



CHAPTER 20

IGMP スヌーピングおよび MVR の設定

この章では、Internet Group Management Protocol (IGMP) スヌーピングを Catalyst 2960 スイッチ上で設定する方法について、ローカル IGMP スヌーピング、Multicast VLAN Registration (MVR) の適用を含めて説明します。また、IGMP フィルタリングを使用したマルチキャスト グループ メンバシップの制御と、IGMP スロットリング アクションの設定手順についても説明します。



(注)

この章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スイッチ コマンド リファレンスおよび『Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.2』の「IP Multicast Routing Commands」のセクションを参照してください。これには、Cisco.com のホームページ (**Documentation > Cisco IOS Software > 12.2 Mainline > Command References**) からアクセス可能です。

この章で説明する内容は、次のとおりです。

- 「IGMP スヌーピングの概要」 (P.20-1)
- 「IGMP スヌーピングの設定」 (P.20-7)
- 「IGMP スヌーピング情報の表示」 (P.20-16)
- 「MVR の概要」 (P.20-18)
- 「MVR の設定」 (P.20-20)
- 「MVR 情報の表示」 (P.20-24)
- 「IGMP フィルタリングおよびスロットリングの設定」 (P.20-24)
- 「IGMP フィルタリングおよび IGMP スロットリング設定の表示」 (P.20-29)



(注)

IGMP スヌーピング、MVR などの機能を使用して IP マルチキャスト グループ アドレスを管理することもできますし、スタティック IP アドレスを使用することもできます。

IGMP スヌーピングの概要

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だけ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、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、ホストから IGMP レポートを受信したスイッチは、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 に一般クエリーを定期的送信します。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 (メディア アクセス制御) 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 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。IGMP スヌーピング クエリーの詳細については、「[IGMP スヌーピング クエリアの設定](#)」(P.20-14) を参照してください。

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

ここでは、IGMP スヌーピングの特性について説明します。

- 「[IGMP バージョン](#)」(P.20-3)
- 「[マルチキャスト グループへの加入](#)」(P.20-3)
- 「[マルチキャスト グループからの脱退](#)」(P.20-5)
- 「[即時脱退](#)」(P.20-6)
- 「[IGMP 脱退タイマーの設定](#)」(P.20-6)
- 「[IGMP レポート抑制](#)」(P.20-6)

IGMP 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 3 つのバージョンは、スイッチ上でそれぞれ相互運用できます。たとえば、IGMPv2 スイッチ上で IGMP スヌーピングがイネーブルの場合、このスイッチが IGMPv3 レポートをホストから受信すると、この IGMPv3 レポートをマルチキャスト ルータへ転送できます。



(注) スイッチは、宛先マルチキャスト MAC アドレスのみに基づいて IGMPv3 スヌーピングをサポートしています。送信元 MAC アドレスやプロキシ レポートに基づいてスヌーピングをサポートすることはありません。

IGMPv3 スイッチは、Basic IGMPv3 Snooping Support (BISS) をサポートしています。BISS は、IGMPv1 および IGMPv2 スイッチでのスヌーピング機能と、IGMPv3 メンバシップ レポート メッセージをサポートしています。ネットワークに IGMPv3 ホストがある場合、BISS によりマルチキャスト トラフィックのフラッディングは抑制されます。トラフィックは、IGMPv2 または IGMPv1 ホストの IGMP スヌーピング機能の場合とほぼ同じポート セットに抑制されます。



(注) IGMP フィルタリングまたは 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ていません。

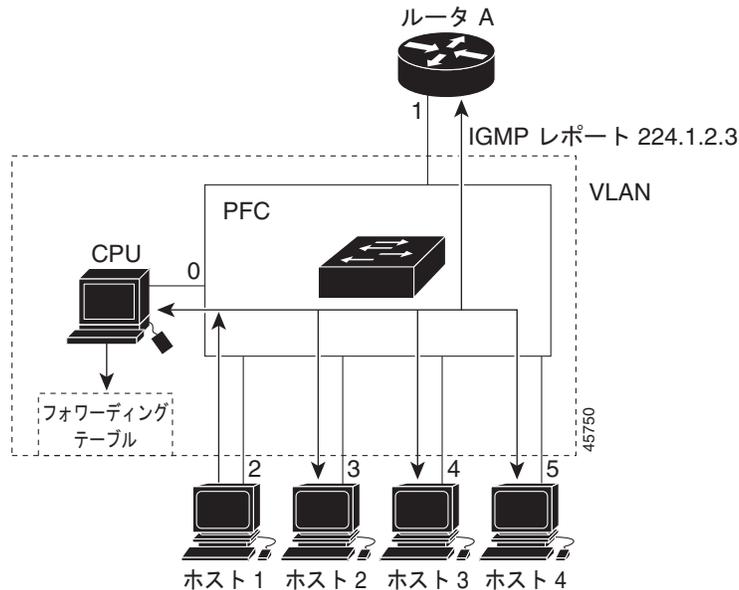
IGMPv3 スイッチは、Source Specific Multicast (SSM) 機能を実行しているデバイスとメッセージの送受信を行うことができます。IGMPv3 および IGMP の送信元固有のマルチキャストの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a008008048a.html

