IGMP スヌーピング

このモジュールでは、グローバルにブリッジ ドメインでイーサネット仮想接続（EVC）ベースの IGMP スヌーピング機能をイネーブルにし、設定する方法について説明します。

- 機能情報の確認，1 ページ
- IGMP スヌーピングの情報，1 ページ
- IGMP スヌーピングを設定する方法，3 ページ
- その他の関連資料，13 ページ
- IGMP スヌーピングの機能情報，14 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IGMP スヌーピングの情報

IGMP スヌーピング

通常、デバイスは受信するすべてのフレームのソース アドレス フィールド内を確認することで MAC アドレスを学習するため、マルチキャスト トラフィックはフラッディングするようになり

ます。 マルチキャスト MAC アドレスは、パケットのソース アドレスとして使用されることはありません。 そのようなアドレスは MAC アドレス テーブルには現れないので、デバイスはマルチキャスト MAC アドレスを学習する方法を持っていません。

マルチキャスト デバイスのレイヤ 3 で実行される IP マルチキャスト インターネット グループ管理プロトコル（IGMP）は、マルチキャスト トラフィックのルーティングが必要なサブネットでレイヤ 3 IGMP クエリーを生成します。 （デバイスの）IGMP は、一般的な IGMP クエリーを定期的に送信します。

IGMP スヌーピングは、イーサネット仮想回線（EVC）ベースのフィーチャ セットです。 EVC は VLAN の概念とブロードキャスト ドメインを分離します。 EVC は、プロバイダーが提供しているレイヤ 2 サービスの単一インスタンスのエンドツーエンド表現です。 シスコ EVC フレームワークでは、ブリッジ ドメインは、サービス インスタンスと呼ばれているレイヤ 2 インターフェイス（1 つまたは複数）で構成されます。 サービス インスタンスは、あるデバイス上のあるポート上で EVC をインスタンス化したものです。 サービス インスタンスは、設定に基づいてブリッジ ドメインに関連付けられます。

従来、VLAN はブロードキャスト ドメインであり、物理ポートはアクセス ポートとして VLAN に割り当てられていました。トランク ポートによって受信されるパケットの VLAN タグと内部 VLAN ブロードキャスト ドメインは同じ番号です。 EVC によって、イーサネット フロー ポイント（EFP）が設定され、ブロードキャスト ドメインと関連付けられます。 VLAN タグは EFP を識別するためにだけ使用され、ブロードキャスト ドメインの識別には使用されません。

ブリッジ ドメインの EVC ベースの IGMP スヌーピングをイネーブルにすると、ブリッジ ドメイン インターフェイスは、1 つのレイヤ 2 マルチキャスト グループごとに 1 つの IGMP 加入要求のみを含む IGMP クエリーにレイヤ 2 で応答します。 各ブリッジ ドメインは、レイヤ 2 ブロードキャスト ドメインを表します。 ブリッジ ドメイン インターフェイスは、IGMP 加入要求を受信する各レイヤ 2 マルチキャスト グループのレイヤ 2 転送テーブルに、サブネットごとに 1 個のエントリを作成します。 このマルチキャスト トラフィックに関係するすべてのホストが、IGMP 加入要求を送信して、転送テーブル エントリに追加されます。 ブリッジ ドメイン インターフェイスが属するブリッジ ドメインのレイヤ 2 ルックアップ時に、ブリッジ ドメインは正しい EFP にパケットを転送します。 ブリッジ ドメイン インターフェイスがホストから IGMP グループ脱退メッセージを受信すると、ホストのテーブル エントリが削除されます。

レイヤ 2 マルチキャスト グループは IGMP スヌーピングを通して動的に学習されます。 ただし、スタティックにレイヤ 2 マルチキャスト グループを設定できます。 グループ メンバーシップをマルチキャスト グループ アドレスに静的に指定すると、その静的な設定値は IGMP スヌーピングによる自動操作より優先されます。 マルチキャスト グループ メンバーシップのリストは、ユーザが定義した設定値と IGMP スヌーピングによって学習された設定値の両方で構成できます。

IGMP スヌーピングを設定する方法

IGMP スヌーピングのイネーブル化

IGMP スヌーピングをイネーブルにする次の作業は、IGMP スヌーピングを明示的にディセーブルにした後でのみ実行します。 デフォルトでは、IGMP スヌーピングはすべての既存の VLAN インターフェイスおよびブリッジ ドメイン インターフェイスでイネーブルです。

