IGMP スヌーピングを使用したレイヤ 2 マルチキャストの実装

インターネット グループ管理プロトコル（IGMP）スヌーピングは、少なくとも 1 つの関与する受信先を持つセグメントに対してのみにレイヤ 2 でマルチキャスト フローを制限します。このモジュールでは、IGMP スヌーピングの実装方法について説明します。

IGMP スヌーピングの前提条件

IGMP スヌーピングを実装する前に、次の前提条件を満たす必要があります。

- ネットワークは、レイヤ 2 VPN（L2VPN）で設定する必要があります。
- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

IGMP スヌーピングの制約事項

- IGMP スヌーピングは、L2VPN ブリッジ ドメインだけでサポートされます。

- IPv4 マルチキャストは、BVI インターフェイスの背後にあるマルチキャスト送信元でサポートされています。たとえば、次の設定は、IPv4 マルチキャストの BVI の背後にある送信元を設定する方法を示しています。

```
l2vpn
bridge group 1
  bridge-domain 1
   multicast-source ipv4
   igmp snooping profile grp1
   !
   interface TenGigE0/0/0/3.32
   !
   routed interface BVI1
```

- 明示的ホスト トラッキング（IGMPv3 スヌーピング機能）はサポートされません。
- IGMPv1 はサポートされていません。

IGMP スヌーピングの情報

IGMP スヌーピングの概要

基本機能の説明

IGMP スヌーピングは、レイヤ 2 でマルチキャスト トラフィックを抑制する方法を提供します。IGMP スヌーピング アプリケーションは、ブリッジ ドメインのホストによって送信された IGMP メンバーシップ レポートをスヌーピングすることで、レイヤ 2 マルチキャスト転送テーブルを設定して、少なくとも 1 つの関係メンバーを持つポートだけにトラフィックを送信できます。これにより、マルチキャスト トラフィックの量が大幅に削減されます。

IGMP は、レイヤ 3 で設定され、IPv4 マルチキャスト ネットワーク内のホストが、関与するマルチキャスト トラフィックを通知する手段、ルータがレイヤ 3のネットワーク内のマルチキャスト トラフィックのフローを制御および制限する手段を提供します。

IGMP スヌーピングは、IGMP メンバーシップ レポート メッセージの情報を使用して、対応する情報を転送テーブルに構築し、レイヤ 2 の IP マルチキャスト トラフィックを制限します。転送テーブルのエントリは <ルート, OIF リスト> という形式で、

- ルートは <*, G> ルートまたは <S, G> ルートです。
- OIF リストは、指定されたルートに関する IGMP メンバーシップ レポートを送信したすべてのブリッジ ポートで構成されます。

マルチキャスト ネットワークに実装された IGMP スヌーピングには、次の属性があります。

- 基本的には、IGMP スヌーピングはブリッジ ドメイン全体をフラッディングする可能性があるマルチキャスト トラフィックを削減することにより、帯域幅使用量を減らします。

- 一部のオプションの設定を使用して、1 つのブリッジ ポートのホストから受信した IGMP レポートをフィルタリングし、他のブリッジポートのホストへの漏洩を防止することで、ブリッジ ドメイン間のセキュリティを提供します。

ハイ アベイラビリティ機能

すべてのハイ アベイラビリティ機能は、IGMP スヌーピングを有効にする以上の追加設定を行わずに、IGMP スヌーピング プロセスに適用されます。次のハイ アベイラビリティ機能がサポートされています。

- プロセスの再起動
- RP フェールオーバー
- ステートフル スイッチオーバー（SSO）
- ノンストップ フォワーディング（NSF）：プロセスの再起動またはルート プロセッサ（RP）のフェールオーバー後にコントロールプレーンが復元されている間、フォワーディングは影響を受けません。
- ラインカードの活性挿抜（OIR）

ブリッジ ドメインのサポート

IGMP スヌーピングは、ブリッジ ドメイン レベルで動作します。IGMP スヌーピングがブリッジ ドメインでイネーブルの場合、スヌーピング機能は、ブリッジ ドメインに属する次のポートを含むすべてのポートに適用されます。

- ブリッジ ドメインの物理ポート。
- イーサネット フロー ポイント（EFP）：EFP には VLANを指定できます。
- イーサネット バンドル：イーサネット バンドルには、IEEE 802.3ad リンク バンドルおよび Cisco EtherChannel バンドルが含まれます。IGMP スヌーピング アプリケーションの観点では、イーサネット バンドルは単なる EFP の 1 つです。 の転送アプリケーションは、バンドルから単一のポートをランダムに指定して、マルチキャスト トラフィックを伝送します。

マルチキャスト ホスト ポート

IGMP スヌーピングは、各ポート（EFP、物理ポート、または EFP バンドルなど）をホスト ポートとして分類します。つまり、mrouter ポートではないすべてのポートはホスト ポートです。