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 20-1 を参照してください。

図 20-1 IGMP Join の初期メッセージ



ルータ A がスイッチに一般クエリーを送り、スイッチはそのクエリーをポート 2 ~ 5、つまり同一 VLAN のすべてのメンバーに転送します。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 (表 20-1 を参照)。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 20-1 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、マルチキャストグループの他のパケットと IGMP 情報パケットを区別できます。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）が同じグループに非請求の IGMP Join メッセージを送信する場合（図 20-2 を参照）、CPU はメッセージを受信して、転送テーブルにホスト 4 のポート番号を追加します（表 20-2 を参照）。転送テーブルによって、CPU だけに IGMP メッセージが転送されるので、スイッチ上の他のポートにメッセージがフラッディングされることはありません。既知のマルチキャストトラフィックはすべて、CPU ではなくグループに転送されます。

図 20-2 2 番めのホストのマルチキャスト グループへの加入

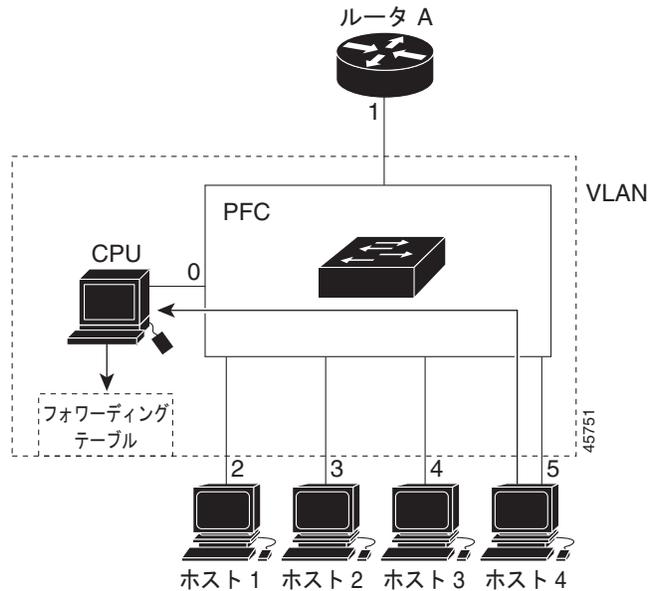


表 20-2 更新された IGMP スヌーピング転送テーブル

| 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ーを定期的送信し、スイッチはそれらのクエリーを VLAN のすべてのポートを通じて転送します。関心のあるホストがクエリーに応答します。VLAN 内の少なくとも 1 つのホストがマルチキャストトラフィックを受信しなければならない場合、ルータは VLAN に引き続き、マルチキャストトラフィックを転送します。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。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

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼動しているホストだけです。

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。



(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。1 つのポートに複数のホストが接続されている VLAN で即時脱退機能をイネーブルにすると、一部のホストが誤って切断される可能性があります。

設定手順については、「[IGMP 即時脱退のイネーブル化](#)」(P.20-11) を参照してください。

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あと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 ~ 5000 ミリ秒の間で設定できます。タイマーはグローバルにまたは VLAN 単位で設定できますが、VLAN に脱退時間を設定すると、グローバルに設定した脱退時間は上書きされます。

設定手順については、「[IGMP 脱退タイマーの設定](#)」(P.20-11) を参照してください。

IGMP レポート抑制



(注) IGMP レポート抑制がサポートされるのは、マルチキャスト クエリーが IGMPv1 および IGMPv2 レポートを持つ場合だけです。クエリーに IGMPv3 レポートがある場合、この機能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の場合 (デフォルト)、このスイッチは、グループに対応するすべてのホストからの最初の IGMP レポートを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、グループに対応する残りの IGMP レポートについては、マルチキャスト ルータに送信しません。この機能により、重複したレポートがマルチキャスト デバイスに送信されるのを防ぎます。

マルチキャスト ルータのクエリーに、IGMPv1 および IGMPv2 レポートだけに対応したレポートが含まれている場合、スイッチはグループ内のすべてのホストから、最初の IGMPv1 または IGMPv2 レポートだけを、すべてのマルチキャスト ルータに転送します。

また、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ている場合、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。設定手順については、「[IGMP レポート抑制のディセーブル化](#)」(P.20-16) を参照してください。

IGMP スヌーピングの設定

IGMP スヌーピングにより、スイッチで IGMP パケットを調べたり、パケットの内容に基づいて転送先を決定したりできます。ここでは、次の設定情報について説明します。

