



# 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

- [機能情報の確認, 1 ページ](#)
- [IGMP スヌーピングおよび MVR の設定の前提条件, 2 ページ](#)
- [IGMP スヌーピングおよび MVR の設定の制約事項, 3 ページ](#)
- [IGMP スヌーピングおよび MVR に関する情報, 5 ページ](#)
- [IGMP スヌーピングおよび MVR の設定方法, 16 ページ](#)
- [IGMP スヌーピングおよび MVR のモニタリング, 50 ページ](#)
- [IGMP スヌーピングおよび MVR の設定例, 53 ページ](#)

## 機能情報の確認

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

プラットフォームのサポートおよびシスコソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://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。

# 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 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) の使用を試みます。SVI IP アドレスが存在しない場合、スイッチはスイッチ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 クエリアはスイッチ上で利用可能な 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

### 関連トピック

[IGMP スヌーピング クエリアの設定, \(32 ページ\)](#)

[IGMP スヌーピング, \(5 ページ\)](#)

## 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、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 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) が実行されているスイッチは、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 クエリーに 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、クエリーに 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 はスイッチ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。

### 関連トピック

[IGMP のバージョン](#)

[IGMP プロファイルの設定, \(42 ページ\)](#)

[IGMP プロファイルの適用, \(44 ページ\)](#)

[IGMP グループの最大数の設定, \(46 ページ\)](#)

[IGMP スロットリングアクションの設定, \(48 ページ\)](#)

[IGMP フィルタリングおよびスロットリング, \(15 ページ\)](#)

## 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。
- 各スイッチまたはスイッチ 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。スイッチのレシーバ 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。
- スイッチ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、スイッチで存続可能時間（TTL）が 1 だけ少なくなります。
- スイッチ上の 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、スイッチ上でエイリアス IP マルチキャスト アドレスを使用できます。ただし、スイッチが Catalyst 3550 または Catalyst 3500 XL スイッチ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。
- スイッチ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と、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スイッチは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スイッチ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ーポートを追跡する必要があります。特定のマルチキャストグループについて、スイッチがホストからIGMPレポートを受信すると、そのスイッチ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。スイッチは、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。

スイッチは、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。スイッチでは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 vlanvlan-id staticip\_addressinterfaceinterface-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。

## 関連トピック

[IGMP スヌーピング クエリアの設定, \(32 ページ\)](#)

[IGMP スヌーピングの前提条件, \(2 ページ\)](#)

[例 : IGMP スヌーピング クエリアの送信元アドレスの設定, \(54 ページ\)](#)

[例 : IGMP スヌーピング クエリアの最大応答時間の設定, \(54 ページ\)](#)

[例 : IGMP スヌーピング クエリア タイムアウトの設定, \(55 ページ\)](#)

[例 : IGMP スヌーピング クエリア機能の設定, \(55 ページ\)](#)

## IGMP のバージョン

スイッチは、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、スイッチ上で相互運用できます。たとえば、IGMP スヌーピングがイネーブルになっており、クエリーのバージョンが IGMPv2 で、スイッチがホストから IGMPv3 レポートを受信している場合、スイッチは IGMPv3 レポートをマルチキャスト ルータに転送できます。

IGMPv3 スwitch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。

## 関連トピック

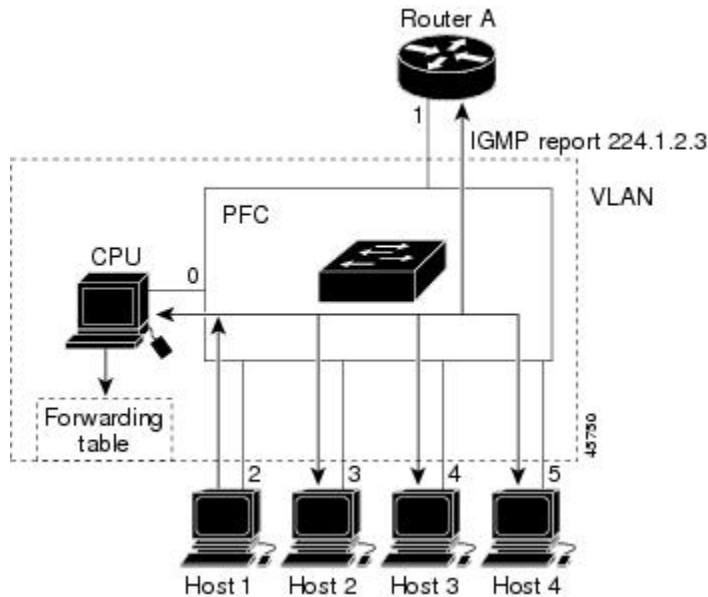
[IGMP バージョンの変更](#)

[IGMP スヌーピングの制約事項, \(3 ページ\)](#)

## マルチキャスト グループへの加入

スイッチ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スイッチは、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、ホストはスイッチに Join メッセージを送信することによって応答します。スイッチの 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。

