しく生成されていることを確認する場合は、このコマンドを使用します。

次に、 **show ip mroute** コマンドの出力例を示します。

例：

```
Router# show ip mroute
(*, 239.1.2.3), 00:05:14/00:03:04, RP 172.16.0.1, flags: SJC
```

```
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
  Outgoing interface list:
  GigabitEthernet1/0, Forward/Sparse-Dense, 00:05:10/00:03:04

(10.0.0.1, 239.1.2.3), 00:02:49/00:03:29, flags: T
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
  Outgoing interface list:
  GigabitEthernet1/0, Forward/Sparse-Dense, 00:02:49/00:03:04

(*, 224.0.1.39), 00:10:05/stopped, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet1/0, Forward/Sparse-Dense, 00:05:15/00:00:00
    GigabitEthernet0/0, Forward/Sparse-Dense, 00:10:05/00:00:00

(172.16.0.1, 224.0.1.39), 00:02:00/00:01:33, flags: PTX
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
```

ステップ 5 **show ip interface** [*type number*]

マルチキャスト高速スイッチングがラスト ホップ ルータの発信インターフェイスで、最適化されたパフォーマンスでイネーブルになっていることを確認するには、このコマンドを使用します。

（注） **no ip mroute-cache** インターフェイス コマンドを使用すると、IP マルチキャスト高速スイッチングをディセーブルにされます。 IP マルチキャスト高速スイッチングがディセーブルの場合、パケットはプロセス スイッチド パスを使用して転送されます。

次に、特定のインターフェイスに対する **show ip interface** コマンドの出力例を示します。

例：

```
Router# show ip interface GigabitEthernet 0/0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 172.31.100.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.1 224.0.0.22 224.0.0.13
      224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
```

```
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

ステップ 6 **show ip mfib**

IP マルチキャスト転送情報ベース（MFIB）の転送エントリおよびインターフェイスを表示するには、このコマンドを使用します。

例：

ステップ 7 **show ip pim interface count**

マルチキャスト トラフィックがラスト ホップ ルータに転送されていることを確認する場合は、このコマンドを使用します。

次に、**show ip pim interface** コマンドに **count** キーワードを指定した場合の出力例を示します。

例：

```
Router# show ip pim interface count

State: * - Fast Switched, D - Distributed Fast Switched
       H - Hardware Switching Enabled
Address          Interface                FS Mpackets In/Out
172.31.100.2     GigabitEthernet0/0/0     *   4122/0
10.1.0.1         GigabitEthernet1/0/0     *   0/3193
```

ステップ 8 **show ip mroute count**

マルチキャスト トラフィックがラスト ホップ ルータに転送されていることを確認する場合は、このコマンドを使用します。

次に、**show ip mroute** コマンドに **count** キーワードを指定した場合の出力例を示します。

例：

```
Router# show ip mroute count
IP Multicast Statistics
6 routes using 4008 bytes of memory
3 groups, 1.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 239.1.2.3, Source count: 1, Packets forwarded: 3165, Packets received: 3165
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
  Source: 10.0.0.1/32, Forwarding: 3165/20/28/4, Other: 0/0/0

Group: 224.0.1.39, Source count: 1, Packets forwarded: 21, Packets received: 120
  Source: 172.16.0.1/32, Forwarding: 21/1/48/0, Other: 120/0/99

Group: 224.0.1.40, Source count: 1, Packets forwarded: 10, Packets received: 10
  Source: 172.16.0.1/32, Forwarding: 10/1/48/0, Other: 10/0/0
```

ステップ 9 **show ip mroute active** [*kb/s*]

ラスト ホップ ルータ上のグループに送信を実行しているアクティブなマルチキャスト ソースに関する情報を表示する場合は、ラスト ホップ ルータ上でこのコマンドを使用します。 このコマンドの出力では、アクティブなソースのマルチキャスト パケット レートに関する情報が示されます。

（注） デフォルトでは、**active** キーワードを指定した **show ip mroute** コマンドの出力では、4 kb/s. 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。 より低いレートのトラフィック（4 kb/s 未満のトラフィック）をグループに送信しているアクティブなソースに関する情報を表示する場合は、*kb/s* 引数に 1 の値を指定します。 この引数に 1 の値を指定すると、1 kb/s 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソース トラフィックに関する情報が効果的に表示されます。

次に、**show ip mroute** コマンドに **active** キーワードを指定した場合の出力例を示します。

例：

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 50 secs), 4 kbps(life avg)
```

SPT が使用されているルータでの IP マルチキャストの確認

PIM-SM ネットワークまたは PIM-SSM ネットワークで SPT が使用されているルータ上で IP マルチキャストのオペレーションを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show ip mroute** [*group-address*]
3. **show ip mroute active**

手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

```
Router> enable
```

ステップ 2 **show ip mroute** [*group-address*]

特定の 1 つまたは複数のグループのソースへの RPF ネイバーを確認する場合は、SPT が使用されているルータでこのコマンドを使用します。

次に、特定のグループに対する **show ip mroute** コマンドの出力例を示します。

例：

```
Router# show ip mroute 239.1.2.3
(*, 239.1.2.3), 00:17:56/00:03:02, RP 172.16.0.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:17:56/00:03:02

(10.0.0.1, 239.1.2.3), 00:15:34/00:03:28, flags: T
  Incoming interface: Serial1/0, RPF nbr 172.31.200.1
  Outgoing interface list:
    GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:15:34/00:03:02
```

ステップ 3 **show ip mroute active**

グループに送信を実行しているアクティブなマルチキャスト ソースに関する情報を表示する場合は、SPT が使用されているルータ上でこのコマンドを使用します。このコマンドの出力では、アクティブなソースのマルチキャスト パケット レートに関する情報が示されます。

（注） デフォルトでは、**active** キーワードを指定した **show ip mroute** コマンドの出力では、4 kb/s. 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。 より低いレートのトラフィック（4 kb/s 未満のトラフィック）をグループに送信しているアクティブなソースに関する情報を表示する場合は、*kb/s* 引数に 1 の値を指定します。 この引数に 1 の値を指定すると、1 kb/s 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソース トラフィックに関する情報が効果的に表示されます。

次に、**show ip mroute** コマンドに **active** キーワードを指定した場合の出力例を示します。

例：

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)
```

ファースト ホップ ルータでの IP マルチキャストの確認

ファースト ホップ ルータで IP マルチキャストのオペレーションを確認するには、次の作業を実行します。

手順の概要

1. **enable**
2. **show ip mroute** [*group-address*]
3. **show ip mroute active** [*kb/s*]

手順の詳細

ステップ 1 **enable**

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

```
Router> enable
```

ステップ 2 **show ip mroute** [*group-address*]

F フラグがファースト ホップ ルータの mroute に設定されていることを確認するには、ファースト ホップ ルータでこのコマンドを使用します。

次に、特定のグループに対する **show ip mroute** コマンドの出力例を示します。

例：

```
Router# show ip mroute 239.1.2.3
(*, 239.1.2.3), 00:18:10/stopped, RP 172.16.0.1, flags: SPF
  Incoming interface: Serial1/0, RPF nbr 172.31.200.2
  Outgoing interface list: Null

(10.0.0.1, 239.1.2.3), 00:18:10/00:03:22, flags: FT
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Serial1/0, Forward/Sparse-Dense, 00:18:10/00:03:19
```

ステップ 3 **show ip mroute active** [*kb/s*]

グループに送信を実行しているアクティブなマルチキャスト ソースに関する情報を表示する場合は、ファースト ホップ ルータ上でこのコマンドを使用します。 このコマンドの出力では、アクティブなソースのマルチキャスト パケット レートに関する情報が示されます。

（注） デフォルトでは、**active** キーワードを指定した **show ip mroute** コマンドの出力では、4 kb/s. 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。 より低いレートのトラフィック（4 kb/s 未満のトラフィック）をグループに送信しているアクティブなソースに関する情報を表示する場合は、*kb/s* 引数に 1 の値を指定します。 この引数に 1 の値を指定すると、1 kb/s 以上のレートでグループにトラフィックを送信しているアクティブなソースに関する情報が表示されます。これによって、存在する可能性があるすべてのアクティブなソース トラフィックに関する情報が効果的に表示されます。

次に、**show ip mroute** コマンドに **active** キーワードを指定した場合の出力例を示します。

例：

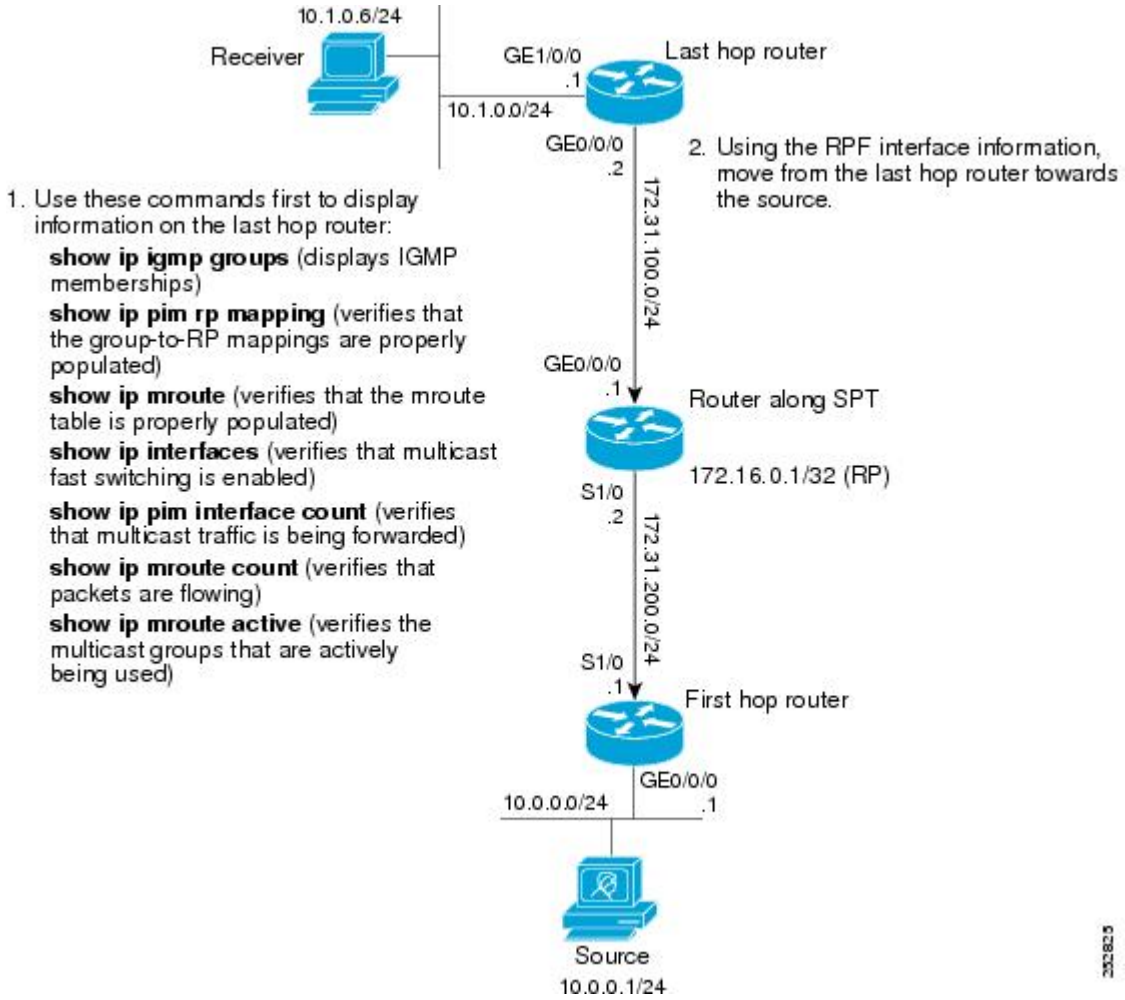
```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)
```

IP マルチキャスト オペレーションの設定例

PIM-SM ネットワークまたは PIM-SSM ネットワークでの IP マルチキャスト オペレーションの確認例

次に、ネットワークに PIM-SM が導入された後で、IP マルチキャスト オペレーションを確認する例を示します。 例は、図に示された PIM-SM トポロジに基づいています。

図に示されているラストホップルータからファーストホップルータで、この特定の PIM-SM ネットワーク トポロジの IP マルチキャスト オペレーションを確認する例を示します。



ラスト ホップ ルータでの IP マルチキャストの確認例

次に、**show ip igmp groups** コマンドの出力例を示します。 出力例では、図に示されているラスト ホップ ルータの IGMP メンバーシップが表示されます。 このコマンドは、LAN 上のレシーバが加入したグループに対して、IGMP キャッシュが適切に生成されていることを確認するために、この例で使用されています。

```
Router# show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
239.1.2.3        GigabitEthernet1/0/0     00:05:14  00:02:14  10.1.0.6
224.0.1.39       GigabitEthernet0/0/0     00:09:11  00:02:08  172.31.100.1
```

次に、**show ip pim rp mapping** コマンドの出力例を示します。 出力例では、RP フィールドに表示されている RP アドレスに注意してください。 図に示されているラスト ホップ ルータ上でグループから RP へのマッピング適切に生成されたことを確認するには、RP アドレスとグループ情報を使用します。

（注） 出力の「（?）」は、ルータによって、IP アドレスをホスト名に解決できなかったことを示します。

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 172.16.0.1 (?), v2v1
    Info source: 172.16.0.1 (?), elected via Auto-RP
         Uptime: 00:09:11, expires: 00:02:47
```

次に、**show ip mroute** コマンドの出力例を示します。 このコマンドは、図に示されているラスト ホップ ルータ上で mroute テーブルが正しく生成されていることを確認する場合に使用します。 出力例では、（10.0.0.1, 239.1.2.3）mroute の T フラグに注意してください。 T フラグは、SPT ビットが設定されたことを示します。これは、マルチキャスト パケットが特定の mroute の SPT ツリーで受信されたことを意味します。 また、RPF nbr フィールドは、マルチキャスト ソースへのユニキャスト ルーティングによって特定された最上位の IP アドレスを持つ RPF ネイバーを指す必要があります。

```
Router# show ip mroute
(*, 239.1.2.3), 00:05:14/00:03:04, RP 172.16.0.1, flags: SJC
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
  Outgoing interface list:
    Ethernet1/0, Forward/Sparse-Dense, 00:05:10/00:03:04

(10.0.0.1, 239.1.2.3), 00:02:49/00:03:29, flags: T
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
  Outgoing interface list:
    Ethernet1/0, Forward/Sparse-Dense, 00:02:49/00:03:04

(*, 224.0.1.39), 00:10:05/stopped, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet1/0, Forward/Sparse-Dense, 00:05:15/00:00:00
    Ethernet0/0, Forward/Sparse-Dense, 00:10:05/00:00:00
```

次に、着信インターフェイスに対する **show ip interface** コマンドの出力例を示します。 図に示されているラスト ホップ ルータ上で IP マルチキャスト高速スイッチングがイネーブルにされてい

