MSDP の設定

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、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース 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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

MSDP の設定について

このセクションでは、スイッチに Multicast Source Discovery Protocol（MSDP）を設定する方法について説明します。MSDP によって、複数の Protocol-Independent Multicast Sparse-Mode（PIM-SM）ドメインが接続されます。

このソフトウェア リリースでは、MSDP と連携して動作する Multicast Border Gateway Protocol（MBGP）がサポートされていないため、MSDP は完全にはサポートされていません。ただし、MBGP が動作していない場合、MSDP と連携して動作するデフォルト ピアを作成できます。

（注） この機能を使用するには、アクティブ スイッチ上で IP Services フィーチャー セットが稼働している必要があります。

MSDP の概要

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 ドメインでは独自の RP が使用され、他のドメインの RP には依存しません。RP は伝送制御プロトコル（TCP）を通じて MSDP を実行し、他のドメイン内のマルチキャスト送信元を検出します。

PIM-SM ドメイン内の RP は、他のドメイン内の MSDP 対応デバイスと MSDP ピアリング関係にあります。ピアリング関係は TCP 接続を通じて発生します。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を交換します。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。

このトポロジの目的は、ドメインから、他のドメイン内のマルチキャスト送信元を検出することです。マルチキャスト送信元がレシーバーのあるドメインを対象としている場合、マルチキャストデータは PIM-SM の通常の送信元ツリー構築メカニズムを通じて配信されます。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。

MSDP のドメイン間動作は、Border Gateway Protocol（BGP）または MBGP に大きく依存します。ドメイン内の RP（インターネットへのアナウンス対象であるグローバル グループを送信する送信元用の RP）で、MSDP を実行してください。

MSDP の動作

送信元が最初のマルチキャスト パケットを送信すると、送信元に直接接続された先頭ホップ ルータ（指定ルータまたは RP）によって RP に PIM 登録メッセージが送信されます。RP は登録メッセージを使用し、アクティブな送信元を登録したり、ローカル ドメイン内の共有ツリーの下方向にマルチキャスト パケットを転送します。MSDP が設定されている場合は、Source-Active（SA）メッセージも、すべての MSDP ピアに転送します。送信元、送信元からの送信先であるグループ、および RP のアドレスまたは発信元 ID（RP アドレスとして使用されるインターフェイスの IP アドレス）が設定されている場合は、SA メッセージによってこれらが識別されます。

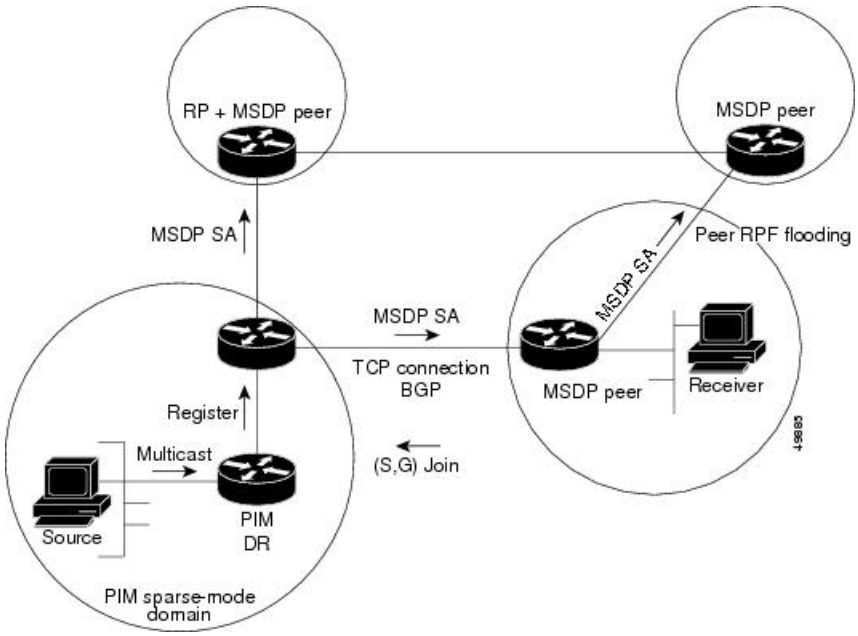
各 MSDP ピアは SA メッセージを発信元の RP から受信して転送し、ピア Reverse-Path Forwarding（RPF）フラッディングを実現します。MSDP デバイスは、BGP または MBGP ルーティング テーブルを調べ、どのピアが SA メッセージの発信元 RP へのネクスト ホップであるかを検出します。このようなピアは *RPF* ピアと呼ばれます。MSDP デバイスでは、RPF ピア以外のすべての MSDP ピアにメッセージが転送されます。BGP および MBGP がサポートされていない場合に MSDP を設定する方法については、デフォルトの MSDP ピアの設定 （4 ページ）を参照してください。

