



IGMP スヌーピングの設定

- [IGMP スヌーピングの前提条件](#) (1 ページ)
- [IGMP スヌーピングの制約事項](#) (2 ページ)
- [IGMP スヌーピングについて](#) (2 ページ)
- [IGMP スヌーピングを設定する方法](#) (9 ページ)
- [IGMP スヌーピングのモニタリング](#) (25 ページ)
- [IGMP スヌーピングの設定例](#) (27 ページ)
- [IGMP スヌーピングの機能履歴と情報](#) (29 ページ)

IGMP スヌーピングの前提条件

IGMP スヌーピング クエリアを設定するときには、次の注意事項を順守します。

- VLAN をグローバル コンフィギュレーション モードに設定してください。
- IP アドレスおよび VLAN インターフェイスを設定してください。IGMP スヌーピング クエリアは、イネーブルの場合この IP アドレスをクエリーの送信元アドレスとして使用します。
- VLAN インターフェイス上で IP アドレスが設定されていない場合、IGMP スヌーピング クエリアは IGMP クエリア用に設定されたグローバル IP アドレスを使用しようとします。グローバル IP アドレスが指定されていない場合、IGMP クエリアは VLAN スイッチ仮想 インターフェイス (SVI) IP アドレス (存在する場合) を使用しようとします。SVI IP アドレスが存在しない場合、デバイスはデバイス上で設定された利用可能な最初の IP アドレスを使用します。利用可能な最初の IP アドレスは、**show ip interface** 特権 EXEC コマンドの出力に表示されます。IGMP スヌーピングクエリアはデバイス上で利用可能な 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、VLAN で IGMP スヌーピングが無効になっていると、IGMP スヌーピングクエリアは動作無効状態に移行します。

- レイヤ3 マルチキャストはサポートされていません。
- MAC ベースのスヌーピングはハードウェアでサポートされています。

IGMP スヌーピングの制約事項

次に、IGMP スヌーピングの制約事項を示します。

- IGMP レポート抑制は、マルチキャストクエリに 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、クエリに IGMPv3 レポートが含まれている場合はサポートされません。
- IGMP の脱退時間の設定は、IGMP バージョン 2 が稼働しているホストでのみサポートされます。IGMP バージョン 2 は、デバイスのデフォルトバージョンです。

ネットワークで実際の脱退にかかる待ち時間は、通常、設定した脱退時間どおりになります。ただし、脱退時間は、リアルタイムの CPU の負荷の状態、およびネットワークの遅延状態、インターフェイスから送信されたトラフィック量によって、設定された時間を前後することがあります。

- IGMP スロットリングアクションの制約事項は、レイヤ2 ポートにだけ適用されます。**ip igmp max-groups action replace** インターフェイス コンフィギュレーション コマンドは論理 EtherChannel インターフェイスで使用できますが、EtherChannel ポートグループに属するポートでは使用できません。

グループの最大数に関する制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups action {deny | replace}** コマンドを入力しても効果はありません。

インターフェイスによりマルチキャスト エントリが転送テーブルに追加されてから、スロットリングアクションを設定し、グループの最大数の制限を設定すると、転送テーブルのエントリは、スロットリングアクションに応じて期限切れになるか削除されます。

IGMP スヌーピングについて

IGMP スヌーピング

レイヤ2 デバイスは 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 デバイス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。デバイスが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場合、デバイスはホストのポート番号を転送テーブルエントリに追加します。ホストから IGMP Leave Group メッセージを受信した場合は、テーブルエントリからホス

トポートを削除します。マルチキャスト クライアントから IGMP メンバーシップ レポートを受信しなかった場合にも、スイッチはエントリを定期的に削除します。



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

マルチキャスト ルータは、すべての VLAN に定期的にジェネラル 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。デバイスは、IGMP Join 要求の送信元となる各グループの IGMP スヌーピング IP マルチキャスト転送テーブルで、VLAN ごとに1つずつエントリを作成します。

デバイスは、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。デバイスでは IP マルチキャストグループを使用するので、アドレスエイリアスの問題は発生しません。

IGMP スヌーピングによって、IP マルチキャストグループは動的に学習されます。ただし、**ip igmp snooping vlan *vlan-id* static *ip_address* interface *interface-id*** グローバル コンフィギュレーション コマンドを使用すると、マルチキャストグループを静的に設定できます。グループメンバ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。

