CGMP とスパニング ツリー トポロジの変更に関するマルチキャスト エントリの再構築

内容

概要
前提条件
要件
使用するコンポーネント
表記法
CGMP およびトポロジーの変更
安定状態
トポロジー変更中およびトポロジー変更後
トポロジ変更通知の後の2つのIGMP概要クエリー
CGMP 機能拡張
スイッチとルータ間の通信
ルータの動作
Catalyst スイッチの動作
関連情報

概要

このドキュメントでは、スパニングツリー トポロジの変更発生後に、CGMP のマルチキャスト エントリの再構築に関して、Cisco Catalyst スイッチと Cisco IOS® ルータ上で、Cisco Group Management Protocol（CGMP）がどのように動作しているかを説明します。

前提条件

要件

次の項目に関する知識があることを推奨しています。

- スイッチ、ルータ、およびマルチキャスティングの基本動作
- スパニング ツリー、CGMP、および Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）の基本動作

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Catalyst 3550 バージョン 12.1(9)EA1c

- Catalyst 2900/3500XL バージョン 12.0(5)WC3b
- Catalyst 4000 スーパバイザ エンジン III バージョン 12.1(11b)EW
- Catalyst 4000 スーパバイザ エンジン I/II バージョン 7.2(2)
- Catalyst 6500 スーパバイザ エンジン Cisco IOS ソフトウェア リリース 12.1(11b)EX
- Catalyst 6500 Catalyst OS（CatOS）バージョン 7.2(2)
- Catalyst 5500 CatOS バージョン 4.5(13a)

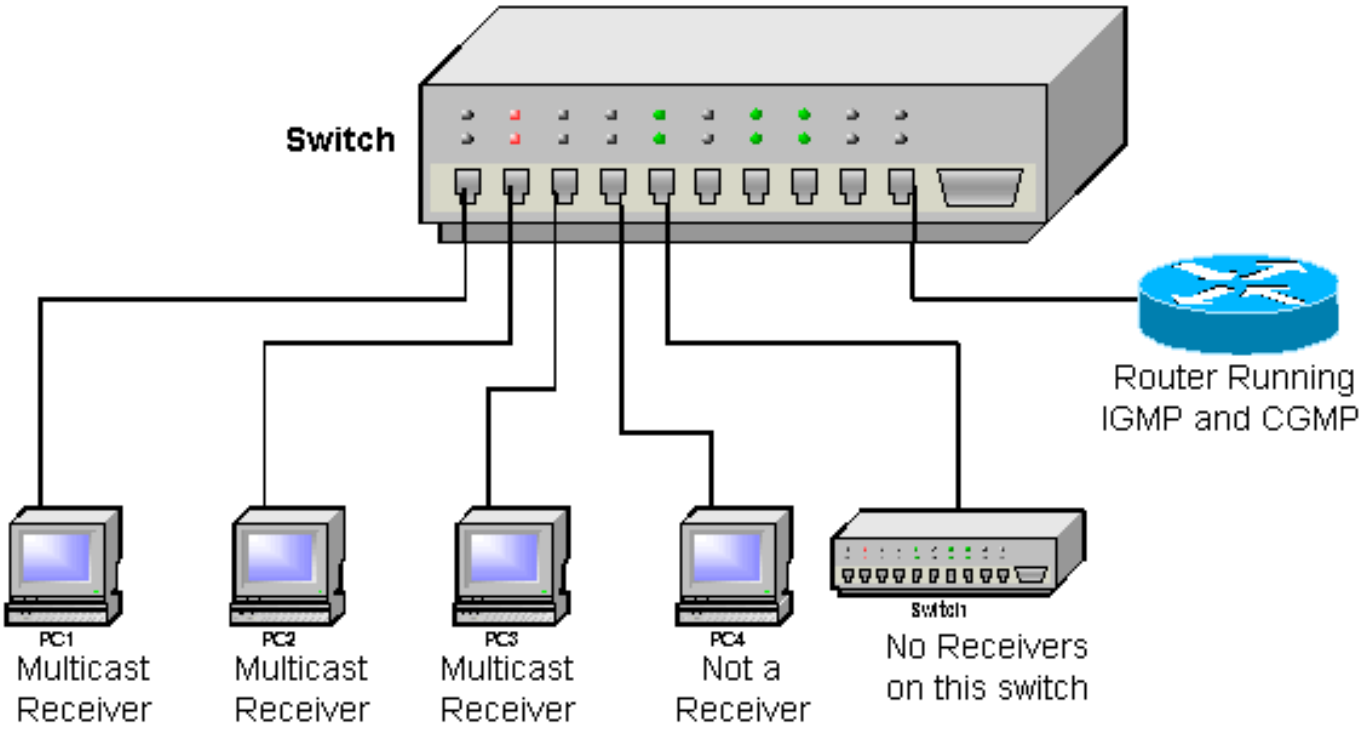
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

