IGMP スヌーピングの設定

この章では、Cisco NX-OS デバイスにインターネット グループ管理プロトコル（IGMP）スヌーピングを設定する方法を説明します。

IGMP スヌーピングについて

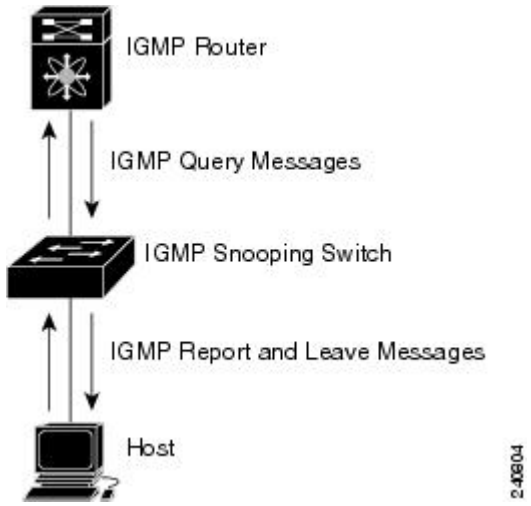
（注） デバイスの IGMP スヌーピングはディセーブルにしないことを推奨します。IGMP スヌーピングをディセーブルにすると、デバイス内で不正なフラッディングが過度に発生し、マルチキャストのパフォーマンスが低下する場合があります。

IGMP スヌーピング ソフトウェアは、VLAN 内のレイヤ 2 IP マルチキャスト トラフィックを調べて、該当する受信側が入っているポートを検出します。IGMP スヌーピングではポート情報を利用することにより、マルチアクセス LAN 環境における帯域幅消費量を削減し、VLAN 全体へのフラッディングを回避します。IGMP スヌーピング機能は、マルチキャスト対応ルータに接続されたポートを追跡して、ルータによる IGMP メンバーシップ レポートの転送機能を強化します。ト

ポロジの変更通知には、IGMP スヌーピング ソフトウェアが応答します。デバイスでは、IGMP スヌーピングがデフォルトでイネーブルになっています。

この図に、ホストと IGMP ルータ間に設置された IGMP スヌーピング スイッチを示します。IGMP スヌーピング スイッチは、IGMP メンバーシップ レポートおよび Leave メッセージをスヌーピングして、必要な場合にだけ接続された IGMP ルータに転送します。

図 *1* : *IGMP* スヌーピング スイッチ



IGMP スヌーピング ソフトウェアは、IGMPv1、IGMPv2、および IGMPv3 コントロール プレーン パケットの処理に関与し、レイヤ 3 コントロール プレーン パケットを代行受信して、レイヤ 2 の転送処理を操作します。

Cisco NX-OS IGMP スヌーピング ソフトウェアには、次の独自機能があります。

- 宛先および送信元の IP アドレスに基づいたマルチキャスト パケットの転送が可能な送信元フィルタリング
- MAC アドレスではなく、IP アドレスに基づいたマルチキャスト転送
- MAC アドレスに基づいた代わりのマルチキャスト転送

IGMP スヌーピングの詳細については、RFC 4541 を参照してください。

IGMPv1 および IGMPv2

IGMPv1 と IGMPv2 は両方とも、メンバーシップ レポート抑制をサポートします。つまり、同一サブネット上の 2 つのホストが同一グループのマルチキャスト データを受信する場合、他方のホストからメンバー レポートを受信するホストは、そのレポートを送信しません。メンバーシップ レポート抑制は、同じポートを共有しているホスト間で発生します。

各 VLAN スイッチ ポートに接続されているホストが 1 つしかない場合は、IGMPv2 の高速脱退機能を設定できます。高速脱退機能を使用すると、最終メンバのクエリー メッセージがホストに送

信されません。ソフトウェアはIGMP Leaveメッセージを受信すると、ただちに該当するポートへのマルチキャスト データ転送を停止します。

IGMPv1 では、明示的な IGMP Leave メッセージが存在しないため、特定のグループについてマルチキャストデータを要求するホストが存続しないことを示すために、メンバーシップ メッセージ タイムアウトが利用されます。

