



IPv4 マルチキャスト トラフィックの IGMP スヌーピング

- 「IGMP スヌーピングの前提条件」 (P.40-1)
- 「IGMP スヌーピングの制約事項」 (P.40-2)
- 「IGMP スヌーピングの情報」 (P.40-3)
- 「IGMP スヌーピングのデフォルト設定」 (P.40-8)
- 「IGMP スヌーピングの設定方法」 (P.40-8)



(注)

- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html

- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- IPv6 マルチキャスト トラフィックを抑制する場合は、第 47 章「IPv6 MLD スヌーピング」を参照してください。



ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

IGMP スヌーピングの前提条件

なし。

IGMP スヌーピングの制約事項

- 「一般的な IGMP スヌーピングの制約事項」 (P.40-2)
- 「IGMP スヌーピング クエリアの制約事項」 (P.40-2)

一般的な IGMP スヌーピングの制約事項

- PIM スヌーピングが VLAN でイネーブルであり、IGMP スヌーピングが VLAN でディセーブルである場合、マルチキャスト パケットは、IGMP Join を送信するローカル レシーバへブリッジングされません。(CSCta03980)
- 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。
- IGMP スヌーピングは、プライベート VLAN をサポートします。プライベート VLAN は、IGMP スヌーピングに制約を課しません。
- IGMP スヌーピングは MAC マルチキャスト グループ 0100.5e00.0001 ~ 0100.5eff.ffff のトラフィックを抑制します。
- IGMP スヌーピングは、ルーティング プロトコルによって生成されたレイヤ 2 マルチキャストは抑制しません。

IGMP スヌーピング クエリアの制約事項

- IGMP スヌーピング クエリアはクエリア選択をサポートしません。VLAN 内の 1 つのスイッチだけで IGMP スヌーピング クエリアをイネーブルにします。(CSCsk48795)。
- グローバル コンフィギュレーション モードで VLAN を設定してください (第 25 章「仮想ローカル エリア ネットワーク (VLAN)」を参照)。
- VLAN インターフェイスの IP アドレスを設定してください (第 34 章「レイヤ 3 インターフェイス」を参照)。IGMP スヌーピング クエリアは、イネーブルの場合この IP アドレスをクエリアの送信元アドレスとして使用します。
- VLAN インターフェイスに IP アドレスが設定されていないと、IGMP スヌーピング クエリアは起動しません。IP アドレスが消去されると、IGMP スヌーピング クエリアは自身をディセーブルにします。IGMP スヌーピング クエリアをイネーブルにした場合、IP アドレスが設定されていれば、IGMP スヌーピング クエリアが再起動します。
- IGMP スヌーピング クエリアは、IGMPv3 クエリア メッセージを送信します。クエリア メッセージの IGMP バージョンは設定できませんが、クエリアは IGMPv2 ホストと互換性があります。
- IGMP スヌーピング クエリアは、イネーブルの場合、マルチキャスト ルータから IGMP トラフィックが検出されなければ、60 秒後に起動します。IGMP スヌーピング クエリアの起動後、マルチキャスト ルータまたは VLAN 内の他の IGMP スヌーピング クエリアからの IGMP トラフィックが検出されると、クエリアはディセーブルになります。
- IGMP スヌーピングがイネーブルの場合、QoS は IGMP パケットをサポートしません。

IGMP スヌーピングの情報

- 「IGMP スヌーピングの概要」(P.40-3)
- 「マルチキャスト グループへの加入」(P.40-3)
- 「マルチキャスト グループからの脱退」(P.40-5)
- 「IGMP スヌーピング クエリアについて」(P.40-6)
- 「IGMP バージョン 3 サポートについて」(P.40-6)

IGMP スヌーピングの概要

IGMP スヌーピングにより、スイッチで IGMP パケットを調べたり、パケットの内容に基づいて転送先を決定したりできます。IGMP または IGMP スヌーピング クエリアからの IGMP クエリーを受信するサブネットで、IGMP スヌーピングを使用するように、スイッチを設定できます。IGMP スヌーピングは、IPv4 マルチキャスト トラフィックを受信するポートだけにそのトラフィックをダイナミックに転送するように、レイヤ 2 LAN ポートを設定することにより、レイヤ 2 で IPv4 マルチキャスト トラフィックを抑制します。

IGMP は、マルチキャスト ルータのレイヤ 3 で稼働し、マルチキャスト トラフィックのルーティングが必要なサブネットでレイヤ 3 IGMP クエリーを生成します。

IGMP スヌーピング クエリアをスイッチに設定して、マルチキャスト ルータ インターフェイスがないサブネットにおいて IGMP スヌーピングをサポートできます。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 クエリアのイネーブル化](#)」(P.40-9) を参照してください。

IGMP (マルチキャスト ルータ上) またはローカルで、IGMP スヌーピング クエリアは、スイッチが VLAN のすべてのポートを通じて転送する、一般的な IGMP クエリーを定期的に送信し、ホストがそれに応答します。IGMP スヌーピングはレイヤ 3 IGMP トラフィックをモニタします。



