



IGMP スヌーピングの設定

この章の内容は、次のとおりです。

- [IGMP スヌーピングの情報, 1 ページ](#)
- [IGMP スヌーピング パラメータの設定, 4 ページ](#)
- [IGMP スヌーピングの設定確認, 8 ページ](#)

IGMP スヌーピングの情報

IGMP スヌーピング ソフトウェアは、VLAN 内の IGMP プロトコル メッセージを調べて、このトラフィックの受信に関連のあるホストまたはその他のデバイスに接続されているのはどのインターフェイスかを検出します。IGMP スヌーピングは、インターフェイス情報を使用して、マルチアクセス LAN 環境での帯域幅消費を減らすことができ、これによって VLAN 全体のフラッディングを防ぎます。IGMP スヌーピング機能は、どのポートがマルチキャスト対応ルータに接続されているかを追跡して、IGMP メンバーシップ レポートの転送管理を支援します。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。



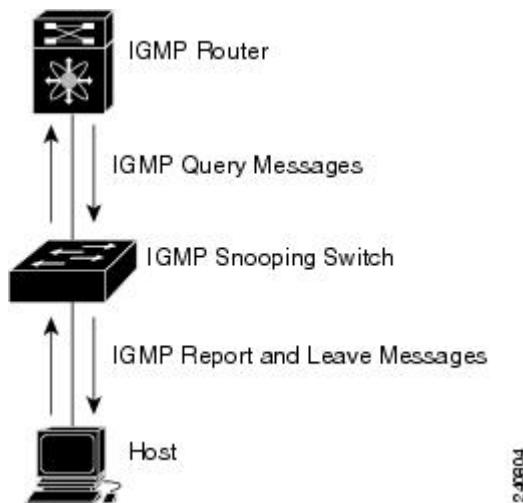
(注)

IGMP スヌーピングは、すべてのイーサネットインターフェイスでサポートされます。スヌーピングという用語が使用されるのは、レイヤ 3 コントロールプレーン パケットが代行受信され、レイヤ 2 の転送決定に影響を与えるためです。

Cisco NX-OS は、IGMPv2 と IGMPv3 をサポートします。IGMPv2 は IGMPv1 をサポートし、IGMPv3 は IGMPv2 をサポートします。以前のバージョンの IGMP のすべての機能がサポートされるわけではありませんが、メンバーシップ クエリーとメンバーシップ レポートに関連した機能はすべての IGMP バージョンについてサポートされます。

次の図に、ホストと IGMP ルータの間に置かれた 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と脱退メッセージをスヌーピングし、それらを必要な場合にだけ、接続されている IGMP ルータに転送します。

図 1: IGMP スヌーピングスイッチ



(注)

スイッチは、宛先マルチキャスト MAC アドレスのみに基づいて IGMPv3 スヌーピングをサポートしています。送信元 MAC 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。

Cisco NX-OS IGMP スヌーピング ソフトウェアは、最適化されたマルチキャスト フラッディング (OMF) をサポートします。これは、不明トライフィックをルータだけに転送し、データ駆動の状態生成は一切実行しません。IGMP スヌーピングの詳細については、<http://tools.ietf.org/wg/magma/draft-ietf-magma-snoop/rfc4541.txt>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)

高速脱退機能をイネーブルにすると、残っているホストのチェックを行わないため、Cisco NX-OS は、最後のメンバクエリーの間隔の設定を無視します。

IGMPv3

スイッチ上の IGMPv3 スヌーピングの実装は、アップストリームマルチキャストルータが送信元に基づいたフィルタリングを行えるように、IGMPv3 レポートを転送します。

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。この明示的な追跡機能は、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、レポート抑制機能によって、スイッチが他のマルチキャスト対応ルータに送信するトラフィックの量が制限されます。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

クエリーを発生させる VLAN 内にマルチキャストルータが存在しない場合、IGMP スヌーピング クエリアを設定して、メンバーシップ クエリーを送信させる必要があります。