ることを確認する場合は、この例のこのコマンドを使用します。IP マルチキャスト高速スイッチングがイネーブルの場合、「IP multicast fast switching is enabled」という行が出力に表示されます。

```
Router# show ip interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 172.31.100.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.1 224.0.0.22 224.0.0.13
      224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

次に、**show ip pim interface count** コマンドの出力例を示します。図に示されているラスト ホップルータにマルチキャスト トラフィックが転送されていることを確認する場合は、この例のこのコマンドを使用します。出力例では、Mpackets In/Out フィールドに注意してください。このフィールドでは、出力に一覧表示されている各インターフェイスで送受信されたマルチキャスト パケットの数が表示されます。

```
Router# show ip pim interface count

State: * - Fast Switched, D - Distributed Fast Switched
       H - Hardware Switching Enabled
Address          Interface                FS Mpackets In/Out
172.31.100.2     GigabitEthernet0/0/0     *   4122/0
10.1.0.1         GigabitEthernet1/0/0     *   0/3193
```

次に、**show ip mroute** コマンドに **count** キーワードを指定した場合の出力例を示します。図に示されているラストホップルータで、アクティブなソースからグループへパケットが送信されているを確認する場合は、このコマンドを使用します。出力例では、Forwarding フィールドに表示されているパケット数に注意してください。このフィールドでは、グループに送信を実行しているソースに対するパケット転送カウントが表示されます。

```
Router# show ip mroute count
IP Multicast Statistics
6 routes using 4008 bytes of memory
3 groups, 1.00 average sources per group
```

```
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 239.1.2.3, Source count: 1, Packets forwarded: 3165, Packets received: 3165
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
  Source: 10.0.0.1/32, Forwarding: 3165/20/28/4, Other: 0/0/0

Group: 224.0.1.39, Source count: 1, Packets forwarded: 21, Packets received: 120
  Source: 172.16.0.1/32, Forwarding: 21/1/48/0, Other: 120/0/99

Group: 224.0.1.40, Source count: 1, Packets forwarded: 10, Packets received: 10
  Source: 172.16.0.1/32, Forwarding: 10/1/48/0, Other: 10/0/0
```

次に、**show ip mroute** コマンドに **active** キーワードを指定した場合の出力例を示します。 ラスト ホップルータ上でアクティブなソースがあるマルチキャスト グループを確認する場合は、図に示されているラスト ホップ ルータでこのコマンドを使用します。

（注） 出力の「（?）」は、ルータによって、IP アドレスをホスト名に解決できなかったことを示します。

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 50 secs), 4 kbps(life avg)
```

SPT が使用されているルータでの IP マルチキャストの確認例

次に、特定のグループに対する **show ip mroute** コマンドの出力例を示します。 ソースへの RPF ネイバーが、図に示されている SPT が使用されているルータで想定されている RPF ネイバーであることを確認する場合は、この例のコマンドを使用します。

```
Router# show ip mroute 239.1.2.3
(*, 239.1.2.3), 00:17:56/00:03:02, RP 172.16.0.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0/0, Forward/Sparse-Dense, 00:17:56/00:03:02

(10.0.0.1, 239.1.2.3), 00:15:34/00:03:28, flags: T
  Incoming interface: Serial1/0, RPF nbr 172.31.200.1
  Outgoing interface list:
```

Ethernet0/0, Forward/Sparse-Dense, 00:15:34/00:03:02

次に、図に示されている SPT が使用されているルータからの、**active** キーワードを指定した **show ip mroute** コマンドの出力例を示します。 このルータでアクティブなソースがあるマルチキャスト グループを確認する場合は、このコマンドを使用します。

（注） 出力の「（?）」は、ルータによって、IP アドレスをホスト名に解決できなかったことを示します。

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
```

```
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)
```

ファースト ホップ ルータでの IP マルチキャストの確認例

次に、特定のグループに対する **show ip mroute** コマンドの出力例を示します。 図に示されているファーストホップルータで、アクティブなソースからグループへパケットが送信されていることを確認する場合は、この例のこのコマンドを使用します。 出力例では、Forwarding フィールドに表示されているパケット数に注意してください。 このフィールドでは、ファースト ホップ ルータ上のグループに送信を実行しているソースに対するパケット転送カウントが表示されます。

（注） RPF nbr 0.0.0.0 のフィールドは、mroute のソースが到達したことを示します。

```
Router# show ip mroute 239.1.2.3
(*, 239.1.2.3), 00:18:10/stopped, RP 172.16.0.1, flags: SPF
  Incoming interface: Serial1/0, RPF nbr 172.31.200.2
  Outgoing interface list: Null

(10.0.0.1, 239.1.2.3), 00:18:10/00:03:22, flags: FT
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Serial1/0/0, Forward/Sparse-Dense, 00:18:10/00:03:19
```

次に、図に示されているファースト ホップ ルータからの、**active** キーワードを指定した **show ip mroute** コマンドの出力例を示します。

（注） 出力の「（?）」は、ルータによって、IP アドレスをホスト名に解決できなかったことを示します。

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IP マルチキャスト テクノロジー分野の概要	「IP マルチキャスト テクノロジーの概要」モジュール
PIM-SM と SSM の概念および設定例	「基本的な IP マルチキャスト設定」モジュール

関連項目	マニュアル タイトル
IP マルチキャスト コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用に関する注意事項、および例	『*Cisco IOS IP Multicast Command Reference*』

標準

標準	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IP マルチキャスト オペレーションに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *14*：*IP* マルチキャスト オペレーションに関する機能情報

機能名	リリース	機能情報
Cisco IOS XE Release 2(1) 以降にこのモジュールで導入または変更された機能はないため、この表は空白になっています。この表は、このモジュールに機能情報が追加されると更新されます。	--	--

第 11 章

IP マルチキャストのモニタリングおよび保持

このモジュールでは、IP マルチキャスト ネットワークをモニタリングおよび保持する方法について説明します。

- ローカル ルータとピアリングしている隣接マルチキャスト ルータを表示する方法
- マルチキャスト パケット レートおよび損失情報を表示する方法
- マルチキャスト配信ツリーでソースから宛先ブランチまでのパスを追跡する方法
- IP マルチキャスト ルーティング テーブルの内容、PIM に設定されているインターフェイスに関する情報、ルータによって検出された PIM ネイバー、および IP 高速スイッチング キャッシュの内容を表示する方法
- キャッシュ、テーブル、およびデータベースをクリアする方法
- IP マルチキャスト パケットの配信をモニタリングし、配信によって特定のパラメータが満たされなかった場合にアラートを受け取る方法（IP マルチキャスト ハートビート）
- セッション記述プロトコル、セッション通知プロトコル、およびアプリケーションを使用して、マルチキャスト マルチメディア会議および他のマルチキャスト セッションのアドバタイズメントを補助し、参加者予定者に対して関連セッションの設定情報を通信する方法（SAP リスナー サポート）
- IP マルチキャスト パケット ヘッダーをキャッシュに格納する方法、およびネットワーク内で誰がどのグループに IP マルチキャスト パケットを送信しているかについての情報や、マルチキャスト転送ループなどの情報を検索して表示する方法
- 簡易ネットワーク管理プロトコル（SNMP）を使用して、管理対象オブジェクトをリモートにモニタリングし、PIM を設定する方法
- デバッグ メッセージを記録するために IP マルチキャストの高速スイッチングをディセーブルにする方法

- 機能情報の確認，242 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

IP マルチキャストのモニタリングおよび保持の前提条件

- このモジュールの作業を実行する前に、「IP マルチキャスト テクノロジーの概要」モジュールで説明している概念をよく理解しておく必要があります。
- 使用しているネットワークで IP マルチキャストをイネーブルにし、Protocol Independent Multicast（PIM）を設定して実行しておく必要もあります。 「基本的な IP マルチキャスト設定」モジュールを参照してください。

IP マルチキャストのモニタリングおよび保持について

IP マルチキャスト ハートビート

IP マルチキャスト ハートビート機能を使用すると、IP マルチキャスト パケットの配信をモニタリングし、配信によって特定のパラメータが満たされなかった場合にアラートを受け取ることができます。

代わりに MRM を使用して IP マルチキャストをモニタリングすることもできますが、MRM で実行できない IP マルチキャスト ハートビートでは、次の作業を実行できます。

- SNMP トラップの生成

- 実働マルチキャスト ストリームのモニタリング

IPマルチキャストハートビートがイネーブルの場合、ルータは、特定の間隔で特定のマルチキャスト グループ宛ての IP マルチキャスト パケットをモニタします。 観察されたパケット数が設定された最小量よりも少ない場合、ルータは指定されたネットワーク管理ステーションにハートビート例外の損失を示す SNMP トラップを送信します。

ルータの *group* に既存のマルチキャスト転送状態がない場合、**ip multicast heartbeat** コマンドによってハートビートは作成されません。 このコマンドでは、ルータでのマルチキャスト転送状態は作成されません。IPマルチキャストトラフィックを強制的に転送する場合は、ルータまたはダウンストリーム ルータ上で **ip igmp static-group** コマンドを実行します。 特定のレシーバ ホストへの IP マルチキャスト トラップの送信をイネーブルにする場合は、**snmp-server host ipmulticast** コマンドを使用します。 マルチキャスト ハート ビート機能をデバッグする場合は、**debug ip mhbeat** コマンドを使用します。

セッション通知プロトコル（SAP）

セッション記述プロトコル、セッション通知プロトコル、およびアプリケーションを使用して、マルチキャストマルチメディア会議および他のマルチキャストセッションのアドバタイズメントを補助し、参加予定者に対して関連セッション設定情報を通信するには、セッション通知プロトコル（SAP）リスナー サポートが必要です。

セッションは、RFC 2327 で定義されているセッション記述プロトコル（SDP）で記述されます。SDP では、存続可能時間（TTL）スコープ、グループアドレス、およびユーザデータグラムプロトコル（UDP）ポート番号などの特定の属性で、セッション（たとえば、音声、ビデオ、ホワイトボードなど）で使用されているセッションプロパティ（たとえば、連絡情報、セッションライフタイム、メディアなど）の、書式化されたテキスト説明が提供されます。

多くのマルチメディア アプリケーションは、セッションの説明について SDP に依存します。 ただし、これらは異なる方法を使用してこれらのセッションの説明が配信される場合があります。たとえば、IP/TV では、Web に依存して、参加者にセッションの説明が配信されます。 この例では、参加者は、セッション情報を提供する Web サーバを認識する必要があります。

MBONEアプリケーション（たとえば、vic、vat、wbなど）やその他のアプリケーションは、ネットワーク中に送信されるマルチキャストセッション情報に依存します。 これらの場合、SDPセッション通知の転送に SAP が使用されます。 SAP バージョン 2 では、周知のセッション ディレクトリ マルチキャスト グループ 224.2.127.254 が使用されて、グローバル スコープ セッションおよび管理スコープ セッションのグループ 239.255.255.255 の SDP セッションの説明が配信されます。

（注） Session Directory（SDR）アプリケーションは、通常、SDP/SAP セッション通知の送受信に使用されます。

IP マルチキャストに対する SNMP トラップの PIM MIB 拡張

Protocol Independent Multicast（PIM）は、マルチキャスト グループにマルチキャスト データ パケットをルーティングするために使用される IP マルチキャスト ルーティング プロトコルです。 RFC 2934 には、IPv4 対応 PIM MIB が定義されています。これは、簡易ネットワーク管理プロトコル（SNMP）を使用した PIM のリモート モニタリングと設定を可能にする管理対象オブジェクトに関する記述です。

PIM MIB 拡張は、次の新しいクラスの PIM 通知を導入します。

- neighbor-change：この通知は、次の条件により発生します。
  - ルータの PIM インターフェイスが（インターフェイス コンフィギュレーション モードで **ip pim** コマンドを使用して）無効化、または有効化されている。
  - ルータの PIM ネイバーの隣接関係が失効している（RFC 2934 の定義による）。
- rp-mapping-change：この通知は、自動 RP メッセージまたはブートストラップ ルータ（BSR）メッセージが原因でランデブーポイント（RP）マッピング情報が変更された場合に発生します。
- invalid-pim-message：この通知は、次の条件により発生します。
  - デバイスが、無効な（*, G）加入またはプルーニング メッセージを受信した場合（たとえば、パケットで指定された RP がマルチキャスト グループの RP ではない加入またはプルーニング メッセージを、ルータが受信した場合）
  - デバイスが、無効な PIM 登録メッセージを受信した場合（たとえば、RP ではないマルチキャスト グループからの登録メッセージをルータが受信した場合）

PIM MIB 拡張の利点

PIM MIB 拡張：

- RP マッピングの変更点を検出することで、ネットワークにおけるマルチキャスト トポロジの変更点を特定できます。
- PIM が有効なインターフェイス上で、PIM プロトコルをモニタリングするトラップを提供します。
- マルチキャスト インターフェイスでマルチキャスト ネイバー隣接関係が失効している場合、ルーティングの問題の特定に役立ちます。
- RP 設定のエラー（たとえば、Auto-RP のような、ダイナミック RP 割り当てプロトコルにおけるフラッピングによるエラー）をモニタリングできます。

IP マルチキャストのモニタリングおよび保持の方法

マルチキャスト ピア、パケット レート、および損失情報を表示し、パスを追跡する

ローカル ルータとピアリングしている隣接マルチキャスト ルータ、マルチキャスト パケット レート、および損失情報を確認する場合、または、マルチキャスト配信ツリーでソースから宛先ブランチまでのパスを追跡する場合には、IP マルチキャスト ルーティングをモニタリングします。

手順の概要

1. **enable**
2. **mrinfo** [*host-name* | *host-address*] [*source-address* | *interface*]
3. **mstat** {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*]
4. **mtrace** {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**mrinfo** [*host-name* | *host-address*] [*source-address* | *interface*] 例： `Router# mrinfo`	（任意）ローカル ルータと「ピアリング」している隣接マルチキャスト ルータを問い合わせます。
ステップ 3	**mstat** {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*] 例： `Router# mstat allsource`	（任意）IP マルチキャスト パケット レートおよび損失情報を表示します。

	コマンドまたはアクション	目的
ステップ 4	**mtrace** {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*] 例： `Router# mtrace allsource`	（任意）マルチキャスト配信ツリーでソースから宛先ブランチへのパスを追跡します。

IP マルチキャスト システムおよびネットワーク統計情報の表示

IP マルチキャスト ルーティング テーブルの内容、PIM で設定されているインターフェイスに関する情報、ルータによって検出される PIM ネイバー、IP 高速スイッチング キャッシュの内容、および循環キャッシュ ヘッダー バッファの内容を表示する場合は、IP マルチキャスト システム統計情報を表示します。

手順の概要

1. **enable**
2. **ping** [*group-name* | *group-address*]
3. **show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*type number*] [**summary**] [**count**] [**active** *kbps*]
4. **show ip pim interface** [*type number*] [**df** | **count**] [*rp-address*] [**detail**]
5. **show ip pim neighbor** [*type number*]
6. **show ip pim rp** [**mapping** | **metric**] [*rp-address*]
7. **show ip rpf** {*source-address* | *source-name*} [**metric**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**ping** [*group-name* | *group-address*] 例： `Router# ping cbone-audio`	（任意）マルチキャスト グループ アドレスまたはグループ名に、ICMP エコー要求メッセージを送信します。

	コマンドまたはアクション	目的
ステップ 3	**show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*type number*] [**summary**] [**count**] [**active** *kbps*] 例： `Router# show ip mroute cbone-audio`	（任意）IP マルチキャスト ルーティング テーブルの内容を表示します。
ステップ 4	**show ip pim interface** [*type number*] [**df** | **count**] [*rp-address*] [**detail**] 例： `Router# show ip pim interface gigabitethernet1/0/0 detail`	（任意）PIM に対して設定されたインターフェイスに関する情報を表示します。
ステップ 5	**show ip pim neighbor** [*type number*] 例： `Router# show ip pim neighbor`	（任意）ルータによって検出された PIM ネイバーのリストを表示します。
ステップ 6	**show ip pim rp** [**mapping** | **metric**] [*rp-address*] 例： `Router# show ip pim rp metric`	（任意）スパース モード マルチキャスト グループに関連付けられた RP ルータを表示します。
ステップ 7	**show ip rpf** {*source-address* | *source-name*} [**metric**] 例： `Router# show ip rpf 172.16.10.13`	（任意）ルータによる RPF の実行方法（つまり、ユニキャスト ルーティング テーブルからか、DVMRP ルーティング テーブルからか、またはスタティック mroute からか）を表示します。また、ユニキャスト ルーティング メトリックも表示します。

IP マルチキャスト ルーティング テーブルまたはキャッシュのクリア

IP マルチキャスト ルーティング テーブル、Auto-RP キャッシュ、IGMP キャッシュ、および Catalyst スイッチのキャッシュからエントリを削除する場合は、IP マルチキャスト キャッシュをクリアします。 これらのエントリがクリアされると、再認識、つまり不正確なエントリの削除によって、情報がリフレッシュされます。

手順の概要

1. **enable**
2. **clear ip mroute** {* | *group-name* [*source-name* | *source-address*] | *group-address* [*source-name* | *source-address*]}
3. **clear ip pim auto-rp** *rp-address*
4. **clear ip igmp group** [*group-name* | *group-address* | *interface-type interface-number*]
5. **clear ip cgmp** [*interface-type interface-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear ip mroute** {*	*group-name* [*source-name*	*source-address*]	*group-address* [*source-name*	*source-address*]} 例： `Router# clear ip mroute 224.2.205.42 228.3.0.0`	（任意）IP マルチキャスト ルーティング テーブルからエントリを削除します。
ステップ 3	**clear ip pim auto-rp** *rp-address* 例： `Router# clear ip pim auto-rp 224.5.6.7`	（任意）Auto-RP キャッシュをクリアします。
ステップ 4	**clear ip igmp group** [*group-name*	*group-address*	*interface-type interface-number*] 例： `Router# clear ip igmp group 224.0.255.1`	（任意）IGMP キャッシュからエントリを削除します。
ステップ 5	**clear ip cgmp** [*interface-type interface-number*] 例： `Router# clear ip cgmp`	（任意）Catalyst スイッチのキャッシュから、すべてのグループ エントリをクリアします。

IP マルチキャスト ハート ビートを使用した IP マルチキャスト配信のモニタリング

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast-routing distributed**
4. **snmp-server host** {*hostname* | *ip-address*} [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string*[**udp-port** *port*] [*notification-type*]
5. **snmp-server enable traps ipmulticast**
6. **ip multicast heartbeat** *group-address minimum-number window-size interval*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip multicast-routing distributed** 例： `Router(config)# ip multicast-routing distributed`	IP マルチキャスト ルーティングをイネーブルにします。
ステップ 4	**snmp-server host** {*hostname* | *ip-address*} [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string*[**udp-port** *port*] [*notification-type*] 例： `Router(config)# snmp-server host 224.1.0.1 traps public`	SNMP 通知動作の受信者を指定します。

	コマンドまたはアクション	目的
ステップ 5	**snmp-server enable traps ipmulticast** 例： `Router(config)# snmp-server enable traps ipmulticast`	IP マルチキャスト トラップを送信するようにルータをイネーブルにします。
ステップ 6	**ip multicast heartbeat** *group-address minimum-number window-size interval* 例： `Router(config)# ip multicast heartbeat 224.1.1.1 1 1 10`	IP マルチキャスト パケット配信のモニタリングをイネーブルにします。 • マルチキャスト高速スイッチング（MDFS）が使用されるプラットフォームでは、パケット カウンタは 10 秒ごとにのみ更新されるため、これらのプラットフォームでは、*interval* を 10 秒の倍数で設定する必要があります。他のプラットフォームでは、増分が異なる場合があります。

SAP リスナーを使用したマルチキャスト マルチメディア セッションのアドバタイズ

セッション記述プロトコル、セッション通知プロトコル、およびアプリケーションを使用して、マルチキャスト マルチメディア会議および他のマルチキャスト セッションのアドバタイズメントを補助し、参加予定者に対して関連セッション設定情報を通信する場合は、SAP リスナー サポートをイネーブルにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sap cache-timeout** *minutes*
4. **interface** *type number*
5. **ip sap listen**
6. **end**
7. **clear ip sap** [*group-address* | **“** *session-name* **”**]
8. **show ip sap** [*group-address* | **“** *session-name* **”**| **detail**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip sap cache-timeout** *minutes* 例： `Router(config)# ip sap cache-timeout 600`	（任意）SAP キャッシュ エントリがキャッシュ内でアクティブのままである期間を制限します。 • デフォルトでは、SAP キャッシュ エントリはネットワークから受信した 24 時間後に削除されます。
ステップ 4	**interface** *type number* 例： `Router(config)# interface gigabitethernet 1/0/0`	IGMPv3 をイネーブルにできるホストに接続されているインターフェイスを選択します。
ステップ 5	**ip sap listen** 例： `Router(config-if)# ip sap listen`	セッション ディレクトリ通知をリッスンするように、Cisco IOS XE ソフトウェアをイネーブルにします。
ステップ 6	**end** 例： `Router(config-if)# end`	セッションを終了し、EXEC モードに戻ります。
ステップ 7	**clear ip sap** [*group-address* | **“** *session-name* **”**] 例： `Router# clear ip sap "Sample Session"`	SAP キャッシュ エントリまたは SAP キャッシュ全体をクリアします。
ステップ 8	**show ip sap** [*group-address* | **“** *session-name* **”**| **detail**]	（任意）SAP キャッシュを表示します。

	コマンドまたはアクション	目的
	例： `Router# show ip sap 224.2.197.250 detail`	

IP マルチキャストの高速スイッチングのディセーブル化

高速スイッチングがイネーブルの場合、デバッグメッセージは記録されないため、デバッグメッセージを記録する場合は高速スイッチングをディセーブルにします。

パケットが宛先に到達していない場合にも、ルータがプロセス スイッチングに置かれる高速スイッチングをディセーブルにすると効果的な場合があります。 高速スイッチングがディセーブルで、パケットが宛先に到達している場合は、スイッチングが原因の可能性があります。

IPマルチキャストパケットの高速スイッチングは、デフォルトで、1つの例外を除き、（総称ルーティング カプセル化（GRE）およびDVMRP トンネルを含む）すべてのインターフェイス上でイネーブルです。例外とは、X.25 カプセル化インターフェイスを介する場合で、この場合、IP マルチキャストパケットの高速スイッチングはディセーブルにされ、サポートされません。次は、高速スイッチングのプロパティです。

- マルチキャスト ルーティング テーブル エントリの着信インターフェイス上で高速スイッチングがディセーブルの場合、発信インターフェイス リストのすべてのインターフェイスのプロセス レベルで、パケットが送信されます。
- マルチキャスト ルーティング テーブル エントリの発信インターフェイス上で高速スイッチングがディセーブルの場合、パケットは、そのインターフェイスのプロセス レベルのスイッチングですが、発信インターフェイス リストにある他のインターフェイスの高速スイッチングの可能性があります。
- 高速スイッチングがイネーブルの場合、デバッグ メッセージのロギングは行われません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip mroute-cache**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface gigabitethernet 1/0/0`	インターフェイスを指定します。
ステップ 4	**no ip mroute-cache** 例： `Router(config-if)# no ip mroute-cache`	IP マルチキャストの高速スイッチングをディセーブルにします。

IP マルチキャストに対する PIM MIB 拡張のイネーブル化

IP マルチキャストの PIM MIB 拡張をイネーブルにするには、この作業を実行します。

（注） 次の MIB テーブルは、Cisco IOS および Cisco IOS XE ソフトウェアではサポートされていません。

- pimIpMRouteTable
- pimIpMRouteNextHopTable
- pimInterfaceVersion オブジェクトは RFC 2934 から削除されたため、ソフトウェアではサポートされなくなりました。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pim** [**neighbor-change** | **rp-mapping-change** | **invalid-pim-message**]
4. **snmp-server host** *host-address* [**traps** | **informs**] *community-string* **pim**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server enable traps pim** [**neighbor-change**	**rp-mapping-change**	**invalid-pim-message**] 例： `Router(config)# snmp-server enable traps pim neighbor-change`	ルータを、PIM通知を送信するようにルータをイネーブルにします。 • **neighbor-change**：このキーワードは、ルータのPIMインターフェイスがディセーブル、またはイネーブルである、あるいはルータの PIM ネイバー隣接関係が失効していることを示す通知をイネーブル化します。 • **rp-mapping-change**：このキーワードは、Auto-RP メッセージまたはBSRメッセージによるRPマッピング情報の変更を示す通知をイネーブルにします。 • **invalid-pim-message**：このキーワードは、無効なPIMプロトコル操作のモニタリングの通知をイネーブルにします（たとえば、パケットで指定されたRPがマルチキャスト グループのRPではない加入またはプルーニング メッセージをルータが受信した場合や、RP ではないマルチキャスト グループからの登録メッセージをルータが受信した場合）。
ステップ 4	**snmp-server host** *host-address* [**traps**	**informs**] *community-string* **pim** 例： `Router(config)# snmp-server host 10.10.10.10 traps public pim`	PIM SNMP 通知動作の受信者を指定します。

IP マルチキャストのモニタリングおよび保持の設定例

IP マルチキャスト システムおよびネットワーク統計情報の表示例

次に、**mrinfo** コマンドの出力例を示します。