MSDP ピアは、非 RPF ピアから発信元 RP へ向かう同じ SA メッセージを受信すると、そのメッセージをドロップします。それ以外の場合、すべての MSDP ピアにメッセージが転送されます。

ドメインの RP ピアは MSDP ピアから SA メッセージを受信します。この RP が SA メッセージに記述されているグループへの加入要求を持ち、空でない発信インターフェイス リストに（*,G）エントリが含まれている場合、そのグループはドメインの対象となり、RP から送信元方向に（S,G）Join メッセージが送信されます。（S,G）Join メッセージが送信元の DR に到達してからは、送信元からリモート ドメイン内の RP への送信元ツリーのブランチが構築されています。この結果、マルチキャスト トラフィックを送信元から送信元ツリーを経由して RP へ、そしてリモート ドメイン内の共有ツリーを下ってレシーバへと送信できます。

図 *1 : RP* ピア間で動作する *MSDP*

この図に、2 つの MSDP ピアの間での 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。MSDP が設定されている場合は、次のシーケンスが発生します。



デフォルトでは、スイッチで受信された SA メッセージ内の送信元やグループのペアは、キャッシュに格納されません。また、MSDP SA 情報が転送される場合、この情報はメモリに格納されません。したがって、ローカル RP で SA メッセージが受信された直後にメンバーがグループに加入した場合、そのメンバーは、その次の SA メッセージによって送信元に関する情報が取得されるまで、待機する必要があります。この遅延は加入遅延と呼ばれます。

ローカル RP では、SA 要求を送信し、指定されたグループに対するすべてのアクティブな送信元の要求をすぐに取得できます。デフォルトでは、新しいメンバーがグループに加入してマルチキャスト トラフィックを受信する必要が生じた場合、スイッチは MSDP ピアに SA 要求メッセージを送信しません。新しいメンバーは次の定期的な SA メッセージを受信する必要があります。

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 要求メッセージを送信するようにスイッチを設定します。

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。

MSDP の設定方法

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。

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： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： デバイス# **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： Router(config)# **ip msdp default-peer 10.1.1.1 prefix-list site-a**	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。 • *ip-address* | *name* 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。 **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ビス プロバイダー クラウドで使用されます。 **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。
ステップ 4	**ip prefix-list** *name* [**description** *string*] | **seq** *number* {**permit** | **deny**} *network length* 例：	（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。

	コマンドまたはアクション	目的
	`Router(config)# prefix-list site-a seq 3 permit 12 network length 128`	• （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。
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： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `デバイス# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `デバイス# copy running-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。

	コマンドまたはアクション	目的
	startup-config	

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Device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：** デバイス> **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：** デバイス# **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 cache-sa-state** [**list** *access-list-number*] **例：** デバイス(config)# **ip msdp cache-sa-state 100**	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。 **list** *access-list-number* の範囲は 100 ～ 199 です。 （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Deviceから MSDP ピアに送信されます。

	コマンドまたはアクション	目的
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* 例： デバイス(config)# **access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255**	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。 • *access-list-number* 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。 • *protocol* には、プロトコル名として **ip** を入力します。 • *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。 • *source-wildcard* 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。 • *destination* 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。 • *destination-wildcard* 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。 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： デバイス(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： デバイス# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： デバイス# **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。

スイッチから発信される送信元情報の制御

Device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 （9 ページ）およびSA 要求メッセージのフィルタリング （12 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： デバイス> **enable**	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	デバイス# **configure terminal**	
ステップ 3	**ip msdp redistribute** [**list** *access-list-name*] [**asn** *aspath-access-list-number*] [**route-map** *map*] 例： デバイス(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。 • （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 access-list** コマンドでも設定する必要があります。 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、Deviceが（S,G）ペアをアドバタイズします。
ステップ 4	次のいずれかを使用します。 • access-list*access-list-number* {deny | permit} *source* [*source-wildcard*]	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。 または

