



CHAPTER 28

IGMP スヌーピングおよび MVR の設定

この章では、ローカルの IGMP スヌーピングの適用、Multicast VLAN Registration (MVR; マルチキャスト VLAN レジストレーション) など、IE 3000 スイッチに Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル) スヌーピングを設定する手順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 グループのメンバーシップを制御する手順と、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。



(注) IP バージョン 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 スヌーピングと同じ機能を実行します。MLD スヌーピングの詳細については、[第 43 章「IPv6 MLD スヌーピングの設定」](#)を参照してください。



(注) この章で使用されるコマンドの構文と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 リファレンスと、『*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。このリリースは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にあります。

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.28-2)
- 「[IGMP スヌーピングの設定](#)」 (P.28-7)
- 「[IGMP スヌーピング情報の表示](#)」 (P.28-17)
- 「[マルチキャスト VLAN レジストレーションの概要](#)」 (P.28-18)
- 「[MVR の設定](#)」 (P.28-21)
- 「[MVR 情報の表示](#)」 (P.28-25)
- 「[IGMP フィルタリング/スロットリングの設定](#)」 (P.28-26)
- 「[IGMP フィルタリング/スロットリング設定の表示](#)」 (P.28-31)



(注) IGMP スヌーピングや 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か、またはスタティック 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 インターフェイスのダイナミックな設定によるマルチキャストトラフィックのフラッディングを抑制します。これにより、マルチキャストトラフィックが、IP マルチキャスト装置と関連付けられたインターフェイスだけに転送されるようにします。名前が暗示するように、IGMP スヌーピングに必要となる LAN スイッチは、ホストおよびルータ間の IGMP 伝送にスヌーピングを行い、マルチキャストグループとメンバーポートの追跡を続けます。このスイッチが、特定のマルチキャストグループに関する IGMP レポートをホストから受信すると、スイッチは転送テーブルエントリにこのホスト番号を追加します。ホストから IGMP Leave Group メッセージを受信すると、そのホストポートをテーブルエントリから削除します。また、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い場合は、スイッチが定期的にエントリを削除します。



(注) IP マルチキャストおよび IGMP の詳細については、RFC 1112 および RFC 2236 を参照してください。

マルチキャストルータはすべての VLAN に一般的クエリーを定期的に送信します。このマルチキャストトラフィックに関係し、Join 要求を送信するすべてのホストが、転送テーブルエントリに追加されます。スイッチは、IGMP Join 要求を受信すると、各グループの IGMP スヌーピング IP マルチキャストの転送テーブルに VLAN あたり 1 つのエントリを生成します。

スイッチは、MAC アドレスグループではなく、IP マルチキャストグループに基づいてブリッジをサポートします。マルチキャスト MAC アドレスに基づくグループを使用すると、設定済みの IP アドレスが以前に設定した MAC アドレスや予約済みの任意のマルチキャスト MAC アドレス (224.0.0.xxx の範囲内) に変換されると (エイリアスが作成されると)、コマンドが失敗します。スイッチは IP マルチキャストグループを使用しているため、アドレスのエイリアス作成の問題は発生しません。

IGMP スヌーピングによって学習される IP 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 *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、その設定は IGMP スヌーピングによる自動的な処理よりも優先されます。マルチキャストグループメンバーシップのリストは、ユーザ定義の設定と、IGMP スヌーピングによって学習された設定の両方で構成できます。

IGMP スヌーピングクエリアを設定すると、マルチキャストインターフェイスを使用しないでサブネット内の IGMP スヌーピングをサポートできます。これは、マルチキャストトラフィックがルーティングを必要としないためです。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.28-14) 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 に変更が発生すると、IGMP スヌーピングによって学習されたマルチキャストグループは、VLAN 内のこのポートから削除されます。

ここでは、IGMP スヌーピングの特性について説明します。

- 「[IGMP のバージョン](#)」(P.28-3)
- 「[マルチキャストグループへの加入](#)」(P.28-3)
- 「[マルチキャストグループからの脱退](#)」(P.28-5)
- 「[即時脱退](#)」(P.28-6)
- 「[IGMP の設定可能な Leave タイマー](#)」(P.28-6)
- 「[IGMP レポート抑制](#)」(P.28-6)

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 をサポートします。これらのバージョンはスイッチ上で相互運用が可能です。たとえば、IGMP スヌーピングが IGMPv2 スイッチ上でイネーブルであり、このスイッチがホストから IGMPv3 レポートを受信する場合、スイッチは IGMPv3 レポートをマルチキャスト ルータに転送できます。



(注)

スイッチがサポートする IGMPv3 スヌーピングは、宛先マルチキャスト MAC アドレスだけに基づいています。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されません。

IGMPv3 スイッチがサポートする Basic IGMPv3 Snooping Support (BISS) には、IGMPv1 スイッチおよび IGMPv2 スイッチ上のスヌーピング機能と IGMPv3 メンバーシップ レポート メッセージのサポートが含まれます。BISS は、ネットワークに IGMPv3 ホストが含まれる場合にマルチキャスト トラフィックのフラグディングを抑制します。IGMPv2 ホストまたは IGMPv1 ホスト上の IGMP スヌーピング機能と、ほぼ同等のポート セットへのトラフィックを抑制します。



(注)

