



IGMP スヌーピング

- [Cisco APIC および IGMP スヌーピングについて \(1 ページ\)](#)
- [IGMP スヌーピング ポリシーの設定と割り当て \(5 ページ\)](#)
- [IGMP スヌーピングの静的ポート グループの有効化 \(7 ページ\)](#)
- [IGMP スヌープ アクセス グループの有効化 \(9 ページ\)](#)

Cisco APIC および IGMP スヌーピングについて

ACI ファブリックに IGMP スヌーピングを実装するには



- (注) ブリッジドメインで 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、ブリッジドメイン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、ブリッジドメイン内の IP マルチキャストトラフィックを調べて、該当する受信側が常駐す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、マルチアクセスブリッジドメイン環境における帯域幅消費量を削減し、ブリッジドメイン全体へのフラッディングを回避します。デフォルトでは、IGMP スヌーピングがブリッジドメインでイネーブルにされています。

この図は、ホストへの接続を持つ ACI リーフスイッチに含まれる IGMP ルーティング機能と IGMP スヌーピング機能を示しています。IGMP スヌーピング機能は、IGMP メンバーシップレポートをスヌーピングし、メッセージを残し、必要な場合にのみ IGMP ルータ機能に転送します。

その結果、ACI ファブリックは送信元 IP アドレス 0.0.0.0 の IGMP レポートを送信します。



(注) 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。

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。

リーフスイッチでは、**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。

APIC IGMP スヌーピング機能、IGMPv1、IGMPv2、および高速リーフ機能

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。APIC は、IGMP 脱退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 脱退メッセージが存在しないため、APIC の IGMP スヌーピング機能は、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 タイムアウトを使用する必要があります。



(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、IGMP スヌーピング機能は、最終メンバーのクエリー インターバル設定を無視します。

APIC IGMP スヌーピング ファンクションキーと IGMPv3

APIC での IGMPv3 スヌーピング ファンクションでは、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、抑制されたフラグging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。

デフォルトでは、IGMP スヌーピング機能は、ブリッジドメインでは、各 VLAN ポート上のホストを追跡します。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。レポート抑制を有効にしても、IGMPv1 または IGMPv2 ホストが同じグループをリクエストしなかった場合、IGMP スヌーピング機能はプロキシレポートを作成します。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ブリッジドメイン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、ソフトウェアはメンバーシップクエリーを送信します。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、タイムアウトまでのどのホストからも応答がなかった場合、IGMP スヌーピングはグループステートを削除します。

Cisco APIC および IGMP スヌーピング クエリア関数

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機能を設定する必要があります。APIC、IGMP スヌープポリシー内で定義マルチキャストのソースとレシーバが含まれているブリッジドメインでクエリアがないその他のアクティブなクエリアします。

Cisco ACI はデフォルトで、IGMP スヌーピングが有効になっています。さらに、ブリッジドメインサブネット制御は、「クエリア IP」を選択、リーフスイッチによって、クエリアとして動作およびクエリパケット送信を開始します。セグメントは、明示的なマルチキャストルータ (PIM が有効になっていません) があるときに ACI Leaf スイッチでクエリアを有効にする必要があります。ブリッジドメインで、クエリアが設定されている、使用される IP アドレスマルチキャストのホストが設定されている同じサブネットからに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。

APIC IGMP スヌーピング機能の注意事項と制約事項

APIC IGMP スヌーピング機能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、着信ブリッジ ドメインでフラッディングされます。
- IGMPv3 スヌーピングは、ブリッジ ドメインで PIM が有効になっている場合にのみ、グループと送信元エントリに基づいてマルチキャストを転送します。PIM が有効になっていない場合、転送はグループのみに基づいて行われます。

