



MSDP の設定

- [MSDP の前提条件](#) (1 ページ)
- [Multicast Source Discovery Protocol に関する情報](#) (1 ページ)
- [MSDP の設定方法](#) (10 ページ)
- [MSDP のモニタリングおよびメンテナンス](#) (31 ページ)
- [MSDP の設定例](#) (35 ページ)

MSDP の前提条件

MSDP を使用するには、Catalyst 3560-CX スイッチで IP サービス フィーチャセットをイネーブルにする必要があります。

Multicast Source Discovery Protocol に関する情報

MSDP は複数の PIM-SM ドメインを接続するメカニズムです。MSDP は、他の PIM ドメイン内のマルチキャスト送信元を検出することを目的としています。MSDP の主な利点は、(一般的な共有ツリーではなく) ドメイン間ソース ツリーを PIM-SM ドメインで使用できるようにし、複数の PIM-SM ドメインを相互接続する複雑性を軽減することです。MSDP がネットワークで設定されている場合、RP は他のドメイン内の RP と送信元情報を交換します。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。RP は、そのドメイン内の共有ツリーのルートであり、アクティブ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ため、これを行うことができます。PIM-SM ドメイン外の新しい送信元を (共有ツリーの送信元からのマルチキャストパケットの到着によって) ラストホップデバイスが認識すると、その送信元に加入要求を送信してドメイン間ソース ツリーに参加できます。

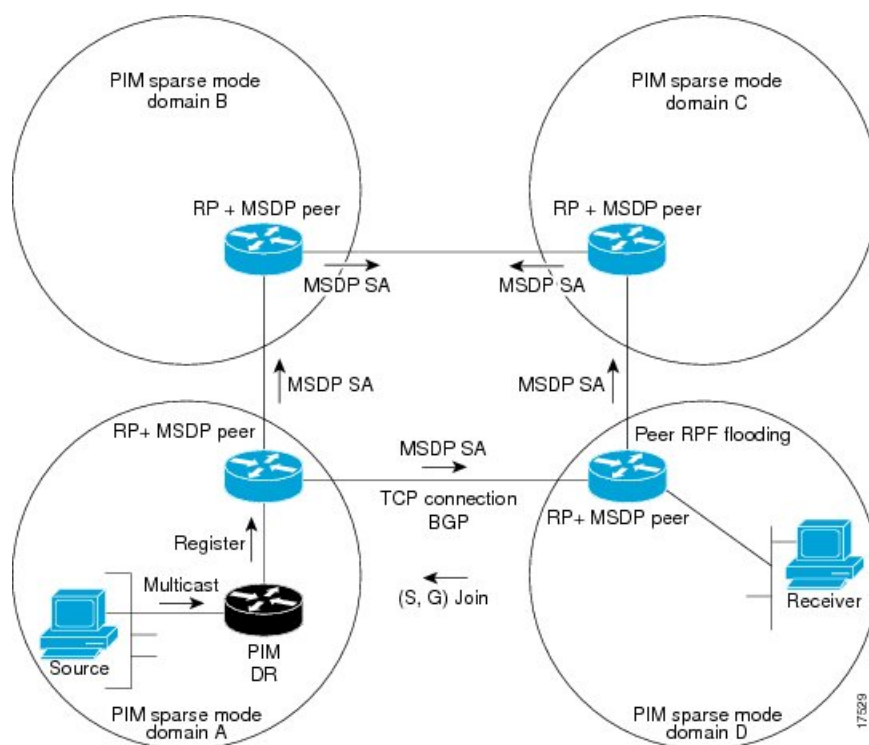


(注) RP に特定グループの共有ツリーがないか、発信インターフェイスリストがヌルの共有ツリーがある場合は、別のドメインの発信元に加入要求を送信しません。

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 対応デバイスとの 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ます。交換されるのは主にマルチキャストグループを送信する送信元のリストです。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場合は、各ピアを明示的に設定する必要があります。さらに、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。

図に、2 つの MSDP ピア間の MSDP の動作を示します。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 1: 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 指定デバイス (DR) が送信元を RP に登録すると、その RP が Source-Active (SA) メッセージをすべての MSDP ピアに送信します。



(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。これは、発信元 RP に登録されているすべての発信元を含んでいる定期的な SA メッセージの場合とは異なります。これらの SA メッセージは MSDP 制御パケットであるため、アクティブな送信元からのカプセル化されたデータを含んでいません。

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 PIM-SM ドメイン B および C 内の RP の場合など)、RP は複数の MSDP ピアからの 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、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、MBGP が最初に確認されてからユニキャスト BGP が確認されます。そのネクストホップ ネイバーが発信元の RPF ピアです。RPF ピアへのインターフェイス以外のインターフェイスにある発信元から受信した 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。
1. SA メッセージを受信した RP は、グループの (*, G) 送信インターフェイスリストにインターフェイスが存在するかどうかを確認することによって、そのドメイン内にアドバタイズされたグループのメンバが存在す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 (S, G) 加入要求を送信元に送信します。その結果、ドメイン間ソースツリーのブランチが自律システムの RP との境界に構築されます。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. 発信元 RP は、送信元がグループにパケットを送信し続ける限り、60 秒ごとに (S, G) ステートに関する SA メッセージを定期的送信し続けます。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、発信元 RP 10.5.4.3 から (172.16.5.4, 228.1.2.3) に対する SA メッセージを受信したとします。RP は mroute テーブルを確認し、グループ 228.1.2.3 にアクティブなメンバが存在しないことを検出すると、SA メッセージを 10.5.4.3 のダウンストリームにあるピアに渡します。次に、ドメイン内のホストが加入要求をグループ 228.1.2.3 の RP に送信した場合、その 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、デバイスは (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対象の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 の利点

