CHAPTER 22

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）スヌーピングを応用した Multicast VLAN Registration（MVR; マルチキャスト VLAN レジストレーション）など、Cisco ME 3400E イーサネット アクセス スイッチ上で 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。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースのスイッチ 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。

（注） IGMP スヌーピングや MVR などの機能を利用して IP マルチキャスト グループ アドレスを管理したり、スタティック IP アドレスを使用したりできます。

IGMP スヌーピングの概要

レイヤ 2 スイッチでは、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ダイナミックに設定することにより、マルチキャスト トラフィックのフラッディングを抑制できるよう、マルチキャスト トラフィックが IP マルチキャスト デバイスに対応付けられたインターフェイスにだけ転送されます。IGMP スヌーピングでは、その名前が示すとおり、LAN スイッチによってホストとルータの間の IGMP 伝送がスヌーピングされ、マルチキャスト グループとメンバー ポートの追跡が行われます。スイッチは、特定のマルチキャスト グループのホストから IGMP レポートを受け取ると、転送テーブル

エントリにホストのポート番号を追加します。また、ホストから IGMP Leave Group メッセージを受け取ると、テーブル エントリからホスト ポートを削除します。さらに、マルチキャスト クライアントから IGMP メンバシップ レポートを受信しない場合、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 ルータは定期的に一般クエリーをすべての VLAN に送信します。このマルチキャスト トラフィックを必要とするすべてのホストは、Join 要求を送信し、これによって転送テーブルのエントリに追加されます。IGMP Join 要求の送信元である各グループについて、IGMP スヌーピング IP マルチキャスト転送テーブルの VLAN ごとに 1 つのエントリが作成されます。

スイッチは、MAC（メディア アクセス制御）アドレスベース グループでなく、IP マルチキャスト グループベースのブリッジングをサポートします。マルチキャスト MAC アドレスベース グループが設定されている場合に、設定中の IP アドレスが設定済みの MAC アドレス、または予約済みマルチキャスト MAC アドレス（224.0.0.xxx の範囲）に変換されると（エイリアスが作成されると）、コマンド エラーになります。スイッチでは IP マルチキャスト グループが使用されるため、アドレスのエイリアスに関する問題は発生しません。

IGMP スヌーピングを通じて学習する 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 コマンドを使用すれば、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。マルチキャスト グループ アドレスのグループ メンバシップをスタティックに設定すると、その設定は IGMP スヌーピングによるどの自動操作よりも優先されます。マルチキャスト グループ メンバシップのリストは、ユーザ側で定義した設定と IGMP スヌーピングにより学習された設定の両方で構成されます。

マルチキャスト トラフィックはルーティングの必要がないので、マルチキャスト インターフェイスを持たないサブネット内でも IGMP スヌーピングがサポートされるように IGMP スヌーピング クエリアを設定できます。IGMP スヌーピング クエリアの詳細については、「IGMP スヌーピング クエリアの設定」（P.22-13）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 スヌーピングにより学習されたマルチキャスト グループは削除されます。

ここでは、IGMP スヌーピングの特性について説明します。

IGMP バージョン

このスイッチでは、IGMP バージョン 1、IGMP バージョン 2、および IGMP バージョン 3 がサポートされています。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、IGMP スヌーピングがイネーブルになっている IGMPv2 スイッチでは、ホストから IGMPv3 レポートを受信した場合、IGMPv3 レポートをマルチキャスト ルータに転送できます。

（注）　スイッチは、宛先マルチキャスト MAC アドレスだけに基づいた IGMPv3 スヌーピングをサポートしています。送信元 MAC アドレスまたはプロキシ レポートに基づくスヌーピングは、サポートしていません。

IGMPv3 スイッチは、IGMPv1 スイッチおよび IGMPv2 スイッチでのスヌーピング機能および IGMPv3 メンバシップ レポート メッセージのサポートを含む、Basic IGMPv3 Snooping Support（BISS）をサポートします。BISS が適用されることで、ネットワークに IGMPv3 ホストが含まれる場合、マルチキャスト トラフィックのフラッディングが抑制されます。また、IGMPv2 ホストまたは IGMPv1 ホストの IGMP スヌーピング機能とほぼ同じポート セットへトラフィックが制限されます。

（注）　IGMP フィルタリングまたは MVR を実行しているスイッチでは、IGMPv3 の Join メッセージおよび Leave メッセージはサポートされません。

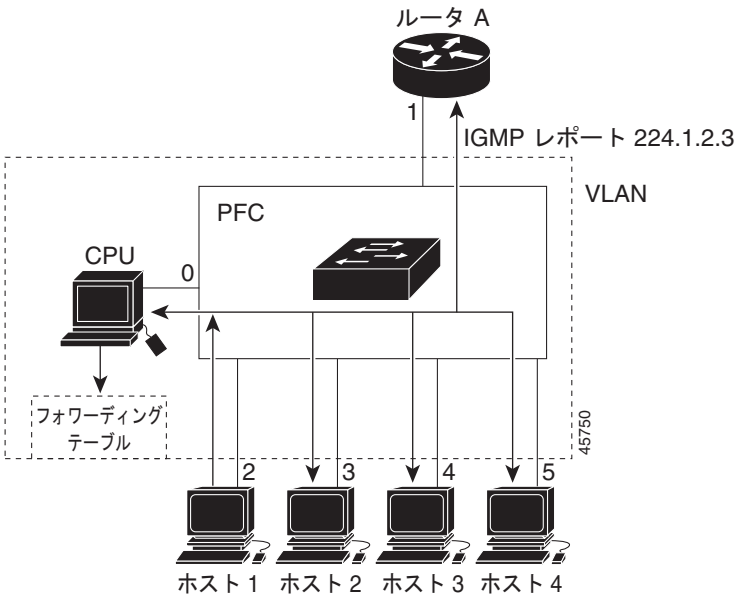
IGMPv3 スイッチは、Source Specific Multicast（SSM）機能を実行しているデバイスとの間でメッセージの送受信を行うことができます。IGMPv3 および IGMP を含む SSM の詳細については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtssm5t.htm

マルチキャスト グループへの参加

スイッチに接続されたホストが IP マルチキャスト グループに参加する場合、このホストが IGMP バージョン 2 クライアントであれば、参加する IGMP マルチキャスト グループを指定して、非請求の IGMP Join メッセージを送信します。また、スイッチはルータから一般クエリーを受信すると、VLAN 内のすべてのポートにそのクエリーを転送します。マルチキャスト グループに参加しようとする IGMP バージョン 1 またはバージョン 2 のホストは、スイッチに Join メッセージを送信して応答します。グループのマルチキャスト転送テーブル エントリがまだ作成されていない場合は、スイッチの CPU により作成されます。また CPU では、Join メッセージを受信したインターフェイスの転送テーブル エントリへの追加も行われます。そのインターフェイスに関連付けられているホストは、マルチキャスト グループのマルチキャスト トラフィックを受信します。図 22-1 を参照してください。

