



IGMP スヌーピングおよびマルチキャスト VLAN レジストレーションの設定

- [IGMP スヌーピングおよび MVR の設定の前提条件](#) (1 ページ)
- [IGMP スヌーピングおよび MVR の設定の制約事項](#) (2 ページ)
- [IGMP スヌーピングおよび MVR に関する情報](#) (4 ページ)
- [IGMP スヌーピングおよび MVR の設定方法](#) (14 ページ)
- [IGMP スヌーピングおよび MVR のモニターリング](#) (45 ページ)
- [IGMP スヌーピングおよび MVR の設定例](#) (48 ページ)

IGMP スヌーピングおよび MVR の設定の前提条件

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 device 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、device は device 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 device 上で利用可能な IP アドレスを検出できない場合、IGMP 一般クエリーを生成しません。
- 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、IGMP スヌーピングクエリアは操作上、次の状況でディセーブル ステートになります。
 - IGMP スヌーピングが VLAN でディセーブルの場合
 - PIM が、VLAN に対応する SVI でイネーブルの場合
-
-

MVR の前提条件

マルチキャスト VLAN レジストレーション (MVR) の前提条件は次のとおりです。

- MVR を使用するには、deviceが LAN Base イメージを実行している必要があります。

IGMP スヌーピングおよび MVR の設定の制約事項

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。

- スイッチは同種スタックおよび混合スタック構成をサポートします。混合スタック構成は、Catalyst 2960-S スイッチだけでサポートされます。同種スタックは 8 つまで、混合スタックは 4 つまでのスタックメンバを持つことができます。スイッチスタック内のすべてのスイッチが LAN Base イメージを実行している必要があります。
- IGMP フィルタリングまたはマルチキャスト VLAN レジストレーション (MVR) が実行されている devices は、IGMPv3 Join および Leave メッセージをサポートしません。
- 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 device 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。

MVR の制約事項

次に、MVR の制約事項を示します。

- MVR に参加するのは、レイヤ 2 ポートだけです。ポートを MVR 受信ポートとして設定する必要があります。
- 各 device または device スタックでサポートされる MVR マルチキャスト VLAN は、1 つのみです。
- 受信ポートはアクセス ポートでなければなりません。トランク ポートにはできません。device のレシーバポートは異なる VLAN に属していてもかまいませんが、マルチキャスト VLAN に属することはできません。
- device 上で設定可能なマルチキャスト エントリ（MVR グループ アドレス）の最大数（つまり、受信可能な TV チャンネルの最大数）は、256 です。
- 送信元 VLAN で受信され、レシーバポートから脱退する MVR マルチキャストデータは、device で存続可能時間（TTL）が 1 だけ少なくなります。
- device 上の MVR は、MAC マルチキャストアドレスではなく IP マルチキャストアドレスを使用するので、device 上でエイリアス IP マルチキャストアドレスを使用できます。ただし、device が Catalyst 3550 または Catalyst 3500 XL devices と連携動作している場合は、それらの間でエイリアスとして使用される IP アドレスや予約済みの IP マルチキャストアドレス（224.0.0.xxx 範囲内）を設定する必要はありません。
- プライベート VLAN ポートに MVR を設定しないでください。
- device 上でマルチキャストルーティングがイネーブルの場合、MVR はサポートされません。MVR がイネーブルの場合に、マルチキャストルーティングおよびマルチキャストルーティング プロトコルをイネーブルにすると、MVR がディセーブルになり、警告メッセージが表示されます。マルチキャストルーティングおよびマルチキャストルーティング プロトコルがイネーブルの場合に、MVR をイネーブルにしようとする、MVR をイネーブルにする操作が取り消され、エラーメッセージが表示されます。
- MVR 受信ポートで受信した MVR データは、MVR 送信元ポートに転送されません。
- MVR は IGMPv3 メッセージをサポートしていません。

- スイッチは同種スタックおよび混合スタック構成をサポートします。混合スタック構成は、Catalyst 2960-S スイッチだけでサポートされます。同種スタックは 8 つまで、混合スタックは 4 つまでのスタックメンバを持つことができます。スイッチスタック内のすべてのスイッチが LAN Base イメージを実行している必要があります。

IGMP スヌーピングおよび MVR に関する情報

IGMP スヌーピング

レイヤ 2 devices 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ドイ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 device 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。device 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、device 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。

上に設定されたマルチキャストルータは、すべての VLAN に一般的なクエリを定期的に送信します。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。device 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。

device 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。device 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。