MSDP には次の利点があります。

- 共有されたマルチキャスト配信ツリーが分割され、共有ツリーがドメインに対してローカルになるように設定できます。ローカルメンバーはローカルツリーに加入します。共有ツリーへの Join メッセージはドメインから脱退する必要はありません。
- PIM SM ドメインは独自の RP だけを信頼するため、他のドメインの RP に対する信頼度が低下します。このため、送信元の情報がドメイン外部に漏れないようにでき、セキュリティが高まります。
- レシーバーだけが配置されているドメインは、グループメンバーシップをグローバルにアドバタイズしなくても、データを受信できます。
- グローバルな送信元マルチキャストルーティングテーブルステートが不要になり、メモリが削減されます。

デフォルト MSDP ピア

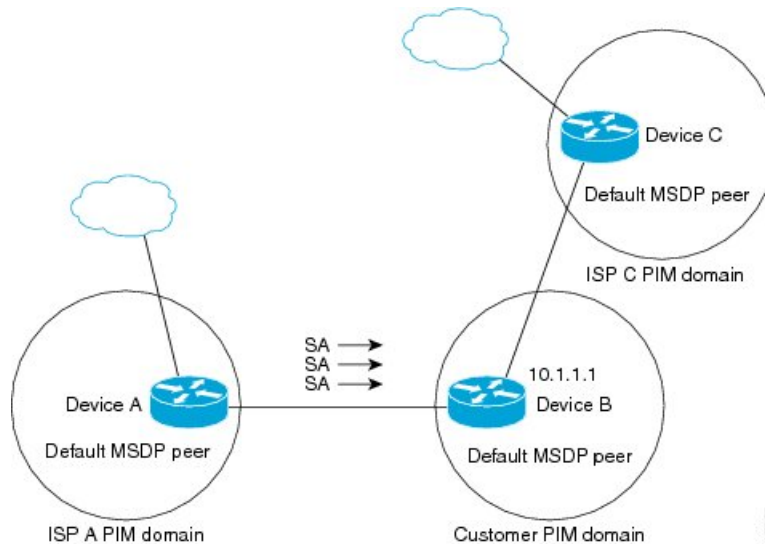
スタブ自律システムには、冗長性を実現するために複数の RP との MSDP ピアリングが必要な場合もあります。たとえば、RPF チェックメカニズムがないため、SA メッセージは複数のデフォルトピアから受け入れられません。その代わりに、SA メッセージは 1 つのピアからだけ受け入れられます。そのピアに障害が発生した場合、SA メッセージは別のピアから受け入れられます。もちろん、デフォルトのピアが両方とも同じ SA メッセージを送信することがこの基本的な前提となっています。

下の図に、デフォルトの MSDP ピアが使用されるシナリオを示します。この図では、デバイス 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 (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 はデバイス A を所有し、もう一方の ISP はデバイス C を所有しています。どちらもそれらの間で BGP も MBGP も実行していません。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、デバイス B はデバイス A をデフォルト MSDP ピアとして識別します。デバイス B はデバイス A とデバイス C の両方に SA メッセージをアドバタイズしますが、デバイス A だけまたはデバイス C だけから SA メッセージを受け入れます。デバイス A が設定内の最初のデフォルトピアである場合、デバイス A が稼働していればデバイス A が使用されます。デバイス A が稼働していない場合に限り、デバイス B がデバイス 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、カスタマーのデバイスから受け入れるプレフィックスを定義する場合があります。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 2: デフォルト MSDP ピアのシナリオ



デバイス B はデバイス A およびデバイス C に SA をアドバタイズしますが、デバイス A またはデバイス C だけを使用して SA メッセージを受け入れます。デバイス A が設定内の最初のデバイスである場合、デバイス A が稼働していればデバイス A が使用されます。デバイス A が稼働していない場合に限り、デバイス B がデバイス 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を使用しない動作です。

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（このピアにデバイスが接続されていて、ピアがアクティブの場合に限りです）。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ドが削減さ

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ドする必要はありません。

MSDP メッシュ グループの利点

- SA フラッドの最適化：グループ内に複数のピアがある場合、SA フラッド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 ピアにフラッドされません。
- 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。

SA メッセージでアドバタイズされるソースを制御するには、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 メッセージで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。この場合もデバイスは通常の方法で他の MSDP ピアからの SA メッセージを転送します。ローカルソースの SA メッセージは発信しません。
- 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（またはそれらの組み合わせ）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イネーブル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](#)」の項を参照してください。

