



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) スヌーピングを構成する方法を説明します。

この章は、次の項で構成されています。

- [IGMP スヌーピングの情報 \(1 ページ\)](#)
- [IGMP スヌーピングに関する注意事項と制限事項 \(4 ページ\)](#)
- [IGMP スヌーピングの前提条件 \(5 ページ\)](#)
- [IGMP スヌーピングのデフォルト設定 \(5 ページ\)](#)
- [IGMP スヌーピングの設定 \(6 ページ\)](#)
- [IGMP スヌーピング パラメータの設定 \(10 ページ\)](#)
- [IGMP スヌーピング設定の確認 \(18 ページ\)](#)
- [IGMP スヌーピング統計情報の表示 \(19 ページ\)](#)
- [IGMP スヌーピング統計情報のクリア \(19 ページ\)](#)
- [IGMP スヌーピングの設定例 \(19 ページ\)](#)
- [その他の参考資料 \(20 ページ\)](#)
- [関連資料 \(20 ページ\)](#)
- [標準 \(20 ページ\)](#)

IGMP スヌーピングの情報



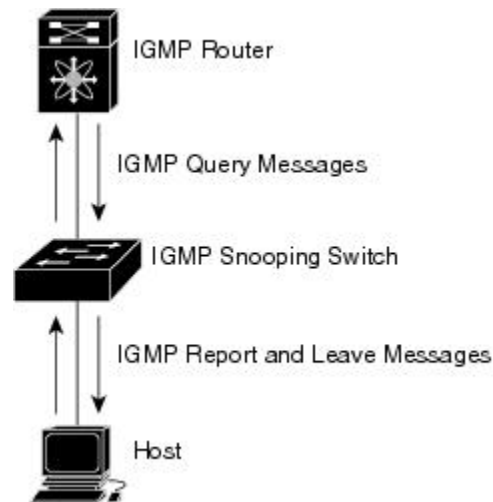
(注) スイッチでは、IGMP スヌーピングをディセーブルにしないことを推奨します。IGMP スヌーピングをディセーブルにすると、スイッチで不正なフラッドイングが過度に発生し、マルチキャストのパフォーマンスが低下する場合があります。

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査し、関係する受信機が常駐するポートを発見します。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 全体へのフラッドイングを回避します。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。デフォルトでは、IGMP スヌーピングがスイッチでイネーブルにされています。

次の図では、ホストと IGMP ルータ間にある 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参与し、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。

IGMPの詳細については、「[IGMP の設定](#)」を参照してください。

Cisco NX-OS IGMP スヌーピングソフトウェアには、次のような独自の機能があります。

- 送信元フィルタリングにより、宛先および送信元の IP アドレスに基づいて、マルチキャストパケットを転送できます。
- MAC アドレスでなく、IP アドレスに基づいてマルチキャスト転送を実行します。
- Optimized Multicast Flooding (OMF) により、未知のトラフィックをルータだけに転送して、データに基づくステート作成を行いません。

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。

このセクションは、次のトピックで構成されています。

IGMPv1 および IGMPv2

IGMPv1 および IGMPv2 は、メンバーシップ レポートの抑制機能をサポートしています。つまり、同じサブネットに属する2つのホストが、同じグループのマルチキャストデータを要求している場合、一方のホストからメンバーレポートを受信した他方のホストで、レポートの送信

が抑制されます。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。

IGMPv3

Cisco NX-OS にはフル機能の IGMPv3 スヌーピングが実装されており、IGMPv3 レポートに含まれる (S、G) 情報に基づいて、フラッドングを制御することができます。この発信元をベースとするフィルタリングにより、マルチキャストグループにトラフィックを送信する発信元に基づくポートのセットにマルチキャストトラフィックを制限するようにスイッチがイネーブルにされます。

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。すべての IGMPv3 ホストがメンバーシップレポートを送信するため、レポート抑制は、スイッチにより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の量を制限します。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。最終メンバー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。

