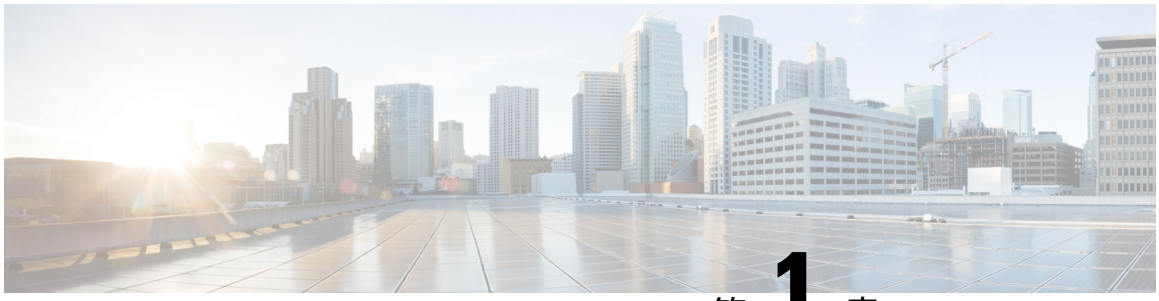
Cisco IOS リリース 15.2(8)E（Catalyst マイクロスイッチ シリーズ）IP マルチキャスト スヌーピング コンフィギュレーション ガイド

初版：2021 年 4 月 26 日

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

目 次



第 1 章

IGMP スヌーピングの設定

IGMP スヌーピングの前提条件

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

- VLAN をグローバル コンフィギュレーション モードに設定してください。
- IP アドレスおよび VLAN インターフェイスを設定してください。IGMP スヌーピング クエリアは、イネーブルの場合この IP アドレスをクエリーの送信元アドレスとして使用します。
- VLAN インターフェイス上で IP アドレスが設定されていない場合、IGMP スヌーピング クエリアは IGMP クエリア用に設定されたグローバル IP アドレスを使用しようとします。グローバル IP アドレスが指定されていない場合、IGMP クエリアは VLAN スイッチ仮想インターフェイス（SVI）IP アドレス（存在する場合）を使用しようとします。SVI IP アドレスが存在しない場合、デバイスはデバイス上で設定された利用可能な最初の IP アドレスを使用します。利用可能な最初の IP アドレスは、**show ip interface** 特権 EXEC コマンドの出力に表示されます。IGMP スヌーピングクエリアはデバイス上で利用可能な IP アドレスを検出できない場合、IGMP 一般クエリを生成しません。
- IGMP スヌーピング クエリアは IGMP バージョン 1 および 2 をサポートします。
- 管理上イネーブルである場合、IGMP スヌーピング クエリアはネットワークにマルチキャスト ルータの存在を検出すると、非クエリア ステートになります。
- 管理上イネーブルである場合、VLAN で IGMP スヌーピングが無効になっていると、IGMP スヌーピングクエリアは動作無効状態に移行します。

- レイヤ 3 マルチキャストはサポートされていません。
- MAC ベースのスヌーピングはハードウェアでサポートされています。

IGMP スヌーピングの制約事項

次に、IGMP スヌーピングの制約事項を示します。

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

  ネットワークで実際の脱退にかかる待ち時間は、通常、設定した脱退時間どおりになります。ただし、脱退時間は、リアルタイムの CPU の負荷の状態、およびネットワークの遅延状態、インターフェイスから送信されたトラフィック量によって、設定された時間を前後することがあります。
- IGMP スロットリング アクションの制約事項は、レイヤ 2 ポートにだけ適用されます。**ip igmp max-groups action replace** インターフェイス コンフィギュレーション コマンドは論理 EtherChannel インターフェイスで使用できますが、EtherChannel ポート グループに属するポートでは使用できません。

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

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

IGMP スヌーピングについて

IGMP スヌーピング

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

トポートを削除します。マルチキャスト クライアントから IGMP メンバーシップ レポートを受信しなかった場合にも、スイッチはエントリを定期的に削除します。

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

マルチキャスト ルータは、すべての VLAN に定期的にジェネラル クエリーを送出します。このマルチキャスト トラフィックに関心のあるホストはすべて Join 要求を送信し、転送テーブルのエントリに追加されます。デバイスは、IGMP Join 要求の送信元となる各グループの IGMP スヌーピング IP マルチキャスト転送テーブルで、VLAN ごとに 1 つずつエントリを作成します。

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

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

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

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

ここでは、IGMP スヌーピングの特性について説明します。

IGMP のバージョン

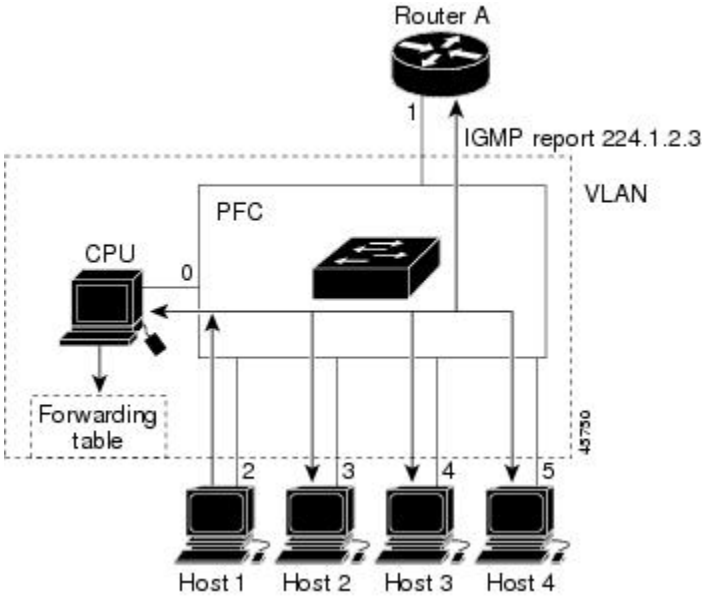
デバイスは、IGMP バージョン 1、IGMP バージョン 2、および IGMP バージョン 3 をサポートしています。これらのバージョンは、デバイス上でそれぞれ相互運用できます。たとえば、IGMP スヌーピングがイネーブルになっていて、クエリアのバージョンが IGMPv2 で、デバイスがホストから IGMPv3 レポートを受信している場合、デバイスは IGMPv3 レポートをマルチキャストルータに転送できます。