(注) マルチキャスト グループで、VLAN 中に送信元だけがありレシーバがない場合は、IGMP スヌーピングはマルチキャスト トラフィックをマルチキャスト ルータ ポート宛てだけに抑制します。

マルチキャスト グループへの加入

ホストは、マルチキャスト ルータからの一般的なクエリーに応じて、非送信請求 IGMP Join メッセージを送信するか、または IGMP Join メッセージを送信して、マルチキャスト グループに参加します (スイッチは、一般的なクエリーを、マルチキャスト ルータから VLAN 中のすべてのポートに転送します)。

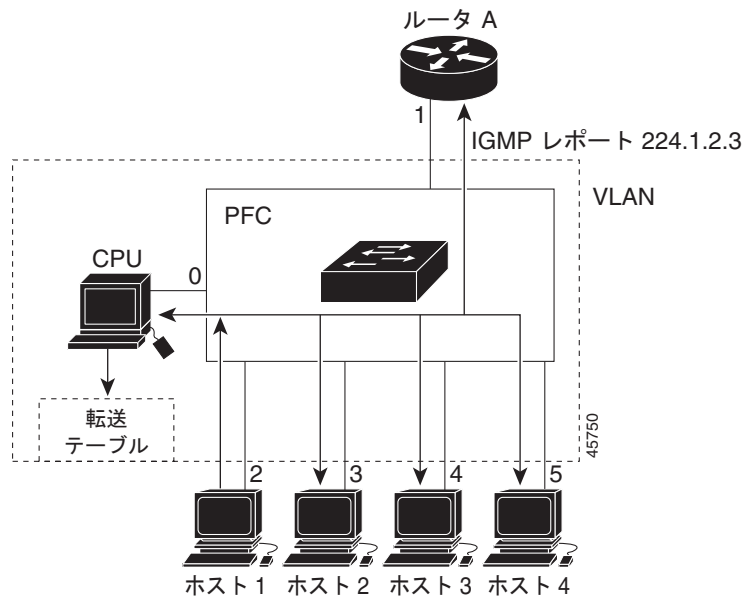
IGMP Join 要求の応答で、スイッチは、Join 要求を受信した VLAN のレイヤ 2 転送テーブルにエントリーを 1 つ作成します。このマルチキャスト トラフィックに関係する別のホストが IGMP Join 要求を送信する場合、スイッチは、既存のレイヤ 2 転送テーブル エントリーに要求を追加します。スイッチは、IGMP Join 要求を受信する各マルチキャスト グループ用レイヤ 2 転送テーブルで、VLAN あたり 1 つのエントリーだけを生成します。

IGMP スヌーピングは、マルチキャスト グループごとに 1 つを残して他のすべてのホスト応答を抑制し、その 1 つの Join メッセージだけをマルチキャスト ルータに転送します。

スイッチは、Join メッセージで指定されたマルチキャスト グループ用のマルチキャスト トラフィックを、Join メッセージを受信したインターフェイスに転送します (図 40-1 を参照)。

IGMP スヌーピングを通じて学習されるレイヤ 2 マルチキャスト グループは、ダイナミックです。ただし、`mac address-table static` コマンドを使用して、レイヤ 2 マルチキャスト グループをスタティックに設定することができます。マルチキャスト グループ アドレスのグループ メンバーシップをスタティックに指定した場合、そのスタティックな設定は、IGMP スヌーピングの学習よりも優先されます。マルチキャスト グループ メンバーシップのリストは、スタティックな設定値と、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。

図 40-1 最初の IGMP Join メッセージ



マルチキャスト ルータ A がスイッチに一般的なクエリーを送信し、ルータがそのクエリーをポート 2 ~ 5 (同じ VLAN 内のすべてのメンバ) に転送します。ホスト 1 はマルチキャスト グループ 224.1.2.3 への加入を希望し、IGMP メンバーシップ レポート (IGMP Join メッセージ) を同等の MAC 宛先アドレス 0x0100.5E01.0203 を持つグループにマルチキャストします。CPU が、ホスト 1 による IGMP レポート マルチキャストを受信すると、この CPU は IGMP レポート内の情報を利用して、転送テーブル エントリを設定します。これには、ホスト 1 のポート番号、マルチキャスト ルータ、スイッチの内部 CPU が含まれます。

CPU は、検索の種類 (IP または MAC、デフォルトでは、IP ベース) に基づいてスヌーピング転送 エントリをインストールします。IP ベースの転送を使用すると、グループ アドレス エイリアス問題が回避され、グループごとまたはグループと送信元ごとに転送を最適化できます。

IP ベースが設定されている場合、IGMP スヌーピング転送テーブルには、次のエントリがあります。スイッチのエンジンは、マルチキャスト データ パケットの宛先 IP アドレスのマッチングを行います。これらが 224.1.2.3 の場合、グループおよびマルチキャスト ルータに参加しているホストに送信しません。

| vlan | mac/ip address | LTL | ports |
|------|----------------|-------|----------------|
| 200 | (*,224.1.2.3) | 0x924 | Router, Gi3/11 |