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

ここでは、IGMP スヌーピングの特性について説明します。

IGMP のバージョン

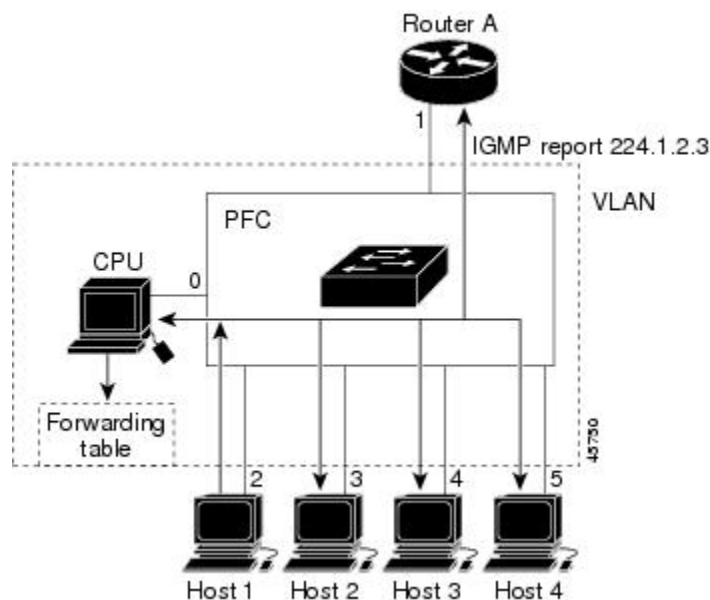
デバイスは、IGMP バージョン 1、IGMP バージョン 2、および IGMP バージョン 3 をサポートしています。これらのバージョンは、デバイス上でそれぞれ相互運用できます。たとえば、IGMP スヌーピングがイネーブルになっていて、クエリアのバージョンが IGMPv2 で、デバイスがホストから IGMPv3 レポートを受信している場合、デバイスは IGMPv3 レポートをマルチキャストルータに転送できます。

IGMPv3 デバイスは、Source Specific Multicast (SSM; 送信元特定マルチキャスト) 機能を実行しているデバイスとの間で、メッセージを送受信できます。

マルチキャスト グループへの加入

図 1: 最初の IGMP Join メッセージ

デバイスに接続したホストが IP マルチキャストグループに加入し、なおかつそのホストが IGMP バージョン 2 クライアントの場合、ホストは加入する IP マルチキャストグループを指定した非送信請求 IGMP Join メッセージを送信します。別の方法として、ルータから一般クエリを受信したデバイスは、そのクエリを VLAN 内のすべてのポートに転送します。IGMP バージョン 1 またはバージョン 2 のホストがマルチキャストグループに加入する場合、ホストはデバイスに Join メッセージを送信することによって応答します。デバイスの 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。



ルータ A がデバイスに一般クエリを送信し、そこでそのクエリは同じ VLAN のすべてのメンバーであるポート 2 ~ 5 に転送されます。ホスト 1 はマルチキャストグループ 224.1.2.3 に加入するために、グループに IGMP メンバーシップ レポート (IGMP Join メッセージ) をマルチキャストします。デバイスの CPU は IGMP レポートの情報を使用して、転送テーブルのエントリを設定します。転送テーブルにはホスト 1 およびルータに接続しているポート番号が含まれます。

表 1: IGMP スヌーピング転送テーブル

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

デバイスのハードウェアは、IGMP 情報パケットをマルチキャストグループの他のパケットと区別できます。テーブルの情報は、224.1.2.3 マルチキャスト IP アドレス宛ての、IGMP パケッ

トではないフレームを、ルータおよびグループに加入したホストに対して送信するように、スイッチングエンジンに指示します。

図 2:2 番目のホストのマルチキャストグループへの加入

別のホスト（たとえば、ホスト 4）が、同じグループ用に非送信請求 IGMP Join メッセージを送信する場合、CPU がそのメッセージを受け取り、ホスト 4 のポート番号を転送テーブルに追加します。転送テーブルは CPU 宛てだけに IGMP メッセージを送るので、メッセージはデバイスの他のポートにフラッディングされません。認識されているマルチキャストトラフィックは、CPU 宛てではなくグループ宛てに転送されます。