（注） 高速脱退機能がイネーブルになっている場合、他のホストの存在は確認されないため、最終メンバーのクエリー インターバル設定が無視されます。

IGMPv3

Cisco NX-OS での IGMPv3 スヌーピングの実装では完全な IGMPv3 スヌーピングがサポートされています。これにより、IGMPv3 レポートの（S、G）情報に基づいて、抑制されたフラッディングが提供されます。この送信元ベースのフィルタリングにより、デバイスは対象のマルチキャスト グループにトラフィックを送信する送信元に基づいて、マルチキャスト トラフィックの宛先ポートを制限できます。

ソフトウェアのデフォルト設定では、各 VLAN ポートに接続されたホストが追跡されます。この明示的なトラッキング機能は、高速脱退メカニズムをサポートしています。IGMPv3 ではすべてのホストがメンバーシップ レポートを送信するため、レポート抑制機能を利用すると、デバイスから他のマルチキャスト対応ルータに送信されるトラフィック量を制限できます。レポート抑制をイネーブルにすると、過去にいずれのIGMPv1 ホストまたはIGMPv2 ホストからも対象のグループへの要求がなかった場合には、プロキシ レポートが作成されます。プロキシ機能により、ダウンストリーム ホストが送信するメンバーシップ レポートからグループ ステートが構築され、アップストリーム クエリアからのクエリーに応答するためにメンバーシップ レポートが生成されます。

IGMPv3 メンバーシップ レポートには LAN セグメント上のグループ メンバの一覧が含まれていますが、最終ホストが脱退すると、メンバーシップ クエリーが送信されます。最終メンバのクエリー インターバルについてパラメータを設定すると、タイムアウトまでにどのホストからも応答がなかった場合に、グループ ステートが解除されます。

IGMP スヌーピング クエリア

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に、Protocol-Independent Multicast（PIM）がインターフェイス上でディセーブルになっている場合は、メンバーシップ クエリーを送信するように IGMP スヌーピング クエリアを設定する必要があります。このクエリアは、マルチキャスト送信元と受信者を含み、その他のアクティブ クエリアを含まない VLAN で定義します。

VLAN の任意の IP ドレスを使用するようにクエリアを設定できます。

ベスト プラクティスとして、簡単にクエリアを参照するには、一意の IP アドレス（スイッチ インターフェイスまたは Hot Standby Router Protocol（HSRP）仮想 IP アドレスでまだ使用されていない）を設定する必要があります。

（注） クエリアの IP アドレスは、ブロードキャスト IP アドレス、マルチキャスト IP アドレス、または 0（0.0.0.0）にしないでください。

IGMP スヌーピング クエリアがイネーブルな場合は、定期的に IGMP クエリーが送信されるため、IP マルチキャスト トラフィックを要求するホストから IGMP レポート メッセージが発信されます。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 スヌーピング クエリアは、RFC 2236 に記述されているようにクエリア選択を実行します。クエリア選択は、次の構成で発生します。

- 異なるスイッチ上の同じ VLAN に同じサブネットに複数のスイッチ クエリアが設定されている場合。
- 設定されたスイッチ クエリアが他のレイヤ 3 SVI クエリアと同じサブネットにある場合。

仮想化のサポート

IGMP スヌーピングに対して、複数の仮想ルーティングおよび転送（VRF）インスタンスを定義できます。

show コマンドに VRF 引数を指定して実行すると、表示される情報のコンテキストを確認できます。VRF 引数を指定しない場合は、デフォルト VRF が使用されます。

VRF の設定については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

IGMP スヌーピングのライセンス要件

製品	ライセンス要件
Cisco NX-OS	IGMP スヌーピングにはライセンスは不要です。ライセンス パッケージに含まれていない機能は nx-os イメージにバンドルされており、無料で提供されます。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

IGMP スヌーピングの前提条件

IGMP スヌーピングには、次の前提条件が適用されます。

- デバイスにログインしている。
- 現在の仮想ルーティングおよびフォワーディング（VRF）モードが正しい（グローバル コマンドの場合）。この章の例で示すデフォルトのコンフィギュレーション モードは、デフォルト VRF に適用されます。