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

- 指定した MSDP ピアへ転送したすべての発信 SA メッセージをフィルタリングするには、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します。
- 指定した MSDP ピアへ転送した発信 SA メッセージのサブセットを拡張アクセスリストに定義された (S,G) ペアに基づいてフィルタリングするには、拡張アクセスリストで許可されている (S,G) ペアに一致する MSDP ピアへの SA メッセージだけを転送するようにデバイスを設定します。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。
- 指定した MSDP へ転送した発信 SA メッセージのサブセットをルートマップに定義された一致基準に基づいてフィルタリングするには、ルートマップに定義された基準に一致する SA メッセージだけを転送するようにデバイスを設定します。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。
- 指定したピアからの発信 SA メッセージのサブセットを SA メッセージに含まれているアナウンス側 RP アドレスに基づいてフィルタリングするには、SA メッセージが1つ以上の MSDP ピアに送信されていても、それらの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します。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。この場合、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 リストを作成することによって、MSDP ピアからデバイスが受信する送信元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。

- 指定した 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するには、指定した 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します。
- 指定したピアからの着信 SA メッセージのサブセットを拡張アクセスリストに定義された (S,G) ペアに基づいてフィルタリングするには、拡張アクセスリストに定義された (S,G) ペアに一致する 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します。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。
- 指定したピアからの着信 SA 要求メッセージのサブセットをルートマップに定義された一致基準に基づいてフィルタリングするには、ルートマップに指定された基準に一致する SA メッセージだけを受信するようにデバイスを設定します。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。
- 指定したピアからの着信 SA メッセージのサブセットを拡張アクセスリストに定義された (S,G) ペアと、ルートマップに定義された基準の両方に基づいてフィルタリングするには、拡張アクセスリストに定義された (S,G) ペアと、ルートマップに定義された基準の両方に一致する着信 SA メッセージだけを受信するようにデバイスを設定します。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。
- 指定したピアからの着信 SA メッセージのサブセットを SA メッセージに含まれているアナウンス側 RP アドレスに基づいてフィルタリングするには、SA メッセージがすでに1つ以上の MSDP ピア全体に送信されている可能性がある場合でも、それらの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します。
- 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。この場合、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、したがってリモート 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。

MSDP メッセージタイプ

MSDP メッセージには4つの基本タイプがあり、それぞれが固有の Type、Length、および Value (TLV) データフォーマットでエンコードされています。

SA メッセージ

SA メッセージを使用して、ドメイン内のアクティブなソースをアドバタイズします。また、これらの SA メッセージには送信元によって送信された最初のマルチキャストデータパケットが含まれていることがあります。

SA メッセージには、発信元 RP の IP アドレスと、アドバタイズされる 1 つ以上の (S,G) ペアが含まれています。また、SA メッセージにカプセル化されたデータパケットが含まれていることがあります。

SA 要求メッセージ

SA 要求メッセージを使用して、特定のグループにアクティブなソースのリストを要求します。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。グループ内のすべてのアクティブなソースが発信元の RP によって再アドバタイズされるまで待つ代わりに、SA 要求メッセージを使用してアクティブなソースのリストを要求すると、加入遅延を短縮できます。

SA 応答メッセージ

SA 応答メッセージは SA 要求メッセージに回答する MSDP ピアによって送信されます。SA 応答メッセージには、発信元の RP の IP アドレスと、キャッシュに保存されている発信元 RP のドメイン内のアクティブなソースの 1 つ以上の (S, G) ペアが含まれています。

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 60 秒ごとに送信され、MSDP セッションをアクティブに保ちます。キープアライブメッセージまたは SA メッセージを 75 秒間受信しなかった場合、MSDP セッションがリセットされます。

MSDP のデフォルト設定

MSDP はイネーブルになっていません。デフォルトの MSDP ピアはありません。

MSDP の設定方法

デフォルトの MSDP ピアの設定

始める前に

MSDP ピアを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： スイッチ> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： スイッチ# 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 ip-address name [prefix-list list] 例：	すべての MSDP SA メッセージの受信元となるデフォルト ピアを定義します。

	コマンドまたはアクション	目的
	<pre>Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a</pre>	<ul style="list-style-type: none"> • <i>ip-address / name</i> には、MSDP デフォルト ピアの IP アドレスまたはドメイン ネーム システム (DNS) サーバー名を入力します。 • (任意) prefix-list list を指定する場合は、リスト内のプレフィックス専用のデフォルトピアとなるピアを指定するリスト名を入力します。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。 <p>prefix-list キーワードが指定された ip msdp default-peer コマンドを複数入力すると、複数の RP プレフィックスに対してすべてのデフォルトピアが同時に使用されます。この構文は通常、スタブ サイトクラウドに接続されたサーバ プロバイダクラウドで使用されます。</p> <p>prefix-list キーワードを指定せずに ip msdp default-peer コマンドを複数入力すると、単一のアクティブピアですべての SA メッセージが受信されます。このピアに障害がある場合は、次の設定済みデフォルトピアですべての SA メッセージが受信されます。この構文は通常、スタブ サイトで使用されます。</p>
ステップ 4	<pre>ip prefix-list name [description string] seq number { permit deny } network length</pre> <p>例 :</p> <pre>Router(config)# prefix-list site-a seq 3 permit 12 network length 128</pre>	<p>(任意) ステップ 2 で指定された名前を使用し、プレフィックスリストを作成します。</p> <ul style="list-style-type: none"> • (任意) description string を指定する場合は、このプレフィックスリストを説明する 80 文字以下のテキストを入力します。 • seq number には、エントリのシーケンス番号を入力します。指定できる範囲は 1 ~ 4294967294 です。 • deny キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。 • permit キーワードを指定すると、条件が一致した場合にアクセスが許可されます。 • network length には、許可または拒否されているネットワークの番号およびネットワーク マスク長 (ビット単位) 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	ip msdp description {peer-name peer-address} text 例 : Router(config)# ip msdp description peer-name site-b	(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。 デフォルトでは、MSDP ピアに説明は関連付けられていません。
ステップ 6	end 例 : スイッチ(config)# end	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例 : スイッチ# show running-config	入力を確認します。
ステップ 8	copy running-config startup-config 例 : スイッチ# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