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

マルチキャスト グループへの加入

図 *1 :* 最初の *IGMP Join* メッセージ

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



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

表 *1 : IGMP* スヌーピング転送テーブル

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

デバイスのハードウェアは、IGMP 情報パケットをマルチキャストグループの他のパケットと区別できます。テーブルの情報は、224.1.2.3 マルチキャスト IP アドレス宛ての、IGMP パケッ

トではないフレームを、ルータおよびグループに加入したホストに対して送信するように、スイッチング エンジンに指示します。

図 *2:2* 番目のホストのマルチキャスト グループへの加入

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

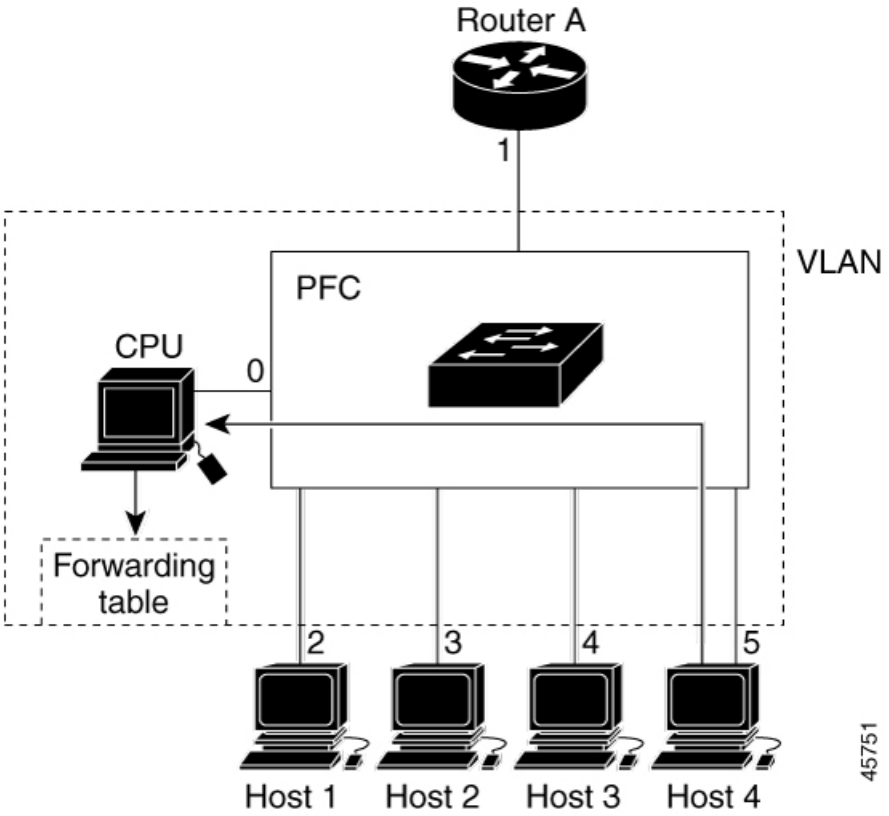


表 *2:* 更新された *IGMP* スヌーピング転送テーブル

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

マルチキャスト グループからの脱退

ルータはマルチキャスト一般クエリを定期的に送信し、デバイスはそれらのクエリを VLAN のすべてのポートを通じて転送します。関心のあるホストがクエリーに応答します。VLAN内の少なくとも1つのホストがマルチキャスト トラフィックを受信するようなら、ルータは、その VLAN へのマルチキャスト トラフィックの転送を続行します。デバイスは、その IGMP ス

ヌーピングによって維持された IP マルチキャストグループの転送テーブルで指定されたホストに対してだけ、マルチキャスト グループ トラフィックを転送します。

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

即時脱退

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

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

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

IGMP 脱退タイマーの設定

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

IGMP レポート抑制

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

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

ベてのマルチキャストルータに送信します。デバイスは、グループの残りのIGMP レポートをマルチキャストルータに送信しません。この機能により、マルチキャストデバイスにレポートが重複して送信されることを防ぎます。

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

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

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

IGMP スヌーピングのデフォルト設定

次の表に、デバイスのIGMP スヌーピングのデフォルト設定を示します。

表 *3 : IGMP* スヌーピングのデフォルト設定

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

[1] (1) TCN = トポロジ変更通知

IGMP フィルタリングおよびスロットリング

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

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

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

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

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

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

IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定

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

表 *4: IGMP* フィルタリングのデフォルト設定

機能	デフォルト設定
IGMP フィルタ	適用なし
IGMP グループの最大数	最大数の設定なし （注） 転送テーブルに登録されているグループが最大数に達していると、デフォルトのIGMPスロットリング アクションはIGMP レポートを拒否します。

機能	デフォルト設定
IGMP プロファイル	未定義
IGMP プロファイル アクション	範囲で示されたアドレスを拒否

IGMP スヌーピングを設定する方法

デバイスでの IGMP スヌーピングのイネーブル化またはディセーブル化

IGMP スヌーピングがグローバルにイネーブルまたはディセーブルに設定されている場合は、既存のすべての VLAN インターフェイスでもイネーブルまたはディセーブルになります。デフォルトでは IGMP スヌーピングはすべての VLAN でイネーブルになっていますが、VLAN 単位でイネーブルまたはディセーブルにすることができます。

グローバル IGMP スヌーピングは、VLAN IGMP スヌーピングより優先されます。グローバル スヌーピングがディセーブルの場合、VLAN スヌーピングをイネーブルに設定することはできません。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

デバイスで IGMP スヌーピングをグローバルにイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping** 例： `Device(config)# ip igmp snooping`	既存のすべての VLAN インターフェイスでグローバルに IGMP スヌーピングを有効にします。

	コマンドまたはアクション	目的
		（注） すべての VLAN インターフェイス上で IGMP スヌーピングをグローバルにディセーブルにするには、**no ip igmp snooping** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping vlan** *vlan-id* 例： `Device(config)# ip igmp snooping vlan 7`	VLAN インターフェイス上で IGMP スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 VLANスヌーピングをイネーブルにするには、IGMPスヌーピングをグローバルにイネーブルに設定しておく必要があります。

	コマンドまたはアクション	目的
		（注） 特定の VLAN インターフェイス上で IGMP スヌーピングをディセーブルにするには、**no ip igmp snooping vlan** *vlan-id* グローバル コンフィギュレーション コマンドを、指定した VLAN 番号に対して使用します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

マルチキャスト ルータ ポートの設定

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id* 例：	マルチキャスト ルータの VLAN ID およびマルチキャスト ルータに対するインターフェイスを指定します。