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。

現在は、スイッチ クエリアと IGMP スヌーピング クエリアに対して同じ SVI IP アドレスを設定できます。そうすれば、両方のクエリアが同時にアクティブになって、一般的なクエリーを定期的に VLAN に送信するようになります。これを回避するには、IGMP スヌーピング クエリアとスイッチ クエリアで別々の IP アドレスを使用します。

IGMP スヌーピング フィルタ

Cisco NX-OS リリース 6.0(2)A4(1) は、スヌーピング レイヤでの IGMP パケットのフィルタリングをサポートします。インターフェイス レベルで IGMP スヌーピング レポートを除外できます。このフィルタリングは、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います。ルータは、定義されたプレフィックス リストまたはルート マップ ポリシーとグループを比較し、指定されたアクションを実行します。したがって、指定したプレフィックス リストまたはルート マップ に一致するグループのみが、IGMP スヌーピング レポートにフィルタリングされます。

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。

- PVLAN の IGMP スヌーピングはサポートされていません。
- VLAN 上の IGMPv3 ホストが離脱すると、他のホストでトラフィックがドロップする可能性があります。これは主に、すでに離脱したポートから2回連続して離脱を受信した場合に見られ、これが VLAN 上の他のレシーバに影響を与えます。

この損失を回避するには、**no ip igmp snooping explicit-tracking** コマンドを使用して VLAN 構成で明示的なホスト トラッキングを無効にする必要があります。

例：

```
configure terminal
vlan configuration 10
no ip igmp snooping explicit-tracking
```

- ホップバイホップ トポロジでは、IGMP スヌーピング クエリアではない中間ボックス（2番目のデバイス）で SVI を構成すると、別のダウンストリーム L2 スイッチ（3番目のデバイス）の背後にある他のレシーバポートの1つが離脱を送信すると、その背後にあるホストへのトラフィック損失を引き起こします。これは、v3 抑制が無効になっているためであり、IGMPv3 Leave が 2 番目のデバイスで消費されます。この問題の回避策は次のとおりです。
 - PIM DR と IGMP クエリアは、ホップバイホップ トポロジの同じボックスに同じ場所に配置する必要があります。最初のデバイスの SVI は、DR を 2 番目のデバイスから最初のデバイスにシフトするように **ip pim dr-priority 10** を使用して構成する必要があります。

あり、デフォルトの抑制は2番目のデバイス、3番目のデバイスなどで無効にする必要があります。

- IGMPV3 抑制は、2番目のデバイスや3番目のデバイスなどのすべてのホップで、影響を受ける VLAN の VLAN 構成で有効にする必要があります。

例：

```
configure terminal
vlan configuration 203
ip igmp snooping v3-report-suppression
```

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。

- スイッチ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 スヌーピングのデフォルト設定

次のテーブルでは、IGMP スヌーピングパラメータのデフォルト設定をリスト化しています。

表 1: デフォルト IGMP スヌーピングパラメータ

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
スイッチ全体での IGMPv3 レポート抑制	無効

パラメータ	デフォルト
VLAN ごとの IGMPv3 レポート抑制	有効 (Enabled)



- (注)
- マルチキャスト ルータ ポートを送信元ポートとして SPAN セッションが構成されている場合、送信元ポートに実際に転送されているトラフィックがない場合でも、宛先ポートはすべてのマルチキャスト トラフィックを認識します。これは、マルチキャスト/SPAN 実装の現在の制限によるものです。
 - Cisco Nexus 3548 シリーズ スイッチは、未知のマルチキャスト トラフィックをすべての VLAN のマルチキャスト ルータ ポートに複製しますが、マルチキャスト トラフィックは 1 つの特定の VLAN で受信されます。これはデフォルトの動作であり、構成できません。