- 「IGMP スヌーピングのデフォルト設定」 (P.20-7)
- 「IGMP スヌーピングのイネーブル化およびディセーブル化」 (P.20-7)
- 「スヌーピング方法の設定」 (P.20-8)
- 「マルチキャスト ルータ ポートの設定」 (P.20-9)
- 「グループに加入するホストの静的な設定」 (P.20-10)
- 「IGMP 即時脱退のイネーブル化」 (P.20-11)
- 「IGMP 脱退タイマーの設定」 (P.20-11)
- 「TCN 関連のコマンドの設定」 (P.20-12)
- 「IGMP スヌーピング クエリアの設定」 (P.20-14)
- 「IGMP レポート抑制のディセーブル化」 (P.20-16)

IGMP スヌーピングのデフォルト設定

表 20-3 に、IGMP スヌーピングのデフォルト設定を示します。

表 20-3 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 |
| マルチキャスト ルータの学習 (スヌーピング) 方式 | PIM-DVMRP |
| 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 フラッドクエリー 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 |

1. TCN = Topology Change Notification (トポロジ変更通知)

IGMP スヌーピングのイネーブル化およびディセーブル化

デフォルトでは、IGMP スヌーピングはスイッチ上でグローバルにイネーブルです。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、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です。デフォルトでは、IGMP スヌーピングはすべての VLAN でイネーブルですが、VLAN 単位で IGMP スヌーピングをイネーブルおよびディセーブルに設定できます。

■ IGMP スヌーピングの設定

グローバル IGMP スヌーピングは、VLAN IGMP スヌーピングよりも優先されます。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。

スイッチ上で IGMP スヌーピングをグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|---|---|
| ステップ 1 | <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 2 | <code>ip igmp snooping</code> | 既存のすべての VLAN インターフェイスで、IGMP スヌーピングをグローバルにイネーブルにします。 |
| ステップ 3 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ 4 | <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。 |

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。

特定の 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するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|---|---|
| ステップ 1 | <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 2 | <code>ip igmp snooping vlan <i>vlan-id</i></code> | 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。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 (注) VLAN スヌーピングをイネーブルにするには、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。 |
| ステップ 3 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ 4 | <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。 |

特定の VLAN インターフェイス上で IGMP スヌーピングをディセーブルにするには、**no ip igmp snooping vlan *vlan-id*** グローバル コンフィギュレーション コマンドを、指定した VLAN 番号に対して使用します。

ス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 Distance Vector Multicast Routing Protocol (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) パケットの待ち受け
- **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 パケットと 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。



(注) 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。

VLAN インターフェイスがマルチキャスト ルータに動的にアクセスする方法を変更するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|--|---|
| ステップ 1 | 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 2 | ip igmp snooping vlan <i>vlan-id</i> mrouter learn {cgmp pim-dvmrp} | VLAN で IGMP スヌーピングをイネーブルにします。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 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用です。 • pim-dvmrp : IGMP クエリーおよび PIM パケットと DVMRP パケットをスヌーピングします。これがデフォルトです。 |
| ステップ 3 | end | 特権 EXEC モードに戻ります。 |
| ステップ 4 | show ip igmp snooping | 設定を確認します。 |
| ステップ 5 | 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。 |

デフォルトの学習方式に戻すには、**no 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。

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
```

マルチキャスト ルータ ポートの設定

マルチキャスト ルータ ポートを追加 (マルチキャスト ルータに静的な接続を追加) するには、スイッチ上で **ip igmp snooping vlan mrouter** 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。

■ IGMP スヌーピングの設定

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には、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|---|---|
| ステップ 1 | <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 2 | <code>ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i></code> | 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"> VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 インターフェイスは物理インターフェイスにすることもポートチャネルにすることもできます。指定できるポートチャネルの範囲は 1 ~ 6 です。 |
| ステップ 3 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ 4 | <code>show ip igmp snooping mrouter [vlan <i>vlan-id</i>]</code> | 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 5 | <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。 |

VLAN からマルチキャスト ルータ ポートを削除するには、`no ip igmp snooping vlan vlan-id mrouter interface interface-id` グローバル コンフィギュレーション コマンドを使用します。

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(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet0/2
Switch(config)# end
```

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、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|--|---|
| ステップ 1 | <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 2 | <code>ip igmp snooping vlan <i>vlan-id</i> static <i>ip_address</i> interface <i>interface-id</i></code> | マルチキャスト グループのメンバーとしてレイヤ 2 ポートを静的に設定します。 <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。VLAN ID の範囲は 1 ~ 1001 および 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、メンバー ポートです。物理インターフェイスまたはポートチャネル (1 ~ 6) に設定できます。 |
| ステップ 3 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ 4 | <code>show ip igmp snooping groups</code> | メンバー ポートおよび IP アドレスを確認します。 |
| ステップ 5 | <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。 |

マルチキャストグループからレイヤ 2 ポートを削除するには、**no ip igmp snooping vlan *vlan-id* static ip-address interface *interface-id*** グローバル コンフィギュレーション コマンドを使用します。