ポートスパンニングツリー、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

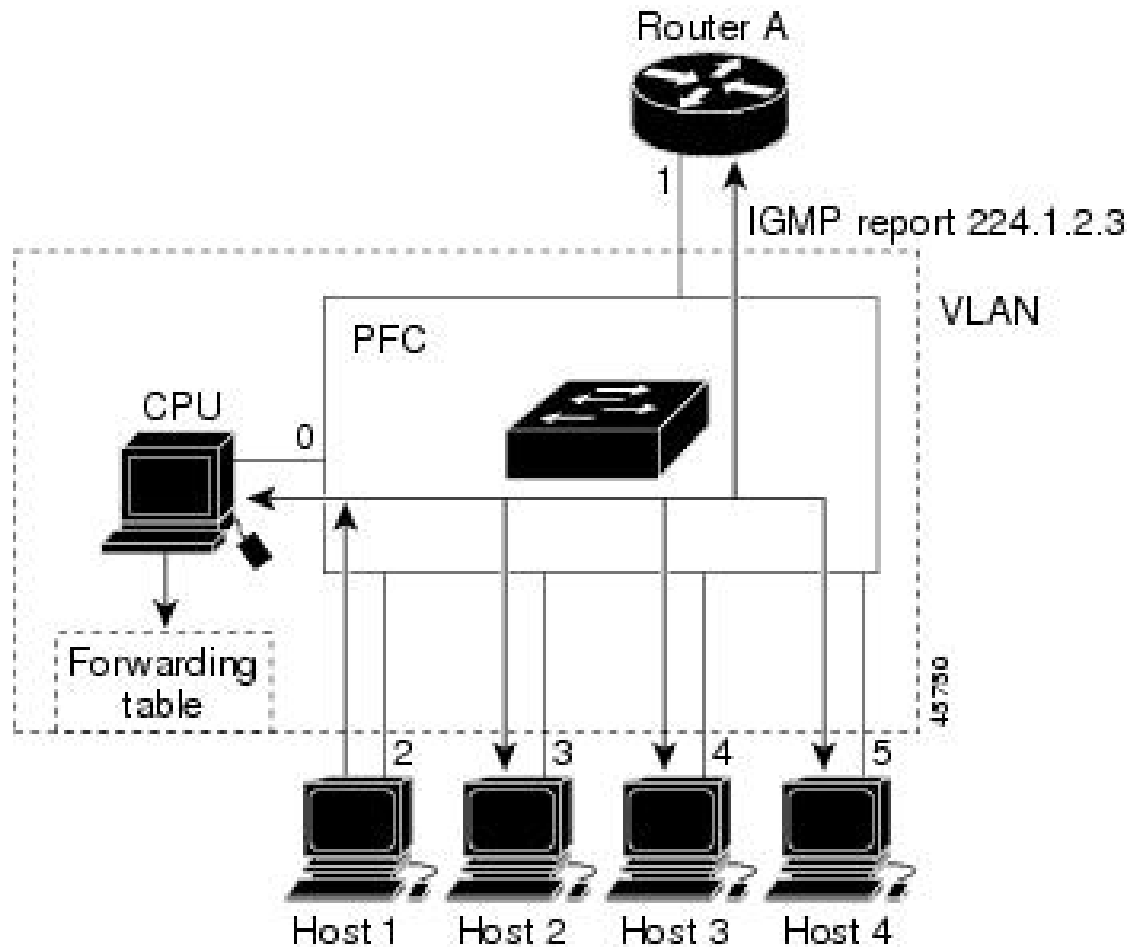
device は、IGMP バージョン1、IGMP バージョン2、およびIGMP バージョン3をサポートしています。これらバージョンは、device 上でそれぞれ相互運用できます。たとえば、IGMP スヌーピングがイネーブルになっており、クエリアのバージョンがIGMPv2で、device がホストからIGMPv3 レポートを受信している場合、device はIGMPv3 レポートをマルチキャストルータに転送できます。

IGMPv3 device は、Source Specific Multicast (SSM) 機能を実行しているデバイスとメッセージの送受信を行うことができます。

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

device 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ーを受信したdevice は、そのクエリーを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device にJoin メッセージを送信することによって応答します。device 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 device 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。device 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

device 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 アドレス宛での、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 device 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。

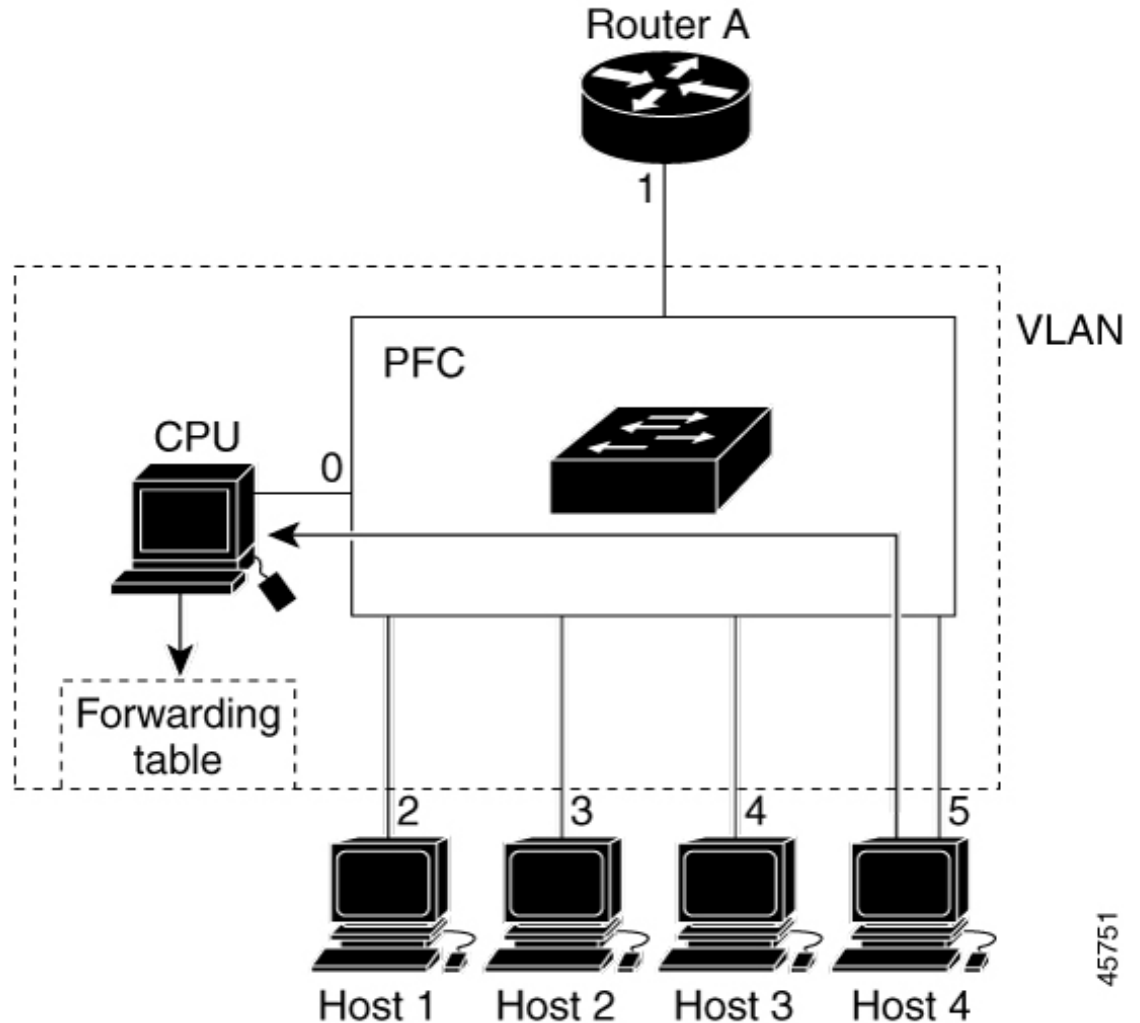


表 2:更新された IGMP スヌーピング転送テーブル

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を送信し、device 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。device 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 device は、グループ固有のクエリーを送信して、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。device 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

device は IGMP スヌーピングの即時脱退を使用して、先に device からインターフェイスにグループ固有のクエリーを送信しなくても、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 device 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ーを送信した後の device 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。

device 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、device 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べてのマルチキャストルータに送信します。device 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、device 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、device 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、device 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

