Cisco ASR 9000 シリーズ ルータ への 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だけにレイヤ 2 のマルチキャスト フローを制限します。 このモジュールでは、Cisco ASR 9000 シリーズ ルータ への IGMP スヌーピングの実装方法について説明します。

IGMP スヌーピングの機能の履歴

リリース	変更内容
リリース 3.7.2	この機能が導入されました。
リリース 3.9.2	次の機能に対するサポートが追加されました。 • IGMP スヌーピング グループ制限およびアクセス グループ。
リリース 4.0.0	次の機能に対するサポートが追加されました。 • マルチシャーシ リンク集約（MC-LAG）を使用するマルチキャスト冗長性。

- IGMP スヌーピングの前提条件，2 ページ
- IGMP スヌーピングの制約事項，2 ページ
- IGMP スヌーピングの情報，2 ページ
- IGMP スヌーピングの設定方法，22 ページ

- IGMP スヌーピングの設定例，48 ページ
- その他の参考資料，65 ページ

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。

  このコマンドを使用するには、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。 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場合は、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。
- 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。
- IPv6 マルチキャスト リスナー検出（MLD）スヌーピング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。

レイヤ 3 に設定された IGMP を使用すると、IPv4 マルチキャスト ネットワーク内のホストは関与するマルチキャスト トラフィックを通知し、ルータはレイヤ 3 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できます。

IGMP スヌーピングは、レイヤ 2 の IP マルチキャスト トラフィックを制限するための、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、転送テーブルに対応する情報を構築します。 転送テーブルのエントリは <ルート, OIF リスト> という形式です。

- ルートは <*,G> ルートまたは <S,G> ルートです。
- OIF List は、ブリッジ ドメインのすべてのマルチキャスト ルータ（mrouter）ポートと、指定されたルートの 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。

IGMP スヌーピングはマルチキャスト ネットワークに実装され、次の属性を持ちます。

- 基本的には、IGMP スヌーピングは VPLS 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。
- オプションの設定を使用して、IGMP メンバーシップ レポート（IGMPv2）を抑制するか、アップストリーム IP マルチキャスト ルータに対して IGMP プロキシ レポーター（IGMPv3）として動作することで、アップストリーム IP マルチキャスト ルータへのトラフィックの影響を軽減します。

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 スヌーピングのイネーブル化以外に追加で設定することなく、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 のフェールオーバー
- 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）：コントロール プレーンが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復元している間も、転送は引き続き影響を受けません。
- 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、VLAN の範囲、VLAN のリスト、またはインターフェイス ポート全体を指定できます。
- VPLS ブリッジ ドメインの疑似配線（PW）。
- 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。 Cisco ASR 9000 シリーズ ルータ 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 ルータおよびホスト ポート

IGMP スヌーピングは各ポート（EFP、PW、物理ポート、EFP バンドルなど）を次のいずれかに分類します。

- マルチキャスト ルータ ポート（mrouter ポート）：マルチキャスト対応ルータが接続されているポートです。 mrouter ポートは通常動的に検出されますが、静的に設定されている場合もあります。 マルチキャスト トラフィックは、mrouter ポートが入力ポートの場合を除き、常にすべての mrouter ポートに転送されます。
- ホスト ポート：mrouter ポートでないポートはすべてホスト ポートです。

マルチキャスト ルータ検出および静的な設定

IGMP スヌーピングは、mrouter ポートを動的に検出します。 ポートを mrouter ポートとして明示的に設定することもできます。

- 検出：IGMP スヌーピングは IGMP クエリー メッセージおよび Protocol Independent Multicast Version 2（PIMv2）のハロー メッセージをスヌーピングすることで、ブリッジ ドメインのアップストリーム mrouter ポートを識別します。 PIMv2 ハロー メッセージをスヌーピングすることで、ブリッジ ドメインの IGMP 非クエリアを識別します。
- 静的設定：ポートに適用されたプロファイルで mrouter コマンドを使用して、ポートを **mrouter** ポートとして静的に設定できます。 静的設定は、シスコ以外の機器との非互換性により動的検出ができないときに役立つ場合があります。

router-guard コマンドは、IGMP クエリーや PIM メッセージなどのマルチキャスト ルータ メッセージをフィルタリングすることによって、ポートが動的に検出された mrouter ポートになること

を防止します。 **router-guard** コマンドをポートに設定した後に、スタティック mrouter として設定することができます。 同一ポートへの router-guard コマンドおよび mrouter コマンドの設定の詳細については、ルータ ガードおよびスタティック mrouter, （18 ページ）を参照してください。

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 スヌーピングの mrouter ポートおよびホスト 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。 表 1：IGMPv2 クエリアのマルチキャスト トラフィック処理, （5 ページ） では、IGMPv2 クエリアのトラフィック処理について説明します。 表 2：IGMPv3 クエリアのマルチキャスト トラフィック処理, （6 ページ） は IGMPv3 クエリアの場合です。

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 クエリア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。 デフォルトを変更して、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た場合、IGMP スヌーピングは IGMPv2 クエリアを無視します。

表 *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	mrouter ポートで受信した場合	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。	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	すべてのポートに転送します。	—
IGMP グループに固有なクエリー	他のすべての mrouter ポートに転送します。	Dropped
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。	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。

トラフィック タイプ	mrouter ポートで受信した場合	ホスト ポートで受信した場合
IGMPv3 の report	無視	無視
IGMPv2 の leave	最後のメンバ クエリー処理を呼び出します。	最後のメンバ クエリー処理を呼び出します。

表 *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	mrouter ポートで受信した場合	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。	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	すべてのポートに転送します。	—
IGMP グループに固有なクエリー	クエリア ポートで受信した場合は、すべてのポートにフラッディングします。	—
IGMPv2 の join	IGMPv3 IS_EX{} レポートとして処理します。	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。	• 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。
IGMPv2 の leave	IGMPv3 IS_IN{} レポートとして処理します。	IGMPv3 IS_IN{} レポートとして処理します。

マルチシャーシ リンク集約

マルチシャーシ リンク集約（MC-LAG）機能は、デジタル加入者線アクセス マルチプレクサ（DSLAM）が Cisco ASR 9000 シリーズ ルータ にアクセスするための単純な冗長メカニズムを提供します。 冗長性は、2 つ以上の Cisco ASR 9000 シリーズ ルータ に対してデュアルホーム接続を許容することによって実現されます。

DSLAM はデュアルホーム接続デバイス（DHD）と呼ばれ、Cisco ASR 9000 シリーズ ルータは接続ポイント（PoA）と呼ばれます。 MC-LAG は冗長グループ（RG）に割り当てられます。 特定の MC-LAG を管理する Cisco ASR 9000 シリーズ ルータ（PoA）は、この RG のメンバです。 RG には複数の MC-LAG が存在する場合があります。 これは、同一の RG が他の DSLAM と MC-LAG との接続をカバーする場合があることを示します。 したがって、RG は冗長グループ ID（RGID）によって、PoA 上で一意に識別されます。 MC-LAG は一意の冗長オブジェクト ID（ROID）によって、各 PoA で識別されます。 VLAN サブインターフェイスが MC-LAG で設定されている場合は、各 VLAN サブインターフェイスに一意の ROID が存在します。

Cisco ASR 9000 シリーズ ルータの IGMP スヌーピングでは、DSLAM へのダウンストリームまたはマルチキャスト ルータへのアップストリームを監視する MC-LAG 設定をサポートしています。

（注） アクティブおよびスタンバイ POA における MC-LAG 機能の動作設定は同一である必要があります。

リンク バンドリングの設定および使用されるプロトコルの詳細については、『Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide』の「Configuring Link Bundling」の章を参照してください。

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, （11 ページ）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。

アクセス コントロールの設定

アクセス コントロール設定では、アクセス グループと重み付けグループの制限を設定します。

IGMP v2/v3 メッセージ フィルタリングでのアクセス グループの役割は、マルチキャスト グループ (*,G) およびマルチキャスト送信元グループ (S,G) へのホスト メンバーシップ要求を許可または拒否することです。 この役割は、IPTV チャネル パッケージへのブラック リストおよびホワイト リスト アクセスを提供するためには必須です。

重み付けグループ制限では IGMP v2/v3 グループの数が制限され、グループ内で同時に許容されるマルチキャスト チャネルの最大数を EFP および PW 単位で設定できます。

