



# CHAPTER 24

## IGMP スヌーピングおよび MVR の設定

この章では、ローカル Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル) スヌーピングのアプリケーションである Multicast VLAN Registration (MVR; マルチキャスト VLAN レジストレーション) など、スイッチに IGMP スヌーピングを設定する方法について説明します。また、IGMP フィルタリングを使用してマルチキャスト グループ メンバーシップを制御する手順および IGMP スロットリング アクションを設定する手順についても説明します。特に記述がない限り、スイッチという用語はスタンドアロンスイッチとスイッチ スタックを意味しています。



(注) IP Version 6 (IPv6) トラフィックの場合、Multicast Listener Discovery (MLD) スヌーピングは、IPv4 トラフィックの IGMP スヌーピングの同一機能として動作します。MLD の詳細については、[第 25 章「IPv6 MLD スヌーピングの設定」](#)を参照してください。



(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.24-2)
- 「IGMP スヌーピングの設定」 (P.24-7)
- 「IGMP スヌーピング情報の表示」 (P.24-17)
- 「マルチキャスト VLAN レジストレーションの概要」 (P.24-18)
- 「MVR の設定」 (P.24-20)
- 「MVR 情報の表示」 (P.24-24)
- 「IGMP フィルタリングおよびスロットリングの設定」 (P.24-24)
- 「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.24-29)



(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だけに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、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トラッキング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フォワーディング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（スタックマスターに設定された IP サービス機能のあるスイッチを含む）は、すべての VLAN に定期的に一般クエリーを送出します。このマルチキャストトラフィックに関係のあるホストはすべて Join 要求を送信し、フォワーディング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 マルチキャストフォワーディングテーブルで、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ため、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ダイナミックに学習されます。 **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スタティックに設定できます。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スタティックに指定すると、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ため、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.24-15) 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 スヌーピングの特徴について説明します。

- 「[IGMP バージョン](#)」(P.24-3)
- 「[マルチキャストグループへの加入](#)」(P.24-3)
- 「[マルチキャストグループからの脱退](#)」(P.24-5)
- 「[即時脱退](#)」(P.24-6)
- 「[IGMP の設定可能な Leave タイマー](#)」(P.24-6)
- 「[IGMP レポート抑制](#)」(P.24-6)
- 「[IGMP スヌーピングおよびスイッチスタック](#)」(P.24-7)

## 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、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ドは抑制されます。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。

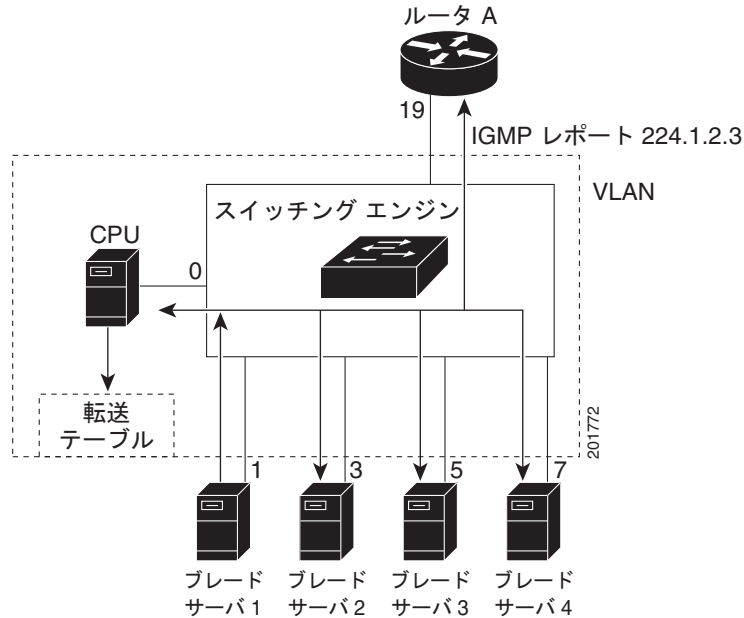
IGMPv3 スイッチは、Source Specific Multicast (SSM) 機能を実行しているデバイスとメッセージの送受信を行うことができます。IGMPv3 と IGMP の Source Specific Multicast の詳細については、次の URL を参照してください。