はじめる前に

インターフェイスで IGMP スヌーピングをイネーブルにするには、IP マルチキャスト用に設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping**
4. **bridge-domain** *bridge-id*
5. **ip igmp snooping**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip igmp snooping** 例： `Device(config)# ip igmp snooping`	ディセーブルにした後で、IGMP スヌーピングをグローバルにイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**bridge-domain** *bridge-id* 例： `Device(config)# bridge-domain 100`	（任意）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	**ip igmp snooping** 例： `Device(config-bdomain)# ip igmp snooping`	（任意）設定されたブリッジ ドメイン インターフェイス上で IGMP スヌーピングをイネーブルにします。 • 指定されたブリッジ ドメインで IGMP スヌーピングが明示的にディセーブルにされた場合にだけ必要です。
ステップ 6	**end** 例： `Device(config-bdomain)# end`	特権 EXEC モードに戻ります。

IGMP スヌーピングのグローバルな設定

IGMP スヌーピングのグローバル コンフィギュレーションを変更するには、次の作業を実行します。

はじめる前に

IGMP スヌーピングがイネーブルであること。 IGMP スヌーピングは、デフォルトでイネーブルになっています。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip igmp snooping robustness-variable** *variable*
4. **ip igmp snooping tcn query solicit**
5. **ip igmp snooping tcn flood query count** *count*
6. **ip igmp snooping report-suppression**
7. **ip igmp snooping explicit-tracking-limit** *limit*
8. **ip igmp snooping last-member-query-count** *count*
9. **ip igmp snooping last-member-query-interval** *interval*
10. **ip igmp snooping check** {**ttl** | **rtr-alert-option**}
11. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**ip igmp snooping robustness-variable** *variable* 例： `Device(config)# ip igmp snooping robustness-variable 3`	（任意）IGMP スヌーピング ロバストネス変数を設定します。
ステップ 4	**ip igmp snooping tcn query solicit** 例： `Device(config)# ip igmp snooping tcn query solicit`	（任意）デバイスがスパニングツリールートでない場合でも、デバイスがTCNクエリー要求を送信できるようにします。
ステップ 5	**ip igmp snooping tcn flood query count** *count* 例： `Device(config)# ip igmp snooping tcn flood query count 4`	（任意）IGMP スヌーピングの TCN フラッディング クエリー カウントを設定します。
ステップ 6	**ip igmp snooping report-suppression** 例： `Device(config)# ip igmp snooping report-suppression`	（任意）IGMPスヌーピングのレポート抑制をイネーブルにします。
ステップ 7	**ip igmp snooping explicit-tracking-limit** *limit* 例： `Device(config)# ip igmp snooping explicit-tracking-limit 200`	（任意）IGMP スヌーピングの明示的トラッキング データベースのレポートの数を制限します。

	コマンドまたはアクション	目的
ステップ 8	**ip igmp snooping last-member-query-count** *count* 例： `Device (config)# ip igmp snooping last-member-query-count 5`	（任意）インターネット グループ管理プロトコル（IGMP）が IGMP leave メッセージの受信に対してクエリー メッセージを送信する頻度を設定します。デフォルト値は 2 ミリ秒です。
ステップ 9	**ip igmp snooping last-member-query-interval** *interval* 例： `Device (config)# ip igmp snooping last-member-query-interval 200`	（任意）この時間内にレポートが受信されなかった場合に、グループ レコードが削除されるという値を設定します。 デフォルトは 1000 ミリ秒です。
ステップ 10	**ip igmp snooping check** {**ttl** | **rtr-alert-option**} 例： `Device (config)# ip igmp snooping check ttl`	（任意）IGMP スヌーピング チェックを実行します。
ステップ 11	**exit** 例： `Device (config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ブリッジ ドメイン インターフェイス上での IGMP スヌーピングの設定

ブリッジ ドメイン インターフェイス上で IGMP スヌーピング設定を変更するには、次の作業を実行します。

はじめる前に

- ブリッジ ドメイン インターフェイスが作成されている必要があります。『*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*』の「Configuring Bridge Domain Interfaces」の項を参照してください。
- IGMP スヌーピングが、設定するインターフェイスでイネーブルになっている必要があります。 IGMP スヌーピングは、デフォルトでイネーブルになっています。