図 1：最初の IGMP Join メッセージ



ルータ A がスイッチに一般クエリを送信し、スイッチがそのクエリを同じ VLAN のすべてのメンバであるポート 2～5 に転送します。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。スイッチの 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

スイッチのハードウェアは、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。

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、メッセージはスイッチの他の

ポートへ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。

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

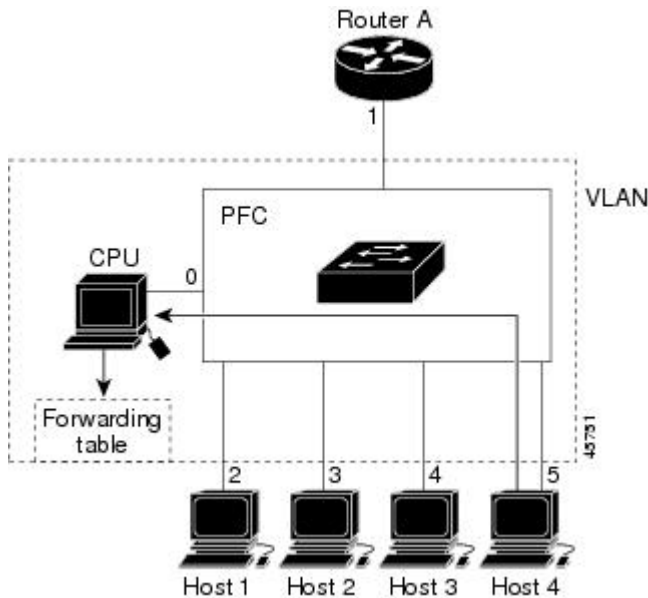


表 2： 更新された IGMP スヌーピング転送テーブル

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

## 関連トピック

[グループに加入するホストの静的な設定, \(23 ページ\)](#)

[例：グループに加入するホストの静的な設定, \(54 ページ\)](#)

## マルチキャスト グループからの脱退

ルータは定期的にマルチキャスト一般クエリを送信し、スイッチはそれらのクエリを VLAN 内のすべてのポート経由で転送します。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。スイッチは、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スイッチは、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。スイッチはさらに、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

スイッチは IGMP スヌーピングの即時脱退を使用して、先にスイッチ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 はスイッチ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。

### 関連トピック

[IGMP 即時脱退のイネーブル化, \(24 ページ\)](#)

[例: IGMP 即時脱退のイネーブル化, \(54 ページ\)](#)

## IGMP 設定可能 Leave タイマー

特定のマルチキャストグループへの参加がまだ必要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スイッチ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。

### 関連トピック

[IGMP 脱退タイマーの設定, \(26 ページ\)](#)

## 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ーに 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、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

スイッチは、IGMP レポート抑制を使用して、1つのマルチキャストルータクエリーごとに IGMP レポートを1つだけマルチキャスト デバイスに転送します。IGMP ルータ抑制がイネーブル（デフォルト）である場合、スイッチは最初の IGMP レポートをグループのすべてのポートからすべてのマルチキャストルータに送信します。スイッチは、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ーに IGMPv1 および IGMPv2 レポートに対する要求だけが含まれている場合、スイッチは最初の IGMPv1 レポートまたは IGMPv2 レポートだけを、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。

マルチキャストルータクエリーに IGMPv3 レポートの要求も含まれる場合は、スイッチ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。

#### 関連トピック

[IGMP レポート抑制のディセーブル化、（35 ページ）](#)

## IGMP スヌーピングのデフォルト設定

次の表に、スイッチの 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 <sup>1</sup> 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	イネーブル

<sup>1</sup> (1) TCN = トポロジ変更通知

## 関連トピック

[スイッチでの IGMP スヌーピングのイネーブル化またはディセーブル化](#), (16 ページ)

[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](#), (18 ページ)

# 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 プロバイダー 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 プロバイダー 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) スイッチ上で、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。

スイッチの CPU は、MVR IP マルチキャスト ストリームとそれに対応するスイッチ転送テーブル内の 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