CGMP およびトポロジーの変更

このセクションでは、CGMP が使用されている VLAN 上でスパニング ツリー トポロジの変更が検出された場合、マルチキャスト トラフィックがすべてのポートでフラッディングしないように、どのような動作が行われるか、およびどのような問題が発生する可能性があるかを、順を追って説明します。次の例が示すように、このドキュメントで説明されているネットワークは、1 つのルータ、1 つのスイッチ、および 4 つの PC で構成されています。



- ポート1：レシーバPC 1
- ポート2：レシーバPC 2
- ポート3：レシーバPC 3
- ポート4：レシーバPC 4ではありません
- ポート 5 — 他のスイッチ（このスイッチにはレシーバやルータは備わっていません）
- ポート 48 — IGMP と CGMP を実行している Cisco IOS ルータ

このドキュメントでは、レシーバ PC が IGMP を使用し、スイッチが CGMP を実行することを

前提としています。Cisco IOS ルータでは、別のインターフェイスでビデオ サーバからマルチキャスト ストリームを受信する IGMP と CGMP を実行しています。このインターフェイスは、IP マルチキャスト グループ 239.100.100.100 に送信します。

安定状態

すべてのデバイスを起動し、レシーバ PC がグループ 239.100.100.100 に対して IGMP 加入メッセージを送信すると、これらのデバイスはすべて、CGMP によって対応するレイヤ 2 グループ（MAC アドレス 01-00-5e-64-64-64）に追加されます。

次のリストでは、Cisco IOS ルータ経由でマルチキャスト ストリームを受信する、スイッチ上のポートを太字で示しています。

- **ポート1：レシーバPC 1**
- **ポート2：レシーバPC 2**
- **ポート3：レシーバPC 3**
- ポート4：レシーバPC 4ではありません
- ポート 5 — 他のスイッチ（このスイッチにはレシーバやルータは備わっていません）
- ポート 48 — IGMP と CGMP を実行している Cisco IOS ルータ

注：Cisco IOSルータはマルチキャストグループにも追加されますが、送信元であるため、独自のパケットを受信しません。

すべてのクエリ インターバルで、Cisco IOS ルータは IGMP 一般クエリを送信します（これは、マルチキャスト グループ 224.0.0.1 に送信されるため、他のすべてのコンポーネントにフラッディングされます）。 この場合に、すべてのレシーバで 239.100.100.100 グループの IGMP レポートの作成が開始されます。レシーバはこのレポートをIPマルチキャストグループ239.100.100.100に送り返し、レイヤ2 MACアドレスは01-00-5E-64-64-64です。これはグループアドレスに送られるため、すべてのレシーバは他のレシーバから送られたレポートと最初のレシーバから送り返されたレポートを受信します。このため、他のレシーバ PC は、このグループに対するレポートをキャンセルします。つまり、このグループには、最初に応答した PC のソース MAC アドレスを使用して CGMP 加入メッセージが 1 つしか送信されないことになります。この状態は長期間継続し、すべてのレシーバ PC がビデオ ブロードキャストを受信します。

トポロジー変更中およびトポロジー変更後

この時点で、他のスイッチは、ネットワークのトポロジの変更をトリガーします。トポロジの変更受信時の CGMP 仕様ごとに、スイッチは、CGMP を介して学習していたすべてのマルチキャスト項目をクリアします。ルータからのマルチキャスト トラフィックは、スイッチ上のすべてのポートにフラッディングされます。