```
Router# mrinfo

192.31.7.37 (labs-allcompany) [version cisco 12.3] [flags: PMSA]:
192.31.7.37 -> 192.31.7.34 (lab-southwest) [1/0/pim]
192.31.7.37 -> 192.31.7.47 (lab-northwest) [1/0/pim]
192.31.7.37 -> 192.31.7.44 (lab-southeast) [1/0/pim]
131.119.26.10 -> 131.119.26.9 (lab-northeast) [1/32/pim]
```

ユーザ EXEC モードで実行した **mstat** コマンドからの出力例は次のとおりです。

```
Router> mstat labs-in-china 172.16.0.1 224.0.255.255

Type escape sequence to abort.
Mtrace from 172.16.0.0 to 172.16.0.10 via group 224.0.255.255
>From source (labs-in-china) to destination (labs-in-africa)
Waiting to accumulate statistics......
Results after 10 seconds:
Source Response Dest Packet Statistics For Only For Traffic
172.16.0.0      172.16.0.10 All Multicast Traffic From 172.16.0.0
| __/ rtt 48 ms Lost/Sent = Pct Rate To 224.0.255.255
v / hop 48 ms -------------------- --------------------
172.16.0.1      labs-in-england
| ^ ttl 1
v | hop 31 ms 0/12 = 0% 1 pps 0/1 = --% 0 pps
172.16.0.2
172.16.0.3   infolabs.com
| ^ ttl 2
v | hop -17 ms -735/12 = --% 1 pps 0/1 = --% 0 pps
172.16.0.4
172.16.0.5      infolabs2.com
| ^ ttl 3
v | hop -21 ms -678/23 = --% 2 pps 0/1 = --% 0 pps
172.16.0.6
172.16.0.7      infolabs3.com
| ^ ttl 4
v | hop 5 ms 605/639 = 95% 63 pps 1/1 = --% 0 pps
172.16.0.8
172.16.0.9      infolabs.cisco.com
| \__ ttl 5
v \ hop 0 ms 4 0 pps 0 0 pps
172.16.0.0      172.16.0.10
Receiver Query Source
```

ユーザ EXEC モードで実行した **mtrace** コマンドからの出力例は次のとおりです。

```
Router> mtrace 172.16.0.0 172.16.0.10 239.254.254.254
Type escape sequence to abort.
Mtrace from 172.16.0.0 to 172.16.0.10 via group 239.254.254.254
From source (?) to destination (?)
Querying full reverse path...
0 172.16.0.10
-1 172.16.0.8 PIM thresh^ 0 0 ms
-2 172.16.0.6 PIM thresh^ 0 2 ms
```

```
-3 172.16.0.5 PIM thresh^ 0 894 ms
-4 172.16.0.3 PIM thresh^ 0 893 ms
-5 172.16.0.2 PIM thresh^ 0 894 ms
-6 172.16.0.1 PIM thresh^ 0 893 ms
```

IP マルチキャスト ハート ビートを使用した IP マルチキャスト配信のモニタリング例

次に、このルータを介してグループ アドレス 244.1.1.1 に転送される IP マルチキャスト パケットをモニタリングする例を示します。このグループのパケットが10秒間受信されなかった場合、IP アドレス 224.1.0.1 で SNMP 管理ステーションに SNMP トラップが送信されます。

```
!
ip multicast-routing
!
snmp-server host 224.1.0.1 traps public
snmp-server enable traps ipmulticast
ip multicast heartbeat 224.1.1.1 1 1 10
```

SAP リスナーを使用したマルチキャストマルチメディアセッションのアドバタイズ例

次に、セッションディレクトリ通知をルータでリッスンできるようにし、SAP キャッシュ タイムアウトを 30 分に変更します。

```
ip multicast routing
ip sap cache-timeout 30
interface loopback 0
 ip address 10.0.0.51 255.255.255.0
 ip pim sparse-dense mode
 ip sap listen
```

次に、マルチキャスト グループ 224.2.197.250 を使用したセッションに対する **show ip sap** コマンドの出力例を示します。

```
Router# show ip sap 224.2.197.250
SAP Cache - 198 entries
Session Name: Session1
   Description: This broadcast is brought to you courtesy of Name1.
   Group: 0.0.0.0, ttl: 0, Contiguous allocation: 1
   Lifetime: from 10:00:00 PDT Jul 4 1999 until 10:00:00 PDT Aug 1 1999
   Uptime: 4d05h, Last Heard: 00:01:40
   Announcement source: 128.102.84.134
   Created by: sample 3136541828 3139561476 IN IP4 128.102.84.134
   Phone number: Sample Digital Video Lab (555) 555-5555
   Email: email1 <name@email.com>
   URL: http://url.com/
   Media: audio 20890 RTP/AVP 0
     Media group: 224.2.197.250, ttl: 127
     Attribute: ptime:40
   Media: video 62806 RTP/AVP 31
     Media group: 224.2.190.243, ttl: 127
```

IP マルチキャスト システムおよびネットワーク統計情報の表示例

show ip mroute

次に、スパース モードで動作しているルータに関する **show ip mroute** コマンドの出力例を示します。

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode
(*, 224.0.255.3), uptime 5:29:15, RP is 192.168.37.2, flags: SC
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1, Dvmrp
  Outgoing interface list:
    GigabitEthernet0, Forward/Sparse, 5:29:15/0:02:57
(192.168.46.0/24, 224.0.255.3), uptime 5:29:15, expires 0:02:59, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1
  Outgoing interface list:
 GigabitEthernet0, Forward/Sparse, 5:29:15/0:02:57
```

show ip pim interface

次に、インターフェイスを指定した場合の **show ip pim interface** コマンドのサンプル出力を示します。

```
Router# show ip pim interface GigabitEthernet1/0/0

Address          Interface                Ver/   Nbr    Query  DR     DR
                                          Mode   Count  Intvl  Prior
172.16.1.4       GigabitEthernet1/0/0     v2/S   1      100 ms 1      172.16.1.4
```