スイッチの 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。

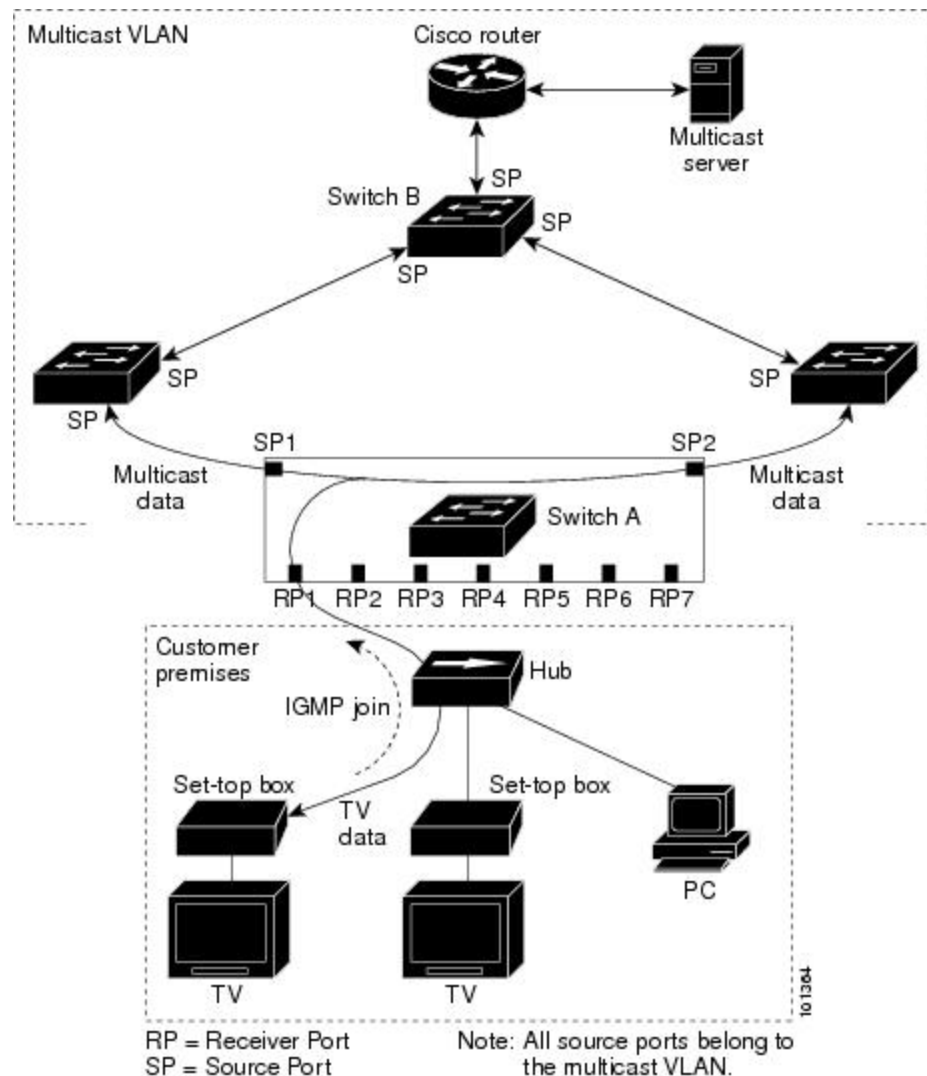
- 互換モードの場合、MVR ホストが受信したマルチキャスト データはすべての MVR データ ポートに転送されます。MVR データ ポートの MVR ホスト メンバーシップは無関係です。マルチキャスト データは、IGMP レポートまたは静的な MVR 設定のどちらかによって、MVR ホストが加入しているレシーバポートだけに転送されます。MVR ホストから受信した IGMP レポートが、スイッチに設定された MVR データ ポートから転送されることはありません。
- ダイナミック モードの場合、スイッチ上の MVR ホストが受信したマルチキャスト データは、IGMP レポートまたは静的な MVR 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、互換モードでスイッチ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 つの加入者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。加入者ポートは、MVR レシーバポートとして設定されたスイッチポートです。

次に、設定例を示します。

図 3: マルチキャスト VLAN レジストレーションの例



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加入するために、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、設定されている IP マルチキャストグループアドレスの 1 つと一致すると、スイッチの CPU がハードウェアアドレステーブルを変更して、指定のマルチキャストストリームをマルチキャスト VLAN から受信したときの転送先として、レシーバポートと VLAN を追加します。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。スイッチの CPU は、受信ポートの VLAN を介して 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ー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、レシーバポートの加入者から IGMP Leave メッセージを受信したスイッチは、そのポートに IGMP クエリーを送信し、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 クエリーが送信されません。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。アクセスレイヤスイッチ（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
モード	互換
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

機能	デフォルト設定
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

都市部や集合住宅（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スイッチは、IGMPv3 Join および Leave メッセージをサポートしていません。

### 関連トピック

[IGMP プロファイルの設定、（42 ページ）](#)

[IGMP プロファイルの適用, \(44 ページ\)](#)

[IGMP グループの最大数の設定, \(46 ページ\)](#)

[IGMP スロットリング アクションの設定, \(48 ページ\)](#)

[IGMP スヌーピングの制約事項, \(3 ページ\)](#)

## 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、スイッチの 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

### スイッチでの 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。

スイッチで 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. **configureterminal**
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	<b>enable</b>  例 :  Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例 :  Switch# <b>configure terminal</b>	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	<b>ip igmp snooping</b>  例 :  Switch(config)# <b>ip igmp snooping</b>	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、 <b>no ip igmp snooping</b> 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	<b>end</b>  例 :  Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>copy running-config startup-config</b>  例 :  Switch# <b>copy running-config startup-config</b>	(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。

## 関連トピック

[IGMP スヌーピングのデフォルト設定, \(10 ページ\)](#)

## 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. **configureterminal**
3. **ip igmp snooping vlanvlan-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	<b>enable</b>  例 : Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例 : Switch# <b>configure terminal</b>	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	<b>ip igmp snooping vlanvlan-id</b>  例 : Switch(config)# <b>ip igmp snooping vlan 7</b>	<p>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。</p> <p>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。</p> <p>(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、<b>no ip igmp snooping vlanvlan-id</b> 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。</p>