IGMPスヌーピングをイネーブルにしたブリッジドメイン内のマルチキャストトラフィック処理

次の表では、IGMP スヌーピングおよびホスト ポートによるトラフィック処理の動作について説明します。Table 1: IGMPv2 クエリアのマルチキャスト トラフィック処理, on page 4 では

IGMPv2 クエリのトラフィック処理について説明します。Table 2: IGMPv3 クエリアのマルチキャスト トラフィック処理, on page 4 は IGMPv3 クエリに適用されます。

デフォルトでは、IGMP スヌーピングは IGMPv2 および IGMPv3 をサポートしています。ブリッジ ドメインで検出された IGMP クエリのバージョンによって、スヌーピング プロセスの動作のバージョンが決まります。IGMPv3 の最小バージョンをサポートするように IGMP スヌーピングを設定してデフォルトを変更すると、IGMP スヌーピングは IGMPv2 クエリを無視します。

***Table 1: IGMPv2* クエリアのマルチキャスト トラフィック処理**

トラフィック タイプ	ホスト ポートで受信した場合
IP マルチキャストの送信元トラフィック	すべての mrouter ポートと、関与を示しているホスト ポートに転送します。
IGMP の一般クエリー	—
IGMP グループに固有なクエリー	切断
IGMPv2 の join	レポートを検査（スヌーピング）します。 • レポート抑制がイネーブルの場合、新しいグループに対する最初の join か、既存のグループに対する一般クエリーに続く最初の join を転送します。 • レポート抑制がディセーブルの場合、すべての mrouter ポートに転送します。
IGMPv3 の report	無視
IGMPv2 の leave	最後のメンバ クエリー処理を呼び出します。

***Table 2: IGMPv3* クエリアのマルチキャスト トラフィック処理**

トラフィック タイプ	ホスト ポートで受信した場合
IP マルチキャストの送信元トラフィック	すべての mrouter ポートと、関与を示しているホスト ポートに転送します。
IGMP の一般クエリー	—
IGMP グループに固有なクエリー	—
IGMPv2 の join	IGMPv3 IS_EX{} レポートとして処理します。
IGMPv3 の report	• プロキシ レポート機能がイネーブルの場合：状態または送信元リストが変更されると、すべての mrouter ポートで状態変更レポートを生成します。 • プロキシ レポート機能がディセーブルの場合：すべての mrouter ポートに転送します。

トラフィック タイプ	ホスト ポートで受信した場合
IGMPv2 の leave	IGMPv3 IS_IN{} レポートとして処理します。

IGMP スヌーピング設定プロファイルに関する情報

ブリッジ ドメインで IGMP スヌーピングをイネーブルにするには、ブリッジ ドメインにプロファイルを対応付ける必要があります。最小設定は、空のプロファイルです。プロファイルが空の場合、IGMP スヌーピングのデフォルト設定, on page 7に記載されている IGMP スヌーピングのデフォルト設定オプションおよび設定値がイネーブルになります。

ブリッジ ドメインまたはブリッジ ドメインに属するポートに、IGMP スヌーピング プロファイルを適用できます。次のガイドラインでは、ポートおよびブリッジ ドメインに適用されるプロファイル間の関係について説明します。

- ブリッジ ドメインに適用されている任意の IGMP プロファイル（空のプロファイルを含む）によって、IGMP スヌーピングがイネーブルになります。IGMP スヌーピングをディセーブルにするには、ブリッジ ドメインからプロファイルの適用を解除します。
- プロファイルが空の場合、デフォルト設定を使用して、ブリッジ ドメインおよびブリッジに属するすべてのポートに IGMP スヌーピングが設定されます。
- ブリッジ ドメインに（ブリッジ ドメイン レベルで）適用できる IGMP スヌーピング プロファイルは常に 1 つだけです。プロファイルはブリッジに属するポートに適用でき、ポートあたり 1 つのプロファイルが適用できます。
- ポート プロファイルは、ブリッジ ドメインにプロファイルが適用されていない場合は有効になりません。
- ポート固有の設定を有効にするには、ブリッジ ドメインで IGMP スヌーピングがイネーブルになっている必要があります。
- ブリッジ ドメインに適用されたプロファイルにポート固有の設定オプションが含まれている場合は、別のポート固有プロファイルがポートに適用されていない限り、値はそのブリッジに属する mrouter ポートおよびホスト ポートを含むすべてのポートに適用されます。
- ポートにプロファイルが対応付けられていると、IGMP スヌーピングは、ブリッジ レベルのプロファイルに存在するポート設定に関係なく、そのポートを再設定します。

プロファイルの作成

プロファイルを作成するには、グローバル コンフィギュレーション モードで **igmp snooping profile** コマンドを使用します。

プロファイルの適用と解除

ブリッジ ドメインにプロファイルを適用するには、l2vpn ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードで **igmp snooping profile** コマンドを使用します。ポートにプロファイルを適用するには、ブリッジドメインに属するインターフェイス コンフィギュレーション モードで **igmp snooping profile** コマンドを使用します。プロファイルの適用を解除するには、適切なコンフィギュレーション モードでこのコマンドの **no** 形式を使用します。

