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 3550 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、マルチキャスト VLAN レジストレーション（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 メンバーシップの制御と、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） ここで使用されるコマンドの構文および使用方法の詳細については、このリリースのスイッチ 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」を参照してください。

この章の内容は、次のとおりです。



（注） IP マルチキャスト グループにマッピングされる MAC アドレスの場合、IGMP スヌーピングおよび MVR などの機能を使用して管理するか、スタティック MAC アドレスを使用できます。ただし、両方の方法を同時に使用することはできません。したがって、IGMP スヌーピングまたは MVR を使用する前に、静的に設定され、IP マルチキャスト グループにマップされたすべての MAC アドレスを削除する必要があります。

# 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のみ転送されるようにすることによって、マルチキャスト トラフィックのフラッディングを制限できます。名称が示すとおり、IGMP スヌーピングの場合は、LAN 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 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（拡張マルチレイヤ ソフトウェア イメージを搭載した Catalyst 3550 スイッチも含む）は、すべての VLAN に定期的に一般クエリーを送信します。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、IP マルチキャスト グループごとに 1 つの Join 要求のみをマルチキャスト ルータに転送し、IGMP Join 要求を受信する各 MAC グループ用レイヤ 2 転送テーブルで、VLAN あたり 1 つのエントリを生成します。

IGMP スヌーピングを通じて学習されるレイヤ 2 マルチキャスト グループは、ダイナミックです。ただし、**ip igmp snooping vlan static** 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、MAC マルチキャスト グループを静的に設定することができます。グループ メンバーシップをマルチキャスト グループ アドレスに静的に指定すると、その設定値は IGMP スヌーピングによる自動操作より優先されます。マルチキャスト グループ メンバーシップのリストは、ユーザが定義した設定値および IGMP スヌーピングによって学習された設定値の両方で構成できます。

マルチキャスト トラフィックはルーティングする必要がないのでマルチキャスト インターフェイスを使用せずに、サブネットの IGMP スヌーピングをサポートするよう IGMP スヌーピング クエリーを設定できます。IGMP スヌーピング クエリアの詳細については、「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、スイッチの IGMP スヌーピングに関する特性について説明します。

# 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 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 アドレスだけに基づいた IGMPv3 スヌーピングをサポートしています。送信元 MAC アドレスまたはプロキシ レポートに基づくスヌーピングは、サポートしていません。

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 メンバーシップ 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。

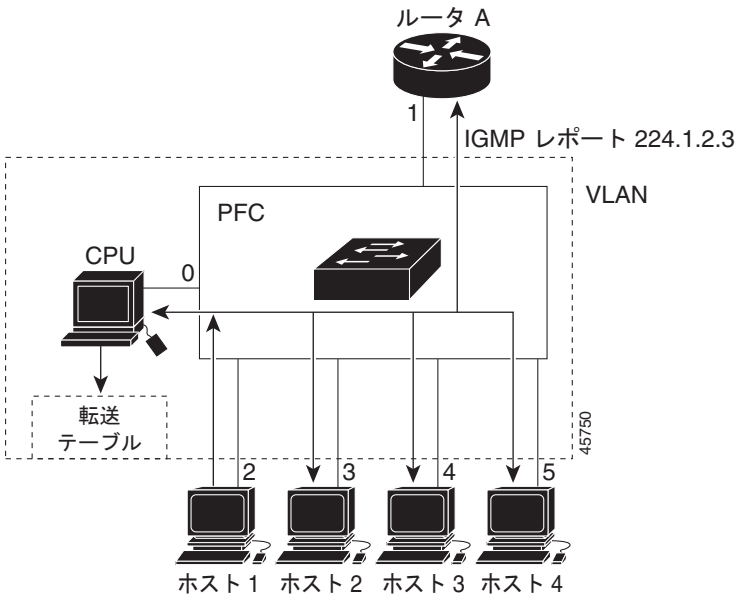
IGMPv3 スイッチは、Source Specific Multicast（SSM）機能を実行しているデバイスとメッセージの送受信を行うことができます。詳細については、次の URL にある『*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, Cisco IOS Release 12.1(12c)EW*』の「Configuring IP Multicast Layer 3 Switching」の章を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_1_12/config/mcastmls.htm