	コマンドまたはアクション	目的
ステップ 4	<b>end</b>  例 : Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>copy running-config startup-config</b>  例 : Switch# <b>copy running-config startup-config</b>	(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。

### 関連トピック

[IGMP スヌーピングのデフォルト設定, \(10 ページ\)](#)

## 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. **configureterminal**
3. **ip igmp snooping vlanvlan-idmrouterlearn {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	<b>enable</b>  例 : Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例 : Switch# <b>configure terminal</b>	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	<b>ip igmp snooping vlanvlan-idmrouterlearn {cgmp   pim-dvmrp }</b>  例 : Switch(config)# <b>ip igmp snooping vlan 1 mrouter learn cgmp</b>	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"> <li>• <b>cgmp</b>—Listens for CGMP packets. この方法は、制御トラフィックを減らす場合に有効です。</li> <li>• <b>pim-dvmrp</b> : 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。</li> </ul> (注) デフォルトの学習方式に戻すには、 <b>no ip igmp snooping vlanvlan-idmrouter learn cgmp</b> 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	<b>end</b>  例 : Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	<b>show ip igmp snooping</b>  例 : Switch# <b>show ip igmp snooping</b>	設定を確認します。
ステップ 6	<b>copy running-config startup-config</b>  例 : Switch# <b>copy running-config startup-config</b>	(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

スイッチにマルチキャスト 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イネーブルにする）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、スイッチ ポートに限りサポートされます。

### 手順の概要

1. **enable**
2. **configureterminal**
3. **ip igmp snooping vlanvlan-idmrouter interfaceinterface-id**
4. **end**
5. **show ip igmp snooping mrouter [vlanvlan-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	<b>enable</b>  例 : Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b>  例 : Switch# <b>configure terminal</b>	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	<b>ip igmp snooping vlanvlan-idmrouter interfaceinterface-id</b>  例 : Switch(config)# <b>ip igmp snooping vlan 5 mrouter interface gigabitethernet1/0/1</b>	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"> <li>指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。</li> <li>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。</li> </ul> (注) VLAN からマルチキャスト ルータ ポートを削除するには、 <b>no ip igmp snooping vlanvlan-idmrouter interfaceinterface-id</b> 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	<b>end</b>  例 : Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show ip igmp snooping mrouter [vlanvlan-id]</b>  例 : Switch# <b>show ip igmp snooping mrouter vlan 5</b>	VLAN インターフェイス上で IGMP スヌーピングがイネーブルになっていることを確認します。
ステップ 6	<b>copy running-config startup-config</b>  例 : Switch# <b>copy running-config startup-config</b>	(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。

## 関連トピック

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, (53 ページ)

## 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. **configureterminal**
3. **ip igmp snooping vlanvlan-idstaticip\_addressinterfaceinterface-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	<b>enable</b>  例： Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例： Switch# <b>configure terminal</b>	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	<b>ip igmp snooping vlanvlan-idstaticip_addressinterfaceinterface-id</b>  例： Switch(config)# <b>ip igmp snooping vlan 105 static 230.0.0.1 interface gigabitethernet1/0/1</b>	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。 <ul style="list-style-type: none"><li>• <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。</li><li>• <i>ip-address</i> は、グループの IP アドレスです。</li><li>• <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。</li></ul>

	コマンドまたはアクション	目的
		(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、 <b>no ip igmp snooping vlan <i>vlan-id</i> static mac-address <i>interface interface-id</i></b> 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	<b>end</b>  例：  Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show ip igmp snooping groups</b>  例：  Switch# <b>show ip igmp snooping groups</b>	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	<b>copy running-config startup-config</b>  例：  Switch# <b>copy running-config startup-config</b>	(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。

#### 関連トピック

[マルチキャスト グループへの加入, \(6 ページ\)](#)

[例：グループに加入するホストの静的な設定, \(54 ページ\)](#)

## 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、スイッチはポート上で 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 はスイッチのデフォルト バージョンです。



## 手順の概要

1. **enable**
2. **configureterminal**
3. **ip igmp snooping vlanvlan-idimmediate-leave**
4. **end**
5. **show ip igmp snooping vlanvlan-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	<b>enable</b>  例 : Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例 : Switch# <b>configure terminal</b>	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	<b>ip igmp snooping vlanvlan-idimmediate-leave</b>  例 : Switch(config)# <b>ip igmp snooping vlan 21 immediate-leave</b>	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、 <b>no ip igmp snooping vlanvlan-idimmediate-leave</b> 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	<b>end</b>  例 : Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show ip igmp snooping vlanvlan-id</b>  例 : Switch# <b>show ip igmp snooping vlan 21</b>	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
ステップ 6	<b>end</b>  例 :  Switch(config) # <b>end</b>	特権 EXEC モードに戻ります。

### 関連トピック

[即時脱退](#), (9 ページ)