ブリッジドメインまたはポートとプロファイルの対応付けを解除しても、プロファイルはそのまま存在し、後で使用できます。プロファイルの対応付けを解除すると、次の処理が行われます。

- ブリッジ ドメインとプロファイルの対応付けを解除すると、ブリッジ ドメインで IGMP スヌーピングが非アクティブになります。
- ポートとプロファイルの対応付けを解除すると、そのポートの IGMP スヌーピング設定値は、ブリッジ ドメイン プロファイルからインスタンス化されます。

プロファイルの変更

アクティブなプロファイルは変更を加えることはできません。アクティブなプロファイルとは、現在対応付けられているプロファイルです。

アクティブなプロファイルを変更する必要がある場合は、すべてのブリッジまたはポートとの対応付けを解除して、変更し、もう一度対応付ける必要があります。

アクティブなプロファイルを変更するもう 1 つの方法は、必要な変更を含む新しいプロファイルを作成し、ブリッジまたはポートに適用することで既存のプロファイルを置き換える方法です。これにより、IGMP スヌーピングは無効になり、新しいプロファイルのパラメータを使用して再びアクティブになります。

IGMP スヌーピングのデフォルト設定

Table 3: IGMP スヌーピングのデフォルト設定値

スコープ	機能	デフォルト値
ブリッジ ドメイン	IGMP snooping	イネーブル化する IGMP プロファイルはブリッジ ドメインに適用されるまで、ブリッジ ドメインではディセーブルです。
	internal querier	未設定
	last-member-query-count	2
	last-member-query-interval	1000 ミリ秒
	minimum-version	2（IGMPv2 と IGMPv3 をサポート）
	querier query-interval	60（秒） **Note** これは、非標準デフォルト値です。
	report-suppression	イネーブル（IGMPv2 のレポート抑制機能と、IGMPv3 のプロキシ レポート機能をイネーブルにします）
	querier robustness-variable	2
	router alert check	イネーブル
	tcn query solicit	ディセーブル
	tcn flood	イネーブル
	ttl-check	イネーブル
	unsolicited-report-timer	1000 ミリ秒
ポート	immediate-leave	ディセーブル
	mrouter	スタティック mrouter は設定されていません。デフォルトで動的な検出が実行されます。
	router guard	ディセーブル
	static group	未設定

ブリッジ ドメイン レベルでの IGMP スヌーピング設定

IGMP の最小バージョン

minimum-version コマンドは、ブリッジ ドメインの IGMP スヌーピングでサポートされる IGMP バージョンを決定します。

- minimum-version が 2 の場合、IGMP スヌーピングは IGMPv2 および IGMPv3 メッセージを受信します。これはデフォルト値です。
- minimum-version が 3 の場合、IGMP スヌーピングは IGMPv3 メッセージだけを受信し、IGMPv2 メッセージをすべてドロップします。

IGMPv1 はサポートされていません。このコマンドのスコープは、ブリッジ ドメインです。コマンドは、ポートに適用されているプロファイルでは無視されます。

グループ メンバーシップ インターバル、ロバストネス変数、およびクエリー間隔

グループ メンバーシップ インターバル（GMI）は、IGMP スヌーピングが古いグループ メンバーシップ状態を失効させるタイミングを制御します。**show igmp snooping group** コマンドは、次のクエリ インターバルの後に古い状態が消去されるまで、有効期間 0 のグループを表示します。

GMI は次のように計算されます。

GMI = (robustness-variable * query-interval) + maximum-response-time

値は次のとおりです。

- maximum-response-time（MRT）は時間を表します。受信先はこの時間中にメンバーシップ状態を報告する必要があります。
- robustness-variable は、GMI の計算に影響を与える整数です。
- query-interval は一般クエリーの送信間隔を表します。

GMI のコンポーネントの値は、次のように取得されます。

- MRT は IGMPv2 および IGMPv3 両方の一般クエリーでアドバタイズされます。
- クエリアが IGMPv2 を実行している場合、IGMP スヌーピングは、robustness-variable と query-interval に IGMP スヌーピングで設定された値を使用します。これらのパラメータ値は、クエリアに設定された値と一致している必要があります。ほとんどの場合、他のシスコ ルータと対話する場合、これらの値を明示的に設定する必要はありません。通常、IGMP スヌーピングのデフォルト値は、クエリアのデフォルト値と一致しています。一致していない場合は、**querier robustness-variable** および **querier query-interval** コマンドを使用して、一致する値を設定する必要があります。
- IGMPv3 の一般クエリーは、robustness-variable と query-interval の値（それぞれ QRV と QQI）を伝えます。IGMP スヌーピングは、クエリーからの値を使用して、IGMP スヌーピングの GMI をクエリアの GMI と一致させます。