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(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet0/1
Switch(config)# end
```

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。即時脱退機能を使用するのは、VLAN の各ポート上にレシーバーが 1 つだけ存在する場合に限定してください。



(注) 即時脱退機能をサポートするのは、IGMP バージョン 2 が稼動しているホストだけです。

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

| | コマンド | 目的 |
|--------|---|--|
| ステップ 1 | 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 2 | ip igmp snooping vlan <i>vlan-id</i> 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。 |
| ステップ 3 | end | 特権 EXEC モードに戻ります。 |
| ステップ 4 | show ip igmp snooping vlan <i>vlan-id</i> | 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。 |
| ステップ 5 | 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 上で IGMP 即時脱退をディセーブルにするには、**no ip igmp snooping vlan *vlan-id* immediate-leave** グローバル コンフィギュレーション コマンドを使用します。

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
```

IGMP 脱退タイマーの設定

IGMP 脱退タイマーを設定するときには、次の注意事項に従ってください。

- 脱退時間はグローバルまたは VLAN 単位で設定できます。
- 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。
- デフォルトの脱退時間は 1000 ミリ秒です。
- IGMP の脱退時間の設定は、IGMP バージョン 2 が稼動しているホストでのみサポートされます。
- 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 脱退タイマーの設定をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|--|---|
| ステップ 1 | <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 2 | <code>ip igmp snooping last-member-query-interval time</code> | グローバルに IGMP 脱退タイマーを設定します。指定できる範囲は 100 ~ 5000 ミリ秒です。デフォルト値は 1000 秒です。 |
| ステップ 3 | <code>ip igmp snooping vlan vlan-id last-member-query-interval time</code> | (任意) VLAN インターフェイス上で、IGMP 脱退タイマーを設定します。指定できる範囲は 100 ~ 5000 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。 |
| ステップ 4 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ 5 | <code>show ip igmp snooping</code> | (任意) 設定された IGMP 脱退タイマーを表示します。 |
| ステップ 6 | <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 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。

特定の VLAN から IGMP 脱退タイマーの設定を削除するには、**no ip igmp snooping vlan vlan-id last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。

TCN 関連のコマンドの設定

ここでは、TCN イベント中にフラッディングしたマルチキャスト トラフィックを制御する方法を説明します。

- ・「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」(P.20-12)
- ・「フラッディング モードからの回復」(P.20-13)
- ・「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」(P.20-13)

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

ip igmp snooping tcn flood query count グローバル コンフィギュレーション コマンドを使用して、TCN イベント後にフラッディングするマルチキャスト トラフィックの時間を制御できます。このコマンドは、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します。クライアントが場所を変更することで同ポートの受信者がブロックされたあと、現在転送中の場合、またはポートが Leave メッセージを送信せずにダウンした場合などが、TCN イベントに該当します。

ip igmp snooping tcn flood query count コマンドを使用して、TCN フラッディング クエリー カウントを 1 に設定した場合、一般クエリーを 1 つ受信するまでフラッディングが続きます。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クエリーに基づいて再度学習されます。

TCN フラッディング クエリー カウントを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|-------|---|--|
| ステップ1 | 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2 | ip igmp snooping tcn flood query count <i>count</i> | マルチキャスト トラフィックのフラッディングに使用する一般 IGMP 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。 |
| ステップ3 | end | 特権 EXEC モードに戻ります。 |
| ステップ4 | show ip igmp snooping | TCN の設定を確認します。 |
| ステップ5 | 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。 |

デフォルトのフラッディング クエリー カウントに戻す場合は、**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。

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、**ip igmp snooping tcn query solicit** グローバル コンフィギュレーション コマンドをイネーブルにしている場合、スイッチはスパニング ツリーのルートであるかどうかに関わらず、グローバル Leave メッセージを送信します。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 モードからの回復に努めます。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 コマンドに関係なく、Leave メッセージが常に送信されます。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。

スイッチがスパニング ツリー ルートであるかどうかに関わらず、グローバル Leave メッセージを送信するように設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|-------|---|--|
| ステップ1 | 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2 | ip igmp snooping tcn query solicit | IGMP Leave (グローバル Leave) メッセージを送信し、TCN イベント中のフラッディング モードからの回復を促します。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。 |
| ステップ3 | end | 特権 EXEC モードに戻ります。 |
| ステップ4 | show ip igmp snooping | TCN の設定を確認します。 |
| ステップ5 | 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。 |

デフォルトのクエリー送信要求に戻す場合は、**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。

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。その場合、**ip igmp snooping tcn flood** インターフェイス コンフィギュレーション コマンドを使用して、この状態を制御できます。

インターフェイス上でマルチキャスト フラッディングをディセーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|---|---|
| ステップ 1 | <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 2 | <code>interface interface-id</code> | 設定する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。 |
| ステップ 3 | <code>no ip igmp snooping tcn flood</code> | 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。 |
| ステップ 4 | <code>exit</code> | 特権 EXEC モードに戻ります。 |
| ステップ 5 | <code>show ip igmp snooping</code> | TCN の設定を確認します。 |
| ステップ 6 | <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。 |

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場合、`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。