例 : [IGMP 即時脱退のイネーブル化](#), (54 ページ)

## 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. **configureterminal**
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	<b>enable</b>  例 :  Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b>  例 : Switch# <b>configure terminal</b>	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	<b>ip igmp snooping last-member-query-interval time</b>  例 : Switch(config)# <b>ip igmp snooping last-member-query-interval 1000</b>	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、 <b>no ip igmp snooping last-member-query-interval</b> 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	<b>ip igmp snooping vlan vlan-id last-member-query-interval time</b>  例 : Switch(config)# <b>ip igmp snooping vlan 210 last-member-query-interval 1000</b>	(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、 <b>no ip igmp snooping vlan vlan-id last-member-query-interval</b> 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	<b>end</b>  例 : Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show ip igmp snooping</b>  例 : Switch# <b>show ip igmp snooping</b>	(任意) 設定された IGMP 脱退時間を表示します。
ステップ 7	<b>copy running-config startup-config</b>  例 : Switch# <b>copy running-config startup-config</b>	(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。

## 関連トピック

[IGMP 設定可能 Leave タイマー, \(9 ページ\)](#)

## TCN 関連コマンドの設定

## TCN イベント後のマルチキャスト フラッディング時間の制御

トポロジ変更通知 (TCN) イベント後にフラッディ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 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ディングが停止します。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. **configureterminal**
3. **ip igmp snooping tcn flood query countcount**
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	<b>enable</b>  例 : Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configureterminal</b>  例 : Switch# <b>configure terminal</b>	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	<b>ip igmp snooping tcn flood query count</b> <b>count</b>  例 : <pre>Switch(config)# ip igmp snooping tcn flood query count 3</pre>	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、 <b>no ip igmp snooping tcn flood query count</b> 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	<b>end</b>  例 : <pre>Switch(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 5	<b>show ip igmp snooping</b>  例 : <pre>Switch# show ip igmp snooping</pre>	TCN の設定を確認します。
ステップ 6	<b>copy running-config startup-config</b>  例 : <pre>Switch# 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。

## 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スイッチを設定できます。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。スイッチ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. **configureterminal**
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	<b>enable</b>  例 : Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例 : Switch# <b>configure terminal</b>	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	<b>ip igmp snooping tcn query solicit</b>  例 : Switch(config)# <b>ip igmp snooping tcn query solicit</b>	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ー送信要求に戻すには、 <b>no ip igmp snooping tcn query solicit</b> 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	<b>end</b>  例 : Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show ip igmp snooping</b>  例 : Switch# <b>show ip igmp snooping</b>	TCN 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 6	<b>copy running-config startup-config</b>  例 :  Switch# <b>copy running-config startup-config</b>	(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 フラッディングのディセーブル化

スイッチは TCN を受信すると、一般クエリーを 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ディングします。異なるマルチキャスト グループのホストに接続しているポートが複数ある場合、リンク範囲を超えてスイッチによるフラッディングが行われ、パケット損失が発生する可能性があります。TCN フラッディ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. **configureterminal**
3. **interfaceinterface-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	<b>enable</b>  例 :  Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configureterminal</b>  例 :  Switch# <b>configure terminal</b>	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	<b>interface</b> <i>interface-id</i>  例 :  Switch(config)# <b>interface</b> <b>gigabitethernet 1/0/1</b>	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	<b>no ip igmp snooping tcn flood</b>  例 :  Switch(config-if)# <b>no ip igmp</b> <b>snooping tcn flood</b>	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ディング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ディングはイネーブルです。  (注) インターフェイス上でマルチキャストフラッディングを再度イネーブルにするには、 <b>ip igmp snooping tcn flood</b> 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	<b>end</b>  例 :  Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show ip igmp snooping</b>  例 :  Switch# <b>show ip igmp snooping</b>	TCN の設定を確認します。
ステップ 7	<b>copy running-config startup-config</b>  例 :  Switch# <b>copy running-config</b> <b>startup-config</b>	(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. **configureterminal**
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** [*countcount* | *intervalinterval*]
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	<b>enable</b>  例 : Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例 : Switch# <b>configure terminal</b>	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	<b>ip igmp snooping querier</b>  例 : Switch(config)# <b>ip igmp snooping querier</b>	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	<b>ip igmp snooping querier address</b> <i>ip_address</i>  例 : Switch(config)# <b>ip igmp snooping querier address 172.16.24.1</b>	（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 クエリアはスイッチ上で 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。

	コマンドまたはアクション	目的
ステップ 5	<b>ip igmp snooping querier query-intervalinterval-count</b>  例 :  <pre>Switch(config)# ip igmp snooping querier query-interval 30</pre>	(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	<b>ip igmp snooping querier tcn query [countcount   intervalinterval]</b>  例 :  <pre>Switch(config)# ip igmp snooping querier tcn query interval 20</pre>	(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	<b>ip igmp snooping querier timer expirytimeout</b>  例 :  <pre>Switch(config)# ip igmp snooping querier timer expiry 180</pre>	(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	<b>ip igmp snooping querier versionversion</b>  例 :  <pre>Switch(config)# ip igmp snooping querier version 2</pre>	(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	<b>end</b>  例 :  <pre>Switch(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 10	<b>show ip igmp snooping vlanvlan-id</b>  例 :  <pre>Switch# show ip igmp snooping vlan 30</pre>	(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	<b>copy running-config startup-config</b>  例 :  <pre>Switch# 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。