IGMP スヌーピングのアクセス グループ

レイヤ 3 IGMP ルーティングは **igmp access-group** コマンドを使用することでアクセス グループをサポートしていますが、レイヤ 3 IGMP ルーティング アクセス グループ機能は送信元グループをサポートしていないため、サポート内容はレイヤ 2 IGMP と同じではありません。

アクセス グループは、ブリッジ ドメインまたはポートに適用する IGMP スヌーピング プロファイルで参照されている拡張 IP アクセス リストを使用して指定されます。

（注） ポートレベルのアクセス グループはブリッジ ドメインレベルのアクセス グループよりも優先されます。

access-group コマンドは、受信したメンバーシップ レポートに指定されたアクセス リスト フィルタを適用するよう IGMP スヌーピングに指示します。 デフォルトでは、アクセス リストは適用されていません。

プロファイルで参照されているアクセス リストへの変更（または IGMP スヌーピング プロファイルで参照されているアクセス リストの置換）により、受信する IGMP グループ レポートおよび既存のグループ状態はただちにフィルタリングされます。このため、変更を実行するたびに、ブリッジドメインの IGMP スヌーピング プロファイルを適用解除および再適用する必要はありません。

IGMP スヌーピング グループの重み付け

IGMP v2/v3 グループの数を制限するには、グループ内で同時に許容されるマルチキャスト チャネルの最大数が EFP および PW 単位で設定可能になっている必要があり、そのうえでグループの重み付けを設定します。

IGMP スヌーピングでは、ブリッジ ポートでのメンバーシップを設定された最大数に制限しますが、IGMPv3 送信元グループをサポートし、さまざまな重み付けを個別グループまたは送信元グループに割り当てられるように機能が拡張されます。 これにより、たとえば、IPTV プロバイダー

は必要に応じて、標準画質および高解像度の IPTV ストリームを特定の加入者に関連付けることができます。

この機能は、ポートで送信される実際のマルチキャストの帯域幅を制限しません。 ただし、ポートがメンバとなる可能性がある IGMP グループと送信元グループの数を制限します。 加入者のメンバーシップ要求を適切なマルチキャスト フローに設定するのは、IPTV オペレータの責任です。

IGMP スヌーピング プロファイル コンフィギュレーション モードに属している **group policy** コマンドは、指定されたルート ポリシーを使用して新しい <*,G> または <S,G> メンバーシップ要求により追加される重みを決定するように、IGMP スヌーピングに指示します。 デフォルトは、グループの重みが設定されていない動作になります。

group limit コマンドは、ポートのグループの上限を指定します。 新しいグループまたは送信元グループによって追加される重みがこの制限を超える場合、このグループは許容されません。 （グループ ポリシーを設定せずに）グループの上限を設定した場合、<S/*,G> グループ状態にはデフォルトの重みである 1 が適用されます。

（注） デフォルトでは、各グループまたは送信元グループは、グループの上限に 1 の重みを追加します。 group policy コマンドを使用して、さまざまな重みをグループまたは送信元グループに割り当てることができます。

グループ上限ポリシーの設定は、次の条件に基づいています。

- <*,G> および <S,G> メンバーシップのグループ重み値は、BD またはポートに適用されている IGMP スヌーピング プロファイルに含まれているルート ポリシーに設定されています。
- ポート レベルの重みポリシーは、グループ制限とルート ポリシーが設定されている場合には、ブリッジ ドメイン レベルのポリシーよりも優先されます。
- ポリシーが設定されていない場合、各グループの重みは均等にカウントされ、1 になります。
- ポリシーが設定されている場合、一致するすべてのグループの重みは 1 になり、一致しないグループの重みは 0 になります。

IGMP スヌーピングのデフォルト設定

表 *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 スヌーピング	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。
	内部クエリア	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） （注） 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
	ルータ アラート チェック	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

スコープ	機能	デフォルト値
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。
	ルータ ガード	ディセーブル
	スタティック グループ	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。 768 ビットは、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 メッセージは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。

システム IP アドレス

system-ip-address コマンドでは、IGMP スヌーピング用の IP アドレスを設定します。 明示的に設定しない場合、デフォルトアドレスは 0.0.0.0 です。 次の場合を除いて、デフォルトで十分です。

- 内部クエリアを設定している場合。 内部クエリアには、0.0.0.0 は使用できません。
- ブリッジが、0.0.0.0 アドレスを受け付けない IGMP ルータと通信する必要がある場合。

IGMP スヌーピングのシステム IP アドレスは、次の方法で使用されます。

- 内部クエリアは、システム IP アドレスからクエリーを送信します。 デフォルトの 0.0.0.0 以外のアドレスを設定する必要があります。
- IGMPv3 は、システム IP アドレスからプロキシ レポートを送信します。 デフォルトのアドレス 0.0.0.0 が推奨されますが、一部の IGMP ルータは受け付けない場合があります。

- ブリッジ ドメインでのトポロジ変更通知（TCN）への応答として、IGMP スヌーピングはシステム IP アドレスからグローバル脱退を送信します。 デフォルトのアドレス 0.0.0.0 が推奨されますが、一部の IGMP ルータは受け付けない場合があります。

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、次のクエリー 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

ここで、

- 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** コマンドと **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。

レポート抑制機能（IGMPv2）とプロキシ レポート機能（IGMPv3）

次の IGMP スヌーピング機能は、ブリッジ ドメインのマルチキャスト トラフィックを削減します。 両方はデフォルトでイネーブルです。

- IGMPv2 レポート抑制機能：ブリッジ ドメイン クエリアが IGMPv2 を実行している場合に、現在のクエリー間隔の間に別のホストから同じ join を転送していた場合、IGMP スヌーピングはホストからの join を抑制します。 IGMP スヌーピングは、すべての mrouter ポートに最後の leave メッセージを転送します。

レポート抑制機能がイネーブルの場合にレポートが失われた場合のために、IGMP スヌーピングはIGMPv2 の join レポートを新しいグループに対して設定された querier robustness-variable で指定された回数分転送します。 querier robustness-variable コマンドを使用して、**querier robustness-variable** を設定します。

- IGMPv3 プロキシ レポート機能：ブリッジ ドメイン クエリアが IGMPv3 を実行している場合、IGMP スヌーピングはプロキシとして動作し、プロキシ レポート アドレスからレポートを生成します。 **system-ip-address** コマンドを使用して、プロキシ レポート アドレスを設定します。 デフォルト値は 0.0.0.0 です。

  プロキシ レポート機能がイネーブルの場合にレポートが失われた場合のために、IGMP スヌーピングは、状態変更レポートを robustness-variable で指定された回数分生成し、転送します。robustness-variable は、クエリアの一般クエリーの QRV 値です。 **unsolicited-report-timer** コマンドで設定された期間、レポートは不定期に転送されます。

レポート抑制機能およびプロキシ レポート機能をディセーブルにするには、**report-suppression disable** コマンドを使用します。

この項で説明する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。

グループ脱退処理

グループ脱退オプション

ホストをマルチキャスト グループから脱退させたい場合は、そのホストで定期的な一般 IGMP クエリーを無視するか（暗黙的脱退と呼ばれます）、またはグループ固有の leave メッセージを送信します。

IGMP スヌーピングは、グループ脱退に次のように応答します。

- 最後のメンバ クエリー処理：これは、グループ脱退を処理するデフォルトの方法です。
- 即時脱退：即時脱退に対して、任意で個別のポートを設定できます。

（注） マルチホスト LAN 上でホスト単位の即時脱退機能を提供する IGMPv3 明示的ホスト トラッキングはサポートされていません。

IGMPv2 および IGMPv3 の最後のメンバ クエリー処理

最後のメンバ クエリーは、IGMP スヌーピングで使用されるデフォルトのグループ脱退処理方法です。 最後のメンバ クエリー処理では、IGMP スヌーピングは脱退メッセージを次のように処理します。

- IGMP スヌーピングは、脱退メッセージを受信するポートでグループ固有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他のデバイスが指定されたマルチキャスト グ

ループのトラフィックに関与しているかどうかを確認します。 次の 2 つのコンフィギュレーション コマンドを使用して、脱退の要求と実際の脱退間の遅延を制御できます。

- **last-member-query-count** コマンド：IGMP スヌーピングが脱退メッセージへの応答として送信するグループ固有クエリーの数を制御します。
- **last-member-query-interval** コマンド：グループ固有クエリーの間隔を制御します。