図 22-1　最初の IGMP Join メッセージ



ルータ A からスイッチに送信された一般クエリーは、さらにスイッチから同じ 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 に参加し、このグループに IGMP メンバシップ レポート（IGMP Join メッセージ）をマルチキャストしようとします。スイッチの CPU は、IGMP レポート内の情報を使用して、ホスト 1 およびルータに接続されたポート番号を含む転送テーブル エントリを設定します（表 22-1 を参照）。

表 22-1　IGMP スヌーピング転送テーブル

宛先アドレス	パケット タイプ	Ports
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 グループの他のパケットと区別できます。スイッチング エンジンでは、テーブル内の情報に従って、IGMP パケットではない 224.1.2.3 マルチキャスト IP アドレス宛のフレームが、ルータおよびグループに参加しているホストに送信されます。

別のホスト（たとえばホスト 4）が同じグループに非請求の IGMP Join メッセージを送信する場合（図 22-2 を参照）、CPU はそのメッセージを受信し、転送テーブルにホスト 4 のポート番号を追加します（表 22-2 を参照）。ただし、転送テーブルにより指定される IGMP メッセージの送信先は CPU に限られるため、スイッチの他のポートにメッセージがフラッディングされることはありません。既知のマルチキャスト トラフィックはグループには転送されますが、CPU には転送されません。

図 22-2　　2 番めのホストのマルチキャスト グループへの参加

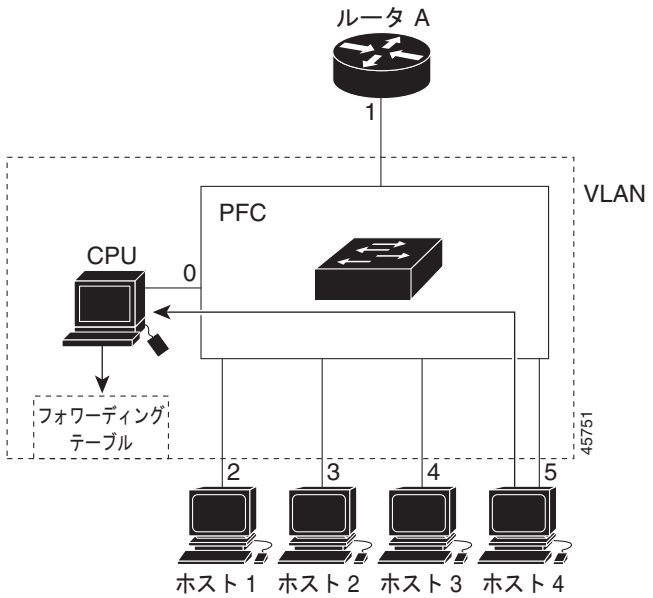


表 22-2　　アップデートされた IGMP スヌーピング転送テーブル

宛先アドレス	パケット タイプ	Ports
224.1.2.3	IGMP	1, 2, 5

マルチキャスト対応ルータ ポートは、各レイヤ 2 マルチキャスト エントリごとに転送テーブルに追加されます。スイッチは、次のいずれか 1 つの方式でそれらのポートを学習します。

- IGMP クエリーおよび Protocol Independent Multicast（PIM）パケットのスヌーピング
- **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

マルチキャスト グループからの脱退

ルータは定期的にマルチキャスト一般クエリーを送信し、スイッチはこのクエリーを VLAN のすべてのポートを通じて転送します。このクエリーを必要とするホストがこれに応答します。VLAN にマルチキャスト トラフィックを必要とするホストが少なくとも 1 つ存在すれば、ルータは引き続き VLAN にマルチキャスト トラフィックを転送します。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ている、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ているホストに限られます。

ホストは、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 メッセージを送信して脱退することもできます。スイッチは、ホストから Leave メッセージを受信すると、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が、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かどうかを学習します。次に、その MAC グループの転送テーブルをアップデートして、そのグループのマルチキャスト トラフィックを必要とするホストだけが転送テーブルにリストされるようにします。ルータは、VLAN からのレポートを受信しなかった場合は、IGMP キャッシュからその VLAN のグループを削除します。

即時脱退

即時脱退をサポートしているのは、IGMP バージョン 2 のホストだけです。

IGMP スヌーピングの即時脱退処理機能を使用すると、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、転送テーブルから 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 ツリーから削除されます。即時脱退処理によって、複数のマルチキャスト グループを同時に使用する場合でも、スイッチド ネットワーク上のすべてのホストに対して最適な帯域幅管理を行えます。

（注）　即時脱退処理機能は、各ポートに 1 つのホストしか接続されていない VLAN 上に限って使用してください。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廃棄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.22-10）を参照してください。

IGMP の設定可能な Leave タイマー

ホストが現在も特定のマルチキャスト グループを必要としているかどうかを判別するため、スイッチがグループ固有のクエリーを送信してから待機する時間を設定できます。IGMP 脱退応答時間は、100 ～ 5000 ミリ秒の間で設定できます。このタイマーは、グローバルに設定できるほか、VLAN ごとに設定することもできます。グローバル設定は、脱退時間の VLAN 設定によって上書きされます。

設定手順については、「IGMP Leave タイマーの設定」（P.22-10）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 ルータ抑制がイネーブル（デフォルト）である場合、スイッチは最初の IGMP レポートをグループのすべてのポートからすべてのマルチキャスト ルータに送信します。スイッチは、グループの残りの IGMP レポートをマルチキャスト ルータに送信しません。この機能により、マルチキャスト デバイスにレポートが重複して送信されることを防ぎます。

マルチキャスト ルータ クエリーに IGMPv1 および IGMPv2 レポートに対する要求のみ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 ルータに送信します。

マルチキャスト ルータ クエリーに IGMPv3 レポートの要求も含まれる場合は、スイッチはグループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャスト デバイスに転送します。

IGMP レポート抑制がディセーブルの場合は、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。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.22-15）を参照してください。

IGMP スヌーピングの設定

IGMP スヌーピングを使用すると、スイッチは、IGMP パケットを検証できるほか、その内容に基づいて転送に関する判断を行えます。

IGMP スヌーピングのデフォルト設定

表 22-3 は、IGMP スヌーピングのデフォルト設定をまとめたものです。

表 22-3　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
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[1] フラッド クエリー カウント	2
TCN クエリー請求	ディセーブル
IGMP スヌーピング クエリア	ディセーブル
IGMP レポート抑制	イネーブル

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

IGMP スヌーピングのイネーブル化またはディセーブル化

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化されています。グローバルにイネーブル化またはディセーブル化されている IGMP スヌーピングは、すべての既存 VLAN インターフェイスでもイネーブル化またはディセーブル化されます。IGMP スヌーピングは、すべての VLAN においてデフォルトでイネーブルになっていますが、VLAN 単位でイネーブルおよびディセーブルに設定することもできます。