	コマンドまたはアクション	目的
	`Device(config)# ip igmp snooping vlan 5 mrouter interface gigabitethernet 1/0/1`	• 指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポートチャネル範囲は 1 ～ 128 です。 （注） VLAN からマルチキャスト ルータポートを削除するには、**no ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping mrouter** [**vlan** *vlan-id*] 例： `Device# show ip igmp snooping mrouter vlan 5`	VLAN インターフェイス上で IGMP スヌーピングが有効になっていることを確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

グループに加入するホストの静的な設定

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

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

手順

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

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping vlan** *vlan-id* **static** *mac_address* **interface** *interface-id* 例： `Device(config)# ip igmp snooping vlan 105 static 0100.5exx.xxxx interface gigabitethernet1/0/1`	マルチキャスト グループのメンバとしてレイヤ 2 ポートを静的に設定します。 • *vlan-id* は、マルチキャスト グループの VLAN ID です。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。 • *mac-address* は、グループ MAC アドレスです。 • *interface-id* は、メンバ ポートです。物理インターフェイスまたはポート チャネル（1 ～ 6）に設定できます。 （注） マルチキャストグループからレイヤ 2 ポートを削除するには、 **no ip igmp snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping groups** 例： `Device# show ip igmp snooping groups`	メンバ ポートおよび IP アドレスを確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP 即時脱退のイネーブル化

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping vlan** *vlan-id* **immediate-leave** 例： `Device(config)# ip igmp snooping vlan 21 immediate-leave`	VLAN インターフェイス上で、IGMP 即時脱退をイネーブルにします。 （注） VLAN 上で IGMP 即時脱退をディセーブルにするには、 **no ip igmp snooping vlan** *vlan-id* **immediate-leave** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping vlan** *vlan-id* 例： `Device# show ip igmp snooping vlan 21`	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。

IGMP 脱退タイマーの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp snooping last-member-query-interval** *time* 例： `Device(config)# ip igmp snooping last-member-query-interval 1000`	IGMP 脱退タイマーをグローバルに設定します。指定できる範囲は 100 ～ 32767 ミリ秒です。 デフォルトの脱退時間は 1000 ミリ秒です。 （注） IGMP 脱退タイマーをグローバルにリセットしてデフォルト設定に戻すには、 **no ip igmp snooping last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *time* 例： `Device(config)# ip igmp snooping vlan 210 last-member-query-interval 1000`	（任意）VLAN インターフェイス上で IGMP 脱退時間を設定します。有効値は 100 ～ 32767 ミリ秒です。 （注） VLAN 上に脱退時間を設定すると、グローバルに設定された内容は上書きされます。 （注） 特定の VLAN から IGMP 脱退タイマーの設定を削除するには、**no ip igmp snooping vlan** *vlan-id* **last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例：	特権 EXEC モードに戻ります。

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

IGMP スヌーピング クエリアの設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**ip igmp snooping querier** 例： `Device(config)# ip igmp snooping querier`	IGMP スヌーピング クエリアをイネーブルにします。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**ip igmp snooping querier address** *ip_address* 例： `Device(config)# ip igmp snooping querier address 172.16.24.1`	（任意）IGMP スヌーピング クエリアの IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。 （注） IGMP スヌーピングクエリアがデバイス上で IP アドレスを検出できない場合、IGMP 一般クエリを生成しません。

	コマンドまたはアクション	目的
ステップ 5	**ip igmp snooping querier query-interval** *interval-count* 例： `Device(config)# ip igmp snooping querier query-interval 30`	（任意）IGMP クエリアの間隔を設定します。指定できる範囲は 1 ～ 18000 秒です。
ステップ 6	**ip igmp snooping querier tcn query** [**count** *count* | **interval** *interval*] 例： `Device(config)# ip igmp snooping querier tcn query interval 20`	（任意）トポロジ変更通知（TCN）クエリーの間隔を設定します。指定できる count の範囲は 1 ～ 10 です。指定できる interval の範囲は 1 ～ 255 秒です。
ステップ 7	**ip igmp snooping querier timer expiry** *timeout* 例： `Device(config)# ip igmp snooping querier timer expiry 180`	（任意）IGMP クエリアが期限切れになる時間を設定します。指定できる範囲は 60 ～ 300 秒です。
ステップ 8	**ip igmp snooping querier version** *version* 例： `Device(config)# ip igmp snooping querier version 2`	（任意）クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show ip igmp snooping vlan** *vlan-id* 例： `Device# show ip igmp snooping vlan 30`	（任意）VLAN インターフェイス上で IGMP スヌーピング クエリアがイネーブルになっていることを確認します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP レポート抑制のディセーブル化

IGMP レポート抑制をディセーブルにするには、次の手順を実行します。

手順

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

IGMP プロファイルの設定

IGMP プロファイルを作成するには、次の手順を実行します。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip igmp profile** *profile number* 例： `Device(config)# ip igmp profile 3`	設定するプロファイルに番号を割り当て、IGMP プロファイル コンフィギュレーション モードを開始します。指定できるプロファイル番号の範囲は 1 ～ 4294967295 です。IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。 • **deny**：一致するアドレスを拒否します。デフォルトで設定されています。 • **exit**：IGMP プロファイル コンフィギュレーション モードを終了します。 • **no**：コマンドを否定するか、または設定をデフォルトに戻します。 • **permit**：一致するアドレスを許可するように指定します。 • **range**：プロファイルの IP アドレスの範囲を指定します。単一の IP アドレス、または開始アドレスと終了アドレスで指定された IP アドレス範囲を入力できます。

	コマンドまたはアクション	目的
		デフォルトでは、デバイスにはIGMPプロファイルが設定されていません。 （注） プロファイルを削除するには、**no ip igmp profile** *profile number* グローバル コンフィギュレーション コマンドを使用します。
ステップ 4	**permit** | **deny** 例： `Device(config-igmp-profile)# permit`	（任意）IP マルチキャスト アドレスへのアクセスを許可または拒否するアクションを設定します。アクションを設定しないと、プロファイルのデフォルト設定はアクセス拒否になります。
ステップ 5	**range** *ip multicast address* 例： `Device(config-igmp-profile)# range 229.9.9.0`	アクセスを制御する IP マルチキャスト アドレスまたは IP マルチキャスト アドレスの範囲を入力します。範囲を入力する場合は、IP マルチキャスト アドレスの下限値、スペースを 1 つ、IP マルチキャスト アドレスの上限値を入力します。 **range** コマンドを複数回入力し、複数のアドレスまたはアドレス範囲を入力できます。 （注） IP マルチキャストアドレスまたはIP マルチキャストアドレス範囲を削除するには、**no range** *ip multicast address* IGMP プロファイル コンフィギュレーション コマンドを使用します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip igmp profile** *profile number* 例： `Device# show ip igmp profile 3`	プロファイルの設定を確認します。
ステップ 8	**show running-config** 例：	入力を確認します。