SA ステートのキャッシング

メモリを消費して送信元情報の遅延を短縮する場合は、SA メッセージをキャッシュに格納するようにデバイスを設定できます。送信元とグループのペアのキャッシングをイネーブルにするには、次の手順を実行します。

送信元とグループのペアのキャッシングをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : スイッチ> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 :	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
	スイッチ# <code>configure terminal</code>	
ステップ 3	<p>ip msdp cache-sa-state [<i>list access-list-number</i>]</p> <p>例 :</p> <p>スイッチ(config)# <code>ip msdp cache-sa-state 100</code></p>	<p>送信元とグループのペアのキャッシングをイネーブ ルにします (SA ステートを作成します)。アクセ スリストを通過したこれらのペアがキャッシュに格 納されます。</p> <p>list access-list-number の範囲は 100 ~ 199 です。</p> <p>(注) このコマンドの代わりに、ip msdp sa-reques グローバルコンフィギュレーション コマンドを使用できます。この代替コ マンドを使用すると、グループの新しいメ ンバがアクティブになった場合に、SA 要 求メッセージがデバイスから MSDP ピア に送信されます。</p>
ステップ 4	<p>access-list <i>access-list-number</i> {deny permit} <i>protocol source source-wildcard destination destination-wildcard</i></p> <p>例 :</p> <p>スイッチ(config)# <code>access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255</code></p>	<p>IP 拡張アクセスリストを作成します。必要な回数だ けこのコマンドを繰り返します。</p> <ul style="list-style-type: none"> • <i>access-list-number</i> の範囲は 100 ~ 199 です。ス テップ 2 で作成した番号と同じ値を入力しま す。 • deny キーワードは、条件が一致した場合にアク セスを拒否します。permit キーワードは、条件 が一致した場合にアクセスを許可します。 • <i>protocol</i> には、プロトコル名として ip を入力し ます。 • <i>source</i> には、パケットの送信元であるネットワ ークまたはホストの番号を入力します。 • <i>source-wildcard</i> には、送信元に適用するワイル ドカード ビットをドット付き 10 進表記で入力 します。無視するビット位置には 1 を設定しま す。 • <i>destination</i> には、パケットの送信先であるネッ トワークまたはホストの番号を入力します。 • <i>destination-wildcard</i> には、宛先に適用するワイ ルドカード ビットをドット付き 10 進表記で入 力します。無視するビット位置には 1 を設定し ます。

	コマンドまたはアクション	目的
		アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 5	end 例： スイッチ(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例： スイッチ# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例： スイッチ# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

MSDP ピアからの送信元情報の要求

グループへの送信元である接続 PIM SM ドメイン内のアクティブなマルチキャスト送信元を、グループの新しいメンバーが学習する必要がある場合は、新しいメンバーがグループに加入したときに、指定された MSDP ピアに SA 要求メッセージがデバイスから送信されるようにこのタスクを実行します。ピアは SA キャッシュ内の情報に応答します。ピアにキャッシュが設定されていない場合、このコマンドを実行しても何も起こりません。この機能を設定すると加入遅延は短縮されますが、メモリが消費されます。

新しいメンバーがグループに加入し、マルチキャストトラフィックを受信する必要がある場合、MSDP ピアに SA 要求メッセージを送信するようにデバイスを設定するには、次の手順を実行します。

手順

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

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例： スイッチ# <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip msdp sa-request {ip-address name} 例： スイッチ (config)# <code>ip msdp sa-request 171.69.1.1</code>	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デバイスを設定します。 <i>ip-address name</i> を指定する場合は、グループの新しいメンバーがアクティブになるときにローカルデバイスの SA メッセージの要求元になる MSDP ピアの IP アドレス、または名前を入力します。 SA メッセージを送信する必要がある MSDP ピアごとに、このコマンドを繰り返します。
ステップ 4	end 例： スイッチ (config)# <code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例： スイッチ# <code>show running-config</code>	入力を確認します。
ステップ 6	copy running-config startup-config 例： スイッチ# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

スイッチから発信される送信元情報の制御

デバイスから発信されるマルチキャスト送信元情報を制御できます。

- アドバタイズ対象の送信元 (送信元ベース)
- 送信元情報のレシーバー (要求元認識ベース)