IGMP スヌーピング クエリアの設定

IGMP スヌーピング クエリアを設定するときには、次の注意事項に従ってください。

- 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。イネーブルになると、IGMP スヌーピング クエリアはクエリー送信元アドレスとして IP アドレスを使用します。
- 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 Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) 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、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せん。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

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、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|---------|---|--|
| ステップ 1 | <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 2 | <code>ip igmp snooping querier</code> | IGMP スヌーピング クエリア機能をイネーブルにします。 |
| ステップ 3 | <code>ip igmp snooping querier address ip_address</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 アドレスを使用しようとします。 (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 一般クエリを生成しません。 |
| ステップ 4 | <code>ip igmp snooping querier query-interval interval-count</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 5 | <code>ip igmp snooping querier tcn query [count count interval interval]</code> | (任意) Topology Change Notification (TCN; トポロジ変更通知) 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 6 | <code>ip igmp snooping querier timer expiry timeout</code> | (任意) IGMP クエリアが期限切れになるまでの時間を設定します。指定できる範囲は 60 ~ 300 秒です。 |
| ステップ 7 | <code>ip igmp snooping querier version version</code> | (任意) クエリア機能が使用する IGMP バージョン番号 1 または 2 を選択します。 |
| ステップ 8 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ 9 | <code>show ip igmp snooping vlan vlan-id</code> | (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。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 |
| ステップ 10 | <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。 |

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
```

次に、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する例を示します。

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

次に、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する例を示します。

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

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
```

IGMP レポート抑制のディセーブル化



(注) IGMP レポート抑制がサポートされるのは、マルチキャスト クエリーが IGMPv1 および IGMPv2 レポートを持つ場合だけです。クエリーに IGMPv3 レポートがある場合、この機能はサポートされません。

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。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 レポート抑制をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|---|-----------------------------------|
| ステップ 1 | 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 2 | no ip igmp snooping report-suppression | IGMP レポート抑制をディセーブルにします。 |
| ステップ 3 | end | 特権 EXEC モードに戻ります。 |
| ステップ 4 | show ip igmp snooping | IGMP レポート抑制がディセーブルになっていることを確認します。 |
| ステップ 5 | 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 レポート抑制を再びイネーブルにする場合は、**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。

IGMP スヌーピング情報の表示

動的に学習された、あるいは静的に設定されたルータ ポートおよび VLAN インターフェイスに関する 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。

IGMP スヌーピング情報を表示するには、表 20-4 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 20-4 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 |
|---|---|
| <code>show ip igmp snooping [vlan <i>vlan-id</i>]</code> | <p>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。</p> <p>(任意) 個々の VLAN に関する情報を表示するには、vlan <i>vlan-id</i> を入力します。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。</p> |
| <code>show ip igmp snooping groups [count dynamic [count] user [count]]</code> | <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"> • count : 実際のエントリではなく、特定のコマンド オプションに対応するエントリの総数を表示します。 • 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。 |
| <code>show ip igmp snooping groups vlan <i>vlan-id</i> [<i>ip_address</i> count dynamic [count] user[count]]</code> | <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"> • vlan-id : VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 • count : 実際のエントリではなく、特定のコマンド オプションに対応するエントリの総数を表示します。 • 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。 • ip_address : 指定のグループ IP アドレスのマルチキャスト グループについて、特性を表示します。 • user : 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。 |
| <code>show ip igmp snooping mrouter [vlan <i>vlan-id</i>]</code> | <p>動的に学習された、あるいは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) 個々の VLAN に関する情報を表示するには、vlan <i>vlan-id</i> を入力します。</p> |
| <code>show ip igmp snooping querier [vlan <i>vlan-id</i>]</code> | <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を表示します。</p> <p>(任意) 個々の VLAN に関する情報を表示するには、vlan <i>vlan-id</i> を入力します。</p> |
| <code>show ip igmp snooping querier [vlan <i>vlan-id</i>] detail</code> | <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> |

各コマンドのキーワードおよびオプションの詳細については、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。

MVR の概要

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 ネットワークにおいて、マルチキャスト トラフィックを大規模展開するアプリケーション（サービス プロバイダー ネットワークによる複数のテレビ チャンネルのブロードキャストなど）を想定して開発されました。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。加入者は別個の VLAN 上にありながら、ネットワークで単一マルチキャスト VLAN を共有できます。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。

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、イーサネットで接続され、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カニズムで動作しますが、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。

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ー 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、スイッチのすべての 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。