IGMPv3 の Join メッセージと Leave メッセージは、IGMP フィルタリングまたは MVR を実行中のスイッチにはサポートされません。

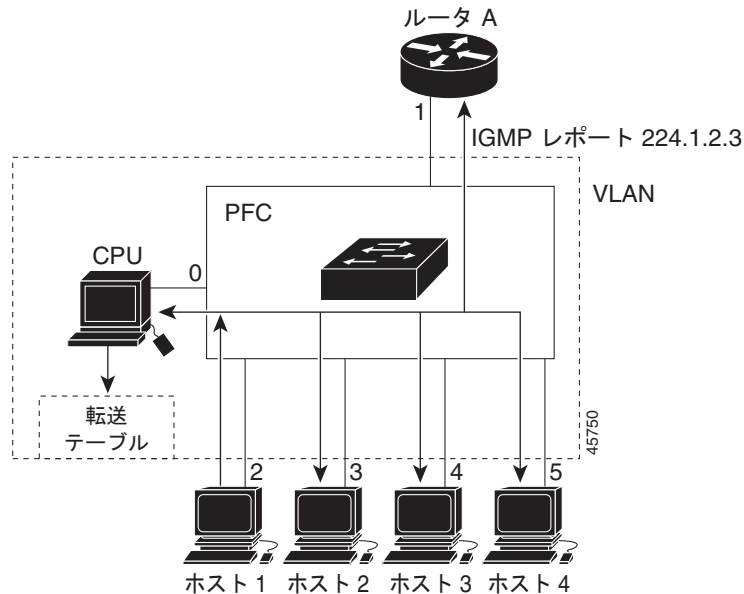
IGMPv3 スイッチは、Source Specific Multicast (SSM) 機能を実行中の装置とメッセージを送受信できます。IGMPv3 および IGMP の送信元固有のマルチキャストの詳細については、次の URL を参照してください。

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

スイッチに接続済みのホストを IP マルチキャスト グループに加入させ、そのグループが IGMP バージョン 2 のクライアントである場合、加入する IP マルチキャスト グループを指定して、非送信請求の IGMP Join メッセージを送信します。または、スイッチがルータから一般的クエリーを受信する場合、クエリーは VLAN 内のすべてのポートに転送されます。マルチキャスト グループに加入する IGMP バージョン 1 またはバージョン 2 のホストは、Join メッセージをスイッチに送信することで応答します。スイッチの CPU は、マルチキャスト転送テーブル エントリがまだ存在しない場合、グループ用にテーブル エントリを作成します。また、CPU は 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に関連付けられたホストは、マルチキャスト グループに対応するマルチキャスト トラフィックを受信します。図 28-1 を参照してください。

図 28-1 最初の IGMP Join メッセージ



ルータ A が一般的クエリーをスイッチに送信すると、スイッチがそのクエリーを同じ VLAN の全メンバーのポート 2 ~ 5 に転送します。ホスト 1 をマルチキャスト グループ 224.1.2.3 に加入させ、IGMP メンバーシップ レポート (IGMP Join メッセージ) をグループにマルチキャストします。スイッチの CPU は IGMP レポート内の情報を使用して、転送テーブル エントリ (表 28-1 を参照) を設定します。これにはホスト 1 とルータに接続済みのポート番号が含まれています。

表 28-1 IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1, 2

スイッチのハードウェアは、IGMP 情報パケットをマルチキャスト グループ用の他のパケットと区別できます。テーブルに含まれる情報の指示により、スイッチング エンジンが、224.1.2.3 マルチキャスト IP アドレス宛てにフレームを送信します。このフレームは、グループに加入済みのルータおよびホスト宛ての IGMP パケットではありません。

別のホスト (たとえば、ホスト 4) が、同じグループに対して非送信請求 IGMP Join メッセージを送信する場合 (図 28-2 を参照)、そのメッセージを受信した CPU は、ホスト 4 のポート番号を転送テーブルに追加します (表 28-2 を参照)。転送テーブルは CPU だけを IGMP メッセージの宛先に指示するため、メッセージがスイッチ上の他のポートへフラッドされないことに注意してください。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 28-2 2 番目のホストのマルチキャスト グループへの加入

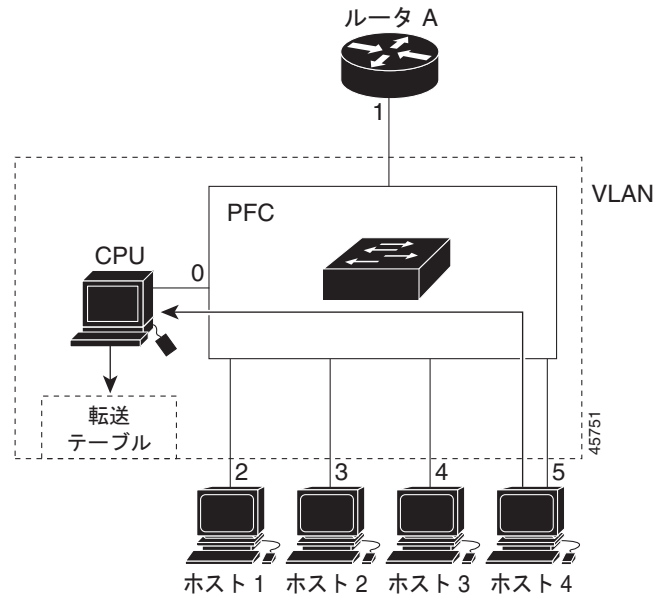


表 28-2 更新された IGMP スヌーピング転送テーブル

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

ルータは一般的なマルチキャスト クエリーを定期的送信し、スイッチはこれらのクエリーを VLAN 内のすべてのポートを経由して転送します。対象ホストがクエリーに応答します。VLAN 内で少なくとも 1 つのホストがマルチキャスト トラフィックを受信する場合、ルータは VLAN へのマルチキャスト トラフィックの転送を続行します。スイッチがマルチキャストグループ トラフィックを転送するのは、IGMP スヌーピングによって維持される IP マルチキャスト グループの転送テーブルにリストされたホストだけです。

ホストをマルチキャスト グループから脱退させる場合は、暗黙的に脱退するか、または Leave メッセージを送信することができます。スイッチがホストから 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信して、そのインターフェイスに接続済みの他の装置が、特定のマルチキャストグループのトラフィックに関係しているかどうかを学習します。次に、スイッチはその MAC グループの転送テーブルを更新し、グループに対応したマルチキャスト トラフィックの受信に関するホストだけが転送テーブルにリストされるようになります。ルータが VLAN からレポートを受信しない場合、ルータはその VLAN のグループを IGMP キャッシュから削除します。