- IGMP スヌーピングがグループ固有クエリーへの応答として IGMP join メッセージを受信しない場合、ポートに接続されている他のデバイスは、このマルチキャスト グループのトラフィックの受信に関与していないと見なし、そのマルチキャスト グループのレイヤ 2 転送テーブルのエントリからポートを削除します。
- 脱退メッセージが唯一残っているポートから送られた場合、IGMP スヌーピングはグループのエントリを削除し、マルチキャスト ルータに IGMP の脱退を生成します。

即時脱退設定

即時脱退は、任意のポートレベルの設定パラメータです。 即時脱退処理では、IGMP スヌーピングは、事前にインターフェイスに IGMP グループ固有のクエリーを送信することなく、レイヤ 2 インターフェイスを転送テーブルのエントリから即座に削除します。 IGMP 脱退メッセージを受信すると、そのポートでマルチキャスト ルータが学習されていない限り、IGMP スヌーピングは、そのマルチキャスト グループのレイヤ 2 転送テーブル エントリからインターフェイスを即座に削除します。

即時脱退処理により脱退遅延は改善されますが、この処理が適しているのは、ポートで 1 つの受信先が設定されている場合だけです。 たとえば、即時脱退は、次の状況に適しています。

- IPTV チャネル受信先などのポイントツーポイント構成
- プロキシ レポート付きのダウンストリーム DSLAM

1 つのポートに複数の受信先が存在する可能性がある場合は、ポートで即時脱退を使用しないでください。 使用すると、関与する受信機がトラフィックを受信できなくなるおそれがあります。 たとえば、即時脱退は、LAN には適していません。

即時脱退処理は、ポートレベルのオプションです。 このオプションは、ポート プロファイルでポートごとに、またはブリッジ ドメイン プロファイルで明示的に設定できます。ブリッジ ドメイン プロファイルの場合は、ブリッジに属するすべてのポートに適用されます。

トポロジ変更通知への反応

スパニングツリー プロトコル（STP）トポロジでは、トポロジ変更通知（TCN）は、STP トポロジ変更が発生したことを示します。 トポロジ変更の結果、mrouter とグループ メンバーシップを報告するホストはブリッジ ドメインに属する他の STP ポートに移行することがあります。 TCN 後、mrouter とメンバーシップの状態を再学習する必要があります。

IGMP スヌーピングは次のように TCN に反応します。

1 IGMP スヌーピングは、すべての既知のマルチキャスト ルートに設定されているフラッディングを、転送状態にある STP に参加するすべてのポートを含めるように一時的に拡張します。短期的なフラッディングにより、マルチキャスト配信はブリッジ ドメインのすべての mrouter とすべてのメンバ ホストに対して続行され、mrouter とメンバーシップの状態が再学習されます。

ただし、この TCN フラッディングの結果として、これらの追加のマルチキャスト フローにより、ダウンストリーム STP リンクがオーバーサブスクライブになる可能性があります。 このような場合は **tcn flood disable** コマンドを使用して、この機能をディセーブルにすることができます。

2 STP ルート ブリッジは、すべてのポートで（グループ 0.0.0.0 の）グローバル脱退を発行します。 この動作により、相互運用可能な IGMP クエリアは一般クエリーを送信して、再学習プロセスを促進します。

（注） グローバル脱退の送信によるクエリー要請は、シスコ固有の実装です。

3 TCN リフレッシュ期間が終了すると、IGMP スヌーピングは、マルチキャスト ルート フラッディング セットから非 mrouter および非メンバの STP ポートを除外します。 フラッディングを行う時間は、**tcn flood query count** コマンドで制御できます。 このコマンドは、TCN 後にマルチキャスト トラフィックのフラッディングに使用する IGMP 一般クエリーの数を設定するので、リフレッシュ期間に影響します。

IGMP スヌーピングのデフォルトの動作では、STP ルート ブリッジは、TCN への応答として常にグローバル脱退を発行し、非ルート ブリッジはグローバル脱退を発行しません。

tcn query solicit コマンドを使用すると、ルート ブリッジではないブリッジでも、TCN への応答として常にグローバル脱退の発行をイネーブルにできます。その場合、ルートブリッジと非ルートブリッジがグローバル脱退を発行し、両方が、TCN への応答として一般クエリーを要請します。ブリッジがルートではない場合の要請をオフにするには、コマンドの **no** 形式を使用します。

（注） **tcn query solicit** コマンドを使用する方法の 1 つは、リバース レイヤ 2 ゲートウェイ プロトコル（RL2GP）が MSTP アクセス ゲートウェイを設定するように設定されている場合です。 このシナリオで、IGMP スヌーピングはブリッジのルート ステータスまたは非ルート ステータスを認識しないため、TCN が発生すると、IGMP スヌーピングが少なくとも 1 つのブリッジで明示的に応答するように設定されていない限り、ドメイン内のどのクエリーも応答しません。

ルート ブリッジは常に、TCN への応答としてグローバル脱退を発行します。 この動作はディセーブルにできません。

内部クエリアには、TCN への反応を制御する独自の設定オプションがあります。

すべての TCN 関連設定オプションのスコープは、ブリッジ ドメイン単位です。 ポートに対応付けられたプロファイルにコマンドを使用しても効果はありません。

IGMP スヌーピングのパケット チェック

デフォルトでは、IGMP スヌーピングは次の検証を実行します。 ネットワークがこれらの検証を別の場所で実行する場合は、IGMP スヌーピング検証をディセーブルにできます。

- IGMP スヌーピングは、IGMP ヘッダーの存続可能時間（TTL）フィールドを確認し、TTL が 1 でないパケットをドロップします。 IGMP レポートおよびクエリーのヘッダーでは、TTL フィールドは常に 1 に設定されている必要があります。

  このチェックは **ttl-check disable** コマンドを使用してディセーブルにできます。この場合、IGMP スヌーピングは IGMP ヘッダーの TTL フィールドを検証することなく、すべてのパケットを処理します。

- IGMP スヌーピングは、IGMP メッセージの IP パケット ヘッダーにルータ アラート オプションがあるかどうかをチェックし、このオプションを含んでいないパケットをドロップします。

  このチェックは **router-alert-check disable** コマンドを使用してディセーブルにできます。この場合、IGMP スヌーピングはメッセージを処理する前に検証を実行しません。

スタートアップ クエリーの設定

スタートアップ クエリー機能は新しい IGMP スヌーピング プロファイル パラメータを使用して設定されます。 次のイベントに応答するように、スタートアップ クエリー処理を設定することができます。

- MC-LAG ポートがアクティブになったとき
- トポロジの変更
- ポートの起動
- 処理の開始

上記のパラメータは MC-LAG 機能に固有です。 これらはカウント、MRT、クエリー インターバルなどの既存のブリッジ ドメイン レベル パラメータとは異なります。 これらの CLI の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference*』を参照してください。

（注）

- IGMP スヌーピングが MC-LAG で正しく動作するには、両方の POA の IGMP スヌーピング設定が同じである必要があります。
- ダウンストリーム MC-LAG の場合、MC-LAG が設定され稼働している場合は、MC-LAG ポートを IGMP スヌーピング対応ブリッジドメインに追加する必要があります。
- アップストリーム MC-LAG の場合、POA がマルチキャスト ルータに適用されている場合は、トラフィックが両方の POA に供給されるようにするため、スタティック mrouter ポートを両方の POA に向いているマルチキャスト ルータに設定する必要があります。

ホスト ポート レベルの IGMP スヌーピング設定

ルータ ガードおよびスタティック mrouter

ルータ ガードは、悪意のあるユーザがホスト ポートを mrouter ポートにするのを防ぐセキュリティ機能です（この不正な動作はスプーフィングと呼ばれます）。ポートが **router-guard** コマンドで保護されていると、そのポートが mrouter としてダイナミックに検出されることはありません。ポート上でルータ ガードを設定すると、IGMP スヌーピングはポートに送信されたプロトコル パケットをフィルタリングして、マルチキャスト ルータ制御パケットの場合は破棄します。

mrouter コマンドはポートをスタティック mrouter として設定します。

たとえば次のような場合、同じポートで、**router-guard** コマンドと **mrouter** コマンドを使用して、ガードされたポートをスタティック mrouter として設定できます。

