IGMP スヌーピング

この章の内容は、次のとおりです。

Cisco APIC および IGMP スヌーピングについて

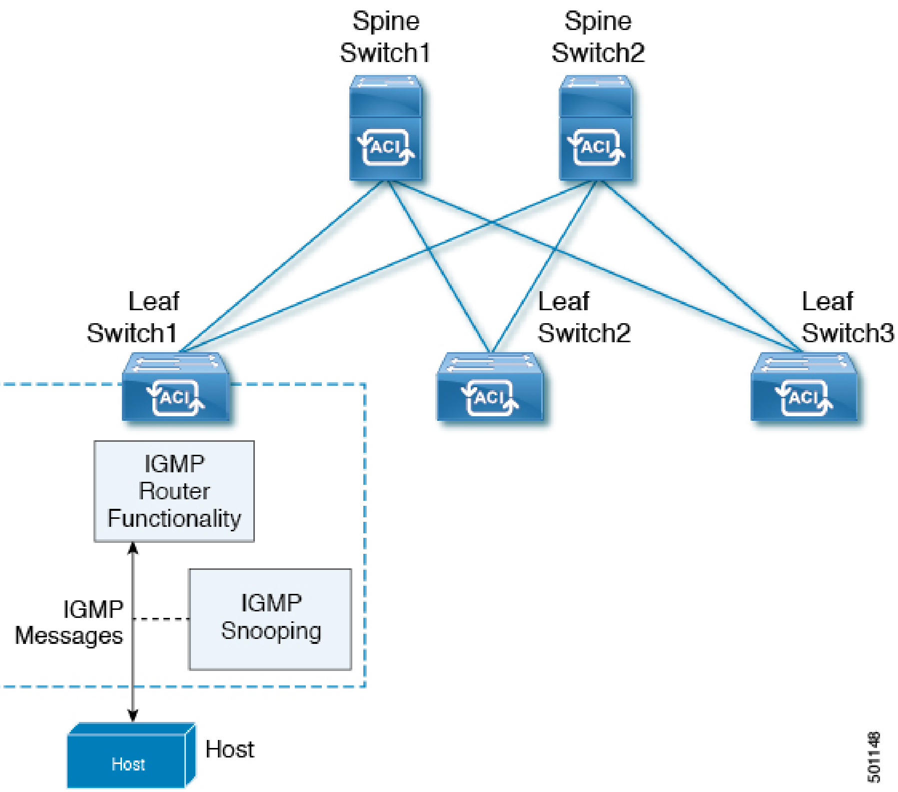
ACI ファブリックに IGMP スヌーピングを実装するには

（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。

図 *1 : IGMP* スヌーピング機能



IGMP スヌーピングは、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。

IGMP スヌーピングには、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

ACI ファブリックは、RFC 4541の2.1.1 項「IGMP 転送ルール」に記載されているガイドラインに従って、プロキシ レポーティング モードでのみ IGMP スヌーピングをサポートします。

IGMP □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□ □□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□
□□□□□□□□□□□□□□□□□□□□□□□ IP □□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□ □□□□□□□□□ IGMP □□□□□□□ □□□□□□
□□□ IP □□□□□ 0.0.0.0 □□□□□□□□□□□□□□□□□□□□□□□□□

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、および高速リーブ機能

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。

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いても、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、タイムアウトまでに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、IGMP スヌーピングおよび IGMP スヌーピング クエリアを有効になっている by default(デフォルトで、デフォルトでは) があります。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) があるないときに 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。

一意の IP アドレスは、簡単にクエリア機能を参照するように設定する必要があります。IGMP スヌーピング クエリア設定の一意の IP アドレスを使用して、ホスト IP アドレスまたは同じセグメント上にあるルータの IP アドレスが重複しないようにする必要があります。クエリア IP アドレスとして SVI IP アドレスを使用する必要がないか、クエリア選定の問題になります。例として、IGMP スヌーピング クエリアを使用する IP アドレスが、セグメント上の別のルータにも使用されている場合があります、IGMP クエリア選定プロトコルの問題。クエリア機能に使用される IP アドレスも使用しないでください HSRP または VRRP などの他の機能です。