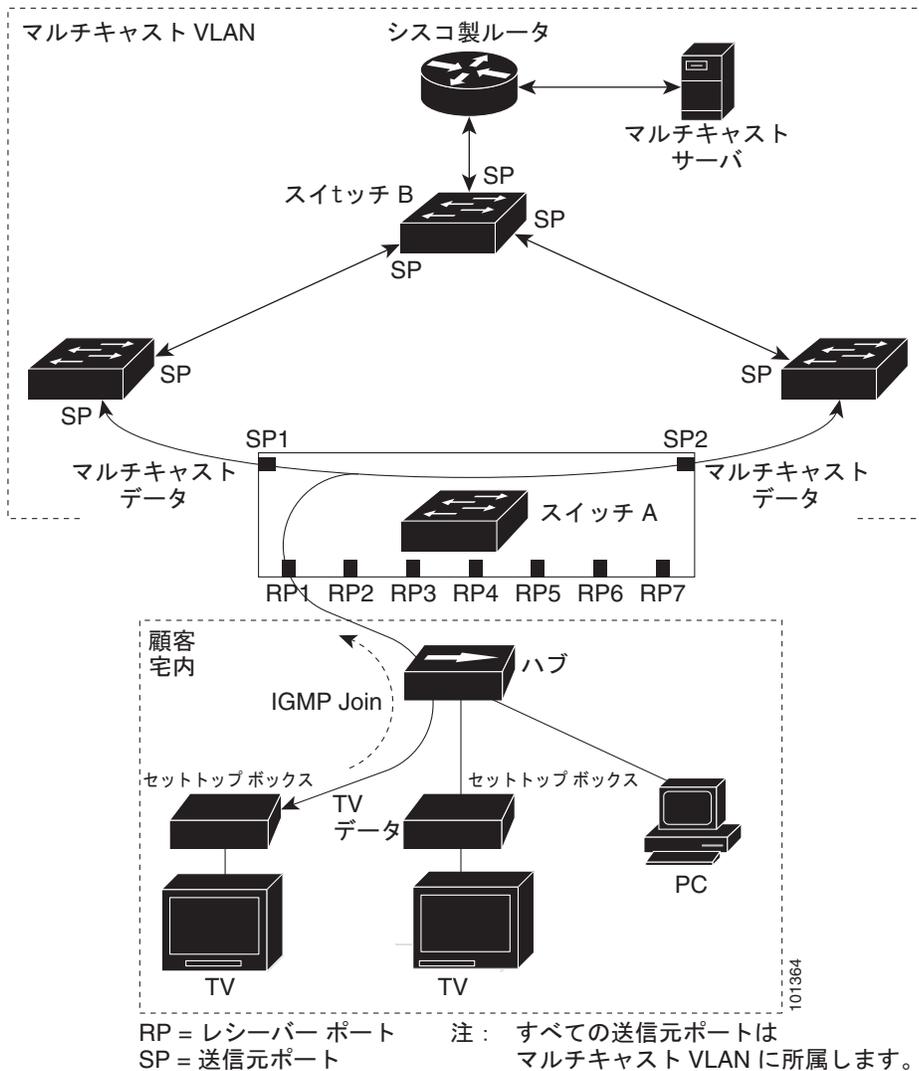
MVR に関与するのはレイヤ 2 ポートだけです。ポートを MVR レシーバー ポートとして設定する必要があります。各スイッチ スタックでサポートされる MVR マルチキャスト VLAN は、1 つだけです。

マルチキャスト TV アプリケーションで MVR を使用する場合

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 レシーバー ポートとして設定されたスイッチ ポートです。

図 20-3 に構成例を示します。Dynamic Host Configuration Protocol (DHCP) はセットトップ ボックスまたは PC に IP アドレスを割り当てます。加入者がチャンネルを選択すると、セットトップ ボックスまたは PC からスイッチ A に、所定のマルチキャストに加入するための 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、レシーバー 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 送信元ポートといいます。

図 20-3 MVR の例



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、レシーバー ポートの VLAN 経由で MAC ベースの一般クエリーを送信します。VLAN に、同じ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 はそのグループの転送先としてのレシーバー ポートを除外します。

即時脱退機能を使用しない場合、レシーバー 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が届かないと、レシーバー ポートがマルチキャスト グループ メンバ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ー 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、マルチキャスト グループ メンバシップからレシーバー ポートが削除されるので、脱退のための待ち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ー デバイスが 1 つだけのレシーバー ポートに限定してください。

MVR を使用すると、VLAN ごとに加入者用のテレビ チャンネル マルチキャスト トラフィックを複製しなくて済みます。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 トランク全体で 1 回送信されます。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 に送られます。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) が転送動作を変更し、マルチキャスト VLAN から別個の VLAN 上の加入者ポートへトラフィックを転送できるようにするので、選択されたトラフィックが 2 つの VLAN 間を伝送されます。

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、レシーバー 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 の設定

ここでは、次の設定情報について説明します。

- 「MVR のデフォルト設定」 (P.20-20)
- 「MVR 設定時の注意事項および制限事項」 (P.20-21)
- 「MVR グローバル パラメータの設定」 (P.20-21)
- 「MVR インターフェイスの設定」 (P.20-23)

MVR のデフォルト設定

表 20-5 に、MVR のデフォルト設定を示します。

表 20-5 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 |

表 20-5 MVR のデフォルト設定 (続き)

| 機能 | デフォルト設定 |
|------------------------|-----------------------|
| マルチキャスト VLAN | VLAN 1 |
| モード | compatible |
| インターフェイスのデフォルト (ポート単位) | レシーバー 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 |