IGMP スヌーピングの設定

表 2: IGMP スヌーピング パラメータ

パラメータ	説明
IGMP スヌーピング	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) グローバルな設定が無効になっている場合は、すべての VLAN が有効化されてるかどうか関係なく無効化されていると見なされます。
イベント履歴	IGMP スヌーピング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。
グループ タイムアウト	デバイス上のすべての VLAN のグループ メンバシップ タイムアウトを構成します。
リンクローカル グループ抑制	デバイスのリンクローカル 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。
Optimise-multicast-flood	デバイス上のすべての VLAN で Optimized Multicast Flood (OMF) 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。

パラメータ	説明
プロキシ	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。
レポート抑制	デバイスのマルチキャスト対応ルータに送信されるメンバー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。
IGMPv3 レポート抑制	デバイスの IGMPv3 レポート抑制およびプロキシ レポートを構成します。デフォルトではディセーブルになっています。

手順の概要

1. **configure terminal**
- 2.
3. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的						
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	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	<table border="1"> <thead> <tr> <th>オプション</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>コマンド</td> <td>目的</td> </tr> <tr> <td> ip igmp snooping 例 : <pre>switch(config-vlan-config)# ip igmp snooping</pre> </td> <td>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。</td> </tr> </tbody> </table>	オプション	説明	コマンド	目的	ip igmp snooping 例 : <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。	
	オプション	説明						
	コマンド	目的						
ip igmp snooping 例 : <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。							

コマンドまたはアクション		目的
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。</p> <p>IGMPスヌーピングを無効にすると、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グディングします。</p>	

コマンドまたはアクション		目的
オプション	説明	
ip igmp snooping event-history 例 : <pre>switch(config)# ip igmp snooping event-history</pre>	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 syslog-threshold percentage 例 : <pre>switch(config)# ip igmp snooping syslog-threshold 80</pre>	IGMP スヌーピングテーブルの syslog しきい値を構成します。	
ip igmp snooping link-local-groups-suppression 例 : <pre>switch(config)# ip igmp snooping link-local-groups-suppression</pre>	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 optimise-multicast-flood 例 : <pre>switch(config)# ip igmp snooping optimise-multicast-flood</pre>	デバイス上のすべての VLAN で OMF を最適化します。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 例 : <pre>switch(config)# ip igmp snooping v3-report-suppression</pre>	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、スイッチ全体のグローバルコマンドでディセーブルになっており、VLAN ごとにイネーブルになっています。	
ip igmp snooping report-suppression 例 : <pre>switch(config)# ip igmp snooping 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	

コマンドまたはアクション		目的
オプション	説明	
	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せん。デフォルトではイネーブルになっています。	
ステップ 3	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	設定変更を保存します。

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に影響を与えるには、次の表に示すオプションの IGMP スヌーピングパラメータを構成します。

表 3: IGMP スヌーピングパラメータ

パラメータ	説明
IGMP スヌーピング	VLAN ごとに 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。 グローバルな設定が無効になっている場合は、すべての VLAN が有効化されているかどうか関係なく無効化されていると見なされます。
アクセスグループ	スヌーピングレイヤで IGMP パケットをフィルタ処理します。デフォルトではディセーブルになっています。
明示的な追跡	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。デフォルトではイネーブルになっています。