即時脱退

即時脱退は IGMP バージョン 2 のホストにだけサポートされます。

スイッチは IGMP スヌーピングの即時脱退を使用して、グループ固有のクエリーをインターフェイスに送信せずに、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します。VLAN のインターフェイスは、元の Leave メッセージに指定されたマルチキャスト グループに対するマルチキャスト ツリーからプルーニングされます。即時脱退により、複数のマルチキャスト グループが同時に使用中であっても、スイッチド ネットワーク上のすべてのホストに最適な帯域幅の管理を実現します。



(注)

即時脱退機能は、各ポートにシングル ホストが接続されている VLAN 上でしか使用できません。各ポートに複数のホストが接続されている VLAN 上で即時脱退をイネーブルにすると、一部のホストが偶発的に廃棄される可能性があります。

設定の手順については、「[IGMP 即時脱退のイネーブル化](#) (P.28-11) を参照してください。

IGMP の設定可能な Leave タイマー

ホストが特定のマルチキャスト グループにまだ関係し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あとにスイッチが待機する時間を設定できます。IGMP 脱退の応答時間は、100 ~ 5000 ミリ秒の範囲で設定できます。タイマーはグローバルまたは VLAN 単位のいずれかを設定できます。VLAN 単位で Leave タイムを設定すると、グローバル設定値が上書きされます。

設定の手順については、「[IGMP Leave タイマーの設定](#) (P.28-11) 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装置に転送します。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、マルチキャスト装置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装置に転送します。

IGMP レポート抑制をディセーブルにすると、IGMP レポートはすべてマルチキャスト ルータに転送されます。設定の手順については、「[IGMP レポート抑制のディセーブル化](#) (P.28-16) 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、スイッチは IGMP パケットを調べ、パケットの内容に基づいて転送先を決定できるようになります。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.28-7)
- 「IGMP スヌーピングのイネーブルまたはディセーブル」 (P.28-7)
- 「スヌーピング方式の設定」 (P.28-8)
- 「マルチキャスト ルータ ポートの設定」 (P.28-9)
- 「グループにスタティックに加入するホストの設定」 (P.28-10)
- 「IGMP 即時脱退のイネーブル化」 (P.28-11)
- 「IGMP Leave タイマーの設定」 (P.28-11)
- 「TCN 関連コマンドの設定」 (P.28-12)
- 「IGMP スヌーピング クェリアの設定」 (P.28-14)
- 「IGMP レポート抑制のディセーブル化」 (P.28-16)

IGMP スヌーピングのデフォルト設定

表 28-3 に、IGMP スヌーピングのデフォルト設定を示します。

表 28-3 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 単位にイネーブル
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 スヌーピングの即時脱退	ディセーブル
スタティック グループ	設定なし
TCN ¹ フラッドイング クェリー カウント	2
TCN クェリー送信請求	ディセーブル
IGMP スヌーピング クェリア	ディセーブル
IGMP レポート抑制	イネーブル

1. TCN は、トポロジの変更通知のこと

IGMP スヌーピングのイネーブルまたはディセーブル

デフォルトで、スイッチ上の IGMP スヌーピングはグローバルにイネーブルになります。グローバルにイネーブルまたはディセーブルになっている場合、IGMP スヌーピングは既存のすべての VLAN インターフェイスでもイネーブルまたはディセーブルになります。デフォルトで、IGMP スヌーピングはすべての VLAN 上でイネーブルになりますが、VLAN 単位でイネーブルまたはディセーブルにすることができます。

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 スヌーピングを上書きします。グローバル スヌーピングがディセーブルの場合、VLAN のスヌーピングをイネーブルにできません。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することができます。

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) 設定をコンフィギュレーション ファイルに保存します。

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。

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。指定できる 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する必要があります。
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) 設定をコンフィギュレーション ファイルに保存します。

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、指定された VLAN 番号に対して `no ip igmp snooping vlan vlan-id` グローバル コンフィギュレーション コマンドを使用します。

スヌーピング方式の設定

マルチキャスト対応ルータ ポートは、レイヤ 2 のマルチキャスト エントリの転送テーブルに追加されます。次の方式のいずれかにより、スイッチはこのような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) の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 ポートへのスタティックな接続

スイッチを設定して、IGMP クエリーおよび PIM/DVMRP パケットをスヌーピングするか、CGMP self-join パケットまたは proxy-join パケットを待ち受けすることができます。デフォルトで、スイッチはすべての VLAN 上の PIM/DVMRP パケットをスヌーピングします。マルチキャスト ルータ ポートを CGMP パケットだけで学習させるには、**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、他の CGMP パケットを無視します。マルチキャスト ルータ ポートを PIM-DVMRP パケットだけで学習させるには、**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 に、CGMP proxy に対応したマルチキャスト ルータが存在しない場合、**ip cgmp router-only** コマンドを入力してルータにダイナミックにアクセスする必要があります。詳細については、第 49 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	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 上で IGMP スヌーピングをイネーブルにします。指定できる VLAN ID 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。この方式は制御トラフィックの削減に役立ちます。 • pim-dvmrp : IGMP クエリーおよび PIM-DVMRP パケットをスヌーピングします。これはデフォルトです。
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) 設定をコンフィギュレーション ファイルに保存します。

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

```
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 ポートを追加するには（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）、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な接続は、スイッチ ポート上でだけサポートされます。

■ IGMP スヌーピングの設定

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 と、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。 <ul style="list-style-type: none"> 指定できる VLAN ID 範囲は 1 ~ 1001 および 1006 ~ 4094 です。 このインターフェイスには物理インターフェイスまたはポート チャネルを指定できます。ポート チャネル範囲は 1 ~ 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) 設定をコンフィギュレーション ファイルに保存します。

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 gigabitethernet1/2
Switch(config)# end
```

グループにスタティックに加入するホストの設定

ホストまたはレイヤ 2 ポートは、通常、ダイナミックにマルチキャスト グループに加入しますが、インターフェイス上にホス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 <i>ip_address</i> interface <i>interface-id</i></code>	レイヤ 2 ポートをマルチキャスト グループのメンバーとしてスタティックに設定します。 <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。指定できる範囲は 1 ~ 1001 および 1006 ~ 4094 です。 <i>ip-address</i> はグループ 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) を指定できます。
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) 設定をコンフィギュレーション ファイルに保存します。