（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。

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、IGMPP 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]** ペインで、**[ネットワー キング]** > **[プロトコル ポリシー]** > **[IGMP スヌープ]** 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 **[IGMP スヌープ ポリシーの作成]** 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]** フィールドで **[有効]** または **[無効]** を選択して、このポリシー全体を有効または無効にします。

c) **[ファスト リーブ]** 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]** を選択または選択解除して、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を有効にするには、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。

e) 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。

f) 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。

g) 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。

h) 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。

i) 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 [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。

NX-OS スタイル CLI を使用した IGMP スヌーピング ポリシーの設定とブリッジ ドメインへの割り当て

始める前に

- IGMP スヌーピングのポリシーを消費するテナントを作成します。
- IGMP スヌーピング ポリシーを接続するテナントのブリッジ ドメインを作成します。

手順

	コマンドまたはアクション	目的

ステップ 1	デフォルト値に基づいてスヌーピング ポリシーを作成します。
	例：
	apic1(config-tenant)# template ip igmp snooping policy cookieCut1
	apic1(config-tenant-template-ip-igmp-snooping)# show run all
	`# Command: show running -config all`
	`tenant foo template ip igmp snooping policy cookieCut1`
	`# Time: Thu Oct 13 18:26:03 2016`
	`tenant t_10`
	`template ip igmp snooping policy cookieCut1`
	`ip igmp snooping`
	`no ip igmp snooping fast-leave`
	`ip igmp snooping last-member-query-interval 1`
	`no ip igmp snooping querier`
	`ip igmp snooping query-interval 125`
	`ip igmp snooping query-max-response-time 10`
	`ip igmp snooping stqrtup-query-count 2`
	`ip igmp snooping startup-query-interval 31`
	`no description`
	`exit`
	`exit`
	`apic1(config-tenant-template-ip-igmp-snooping)#`
		例の NX-OS スタイル CLI シーケンス：
		• デフォルト値を持つ cookieCut1 という名前の IGMP スヌーピング ポリシーを作成します。
		• ポリシー cookieCut1 のデフォルト IGMP スヌーピングの値が表示されます。

ステップ 2	必要に応じてスヌーピング ポリシーを変更します。
	例：
	apic1(config-tenant-template-ip-igmp-snooping)# ip igmp snooping query-interval 300
	apic1(config-tenant-template-ip-igmp-snooping)# show run all
	`# Command: show running -config all`
	`tenant foo template ip igmp snooping policy cookieCut1`
	`#Time: Thu Oct 13 18:26:03 2016`
	`tenant foo`
	`template ip igmp snooping policy cookieCut1`
	`ip igmp snooping`
	`no ip igmp snooping fast-leave`
	`ip igmp snooping last-member-query-interval 1`
	`no ip igmp snooping querier`
		例の NX-OS スタイル CLI シーケンス：
		• cookieCut1 という名前の IGMP スヌーピング ポリシーのクエリ間隔値のカスタム値を指定します。
		• ポリシー cookieCut1 の変更された IGMP スヌーピング値を確認します。

	コマンドまたはアクション	目的

	`ip igmp snooping query-interval 300`
	`ip igmp snooping query-max-response-time 10`
	`ip igmp snooping stqrtup-query-count 2`
	`ip igmp snooping startup-query-interval 31`
	`no description`
	`exit`
	`exit`
	`apic1(config-tenant-template-ip-igmp-snooping)# exit`
	`apic1(config--tenant)#`	

ステップ 3	ブリッジ ドメインにポリシーを割り当てます。 **例：** **`apic1(config-tenant)# int bridge-domain bd3`** **`apic1(config-tenant-interface)# ip igmp snooping policy cookieCut1`**	例の NX-OS スタイル CLI シーケンス： • ブリッジ ドメインの BD3 に移動します。IGMP スヌーピング ポリシーのクエリ間隔値は cookieCut1 という名前です。 • ポリシー cookieCut1 の変更された IGMP スヌーピングの値を持つ IGMP スヌーピングのポリシーを割り当てます。

