IGMP の設定

IGMP および IGMP スヌーピングの前提条件

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 デバイスの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、IGMP スヌーピング クエリアは操作上、次の状況でディセーブル ステートになります。
  - IGMP スヌーピングが VLAN でディセーブルの場合
  - PIM が、VLAN に対応する SVI でイネーブルの場合

IGMP および IGMP スヌーピングの制約事項

IGMP 設定の制約事項

次に、IGMP を設定する際の制約事項を示します。

- デバイスは IGMP バージョン 1 、2、3 をサポートしています。

（注） IGMP バージョン 3 の場合、IGMP バージョン 3 BISS（基本的な IGMPv3 スヌーピング サポート）のみがサポートされます。

- IGMP バージョン 3 では新しいメンバーシップ レポート メッセージを使用しますが、これらは以前の IGMP スヌーピングデバイスで正しく認識されない可能性があります。
- IGMPv3 は、ISM および SSM と同時に動作可能です。ISM では、exclude と include の両方のモードのレポートを適用できます。SSM では、ラストホップ ルータは include モードのレポートだけを受け入れます。exclude モードのレポートは無視されます。
- ACL により、指定のポートをマルチキャストルータポートではなく、マルチキャストホストポートとしてだけ指定できます。このポートで受信されたマルチキャストルータ制御パケットは、ドロップされます。

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。

- このデバイスは、宛先マルチキャスト IP アドレスのみに基づいて IGMPv3 スヌーピングをサポートします。送信元 IP アドレスやプロキシ レポートに基づいてスヌーピングをサポートすることはありません。
- IGMP フィルタリングまたはマルチキャスト VLAN レジストレーション（MVR）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ません。

- 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 に関する情報

Internet Group Management Protocol の役割

IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。インターフェイスで PIM をイネーブルにすると、IGMP もイネーブルになります。IGMP は、特別なマルチキャスト クエリアおよびホストを使用して、ネットワーク全体でマルチキャスト トラフィックのフローを自動的に制御および制限する手段を提供します。

- クエリアは、クエリー メッセージを送信して、特定のマルチキャスト グループのメンバであるネットワーク デバイスを検出するネットワーク デバイス（ルータなど）です。
- ホストは、クエリアにホスト メンバーシップを通知するためのレポート メッセージ（クエリー メッセージに応答するメッセージ）を送信するレシーバで、ルータも含まれます。ホストでは、IGMP メッセージを使用して、マルチキャスト グループに加入し、マルチキャスト グループを脱退します。

ホストは、そのローカル マルチキャスト デバイスに IGMP メッセージを送信することで、グループ メンバーシップを識別します。IGMP では、デバイスは IGMP メッセージを受信し、定期的にクエリーを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

IGMP マルチキャスト アドレス

IP マルチキャスト トラフィックには、グループ アドレス（クラス D IP アドレス）が使用されます。クラス D アドレスの上位 4 ビットは 1110 です。したがって、ホスト グループ アドレスの範囲は 224.0.0.0 ～ 239.255.255.255 であると考えられます。

224.0.0.0 ～ 224.0.0.255 のマルチキャスト アドレスは、ルーティング プロトコルおよびその他のネットワーク制御トラフィックが使用するために予約されています。アドレス 224.0.0.0 は、どのグループにも割り当てられません。

IGMP パケットは IP マルチキャスト グループ アドレスを使用して次のように送信されます。

- IGMP 汎用クエリーは、アドレス 224.0.0.1（サブネット上のすべてのシステム）を宛先とします。
- IGMP グループ固有のクエリーは、クエリー対象デバイスのグループ IP アドレスを宛先とします。
- IGMP グループ メンバーシップ レポートは、レポート対象デバイスのグループ IP アドレスを宛先とします。
- IGMPv2 グループ脱退メッセージは、アドレス 224.0.0.2（サブネット上のすべてのデバイス）を宛先とします。
- IGMPv3 メンバーシップ レポートはアドレス 224.0.0.22 を宛先とします。すべての IGMPv3 対応マルチキャスト デバイスはこのアドレスをリッスンする必要があります。

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。

IGMP バージョン 1

IGMP バージョン 1（IGMPv1）にはクエリ応答モデルが使用されているため、マルチキャスト ルータおよびマルチレイヤ デバイスは、ローカル サブネット上のどのマルチキャスト グループがアクティブであるか（マルチキャスト グループに関係するホストが 1 台または複数存在するか）を判別できます。IGMPv1 では別のプロセスを使用して、ホストをマルチキャスト グループに加入および脱退させることができます。詳細については、RFC 1112 を参照してください。

IGMPv2

IGMP バージョン 2 は IGMP 機能の拡張版です。IGMP 脱退処理などの機能を提供して、脱退遅延を短縮し、グループ固有のクエリー数を削減し、明示的な最大クエリー応答時間を短縮します。また、この作業を実行するために、マルチキャストプロトコルに依存することなく IGMP クエリアを選択する機能もルータに追加されます。詳細については、RFC 2236 を参照してください。

（注） 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。

IGMP バージョン 3

デバイスは IGMP バージョン 3 をサポートしています。

IGMPv3 デバイスは、Basic IGMPv3 Snooping Support（BISS）をサポートしています。BISS は、IGMPv1 および IGMPv2 スイッチでのスヌーピング機能と、IGMPv3 メンバーシップ レポート メッセージをサポートしています。ネットワークに IGMPv3 ホストがある場合、BISS によりマルチキャスト トラフィックのフラッディングは抑制されます。トラフィックは、IGMPv2 または IGMPv1 ホストの IGMP スヌーピング機能の場合とほぼ同じポート セットに抑制されます。

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。

IGMPv3 ホスト シグナリング

IGMPv3 は、ホストがマルチキャスト グループのラスト ホップ デバイスにメンバーシップを伝える IETF 標準トラック プロトコルの第 3 バージョンです。IGMPv3 は、グループ メンバーシップを伝える能力をホストに与えます。これによってソースに関するフィルタリングが可能になります。ホストは、特定のソースを除いて、グループに送信するすべてのソースからトラフィックを受信したい（EXCLUDE と呼ばれるモード）、またはグループに送信する特定のソースからのみトラフィックを受信したい（INCLUDE と呼ばれるモード）と伝えることができます。

IGMPv3 は、ISM および SSM と同時に動作可能です。ISM では、EXCLUDE モードと INCLUDE モードの両方のレポートがラスト ホップ ルータによって受け入れられます。SSM では、INCLUDE モード レポートのみがラスト ホップ ルータによって受け入れられます。

IGMP のバージョンの違い

Internet Engineering Task Force（IETF）の Request for Comments（RFC）ドキュメントで定義されているように、IGMP には 3 種類のバージョンがあります。IGMPv2 は IGMPv1 の強化版で、ホストがマルチキャスト グループからの脱退を通知する機能が追加されていいます。IGMPv3 は IGMPv2 の強化版で、あるソース IP アドレスのセットから送信されたマルチキャストだけをリッスンする機能が追加されています。

表 *1 : IGMP* のバージョン

IGMP のバージョン	説明
IGMPv1	どのマルチキャスト グループがアクティブであるかをマルチキャスト デバイスが判断できる基本的なクエリー応答メカニズムと、ホストがマルチキャスト グループに加入および脱退できるようにするためのその他のプロセスを提供します。RFC 1112 で、IP マルチキャスト用の IGMPv1 ホスト拡張が定義されています。
IGMPv2	IGMP の拡張で、IGMP の脱退処理、グループ固有のクエリーおよび明示的な最大応答時間フィールドなどの機能が可能になっています。また、IGMPv2 ではこの作業を実行するために、マルチキャスト プロトコルに依存することなく IGMP クエリアを選択する機能もデバイスに追加されます。IGMPv2 は RFC 2236 で定義されています。
IGMPv3	ソース フィルタリングを提供します。これにより、マルチキャスト レシーバ ホストは、どのグループからマルチキャスト トラフィックを受信するか、およびこのトラフィックがどのソースからのものと想定されているかをデバイスに知らせることができます。さらに、IGMPv3 は IGMPv3 メンバーシップ レポートの宛先 IP アドレスであるリンク ローカル アドレス 224.0.0.22 をサポートしています。すべての IGMPv3 対応マルチキャスト デバイスは、このアドレスをリッスンする必要があります。IGMPv3 は RFC 3376 で定義されています。