MAC ベースが設定されている場合、エントリは次のように設定されます。この場合、スイッチ エンジンは、パケットの宛先 MAC アドレスのマッチングを行います。0100.5e01.0203 のパケットは、グループおよびマルチキャスト ルータに参加しているホストに送信されます。

| vlan | mac/ip address | LTL | ports |
|------|----------------|-----|-------|
|------|----------------|-----|-------|

200

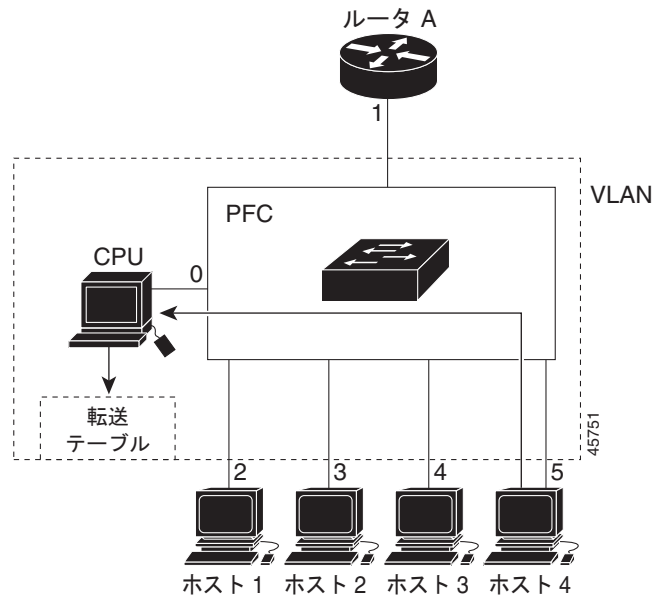
0100.5e01.0203

0x92C

Router, Gi3/11

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（図 40-2 を参照）、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、メッセージは他のポートへ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。

図 40-2 2 番めのホストのマルチキャスト グループへの加入



| vlan | mac/ip address | LTL | ports |
|------|------------------|-------|------------------------|
| 200 | (*,224.1.1.2.3) | 0x924 | Router, Gi3/11, Gi1/10 |

マルチキャスト グループからの脱退

- 「通常の脱退処理」 (P.40-5)
- 「高速脱退処理」 (P.40-6)

通常の脱退処理

関係するホストは、一般的 IGMP クエリーに定期的に応答を続ける必要があります。VLAN 中の少なくとも 1 つのホストが一般的 IGMP クエリーに定期的に応答している限り、マルチキャスト ルータはマルチキャスト トラフィックを VLAN に転送し続けます。ホストをマルチキャスト グループから脱退させたい場合は、そのホストで定期的な一般 IGMP クエリーを無視するか（「暗黙の脱退」と呼びます）、またはグループ固有の IGMPv2 Leave メッセージを送信します。

IGMP スヌーピングがグループ固有の IGMPv2 Leave メッセージをホストから受信すると、MAC ベースの一般的なクエリーを送信して、そのインターフェイスに接続されている他のデバイスがその特定のマルチキャスト グループに対するトラフィックに関係があるかどうかを判断します。IGMP スヌーピングが、この一般的なクエリーに応答して IGMP Join メッセージを受信しなかった場合、インターフェイスに接続されている他のデバイスの中に、このマルチキャスト グループのトラフィックの受信に関

与しているデバイスはないと見なし、マルチキャスト グループに対応するレイヤ 2 転送テーブル エントリからそのインターフェイスを削除します。残りのインターフェイスのうち、グループに関するホストのインターフェイスだけから Leave メッセージが送信され、一般的なクエリーに応答する IGMP Join メッセージを IGMP スヌーピングが受信しない場合、IGMP スヌーピングはグループ エントリを削除して、IGMP 脱退をマルチキャスト ルータにリレーします。マルチキャスト ルータが VLAN からレポートを受信しない場合、マルチキャスト ルータは IGMP キャッシュからその VLAN 用のグループを削除します。

テーブル エントリを更新するまでスイッチが待機する時間は、「最終メンバクエリー時間」といいます。時間を設定するには、`ip igmp snooping last-member-query-interval interval` コマンドを入力します。

高速脱退処理

IGMP スヌーピングの高速脱退処理を使用すると、IGMP スヌーピングは、最初にレイヤ 2 LAN インターフェイスに IGMP グループ対象のクエリーを送信せずに、転送テーブル エントリからそのインターフェイスを削除します。グループ特定の IGMPv2 Leave メッセージを受信すると、IGMP スヌーピングはすぐに、そのマルチキャスト グループ用のレイヤ 2 転送テーブル エントリからインターフェイスを削除します（ポート上でマルチキャスト ルータが学習された場合は除きます）。高速脱退処理により、スイッチド ネットワーク上のすべてのホストの帯域幅管理が強化されます。



(注)

高速脱退処理は、各レイヤ 2 LAN ポートに 1 つのホストしか接続されていない VLAN に限って使用してください。レイヤ 2 LAN ポートに複数のホストが接続されている VLAN 上で高速脱退をイネーブルにすると、一部のホストが偶発的にドロップされる可能性があります。高速脱退処理は、IGMP バージョン 2 およびバージョン 3 のホストについてだけサポートされます。