統合ルーティング ブリッジング アクティブ/アクティブ マルチホーム上のマルチキャスト

統合ルーティング ブリッジングのアクティブ/アクティブ マルチホーム機能を介したマルチキャストにより、ルータは、障害が発生しても、トラフィックを損失することなく、ルータ間のトラフィックを迅速かつ安全に切り替えることができます。この機能は、ソリューションとして連携する次の 4 つのサブ機能で構成されています。

- 最初に、ピア ルータに対して IGMPv2 スヌーピングが有効になり、どのレイヤ 2 インターフェイスの受信者が特定グループに関与しているかが分かります。
- スヌーピングの後、この情報は、レイヤ 2 EVPN 同期機能を使用してピアルータに同期されます。
- 両方のピア ルータが同期されると、最後のホップ ルータのように動作し、PIM join アップストリームを送信します。
- トラフィックが両方のピア ルータに到着すると、1 つのピア ルータだけが、指定されたフォワーダ選択機能を使用してトラフィックを受信者に転送します。

IGMP スヌーピングを設定する方法

最初の 2 つの作業は、基本的な IGMP スヌーピングの設定に必須です。

IGMP スヌーピング プロファイルの作成

Procedure

	Command or Action	Purpose
ステップ 1	**configure**	
ステップ 2	**igmp snooping profile** *profile-name* **Example:** `RP/0/RP0/cpu 0: router(config)# igmp snooping profile default-bd-profile`	IGMP スヌーピング プロファイル コンフィギュレーション モードを開始し、名前付きプロファイルを作成します。 デフォルト プロファイルは、IGMP スヌーピングをイネーブルにします。追加の設定をせずに新しいプロファイルをコミットするか、プロファイルに追加の設定オプションを含めることができます。後でプロファイルに戻って、このモジュールの他の作業で記載されている手

	Command or Action	Purpose
		順に従って、設定を追加することもできます。
ステップ 3	オプションで、デフォルト設定値を上書きするコマンドを追加します。	ブリッジ ドメイン プロファイルを作成する場合は、次の点を考慮します。 • 空のプロファイルは、ブリッジ ドメインへの適用に適しています。空のプロファイルは、デフォルト設定値でIGMP スヌーピングをイネーブルにします。 • オプションで、デフォルト設定値を上書きするコマンドをプロファイルに追加できます。 • ブリッジ ドメイン プロファイルにポート固有の設定を含める場合、別のプロファイルがポートに適用されていない限り、設定はそのブリッジに属するすべてのポートに適用されます。 ポート固有のプロファイルを作成する場合は、次の点を考慮します。 • 空のプロファイルはポートに適用できますが、ポートの設定には影響を与えません。 • ポートにプロファイルを適用する際、IGMP スヌーピングはブリッジ ドメイン プロファイルからの設定値の継承を上書きして、ポートを再設定します。これらの設定を保持する場合は、ポート プロファイルのコマンドを繰り返し実行する必要があります。 後でプロファイルにコマンドを追加するには、プロファイルの適用を解除し、プロファイルを変更してから再適用します。
ステップ 4	**commit**	

次の作業

プロファイルをブリッジ ドメインまたはポートに適用し、プロファイルを有効にする必要があります。次のいずれかの作業を参照してください。

プロファイルの適用およびブリッジ ドメインでの IGMP スヌーピングのアクティブ化

ブリッジ ドメインで IGMP スヌーピングをアクティブにするには、次の手順の説明に従って、ブリッジ ドメインに IGMP スヌーピング プロファイルを適用します。

Procedure

	Command or Action	Purpose
ステップ 1	**configure**	
ステップ 2	**l2vpn** **Example:** `RP/0/RP0/cpu 0: router(config)# l2vpn`	レイヤ 2 VPN コンフィギュレーション モードを開始します。
ステップ 3	**bridge group** *bridge-group-name* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group GRP1`	名前付きブリッジ グループのレイヤ 2 VPNブリッジ グループ 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	**bridge-domain** *bridge-domain-name* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain ISP1`	名前付きブリッジ ドメインのレイヤ 2 VPNブリッジグループブリッジドメイン コンフィギュレーション モードを開始します。
ステップ 5	**igmp snooping profile** *profile-name* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# igmp snooping profile default-bd-profile`	ブリッジ ドメインに名前付き IGMP スヌーピング プロファイルを適用し、ブリッジ ドメインで IGMP スヌーピングをイネーブルにします。
ステップ 6	**commit**	
ステップ 7	**show igmp snooping bridge-domain detail** **Example:**	（任意）IGMP スヌーピングがブリッジ ドメインでイネーブルであることを確認し、ブリッジ ドメインおよびポートに