グローバル IGMP スヌーピングは、VLAN IGMP スヌーピングに優先します。グローバル スヌーピングがディセーブルになっている場合、VLAN スヌーピングは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は、VLAN スヌーピングをイネーブルまたはディセーブルのどちらにも設定できます。

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化するには、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**	すべての既存 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化します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

すべての VLAN インターフェイスで IGMP スヌーピングをグローバルにディセーブルにする場合は、**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 インターフェイスで IGMP スヌーピングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping vlan** *vlan-id*	VLAN インターフェイスで 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、事前に IGMP スヌーピングをグローバルにイネーブル化する必要があります。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN インターフェイスで 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 番号について **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。

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（マルチキャスト ルータにスタティック接続を追加する）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	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id*	マルチキャスト ルータの VLAN ID とインターフェイスをマルチキャスト ルータに指定します。 • 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 ～ 48 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping mrouter** [**vlan** *vlan-id*]	VLAN インターフェイスで IGMP スヌーピングがイネーブルになっていることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

次に、マルチキャスト ルータへのスタティック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
```

グループに参加するホストのスタティックな設定

ホストまたはレイヤ 2 ポートは通常、マルチキャスト グループにダイナミックに参加しますが、インターフェイスで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	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping vlan** *vlan-id* **static** *ip_address* **interface** *interface-id*	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。 • *vlan-id* には、マルチキャスト グループの VLAN ID を指定します。指定できる範囲は 1 ～ 1001 または 1006 ～ 4094 です。 • *ip-address* には、グループ IP アドレスを指定します。 • *interface-id* にはメンバー ポートを指定します。物理インターフェイスまたはポート チャネル（1 ～ 48）を指定できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show ip igmp snooping groups**	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	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

マルチキャスト グループからレイヤ 2 ポートを削除する場合は、**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 gigabitethernet0/1
Switch(config)# end
```

IGMP 即時脱退のイネーブル化

IGMP 即時脱退をイネーブルにすると、スイッチは、ポート上で IGMP バージョン 2 Leave メッセージを検出した時点で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 の各ポートにレシーバーが 1 つ存在する場合だけです。

（注）　即時脱退は、IGMP バージョン 2 のホストに限ってサポートされています。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping vlan** *vlan-id* **immediate-leave**	VLAN インターフェイス上で IGMP 即時脱退をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping vlan** *vlan-id*	VLAN インターフェイス上で即時脱退がイネーブルになっていることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VLAN 上で IGMP 即時脱退をディセーブルにする場合は、**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ときは、次の注意事項に従ってください。

- 脱退時間は、グローバルに設定することも、VLAN ごとに設定することもできます。
- VLAN で脱退時間を設定すると、グローバル設定は無効となります。
- デフォルトの脱退時間は 1000 ミリ秒です。

- IGMP の設定可能な脱退時間は、IGMP バージョン 2 を実行しているホストに限りサポートされています。
- ネットワークの実際の脱退遅延時間は通常、設定した脱退時間になります。ただし、リアルタイムの CPU 負荷条件、ネットワーク遅延、インターフェイスを介して送信されたトラフィック量によっては、実際の脱退時間と設定した脱退時間に若干の誤差が生じることがあります。

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	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping last-member-query-interval** *time*	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	**ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *time*	（任意）IGMP 脱退時間を VLAN インターフェイス上で設定します。指定できる範囲は 100 ～ 32768 ミリ秒です。 **（注）** VLAN で脱退時間を設定すると、グローバルに設定したタイマーは無効となります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip igmp snooping**	（任意）設定した IGMP 脱退時間を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP Leave タイマーをグローバルにリセットしてデフォルト設定に戻す場合は、**no ip igmp snooping last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。

設定した IGMP 脱退時間設定を特定の VLAN から削除する場合は、**no ip igmp snooping vlan** *vlan-id* **last-member-query-interval** グローバル コンフィギュレーション コマンドを使用します。

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 トラフィックの制御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 フラッディング時間の制御」（P.22-11）
- 「フラッディング モードからの回復」（P.22-12）
- 「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.22-13）

TCN イベント後のマルチキャスト フラッディング時間の制御

ip igmp snooping tcn flood query count グローバル コンフィギュレーション コマンドを使用すると、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される時間を制御できます。このコマンドにより、TCN イベント後にマルチキャスト データ トラフィックが フラッディングされる間の一般クエリー数を設定します。TCN イベントが発生するのは、クライアントの位置が変更され、レシーバーの位置は同じポートのままブロッキングからフォワーディングに変更された場合や、ポートが Leave メッセージを送信せずにダウンした場合などです。

ip igmp snooping tcn flood query count コマンドを使用して TCN フラッディング クエリー数を 1 に設定した場合、フラッディングは一般クエリーを 1 つ受信した時点で停止します。カウントを 7 に設定すると、TCN イベントによるマルチキャスト トラフィックのフラッディングは、7 つの一般的クエリーを受信するまで継続します。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 クエリー数を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping tcn flood query count** *count*	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。デフォルトのフラッディング クエリー数は 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）コンフィギュレーション ファイルに設定を保存します。

フラッディング クエリー数をデフォルト値に戻す場合は、**no ip igmp snooping tcn flood query count** グローバル コンフィギュレーション コマンドを使用します。

フラッディング モードからの回復

トポロジ変更が発生すると、スパニング ツリーのルートはグループ マルチキャスト アドレス（0.0.0.0.）を使用して特別な IGMP Leave メッセージ（グローバル Leave とも呼ぶ）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している場合、スイッチはスパニング ツリーのルートであるかどうかに関係なく、グローバル Leave メッセージを送信します。ルータはこの特別な Leave メッセージを受信すると、ただちに一般クエリーを送信します。これにより、TCN イベント中にフラッディング モードからの回復処理が迅速に行われます。このコンフィギュレーション コマンドがイネーブルかディセーブルかに関わらず、スイッチがスパニング ツリーのルートである場合は常に、Leave メッセージが送信されます。デフォルトでは、クエリー請求はディセーブルに設定されています。

スイッチがスパニング ツリーのルートであるかどうかに関係なく、スイッチによるグローバル Leave メッセージの送信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 脱退メッセージ（グローバル脱退）を送信します。デフォルトでは、クエリー請求はディセーブルに設定されています。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping**	TCN 設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

クエリー請求をデフォルトに戻すときは、**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 グループに参加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。**ip igmp snooping tcn flood** インターフェイス コンフィギュレーション コマンドを使用すると、この動作を制御できます。