	コマンドまたはアクション	目的
	`Device# show running-config`	
ステップ 9	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP プロファイルの適用

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

スイッチ ポートに IGMP プロファイルを適用するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポート グループに所属していないレイヤ 2 ポートでなければなりません。
ステップ 4	**ip igmp filter** *profile number* 例： `Device(config-if)# ip igmp filter 321`	インターフェイスに指定された IGMP プロファイルを適用します。指定できる範囲は 1 ～ 4294967295 です。

	コマンドまたはアクション	目的
		（注） インターフェイスからプロファイルを削除するには、 **no ip igmp filter***profile number* インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP グループの最大数の設定

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

始める前に

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

手順

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

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/2`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポート グループに所属しないレイヤ 2 ポート、または EtherChannel インターフェイスのいずれかにできます。
ステップ 4	**ip igmp max-groups** *number* 例： `Device(config-if)# ip igmp max-groups 20`	インターフェイスが加入できる IGMP グループの最大数を設定します。指定できる範囲は 0 ～ 4294967294 です。デフォルトでは最大数は設定されません。 （注） グループの最大数に関する制限を削除し、デフォルト設定（制限なし）に戻すには、**no ip igmp max-groups** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id* 例： `Device# show running-config interface gigabitethernet1/0/1`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP スロットリング アクションの設定

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

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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポート グループに所属しないレイヤ 2 ポート、または EtherChannel インターフェイスのいずれかにできます。トランク ポートをインターフェイスにすることはできません。
ステップ 4	**ip igmp max-groups action** {**deny** | **replace**} 例： `Device(config-if)# ip igmp max-groups action replace`	インターフェイスが IGMP レポートを受信したときに、転送テーブルに最大数のエントリが登録されている場合は、次のいずれかのアクションをインターフェイスに指定します。 • **deny**：レポートを破棄します。このスロットリング アクションを設定すると、すでに転送テーブルに登録されていたエントリは、削除されることはありませんが期限切れになります。エントリが期限切れになり、最大数のエントリが転送テーブルに登録されていると、デバイスは、インターフェイスで受信した次の IGMP レポートを廃棄します。 • **replace**：既存のグループを、IGMP レポートを受信した新しいグループで上書きします。このスロットリング アクションを設定すると、すでに転送テーブルに登録されていたエントリは削除されます。転送テーブルのエントリが最大数まで達したら、デバイスはランダムに選択した

	コマンドまたはアクション	目的
		エントリを受信したIGMP レポートで上書きします。 デバイスが転送テーブルのエントリを削除しないようにするには、インターフェイスにより転送テーブルにエントリが追加される前に、IGMP スロットリングアクションを設定します。 （注） レポートの廃棄というデフォルトのアクションに戻すには、**no ip igmp max-groups action** インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id* 例： `Device(config)# show running-config interface gigabitethernet 1/0/1`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP スヌーピングのモニタリング

IGMP スヌーピング情報の監視

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

表 *5: IGMP* スヌーピング情報を表示するためのコマンド

コマンド	目的
show ip igmp snooping [**vlan** *vlan-id* [detail]]	デバイス上のすべての VLAN または特定の VLAN のスヌーピング設定情報を表示します。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ip igmp snooping groups [**count** | **vlan** *vlan-id*]	デバイスまたは特定のパラメータに関して、マルチキャストテーブル情報を表示します。 • **count**：実エントリの代わりに、指定のコマンドオプションのエントリ総数を表示します。 • *vlan-id*：VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ip igmp snooping mrouter [**vlan** *vlan-id*]	ダイナミックに学習され、手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。 （注） IGMP スヌーピングを有効にすると、デバイスはマルチキャストルータの接続先インターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。 （オプション）**vlan** *vlan-id* を入力すると、特定の VLAN に関する情報が表示されます。
show ip igmp snooping querier [**vlan** *vlan-id*] **detail**	IP アドレスおよび VLAN で受信した最新の IGMP クエリーメッセージの受信ポートに関する情報、VLAN の IGMP スヌーピング クエリアの設定および動作ステートに関する情報を表示します。

IGMP フィルタリングのモニタリング

IGMP プロファイルの特性を表示したり、デバイス上のすべてのインターフェイスまたは指定されたインターフェイスの IGMP プロファイルや最大グループ設定を表示したりできます。

表 *6 : IGMP* フィルタリングの表示コマンド

コマンド	目的
show ip igmp profile [*profile number*]	特定の IGMP プロファイルまたはデバイス上で定義されているすべての IGMP プロファイルを表示します。
show running-config [**interface** *interface-id*]	インターフェイスが所属できる IGMP グループの最大数（設定されている場合）や、インターフェイスに適用される IGMP プロファイルを含む、特定のインターフェイスまたはデバイス上のすべてのインターフェイスの設定を表示します。

IGMP スヌーピングの設定例

例：マルチキャスト ルータへの静的な接続のイネーブル化

次に、マルチキャスト ルータへの静的な接続をイネーブルにする例を示します。

```
Device# configure terminal
Device# ip igmp snooping vlan 200 interface gigabitethernet 1/0/2
Device# end
```

例：グループに加入するホストの静的な設定

次に、ポート上のホストを静的に設定する例を示します。

```
Device#  configure terminal
Device#  ip igmp snooping vlan 105 static 0100.1212.0000 interface gigabitethernet 1/0/1
Device#  end
```

例：IGMP 即時脱退のイネーブル化

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

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

例：IGMP スヌーピング クエリアの送信元アドレスの設定

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

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

例：IGMP スヌーピング クエリアの最大応答時間の設定

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

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

例：IGMP スヌーピング クエリア タイムアウトの設定

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

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

例：IGMP スヌーピング クエリア機能の設定

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

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

例：IGMP プロファイルの設定

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

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

例：IGMP プロファイルの適用

次に、ポートに IGMP プロファイル 4 を適用する例を示します。

```
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# ip igmp filter 4
Device(config-if)# end
```