次のリストでは、Cisco IOS ルータ経由でマルチキャスト ストリームを受信する、スイッチ上のポートを太字で示しています。

- **ポート1：レシーバPC 1**
- **ポート2：レシーバPC 2**
- **ポート3：レシーバPC 3**
- **ポート4：レシーバPC 4ではありません**
- **ポート 5 — 他のスイッチ（このスイッチにはレシーバやルータは備わっていません）**
- ポート 48 — IGMP と CGMP を実行している Cisco IOS ルータ

トラフィックはすべてのポートにフラッディングされるので、レシーバ PC は差異に気付かず、

ビデオ ブロードキャストを受信し続けます。しかし、トラフィックはすべてのポートにフラッディングされるので、非レシーバである PC 4 とその他のスイッチも、要求していなくても、マルチキャスト ストリームを受信するようになります。この状態は、Cisco IOS ルータが周期的な IGMP 一般クエリーを再び送信するまで続きます。Cisco IOS ルータでは、このデフォルト値が 60 秒に設定されています (IP IGMP クエリー インターバルを使用して設定) 。

トポロジ変更通知の後の2つのIGMP概要クエリー

Cisco IOS ルータが最初の IGMP 一般クエリを送信すると、すべてのレシーバ PC で 239.100.100.100 グループの IGMP レポートの作成が開始します。その内の 1 台 (この文書では PC 3) が、最初に IGMP レポートを送り返します。スイッチ上ではマルチキャスト エントリがまだ構築されていないので、このレポートはすべての PC で受信され、他のレシーバ PC は自分の IGMP レポートをキャンセルします。Cisco IOS ルータはそのレポートを受信し、レシーバ PC 3 の送信元アドレスを付加して、以降の CGMP 加入メッセージを送信します。

スイッチはグループ 01-00-5e-64-64-64 に対してマルチキャスト エントリを再度作成し、ポート 3 をそのエントリに追加します。これはポート 3 が CGMP 加入パケットの送信元アドレスであることを示します。ポート 5 はマルチキャスト ルータ ポートであるため、ポート 5 はマルチキャスト グループにも追加されます。したがって、レシーバ PC 3 だけがビデオ ストリームを受信し、PC1 と PC 2 のビデオ ストリームは静止したままです。

次のリストでは、Cisco IOS ルータ経由でマルチキャスト ストリームを受信する、スイッチ上のポートを太字で示しています。

- ポート1：レシーバPC 1
- ポート2：レシーバPC 2
- **ポート3：レシーバPC 3**
- ポート4：レシーバPC 4ではありません
- ポート 5 — 他のスイッチ (このスイッチにはレシーバやルータは備わっていません)
- ポート 48 — IGMP と CGMP を実行している Cisco IOS ルータ

IGMP クエリ インターバルの終了時に、Cisco IOS ルータは、別の IGMP 一般クエリを送信します。クエリーが受信されると、すべてのレシーバ PC で 239.100.100.100 グループのレポートが作成されます。ただし今回は、他の PC からのレポートを受信するのはレシーバ PC 3 と Cisco IOS ルータのみです。(ルータのポートは、すべてのマルチキャスト グループに自動的に追加されます) 。

レシーバ PC 1 と PC 2 は他のレシーバからのレポートを受信しないため、PC1 と PC 2 は両方とも自分のレポートを送信します。次に Cisco IOS ルータは、それぞれの PC の送信元 MAC アドレスを付加した CGMP 加入メッセージを送信するため、2 台の PC は両者とも追加され、Cisco IOS ルータ経由のマルチキャスト ストリームの受信を再開します。

次のリストでは、Cisco IOS ルータ経由でマルチキャスト ストリームを受信する、スイッチ上のポートを太字で示しています。

- **ポート1：レシーバPC 1**
- **ポート2：レシーバPC 2**
- **ポート3：レシーバPC 3**
- ポート4：レシーバPC 4ではありません
- ポート 5 — 他のスイッチ (このスイッチにはレシーバやルータは備わっていません)
- ポート 48 — IGMP と CGMP を実行している Cisco IOS ルータ