インターフェイスのマルチキャスト 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 shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）と Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）はディセーブルに、Network Node Interface（NNI; ネットワーク ノード インターフェイス）はイネーブルに設定されています。
ステップ 4	**no ip igmp snooping tcn flood**	スパニング ツリー TCN イベント中のマルチキャスト 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、インターフェイスのマルチキャスト フラッディングはイネーブルに設定されています。
ステップ 5	**exit**	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp snooping**	TCN 設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスでマルチキャスト 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ときは、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。イネーブルの場合、IGMP スヌーピング クエリアは IP アドレスをクエリー送信元アドレスとして使用します。
- VLAN インターフェイスに 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 クエリア用に設定されているグローバル 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は、IGMP スヌーピング クエリアは（存在する場合）VLAN Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）IP アドレスの使用を試みます。SVI IP アドレスがない場合は、スイッチはスイッチに設定されている使用可能な最初の IP アドレスを使用します。使用可能な最初の 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、スイッチで使用可能な IP アドレスが見つからなければ、IGMP 一般クエリーの生成を行いません。
- IGMP スヌーピング クエリアは、IGMP バージョン 1 および 2 をサポートしています。

- 管理上のイネーブルの場合、IGMP スヌーピング クエリアはネットワーク内でマルチキャスト ルータを検出すると非クエリア ステートに移行します。
- 管理上のイネーブルの場合、IGMP スヌーピング クエリアは次の条件下にあるときは操作上のディセーブル ステートに移行します。
  - IGMP スヌーピングが VLAN でディセーブルに設定されている。
  - PIM が、対応する VLAN の SVI でイネーブルに設定されている。