	コマンドまたはアクション	目的
	• access-list*access-list-number* {deny|permit} *protocol source source-wildcard destination destination-wildcard* 例： デバイス(config)# **access list 21 permit 194.1.22.0** または デバイス(config)# **access list 21 permit ip 194.1.22.0 1.1.1.1 194.3.44.0 1.1.1.1**	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。 • *access-list-number*：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。 • *protocol*：プロトコル名として **ip** を入力します。 • *source*：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。 • *source-wildcard*：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。 • *destination*：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。 • *destination-wildcard*：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。 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： デバイス(config)# **end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： デバイス# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： デバイス# **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Deviceだけが、SA 要求に応答できます。このようなDevice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、Device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： デバイス> **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： デバイス# **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	次のいずれかを使用します。 • `ip msdp filter-sa-request` {*ip-addressname*} • `ip msdp filter-sa-request` {*ip-addressname*} `list` *access-list-number* 例： `デバイス(config)# ip msdp filter sa-request 171.69.2.2`	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。 または 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。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `デバイス(config)# access-list 1 permit 192.4.22.0 0.0.0.255`	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。 • *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。 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： `デバイス(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config** 例： デバイス# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： デバイス# **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。

スイッチで転送される送信元情報の制御

デフォルトでは、Device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： デバイス> **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： デバイス# **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	次のいずれかを使用します。
	• **ip msdp sa-filter out** {*ip-address name*}
	• **ip msdp sa-filter out** {*ip-address name*} `list` *access-list-number*
	• **ip msdp sa-filter out** {*ip-address name*} `route-map` *map-tag*
	例：
	`デバイス(config)# ip msdp sa-filter out switch.cisco.com`
	または
	`デバイス(config)# ip msdp sa-filter out list 100`
	または
	`デバイス(config)# ip msdp sa-filter out switch.cisco.com route-map 22`
		• 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。
		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。
		• 指定されたMSDPピアへのルートマップ *map-tag* で一致基準を満たすSAメッセージのみを渡します。
		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す。

ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* 例： `デバイス(config)# access list 100 permit ip 194.1.22.0 1.1.1.1 194.3.44.0 1.1.1.1`	（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。 • *access-list-number* 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。 • *protocol* には、プロトコル名として **ip** を入力します。 • *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。 • *source-wildcard* には、送信元に適用するワイルドカードビットをドッ

	コマンドまたはアクション	目的
		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。 • *destination* 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。 • *destination-wildcard* 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。 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： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `デバイス# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `デバイス# 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： デバイス> **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： デバイス# **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** {*ip-address* | *name*} *ttl* 例： デバイス(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。 • *ip-address* | *name* 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。 • *ttl* 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： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： デバイス# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： デバイス# **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、Device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 メッセージを受信しないようにDevice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**： デバイス> **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**： デバイス# **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。 • **ip msdp sa-filter in** {*ip-address name*} • **ip msdp sa-filter in** {*ip-address name*} list *access-list-number* • **ip msdp sa-filter in** {*ip-address name*} route-map *map-tag* **例**： デバイス(config)# **ip msdp sa-filter in switch.cisco.com**	• 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 *access-list-number* 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 *map-tag* 内の一致条件を満たす、指定された MSDP ピ

	コマンドまたはアクション	目的
	または デバイス(config)# **ip msdp sa-filter in list 100** または デバイス(config)# **ip msdp sa-filter in switch.cisco.com route-map 22**	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す。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* **例**： デバイス(config)# **access list 100 permit ip 194.1.22.0 1.1.1.1 194.3.44.0 1.1.1.1**	（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。 • *Access-list-number* 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。 • *protocol* には、プロトコル名として **ip** を入力します。 • *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。 • *source-wildcard* 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。 • *destination* 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。 • *destination-wildcard* 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。 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。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： デバイス# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： デバイス# **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 メッシュ グループの設定

MSDP メッシュ グループは、MSDPによって完全な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。メッシュ グループ内のピアから受信されたSAメッセージは、同じメッシュ グループ内の他のピアに転送されません。したがって、SA メッセージのフラッディングが削減され、ピア RPF フラッディングが簡素化されます。ドメイン内に複数の RP がある場合は、**ip msdp mesh-group** 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。特に、ドメインを越えてSAメッセージを送信する場合に使用します。単一のDeviceに複数のメッシュ グループを（異なる名前で）設定できます。

メッシュ グループを作成するには、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： デバイス> **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： デバイス# **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 mesh-group** *name* {*ip-address* | *name*} 例： `デバイス(config)# ip msdp mesh-group 2 switch.cisco.com`	MSDP メッシュ グループを設定し、そのメッシュ グループに属する MSDP ピアを指定します。 デフォルトでは、MSDP ピアはメッシュ グループに属しません。 • *name* には、メッシュ グループの名前を入力します。 • *ip-address* | *name* には、メッシュ グループのメンバーになる MSDP ピアの IP アドレスまたは名前を入力します。 グループ内の MSDP ピアごとに、この手順を繰り返します。
ステップ 4	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `デバイス# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `デバイス# 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