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 *mac-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、ポート上でホスト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 gigabitethernet1/1
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して、ポート上に IGMP バージョン 2 の Leave メッセージが検出された場合、スイッチはすぐ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) 即時脱退は、IGMP バージョン 2 のホストにだけサポートされます。

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 <i>vlan-id</i> immediate-leave	VLAN インターフェイスで 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) 設定をコンフィギュレーション ファイルに保存します。

VLAN 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 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場合、次の注意事項に従ってください。

- Leave タイムは、グローバルまたは VLAN 単位で設定できます。
- 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だけにサポートされています。
- 通常は、ネットワークにおける脱退の実際の待ち時間が、Leave タイムに設定されます。ただし、Leave タイムは、リアルタイムの CPU 負荷の状態、ネットワークの遅延、およびインターフェイスを経由して送信されるトラフィックの量によって、設定時間の前後に変動する可能性があります。

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 time</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に 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、グローバル設定の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) 設定をコンフィギュレーション ファイルに保存します。

IGMP Leave タイマーをグローバルにデフォルト設定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。

設定済みの IGMP Leave タイム設定を、指定の VLAN から削除するには、**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されたマルチキャスト トラフィックを制御する方法を示します。

- 「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.28-12)
- 「フラッドモードからの回復」(P.28-13)
- 「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.28-14)

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 イベントのあとにマルチキャスト トラフィックがフラッディングされる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されたマルチキャスト データ トラフィックに対する一般的クエリーの数を設定します。TCN イベントの例としては、クライアントが位置を変更したときに、レシーバーの存在する同じポートが、以前ブロックされていたが現在は転送中であったり、ポートが Leave メッセージを送信せずにダウンしたりする場合などです。

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 に設定すると、一般的クエリーを 7 件受信するまでフラッディングが継続します。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。デフォルトでは、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 設定を確認します。
ステップ 5	copy running-config startup-config	(任意) 設定をコンフィギュレーション ファイルに保存します。

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

フラッド モードからの回復

トポロジに変更が発生すると、スパニング ツリー ルートによって、グループ マルチキャスト アドレスを 0.0.0.0 に指定した、特定の IGMP Leave メッセージ (グローバル脱退) が送信されます。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 ルートであるかどうかに関係なく、スイッチがグローバル脱退メッセージを送信します。ルータがこの特定の Leave メッセージを受信すると、すぐに一般的クエリーが送信され、TCN イベント中のフラッド モードからの回復が速やかに処理されます。スイッチがスパニング ツリー ルートである場合、コンフィギュレーション コマンドに関係なく、常に Leave メッセージが送信されます。デフォルトでは、クエリー送信請求はディセーブルです。

スパニング ツリー ルートであるかどうかに関係なく、グローバル脱退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	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	TCN イベント中に発生したフラッド モードから回復するプロセスの速度を上げるために、IGMP Leave メッセージ (グローバル脱退) を送信します。デフォルトでは、クエリー送信請求はディセーブルです。
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 設定を確認します。
ステップ 5	copy running-config startup-config	(任意) 設定をコンフィギュレーション ファイルに保存します。

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

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、一般的クエリーが 2 件受信されるまで、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されます。スイッチ内の多数のポートが、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。**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、この動作を制御できます。

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	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	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	no ip igmp snooping tcn flood	スパニング ツリーの 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	exit	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp snooping	TCN 設定を確認します。
ステップ 6	copy running-config startup-config	(任意) 設定をコンフィギュレーション ファイルに保存します。

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場合は、次の注意事項に従ってください。

- グローバル コンフィギュレーション モードで VLAN を設定します。
- VLAN インターフェイス上に IP アドレスを設定します。イネーブルにすると、IGMP スヌーピング クエリアは、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に 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 クエリアに設定されたグローバル IP アドレスの使用を試みます。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) の IP アドレスの使用を試みます (存在する場合)。SVI の IP アドレスが存在しない場合、スイッチは、スイッチ上に設定された最初の利用可能な IP アドレスを使用します。最初に利用可能な IP アドレスは、**show ip interface** 特権 EXEC コマンドの出力に表示されます。スイッチ上に利用可能な IP アドレスを検出できない場合、IGMP スヌーピング クエリアは、IGMP の一般的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。
- 管理上イネーブルになっている場合、IGMP スヌーピング クエリアは、ネットワークでマルチキャスト ルータの存在を検出すると、非クエリア ステートに移行します。
- 管理上イネーブルになっている場合、IGMP スヌーピング クエリアは、次の条件に一致すると、動作上のディセーブル ステートに移行します。
 - VLAN で IGMP スヌーピングがディセーブルになっている。
 - 対応する VLAN の SVI 上で PIM がイネーブルになっている。

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、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 クエリアに IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。 (注) スイッチ上に IP アドレスを検出できない場合、IGMP スヌーピング クエリアは、IGMP の一般的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) トポロジ変更通知 (TCN) クエリ間の時間を設定します。カウントの範囲は 1 ~ 10 です。間隔の範囲は 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の長さを設定します。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	<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) IGMP スヌーピング クエリアが VLAN インターフェイス上で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) 設定をコンフィギュレーション ファイルに保存します。

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 レポート抑制はデフォルトでイネーブルになっています。この機能がイネーブルの場合、マルチキャスト ルータ クエリーごとに IGMP レポートが 1 つだけ転送されます。レポート抑制をディセーブルにすると、IGMP レポートはすべてマルチキャスト 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) 設定をコンフィギュレーション ファイルに保存します。

IGMP レポート抑制を再度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。

IGMP スヌーピング情報の表示

ダイナミックに学習された、またはスタティックに設定されたルータ ポートおよび VLAN インターフェイスの IGMP スヌーピング情報を表示できます。IGMP スヌーピング用に設定した VLAN の MAC アドレス マルチキャスト エントリも表示できます。

