



IGMP スヌーピングの設定

この章では、IPv4 ネットワークの Cisco NX-OS デバイスに対するインターネット グループ管理プロトコル (IGMP) スヌーピングの構成方法を説明します。

- [IGMP スヌーピングについて \(1 ページ\)](#)
- [IGMP スヌーピングの前提条件 \(3 ページ\)](#)
- [IGMP スヌーピングに関する注意事項と制限事項 \(4 ページ\)](#)
- [デフォルト設定 \(4 ページ\)](#)
- [IGMP スヌーピング パラメータの設定 \(5 ページ\)](#)
- [IGMP スヌーピング設定の確認 \(12 ページ\)](#)
- [IGMP スヌーピング統計情報の表示 \(13 ページ\)](#)
- [IGMP スヌーピング統計情報のクリア \(13 ページ\)](#)
- [IGMP スヌーピングの設定例 \(13 ページ\)](#)

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、デバイス内で誤った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。

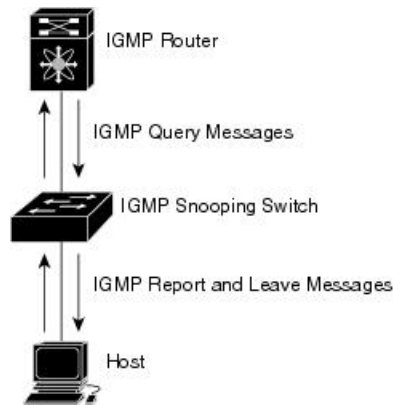
IGMP スヌーピング ソフトウェアは、VLAN 内のレイヤ 2 IP マルチキャスト トラフィックを調べて、該当する受信側が入っているポートを検出します。IGMP スヌーピングではポート情報を利用することにより、マルチアクセス LAN 環境における帯域幅消費量を削減し、VLAN 全体へのフラッディングを回避します。IGMP スヌーピングは、マルチキャスト対応ルータに接続されたポートを追跡して、ルータによる IGMP メンバシップ レポートの転送機能を強化します。トポロジの変更通知には、IGMP スヌーピング ソフトウェアが応答します。デバイスでは、IGMP スヌーピングがデフォルトでイネーブルになっています。

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。



(注) {Vlan,Mac} ルックアップにより、IGMPv2 のレポートはすでにアタッチされている受信者にフラッド/転送され、この結果は report-suppression に表示されます。これは、Cisco Nexus 3550-T 10.1(2t) リリースのみに固有のものであります。

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、次のような独自機能があります。

- MAC アドレスに基づいたマルチキャスト転送

IGMP スヌーピングの詳細については、「[RFC4541](#)」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、最終メンバー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。

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 で任意の IP ア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できるようにするには、一意の IP アドレス (スイッチ インターフェイスまたはホット スタンバイ ルータ プロトコル (HSRP) 仮想 IP アドレスでまだ使用されていないもの) 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。

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。
- 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 スヌーピングに関する注意事項および制約事項は次のとおりです。

- Cisco Nexus® 3550-T スイッチは、遅延を減らすために PIM が無効になっている着信ポートのパケットのマルチキャスト DestMAC に基づいて、既知のマルチキャストパケットを転送します。したがって、Cisco Nexus® 3550-T スイッチの IGMPv1/v2 着信レポートは、既知のマルチキャストの受信者に転送されます。
- 低遅延のために、Cisco Nexus® 3550-T スイッチは L2 ポートの {Vlan,MAC} ルックアップのみをサポートします。IP ベースの {VLAN,G} または {VLAN,G,S} ルックアップはありません。
- {Vlan,Mac} ルックアップにより、IGMPv2 のレポートはすでにアタッチされている受信者にフラッドされ、この結果は report-suppression に表示されます。IGMPv3 として構成済みのホストを保持することが推奨されます。
- **ip igmp snooping group-timeout** を有効にする必要があります **ip igmp snooping proxy general-queries** を使用する場合のコマンドを参照してください。これを「never」に設定することをお勧めします。そのように設定しないと、マルチキャストパケットが損失する場合があります。
- Cisco Nexus® 3550-T スイッチは、IPv4 の IGMP スヌーピングをサポートしていますが、IPv6 の MLD スヌーピングはサポートしていません。
- 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。

デフォルト設定

パラメータ	デフォルト
IGMP スヌーピング	有効
明示的な追跡	有効
高速脱退	無効
最終メンバー クエリ間隔	1 秒
スヌーピング クエリア	無効
レポート抑制	有効
リンクローカル グループ抑制	有効
Optimise-multicast-flood	無効

パラメータ	デフォルト
デバイス全体での IGMPv3 レポート抑制	無効
VLAN ごとの IGMPv3 レポート抑制	有効 (Enabled)

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

グローバルに IGMP スヌーピング プロセスの動作を変更するには、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、マルチキャスト ルータからの一般クエリーを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た MRT で指定されている期間でプロキシ レポートを配布します。同時に、マルチキャスト ルータの定期的な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、次の式によって算出されるレートで VLAN のすべてのインターフェイスを順に処理します。

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

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、システムの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 レートが保持され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** を変更する必要があります。パラメータを高い値に設定するか、タイムアウトしないようにします。

ip igmp snooping プロキシの一般的なクエリ **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式の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かった場合の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な 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。

The **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 次のコマンドを使用して、グローバル IGMP スヌーピング パラメータを設定します。

オプション	説明
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。
switch(config)# ip igmp snooping	