# マルチキャスト グループへの加入

スイッチに接続されているホストは、IP マルチキャスト グループに参加する場合に、参加する IP マルチキャスト グループを指定して、要求されていない IGMP 参加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。マルチキャスト グループに参加するホストは、スイッチに参加メッセージを送信することにより応答します。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　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ーを送信し、スイッチがそのクエリーを同じ 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 への加入を希望し、IGMP メンバーシップ レポート（IGMP Join メッセージ）を同等の MAC 宛先アドレス 0x0100.5E01.0203 を持つグループにマルチキャストします。CPU が、ホスト 1 による IGMP レポート マルチキャストを受信すると、この CPU は IGMP レポート内の情報を利用して、表 20-1 に示すように転送テーブル エントリを設定します。これには、ホスト 1 のポート番号、ルータ、スイッチの内部 CPU 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 |
|---|---|---|
| 0100.5exx.xxxx | IGMP | 0 |
| 0100.5e01.0203 | !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ることに注意してください。

- テーブル中の最初のエントリは、スイッチング エンジンに対して、IGMP パケットをスイッチ CPU だけに送信するように指示します。これによって、CPU がマルチキャスト フレームで過負荷になるのを防止できます。
- 第 2 のエントリは、スイッチング エンジンに、0x0100.5E01.0203 マルチキャスト MAC アドレス宛てのフレームを送信するように指示します。このフレームは、ルータ宛て、およびグループに加入しているホスト宛ての IGPM パケット（!IGMP）ではありません。

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（図 20-2 を参照）、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（表 20-2 を参照）。ただし、転送テーブルにより指定される IGMP メッセージの送信先は CPU に限られるため、スイッチ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。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 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

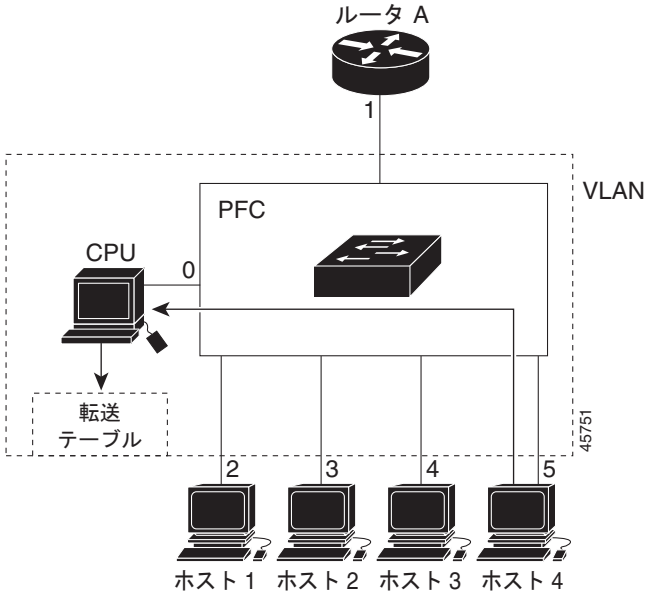



表 20-2　更新された IGMP スヌーピング転送テーブル

| 宛先アドレス | パケットのタイプ | ポート |
|---|---|---|
| 0100.5exx.xxxx | IGMP | 0 |
| 0100.5e01.0203 | !IGMP | 1, 2, 5 |

# 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ーを送信し、スイッチはそれらのクエリーを 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、レイヤ 2 マルチキャスト グループの転送テーブルに含まれるホストだけに、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ときには、ホストは、通知なしで脱退することもできれば、脱退メッセージを送信することもできます。スイッチは、ホストから Leave メッセージを受信すると、MAC ベースの一般クエリーを送出して、そのインターフェイスに接続しているその他のデバイスに、特定のマルチキャスト グループのトラフィックを必要としているものがあるかどうかを判別します。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。

# 即時脱退処理

即時脱退は、IGMP バージョン 2 のホストについてだけサポートされます。

IGMP スヌーピングの即時脱退処理を使用すると、スイッチは、MAC ベースの一般クエリーをインターフェイスに送信することなく、転送テーブルから Leave メッセージを送信するインターフェイスを削除できます。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。即時脱退処理によって、複数のマルチキャスト グループを同時に使用する場合でも、スイッチド ネットワーク上のすべてのホストに対して最適な帯域幅管理を行うことができます。