手順の概要

1. **enable**
2. **configure terminal**
3. **bridge-domain** *bridge-id*
4. **ip igmp snooping immediate-leave**
5. **ip igmp snooping robustness-variable** *variable*
6. **ip igmp snooping report-suppression**
7. **ip igmp snooping explicit-tracking**
8. **ip igmp snooping explicit-tracking-limit** *limit*
9. **ip igmp snooping last-member-query-count** *count*
10. **ip igmp snooping last-member-query-interval** *interval*
11. **ip igmp snooping access-group** {*acl-number* | *acl-name*}
12. **ip igmp snooping limit** *num* [**except** {*acl-number* | *acl-name*}]
13. **ip igmp snooping minimum-version** {**2** | **3**}
14. **ip igmp snooping check** {**ttl** | **rtr-alert-option**}
15. **ip igmp snooping static source** *source-address* **interface** *port-type port-number*
16. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**bridge-domain** *bridge-id* 例： `Device(config)# bridge-domain 100`	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 4	**ip igmp snooping immediate-leave** 例： `Device(config-bdomain)# ip igmp snooping immediate-leave`	（任意）IGMPv2 即時脱退処理をイネーブルにします。 （注） 即時脱退処理とクエリー カウントの両方を設定した場合は、高速脱退処理が優先されます。

	コマンドまたはアクション	目的
ステップ 5	**ip igmp snooping robustness-variable** *variable* 例： `Device(config-bdomain)# ip igmp snooping robustness-variable 3`	（任意）IGMP スヌーピング ロバストネス変数を設定します。 デフォルトは 2 です。
ステップ 6	**ip igmp snooping report-suppression** 例： `Device(config-bdomain)# ip igmp snooping report-suppression`	（任意）ブリッジ ドメイン インターフェイス上で、すべてのホストに対してレポート抑制をイネーブルにします。
ステップ 7	**ip igmp snooping explicit-tracking** 例： `Device(config-bdomain)#  ip igmp snooping explicit-tracking`	（任意）IGMP スヌーピングの明示的トラッキングをイネーブルにします。 明示的トラッキングはデフォルトでイネーブルになっています。
ステップ 8	**ip igmp snooping explicit-tracking-limit** *limit* 例： `Device(config-bdomain)# ip igmp snooping explicit-tracking-limit 200`	（任意）IGMP スヌーピングの明示的トラッキング データベースのレポートの数を制限します。
ステップ 9	**ip igmp snooping last-member-query-count** *count* 例： `Device(config-bdomain)# ip igmp snooping last-member-query-count 5`	（任意）IGMP leave メッセージの受信に対して送信されるスヌーピング クエリー メッセージの間隔を設定します。 デフォルト値は 2 ミリ秒です。 （注） 即時脱退処理とクエリー カウントの両方を設定した場合は、高速脱退処理が優先されます。
ステップ 10	**ip igmp snooping last-member-query-interval** *interval* 例： `Device(config-bdomain)#  ip igmp snooping last-member-query-interval 2000`	（任意）この時間内にレポートが受信されなかった場合に、グループ レコードが削除されるという値を設定します。 デフォルトは 1000 ミリ秒です。
ステップ 11	**ip igmp snooping access-group** {*acl-number* | *acl-name*} 例： `Device(config-bdomain)# ip igmp snooping access-group 1300`	ブリッジ ドメインで ACL ベースのフィルタリングを設定します。

	コマンドまたはアクション	目的
ステップ 12	**ip igmp snooping limit** *num* [**except** {*acl-number* | *acl-name*}] 例： `Device(config-bdomain)# ip igmp snooping 4400 except test1`	（任意）ブリッジ ドメインで許可されるグループまたはチャネルの数を制限します。
ステップ 13	**ip igmp snooping minimum-version** {**2** | **3**} 例： `Device(config-bdomain)# ip igmp snooping minimum-version 2`	（任意）IGMPプロトコルフィルタリングを設定します。
ステップ 14	**ip igmp snooping check** {**ttl** | **rtr-alert-option**} 例： `Device(config-bdomain)# ip igmp snooping check ttl`	（任意）IGMP スヌーピング チェックを実行します。
ステップ 15	**ip igmp snooping static source** *source-address* **interface** *port-type port-number* 例： `Device(config-bdomain)# ip igmp snooping static source 192.0.2.1 interface gigbitethernet 1/1/1`	（任意）レイヤ 2 LAN ポートにホストを静的に設定します。
ステップ 16	**end** 例： `Device(config-bdomain)# end`	特権 EXEC モードに戻ります。

EFP の設定

EFP で IGMP スヌーピング機能を設定するには、この作業を実行します。

はじめる前に

EFP およびブリッジ ドメインはあらかじめ設定しておく必要があります。 レイヤ 2 ポートでサービス インスタンスを設定すると、イーサネット仮想接続（EVC）機能を設定する疑似ポートまたはイーサネット フロー ポイント（EFP）が作成されます。 設定の詳細については、『*Carrier*