（注） デフォルトでは、インターフェイスで PIM をイネーブルにすると、そのデバイスで IGMPv2 がイネーブルになります。IGMPv2 は、可能な限り IGMPv1 と下位互換性を保つよう設計されました。この下位互換性を実現するために、RFC 2236 は特別な相互運用性ルールを定義しています。ネットワークにレガシー IGMPv1 ホストが含まれている場合は、これらの運用性ルールをよく知っておく必要があります。IGMPv1 と IGMPv2 の相互運用性の詳細については、RFC 2236『Internet Group Management Protocol, Version 2』を参照してください。

IGMPv1 を実行するデバイス

IGMPv1 デバイスは、「全ホスト」へのマルチキャスト アドレスである 224.0.0.1 に IGMP クエリーを送信して、アクティブ マルチキャスト レシーバが存在するマルチキャスト グループを求めます。マルチキャスト レシーバも、デバイスに IGMP レポートを送信して、特定のマルチキャスト ストリームの受信を待機していることを通知できます。ホストは非同期に、またはデバイスによって送信される IGMP クエリーに対応して、レポートを送信できます。同じマルチキャスト グループに複数のマルチキャスト レシーバが存在する場合、これらのホストの 1 つ

のみで、IGMP レポート メッセージが送信されます。他のホストでは、レポート メッセージが抑制されます。

IGMPv1 では、IGMP クエリア選択はありません。セグメント内に複数のデバイスがある場合、すべてのデバイスが定期的に IGMP クエリーを送信します。IGMPv1 には、ホストがグループから脱退できる特別なメカニズムはありません。ホストで、特定のグループに対するマルチキャスト パケットを受信する必要がなくなった場合は、デバイスから送信される IGMP クエリー パケットに対する応答を行わないだけです。デバイスはクエリー パケットを送信し続けます。デバイスが 3 回 IGMP クエリーの応答を受信しないと、グループはタイムアウトし、デバイスはグループのセグメントへのマルチキャスト パケットの送信を停止します。ホストがタイムアウト期間後にマルチキャスト パケットを受信する場合、そのホストは新しい IGMP join をデバイスに送信するだけです。これにより、デバイスはマルチキャスト パケットの転送を再開します。

LAN 上に複数のデバイスが存在する場合は、指定ルータ（DR）を選択して、接続されているホストに対するマルチキャスト トラフィックの重複を回避する必要があります。PIM デバイスは DR を選択する選定プロセスに従います。最も大きい IP アドレスを持つ PIM デバイスが DR になります。

DR は、次のタスクを担当します。

- PIM 登録メッセージ、PIM 加入メッセージ、および PIM プルーニング メッセージをランデブー ポイント（RP）に送信し、ホスト グループ メンバーシップに関する情報を通知する。
- IGMP ホスト クエリー メッセージを送信する。
- IGMP オーバーヘッドをホストおよびネットワークでできるだけ低く維持するために、ホスト クエリー メッセージをデフォルトで 60 秒ごとに送信する。

IGMPv2 を実行するデバイス

IGMPv2 では、IGMPv1 のクエリー メッセージング機能が改善されました。

IGMPv2 のクエリーおよびメンバーシップ レポート メッセージは、次の 2 つの例外を除き、IGMPv1 メッセージと同じです。

- IGMPv2 クエリー メッセージは、一般クエリー（IGMPv1 クエリーと同じ）とグループ固有クエリーの 2 つのカテゴリに分かれる。
- IGMPv1 メンバーシップ レポートと IGMPv2 メンバーシップ レポートの IGMP タイプ コードが異なる。

IGMPv2 では、次の機能に対するサポートを追加することにより、IGMP の機能の強化も行われました。

- クエリア選択プロセス：IGMPv2 デバイスが、プロセスを実行するマルチキャスト ルーティング プロトコルに依存せずに、IGMP クエリアを選択できる機能を提供します。

- [Maximum Response Time] フィールド：IGMP クエリアを使用して最大クエリー応答時間を指定できる、クエリーメッセージの新しいフィールド。このフィールドで、応答のバースト性を制御し、脱退遅延を調整するクエリー応答プロセスの調整ができます。
- グループ固有クエリーメッセージ：すべてのグループではなく特定の 1 つのグループでクエリー操作を実行する目的で、IGMP クエリアを使用することができます。
- グループ脱退メッセージ：グループから脱退することをネットワーク上のデバイスに通知する手段をホストに提供します。

DR と IGMP クエリアが通常同じデバイスである IGMPv1 とは異なり、IGMPv2 では 2 つの機能は分離されます。DR と IGMP クエリアは異なる基準で選択され、同じサブネット上の異なるデバイスである場合があります。DR はサブネットで IP アドレスが最大のデバイスで、IGMP クエリアは最小の IP アドレスを持つデバイスです。

次のように、クエリー メッセージは IGMP クエリアの選択に使用されます。

1. 各 IGMPv2 デバイスは起動時に、そのインターフェイスアドレスを一般クエリーメッセージのソース IP アドレス フィールドに使用して、当該メッセージを全システムのグループアドレス 224.0.0.1 にマルチキャスト送信します。
2. IGMPv2 デバイスが一般クエリー メッセージを受信すると、デバイスは自分のインターフェイス アドレスとメッセージのソース IP アドレスを比較します。サブネット上の最下位 IP アドレスが使用されているデバイスにより、IGMP クエリアが選択されます。
3. すべてのデバイス（クエリアは除く）でクエリー タイマーが開始されます。IGMP クエリアから一般クエリー メッセージを受信するたびに、タイマーはリセットされます。クエリー タイマーが切れると、IGMP クエリアがダウンしたと見なされ、新しい IGMP クエリアを選択するために選択プロセスが再度実行されます。

デフォルトでは、タイマーはクエリー インターバルの 2 倍です。

IGMPv3 を実行するデバイス

IGMPv3 では、ソース フィルタリングのサポートが追加されています。これにより、マルチキャスト レシーバ ホストは、どのグループからマルチキャスト トラフィックを受信するか、およびこのトラフィックがどのソースからのものと想定されているかをデバイスに知らせることができます。このメンバーシップ情報によって、レシーバがトラフィックを要求したソースからのトラフィックだけを転送できます。

IGMPv3 では、トラフィックを受信するソースに明示的に信号を送信するアプリケーションがサポートされます。IGMPv3 では、次の 2 つのモードで、レシーバにより、マルチキャスト グループにメンバーシップの信号が送信されます。

- INCLUDE モード：このモードでは、レシーバはグループにメンバーシップをアナウンスし、トラフィックを受信する IP アドレスのリスト（INCLUDE リスト）を提供します。
- EXCLUDE モード：このモードでは、レシーバはグループにメンバーシップをアナウンスし、トラフィックを受信しない IP アドレスのリスト（EXCLUDE リスト）を提供します。つまり、ホストは IP アドレスが EXCLUDE リストに記載されていないソースからのトラ

フィックだけを受信します。インターネット標準マルチキャスト（ISM）サービスモデルの場合など、すべてのソースからトラフィックを受信するには、空のEXCLUDEリストを使用してEXCLUDEモードのメンバーシップを通知します。