（注）　即時脱退処理機能は、各ポートに 1 つのホストが接続された VLAN 上だけで使用してください。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。

# IGMP 脱退タイマーの設定

Cisco IOS Release 12.2(25)SEA およびそれよりも前のリリースでは、IGMP スヌーピングの脱退時間は 5 秒間に固定されていました。クエリーのクエリー応答時間が満了する前にスイッチがメンバーシップ レポートを受信しなかった場合、ポートはマルチキャスト グループ メンバーシップから削除されます。ところが、アプリケーションによっては 5 秒未満の Leave 遅延が必要です。

Cisco IOS Release 12.2(25)SEB 以降のリリースでは、ホストの特定マルチキャスト グループへの関心が続いているかどうかを判断するために、グループ固有のクエリーを送信した後にスイッチが待機する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。

## IGMP 脱退タイマーの注意事項

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 が稼働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 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。

# IGMP スヌーピング クエリア設定時の注意事項および制約事項

Catalyst 2955 スイッチで IGMP スヌーピング クエリアを設定するときは、次の注意事項および制約事項に従ってください。

- IGMP スヌーピング クエリアはデフォルトでディセーブルです。
- VLAN をグローバル コンフィギュレーション モードに設定してください。
- IP アドレスおよび VLAN インターフェイスを設定してください。IGMP スヌーピング クエリアは、イネーブルの場合この IP アドレスをクエリーの送信元アドレスとして使用します。
- VLAN インターフェイス上で IP アドレスが設定されていない場合、IGMP スヌーピング クエリアは IGMP クエリア用に設定されたグローバル IP アドレスを使用しようとします。グローバル IP アドレスが指定されていない場合、IGMP クエリアは VLAN スイッチ仮想インターフェイス（SVI）IP アドレス（存在する場合）を使用しようとします。SVI IP アドレスが存在しない場合、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 は、**show ip interface** privileged 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

# Source-Only ネットワーク

送信元限定ネットワークでは、スイッチ ポートはマルチキャスト送信元ポートおよびマルチキャスト ルータ ポートに接続されています。スイッチ ポートは、IGMP Join または Leave メッセージを送信するホストには接続されません。

スイッチは、Source-Only 学習方式を使用して IP マルチキャスト データ ストリームから予約済み、宛先、マルチキャスト IP アドレス（224.0.0.x）でエイリアス指定される IP マルチキャスト グループについて学習します。スイッチは、これらのマルチキャスト アドレスでエイリアス指定されるマルチキャスト ルータ ポートだけにトラフィックを転送します。

予約済み、宛先、マルチキャスト IP アドレスでエイリアス指定されるトラフィックのデフォルトの学習方式は、IP Multicast-Source-Only 学習方式です。これらのマルチキャスト アドレスによってエイリアス指定されないトラフィックは、マルチキャスト送信元ポートおよびマルチキャスト ルータ ポートの両方に転送されます。予約済み、宛先、マルチキャスト IP アドレスに対して、IP マルチキャスト Source-Only 学習をディセーブルにすることはできません。

デフォルトでは、スイッチは、Source-Only 学習方式で学習され、使用されていない転送テーブルを期限切れにします。エージング タイムが長すぎる場合、またはディセーブルの場合には、Source-Only ラーニングを使用するか、または IGMP Join メッセージを使用してスイッチが学習した未使用のエントリによって、転送テーブルが満杯になります。スイッチは、新しい IP マルチキャスト グループのトラフィックを受信すると、そのパケットを同じ VLAN 内のすべてのポートにフラッディングします。この不要なフラッディングは、スイッチのパフォーマンスに影響します。

エージングがディセーブルの場合で、Source-Only ラーニングを使用してスイッチが学習したマルチキャスト アドレスを削除したい場合には、転送テーブル エントリのエージングを再度イネーブルにします。スイッチは、Source-Only 学習方式で学んだ未使用のマルチキャスト アドレスをエージング アウトできます。

# 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。外部のマルチキャスト ルータを検出するために、スイッチ上で IGMP スヌーピングをイネーブルにするには、VLAN のルータのレイヤ 3 インターフェイスは、マルチキャスト ルーティング用にあらかじめ設定されている必要があります。詳細については、第 34 章「IP マルチキャスト ルーティングの設定」を参照してください。