MVR 設定時の注意事項および制限事項

MVR を設定するときには、次の注意事項に従ってください。

- レシーバー 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 ポートにすることはできません。スイッチ上のレシーバー ポートは、異なる VLAN に所属していてもかまいませんが、マルチキャスト VLAN には所属させないでください。
- スイッチ上で設定できるマルチキャスト エントリ (MVR グループ アドレス) の最大数 (受信できるテレビチャンネルの最大数) は 256 です。
- 送信元 VLAN で受信され、レシーバー 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 Time to Live (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の 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 スイッチと相互運用している場合は、相互間でエイリアスとなる、または予約済みの IP マルチキャスト アドレス (224.0.0.xxx の範囲) を使用して IP アドレスを設定しないでください。
- MVR はスイッチ上で IGMP スヌーピングと共存できます。
- MVR レシーバー 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。

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。

MVR パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|---------------------------------|------------------------------|
| ステップ 1 | <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 2 | <code>mvr</code> | スイッチ上で MVR をイネーブルに設定します。 |

MVR の設定

| | コマンド | 目的 |
|--------|---|--|
| ステップ 3 | mvr group ip-address [count] | 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、連続する MVR グループ アドレスを設定します (<i>count</i> の範囲は 1 ~ 256、デフォルトは 1)。このアドレスに送信されたマルチキャスト データは、スイッチ上のすべての送信元ポートおよびそのマルチキャスト アドレスのデータを受信するために選ばれたすべてのレシーバー 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。 |
| ステップ 4 | mvr querytime value | (任意) マルチキャスト グループ メンバシップからポートを削除する前に、レシーバー ポートで IGMP レポートのメンバシップを待機する最大時間を設定します。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、すなわち 0.5 秒です。 |
| ステップ 5 | mvr vlan vlan-id | (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をこの VLAN に所属させる必要があります。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 6 | mvr mode {dynamic compatible} | (任意) 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 メンバシップを使用できます。 • compatible : Catalyst 3500 XL スイッチおよび 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。 デフォルトは compatible モードです。 |
| ステップ 7 | end | 特権 EXEC モードに戻ります。 |
| ステップ 8 | show mvr または show mvr members | 設定を確認します。 |
| ステップ 9 | copy running-config startup-config | (任意) コンフィギュレーション ファイルに設定を保存します。 |

スイッチをデフォルトの設定に戻すには、**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。

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
```

show mvr members 特権 EXEC コマンドを使用すると、スイッチ上の MVR マルチキャスト グループ アドレスを確認できます。

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、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|--|--|
| ステップ 1 | <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 2 | <code>mvr</code> | スイッチ上で MVR をイネーブルに設定します。 |
| ステップ 3 | <code>interface interface-id</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 4 | <code>mvr type {source 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。スイッチ上のすべての送信元ポートは、単一マルチキャスト VLAN に所属します。 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、レシーバー ポートとしてポートを設定します。静的に、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。レシーバー 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> |
| ステップ 5 | <code>mvr vlan vlan-id group [ip-address]</code> | <p>(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 メンバーとして静的に設定されたポートは、静的に削除されないかぎり、グループ メンバーのままです。</p> <p>(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ー ポートだけです。ダイナミック モードでは、レシーバー ポートおよび送信元ポートに適用されます。</p> <p>レシーバー 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。</p> |
| ステップ 6 | <code>mvr immediate</code> | <p>(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。</p> <p>(注) このコマンドが適用されるのは、レシーバー ポートだけです。また、イネーブルにするのは、単一のレシーバー デバイスが接続されているレシーバー ポートに限定してください。</p> |
| ステップ 7 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ 8 | <code>show mvr</code> <code>show mvr interface</code> または <code>show mvr members</code> | 設定を確認します。 |
| ステップ 9 | <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。 |

インターフェイスをデフォルトの設定に戻すには、`no mvr [type | immediate | vlan vlan-id | group]` 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。

MVR 情報の表示

次に、ポートをレシーバー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 gigabitethernet0/2
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
----      -
Gi0/2    RECEIVER  ACTIVE/DOWN  ENABLED
```

MVR 情報の表示

スイッチまたは指定されたインターフェイスの MVR 情報を表示できます。MVR の設定を表示するには、特権 EXEC モードで表 20-6 のコマンドを使用します。

表 20-6 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> | すべての MVR インターフェイスおよびそれぞれの 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"> Type : RECEIVER (レシーバー) または SOURCE (送信元) Status : 次のいずれか 1 つ <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 (即時脱退機能) : イネーブルまたはディセーブル 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ーが表示されます。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ーが表示されます。VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。 |
| <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ー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スロットリングの設定

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

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

IGMP フィルタリングで制御されるのは、グループ固有のクエリーおよびメンバシップ 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。