次に、**show ip pim rp** コマンドの出力例を示します。

```
Router# show ip pim rp

Group:227.7.7.7, RP:10.10.0.2, v2, v1, next RP-reachable in 00:00:48
```

show ip pim rp

次に、**mapping** キーワードを指定した **show ip pim rp** コマンドの出力例を示します。

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent
Group(s) 227.0.0.0/8
  RP 10.10.0.2 (?), v2v1, bidir
    Info source:10.10.0.2 (?), via Auto-RP
         Uptime:00:01:42, expires:00:00:32
Group(s) 228.0.0.0/8
  RP 10.10.0.3 (?), v2v1, bidir
    Info source:10.10.0.3 (?), via Auto-RP
         Uptime:00:01:26, expires:00:00:34
Group(s) 229.0.0.0/8
  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir
```

```
    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP
         Uptime:00:00:52, expires:00:00:37
Group(s) (-)230.0.0.0/8
  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir
    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP
         Uptime:00:00:52, expires:00:00:37
```

次に、**metric** キーワードを指定した **show ip pim rp** コマンドの出力例を示します。

```
Router# show ip pim rp metric

RP Address      Metric Pref    Metric       Flags   RPF Type   Interface
10.10.0.2       0              0              L     unicast    Loopback0
10.10.0.3       90             409600         L     unicast    GigabitEthernet3/3/0
10.10.0.5       90             435200         L     unicast    GigabitEthernet3/3/0
```

show ip rpf

次に、**show ip rpf** コマンドの出力例を示します。

```
Router# show ip rpf 172.16.10.13

RPF information for host1 (172.16.10.13)
  RPF interface: BRI0
  RPF neighbor: sj1.cisco.com (172.16.121.10)
  RPF route/mask: 172.16.0.0/255.255.0.0
  RPF type: unicast
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
```

次に、**metric** キーワードを指定した **show ip rpf** コマンドの出力例を示します。

```
Router# show ip rpf 172.16.10.13 metric
RPF information for host1.cisco.com (172.16.10.13)
  RPF interface: BRI0
  RPF neighbor: neighbor.cisco.com (172.16.121.10)
  RPF route/mask: 172.16.0.0/255.255.0.0
  RPF type: unicast
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Metric preference: 110
```

例：IP マルチキャストに対する PIM MIB 拡張のイネーブル化例

次に、デバイスの PIM インターフェイスがイネーブルにされたことを示す通知を生成するようにデバイスを設定する例を示します。 最初の行では、PIM トラップが、IP アドレス 10.0.0.1 のホストに SNMP v2c として送信されるように設定されます。2行目では、トラップ通知の neighbor-change クラスをホストに送信するように、デバイスが設定されます。

```
snmp-server host 10.0.0.1 traps version 2c public pim
snmp-server enable traps pim neighbor-change
interface ethernet0/0
 ip pim sparse-dense-mode
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP SLA コマンド	『Cisco IOS IP Multicast Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 2934	『*Protocol Independent Multicast for IPv4 MIB*』

MIB

MIB	MIB のリンク
• CISCO-IPMROUTE-MIB • MSDP-MIB • IGMP-STD-MIB	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP マルチキャストのモニタリングおよび保持の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *15*：*IP* マルチキャストのモニタリングおよび保持の機能情報

機能名	リリース	機能の設定情報
PIM MIB 拡張	Cisco IOS XE Release 2.1	Protocol Independent Multicast（PIM）は、マルチキャスト グループにマルチキャスト データ パケットをルーティングするために使用される IP マルチキャスト ルーティング プロトコルです。 RFC 2934 には、IPv4 MIB 対応 PIM が定義されています。これは、簡易ネットワーク管理プロトコル（SNMP）を使用した PIM のリモート モニタリングと設定を可能にする管理対象オブジェクトに関する記述です。
マルチキャスト ハートビート	Cisco IOS XE Release 2.1	IP マルチキャスト ハートビート機能によって、IP マルチキャスト配信のステータスをモニタリングし、配信に障害が発生した場合に（簡易ネットワーク管理プロトコル（SNMP）トラップを介して）通知を受ける手段が提供されます。

第 12 章

IPv6 マルチキャスト：PIM スパース モード

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

IPv6 マルチキャスト PIM スパース モードに関する情報

プロトコル独立マルチキャスト

プロトコル独立マルチキャスト（PIM）は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにデバイス間で使用されます。 PIM は、ユニキャスト ルーティング プロトコルとは独立して動作し、他のプロ

トコルと同様に、マルチキャスト ルート アップデートの送受信を実行します。ユニキャスト ルーティング テーブルに値を入力するために LAN でどのユニキャスト ルーティング プロトコルが使用されているかどうかにかかわらず、Cisco IOS PIM では、独自のルーティング テーブルを構築および管理する代わりに、既存のユニキャスト テーブル コンテンツを使用して、リバース パス転送（RPF）チェックを実行します。

PIM スパース モード（SM）または PIM 送信元固有マルチキャスト（SSM）動作のいずれかを使用するように IPv6 マルチキャストを設定することも、ネットワークで PIM-SM と PIM-SSM の両方を使用することもできます。

PIM スパース モード

IPv6 マルチキャストでは、PIM-SM を使用したドメイン内マルチキャスト ルーティングがサポートされています。PIM-SM は、ユニキャスト ルーティングを使用して、マルチキャスト ツリー構築用のリバース パス情報を提供しますが、特定のユニキャスト ルーティング プロトコルには依存しません。

PIM-SM は、トラフィックに対して明示的な要求がある場合を除いて、各マルチキャストに関与しているデバイスの数が比較的少なく、これらのデバイスがグループのマルチキャスト パケットを転送しないときに、マルチキャスト ネットワークで使用されます。PIM-SM は、共有ツリー上のデータ パケットを転送することによって、アクティブな送信元に関する情報を配布します。PIM-SM は最初に共有ツリーを使用しますが、これには RP の使用が必要となります。

要求は、ツリーのルート ノードに向けてホップバイホップで送信される PIM join を使用して行われます。PIM-SM のツリーのルート ノードは、共有ツリーの場合は RP、最短パス ツリー（SPT）の場合はマルチキャスト送信元に直接接続されているファーストホップ デバイスになります。RP はマルチキャスト グループを追跡し、マルチキャスト パケットを送信するホストはそのホストのファーストホップ デバイスによって RP に登録されます。

PIM join がツリーの上位方向に送信されると、要求されたマルチキャスト トラフィックがツリーの下位方向に転送されるように、パス上のデバイスがマルチキャスト転送ステートを設定します。マルチキャスト トラフィックが不要になったら、デバイスはルート ノードに向けてツリーの上位方向に PIM prune を送信し、不必要なトラフィックをプルーニング（削除）送信します。この PIM prune がホップごとにツリーを上位方向に移動する際、各デバイスはその転送状態を適切に更新します。最終的に、マルチキャスト グループまたは送信元に関連付けられている転送ステートは削除されます。

マルチキャスト データの送信側は、マルチキャスト グループを宛先としたデータを送信します。送信側の指定ルータ（DR）は、これらのデータ パケットを受け取り、ユニキャストでカプセル化し、RP に直接送信します。RP は、カプセル化されたこれらのデータ パケットを受信し、カプセル化を解除し、共有ツリー上に転送します。その後、パケットは、RP ツリー上のデバイスの（*, G）マルチキャスト ツリー ステートに従って、RP ツリー ブランチの任意の場所に複製され、そのマルチキャスト グループのすべての受信側に最終的に到達します。RP へのデータ パケットのカプセル化のプロセスは登録と呼ばれ、カプセル化されたパケットは PIM レジスタ パケットと呼ばれます。

指定ルータ

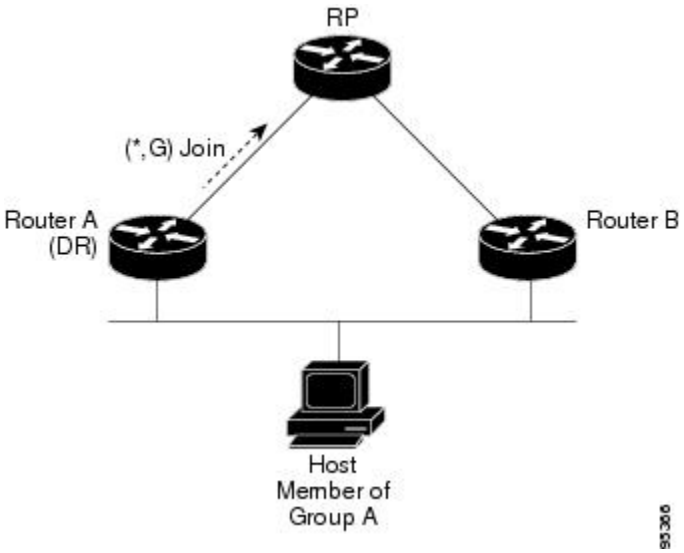
シスコ デバイスは、LAN セグメント上に複数のデバイスが存在する場合、PIM-SM を使用してマルチキャスト トラフィックを転送し、選択プロセスに従って指定デバイスを選択します。

指定ルータ（DR）は、PIM register メッセージ、PIM join メッセージ、および PIM prune メッセージを RP に送信し、アクティブな送信元およびホスト グループ メンバーシップに関する情報を通知します。

LAN 上に複数の PIM-SM デバイスが存在する場合は、DR を選択して、接続されているホストに対するマルチキャスト トラフィックの重複を回避する必要があります。 **ipv6 pim dr-priority** コマンドを使用して DR の選択を強制することを選択しない限り、最も大きい IPv6 アドレスの PIM デバイスが LAN の DR になります。 このコマンドでは、LAN セグメント上の各デバイスの DR プライオリティ（デフォルトのプライオリティ=1）を指定して、最もプライオリティの高いデバイスが DR として選択されるようにすることができます。 LAN セグメント上のすべてのデバイスのプライオリティが同じ場合にも、最上位 IPv6 アドレスを持つデバイスが選択されます。

下の図に、マルチアクセス セグメントでの動作を示します。 デバイス A およびデバイス B は、ホスト A をグループ A のアクティブな受信側として使用する共通のマルチアクセス イーサネット セグメントに接続されます。 DR として動作するデバイス A だけが join を RP に送信して、グループ A の共有ツリーを構築します。 デバイス B も RP への（*, G）join の送信を許可されている場合は、パラレル パスが作成され、ホスト A が重複マルチキャスト トラフィックを受信します。 ホスト A がグループにマルチキャスト トラフィックを送信し始めたら、DR は register メッセージを RP に送信する役割を担います。 両方のデバイスに役割が割り当てられている場合は、RP が重複マルチキャスト パケットを受信します。

図 *16*：マルチアクセス セグメントでの代表ルータの選択



DR で障害が発生した場合、PIM-SM はデバイス A の障害を検出し、フェールオーバー DR を選択する手段を提供します。 DR（デバイス A）が動作不能になった場合、デバイス A とネイバーとの隣接関係がタイムアウトすると、デバイス B はその状況を検出します。 デバイス B はホスト A

から MLD メンバーシップ レポートを受けているため、このインターフェイスでグループ A の MLD ステートをすでに持ち、新しい DR になると即座に RP に join を送信します。 この段階で、デバイス B を経由する共有ツリーの新しいブランチの下位方向へのトラフィック フローが再び確立されます。 また、ホスト A がトラフィックを送信していた場合、デバイス B は、ホスト A から次のマルチキャスト パケットを受信した直後に、新しい登録プロセスを開始します。 このアクションがトリガーとなって、RP は、デバイス B を経由する新しいブランチを介して、ホスト A への SPT に加入します。

ヒント　2 つの PIM デバイスが直接接続されている場合、これらのデバイスはネイバーになります。 PIM ネイバーを表示するには、特権 EXEC モードで **show ipv6 pim neighbor** コマンドを使用します。

（注）　DR 選択プロセスは、マルチアクセス LAN のみで必要です。

ランデブー ポイント

IPv6 PIM では、組み込み RP がサポートされています。 組み込み RP サポートを利用すると、デバイスは、スタティックに設定されている RP の代わりに、マルチキャスト グループ宛先アドレスを使用して RP 情報を学習できるようになります。 デバイスが RP である場合、RP としてスタティックに設定する必要があります。

デバイスは、MLD レポート内、または PIM メッセージおよびデータ パケット内の組み込み RP グループアドレスを検索します。 このようなアドレスが見つかったら、デバイスはアドレス自体からグループの RP を学習します。 この学習された RP は、グループのすべてのプロトコル アクティビティに使用されます。 デバイスが RP である場合、組み込み RP を RP として設定する必要があり、デバイスはそのようにアドバタイズされます。

組み込み RP よりも優先するスタティック RP を選択するには、特定の組み込み RP グループ範囲またはマスクをスタティック RP のアクセス リストに設定する必要があります。 PIM がスパース モードで設定されている場合は、RP として動作する 1 つ以上のデバイスを選択する必要もあります。 RP は、共有配布ツリーの選択ポイントに配置された単一の共通ルートであり、各ボックスでスタティックに設定されます。

PIM DR は、共有ツリーの下位方向に配布するために、直接接続されているマルチキャスト送信元から RP にデータを転送します。 データは次の 2 つの方法のいずれかを使用して RP に転送されます。

- データは、登録パケットにカプセル化され、DR として動作するファーストホップ デバイスによって直接 RP にユニキャストされます。
- RP 自身が送信元ツリーに加入している場合は、PIM スパース モードの項で説明したように、RPF 転送アルゴリズムに従ってマルチキャスト転送されます。

RP アドレスは、パケットをグループに送信するホストの代わりに、ファーストホップ デバイスで PIM register メッセージを送信するために使用されます。 また、ラストホップ デバイスでも、

PIM join および prune メッセージを RP に送信してグループ メンバーシップについて通知するために使用されます。 すべてのデバイス（RP デバイスを含む）で RP アドレスを設定する必要があります。

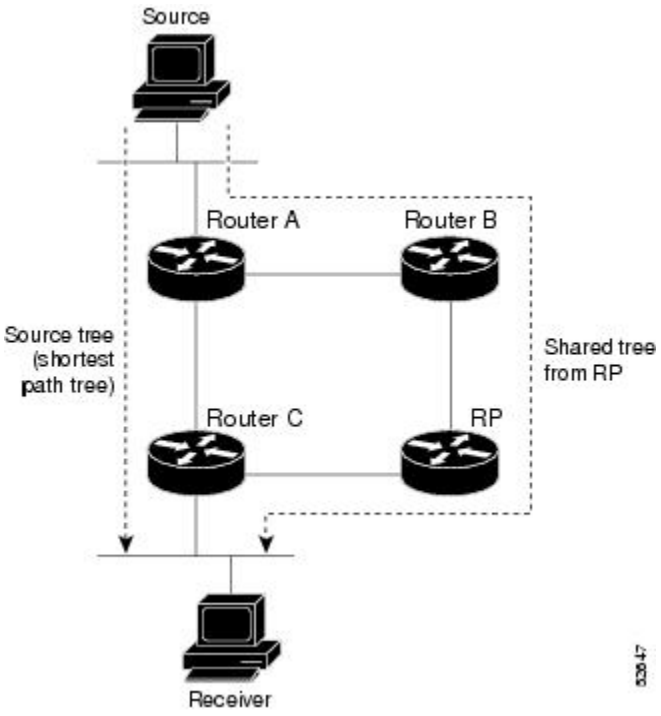
1 台の PIM デバイスを、複数のグループの RP にできます。 特定のグループの PIM ドメイン内で一度に使用できる RP アドレスは 1 つだけです。 アクセス リストで指定されている条件によって、デバイスがどのグループの RP であるかが判別されます。