ここでは、IGMP スヌーピングを設定する手順について説明します。



# 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 |

表 20-3　IGMP スヌーピングのデフォルト設定 （続き）

| 機能 | デフォルト設定 |
|---|---|
| マルチキャスト 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 |
| 転送テーブル エントリのエージング（予約済み、宛先、マルチキャスト IP アドレスでエイリアス指定されたトラフィックの場合） | イネーブル デフォルト値は 600 秒（10 分） |
| IGMP レポート抑制 | イネーブル |

# 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。マルチキャスト ルーティング用の VLAN インターフェイスを設定すると、IGMP スヌーピングを使用して外部マルチキャスト ルータにスイッチが動的にアクセスするための設定は必要ありません。

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 | **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** | 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 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **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。 |

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 | **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** *vlan-id* | 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。 |
| ステップ 3 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 4 | **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。 |

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 および proxy-join パケットだけを待ちうけ、その他の CGMP パケットは待ち受けなくなります。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。詳細については、第 34 章「IP マルチキャスト ルーティングの設定」を参照してください。

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** *vlan-id* **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 ～ 4094 です。<br>マルチキャスト ルータの学習方式を指定します。<br>• **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。<br>• **pim-dvmrp**：IGMP クエリーおよび PIM/DVMRP パケットをスヌーピングします。これはデフォルトです。 |
| 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。 |

次に、CGMP パケットを学習方式として使用するように 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
```

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。

# 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。

（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。

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 | **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** *vlan-id* **mrouter interface** *interface-id* | マルチキャスト ルータの VLAN ID を指定し、マルチキャスト ルータへのインターフェイスを指定します。VLAN ID の範囲は 1 ～ 4094 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 mrouter** [**vlan** *vlan-id*] | 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 | **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 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し、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet0/1
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 | **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** *vlan-id* **static** *mac-address* **interface** *interface-id* | 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。<br>• *vlan-id* は、マルチキャスト グループの VLAN ID です。<br>• *mac-address* は、グループ MAC アドレスです。<br>• *interface-id* は、メンバ ポートです。 |
| 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 groups** | メンバ ポートおよび IP アドレスを確認します。 |
| ステップ 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。 |

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、インターフェイス上でホストを静的に設定して、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 static 0100.5e00.0203 interface gigabitethernet0/1
Switch(config)# end
```

# IGMP 即時脱退処理のイネーブル化

IGMP 即時脱退処理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。

即時脱退は、IGMP バージョン 2 のホストでのみサポートされます。

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** *vlan-id* **immediate-leave** | VLAN インターフェイス上で IGMP 即時脱退処理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** *vlan-id* | VLAN 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 の即時脱退処理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 Leave タイマーの設定

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 | **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 last-member-query-interval** *time* | グローバルに IGMP 脱退タイマーを設定します。範囲は 100 ～ 5000 ミリ秒です。 |
| ステップ 3 | **ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *time* | （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。範囲は 100 ～ 5000 ミリ秒です。<br>**（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 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show ip igmp snooping** | （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 | **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 Leave タイマーをグローバルにリセットしてデフォルト設定（1000 ミリ秒）に戻す場合は、**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。

設定した IGMP 脱退時間設定を特定の VLAN から削除する場合は、**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。

# IGMP レポート抑制のディセーブル化

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。

**（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。

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には、**ip igmp snooping report-suppression** グローバル コンフィギュレーション コマンドを使用します。

# エージング タイムの設定

スイッチが IP Multicast-Source-Only 学習方式を使用して学習する、転送テーブル エントリのエージング タイムを設定できます。

エージング タイムを設定するには、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 source-only learning age-timer** *time* | エージング タイムを設定します。範囲は 0 ～ 2880 秒です。デフォルトは 600 秒（10 分）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 running-config \| include source-only-learning** | エージング タイムを確認します。 |
| 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。 |

転送テーブル エントリのエージングをディセーブルにするには、**ip igmp snooping source-only-learning age-timer 0** グローバル コンフィギュレーション コマンドを入力します。