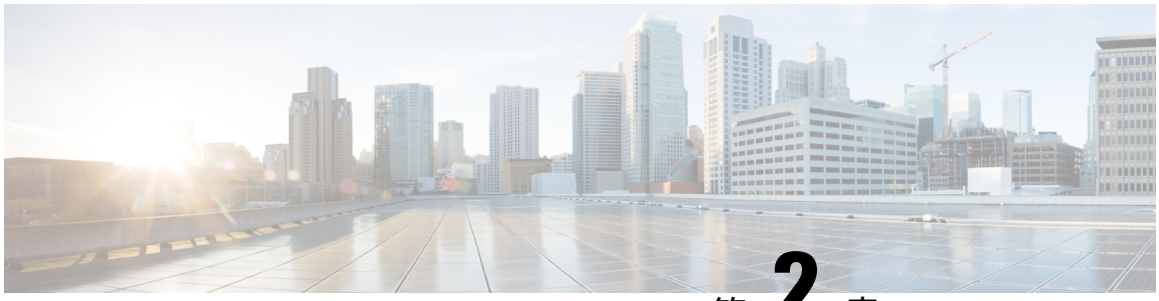
例：IGMP グループの最大数の設定

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

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip igmp max-groups 25
Device(config-if)# end
```

IGMP スヌーピングの機能履歴と情報

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	この機能が導入されました。



第 2 章

IPv6 MLD スヌーピングの設定

IPv6 MLD スヌーピングについて

スイッチ上でマルチキャストリスナー検出（MLD）スヌーピングを使用して、スイッチドネットワーク内のクライアントおよびルータに IPv6 マルチキャストデータを効率的に配信することができます。

MLD スヌーピングの概要

IPv4 では、レイヤ 2 スイッチはインターネットグループ管理プロトコル（IGMP）スヌーピングを使用して、動的にレイヤ2 インターフェイスを設定することにより、マルチキャストトラフィックのフラッディングを抑制します。そのため、マルチキャストトラフィックは IP マルチキャストデバイスに対応付けられたインターフェイスにだけ転送されます。IPv6 では、MLD スヌーピングが同様の機能を実行します。MLD スヌーピングを使用すると、IPv6 マルチキャスト データは VLAN（仮想 LAN）内のすべてのポートにフラッディングされるのではなく、データを受信するポートのリストに選択的に転送されます。このリストは、IPv6 マルチキャスト制御パケットをスヌーピングすることにより構築されます。

MLD は IPv6 マルチキャスト ルータで使用されるプロトコルで、ルータに直接接続されたリンク上のマルチキャスト リスナー（IPv6 マルチキャスト パケットを受信するノード）の存在、および隣接ノードを対象とするマルチキャスト パケットを検出します。MLD は IGMP から派生しています。MLD バージョン 1（MLDv1）は IGMPv2 と、MLD バージョン 2（MLDv2）は IGMPv3 とそれぞれ同等です。MLD は Internet Control Message Protocol バージョン 6（ICMPv6）のサブプロトコルです。MLD メッセージは ICMPv6 メッセージのサブセットで、IPv6 パケット内で先頭の Next Header 値 58 により識別されます。

スイッチは、次の 2 つのバージョンの MLD スヌーピングをサポートします。

- MLDv1 スヌーピング：MLDv1 制御パケットを検出し、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックのブリッジングを設定します。
- MLDv2 基本スヌーピング（MBSS）：MLDv2 制御パケットを使用して、IPv6 宛先マルチキャスト アドレスに基づいてトラフィックの転送を設定します。

スイッチは MLDv1 プロトコル パケットと MLDv2 プロトコル パケットの両方でスヌーピングでき、IPv6 宛先マルチキャスト アドレスに基づいて IPv6 マルチキャスト データをブリッジングします。

（注） スイッチは、IPv6 送信元および宛先マルチキャスト アドレスベースの転送を設定する MLDv2 拡張スヌーピングをサポートしません。

MLD スヌーピングは、グローバルまたは VLAN 単位でイネーブルまたはディセーブルに設定できます。MLD スヌーピングがイネーブルの場合、VLAN 単位の IPv6 マルチキャスト アドレス テーブルはソフトウェアおよびハードウェアで構築されます。その後、スイッチはハードウェアで IPv6 マルチキャストアドレスに基づくブリッジングを実行します。

MLD メッセージ

MLDv1 は、次の 3 種類のメッセージをサポートします。

- Listener Query：IGMPv2 クエリーと同等で、General Query または Mulicast-Address-Specific Query（MASQ）のいずれかになります。
- Multicast Listener Report：IGMPv2 レポートと同等です。
- Multicast Listener Done メッセージ：IGMPv2 Leave メッセージと同等です。

MLDv2 では、MLDv1 レポートおよび Done メッセージに加えて、MLDv2 クエリーおよび MLDv2 レポートもサポートします。

メッセージの送受信の結果生じるメッセージ タイマーおよびステート移行は、IGMPv2 メッセージの場合と同じです。リンクに対してローカルで有効な IPv6 送信元アドレスを持たない MLD メッセージは、MLD ルータおよび MLD スイッチで無視されます。

MLD クエリー

スイッチは MLD クエリーを送信し、IPv6 マルチキャスト アドレス データベースを構築し、MLD グループ固有クエリー、MLD グループおよび送信元固有クエリーを生成して、MLD Done メッセージに応答します。また、スイッチはレポート抑制、レポート プロキシング、即時脱退機能、およびスタティックな IPv6 マルチキャスト グループ アドレス設定もサポートします。

MLD スヌーピングがディセーブルの場合、すべての MLD クエリーが入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合、受信された MLD クエリーが入力 VLAN でフラッディングされ、クエリーのコピーは CPU に送信され、処理されます。MLD スヌーピングでは、受信されたクエリーから IPv6 マルチキャスト アドレス データベースを構築します。MLD スヌーピングは、マルチキャスト ルータ ポートを検出して、タイマーを維持し、レポート応答時間を設定します。また、VLAN のクエリア IP 送信元アドレス、VLAN 内のクエリア ポートを学習して、マルチキャスト アドレス エージングを維持します。

（注） IPv6 マルチキャスト ルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、Catalyst 2960、2960-S、2960-C、2960-X、または 2960-CX スイッチが VLAN 上でクエリを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。

グループが MLD スヌーピング データベースに存在する場合、スイッチは MLDv1 レポートを送信して、グループ固有のクエリーに応答します。このグループが不明の場合、グループ固有のクエリーは入力 VLAN にフラッディングされます。

ホストがマルチキャスト グループから脱退する場合、MLD Done メッセージ（IGMP Leave メッセージと同等）を送信できます。スイッチが MLDv1 Done メッセージを受信した際に、即時脱退がイネーブルでなければ、スイッチは メッセージを受信したポートに MASQ を送信して、ポートに接続する他のデバイスがマルチキャスト グループに残る必要があるかどうか判別します。

マルチキャスト クライアント エージングの堅牢性

クエリー数に基づいて、アドレスからのポート メンバーシップの削除を設定できます。1 つのアドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対するレポートがない場合のみです。デフォルトの回数は 2 回です。

マルチキャスト ルータ検出

IGMP スヌーピングと同様に、MLD スヌーピングでは次の特性を持つマルチキャスト ルータ検出を行います。

- ユーザにより設定されたポートには、期限切れがありません。
- ダイナミックなポート学習は、MLDv1 スヌーピング クエリーおよび IPv6 PIMv2 パケットにより行われます。
- 複数のルータが同じレイヤ 2 インターフェイス上にある場合、MLD スヌーピングではポート上の単一のマルチキャスト ルータ（直前にルータ制御パケットを送信したルータ）を追跡します。

- マルチキャスト ルータ ポートのダイナミックなエージングは、デフォルト タイマーの 5 分に基づきます。ポート上で制御パケットが 5 分間受信されない場合、マルチキャスト ルータはルータのポート リストから削除されます。