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、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip igmp snooping querier**	IGMP スヌーピング クエリアをイネーブルにします。
ステップ 3	**ip igmp snooping querier** *ip_address*	（任意）IGMP スヌーピング クエリアの IP アドレスを指定します。IP アドレスを指定しない場合、クエリアは IGMP クエリアに設定されたグローバル IP アドレスを使用します。 **（注）** スイッチ上で 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 一般クエリーを生成しません。
ステップ 4	**ip igmp snooping querier query-interval** *interval-count*	（任意）IGMP クエリアの間隔を設定します。指定できる範囲は 1 ～ 18000 秒です。
ステップ 5	**ip igmp snooping querier tcn query** [**count** *count* | **interval** *interval*]	（任意）TCN クエリアの間隔を設定します。指定できる数の範囲は 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	**ip igmp snooping querier timer expiry** *timeout*	（任意）IGMP クエリアの期限が切れ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	**ip igmp snooping querier version** *version*	（任意）クエリア機能が使用する IGMP バージョン番号を選択します。選択できる番号は 1 または 2 です。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show ip igmp snooping vlan** *vlan-id*	（任意）VLAN インターフェイスで 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	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

```
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、デフォルトではイネーブルに設定されています。この機能がイネーブルになると、スイッチはマルチキャスト ルータ クエリーごとに IGMP レポートを 1 つだけ転送します。レポート抑制がディセーブルの場合は、すべての IGMP レポートがマルチキャスト ルータに転送されます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no ip igmp snooping report-suppression**	IGMP レポート抑制をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show ip igmp snooping**	IGMP レポート抑制がディセーブルであることを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

IGMP レポート抑制を再びイネーブルにする場合は、**ip igmp snooping report-suppression** グローバル コンフィギュレーション コマンドを使用します。

IGMP スヌーピング情報の表示

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。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 22-4 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 22-4　IGMP スヌーピング情報を表示するためのコマンド

コマンド	目的
show ip igmp snooping [**vlan** *vlan-id*]	スイッチのすべての VLAN または指定された VLAN のスヌーピング設定情報を表示します。 （任意）単一の VLAN に関する情報を表示するには、**vlan** *vlan-id* を使用します。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。
show ip igmp snooping groups [**count** |**dynamic** [**count**] | **user** [**count**]]	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。 • **count**：実際のエントリではなく、指定されたコマンド オプションに対するエントリの総数を表示します。 • **dynamic**：IGMP スヌーピングを通して学習されたエントリを表示します。 • **user**：ユーザが設定したマルチキャスト エントリに限って表示します。
show ip igmp snooping groups vlan *vlan-id* [*ip_address* | **count** | **dynamic** [**count**] | **user** [**count**]]	マルチキャスト VLAN または VLAN の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。 • *vlan-id*：VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。 • **count**：実際のエントリではなく、指定されたコマンド オプションに対するエントリの総数を表示します。 • **dynamic**：IGMP スヌーピングを通して学習されたエントリを表示します。 • *ip_address*：指定されたグループ IP アドレスを持つマルチキャスト グループの特性を表示します。 • **user**：ユーザが設定したマルチキャスト エントリに限って表示します。
show ip igmp snooping mrouter [**vlan** *vlan-id*]	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 インターフェイスに関する情報を表示します。 **（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 ルータの接続先であるインターフェイスを自動的に学習します。これらはダイナミックに学習されるインターフェイスです。 （任意）単一の VLAN に関する情報を表示するには、**vlan** *vlan-id* を使用します。
show ip igmp snooping querier [**vlan** *vlan-id*]	VLAN 内で直前に受信した IGMP クエリー メッセージの IP アドレスおよび着信ポートに関する情報を表示します。 （任意）単一の VLAN に関する情報を表示するには、**vlan** *vlan-id* を使用します。
show ip igmp snooping querier [**vlan** *vlan-id*] **detail**	VLAN 内で直前に受信した IGMP クエリー メッセージの IP アドレスおよび着信ポートに関する情報と、VLAN 内の IGMP スヌーピング クエリアの設定および動作ステートを表示します。

これらの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、このリリースのコマンド リファレンスを参照してください。

MVR の概要

MVR は、イーサネット リングベースのサービス プロバイダー ネットワークで、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 により、ポート上の参加者は、ネットワーク全般のマルチキャスト VLAN のマルチキャスト ストリームに対して参加または脱退を設定できます。これにより、各参加者が別々の VLAN に属しながら、ネットワーク上で 1 つのマルチキャスト VLAN を共有できます。MVR を使用すると、マルチキャスト VLAN 内でマルチキャスト ストリームを継続的に送信しながら、帯域幅およびセキュリティを確保するために、参加者 VLAN からストリームを隔離できます。

MVR では、参加者ポートが、IGMP の Join メッセージまたは Leave メッセージを送信することによって、マルチキャスト ストリームに参加またはマルチキャスト ストリームから脱退（Join または Leave）することを前提にしています。これらのメッセージは、イーサネット接続の IGMP バージョン 2 互換ホストから発信できます。MVR は IGMP スヌーピングの基本メカニズムで動作しますが、2 つの機能は相互に独立して動作します。それぞれ、他方の動作に影響を与えることなく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 がともにイネーブルの場合、MVR は、MVR 上で設定されたマルチキャスト グループからの Join メッセージおよび Leave メッセージに対してだけ対応します。それ以外のマルチキャスト グループからの Join メッセージおよび 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 ストリームおよびスイッチ転送テーブル上の関連 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ます。また、レシーバーが送信元とは別の VLAN に属する場合でも、参加者をマルチキャスト ストリームのレシーバーとしてテーブルに追加したりテーブルから削除したりするように転送テーブルを書き換えます。この転送動作により、さまざまな VLAN 間で伝送されるトラフィックが選択的に許可されます。

スイッチの MVR 動作は、互換モードまたはダイナミック モードに設定できます。

- 互換モードの場合、MVR ホストが受信したマルチキャスト データは、ポートの MVR ホスト メンバシップに関係なく、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 スタティック設定を使用して、MVR ホストが参加したレシーバー ポートにだけ転送されます。また、MVR ホストから受信した IGMP レポートは、スイッチに設定された MVP 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 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 スタティック設定を使用して、MVR ホストが参加した MVR データ ポートおよびクライアント ポートからだけ転送されます。MVR ホストから受信した IGMP レポートは、スイッチ内のすべての MVR データ ポートからも転送されます。これにより、スイッチが互換モードで動作している場合と異なり、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。

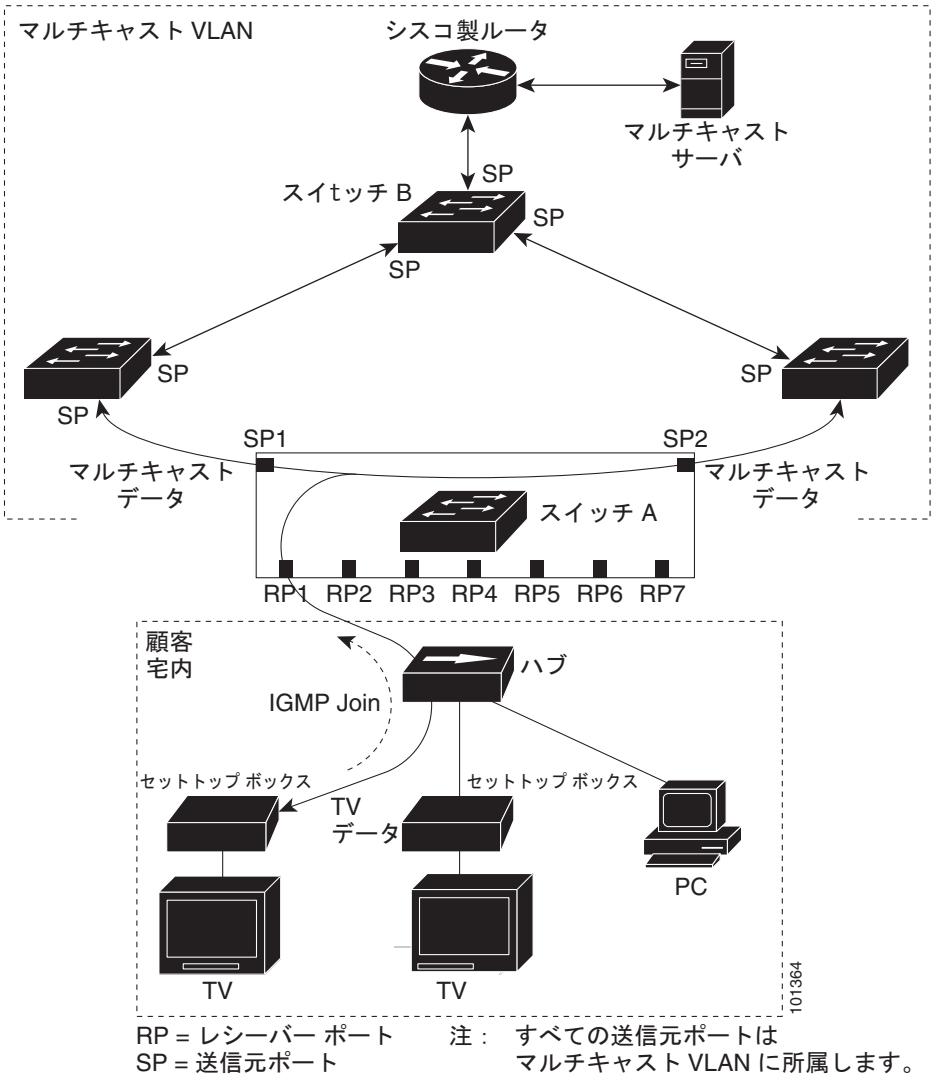
MVR に参加するのは、レイヤ 2 ポートだけです。ポートは MVR レシーバー ポートとして設定する必要があります。各スイッチでサポートされる MVR マルチキャスト VLAN は 1 つだけです。