# IGMP スヌーピング クエリアの設定

VLAN の 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。

| | 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 querier** | 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 | **ip igmp snooping querier** *ip_address* | （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。<br>**（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。 |
| ステップ 4 | **ip igmp snooping querier query-interval** *interval-count* | （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 | **ip igmp snooping querier tcn query [count** *count* **\| interval** *interval***]** | （任意）Topology Change Notification（TCN; トポロジ変更通知）クエリーの間隔（秒）を設定します。count の範囲は 1 ～ 10 です。指定できる範囲は 1 ～ 255 秒です。 |
| ステップ 6 | **ip igmp snooping querier timer expiry** *timeout* | （任意）IGMP クエリアが期限切れになるまでの時間（秒）を設定します。指定できる範囲は 60 ～ 300 秒です。 |
| ステップ 7 | **ip igmp snooping querier version** *version* | （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 8 | **end** | 特権 EXEC モードに戻ります。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 9 | **show ip igmp snooping vlan** *vlan-id* | （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。 |
| ステップ 10 | **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。 |

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 に設定して、その設定を確認する例を示します。

```
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 秒に設定して、その設定を確認する方法を示します。

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

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 秒に設定して、その設定を確認する方法を示します。

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

次の例では、IGMP スヌーピング クエリア機能をバージョン 2 に設定して、その設定を確認する方法を示します。

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

# 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 MAC 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 |
|---|---|
| **show ip igmp snooping** [**vlan** *vlan-id*] | 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。<br>（任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。 |
| **show ip igmp snooping groups** [**count** \| **vlan** *vlan-id* [*ip_address* \| **count**]] | スイッチ、マルチキャスト VLAN、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。<br>• **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。<br>• *ip_address*：指定されたグループ IP アドレスを持つマルチキャスト グループの情報を表示します。 |
| **show ip igmp snooping mrouter** [**vlan** *vlan-id*] | 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。<br>**（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。<br>（任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。 |
| **show ip igmp snooping querier** [**vlan** *vlad-id*] | インターフェイスがサポートする IGMP バージョンに関する情報を表示します。<br>（任意）個々の VLAN に関する情報を表示するには、**vlan** *vlan-id* を入力します。 |
| **show mac address-table multicast** [**vlan** *vlan-id*] [**user** \| **igmp-snooping**] [**count**] | VLAN に関するレイヤ 2 MAC アドレス テーブル エントリを表示します。キーワードはすべてオプションであり、次のように表示を限定します。<br>• **vlan** *vlan-id*：指定されたマルチキャスト グループ VLAN だけを表示します。<br>• **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。<br>• **igmp-snooping**：IGMP スヌーピングによって学習されたエントリだけを表示します。<br>• **count**：実際のエントリではなく、選択された基準の総エントリ数だけが表示されます。 |

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。

表 20-4 にあるコマンドの出力例については、このリリースのコマンド リファレンスを参照してください。

# MVR の概要

Multicast VLAN Registration（MVR; マルチキャスト VLAN レジストレーション）は、イーサネット リングベースのサービス プロバイダー ネットワークで、マルチキャスト トラフィックを広範囲に配信する用途（サービス プロバイダー ネットワークでの複数の TV チャネルのブロードキャストなど）用に設計された機能です。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。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 MAC アドレスを識別し、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 動作には、dynamic と compatible というモードがあります。