IGMP スヌーピング情報を表示するには、表 28-4 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 28-4 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>スイッチのすべての VLAN または指定した 1 つの VLAN のスヌーピング設定情報を表示します。</p> <p>(任意) 1 つの 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。指定できる VLAN ID 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するマルチキャスト テーブル情報を表示します。</p> <ul style="list-style-type: none"> • count : 実際のエントリの代わりに、指定のコマンド オプションに関するエントリの合計数を表示します。 • 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 : ユーザ設定のマルチキャスト 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 VLAN の特定パラメータに関するマルチキャスト テーブル情報を表示します。</p> <ul style="list-style-type: none"> • vlan-id : VLAN ID 範囲は 1 ~ 1001 および 1006 ~ 4094 です。 • count : 実際のエントリの代わりに、指定のコマンド オプションに関するエントリの合計数を表示します。 • 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 : グループ IP アドレスを指定したマルチキャスト グループの特性を表示します。 • user : ユーザ設定のマルチキャスト 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>ダイナミックに学習された、また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 ルータの接続先である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。</p> <p>(任意) 1 つの 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>

表 28-4 IGMP スヌーピング情報を表示するためのコマンド (続き)

コマンド	目的
<code>show ip igmp snooping querier [vlan vlan-id]</code>	VLAN 内で直前に受信した IGMP クエリー メッセージの IP アドレス および受信ポートに関する情報を表示します。 (任意) 1 つの VLAN に関する情報を表示するには、 <code>vlan vlan-id</code> を入力します。
<code>show ip igmp snooping querier [vlan vlan-id] detail</code>	VLAN 内で直前に受信した IGMP クエリー メッセージの IP アドレス および受信ポートに関する情報と、VLAN 内の IGMP スヌーピング クエリアの設定ステートおよび動作ステートに関する情報を表示します。

これらのコマンドのキーワードとオプションの詳細については、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。

マルチキャスト VLAN レジストレーションの概要

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 ネットワーク全体に、広範囲なマルチキャストトラフィックを展開する (たとえば、サービス プロバイダー ネットワーク上で複数のテレビチャンネルをブロードキャストする) アプリケーション向けに設計されています。MVR を使用すると、ポート上の加入者は、ネットワーク全体のマルチキャスト VLAN 上でマルチキャスト ストリームへの加入およびそこから脱退ができるようになります。また、加入者は個別の VLAN に残りながら、ネットワークで単一のマルチキャスト VLAN を共有することができます。MVR はマルチキャスト VLAN でマルチキャスト ストリームを連続送信する機能を持つと同時に、帯域幅やセキュリティ上の理由から、それらのストリームを加入者 VLAN から分離します。

MVR は、加入者ポートが、IGMP の Join メッセージと Leave メッセージを送信することにより、これらのマルチキャスト ストリームに加入したりそこから脱退したりすると想定します。これらのメッセージは、IGMP バージョン 2 と互換性のあるホストからイーサネット接続によって送信できます。MVR は IGMP スヌーピングのメカニズムに基づいて動作しますが、2 つの機能は互いに独立して動作します。1 つの機能を、もう一方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することができます。ただし、IGMP スヌーピングと MVR がどちらもイネーブルの場合、MVR は、MVR に基づいて設定されたマルチキャスト グループからの Join メッセージと Leave メッセージだけに反応しません。他のすべてのマルチキャスト グループからの Join メッセージと Leave メッセージは、IGMP スヌーピングによって管理されます。

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関連付けられた IP マルチキャスト グループを、スイッチ転送テーブル内で特定します。また、IGMP メッセージを代行受信し、レシーバーが送信元と異なる VLAN に属していても、マルチキャスト ストリームのレシーバーとして加入者を含めるか、または削除するために転送テーブルを変更します。この転送動作により、異なる VLAN 間へのトラフィックの通過が選択的に許可されます。

スイッチは、MVR 動作を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、ポート上の MVR ホストメンバーシップに関係なく、すべての MVR データ ポートに転送されます。マルチキャスト データは、IGMP レポートまたは MVR スタティック設定のいずれかにより、MVR ホストが加入しているレシーバー ポートにだけ転送されます。MVR ホストから受信した IGMP レポートは、スイッチで設定された MVR データ ポートから転送されることはありません。

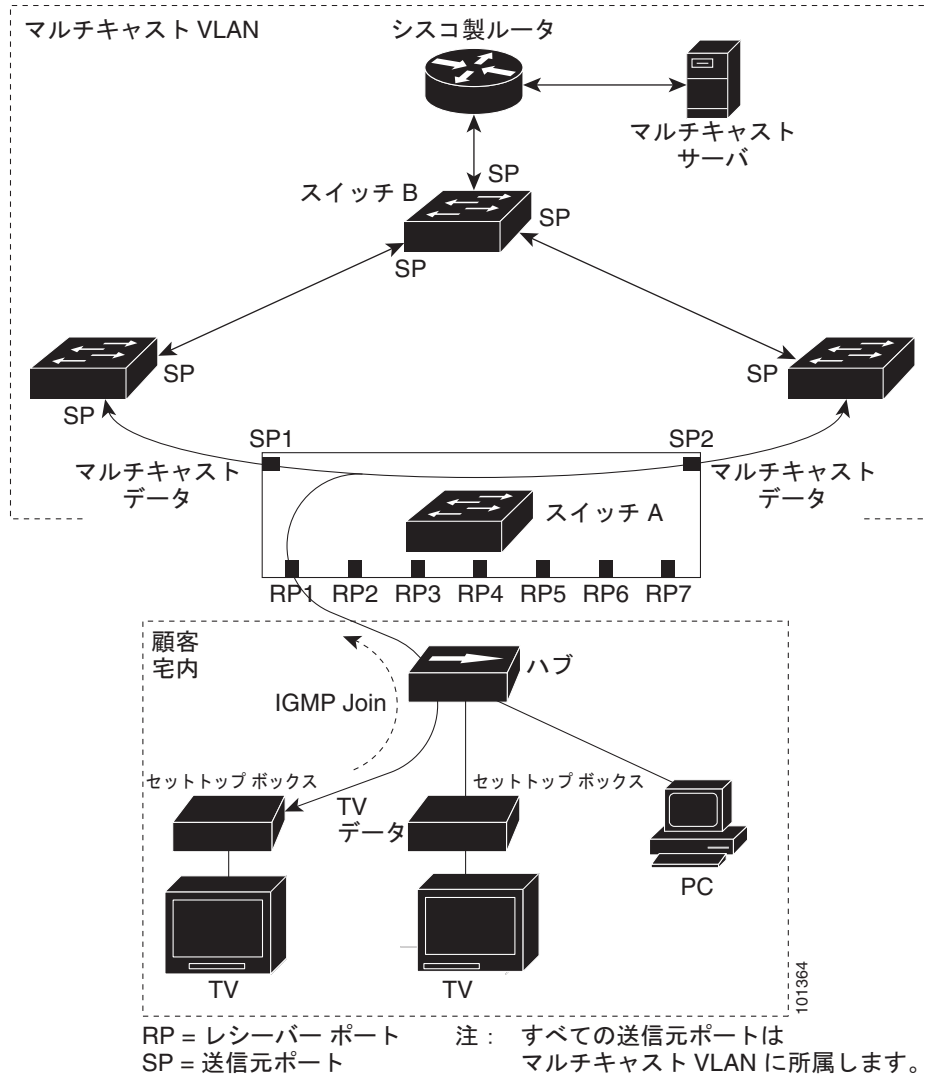
- ダイナミック モードの場合、スイッチ上の MVR ホストが受信したマルチキャスト データは、IGMP レポートまたは MVR スタティック設定のいずれかにより、MVR ホストが加入している MVR データ ポートとクライアント ポートだけから転送されます。MVR ホストから受信したすべての IGMP レポートも、スイッチのすべての MVR データ ポートから転送されます。これにより、MVR データ ポート リンクで不要な帯域幅が使用されなくなります。帯域幅の問題は、スイッチを互換モードで実行すると発生します。