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products\\_feature\\_guide09186a008008048a.html](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

スイッチに接続されたブレード サーバが IP マルチキャスト グループに加入しようとする場合、このホストが IGMP バージョン 2 クライアントであれば、加入する IP マルチキャスト グループを指定して、割り込み 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 のブレード サーバがマルチキャスト 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 フォワーディングテーブル 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フォワーディング 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ブレード サーバが、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 24-1 を参照してください。

図 24-1 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 のすべてのメンバーであるポート 3、5、7 に転送します。ブレード サーバ 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 CPU は、IGMP レポートの情報を使用して、表 24-1 で示すようなフォワーディング テーブル エントリを設定します。これには、ブレード サーバ 1 およびルータのポート番号が含まれます。

表 24-1 IGMP スヌーピング フォワーディング 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	19、1

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。

別のブレード サーバ (たとえばブレード サーバ 4) が同じグループに割り込み IGMP Join メッセージを送信する場合 (図 24-2 を参照)、CPU はメッセージを受信して、フォワーディング テーブルにブレード サーバ 4 のポート番号を追加します (表 24-2 を参照)。フォワーディング テーブルは CPU にに対してだけ IGMP メッセージを送るため、メッセージはスイッチの他のポートにはフラッドしないことに注意してください。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 24-2 2 番めのホストのマルチキャスト グループへの加入

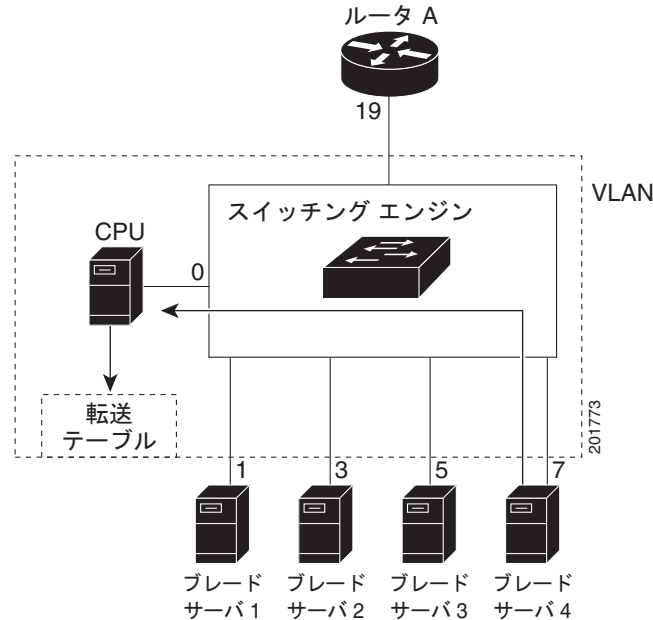


表 24-2 アップデートされた IGMP スヌーピング フォワーディング テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	19、1、7

## 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。関係のあるブレードサーバがクエリーに応答します。VLAN 内の少なくとも 1 つのブレードサーバ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フォワーディングテーブルで指定されたブレードサーバに対してだけ、マルチキャストグループトラフィックを転送します。

ブレードサーバは、マルチキャストグループを脱退する場合、メッセージを送信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。スイッチは、ブレードサーバから Leave メッセージを受信すると、グループ固有の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調べます。スイッチはさらに、フォワーディングテーブルでその MAC グループの情報をアップデートし、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係のあるブレードサーバだけが、フォワーディング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

即時脱退は、IGMP バージョン 2 のホストだけでサポートされます。

IGMP スヌーピングの即時脱退 (immediate-leave) 処理を使用すると、スイッチは、グループ固有のクエリーをインターフェイスに送信することなく、フォワーディング テーブルから Leave メッセージを送信した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ブレード サーバ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 つのブレード サーバが接続された VLAN 上だけで使用してください。ポートに複数のブレード サーバが接続されている VLAN 上で即時脱退をイネーブルにすると、一部のブレード サーバが誤ってドロップ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.24-11) を参照してください。