IGMP スヌーピングに関する注意事項と制限事項

IGMP に関する注意事項および制約事項は次のとおりです。

- レイヤ 3 IPv6 マルチキャスト ルーティングはサポートされていません。
- レイヤ 2 IPv6 マルチキャスト パケットは、着信 VLAN でフラッディングされます。
- virtual Port Channel（vPC; 仮想ポート チャネル）ピアを設定している場合、2 台のデバイス間の IGMP スヌーピング設定オプションに相違があると、次のような結果になります。
  - 一方のデバイスで IGMP スヌーピングをイネーブルにして、他方でディセーブルにすると、スヌーピングがディセーブルであるデバイスではすべてのマルチキャスト トラフィックがフラッディングします。
  - マルチキャスト ルータまたはスタティック グループの設定の相違は、トラフィック損失の原因になり得ます。
  - 高速脱退、明示的な追跡、およびレポート抑制のオプションをトラフィックの転送に使用する場合、これらのオプションに相違が生じる可能性があります。
  - デバイス間でクエリー パラメータが異なると、一方のデバイスではマルチキャスト ステートが期限切れとなり、もう一方のデバイスでは転送が継続されます。この相違によって、トラフィック損失または転送の長時間化が発生します。
  - IGMP スヌーピング クエリアを両方のデバイスで設定している場合、クエリーがトラフィックで確認されると、IGMP スヌーピング クエリアはシャットダウンするので、一方のクエリアだけがアクティブになります。
- **ip igmp snooping group-timeout** コマンドは、 **ip igmp snooping proxy general-queries** コマンドを使用する場合、イネーブルにする必要があります。これを「never」に設定することをお勧めします。そのようにしない場合、マルチキャストパケットが損失する場合があります。
- 外部マルチキャスト ルータ ポート（静的構成、動的学習のいずれの場合も）では、すべてグローバル ltl インデックスが使用されます。結果として、両方のマルチキャスト ルータ ポート（Layer 2 トランク）に VLAN X と VLAN Y の両方が接続されている場合、VLAN X のトラフィックは、VLAN X と VLAN Y の両方のマルチキャスト ルータ ポートで送出されます。

デフォルト設定

パラメータ（Parameters）	デフォルト
IGMP スヌーピング	イネーブル
明示的な追跡	イネーブル
高速脱退	ディセーブル
最終メンバのクエリー インターバル	1 秒
スヌーピング クエリア	ディセーブル
レポート抑制	イネーブル
リンクローカル グループ抑制	イネーブル
デバイス全体での IGMPv3 レポート抑制	ディセーブル
VLAN ごとの IGMPv3 レポート抑制	イネーブル

IGMP スヌーピング パラメータの設定

（注） Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

（注） 他のコマンドを有効にする前に、IGMP スヌーピングをグローバルにイネーブルにする必要があります。

グローバル IGMP スヌーピング パラメータの設定

IGMP スヌーピング プロセスの動作をグローバルに変更するには、各種オプションの IGMP スヌーピング パラメータを設定します。

IGMP スヌーピング パラメータの注記

- IGMP スヌーピング プロキシ パラメータ

  IGMP 一般クエリー（GQ）の各インターバルでスヌーピング スイッチにかかる負担を減らすために、Cisco NX-OS ソフトウェアには、マルチキャスト ルータに設定されたクエリー インターバルから、IGMP スヌーピング スイッチの定期的な一般クエリー動作を分離する方法が用意されています。

  IGMP 一般クエリーをすべてのスイッチ ポートにフラッディングする代わりに、一般クエリーをマルチキャスト ルータから消費するようにデバイスを設定できます。デバイスが一般クエリーを受信すると、現在アクティブなすべてのグループに対してプロキシ レポートを生成し、ルータのクエリーで指定される MRT で指定された期間でプロキシ レポートを配布します。同時に、マルチキャスト ルータの一般クエリーのアクティビティに関係なく、デバイスは、ラウンドロビン方式で VLAN の各ポート上に IGMP 一般クエリーを送信します。これは、次の式によって求められるレートで VLAN のすべてのインターフェイスを順に処理します。

  レート = {VLAN 内のインターフェイスの数} * {設定された MRT} * {VLAN の数}

  このモードでクエリーを実行する場合、デフォルト MRT 値は 5,000 ミリ秒（5 秒）です。VLAN にスイッチポートが 500 個あるデバイスの場合、システムですべてのインターフェイスを一巡するには 2,500 秒（40 分）かかります。これは、デバイス自体がクエリアの場合でも同様です。