IPv6 マルチキャストでは、PIM accept register 機能がサポートされています。これは、RP で PIM-SM register メッセージのフィルタリングを実行するための機能です。 ユーザは、アクセス リストを照合するか、または登録されている送信元の AS パスとルート マップに指定されている AS パスを比較できます。

PIM 共有ツリーおよび送信元ツリー（最短パス ツリー）

デフォルトでは、グループのメンバは、RP をルートとする単一のデータ配布ツリーを通じて、送信側からグループへのデータを受信します。 このタイプの配布ツリーは、共有ツリーまたはランデブー ポイント ツリー（RPT）と呼ばれます（下の図を参照）。 送信側からのデータは、RP に配信され、その共有ツリーに加入しているグループ メンバに配布されます。

図 *17*：共有ツリーおよび送信元ツリー（最短パス ツリー）



データしきい値で保証される場合、共有ツリー上のリーフ デバイスは、送信元をルートとするデータ配布ツリーへの切り替えを開始できます。 このタイプの配布ツリーは、最短パスツリーまたは送信元ツリーと呼ばれます。 デフォルトでは、ソフトウェアが送信元から最初のデータ パケットを受信すると、送信元ツリーに切り替わります。

次に、共有ツリーから送信元ツリーに切り替わるプロセスの詳細を示します。

1. 受信側がグループに加入します。リーフ デバイス C が RP に join メッセージを送信します。
2. RP がデバイス C へのリンクを発信インターフェイス リストに登録します。
3. 送信元がデータを送信します。デバイス A が register にデータをカプセル化し、それを RP に送信します。
4. RP が共有ツリーの下位方向のデバイス C にデータを転送し、送信元に join メッセージを送信します。 この時点で、データはデバイス C に 2 回（カプセル化された状態で 1 回、ネイティブの状態で 1 回）着信する可能性があります。
5. データがネイティブの（カプセル化されていない）状態で RP に着信すると、RP はデバイス A に register-stop メッセージを送信します。
6. デフォルトでは、デバイスCは、最初のデータパケットを受信した時点で、送信元にjoinメッセージを送信します。
7. デバイスCが（S, G）でデータを受信すると、デバイスCは共有ツリーの上位方向にある送信元に prune メッセージを送信します。
8. RP が（S, G）の発信インターフェイスからデバイス C へのリンクを削除します。
9. RP が送信元への prune メッセージをトリガーします。

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

リバース パス転送

リバース パス転送は、マルチキャスト データグラムの転送に使用されます。 これは、次のように機能します。

- デバイスで送信元へのユニキャストパケットの送信に使用しているインターフェイスでデータグラムを受信すると、パケットは RPF インターフェイスに着信しています。
- パケットが RPF インターフェイスに着信した場合、デバイスは、マルチキャスト ルーティング テーブルエントリの発信インターフェイス リストに存在するインターフェイスにパケットを転送します。
- パケットがRPFインターフェイスに着信しない場合、パケットはループを回避するためにサイレントにドロップされています。

PIM では、送信元ツリーと RP をルートとする共有ツリーの両方を使用してデータグラムを転送します。RPF チェックは、次のようにそれぞれ異なる方法で実行されます。

- PIM デバイスが送信元ツリー ステートである場合（つまり、（S, G）エントリがマルチキャスト ルーティング テーブル内にある場合）、マルチキャスト パケットの送信元の IPv6 アドレスに対して RPF チェックが実行されます。
- PIM デバイスが共有ツリー ステートである場合（および送信元ツリー ステートが明示されていない場合）、（メンバがグループに加入している場合は既知である）RP のアドレスに対して RPF チェックが実行されます。

空間モード PIM では、RPF ルックアップ機能を使用して、join および prune の送信先を決定します。（S, G）join（送信元ツリー ステート）は送信元に向けて送信されます。（*, G）join（共有ツリー ステート）は RP に向けて送信されます。

IPv6 マルチキャスト PIM スパース モードの設定方法

IPv6 マルチキャスト ルーティングのイネーブル化

IPv6 マルチキャストは、MLD バージョン 2 を使用します。 このバージョンの MLD には、MLD バージョン 1 との完全な下位互換性があります（*RFC 2710* で規定）。 MLD バージョン 1 だけをサポートするホストは、MLD バージョン 2 を実行しているデバイスと相互運用します。 MLD バージョン 1 ホストと MLD バージョン 2 ホストの両方が混在する LAN もサポートされています。

はじめる前に

最初に、IPv6 マルチキャスト ルーティングをイネーブルにするデバイスのすべてのインターフェイスで、IPv6 ユニキャスト ルーティングをイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 multicast-routing** [**vrf** *vrf-name*]

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 multicast-routing** [**vrf** *vrf-name*] 例： `Device(config)# ipv6 multicast-routing`	すべての IPv6 対応インターフェイスでマルチキャスト ルーティングをイネーブルにし、イネーブルになっているすべてのデバイス インターフェイスで PIM および MLD に対してマルチキャスト転送をイネーブルにします。 • IPv6 マルチキャスト ルーティングは、IPv6 ユニキャスト ルーティングがイネーブルの場合、デフォルトでディセーブルです。 特定のデバイスでは、IPv6 ユニキャスト ルーティングを使用するには、IPv6 マルチキャスト ルーティングもイネーブルにする必要があります。

PIM-SM の設定およびグループ範囲の PIM-SM 情報の表示

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] [**bidir**]
4. **end**
5. **show ipv6 pim** [**vrf** *vrf-name*] **interface** [**state-on**] [**state-off**] [*type number*]
6. **show ipv6 pim** [**vrf** *vrf-name*] **group-map** [*group-name* | *group-address*] | [*group-range* | *group-mask*] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}]
7. **show ipv6 pim** [**vrf** *vrf-name*] **neighbor** [**detail**] [*interface-type interface-number* | **count**]
8. **show ipv6 pim** [**vrf** *vrf-name*] **range-list**[**config**] [*rp-address* | *rp-name*]
9. **show ipv6 pim** [**vrf** *vrf-name*] **tunnel** [*interface-type interface-number*]
10. **debug ipv6 pim** [*group-name* | *group-address* | **interface** *interface-type* | **bsr** | **group** | **mvpn** | **neighbor**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] [**bidir**] 例： `Device(config)# ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C acc-grp-1`	特定のグループ範囲の PIM RP のアドレスを設定します。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 pim** [**vrf** *vrf-name*] **interface** [**state-on**] [**state-off**] [*type number*] 例： `Device# show ipv6 pim interface`	PIM に対して設定されたインターフェイスに関する情報を表示します。
ステップ 6	**show ipv6 pim** [**vrf** *vrf-name*] **group-map** [*group-name* | *group-address*] | [*group-range* | *group-mask*] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}] 例： `Device# show ipv6 pim group-map`	IPv6 マルチキャスト グループ マッピング テーブルを表示します。
ステップ 7	**show ipv6 pim** [**vrf** *vrf-name*] **neighbor** [**detail**] [*interface-type interface-number* | **count**] 例： `Device# show ipv6 pim neighbor`	Cisco IOS ソフトウェアで検出された PIM ネイバーを表示します。

	コマンドまたはアクション	目的
ステップ 8	**show ipv6 pim** [**vrf** *vrf-name*] **range-list**[**config**] [*rp-address* | *rp-name*] 例： `Device# show ipv6 pim range-list`	IPv6 マルチキャスト範囲リストに関する情報を表示します。
ステップ 9	**show ipv6 pim** [**vrf** *vrf-name*] **tunnel** [*interface-type interface-number*] 例： `Device# show ipv6 pim tunnel`	インターフェイス上の PIM レジスタのカプセル化およびカプセル化解除トンネルに関する情報を表示します。
ステップ 10	**debug ipv6 pim** [*group-name* | *group-address* | **interface** *interface-type* | **bsr** | **group** | **mvpn** | **neighbor**] 例： `Device# debug ipv6 pim`	PIM プロトコルアクティビティに対するデバッグをイネーブルにします。

PIM オプションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **spt-threshold infinity** [**group-list** *access-list-name*]
4. **ipv6 pim** [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}
5. **interface** *type number*
6. **ipv6 pim dr-priority** *value*
7. **ipv6 pim hello-interval** *seconds*
8. **ipv6 pim join-prune-interval** *seconds*
9. **exit**
10. **show ipv6 pim** [**vrf** *vrf-name*] **join-prune statistic** [*interface-type*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 pim** [**vrf** *vrf-name*] **spt-threshold infinity** [**group-list** *access-list-name*] 例： `Device(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1`	PIM リーフ デバイスが指定したグループの SPT に加入するタイミングを設定します。
ステップ 4	**ipv6 pim** [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*} 例： `Device(config)# ipv6 pim accept-register route-map reg-filter`	RP のレジスタを許可または拒否します。
ステップ 5	**interface** *type number* 例： `Device(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 6	**ipv6 pim dr-priority** *value* 例： `Device(config-if)# ipv6 pim dr-priority 3`	PIM デバイスの DR プライオリティを設定します。
ステップ 7	**ipv6 pim hello-interval** *seconds* 例： `Device(config-if)# ipv6 pim hello-interval 45`	インターフェイスにおける PIM hello メッセージの頻度を設定します。

	コマンドまたはアクション	目的
ステップ 8	**ipv6 pim join-prune-interval** *seconds* 例： `Device(config-if)# ipv6 pim join-prune-interval 75`	指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。
ステップ 9	**exit** 例： `Device(config-if)# exit`	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 10	**show ipv6 pim** [**vrf** *vrf-name*] **join-prune statistic** [*interface-type*] 例： `Device# show ipv6 pim join-prune statistic`	各インターフェイスの最後の集約パケットに関する平均 join-prune 集約を表示します。

PIM トラフィック カウンタのリセット

PIM が誤動作する場合、または予想される PIM パケット数が送受信されていることを確認するために、PIM トラフィック カウンタをクリアします。 トラフィック カウンタがクリアされると、PIM が正しく動作していること、および PIM パケットが正しく送受信されていることを確認できます。

手順の概要

1. **enable**
2. **clear ipv6 pim** [**vrf** *vrf-name*] **traffic**
3. **show ipv6 pim** [**vrf** *vrf-name*] **traffic**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**clear ipv6 pim** [**vrf** *vrf-name*] **traffic** 例： `Device# clear ipv6 pim traffic`	PIM トラフィック カウンタをリセットします。
ステップ 3	**show ipv6 pim** [**vrf** *vrf-name*] **traffic** 例： `Device# show ipv6 pim traffic`	PIM トラフィック カウンタを表示します。

指定したインターフェイスでの IPv6 PIM のオフ

特定のインターフェイスだけで IPv6 マルチキャストを実行する必要がある場合、指定したインターフェイスで PIM をオフにすることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ipv6 pim**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* 例： `Device(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**no ipv6 pim** 例： `Device(config-if)# no ipv6 pim`	指定したインターフェイスで IPv6 PIM をオフにします。

IPv6 マルチキャスト PIM スパース モードの設定例

例：IPv6 マルチキャスト ルーティングのイネーブル化

次に、すべてのインターフェイスでマルチキャスト ルーティングをイネーブルにし、イネーブルになっているすべてのデバイス インターフェイスで PIM および MLD に対してマルチキャスト転送をイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 multicast-routing
```

例：PIM の設定

次に、2001:DB8::1 を RP として使用して、PIM-SM を使用するようにデバイスを設定する例を示します。 ここでは、SPT しきい値を infinity（無制限）に設定して、送信元がトラフィックの送信を開始したときに送信元ツリーへの切り替えが起こらないようにしています。また、ローカル マルチキャスト BGP プレフィックスを持たないすべての送信元でフィルタを設定しています。

```
Device(config)# ipv6 multicast-routing
Device(config)# ipv6 pim rp-address 2001:DB8::1
Device(config)# ipv6 pim spt-threshold infinity
Device(config)# ipv6 pim accept-register route-map reg-filter
```

例：IPv6 PIM トポロジ情報の表示

```
Device# show ipv6 pim topology

IP PIM Multicast Topology Table
Entry state:(*/S,G)[RPT/SPT] Protocol Uptime Info
```

```
Entry flags:KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state:Name, Uptime, Fwd, Info
Interface flags:LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,FF05::1)
SM UP:02:26:56 JP:Join(now) Flags:LH
RP:2001:DB8:1:1:2
RPF:Ethernet1/1,FE81::1
  Ethernet0/1          02:26:56  fwd LI LH

(2001:DB8:1:1:200,FF05::1)
SM UP:00:00:07 JP:Null(never) Flags:
RPF:Ethernet1/1,FE80::30:1:4
  Ethernet1/1          00:00:07  off LI
```

例：グループ範囲の PIM-SM 情報の表示

次に、PIM に対して設定されたインターフェイスに関する情報を表示する例を示します。

```
Device# show ipv6 pim interface state-on

Interface          PIM  Nbr   Hello  DR
                        Count Intvl  Prior

Ethernet0          on   0     30     1
    Address:FE80::208:20FF:FE08:D7FF
    DR     :this system
POS1/0             on   0     30     1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
POS4/0             on   1     30   1
    Address:FE80::208:20FF:FE08:D554
    DR     :FE80::250:E2FF:FE8B:4C80
POS4/1             on   0     30   1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
Loopback0          on   0     30     1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
```

次に、IPv6 マルチキャスト グループ マッピング テーブルを表示する例を示します。

```
Device# show ipv6 pim group-map

FF33::/32*
      SSM
      Info source:Static
      Uptime:00:08:32, Groups:0
  FF34::/32*
      SSM
      Info source:Static
      Uptime:00:09:42, Groups:0
```

次に、IPv6 マルチキャスト範囲リストに関する情報を表示する例を示します。

```
Device# show ipv6 pim range-list

config SSM Exp:never Learnt from :::
 FF33::/32 Up:00:26:33
 FF34::/32 Up:00:26:33
 FF35::/32 Up:00:26:33
 FF36::/32 Up:00:26:33
 FF37::/32 Up:00:26:33
 FF38::/32 Up:00:26:33
 FF39::/32 Up:00:26:33
 FF3A::/32 Up:00:26:33
```

```
 FF3B::/32 Up:00:26:33
 FF3C::/32 Up:00:26:33
 FF3D::/32 Up:00:26:33
 FF3E::/32 Up:00:26:33
 FF3F::/32 Up:00:26:33
config SM RP:40::1:1:1 Exp:never Learnt from :::
 FF13::/64 Up:00:03:50
config SM RP:40::1:1:3 Exp:never Learnt from :::
 FF09::/64 Up:00:03:50
```

例：PIM オプションの設定

次に、イーサネットインターフェイス 0/0 で DR プライオリティ、PIM hello 間隔、および join/prune の定期的な通知間隔を設定する例を示します。