## IGMP の設定可能な Leave タイマー

ホストがまだ特定のマルチキャスト グループと関係があるかどうかを判別するために、グループ固有のクエリーの送信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 ミリ秒で設定できます。タイマーは、グローバルまたは VLAN ベースで設定できます。Leave タイムの VLAN 設定は、グローバル設定を上書きします。

設定手順については、「[IGMP Leave タイマーの設定](#)」(P.24-12) を参照してください。

## 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、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 ルータの抑制がイネーブル (デフォルト) になっている場合、スイッチは、グループのすべてのブレード サーバからの最初の 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る場合、スイッチは、グループのすべてのブレード サーバからの最初の 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。

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。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.24-16) を参照してください。

## IGMP スヌーピングおよびスイッチ スタック

IGMP スヌーピングは、スイッチ スタック全体で機能します。つまり、あるスイッチからの IGMP 制御情報がスタック内の全スイッチに配信されます（スイッチ スタックの詳細については第 7 章「スイッチ スタックの管理」を参照してください）。IGMP マルチキャスト データがスタックを入力するスタック メンバーに関係なく、データはそのグループに対して登録されたホストに到達します。

スタック内のスイッチに障害が発生したり、スタックから削除された場合、スイッチ上のマルチキャスト グループのメンバーだけがマルチキャスト データを受信しません。スタック内の別のスイッチ上にあるマルチキャスト グループの全メンバーは、引き続きマルチキャスト データ ストリームを受信します。ただし、スタック マスターが削除される場合、レイヤ 2 とレイヤ 3 に共通のマルチキャスト グループ（IP マルチキャスト ルーティング）は、収束時に時間がかかる可能性があります。

## 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。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.24-7)
- 「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.24-8)
- 「スヌーピング方法の設定」 (P.24-9)
- 「マルチキャスト ルータ ポートの設定」 (P.24-10)
- 「グループに加入するブレード サーバのスタティックな設定」 (P.24-11)
- 「IGMP 即時脱退のイネーブル化」 (P.24-11)
- 「IGMP Leave タイマーの設定」 (P.24-12)
- 「TCN 関連コマンドの設定」 (P.24-13)
- 「IGMP スヌーピング クエリアの設定」 (P.24-15)
- 「IGMP レポート抑制のディセーブル化」 (P.24-16)

## IGMP スヌーピングのデフォルト設定

表 24-3 に、IGMP スヌーピングのデフォルト設定を示します。

表 24-3 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	設定なし
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	設定なし
TCN <sup>1</sup> フラッドクエリー カウント	2
TCN クエリー送信請求	ディセーブル

表 24-3 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
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。

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。 <b>(注)</b> 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 エントリごとにフォワーディング 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; 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) パケットのスヌーピング
- 他のルータからの Cisco Group Management Protocol (CGMP) パケットの受信
- **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 ポートへのスタティックな接続

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受信を行うように、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 または proxy-join パケットだけを受信し、その他の CGMP パケットは受信しません。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)

学習方式として CGMP を使用し、VLAN 内のマルチキャスト ルータを CGMP プロキシ対応にしない場合、ダイナミックにルータにアクセスするには **ip cgmp router-only** コマンドを実行する必要があります。詳細については、第 45 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 ルータにダイナミック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	<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 2	<b>ip igmp snooping vlan <i>vlan-id</i> mrouter learn {cgmp   pim-dvmrp}</b>	VLAN 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 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"> <li>• <b>cgmp</b> : CGMP パケットを受信します。この方式は、制御トラフィックを減らす場合に有用です。</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。これがデフォルトです。</li> </ul>
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 4	<b>show ip igmp snooping</b>	設定を確認します。
ステップ 5	<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。