IGMPv3はSSMネットワーク環境でホストがチャネル加入者に信号を送信する業界指定の標準プロトコルです。IGMPv3に依存するSSMでは、ラストホップデバイスおよびホストで実行されているオペレーティングシステムのネットワークスタック部分でIGMPv3が使用でき、そのホスト上で動作しているアプリケーションで使用されている必要があります。

IGMPv3では、ホストは224.0.0.22にメンバーシップレポートを送信します。そのため、すべてのIGMPv3デバイスでこのアドレスをリッスンする必要があります。ただし、ホストは224.0.0.22をリッスンせず、応答しません。ホストはこのアドレスにレポートを送信するだけです。さらに、IGMPv3ではIGMPv3ホストが他のホストによって送信されたレポートをリッスンしないため、メンバーシップレポートの抑制はありません。したがって、一般クエリーが送信されると、ネットワークのすべてのホストが応答します。

IGMP の加入および脱退処理

IGMP の加入処理

ホストがマルチキャストグループに加入するとき、ホストは、加入するマルチキャストグループに1つ以上の送信要求されていないメンバーシップレポートを送信します。IGMP加入処理は、IGMPv1ホストとIGMPv2ホストで同じです。

IGMPv3では、ホストの加入処理は次のように処理されます。

- ホストがグループに加入する場合は、空のEXCLUDEリストを使用して、224.0.0.22にIGMPv3メンバーシップレポートを送信します。
- ホストが特定のチャネルに加入する場合は、特定のソースアドレスを含むINCLUDEリストを使用して、224.0.0.22にIGMPv3メンバーシップレポートを送信します。
- ホストが特定のソースを除くグループに加入する場合は、これらのソースをEXCLUDEリストで除外して、224.0.0.22にIGMPv3メンバーシップレポートを送信します。

（注） LAN上にある一部のIGMPv3ホストでソースが除外され、その他のホストで同じソースが含まれている場合、デバイスはLAN上でそのソースのトラフィックを送信します（つまり、この場合、包含が除外より優先されます）。

IGMP の脱退処理

ホストがグループから脱退するために使用する方法は、動作中のIGMPのバージョンによって異なります。

IGMPv1 の脱退処理

IGMPv1には、ホストがあるグループからのマルチキャストトラフィックを受信しないことをそのサブネットのデバイスに通知するグループ脱退メッセージはありません。ホストでは、マルチキャストグループに対するトラフィックの処理が停止するだけで、そのグループに対するIGMP メンバーシップ レポートを使用したIGMP クエリーへの応答が終了します。その結果、IGMPv1デバイスがサブネットの特定のマルチキャストグループにアクティブなレシーバがなくなったことを認識する唯一の方法は、デバイスがメンバーシップ レポートを受信しなくなったときになります。このプロセスを容易にするために、IGMPv1 デバイスは、サブネットのIGMP グループとカウントダウンタイマーを関連付けます。サブネットのグループがメンバーシップ レポートを受信すると、タイマーがリセットされます。IGMPv1デバイスでは、このタイムアウト間隔は通常クエリー間隔の3倍（3分）です。このタイムアウト間隔は、すべてのホストがマルチキャストグループから脱退した後最大3分間、デバイスがサブネットにマルチキャスト トラフィックを転送し続ける可能性があることを意味します。

IGMPv2 の脱退処理

IGMPv2には、特定のグループのマルチキャストトラフィックの受信を停止することをホストが提示する手段を提供するグループ脱退メッセージが組み込まれています。IGMPv2 ホストがマルチキャスト グループから脱退するとき、そのホストがそのグループのメンバーシップ レポートでクエリーに応答する最後のホストである場合、デバイス全体のマルチキャストグループ（224.0.0.2）にグループ脱退メッセージを送信します。

IGMPv3 の脱退処理

IGMPv3 は、IGMPv3 メンバーシップ レポートにソース、グループ、またはチャネルを含めるか除外することによって、ホストが特定のグループ、ソース、またはチャネルからのトラフィックの受信を停止できる機能を導入することで、脱退処理を拡張しています。

IGMP のデフォルト設定

次の表に、デバイスの IGMP デフォルト設定を示します。

表 *2: IGMP* のデフォルト設定

機能	デフォルト設定
マルチキャストグループのメンバとしてのマルチレイヤデバイス	グループ メンバーシップは未定義
マルチキャスト グループへのアクセス	インターフェイスのすべてのグループを
IGMP のバージョン	すべてのインターフェイスでバージョン
IGMP ホストクエリー メッセージ インターバル	すべてのインターフェイスで 60 秒
IGMP クエリー タイムアウト	すべてのインターフェイスで 60 秒
IGMP 最大クエリー応答時間	すべてのインターフェイスで 10 秒

機能	デフォルト設定
静的に接続されたメンバーとしてのマルチレイヤ デバイス	ディセーブル

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
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 クエリー送信要求	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 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 していると、デフォルトの IGMP スロッ ションは IGMP レポートを拒否します。
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

レイヤ 2 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。デバイスがホストから特定のマルチキャストグループについての 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。

アクティブデバイスに設定されたマルチキャストルータは、すべての VLAN に対して定期的に一般クエリを送信します。このマルチキャスト トラフィックに関心のあるホストはすべて Join 要求を送信し、転送テーブルのエントリに追加されます。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。

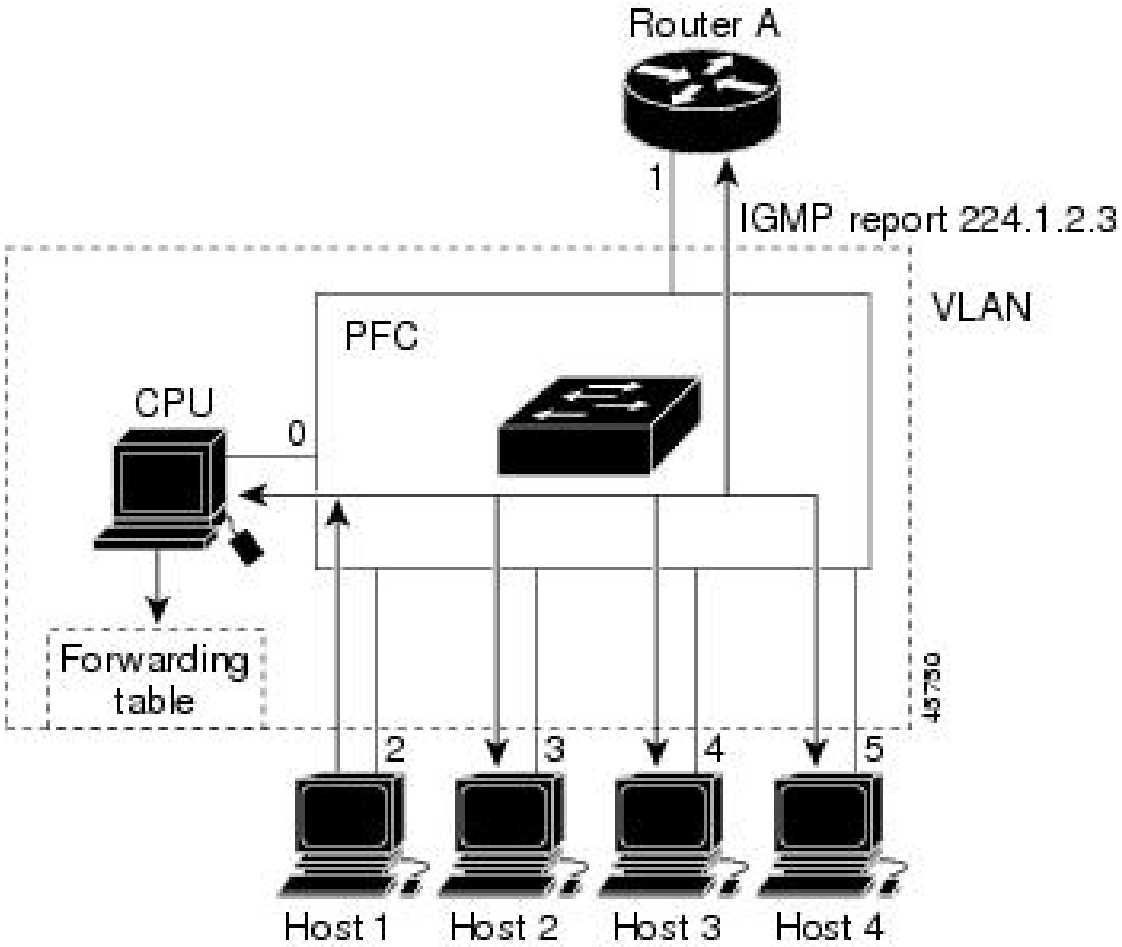
ポート スパニングツリー、ポート グループ、または VLAN ID が変更された場合、VLAN 上のこのポートから IGMP スヌーピングで学習されたマルチキャスト グループは削除されます。