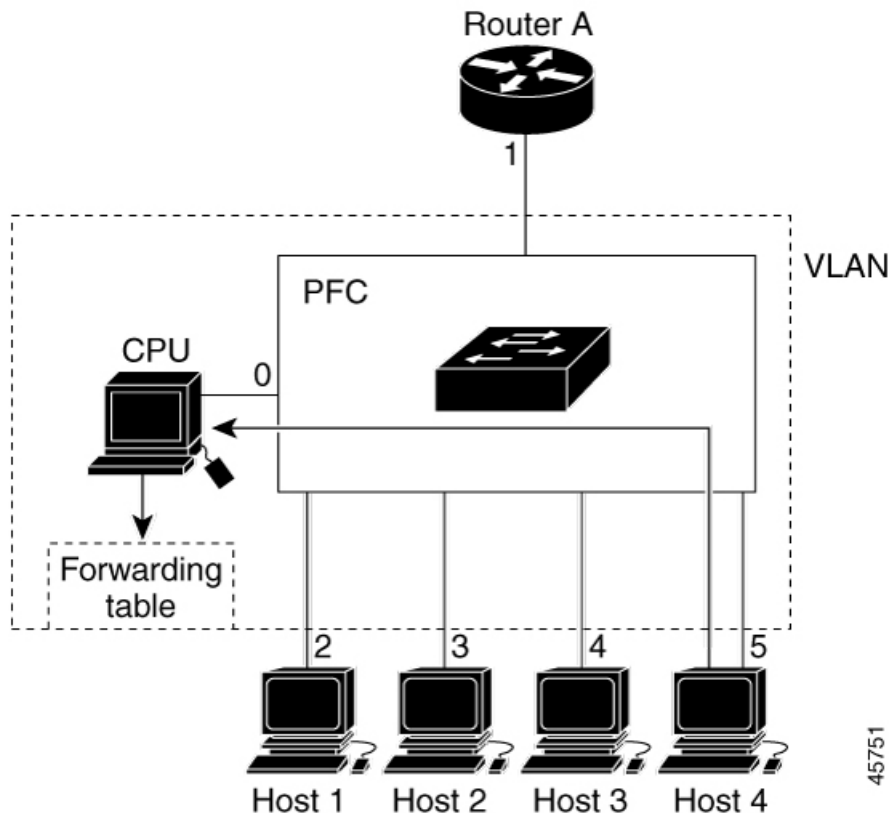


表 2:更新された IGMP スヌーピング転送テーブル

宛先アドレス	パケットのタイプ	ポート
224.1.2.3	IGMP	1, 2, 5

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を定期的を送信し、デバイスはそれらのクエリを VLAN のすべてのポートを通じて転送します。関心のあるホストがクエリーに応答します。VLAN 内の少なくとも 1 つのホストがマルチキャストトラフィックを受信するようなら、ルータは、その VLAN へのマルチキャストトラフィックの転送を続行します。デバイスは、その IGMP ス

スヌーピングによって維持された IP マルチキャストグループの転送テーブルで指定されたホストに対してだけ、マルチキャストグループトラフィックを転送します。

ホストがマルチキャストグループから脱退する場合、何も通知せずに脱退することも、Leave メッセージを送信することもできます。ホストから Leave メッセージを受信したデバイスは、グループ固有のクエリを送信して、そのインターフェイスに接続された他のデバイスが所定のマルチキャストグループのトラフィックに関与しているかどうかを学習します。デバイスはさらに、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

デバイスは IGMP スヌーピングの即時脱退を使用して、先にデバイスからインターフェイスにグループ固有のクエリを送信しなくても、Leave メッセージを送信するインターフェイスを転送テーブルから削除できるようにします。VLAN インターフェイスは、最初の Leave メッセージで指定されたマルチキャストグループのマルチキャストツリーからブルーニングされます。即時脱退によって、複数のマルチキャストグループが同時に使用されている場合でも、スイッチドネットワークのすべてのホストに最適な帯域幅管理が保証されます。

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。IGMP バージョン 2 は、デバイスのデフォルトバージョンです。



- (注) 即時脱退機能を使用するのは、各ポートに接続されているホストが 1 つだけの VLAN に限定してください。ポートに複数のホストが接続されている VLAN 上で即時脱退をイネーブルにすると、一部のホストが誤ってドロップされる可能性があります。

IGMP 脱退タイマーの設定

まだ指定のマルチキャストグループに関心があるかどうかを確認するために、グループ固有のクエリを送信した後のデバイスの待機時間を設定できます。IGMP 脱退応答時間は、100 ~ 32767 ミリ秒の間で設定できます。