マルチキャスト VLAN レジストレーション

マルチキャスト VLAN レジストレーション (MVR) は、イーサネットリングベースのサービスプロバイダネットワーク上でマルチキャストトラフィックの広範囲展開を使用するアプリケーション (サービスプロバイダネットワーク上の複数の TV チャンネルのブロードキャストなど) 用に設計されています。MVR によってポート上の加入者は、ネットワークワイドなマ

マルチキャスト VLAN 上のマルチキャスト ストリームに加入し、脱退できます。また、ネットワーク上で1つのマルチキャスト VLAN を共有しながら、加入者が別の VLAN に接続できます。MVRによって、マルチキャスト VLAN でマルチキャスト ストリームを連続送信する能力が得られますが、ストリームと加入者の VLAN は、帯域幅およびセキュリティ上の理由で分離されます。

ここでは、MVR について説明します。

MVR と IGMP



(注) device上で、MVR は IGMP スヌーピングと共存できます。

MVR では、加入者ポートが IGMP Join および Leave メッセージを送信することによって、マルチキャスト ストリームへの加入および脱退 (Join および Leave) を行うことが前提です。これらのメッセージは、イーサネットに接続され、IGMP バージョン 2 に準拠しているホストから発信できます。MVR は IGMP スヌーピングの基本メソッドで動作しますが、この2つの機能はそれぞれ単独で動作します。それぞれ他方の機能の動作に影響を与えずに、イネーブルまたはディセーブルにできます。ただし、IGMP スヌーピングと MVR が両方ともイネーブルの場合、MVR は MVR 環境で設定されたマルチキャスト グループが送信した Join および Leave メッセージだけに反応します。他のマルチキャスト グループから送信された Join および Leave メッセージはすべて、IGMP スヌーピングが管理します。

device の CPU は、MVR IP マルチキャスト ストリームとそれに対応する device 転送テーブル内の IP マルチキャスト グループを識別し、IGMP メッセージを代行受信し、転送テーブルを変更して、マルチキャスト ストリームの受信側としての加入者を追加または削除します。受信側が送信元と異なる VLAN 上に存在している場合でも同じです。この転送動作により、異なる VLAN の間でトラフィックを選択して伝送できます。

動作モード

device の MVR 動作は、互換モードまたはダイナミックモードに設定できます。

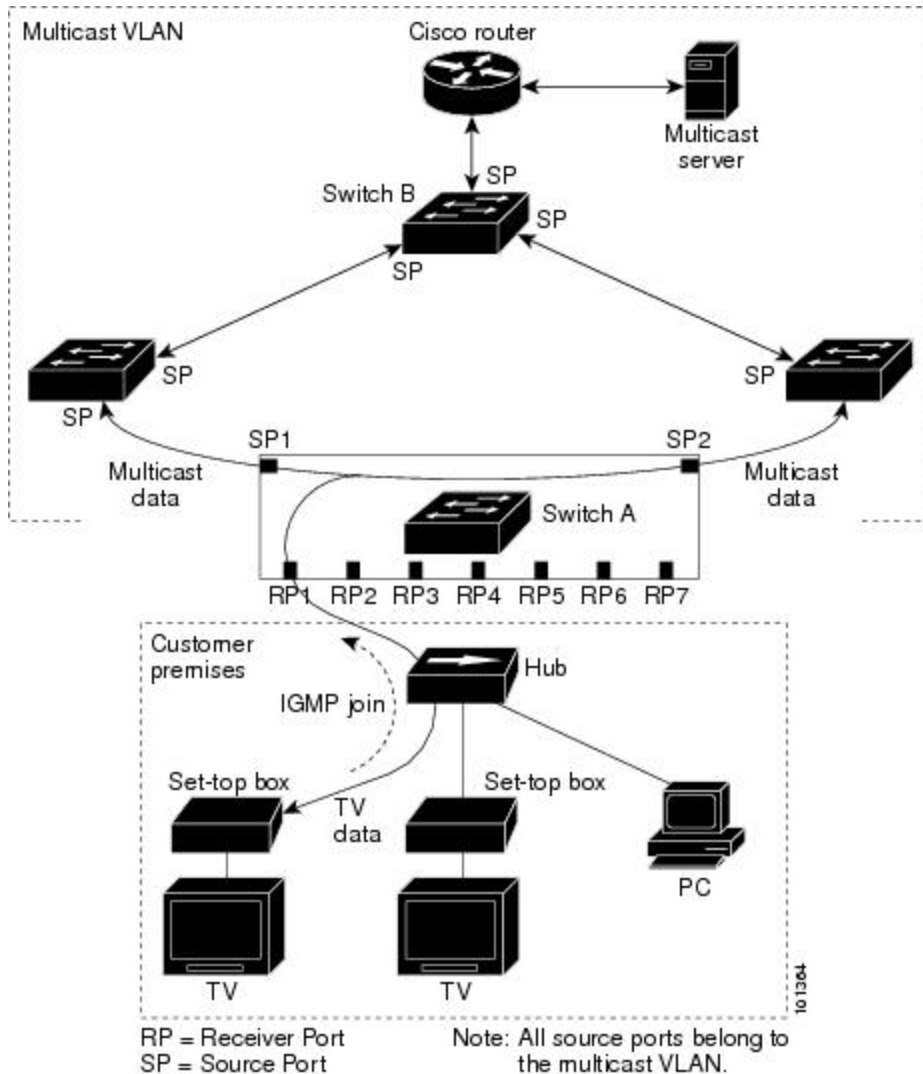
- 互換モードの場合、MVR ホストが受信したマルチキャスト データはすべての MVR データポートに転送されます。MVR データポートの MVR ホストメンバーシップは無関係です。マルチキャスト データは、IGMP レポートまたは静的な MVR 設定のどちらかによって、MVR ホストが加入しているレシーバポートだけに転送されます。MVR ホストから受信した IGMP レポートが、device に設定された MVR データポートから転送されることはありません。
- ダイナミックモードの場合、device 上の MVR ホストが受信したマルチキャスト データは、IGMP レポートまたは静的な MVR 設定のどちらかによって、MVR ホストが加入している MVR データおよびクライアントポートから転送されます。それ以外のポートからは転送されません。MVR ホストから受信した IGMP レポートも、ホストのすべての MVR データポートから転送されます。したがって、互換モードで device を稼働させた場合と異なり、MVR データポートリンクで不要な帯域幅を使用しなくて済みます。