	Command or Action	Purpose
	`RP/0/RP0/cpu 0: router# show igmp snooping bridge-domain detail`	適用される IGMP スヌーピング プロファイルの名前を表示します。
ステップ 8	**show l2vpn bridge-domain detail** **Example:** `RP/0/RP0/cpu 0: router# show l2vpn bridge-domain`	（任意）IGMP スヌーピングがブリッジ ドメインのフォワーディング プレーン（レイヤ 2）に実装されていることを確認します。

プロファイルの適用解除とブリッジ ドメインでの IGMP スヌーピングの非アクティブ化

ブリッジ ドメインで IGMP スヌーピングを非アクティブ化するには、次の手順を使用して、ブリッジ ドメインからプロファイルを削除します。

Note ブリッジ ドメインに一度に適用できるプロファイルは 1 つだけです。

Procedure

	Command or Action	Purpose
ステップ 1	**configure**	
ステップ 2	**l2vpn** **Example:** `RP/0/RP0/cpu 0: router(config)# l2vpn`	レイヤ 2 VPN コンフィギュレーション モードを開始します。
ステップ 3	**bridge group** *bridge-group-name* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group GRP1`	名前付きブリッジ グループのレイヤ 2 VPNブリッジ グループ 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	**bridge-domain** *bridge-domain-name* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain ISP1`	名前付きブリッジ ドメインのレイヤ 2 VPNブリッジグループブリッジドメイン コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 5	**no igmp snooping** **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# no igmp snooping`	ブリッジ ドメインから IGMP スヌーピング プロファイルの適用を解除し、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ます。 **Note** 同時にブリッジ ドメインに適用できるプロファイルは 1 つだけです。プロファイルが適用されている場合、IGMP スヌーピングはイネーブルです。プロファイルが適用されていない場合、IGMP スヌーピングはディセーブルです。
ステップ 6	**commit**	
ステップ 7	**show igmp snooping bridge-domain detail** **Example:** `RP/0/RP0/cpu 0: router# show igmp snooping bridge-domain detail`	（任意）IGMP スヌーピングがブリッジ ドメインでディセーブルであることを確認します。
ステップ 8	**show l2vpn bridge-domain detail** **Example:** `RP/0/RP0/cpu 0: router# show l2vpn bridge-domain`	（任意）IGMP スヌーピングがブリッジ ドメインのフォワーディング プレーン（レイヤ 2）でディセーブルであることを確認します。

ブリッジに属するポートへのプロファイルの適用と解除

Before you begin

ポート固有のプロファイルが IGMP スヌーピングの動作に影響を与えるようにするには、ブリッジ ドメインで IGMP スヌーピングがイネーブルになっている必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	**configure**	
ステップ 2	**l2vpn** **Example:** `RP/0/RP0/cpu 0: router(config)# l2vpn`	レイヤ 2 VPN コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 3	**bridge group** *bridge-group-name* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group GRP1`	名前付きブリッジ グループのレイヤ 2 VPN ブリッジ グループ 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	**bridge-domain** *bridge-domain-name* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain ISP1`	名前付きブリッジ ドメインのレイヤ 2 VPN ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。
ステップ 5	**interface** *interface-type interface-number* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# interface gig 1/1/1/1`	名前付きインターフェイスまたは PW のレイヤ 2 VPN ブリッジ グループ ブリッジ ドメイン インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	次のいずれかを実行します。 • **igmp snooping profile** *profile-name* • **no igmp snooping** **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-if)# igmp snooping profile mrouter-port-profile`	名前付き IGMP スヌーピング プロファイルをポートに適用します。 **Note** ポートのプロファイルは、ブリッジに他のプロファイルが適用されていない限り、無効です。 コマンドの **no** 形式を使用して、ポートからプロファイルの適用を解除します。ポートに適用できるプロファイルは 1 つだけです。
ステップ 7	**routed interface BVI** *BVI 番号* **Example:** `RP/0/(config-l2vpn-bg-bd-if)# routed interface bvi 2`	BVI をブリッジ ドメインに接続します。 *BVI 番号*には任意の番号を指定できます。
ステップ 8	**commit**	
ステップ 9	**show igmp snooping bridge-domain detail** **Example:** `RP/0/RP0/cpu 0: router# show igmp`	（任意）IGMP スヌーピングがブリッジドメインでイネーブルであることを確認し、ブリッジドメインおよびポー

	Command or Action	Purpose
	`snooping bridge-domain detail`	トに適用される IGMP スヌーピング プロファイルの名前を表示します。
ステップ 10	**show l2vpn bridge-domain detail** **Example:** `RP/0/RP0/cpu 0: router# show l2vpn bridge-domain`	（任意）IGMP スヌーピングがブリッジ ドメインのフォワーディング プレーン（レイヤ 2）に実装されていることを確認します。