ここでは、IGMP スヌーピングの特性について説明します。

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 *5: 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。

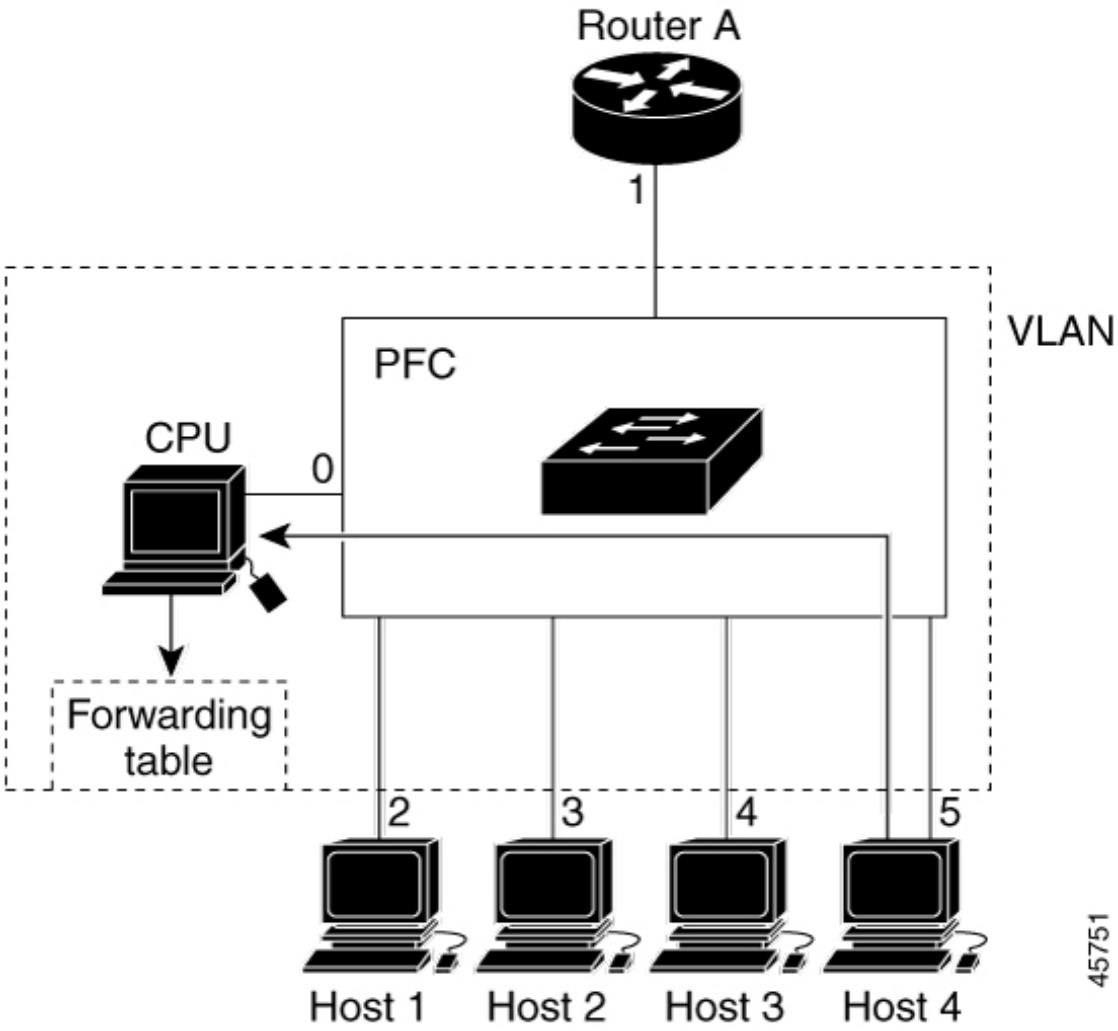


表 *6 :* 更新された *IGMP* スヌーピング転送テーブル

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に送信し、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プ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

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 スヌーピングとデバイススタック

IGMP スヌーピング機能はデバイススタック間で機能します。つまり、1 つのデバイスからの IGMP 制御情報は、スタックにあるすべてのデバイスに配信されます。スタック メンバが、どの IGMP マルチキャスト データ経由でスタックに入ったかに関係なく、データは、そのグループで登録されたホストに到達します。

スタック内のデバイスで障害が発生した場合、またはデバイスがスタックから削除された場合、そのデバイス上にあるマルチキャストグループのメンバのみが、マルチキャストデータを受信しません。スタック内にあるその他のデバイスでは、マルチキャストグループの他のすべてのメンバが、マルチキャスト データ ストリームを継続して受信します。ただし、アクティブなデバイスが削除された場合、レイヤ 2 およびレイヤ 3（IP マルチキャストルーティング）の両方に共通のマルチキャストグループでは、コンバージェンスに時間がかかる場合があります。

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 の設定方法

グループのメンバとしてデバイスを設定

デバイスをマルチキャストグループのメンバとして設定し、マルチキャストがネットワークに到達可能かどうかを検出できます。管理対象のすべてのマルチキャスト対応ルータおよびマルチレイヤデバイスがマルチキャストグループのメンバーである場合、グループに ping を送信すると、これらのすべてのデバイスが応答します。デバイスは、所属グループにアドレス指定された ICMP エコー要求パケットに応答します。もう 1 つの例は、ソフトウェア付属のマルチキャスト トレースルート ツールです。

注意 この手順を実行すると、グループ アドレス用のデータ トラフィックがすべて CPU に送られるため、CPU のパフォーマンスが低下する場合があります。

この手順は任意です。

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：	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
	`Device# configure terminal`	
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ3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。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッドポート：レイヤ3ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip igmp join-group** *group-address* 例： `Device(config-if)# ip igmp join-group 225.2.2.2`	デバイスをマルチキャストグループに加入するように設定します。デフォルトで、グループのメンバーシップは定義されていません。 *group-address* には、マルチキャスト IP アドレスをドット付き 10 進表記で指定します。
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 ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface GigabitEthernet 1/0/1`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例：	（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。

	コマンドまたはアクション	目的
	`Device# copy running-config startup-config`	

IGMP バージョンの変更

スイッチでは、IGMP クエリータイムアウトや最大クエリー応答時間などの機能を使用できる IGMP バージョン 2 がデフォルトで使用されます。

サブネット上のすべてのシステムで、同じバージョンをサポートする必要があります。スイッチは自動的にバージョン 1 のシステムを検出せず、バージョン 1 へのスイッチングも行いません。バージョン 2 のルータまたはスイッチは、常に IGMPv1 ホストと正しく連動しているため、バージョン 1 とバージョン 2 のホストはサブネット上で混在できます。

使用しているホストでバージョン 2 がサポートされていない場合は、スイッチをバージョン 1 に設定してください。

この手順は任意です。

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	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	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。