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。

デバイスは 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ごとに 1 つの IGMP レポートのみをマルチキャストデバイスに転送します。IGMP レポート抑制がイネーブル（デフォルト）である場合、デバイスは最初の IGMP レポートをグループのすべてのホストからす

すべてのマルチキャストルータに送信します。デバイスは、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にIGMPv1 およびIGMPv2 レポートに対する要求のみが含まれている場合、デバイスは最初のIGMPv1 レポートまたはIGMPv2 レポートのみを、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転送します。

マルチキャストルータクエリにIGMPv3 レポートに対する要求も含まれる場合、デバイス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 スヌーピングのデフォルト設定

次の表に、デバイスのIGMP スヌーピングのデフォルト設定を示します。

表 3: IGMP スヌーピングのデフォルト設定

機能	デフォルト設定
IGMP スヌーピング	グローバルおよび VLAN 単位でイネーブル
マルチキャスト ルータ	未設定
IGMP スヌーピング即時脱退	ディセーブル
スタティック グループ	未設定
TCN ¹ フラッドクエリ カウント	2
TCN クエリ送信要求	ディセーブル
IGMP スヌーピング クエリア	ディセーブル
IGMP レポート抑制	有効

¹ (1) TCN = トポロジ変更通知

IGMP フィルタリングおよびスロットリング

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

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

IGMP フィルタリングで制御されるのは、グループ固有のクエリーおよびメンバーシップレポート (Join および Leave レポートを含む) だけです。一般 IGMP クエリーは制御されません。IGMP フィルタリングは、IP マルチキャストトラフィックの転送を指示する機能とは無関係です。フィルタリング機能は、マルチキャストトラフィックの転送に CGMP が使用されているか、または MVR が使用されているかに関係なく、同じように動作します。

IGMP フィルタリングが適用されるのは、IP マルチキャストグループアドレスを動的に学習する場合だけです。静的な設定には適用されません。

IGMP スロットリング機能を使用すると、レイヤ2 インターフェイスが加入できる IGMP グループの最大数を設定できます。IGMP グループの最大数が設定され、IGMP スヌーピング転送テーブルに最大数のエントリが登録されていて、インターフェイスで IGMP Join レポートを受信する場合、インターフェイスを設定することにより、IGMP レポートを廃棄するか、あるいは受信した IGMP レポートでランダムに選択されたマルチキャストエントリを上書きします。



- (注) IGMP フィルタリングが実行されているデバイスは、IGMPv3 Join および Leave メッセージをサポートしていません。

IGMP フィルタリングおよび IGMP スロットリングのデフォルト設定

次の表に、デバイスの IGMP フィルタリングおよびスロットリングのデフォルト設定を示します。

表 4: IGMP フィルタリングのデフォルト設定

機能	デフォルト設定
IGMP フィルタ	適用なし
IGMP グループの最大数	最大数の設定なし (注) 転送テーブルに登録されているグループが最大数に達していると、デフォルトの IGMP スロットリングアクションは IGMP レポートを拒否します。

機能	デフォルト設定
IGMP プロファイル	未定義
IGMP プロファイルアクション	範囲で示されたアドレスを拒否

IGMP スヌーピングを設定する方法

デバイスでの IGMP スヌーピングのイネーブル化またはディセーブル化

IGMP スヌーピングがグローバルにイネーブルまたはディセーブルに設定されている場合は、既存のすべての VLAN インターフェイスでもイネーブルまたはディセーブルになります。デフォルトでは IGMP スヌーピングはすべての VLAN でイネーブルになっていますが、VLAN 単位でイネーブルまたはディセーブルにすることができます。

グローバル IGMP スヌーピングは、VLAN IGMP スヌーピングより優先されます。グローバル スヌーピングがディセーブルの場合、VLAN スヌーピングをイネーブルに設定することはできません。グローバル スヌーピングがイネーブルの場合、VLAN スヌーピングをイネーブルまたはディセーブルに設定できます。

デバイスで IGMP スヌーピングをグローバルにイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# 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 3	ip igmp snooping 例： Device(config)# ip igmp snooping	既存のすべての VLAN インターフェイスでグローバルに IGMP スヌーピングを有効にします。

	コマンドまたはアクション	目的
		(注) すべての VLAN インターフェイス上で IGMP スヌーピングをグローバルにディセーブルにするには、 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。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config 例： Device# 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 インターフェイスでの IGMP スヌーピングのイネーブル化またはディセーブル化