```
Device(config)# interface Ethernet0/0
Device(config)# ipv6 pim hello-interval 60
Device(config)# ipv6 pim dr-priority 3
```

例：PIM トラフィック情報の表示

```
Device# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared:00:05:29

                              Received     Sent
Valid PIM Packets               22          22
Hello                           22          22
Join-Prune                      0           0
Register                        0           0
Register Stop                   0           0
Assert                          0           0
Bidir DF Election               0           0

Errors:
Malformed Packets                           0
Bad Checksums                               0
Send Errors                                 0
Packet Sent on Loopback Errors              0
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 用 RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 マルチキャスト PIM スパース モードに関する機能情報

表 *16*：*IPv6* マルチキャストに関する機能情報：*PIM* スパース モード

機能名	リリース	機能情報
IPv6 マルチキャスト：PIM Accept Register	12.0(26)S 12.3(4)T 12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.4 12.4(2)T Cisco IOS XE Release 2.1 15.0(1)S	PIM accept register は、RP で PIM-SM register メッセージのフィルタリングを実行するための機能です。 **ipv6 pim accept-register** コマンドが導入または変更されました。
IPv6マルチキャスト：PIM組み込み RP サポート	12.3(4)T 12.4 12.2(40)SG 15.0(2)SG 12.2(33)SRA 12.2(33)SXH	組み込み RP サポートを利用すると、ルータは、スタティックに設定されている RP の代わりに、マルチキャスト グループ宛先アドレスを使用して RP 情報を学習できるようになります。 次のコマンドが導入または変更されました。**ipv6 pim**、**ipv6 pim rp embedded**。

機能名	リリース	機能情報
IPv6 マルチキャスト：PIM スパース モード	12.0(26)S 12.2(18)S 12.2(25)SG 12.2(33)SRA 12.3(2)T 12.4 12.4(2)T Cisco IOS XE Release 2.4 15.0(1)S	PIM-SM は、ユニキャスト ルーティングを使用して、マルチキャスト ツリー構築用のリバース パス情報を提供します。PIM-SM は、トラフィックに対して明示的な要求がある場合を除いて、各マルチキャストに関与しているルータの数が比較的少なく、これらのルータがグループのマルチキャスト パケットを転送しないときに、マルチキャスト ネットワークで使用されます。 次のコマンドが導入または変更されました。**clear ipv6 pim topology**、**debug ipv6 pim**、**debug ipv6 pim neighbor**、**ipv6 pim**、**ipv6 pim dr-priority**、**ipv6 pim hello-interval**、**ipv6 pim rp-address**、**ipv6 pim spt-threshold infinity**、**show ipv6 mroute**、**show ipv6 pim group-map**、**show ipv6 pim interface**、**show ipv6 pim neighbor**、**show ipv6 pim range-list**、**show ipv6 pim topology**、**show ipv6 pim tunnel**。

第 13 章

IPv6 マルチキャスト：IPv6 のスタティック マルチキャスト ルーティング

IPv6 スタティック マルチキャスト ルート、つまり、mroute は、IPv6 スタティック ルートと同じデータベースを共有し、リバース パス転送（RPF）チェックに対するスタティック ルート サポートを拡張することによって実装されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

IPv6 スタティック mroute について

IPv6 スタティック mroute は、RPF チェックを変化させるために使用する IPv4 スタティック mroute とほぼ同様に動作します。 IPv6 スタティック mroute は、IPv6 スタティック ルートと同じデータベースを共有し、RPF チェックに対するスタティック ルート サポートを拡張することによって実装されます。 スタティック mroute では、等コスト マルチパス mroute がサポートされています。また、ユニキャスト専用スタティック ルートもサポートされています。

IPv6 スタティック マルチキャスト ルートの設定方法

スタティック mroute の設定

IPv6 のスタティック マルチキャスト ルート（mroute）は、IPv6 スタティック ルートの拡張として実装できます。デバイスを設定する際には、ユニキャストルーティング専用としてスタティック ルートを使用するか、マルチキャスト RPF 選択専用としてスタティック マルチキャスト ルートを使用するか、またはユニキャストルーティングとマルチキャストRPF選択の両方にスタティック ルートを使用するように設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 route** *ipv6-prefix / prefix-length ipv6-address* | *interface-type interface-number ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast**| **multicast**] [**tag** *tag*
4. **end**
5. **show ipv6 mroute** [**vrf** *vrf-name*] [**link-local** | [*group-name* | *group-address* [*source-address* | *source-name*]] [**summary**] [**count**]
6. **show ipv6 mroute** [**vrf** *vrf-name*] [**link-local** | *group-name* | *group-address*] **active**[*kbps*]
7. **show ipv6 rpf** [**vrf** *vrf-name*] *ipv6-prefix*

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 route** *ipv6-prefix / prefix-length ipv6-address* | *interface-type interface-number ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast**| **multicast**] [**tag** *tag* 例： `Device(config)# ipv6 route 2001:DB8::/64 6::6 100`	スタティック IPv6 ルートを確立します。 この例は、ユニキャスト ルーティングとマルチキャスト RPF 選択の両方に使用されるスタティック ルートを示しています。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 mroute** [**vrf** *vrf-name*] [**link-local** | [*group-name* | *group-address* [*source-address* | *source-name*]] [**summary**] [**count**] 例： `Device# show ipv6 mroute ff07::1`	IPv6 マルチキャスト ルーティング テーブルの内容を表示します。
ステップ 6	**show ipv6 mroute** [**vrf** *vrf-name*] [**link-local** | *group-name* | *group-address*] **active**[*kbps*] 例： `Device# show ipv6 mroute active`	デバイス上のアクティブなマルチキャスト ストリームを表示します。
ステップ 7	**show ipv6 rpf** [**vrf** *vrf-name*] *ipv6-prefix* 例： `Device# show ipv6 rpf 2001:DB8::1:1:2`	特定のユニキャスト ホスト アドレスおよびプレフィックスの RPF 情報を確認します。

IPv6 スタティック マルチキャスト ルートの設定例

例：スタティック mroute の設定

show ipv6 mroute コマンドを使用すると、マルチキャスト IPv6 データが流れていることを確認することができます。

```
Device# show ipv6 mroute ff07::1

Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State

(*, FF07::1), 00:04:45/00:02:47, RP 2001:DB8:6::6, flags:S
  Incoming interface:Tunnel5
  RPF nbr:6:6:6::6
  Outgoing interface list:
    POS4/0, Forward, 00:04:45/00:02:47

(2001:DB8:999::99, FF07::1), 00:02:06/00:01:23, flags:SFT
  Incoming interface:POS1/0
  RPF nbr:2001:DB8:999::99
  Outgoing interface list:
    POS4/0, Forward, 00:02:06/00:03:27
```

次に、**show ipv6 mroute active** コマンドの出力例を示します。

```
Device# show ipv6 mroute active

Active IPv6 Multicast Sources - sending >= 4 kbps
Group:FF05::1
 Source:2001:DB8:1:1:1
   Rate:11 pps/8 kbps(1sec), 8 kbps(last 8 sec)
```