マルチキャスト TV アプリケーションでの MVR の使用方法

マルチキャスト TV アプリケーションでは、PC またはセットトップ ボックスを装備した TV で、マルチキャスト ストリームを受信できます。MVR のレシーバー ポートとして設定されたスイッチ ポートである各参加者ポートには、セットトップ ボックスまたは PC を複数接続できます。図 22-3 は設定例です。セットトップ ボックスまたは PC には、DHCP によって IP アドレスが割り当てられます。参加者がチャネルを選択すると、セットトップ ボックスまたは PC では、対応するマルチキャストに参加するために、スイッチ A に対して IGMP レポートが送信されます。IGMP レポートが設定済み IP マルチキャスト グループ アドレスの 1 つに一致した場合、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

にそのマルチキャスト ストリームを転送する宛先として、このレシーバー ポートと VLAN をアドレス テーブルに追加します。マルチキャスト VLAN との間でマルチキャスト データを送受信するアップリンク ポートを、MVR 送信元ポートと呼びます。

図 22-3　MVR の例



参加者がチャネルを変更するか、TV をオフにすると、セットトップ ボックスからマルチキャスト ストリームの 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 を介して、MAC ベースの一般クエリーを送信します。このグループに参加している他のセットトップ ボックスが VLAN 内に存在する場合、そのセットトップ ボックスはクエリーで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。応答を受信しない場合、CPU はこのグループの転送宛先からレシーバー ポートを除外します。

即時脱退機能がイネーブルになっていない場合、スイッチはレシーバー ポートの参加者から IGMP Leave メッセージを受信すると、そのポートに IGMP クエリーを送信して IGMP グループ メンバシップ レポートを待ちます。設定された時間内にレポートが届かないと、レシーバー ポートがマルチキャスト グループ メンバシップから削除されます。即時脱退機能がイネーブルになっている場合、IGMP Leave メッセージを受信したレシーバー ポートからは IGMP クエリーは送信されません。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 ポートに限ってイネーブルにしてください。

MVR では、各 VLAN に属する複数の参加者に対して TV チャネルのマルチキャスト トラフィックを重複して送信する必要がありません。すべてのチャネルに対するマルチキャスト トラフィックが、VLAN トランクで一度に送信されます（マルチキャスト VLAN に限る）。IGMP の Leave メッセージおよび Join メッセージは、参加者ポートが割り当てられている VLAN 内で送信されます。これらのメッセージにより、レイヤ 3 デバイス（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 ストリームがダイナミックに登録されます。アクセス レイヤ スイッチ（スイッチ A）は、マルチキャスト VLAN から別の VLAN 上の参加者ポートにトラフィックが転送されるように転送動作を変更し、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す。スイッチ A の CPU は、レシーバー ポートからの IGMP の Join メッセージおよび Leave メッセージをすべて取り込み、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 に転送する必要があります。

MVR の設定

MVR のデフォルト設定

表 22-5 は、MVR のデフォルト設定をまとめたものです。

表 22-5　MVR のデフォルト設定

機能	デフォルト設定
MVR	グローバルおよびインターフェイス単位でディセーブル
マルチキャスト アドレス	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）のデフォルト	レシーバーおよび送信元のどちらのポートでもない
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

- スイッチのレシーバー ポートはそれぞれ別々の VLAN に属していてもかまいませんが、マルチキャスト VLAN には属することができません。
- レシーバー ポートとしては、トランク ポートまたはアクセス ポートを設定できます。
- MVR モードが互換に設定されている（デフォルト）場合、設定できる MVR グループの最大数は 512 です。
- MVR モードがダイナミックに設定されている場合、各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）の最大数は 2000 です。同時にアクティブにできるマルチキャスト ストリームの最大数（受信できる TV チャネルの最大数）は 512 です。この上限に達すると、「*ハードウェアで規定されたグループ数の上限に達しました*」という内容のメッセージが生成されます。ただし、ポート上に IGMP Join が存在する場合、または **mvr vlan** *vlan-id* **group** *ip-address* 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ポートがグループに参加するよう設定した場合は、ハードウェア エントリが発生します。
- 各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（受信できる TV チャネルの最大数）は 512 です。
- 送信元 VLAN で受信されレシーバー ポートから送信される MVR マルチキャスト データの Time To Live（TTL; 存続可能時間）は、スイッチを通過するたびに値が 1 ずつ減少します。
- スイッチの MVR では、MAC マルチキャスト アドレスではなく IP マルチキャスト アドレスが使用されるため、スイッチ上ではエイリアスが設定された 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と、MVR をイネーブルにする操作が取り消され、エラーメッセージが表示されます。
- MVR はスイッチで IGMP スヌーピングと共存できます。
- MVR レシーバー ポートで受信された MVR データは、MVR 送信元ポートには転送されません。
- MVR では、IGMPv3 メッセージはサポートされていません。
- Cisco IOS リリース 12.2(52)SE を使用するときは、**mvr ringmode flood** グローバル コンフィギュレーション コマンドを入力することで、メンバーとして検出されたポートにリング トポロジにおけるデータ フォワーディングを制限し、マルチキャスト ルータ ポートへのフォワーディングを排除できます。これにより、MVR マルチキャスト トラフィックの転送方向とユニキャスト トラフィックの転送方向が逆の場合でも、リング環境でユニキャスト トラフィックが廃棄されるのを回避できます。

MVR グローバル パラメータの設定

デフォルト設定を使用する場合には、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値を変更する場合（MVR VLAN を除く）は、先に MVR をイネーブルにする必要があります。

（注）　この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド 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	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mvr**	スイッチ上で MVR をイネーブルに設定します。
ステップ 3	**mvr group** *ip-address* [*count*]	スイッチ上に IP マルチキャスト アドレスを設定します。または、*count* パラメータを使用して、連続した MVR グループ アドレスを設定します。count に指定できる値の範囲は 1 ～ 2000 です。ただし、MVR モードが互換に設定されている場合、スイッチ上に設定できる連続した MVR グループ アドレスの最大数は 512 です。モードがダイナミックに設定されている場合、作成できる MVR グループの最大数は 2000 です。デフォルトは 1 です。 このアドレス宛のマルチキャスト データは、スイッチ上のすべての送信元ポート、およびこのマルチキャスト アドレス上のデータを受信するように設定されている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 TV チャネルに対応付けられます。
ステップ 4	**mvr querytime** *value*	（任意）マルチキャスト グループ メンバシップからレシーバー ポートを削除するまでに、そのレシーバー ポートで IGMP レポート メンバシップを待機する最大待機時間を指定します。値は、1/10 秒単位で指定します。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	**mvr vlan** *vlan-id*	（任意）マルチキャスト データを受信する VLAN を指定します。すべての送信元ポートはこの VLAN に属する必要があります。指定できる VLAN ID の範囲は 1 ～ 1001 および 1006 ～ 4094 です。デフォルトは VLAN 1 です。
ステップ 6	**mvr mode** {**dynamic** | **compatible**}	（任意）MVR の動作モードを指定します。 • **dynamic**：送信元ポートでのダイナミック MVR メンバシップを使用可能にします。MVR グループの最大数を 2000 に設定する場合は、モードを **dynamic**（ダイナミック）に設定する必要があります。 • **compatible**：Catalyst 3500 XL スイッチおよび Catalyst 2900 XL スイッチを使用できるようになり、送信元ポートでは IGMP ダイナミック Join が使用できなくなります。 デフォルトのモードは **compatible**（互換）です。
ステップ 7	**mvr ringmode flood**	（任意）アクセス リングに対する MVR リングモード フラッディングをイネーブルにします。このコマンドを入力すると、ユニキャスト トラフィックが廃棄されないよう、リング環境内の出力ポートでトラフィック フローを制御できます。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show mvr** or **show mvr members**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スイッチをデフォルト設定に戻す場合は、**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。

次に示すのは、MVR をイネーブルにし MVR グループ アドレスを設定した上で、クエリー時間を 1 秒（10×1/10）に、MVR マルチキャスト VLAN を VLAN 22 に、MVR モードをダイナミックにそれぞれ設定した例です。