VLAN インターフェイス上で IGMP スヌーピングを有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# 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 3	ip igmp snooping vlan <i>vlan-id</i> 例： Device(config)# ip igmp snooping vlan 7	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。 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。

	コマンドまたはアクション	目的
		(注) 特定の VLAN インターフェイス上で IGMP スヌーピングをディセーブルにするには、 no ip igmp snooping vlan <i>vlan-id</i> 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。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config 例： Device# 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 ルータ ポートの設定

デバイスにマルチキャスト ルータ ポートを追加する (マルチキャスト ルータへのスタティック接続を有効にする) には、次の手順を実行します。



(注) マルチキャスト ルータへのスタティック接続は、デバイスポートに限りサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# 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 3	ip igmp snooping vlan <i>vlan-id</i> mrouter interface <i>interface-id</i> 例：	マルチキャスト ルータの VLAN ID およびマルチキャスト ルータに対するインターフェイスを指定します。

	コマンドまたはアクション	目的
	<pre>Device(config)# ip igmp snooping vlan 5 mrouter interface gigabitethernet 1/0/1</pre>	<ul style="list-style-type: none"> 指定できる VLAN ID の範囲は 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 ~ 128 です。 <p>(注) 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。</p>
ステップ 4	<pre>end</pre> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 5	<pre>show ip igmp snooping mrouter [vlan vlan-id]</pre> <p>例 :</p> <pre>Device# show ip igmp snooping mrouter vlan 5</pre>	VLAN インターフェイス上で IGMP スヌーピングが有効になっていることを確認します。
ステップ 6	<pre>copy running-config startup-config</pre> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

グループに加入するホストの静的な設定

ホストまたはレイヤ 2 ポートは通常、マルチキャストグループに動的に加入しますが、インターフェイス上にホストを静的に設定することもできます。

マルチキャストグループのメンバーとしてレイヤ 2 ポートを追加するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	<pre>enable</pre> <p>例 :</p>	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> enable	<ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# 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 3	ip igmp snooping vlan <i>vlan-id</i> static <i>mac_address</i> interface <i>interface-id</i> 例： Device(config)# ip igmp snooping vlan 105 static 0100.5exx.xxxx interface gigabitethernet1/0/1	<p>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。</p> <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 または 1006 ~ 4094 です。 <i>mac-address</i> は、グループ MAC アドレスです。 <i>interface-id</i> は、メンバポートです。物理インターフェイスまたはポートチャンネル (1 ~ 6) に設定できます。 <p>(注) マルチキャストグループからレイヤ2ポートを削除するには、no ip igmp snooping vlan <i>vlan-id</i> static <i>mac-address</i> interface <i>interface-id</i> グローバルコンフィギュレーションコマンドを使用します。</p>
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp snooping groups 例： Device# 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 6	copy running-config startup-config 例： Device# 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 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、デバイスはポート上で IGMP バージョン 2 の Leave メッセージを検出した場合、ただちにそのポートを削除します。即時脱退機能は、VLAN の各ポートにレシーバが 1 つ存在する場合にだけ使用してください。



(注) 即時脱退機能をサポートするのは、IGMP バージョン 2 が稼働しているホストだけです。IGMP バージョン 2 は、デバイスのデフォルトバージョンです。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# 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 3	ip igmp snooping vlan <i>vlan-id</i> immediate-leave 例： Device(config)# ip igmp snooping vlan 21 immediate-leave	VLAN インターフェイス上で、IGMP 即時脱退をイネーブルにします。 (注) 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 <i>vlan-id</i> 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。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp snooping vlan <i>vlan-id</i> 例： Device# show ip igmp snooping vlan 21	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。

IGMP 脱退タイマーの設定

脱退時間はグローバルまたは VLAN 単位で設定できます。IGMP 脱退タイマーの設定をイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# 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 3	ip igmp snooping last-member-query-interval time 例： Device(config)# ip igmp snooping last-member-query-interval 1000	IGMP 脱退タイマーをグローバルに設定します。指定できる範囲は 100 ~ 32767 ミリ秒です。 デフォルトの脱退時間は 1000 ミリ秒です。 (注) IGMP 脱退タイマーをグローバルにリセットしてデフォルト設定に戻すには、 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。
ステップ 4	ip igmp snooping vlan vlan-id last-member-query-interval time 例： Device(config)# ip igmp snooping vlan 210 last-member-query-interval 1000	(任意) VLAN インターフェイス上で IGMP 脱退時間を設定します。有効値は 100 ~ 32767 ミリ秒です。 (注) VLAN 上に脱退時間を設定すると、グローバルに設定された内容は上書きされます。 (注) 特定の VLAN から IGMP 脱退タイマーの設定を削除するには、 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。
ステップ 5	end 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device(config)# end	
ステップ 6	show ip igmp snooping 例： Device# show ip igmp snooping	(任意) 設定された IGMP 脱退時間を表示します。
ステップ 7	copy running-config startup-config 例： Device# 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 スヌーピング クエリアの設定