- 大量のダウンストリーム ホスト ポートが存在する場合に、動的な mrouter 検出をブロックして、スタティック mrouter を設定する場合。 この場合、ドメイン レベルでルータ ガード機能を設定します。 デフォルトでは、一般に大量のダウンストリーム ホスト ポートを含むすべてのポートに適用されます。 次に、比較的少数のアップストリーム ポートに、ルータ ガードを設定していない別のプロファイルを指定して動的な mrouter 検出を許可するか、スタティック mrouter を設定します。
- シスコ以外の機器との非互換性により動的検出を正しく行えない場合は、ルータ ガード機能を使用して動的検出をすべてディセーブルにして、mrouter を静的に設定できます。

  ポートに非互換 IGMP ルータがあるためにルータ ガード機能を使用している場合、そのポートで **mrouter** コマンドも設定して、ルータが IGMP レポートとマルチキャスト フローを受信できるようにする必要があります。

即時脱退

グループ脱退処理, （14 ページ）を参照してください。

スタティック グループ

IGMP スヌーピングは、レイヤ 2 マルチキャスト グループを動的に学習します。 レイヤ 2 マルチキャスト グループを静的に設定することもできます。

ブリッジ ドメインまたはポート用のプロファイルで **static group** コマンドを使用できます。 このオプションをブリッジ ドメインに対応付けられたプロファイルで設定すると、そのブリッジに属するすべてのポートに適用されます。

プロファイルには、複数のスタティック グループを含めることができます。 同じグループ アドレスに異なるソース アドレスを定義できます。 **source** キーワードを使用して、IGMPv3 ソース グループを設定できます。

スタティック グループ メンバーシップは、IGMP スヌーピングによるダイナミック操作より優先されます。 マルチキャスト グループ メンバーシップ リストには、スタティックとダイナミック両方のグループ定義を表示できます。

ポートでスタティック グループまたは送信元グループを設定すると、IGMP スヌーピングは、対応する <S/*,G> 転送エントリにポートを発信ポートとして追加し、IGMPv2 join または IGMPv3 report をすべての mrouter ポートに送信します。 IGMP スヌーピングは、スタティック グループがポート上で設定されている限り、一般クエリーへの応答としてメンバーシップ レポートを送信し続けます。

内部クエリア

内部クエリアを使用する場合

IP マルチキャスト ルーティングが設定されているネットワークでは、IP マルチキャスト ルータは IGMP クエリアとして機能します。 ブリッジ ドメインに外部クエリアは存在しない（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）が、ローカル マルチキャスト ソースが存在する状況では、内部クエリアを設定して IGMP スヌーピングを実装する必要があります。内部クエリアは、ブリッジ ドメインのホストからメンバーシップ レポートを要請し、IGMP スヌーピングがブリッジドメイン内のマルチキャストトラフィック用の制約的なマルチキャスト転送テーブルを作成できるようにします。

内部クエリアは、シスコ以外の機器での相互運用性の問題により、IGMP スヌーピングが外部クエリアと正しく連携できない場合にも役立つことがあります。 この場合、次のように対処できます。

1. 対象のポートに **router-guard** コマンドを発行して、関係のない外部クエリアが検出されるのを防ぐ。
2. ブリッジ ドメインのポートから、関連するグループ メンバーシップを学習するように内部クエリアを設定する。
3. マルチキャスト トラフィックを受信するスタティック mrouter ポートを設定する。

内部クエリアのデフォルト設定

内部クエリアの最小構成は次のとおりです。

- ブリッジ ドメインに対応付けられたプロファイルに、**internal-querier** コマンドを追加します。 デフォルト設定を表 4：内部クエリアのデフォルト設定値, （20 ページ） に示します。
- ブリッジ ドメインに対応付けられたプロファイルに、**system-ip-address** コマンドを追加して、デフォルトの 0.0.0.0 以外のアドレスを設定します。

表 *4*：内部クエリアのデフォルト設定値

コンフィギュレーション コマンド	デフォルト値
system-ip-address	0.0.0.0。デフォルトのアドレスは、内部クエリアでは無効です。
internal-querier *max-response-time*	10
internal-querier *query-interval*	60（秒） （注） これは、非標準デフォルト値です。
internal-querier *robustness-variable*	2
internal-querier tcn query *count*	2
internal-querier tcn query *interval*	10 秒
internal-querier timer *expiry* （注） これは RFC-3376 Section 8.5 で定義されている Other Querier Present Interval です。	125（秒）： robustness-variable * query-interval + 1/2(max-response-time) たとえば、すべてのコンポーネントのデフォルト値を使用した場合： (2 * 60) + 1/2 (10) = 125
internal-querier *version*	3

他の内部クエリア コマンドを削除することなく、（**internal-querier** コマンドの **no** 形式を使用して）内部クエリアをディセーブルにできます。その場合、追加の内部クエリア コマンドは無視されます。

internal-querier コマンドのスコープは、ブリッジ ドメイン単位です。 ポートに対応付けられたプロファイルにコマンドを使用しても効果はありません。

内部クエリアの処理

内部クエリアがドメインで選定されたクエリアである場合、ブリッジ ドメインのすべてのアクティブ ポートに **internal-querier query-interval** コマンドで指定された間隔で IGMP 一般クエリーを送信することで、メンバーシップ レポートを要請します。 内部クエリアは、IGMPv3 クエリーをデフォルトで送信します。 代わりに **internal-querier version** コマンドを使用して、内部クエリアが IGMPv2 メッセージを送信するように設定できます。

ローカル IGMP スヌーピング プロセスは、内部クエリアの一般クエリーに応答します。 特に、IGMPv3 プロキシ（イネーブルの場合）は、現在の状態レポートを生成し、すべての mrouter に転送します。 IGMPv2 の場合、または IGMPv3 プロキシがディセーブルになっている場合、IGMP スヌーピングはスタティック グループの状態についてのみ現在の状態レポートを生成します。

クエリーは、**system-ip-address** コマンドを使用して IGMP スヌーピング用に設定したアドレスから送信されます。 クエリーには、**internal-querier max-response-time** コマンドで設定された最大応答時間が含まれます。

internal-querier robustness-variable コマンドおよび **internal-querier query-interval** コマンドは、IGMPv2 および IGMPv3 処理の両方の値を設定します。

1 つのアクティブなクエリアの選定

ブリッジ ドメインで一度に使用できるアクティブなクエリアは 1 つだけです。 内部クエリアが、ブリッジ ドメインの他のクエリアからクエリーを受信すると、クエリアの選定が行われます。 最下位の IP アドレスが選択されます。 内部クエリアが選定されなかったクエリアの場合、IGMP スヌーピングは **internal-querier timer expiry** コマンドで設定された値でタイマーを開始します。 このタイマーの期限が、選択されたクエリアから別のクエリーを受信するまでに切れた場合、内部クエリアがアクティブなクエリアになります。

（注） デフォルトの **internal-querier timer expiry** コマンドの値は、表 4：内部クエリアのデフォルト設定値，（20 ページ） に記載されている他の設定オプションの値から取得されます。 デフォルトの計算を上書きする別の値を設定できます。

TCN への内部クエリアの反応

IGMP スヌーピングはトポロジ変更通知への応答として、グループの脱退を生成します。 IGMP スヌーピングの TCN への反応方法の詳細については、トポロジ変更通知への反応，（15 ページ）を参照してください。

内部クエリアがドメインで選定されたクエリアの場合に、グループの脱退を受信すると、次のように反応します。

- IGMP 一般クエリーをただちに生成します。

- **internal-querier tcn query interval** コマンドで設定されている時間待機し、別の IGMP 一般クエリーを生成します。
- クエリー回数が **internal querier tcn query count** コマンドで設定された値に達するまで、指定された間隔待機して、一般クエリーを送信する動作を続けます。

（注） internal querier TCN query count を 0 に設定することで、内部クエリアがグローバル脱退を無視するように設定できます。

IGMP スヌーピングの設定方法

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。 オプションの作業では、追加の IGMP スヌーピング機能を設定し、統計情報およびカウンタを表示します。

- プロファイルへのスタティック mrouter 設定の追加, （32 ページ）（任意）
- プロファイルへのルータ ガードの追加, （34 ページ）（任意）
- 即時脱退の設定, （36 ページ）（任意）
- スタティック グループの設定, （38 ページ）（任意）
- 内部クエリアの設定, （40 ページ）（任意）
- マルチキャスト転送の確認, （43 ページ）（任意）