IGMP スヌーピング クエリアについて

マルチキャスト トラフィックをルーティングする必要がないため、PIM および IGMP を設定していない VLAN 内で IGMP スヌーピングをサポートするには、IGMP スヌーピング クエリアを使用します。

IP マルチキャスト ルーティングが設定されているネットワークでは、IP マルチキャスト ルータは IGMP クエリアとして機能します。VLAN の IP マルチキャスト トラフィックに、レイヤ 2 スイッチングだけを行う必要がある場合、IP マルチキャスト ルータは必要ではありません。ただし、VLAN 上に IP マルチキャスト ルータがない場合には、クエリーを送信できるよう他のスイッチを IGMP クエリアとして設定する必要があります。

IGMP スヌーピング クエリアは、イネーブルの場合、定期的に IGMPv3 クエリーを送信し、IP マルチキャスト トラフィックを受信するスイッチからの IGMP レポート メッセージをトリガーします。IGMP スヌーピングはこれらの IGMP レポートを待ち受けて、適切な転送を確立します。

IGMP を使用して IP マルチキャスト トラフィックへの関与をレポートするスイッチでサポートされている VLAN ごとに、1 つのスイッチを IGMP スヌーピング クエリアとして設定します。

IP マルチキャスト ルーティングがイネーブルであるかどうかにかかわらず、VLAN 上で IGMP クエリーを生成するようにスイッチを設定できます。

IGMP バージョン 3 サポートについて

- 「IGMP バージョン 3 サポートの概要」(P.40-7)
- 「IGMPv3 高速脱退処理」(P.40-7)

- 「プロキシ レポート機能」(P.40-7)
- 「明示的なホスト トラッキング」(P.40-8)

IGMP バージョン 3 サポートの概要

IGMP スヌーピングは、IGMP バージョン 3 (IGMPv3) をサポートします。IGMPv3 は送信元ベースのフィルタリングを使用します。これによりホストおよびルータは、特定のマルチキャスト グループで許可またはブロックされる送信元アドレスを指定できます。IGMPv3 スヌーピングをイネーブルにした場合、スイッチは特定の VLAN の特定のグループ用に受信したメッセージに基づいて IGMPv3 ステータスを維持し、このメッセージ内の次の情報に基づいてトラフィックを許可またはブロックします。

- 送信元リスト
- 許可 (include) またはブロック (exclude) フィルタリング オプション

ホストが限定された特定の送信元からのマルチキャスト トラフィックを受信する必要がある場合、ソース フィルタリングによって IGMPv3 join を送信できます。たとえば、ポート 3/11 の host1 が送信元 10.1.1.1 からグループ 224.1.2.3 へ join を送信し、ポート 3/12 の host2 が異なる送信元 20.1.1.1 から同じグループに join を送信するとき、IP ベースの検索が設定されている場合は、次のエントリが転送テーブルにインストールされます。

| vlan | mac/ip address | LTL | ports |
|------|----------------------|-------|--------|
| 200 | (*,224.1.2.3) | 0x920 | |
| 200 | (10.1.1.1,224.1.2.3) | 0x93E | Gi3/11 |
| 200 | (20.1.1.1,224.1.2.3) | 0x940 | Gi3/12 |

2 番目のエントリは、送信元 10.1.1.1 から host1 だけにグループ トラフィックを限定し、3 番目のエントリは、送信元 20.1.1.1 から Host2 へトラフィックを限定します。最初のエントリは、他の発信元を対象とする受信者が存在しないので、他の発信元からのグループ トラフィックをドロップします。

IGMPv3 高速脱退処理

明示的なホスト トラッキングがイネーブルの場合、IGMPv3 高速脱退処理はアクティブになります。IGMP バージョン 2 高速脱退処理をイネーブルにする `ip igmp snooping fast-leave` コマンドは、IGMPv3 高速脱退処理には影響しません。

IGMPv3 での高速脱退処理は、ソフトウェアの送信元グループ ベースのメンバーシップ情報を維持し、LTL インデックスを MAC GDA 単位で割り当てることによって実装されます。

高速脱退処理がアクティブになると、ホストは送信元からこれ以上トラフィックを受信しない場合に特定のグループに対し `BLOCK_OLD_SOURCES{src-list}` メッセージを送信します。このようなメッセージをホストから受信すると、スイッチは所定のグループに対応するホストの送信元リストを解析します。この送信元リストが脱退メッセージで受信された送信元リストとまったく同じである場合、スイッチはこのホストを LTL インデックスから削除し、ホストへのマルチキャスト グループ トラフィックの転送を停止します。

送信元リストが一致しない場合、このホストがどの送信元からのトラフィック受信にも関与しなくなるまで、スイッチは LTL インデックスからホストを削除しません。

プロキシ レポート機能

IGMP では、IGMPv1 メッセージおよび IGMPv2 メッセージでプロキシ レポート機能がサポートされ、グループ固有のクエリーが処理されます。このクエリーはダウンストリームに送信されませんが、スイッチはクエリーに直接応答します。スイッチは、グループ固有のクエリーを受信すると、グループのレシーバがある場合、クエリーを終了して IGMP プロキシ レポートを送信します。IGMPv3 メッセージ