マルチキャスト TV アプリケーションでの MVR

マルチキャスト TV アプリケーションでは、PC またはセットトップボックスを装備したテレビでマルチキャストストリームを受信できます。1つのサブスライバポートに複数のセットトップボックスまたはPCを接続できます。サブスライバポートは、MVR受信ポートとして設定された device ポートです。

図 3: マルチキャスト VLAN レジストレーションの例

次に、設定例を示します。



この設定例では、Dynamic Host Configuration Protocol (DHCP) によって、セットトップボックスまたはPCにIPアドレスが割り当てられます。加入者がチャンネルを選択すると、適切なマルチキャストに参加するために、セットトップボックスまたはPCからスイッチAにIGMPレポートが送信されます。IGMPレポートが設定済みのIPマルチキャストグループアドレスのいずれかに一致する場合、device CPUは、この受信ポートおよびVLANが指定のマルチキャストストリームの転送先として含まれるように、マルチキャストVLANからマルチキャスト

ストリームを受信した際に、ハードウェア アドレス テーブルを変更します。マルチキャスト VLAN との間でマルチキャスト データを送受信するアップリンク ポートを、MVR 送信元ポートと呼びます。

加入者がチャンネルを切り替えた場合、またはテレビのスイッチを切った場合には、セットトップボックスからマルチキャストストリームに対する IGMP Leave メッセージが送信されます。device CPU は、受信ポートの VLAN 経由で MAC ベースの一般クエリを送信します。VLAN に、このグループに加入している別のセットトップボックスがある場合、そのセットトップボックスはクエリに指定された最大応答時間内に応答しなければなりません。応答を受信しなかった場合、CPU はこのグループの転送先としての受信ポートを除外します。

即時脱退機能を使用しない場合、受信ポートのサブスクリバから IGMP Leave メッセージを受信した device は、そのポートに IGMP クエリを送信し、IGMP グループ メンバーシップ レポートを待ちます。設定された時間内にレポートを受信しなかった場合は、受信ポートがマルチキャスト グループ メンバーシップから削除されます。即時脱退機能がイネーブルの場合、IGMP Leave を受信したレシーバポートから IGMP クエリが送信されません。Leave メッセージの受信後ただちに、受信ポートがマルチキャスト グループ メンバーシップから削除されるので、脱退遅延時間が短縮されます。即時脱退機能をイネーブルにするのは、接続されているレシーバ デバイスが 1 つだけのレシーバポートに限定してください。

MVR を使用すると、各 VLAN の加入者に対してテレビチャンネルのマルチキャストトラフィックを重複して送信する必要がなくなります。すべてのチャンネル用のマルチキャストトラフィックは、マルチキャスト VLAN 上でのみ、VLAN トランクに 1 回だけ送信されます。IGMP Leave および Join メッセージは、加入者ポートが割り当てられている VLAN で送信されます。これらのメッセージは、レイヤ 3 デバイス上のマルチキャスト VLAN のマルチキャストトラフィック ストリームに対し、動的に登録します。アクセス レイヤ device (スイッチ A) は、マルチキャスト VLAN から別の VLAN 内の加入者ポートにトラフィックが転送されるよう転送動作を変更し、2 つの VLAN 間で選択的にトラフィックが送信されるようにします。

IGMP レポートは、マルチキャストデータと同じ IP マルチキャスト グループ アドレスに送信されます。スイッチ A の CPU は、レシーバポートから送られたすべての IGMP Join および Leave メッセージを取り込み、MVR モードに基づいて、送信元 (アップリンク) ポートのマルチキャスト VLAN に転送しなければなりません。

MVR のデフォルト設定

表 4: MVR のデフォルト設定

機能	デフォルト設定
MVR	グローバルおよびインターフェイス単位でディセーブル
マルチキャスト アドレス	未設定
クエリーの応答時間	0.5 秒
マルチキャスト VLAN	VLAN 1

機能	デフォルト設定
モード	compatible
インターフェイスのデフォルト（ポート単位）	受信ポートでも送信元ポートでもない
即時脱退	すべてのポートでディセーブル

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、device ポート上のユーザー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、device ポート上でユーザー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 device 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 device 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 devices 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、device 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 5: 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。
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 スヌーピングおよび MVR の設定方法

デバイス

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。

device 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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping**
4. **end**
5. **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> 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 igmp snooping 例： スイッチ(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。 (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： スイッチ(config)# end	特権 EXEC モードに戻ります。
ステップ 5	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。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping vlan *vlan-id***

4. end
5. 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> 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 igmp snooping vlan <i>vlan-id</i> 例： スイッチ(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。 (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 <i>vlan-id</i> 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： スイッチ(config)# end	特権 EXEC モードに戻ります。
ステップ 5	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。

スヌーピング方法の設定

マルチキャスト対応のルータ ポートは、レイヤ 2 マルチキャスト エントリごとに転送テーブルに追加されます。スイッチは、次のいずれかの方法でポートを学習します。

- IGMP クエリー、Protocol-Independent Multicast (PIM) パケット、およびディスタンスベクトル マルチキャスト ルーティング プロトコル (DVMRP) パケットのスヌーピング
- 他のルータからの Cisco Group Management Protocol (CGMP) パケットのリスニング
- **ip igmp snooping mrouter** グローバル コンフィギュレーション コマンドによるマルチキャストルータポートへの静的な接続

IGMP クエリーおよび PIM パケットと DVMRP パケットのスヌーピング、または CGMP self-join パケットまたは proxy-join パケットのいずれかの待ち受けを行うように、スイッチを設定できます。デフォルトでは、スイッチはすべての VLAN 上の PIM パケットと DVMRP パケットをスヌーピングします。CGMP パケットだけでマルチキャストルータポートを学習するには、**ip igmp snooping vlan vlan-id mrouter learn cgmp** 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。このコマンドを入力すると、ルータは CGMP self-join パケットおよび CGMP proxy-join パケットだけを待ち受け、その他の CGMP パケットは待ち受けません。PIM-DVMRP パケットだけでマルチキャストルータポートを学習するには、**ip igmp snooping vlan vlan-id mrouter learn pim-dvmrp** 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。