	コマンドまたはアクション	目的
ステップ 4	**ip igmp version** {**1** | **2** | **3** } 例： `Device(config-if)# ip igmp version 2`	スイッチで使用する IGMP バージョンを指定します。 （注） バージョン 1 に変更すると、 **ip igmp query-interval** および **ip igmp query-max-response-time** インターフェイス コンフィギュレーション コマンドを設定できません。 デフォルトの設定に戻す場合は、 **no ip igmp version** 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 ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	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 ホストクエリー メッセージ インターバルの変更

デバイスは、IGMP ホストクエリメッセージを定期的に送信し、接続されたネットワーク上にあるマルチキャストグループを検出します。これらのメッセージは、TTL が 1 の全ホスト マルチキャスト グループ（224.0.0.1）に送信されます。デバイスはホストクエリメッセージを送信し、ネットワーク上に存在するメンバーシップに関する情報をリフレッシュします。クエリーをいくつか実行したあとで、マルチキャスト グループのメンバーであるローカルホストが存在しないことをソフトウェアが検出した場合、そのグループのリモート送信元からローカル ネットワークへのマルチキャスト パケット転送が停止され、プルーニング メッセージが送信元のアップストリーム方向へ送信されます。

デバイスは LAN（サブネット）用の PIM DR を選択します。DR は、LAN 上のすべてのホストに IGMP ホストクエリー メッセージを送信します。SM の場合、DR は PIM 登録メッセージおよび PIM Join メッセージも RP ルータに向けて送信します。IGMPv2 では、DR は IP アドレスが最大である、ルータまたはマルチレイヤデバイスです。IGMPv1 では、DR は LAN 上で動作するマルチキャスト ルーティング プロトコルに従って選択されます。

この手順は任意です。

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	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ 3 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。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッドポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip igmp query-interval** *seconds* 例：	DR が IGMP ホストクエリー メッセージを送信する頻度を設定します。

	コマンドまたはアクション	目的
	`Device(config-if)# ip igmp query-interval 75`	デフォルトでは、DR は IGMP ホストクエリー メッセージを 60 秒ごとに送信し、ホストおよびネットワークでの IGMP オーバーヘッドを抑制します。 指定できる範囲は 1 ～ 65535 です。
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 ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	Displays
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。

IGMPv2 の最大クエリー応答時間の変更

IGMPv2 を使用している場合は、IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更できます。デバイスは最大クエリ応答時間を使用し、LAN 上に直接接続されたグループメンバが存在しないことを短時間で検出します。値を小さくすると、デバイスによるグループのプルーニング速度が向上します。

この手順は任意です。

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。

	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 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ 3 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。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッドポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip igmp query-max-response-time** *seconds* 例： `Device(config-if)# ip igmp query-max-response-time 15`	IGMP クエリーでアドバタイズされる最大クエリー応答時間を変更します。 デフォルトは 10 秒です。指定できる範囲は 1 ～ 25 です。
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 ip igmp interface** [*interface-id*] 例： `Device# show ip igmp interface`	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。

静的に接続されたメンバとしてデバイスを設定

ネットワーク セグメント上にグループ メンバが存在しなかったり、ホストで IGMP を使用してグループ メンバーシップを報告できないことがあります。しかし、そのネットワーク セグメントに対して、マルチキャスト トラフィックの送信が必要な場合もあります。マルチキャスト トラフィックをネットワーク セグメントに送り込むには、次のコマンドを使用します。

- **ip igmp join-group**：デバイスはマルチキャストパケットの転送だけでなく、マルチキャストパケットを受け入れます。マルチキャストパケットを受信する場合は、高速スイッチングを実行できません。
- **ip igmp static-group**： デバイスは、パケットを転送するだけで、パケット自体は受け入れません。この方法を使用すると、高速スイッチングが可能です。発信インターフェイスが IGMP キャッシュに格納されますが、マルチキャスト ルート エントリに「L」（ローカル）フラグが付かないことからも明らかなように、デバイス自体はメンバではありません。

この手順は任意です。

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	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet 1/0/1`	マルチキャスト ルーティングをイネーブルにするレイヤ 3 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。 次のいずれかのインターフェイスを指定する必要があります。 • ルーテッドポート：レイヤ 3 ポートとして **no switchport** インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。 • SVI：**interface vlan** *vlan-id* グローバル コンフィギュレーション コマン

	コマンドまたはアクション	目的
		ドを使用して作成された VLAN インターフェイスです。 これらのインターフェイスには、IP アドレスを割り当てる必要があります。
ステップ 4	**ip igmp static-group** *group-address* 例： `Device(config-if)# ip igmp static-group 239.100.100.101`	デバイスを静的に接続されたグループのメンバとして設定します。デフォルトでは、この機能はディセーブルになっています。
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 ip igmp interface** [*interface-id*] 例： `Device# show ip igmp 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 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。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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。 • **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。 デバイスのデフォルトでは、IGMP プロファイルが設定されていません。 （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。
ステップ 4	**permit** | **deny** 例： `Device(config-igmp-profile)# permit`	（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。

	コマンドまたはアクション	目的
ステップ 5	**range** *ip multicast address* 例： `Device(config-igmp-profile)# range 229.9.9.0`	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 アドレスの下限値、スペースを 1 つ、IP マルチキャスト アドレスの上限値を入力します。 **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。 （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。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip igmp profile** *profile number* 例： `Device# show ip igmp profile 3`	プロファイルの設定を確認します。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
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。 （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。

	コマンドまたはアクション	目的
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。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/2`	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。

	コマンドまたはアクション	目的
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。
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。 • 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：	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
	`Device# configure terminal`	
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	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。 • **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エントリを受信した IGMP レポートで上書きします。 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。

	コマンドまたはアクション	目的
		（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。
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 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。

直接接続の IGMP ホストがない場合にマルチキャスト トラフィックが転送されるようにデバイスを設定する方法

直接接続された IGMP ホストがない場合に、マルチキャスト トラフィックを転送するようにデバイスを設定するには、次のオプション作業を実行します。

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：	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
	`Device# configure terminal`	
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/1`	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。 • *type* 引数および *number* 引数に、ホストに接続されているインターフェイスを指定します。

ステップ 4	次のいずれかを実行します。
	• **ip igmp join-group** *group-address*
	• **ip igmp static-group** {***** | *group-address* [**source** *source-address*]}
	例：
	`Device(config-if)# ip igmp join-group 225.2.2.2`
	例：
	`Device(config-if)# ip igmp static-group 225.2.2.2`
		最初の例では、指定したグループに加入するデバイスのインターフェイスを設定する例を示します。
		この方法では、デバイスは、マルチキャスト パケットの転送に加えて、マルチキャスト パケットを受信します。マルチキャストパケットを受信する場合は、高速スイッチングを実行できません。
		2番目の例では、インターフェイスでスタティック グループ メンバーシップ エントリを設定する例を示します。この方法の場合、デバイスはパケットそのものを受信せず、転送だけを実行します。したがって、この方法では、高速スイッチングを実行できます。発信インターフェイスがIGMPキャッシュに格納されますが、マルチキャスト ルート エントリに「L」（ローカル）フラグが付かないことからも明らかなように、デバイス自体はメンバではありません。

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 ip igmp interface** [*interface-type interface-number*] 例： `Device# show ip igmp interface`	（任意）インターフェイスに関するマルチキャスト関連情報を表示します。

IGMP 拡張アクセス リストを使用して SSM ネットワークへのアクセスを制御する方法

ソース アドレス、グループ アドレス、またはその両方に基づいて SSM トラフィックをフィルタする IGMP 拡張アクセス リストを使用して SSM ネットワークへのアクセスを制御するには、次のオプション作業を実行します。