## 関連トピック

[IGMP スヌーピング, \(5 ページ\)](#)

[IGMP スヌーピングの前提条件, \(2 ページ\)](#)

[例: IGMP スヌーピング クエリアの送信元アドレスの設定, \(54 ページ\)](#)

[例: IGMP スヌーピング クエリアの最大応答時間の設定, \(54 ページ\)](#)

[例: IGMP スヌーピング クエリア タイムアウトの設定, \(55 ページ\)](#)

[例: IGMP スヌーピング クエリア機能の設定, \(55 ページ\)](#)

# 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. **configureterminal**
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	<b>enable</b>  例 : Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例 : Switch# <b>configure terminal</b>	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	<b>no ip igmp snooping report-suppression</b>  例 : <pre>Switch(config)# no ip igmp snooping report-suppression</pre>	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、スイッチはマルチキャスト ルータ クエリーごとに 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、 <b>ip igmp snooping report-suppression</b> 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	<b>end</b>  例 : <pre>Switch(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 5	<b>show ip igmp snooping</b>  例 : <pre>Switch# show ip igmp snooping</pre>	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	<b>copy running-config startup-config</b>  例 : <pre>Switch# 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。

#### 関連トピック

[IGMP レポート抑制, \(9 ページ\)](#)

## 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. **configureterminal**
3. **mvr**
4. **mvr groupip-address [count]**
5. **mvrquerytimevalue**
6. **mvrvlanvlan-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	<b>enable</b>  例 : Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例 : Switch# <b>configure terminal</b>	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	<b>mvr</b>  例 : Switch (config)# <b>mvr</b>	スイッチ上で MVR をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	<b>mvr groupip-address [count]</b>  例 :  <pre>Switch(config)# mvr group 228.1.23.4</pre>	<p>スイッチ上で 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、スイッチ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。</p> <p>(注) スイッチをデフォルトの設定に戻すには、<b>no mvr [mode   groupip-address   querytime   vlan]</b> 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 5	<b>mvrquerytimevalue</b>  例 :  <pre>Switch(config)# mvr querytime 10</pre>	<p>(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。</p>
ステップ 6	<b>mvrvlanvlan-id</b>  例 :  <pre>Switch(config)# mvr vlan 22</pre>	<p>(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。</p>
ステップ 7	<b>mvr mode {dynamic   compatible}</b>  例 :  <pre>Switch(config)# mvr mode dynamic</pre>	<p>(任意) 次の MVR の動作モードを指定します。</p> <ul style="list-style-type: none"> <li>• <b>dynamic</b> : 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。</li> <li>• <b>compatible</b> : Catalyst 3500 XL および Catalyst 2900 XL スイッチ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。</li> </ul> <p>デフォルトは <b>compatible</b> モードです。</p> <p>(注) スイッチをデフォルトの設定に戻すには、<b>no mvr [mode   groupip-address   querytime   vlan]</b> 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 8	<b>end</b>  例 :  <pre>Switch(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 9	次のいずれかを使用します。  • <b>show mvr</b>	<p>設定を確認します。</p>

	コマンドまたはアクション	目的
	<ul style="list-style-type: none"> <li>• <b>show mvr members</b></li> </ul> <p>例 :</p> <pre>Switch# show mvr</pre> <p>OR</p> <pre>Switch# show mvr members</pre>	
ステップ 10	<b>copy running-config startup-config</b> <p>例 :</p> <pre>Switch# 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。

## 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. **configureterminal**
3. **mvr**
4. **interfaceinterface-id**
5. **mvr type {source | receiver}**
6. **mvr vlanvlan-idgroup [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	<b>enable</b>  例 : Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例 : Switch# <b>configure terminal</b>	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	<b>mvr</b>  例 : Switch (config)# <b>mvr</b>	スイッチ上で MVR をイネーブルにします。
ステップ 4	<b>interfaceinterface-id</b>  例 : Switch(config)# <b>interface</b> <b>gigabitethernet1/0/2</b>	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	<b>mvr type {source   receiver}</b>  例 : Switch(config-if)# <b>mvr type</b> <b>receiver</b>	<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"> <li>• <b>source</b> : 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。スイッチ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。</li> <li>• <b>receiver</b> : ポートが加入者ポートで、マルチキャスト データの受信だけを行う場合には、ポートを受信ポートとして設定します。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。</li> </ul> <p>デフォルトでは、非 MVR ポートとして設定されます。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>