学習方法として CGMP を使用する場合で、なおかつ VLAN に CGMP プロキシ対応のマルチキャストルータがない場合は、**ip cgmp router-only** コマンドを入力し、ルータに動的にアクセスする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping vlan vlan-id mrouter learn {cgmp | pim-dvmrp }**
4. **end**
5. **show ip igmp snooping**
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> 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
	スイッチ# <code>configure terminal</code>	
ステップ 3	ip igmp snooping vlan <i>vlan-id</i> mrouter learn {cgmp pim-dvmrp } 例： スイッチ(config)# <code>ip igmp snooping vlan 1 mrouter learn cgmp</code>	マルチキャスト ルータの学習方式を指定します。 <ul style="list-style-type: none"> • cgmp : CGMP パケットを待ち受けます。この方法は、制御トラフィックを減らす場合に有効です。 • pim-dvmrp : IGMP クエリーおよび PIM/DVMRP パケットをスヌーピングします。これはデフォルトです。 (注) デフォルトの学習方式に戻すには、 no ip igmp snooping vlan <i>vlan-id</i> mrouter learn cgmp 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： 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 ip igmp snooping 例： スイッチ# <code>show ip igmp snooping</code>	設定を確認します。
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。

マルチキャスト ルータ ポートの設定

device 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、device ポートに限りサポートされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping vlan *vlan-id* mrouter interface *interface-id***
4. **end**
5. **show ip igmp snooping mrouter [vlan *vlan-id*]**
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> 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 igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i> 例： スイッチ(config)# ip igmp snooping vlan 5 mrouter interface gigabitethernet1/0/1	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。 <ul style="list-style-type: none"> • 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 <i>vlan-id</i> mrouter interface <i>interface-id</i> 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： スイッチ(config)# end	特権 EXEC モードに戻ります。

グループに加入するホストの静的な設定

	コマンドまたはアクション	目的
ステップ 5	show ip igmp snooping mrouter [vlan <i>vlan-id</i>] 例： スイッチ# 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： 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。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping vlan *vlan-id* static *ip_address* interface *interface-id***
4. **end**
5. **show ip igmp snooping groups**
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> 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。

	コマンドまたはアクション	目的
ステップ 3	<p>ip igmp snooping vlan <i>vlan-id</i> static <i>ip_address</i> interface <i>interface-id</i></p> <p>例 :</p> <pre>スイッチ(config)# ip igmp snooping vlan 105 static 230.0.0.1 interface gigabitethernet1/0/1</pre>	<p>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。</p> <ul style="list-style-type: none"> • <i>vlan-id</i> 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。 • <i>ip-address</i> は、グループの IP アドレスです。 • <i>interface-id</i> 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 ~ 128) に設定できます。 <p>(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 <i>vlan-id</i> static <i>mac-address</i> interface <i>interface-id</i> 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。</p>
ステップ 4	<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 5	<p>show ip igmp snooping groups</p> <p>例 :</p> <pre>スイッチ# show ip igmp snooping groups</pre>	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	<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。

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、device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、device のデフォルトバージョンです。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping vlan *vlan-id* immediate-leave**
4. **end**
5. **show ip igmp snooping vlan *vlan-id***
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： 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 igmp snooping vlan <i>vlan-id</i> immediate-leave 例： スイッチ(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 <i>vlan-id</i> 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： スイッチ(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp snooping vlan <i>vlan-id</i> 例：	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。

	コマンドまたはアクション	目的
	スイッチ# <code>show ip igmp snooping vlan 21</code>	
ステップ 6	end 例： スイッチ(config)# <code>end</code>	特権 EXEC モードに戻ります。

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。

手順の概要

1. `enable`
2. `configure terminal`
3. `ip igmp snooping last-member-query-interval time`
4. `ip igmp snooping vlan vlan-id last-member-query-interval time`
5. `end`
6. `show ip igmp snooping`
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： スイッチ> <code>enable</code>	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# <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 igmp snooping last-member-query-interval time 例： スイッチ(config)# <code>ip igmp snooping</code>	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。

	コマンドまたはアクション	目的
	<code>last-member-query-interval 1000</code>	(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 <i>vlan-id</i> last-member-query-interval <i>time</i> 例： スイッチ(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 <i>vlan-id</i> 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： スイッチ(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show ip igmp snooping 例： スイッチ# 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： 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。

TCN 関連コマンドの設定

TCN イベント後のマルチキャスト フラッドイング時間の制御

トポロジ変更通知 (TCN) イベント後にフラッドイングするマルチキャストデータのトラフィックに対し、一般クエリー数を設定できます。TCN フラッドクエリーカウントを 1 に設定した場合は、1 つの一般クエリーを受信した後にフラッドイングが停止します。カウントを 7 に設定

した場合、一般クエリーを7つ受信するまでフラッディングが続きます。グループは、TCN イベント中に受信した一般的クエリーに基づいて学習されます。

クライアントロケーションが変更され、ブロックされていた後に現在は転送中の受信者が同じポートに存在する場合や、ポートが脱退メッセージを送信せずにダウンした場合などに TCN イベントが発生します。

TCN フラッドクエリー カウントを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping tcn flood query count count**
4. **end**
5. **show ip igmp snooping**
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> 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 igmp snooping tcn flood query count count 例： スイッチ(config)# ip igmp snooping tcn flood query count 3	マルチキャストトラフィックがフラッディングする IGMP の一般クエリー数を指定します。 指定できる範囲は1～10です。デフォルトのフラッディングクエリーカウントは2です。 (注) デフォルトのフラッディングクエリーカウントに戻すには、 no ip igmp 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ます。
ステップ 4	end 例：	特権 EXEC モードに戻ります。

フラッディングモードからの回復

	コマンドまたはアクション	目的
	スイッチ(config)# end	
ステップ 5	show ip igmp snooping 例： スイッチ# show ip igmp snooping	TCN の設定を確認します。
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。