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 multicast-routing** [**distributed**] 例： `Device(config)# ip multicast-routing distributed`	IP マルチキャスト ルーティングを有効にします。 • **distributed** キーワードは、IPv4 マルチキャストの場合に必要です。
ステップ 4	**ip pim ssm** {**default** | **range** *access-list*} 例： `Device(config)# ip pim ssm default`	SSM サービスを設定します。 • **default** キーワードは SSM 範囲のアクセスリストを 232/8 と定義します。 • **range** キーワードは標準の IP アクセスリスト番号または SSM 範囲を定義する名前を指定します。
ステップ 5	**ip access-list extended** *access-list* -name 例： `Device(config)# ip access-list extended mygroup`	名前付き拡張 IP アクセス リストを指定します。
ステップ 6	**deny igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]	（任意）IGMP レポートから指定したソースアドレスまたはグループアドレスをフィルタリングすることで、サブネットのホストをメンバーシップから (S, G) チャネルに制限します。

	コマンドまたはアクション	目的
	例： `Device(config-ext-nacl)# deny igmp host 10.1.2.3 any`	• サブネットメンバーシップから他の (S, G) チャネルにホストを制限するには、この手順を繰り返します。（特に許可されない送信元またはグループは拒否されるため、これらの送信元は後続の **permit** ステートメントより限定的になります）。 • アクセスリストは、暗黙の **deny** ステートメントで終了することに注意してください。 • 次に、ソース 10.1.2.3 に対してすべてのグループをフィルタリングして、効果的にソースを拒否する deny ステートメントを作成する例を示します。
ステップ 7	**permit igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# permit igmp any any`	IGMP レポートのソース アドレスまたはグループ アドレスが IP アクセス リストを渡すことができます。 • アクセスリストには少なくとも 1 つの **permit** ステートメントが必要です。 • 他のソースが IP アクセス リストを渡せるようにする場合は、この手順を繰り返します。 • この例では、前の **deny** ステートメントによって拒否されていない送信元およびグループに対するメンバーシップを許可する方法を示します。
ステップ 8	**exit** 例： `Device(config-ext-nacl)# exit`	現在のコンフィギュレーション セッションを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 9	interface type number 例： `Device(config)# interface ethernet 0`	IGMPv3 をイネーブルにできるホストに接続されているインターフェイスを選択します。

	コマンドまたはアクション	目的
ステップ 10	**ip igmp access-group** *access-list* 例： `Device(config-if)# ip igmp access-group mygroup`	IGMP レポートに指定されたアクセスリストが適用されます。
ステップ 11	**ip pim sparse-mode** 例： `Device(config-if)# ip pim sparse-mode`	インターフェイスで PIM-SM をイネーブルにします。 （注） スパースモードを使用する必要があります。
ステップ 12	SSM チャネル メンバーシップのアクセス コントロールを必要とするすべてのインターフェイスでステップ 1 ～ 11 を繰り返します。	--
ステップ 13	**ip igmp version 3** 例： `Device(config-if)# ip igmp version 3`	このインターフェイス上で IGMPv3 をイネーブルにします。デフォルトの IGMP バージョンは IGMP バージョン 2 です。SSM にはバージョン 3 が必要です。
ステップ 14	ホスト方向のインターフェイスすべてでステップ 13 を繰り返します。	--
ステップ 15	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

IGMP スヌーピングを設定する方法

IGMP スヌーピングのイネーブル化

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）。

	コマンドまたはアクション	目的
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`	ディセーブルにした後で、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 4	**bridge-domain** *bridge-id* 例： `Device(config)# bridge-domain 100`	（任意）ブリッジ ドメイン コンフィギュレーション モードを開始します。
ステップ 5	**ip igmp snooping** 例： `Device(config-bdomain)# ip igmp snooping`	（任意）設定されたブリッジ ドメイン 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。 • 指定されたブリッジ ドメインで IGMP スヌーピングが明示的にディセーブルにされた場合にだけ必要です。
ステップ 6	**end** 例： `Device(config-bdomain)# end`	特権 EXEC モードに戻ります。

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。 • 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：	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
	`Device# configure terminal`	
ステップ 3	**ip igmp snooping vlan** *vlan-id* 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。 （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** *vlan-id* グローバル コンフィギュレーション コマンドを、指定した VLAN 番号に対して使用します。
ステップ 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。

スヌーピング方法の設定

マルチキャスト対応のルータ ポートは、レイヤ 2 マルチキャスト エントリごとに転送テーブルに追加されます。デバイスは、次のいずれかの方法でポートを学習します。

- IGMP クエリおよび 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静的な接続

VLAN インターフェイスがマルチキャストルータ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。

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。プロンプトが表示されたらパスワードを入力します。
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** *vlan-id* **mrouter interface** {**GigabitEthernet** | **Port-Channel** | **TenGigabitEthernet**} 例： `Device(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet1/0/3`	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 の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
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`	設定を確認します。
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。

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** *vlan-id* **mrouter interface** *interface-id* 例： `Device(config)# ip igmp snooping vlan 5 mrouter interface GigabitEthernet 1/0/1`	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。 • 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。 （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。
ステップ 4	**end** 例： `Device(config-if)# end`	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
ステップ 5	**show ip igmp snooping mrouter** [**vlan** *vlan-id*] 例： `Device# show ip igmp snooping mrouter vlan 5`	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	**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。

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	**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** *vlan-id* **static** *ip_address* **interface** *interface-id* 例： `Device(config)# ip igmp snooping vlan 105 static 230.0.0.1 interface gigabitethernet1/0/1`	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。 • *vlan-id* 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。 • *ip-address* は、グループの IP アドレスです。

	コマンドまたはアクション	目的
		• *interface-id* 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 チャネル（1 ～ 128）に設定できます。 （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** *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。
ステップ 4	**end** 例： `Device(config-if)# 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** *vlan-id* **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** *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。
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** *vlan-id* 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。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

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。

	コマンドまたはアクション	目的
		（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： `Device(config-if)# end`	特権 EXEC モードに戻ります。
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 堅牢性変数の設定

このデバイスで IGMP 堅牢性変数を設定するには、次の手順を使用します。

堅牢性変数は、IGMP メッセージの計算時に IGMP スヌーピングで使用される整数です。堅牢性変数により、想定されるパケット損失を考慮した微調整を実施できます。

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：	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
	`Device# configure terminal`	
ステップ 3	**ip igmp snooping robustness-variable** *count* 例： `Device(config)# ip igmp snooping robustness-variable 3`	IGMP 堅牢性変数を設定します。範囲は、1 ～ 3 回です。 堅牢性変数の推奨値は 2 です。IGMP スヌーピングの堅牢性変数の値をデフォルトの 2 から指定した値に変更するには、このコマンドを使用します。
ステップ 4	**ip igmp snooping vlan** *vlan-id* **robustness-variable** *count* 例： `Device(config)#ip igmp snooping vlan 100 robustness-variable 3`	（任意）VLAN インターフェイス上で IGMP 堅牢性変数を設定します。範囲は、1 ～ 3 回です。堅牢性変数の推奨値は 2 です。 （注） VLAN で堅牢性変数カウントを設定すると、グローバルに設定された値が上書きされます。
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 ip igmp snooping** 例： `Device# show ip igmp snooping`	（任意）設定された IGMP 堅牢性変数カウントを表示します。
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 最終メンバー クエリ回数の設定

グループ固有またはグループソース固有の leave メッセージの受信に応答して、IGMP グループ固有またはグループソース固有の（IGMP バージョン 3 で）クエリメッセージをデバイスが送信する回数を設定するには、次のコマンドを使用します。