- IPv6 マルチキャスト ルータ検出が実行されるのは、MLD スヌーピングがスイッチでイネーブルの場合のみです。
- 受信された IPv6 マルチキャスト ルータ制御パケットは、スイッチで MLD スヌーピングがイネーブルかどうかにかかわらず、常に入力 VLAN にフラッディングされます。
- 最初の IPv6 マルチキャスト ルータ ポートが検出された後は、不明の IPv6 マルチキャスト データは、検出されたルータ ポートに対してのみ転送されます（それまでは、すべての IPv6 マルチキャスト データは入力 VLAN にフラッディングされます）。

MLD レポート

MLDv1 join メッセージは、本質的には IGMPv2 と同じように処理されます。IPv6 マルチキャスト ルータが VLAN で検出されない場合は、レポートが処理されないか、またはスイッチから転送されません。IPv6 マルチキャスト ルータが検出され、MLDv1 レポートが受信されると、IPv6 マルチキャスト グループ アドレスが VLAN の MLD データベースに入力されます。その後、VLAN 内のグループに対するすべての IPv6 マルチキャスト トラフィックが、このアドレスを使用して転送されます。MLD スヌーピングがディセーブルの場合、レポートは入力 VLAN でフラッディングされます。

MLD スヌーピングがイネーブルの場合は、MLD レポート抑制（リスナー メッセージ抑制）は自動的にイネーブルになります。レポート抑制により、スイッチはグループで受信された最初の MLDv1 レポートを IPv6 マルチキャスト ルータに転送します。グループのそれ以降のレポートはルータに送信されません。MLD スヌーピングがディセーブルの場合は、レポート抑制がディセーブルになり、すべての MLDv1 レポートは入力 VLAN にフラッディングされます。

スイッチは、MLDv1 プロキシ レポーティングもサポートします。MLDv1 MASQ が受信されると、スイッチに他のポートのグループが存在する場合、およびクエリーを受信したポートとアドレスの最後のメンバ ポートが異なる場合は、スイッチはクエリーを受信したアドレスに関する MLDv1 レポートで応答します。

MLD Done メッセージおよび即時脱退

即時脱退機能がイネーブルの場合にホストが MLDv1 Done メッセージ（IGMP Leave メッセージと同等）を送信すると、Done メッセージを受信したポートはグループからただちに削除されます。VLAN で即時脱退をイネーブルにする場合は（IGMP スヌーピングと同様に）、ポートに単一のホストが接続されている VLAN でのみこの機能を使用します。ポートがグループの最後のメンバである場合、グループも削除され、検出された IPv6 マルチキャスト ルータに脱退情報が転送されます。

VLAN で即時脱退がイネーブルでない場合に（1 つのポート上にグループのクライアントが複数ある場合）、Done メッセージがポートで受信されると、このポートで MASQ が生成されます。ユーザは、既存アドレスのポート メンバーシップが削除される時期を MASQ 数の観点か

ら制御できます。アドレスに対するメンバーシップからポートが削除されるのは、設定された数のクエリーに関してポート上のアドレスに対する MLDv1 レポートがない場合です。

生成される MASQ 数は、 **ipv6 mld snooping last-listener-query count** グローバル コンフィギュレーション コマンドにより設定されます。デフォルトの回数は 2 回です。

MASQ は、Done メッセージが送信された IPv6 マルチキャスト アドレスに送信されます。スイッチの最大応答時間内に MASQ で指定された IPv6 マルチキャスト アドレスにレポートが送信されなければ、MASQ が送信されたポートは IPv6 マルチキャスト アドレス データベースから削除されます。最大応答時間は、 **ipv6 mld snooping last-listener-query-interval** グローバル コンフィギュレーション コマンドにより設定します。削除されたポートがマルチキャスト アドレスの最後のメンバである場合は、マルチキャストアドレスも削除され、スイッチは検出されたマルチキャスト ルータすべてにアドレス脱退情報を送信します。

TCN 処理

ipv6 mld snooping tcn query solicit グローバル コンフィギュレーション コマンドを使用して、トポロジ変更通知（TCN）送信要求を有効にすると、MLDv1 スヌーピングは、設定された数の MLDv1 クエリによりすべての IPv6 マルチキャストトラフィックをフラッディングするよう VLAN に設定してから、選択されたポートにのみマルチキャストデータの送信を開始します。この値は、**ipv6 mld snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用して設定します。デフォルトでは、2 つのクエリーが送信されます。スイッチが VLAN 内の STP ルートになる場合、またはスイッチがユーザにより設定された場合は、リンクに対してローカルで有効な IPv6 送信元アドレスを持つ MLDv1 グローバル Done メッセージも生成されます。これは IGMP スヌーピングの場合と同じです。

MLD スヌーピングのデフォルト設定

表 *7: MLD* スヌーピングのデフォルト設定

機能	デフォルト設定
MLD スヌーピング（グローバル）	無効
MLD スヌーピング（VLAN 単位）	イネーブルVLAN MLD スヌーピングが実行されるためには、MLD スヌーピングがグローバルにイネーブルである必要があります。
IPv6 マルチキャスト アドレス	未設定
IPv6 マルチキャスト ルータ ポート	未設定
MLD スヌーピング即時脱退	無効

機能	デフォルト設定
MLD スヌーピングの堅牢性変数	グローバル：2、VLAN 単位：0 （注） VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリー カウント	グローバル：2、VLAN 単位：0 （注） VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバル数を使用します。
最後のリスナー クエリーインターバル	グローバル：1000（1 秒）、VLAN：0 （注） VLAN 値はグローバル設定を上書きします。VLAN 値が 0 の場合、VLAN はグローバルのインターバルを使用します。
TCN クエリー送信請求	無効
TCN クエリカウント	2
MLD リスナー抑制	有効

IPv6 MLD スヌーピングの設定方法

MLD スヌーピング設定時の注意事項

MLD スヌーピングの設定時は、次の注意事項に従ってください。

- MLD スヌーピングの特性はいつでも設定できますが、設定を有効にする場合は、 **ipv6 mld snooping** グローバル コンフィギュレーション コマンドを使用して MLD スヌーピングをグローバルにイネーブルにする必要があります。
- IPv6 マルチキャストルータが Catalyst 6500 スイッチであり、拡張 VLAN（範囲 1006 ～ 4094）を使用する場合、スイッチが VLAN 上でクエリを受信できるようにするため、IPv6 MLD スヌーピングを Catalyst6500 スイッチの拡張 VLAN でイネーブルにする必要があります。標準範囲 VLAN（1 ～ 1005）の場合、IPv6 MLD スヌーピングを Catalyst 6500 スイッチの VLAN でイネーブルにする必要はありません。
- MLD スヌーピングと IGMP スヌーピングは相互に独立して動作します。スイッチで両方の機能を同時にイネーブルにできます。
- スイッチで許容されるアドレス エントリの最大値は 1000 です。

スイッチでのIPv6MLDスヌーピングのイネーブル化またはディセーブル化

デフォルトでは、IPv6 MLD スヌーピングはスイッチではグローバルにディセーブルで、すべての VLAN ではイネーブルです。MLD スヌーピングがグローバルにディセーブルの場合は、すべての VLAN でもディセーブルです。MLD スヌーピングをグローバルにイネーブルにすると、VLAN 設定はグローバル設定を上書きします。つまり、MLD スヌーピングはデフォルトステート（イネーブル）の VLAN インターフェイスでのみイネーブルになります。