次に、IPv6 アドレスが 2001:DB8:1:1:2 のユニキャスト ホストの RPF 情報を表示する例を示します。

```
Device# show ipv6 rpf 2001:DB8:1:1:2

RPF information for 2001:DB8:1:1:2
  RPF interface:Ethernet3/2
  RPF neighbor:FE80::40:1:3
  RPF route/mask:20::/64
  RPF type:Unicast
  RPF recursion count:0
  Metric preference:110
  Metric:30
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 用 RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 マルチキャストの機能情報：IPv6 のスタティック マルチキャスト ルーティング

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *17*：*IPv6* マルチキャストの機能情報：*IPv6* のスタティック マルチキャスト ルーティング

機能名	リリース	機能情報
IPv6 マルチキャスト：IPv6 のスタティック マルチキャスト ルーティング（mroute）	12.0(26)S 12.3(4)T 12.2(25)S 12.2(33)SRA 12.2(33)SXH 12.4 12.4(2)T Cisco IOS XE Release 2.4 15.0(1)S	IPv6 スタティック mroute は、IPv6 スタティック ルートと同じデータベースを共有し、スタティック ルート サポートを拡張することによって実装されます。 次のコマンドが導入または変更されました。**ipv6 route**、**show ipv6 mroute**、**show ipv6 mroute active**、**show ipv6 rpf**。

第 14 章

IPv6 マルチキャスト：PIM Source-Specific Multicast

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

IPv6 マルチキャストの前提条件：PIM Source-Specific Multicast

- Source Specific Multicast（SSM）を動作させるには、マルチキャスト リスナー検出（MLD）バージョン 2 が必要です。
- MLD を使用して SSM を動作させるには、Cisco IPv6 デバイス、アプリケーションが実行されているホスト、およびアプリケーション自体で SSM がサポートされている必要があります。

IPv6 マルチキャストについて：PIM Source-Specific Multicast

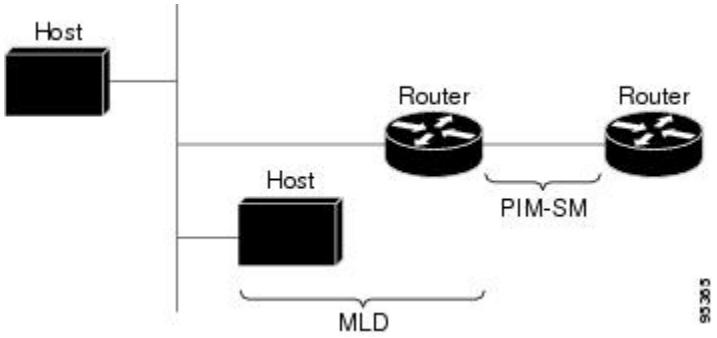
IPv6 マルチキャスト ルーティングの実装

Cisco ソフトウェアでは、IPv6 マルチキャスト ルーティングを実装するため、次のプロトコルがサポートされています。

- MLD は、直接接続されているリンク上のマルチキャスト リスナー（特定のマルチキャスト アドレスを宛先としたマルチキャスト パケットを受信するために使用するノード）を検出するために IPv6 デバイスで使用されます。 MLD には 2 つのバージョンがあります。
  - MLD バージョン 1 は、バージョン 2 の Internet Group Management Protocol（IGMP）for IPv4 をベースとしています。
  - MLD バージョン 2 は、バージョン 3 の IGMP for IPv4 をベースとしています。
- Cisco ソフトウェアの IPv6 マルチキャストでは、MLD バージョン 2 と MLD バージョン 1 の両方が使用されます。 MLD バージョン 2 は、MLD バージョン 1 と完全な下位互換性があります（RFC 2710 で規定）。 MLD バージョン 1 だけをサポートするホストは、MLD バージョン 2 を実行しているデバイスと相互運用します。 MLD バージョン 1 ホストと MLD バージョン 2 ホストの両方が混在する LAN もサポートされています。
- PIM-SM は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにデバイス間で使用されます。
- PIM in Source Specific Multicast（PIM-SSM）は PIM-SM と類似していますが、IP マルチキャスト アドレスを宛先とした特定の送信元アドレス（または特定の送信元アドレスを除くすべてのアドレス）からのパケットを受信する対象をレポートする機能を別途備えています。

下の図に、MLD と PIM-SM が IPv6 マルチキャスト環境で動作する場所を示します。

図 *18*：*IPv6* でサポートされている *IPv6* マルチキャスト ルーティング プロトコル



プロトコル独立マルチキャスト

プロトコル独立マルチキャスト（PIM）は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにデバイス間で使用されます。 PIM は、ユニキャスト ルーティング プロトコルとは独立して動作し、他のプロトコルと同様に、マルチキャスト ルート アップデートの送受信を実行します。ユニキャスト ルーティング テーブルに値を入力するために LAN でどのユニキャスト ルーティング プロトコルが使用されているかどうかにかかわらず、Cisco IOS PIM では、独自のルーティング テーブルを構築および管理する代わりに、既存のユニキャスト テーブル コンテンツを使用して、リバース パス転送（RPF）チェックを実行します。

PIM スパース モード（SM）または PIM 送信元固有マルチキャスト（SSM）動作のいずれかを使用するように IPv6 マルチキャストを設定することも、ネットワークで PIM-SM と PIM-SSM の両方を使用することもできます。

PIM 送信元固有マルチキャスト

PIM-SSM は、SSM の実装をサポートするルーティング プロトコルであり、PIM-SM から派生したものです。 ただし、PIM-SM では PIM join を受けてすべてのマルチキャスト送信元からデータが送信されるのに対し、SSM 機能では、受信側が明示的に加入しているマルチキャスト送信元だけからその受信側にデータグラム トラフィックが転送されます。これにより、帯域利用率が最適化され、不要なインターネット ブロードキャスト トラフィックが拒否されます。 さらに、SSM では、RP と共有ツリーを使用する代わりに、マルチキャスト グループの送信元アドレスで見つかった情報を使用します。 この情報は、MLD メンバーシップ レポートによってラストホップ デバイスにリレーされる送信元アドレスを通して受信側から提供されます。その結果として、送信元に直接つながる最短パス ツリーが得られます。

SSM では、データグラムは（S, G）チャネルに基づいて配信されます。 1 つの（S, G）チャネルのトラフィックは、IPv6 ユニキャスト送信元アドレス S とマルチキャスト グループ アドレス G を IPv6 宛先アドレスとして使用するデータグラムで構成されます。 システムは、（S, G）チャネルのメンバになることによって、このトラフィックを受信します。 シグナリングは不要ですが、

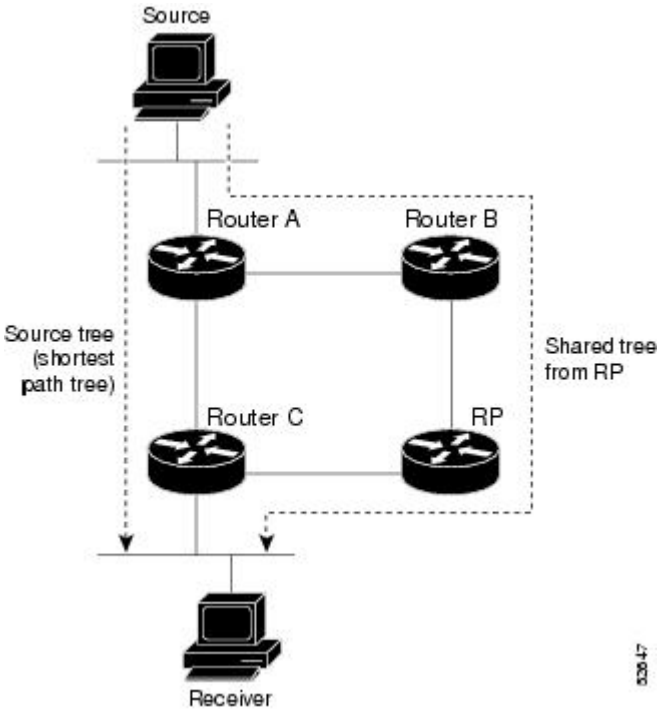
受信側は特定の送信元からのトラフィックを受信する場合は（S, G）チャネルに加入し、トラフィックを受信しない場合はチャネルから脱退する必要があります。

SSM を動作させるには、MLD バージョン 2 が必要です。 MLD を使用すると、ホストが送信元の情報を提供できるようになります。 MLD を使用して SSM を動作させるには、Cisco IPv6 デバイス、アプリケーションが実行されているホスト、およびアプリケーション自体でSSMがサポートされている必要があります。

PIM 共有ツリーおよび送信元ツリー（最短パス ツリー）

デフォルトでは、グループのメンバは、RP をルートとする単一のデータ配布ツリーを通じて、送信側からグループへのデータを受信します。 このタイプの配布ツリーは、共有ツリーまたはランデブー ポイント ツリー（RPT）と呼ばれます（下の図を参照）。 送信側からのデータは、RP に配信され、その共有ツリーに加入しているグループ メンバに配布されます。

図 *19*：共有ツリーおよび送信元ツリー（最短パス ツリー）



データしきい値で保証される場合、共有ツリー上のリーフ デバイスは、送信元をルートとするデータ配布ツリーへの切り替えを開始できます。 このタイプの配布ツリーは、最短パスツリーまたは送信元ツリーと呼ばれます。 デフォルトでは、ソフトウェアが送信元から最初のデータ パケットを受信すると、送信元ツリーに切り替わります。

次に、共有ツリーから送信元ツリーに切り替わるプロセスの詳細を示します。

1. 受信側がグループに加入します。リーフ デバイス C が RP に join メッセージを送信します。
2. RP がデバイス C へのリンクを発信インターフェイス リストに登録します。

3 送信元がデータを送信します。デバイス A が register にデータをカプセル化し、それを RP に送信します。

4 RP が共有ツリーの下位方向のデバイス C にデータを転送し、送信元に join メッセージを送信します。 この時点で、データはデバイス C に 2 回（カプセル化された状態で 1 回、ネイティブの状態で 1 回）着信する可能性があります。

5 データがネイティブの（カプセル化されていない）状態で RP に着信すると、RP はデバイス A に register-stop メッセージを送信します。

6 デフォルトでは、デバイス C は、最初のデータ パケットを受信した時点で、送信元に join メッセージを送信します。

7 デバイス C が（S, G）でデータを受信すると、デバイス C は共有ツリーの上位方向にある送信元に prune メッセージを送信します。

8 RP が（S, G）の発信インターフェイスからデバイス C へのリンクを削除します。

9 RP が送信元への prune メッセージをトリガーします。

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

リバース パス転送

リバース パス転送は、マルチキャスト データグラムの転送に使用されます。 これは、次のように機能します。

- デバイスで送信元へのユニキャスト パケットの送信に使用しているインターフェイスでデータグラムを受信すると、パケットは RPF インターフェイスに着信しています。
- パケットが RPF インターフェイスに着信した場合、デバイスは、マルチキャスト ルーティング テーブル エントリの発信インターフェイス リストに存在するインターフェイスにパケットを転送します。
- パケットが RPF インターフェイスに着信しない場合、パケットはループを回避するためにサイレントにドロップされています。

PIM では、送信元ツリーと RP をルートとする共有ツリーの両方を使用してデータグラムを転送します。RPF チェックは、次のようにそれぞれ異なる方法で実行されます。

- PIM デバイスが送信元ツリー ステートである場合（つまり、（S, G）エントリがマルチキャスト ルーティング テーブル内にある場合）、マルチキャスト パケットの送信元の IPv6 アドレスに対して RPF チェックが実行されます。
- PIM デバイスが共有ツリー ステートである場合（および送信元ツリー ステートが明示されていない場合）、（メンバがグループに加入している場合は既知である）RP のアドレスに対して RPF チェックが実行されます。

空間モード PIM では、RPF ルックアップ機能を使用して、join および prune の送信先を決定します。（S, G）join（送信元ツリー ステート）は送信元に向けて送信されます。（*, G）join（共有ツリー ステート）は RP に向けて送信されます。

IPv6 マルチキャストの設定方法：PIM Source-Specific Multicast

PIM オプションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **spt-threshold infinity** [**group-list** *access-list-name*]
4. **ipv6 pim** [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}
5. **interface** *type number*
6. **ipv6 pim dr-priority** *value*
7. **ipv6 pim hello-interval** *seconds*
8. **ipv6 pim join-prune-interval** *seconds*
9. **exit**
10. **show ipv6 pim** [**vrf** *vrf-name*] **join-prune statistic** [*interface-type*]

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ipv6 pim** [**vrf** *vrf-name*] **spt-threshold infinity** [**group-list** *access-list-name*] 例： `Device(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1`	PIM リーフ デバイスが指定したグループの SPT に加入するタイミングを設定します。
ステップ 4	**ipv6 pim** [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*} 例： `Device(config)# ipv6 pim accept-register route-map reg-filter`	RP のレジスタを許可または拒否します。
ステップ 5	**interface** *type number* 例： `Device(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 6	**ipv6 pim dr-priority** *value* 例： `Device(config-if)# ipv6 pim dr-priority 3`	PIM デバイスの DR プライオリティを設定します。
ステップ 7	**ipv6 pim hello-interval** *seconds* 例： `Device(config-if)# ipv6 pim hello-interval 45`	インターフェイスにおける PIM hello メッセージの頻度を設定します。
ステップ 8	**ipv6 pim join-prune-interval** *seconds* 例： `Device(config-if)# ipv6 pim join-prune-interval 75`	指定したインターフェイスに対して join および prune の定期的な通知間隔を設定します。
ステップ 9	**exit** 例： `Device(config-if)# exit`	このコマンドを 2 回入力して、インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**show ipv6 pim** [**vrf** *vrf-name*] **join-prune statistic** [*interface-type*] 例： `Device# show ipv6 pim join-prune statistic`	各インターフェイスの最後の集約パケットに関する平均 join-prune 集約を表示します。

PIM トラフィック カウンタのリセット

PIM が誤動作する場合、または予想される PIM パケット数が送受信されていることを確認するために、PIM トラフィック カウンタをクリアします。 トラフィック カウンタがクリアされると、PIM が正しく動作していること、および PIM パケットが正しく送受信されていることを確認できます。

手順の概要

1. **enable**
2. **clear ipv6 pim** [**vrf** *vrf-name*] **traffic**
3. **show ipv6 pim** [**vrf** *vrf-name*] **traffic**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear ipv6 pim** [**vrf** *vrf-name*] **traffic** 例： `Device# clear ipv6 pim traffic`	PIM トラフィック カウンタをリセットします。
ステップ 3	**show ipv6 pim** [**vrf** *vrf-name*] **traffic** 例： `Device# show ipv6 pim traffic`	PIM トラフィック カウンタを表示します。

PIM トポロジ テーブルをクリアすることによる MRIB 接続のリセット

MRIB を使用するのに設定は不要です。 ただし、特定の状況においては、ユーザは PIM トポロジ テーブルをクリアして MRIB 接続をリセットし、MRIB 情報を確認する必要がある場合があります。

手順の概要

1. **enable**
2. **clear ipv6 pim** [**vrf** *vrf-name*] **topology** [*group-name* | *group-address*]
3. **show ipv6 mrib** [**vrf** *vrf-name*] **client** [**filter**] [**name** {*client-name* | *client-name* **:** *client-id*}]
4. **show ipv6 mrib** [**vrf** *vrf-name*] **route** [**link-local**| **summary** | [*sourceaddress-or-name* | *****] [*groupname-or-address* [*prefix-length*]]]
5. **show ipv6 pim** [**vrf** *vrf-name*] **topology** [*groupname-or-address* [*sourcename-or-address*] | **link-local** | **route-count** [**detail**]]
6. **debug ipv6 mrib** [**vrf** *vrf-name*] **client**
7. **debug ipv6 mrib** [**vrf** *vrf-name*] **io**
8. **debug ipv6 mrib proxy**
9. **debug ipv6 mrib** [**vrf** *vrf-name*] **route** [*group-name* | *group-address*]
10. **debug ipv6 mrib** [**vrf** *vrf-name*] **table**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear ipv6 pim** [**vrf** *vrf-name*] **topology** [*group-name* | *group-address*] 例： `Device# clear ipv6 pim topology FF04::10`	PIM トポロジ テーブルをクリアします。
ステップ 3	**show ipv6 mrib** [**vrf** *vrf-name*] **client** [**filter**] [**name** {*client-name* | *client-name* **:** *client-id*}] 例： `Device# show ipv6 mrib client`	インターフェイスのマルチキャスト関連情報を表示します。

	コマンドまたはアクション	目的
ステップ 4	**show ipv6 mrib** [**vrf** *vrf-name*] **route** [**link-local**| **summary** | [*sourceaddress-or-name* | *****] [*groupname-or-address* [*prefix-length*]]] 例： `Device# show ipv6 mrib route`	MRIB ルート情報を表示します。
ステップ 5	**show ipv6 pim** [**vrf** *vrf-name*] **topology** [*groupname-or-address* [*sourcename-or-address*] | **link-local** | **route-count** [**detail**]] 例： `Device# show ipv6 pim topology`	特定のグループまたはすべてのグループの PIM トポロジ テーブル情報を表示します。
ステップ 6	**debug ipv6 mrib** [**vrf** *vrf-name*] **client** 例： `Device# debug ipv6 mrib client`	MRIB クライアント管理アクティビティに対するデバッグをイネーブルにします。
ステップ 7	**debug ipv6 mrib** [**vrf** *vrf-name*] **io** 例： `Device# debug ipv6 mrib io`	MRIB I/O イベントに対するデバッグをイネーブルにします。
ステップ 8	**debug ipv6 mrib proxy** 例： `Device# debug ipv6 mrib proxy`	分散型ルータ プラットフォームにおけるルート プロセッサとラインカード間の MRIB プロキシ アクティビティに対するデバッグをイネーブルにします。
ステップ 9	**debug ipv6 mrib** [**vrf** *vrf-name*] **route** [*group-name* | *group-address*] 例： `Device# debug ipv6 mrib route`	MRIB ルーティング エントリ関連のアクティビティに関する情報を表示します。
ステップ 10	**debug ipv6 mrib** [**vrf** *vrf-name*] **table** 例： `Device# debug ipv6 mrib table`	MRIB テーブル管理アクティビティに対するデバッグをイネーブルにします。

IPv6 マルチキャストの設定例：PIM Source-Specific Multicast

例：IPv6 PIM トポロジ情報の表示

```
Device# show ipv6 pim topology

IP PIM Multicast Topology Table
Entry state:(*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags:KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state:Name, Uptime, Fwd, Info
Interface flags:LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,FF05::1)
SM UP:02:26:56 JP:Join(now) Flags:LH
RP:2001:DB8:1:1:2
RPF:Ethernet1/1,FE81::1
  Ethernet0/1          02:26:56  fwd LI LH

(2001:DB8:1:1:200,FF05::1)
SM UP:00:00:07 JP:Null(never) Flags:
RPF:Ethernet1/1,FE80::30:1:4
  Ethernet1/1          00:00:07  off LI
```

例：Join/Prune 集約の設定

次に、イーサネット インターフェイス 0/0 で join/prune 集約を提供する例を示します。

```
Device# show ipv6 pim join-prune statistic Ethernet0/0

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface             Transmitted             Received
Ethernet0/0      0    / 0             1    / 0
```

例：PIM トラフィック情報の表示

```
Device# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared:00:05:29

                              Received     Sent
Valid PIM Packets               22          22
Hello                           22          22
Join-Prune                      0           0
Register                        0           0
Register Stop                   0           0
Assert                          0           0
Bidir DF Election               0           0

Errors:
Malformed Packets                           0
```

```
Bad Checksums                                 0
Send Errors                                   0
Packet Sent on Loopback Errors                0
Packets Received on PIM-disabled Interface    0
Packets Received with Unknown PIM Version     0
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 用 RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 マルチキャストの機能情報：PIM Source-Specific Multicast

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *18*：*IPv6* マルチキャストの機能情報：*PIM Source-Specific Multicast*

機能名	リリース	機能情報
IPv6 マルチキャスト：PIM Source-Specific Multicast	12.0(26)S 12.2(18)S 12.2(25)SG 12.2(33)SRA 12.3(2)T 12.4 12.4(2)T Cisco IOS XE Release 2.1 15.0(1)S	PIM-SSM は、PIM-SM から派生したものであり、SSM の実装をサポートしています。 SSM 機能では、受信側が明示的に加入しているマルチキャスト送信元だけからその受信側にデータグラム トラフィックが転送されます。これにより、帯域利用率が最適化され、不要なインターネット ブロードキャスト トラフィックが拒否されます。 次のコマンドが導入または変更されました。**clear ipv6 pim topology**、**debug ipv6 pim**、**debug ipv6 pim neighbor**、**ipv6 pim**、**ipv6 pim dr-priority**、**ipv6 pim hello-interval**、**ipv6 pim rp-address**、**ipv6 pim spt-threshold infinity**、**show ipv6 mroute**、**show ipv6 pim group-map**、**show ipv6 pim interface**、**show ipv6 pim neighbor**、**show ipv6 pim range-list**、**show ipv6 pim topology**、**show ipv6 pim tunnel**。

第 15 章

IPv6 Source Specific Multicast マッピング

IPv6 用の Source-specific multicast（SSM）マッピングでは、MLD バージョン 1 の受信側用にスタティックとダイナミックの両方のドメイン ネーム システム（DNS）マッピングがサポートされています。 この機能を使用すると、TCP/IP ホスト スタックおよび IP マルチキャスト受信アプリケーションで MLD バージョン 2 サポートを提供できないホストで IPv6 SSM を展開できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

IPv6 Source Specific Multicast マッピングについて

IPv6 用の SSM マッピングでは、MLD バージョン 1 の受信側用にスタティックとダイナミックの両方のドメイン ネーム システム（DNS）マッピングがサポートされています。 この機能を使用

すると、TCP/IP ホスト スタックおよび IP マルチキャスト受信アプリケーションで MLD バージョン 2 サポートを提供できないホストで IPv6 SSM を展開できます。

SSM マッピングにより、デバイスは実行コンフィギュレーションまたは DNS サーバのいずれかでマルチキャスト MLD バージョン 1 レポートの送信元を検索できるようになります。 その後、デバイスは送信元に対する（S, G）join を開始できます。

IPv6 Source Specific Multicast マルチキャスト マッピングの設定方法

IPv6 SSM の設定

SSM マッピング機能をイネーブルにすると、DNS ベースの SSM マッピングが自動的にイネーブルになります。つまり、デバイスは、マルチキャスト MLD バージョン 1 レポートの送信元を DNS サーバから検索するようになります。

デバイス設定に応じて、DNS ベースのマッピングまたはスタティック SSM マッピングのいずれかを設定できます。 スタティック SSM マッピングを使用する場合は、複数のスタティック SSM マッピングを設定できます。 複数のスタティック SSM マッピングを設定すると、一致するすべてのアクセス リストの送信元アドレスが使用されるようになります。

はじめる前に

（注） DNS ベースの SSM マッピングを使用するには、デバイスは正しく設定されている DNS サーバを少なくとも 1 つ見つける必要があります。デバイスは、その DNS サーバに直接接続される可能性があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 mld** [**vrf** *vrf-name*] **ssm-map enable**
4. **no ipv6 mld** [**vrf** *vrf-name*] **ssm-map query dns**
5. **ipv6 mld** [**vrf** *vrf-name*] **ssm-map static** *access-list source-address*
6. **end**
7. **show ipv6 mld** [**vrf** *vrf-name*] **ssm-map** [*source-address*]