```
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。

アクセス ポート上での MVR の設定

（注）　アクセス ポートおよびトランク ポートの詳細については、第 10 章「インターフェイスの設定」を参照してください。

アクセス ポート上にレイヤ 2 MVR インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mvr**	スイッチ上で MVR をイネーブルに設定します。
ステップ 3	**interface** *interface-id*	設定するレイヤ 2 ポートを指定し、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	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 5	**mvr type** {**source** | **receiver**}	MVR ポートを次のいずれかに設定します。 • **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。参加者は、送信元ポートに直接接続できません。スイッチ上の送信元ポートはすべて 1 つのマルチキャスト VLAN に属します。 • **receiver**：ポートが参加者ポートで、マルチキャスト データの受信だけを行う場合には、そのポートをレシーバー ポートとして設定します。このポートでデータを受信するためには、スタティックな設定、または IGMP の Join メッセージおよび Leave メッセージによりこのポートがマルチキャスト グループのメンバーになる必要があります。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。 デフォルト設定は非 MVR ポートです。非 MVR ポートに MVR 特性で設定しようとすると、操作は無効になります。

	コマンド	目的
ステップ 6	**mvr vlan** *vlan-id* **group** [*ip-address*]	（任意）マルチキャスト VLAN および IP マルチキャスト アドレスに送信されたマルチキャスト トラフィックを受信するように、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グループ メンバーのままです。 **（注）** 互換モードでは、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。 レシーバー ポートは、IGMP の Join メッセージおよび Leave メッセージによって、マルチキャスト グループにダイナミックに参加することもできます。
ステップ 7	**mvr immediate**	（任意）ポート上の MVR の即時脱退機能をイネーブルにします。 **（注）** このコマンドはレシーバー ポートにだけ適用されます。この機能は単一の受信デバイスが接続されているレシーバー ポート上に限りイネーブルにしてください。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show mvr** **show mvr interface** または **show mvr members**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスをデフォルト設定に戻す場合は、**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たうえで、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その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、結果を確認する方法を示します。

```
Switch(config)# mvr
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr type receiver
Switch(config-if)# mvr vlan 22 group 228.1.23.4
Switch(config-if)# mvr immediate
Switch(config)# end
Switch# show mvr interface
Port    Type            Mode            VLAN    Status          Immediate Leave
----    ----            ----            ----    -------         ---------------
Gia0/2  RECEIVER        Trunk           201     ACTIVE/DOWN     DISABLED
```

トランク ポート上での MVR の設定

トランク ポートを MVR レシーバー ポートとして設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mvr**	スイッチ上で MVR をイネーブルに設定します。

	コマンド	目的
ステップ 3	**interface** *interface-id*	設定するレイヤ 2 ポートを入力し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport mode trunk**	トランキング モードを無条件に TRUNK に設定します。 **（注）** トランク ポートを MVR レシーバー ポートとして設定する場合、送信元ポートは NNI として設定し、MVR トランク レシーバー ポートは UNI または ENI として設定することを推奨します。
ステップ 5	**mvr type receiver**	トランク ポートが MVR レシーバー ポートとして使用されるよう指定します。
ステップ 6	**mvr vlan** ***source****-vlan-id* **receiver vlan** *receiver-vlan-id*	MVR VLAN から受信した MVR トラフィックが、レシーバー VLAN により認識されたトランク上の VLAN に配信されるよう、このトランク ポートをイネーブルにします。
ステップ 7	**mvr vlan** *vlan-id* **group** *ip-address* **receiver** ***vlan****-id*	（任意）トランク ポートをレシーバー VLAN 上のグループのスタティック メンバーとして設定します。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show mvr** **show mvr interface** **show mvr members**	設定を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、ポートを MVR トランク レシーバー ポートとして設定し、それを VLAN に割り当てたあと、グループのスタティック メンバーとなるように設定して、その結果を確認する例を示します。

```
Switch(config)# mvr
Switch(config)# interface fastethernet 0/10
Switch(config)# switchport mode trunk
Switch(config)# mvr type receiver
Switch(config)# mvr vlan 100 receiver vlan 201
Switch(config)# mvr vlan 100 group 239.1.1.1 receiver vlan 201
Switch(config)# end
Switch# show mvr interface

To return the interface to its default settings, use the no mvr [type | immediate | vlan
vlan-id | group] interface configuration command.
```

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 22-6 のコマンドを実行します。

表 22-6　MVR 情報を表示するためのコマンド

コマンド	目的
show mvr	スイッチの MVR ステータスと MVR 値を表示します。具体的には、MVR がイネーブルであるかディセーブルであるか、マルチキャスト VLAN、マルチキャスト グループの最大数（512）および現在の数（0 ～ 512）、クエリー応答時間、および MVR モードが表示されます。
show mvr interface [*interface-id*] [**members** [**vlan** *vlan*-**id**]]	すべての MVR インターフェイスおよびそれぞれの MVR 設定を表示します。 特定のインターフェイスを入力すると、次の情報が表示されます。 • Type：RECEIVER（レシーバー）または SOURCE（送信元） • Mode：アクセスまたはトランク • VLAN：送信元ポートの MVR VLAN およびレシーバー ポートのレシーバー VLAN • Status：次のいずれかになります。 – 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非転送中のどちらかであることを意味します。 – INACTIVE はポートがどの VLAN にも属していないことを意味します。 • Immediate Leave：イネーブルまたはディセーブル キーワード **members** を指定すると、このポート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。また、VLAN 識別子を指定すると、VLAN 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。
show mvr members [*ip-address*]	任意の IP マルチキャスト グループまたは指定された IP マルチキャスト グループ IP アドレスのメンバーであるすべてのレシーバー ポートおよび送信元ポートを表示します。

IGMP フィルタリングおよび IGMP スロットリングの設定

一部の環境（たとえば、メトロポリタンまたは Multiple-Dwelling Unit [MDU; 集合住宅] インストレーション）では、スイッチ ポート上のユーザが所属可能な複数のマルチキャスト グループを管理する必要があります。この機能により、契約やサービス計画のタイプに基づいて IP/TV などのマルチキャスト サービスの配信を制御できます。また、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を個々のスイッチ ポートに対応付けることにより、ポート単位でマルチキャスト参加をフィルタリングできます。IGMP プロファイルには 1 つまたは複数のマルチキャスト グループを格納できます。また、IGMP プロファイルによって、この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 ポートに適用された場合、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 参加レポートは廃棄され、そのポートでは該当グループからの IP マルチキャスト トラフィックを受信できません。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た場合、ポートからの IGMP レポートが転送され、通常の処理が行われます。レイヤ 2 インターフェイスが参加できる 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 レポートや Leave レポートなど、グループ固有のクエリー リポートやメンバシップ レポートだけです。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指示機能には関係しません。フィルタリング機能によって行われる処理は、マルチキャスト トラフィックの転送に IGMP を使用した場合でも MVR を使用した場合でも同じです。

IGMP フィルタリングは、IP マルチキャスト グループ アドレスをダイナミックに学習する場合にだけ適用されます。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には適用されません。

IGMP スロットリング機能により、レイヤ 2 インターフェイスが参加できる 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おり、かつ 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、さらにインターフェイスが IGMP Join レポートを受信する場合は、IGMP レポートを廃棄するか、またはランダムに選択されたマルチキャスト エントリを受信 IGMP レポートに置き換えるようインターフェイスを設定できます。