IGMP スヌーピング プロファイルの作成

手順の概要

1. **configure**
2. **igmp snooping profile** *profile-name*
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。
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**igmp snooping profile** *profile-name* 例： `RP/0/RSP0/CPU0: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	次のいずれかのコマンドを使用します。	設定変更を保存します。

	コマンドまたはアクション	目的

	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

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。

手順の概要

1. **configure**
2. **l2vpn**
3. **bridge group** *bridge-group-name*
4. **bridge-domain** *bridge-domain-name*
5. **igmp snooping profile** *profile-name*
6. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
7. **show igmp snooping bridge-domain detail**
8. **show l2vpn bridge-domain detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**l2vpn** 例： `RP/0/RSP0/CPU0: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* 例： `RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group GRP1`	名前付きブリッジ グループのレイヤ 2 VPN VPLS 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* 例： `RP/0/RSP0/CPU0: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 VPLS 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。

	コマンドまたはアクション	目的
ステップ 5	**igmp snooping profile** *profile-name* 例： `RP/0/RSP0/CPU0: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	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 7	**show igmp snooping bridge-domain detail** 例： `RP/0/RSP0/CPU0: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** 例： `RP/0/RSP0/CPU0: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。

（注） 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。

手順の概要

1. **configure**
2. **l2vpn**
3. **bridge group** *bridge-group-name*
4. **bridge-domain** *bridge-domain-name*
5. **no igmp snooping**
6. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
7. **show igmp snooping bridge-domain detail**
8. **show l2vpn bridge-domain detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**l2vpn** 例： `RP/0/RSP0/CPU0: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。

	コマンドまたはアクション	目的
ステップ 3	**bridge group** *bridge-group-name* 例： `RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group GRP1`	名前付きブリッジ グループのレイヤ 2 VPN VPLS 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* 例： `RP/0/RSP0/CPU0: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 VPLS 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	**no igmp snooping** 例： `RP/0/RSP0/CPU0: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。 （注） 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	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。

	コマンドまたはアクション	目的
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。
ステップ 7	**show igmp snooping bridge-domain detail** 例： `RP/0/RSP0/CPU0: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** 例： `RP/0/RSP0/CPU0: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

はじめる前に

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。

手順の概要

1. **configure**
2. **l2vpn**
3. **bridge group** *bridge-group-name*
4. **bridge-domain** *bridge-domain-name*
5. **interface** *interface-type interface-number*
6. 次のいずれかを実行します。
   - **igmp snooping profile** *profile-name*
   - **no igmp snooping**
7. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
8. **show igmp snooping bridge-domain detail**
9. **show l2vpn bridge-domain detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**l2vpn** 例： `RP/0/RSP0/CPU0: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* 例： `RP/0/RSP0/CPU0: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* 例： `RP/0/RSP0/CPU0:router(config-l2vpn-bg)#`	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。

	コマンドまたはアクション	目的
	`bridge-domain ISP1`	
ステップ 5	**interface** *interface-type interface-number* 例： `RP/0/RSP0/CPU0: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 VPLS 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** 例： `RP/0/RSP0/CPU0: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。 （注） 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	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 8	**show igmp snooping bridge-domain detail** 例： `RP/0/RSP0/CPU0: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 9	**show l2vpn bridge-domain detail** 例： `RP/0/RSP0/CPU0: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。

プロファイルへのスタティック mrouter 設定の追加

はじめる前に

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。

（注） スタティック mrouter ポート設定はポートレベルのオプションであり、ポートを対象としたプロファイルに追加する必要があります。ブリッジドメインを対象としたプロファイルに mrouter ポート設定を追加することは推奨しません。

手順の概要

1. **configure**
2. **igmp snooping profile** *profile-name*
3. **mrouter**
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
5. **show igmp snooping profile** *profile-name* **detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**igmp snooping profile** *profile-name* 例： `RP/0/RSP0/CPU0:router(config)# igmp snooping profile mrouter-port-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、新しいプロファイルを作成するか、または既存のプロファイルにアクセスします。
ステップ 3	**mrouter** 例： `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# mrouter`	スタティック mrouter ポートとしてポートを設定します。

ステップ 4	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーションファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 設定変更を実行コンフィギュレーションファイルに保存し、コンフィギュレーションセッ

	コマンドまたはアクション	目的
		ションを継続するには、**commit** コマンドを使用します。
ステップ 5	**show igmp snooping profile** *profile-name* **detail** 例： `RP/0/RSP0/CPU0:router# show igmp snooping profile mrouter-port-profile detail`	（任意）名前付きプロファイルの設定を表示します。

次の作業

スタティック mrouter 設定を完了するには、ポートにプロファイルを適用します。 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, （29 ページ）を参照してください。

プロファイルへのルータ ガードの追加

マルチキャスト ルーティング プロトコル メッセージをポート上で受信しないようにして、ポートが動的 mrouter ポートになることを防止するには、次の手順を実行します。 ルータ ガードとスタティック mrouter コマンドの両方が同じポートで設定されることに注意してください。 詳細については、ルータ ガードおよびスタティック mrouter, （18 ページ）を参照してください。

はじめる前に

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。

（注） ルータ ガード設定はポートレベルのオプションであり、ポートを対象としたプロファイルに追加する必要があります。 ブリッジ ドメインを対象としたプロファイルにルータ ガード設定を追加することは推奨しません。 設定すると、IGMP クエリアを含むすべての mrouter がブリッジ ドメインでは検出されなくなります。

手順の概要

1. **configure**
2. **igmp snooping profile** *profile-name*
3. **router-guard**
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
5. **show igmp snooping profile** *profile-name* **detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**igmp snooping profile** *profile-name* 例： `RP/0/RSP0/CPU0:router(config)# igmp snooping profile host-port-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、新しいプロファイルを作成するか、または既存のプロファイルにアクセスします。
ステップ 3	**router-guard** 例： `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# router-guard`	動的検出からポートを保護します。

ステップ 4	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーションファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。

	コマンドまたはアクション	目的
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 ◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 設定変更を実行コンフィギュレーションファイルに保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。
ステップ 5	**show igmp snooping profile** *profile-name* **detail** 例： `RP/0/RSP0/CPU0:router# show igmp snooping profile host-port-profile detail`	（任意）名前付きプロファイルの設定を表示します。

次の作業

ルータ ガード設定を完了するには、ポートにプロファイルを適用します。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, （29 ページ）を参照してください。

即時脱退の設定

IGMP スヌーピング プロファイルに IGMP スヌーピング即時脱退オプションを追加する手順は、次のとおりです。

はじめる前に

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。

手順の概要

1. **configure**
2. **igmp snooping profile** *profile-name*
3. **immediate-leave**
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
5. **show igmp snooping profile** *profile-name* **detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**igmp snooping profile** *profile-name* 例： `RP/0/RSP0/CPU0:router(config)# igmp snooping profile host-port-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、新しいプロファイルを作成するか、または既存のプロファイルにアクセスします。
ステップ 3	**immediate-leave** 例： `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# immediate-leave`	immediate-leave オプションをイネーブルにします。 • ブリッジドメインに適用されたプロファイルにこのオプションを追加すると、そのブリッジに属するすべてのポートに適用されます。 • ポートに適用されたプロファイルにこのオプションを追加すると、このオプションはそのポートに適用されます。
ステップ 4	次のいずれかのコマンドを使用します。 • **end** • **commit** 例： `RP/0/RSP0/CPU0:router(config)# end`	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 `Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:` ◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コン

	コマンドまたはアクション	目的
	または `RP/0/RSP0/CPU0:router(config)# commit`	フィギュレーションセッションが終了して、ルータがEXECモードに戻ります。 ◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 ◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 • 設定変更を実行コンフィギュレーションファイルに保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。
ステップ 5	**show igmp snooping profile** *profile-name* **detail** 例： `RP/0/RSP0/CPU0:router# show igmp snooping profile host-port-profile detail`	（任意）名前付きプロファイルの設定を表示します。