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-count** *count* 例： `Device(config)# ip igmp snooping last-member-query-count 3`	IGMP 最終メンバー クエリ回数を設定します。指定できる範囲は 1 ～ 7 です。デフォルト値は 2 メッセージです。
ステップ 4	**ip igmp snooping vlan** *vlan-id* **last-member-query-count** *count* 例： `Device(config)#ip igmp snooping vlan 100 last-member-query-count 3`	（任意）VLAN インターフェイス上で IGMP 最終メンバー クエリ回数を設定します。指定できる範囲は 1 ～ 7 です。 （注） VLAN で最終メンバー クエリ回数を設定すると、グローバルに設定されたタイマーが上書きされます。
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 ip igmp snooping** 例： `Device# show ip igmp snooping`	（任意）設定された IGMP 最終メンバー クエリ回数を表示します。
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。

TCN 関連コマンドの設定

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

トポロジ変更通知（TCN）イベント後にフラッディングするマルチキャストデータのトラフィックに対し、一般クエリー数を設定できます。TCN フラッド クエリ カウントを 1 に設定した場合は、1 つの一般クエリーを受信した後にフラッディングが停止します。カウントを 7 に設定した場合、一般クエリーを 7 つ受信するまでフラッディングが続きます。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。

クライアント ロケーションが変更され、ブロックされていた後に現在は転送中の受信者が同じポートに存在する場合や、ポートが脱退メッセージを送信せずにダウンした場合などに TCN イベントが発生します。

TCN フラッド クエリー カウントを設定するには、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。 • 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 tcn flood query count** *count* 例： `Device(config)# ip igmp snooping tcn flood query count 3`	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 カウントは 2 です。 （注） デフォルトのフラッディング クエリ カウントに戻すには、**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。
ステップ 4	**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-if)# end`	
ステップ 5	**show ip igmp snooping** 例： `Device# show ip igmp snooping`	TCN の設定を確認します。
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。

フラッディング モードからの回復

トポロジの変更が発生した場合、スパニングツリーのルートは特別な IGMP Leave メッセージ（グローバル Leave メッセージ）をグループ マルチキャスト アドレス 0.0.0.0. に送信します。ただし、スパニングツリープロトコルのルートであるかどうかにかかわらず、グローバルな Leave メッセージを送信するようにデバイスを設定できます。ルータはこの特別な Leave メッセージを受信した場合、即座に一般クエリーを送信して、TCN 中のフラッディング モードからできるだけ早く回復するようにします。デバイスがスパニングツリープロトコルのルートであれば、このコンフィギュレーションに関係なく、Leave メッセージが常に送信されます。

Leave メッセージを送信できるようにするには、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 tcn query solicit** 例：	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

	コマンドまたはアクション	目的
	`Device(config)# ip igmp snooping tcn query solicit`	（グローバル脱退）を送信します。デフォルトでは、クエリー送信要求はディセーブルに設定されています。 （注） デフォルトのクエリソリューションに戻すには、**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。
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`	TCN の設定を確認します。
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。

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

デバイスは TCN を受信すると、一般クエリを 2 つ受信するまで、すべてのポートに対してマルチキャストトラフィックをフラッディングします。異なるマルチキャストグループのホストに接続されているポートが複数ある場合、リンク範囲を超えてにデバイスよるフラッディングが行われ、パケット損失が発生する可能性があります。TCN フラッディングを制御するには、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）。

	コマンドまたはアクション	目的
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。
ステップ 4	**no ip igmp snooping tcn flood** 例： `Device(config-if)# no ip igmp snooping tcn flood`	スパニングツリーの TCN イベント中に発生するマルチキャスト 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。 （注） 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。
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 ip igmp snooping** 例： `Device# show ip igmp snooping`	TCN の設定を確認します。
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 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	**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 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 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。
ステップ 5	**ip igmp snooping querier query-interval** *interval-count* 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** [**count** *count* | **interval** *interval*] 例：	（任意）トポロジ変更通知（TCN）クエリーの間隔を設定します。指定でき

	コマンドまたはアクション	目的
	`Device(config)# ip igmp snooping querier tcn query interval 20`	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** *timeout* 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** *version* 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-if)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show ip igmp snooping vlan** *vlan-id* 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 VLAN ID 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。 • 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-if)# 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`	（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。

	コマンドまたはアクション	目的
	startup-config	

IGMP のモニタリング

IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。

（注） このリリースでは、ルート単位の統計情報がサポートされていません。

また、リソースの使用状況を学習し、ネットワーク問題を解決するための情報を表示することもできます。さらに、ノードの到達可能性に関する情報を表示し、そのパケットが経由するネットワーク内のパスを検出することもできます。

次の表に示す特権EXECコマンドのいずれかを使用すると、さまざまなルーティング統計情報を表示できます。

表 *7:* システムおよびネットワーク統計情報を表示するコマンド

コマンド	目的
show ip igmp filter	IGMP フィルタ情報を表示します。
show ip igmp groups [*type-number* | *detail*]	デバイスに直接接続され、IGMP に す。
show ip igmp interface [*type number*]	インターフェイスのマルチキャス
show ip igmp membership [*name/group address* | **all** | **tracked**]	転送に関する IGMP メンバーシッ
show ip igmp profile [*profile_number*]	IGMP プロファイル情報を表示し
show ip igmp ssm-mapping [*hostname/IP address*]	IGMP SSM マッピング情報を表示
show ip igmp static-group {**class-map** [**interface** [*type*]]	スタティック グループ情報を表示
show ip igmp vrf	選択した VPN ルーティング/転送

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 *8 : 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 detail	動作状態情報を表示します。
show ip igmp snooping groups [**count** |**dynamic** [**count**] | **user** [**count**]]	デバイスまたは特定のパラメ • **count**：実エントリの代わ す。 • **dynamic**：IGMP スヌー • **user**：ユーザーによって
show ip igmp snooping groups [**count** | [**vlan** *vlan-id* [*A.B.C.D* | **count**]]	デバイスまたは特定のパラメ • **count**：グループの合計数 • **vlan**：VLAN ID によるク
show ip igmp snooping igmpv2-tracking	IGMP スヌーピング トラッキ （注） このコマンドでは プおよびIPアドレ ません。このコマ にしておく必要が
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 テーブル情報を表示します。 • *vlan-id*：VLAN ID の範囲 • **count**：実エントリの代わ す。 • **dynamic**：IGMP スヌー • *ip_address*：指定したグル ます。 • **user**：ユーザーによって
show ip igmp snooping mrouter [**vlan** *vlan-id*]	ダイナミックに学習され、手 報を表示します。 （注） IGMP スヌーピン 先インターフェイ に学習されます。 （任意）個々の VLAN に関す

コマンド	目的
show ip igmp snooping querier [**detail** | **vlan** *vlan-id*]	IP アドレス、および VLAN で受 る情報を表示します。 （任意）VLAN の詳細な IGMP （任意）個々の VLAN に関する
show ip igmp snooping querier [**vlan** *vlan-id*] **detail**	IP アドレスおよび VLAN で受信 る情報、VLAN の IGMP スヌー 表示します。
show ip igmp snooping [**vlan** *vlan-id* [**detail**]]	デバイス上のすべての VLAN ま （任意）個々の VLAN に関する る VLAN ID の範囲は 1 ～ 1001

IGMP フィルタリングおよび IGMP スロットリングの設定のモニタリング

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。また、デバイス上のすべてのインターフェイスまたは指定したインターフェイスに関する IGMP スロットリング設定を表示することもできます。

表 *9: IGMP* フィルタリングおよび *IGMP* 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
show ip igmp profile [*profile number*]	特定の IGMP プロファイルまたはデバイ れているすべての IGMP プロファイルを表
show running-config [**interface** *interface-id*]	インターフェイスが所属できる IGMP グ 数（設定されている場合）や、インター 用される IGMP プロファイルを含む、特定 フェイスまたはデバイス上のすべてのイン スの設定を表示します。

IGMP の設定例

例：マルチキャストグループのメンバとしてデバイスを設定

次に、マルチキャストグループ 255.2.2.2 へのデバイス加入を許可する例を示します。

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip igmp join-group 255.2.2.2
Device(config-if)#
```

例：マルチキャスト グループへのアクセスの制御

インターフェイスで参加数を制限するには、IGMPプロファイルと関連付けるフィルタ用のポートを設定します。

```
Device# configure terminal
Device(config)# ip igmp profile 10
Device(config-igmp-profile)# ?