パラメータ	説明
高速脱退	ソフトウェアが IGMP Leave レポートを受信した場合に、IGMP クエリーメッセージを送信することなく、グループステートを解除できるようにします。このパラメータは、IGMPv2 ホストに関して、各 VLAN ポート上のホストが 1 つしか存在しない場合に使用されます。デフォルトではディセーブルになっています。
最終メンバー クエリ間隔	IGMP クエリーの送信後に待機する時間を設定します。この時間が経過すると、ソフトウェアは、特定のマルチキャストグループについてネットワークセグメント上に受信要求を行うホストが存在しないと見なします。いずれのホストからも応答がないまま、最終メンバーのクエリインターバルの期限が切れると、対応する VLAN ポートからグループが削除されます。有効範囲は 1～25 秒です。デフォルト値は 1 秒です。
Optimise-multicast-flood	指定した VLAN で Optimized Multicast Flood (OMF) 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。
レポート ポリシー	スヌーピングレイヤで IGMP パケットをフィルタ処理します。デフォルトではディセーブルになっています。
スヌーピング クエリア	<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、インターフェイスにスヌーピングクエリアを設定します。</p> <p>スヌーピングクエリアに次の値を構成することもできます。</p> <ul style="list-style-type: none"> • タイムアウト：IGMPv2 のタイムアウト値 • 間隔：クエリ送信間の時間 • 最大応答時間：クエリメッセージの MRT • スタートアップカウント：起動時に送信されるクエリ数 • スタートアップ間隔：起動時のクエリ間隔

パラメータ	説明
堅牢性変数	指定した VLAN のロバストネス値を設定します。
マルチキャスト ルータ	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。
スタティック グループ	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。
リンクローカル グループ抑制	スイッチまたは各 VLAN に対して、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。
バージョン	指定した VLAN の IGMP バージョン番号を設定します。



(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。

手順の概要

1. **configure terminal**
2. **ip igmp snooping**
3. **vlan configuration** *vlan-id*
- 4.
5. (任意) **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	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：	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。

	コマンドまたはアクション	目的										
	switch(config)# ip igmp snooping	(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 <i>vlan-id</i> 例 : <pre>switch(config)# vlan configuration 100 switch(config-vlan-config) #</pre>	VLAN を構成し、VLAN 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	<table border="1"> <thead> <tr> <th>オプション</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>コマンド</td> <td>目的</td> </tr> <tr> <td> ip igmp snooping 例 : <pre>switch(config-vlan-config) # ip igmp snooping</pre> </td> <td>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。</td> </tr> <tr> <td> ip igmp snooping access-group {prefix-list route-map} policy-name interface <i>interface slot/port</i> 例 : <pre>switch(config-vlan-config) # ip igmp snooping access-group prefix-list plist interface ethernet 2/2</pre> </td> <td>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 アクセスグループにフィルタを構成します。</td> </tr> <tr> <td> ip igmp snooping explicit-tracking 例 : <pre>switch(config-vlan-config) # ip igmp snooping explicit-tracking</pre> </td> <td>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 メンバシップ レポートを、VLAN 別に追跡します。デフォルトは、すべ</td> </tr> </tbody> </table>	オプション	説明	コマンド	目的	ip igmp snooping 例 : <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。	ip igmp snooping access-group {prefix-list route-map} policy-name interface <i>interface slot/port</i> 例 : <pre>switch(config-vlan-config) # ip igmp snooping access-group prefix-list plist interface ethernet 2/2</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 アクセスグループにフィルタを構成します。	ip igmp snooping explicit-tracking 例 : <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 メンバシップ レポートを、VLAN 別に追跡します。デフォルトは、すべ	
オプション	説明											
コマンド	目的											
ip igmp snooping 例 : <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。											
ip igmp snooping access-group {prefix-list route-map} policy-name interface <i>interface slot/port</i> 例 : <pre>switch(config-vlan-config) # ip igmp snooping access-group prefix-list plist interface ethernet 2/2</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 アクセスグループにフィルタを構成します。											
ip igmp snooping explicit-tracking 例 : <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 メンバシップ レポートを、VLAN 別に追跡します。デフォルトは、すべ											

コマンドまたはアクション		目的
オプション	説明	
	ての VLAN でイネーブルです。	
ip igmp snooping fast-leave 例 : <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。	
ip igmp snooping last-member-query-interval seconds 例 : <pre>switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3</pre>	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。	
ip igmp snooping link-local-groups-suppression 例 : <pre>switch(config-vlan-config)# ip igmp snooping link-local-groups-suppression</pre>	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。	