マルチキャスト転送の確認

Procedure

	Command or Action	Purpose
ステップ 1	**configure**	
ステップ 2	**show l2vpn forwarding bridge-domain** [*bridge-group-name*:*bridge-domain-name*] **mroute ipv4** [**detail**] [**hardware** {**ingress** | **egress**}] **location** *node-id* **Example:** `RP/0/RP0/cpu 0: router# show l2vpn forwarding bridge-domain bridgeGroup1:ABC mroute ipv4 detail location 0/3/CPU0`	フォワーディング プレーンの転送テーブルに変換されるマルチキャスト ルートを表示します。特定のブリッジ グループまたはブリッジ ドメインに表示を制限するには、任意の引数を使用します。 これらのルートが期待したルートではない場合は、コントロール プレーンの設定を確認し、対応する IGMP スヌーピング プロファイルを訂正してください。
ステップ 3	**show l2vpn forwarding bridge-domain** [*bridge-group-name*:*bridge-domain-name*] **mroute ipv4 summary location** *node-id* **Example:** `RP/0/RP0/cpu 0: router# show l2vpn forwarding bridge-domain bridgeGroup1:ABC mroute ipv4 summary location 0/3/CPU0`	フォワーディング プレーンの転送テーブルに保存されているマルチキャスト ルートの要約レベルの情報を表示します。特定のブリッジ ドメインに表示を制限するには、任意の引数を使用します。

IGMP スヌーピングの設定例

次に、のレイヤ2ブリッジ ドメインでIGMP スヌーピングをイネーブルにする例を示します。

ブリッジに属する物理インターフェイスでの IGMP スヌーピングの設定：例

1. 2 つのプロファイルを作成します。

```
igmp snooping profile bridge_profile
!
igmp snooping profile port_profile

!
```

2. L2 転送用の 2 つの物理インターフェイスを設定します。

```
interface GigabitEthernet0/8/0/38
   negotiation auto
   l2transport
   no shut
   !
!
interface GigabitEthernet0/8/0/39
   negotiation auto
   l2transport
   no shut
   !
!
```

3. ブリッジ ドメインにインターフェイスを追加します。ブリッジ ドメインに bridge_profile を適用し、イーサネット インターフェイスのいずれかに port_profile を適用します。2 番目のイーサネット インターフェイスは、ブリッジ ドメイン プロファイルから IGMP スヌーピング設定属性を継承します。

```
l2vpn
  bridge group bg1
     bridge-domain bd1
     igmp snooping profile bridge_profile
     interface GigabitEthernet0/8/0/38
       igmp snooping profile port_profile
     interface GigabitEthernet0/8/0/39

!
  !
!
```

4. 設定されたブリッジ ポートを確認します。

```
show igmp snooping port
```

ブリッジに属する VLAN インターフェイスでの IGMP スヌーピングの設定：例

1. 2 つのプロファイルを設定します。

```
igmp snooping profile bridge_profile
igmp snooping profile port_profile

!
```

2. L2 転送用の VLAN インターフェイスを設定します。

```
interface GigabitEthernet0/8/0/8
   negotiation auto
   no shut
   !
!
interface GigabitEthernet0/8/0/8.1 l2transport
   encapsulation dot1q 1001
   mtu 1514
   !
!
interface GigabitEthernet0/8/0/8.2 l2transport
   encapsulation dot1q 1002
   mtu 1514
   !
!
```

3. プロファイルを適用し、ブリッジ ドメインにインターフェイスを追加します。インターフェイスのいずれかにプロファイルを適用します。他のインターフェイスは、ブリッジ ドメイン プロファイルから IGMP スヌーピング設定属性を継承します。

```
l2vpn
  bridge group bg1
     bridge-domain bd1
     igmp snooping profile bridge_profile
     interface GigabitEthernet0/8/0/8.1
       igmp snooping profile port_profile
     interface GigabitEthernet0/8/0/8.2

     !
  !
!
```

4. 設定されたブリッジ ポートを確認します。

```
show igmp snooping port
```

ブリッジに属するイーサネット バンドルでの IGMP スヌーピングの設定：例

1. この例では、バンドルのフロントエンドが事前に設定されていることを前提にしています。たとえば、バンドル設定が次の 3 つのスイッチインターフェイスから構成されているとします。

```
    interface Port-channel1
    !
interface GigabitEthernet0/0/0/0
    !
interface GigabitEthernet0/0/0/1
!
    interface GigabitEthernet0/0/0/2
       channel-group 1 mode on
    !
    interface GigabitEthernet0/0/0/3
       channel-group 1 mode on
    !
```

2. 2 つの IGMP スヌーピング プロファイルを設定します。

```
       igmp snooping profile bridge_profile
       !
       igmp snooping profile port_profile

       !
```