  この動作は、随時 1 台のホストだけが一般クエリーに応答し、デバイスのパケット/秒 IGMP 機能を下回るレートによる同時レポート レートを保持することを確実にします（約 3,000 ～ 4,000 pps）。

  （注） このオプションを使用する場合は、**ip igmp snooping group-timeout** パラメータの値を大きくするか、タイムアウトしないように変更する必要があります。

  ip igmp snooping proxy general-queries [**mrt**] コマンドを使用すると、スヌーピング機能はマルチキャスト ルータからの一般クエリーにプロキシ応答するようになる一方で、指定された MRT 値を持つ各スイッチポートに対するラウンドロビン一般クエリーの送信も行われます。（デフォルトの MRT 値は 5 秒です。）

- IGMP スヌーピング グループ タイムアウト パラメータ

  グループ タイムアウト パラメータを設定すると 3 回連続で一般クエリーの処理できない事象に基づくメンバーシップの期限切れ動作がディセーブルになります。グループ メンバーシップは、デバイスがそのポートで明示的に IGMP 脱退を受信するまで、特定のスイッチ ポートに残ります。

  ip igmp snooping group-timeout {*timeout* | **never**} コマンドは 3 回連続で一般クエリーを受信しなかったときの IGMP スヌーピング グループ メンバーシップの期限切れ動作を変更するかディセーブルにします。

手順

ステップ 1 **configure terminal**

例：
```
switch# configure terminal
switch(config)#
```

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 グローバル IGMP スヌーピング パラメータを設定するには、次のコマンドを使用します。

オプション	説明
ip igmp snooping `switch(config)# ip igmp snooping`	デバイスの IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。 （注） このコマンドの **no** 形式により、グローバル設定がディセーブルになっている場合は、個々の VLAN で IGMP スヌーピングがイネーブルであるかどうかに関係なく、すべての VLAN で IGMP スヌーピングがディセーブルになります。IGMP スヌーピングをディセーブルにすると、レイヤ 2 マルチキャスト フレームがすべてのモジュールにフラッディングします。
ip igmp snooping event-history `switch(config)# ip igmp snooping event-history`	イベント履歴バッファのサイズを設定します。デフォルトは small です。
ip igmp snooping group-timeout {*minutes* | **never**} `switch(config)# ip igmp snooping group-timeout never`	デバイス上のすべての VLAN のグループ メンバーシップ タイムアウト値を設定します。
ip igmp snooping link-local-groups-suppression `switch(config)# ip igmp snooping link-local-groups-suppression`	デバイス全体のリンクローカル グループ抑制を設定します。デフォルトではイネーブルになっています。
ip igmp snooping proxy general-inquiries [**mrt***seconds*] `switch(config)# ip igmp snooping proxy general-inquiries`	デバイスの IGMP スヌーピング プロキシを設定します。デフォルトは 5 秒です。

オプション	説明
ip igmp snooping v3-report-suppression `switch(config)# ip igmp snooping v3-report-suppression`	マルチキャスト対応ルータに送信されるメンバシップ レポート トラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。
ip igmp snooping report-suppression `switch(config)# ip igmp snooping report-suppression`	IGMPv3 レポート抑制およびプロキシ レポートを設定します。デフォルトではディセーブルになっています。

ステップ 3 **copy running-config startup-config**

例：
```
switch(config)# copy running-config startup-config
```

（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

VLAN ごとの IGMP スヌーピング パラメータの設定

IGMP スヌーピング プロセスの動作を VLAN ごとに変更するには、各種オプションの IGMP スヌーピング パラメータを設定します。

（注） このコンフィギュレーション モードを使用して目的の IGMP スヌーピング パラメータを設定します。ただし、この設定は指定した VLAN を明確に作成した後にのみ適用されます。VLAN の作成については、『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

手順

ステップ 1 **configure terminal**

例：
```
switch# configure terminal
switch(config)#
```

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**

例：
```
switch(config)# ip igmp snooping
```

IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。

（注） このコマンドの **no** 形式により、グローバル設定がディセーブルになっている場合は、個々の VLAN で IGMP スヌーピングがイネーブルであるかどうかに関係なく、すべての VLAN で IGMP スヌーピングがディセーブルになります。IGMP スヌーピングをディセーブルにすると、レイヤ 2 マルチキャスト フレームがすべてのモジュールにフラッディングします。