フラッディングモードからの回復

トポロジの変更が発生した場合、スパニングツリーのルートは特別な IGMP Leave メッセージ (グローバル Leave メッセージ) をグループマルチキャストアドレス 0.0.0.0 に送信します。ただし、スパニングツリーのルートであるかどうかにかかわらず、グローバルな Leave メッセージを送信するように device を設定できます。ルータはこの特別な Leave メッセージを受信した場合、即座に一般クエリーを送信して、TCN 中のフラッディングモードからできるだけ早く回復するようにします。device がスパニングツリーのルートであれば、このコンフィギュレーションに関係なく、Leave メッセージが常に送信されます。

Leave メッセージを送信できるようにするには、次の手順を実行します。

手順の概要

1. enable
2. configure terminal
3. ip igmp snooping tcn query solicit
4. end
5. show ip igmp snooping
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> 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： 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 igmp snooping tcn query solicit 例： スイッチ(config)# <code>ip igmp snooping tcn query solicit</code>	TCN イベント中に発生したフラッドモードから回復するプロセスの速度を上げるために、IGMP Leave メッセージ（グローバル脱退）を送信します。デフォルトでは、クエリー送信要求はディセーブルに設定されています。 (注) デフォルトのクエリソリューションに戻すには、 no ip igmp 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 ip igmp snooping 例： スイッチ# <code>show ip igmp snooping</code>	TCN の設定を確認します。
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。

TCN イベント中のマルチキャスト フラッドिंगのディセーブル化

deviceはTCNを受信すると、一般クエリを2つ受信するまで、すべてのポートに対してマルチキャストトラフィックをフラッドングします。異なるマルチキャストグループのホストに接続されているポートが複数ある場合、リンク範囲を超えてdeviceによるフラッドングが行われ、パケット損失が発生する可能性があります。TCN フラッドングを制御するには、次の手順を実行します。

手順の概要

1. enable

2. **configure terminal**
3. **interface interface-id**
4. **no ip igmp snooping tcn flood**
5. **end**
6. **show ip igmp snooping**
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： 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	interface interface-id 例： スイッチ(config)# interface gigabitethernet 1/0/1	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。
ステップ 4	no ip igmp snooping tcn flood 例： スイッチ(config-if)# no ip igmp snooping tcn flood	スパニングツリーの TCN イベント中に発生するマルチキャストトラフィックのフラッドをディセーブルにします。 デフォルトでは、インターフェイス上のマルチキャストフラッドはイネーブルです。 (注) インターフェイス上でマルチキャストフラッドを再度イネーブルにするには、 ip igmp snooping tcn flood 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： スイッチ(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 ip igmp snooping 例： スイッチ# <code>show ip igmp snooping</code>	TCN の設定を確認します。
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。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping querier**
4. **ip igmp snooping querier address *ip_address***
5. **ip igmp snooping querier query-interval *interval-count***
6. **ip igmp snooping querier tcn query [*count count* | *interval interval*]**
7. **ip igmp snooping querier timer expiry *timeout***
8. **ip igmp snooping querier version *version***
9. **end**
10. **show ip igmp snooping vlan *vlan-id***
11. **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：	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	ip igmp snooping querier 例： スイッチ(config)# <code>ip igmp snooping querier</code>	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 4	ip igmp snooping querier address ip_address 例： スイッチ(config)# <code>ip igmp snooping querier address 172.16.24.1</code>	(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がdevice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。
ステップ 5	ip igmp snooping querier query-interval interval-count 例： スイッチ(config)# <code>ip igmp snooping querier query-interval 30</code>	(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： スイッチ(config)# <code>ip igmp snooping querier tcn query interval 20</code>	(任意) トポロジ変更通知 (TCN) クエリ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： スイッチ(config)# <code>ip igmp snooping querier timer expiry 180</code>	(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： スイッチ(config)# <code>ip igmp snooping querier version 2</code>	(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。

	コマンドまたはアクション	目的
ステップ 9	end 例： スイッチ(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： スイッチ# 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： 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。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ip igmp snooping report-suppression**
4. **end**
5. **show ip igmp snooping**
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> 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
	スイッチ# <code>configure terminal</code>	
ステップ 3	no ip igmp snooping report-suppression 例： スイッチ(config)# <code>no ip igmp snooping report-suppression</code>	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、device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： 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 ip igmp snooping 例： スイッチ# <code>show ip igmp snooping</code>	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： 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。

MVR グローバルパラメータの設定

デフォルト値を使用する場合は、オプションの MVR パラメータを設定する必要はありません。デフォルトのパラメータを変更する場合には (MVR VLAN 以外)、最初に MVR をイネーブルにする必要があります。



(注) ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンドリファレンスを参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **mvr**
4. **mvr group ip-address [count]**
5. **mvr querytime value**
6. **mvr vlan vlan-id**
7. **mvr mode {dynamic | compatible}**
8. **end**
9. 次のいずれかを使用します。
 - **show mvr**
 - **show mvr members**
10. **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> 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	mvr 例： スイッチ (config)# mvr	device 上で MVR をイネーブルにします。
ステップ 4	mvr group ip-address [count] 例： スイッチ (config)# mvr group 228.1.23.4	device 上で IP マルチキャストアドレスを設定するか、または <i>count</i> パラメータを使用して (<i>count</i> の範囲は 1～256 で、デフォルトは 1) 連続する MVR グループアドレスを設定します。このアドレスに送信されるすべてのマルチキャストデータは、device 上の送信元ポートおよびこのマルチキャストアドレス上のデータを受信するよう選択されたすべての受信ポートに送信されます。マルチキャストアドレスとテレビチャンネルは 1 対 1 の対応です。

	コマンドまたはアクション	目的
		(注) スイッチをデフォルト設定に戻すには、 no mvr [mode group ip-address querytime vlan] 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	mvr querytime value 例： スイッチ (config) # mvr querytime 10	(任意) マルチキャスト グループ メンバーシップ からポートを削除する前に、受信ポート上で IGMP レポート メンバーシップを待機する最大時間を定義します。この値は10分の1秒単位で設定します。範囲は1～100、デフォルトは10分の5秒、つまり0.5秒です。
ステップ 6	mvr vlan vlan-id 例： スイッチ (config) # mvr vlan 22	(任意) マルチキャスト データを受信する VLAN を指定します。すべての送信元ポートはこの VLAN に属する必要があります。VLAN の範囲は1～1001 および 1006～4094 です。デフォルトは VLAN 1 です。
ステップ 7	mvr mode {dynamic compatible} 例： スイッチ (config) # mvr mode dynamic	(任意) 次の MVR の動作モードを指定します。 <ul style="list-style-type: none"> • dynamic : 送信元ポートでダイナミック MVR メンバーシップを使用できます。 • compatible : Catalyst 3500 XL および Catalyst 2900 XL devices との互換性が得られます。送信元ポートでのダイナミック IGMP Join はサポートされません。 デフォルトは compatible モードです。 (注) スイッチをデフォルト設定に戻すには、 no mvr [mode group ip-address querytime vlan] 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 8	end 例： スイッチ (config) # end	特権 EXEC モードに戻ります。
ステップ 9	次のいずれかを使用します。 <ul style="list-style-type: none"> • show mvr • show mvr members 例：	設定を確認します。