IGMP スヌーピング ポリシーの設定と割り当て

拡張 GUI のブリッジ ドメインへの IGMP スヌーピング ポリシーの設定と割り当て

IGMP スヌーピング機能を実装するには、IGMP スヌーピングポリシーを設定し、そのポリシーを1つまたは複数のブリッジ ドメインに割り当てます。

GUI を使用した IGMP スヌーピング ポリシーの設定

IGMP 設定を1つまたは複数のブリッジ ドメインに割り当てることが可能な IGMP スヌーピングポリシーを作成します。

手順

- ステップ 1 [テナント] タブと、IGMP スヌーピング サポートを設定することを意図したブリッジ ドメインのテナントの名前をクリックします。
- ステップ 2 [ナビゲーション (Navigation)] ペインで、[ポリシー (Policies)] > [プロトコル (Protocol)] > [IGMP スヌープ (IGMP Snoop)] をクリックします。
- ステップ 3 [IGMP スヌープ] を右クリックし、[IGMP スヌープ ポリシーの作成] を選択します。
- ステップ 4 **Create IGMP Snoop Policy** ダイアログで、次のようにポリシーを設定します。
 - a) [Name] フィールドと [Description] フィールドに、ポリシーの名前と説明をそれぞれ入力します。
 - b) [管理状態 (Admin State)] フィールドで [有効化 (Enables)] または [無効化 (Disabled)] を選択して、この特定のポリシーの IGMP スヌーピングを有効または無効にします。
 - c) [ファスト リーブ (Fast Leave)] を選択または選択解除し、このポリシーを通してクエリが即時ドロップする IGMP V2 を有効または無効にします。

- d) [クエリアの有効化 (Enable querier)] を選択して、このポリシーを通して IGMP クエリア アクティビティを有効または無効にします。
- (注) このオプションを効果的に有効にするには、ポリシーを適用するブリッジドメインに割り当てられるサブネットで [サブネット制御: クエリア IP] 設定も有効にする必要があります。この設定のプロパティ ページへのナビゲーションパスは次のとおりです。[テナント (Tenants)] > [tenant_name] > [ネットワーク (Networking)] > [ブリッジドメイン (Bridge Dmains)] > [bridge_domain_name] > [サブネット (Subnets)] > [subnet_subnet]
- e) [クエリア バージョン (Querier Version)] フィールドで、[バージョン 2 (Version 2)] または [バージョン 3 (Version 3)] を選択して、この特定のポリシーの IGMP スヌーピング クエリア バージョンを選択します。
- f) このポリシーの [最後のメンバのクエリ間隔] 値を秒で指定します。
- IGMPv2 リーブ レポートを受信したら、IGMP がこの値を使用します。これは、少なくとも 1 個以上のホストをグループに残すことを意味します。リーブ レポートを受信した後、インターフェイスが IGMP ファスト リーブに設定されていないか確認し、されていない場合は out-of-sequence クエリを送信します。
- g) このポリシーの [クエリ間隔] 値を秒で指定します。
- この値は、グループ内でレポートを確認できない場合、IGMP 機能が特定の IGMP 状態を保存する合計時間を定義するために使用されます。
- h) このポリシーの [クエリの応答間隔] 値を秒で指定します。
- ホストがクエリ パケットを受信すると、最大応答所要時間以下のランダムな値でカウントが開始されます。このタイマーの期限が切れると、ホストはレポートで応答します。
- i) このポリシーの [クエリ カウントの開始] を指定します。
- スタートアップクエリー インターバル中に送信される起動時のクエリー数。有効範囲は 1 ~ 10 です。デフォルトは 2 です。
- j) このポリシーの [クエリ間隔の開始] を秒で指定します。
- デフォルトでは、ソフトウェアができるだけ迅速にグループ ステートを確立できるように、このインターバルはクエリー インターバルより短く設定されています。有効範囲は 1 ~ 18,000 秒です。デフォルト値は 31 秒です。

ステップ 5 [送信 (Submit)] をクリックします。

新しい IGMP スヌープ ポリシーは、[プロトコル ポリシー - IGMP スヌープ] サマリ ページに一覧になっています。

次のタスク

このポリシーを有効にするには、ブリッジドメインに割り当てます。

GUI を使用した IGMP スヌーピング ポリシーのブリッジ ドメインへの割り当て

IGMP スヌーピング ポリシーをブリッジ ドメインに割り当てると、そのブリッジ ドメインは、そのポリシーで指定された IGMP スヌーピング ポリシーを使用するように設定されます。

始める前に

- テナントのブリッジ ドメインを設定します。
- ブリッジ ドメインにアタッチする IGMP スヌーピング ポリシーを設定します。



(注) 割り当てられるポリシーで **Enable Querier** オプションを効果的に有効にするには、ポリシーを適用するブリッジ ドメインに割り当てられるサブネットで **Subnet Control: Querier IP** 設定も有効にする必要があります。この設定があるプロパティ ページへのナビゲーションパスは、**Tenants > tenant_name > Networking > Bridge Domains > bridge_domain_name > Subnets > subnet_name** です。