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
```

## 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 ルータにスタティックな接続を追加）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 ルータへのスタティック接続をイネーブルに設定するには、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	<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 2	<b>ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i></b>	マルチキャスト ルータの VLAN ID を指定し、そのマルチキャスト 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 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 ~ 64 です。</li> </ul>
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 4	<b>show ip igmp snooping mrouter [vlan <i>vlan-id</i>]</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 5	<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。

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 ルータへのスタティック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ブレード サーバのスタティックな設定

レイヤ 2 ポートに接続されているブレード サーバは、通常マルチキャスト グループにダイナミックに加入します。ポートがマルチキャスト グループに加入するように、ブレード サーバが接続されるレイヤ 2 ポートをスタティックに設定することもできます。

マルチキャスト グループのメンバーとしてレイヤ 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 ip_address 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 ポートをスタティックに設定します。 <ul style="list-style-type: none"> <li><code>vlan-id</code> 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><code>ip-address</code> は、グループの IP アドレスです。</li> <li><code>interface-id</code> 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 ~ 64) に設定できます。</li> </ul>
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、ポートにブレード サーバをスタティック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 gigabitethernet1/0/1
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。即時脱退処理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) 即時脱退は、IGMP バージョン 2 のブレード サーバだけでサポートされます。

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	<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> immediate-leave</code>	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	<code>end</code>	特権 EXEC モードに戻ります。

## ■ IGMP スヌーピングの設定

	コマンド	目的
ステップ 4	<code>show ip igmp snooping vlan <i>vlan-id</i></code>	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	<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 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 Leave タイマーの設定

IGMP Leave 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。

- グローバルまたは VLAN 単位で Leave タイムをグローバルに設定できます。
- VLAN 上に Leave タイムを設定すると、グローバル設定を上書きします。
- デフォルトの Leave タイムは 1000 ミリ秒です。
- IGMP の設定可能な Leave タイムは、IGMP バージョン 2 を実行しているホスト上だけでサポートされています。
- ネットワークにおける実際の脱退のための待ち時間は、通常設定済みの Leave タイムです。ただし、リアルタイムの CPU ロード状態、ネットワーク遅延、およびインターフェイスを通じて送信されるトラフィック量に応じて、Leave タイムは設定時間周りで変化する可能性ががあります。

IGMP の設定可能な Leave タイマー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 <i>time</i></code>	IGMP Leave 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 ~ 32768 ミリ秒です。デフォルトは 1000 秒です。
ステップ 3	<code>ip igmp snooping vlan <i>vlan-id</i> last-member-query-interval <i>time</i></code>	(任意) VLAN インターフェイスの IGMP Leave タイムを設定します。指定できる範囲は 100 ~ 32768 ミリ秒です。  (注) VLAN 上に Leave タイムを設定すると、グローバルに設定されたタイマーを上書きします。
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 ip igmp snooping</code>	(任意) 設定された IGMP Leave タイムを表示します。
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 Leave タイマーをデフォルト設定にグローバルにリセットするには、`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。

指定した VLAN から IGMP Leave タイム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について説明します。

- 「TCN イベント後のマルチキャスト フラッディング タイムの制御」(P.24-13)
- 「フラッド モードからの回復」(P.24-13)
- 「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.24-14)