コマンドまたはアクション		目的
オプション	説明	
	(注) グローバルコンフィギュレーションモードでこのコマンドを実行し、すべてのインターフェイスを変更することもできます。	
ip igmp snooping mrouter interface interface 例 : <pre>switch(config-vlan-config)# ip igmp snooping mrouter interface ethernet 2/1</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 スロット番号/ポート番号」などのように、タイプと番号でインターフェイスを指定できます。	
ip igmp snooping optimise-multicast-flood 例 : <pre>switch(config-vlan-config)# ip igmp snooping optimise-multicast-flood</pre>	選択された VLAN の OMF を最適化します。デフォルトではイネーブルになっています。	
ip igmp snooping querier ip-address 例 :	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	

コマンドまたはアクション		目的
オプション	説明	
<pre>switch(config-vlan-config)# ip igmp snooping querier 172.20.52.106</pre>	<p>をイネーブルにしている場合、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>	
<p>ip igmp snooping querier-timeout seconds</p> <p>例：</p> <pre>switch(config-vlan-config)# ip igmp snooping 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る場合、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>	
<p>ip igmp snooping query-interval seconds</p> <p>例：</p> <pre>switch(config-vlan-config)# ip igmp snooping 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る場合、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>	
<p>ip igmp snooping report-policy { prefix-list route-map } policy-name interface interface slot/port</p> <p>例：</p> <pre>switch(config-vlan-config)# ip igmp snooping report-policy route-map rmap interface ethernet 2/4</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構成します。</p>	

コマンドまたはアクション		目的
オプション	説明	
ip igmp snooping startup-query-count value 例 : <pre>switch(config-vlan-config)# ip igmp snooping 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うちに、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 例 : <pre>switch(config-vlan-config)# ip igmp snooping 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 を有効にしていないうちに、起動時のスヌーピングクエリー間隔を構成します	
ip igmp snooping robustness-variable value 例 : <pre>switch(config-vlan-config)# ip igmp snooping 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。	
ip igmp snooping static-group group-ip-addr [source source-ip-addr] interface interface 例 : <pre>switch(config-vlan-config)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1</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 などタイプと数でインターフェイスを指定できます。	
ip igmp snooping version value 例 : <pre>switch(config-vlan-config)# ip igmp snooping version 2</pre>	指定した VLAN の IGMP バージョン番号を設定します。	

	コマンドまたはアクション	目的
ステップ 5	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	設定変更を保存します。

IGMP スヌーピング設定の確認

IGMP スヌーピングの設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
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 look-up mode [vlan vlan-id]	VLAN ごとに IGMP スヌーピング ルックアップ モード情報を表示します。
show ip igmp snooping mac-oif [detail vlan vlan-id]	IGMP スヌーピングのスタティック mac oif 情報を VLAN ごとおよびすべての詳細ごとに表示します
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 otv groups [source [group] group [source]] [vlan vlan-id]	VLAN ごとに IGMP スヌーピング OTV 情報を表示します。
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 [vlan vlan-id]	IGMP スヌーピング設定を VLAN 別に表示します。

これらのコマンドからの出力のフィールドに関する詳細は、『[Cisco Nexus 3000 シリーズ マルチキャスト ルーティング コマンドリファレンス](#)』を参照してください。

IGMP スヌーピング統計情報の表示

コマンド	目的
<code>show ip igmp snooping statistics [global vlan <i>vlan-id</i>]</code>	グローバルまたは VLAN ごとのパケットとエラー カウンタの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	目的
<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。

IGMP スヌーピングの設定例

次に、IGMP スヌーピング パラメータの設定例を示します。

```
configure terminal
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 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
```

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。

その他の参考資料

IGMP スヌーピングの実装に関する詳細情報については、次の項目を参照してください。

- [標準](#)
- [関連資料](#)

関連資料

関連項目	マニュアルタイトル
CLI コマンド	Cisco Nexus 3548 スイッチ マルチキャストルーティング コマンドリファレンス

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	-

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。