詳細については、[送信元の再配信 \(16 ページ\)](#) および [SA 要求メッセージのフィルタリング \(18 ページ\)](#) を参照してください。

送信元の再配信

SA メッセージは、送信元が登録されている RP で発信されます。デフォルトでは、RP に登録されているすべての送信元がアドバタイズされます。送信元が登録されている場合は、RP に A フラグが設定されています。このフラグは、フィルタリングされる場合を除き、送信元が SA に格納されてアドバタイズされることを意味します。

アドバタイズされる登録済みの送信元をさらに制限するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： スイッチ> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： スイッチ# 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-name] [asn aspath-access-list-number] [route-map map] 例： スイッチ(config)# ip msdp redistribute list 21	SA メッセージに格納されてアドバタイズされる、マルチキャストルーティングテーブル内の (S,G) エントリを設定します。 デフォルトでは、ローカルドメイン内の送信元だけがアドバタイズされます。 <ul style="list-style-type: none"> (任意) list access-list-name : IP 標準または IP 拡張アクセスリストの名前または番号を入力します。標準アクセスリストの範囲は 1 ~ 99、拡張アクセスリストの範囲は 100 ~ 199 です。アクセスリストによって、アドバタイズされるローカルな送信元、および送信されるグループが制御されます。 (任意) asn aspath-access-list-number : 1 ~ 199 の範囲の IP 標準または IP 拡張アクセスリスト番号を入力します。このアクセスリスト番号は、ip as-path access-list コマンドでも設定する必要があります。 (任意) route-map map : 1 ~ 199 の範囲の IP 標準または IP 拡張アクセスリスト番号を入力します。このアクセスリスト番号は、ip as-path

	コマンドまたはアクション	目的
		<p>access-list コマンドでも設定する必要があります。</p> <p>アクセスリストまたは自律システムパスアクセスリストに従って、デバイスが (S, G) ペアをアドバタイズします。</p>
<p>ステップ 4</p>	<p>次のいずれかを使用します。</p> <ul style="list-style-type: none"> • <code>access-list</code><i>access-list-number</i> {deny permit} <i>source</i> [<i>source-wildcard</i>] • <code>access-list</code><i>access-list-number</i> {deny permit} <i>protocol source source-wildcard destination destination-wildcard</i> <p>例 :</p> <pre>スイッチ(config)# access list 21 permit 194.1.22.0</pre> <p>または</p> <pre>スイッチ(config)# access list 21 permit ip 194.1.22.0 10.1.1.10 194.3.44.0 10.1.1.10</pre>	<p>IP 標準アクセスリストを作成します。必要な回数だけこのコマンドを繰り返します。</p> <p>または</p> <p>IP 拡張アクセスリストを作成します。必要な回数だけこのコマンドを繰り返します。</p> <ul style="list-style-type: none"> • <i>access-list-number</i> : ステップ 2 で作成した同じ番号を入力します。標準アクセスリストの範囲は 1 ~ 99、拡張アクセスリストの範囲は 100 ~ 199 です。 • deny : 条件に合致している場合、アクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 • <i>protocol</i> : プロトコル名として ip を入力します。 • <i>source</i> : パケットの送信元であるネットワークまたはホストの番号を入力します。 • <i>source-wildcard</i> : 送信元に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 • <i>destination</i> : パケットの宛先であるネットワークまたはホストの番号を入力します。 • <i>destination-wildcard</i> : 宛先に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
<p>ステップ 5</p>	<p>end</p> <p>例 :</p>	<p>特権 EXEC モードに戻ります。</p>

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

SA 要求メッセージのフィルタリング

デフォルトでは、SA 情報をキャッシングしているデバイスだけが、SA 要求に応答できます。このようなデバイスでは、デフォルトで MSDP ピアからのすべての SA 要求メッセージが採用され、アクティブな送信元の IP アドレスが取得されます。

ただし、MSDP ピアからの SA 要求をすべて無視するように、デバイスを設定できます。標準アクセスリストに記述されたグループのピアからの SA 要求メッセージだけを採用することもできます。アクセスリスト内のグループが指定された場合は、そのグループのピアからの SA 要求メッセージが受信されます。他のグループのピアからの他のメッセージは、すべて無視されます。

デフォルト設定に戻すには、**no ip msdp filter-sa-request {ip-address|name}** グローバル コンフィギュレーション コマンドを使用します。