レイヤ 2 ポートだけが MVR に属しています。ポートを MVR のレシーバー ポートとして設定する必要があります。スイッチごとに 1 つの MVR マルチキャスト VLAN だけがサポートされます。

マルチキャスト テレビ アプリケーションでの MVR の使用

マルチキャスト テレビ アプリケーションの場合、セットトップ ボックス搭載の PC またはテレビでマルチキャスト ストリームを受信することができます。複数のセットトップ ボックスまたは PC を、1 つの加入者ポートに接続できます。それには、MVR レシーバー ポートとしてスイッチ ポートを設定します。図 28-3 に設定の例を示します。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 が適切なマルチキャストに加入するように IGMP レポートをスイッチ A に送信します。IGMP レポートが、設定済みの IP マルチキャスト グループ アドレスのいずれかと一致すると、スイッチの CPU はハードウェアのアドレステーブルを変更し、指定されたマルチキャスト ストリームをマルチキャスト VLAN から受信した場合の転送宛先として、このレシーバー ポートと VLAN をテーブルに含めます。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 ポートは、MVR 送信元ポートと呼ばれます。

図 28-3 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変更したり、テレビのスイッチを切ったりした場合、セットトップボックスはマルチキャストストリームに対する IGMP Leave メッセージを送信します。スイッチの CPU は、MAC ベースの一般的クエリをレシーバーポート VLAN を介して送信します。VLAN に別のセットトップボックスが存在し、まだこのグループに加入している場合、そのセットトップボックスは、クエリに指定された最大応答時間内に応答する必要があります。CPU が応答を受信しないと、このグループの転送宛先としてそのレシーバーポートが破棄されます。

即時脱退を使用しない場合、スイッチがレシーバーポート上の加入者から IGMP Leave メッセージを受信すると、そのポート上で IGMP クエリを送信し、IGMP グループメンバーシップレポートを待機します。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。即時脱退を使用すると、IGMP Leave メッセージを受信したレシーバーポートから IGMP クエリは送信されません。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。即時脱退機能をイネーブルにするのは、レシーバー装置が 1 つだけ接続されたレシーバーポート上に限定してください。

MVR では、それぞれの VLAN の加入者に、テレビチャネルのマルチキャスト トラフィックを重複させる必要はありません。すべてのチャネルに対するマルチキャスト トラフィックは、マルチキャスト VLAN 上に限定して、VLAN トランクに一度だけ送信されます。IGMP Leave メッセージと Join メッセージは、加入者ポートの割り当て先の VLAN に含まれます。これらのメッセージは、レイヤ 3 装置 (スイッチ B) 上でマルチキャスト VLAN のマルチキャスト トラフィックのストリームにダイナミックに登録されます。アクセス レイヤ スイッチであるスイッチ A が、トラフィックがマルチキャスト VLAN から異なる VLAN の加入者ポートへ転送されるように転送動作を変更すると、2 つの VLAN 間でトラフィックの通過が選択的に許可されます。

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 グループのアドレスに送信されます。スイッチ A の CPU は、レシーバー ポートからのすべての IGMP Join メッセージと Leave メッセージをキャプチャし、MVR モードに基づき送信元 (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、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.28-21)
- 「MVR 設定時の注意事項および制約事項」 (P.28-22)
- 「MVR グローバル パラメータの設定」 (P.28-22)
- 「MVR インターフェイスの設定」 (P.28-24)

MVR のデフォルト設定

表 28-5 に、MVR のデフォルト設定を示します。

表 28-5 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にディセーブル
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 (ポート単位) デフォルト	レシーバー ポートと送信元ポートのどちらでもない
即時脱退	すべてのポート上でディセーブル

MVR 設定時の注意事項および制約事項

MVR を設定する場合、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 ポートだけにしてください。トランク ポートにすることはできません。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。
- スイッチ上に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 (つまり、受信可能なテレビ チャンネルの最大数) は 256 です。
- 送信元 VLAN で受信された MVR マルチキャスト データがレシーバー ポートから脱退すると、スイッチの Time to Live (TTL) が 1 つ減少します。
- 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ため、スイッチ上ではエイリアス IP マルチキャスト アドレスが許可されます。ただし、スイッチが Catalyst 3550 または Catalyst 3500 XL スイッチと連携動作している場合は、それらの間でエイリアスとして使用される IP アドレスや予約済みの IP マルチキャスト アドレス (224.0.0.xxx 範囲内) を設定する必要はありません。
- プライベート VLAN ポートには 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になっている場合、MVR はサポートされません。MVR がイネーブルになっている状態で、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 は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状態、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動作はキャンセルされ、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