次の作業

即時脱退の設定を完了するには、ブリッジ ドメインまたはポートにプロファイルを適用します。次のいずれかの項を参照してください。

スタティック グループの設定

IGMP スヌーピング プロファイルに 1 つ以上のスタティック グループまたは IGMPv3 送信元グループを追加するには、次の手順を実行します。

はじめる前に

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。

手順の概要

1. **configure**
2. **igmp snooping profile** *profile-name*
3. **static-group** *group-addr* [**source** *source-addr*]
4. スタティック グループをさらに追加する場合は、必要に応じて前の手順を繰り返します。
5. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
6. **show igmp snooping profile** *profile-name* **detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**igmp snooping profile** *profile-name* 例： `RP/0/RSP0/CPU0:router(config)# igmp snooping profile host-port-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、新しいプロファイルを作成するか、または既存のプロファイルにアクセスします。
ステップ 3	**static-group** *group-addr* [**source** *source-addr*] 例： `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# static-group 239.1.1.1 source 10.0.1.1`	スタティック グループを設定します。 • ブリッジ ドメインに適用されたプロファイルにこのオプションを追加すると、そのブリッジに属するすべてのポートに適用されます。 • ポートに適用されたプロファイルにこのオプションを追加すると、このオプションはそのポートに適用されます。
ステップ 4	スタティック グループをさらに追加する場合は、必要に応じて前の手順を繰り返します。	（任意）追加のスタティック グループを追加します。
ステップ 5	次のいずれかのコマンドを使用します。	設定変更を保存します。

	コマンドまたはアクション	目的

	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 6	**show igmp snooping profile** *profile-name* **detail** 例： `RP/0/RSP0/CPU0:router# show igmp snooping profile host-port-profile detail`	（任意）名前付きプロファイルの設定を表示します。

次の作業

スタティック グループ設定を完了するには、ブリッジ ドメインまたはポートにプロファイルを適用します。 次のいずれかの項を参照してください。

内部クエリアの設定

はじめる前に

この手順を有効にするには、IGMP スヌーピングがそのブリッジ ドメインでイネーブルになっている必要があります。

手順の概要

1. **configure**
2. **igmp snooping profile** *profile-name*
3. **system-ip-address** *ip-addr*
4. **internal-querier**
5. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
6. **show igmp snooping profile** *profile-name* **detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**igmp snooping profile** *profile-name* 例： `RP/0/RSP0/CPU0:router(config)# igmp snooping profile internal-querier-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、新しいプロファイルを作成するか、または既存のプロファイルにアクセスします。
ステップ 3	**system-ip-address** *ip-addr* 例： `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# system-ip-address 10.1.1.1`	内部クエリアが使用する IP アドレスを設定します。 デフォルトの system-ip-address の値（0.0.0.0）は、内部クエリアでは無効です。 IP アドレスを明示的に設定する必要があります。
ステップ 4	**internal-querier** 例： `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# internal-querier`	すべてのオプションにデフォルト値を使用して、内部クエリアをイネーブルにします。
ステップ 5	次のいずれかのコマンドを使用します。	設定変更を保存します。

	コマンドまたはアクション	目的

	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 設定変更を実行コンフィギュレーション ファイルに保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 6	**show igmp snooping profile** *profile-name* **detail** 例： `RP/0/RSP0/CPU0:router# show igmp snooping profile internal-querier-profile detail`	（任意）名前付きプロファイルの設定を表示します。

次の作業

内部クエリアの設定を完了するには、ブリッジ ドメインにプロファイルを適用します。

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, （24 ページ）を参照してください。

マルチキャスト転送の確認

手順の概要

1. **configure**
2. **show l2vpn forwarding bridge-domain** [*bridge-group-name*:*bridge-domain-name*] **mroute ipv4** [**detail**] [**hardware** {**ingress** | **egress**}] **location** *node-id*
3. **show l2vpn forwarding bridge-domain** [*bridge-group-name*:*bridge-domain-name*] **mroute ipv4 summary location** *node-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**show l2vpn forwarding bridge-domain** [*bridge-group-name*:*bridge-domain-name*] **mroute ipv4** [**detail**] [**hardware** {**ingress**	**egress**}] **location** *node-id* 例： `RP/0/RSP0/CPU0: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* 例： `RP/0/RSP0/CPU0: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。

グループ制限の設定

この手順では、次の作業について説明します。

ルート ポリシーの設定

手順の概要

1. **configure**
2. **route-policy** *policy-name*
3. **end-policy**
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**route-policy** *policy-name* 例： `RP/0/RSP0/CPU0:router(config)# route-policy sky`	定義されている名前でルート ポリシーを設定します。
ステップ 3	**end-policy** 例： `RP/0/RSP0/CPU0:router(config-rpl)# end-policy`	ルートポリシーの設定を終了します。
ステップ 4	次のいずれかのコマンドを使用します。 • **end** • **commit** 例： `RP/0/RSP0/CPU0:router(config)# end`	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 `Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:` ◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。

	コマンドまたはアクション	目的
	または `RP/0/RSP0/CPU0:router(config)# commit`	◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 ◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 • 設定変更を実行コンフィギュレーションファイルに保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

グループ上限の設定

手順の概要

1. **configure**
2. **igmp snooping profile** *profile-name*
3. **group policy** *policy-name*
4. **group limit** *range*
5. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**igmp snooping profile** *profile-name* 例： `RP/0/RSP0/CPU0:router(config)# igmp snooping 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、新しいプロファイルを作成するか、または既存のプロファイルにアクセスします。

	コマンドまたはアクション	目的
	name1	
ステップ 3	**group policy** *policy-name* 例： `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# group policy policy1`	設定されたルートポリシーがグループの重みを設定するように指定します。
ステップ 4	**group limit** *range* 例： `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# group limit 100`	ポートで許容されているグループ（または送信元グループ）の数を制限します。

ステップ 5	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーションファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 設定変更を実行コンフィギュレーションファイルに保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

アクセスグループの設定

この作業では、メンバーシップ レポートを受信するために、IGMP スヌープに指定されたアクセス リスト フィルタを適用するよう指示します。

ユーザはアクセスグループを設定する前にアクセス リストを作成し、設定する必要があります。標準アクセス リストおよび拡張アクセス リストを作成し設定する詳細な設定手順については、『Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide』を参照してください。

手順の概要

1. **configure**
2. **igmp snooping profile** *profile-name*
3. **access-group** *acl-name*
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	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	**igmp snooping profile** *profile-name* 例： `RP/0/RSP0/CPU0:router(config)# igmp snooping profile name1`	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、新しいプロファイルを作成するか、または既存のプロファイルにアクセスします。
ステップ 3	**access-group** *acl-name* 例： `RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# access-group acl1`	グループ メンバーシップ フィルタを設定します。
ステップ 4	次のいずれかのコマンドを使用します。	設定変更を保存します。

	コマンドまたはアクション	目的

	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーションファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 設定変更を実行コンフィギュレーションファイルに保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

IGMP スヌーピングの設定例

次に、Cisco ASR 9000 シリーズ ルータ のレイヤ 2 VPLS 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
```

```
   mrouter
!
```

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
   mrouter
!
```

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
          mrouter
       !
```

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ます。

```
       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
```

ブリッジに属する VFI での IGMP スヌーピングの設定：例

次に、ブリッジ ドメインに属する仮想転送インスタンス（VFI）に IGMP スヌーピングを設定する例を示します。 トポロジは 2 つのルータ（PE1 および PE2）から構成され、ブリッジ ポートとしてアクセス回線（AC）と疑似配線（PW）を持っています。

PE1 の設定

1 IGMP スヌーピング プロファイルを設定します。

```
igmp snooping profile prof1
!
igmp snooping profile prof2
   mrouter
!
```

2 インターフェイスを設定します。

```
interface Loopback0
  ipv4 address 10.1.1.1 255.255.255.255
!
interface GigabitEthernet0/2/0/9
   ipv4 address 10.10.10.1 255.255.255.0
   negotiation auto
!
interface GigabitEthernet0/2/0/39
   negotiation auto
   l2transport
!
```

3 Open Shortest Path First（OSPF）を設定します。

```
router ospf 1
  log adjacency changes
  router-id 10.1.1.1
  area 0
    interface Loopback0
    !
    interface GigabitEthernet0/2/0/9
    !
  !
!
```

4 ラベル配布プロトコル（LDP）を設定します。

```
mpls ldp
   router-id 10.1.1.1
   log neighbor
   !
   interface GigabitEthernet0/2/0/9
   !
!
```

5 ブリッジ ドメインを設定し、ブリッジ上でIGMP スヌーピングをイネーブルにして、ブリッジ ドメインにインターフェイスを追加します。

```
l2vpn
  pw-class atom-dyn
  encapsulation mpls
     protocol ldp
  !
!