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。

IGMP 転送

Cisco Nexus デバイスのコントロールプレーンは、IP アドレスを検出できますが、転送は MAC アドレスだけを使用して発生します。

スイッチに接続されているホストは、IP マルチキャストグループに参加する場合に、参加する IP マルチキャスト グループを指定して、要求されていない IGMP 参加メッセージを送信します。それとは別に、スイッチは、接続されているルータから一般クエリーを受信したら、そのクエリー

を、物理インターフェイスか仮想インターフェイスかにかかわらず、VLAN内のすべてのインターフェイスに転送します。マルチキャストグループに参加するホストは、スイッチに参加メッセージを送信することにより応答します。スイッチのCPUが、そのグループ用のマルチキャスト転送テーブルエントリを作成します（まだ存在しなかった場合）。また、CPUは、参加メッセージを受信したインターフェイスを、転送テーブルの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。

ルータは定期的にマルチキャスト一般クエリーを送信し、スイッチはそれらのクエリーを VLAN 内のすべてのポート経由で転送します。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。スイッチは、そのマルチキャストグループの転送テーブルにリストされているホストだけに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ときには、ホストは、通知なしで脱退することもできれば、脱退メッセージを送信することもできます。スイッチは、ホストから脱退メッセージを受信したら、グループ固有の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その他のデバイスの中に、そのマルチキャスト グループの トラフィックを受信するものがあるかどうかを調べます。スイッチはさらに、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。

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管理するには、次の表で説明する、省略可能なIGMP スヌーピング パラメータを設定します。

表 1: **IGMP スヌーピング パラメータ**

パラメータ	説明
IGMP snooping	VLAN ごとに IGMP スヌーピングをイネーブルにします。デフォルトはイネーブルです。 (注) グローバルな設定がディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。
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。デフォルトはイネーブルです。

パラメータ	説明
Fast leave	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なります。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。デフォルトはディセーブルです。
Last member query interval	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、最終メンバのクエリーア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。デフォルトは 1 秒です。
Snooping querier	クエリーを生成するマルチキャスト ルータが VLAN 内に存在しない場合に、インターフェイスのスヌーピング クエリアを設定します。デフォルトはディセーブルです。
Report suppression	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。デフォルトはイネーブルです。
Multicast router	マルチキャスト ルータへのスタティックな接続を設定します。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。

パラメータ	説明
Multicast router vpc-peer-link	<p>仮想ポートチャネル (vPC) ピアリンクへのスタティック接続を設定します。</p> <p>デフォルトでは、vPC ピアリンクは、マルチキャストルータポートと見なされ、マルチキャストパケットは、各レシーバ VLAN のピアリンクに送信されます。</p> <p>孤立ポートを持つ各レシーバ VLAN に vPC ピアリンク上でマルチキャスト トラフィックを送信するには、no ip igmp snooping mrouter vpc-peer-link コマンドを使用します。no ip igmp snooping mrouter vpc-peer-link コマンドを使用する場合、VLAN に孤立ポートがない限り、マルチキャスト トラフィックは、送信元 VLAN とレシーバ VLAN のピアリンクに送信されません。また、IGMP スヌーピング mrouter vPC ピアリンクをピア VPC スイッチでグローバルにディセーブルにします。</p>
Static group	VLAN に属するインターフェイスを、マルチキャストグループのスタティック メンバとして設定します。

IGMP スヌーピングは、グローバルにも、特定の VLAN に対してだけでもディセーブルにできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# 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 2	switch(config)# ip igmp snooping	<p>IGMP スヌーピングをグローバルにイネーブルにします。デフォルトはイネーブルです。</p> <p>(注) グローバルな設定がディセーブルになっている場合は、すべての VLAN が、イネーブルかどうかに関係なくディセーブルと見なされます。</p>
ステップ 3	switch(config)# vlan configuration vlan-id	VLAN 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	switch(config-vlan)# 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。デフォルトはイネーブルです。 (注) IGMP スヌーピングがグローバルにイネーブル になっている場合は、このコマンドは必要あ りません。
ステップ 5	switch(config-vlan)# 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。
ステップ 6	switch(config-vlan)# 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。
ステップ 7	switch(config-vlan)# ip igmp snooping last-member-query-interval seconds	いずれのホストからも IGMP クエリーメッセージへの応 答がないままで、最終メンバのクエリーアンダーバルの期 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 は 1 秒です。
ステップ 8	switch(config-vlan)# ip igmp snooping querier IP-address	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 ナーピング クエリーアrea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。デフォルトはディ セーブルです。
ステップ 9	switch(config-vlan)# 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でマルチキャスト対応ルータに送信されます。デフォ ルトはイネーブルです。
ステップ 10	switch(config-vlan)# ip igmp snooping mrouter interface interface	マルチキャストルータへのスタティックな接続を設定し 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。インターフェイ スは、タイプと番号で指定できます。
ステップ 11	switch(config-vlan)# ip igmp snooping mrouter vpc-peer-link	仮想ポート チャネル (vPC) ピアリングへのスタティッ ク接続を設定します。デフォルトでは、vPC ピアリン グはマルチキャストルータ ポートと見なされ、マルチ