これらのオプションのいずれかを設定するには、次の手順を実行します。

手順

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

	コマンドまたはアクション	目的
ステップ 3	<p>次のいずれかを使用します。</p> <ul style="list-style-type: none"> ip msdp filter-sa-request {ip-addressname} ip msdp filter-sa-request {ip-addressname} list access-list-number <p>例 :</p> <pre>スイッチ(config)# ip msdp filter sa-request 171.69.2.2</pre>	<p>指定された MSDP ピアからの SA 要求メッセージをすべてフィルタリングします。</p> <p>または</p> <p>標準アクセスリストを通過したグループに対して、指定された MSDP ピアからの SA 要求メッセージをフィルタリングします。アクセスリストには、複数のグループアドレスが記述されています。access-list-number の範囲は 1 ~ 99 です。</p>
ステップ 4	<p>access-list access-list-number {deny permit} source [source-wildcard]</p> <p>例 :</p> <pre>スイッチ(config)# access-list 1 permit 192.4.22.0 0.0.0.255</pre>	<p>IP 標準アクセスリストを作成します。必要な回数だけこのコマンドを繰り返します。</p> <ul style="list-style-type: none"> access-list-number の範囲は 1 ~ 99 です。 deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 source には、パケットの送信元であるネットワークまたはホストの番号を入力します。 (任意) source-wildcard には、source に適用されるワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 5	<p>end</p> <p>例 :</p> <pre>スイッチ(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 6	<p>show running-config</p> <p>例 :</p> <pre>スイッチ# show running-config</pre>	<p>入力を確認します。</p>
ステップ 7	<p>copy running-config startup-config</p> <p>例 :</p>	<p>(任意) コンフィギュレーションファイルに設定を保存します。</p>

	コマンドまたはアクション	目的
	スイッチ# <code>copy running-config startup-config</code>	

スイッチで転送される送信元情報の制御

デフォルトでは、デバイスで受信されたすべての SA メッセージが、すべての MSDP ピアに転送されます。ただし、フィルタリングするか、または存続可能時間 (TTL) 値を設定し、発信メッセージがピアに転送されないようにできます。

フィルタの使用法

フィルタを作成すると、次のいずれかの処理を実行できます。

- すべての送信元とグループのペアのフィルタリング
- 特定の送信元とグループのペアだけが通過するように、IP 拡張アクセス リストを指定
- ルート マップの一致条件に基づくフィルタリング

フィルタを適用するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： スイッチ> <code>enable</code>	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： スイッチ# <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • ip msdp sa-filter out { <i>ip-address name</i> } • ip msdp sa-filter out { <i>ip-address name</i> } list <i>access-list-number</i> • ip msdp sa-filter out	<ul style="list-style-type: none"> • 指定された MSDP ピアへの SA メッセージをフィルタリングします。 • 指定したピアに対する IP 拡張アクセス リストを通過した SA メッセージのみを渡します。拡張アクセスリスト番号の範囲は 100 ~ 199 です。 <p>list と route-map の両方のキーワードを使用すると、すべての条件に一致しなければ、発信 SA</p>

	コマンドまたはアクション	目的
	<pre>{ip-address name} route-map map-tag</pre> <p>例 :</p> <pre>スイッチ(config)# ip msdp sa-filter out switch.cisco.com</pre> <p>または</p> <pre>スイッチ(config)# ip msdp sa-filter out list 100</pre> <p>または</p> <pre>スイッチ(config)# ip msdp sa-filter out switch.cisco.com route-map 22</pre>	<p>メッセージ内のいずれの (S,G) ペアも通過できません。</p> <ul style="list-style-type: none"> 指定された MSDP ピアへのルートマップ <i>map-tag</i> で一致基準を満たす SA メッセージのみを渡します。 <p>すべての一致基準に当てはまる場合、ルートマップの permit がフィルタを通してルートを通過します。 deny はルートをフィルタ処理します。</p>
ステップ 4	<pre>access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard</pre> <p>例 :</p> <pre>スイッチ(config)# access list 100 permit ip 194.1.22.0 10.1.1.10 194.3.44.0 10.1.1.10</pre>	<p>(任意) IP 拡張アクセスリストを作成します。必要な回数だけこのコマンドを繰り返します。</p> <ul style="list-style-type: none"> <i>access-list-number</i> には、ステップ 2 で指定した番号を入力します。 deny キーワードは、条件が一致した場合にアクセスを拒否します。 permit キーワードは、条件が一致した場合にアクセスを許可します。 <i>protocol</i> には、プロトコル名として ip を入力します。 <i>source</i> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 <i>source-wildcard</i> には、送信元に適用するワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <i>destination</i> には、パケットの送信先であるネットワークまたはホストの番号を入力します。 <i>destination-wildcard</i> には、宛先に適用するワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>

SA メッセージに格納されて送信されるマルチキャストデータの TTL による制限

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

SA メッセージに格納されて送信されるマルチキャストデータの TTL による制限

TTL 値を使用して、各送信元の最初の SA メッセージにカプセル化されるデータを制御できます。IP ヘッダー TTL 値が *ttl* 引数以上であるマルチキャストパケットだけが、指定された MSDP ピアに送信されます。たとえば、内部トラフィックの TTL 値を 8 に制限できます。他のグループを外部に送信する場合は、これらのパケットの TTL を 8 より大きく設定して送信する必要があります。

TTL しきい値を確立するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： スイッチ> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： スイッチ# 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 ttl-threshold { <i>ip-address</i> <i>name</i> } <i>ttl</i> 例 : スイッチ (config) # ip msdp ttl-threshold switch.cisco.com 0	指定された MSDP ピア宛ての最初の SA メッセージにカプセル化されるマルチキャストデータを制限します。 <ul style="list-style-type: none"> • <i>ip-address</i> <i>name</i> には、TTL の制限が適用される MSDP ピアの IP アドレスまたは名前を入力します。 • <i>ttl</i> には、TTL 値を入力します。デフォルトは 0 です。この場合、すべてのマルチキャストデータパケットは、TTL がなくなるまでピアに転送されます。指定できる範囲は 0 ~ 255 です。
ステップ 4	end 例 : スイッチ (config) # end	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例 : スイッチ # show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例 : スイッチ # copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