- MVR のダイナミック モードを使用する場合、スイッチは標準の IGMP スヌーピングを実行します。IGMP 情報パケットはスイッチの CPU に送信されますが、マルチキャスト データ パケットは CPU に送信されません。dynamic モードでは、マルチキャスト ルータは正常に動作します。その理由は、スイッチが IGMP Join メッセージをルータに送信し、次にルータは、各グループのインターフェイスから Join メッセージを受信した場合のみ、そのグループのマルチキャスト ストリームをインターフェイスに転送するためです。受信ポートは、MVR マルチキャスト制御トラフィックとデータ トラフィックについて、マルチキャスト VLAN のメンバとして扱われます。MVR グループの IGMP レポートは、マルチキャスト VLAN で送信元ポートに送信されます。
- MVR 互換モードで、Catalyst 3550 スイッチ上の MVR は、Catalyst 3500 XL および Catalyst 2900 XL スイッチ上の MVR と相互動作します。これは、すべてのマルチキャスト データ パケットと、IGMP クエリーおよび脱退パケットについて、ダイナミック モードと同様に動作します。ただし、受信された MVR グループに関する IGMP レポート パケットは、マルチキャスト VLAN 送信元ポート上に送信されません。dynamic モードとは対照的に、スイッチは Join メッセージをルータに送信しません。マルチキャスト ストリームを受信するためには、インターフェイスに対してルータが静的に設定されている必要があります。したがって、このモードでは、MVR は、送信元ポート上でのダイナミック メンバーシップ Join をサポートしません。

（注）　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。

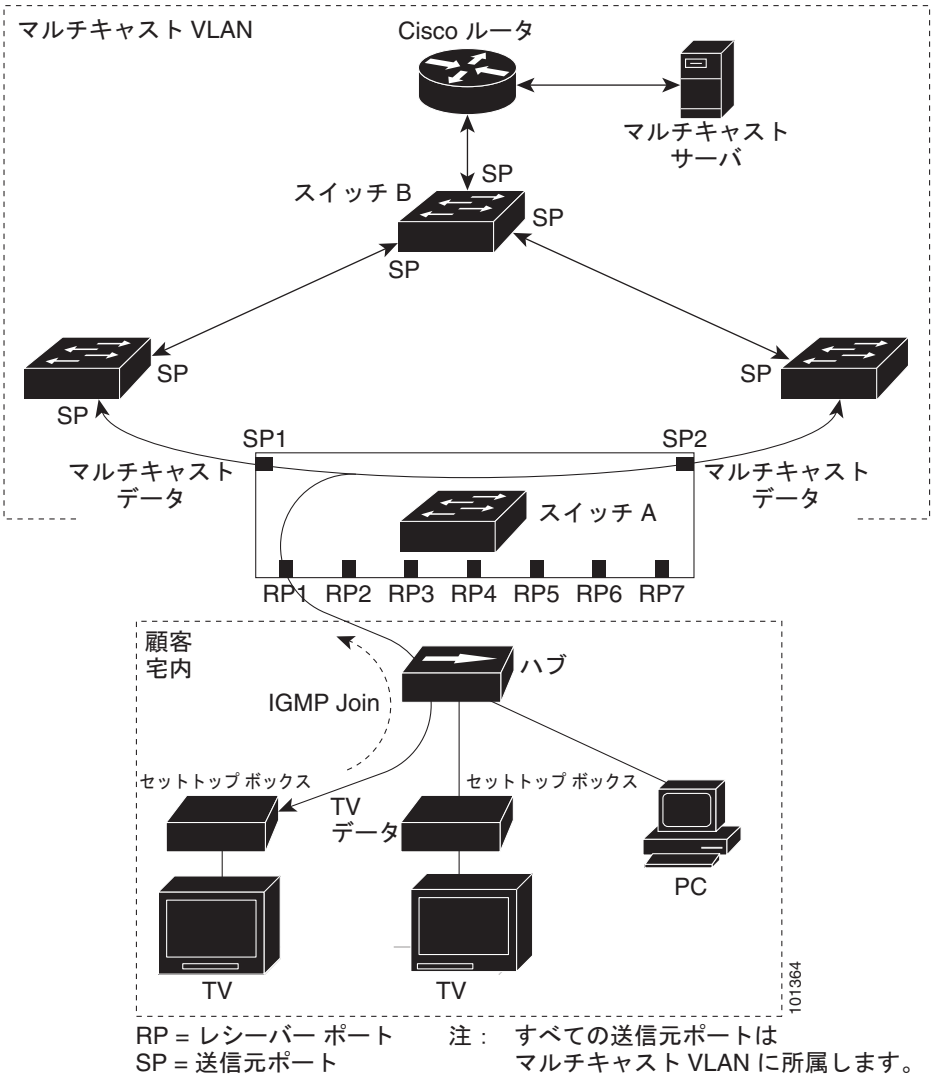
# マルチキャスト TV アプリケーションでの MVR の使用

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 受信ポートとして設定されたスイッチ ポートです。図 20-3 に設定例を示します。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、設定されているマルチキャスト MAC 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 ポートの VLAN 経由で IGMP グループ固有クエリーを送信します。VLAN 内に、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 ボックスは最大応答時間内に応答する必要があります。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。

即時脱退機能が受信ポートでイネーブルの場合、ポートはマルチキャスト グループからより迅速に脱退します。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。即時脱退機能は、1 つの受信デバイスが接続された受信ポートでのみイネーブルにしてください。

図 20-3　MVR の例




MVR では、各 VLAN の加入者に TV 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ありません。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。ただし、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る VLAN にあります。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 ストリームに対して動的に登録されます。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 上の加入者ポートにトラフィックが転送されるようにフォワーディング動作を変更し、2 つの VLAN 間で伝送されるトラフィックを選択的に許可します。

IGMP レポートは、マルチキャスト データと同じ MAC アドレスに送信されます。スイッチ A の CPU は、受信ポートからのすべての IGMP Join および Leave メッセージを取り込んで、送信元（アップリンク）ポートのマルチキャスト VLAN に転送する必要があります。

# MVR の設定

ここでは、基本的な MVR 設定情報について説明します。



## 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 |
| 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 |
| 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 ポートはトランク ポートになることはできません。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。
- スイッチ上で設定できるマルチキャスト エントリの最大数（受信できるテレビ チャネルの最大数）は 256 です。
- 各チャネルは、一意の IP マルチキャスト アドレス宛ての 1 つのマルチキャスト ストリームです。これらの IP アドレスは、それ自体の間または予約された IP マルチキャスト アドレス（224.0.0.xxx の範囲）とエイリアス指定できません。
- マルチキャスト ルーティングおよび MVR はスイッチ上で共存できません。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 は IGMPv3 メッセージをサポートしていません。

（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 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。

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 | **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 | **mvr** | スイッチ上で MVR をイネーブルに設定します。 |
| 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 *count* 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（*count* 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 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 チャネルは 1 対 1 の対応です。<br>（注）　各 IP アドレスはマルチキャスト 48 ビット MAC アドレスに変換されます。設定された IP アドレスが、以前設定された MAC アドレスまたは予約された任意のマルチキャスト MAC アドレスに変換（エイリアス）されると、そのコマンドは失敗します。 |
| ステップ 4 | **mvr querytime** *value* | （任意）マルチキャスト グループ メンバーシップからポートを削除する前に、レシーバ ポートで IGMP レポートのメンバー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。指定できる範囲は 1 ～ 100 で、デフォルトは 5（5/10 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 ID の範囲は 1 ～ 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。<br>• **dynamic**：送信元ポートでダイナミック MVR メンバーシップを使用できます。<br>• **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。<br>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。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 8 | **show mvr**<br>または<br>**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し、結果を確認する例を示します。