### TCN イベント後のマルチキャスト フラッディング タイムの制御

**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 イベント後にマルチキャスト トラフィックがフラッディングする時間を制御できます。このコマンドは、TCN イベント後にマルチキャスト データ トラフィックがフラッディングする一般クエリーの数を設定します。TCN イベントの例としては、クライアントが場所を変更してレシーバがブロックされていたものの現在転送中の同一ポート上にある場合や、ポートが Leave メッセージを送信せずにダウンしたときなどです。

**ip igmp snooping tcn flood query count** コマンドを使用して TCN フラッドクエリー カウントを 1 に設定した場合、1 つの一般的クエリーの受信後にフラッディングが停止します。カウントを 7 に設定する場合、7 一般クエリーまでのフラッディングが受信されます。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。

TCN フラッドクエリー 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	<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 2	<b>ip igmp snooping tcn flood query count count</b>	マルチキャスト トラフィックがフラッディングする IGMP の一般的クエリー数を指定します。指定できる範囲は 1 ~ 10 です。デフォルトで、フラッディングクエリー カウントは 2 です。
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 4	<b>show ip igmp snooping</b>	TCN 設定を確認します。
ステップ 5	<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。

デフォルトのフラッディングクエリー カウントに戻るには、**no ip igmp snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用します。

### フラッド モードからの回復

トポロジ変更が発生した場合、スパニングツリー ルートが、グループ マルチキャスト アドレス 0.0.0.0 の特別な IGMP Leave メッセージ (またはグローバル Leave) を送信します。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すると、スパニングツリー ルートかどうかにかかわらず、スイッチがグローバル Leave メッセージを送信します。ルータがこの特殊脱退を受信すると、TCN イベント中にフラッド モードから復旧するプロセスをスピードアップする一般クエリーを即座に送信します。このコンフィギュレーション コマンドに関係なく、スイッチがスパニングツリー ルートの場合、脱退は常に送信されます。デフォルトで、クエリー送信請求はディセーブルです。

ルートがスパニングツリー ルートであるかどうかに関係なく、グローバル Leave メッセージを送信するようにスイッチ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 tcn query solicit</code>	TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げるために、IGMP Leave メッセージ（グローバル Leave）を送信します。デフォルトで、クエリー送信請求はディセーブルです。
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</code>	TCN 設定を確認します。
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。

デフォルト クエリー送信請求に戻るには、`no ip igmp snooping tcn query solicit` グローバル コンフィギュレーション コマンドを使用します。

## 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

スイッチが TCN を受信すると、2 つの一般的なクエリーが受信されるまで、マルチキャスト トラフィックはすべてのポートに対してフラッディングします。異なるマルチキャスト グループに加入している接続ホストを持つポートがスイッチに多数ある場合、フラッディングがリンクの容量を超過し、パケット損失を招くことがあります。この動作を制御するために、`ip igmp snooping tcn flood interface configuration` コマンドを使用できます。

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 TCN イベント中にマルチキャスト 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、マルチキャスト フラッディングがインターフェイスでイネーブルです。
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 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びイネーブルにするには、`ip igmp snooping tcn flood` インターフェイス コンフィギュレーション コマンドを使用します。

## 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	<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 2	<b>ip igmp snooping querier</b>	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	<b>ip igmp snooping querier address</b> <i>ip_address</i>	(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。 <b>(注)</b> 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	<b>ip igmp snooping querier query-interval</b> <i>interval-count</i>	(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	<b>ip igmp snooping querier tcn query</b> [ <i>count count</i>   <i>interval interval</i> ]	(任意) Topology Change Notification (TCN; トポロジ変更通知) クエリーの間隔を設定します。指定できるカウントの範囲は 1 ~ 10 です。指定できる間隔の範囲は 1 ~ 255 秒です。
ステップ 6	<b>ip igmp snooping querier timer expiry</b> <i>timeout</i>	(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	<b>ip igmp snooping querier version</b> <i>version</i>	(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	<b>end</b>	特権 EXEC モードに戻ります。

## ■ IGMP スヌーピングの設定

	コマンド	目的
ステップ 9	<code>show ip igmp snooping vlan <i>vlan-id</i></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。指定できる VLAN ID 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
```