（注） IGMP フィルタリングを実行しているスイッチでは、IGMPv3 の Join メッセージおよび Leave メッセージ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 フィルタリングおよび IGMP スロットリングのデフォルト設定」（P.22-26）
- 「IGMP プロファイルの設定」（P.22-27）（任意）
- 「IGMP プロファイルの適用」（P.22-28）（任意）
- 「IGMP グループの最大数の設定」（P.22-28）（任意）
- 「IGMP スロットリング アクションの設定」（P.22-29）（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 22-7 は、IGMP フィルタリングのデフォルト設定をまとめたものです。

表 22-7　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 フィルタリング	適用なし
IGMP グループの IGMP 最大数	最大値は設定なし
IGMP プロファイル	定義なし
IGMP プロファイル アクション	範囲アドレスを拒否

転送テーブルにグループの最大数のエントリがある場合、デフォルトの IGMP スロットリング アクションとして IGMP レポートは拒否されます。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.22-29）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、プロファイル番号を指定した **ip igmp profile** 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、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、IGMP プロファイルを作成します。このモードでは、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する IGMP プロファイルのパラメータを指定できます。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）。
- **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。単独の IP アドレスを指定できるほか、開始アドレスおよび終了アドレスによりアドレスの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 プロファイルは設定されていません。プロファイルの設定時に、**permit** と **deny** のどちらのキーワードも指定されていない場合は、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 ～ 4,294,967,295 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に対するアクションとして許可または拒否を設定します。アクションが設定されていない場合は、プロファイルのデフォルト設定によりアクセスは拒否されます。
ステップ 4	**range** *ip multicast address*	アクセスが制御される IP マルチキャスト アドレスまたは IP マルチキャスト アドレスの範囲を入力します。範囲を入力する場合は、最小値の IP マルチキャスト アドレス、スペース、最大値の IP マルチキャスト アドレスの順で入力します。 **range** コマンドを繰り返し使用することで、複数のアドレスまたはアドレス範囲を入力できます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip igmp profile** *profile number*	プロファイル設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

プロファイルを削除するには、**no ip igmp profile** *profile number* グローバル コンフィギュレーション コマンドを使用します。

IP マルチキャスト アドレスまたは IP マルチキャスト アドレス範囲を削除するには、**no range** *ip multicast address* IGMP プロファイル コンフィギュレーション コマンドを使用します。

次に、単独の IP マルチキャスト アドレスに対するアクセスを許可する IGMP プロファイル 4 を作成し、その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、**show ip igmp profile** の出力にはそのアクションは表示されません。

```
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該当するインターフェイスにプロファイルを適用します。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。IGMP プロファイルはルーテッド ポートや SVI には適用できません。また、EtherChannel ポート グループに属するポートにも適用できません。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もできますが、各インターフェイスに適用できるプロファイルは 1 つだけです。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	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。このインターフェイスには、EtherChannel ポート グループに属していないレイヤ 2 ポートを指定する必要があります。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip igmp filter** *profile number*	指定した IGMP プロファイルをこの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 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスからプロファイルを削除するには、**no ip igmp filter** *profile number* インターフェイス コンフィギュレーション コマンドを使用します。

次に、ポートに IGMP プロファイル 4 を適用する例を示します。

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

IGMP グループの最大数の設定

ip igmp max-groups インターフェイス コンフィギュレーション コマンドを使用すると、レイヤ 2 インターフェイスが参加できる IGMP グループの最大数を設定できます。最大数をデフォルト（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 グループの最大数は設定できません。また、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上では使用できません。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	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。このインターフェイスには、EtherChannel グループまたは EtherChannel インターフェイスに属していないレイヤ 2 ポートを指定できます。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**ip igmp max-groups** *number*	インターフェイスが参加できる 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、最大値は設定されません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

最大グループ数の制限を削除し、デフォルト設定（最大値なし）に戻すには、**no ip igmp max-groups** インターフェイス コンフィギュレーション コマンドを使用します。

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

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

IGMP スロットリング アクションの設定

レイヤ 2 インターフェイスが参加可能な IGMP グループの最大数を設定したら、**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、既存のグループを IGMP レポートが受信され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。デフォルト設定（IGMP Join レポートを廃棄）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。

- この制限事項は、レイヤ 2 ポートに対してだけ適用されます。また、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上では使用できません。
- グループ数の上限設定がデフォルト（最大値なし）に設定されている場合は、**ip igmp max-groups action** {**deny** | **replace**} コマンドを入力しても処理は行われません。
- インターフェイスが転送テーブルにマルチキャスト エントリを追加したあとで、スロットリング アクションおよび最大グループ制限を設定すると、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無効になるかまたは削除されます。
  - スロットリング アクションを **deny** に設定すると、すでに転送テーブルにあったエントリは削除されず無効になります。これらのエントリが無効になり、エントリの最大数が転送テーブルにある場合、スイッチはインターフェイスで次に受信した 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** に設定した場合は、すでに転送テーブルにあったエントリは削除されます。エントリの最大数が転送テーブルにある場合、スイッチはランダムに選択されたエントリを受信された IGMP レポートに置き換えます。

スイッチが転送テーブルのエントリを削除しないようにするには、インターフェイス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 アクションを設定します。

転送テーブルにエントリの最大数があるときに、スロットリング アクションを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	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。このインターフェイスには、EtherChannel グループまたは EtherChannel インターフェイスに属していないレイヤ 2 ポートを指定できます。このインターフェイスには、トランク ポートを指定できません。
ステップ 3	**no shutdown**	必要に応じて、ポートをイネーブルにします。デフォルトでは、UNI および ENI はディセーブルに、NNI はイネーブルに設定されています。
ステップ 4	**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、かつ最大数のエントリが転送テーブルにある場合に、インターフェイスが実行するアクションを指定します。 • **deny**：レポートを廃棄します。 • **replace**：既存のグループを IGMP レポートが受信された新しいグループに置き換えます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config interface** *interface-id*	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトのアクション（レポートを廃棄）に戻す場合は、**no ip igmp max-groups action** インターフェイス コンフィギュレーション コマンドを使用します。

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

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

IGMP フィルタリングおよび IGMP スロットリングの設定の表示

IGMP プロファイルの特性を表示できます。また、スイッチ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 プロファイルおよび最大グループ数設定を表示できます。さらには、スイッチ上のすべてのインターフェイスおよび特定のインターフェイスの IGMP スロットリング設定を表示することもできます。

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には、表 22-8 に記載された特権 EXEC コマンドを使用します。

表 22-8　IGMP フィルタリングおよび IGMP スロットリングの設定を表示するためのコマンド

コマンド	目的
show ip igmp profile [*profile number*]	指定されている IGMP プロファイル、またはスイッチ上で定義されているすべての IGMP プロファイルを表示します。
show running-config [**interface** *interface-id*]	指定された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。インターフェイスが参加できる 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ている IGMP プロファイルなどがこれに含まれます。