特定の VLAN で IGMP スヌーピング クエリア機能をイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	ip igmp snooping querier 例： Device(config)# ip igmp snooping querier	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	configure terminal 例： Device# 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 4	ip igmp snooping querier address ip_address 例： Device(config)# ip igmp snooping querier address 172.16.24.1	(任意) IGMP スヌーピング クエリアの IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。 (注) IGMP スヌーピングクエリアがデバイス上で IP アドレスを検出できない場合、IGMP 一般クエリを生成しません。

	コマンドまたはアクション	目的
ステップ 5	ip igmp snooping querier query-interval <i>interval-count</i> 例： Device(config)# ip igmp snooping querier query-interval 30	(任意) IGMP クエリアの間隔を設定します。指定できる範囲は 1 ~ 18000 秒です。
ステップ 6	ip igmp snooping querier tcn query [<i>count count</i> <i>interval interval</i>] 例： Device(config)# ip igmp snooping querier tcn query interval 20	(任意) トポロジ変更通知 (TCN) クエリアの間隔を設定します。指定できる count の範囲は 1 ~ 10 です。指定できる interval の範囲は 1 ~ 255 秒です。
ステップ 7	ip igmp snooping querier timer expiry <i>timeout</i> 例： Device(config)# ip igmp snooping querier timer expiry 180	(任意) IGMP クエリアが期限切れになる時間を設定します。指定できる範囲は 60 ~ 300 秒です。
ステップ 8	ip igmp snooping querier version <i>version</i> 例： Device(config)# ip igmp snooping querier version 2	(任意) クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。
ステップ 9	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 10	show ip igmp snooping vlan <i>vlan-id</i> 例： Device# show ip igmp snooping vlan 30	(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 VLANID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
ステップ 11	copy running-config startup-config 例： Device# 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 レポート抑制のディセーブル化

IGMP レポート抑制をディセーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# 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 3	no ip igmp snooping report-suppression 例： Device(config)# no ip igmp snooping report-suppression	IGMP レポート抑制をディセーブルにします。IGMP レポート抑制がディセーブルの場合、すべての IGMP レポートがマルチキャスト ルータに転送されます。 IGMP レポート抑制はデフォルトでイネーブルです。 IGMP レポート抑制がイネーブルの場合、デバイスはマルチキャスト ルータクエリごとに IGMP レポートを 1 つだけ転送します。 (注) IGMP レポート抑制を再びイネーブルにするには、 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。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show ip igmp snooping 例： Device# 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 6	copy running-config startup-config 例： Device# 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 プロファイルの設定

IGMP プロファイルを作成するには、次の手順を実行します。

このタスクはオプションです。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# 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 3	ip igmp profile profile number 例： Device(config)# ip igmp profile 3	設定するプロファイルに番号を割り当て、IGMP プロファイル コンフィギュレーション モードを開始します。指定できるプロファイル番号の範囲は 1 ~ 4294967295 です。IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用することでプロファイルを作成できます。 <ul style="list-style-type: none"> deny : 一致するアドレスを拒否します。デフォルトで設定されています。 exit : IGMP プロファイル コンフィギュレーション モードを終了します。 no : コマンドを否定するか、または設定をデフォルトに戻します。 permit : 一致するアドレスを許可するように指定します。 range : プロファイルの IP アドレスの範囲を指定します。単一の IP アドレス、または開始アドレスと終了アドレスで指定された IP アドレス範囲を入力できます。