3. バンドルのメンバ リンクとしてインターフェイスを設定します。

```
       interface GigabitEthernet0/0/0/0
         bundle id 1 mode on
         negotiation auto
       !
       interface GigabitEthernet0/0/0/1
         bundle id 1 mode on
         negotiation auto
       !
       interface GigabitEthernet0/0/0/2
         bundle id 2 mode on
         negotiation auto
       !
       interface GigabitEthernet0/0/0/3
         bundle id 2 mode on
         negotiation auto
       !
```

4. L2 転送用のバンドル インターフェイスを設定します。

```
interface Bundle-Ether 1
          l2transport
          !
       !
       interface Bundle-Ether 2
          l2transport
```

```
    !
  !
```

5. インターフェイスをブリッジ ドメインに追加し、IGMP スヌーピング プロファイルを適用し。

```
l2vpn
  bridge group bg1
     bridge-domain bd1
     igmp snooping profile bridge_profile
     interface bundle-Ether 1
       igmp snooping profile port_profile
     interface bundle-Ether 2

     !
  !
!
```

6. 設定されたブリッジ ポートを確認します。

```
show igmp snooping port
```

統合ルーティング ブリッジング アクティブ/アクティブ マルチホーム上のマルチキャストの設定

ピア 1 で実行される設定：

1. レイヤ 2 基本設定

```
hostname peer1
!
interface Bundle-Ether2
!
interface Bundle-Ether2.2 l2transport
 encapsulation dot1q 2
 rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/0/0/0
 bundle id 2 mode on
 no shut
!
interface BVI2
 ipv4 address 100.2.0.1 255.255.255.0
 mac-address 1002.1111.2
!
```

2. EVPN 設定

```
hostname peer1
!
router bgp 100
 bgp router-id 1.1.1.1
 bgp graceful-restart
 address-family l2vpn evpn
 !
```

```
 neighbor 3.3.3.3
  remote-as 100
  update-source Loopback0
  address-family l2vpn evpn
  !
 !
!
evpn
 evi 2
  advertise-mac
  !
 !
 interface Bundle-Ether2
  ethernet-segment
   identifier type 0 02.02.02.02.02.02.02.02.02
   bgp route-target 0002.0002.0002
  !
 !
!
```

3. IGMPv2 スヌーピングの設定

```
hostname peer1
!
router igmp
 interface BVI2
  version 2
 !
!
l2vpn
 bridge group VLAN2
  bridge-domain VLAN2
   igmp snooping profile 1
   interface Bundle-Ether2.2
   !
   routed interface BVI2
   !
   evi 2
   !
  !
 !
igmp snooping profile 1
!
```

ピア 2 で実行される設定：

1. レイヤ 2 基本設定

```
hostname peer2
!
interface Bundle-Ether2
!
interface Bundle-Ether2.2 l2transport
 encapsulation dot1q 2
 rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/0/0/0
 bundle id 2 mode on
 no shut
!
interface BVI2
 ipv4 address 100.2.0.1 255.255.255.0
 mac-address 1002.1111.2
!
```

2. EVPN 設定

```
hostname peer2
!
router bgp 100
 bgp router-id 2.2.2.2
 bgp graceful-restart
 address-family l2vpn evpn
 !
 neighbor 3.3.3.3
  remote-as 100
  update-source Loopback0
  address-family l2vpn evpn
  !
 !
!
evpn
 evi 2
  advertise-mac
  !
 !
 interface Bundle-Ether2
  ethernet-segment
   identifier type 0 02.02.02.02.02.02.02.02.02
   bgp route-target 0002.0002.0002
  !
 !
!
```

3. IGMPv2 スヌーピングの設定

```
hostname peer2
!
router igmp
 interface BVI2
  version 2
 !
!
l2vpn
 bridge group VLAN2
  bridge-domain VLAN2
   igmp snooping profile 1
   interface Bundle-Ether2.2
   !
   routed interface BVI2
   !
   evi 2
   !
  !
 !
igmp snooping profile 1
!
```

IGMP スヌーピングおよび EVPN 同期の確認

この例では、受信者はグループ 239.0.0.2 の IGMPv2 join を送信します。ピア 2 では、このグループには D フラグがあります。これは、ピア 1 ではなく、実際の IGMP がピア 2 に join しましたことを示します。ピア 1 では、このグループには B フラグがあります。これは、このグループが EVPN 同期機能を使用して BGP から学習されたことを示します。

```
RP/0/RP0/CPU0:peer1#show igmp snooping group
Fri Aug 31 22:27:46.363 UTC

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, B=BGP Learnt, E=Explicit Tracking, R=Replicated

                          Bridge Domain VLAN10:VLAN10

Group           Ver GM Source          PM Port                         Exp   Flgs
-----           --- -- ------          -- ----                         ---   ----
239.0.0.2       V2  -  *               -  BE2.2                        never B


RP/0/RP0/CPU0:peer2#show igmp snooping group
Fri Aug 31 22:27:49.686 UTC

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, B=BGP Learnt, E=Explicit Tracking, R=Replicated

                          Bridge Domain VLAN10:VLAN10

Group           Ver GM Source          PM Port                         Exp   Flgs
-----           --- -- ------          -- ----                         ---   ----
239.0.0.2       V2  -  *               -  BE2.2                        74    D
```