デフォルト設定の使用を選択する場合、任意の 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 (MVR VLAN を除く)、最初に MVR をイネーブルにする必要があります。



(注)

この項で使用しているコマンドの構文と使用方法の詳細については、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 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 をイネーブルにします。

	コマンド	目的
ステップ 3	<code>mvr group ip-address [count]</code>	スイッチ上に IP マルチキャスト アドレスを設定するか、 <i>count</i> パラメータ (<i>count</i> の範囲は 1 ~ 256 で、デフォルト値は 1) を使用して、一連の連続 MVR グループ アドレスを設定します。このアドレスに送信されるすべてのマルチキャスト データは、スイッチ上のすべての送信元ポートと、そのマルチキャスト アドレスでデータを受信するように選択されたすべてのレシーバー ポートに送信されます。各マルチキャスト アドレスは、1 つのテレビチャンネルに対応します。
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 ポート上で IGMP レポート メンバーシップを待機する最大時間を定義します。この値は 10 分の 1 秒単位です。指定できる範囲は 1 ~ 100 です。デフォルトは 5/10 秒つまり 1/2 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がこの VLAN に属している必要があります。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	<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"> dynamic : 送信元ポート上でダイナミック MVR メンバーシップが使用できるようになります。 compatible : Catalyst 3500 XL および Catalyst 2900 XL スイッチと互換性があり、送信元ポートで IGMP ダイナミック加入をサポートしません。 デフォルトは compatible 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> or <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) 設定をコンフィギュレーション ファイルに保存します。

スイッチをデフォルト設定に戻すには、`no mvr [mode | group ip-address | querytime | vlan]` グローバル コンフィギュレーション コマンドを使用します。

次に、MVR をイネーブルにし、グループ アドレスを設定し、クエリー時間を 1 秒 (10/10 秒) に設定し、MVR マルチキャスト VLAN を VLAN 22 に指定し、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 コマンドを使用して、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。加入者は、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、単一のマルチキャスト VLAN に属します。 receiver : ポートが加入者ポートで、マルチキャスト データの受信だけを行う場合は、ポートをレシーバー ポートとして設定します。スタティックに、または IGMP の Leave メッセージまたは Join メッセージによってポートがマルチキャスト グループのメンバーにならない限り、データは受信されません。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。 <p>デフォルト設定は、非 MVR ポートです。MVR 特性を使用して非 MVR ポートの設定を試行すると、動作が失敗します。</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 と IP マルチキャスト アドレスに送信されるマルチキャスト 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ます。グループの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るまではそのグループのメンバーのままです。</p> <p>(注) 互換モードの場合、このコマンドはレシーバー ポートにだけ適用されます。ダイナミック モードの場合、このコマンドはレシーバー ポートと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 の Join メッセージと Leave メッセージを使用して、ダイナミックにマルチキャスト グループ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) ポートの MVR の即時脱退機能をイネーブルにします。</p> <p>(注) このコマンドはレシーバー ポートにだけ適用され、レシーバー装置が 1 つだけ接続されたレシーバー ポートに限定してイネーブルにしてください。</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) 設定をコンフィギュレーション ファイルに保存します。

インターフェイスをデフォルト設定に戻すには、`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る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、ポート上で即時脱退を設定し、結果を確認する例を示します。

```
Switch(config)# mvr
Switch(config)# interface gigabitethernet1/2
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
----      -
Gil/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 設定を表示するには、特権 EXEC モードで表 28-6 に示すコマンドを使用します。

表 28-6 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 ステータスと値を表示します。MVR がイネーブルかディセーブルであるかに関係なく、マルチキャスト VLAN、マルチキャストグループの最大値 (256) および現在値 (0 ~ 256)、クエリー応答時間、および MVR モードを表示します。
<code>show mvr interface [interface-id] [members [vlan vlan-id]]</code>	すべての MVR インターフェイスとその MVR 設定を表示します。 特定のインターフェイスを入力すると、この情報が表示されます。 <ul style="list-style-type: none"> タイプ：レシーバーまたは送信元 ステータス：次のいずれかになります。 <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、ポートが転送中か転送中でないかを示します。 INACTIVE は、ポートが VLAN に含まれていないことを意味します。 即時脱退：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、こ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、VLAN ID を入力すると、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>	任意の IP マルチキャストグループのメンバーであるすべてのレシーバーポートと送信元ポート、または指定 IP マルチキャストグループの IP アドレスを表示します。

IGMP フィルタリング/スロットリングの設定

たとえば、首都圏または Multiple-Dwelling Unit (MDU; 集合住宅) での設置など、環境によっては、スイッチポート上のユーザが所属できるマルチキャストグループのセットを制御する場合があります。加入またはサービスプランのタイプに基づき、IP/TV など、マルチキャストサービスの分散を制御できます。スイッチポート上のユーザが所属できるマルチキャストグループの数を制限する場合もあります。

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て個別のスイッチポートに関連付けることで、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。1 つの IGMP プロファイルには 1 つまたは複数のマルチキャストグループを含めることができます。また、IGMP プロファイルは、グループへのアクセスを許可するか拒否するかを指定します。IGMP プロファイルのマルチキャストグループへのアクセス拒否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 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。フィルタリングアクションによってマルチキャストグループへのアクセスが許可されると、ポートからの IGMP レポートは転送されて通常に処理されます。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 フィルタリングは、Join レポートや Leave レポートなど、グループ固有のクエリーとメンバーシップレポートだけを制御します。一般的な IGMP クエリーは制御しません。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関連していません。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 または MVR が使用されていても同様に動作します。

IGMP フィルタリングが適用可能なのは、IP マルチキャストグループアドレスのダイナミックな学習だけで、スタティック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て、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、インターフェイスが IGMP Join レポートを受信した場合、IGMP ポートを廃棄するか、ランダムに選択したマルチキャストエントリを受信済みの IGMP レポートで置き換えるように、インターフェイスを設定できます。



(注)

IGMPv3 の Join メッセージと Leave メッセージは、IGMP フィルタリングを実行中のスイッチにはサポートされません。

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/スロットリングのデフォルト設定」(P.28-27)
- 「IGMP プロファイルの設定」(P.28-27) (任意)
- 「IGMP プロファイルの適用」(P.28-28) (任意)
- 「IGMP グループの最大数の設定」(P.28-29) (任意)
- 「IGMP スロットリングアクションの設定」(P.28-30) (任意)

IGMP フィルタリング/スロットリングのデフォルト設定

表 28-7 に、IGMP フィルタリングのデフォルト設定を示します。

表 28-7 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	適用なし
IGMP グループの IGMP 最大数	最大値の設定なし
IGMP プロファイル	定義なし
IGMP プロファイル アクション	アドレス範囲の拒否

転送テーブル内に最大数のグループが含まれる場合、デフォルトの IGMP スロットリングアクションにより IGMP レポートが拒否されます。設定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.28-30) 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 コマンドをプロファイル番号とともに使用して 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。このモードで、IGMP プロファイルのパラメータを指定し、ポートからの IGMP Join 要求をフィルタリングするために使用できます。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)。
- **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。1 つの IP アドレス、またはアドレスの最初と最後で範囲を指定することもできます。

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ません。プロファイルの設定の際に、**permit** または **deny** キーワードのいずれも含まれない場合、デフォルトで IP アドレスの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。アクションが設定されない場合、プロファイルはデフォルトでアクセスを拒否します。

■ IGMP フィルタリング/スロットリングの設定

	コマンド	目的
ステップ 4	<code>range ip multicast address</code>	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 アドレスの範囲を入力します。範囲を入力する場合、低い方の IP マルチキャスト アドレスを入力してからスペースを入力し、次に高い方の IP マルチキャスト アドレスを入力します。 range コマンドを数回使用して、複数のアドレスまたはアドレスの範囲を入力できます。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show ip igmp profile profile number</code>	プロファイル設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) 設定をコンフィギュレーション ファイルに保存します。

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 アドレスの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、設定を確認する例を示します。アクションがアクセス拒否 (デフォルト) の場合、**show ip igmp profile** の出力に表示されません。