ステップ 3 **vlan configuration***vlan-id*

例：
```
switch(config)# vlan configuration 2
switch(config-vlan-config)#
```

VLAN に対して目的の IGMP スヌーピング パラメータを設定します。これらの設定は、指定した VLAN を作成するまで適用されません。

ステップ 4 VLAN ごとに IGMP スヌーピング パラメータを設定するには、次のコマンドを使用します。

オプション	説明
ip igmp snooping `switch(config-vlan-config)# ip igmp snooping`	現在の VLAN に対して IGMP スヌーピングをイネーブルにします。デフォルトではイネーブルになっています。
ip igmp snooping access-group {**prefix-list** | **route-map**} *policy-name***interface***interfaceslot*/*port* `switch(config-vlan-config)# ip igmp snooping access-group prefix-list plist interface ethernet 2/2`	プレフィックス リストまたはルート マップ ポリシーをベースとする IGMP スヌーピング レポートにフィルタを設定します。デフォルトではディセーブルになっています。
ip igmp snooping explicit-tracking `switch(config-vlan-config)# ip igmp snooping explicit-tracking`	各ポートに接続されたそれぞれのホストから送信される IGMPv3 メンバーシップ レポートを、VLAN 別に追跡します。デフォルトは、すべての VLAN でイネーブルです。
ip igmp snooping fast-leave `switch(config-vlan-config)# ip igmp snooping fast-leave`	IGMPv2 プロトコルのホスト レポート抑制メカニズムのために、明示的に追跡できない IGMPv2 ホストをサポートします。高速脱退がイネーブルの場合、IGMP ソフトウェアは、各 VLAN ポートに接続されたホストが 1 つだけであると見なします。デフォルトは、すべての VLAN でディセーブルです。

オプション	説明
ip igmp snooping group-timeout {*minutes* | **never**} `switch(config-vlan-config)# ip igmp snooping group-timeout never`	指定した VLAN のグループ メンバーシップ タイムアウトを設定します。
ip igmp snooping last-member-query-interval*seconds* `switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3`	いずれのホストからも IGMP クエリー メッセージへの応答がないまま、最終メンバのクエリーインターバルの期限が切れた場合に、対応する VLAN ポートからグループを削除します。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。
ip igmp snooping proxy general-queries [**mrt** *seconds*] `switch(config-vlan-config)# ip igmp snooping proxy general-queries`	指定した VLAN の IGMP スヌーピング プロキシを設定します。デフォルトは 5 秒です。
[**no**] **ip igmp snooping proxy-leave use-group-address** `switch(config-vlan-config)# ip igmp snooping proxy-leave use-group-address`	プロキシの Leave メッセージの宛先アドレスを、脱退するグループのアドレスに変更します。 通常、IGMP スヌーピングのモジュールによって生成される IGMP プロキシの Leave メッセージは、すべてのホストがグループを脱退する際に、マルチキャスト ルータ アドレス 224.0.0.2 を使用します。この設定が必要になるのは、マルチキャスト アプリケーションがレポートの受信および Leave メッセージに依存して、パケットの宛先アドレスに基づいたマルチキャスト トラフィックの開始または停止を行う場合です。
ip igmp snooping querier *ip-address* `switch(config-vlan-config)# ip igmp snooping querier 172.20.52.106`	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 をイネーブルにしていない場合に、スヌーピング クエリアを設定します。IP アドレスは、メッセージの送信元として使用します。
ip igmp snooping querier-timeout*seconds* `switch(config-vlan-config)# ip igmp snooping querier-timeout 300`	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 をイネーブルにしていない場合に、IGMPv2 のスヌーピング クエリア タイムアウト値を設定します。デフォルト値は 255 秒です。
ip igmp snooping query-interval*seconds* `switch(config-vlan-config)# ip igmp snooping query-interval 120`	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 をイネーブルにしていない場合に、スヌーピング クエリーインターバルを設定します。デフォルト値は 125 秒です。