Ethernet Configuration Guide』「Configuring Ethernet Virtual Connections on the Cisco ASR 1000 Router」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **router-guard ip multicast efps**
4. **interface** *type number*
5. **service instance** *id* **ethernet**
6. **router-guard multicast**
7. **ip igmp snooping tcn flood**
8. **ip igmp snooping access-group** {*acl-number* | *acl-name*}
9. **ip igmp snooping limit** *num* [**except** {*acl-number* | *acl-name*}]
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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 3	**router-guard ip multicast efps** 例： `Device(config)# router-guard ip multicast efps`	（任意）すべての EFP に対するルータ ガードをイネーブルにします。
ステップ 4	**interface** *type number* 例： `Device(config)# interface BDI100`	（任意）設定するブリッジドメインインターフェイスを指定します。
ステップ 5	**service instance** *id* **ethernet** 例： `Device(config-if)# service instance 333 ethernet`	（任意）EFP を設定するイーサネット サービス 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 6	**router-guard multicast** 例： `Device(config-if-srv)# router-guard multicast`	（任意）EFP でルータ ガードを設定します。
ステップ 7	**ip igmp snooping tcn flood** 例： `Device(config-if-srv)# no ip igmp snooping tcn flood`	（任意）EFP で TCN フラッディングをディセーブルにします。 TCN フラッディングはデフォルトでイネーブルです。
ステップ 8	**ip igmp snooping access-group** {*acl-number* | *acl-name*} 例： `Device(config-if-srv)# ip igmp snooping access-group 44`	（任意）EFP で ACL ベースのフィルタリングを設定します。
ステップ 9	**ip igmp snooping limit** *num* [**except** {*acl-number* | *acl-name*}] 例： `Device(config-if-srv)# ip igmp snooping limit 1300 except test1`	（任意）EFP で許可される IGMP グループまたはチャネルの数を制限します。
ステップ 10	**end** 例： `Device(config-if-srv)# end`	特権 EXEC モードに戻ります。

IGMP スヌーピングの確認

手順の概要

1. **enable**
2. **show igmp snooping** [**count** [**bd** *bd-id*]]
3. **show igmp snooping groups bd** *bd-id* [**count** | *ip-address* [**verbose**] [**hosts** | **sources** | **summary**]]
4. **show igmp snooping membership bd** *bd-id*
5. **show igmp snooping mrouter** [**bd** *bd-id*]
6. **show igmp snooping counters** [**bd** *bd-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	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show igmp snooping** [**count** [**bd** *bd-id*]] 例： `Device(config)# show igmp snooping`	グローバル、またはブリッジ ドメインごとの IGMP スヌーピングの設定を表示します。
ステップ 3	**show igmp snooping groups bd** *bd-id* [**count**	*ip-address* [**verbose**] [**hosts**	**sources**	**summary**]] 例： `Device(config)# show igmp snooping groups bd 100`	ブリッジ ドメインごとにグループのスヌーピング情報を表示します。
ステップ 4	**show igmp snooping membership bd** *bd-id* 例： `Device(config)# show igmp snooping membership bd 100`	IGMPv3 ホスト メンバーシップ情報を表示します。
ステップ 5	**show igmp snooping mrouter** [**bd** *bd-id*] 例： `Device(config)# show igmp snooping mrouter`	グローバル、またはブリッジ ドメインごとにマルチキャスト ポートを表示します。

	コマンドまたはアクション	目的
ステップ 6	**show igmp snooping counters** [**bd** *bd-id*] 例： `Device(config)# show snooping counters`	グローバル、またはブリッジ ドメインごとに IGMP スヌーピング カウンタを表示します。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP マルチキャスト コマンド	『Cisco IOS IP Multicast Command Reference』
ASR 1000 シリーズ ルータの設定	『Cisco ASR 1000 Series Aggregation Services Routers Configuration Guides』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IGMP スヌーピングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *1*：*IGMP* スヌーピング設定の機能情報

機能名	リリース	機能情報
IGMP スヌーピング	Cisco IOS XE Release 3.5S 15.2(4)S	IGMP スヌーピングは、イーサネット仮想接続（EVC）インフラストラクチャに基づいた、IP マルチキャスト抑制メカニズムです。 IGMP スヌーピングは、ホストとルータ間で送信される IGMP パケットのレイヤ 3 情報（IGMP Join/Leave メッセージ）を検査します。 次のコマンドが導入または変更されました。**ip igmp snooping**、**ip igmp snooping check**、 **ip igmp snooping explicit-track ing limit**、**ip igmp snooping immediate leave**、**ip igmp snooping last-member-query count**、**ip igmp snooping last-member-query interval**、**ip igmp snooping report-suppression**、**ip igmp snooping robustness-variable**、**ip igmp snooping static**、**ip igmp snooping tcn flood** (if-srv)、**ip igmp snooping tcn flood query**、**ip igmp snooping tcn flood query solicit**、**router guard ip multicast efps**