次のタスク

複数のブリッジ ドメインに IGMP スヌーピングのポリシーを割り当てることができます。

REST API を使用したブリッジ 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

手順

IGMP スヌーピング ポリシーを設定してブリッジ ドメインに割り当てるには、次の例のように XML で POST を送信します。

例：

```
https://apic-ip-address/api/node/mo/uni/.xml
<fvTenant name="mcast_tenant1">

<!-- Create an IGMP snooping template, and provide the options -->
<igmpSnoopPol name="igmp_snp_bd_21"
              adminSt="enabled"
              lastMbrIntvl="1"
              queryIntvl="125"
              rspIntvl="10"
```

```
              startQueryCnt="2"
              startQueryIntvl="31"
              />
<fvCtx name="ip_video"/>

<fvBD name="bd_21">
  <fvRsCtx tnFvCtxName="ip_video"/>

  <!-- Bind IGMP snooping to a BD -->
  <fvRsIgmpsn tnIgmpSnoopPolName="igmp_snp_bd_21"/>
</fvBD></fvTenant>
```

この例では、次のプロパティで IGMP スヌーピング ポリシー、igmp_snp_bd_12 を作成および設定し、IGNPポリシー、igmp_snp_bd_12 をブリッジ ドメイン bd_21 にバインドします。

- 管理状態が有効です。
- 最後のメンバ クエリ間隔は、デフォルトでは、1 秒です。
- クエリ間隔は、デフォルトでは 125 です。
- クエリの応答間隔はデフォルトでは 10 秒です。
- クエリの開始カウントは、デフォルトでは 2 メッセージです。
- クエリの開始間隔は 35 秒です。

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スヌープ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 に静的に割り当てられ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。`

NX-OS スタイル CLI によりスタティック ポートで IGMP スヌーピングおよびマルチキャストの有効化

EPG に静的に割り当てられたポートで IGMP スヌーピングおよびマルチキャストをイネーブルにできます。それらのポートで有効な IGMP スヌーピングおよびマルチキャスト トラフィックへのアクセスを許可または拒否するアクセスユーザーのグループを作成および割り当てることができます。

このタスクで説明されている手順には、次のエンティティの事前設定を前提とします。

- テナント：tenant_A
- アプリケーション：application_A
- EPG：epg_A
- ブリッジ ドメイン：bridge_domain_A
- vrf：vrf_A -- a member of bridge_domain_A
- VLAN ドメイン：vd_A（300 ～ 310 の範囲で設定される）
- リーフ スイッチ：101 およびインターフェイス 1/10

  スイッチ 101 のターゲット インターフェイス 1/10 が VLAN 305 に関連付けられており、enant_A、application_A、epg_A に静的にリンクされています。
- リーフ スイッチ：101 およびインターフェイス 1/11

  スイッチ 101 のターゲット インターフェイス 1/11 が VLAN 309 に関連付けられており、enant_A、application_A、epg_A に静的にリンクされています。

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て静的に EPG に割り当てるインターフェイスを特定する

（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「*NX-OS* スタイル *CLI* を使用した *APIC* で特定のポートの *EPG* を展開する」を参照してください。

- IGMP スヌーピング マルチキャスト トラフィックの受信者の IP アドレスを特定します。

手順

	コマンドまたはアクション	目的

ステップ 1	ターゲット インターフェイスで IGMP スヌーピングおよびレイヤ2マルチキャスティングを有効にします
	例：
	`apic1# conf t`
	`apic1(config)# tenant tenant_A`
	`apic1(config-tenant)# application application_A`
	`apic1(config-tenant-app)# epg epg_A`
	`apic1(config-tenant-app-epg)# ip igmp snooping static-group 225.1.1.1 leaf 101 interface ethernet 1/10 vlan 305`
	`apic1(config-tenant-app-epg)# end`
	
	`apic1# conf t`
	`apic1(config)# tenant tenant_A; application application_A; epg epg_A`
	`apic1(config-tenant-app-epg)# ip igmp snooping static-group 227.1.1.1 leaf 101 interface ethernet 1/11 vlan 309`
	`apic1(config-tenant-app-epg)# exit`
	`apic1(config-tenant-app)# exit`
		例のシーケンスでは次を有効にします。
		• 静的にリンクされているターゲット インターフェイス 1/10 の IGMP スヌーピング、そしてマルチキャスト IP アドレス、225.1.1.1 に関連付けます
		• 静的にリンクされているターゲット インターフェイス 1/11 の IGMP スヌーピング、そしてマルチキャスト IP アドレス、227.1.1.1 に関連付けます