手順の詳細

ステップ 1　**enable**

例：

```
Device> enable
```

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **ipv6 mld** [**vrf** *vrf-name*] **ssm-map enable**

例：

```
Device(config)# ipv6 mld ssm-map enable
```

設定済みの SSM 範囲内のグループに対して SSM マッピング機能をイネーブルにします。

ステップ 4 **no ipv6 mld** [**vrf** *vrf-name*] **ssm-map query dns**

例：

```
Device(config)# no ipv6 mld ssm-map query dns
```

DNS ベースの SSM マッピングをディセーブルにします。

ステップ 5 **ipv6 mld** [**vrf** *vrf-name*] **ssm-map static** *access-list source-address*

例：

```
Device(config)# ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1
```

スタティック SSM マッピングを設定します。

ステップ 6 **end**

例：

```
Device(config-if)# end
```

特権 EXEC モードに戻ります。

ステップ 7 **show ipv6 mld** [**vrf** *vrf-name*] **ssm-map** [*source-address*]

例：

```
Device# show ipv6 mld ssm-map
```

SSM マッピング情報を表示します。

IPv6 Source Specific Multicast マッピングの設定例

例：IPv6 SSM マッピング

```
Device# show ipv6 mld ssm-map 2001:DB8::1

 Group address  : 2001:DB8::1
 Group mode ssm : TRUE
 Database       : STATIC
 Source list    : 2001:DB8::2
                  2001:DB8::3

Device# show ipv6 mld ssm-map 2001:DB8::2

 Group address  : 2001:DB8::2
 Group mode ssm : TRUE
 Database       : DNS
 Source list    : 2001:DB8::3
                  2001:DB8::1
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 用 RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 Source Specific Multicast マッピングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *19*：*IPv6 Source Specific Multicast* マッピングの機能情報

機能名	リリース	機能情報
IPv6 Source Specific Multicast マッピング	12.2(33)SRA 12.2(18)SXE 12.4(2)T Cisco IOS XE Release 2.1 15.0(1)S	この機能を使用すると、TCP/IP ホスト スタックおよび IP マルチキャスト受信アプリケーションで MLD バージョン 2 サポートを提供できないホストで IPv6 SSM を展開できます。 次のコマンドが導入または変更されました。**ipv6 mld ssm-map enable**、**ipv6 mld ssm-map query dns**、**ipv6 mld ssm-map static**、**show ipv6 mld ssm-map**。

第 16 章

IPv6 マルチキャスト：受信側の明示的トラッキング

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

IPv6 マルチキャスト受信側の明示的トラッキングについて

受信側の明示的トラッキング

明示的トラッキング機能を使用すると、デバイスがIPv6ネットワーク内のホストの動作を追跡できるようになります。 また、この機能により、高速脱退メカニズムをMLDバージョン2のホスト レポートで使用できるようになります。

IPv6 マルチキャスト受信側の明示的トラッキングの設定方法

受信側の明示的トラッキングによってホストの動作を追跡するための設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 mld explicit-tracking** *access-list-name*

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* 例： `Device(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6 mld explicit-tracking** *access-list-name* 例： `Device(config-if)# ipv6 mld explicit-tracking list1`	ホストの明示的トラッキングをイネーブルにします。

IPv6 マルチキャスト受信側の明示的トラッキングの設定例

例：受信側の明示的トラッキングの設定

```
Device> enable
Device# configure terminal
Device(config)# interface FastEthernet 1/0
Device(config-if)# ipv6 mld explicit-tracking list1
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』

関連項目	マニュアル タイトル
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 用 RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 マルチキャストに関する機能情報：受信側の明示的トラッキング

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *20*：*IPv6* マルチキャストに関する機能情報：受信側の明示的トラッキング

機能名	リリース	機能情報
IPv6 マルチキャスト：受信側の明示的トラッキング	12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.3(7)T 12.4 12.4(2)T Cisco IOS XE Release 2.1 15.0(1)S	この機能を使用すると、デバイスが IPv6 ネットワーク内のホストの動作を追跡できるようになります。 次のコマンドが導入されました。**ipv6 mld explicit-tracking**。

第 17 章

IPv6 双方向 PIM

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

IPv6 双方向 PIM の制約事項

ネットワークで双方向（bidir）範囲が使用されている場合は、そのネットワーク内のすべてのデバイスがブートストラップ メッセージ（BSM）内の双方向範囲を理解できる必要があります。

IPv6 双方向 PIM について

双方向 PIM

双方向 PIM により、マルチキャスト デバイスは、PIM-SM の単方向共有ツリーと比較して、保持するステート情報を減らすことができます。 双方向共有ツリーは、送信元から RPA にデータを伝送し、それらを RPA から受信側に配布します。 PIM-SM とは異なり、双方向 PIM は送信元ツリーへの切り替えは実行しません。また、送信元から RP へのデータの登録カプセル化は行われません。

指定された単一のフォワーダ（DF）が、双方向 PIM ドメイン内のすべてのリンク（マルチアクセスおよびポイントツーポイント リンクを含む）の各 RPA 用に存在しています。 唯一の例外は、DF が存在しない RPL です。 DF は、MRIB が提供するメトリックとの比較で決定される、RPA への最適なルートを持つリンク上のデバイスです。 指定された RPA の DF は、リンクにダウンストリーム トラフィックを転送し、リンクからのアップストリーム トラフィックをランデブー ポイント リンク（RPL）に転送します。 DF は、RPA にマップするすべての双方向グループに対してこの機能を実行します。 また、リンク上の DF は、リンク上のダウンストリーム デバイスからの Join メッセージを処理するとともに、MLD などのローカル メンバーシップ メカニズムによって検出されたローカル受信者にパケットが転送されることを保証します。

双方向 PIM は、中レートまたは低レートの送信元が多数存在する場合に役立ちます。 ただし、双方向共有ツリーの遅延特性は、PIM-SM で構築された送信元ツリーよりもさらに劣る可能性があります（トポロジに依存）。

IPv6 では、双方向 RP のスタティック設定だけがサポートされています。

IPv6 双方向 PIM の設定方法

双方向 PIM の設定および双方向 PIM 情報の表示

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] [**bidir**]
4. **exit**
5. **show ipv6 pim** [**vrf** *vrf-name*] **df** [*interface-type interface-number*] [*rp-address*]
6. **show ipv6 pim** [**vrf** *vrf-name*] **df winner**[*interface-type interface-number*] [*rp-address*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] [**bidir**] 例： `Device(config)# ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C bidir`	特定のグループ範囲の PIM RP のアドレスを設定します。**bidir** キーワードを使用すると、そのグループ範囲が双方向共有ツリー転送に使用されるようになります。
ステップ 4	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードを終了し、デバイスを特権 EXEC モードに戻します。
ステップ 5	**show ipv6 pim** [**vrf** *vrf-name*] **df** [*interface-type interface-number*] [*rp-address*] 例： `Device# show ipv6 pim df`	RP の各インターフェイスの Designated Forwarder（DF）選択ステートを表示します。
ステップ 6	**show ipv6 pim** [**vrf** *vrf-name*] **df winner**[*interface-type interface-number*] [*rp-address*] 例： `Device# show ipv6 pim df winner ethernet 1/0 200::1`	各 RP の各インターフェイスの DF 選択ウィナーを表示します。

IPv6 双方向 PIM の設定例

例：双方向 PIM の設定および双方向 PIM 情報の表示

次に、DF-election 状態を表示する例を示します。

```
Device# show ipv6 pim df

Interface          DF State     Timer         Metrics
Ethernet0/0        Winner       4s 8ms        [120/2]
    RP :200::1
Ethernet1/0        Lose         0s 0ms        [inf/inf]
    RP :200::1
```

次に、RP に関する情報を表示する例を示します。

```
Device# show ipv6 pim df

Interface          DF State     Timer         Metrics
Ethernet0/0        None:RP LAN 0s 0ms        [inf/inf]
    RP :200::1
Ethernet1/0        Winner       7s 600ms      [0/0]
    RP :200::1
Ethernet2/0        Winner       9s 8ms        [0/0]
    RP :200::1
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 用 RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 双方向 PIM に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *21*：*IPv6* 双方向 *PIM* に関する機能情報

機能名	リリース	機能情報
IPv6 双方向 PIM	12.2(25)SG 12.2(33)SRA 12.2(25)S 12.3(7)T 12.4 12.4(2)T Cisco IOS XE release 2.3 15.0(1)S	双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。 双方向共有ツリーは、送信元から RP にデータを伝送し、それらを RP から受信側に配布します。 次のコマンドが導入または変更されました。**debug ipv6 pim df-election**、**ipv6 pim rp-address**、**show ipv6 pim df**、**show ipv6 pim df winner**。

第 18 章

IPv6 PIM パッシブ モード

この機能を使用すると、PIMパッシブモードをインターフェイスでイネーブルにして、PIMパッシブ インターフェイスを、PIM 制御メッセージは送受信できないが、マルチキャスト ルート エントリのリバース パス転送（RPF）インターフェイスとして機能し、マルチキャスト データ パケットを受信して転送できるようにすることができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

IPv6 PIM パッシブ モードに関する情報

PIM を使用して設定されたデバイスは、LAN 上のいずれのネイバーからの PIM メッセージも受け取らないように設定されている場合にも、IPv6 マルチキャスト ルーティングが有効になっているすべてのインターフェイスに PIM hello メッセージを常に送信します。 IPv6 PIM パッシブ モード

機能を使用すると、PIM パッシブ モードをインターフェイスでイネーブルにして、PIM パッシブ インターフェイスを、PIM 制御メッセージは送受信できないが、マルチキャスト ルート エントリの RPF インターフェイスとして機能し、マルチキャスト データ パケットを受信して転送できるようにすることができます。

IPv6 PIM パッシブ モードの設定方法

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 multicast pim-passive-enable**
4. **interface** *type number*
5. **ipv6 pim passive**

手順の詳細

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **ipv6 multicast pim-passive-enable**

例：

```
Device(config)# ipv6 multicast pim-passive-enable
```

IPv6 デバイスの PIM パッシブ機能をイネーブルにします。

ステップ 4 **interface** *type number*

例：

```
Device(config)# interface GigabitEthernet 1/0/0
```

インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。

ステップ 5 **ipv6 pim passive**

例：

```
Device(config-if)# ipv6 pim passive
```

特定のインターフェイスの PIM パッシブ機能をイネーブルにします。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 用 RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 PIM パッシブの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *22* : *IPv6 PIM* パッシブの機能情報

機能名	リリース	機能情報
IPv6 PIM パッシブ	Cisco IOS XE Release 2.6	この機能を使用すると、PIM パッシブ モードをインターフェイスでイネーブルにして、PIM パッシブ インターフェイスを、PIM 制御メッセージは送受信できないが、マルチキャスト ルート エントリの RPF インターフェイスとして機能し、マルチキャスト データ パケットを受信して転送できるようにすることができます。 次のコマンドが導入または変更されました。**ipv6 multicast pim-passive-enable**、**ipv6 pim passive**、**show ipv6 pim interface**。

第 19 章

IPv6 マルチキャスト：ルーティング可能アドレスの hello オプション

ルーティング可能アドレスの hello オプションを使用すると、PIM hello メッセージがアドバタイズされるインターフェイス上のすべてのアドレスを含む PIM hello メッセージ オプションが追加されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、Bug Search Tool およびプラットフォームとソフトウェア リリースのリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

ルーティング可能アドレスの hello オプションについて

IPv6 内部ゲートウェイ プロトコルを使用してユニキャスト ルーティング テーブルを構築する場合、アップストリーム デバイス アドレスを検出するための手順では、PIM ネイバーとネクストホップ デバイスが同じルータを表している限り、これらのアドレスは常に同じであるものと想定されます。 ただし、デバイスがリンク上に複数のアドレスを持つ場合は、このことが当てはまるとは限りません。

この状況は IPv6 において、2 つの一般的な状況で発生することがあります。 1 つめの状況は、ユニキャスト ルーティング テーブルが IPv6 内部ゲートウェイ プロトコル（マルチキャスト BGP など）によって構築されない場合に発生します。 2 つめの状況は、RP のアドレスがダウンストリーム アドレスとサブネット プレフィックスを共有している場合に発生します（RP アドレスはドメインワイドにする必要があるため、リンクローカル アドレスにはできないことに注意してください）。

ルーティング可能アドレスの hello オプションによって、PIM プロトコルでこのような状況を回避できます。このためには、PIM hello メッセージがアドバタイズされるインターフェイス上のすべてのアドレスを含む PIM hello メッセージ オプションを追加します。 PIM デバイスが何らかのアドレスのアップストリーム デバイスを検出すると、RPF 計算の結果は、PIM ネイバーのアドレス自体に加えて、このオプションのアドレスとも比較されます。 このオプションにはそのリンク上の PIM デバイスの考えられるアドレスがすべて含まれているため、対象の PIM デバイスがこのオプションをサポートしている場合、常に RPF 計算の結果が含まれます。

PIM メッセージにサイズ制限があることと、ルーティング可能アドレスの hello オプションが単一の PIM hello メッセージ内に収まる必要があるため、インターフェイスで設定できるアドレスの制限は 16 個になっています。

IPv6 マルチキャストの設定方法：ルーティング可能アドレスの hello オプション

ルーティング可能アドレスの hello オプションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 pim hello-interval** *seconds*

手順の詳細

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **interface** *type number*

例：

```
Device(config)# interface FastEthernet 1/0
```

インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。

ステップ 4 **ipv6 pim hello-interval** *seconds*

例：

```
Device(config-if)# ipv6 pim hello-interval 45
```

インターフェイスにおける PIM hello メッセージの頻度を設定します。

ルーティング可能アドレスの hello オプションの設定例

次に、**show ipv6 pim neighbor** コマンドで **detail** キーワードを指定して、ルーティング可能アドレスのhelloオプションを通して学習されたネイバーの追加アドレスを識別する場合の出力例を示します。

```
Device# show ipv6 pim neighbor detail

Neighbor Address(es)       Interface     Uptime    Expires DR pri Bidir

FE80::A8BB:CCFF:FE00:401   Ethernet0/0   01:34:16  00:01:16 1      B
60::1:1:3

FE80::A8BB:CCFF:FE00:501   Ethernet0/0   01:34:15  00:01:18 1      B
60::1:1:4
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 のアドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 用 RFC	『*IPv6 RFCs*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 マルチキャストの機能情報：ルーティング可能アドレスの hello オプション

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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

表 *23*：*IPv6* マルチキャストの機能情報：ルーティング可能アドレスの *hello* オプション

機能名	リリース	機能情報
IPv6 マルチキャスト：ルーティング可能アドレスの hello オプション	12.0(26)S 12.3(4)T 12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.4 12.4(2)T Cisco IOS XE Release 2.4 15.0(1)S	ルーティング可能アドレスの hello オプションを使用すると、PIM hello メッセージがアドバタイズされるインターフェイス上のすべてのアドレスを含む PIM hello メッセージ オプションが追加されます。 次のコマンドが導入または変更されました。**ipv6 pim hello-interval**、**show ipv6 pim neighbor**。