スイッチで受信される送信元情報の制御

デフォルトでは、デバイスは、MSDP の RPF ピアによって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 SA メッセージをフィルタリングし、MSDP ピアから受信する送信元情報を制御できます。つまり、特定の着信 SA メッセージを受信ないようにデバイスを設定できます。

次のいずれかの処理を実行できます。

- MSDP ピアからのすべての着信 SA メッセージのフィルタリング
- 特定の送信元とグループのペアが通過するように、IP 拡張アクセス リストを指定
- ルート マップの一致条件に基づくフィルタリング

フィルタを適用するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： スイッチ> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： スイッチ# 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	次のいずれかを使用します。 <ul style="list-style-type: none"> ip msdp sa-filter in {<i>ip-address name</i>} ip msdp sa-filter in {<i>ip-address name</i>} list <i>access-list-number</i> ip msdp sa-filter in {<i>ip-address name</i>} route-map <i>map-tag</i> 例： スイッチ(config)# ip msdp sa-filter in switch.cisco.com または スイッチ(config)# ip msdp sa-filter in list 100 または スイッチ(config)# ip msdp sa-filter in switch.cisco.com route-map 22	<ul style="list-style-type: none"> 指定された MSDP ピアへの SA メッセージをフィルタリングします。 IP 拡張アクセスリストを通過する、指定されたピアからの SA メッセージのみを通過させます。拡張アクセスリスト <i>access-list-number</i> の範囲は 100 ~ 199 です。 list と route-map の両方のキーワードを使用すると、すべての条件に一致しなければ、発信 SA メッセージ内のいずれの (S,G) ペアも通過できません。 ルートマップ <i>map-tag</i> 内の一致条件を満たす、指定された MSDP ピアからの SA メッセージのみを通過させます。 すべての一致基準に当てはまる場合、ルートマップの permit がフィルタを通してルートを通過します。deny はルートをフィルタ処理しません。
ステップ 4	access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard 例： スイッチ(config)# access list 100 permit ip	(任意) IP 拡張アクセスリストを作成します。必要な回数だけこのコマンドを繰り返します。 <ul style="list-style-type: none"> <i>Access-list-number</i> には、ステップ 2 で指定した番号を入力します。

	コマンドまたはアクション	目的
	<pre>194.1.22.0 10.1.1.10 194.3.44.0 10.1.1.10</pre>	<ul style="list-style-type: none"> • deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 • <i>protocol</i> には、プロトコル名として ip を入力します。 • <i>source</i> には、パケットの送信元であるネットワークまたはホストの番号を入力します。 • <i>source-wildcard</i> には、送信元に適用するワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 • <i>destination</i> には、パケットの送信先であるネットワークまたはホストの番号を入力します。 • <i>destination-wildcard</i> には、宛先に適用するワイルドカードビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 <p>アクセスリストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 5	<p>end</p> <p>例 :</p> <pre>スイッチ(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 6	<p>show running-config</p> <p>例 :</p> <pre>スイッチ# show running-config</pre>	入力を確認します。
ステップ 7	<p>copy running-config startup-config</p> <p>例 :</p> <pre>スイッチ# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

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**
6. **show running-config**
7. **copy running-config startup-config**

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 モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip 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しているデバイス上のすべてのMSDPピアは、そのグループ内の他のすべてのMSDPピアと完全にメッシュ構造になっ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す。また、 ip msdp mesh-group コマンドを使用して、その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。

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

MSDP ピアのシャットダウン

始める前に

MSDP が動作していて、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 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**
6. **show running-config**
7. **copy running-config startup-config**

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 モードを有効にします。 プロンプトが表示されたらパスワードを入力します。

	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 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。
ステップ 6	show running-config 例： Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

境界 PIM デンス モード領域の MSDP への包含

デンスモード (DM) 領域と PIM スパースモード (SM) 領域の境界となるデバイスに MSDP を設定します。デフォルトでは、DM 領域のアクティブな送信元は MSDP に加入しません。



(注) **ip msdp border sa-address** グローバル コンフィギュレーション コマンドの使用は推奨できません。DM ドメイン内の送信元が SM ドメイン内の RP にプロキシ登録されるように SM ドメイン内の境界ルータを設定し、標準 MSDP 手順でこれらの送信元をアダプタイズするように SM ドメインを設定してください。

ip msdp originator-id グローバル コンフィギュレーション コマンドを実行すると、RP アドレスとして使用されるインターフェイスも識別されます。**ip msdp border sa-address** および **ip msdp**

originator-id グローバル コンフィギュレーション コマンドの両方が設定されている場合、**ip msdp originator-id** コマンドから取得されたアドレスが RP アドレスを指定します。