VLAN 単位または VLAN 範囲で MLD スヌーピングをイネーブルおよびディセーブルにできますが、MLD スヌーピングをグローバルにディセーブルにした場合は、すべての VLAN でディセーブルになります。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

デバイスで MLD スヌーピングをグローバルにイネーブルにするには、ユーザ EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 mld snooping** 例： `Device(config)# ipv6 mld snooping`	スイッチで MLD スヌーピングをイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： `Device(config)# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
ステップ 6	**reload** 例： `Device(config)# reload`	OS（オペレーティング システム）をリロードします。

VLAN に対する IPv6 MLD スヌーピングのイネーブル化またはディセーブル化

VLAN で IPv6 MLD スヌーピングをイネーブルにするには、ユーザ EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 mld snooping** 例： `Device(config)# ipv6 mld snooping`	スイッチで MLD スヌーピングをイネーブルにします。
ステップ 4	**ipv6 mld snooping vlan** *vlan-id* 例： `Device(config)# ipv6 mld snooping vlan1`	VLAN で MLD スヌーピングをイネーブルにします。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 （注） VLAN スヌーピングをイネーブルにするには、MLD スヌーピングがグローバルにイネーブルである必要があります。
ステップ 5	**end** 例： `Device(config)# ipv6 mld snooping vlan1`	特権 EXEC モードに戻ります。

スタティックなマルチキャスト グループの設定

ホストまたはレイヤ 2 ポートは、通常マルチキャスト グループにダイナミックに加入しますが、VLAN に IPv6 マルチキャスト アドレスおよびメンバ ポートをスタティックに設定することもできます。

マルチキャストグループのメンバとしてレイヤ 2 ポートを追加するには、ユーザ EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 mld snooping vlan** *vlan-id* **static** *mac_address* **interface** *interface-id* 例： `Device(config)# ipv6 mld snooping vlan 1 static 3333.0000.1111 interface gigabitethernet 1/0/1`	マルチキャスト グループのメンバとしてレイヤ 2 ポートにマルチキャスト グループを設定します。 • *vlan-id* は、マルチキャスト グループの VLAN ID です。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • *mac_address* は、グループ MAC アドレスです。 • *interface-id* は、メンバ ポートです。物理インターフェイスまたはポート チャネルに設定できます。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	次のいずれかを使用します。 • **show ipv6 mld snooping address** • **show ipv6 mld snooping address vlan** *vlan-id* 例：	スタティック メンバ ポートおよび IPv6 アドレスを確認します。

	コマンドまたはアクション	目的

	`Device# show ipv6 mld snooping address`
	
	または
	`Device# show ipv6 mld snooping vlan 1`	

IPv6 MLD スヌーピング即時脱退のイネーブル化

MLDv1 即時脱退をイネーブルにするには、ユーザ EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 mld snooping vlan** *vlan-id* **immediate-leave** 例： `Device(config)# ipv6 mld snooping vlan 1 immediate-leave`	VLAN インターフェイスで MLD 即時脱退をイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 mld snooping vlan** *vlan-id* 例： `Device# show ipv6 mld snooping vlan 1`	VLANインターフェイス上で即時脱退がイネーブルになっていることを確認します。

IPv6 MLD スヌーピングクエリの設定

スイッチまたは VLAN に MLD スヌーピングクエリの特性を設定するには、ユーザ EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 mld snooping robustness-variable** *value* 例： `Device(config)# ipv6 mld snooping robustness-variable 3`	（任意）スイッチが一般クエリーに応答しないリスナー（ポート）を削除する前に、送信されるクエリー数を設定します。指定できる範囲は 1 ～ 3 です。デフォルトは 2 です。
ステップ 4	**ipv6 mld snooping vlan** *vlan-id* **robustness-variable** *value* 例： `Device(config)# ipv6 mld snooping vlan 1 robustness-variable 3`	（任意）VLAN 単位でロバストネス変数を設定します。これにより、MLD レポート応答がない場合にマルチキャストアドレスがエージングアウトされるまでに、MLD スヌーピングが送信する一般クエリー数が決定されます。指定できる範囲は 1 ～ 3 です。デフォルトは 0 です。0 に設定すると、使用される数はグローバルな堅牢性変数の値になります。
ステップ 5	**ipv6 mld snooping last-listener-query-count** *count* 例： `Device(config)# ipv6 mld snooping last-listener-query-count 7`	（任意）MLD クライアントがエージングアウトされる前にスイッチが送信する MASQ 数を設定します。指定できる範囲は 1 ～ 7 です。デフォルトは 2 です。クエリーは 1 秒後に送信されます。
ステップ 6	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-count** *count* 例： `Device(config)# ipv6 mld snooping vlan 1 last-listener-query-count 7`	（任意）VLAN 単位でラスト リスナー クエリー カウントを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は 1 ～ 7 です。デフォルトは 0 です。0 に設定すると、グローバルなカウント値が使用されます。クエリーは 1秒後に送信されます。

	コマンドまたはアクション	目的
ステップ 7	**ipv6 mld snooping last-listener-query-interval** *interval* 例： `Device(config)# ipv6 mld snooping last-listener-query-interval 2000`	（任意）スイッチがMASQを送信したあと、マルチキャスト グループからポートを削除するまで待機する最大応答時間を設定します。指定できる範囲は、100 ～ 32,768 ミリ秒です。デフォルト値は 1000（1 秒）です。