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
```

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 レポート抑制のディセーブル化



(注)

IGMP レポート抑制は、マルチキャストクエリアに 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、クエリアに 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アごとに 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	<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>no ip igmp snooping report-suppression</code>	IGMP レポート抑制をディセーブルにします。
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</code>	IGMP レポート抑制がディセーブルになっていることを確認します。
ステップ 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。

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

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 24-4 の特権 EXEC コマンドを 1 つ以上使用します。

表 24-4 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>	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>vlan <i>vlan-id</i></b> を入力します。指定できる VLAN ID 範囲は 1 ~ 1001 および 1006 ~ 4094 です。
<code>show ip igmp snooping groups [count  dynamic [count]   user [count]]</code>	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。 <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 オプションに対応する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>
<code>show ip igmp snooping groups vlan <i>vlan-id</i> [<i>ip_address</i>   count   dynamic [count]   user[count]]</code>	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。 <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 オプションに対応する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。</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>
<code>show ip igmp snooping mrouter [vlan <i>vlan-id</i>]</code>	ダイナミックに学習された、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。 (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ダイナミックに学習されます。 (任意) 個々の VLAN に関する情報を表示するには、 <b>vlan <i>vlan-id</i></b> を入力します。
<code>show ip igmp snooping querier [vlan <i>vlan-id</i>]</code>	VLAN で最新の受信 IGMP クエリー メッセージの受信ポートおよび IP アドレスに関する情報を表示します。 (任意) 個々の VLAN に関する情報を表示するには、 <b>vlan <i>vlan-id</i></b> を入力します。
<code>show ip igmp snooping querier [vlan <i>vlan-id</i>] detail</code>	VLAN で最新の受信 IGMP クエリー メッセージの受信ポートおよび IP アドレス、および 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。

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。

## マルチキャスト VLAN レジストレーションの概要

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 ネットワークで、マルチキャストトラフィックを広範囲に配信するアプリケーション (サービス プロバイダー ネットワークでの複数の 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。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、加入者は異なる VLAN に存続できます。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。

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 に準拠しているブレード サーバから発信できます。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 フォワーディング 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、フォワーディング 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。このフォワーディング動作により、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 ブレード サーバ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 ブレード サーバ 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 MVR スタティック設定を使用して、MVR ブレード サーバが加入したレシーバ ポートだけに転送されます。MVR ブレード サーバから受信された IGMP レポートは、ブレード サーバに設定された MVR データ ポートからは転送されません。
- ダイナミック モードの場合、スイッチ上の MVR ブレード サーバで受信されたマルチキャスト データは、IGMP レポートまたは MVR スタティック設定を使用して、MVR ブレード サーバが明示的に加入した MVR データ ポートおよびクライアント ポートだけから転送されます。MVR ブレード サーバから受信した IGMP レポートも、ブレード サーバのすべての MVR データ ポートから転送されます。したがって、互換モードでブレード サーバ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 ポートとして設定する必要があります。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 つだけです。

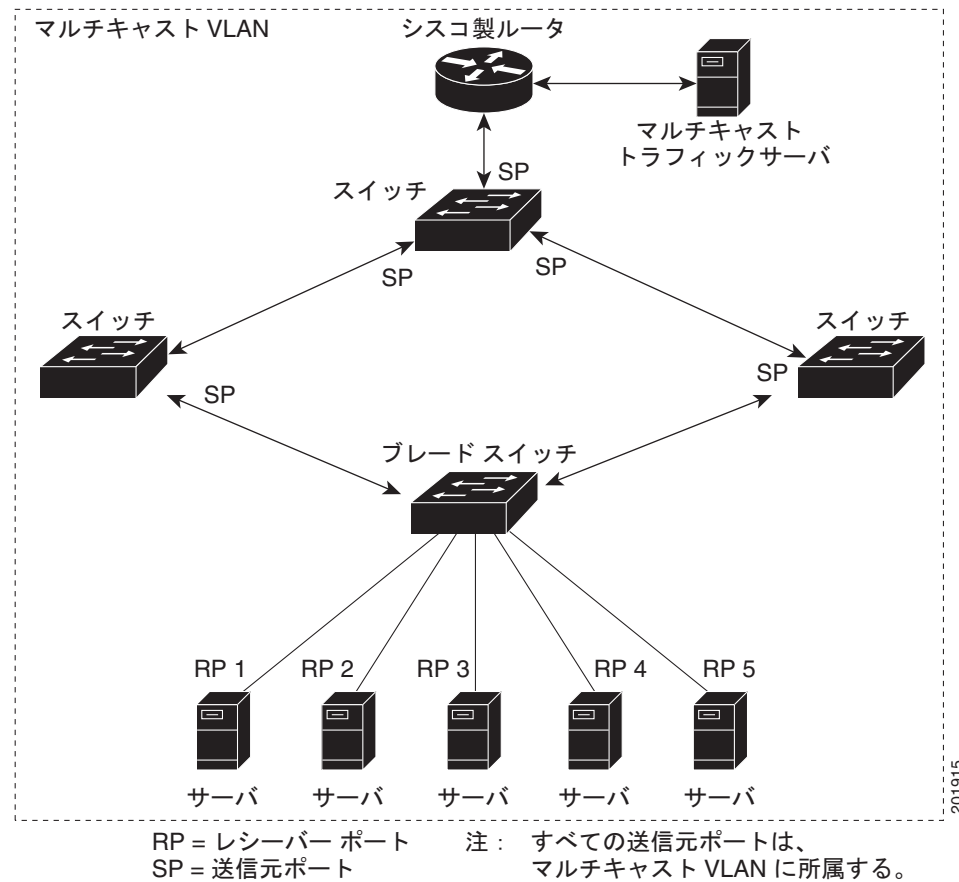
レシーバ ポートとソース ポートは、スタック スイッチ内の別のスイッチに設定可能です。マルチキャスト VLAN で送信されるマルチキャスト データは、スタック内の全 MVR レシーバ ポートに転送されます。新規スイッチがスタックに追加される際に、デフォルトでレシーバ ポートはありません。

スイッチに障害が発生したり、スタックから削除される場合、そのスイッチに属するレシーバ ポートだけがマルチキャスト データを受信しません。スイッチにあるその他のすべてのレシーバ ポートではマルチキャスト データを引き続き受信します。