ジには、プロキシ レポート機能がありません。IGMPv3 の場合は、グループ固有のクエリーまたはグループ送信元固有のクエリーが、すべての VLAN メンバ ポートにフラッディングされます。IGMPv3 メンバーシップ レポートのデータベースは、受信レポートに基づいて構築されます。

特定クエリーに回答するホスト レポートは、レポート抑制機能によって抑制できます。レポート抑制は、IGMPv1、IGMPv2、および IGMPv3 メッセージに関してサポートされています。レポート抑制がイネーブルな状態では（デフォルト）、スイッチが、一般クエリーを受信したとき、すべてのホストから各グループまたはチャンネル (S,G) へのレポート抑制サイクルを開始します。検出されたマルチキャスト ルータへの最初のレポートだけが転送されます。これ以外のレポートは、抑制されます。IGMPv1 および IGMPv2 の場合、抑制の時間は、一般クエリー メッセージに示されているレポート応答時間です。IGMPv3 の場合、抑制は一般クエリー時間全体で行われます。



(注) このステートはソフトウェアでのみ維持され、明示的なホスト トラッキングおよび統計情報収集に使用されます。

明示的なホスト トラッキング

IGMPv3 では、ポート上のメンバーシップ情報の明示的なトラッキングをサポートします。明示的なトラッキング データベースは、IGMPv3 ホストの高速脱退処理、プロキシ レポート機能、および統計情報収集に使用されます。VLAN で明示的なトラッキングがイネーブルの場合、IGMP スヌーピング ソフトウェアはホストから受信する IGMPv3 レポートを処理し、次の情報を含む明示的なトラッキング データベースを作成します。

- ホストに接続されたポート
- ホストによって報告されたチャンネル
- ホストによって報告された各グループのフィルタ モード
- ホストによって報告された各グループの送信元リスト
- 各グループのルータ フィルタ モード
- 送信元を要求するグループごとのホスト リスト



(注) 明示的なトラッキングがイネーブル化されていて、スイッチがプロキシレポート モードで動作している場合、ルータは VLAN インターフェイスの背後にあるホストの一部を追跡できないことがあります。

IGMP スヌーピングのデフォルト設定

なし。

IGMP スヌーピングの設定方法

- 「IGMP スヌーピング クエリアのイネーブル化」(P.40-9)
- 「IGMP スヌーピングのイネーブル化」(P.40-9)
- 「マルチキャスト レシーバへのスタティック接続の設定」(P.40-11)
- 「マルチキャスト ルータ ポートのスタティックな設定」(P.40-11)

- 「IGMP スヌーピング クエリー時間の設定」 (P.40-11)
- 「IGMP スヌーピング高速脱退処理のイネーブル化」 (P.40-12)
- 「CGMP 自動検出」 (P.40-12)
- 「IGMPv3 スヌーピングの明示的ホスト トラッキングの設定」 (P.40-13)
- 「IGMP スヌーピング情報の表示」 (P.40-14)



(注)

IGMP スヌーピングを使用するには、マルチキャストルーティングできるようにサブネットでレイヤ 3 インターフェイスを設定するか (第 39 章「IPv4 マルチキャスト レイヤ 3 機能」を参照)、またはサブネットで IGMP スヌーピング クエリアをイネーブルにします (「IGMP スヌーピング クエリアのイネーブル化」 (P.40-9) を参照)。

IGMP スヌーピング クエリアのイネーブル化

マルチキャストトラフィックをルーティングする必要がないため、PIM および IGMP を設定していない VLAN 内で IGMP スヌーピングをサポートするには、IGMP スヌーピング クエリアを使用します。VLAN で IGMP スヌーピング クエリアをイネーブルにするには、次の作業を行います。

| | コマンド | 目的 |
|-------|---|------------------------------------|
| ステップ1 | Router(config)# ip igmp snooping querier | IGMP スヌーピング クエリアをグローバルにイネーブルにします。 |
| ステップ2 | Router(config)# interface vlan vlan_ID | VLAN インターフェイスを選択します。 |
| ステップ3 | Router(config-if)# ip igmp snooping querier address ip_address | IP アドレスを割り当てます。 |
| ステップ4 | Router(config-if)# ip igmp snooping querier | VLAN で 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5 | Router(config-if)# end | コンフィギュレーション モードを終了します。 |

次に、VLAN 200 で IGMP スヌーピング クエリアをイネーブルにし、設定を確認する例を示します。

```
Router(config)# ip igmp snooping querier
Router(config)# vlan configuration 200
Router(config-if)# ip igmp snooping querier address 10.1.1.1
Router(config-if)# igmp snooping querier
Router(config-if)# end
```

IGMP スヌーピングのイネーブル化

- 「IGMP スヌーピングのグローバルなイネーブル化」 (P.40-10)
- 「VLAN における IGMP スヌーピングのイネーブル化」 (P.40-10)