	コマンドまたはアクション	目的
		(注) インターフェイスをデフォルトの設定に戻すには、 <b>no mvr[type   immediate   vlanvlan-id   group]</b> 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 6	<b>mvr vlanvlan-idgroup [ip-address]</b>  例 :  <pre>Switch(config-if)# mvr vlan 22 group 228.1.23.4</pre>	(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。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	<b>mvr immediate</b>  例 :  <pre>Switch(config-if)# mvr immediate</pre>	(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	<b>end</b>  例 :  <pre>Switch(config)# end</pre>	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"> <li>• <b>show mvr</b></li> <li>• <b>show mvr interface</b></li> <li>• <b>show mvr members</b></li> </ul> 例 :  <pre>Switch# show mvr interface Port      Type      Status   Immediate Leave ----- Gi1/0/2  RECEIVER  ACTIVE/DOWN           ENABLED</pre>	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 10	<b>copy running-config startup-config</b>  例 :  <pre>Switch# 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 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. **configureterminal**
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	<b>enable</b>  例 :  <pre>Switch&gt; enable</pre>	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configureterminal</b>  例 :  <pre>Switch# configure terminal</pre>	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	<b>ip igmp profile</b> <i>profile number</i>  例 :  <pre>Switch(config)# ip igmp profile 3</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>deny</b> : 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。</li> <li>• <b>exit</b> : 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。</li> <li>• <b>no</b> : 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。</li> <li>• <b>permit</b> : 一致するアドレスを許可します。</li> <li>• <b>range</b> : 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。</li> </ul> <p>デフォルトでは、スイッチには 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、<b>no ip igmp profile</b><i>profile number</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	<b>permit   deny</b>  例 :  <pre>Switch(config-igmp-profile)# permit</pre>	<p>(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。</p>
ステップ 5	<b>range</b> <i>ip multicast address</i>  例 :  <pre>Switch(config-igmp-profile)# range 229.9.9.0</pre>	<p>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。</p> <p><b>range</b> コマンドを複数回入力すると、複数のアドレスまたはアドレス範囲を入力できます。</p> <p>(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、<b>no range ip multicast address</b> 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。</p>

	コマンドまたはアクション	目的
ステップ 6	<b>end</b>  例 : Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show ip igmp profile</b> <i>profile number</i>  例 : Switch# <b>show ip igmp profile 3</b>	プロファイルの設定を確認します。
ステップ 8	<b>show running-config</b>  例 : Switch# <b>show running-config</b>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b>  例 : Switch# <b>copy running-config startup-config</b>	(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。

#### 関連トピック

[IGMP フィルタリングおよびスロットリング, \(15 ページ\)](#)

[IGMP スヌーピングの制約事項, \(3 ページ\)](#)

## 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. **configureterminal**
3. **interfaceinterface-id**
4. **ip igmp filterprofile 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	<b>enable</b>  例 : Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例 : Switch# <b>configure terminal</b>	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	<b>interfaceinterface-id</b>  例 : Switch(config)# <b>interface gigabitethernet1/0/1</b>	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	<b>ip igmp filterprofile number</b>  例 : Switch(config-if)# <b>ip igmp filter 321</b>	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、 <b>no ip igmp filterprofile number</b> 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	<b>end</b>  例 : Switch(config-if)# <b>end</b>	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	<b>show running-config</b>  例 : Switch# <b>show running-config</b>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b>  例 : Switch# <b>copy running-config startup-config</b>	(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。

#### 関連トピック

[IGMP フィルタリングおよびスロットリング, \(15 ページ\)](#)

[IGMP スヌーピングの制約事項, \(3 ページ\)](#)

## 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。

#### はじめる前に

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. **configureterminal**
3. **interfaceinterface-id**
4. **ip igmp max-groupsnumber**
5. **end**
6. **show running-config interfaceinterface-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	<b>enable</b>  例 : Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configureterminal</b>  例 : Switch# <b>configure terminal</b>	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	<b>interfaceinterface-id</b>  例 : Switch(config)# <b>interface gigabitethernet1/0/2</b>	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	<b>ip igmp max-groupsnumber</b>  例 : Switch(config-if)# <b>ip igmp max-groups 20</b>	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、 <b>no ip igmp max-groups</b> 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	<b>end</b>  例 : Switch(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config interfaceinterface-id</b>  例 : Switch# <b>show running-config interface gigabitethernet1/0/1</b>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b>  例 : Switch# <b>copy running-config startup-config</b>	（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。

## 関連トピック

[IGMP フィルタリングおよびスロットリング, \(15 ページ\)](#)[IGMP スヌーピングの制約事項, \(3 ページ\)](#)

## 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. **configureterminal**
3. **interfaceinterface-id**
4. **ip igmp max-groups action {deny | replace}**
5. **end**
6. **show running-config interfaceinterface-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	<b>enable</b>  例 : Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configureterminal</b>  例 : Switch# <b>configure terminal</b>	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	<b>interface</b> <i>interface-id</i>  例 :  <pre>Switch(config)# interface gigabitethernet 1/0/1</pre>	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	<b>ip igmp max-groups action {deny   replace}</b>  例 :  <pre>Switch(config-if)# ip igmp max-groups action replace</pre>	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。 <ul style="list-style-type: none"> <li>• <b>deny</b> : レポートを廃棄します。 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、スイッチは、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。</li> <li>• <b>replace</b> : 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、スイッチ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。</li> </ul> スイッチ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、 <b>no ip igmp max-groups action</b> 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	<b>end</b>  例 :  <pre>Switch(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config interface</b> <i>interface-id</i>  例 :  <pre>Switch# show running-config interface gigabitethernet1/0/1</pre>	入力を確認します。