DM 領域でアクティブな送信元の SA メッセージを MSDP ピアに送信するように境界ルータを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： スイッチ> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： スイッチ# 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 interface-id 例： スイッチ(config)# ip msdp border sa-address 0/1	DM 領域内のアクティブな送信元に関する SA メッセージを送信するように、DM 領域と SM 領域の境界スイッチを設定します。 <i>interface-id</i> には、SA メッセージ内の RP アドレスとして使用される、IP アドレスの配信元となるインターフェイスを指定します。 インターフェイスの IP アドレスは、SA メッセージ内の RP フィールド [Originator-ID] の値として使用されます。
ステップ 4	ip msdp redistribute [list access-list-name] [asn aspath-access-list-number] [route-map map] 例： スイッチ(config)# ip msdp redistribute list 100	SA メッセージに格納されてアドバタイズされる、マルチキャストルーティングテーブル内の (S,G) エントリを設定します。 詳細については、 送信元の再配信（16 ページ） を参照してください。
ステップ 5	end 例： スイッチ(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例：	入力を確認します。

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

RP アドレス以外の発信元アドレスの設定

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により、発信元 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 アドレスが発信元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。

手順の概要

1. `enable`
2. `configure terminal`
3. `ip msdp originator-id`
4. `exit`
5. `show running-config`
6. `copy running-config startup-config`

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 : スイッチ> <code>enable</code>	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : スイッチ# <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	ip msdp originator-id 例 : スイッチ(config)# ip msdp originator-id ethernet 1	発信元デバイスのインターフェイスのアドレスとなるように、SA メッセージ内の RP アドレスを設定します。
ステップ 4	exit 例 : スイッチ(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 5	show running-config 例 : スイッチ# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例 : スイッチ# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

MSDP のモニタリングおよびメンテナンス

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 モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ2 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* 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。ip msdp cache-sa-state コマンドは、このコマンドによって出力が生成されるように設定する必要があります。

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
                  AS      State      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、統計情報または 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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	clear ip msdp peer [<i>peer-address</i> <i>peer-name</i>] 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 [<i>peer-address</i> <i>peer-name</i>] 例： Device# clear ip msdp statistics	指定された MSDP ピアの統計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。

	コマンドまたはアクション	目的
ステップ 4	clear ip msdp sa-cache [<i>group-address</i>] 例 : Device# clear ip msdp sa-cache	SA キャッシュ エントリを消去します。 <ul style="list-style-type: none"> • clear ip msdp sa-cache コマンドにオプションの <i>group-address</i> 引数または <i>source-address</i> 引数を指定した場合、すべての SA キャッシュエントリが消去されます。 • 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 <i>group-address</i> 引数を使用します。

MSDP の設定例

デフォルト MSDP ピアの設定 : 例

次に、ルータ A およびルータ C の部分的な設定の例を示します。これらの ISP にはそれぞれに複数のカスタマー（カスタマーと同様）があり、デフォルトのピアリング（BGP または MBGP なし）を使用しています。この場合、両方の ISP で類似した設定となります。つまり、両方の ISP では、対応するプレフィックスリストで SA が許可されている場合、デフォルトピアからの SA だけが受信されます。

ルータ A

```
Router(config)# ip msdp default-peer 10.1.1.1
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

ルータ C

```
Router(config)# ip msdp default-peer 10.1.1.1 prefix-list site-a
Router(config)# ip prefix-list site-b permit 10.0.0.0/1
```

SA ステートのキャッシング : 例

次に、グループ 224.2.0.0/16 への送信元である 171.69.0.0/16 のすべての送信元のキャッシュ ステートをイネーブルにする例を示します。

```
スイッチ(config)# ip msdp cache-sa-state 100
スイッチ(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

MSDP ピアからの送信元情報の要求 : 例

次に、171.69.1.1 の MSDP ピアに SA 要求メッセージを送信するように、スイッチを設定する例を示します。

```
スイッチ(config)# ip msdp sa-request 171.69.1.1
```

スイッチから発信される送信元情報の制御 : 例

次に、171.69.2.2 の MSDP ピアからの SA 要求メッセージをフィルタリングするように、スイッチを設定する例を示します。ネットワーク 192.4.22.0 の送信元からの SA 要求メッセージはアクセスリスト 1 に合格して、受信されます。その他のすべてのメッセージは無視されます。

```
スイッチ(config)# ip msdp filter sa-request 171.69.2.2 list 1  
スイッチ(config)# access-list 1 permit 192.4.22.0 0.0.0.255
```

スイッチから転送される送信元情報の制御 : 例

次に、アクセスリスト 100 を通過する (S,G) ペアだけが SA メッセージに格納され、*switch.cisco.com* という名前のピアに転送されるように設定する例を示します。

```
スイッチ(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet1/0/1  
スイッチ(config)# ip msdp sa-filter out switch.cisco.com list 100  
スイッチ(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.20 0 0.0.255.255
```

スイッチで受信される送信元情報の制御 : 例

次に、*switch.cisco.com* という名前のピアからのすべての SA メッセージをフィルタリングする例を示します。

```
スイッチ(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet1/0/1  
スイッチ(config)# ip msdp sa-filter in switch.cisco.com
```

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
```

MSDP ピアからの送信元情報の要求 : 例

次に、171.69.1.1 の MSDP ピアに SA 要求メッセージを送信するように、スイッチを設定する例を示します。

```
スイッチ(config)# ip msdp sa-request 171.69.1.1
```


翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。