REST API を使用した静的ポートでの IGMP スヌーピングとマルチキャストの有効化

EPG に静的に割り当てられているポートで、IGMP スヌーピングおよびマルチキャスト処理を有効にできます。それらのポートで有効な IGMP スヌープおよびマルチキャスト トラフィックへのアクセスを許可または拒否するアクセス ユーザーのグループを作成および割り当てることができます。

手順

スタティック ポートでアプリケーション EPG を設定するには、それらのポートを IGMP スヌーピングおよびマルチキャスト トラフィックを受信し処理するように有効にして、グループをアクセスに割り当てるかトラフィックへのアクセスを拒否するように割り当て、次の例のように XML で POST を送信します。

次の例では、IGMP スヌーピングが VLAN 202 上の leaf 102 インターフェイス 1/10 で有効になっています。マルチキャスト IP アドレス 224.1.1.1 および 225.1.1. がこのポートに関連付けられます。

例：

```
https://apic-ip-address/api/node/mo/uni/.xml
<fvTenant name="tenant_A">
  <fvAp name="application">
    <fvAEPg name="epg_A">
      <fvRsPathAtt encap="vlan-202" instrImedcy="immediate" mode="regular"
tDn="topology/pod-1/paths-102/pathep-[eth1/10]">
        <!-- IGMP snooping static group case -->
        <igmpSnoopStaticGroup group="224.1.1.1" source="0.0.0.0"/>
        <igmpSnoopStaticGroup group="225.1.1.1" source="2.2.2.2"/>
      </fvRsPathAtt>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

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 **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 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 **Actions** > **Create IGMP Snoop 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) **Create Route Map Policy** を選択して、**Create Route Map Policy** 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) **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、**Tenant** > ***tenant_name*** > **Networking** > > **Protocol Policies** > **Route Maps** > ***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。`

NX-OS スタイル CLI を使用した IGMP スヌーピングおよびマルチ キャスト グループへのアクセスの有効化

EPGに静的に割り当てられたポートでIGMPスヌーピングおよびマルチキャストを有効にした後、それらのポートで有効なIGMPスヌーピングおよびマルチキャスト トラフィックへのアクセスを許可または拒否するユーザーのアクセス グループを作成および割り当てできます。

このタスクで説明されている手順には、次のエンティティの事前設定を前提とします。

- テナント：tenant_A
- アプリケーション：application_A
- EPG：epg_A
- ブリッジ ドメイン：bridge_domain_A
- vrf：vrf_A -- a member of bridge_domain_A
- VLAN ドメイン：vd_A（300 ～ 310 の範囲で設定される）
- リーフ スイッチ：101 およびインターフェイス 1/10

  スイッチ 101 のターゲット インターフェイス 1/10 が VLAN 305 に関連付けられており、enant_A、application_A、epg_A に静的にリンクされています。

- リーフ スイッチ：101 およびインターフェイス 1/11

  スイッチ 101 のターゲット インターフェイス 1/11 が VLAN 309 に関連付けられており、enant_A、application_A、epg_A に静的にリンクされています。

（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「*NX-OS* スタイル *CLI* を使用した *APIC* で特定のポートの *EPG* を展開する」を参照してください。

手順

	コマンドまたはアクション	目的

ステップ 1	route-map「アクセス グループ」を定義します。
	例：
	`apic1# conf t`
	`apic1(config)# tenant tenant_A; application application_A; epg epg_A`
	`apic1(config-tenant)# route-map fooBroker permit`
	`apic1(config-tenant-rtmap)# match ip multicast group 225.1.1.1/24`
	`apic1(config-tenant-rtmap)# exit`
	
	`apic1(config-tenant)# route-map fooBroker deny`
	`apic1(config-tenant-rtmap)# match ip multicast group 227.1.1.1/24`
	`apic1(config-tenant-rtmap)# exit`
		例のシーケンスを設定します。
		• マルチキャスト グループ 225.1.1.1/24 にリンクされる Route-map-access グループ「foobroker」のアクセスが許可されています。