	コマンドまたはアクション	目的
ステップ 7	<b>copy running-config startup-config</b>  例 :  Switch# <b>copy running-config startup-config</b>	(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。

#### 関連トピック

[IGMP フィルタリングおよびスロットリング, \(15 ページ\)](#)

[IGMP スヌーピングの制約事項, \(3 ページ\)](#)

## IGMP スヌーピングおよび MVR のモニタリング

### IGMP スヌーピング情報のモニタリング

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
<b>show ip igmp snooping [vlanvlan-id [detail] ]</b>	スイッチ上のすべての 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、 <b>vlanvlan-id</b> 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
<b>show ip igmp snooping groups</b> [count  dynamic [count]   user [count]]	<p>スイッチ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"> <li>• <b>count</b> : 実際のエントリではなく、特定のコマンド オプションのエントリの総数を表示します。</li> <li>• <b>dynamic</b> : 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。</li> <li>• <b>user</b> : ユーザ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。</li> </ul>
<b>show ip igmp snooping groups vlan</b> <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"> <li>• <b>vlan-id</b> : VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。</li> <li>• <b>count</b> : 実際のエントリではなく、特定のコマンド オプションのエントリの総数を表示します。</li> <li>• <b>dynamic</b> : 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。</li> <li>• <b>ip_address</b> : 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。</li> <li>• <b>user</b> : ユーザ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。</li> </ul>
<b>show ip igmp snooping mrouter</b> [ <i>vlanvlan-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>(任意) 特定の VLAN に関する情報を表示するには、<b>vlanvlan-id</b> を入力します。</p>
<b>show ip igmp snooping querier</b> [ <i>vlanvlan-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
<b>show mvr</b>	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。
<b>show mvr interface</b> [interface-id] <b>[members</b> [vlanvlan-id]]	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。  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。  <ul style="list-style-type: none"> <li>• Type : Receiver または Source</li> <li>• Status : 次のいずれか <ul style="list-style-type: none"> <li>◦ ACTIVE は、ポートが VLAN に含まれていることを意味します。</li> <li>◦ 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。</li> <li>◦ INACTIVE は、ポートが VLAN に含まれていないことを意味します。</li> </ul> </li> <li>• Immediate Leave : Enabled または Disabled</li> </ul> <b>members</b> 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、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。
<b>show mvr members</b> [ip-address]	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 フィルタリングおよび IGMP スロットリングの設定のモニタリング

IGMP プロファイルの特性を表示したり、スイッチ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、スイッチ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 フィルタリングおよび IGMP 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
<b>show ip igmp profile</b> [ <i>profile number</i> ]	特定の IGMP プロファイルまたはスイッチ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。
<b>show running-config</b> [ <i>interface interface-id</i> ]	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スイッチ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。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
Switch(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。

```
Switch configure terminal
Switch ip igmp snooping vlan 200 mrouter interface gigabitethernet1/0/2
Switch end
```

## 関連トピック

[マルチキャスト ルータ ポートの設定, \(21 ページ\)](#)

## 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。

```
Switch# configure terminal
Switch# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet1/0/1
Switch# end
```

## 関連トピック

[グループに加入するホストの静的な設定, \(23 ページ\)](#)[マルチキャスト グループへの加入, \(6 ページ\)](#)

## 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。

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

## 関連トピック

[IGMP 即時脱退のイネーブル化, \(24 ページ\)](#)[即時脱退, \(9 ページ\)](#)

## 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。

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

## 関連トピック

[IGMP スヌーピング クエリアの設定, \(32 ページ\)](#)[IGMP スヌーピング, \(5 ページ\)](#)

## 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。

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

#### 関連トピック

[IGMP スヌーピング クエリアの設定, \(32 ページ\)](#)

[IGMP スヌーピング, \(5 ページ\)](#)

## 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。

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

#### 関連トピック

[IGMP スヌーピング クエリアの設定, \(32 ページ\)](#)

[IGMP スヌーピング, \(5 ページ\)](#)

## 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。

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

#### 関連トピック

[IGMP スヌーピング クエリアの設定, \(32 ページ\)](#)

[IGMP スヌーピング, \(5 ページ\)](#)

## 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。

```
Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# 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。

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip igmp filter 4
```

## 例：IGMP グループの最大数の設定

```
Switch(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。

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

```
Switch(config)# mvr
Switch(config)# mvr group 228.1.23.4
Switch(config)# mvr querytime 10
Switch(config)# mvr vlan 22
Switch(config)# mvr mode dynamic
Switch(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。

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

```
Port Type Status Immediate Leave
----
G11/0/2 RECEIVER ACTIVE/DOWN ENABLED
```