ステップ 8	**ipv6 mld snooping vlan** *vlan-id* **last-listener-query-interval** *interval* 例： `Device(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 2000`	（任意）VLAN 単位で last-listener クエリーインターバルを設定します。この値はグローバルに設定された値を上書きします。指定できる範囲は、0 ～ 32,768 ミリ秒です。デフォルトは 0 です。0 に設定すると、グローバルな最後のリスナー クエリーインターバルが使用されます。
ステップ 9	**ipv6 mld snooping tcn query solicit** 例： `Device(config)# ipv6 mld snooping tcn query solicit`	（任意）トポロジ変更通知（TCN）をイネーブルにします。これにより、VLAN は設定された数のクエリーに関する IPv6 マルチキャスト トラフィックすべてをフラッディングしてから、マルチキャストデータをマルチキャストデータの受信を要求するポートに対してのみ送信します。デフォルトでは、TCNはディセーブルに設定されています。
ステップ 10	**ipv6 mld snooping tcn flood query count** *count* 例： `Device(config)# ipv6 mld snooping tcn flood query count 5`	（任意）TCNがイネーブルの場合、送信される TCN クエリー数を指定します。指定できる範囲は 1 ～ 10 で、デフォルトは 2 です。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show ipv6 mld snooping querier** [**vlan** *vlan-id*] 例： `Device(config)# show ipv6 mld snooping querier vlan 1`	（任意）スイッチまたはVLANのMLDスヌーピング クエリア情報を確認します。

IPv6 MLD スヌーピング リスナー メッセージ抑制のディセーブル化

デフォルトでは、MLD スヌーピング リスナー メッセージ抑制はイネーブルに設定されています。この機能がイネーブルの場合、スイッチはマルチキャスト ルータ クエリーごとに 1 つの MLD レポートのみを転送します。メッセージ抑制がディセーブルの場合は、複数のマルチキャスト ルータに MLD レポートが転送されます。

MLD リスナーメッセージ抑制をディセーブルにするには、ユーザ EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ipv6 mld snooping listener-message-suppression** 例： `Device(config)# no ipv6 mld snooping listener-message-suppression`	MLD メッセージ抑制をディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 mld snooping** 例： `Device# show ipv6 mld snooping`	IPv6 MLD スヌーピング レポート抑制がディセーブルであることを確認します。

IPv6 MLD スヌーピング情報の表示

ダイナミックに学習された、あるいはスタティックに設定されたルータ ポートおよび VLAN インターフェイスの MLD スヌーピング情報を表示できます。また、MLD スヌーピング用に設定された VLAN の IPv6 グループ アドレス マルチキャスト エントリを表示することもできます。

表 *8 : MLD* スヌーピング情報表示用のコマンド

コマンド	目的
show ipv6 mld snooping [**vlan** *vlan-id*]	スイッチのすべての VLAN または指定された VLAN の MLD スヌーピング設定情報を表示します。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping mrouter [**vlan** *vlan-id*]	ダイナミックに学習され、手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。MLD スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先であるインターフェイスを自動的に学習します。これらのインターフェイスは動的に学習されます。 （任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping querier [**vlan** *vlan-id*]	VLAN 内で直前に受信した MLD クエリー メッセージの IPv6 アドレスおよび着信ポートに関する情報を表示します。 （任意） **vlan** *vlan-id* を入力して、単一の VLAN 情報を表示します。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ipv6 mld snooping address [**count** | **vlan** *vlan-id*]	すべての IPv6 マルチキャスト アドレス情報あるいはスイッチまたは VLAN の特定の IPv6 マルチキャスト アドレス情報を表示します。 • **count** を入力して、スイッチまたは VLAN のグループ数を表示します。 • **user** を入力して、スイッチまたは VLAN の MLD スヌーピングユーザ設定グループ情報を表示します。
show ipv6 mld snooping address vlan *vlan-id* [*ipv6-multicast-address*]	指定の VLAN および IPv6 マルチキャスト アドレスの MLD スヌーピングを表示します。

IPv6 MLD スヌーピングの設定例

例：スタティックなマルチキャストグループの設定

次の例では、スタティック IPv6 マルチキャストグループを設定する方法を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping vlan 2 static 3333.0000.1111 interface gigabitethernet
 1/0/1
Device(config)# end
```

例：MLD スヌーピングクエリの設定

次に、MLD スヌーピングのグローバルな堅牢性変数を 3 に設定する例を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping robustness-variable 3
Device(config)# exit
```

次に、VLAN の MLD スヌーピングの最後のリスナー クエリー カウントを 3 に設定する例を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping vlan 200 last-listener-query-count 3
Device(config)# exit
```

次に、MLD スヌーピングの最後のリスナー クエリー インターバル（最大応答時間）を 2000（2 秒）に設定する例を示します。

```
Device# configure terminal
Device(config)# ipv6 mld snooping last-listener-query-interval 2000
Device(config)# exit
```

例：MLD 即時脱退のイネーブル化

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

```
Device# configure terminal
Device(config)# ipv6 mld snooping vlan 130 immediate-leave
Device(config)# exit
```

IPv6 MLD スヌーピングの機能履歴と情報

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。

機能名	リリース	変更内容
IPv6 MLD スヌーピング	Cisco IOS Release 15.2(7)E3k	この機能が導入されました。