```
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 プロファイルに定義された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適切な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 ポートにだけ適用できます。IGMP プロファイルをルーテッド ポートまたは SVI に適用することはできません。EtherChannel ポート グループに属するポートには、プロファイルを適用できません。プロファイルは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は 1 つのプロファイルしか適用できません。

IGMP プロファイルをスイッチ ポートに適用するには、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	<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>	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 グループに属さないレイヤ 2 ポートにする必要があります。
ステップ 3	<code>ip igmp filter profile number</code>	指定した 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	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
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) 設定をコンフィギュレーション ファイルに保存します。

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 をポートに適用する例を示します。

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

IGMP グループの最大数の設定

`ip igmp max-groups` インターフェイス コンフィギュレーション コマンドを使用して、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。最大値をデフォルトの `no limit` に戻すには、このコマンドの `no` 形式を使用します。

この制限はレイヤ 2 ポートにだけ適用されます。ルーテッド ポートまたは SVI 上には IGMP グループの最大数を設定することはできません。このコマンドは論理 EtherChannel インターフェイス上でも使用できますが、EtherChannel ポート グループに属するポートには使用できません。

転送テーブル内の 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 グループに属さないレイヤ 2 ポート、または EtherChannel インターフェイスにすることができます。
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) 設定をコンフィギュレーション ファイルに保存します。

最大グループ制限を削除して、最大数が指定されないデフォルトに戻すには、`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 gigabitethernet1/2
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に、**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、既存グループを IGMP レポートを受信した新しいグループに置き換え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。

- この制約は、レイヤ 2 ポートにだけ適用できます。このコマンドは論理 EtherChannel インターフェイス上で使用できませんが、EtherChannel ポート グループに属するポートには使用できません。
- 最大グループ制限がデフォルト（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無効です。
- インターフェイスがマルチキャスト エントリを転送テーブルに追加したあとに、スロットリング アクションを設定して最大グループ制限を設定する場合、スロットリング アクションに応じて、転送テーブルのエントリは期限切れになるか、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、以前転送テーブルにあったエントリは、削除されませんが期限切れになります。これらのエントリの期限が切れて、最大数のエントリが転送テーブルにある場合、スイッチは、インターフェイス上で受信された次の 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、以前転送テーブルにあったエントリが削除されます。最大数のエントリが転送テーブルにある場合、スイッチはランダムに選択したエントリを、受信した IGMP レポートと置き換えます。

スイッチによって転送テーブルのエントリが削除されないように、インターフェイスがエントリを転送テーブルに追加する前に、IGMP スロットリング アクションを設定できます。

転送テーブルに最大数のエントリが含まれる場合のスロットリング 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	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 グループに属さないレイヤ 2 ポート、または EtherChannel インターフェイスにすることができます。このインターフェイスはトランク ポートにはできません。
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、転送テーブルに最大数のエントリが含まれる場合、インターフェイスが行うアクションを指定します。 <ul style="list-style-type: none"> deny : レポートを廃棄します。 replace : 既存グループを IGMP レポートを受信した新しいグループと置き換えます。
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) 設定をコンフィギュレーション ファイルに保存します。

レポートを廃棄するデフォルト動作に戻すには、**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/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、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の IGMP プロファイルと最大グループ設定を表示できます。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対する IGMP スロットリング設定を表示できます。

IGMP フィルタリング/スロットリング設定を表示するには、表 28-8 に示す各特権 EXEC コマンドを使用します。

表 28-8 IGMP フィルタリング/スロットリング設定を表示するためのコマンド

コマンド	目的
<code>show ip igmp profile [profile number]</code>	指定した IGMP プロファイルまたはスイッチ上に定義されたすべての 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 グループの最大数やインターフェイスに適用される IGMP プロファイル（設定されている場合）など、指定したインターフェイスの設定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/スロットリング設定の表示