オプション	説明
ip igmp snooping query-max-response-time*seconds* `switch(config-vlan-config)# ip igmp snooping query-max-response-time 12`	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 をイネーブルにしていない場合に、クエリー メッセージのスヌーピング MRT を設定します。デフォルト値は 10 秒です。

[**no**] **ip igmp snooping report-flood** {**all** | **interface ethernet***slot/port*}
 	
`switch(config-vlan-config)# ip igmp snooping report-flood interface ethernet 1/2`
`ip igmp snooping report-flood interface ethernet 1/3`
	IGMP レポートのフラッディングを、VLAN のすべてのアクティブなインターフェイスまたは、特定のインターフェイスのみに対して行わせます。
	
	IGMP レポートは通常、IGMP スヌーピング モジュールでの検出時にマルチキャスト ルータ ポートに転送され、VLAN でのフラッディングは行われません。ただし、このコマンドは IGMP レポートの送信を、マルチキャスト ルータ ポートに加えて、VLAN に属するカスタム ポートに対しても行わせるようスイッチを強制します。この設定が必要になるのは、マルチキャスト アプリケーションがトラフィック送信用に IGMP レポートの閲覧を必要とする場合です。

ip igmp snooping report-policy {**prefix-list** | **route-map**} *policy-name***interface***interfaceslot*/*port* `switch(config-vlan-config)# ip igmp snooping report-policy route-map rmap interface ethernet 2/4`	プレフィックス リストまたはルート マップ ポリシーをベースとする IGMP スヌーピング レポートにフィルタを設定します。デフォルトではディセーブルになっています。
ip igmp snooping startup-query-count*value* `switch(config-vlan-config)# ip igmp snooping startup-query-count 5`	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 をイネーブルにしていない場合に、起動時に送信されるクエリー数に対してスヌーピングを設定します。
ip igmp snooping startup-query-interval*seconds* `switch(config-vlan-config)# ip igmp snooping startup-query-interval 15000`	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 をイネーブルにしていない場合に、起動時のスヌーピング クエリー インターバルを設定します。
ip igmp snooping robustness-variable*value* `switch(config-vlan-config)# ip igmp snooping robustness-variable 5`	指定した VLAN のロバストネス値を設定します。デフォルト値は 2 です。

オプション	説明
ip igmp snooping report-suppression `switch(config-vlan-config)# ip igmp snooping report-suppression`	マルチキャスト対応ルータに送信されるメンバシップ レポート トラフィックを制限します。レポート抑制をディセーブルにすると、すべての IGMP レポートがそのままマルチキャスト対応ルータに送信されます。デフォルトではイネーブルになっています。
ip igmp snooping mrouter interface*interface* `switch(config-vlan-config)# ip igmp snooping mrouter interface ethernet 2/1`	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。ルータと接続するインターフェイスが、選択した VLAN に含まれている必要があります。**ethernet***slot*/*port* のように、インターフェイスをタイプおよび番号で指定できます。
ip igmp snooping static-group*group-ip-addr* [**source***source-ip-addr*] **interface***interface* `switch(config-vlan-config)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1`	VLAN のレイヤ 2 ポートをマルチキャスト グループのスタティック メンバーとして設定します。**ethernet***slot*/*port* のように、インターフェイスをタイプおよび番号で指定できます。
ip igmp snooping link-local-groups-suppression `switch(config-vlan-config)# ip igmp snooping link-local-groups-suppression`	指定した VLAN のリンクローカル グループ抑制を設定します。デフォルトではイネーブルになっています。
ip igmp snooping v3-report-suppression `switch(config-vlan-config)# ip igmp snooping v3-report-suppression`	指定した VLAN の IGMPv3 レポート抑制およびプロキシ レポートを設定します。デフォルトでは VLAN ごとに有効になっています。
ip igmp snooping version*value* `switch(config-vlan-config)# ip igmp snooping version 2`	指定した VLAN の IGMP バージョン番号を設定します。