デュアル DR PIM アップリンクの確認

この例では、送信元 126.0.0.100 がグループ 239.0.0.2 にトラフィックを送信すると、ピア 1 とピア 2 の両方が PIM join アップストリームを送信していることがわかります。(*, G) と (S, G) の着信インターフェイスは、それぞれ RP と送信元へのインターフェイスである必要があります。ピア 1 とピア 2 の両方については、発信インターフェイスは、受信者側の BVI インターフェイスである必要があります。

```
RP/0/RP0/CPU0:peer1#show mrib route
:
:

(*,239.0.0.2) RPF nbr: 30.0.0.4 Flags: C RPF
  Up: 00:13:41
  Incoming Interface List
    HundredGigE0/0/0/1 Flags: A NS, Up: 00:13:41
  Outgoing Interface List
    BVI2 Flags: F NS LI, Up: 00:13:41

(126.0.0.100,239.0.0.2) RPF nbr: 30.0.0.4 Flags: RPF
  Up: 00:03:34
  Incoming Interface List
    HundredGigE0/0/0/1 Flags: A, Up: 00:03:34
  Outgoing Interface List
    BVI2 Flags: F NS, Up: 00:03:34
:
:

RP/0/RP0/CPU0:peer2#show mrib route
:
:

(*,239.0.0.2) RPF nbr: 50.0.0.4 Flags: C RPF
  Up: 00:13:33
  Incoming Interface List
```

```
    HundredGigE0/0/0/2 Flags: A NS, Up: 00:13:33
  Outgoing Interface List
    BVI2 Flags: F NS LI, Up: 00:13:33

(126.0.0.100,239.0.0.2) RPF nbr: 50.0.0.4 Flags: RPF
  Up: 00:03:24
  Incoming Interface List
    HundredGigE0/0/0/2 Flags: A, Up: 00:03:24
  Outgoing Interface List
    BVI2 Flags: F NS, Up: 00:03:24
:
:
```

指定されたフォワーダ選択の確認

前の例で説明したように、ピア 1 とピア 2 の両方には発信インターフェイスとしての BVI2 があります。ただし、ピアのうち 1 つだけがトラフィックを転送する必要があります。指定されたフォワーダ選択では、転送を実行するためにそのうちの 1 つを選択します。この例では、ピア 2 がフォワーダとして選択されています。ピア 1 には、NDF としてマークされた Bundle-Ether 2.2 があります。

```
RP/0/RP0/CPU0:peer1#show l2vpn forwarding bridge-domain VLAN2:VLAN2 mroute ipv4 hardware
 ingress detail location 0/0/cPU0
Bridge-Domain: VLAN2:VLAN2, ID: 0
:
:

Bridge-Domain: VLAN2:VLAN2, ID: 0
  Prefix: (0.0.0.0,239.0.0.2/32)
  P2MP enabled: N
  IRB platform data: {0x0, 0x2d, 0x0, 0x0}, len: 32
  Bridge Port:
  EVPN, Xconnect id: 0x80000001 NH:2.2.2.2
  Bundle-Ether2.2, Xconnect id: 0xa0000015 (NDF)


RP/0/RP0/CPU0:peer2#show l2vpn forwarding bridge-domain VLAN2:VLAN2 mroute ipv4 hardware
 ingress detail location 0/0/cPU0
:
:

Bridge-Domain: VLAN2:VLAN2, ID: 0
  Prefix: (0.0.0.0,239.0.0.2/32)
  P2MP enabled: N
  IRB platform data: {0x0, 0x30, 0x0, 0x0}, len: 32
  Bridge Port:
  EVPN, Xconnect id: 0x80000001 NH:1.1.1.1
  Bundle-Ether2.2, Xconnect id: 0xa0000029
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
MPLS VPLS ブリッジの設定	*MPLS Configuration Guide for Cisco NCS 560 Series Routers*の「Implementing Virtual Private LAN Services on Cisco IOS XR ソフトウェア」モジュール
スタートアップ情報	
EFP と EFP バンドルの設定	*Interface and Hardware Component Configuration Guide for Cisco NCS 560 Series Routers*

標準

標準[1]	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。	—

[1] サポートされている標準がすべて記載されているわけではありません。

MIB

MIB	MIB のリンク
MIB は、IGMP スヌーピングをサポートしません。	Cisco IOS XR ソフトウェアを使用して MIB を特定およびダウンロードするには、次の URL にある Cisco MIB Locator を使用し、[Cisco Access Products] メニュー（http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）からプラットフォームを選択します。

RFC

RFC	タイトル
RFC-4541	『Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches』

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/techsupport