```
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
Switch# show mvr
MVR Running: TRUE
MVR multicast vlan: 22
MVR Max Multicast Groups: 256
MVR Current multicast groups: 1
MVR Global query response time: 10 (tenths of sec)
MVR Mode: dynamic
```

**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 | **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 | **mvr** | スイッチ上で MVR をイネーブルに設定します。 |
| ステップ 3 | **interface** *interface-id* | 設定するレイヤ 2 ポートを入力し、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。 |

| | コマンド | 目的 |
|---|---|---|
| ステップ 4 | **mvr type** {**source** \| **receiver**} | MVR ポートを次のいずれかに設定します。<br>• **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。<br>• **receiver**：加入者ポートであり、マルチキャスト データを受信するだけの場合、レシーバ ポートとしてポートを設定します。受信ポートは、スタティックな設定、または IGMP Leave および Join メッセージによってマルチキャスト グループのメンバーになるまでは、データを受信しません。受信ポートをマルチキャスト VLAN に所属させることはできません。<br>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。 |
| ステップ 5 | **mvr vlan** *vlan-id* **group** *ip-address* | （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。<br>**（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。<br>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 6 | **mvr immediate** | （任意）ポート上で MVR の即時脱退機能をイネーブルにします。<br>**（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 7 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show mvr**<br>**show mvr interface**<br>または<br>**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。 |

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。

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、インターフェイス上で即時脱退機能を設定して、結果を確認する例を示します。