オプション	説明
	<p>(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 スヌーピングを無効にすると、Cisco Nexus® 3550-Tswitch は IGMP スヌーピング パケット処理のみを無効にします。したがって、このコマンドの no 形式を使用しても、マルチキャスト パケットを含む IGMP パケットはハードウェアで転送されません。</p>
<p>ip igmp snooping event-history</p> <pre>switch(config)# ip igmp snooping event-history</pre>	<p>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。</p>
<p>ip igmp snooping group-timeout {minutes never}</p> <pre>switch(config)# ip igmp snooping group-timeout never</pre>	<p>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。</p>
<p>ip igmp snooping link-local-groups-suppression</p> <pre>switch(config)# ip igmp snooping link-local-groups-suppression</pre>	<p>デバイス全体のリンクローカル グループ抑制を構成します。デフォルトではイネーブルになっています。</p>
<p>ip igmp snooping proxy general-inquiries [mrt seconds]</p> <pre>switch(config)# ip igmp snooping proxy general-inquiries</pre>	<p>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。</p>
<p>ip igmp snooping v3-report-suppression</p> <pre>switch(config)# ip igmp snooping v3-report-suppression</pre>	<p>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。</p>

オプション	説明
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

VLAN ごとに IGMP スヌーピングプロセスの動作を変更するには、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 を明示的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 次のコマンドを使用して、VLAN ごとに IGMP スヌーピング パラメータを設定します。

オプション	説明
<p>ip igmp snooping</p> <pre>switch(config-vlan-config)# ip igmp snooping</pre>	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。
<p>ip igmp snooping access-group {prefix-list route-map} <i>policy-name</i> interface <i>interface</i> <i>slot/port</i></p> <pre>switch(config-vlan-config)# ip igmp snooping access-group prefix-list plist interface ethernet 1/2</pre>	プレフィックスリストまたはルートマップポリシーに基づいて、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。
<p>ip igmp snooping explicit-tracking</p> <pre>switch(config-vlan-config)# ip igmp snooping explicit-tracking</pre>	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。
<p>ip igmp snooping fast-leave</p> <pre>switch(config-vlan-config)# ip igmp snooping fast-leave</pre>	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。
<p>ip igmp snooping group-timeout {<i>minutes</i> never}</p>	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。

オプション	説明
<pre>switch(config-vlan-config)# ip igmp snoothing group-timeout never</pre>	
<pre>ip igmp snooping last-member-query-interval 秒 switch(config-vlan-config)# ip igmp snoothing last-member-query-interval 3</pre>	<p>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、関連する 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。</p>
<pre>ip igmp snooping proxy general-queries [mrt seconds] switch(config-vlan-config)# ip igmp snoothing proxy general-queries</pre>	<p>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。</p>
<pre>ip igmp snooping querier ip-address switch(config-vlan-config)# ip igmp snoothing querier 172.20.52.106</pre>	<p>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。</p>
<pre>ip igmp snooping querier-timeout 秒 switch(config-vlan-config)# ip igmp snoothing querier-timeout 300</pre>	<p>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の、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。</p>
<pre>ip igmp snooping query-interval 秒 switch(config-vlan-config)# ip igmp snoothing query-interval 120</pre>	<p>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。</p>
<pre>ip igmp snooping query-max-response-time 秒 switch(config-vlan-config)# ip igmp snoothing query-max-response-time 12</pre>	<p>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。</p>
<pre>ip igmp snooping report-policy {prefix-list route-map} policy-name interface interface slot/port</pre>	<p>プレフィックスリストまたはルートマップポリシーに基づいて、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。</p>

オプション	説明
<pre>switch(config-vlan-config)# ip igmp snoping report-policy route-map rmap interface ethernet 1/4</pre>	
<p>ip igmp snooping startup-query-count value</p> <pre>switch(config-vlan-config)# ip igmp snoping startup-query-count 5</pre>	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。
<p>ip igmp snooping startup-query-interval 秒</p> <pre>switch(config-vlan-config)# ip igmp snoping startup-query-interval 15000</pre>	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。
<p>ip igmp snooping robustness-variable value</p> <pre>switch(config-vlan-config)# ip igmp snoping robustness-variable 5</pre>	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。
<p>ip igmp snooping report-suppression</p> <pre>switch(config-vlan-config)# ip igmp snoping report-suppression</pre>	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。
<p>ip igmp snooping mrouter interface interface</p> <pre>switch(config-vlan-config)# ip igmp snoping mrouter interface ethernet 1/1</pre>	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、インターフェイスはタイプおよび番号で指定できます。
<p>ip igmp snooping static-group group-ip-addr [source source-ip-addr] interface interface</p> <pre>switch(config-vlan-config)# ip igmp snoping static-group 230.0.0.1 interface ethernet 1/1</pre>	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、インターフェイスはタイプおよび番号で指定できます。
<p>ip igmp snooping link-local-groups-suppression</p>	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。

オプション	説明
switch(config-vlan-config)# ip igmp snooping link-local-groups-suppression	
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確認

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] [detail]	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
<code>show ip igmp snooping statistics vlan</code>	IGMP スヌーピング統計情報を表示します。この出力で、仮想ポート チャンネル (vPC) の統計情報を確認できます。
<code>show ip igmp snooping {report-policy access-group} statistics [vlan vlan]</code>	IGMP スヌーピングのフィルタが設定されている場合、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
<code>clear ip igmp snooping statistics vlan</code>	IGMP スヌーピングの統計情報をクリアします。
<code>clear ip igmp snooping {report-policy access-group} statistics [vlan vlan]</code>	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) このセクションでの設定は、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 3550-T Layer 2 Switching 構成ガイド」のセクション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 1/1
ip igmp snooping static-group 230.0.0.1 interface ethernet 1/1
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 1/2
 ip igmp snooping report-policy prefix-list plist interface Ethernet 1/3
```

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 1/4
 ip igmp snooping report-policy route-map rmap interface Ethernet 1/5
```

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。

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。