IGMP profile configuration commands:
deny matching addresses are denied
exit Exit from igmp profile configuration mode
no Negate a command or set its defaults
permit matching addresses are permitted
range add a range to the set

Device(config-igmp-profile)# range 172.16.5.1
Device(config-igmp-profile)# exit
Device(config)# interface gigabitEthernet 2/0/10
Device(config-if)# ip igmp filter 10
```

例：IGMP スヌーピングの設定

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(config)# ip igmp snooping vlan 200 mrouter interface gigabitethernet1/0/2
Device(config)# end
```

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(config)# ip igmp snooping vlan 105 static 224.2.4.12 interface gigabitethernet1/0/1
Device(config)# end
```

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
```

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。

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

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

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

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 gigabitethernet1/0/2
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
```

例：ルーテッド ポートとしてのインターフェイス設定

次に、デバイスのインターフェイスをルーテッドポートとして設定する例を示します。**no switchport** コマンドを実行して複数の IP マルチキャストルーティングを設定する必要がある場合、インターフェイスでこの設定を行う必要があります。

```
Device# configure terminal
Device(config)#  interface GigabitEthernet1/0/9
Device(config-if)# description interface to be use as routed port
Device(config-if)# no switchport
Device(config-if)# ip address 10.20.20.1 255.255.255.0
Device(config-if)# ip pim sparse-mode
Device(config-if)# ip igmp join-group 224.1.2.3 source 15.15.15.2
Device(config-if)# end
Device# configure terminal
Device# show run interface gigabitEthernet 1/0/9

Current configuration : 166 bytes
!
interface GigabitEthernet1/0/9
 no switchport
 ip address 10.20.20.1 255.255.255.0
 ip pim sparse-mode
 ip igmp static-group 224.1.2.3 source 15.15.15.2
end
```

例：SVI としてのインターフェイスの設定

次に、デバイスのインターフェイスを SVI として設定する例を示します。**no switchport** コマンドを実行して複数の IP マルチキャストルーティングを設定する必要がある場合、インターフェイスでこの設定を行う必要があります。

```
Device(config)# interface vlan 150
Device(config-if)# ip address 10.20.20.1 255.255.255.0
Device(config-if)# ip pim sparse-mode
Device(config-if)#  ip igmp join-group 224.1.2.3 source 15.15.15.2
Device(config-if)# end
Device# configure terminal
Device(config)# ip igmp snooping vlan 20 static 224.1.2.3 interface gigabitEthernet 1/0/9
Device# show run interface vlan 150

Current configuration : 137 bytes
!
interface vlan 150
 ip address 10.20.20.1 255.255.255.0
 ip pim sparse-mode
 ip igmp static-group 224.1.2.3 source 15.15.15.2
end
```

例：直接接続された IGMP ホストがない場合に、マルチキャスト トラフィックを転送するようにデバイスを設定

ip igmp join-group コマンドを使用して、直接接続された IGMP ホストがない場合に、マルチキャストトラフィックを転送するようデバイスを設定する例を以下に示します。この方法では、デバイスは、マルチキャスト パケットの転送に加えて、マルチキャスト パケットを受信します。マルチキャスト パケットを受信する場合は、高速スイッチングを実行できません。

この例では、デバイスでギガビットイーサネットインターフェイス 1/0/1 が、グループ 225.2.2.2 に加入するように設定されています。

```
interface GigabitEthernet1/0/1
 ip igmp join-group 225.2.2.2
```

ip igmp static-group コマンドを使用して、直接接続された IGMP ホストがない場合に、マルチキャストトラフィックを転送するようデバイスを設定する例を以下に示します。この方法の場合、デバイスはパケットそのものを受信せず、転送だけを実行します。したがって、この方法では、高速スイッチングを実行できます。発信インターフェイスが IGMP キャッシュに格納されますが、マルチキャストルートエントリに「L」（ローカル）フラグが付かないことからも明らかなように、デバイス自体はメンバではありません。

この例では、グループ 225.2.2.2 のスタティック グループ メンバーシップ エントリがファストイーサネット インターフェイス 0/1/0 で設定されます。

```
interface GigabitEthernet1/0/1
 ip igmp static-group 225.2.2.2
```

IGMP 拡張アクセス リストを使用して SSM ネットワークへのアクセスを制御する方法

ここでは、IGMP 拡張アクセス リストを使用して SSM ネットワーク上でアクセスを制御する、次の設定例について説明します。

（注） アクセス リストは非常に柔軟が高いことに留意してください。マルチキャスト トラフィックのフィルタリングに使用できる permit ステートメントと deny ステートメントの組み合わせは多数あります。この項では、少しの例を示します。

例：グループ G のすべての状態を拒否

次に、グループ G のすべての状態を拒否する方法の例を示します。この例では、IGMPv3 レポートの SSM グループ 232.2.2.2 のすべての送信元がフィルタリングされるよう、ファストイーサネット インターフェイス 0/0/0 が設定されます。これにより、このグループが効率的に拒否されます。

```
ip access-list extended test1
 deny igmp any host 232.2.2.2
 permit igmp any any
!
interface GigabitEthernet 1/0/1
 ip igmp access-group test1
```

例：ソース S のすべての状態を拒否

次に、ソース S ですべての状態を拒否する方法の例を示します。この例では、IGMPv3 レポートの送信元の 10.2.1.32 のグループがフィルタリングされるよう、ギガビット イーサネット インターフェイス 1/1/0 が設定されます。これにより、このソースが効果的に拒否されます。

```
ip access-list extended test2
 deny igmp host 10.2.1.32 any
 permit igmp any any
!
interface GigabitEthernet1/0/1
 ip igmp access-group test2
```

例：グループ G のすべての状態を許可

次に、グループ G ですべての状態を許可する例を示します。この例では、IGMPv3 レポートの SSM グループ 232.1.1.10 に対するすべてのソースが受け付けられるよう、ギガビット イーサネット インターフェイス 1/2/0 が設定されます。これにより、このグループ全体が効果的に受け付けられます。

```
ip access-list extended test3
 permit igmp any host 232.1.1.10
!
interface GigabitEthernet 1/2/0
 ip igmp access-group test3
```

例：ソース S のすべての状態を許可

次に、ソース S ですべての状態を許可する例を示します。この例では、IGMPv3 レポートのソース 10.6.23.32 に対するすべてのグループが受け付けられるよう、ギガビット イーサネット インターフェイス 1/2 が設定されます。これにより、このソース全体が効果的に受け付けられます。

```
ip access-list extended test4
 permit igmp host 10.6.23.32 any
!
interface GigabitEthernet1/2/0
 ip igmp access-group test4
```

例：グループ G のソース S をフィルタリング

次に、グループ G の特定のソース S のフィルタリング例を示します。この例では、IGMPv3 レポートの SSM グループ 232.2.30.30 のソース 232.2.2.2 をフィルタリングするよう、ギガビット イーサネット インターフェイス 0/3/0 が設定されます。

```
ip access-list extended test5
 deny igmp host 10.4.4.4 host 232.2.30.30
 permit igmp any any
!
interface GigabitEthernet0/3/0
 ip igmp access-group test5
```

IGMP に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャスト ルーティングのコマンド」の項を参照してください。*Command Reference (Catalyst 9300 Series Switches)*

IGMP の機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IGMP	IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。インターフェイスで PIM をイネーブルにすると、IGMP もイネーブルになります。IGMP は、特別なマルチキャスト クエリアおよびホストを使用して、ネットワーク全体でマルチキャスト トラフィックのフローを自動的に制御および制限する手段を提供します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。