手順

- ステップ 1** テナントのブリッジ ドメインで IGMP スヌープ ポリシーを設定するには、APIC の **Tenants** タブをクリックして、テナントの名前を選択します。
- ステップ 2** APIC のナビゲーションウィンドウで **Networking > Bridge Domains** をクリックして、ポリシー指定の IGMP スヌープ設定を適用するブリッジ ドメインを選択します。
- ステップ 3** メインの **Policy** タブで、**IGMP Snoop Policy** フィールドまでスクロールして、ドロップダウンメニューから適切な IGMP ポリシーを選択します。
- ステップ 4** **Submit** をクリックします。

ターゲットのブリッジ ドメインは、指定された IGMP スヌーピング ポリシーに関連付けられます。

IGMP スヌーピングの静的ポート グループの有効化

静的ポート グループの IGMP スヌーピングを有効にする

IGMP 静的ポートのグループ化により以前アプリケーション EPG に静的に割り当てられた事前プロビジョニングを有効にして、スイッチ ポートが IGMP マルチキャスト トラフィックを受

信および処理できます。この事前プロビジョニングは、通常 IGMP スヌーピング スタックがポートを動的に学習するときに発生する参加遅延を防止します。

静的グループ メンバーシップは、アプリケーション EPG に割り当てられている静的ポートでのみ事前プロビジョニングできます。

APIC GUI、CLI、および REST API インターフェイスを通じて、静的グループ メンバーシップを設定できます。

前提条件: 静的ポートに EPG を導入する

ポートで IGMP スヌーピング処理を有効にするには、前提条件として、ターゲットのポートを、関連付けられている EPG に静的に割り当てる必要があります。

ポートの静的な導入は、APIC GUI、CLI、または REST API インターフェイスを通じて構成できます。詳細については、『Cisco APIC レイヤ 2 ネットワーキング設定ガイド』の次のトピックを参照してください：

- GUI を使用して特定のノードまたはポートへ EPG を導入する
- NX-OS スタイルの CLI を使用した APIC の特定のポートへの EPG の導入
- REST API を使用した APIC の特定のポートへの EPG の導入

GUI を使用した、スタティック ポートでの IGMP スヌーピングとマルチキャストの有効化

IGMP スヌーピングとマルチキャストは、EPG に静的に割り当てられているポートで有効にできます。その後、これらのポートで有効にされている IGMP スヌーピングとマルチキャストへのアクセスを許可または拒否されるユーザのアクセスグループを作成し、割り当てることができます。

始める前に

EPG の IGMP スヌーピングおよびマルチキャストを有効にする前に、次のタスクを実行します：

- この機能を有効にし、その EPG に静的に割り当てるインターフェイスを指定します。



(注) スタティック ポートの割り当てに関する詳細は、『Cisco APIC レイヤ 2 ネットワーキング設定ガイド』の「GUI を使用した特定のノードまたはポートで EPG を展開する」を参照してください。

- IGMP スヌーピングとマルチキャスト トラフィックの受信者とする IP アドレスを指定します。

手順

ステップ 1 **Tenant** > *tenant_name* > **Application Profiles** > *application_name* > **Application EPGs** > *epg_name* > **Static Ports** をクリックします。

このスポットに移動すると、ターゲット EPG に静的に割り当てたすべてのポートが表示されます。

ステップ 2 IGMP スヌーピングのグループ メンバーに静的に割り当てるポートをクリックします。**Static Path** ページが表示されます。

ステップ 3 IGMP スヌープ スタティック グループの表で、+ をクリックして、IGMP スヌープ アドレス グループにエントリを追加します。

IGMP スヌープ アドレス グループにエントリを追加すると、ターゲットの静的ポートが指定されたマルチキャスト IP アドレスに関連付けられ、そのアドレスで受信した IGMP スヌープ トラフィックを処理できるようになります。

- a) **Group Address** フィールドに、このインターフェイスとこの EPG に関連付けるマルチキャスト IP アドレスを入力します。
- b) 当てはまる場合には、**Source Address** フィールドに、マルチキャスト ストリームの送信元となる IP アドレスを入力します。
- c) **Submit** をクリックします。

設定が完了したら、ターゲットインターフェイスは、それに関連付けられているマルチキャスト IP アドレスに送信される IGMP スヌーピング プロトコル トラフィックを処理できるようになります。

(注) ターゲットのスタティックポートにさらにマルチキャストアドレスを関連付けるには、この手順を繰り返します。

ステップ 4 [Submit] をクリックします。

IGMP スヌープ アクセス グループの有効化

IGMP スヌープ アクセス グループの有効化

「アクセス-グループ」ができるストリームを制御するために使用任意ポート背後に参加します。

実際に所属するポートの設定を適用できることを確認するには、アプリケーション EPG に静的に割り当てられているインターフェイスでアクセス グループ設定を適用できる EPG。