ここでは、次の設定情報について説明します。

- 「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」 (P.20-25)
- 「IGMP プロファイルの設定」 (P.20-26) (任意)
- 「IGMP プロファイルの適用」 (P.20-27) (任意)
- 「IGMP グループの最大数の設定」 (P.20-27) (任意)
- 「IGMP スロットリング アクションの設定」 (P.20-28) (任意)

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

表 20-7 に、IGMP フィルタリングのデフォルト設定を示します。

表 20-7 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 | 適用されない |
| IGMP グループの最大数 | 最大数は設定されない |
| IGMP プロファイル | 未設定 |
| 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 |

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場合、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。設定時の注意事項については、「[IGMP スロットリングアクションの設定](#)」(P.20-28) を参照してください。

IGMP プロファイルの設定

IGMP プロファイルを設定するには、**ip igmp profile** グローバル コンフィギュレーション コマンドおよびプロファイル番号を使用して、IGMP プロファイルを作成し、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。ポートから送信される IGMP Join 要求をフィルタリングするために使用される IGMP プロファイルのパラメータは、このモードから指定できます。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して、プロファイルを作成できます。

- **deny** : 一致するアドレスを拒否します。デフォルトで設定されています。
- **exit** : IGMP プロファイル コンフィギュレーション モードを終了します。
- **no** : コマンドを否定するか、または設定をデフォルトに戻します。
- **permit** : 一致するアドレスを許可します。
- **range** : プロファイルの IP アドレス範囲を指定します。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。

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。プロファイルが設定されており、**permit** および **deny** キーワードがいずれも指定されていない場合、デフォルトでは、IP アドレス範囲へのアクセスが拒否されます。

IGMP プロファイルを作成するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|--|--|
| ステップ 1 | 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 2 | ip igmp profile profile number | 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。プロファイル番号の範囲は 1 ~ 4294967295 です。 |
| ステップ 3 | permit deny | (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 4 | range ip multicast address | アクセスが制御される 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。 |
| ステップ 5 | end | 特権 EXEC モードに戻ります。 |
| ステップ 6 | show ip igmp profile profile number | プロファイルの設定を確認します。 |
| ステップ 7 | 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。 |

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。

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。

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
```

IGMP プロファイルの適用

IGMP プロファイルの定義に従ってアクセスを制御するには、**ip igmp filter** インターフェイス コンフィギュレーション コマンドを使用して、プロファイル該当するインターフェイスに適用します。IGMP プロファイルは、レイヤ 2 アクセス ポートにのみ適用できます。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、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|---|---|
| ステップ 1 | 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 2 | interface interface-id | 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 3 | ip igmp filter profile number | 指定された IGMP プロファイルをインターフェイスに適用します。指定できる範囲は 1 ~ 4294967295 です。 |
| ステップ 4 | end | 特権 EXEC モードに戻ります。 |
| ステップ 5 | show running-config interface interface-id | 設定を確認します。 |
| ステップ 6 | 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。 |

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。

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 gigabitethernet0/2
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
```

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、**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。最大数をデフォルト設定（制限なし）に戻すには、このコマンドの **no** 形式を使用します。

このコマンドは、論理 EtherChannel インターフェイスでは使用できますが、EtherChannel ポート グループに属するポートでは使用できません。

■ IGMP フィルタリングおよびスロットリングの設定

転送テーブルの IGMP グループの最大数を設定するには、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|---|---|
| ステップ 1 | <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 2 | <code>interface interface-id</code> | 設定する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。 |
| ステップ 3 | <code>ip igmp max-groups number</code> | 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。 |
| ステップ 4 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ 5 | <code>show running-config interface interface-id</code> | 設定を確認します。 |
| ステップ 6 | <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。 |

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。

次に、ポートが加入できる IGMP グループ数を 25 に制限する例を示します。

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
```

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あと、`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 コマンドを使用して受信した 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します。IGMP Join レポートを廃棄するデフォルトの設定に戻すには、このコマンドの `no` 形式を使用します。

IGMP スロットリングを設定するときには、次の注意事項に従ってください。

- このコマンドは、論理 EtherChannel インターフェイスでは使用できませんが、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。
 - スロットリングアクションを `deny` に設定すると、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。
 - スロットリングアクションを `replace` に設定すると、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。フォワーディング 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。

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。

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、特権 EXEC モードで次の手順を実行します。

| | コマンド | 目的 |
|--------|---|--|
| ステップ 1 | <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 2 | <code>interface interface-id</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 3 | <code>ip igmp max-groups action {deny replace}</code> | 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"> deny : 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。 |
| ステップ 4 | <code>end</code> | 特権 EXEC モードに戻ります。 |
| ステップ 5 | <code>show running-config interface interface-id</code> | 設定を確認します。 |
| ステップ 6 | <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。 |

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。

IGMP フィルタリングおよび IGMP スロットリング設定の表示

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 20-8 の特権 EXEC コマンドを使用して、IGMP フィルタリングおよび IGMP スロットリングの設定を表示します。

表 20-8 IGMP フィルタリングおよび IGMP スロットリングの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。 |
| <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 フィルタリングおよび IGMP スロットリング設定の表示