bridge group bg1
    bridge-domain bd1
    igmp snooping profile prof1
    interface GigabitEthernet0/2/0/39
       igmp snooping profile prof2
    vfi mplscore
       neighbor 10.2.2.2 pw-id 101
       pw-class atom-dyn
       !
    !
  !
!
```

6 設定されたブリッジ ポートを確認します。

```
show igmp snooping port
```

PE2 の設定

1 IGMP プロファイルを設定します。

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

2 インターフェイスを設定します。

```
interface Loopback0
  ipv4 address 10.2.2.2 255.255.255.255
!
interface GigabitEthernet0/2/0/9
   ipv4 address 10.10.10.1 255.255.255.0
   negotiation auto
!
interface GigabitEthernet0/2/0/39
   negotiation auto
   l2transport
!
```

3 OSPF を設定します。

```
router ospf 1
  log adjacency changes
  router-id 10.2.2.2
  area 0
    interface Loopback0
    !
    interface GigabitEthernet0/2/0/9
    !
  !
!
```

4 LDP を設定します。

```
mpls ldp
   router-id 10.2.2.2
   log neighbor
   !
   interface GigabitEthernet0/2/0/9
   !
!
```

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ます。

```
   l2vpn
      pw-class atom-dyn
      encapsulation mpls
         protocol ldp
      !
    !

    bridge group bg1
        bridge-domain bd1
        igmp snooping profile bridge_profile
        interface GigabitEthernet0/2/0/39
           igmp snooping profile port_profile
        vfi mplscore
           neighbor 10.1.1.1 pw-id 101
           pw-class atom-dyn
```

```
            !
          !
        !
      !
```

6 設定されたブリッジ ポートを確認します。

```
show igmp snooping port
```

IGMP アクセスグループの設定

次の例では、<*,G> グループ（225.0.0.0/24 および 228.0.0.0/24）のユーザ メンバーシップだけを許容するリストを設定し、L2VPN ブリッジ ポートに適用します。 <S,G> メンバーシップを許可する 2 番目のアクセス リストを定義します。 このアクセス リストをブリッジ ポートに適用します。

```
interface gig 0/2/0/1.1 l2transport
...
!
ipv4 access-list iptv-basic-white-list
 10 permit ipv4 any 225.0.0.0/24
 20 permit ipv4 any 228.0.0.0/24
!
ipv4 access-list iptv-premium-white-list
 10 permit ipv4 192.168.0.1 232.0.1.0/24
 20 permit ipv4 192.168.0.1 232.0.2.0/24
!
igmp snooping profile iptv
 access-group iptv-white-list
!
igmp snooping profile iptv2
 access-group iptv-premium-white-list
!
l2vpn
 bridge group vz
bridge domain vz-iptv
 igmp snooping profile iptv
 interface gig 0/2/0/1.1
 interface gig 0/2/0/1.2
  igmp snooping profile iptv2
 interface gig 0/2/0/1.3
 ...
!
```

また、IGMP ルーティングでは igmp **access-group** コマンドを使用することでアクセスグループをサポートします。 IGMP ルーティングでは簡易 IP アクセスグループを使用して、グループ アドレス フィルタを指定します。 送信元グループ フィルタおよびグループ フィルタをサポートするには、IGMP スヌーピングに拡張 IP アクセス リストが必要になります。

（注） アクセスグループはスタティック グループおよび送信元グループには適用されません。

MCLAG での IGMP スヌーピングの設定：例

ケース 1：ダウンストリーム MCLAG

トポロジ：PE に順番に接続する、2 つの POA に接続する DHD。

DHD：

1 POA1 および POA2 へのバンドルを設定します。 このデバイスは、2 つの POA の存在をマスクされています。 バンドルは、1 つの POA に接続されていると判断します。

```
interface Bundle-Ether10
 description interface towards POAs
 lacp switchover suppress-flaps 100
 bundle maximum-active links 1
l2transport
 !

!

interface GigabitEthernet0/0/0/28
 description interface towards POA1
 bundle id 10 mode active
!

interface GigabitEthernet0/0/0/29
 description interface towards POA2
 bundle id 10 mode active
!
```

2 デバイスに送信された join は、バンドル上の POA に転送する必要があります。 そのため、L2VPN BD（スヌーピングなし）内の着信ポート（ホスト ポート）とバンドルを設定します。

```
RP/0/RSP0/CPU0:router:DHD# show running-config l2vpn

l2vpn
 bridge group bg1
  bridge-domain bg1_bd1
   interface Bundle-Ether10
   !
interface GigabitEthernet0/0/0/10
   !

  !

 !

!
```

POA1：

1 インターフェイスを設定します（OSPF および MPLS LDP 用）

```
interface Loopback0

ipv4 address 20.20.20.20 255.255.255.255

!
```

```
interface GigabitEthernet0/2/0/1
description interface towards POA2
ipv4 address 10.0.0.1 255.255.255.0

 negotiation auto

!

interface GigabitEthernet0/2/0/8

 description interface towards PE

 ipv4 address 10.0.1.1 255.255.255.0

 negotiation auto

!
```

2 OSPF と MPLS LDP を設定します。

```
router ospf 1
router-id 20.20.20.20
nsf cisco
area 0
interface Loopback0

  !
interface GigabitEthernet0/2/0/1
  !
interface GigabitEthernet0/2/0/8

  !

 !

!
mpls ldp
router-id 20.20.20.20
graceful-restart
interface GigabitEthernet0/2/0/1
 !
interface GigabitEthernet0/2/0/8

 !

!
```

3 DHD への MCLAG バンドルを設定します。

```
interface Bundle-Ether10
description interface towards DHD
lacp switchover suppress-flaps 100
mlacp iccp-group 1
mlacp switchover recovery-delay 60
mlacp port-priority 1
mac-address 0.aaaa.1111
bundle wait-while 0
l2transport

 !

!
interface GigabitEthernet0/2/0/29
bundle id 10 mode active
!
```

4 MCLAG の冗長グループを設定します。

```
redundancy

 iccp
group 1
mlacp node 1
mlacp system mac 0000.aaaa.0000
mlacp system priority 1
member
neighbor 30.30.30.30
!
backbone
interface GigabitEthernet0/2/0/8
  !

  !

 !

!
```

5 IGMP スヌーピング プロファイルを設定します。

```
igmp snooping profile p1
ttl-check disable
router-alert-check disable

!
```

6 PE 方向の DHD と PW に対する MCLAG バンドルを含む L2VPN BD 内の IGMP スヌーピングをイネーブルにします。

```
l2vpn
bridge group bg1
bridge-domain bg1_bd1
igmp snooping profile p1
interface Bundle-Ether10
!
vfi bg1_bd1_vfi
neighbor 40.40.40.40 pw-id 1

    !

   !

  !

 !

!
```

POA2：

1 インターフェイスを設定します（OSPF および MPLS LDP 用）

```
interface Loopback0

ipv4 address 30.30.30.30 255.255.255.255
!
interface GigabitEthernet0/0/0/1
description interface towards POA1
ipv4 address 10.0.0.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/8
```

```
description interface towards PE
ipv4 address 10.0.2.1 255.255.255.0
negotiation auto
!
```

2 OSPF と MPLS LDP を設定します。

```
router ospf 1
router-id 30.30.30.30
nsf cisco
area 0
interface Loopback0
!
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/8
!
!

!
mpls ldp
router-id 30.30.30.30
graceful-restart
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/8

 !

!
```

3 DHD への MCLAG バンドルを設定します。

```
interface Bundle-Ether10
description interface towards DHD
lacp switchover suppress-flaps 100
mlacp iccp-group 1
mlacp switchover recovery-delay 60
mlacp port-priority 2
mac-address 0.aaaa.1111
bundle wait-while 0
l2transport

 !

!
interface GigabitEthernet0/0/0/28
bundle id 10 mode active

!
```

4 MCLAG の冗長グループを設定します。

```
redundancy
iccp
group 1
mlacp node 2
mlacp system mac 0000.aaaa.0000
mlacp system priority 1
member
neighbor 20.20.20.20
!
backbone
interface GigabitEthernet0/0/0/8
   !
  !
 !
!
```

5 IGMP スヌーピング プロファイルを設定します。

```
igmp snooping profile p1
ttl-check disable
router-alert-check disable
!
```

6 PE 方向の DHD と PW に対する MCLAG バンドルを含む L2VPN BD 内の IGMP スヌーピングをイネーブルにします。

```
l2vpn
bridge group bg1
bridge-domain bg1_bd1
igmp snooping profile p1
interface Bundle-Ether10
!
vfi bg1_bd1_vfi
neighbor 40.40.40.40 pw-id 1

    !