ルート マップ ベースのアクセス グループのみが許可されます。

APIC GUI、CLI、および REST API インターフェイスを通じて、IGMP スヌープ アクセス グループを設定できます。

GUI を使用して、IGMP スヌーピングとマルチキャストへのグループアクセスを有効にする

EPG に静的に割り当てられたポートで IGMP スヌーピングとマルチキャストを有効にしたら、ユーザのアクセスグループを作成して割り当て、それらのポートで有効にされた IGMP スヌーピングとマルチキャスト トラフィックへのアクセスを許可または拒否することができます。

始める前に

EPG に IGMP スヌーピングおよびマルチキャストへのアクセスを有効にする前に、この機能を有効にし、それらを静的に EPG に割り当てるインターフェイスを識別します。



(注) スタティック ポートの割り当てに関する詳細は、『Cisco APIC レイヤ 2 ネットワーキング設定ガイド』の「GUI を使用した特定のノードまたはポートで EPG を展開する」を参照してください。

手順

ステップ 1 [テナント (Tenant)] > [tenant_name] > [アプリケーション プロファイル (Application Profiles)] > [application_name] > [アプリケーション EPG (Application EPGs)] > [epg_name] > [スタティック ポート (Static Ports)] をクリックします。

このスポットに移動すると、ターゲット EPG に静的に割り当てたすべてのポートが表示されます。

ステップ 2 マルチキャスト グループアクセスを割り当てる予定のポートをクリックして、**Static Port Configuration** ページを表示します。

ステップ 3 [アクション (Actions)] > [IGMP アドレス グループの作成 (Create IGMP Access Group)] をクリックして、IGMP スヌープ アクセス グループ テーブルを表示します

ステップ 4 IGMP スヌープ アクセス グループのテーブルで + をクリックして、アクセスグループのエントリを追加します。

IGMP スヌープ アクセスグループのエントリを追加すると、このポートへのアクセス権を持つユーザグループを作成すること、それをマルチキャスト IP アドレスと関連付け、そのアドレスで受信された IGMP スヌープ トラフィックへのグループアクセスを許可または拒否することができます。

a) [マルチキャスト向けルートマップポリシーの作成 (Create Route Map Policy for Multicast)] を選択して、[マルチキャスト向けルートマップポリシーの作成 (Create Route Map Policy for Multicast)] ウィンドウを表示します。

- b) **Name** フィールドで、マルチキャスト トラフィックの許可または拒否の対象となるグループの名前を割り当てます。
- c) **Route Maps** テーブルで、+ をクリックして、ルート マップ ダイアログを表示します。
- d) **Order** フィールドでは、このインターフェイスに対して複数のアクセスグループを設定している場合に、このインターフェイスでのマルチキャスト トラフィックへのアクセスをどの順序で許可または拒否するかを反映する番号を選択します。番号の小さいアクセスグループの方が、番号の大きいアクセスグループよりも前の順番になります。
- e) **Group IP** フィールドには、このアクセスグループに対してトラフィックが許可または阻止される、マルチキャスト IP アドレスを入力します。
- f) **Source IP** フィールドでは、当てはまる場合に、送信元の IP アドレスを入力します。
- g) **Action** フィールドでは、ターゲットグループのアクセスを拒否する場合には **Deny** を、ターゲットグループのアクセスを許可する場合には **Permit** を選択します。
- h) [OK] をクリックします。
- i) [送信 (Submit)] をクリックします。

設定が完了すると、設定されている IGMP のスヌープアクセスグループは、ターゲットの静的ポートと、そのアドレスで受信したマルチキャストストリームへの許可または拒否アクセスを通して、マルチキャスト IP アドレスに割り当てられます。

- (注)
- その他のアクセスグループを設定し、ターゲットの静的ポートを通してマルチキャスト IP アドレスに関連付けるには、この手順を繰り返します。
 - 構成されているアクセスグループの設定を確認するには、[テナント (Tenant)]> [tenant_name]> [ポリシー (Policies)]> [プロトコル (Protocol)]> [マルチキャスト向けルートマップ (Route Maps for Multicast)]> [route_map_access_group_name] を選択します。

ステップ 5 [Submit] をクリックします。

■ GUI を使用して、IGMP スヌーピングとマルチキャストへのグループ アクセスを有効にする

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。