		• マルチキャスト グループ 225.1.1.1/24 にリンクされる Route-map-access グループ「foobroker」のアクセスが拒否されています。

ステップ 2	ルート マップ設定を確認します。
	例：
	`apic1(config-tenant)# show running-config tenant test route-map fooBroker`
	`# Command: show running-config tenant test route-map fooBroker`
	`# Time: Mon Aug 29 14:34:30 2016`
	`tenant test`
	`route-map fooBroker permit 10`
	`match ip multicast group 225.1.1.1/24`
	`exit`
	`route-map fooBroker deny 20`
	`match ip multicast group 227.1.1.1/24`
	`exit`
	`exit`	

ステップ 3	アクセス グループ接続パスを指定します。	例のシーケンスを設定します。

	コマンドまたはアクション	目的

	例：
	`apic1(config-tenant)# application application_A`
	`apic1(config-tenant-app)# epg epg_A`
	`apic1(config-tenant-app-epg)# ip igmp snooping access-group route-map fooBroker leaf 101 interface ethernet 1/10 vlan 305`
	`apic1(config-tenant-app-epg)# ip igmp snooping access-group route-map newBroker leaf 101 interface ethernet 1/10 vlan 305`
		• リーフ スイッチ 101、インターフェイス 1/10、VLAN 305 で接続されている Route-map-access グループ「foobroker」。
		• リーフ スイッチ 101、インターフェイス 1/10、VLAN 305 で接続されている Route-map-access グループ「newbroker」。

ステップ 4	アクセスグループ接続を確認します。
	例：
	`apic1(config-tenant-app-epg)# show run # Command: show running-config tenant tenant_A application application_A epg epg_A`
	`# Time: Mon Aug 29 14:43:02 2016`
	`tenant tenent_A`
	`application application_A`
	`epg epg_A`
	`bridge-domain member bridge_domain_A`
	
	`ip igmp snooping access-group route-map fooBroker leaf 101 interface ethernet 1/10 vlan 305`
	`ip igmp snooping access-group route-map fooBroker leaf 101 interface ethernet 1/11 vlan 309`
	`ip igmp snooping access-group route-map newBroker leaf 101 interface ethernet 1/10 vlan 305`
	`ip igmp snooping static-group 225.1.1.1 leaf 101 interface ethernet 1/10 vlan 305`
	`ip igmp snooping static-group 225.1.1.1 leaf 101 interface ethernet 1/11 vlan 309`
	`exit`
	`exit`
	`exit`	

IGMP スヌーピングを REST API を使用するマルチ キャスト グループのアクセスを有効化

IGMP を有効にした後にスヌーピングおよび、EPG に静的に割り当てられているポートでマルチキャストすることができますし、作成を許可または IGMP スヌーピングへのアクセスを拒否するユーザのアクセスのグループを割り当てるおよびマルチキャスト トラフィックは、これらのポートで有効になっています。

手順

アクセスグループを定義する `F23broker` 、送信 XML で post このような次の例のよ。

例は、設定アクセスグループ `F23broker` tenant_A、Rmap_A、application_A、リーフ 102、1/10、インターフェイス VLAN 202 で、epg_A に関連付けられている。Rmap_A、アクセスグループとの関連付けによって `F23broker` マルチキャスト アドレス 226.1.1.1/24 で受信したマルチキャスト トラフィックへのアクセスがあり、マルチキャスト アドレス 227.1.1.1/24 で受信したトラフィックへのアクセスは拒否されます。

例：

```
<!-- api/node/mo/uni/.xml --> <fvTenant name="tenant_A"> <pimRouteMapPol name="Rmap_A">
<pimRouteMapEntry action="permit" grp="226.1.1.1/24" order="10"/> <pimRouteMapEntry action="deny"
grp="227.1.1.1/24" order="20"/> </pimRouteMapPol> <fvAp name="application_A"> <fvAEPg
name="epg_A"> <fvRsPathAtt encap="vlan-202" instrImedcy="immediate" mode="regular"
tDn="topology/pod-1/paths-102/pathep-[eth1/10]"> <!-- IGMP snooping access group case -->
<igmpSnoopAccessGroup name="F23broker"> <igmpRsSnoopAccessGroupFilterRMap
tnPimRouteMapPolName="Rmap_A"/> </igmpSnoopAccessGroup> </fvRsPathAtt> </fvAEPg> </fvAp>
</fvTenant>
```