	コマンドまたはアクション	目的
		<p>デフォルトでは、デバイスにはIGMPプロファイルが設定されていません。</p> <p>(注) プロファイルを削除するには、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。</p>
ステップ 4	permit deny 例： Device(config-igmp-profile)# permit	<p>(任意) IP マルチキャストアドレスへのアクセスを許可または拒否するアクションを設定します。アクションを設定しないと、プロファイルのデフォルト設定はアクセス拒否になります。</p>
ステップ 5	range ip multicast address 例： Device(config-igmp-profile)# range 229.9.9.0	<p>アクセスを制御する IP マルチキャストアドレスまたは IP マルチキャストアドレスの範囲を入力します。範囲を入力する場合は、IP マルチキャストアドレスの下限值、スペースを1つ、IP マルチキャストアドレスの上限値を入力します。</p> <p>range コマンドを複数回入力し、複数のアドレスまたはアドレス範囲を入力できます。</p> <p>(注) IP マルチキャストアドレスまたは IP マルチキャストアドレス範囲を削除するには、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。</p>
ステップ 6	end 例： Device(config)# end	<p>特権 EXEC モードに戻ります。</p>
ステップ 7	show ip igmp profile profile number 例： Device# show ip igmp profile 3	<p>プロファイルの設定を確認します。</p>
ステップ 8	show running-config 例：	<p>入力を確認します。</p>

	コマンドまたはアクション	目的
	Device# show running-config	
ステップ 9	copy running-config startup-config 例： Device# 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 プロファイルの適用

IGMP プロファイルで定義されているとおりにアクセスを制御するには、プロファイルを該当するインターフェイスに適用する必要があります。IGMP プロファイルを適用できるのは、レイヤ2アクセスポートだけです。ルーテッドポートやSVIには適用できません。EtherChannelポートグループに所属するポートに、プロファイルを適用することはできません。1つのプロファイルを複数のインターフェイスに適用できますが、1つのインターフェイスに適用できるプロファイルは1つだけです。

スイッチポートにIGMP プロファイルを適用するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# 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 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	物理インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。インターフェイスは、EtherChannelポートグループに所属していないレイヤ2ポートでなければなりません。
ステップ 4	ip igmp filter profile number 例： Device(config-if)# ip igmp filter 321	インターフェイスに指定されたIGMPプロファイルを適用します。指定できる範囲は1～4294967295です。

	コマンドまたはアクション	目的
		(注) 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。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例： Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# 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 グループの最大数の設定

レイヤ2 インターフェイスが加入できる IGMP グループの最大数を設定するには、次の手順を実行します。

始める前に

この制限が適用されるのはレイヤ2 ポートだけです。ルーテッドポートや SVI には IGMP グループの最大数を設定できません。このコマンドは、論理 EtherChannel インターフェイスでも使用できますが、EtherChannel ポート グループに属するポートでは使用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# 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。

	コマンドまたはアクション	目的
ステップ 3	interface interface-id 例 : Device(config)# interface gigabitethernet 1/0/2	設定するインターフェイスを指定して、インターフェイスコンフィギュレーションモードを開始します。インターフェイスは、EtherChannel ポートグループに所属しないレイヤ 2 ポート、または EtherChannel インターフェイスのいずれかにできます。
ステップ 4	ip igmp max-groups number 例 : Device(config-if)# ip igmp max-groups 20	インターフェイスが加入できる IGMP グループの最大数を設定します。指定できる範囲は 0 ~ 4294967294 です。デフォルトでは最大数は設定されません。 (注) グループの最大数に関する制限を削除し、デフォルト設定 (制限なし) に戻すには、 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。
ステップ 5	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config interface interface-id 例 : Device# show running-config interface gigabitethernet1/0/1	入力を確認します。
ステップ 7	copy running-config startup-config 例 : Device# 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 スロットリングアクションの設定

レイヤ2インターフェイスが加入できる IGMP グループの最大数を設定した後、受信した IGMP レポートの新しいグループで、既存のグループを上書きするようにインターフェイスを設定できます。

転送テーブルに最大数のエントリが登録されているときにスロットリングアクションを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# 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 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	設定する物理インターフェイスを指定し、インターフェイスコンフィギュレーション モードを開始します。インターフェイスは、EtherChannel ポートグループに所属しないレイヤ2ポート、または EtherChannel インターフェイスのいずれかにできます。トランク ポートをインターフェイスにすることはできません。
ステップ 4	ip igmp max-groups action {deny replace} 例： Device(config-if)# ip igmp max-groups action 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。 <ul style="list-style-type: none"> deny : レポートを破棄します。このスロットリングアクションを設定すると、すでに転送テーブルに登録されていたエントリは、削除されることはありませんが期限切れになります。エントリが期限切れになり、最大数のエントリが転送テーブルに登録されていると、デバイスは、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。 replace : 既存のグループを、IGMP レポートを受信した新しいグループで上書きします。このスロットリングアクションを設定すると、すでに転送テーブルに登録されていたエントリは削除されます。転送テーブルのエントリが最大数まで達したら、デバイスはランダムに選択した

