IGMP スヌーピング

Cisco APIC および IGMP スヌーピングについて

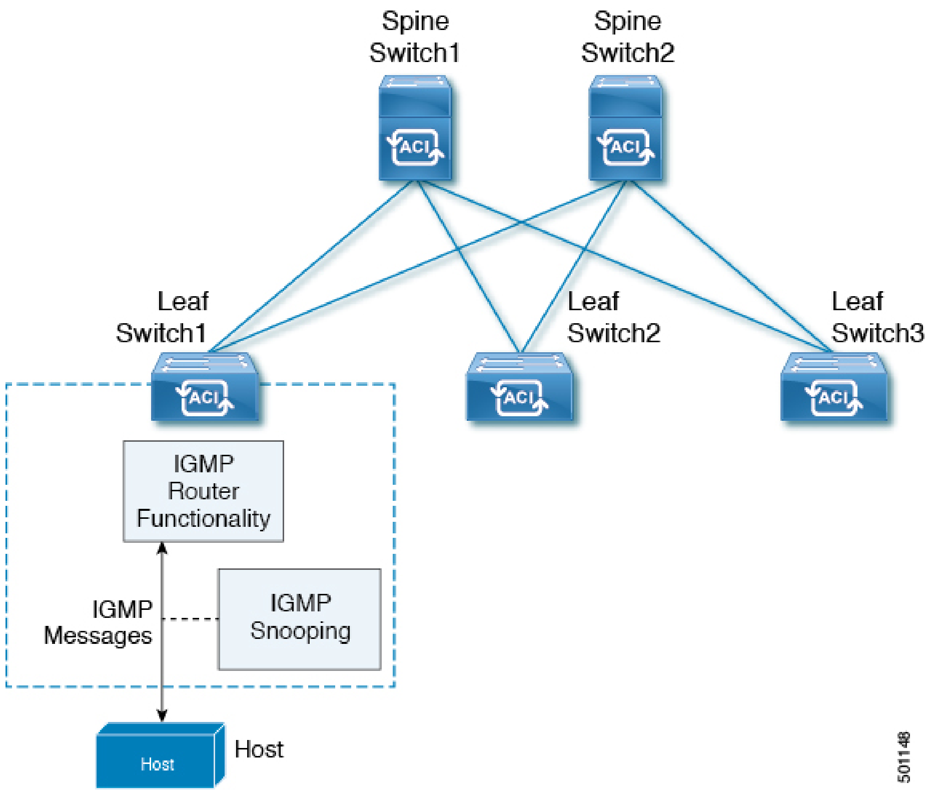
ACI ファブリックに IGMP スヌーピングを実装するには

（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。

（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（Tenants）]** 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（IGMP Snoop）]** を右クリックして、**[IGMP スヌープ ポリシーを作成（Create IGMP Snoop Policy）]**を選択します。

ステップ 4 **[IGMP スヌープ ポリシーを作成（Create IGMP Snoop Policy）]** ダイアログ内で次のようにポリシーを構成します：

a) **[名前（Name）]** と **[説明（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（Enabled）]** または **[無効（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（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 **[テナント（Tenants）]** > ***[tenant_name]*** > **[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（Bridge Domains）]** > ***[bridge_domain_name]*** > **[サブネット（Subnets）]** > ***[subnet_name]*** にあります。

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に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 **[最終メンバークエリ間隔（Last Member Query Interva）]** 値を秒単位で指定します。

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 リーブに構成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** 値を秒単位で指定します。

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 **[クエリ応答間隔（Query Response Interval）]** 値を秒単位で指定します。

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 **[開始クエリ数（Start query Count）]** 値を秒単位で指定します。

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 **[スタート クエリ間隔（Start Query Interval）]** を秒単位で指定します。

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（Protocol Policies - IGMP Snoop）]** サマリー ページにリストされています：

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構成されます。

始める前に

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

（注） **[クエリアの有効化（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 **[サブネット制御：クエリア IP（Subnet Control: Querier IP）]** 設定も有効にする必要があります。この設定が所在するプロパティ ページへのナビゲーション パスは、**[テナント（Tenants）]** > ***[tenant_name]*** > **[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（Bridge Domains）]** > ***[bridge_domain_name]*** > **[サブネット（Subnets）]** > ***[subnet_name]*** にあります。

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 ポリシーを構成するには、APIC の **[テナント（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 ナビゲーション ペインで、次をクリックします。**[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（Bridge Domains）]** をクリックし、ポリシー指定の IGMP スヌープ構成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 **[ポリシー（Policy）]** タブで、**[IGMP スヌープ ポリシー（IGMP Snoop Policy）]** フィールドはへ下にスクロールし、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 **[送信（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 ネットワーク構成ガイド*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） 静的割り当てポートの詳細については、 *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 次の例のように *Cisco APIC* レイヤ *2* ネットワーク設定ガイド。

- 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 登録手続きを開始するには、**[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]*** > **[静的ポート（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 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。
このアクションにより、**[静的パス（Static Path）]** ページが表示されます。

ステップ 3 IGMP スヌープ静的グループの表で、 + をクリックしてIGMPスヌープ アドレス グループ 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) **[グループアドレス（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、**[送信元アドレス（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) **[送信（Submit）]**をクリックします。

構成が完了したら、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）
ターゲットの静的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 **[送信（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） 静的割り当てポートの詳細については、*[GUI* を使用して特定のノードまたはポートへ*EPG* を展開する（*Deploying an EPG on a Specific Node or Port Using the GUI*）*]* を参照します。これは、*[Cisco APIC* レイヤ *2* ネットワーク構成ガイド（*Cisco APIC Layer 2 Networking Configuration Guide*）*]*にあります。

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]*** > **[静的ポート（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、**[静的ポート構成（Static Port Configuration）]** ページを表示します。

ステップ 3 IGMPスヌープ アクセス グループのテーブルを表示するために **[アクション（Actions）]** > **[IGMP アクセス グループを作成（Create IGMP Access Group）]** をクリックします。

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) **[マルチキャストの ルート マップ ポリシーの作成（Create Route Map Policy for Multicast）]]** を選択して **[マルチキャストの ルート マップ ポリシーの作成（Create Route Map Policy for Multicast）]]** ウィンドウに表示されます。

b) **[名前（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) **[ルート マップ（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) **[順序（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) **[グループ IP（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) **送信元 IP（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) **[アクション（Action）]** フィールドで、**[拒否（Deny）]** を選択してターゲット グループへのアクセスを拒否または **[許可（Permit）]** を選択してーゲット グループへのアクセスを許可します。

h) **[OK]**をクリックします。

i) **[送信（Submit）]**をクリックします。

構成が完了すると、構成されている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 グループを構成し、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。
- 構成済みのアクセスグループの設定を確認するには、次の場所に をクリックします：**[テナント（Tenant）]** > ***[tenant_name]*** > **[ポリシー（Policy）]** > **[プロトコル（Protocol）]** > **[ルート マップ マルチキャスト（Route Maps for Multicast）]** > ***[route_map_access_group_name]***。

ステップ 5 **[送信（Submit）]**をクリックします。

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。