## 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、ブレードスイッチに接続されたサーバは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デバイスを接続できます。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 24-3 に構成例を示します。Dynamic Host Configuration Protocol (DHCP) は、サーバに IP アドレスを割り当てます。サーバ上の加入者がチャンネルを選択すると、サーバからブレードスイッチに、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 24-3 マルチキャスト VLAN レジストレーションの例



加入者がチャンネルを切り替えた場合、またはマルチキャストストリームを停止した場合には、サーバ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 経路で MAC ベースの一般クエリを送信します。VLAN に、同じグループに加入している別のデバイスがある場合、そのデバイスはクエリに指定された最大応答時間内に応答しなければなりません。応答を受信しなかった場合、CPU は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 メンバー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。即時脱退機能は、1 つの受信デバイスを接続したレシーバー ポートだけでイネーブルにしてください。

MVR では、各 VLAN の複数の加入者に対して TV チャンネルのマルチキャスト トラフィックを重複して送信する必要がありません。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 上だけで、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、ダイナミックに登録します。アクセス レイヤ ブレード スイッチは、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 IP マルチキャスト グループ アドレスに送信されません。ブレード スイッチの 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。

- 「デフォルト MVR 設定」 (P.24-20)
- 「MVR 設定時の注意事項および制限事項」 (P.24-21)
- 「MVR グローバル パラメータの設定」 (P.24-21)
- 「MVR インターフェイスの設定」 (P.24-22)

## デフォルト MVR 設定

表 24-5 に、MVR のデフォルト設定を示します。

表 24-5 デフォルト MVR 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	設定なし
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	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 の設定時は、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 ポートだけに設定可能で、トランク ポートには設定できません。スイッチのレシーバー 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 (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。
- 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ため、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 スイッチと連携動作している場合は、それらの中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 ポートで 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、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 はスイッチで 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。
ステップ 3	<code>mvr group ip-address [count]</code>	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。

## MVR の設定

	コマンド	目的
ステップ 4	<code>mvr querytime value</code>	(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、レシーバー 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定義します。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 5/10、つまり 0.5 秒です。
ステップ 5	<code>mvr vlan vlan-id</code>	(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。指定できる VLAN ID 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	<code>mvr mode {dynamic   compatible}</code>	(任意) MVR の動作モードを指定します。 <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 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。</li> </ul> デフォルトは <b>compatible</b> モードです。
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> 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。

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	<b>mvr type {source   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。</li> <li><b>receiver</b> : 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。スタティックに、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 ポートはマルチキャスト VLAN に属す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>
ステップ 5	<b>mvr vlan vlan-id group</b> [ip-address]	<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スタティックに設定します。グループ メンバーとしてスタティックに設定されたポートは、スタティックに削除されない限り、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 グループにダイナミックに加入することもできます。</p>
ステップ 6	<b>mvr immediate</b>	<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	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 8	<b>show mvr</b>  <b>show mvr interface</b> または <b>show mvr members</b>	設定を確認します。
ステップ 9	<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。

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スタティックに設定し、ポートに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 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
----      -
Gi1/0/2  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 24-6 のコマンドを使用します。

表 24-6 MVR 情報表示用のコマンド

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"> <li>Type : RECEIVER (レシーバー) または SOURCE (送信元)</li> <li>Status : 次のいずれか 1 つ <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 (即時脱退機能) : イネーブルまたはディセーブル</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。指定できる VLAN ID 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 つ以上格納して、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 レポートがドロップされ、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 グループの最大数を設定することもできます。