	コマンドまたはアクション	目的
	スイッチ# <code>show mvr</code> OR スイッチ# <code>show mvr members</code>	
ステップ 10	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。

MVR インターフェイスの設定

レイヤ 2 MVR インターフェイスを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mvr**
4. **interface interface-id**
5. **mvr type {source | receiver}**
6. **mvr vlan vlan-id group [ip-address]**
7. **mvr immediate**
8. **end**
9. 次のいずれかを使用します。
 - `show mvr`
 - `show mvr interface`
 - `show mvr members`
10. **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：	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	mvr 例： スイッチ (config)# <code>mvr</code>	device上で MVR をイネーブルにします。
ステップ 4	interface interface-id 例： スイッチ (config)# <code>interface gigabitethernet1/0/2</code>	設定するレイヤ2ポートを指定し、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。
ステップ 5	mvr type {source receiver} 例： スイッチ (config-if)# <code>mvr type receiver</code>	<p>MVR ポートを次のいずれかに設定します。</p> <ul style="list-style-type: none"> • source : マルチキャスト データを送受信するアップリンク ポートを送信元ポートとして設定します。加入者が送信元ポートに直接接続することはできません。device上の送信元ポートはいずれも、1つのマルチキャスト VLAN に属する必要があります。 • receiver : 加入者ポートであり、マルチキャスト データを受信するだけの場合、レシーバポートとしてポートを設定します。受信ポートは、スタティックな設定、または IGMP Leave および Join メッセージによってマルチキャスト グループのメンバーになるまでは、データを受信しません。受信ポートをマルチキャスト VLAN に所属させることはできません。 <p>デフォルトでは、非 MVR ポートとして設定されません。非 MVR ポートに MVR 特性を設定しようとしても、エラーになります。</p> <p>(注) インターフェイスをデフォルト設定に戻すには、<code>no mvr [type immediate vlan vlan-id group]</code> 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。</p>
ステップ 6	mvr vlan vlan-id group [ip-address] 例：	(任意) マルチキャスト VLAN および IP マルチキャスト アドレスに送信されたマルチキャスト トラフィックを受信するポートを静的に設定します。

	コマンドまたはアクション	目的
	スイッチ(config-if)# mvr vlan 22 group 228.1.23.4	グループメンバとして静的に設定されたポートは、静的に削除されない限り、グループメンバのままです。 (注) 互換モードでは、このコマンドが適用されるのはレシーバポートだけです。ダイナミックモードでは、レシーバポートおよび送信元ポートに適用されます。 レシーバポートは、IGMP Join および Leave メッセージを使用することによって、マルチキャストグループに動的に加入することもできます。
ステップ 7	mvr immediate 例： スイッチ(config-if)# mvr immediate	(任意) ポート上でMVRの即時脱退機能をイネーブルにします。 (注) このコマンドが適用されるのは、受信ポートだけです。また、イネーブルにするのは、単一の受信デバイスが接続されている受信ポートに限定してください。
ステップ 8	end 例： スイッチ(config)# end	特権 EXEC モードに戻ります。
ステップ 9	次のいずれかを使用します。 <ul style="list-style-type: none"> • show mvr • show mvr interface • show mvr members 例： スイッチ# show mvr interface <pre> Port Type Status Immediate Leave ----- ----- Gi1/0/2 RECEIVER ACTIVE/DOWN ENABLED </pre>	設定を確認します。
ステップ 10	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。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp profile *profile number***
4. **permit | deny**
5. **range *ip multicast address***
6. **end**
7. **show ip igmp profile *profile number***
8. **show running-config**
9. **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> 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 igmp profile <i>profile number</i> 例： スイッチ(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。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • 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。 <p>デフォルトでは、device には IGMP プロファイルが設定されていません。</p> <p>(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。</p>
ステップ 4	permit deny 例 : スイッチ (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 : スイッチ (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 : スイッチ (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 : スイッチ # show ip igmp profile 3	プロファイルの設定を確認します。

	コマンドまたはアクション	目的
ステップ 8	show running-config 例： スイッチ# show running-config	入力を確認します。
ステップ 9	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。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface interface-id**
4. **ip igmp filter profile number**
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： 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：	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	interface interface-id 例： スイッチ(config)# <code>interface gigabitethernet1/0/1</code>	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： スイッチ(config-if)# <code>ip igmp filter 321</code>	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。 (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： スイッチ(config-if)# <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	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 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。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface interface-id**
4. **ip igmp max-groups number**
5. **end**
6. **show running-config interface interface-id**
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： 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	interface interface-id 例： スイッチ(config)# interface gigabitethernet1/0/2	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： スイッチ(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。

	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 interface interface-id 例： スイッチ# interface gigabitethernet1/0/1	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。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface interface-id**
4. **ip igmp max-groups action {deny | replace}**
5. **end**
6. **show running-config interface interface-id**
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：	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
	スイッチ> <code>enable</code>	
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	interface interface-id 例： スイッチ(config)# <code>interface gigabitethernet1/0/1</code>	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： スイッチ(config-if)# <code>ip igmp max-groups action replace</code>	<p>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。</p> <ul style="list-style-type: none"> • 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、device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、deviceはランダムに選択したエントリを受信した IGMP レポートで上書きします。 <p>device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。</p>

	コマンドまたはアクション	目的
		(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： 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 interface interface-id 例： スイッチ# 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： 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。

IGMP スヌーピングおよび MVR のモニターリング

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 6: 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]]	device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。