IGMP スヌーピングのグローバルなイネーブル化

IGMP スヌーピングをグローバルにイネーブルにするには、次の作業を行います。

| | コマンド | 目的 |
|-------|---|------------------------|
| ステップ1 | Router(config)# ip igmp snooping | IGMP スヌーピングをイネーブルにします。 |
| ステップ2 | Router(config)# end | コンフィギュレーション モードを終了します。 |

次に、IGMP スヌーピングをグローバルにイネーブルにし、設定を確認する例を示します。

```
Router(config)# ip igmp snooping
Router(config)# end
Router# show ip igmp interface vlan 200 | include globally
IGMP snooping is globally enabled
Router#
```

VLAN における IGMP スヌーピングのイネーブル化

特定の VLAN で IGMP スヌーピングをイネーブルにするには、次の作業を行います。

| | コマンド | 目的 |
|-------|--|------------------------|
| ステップ1 | Router(config)# interface vlan <i>vlan_ID</i> | VLAN インターフェイスを選択します。 |
| ステップ2 | Router(config-if)# ip igmp snooping | IGMP スヌーピングをイネーブルにします。 |
| ステップ3 | Router(config-if)# end | コンフィギュレーション モードを終了します。 |

次に、VLAN 25 で IGMP スヌーピングをイネーブルにし、設定を確認する例を示します。

```
Router# interface vlan 25
Router(config-if)# ip igmp snooping
Router(config-if)# end
Router# show ip igmp snooping vlan 25
Global IGMP Snooping configuration:
-----
IGMP snooping Oper State      : Enabled
IGMPv3 snooping               : Enabled
Report suppression            : Disabled
EHT DB limit/count            : 100000/2
TCN solicit query             : Disabled
Robustness variable           : 2
Last member query count       : 3
Last member query interval    : 1000
Check TTL=1                   : No
Check Router-Alert-Option     : No

Vlan 25:
-----
IGMP snooping Admin State     : Enabled
IGMP snooping Oper State     : Enabled
IGMPv2 immediate leave       : Disabled
Explicit host tracking         : Enabled
Report suppression            : Enabled
Robustness variable           : 2
Last member query count       : 2
Last member query interval    : 1000
EHT DB limit/count            : 100000/2
Check TTL=1                   : Yes
```

```

Check Router-Alert-Option    : Yes
Query Interval               : 100
Max Response Time           : 10000
Router#

```

マルチキャスト レシーバへのスタティック接続の設定

マルチキャスト レシーバへのスタティックな接続を設定するには、次の作業を行います。

| コマンド | 目的 |
|---|--------------------------------|
| Router(config)# mac address-table static mac_addr vlan vlan_id interface type slot/port [disable-snooping] | マルチキャスト レシーバへのスタティックな接続を設定します。 |

スタティックな接続を設定する場合、**disable-snooping** キーワードを入力して、スタティックに設定されたマルチキャスト MAC アドレスにアドレス指定されたマルチキャスト トラフィックが、同じ VLAN 内の別のポートへ送信されるのを防止します。

次に、マルチキャスト レシーバへのスタティックな接続を設定する例を示します。

```

Router(config)# mac address-table static 0050.3e8d.6400 vlan 12 interface gigabitethernet 5/7

```

上記の **static mac** コマンドは、VLAN の検索の種類が MAC ベースの場合に使用できます。次のコマンドは、検索の種類に関係なく、グループのマルチキャスト レシーバへのスタティックな接続、または特定の送信元からのスタティックな接続を設定するために使用できます。

```

Router(config)# interface vlan 200
Router(config-if)# ip igmp snooping static 224.1.2.3 interface g3/11
Router(config-if)# ip igmp snooping static 224.1.2.3 source 20.1.1.1 interface Gi3/12

```

マルチキャスト ルータ ポートのスタティックな設定

マルチキャスト ルータへのスタティックな接続を設定するには、次の作業を行います。

| | コマンド | 目的 |
|-------|---|------------------------------|
| ステップ1 | Router(config-if)# ip igmp snooping mrouter interface type slot/port | マルチキャスト ルータへのスタティック接続を設定します。 |
| ステップ2 | Router(config-if)# end | コンフィギュレーション モードを終了します。 |

ルータへのインターフェイスは、コマンドを入力する VLAN 内である必要があります。インターフェイスは管理上アップ状態で、回線プロトコルはアップ状態である必要があります。

次に、マルチキャスト ルータへのスタティックな接続を設定する例を示します。

```

Router(config-if)# ip igmp snooping mrouter interface gigabitethernet 5/6

```

IGMP スヌーピング クエリー時間の設定

特定のマルチキャスト グループにホストがまだ関係しているかどうかを判別するグループ固有のクエリーを送信した後で、スイッチが待機する時間を設定できます。



(注) IGMP 高速脱退処理と IGMP クエリー時間の両方を設定した場合は、高速脱退処理が優先されます。

スイッチによって送信される IGMP スヌーピング クエリー時間を設定するには、次の作業を行います。

| | コマンド | 目的 |
|--------|---|---|
| ステップ 1 | Router(config)# interface vlan <i>vlan_ID</i> | VLAN インターフェイスを選択します。 |
| ステップ 2 | Router(config-if)# ip igmp snooping last-member-query-interval <i>interval</i> | スイッチによって送信される IGMP スヌーピング クエリー時間を設定します。デフォルトは 1 秒です。有効な範囲は 100 ~ 999 ミリ秒です。 |