   !

  !

 !

!
```

PE：

1 インターフェイスを設定します。

```
interface Loopback0
ipv4 address 40.40.40.40 255.255.255.255
!
interface GigabitEthernet0/0/0/8
description interface towards POA1
ipv4 address 10.0.1.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/9
description interface towards POA2
ipv4 address 10.0.2.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/20
description interface towards Multicast Router
l2transport
!
!
```

2 OSPF と MPLS LDP を設定します。

```
router ospf 1
router-id 40.40.40.40
nsf cisco
area 0
interface Loopback0
!
interface GigabitEthernet0/0/0/8
!
interface GigabitEthernet0/0/0/9
!
!
```

```
!
mpls ldp
router-id 40.40.40.40
graceful-restart

interface GigabitEthernet0/0/0/8
!
interface GigabitEthernet0/0/0/9
!
!
```

3 IGMP スヌーピング プロファイルを設定します。

```
igmp snooping profile p1
ttl-check disable
router-alert-check disable
!
```

4 マルチキャスト ルータ方向の POA とポートの両方に対する PW を含む L2VPN BD 内の IGMP スヌーピングをイネーブルにします。

```
l2vpn
bridge group bg1
bridge-domain bg1_bd1
igmp snooping profile p1
interface GigabitEthernet0/0/0/20
!
vfi bg1_bd1_vfi
neighbor 20.20.20.20 pw-id 1
!
neighbor 30.30.30.30 pw-id 1
!
!
!
```

ケース 2：アップストリーム MCLAG

トポロジ：マルチキャスト ルータは 2 つの POA に接続されており、順番に PE マルチキャスト ルータに接続します。

1 POA へのバンドルを設定します。

```
interface Bundle-Ether10
description interface towards POAs
ipv4 address 100.0.0.1 255.255.255.0
lacp switchover suppress-flaps 100
bundle maximum-active links 1
!
interface GigabitEthernet0/0/0/28
description interface towards POA1
bundle id 10 mode active
!
interface GigabitEthernet0/0/0/29
description interface towards POA2
bundle id 10 mode active
!
```

2 バンドル インターフェイス上でマルチキャスト ルーティングをイネーブルにします。

```
multicast-routing
address-family ipv4
interface Bundle-Ether10
enable
!
```

```
!
!
```

POA1：

1 インターフェイスを設定します（OSPF および MPLS LDP 用）。

```
interface Loopback0
ipv4 address 20.20.20.20 255.255.255.255
!
interface GigabitEthernet0/2/0/1
description interface towards POA2
ipv4 address 10.0.0.1 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/2/0/8
description interface towards PE
ipv4 address 10.0.1.1 255.255.255.0
negotiation auto
!
```

2 OSPF と MPLS LDP を設定します。

```
router ospf 1
router-id 20.20.20.20
nsf cisco
area 0
interface Loopback0
!
interface GigabitEthernet0/2/0/1
!
interface GigabitEthernet0/2/0/8
!
!
!
mpls ldp
router-id 20.20.20.20
graceful-restart
interface GigabitEthernet0/2/0/1
!
interface GigabitEthernet0/2/0/8
!
!
```

3 DHD への MCLAG バンドルを設定します。

```
interface Bundle-Ether10
description interface towards DHD
lacp switchover suppress-flaps 100
mlacp iccp-group 1
mlacp switchover recovery-delay 60
mlacp port-priority 1
mac-address 0.aaaa.1111
bundle wait-while 0
l2transport
!
!
interface GigabitEthernet0/2/0/29
bundle id 10 mode active
!
```

4 MCLAG の冗長グループを設定します。

```
redundancy
iccp
```

```
group 1
mlacp node 1
mlacp system mac 0000.aaaa.0000
mlacp system priority 1
member
neighbor 30.30.30.30
!
backbone
interface GigabitEthernet0/2/0/8
!
!
!
!
```

5 IGMP スヌーピング プロファイルを設定します。

```
igmp snooping profile p1
ttl-check disable
router-alert-check disable
!
```

6 PE 方向の DHD と PW に対する MCLAG バンドルを含む L2VPN BD 内の IGMP スヌーピングをイネーブルにします。

```
l2vpn
bridge group bg1
bridge-domain bg1_bd1
igmp snooping profile p1
interface Bundle-Ether10
!
vfi bg1_bd1_vfi
neighbor 40.40.40.40 pw-id 1
!
!
!
!
!
```

POA2：

1 インターフェイスを設定します（OSPF および MPLS LDP 用）。

```
interface Loopback0
ipv4 address 30.30.30.30 255.255.255.255
!
interface GigabitEthernet0/0/0/1
description interface towards POA1
ipv4 address 10.0.0.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/8
description interface towards PE
ipv4 address 10.0.2.1 255.255.255.0
negotiation auto
!
```

2 OSPF と MPLS LDP を設定します。

```
router ospf 1
router-id 30.30.30.30
nsf cisco
area 0
interface Loopback0
!
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/8
```

```
!
!
!
mpls ldp
router-id 30.30.30.30
graceful-restart
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/8
!
!
```

3 DHD への MCLAG バンドルを設定します。

```
interface Bundle-Ether10
description interface towards DHD
lacp switchover suppress-flaps 100
mlacp iccp-group 1
mlacp switchover recovery-delay 60
mlacp port-priority 2
mac-address 0.aaaa.1111
bundle wait-while 0
l2transport
!
!
interface GigabitEthernet0/0/0/28
bundle id 10 mode active
!
```

4 MCLAG の冗長グループを設定します。

```
redundancy
iccp
group 1
mlacp node 2
mlacp system mac 0000.aaaa.0000
mlacp system priority 1
member
neighbor 20.20.20.20
!
backbone
interface GigabitEthernet0/0/0/8
!
!
!
```

5 IGMP スヌーピング プロファイルを設定します。

```
igmp snooping profile p1
ttl-check disable
router-alert-check disable
!
```

6 PE 方向の DHD と PW に対する MCLAG バンドルを含む L2VPN BD 内の IGMP スヌーピングをイネーブルにします。

```
l2vpn
bridge group bg1
bridge-domain bg1_bd1
igmp snooping profile p1
interface Bundle-Ether10
!
vfi bg1_bd1_vfi
neighbor 40.40.40.40 pw-id 1
!
!
!
!
```

PE：

1 インターフェイスを設定します。

```
interface Loopback0
ipv4 address 40.40.40.40 255.255.255.255
!
interface GigabitEthernet0/0/0/8
description interface towards POA1
ipv4 address 10.0.1.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/9
description interface towards POA2
ipv4 address 10.0.2.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/20
description interface towards Host
l2transport
!
!
```

2 OSPF と MPLS LDP を設定します。

```
router ospf 1
router-id 40.40.40.40
nsf cisco
area 0
interface Loopback0
!
interface GigabitEthernet0/0/0/8
!
interface GigabitEthernet0/0/0/9
!
!
!
mpls ldp
router-id 40.40.40.40
graceful-restart
interface GigabitEthernet0/0/0/8
!
interface GigabitEthernet0/0/0/9
!
!
```

3 IGMP スヌーピング プロファイルを設定します。

```
igmp snooping profile p1
ttl-check disable
router-alert-check disable
!
igmp snooping profile p2
mrouter
!
```

4 ホスト方向の POA とポートの両方に対する PW を含む L2VPN BD 内の IGMP スヌーピングをイネーブルにします。 両方の POA への PW にスタティック mrouter ポートを設定します。

```
l2vpn
bridge group bg1
bridge-domain bg1_bd1
igmp snooping profile p1
interface GigabitEthernet0/0/0/20
!
vfi bg1_bd1_vfi
neighbor 20.20.20.20 pw-id 1
```

```
igmp snooping profile p2
!
neighbor 30.30.30.30 pw-id 1
igmp snooping profile p2
!
!
!
!
```

その他の参考資料

関連資料

関連項目	参照先
MPLS VPLS ブリッジの設定	『*Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide*』の「Implementing Virtual Private LAN Services on Cisco IOS XR Software」モジュール
スタートアップ情報	『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』
EFP と EFP バンドルの設定	『*Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide*』

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規格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 を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニュー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 サイトには、数千ページに及ぶ検索可能な技術情報があります。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もあります。 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/en/US/support/index.html