コマンド	目的
show ip igmp snooping groups [count dynamic [count] user [count]]	<p>device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。</p> <ul style="list-style-type: none"> • 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。 • dynamic : IGMP スヌーピングによって学習された エントリを表示します。 • user : ユーザーによって設定されたマルチキャスト エントリだけを表示します。
show ip igmp snooping groups vlan <i>vlan-id</i> [<i>ip_address</i> count dynamic [count] user [count]]	<p>マルチキャスト VLAN またはその VLAN の特定の パラメータについて、マルチキャストテーブル情報を表示します。</p> <ul style="list-style-type: none"> • <i>vlan-id</i> : VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 • 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。 • dynamic : IGMP スヌーピングによって学習された エントリを表示します。 • <i>ip_address</i> : 指定したグループ IP アドレスのマルチキャスト グループの特性を表示します。 • user : ユーザーによって設定されたマルチキャスト エントリだけを表示します。
show ip igmp snooping mrouter [vlan <i>vlan-id</i>]	<p>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。</p> <p>(注) IGMP スヌーピングを有効にすると、device 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。</p> <p>(オプション) vlan <i>vlan-id</i> を入力すると、特定の VLAN に関する情報が表示されます。</p>
show ip igmp snooping querier [vlan <i>vlan-id</i>] detail	<p>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。</p>

MVR のモニターリング

スイッチまたは指定されたインターフェイスの MVR をモニターするには、次の MVR 情報を表示します。

表 7: MVR 情報を表示するためのコマンド

コマンド	目的
<code>show mvr</code>	スイッチの MVR ステータスおよび値を表示します。これは、MVR のイネーブルまたはディセーブルの判別、マルチキャスト VLAN、マルチキャストグループの最大数 (256) および現在の数 (0 ~ 256)、クエリーの応答時間、および MVR モードです。
<code>show mvr interface [interface-id] [members [vlan vlan-id]]</code>	<p>すべての MVR インターフェイスおよびその MVR 設定を表示します。</p> <p>特定のインターフェイスを指定すると、次の情報が表示されます。</p> <ul style="list-style-type: none"> • Type : Receiver または Source • Status : 次のいずれか <ul style="list-style-type: none"> • ACTIVE は、ポートが VLAN に含まれていることを意味します。 • UP/DOWN は、ポートが転送中または転送中ではないことを示します。 • INACTIVE は、ポートが VLAN に含まれていないことを意味します。 • Immediate Leave : Enabled または Disabled <p>members キーワードを入力すると、そのポート上のすべてのマルチキャストグループメンバが表示されます。VLAN ID を入力した場合は、その VLAN 上のすべてのマルチキャストグループメンバが表示されます。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。</p>
<code>show mvr members [ip-address]</code>	すべての IP マルチキャストグループまたは指定した IP マルチキャストグループ IP アドレスに含まれているレシーバポートおよび送信元ポートがすべて表示されます。

IGMP のフィルタリングおよびスロットリング設定のモニターリング

IGMP プロファイルの特性を表示したり、device 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。また、device 上のすべてのインターフェイスまたは指定したインターフェイスに関する IGMP スロットリング設定を表示することもできます。

表 8: IGMP のフィルタリングおよびスロットリング設定を表示するためのコマンド

コマンド	目的
<code>show ip igmp profile [profile number]</code>	特定の IGMP プロファイルまたは device 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。
<code>show running-config [interface interface-id]</code>	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 device 上のすべてのインターフェイスの設定を表示します。

IGMP スヌーピングおよび MVR の設定例

例：CGMP パケットを使用した IGMP スヌーピングの設定

次に、CGMP パケットを学習方式として使用するよう IGMP スヌーピングを設定する例を示します。

```
スイッチ# configure terminal
スイッチ(config)# ip igmp snooping vlan 1 mrouter learn cgmp
スイッチ(config)# end
```

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。

```
スイッチ configure terminal
スイッチ ip igmp snooping vlan 200 mrouter interface gigabitethernet1/0/2
スイッチ 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。


```
スイッチ# configure terminal
スイッチ# ip igmp snooping vlan 105 static 0100.1212.0000 interface gigabitethernet1/0/1

スイッチ# 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。

```
スイッチ# configure terminal
スイッチ(config)# ip igmp snooping vlan 130 immediate-leave
スイッチ(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。

```
スイッチ# configure terminal
スイッチ(config)# ip igmp snooping querier 10.0.0.64
スイッチ(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。

```
スイッチ# configure terminal
スイッチ(config)# ip igmp snooping querier query-interval 25
スイッチ(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。

```
スイッチ# configure terminal
スイッチ(config)# ip igmp snooping querier timeout expiry 60
スイッチ(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。

```
スイッチ# configure terminal
スイッチ(config)# no ip igmp snooping querier version 2
スイッチ(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。

```
スイッチ(config)# ip igmp profile 4
スイッチ(config-igmp-profile)# permit
スイッチ(config-igmp-profile)# range 229.9.9.0
スイッチ(config-igmp-profile)# end
スイッチ# 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。

```
スイッチ(config)# interface gigabitethernet1/0/2
スイッチ(config-if)# ip igmp filter 4
スイッチ(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。

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

例：MVR グローバルパラメータの設定

次に、MVR をイネーブルにして、MVR グループアドレスを設定し、クエリータイムを 1 秒（10 分の 10 秒）に設定し、MVR マルチキャスト VLAN を VLAN 22 として指定し、MVR モードをダイナミックに設定する例を示します。

```
スイッチ(config)# mvr
スイッチ(config)# mvr group 228.1.23.4
スイッチ(config)# mvr querytime 10
スイッチ(config)# mvr vlan 22
スイッチ(config)# mvr mode dynamic
スイッチ(config)# end
```

例 : MVR インターフェイスの設定

次に、ポートをレシーバポートとして設定し、マルチキャストグループアドレスに送信されたマルチキャストトラフィックを受信するようにポートを静的に設定し、ポートに即時脱退機能を設定し、結果を確認する例を示します。

```
スイッチ(config)# mvr
スイッチ(config)# interface gigabitethernet1/0/2
スイッチ(config-if)# mvr type receiver
スイッチ(config-if)# mvr vlan 22 group 228.1.23.4
スイッチ(config-if)# mvr immediate
スイッチ(config)# end
スイッチ# show mvr interface

Port Type Status Immediate Leave
-----
Gi1/0/2 RECEIVER ACTIVE/DOWN ENABLED
```

例：MVR インターフェイスの設定

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。