次に、IGMP スヌーピング クエリー時間を設定する例を示します。

```
Router(config-if)# ip igmp snooping last-member-query-interval 200
Router(config-if)# exit
Router# show ip igmp interface vlan 200 | include last
IGMP snooping last member query interval on this interface is 200 ms
```

IGMP スヌーピング高速脱退処理のイネーブル化

高速脱退設定は、IGMP バージョン 2 のホストだけに適用されます。特定の VLAN 上で IGMP スヌーピング高速脱退処理をイネーブルにするには、次の作業を行います。

| | コマンド | 目的 |
|--------|---|--|
| ステップ 1 | Router(config)# interface vlan <i>vlan_ID</i> | VLAN インターフェイスを選択します。 |
| ステップ 2 | Router(config-if)# ip igmp snooping | IGMP スヌーピングをイネーブルにします。この手順は、IGMP スヌーピングがこの VLAN 上でイネーブルになっていない場合に限り必要です。 |
| ステップ 3 | Router(config-if)# ip igmp snooping fast-leave | VLAN 上で IGMP 高速脱退処理をイネーブルにします。 |

次に、VLAN 200 インターフェイスで、IGMP スヌーピング バージョン 2 のホストに対して IGMP 高速脱退処理をイネーブルにし、設定を確認する例を示します。

```
Router# interface vlan 200
Router(config-if)# ip igmp snooping
Router(config-if)# ip igmp snooping fast-leave
Configuring fast leave on vlan 200
Router(config-if)# end
Router# show ip igmp interface vlan 200 | include fast-leave
IGMP snooping fast-leave is enabled on this interface
```

CGMP 自動検出

スイッチは、デフォルトで CGMP 自動検出機能を使用して、Cisco Group Management Protocol (CGMP) パケットを検出します。CGMP 自動検出は次のように動作します。

- CGMP トラフィックが VLAN 上で検出されると、IGMP レポート抑制はその VLAN 上で 5 分間ディセーブルとなります。
- VLAN 上で新しい CGMP トラフィックが検出されるたびに、新たな 5 分間の測定を開始します。

- CGMP トラフィックが新たに検出されない状態が 5 分間続くと、IGMP レポート抑制は設定されているステータスに戻ります。

CGMP 自動検出機能には、VTP 情報へのアクセス権がないため、スイッチは VTP がトランクからルーニングした VLAN に CGMP トラフィックを送信します。この状況を回避するには、**no ip igmp snooping cgmp auto-detect** グローバル コンフィギュレーション コマンドを入力して、CGMP 自動検出機能をディセーブルにします。CGMP 自動検出をディセーブルにすると、レイヤ 2 への CGMP トラフィックが制限されます。CGMP 自動検出がディセーブルの場合は、CGMP を使用するすべての VLAN に対して、IGMP レポート抑制を手動でディセーブルにする必要があります。

CGMP 自動検出をディセーブルにするには、次の作業を行います。

| | コマンド | 目的 |
|-------|--|---|
| ステップ1 | Router(config)# no ip igmp snooping cgmp auto-detect | CGMP auto-detect モードをグローバルにディセーブルにします。 |
| ステップ2 | Router(config)# interface vlan <i>vlan_ID</i> | VLAN インターフェイスを選択します。 |
| ステップ3 | Router(config-if)# no ip igmp snooping report-suppression | IGMP スヌーピング レポート抑制をディセーブルにして、CGMP がこの VLAN 上のすべてのレポート メッセージを受信するようにします。 |
| ステップ4 | Router(config-if)# ip cgmp | この VLAN 上で CGMP モードをイネーブルにします。 |

IGMPv3 スヌーピングの明示的ホスト トラッキングの設定

特定の VLAN で IGMPv3 スヌーピングの明示的なホスト トラッキングをイネーブルにするには、次の作業を行います。

| | コマンド | 目的 |
|-------|--|--|
| ステップ1 | Router(config)# interface vlan <i>vlan_ID</i> | VLAN インターフェイスを選択します。 |
| ステップ2 | Router(config-if)# ip igmp explicit-tracking limit <i>limit</i> | 特定の VLAN で IGMPv3 スヌーピングの明示的なホスト トラッキングをイネーブルにします。 |

次に、IGMPv3 スヌーピングの明示的なホスト トラッキングをイネーブルにする例を示します。

```
Router(config-if)# ip igmp explicit-tracking limit 400
Router# show ip igmp snooping vlan 200
Global IGMP Snooping configuration:
-----
IGMP snooping Oper State      : Enabled
IGMPv3 snooping               : Enabled
Report suppression            : Disabled
EHT DB limit/count            : 100000/2
TCN solicit query             : Disabled
Robustness variable           : 2
Last member query count       : 3
Last member query interval    : 1000
Check TTL=1                   : No
Check Router-Alert-Option     : No

Vlan 200:
-----
IGMP snooping Admin State     : Enabled
```