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。

IGMP フィルタリングを適用できるのは、IP マルチキャスト グループ アドレスをスタティックに設定する場合でなく、ダイナミックに学習する場合だけです。

IGMP スロットリング機能を使用すれば、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ができます。IGMP グループの最大数が設定され、IGMP スヌーピング フォワーディング 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 レポートをドロップするか、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.24-25)
- 「IGMP プロファイルの設定」 (P.24-26) (任意)
- 「IGMP プロファイルの適用」 (P.24-27) (任意)
- 「IGMP グループの最大数の設定」 (P.24-27) (任意)
- 「IGMP スロットリングアクションの設定」 (P.24-28) (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 24-7 に、IGMP フィルタリングのデフォルト設定を示します。

表 24-7 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	設定なし
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

フォワーディング 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.24-28) 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** : 一致するアドレスを拒否します (デフォルト設定の状態)。
- **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、デフォルト設定に戻します。
- **permit** : 一致するアドレスを許可します。
- **range** : プロファイルに対する 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。

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	<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 2	<b>ip igmp profile profile number</b>	設定しているプロファイルに番号を割り当てて、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。
ステップ 3	<b>permit   deny</b>	(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	<b>range ip multicast address</b>	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。  <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。
ステップ 5	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show ip igmp profile profile number</b>	プロファイルの設定を確認します。
ステップ 7	<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。

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 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することができますが、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	<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 2	<b>interface interface-id</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 3	<b>ip igmp filter profile number</b>	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	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config interface interface-id</b>	設定を確認します。
ステップ 6	<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。

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 gigabitethernet1/0/2
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 mac-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 インターフェイス上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上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

フォワーディング テーブルに最大数の IGMP グループを設定するには、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、最大数は設定されていません。
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
```

## 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、`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 レポートをドロップ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 ポートだけに適用されます。このコマンドは、論理 EtherChannel インターフェイス上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上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 エントリがフォワーディング 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、フォワーディング 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エージングアウトするか削除されます。
  - スロットリング アクションを `deny` に設定すると、すでにフォワーディング 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エージングアウトになります。エントリがエージングアウトして、最大数のエントリがフォワーディング テーブルに登録されると、スイッチは、インターフェイスで受信した次の IGMP レポートをドロップします。
  - スロットリング アクションを `replace` に設定すると、すでにフォワーディング 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。

スイッチがフォワーディング 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フォワーディング 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。

フォワーディング 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、フォワーディング 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。</li> <li><b>replace</b> : IGMP レポートを受信した新規グループで、既存のグループを置き換えます。</li> </ul>
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。

レポートのドロップ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 24-8 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 24-8 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