```
Switch(config)# mvr
Switch(config)# interface gigabitethernet0/1
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 gigabitethernet0/1
Type: RECEIVER Status: ACTIVE Immediate Leave: 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 |
|---|---|
| **show mvr** | 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。 |
| **show mvr interface** [*interface-id*] [**members** [**vlan** *vlan*-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。<br>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。<br>• Type：Receiver または Source<br>• Status：次のいずれか<br>– ACTIVE は、ポートが VLAN に含まれていることを意味します。<br>– 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。<br>– INACTIVE は、ポートが VLAN に含まれていないことを意味します。<br>• Immediate Leave：イネーブルまたはディセーブル<br>**members** キーワードを入力すると、そのポート上のすべてのマルチキャスト グループ メンバが表示されます。VLAN ID を入力した場合は、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。VLAN ID の範囲は 1 ～ 4094 です。 |
| **show mvr members** [*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。

IGMP フィルタリングが制御するのは、Join および Leave レポートなど、グループ固有のクエリーやメンバーシップ レポートだけです。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。

（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。

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 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することもできます。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含まれており、インターフェイスが IGMP Join レポートを受け取る場合、IGMP レポートをドロップするか、転送テーブルからランダムに選択されたマルチキャスト エントリを排除し、レポートの IGMP グループをテーブルに追加するようにインターフェイスを設定できます。

ここでは、IGMP フィルタリングおよびスロットリングを設定する方法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.20-25）（任意）
- 「IGMP プロファイルの適用」（P.20-26）（任意）
- 「IGMP グループの最大数の設定」（P.20-28）（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 IGMP 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。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することでプロファイルを作成できます。

- **deny**：一致したアドレスを拒否するように指定します。これはデフォルトの条件です。
- **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**：コマンドを無効にするか、コマンドのデフォルト値を設定します。
- **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* | 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、設定するプロファイルに番号を割り当てます。指定できる範囲は 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。<br>**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、プロファイルを該当するインターフェイスに適用します。IGMP プロファイルを適用できるのは、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、各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* | 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、設定する物理インターフェイスを入力します。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。指定できるプロファイル番号の範囲は 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 configuration 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、IGMP プロファイル 4 をポートに適用し、設定を確認する例を示します。

```
Switch(config)# interface fastethernet0/2
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
Switch# show running-config interface fastethernet0/2
Building configuration...

Current configuration : 123 bytes
!
interface fastethernet0/2
 no ip address
 shutdown
 snmp trap link-status
 ip igmp max-groups 25
 ip igmp filter 4
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。

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 | **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* | 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、設定する物理インターフェイスを入力します。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 | **ip igmp max-groups** *number* | 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 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **show running-configuration 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。 |

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、インターフェイスが加入できる IGMP グループ数を 25 に制限する例を示します。

```
Switch(config)# interface fastethernet0/2
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すると、**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、転送テーブルからランダムに選択されたマルチキャスト エントリを排除し、次の IGMP グループをそれに追加するようにインターフェイスを設定できます。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 アクションを設定する場合には、次の注意事項に従ってください。

- この制限はレイヤ 2 ポートにだけ適用できます。論理 EtherChannel インターフェイスでこのコマンドを使用できますが、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。
  - 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。エントリの最大数が転送テーブルにある場合、スイッチはランダムに選択されたエントリを削除し、インターフェイスで受信した次の IGMP レポートのエントリを追加します。

  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 | **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* | 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、設定する物理インターフェイスを入力します。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 | **ip igmp max-groups action** {**deny** \| **replace**} | インターフェイスが IGMP レポートを受信したときに、転送テーブルに最大数のエントリが登録されている場合は、次のいずれかのアクションをインターフェイスに指定します。<br>• **deny**：レポートを廃棄します。<br>• **replace**：転送テーブルでランダムに選択したマルチキャスト エントリを除外し、レポートの IGMP グループを追加します。 |
| 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。 |

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。

次に、転送テーブル内に最大数のエントリが存在する場合に、テーブルでランダムに選択されたマルチキャスト エントリを削除し、転送テーブルに IGMP グループを追加するようにインターフェイスを設定する例を示します。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip igmp max-groups action replace
Switch(config-if)# end
```

# 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 |
|---|---|
| **show ip igmp profile** [*profile number*] | 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。 |
| **show running-configuration** [**interface** *interface-id*] | インターフェイスが所属できる IGMP グループの最大数（設定されている場合）や、インターフェイスに適用される IGMP プロファイルを含む、特定のインターフェイスまたは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。 |