ステップ 5 **copy running-config startup-config**

例：
```
switch(config)# copy running-config startup-config
```

（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

IGMP スヌーピング設定の検証

コマンド	説明
show ip igmp snooping[**vlan***vlan-id*]	IGMP スヌーピング設定を VLAN 別に表示します。
show ip igmp snooping groups [*source* **[***group***]** |*group* **[***source***]][vlan***vlan-id*] [**detail**]	グループに関する IGMP スヌーピング情報を VLAN 別に表示します。
show ip igmp snooping querier[**vlan***vlan-id*]	IGMP スヌーピング クエリアを VLAN 別に表示します。
show ip igmp snooping mroute[**vlan***vlan-id*]	マルチキャスト ルータ ポートを VLAN 別に表示します。
show ip igmp snooping explicit-tracking[**vlan***vlan-id*]	IGMP スヌーピングの明示的な追跡情報を VLAN 別に表示します。

IGMP スヌーピング統計情報の表示

次のコマンドを使用して、IGMP スヌーピング統計情報を表示できます。

コマンド	説明
show ip igmp snooping statistics vlan	IGMP スヌーピング統計情報を表示します。この出力で、virtual Port Channel（vPC; 仮想ポートチャネル）の統計情報を確認できます。
show ip igmp snooping {**report-policy** | **access-group**} **statistics** [**vlan***vlan*]	IGMP スヌーピングのフィルタが設定されると、VLAN ごとに詳細な統計情報を表示します。

IGMP スヌーピング統計情報のクリア

次のコマンドを使用して、IGMP スヌーピング統計情報をクリアできます。

コマンド	説明
clear ip igmp snooping statistics vlan	IGMP スヌーピングの統計情報をクリアします。

コマンド	説明
clear ip igmp snooping {**report-policy** | **access-group**} **statistics** [**vlan***vlan*]	IGMP スヌーピング フィルタの統計情報をクリアします。

IGMP スヌーピングの設定例

（注） この項での設定は、指定された VLAN を作成した後にのみ適用されます。VLAN の作成については、『*Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*』を参照してください。

次に、IGMP スヌーピング パラメータを設定する例を示します。

```
config t
  ip igmp snooping
  vlan configuration 2
    ip igmp snooping
    ip igmp snooping explicit-tracking
    ip igmp snooping fast-leave
    ip igmp snooping last-member-query-interval 3
    ip igmp snooping querier 172.20.52.106
    ip igmp snooping report-suppression
    ip igmp snooping mrouter interface ethernet 2/1
    ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
    ip igmp snooping link-local-groups-suppression
    ip igmp snooping v3-report-suppression
```

次に、プレフィックス リストを設定し、これらを使用して IGMP スヌーピング レポートをフィルタ処理する例を示します。

```
ip prefix-list plist seq 5 permit 224.1.1.1/32
ip prefix-list plist seq 10 permit 224.1.1.2/32
ip prefix-list plist seq 15 deny 224.1.1.3/32
ip prefix-list plist seq 20 deny 225.0.0.0/8 eq 32

vlan configuration 2
  ip igmp snooping report-policy prefix-list plist interface Ethernet 2/2
  ip igmp snooping report-policy prefix-list plist interface Ethernet 2/3
```

上記の例では、プレフィックス リストは 224.1.1.1 と 224.1.1.2 を許可していますが、224.1.1.3 と 225.0.0.0/8 範囲でのすべてのグループを拒否しています。プレフィックス リストは、一致がない場合は暗黙的な「拒否」になります。その他すべてを許可する場合、**ip prefix-list plist seq 30 permit 224.0.0.0/4 eq 32** を追加します。

次に、ルート マップを設定し、これらを使用して IGMP スヌーピング レポートをフィルタ処理する例を示します。

```
route-map rmap permit 10
  match ip multicast group 224.1.1.1/32
route-map rmap permit 20
  match ip multicast group 224.1.1.2/32
route-map rmap deny 30
  match ip multicast group 224.1.1.3/32
```

```
route-map rmap deny 40
  match ip multicast group 225.0.0.0/8

vlan configuration 2
  ip igmp snooping report-policy route-map rmap interface Ethernet 2/4
  ip igmp snooping report-policy route-map rmap interface Ethernet 2/5
```

上記の例では、ルート マップは 224.1.1.1 と 224.1.1.2 を許可していますが、224.1.1.3 と 225.0.0.0/8 範囲でのすべてのグループを拒否しています。ルート マップは、一致がない場合は暗黙的な「拒否」になります。その他すべてを許可する場合、**route-map rmap permit 50 match ip multicast group 224.0.0.0/4** を追加します。