複数のMSDPコマンドが設定された単一のピアをアクティブにしない場合は、ピアをシャットダウンしてから、あとで起動できます。ピアがシャットダウンすると、TCP接続が終了し、再起動されません。ピアの設定情報を保持したまま、MSDPセッションをシャットダウンすることもできます。

ピアをシャットダウンするには、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： デバイス> **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： デバイス# **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： デバイス(config)# **ip msdp shutdown switch.cisco.com**	設定情報を保持したまま、指定された MSDP ピアをシャットダウン状態にします。 *peer-name* | *peer address* を指定する場合は、シャットダウンする MSDP ピアの IP アドレスまたは名前を入力します。
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： デバイス# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： デバイス# **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Device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ドバタイズするように 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： デバイス> **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： デバイス# **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： デバイス(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。 *interface-id* 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*]	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

	コマンドまたはアクション	目的
	例： デバイス(config)# **ip msdp redistribute list 100**	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 （9 ページ）を参照してください。
ステップ 5	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： デバイス# **show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： デバイス# **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。

RP アドレス以外の発信元アドレスの設定

SA メッセージの発信元である MSDP スピーカーで、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する場合は、送信元 ID を変更します。次のいずれかの場合に送信元 ID を変更できます。

- MSDP メッシュグループ内の複数のDevice上で、論理 RP を設定する場合。
- PIM SM ドメインと DM ドメインの境界となるDeviceがある場合。サイトの DM ドメインの境界となるDeviceがあり、SM がその外部で使用されている場合は、DM の送信元を外部に通知する必要があります。このDeviceは RP でないため、SA メッセージで使用される RP アドレスはありません。したがって、このコマンドではインターフェイスのアドレスを指定し、RP アドレスを提供します。

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。

SA メッセージの発信元である MSDP スピーカーで、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： デバイス> **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： デバイス# **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** *interface-id* 例： デバイス(config)# **ip msdp originator-id 0/1**	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。 *Interface-id* には、ローカルDeviceのインターフェイスを指定します。
ステップ 4	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： デバイス# **show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： デバイス# **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 SA メッセージ、ピア、状態、ピアのステータスをモニタするコマンドは以下のとおりです。

表 *1: MSDP* のモニタおよびメンテナンスのためのコマンド

コマンド	目的
debug ip msdp [*peer-address* | *name*] [**detail**] [**routes**]	MSDP アクティビティをデバッグします。
debug ip msdp resets	MSDP ピアのリセット原因をデバッグします。
show ip msdp count [*autonomous-system-number*]	SA メッセージに格納され、各自律システムから発信された送信元およびグループの個数を表示します。**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。
show ip msdp peer [*peer-address* | *name*]	MSDP ピアに関する詳細情報を表示します。
show ip msdp sa-cache [*group-address* | *source-address* | *group-name* | *source-name*] [*autonomous-system-number*]	MSDP ピアから学習した（S,G）ステートを表示します。
show ip msdp summary	MSDP ピア ステータスおよび SA メッセージ数を表示します。

MSDP 接続、統計情報、SA キャッシュ エントリをクリアするコマンドは以下のとおりです。

表 *2: MSDP* 接続、統計情報、または *SA* キャッシュ エントリをクリアするためのコマンド

コマンド	目的
clear ip msdp peer *peer-address* | *name*	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。
clear ip msdp statistics [*peer-address* | *name*]	セッションをリセットせずに、1 つまたはすべての MSDP ピア統計情報カウンタをクリアします。
clear ip msdp sa-cache [*group-address* | *name*]	すべてのエントリの SA キャッシュ エントリ、特定のグループのすべての送信元、または特定の送信元とグループのペアのすべてのエントリをクリアします。

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）がおり、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。

```
デバイス(config)# ip msdp cache-sa-state 100
デバイス(config)# access-list 100 permit ip 171.69.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

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。

```
デバイス(config)# ip msdp filter sa-request 171.69.2.2 list 1
デバイス(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。

```
デバイス(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet1/0/1
デバイス(config)# ip msdp sa-filter out switch.cisco.com list 100
デバイス(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。

```
デバイス(config)# ip msdp peer switch.cisco.com connect-source gigabitethernet1/0/1
デバイス(config)# ip msdp sa-filter in switch.cisco.com
```

Multicast Source Discovery Protocol の機能情報

表 *3 : Multicast Source Discovery Protocol* の機能情報

機能名	リリース	機能情報
Multicast Source Discovery Protocol	Cisco IOS XE 3.3SE	この機能が導入されました