	コマンドまたはアクション	目的
		キャストパケットが各レシーバ VLAN のピアリンクに送信されます。孤立ポートを持つ各レシーバ VLAN に vPC ピアリンク上でマルチキャストトラフィックを送信するには、 no ip igmp snooping mrouter vpc-peer-link コマンドを使用します。また、IGMP スヌーピング mrouter vPC ピアリンクをピア VPC スイッチでグローバルにディセーブルにします。
ステップ 12	switch(config-vlan)# ip igmp snooping static-group group-ip-addr [source source-ip-addr] interface interface	VLAN に属するインターフェイスを、マルチキャストグループのスタティックメンバとして設定します。インターフェイスは、タイプと番号で指定できます。

次に、VLAN の IGMP スヌーピング パラメータを設定する例を示します。

```
switch# configure terminal
switch(config)# vlan configuration 5
switch(config-vlan)# ip igmp snooping last-member-query-interval 3
switch(config-vlan)# ip igmp snooping querier 172.20.52.106
switch(config-vlan)# ip igmp snooping explicit-tracking
switch(config-vlan)# ip igmp snooping fast-leave
switch(config-vlan)# ip igmp snooping report-suppression
switch(config-vlan)# ip igmp snooping mrouter interface ethernet 1/10
switch(config-vlan)# ip igmp snooping mrouter vpc-peer-link
switch(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 1/10
switch(config-vlan)# end
```

次に、vPC ピアリンクへのスタティックな接続を設定する例と、vPC ピアリンクへのスタティックな接続を削除する例を示します。

```
switch(config)# ip igmp snooping mrouter vpc-peer-link
switch(config)# no ip igmp snooping mrouter vpc-peer-link
Warning: IGMP Snooping mrouter vpc-peer-link should be globally disabled on peer VPC switch
as well.
switch(config)#
```

IGMP スヌーピングの設定確認

IGMP スヌーピングの設定を確認するには、次のコマンドを使用します。

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 [[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。

コマンド	説明
show ip igmp snooping querier [[vlan] <i>vlan-id</i>]	IGMP スヌーピング クエリアを VLAN 別に表示します。
show ip igmp snooping mrouter [[vlan] <i>vlan-id</i>]	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 <i>vlan-id</i>	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。

次に、IGMP スヌーピング パラメータを確認する例を示します。

```
switch# show ip igmp snooping
Global IGMP Snooping Information:
  IGMP Snooping enabled
  IGMP Snooping information for vlan 1
    IGMP snooping enabled
    IGMP querier none
    Switch-querier disabled
    Explicit tracking enabled
    Fast leave disabled
    Report suppression enabled
    Router port detection using PIM Hellos, IGMP Queries
    Number of router-ports: 0
    Number of groups: 0
  IGMP Snooping information for vlan 5
  IGMP snooping enabled
    IGMP querier present, address: 192.0.2.1, version: 3
    Querier interval: 125 secs
    Querier last member query interval: 10 secs
    Querier robustness: 2
    Switch-querier enabled, address 192.0.2.1, currently running
    Explicit tracking enabled
    Fast leave enabled
    Report suppression enabled
    Router port detection using PIM Hellos, IGMP Queries
    Number of router-ports: 1
    Number of groups: 1
```