■ IGMP スヌーピングの設定方法

```

IGMP snooping Oper State      : Enabled
IGMPv2 immediate leave       : Disabled
Explicit host tracking        : Enabled
Report suppression           : Enabled
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000
EHT DB limit/count           : 100000/2
Check TTL=1                  : Yes
Check Router-Alert-Option    : Yes
Query Interval               : 100
Max Response Time            : 10000
Router(config-vlan-config)# ip igmp snooping static 224.1.2.3 source 10.1.1.1 interface Gi3/11
Router# show ip igmp snooping groups vlan 200
Flags: I -- IGMP snooping, S -- Static, P -- PIM snooping, A -- ASM mode
Vlan      Group/source          Type      Version      Port List
-----
200       224.1.2.3                    S         v3           Gi3/11
         /10.1.1.1
Router#

```

IGMP スヌーピング情報の表示

- ・「マルチキャスト ルータ インターフェイスの表示」(P.40-14)
- ・「MAC アドレス マルチキャスト エントリの表示」(P.40-15)
- ・「VLAN インターフェイスの IGMP スヌーピング情報の表示」(P.40-15)

マルチキャスト ルータ インターフェイスの表示

IGMP スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先インターフェイスを自動的に学習します。マルチキャスト ルータ インターフェイスを表示するには、次の作業を行います。

| コマンド | 目的 |
|--|-----------------------------|
| Router# show ip igmp snooping vlan <i>vlan_ID</i> | マルチキャスト ルータ インターフェイスを表示します。 |

次に、VLAN 1 のマルチキャスト ルータ インターフェイスを表示する例を示します。

```

Router# show ip igmp snooping vlan 200
Global IGMP Snooping configuration:
-----
IGMP snooping Oper State      : Enabled
IGMPv3 snooping              : Enabled
Report suppression           : Disabled
EHT DB limit/count           : 100000/2
TCN solicit query            : Disabled
Robustness variable          : 2
Last member query count      : 3
Last member query interval   : 1000
Check TTL=1                  : No
Check Router-Alert-Option    : No

Vlan 200:
-----

```

```

IGMP snooping Admin State : Enabled
IGMP snooping Oper State : Enabled
IGMPv2 immediate leave   : Disabled
Explicit host tracking    : Enabled
Report suppression       : Enabled
Robustness variable      : 2
Last member query count  : 2
Last member query interval : 1000
EHT DB limit/count      : 100000/2
Check TTL=1              : Yes
Check Router-Alert-Option : Yes
Query Interval           : 100
Max Response Time        : 10000
Router#

```

MAC アドレス マルチキャスト エントリの表示

VLAN の MAC アドレス マルチキャスト エントリを表示するには、次の作業を行います。

| コマンド | 目的 |
|---|-------------------------------------|
| Router# show mac address-table multicast vlan_ID [count] | VLAN の MAC アドレス マルチキャスト エントリを表示します。 |

次に、VLAN 1 の MAC アドレス マルチキャスト エントリを表示する例を示します。

```

Router# show mac address-table multicast vlan 1
vlan  mac address      type    qos          ports
-----+-----+-----+-----+-----
  1  0100.5e02.0203  static  --  Gi1/1,Gi2/1,Gi3/48,Router
  1  0100.5e00.0127  static  --  Gi1/1,Gi2/1,Gi3/48,Router
  1  0100.5e00.0128  static  --  Gi1/1,Gi2/1,Gi3/48,Router
  1  0100.5e00.0001  static  --  Gi1/1,Gi2/1,Gi3/48,Router,Switch
Router#

```

次に、特定の VLAN について MAC アドレス エントリの総数を表示する例を示します。

```

Router# show mac address-table multicast 1 count

Multicast MAC Entries for vlan 1:    4
Router#

```

VLAN インターフェイスの IGMP スヌーピング情報の表示

特定の VLAN インターフェイスについて IGMP スヌーピング情報を表示するには、次の作業を行います。

| コマンド | 目的 |
|---|--|
| Router# show ip igmp interface vlan_ID | 特定の VLAN インターフェイス上の IGMP スヌーピング情報を表示します。 |

次に、VLAN 200 インターフェイスの IGMP スヌーピング情報を表示する例を示します。

```

Router# show ip igmp interface vlan 43
Vlan43 is up, line protocol is up
Internet address is 43.0.0.1/24
IGMP is enabled on interface

```

```
Current IGMP host version is 2
Current IGMP router version is 2
IGMP query interval is 60 seconds
IGMP querier timeout is 120 seconds
IGMP max query response time is 10 seconds
Last member query count is 2
Last member query response interval is 1000 ms
Inbound IGMP access group is not set
IGMP activity:1 joins, 0 leaves
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 43.0.0.1 (this system)
IGMP querying router is 43.0.0.1 (this system)
Multicast groups joined by this system (number of users):
    224.0.1.40(1)
IGMP snooping is globally enabled
IGMP snooping is enabled on this interface
IGMP snooping fast-leave is disabled and querier is disabled
IGMP snooping explicit-tracking is enabled on this interface
IGMP snooping last member query interval on this interface is 1000 ms
Router#
```



ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

[技術マニュアルのアイデア フォーラムに参加する](#)