	コマンドまたはアクション	目的
		<p>エントリを受信した IGMP レポートで上書きします。</p> <p>デバイス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。</p> <p>(注) レポートの廃棄というデフォルトのアクションに戻すには、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。</p>
ステップ 5	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config interface interface-id 例： Device(config)# show running-config interface gigabitethernet 1/0/1	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# 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 スヌーピングのモニタリング

IGMP スヌーピング情報の監視

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

表 5: 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 <i>vlan-id</i>] [detail]	デバイス上のすべての 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、 vlan <i>vlan-id</i> を入力します。指定できる VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
show ip igmp snooping groups [count vlan <i>vlan-id</i>]	デバイス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"> • count : 実エントリの代わりに、指定のコマンドオプションのエントリ総数を表示します。 • vlan-id : VLAN ID の範囲は 1 ~ 1001 および 1006 ~ 4094 です。
show ip igmp snooping mrouter [vlan <i>vlan-id</i>]	ダイナミックに学習され、手動で設定されたマルチキャスト ルータ インターフェイスの情報を表示します。 (注) IGMP スヌーピングを有効にすると、デバイス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。 (オプション) vlan <i>vlan-id</i> を入力すると、特定の VLAN に関する情報が表示されます。
show ip igmp snooping querier [vlan <i>vlan-id</i>] detail	IP アドレスおよび VLAN で受信した最新の IGMP クエリーメッセージの受信ポートに関する情報、VLAN の IGMP スヌーピング クエリアの設定および動作ステータスに関する情報を表示します。

IGMP フィルタリングのモニタリング

IGMP プロファイルの特性を表示したり、デバイス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。

表 6: IGMP フィルタリングの表示コマンド

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デバイス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デバイス上のすべてのインターフェイスの設定を表示します。

IGMP スヌーピングの設定例

例：マルチキャスト ルータへの静的な接続のイネーブル化

次に、マルチキャスト ルータへの静的な接続をイネーブルにする例を示します。

```
Device# configure terminal
Device# ip igmp snooping vlan 200 interface gigabitethernet 1/0/2
Device# end
```

例：グループに加入するホストの静的な設定

次に、ポート上のホストを静的に設定する例を示します。

```
Device# configure terminal
Device# ip igmp snooping vlan 105 static 0100.1212.0000 interface gigabitethernet 1/0/1
Device# end
```

例：IGMP 即時脱退のイネーブル化

次に、VLAN 130 上で IGMP 即時脱退をイネーブルにする例を示します。

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

例：IGMP スヌーピング クエリアの送信元アドレスの設定

次に、IGMP スヌーピング クエリアの送信元アドレスを 10.0.0.64 に設定する例を示します。

例：IGMP スヌーピング クエリアの最大応答時間の設定

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

例：IGMP スヌーピング クエリアの最大応答時間の設定

次の例では、IGMP スヌーピング クエリアの最大応答時間を 25 秒に設定する方法を示します。

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

例：IGMP スヌーピング クエリア タイムアウトの設定

次の例では、IGMP スヌーピング クエリアのタイムアウトを 60 秒に設定する方法を示します。

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

例：IGMP スヌーピング クエリア機能の設定

次に、IGMP スヌーピング クエリア機能をバージョン 2 に設定する例を示します。

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

例：IGMP プロファイルの設定

次に、単一の IP マルチキャストアドレスへのアクセスを許可する IGMP プロファイル 4 を作成して、設定を確認する例を示します。アクションが拒否（デフォルト）である場合は、**show ip igmp profile** の出力には表示されません。

```
Device(config)# ip igmp profile 4
Device(config-igmp-profile)# permit
Device(config-igmp-profile)# range 229.9.9.0
Device(config-igmp-profile)# end
Device# show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

例：IGMP プロファイルの適用

次に、ポートに IGMP プロファイル 4 を適用する例を示します。

```
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# ip igmp filter 4
Device(config-if)# end
```

例：IGMP グループの最大数の設定

次の例では、ポートが加入できる IGMP グループ数を 25 に制限する方法を示します。

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

IGMP スヌーピングの機能履歴と情報

リリース	変更内容
Cisco IOS Release 15.2(7)E3k	この機能が導入されました。