設定が元の安定状態に戻り、再び正常に動作します。実際の動作の詳細を次に示します。

1. トポロジの変更が発生します。**ヒント：ホストポートでPortFastが有効になっていない**場合、ホストがリブートされたり、ポートに接続/切断されたりするたびに、リンクステータスが変更されると、VLANのトポロジ変更通知がトリガーされます。トポロジ変更の際にCGMP のデバッグが有効にされる場合、このデバッグ メッセージが表示されます。
   ```
   CGMP SHIM: got short age timer
   ```
2. すべてのポートへのフラッディングが開始します。
3. 最初の IGMP 一般クエリーが送信される。
4. フラッディングが停止します。
5. すべてのレシーバがマルチキャスト ストリームを受信するわけではありません。
6. 2 番目の IGMP 一般クエリーが送信される。
7. すべてのレシーバが追加され、マルチキャスト ストリームを再び受信します。

CGMP 機能拡張

PC の場合、マルチキャスト ストリームの 1 分間 (デフォルトの IGMP クエリ インターバル) の損失は必ずしも許容されるわけではないため、CGMP を実行しているルータとスイッチの両方が強化されています。

スイッチとルータ間の通信

ルータはレイヤ 3 デバイスであり、発生したスパニング ツリーとトポロジの変更を通常は認識しないため、ネットワーク内のスイッチがトポロジの変更をルータに警告する必要があります。これを処理するために IGMP グローバル Leave メッセージが定義されています。

この IGMP グローバル Leave メッセージは、グループ 0.0.0.0 を終了するよう要求するためにスイッチが送信できる IGMP リーブです。

IGMP グローバル Leave メッセージでルータに過負荷がかからないようにするため、トポロジの変更終了後、スパニング ツリー ドメインのルート スイッチだけが、この IGMP グローバル Leave メッセージの送信の役割を負います。

ルータの動作

ルータが Cisco IOS ソフトウェアを実行しているインターフェイス上でこの IGMP グローバル Leave メッセージを受信すると、ルータは、そのインターフェイスでスパニング ツリー トポロジの変更が発生したことを認識し、次のアクションを実行して、マルチキャスト レシーバのマルチキャスト トラフィックの損失を制限しようとします。

1. IGMP グローバル Leave メッセージを受信した後の CGMP 一括加入メッセージの送信。ルータは自分の MAC アドレスを付加した CGMP 加入メッセージを、そのインターフェイスに対する IGMP キャッシュに保存しているすべてのマルチキャスト グループのユーザ送信元アドレスとして送信します。これらの CGMP 自己加入メッセージを送信することにより、CGMP スイッチは、ルータ ポートのみを含めてグループごとにエントリを自動的に作成します。次のリストは、CGMP 一括加入後に、この文書で使用されたネットワークを示しています。太字で示されているように、Cisco IOS ルータだけがマルチキャスト グループに追加されています。**注：このドキュメントの前の例では、マルチキャストルータからトラフィックを受信するポートは太字で示されていましたが、この例では、スイッチ上でマルチキャストグループに追加されたすべてのポートを示しています。**ポート1：レシーバPC 1ポート2：レシーバPC 2ポート3：レシーバPC 3ポート4：レシーバPC 4ではありませんポート 5

— 他のスイッチ（このスイッチにはレシーバやルータは備わっていません）**ポート 48 — IGMP と CGMP を実行している Cisco IOS ルータ**

2. IGMP 一般クエリの送信。すべてのレシーバがこの IGMP 一般クエリを受信し、加入したすべてのグループに対してレポートを作成します。CGMP スイッチでは、ルータのみをレシーバとしてグループごとにマルチキャスト エントリがすでに構築されているので、レポートはすべてルータのみに送信されます。すべてのレシーバを対応するグループに追加するため、ルータは後続の CGMP 加入メッセージを送信します。すべてのレシーバが IGMP レポートを送り返して、ルータが対応する CGMP 加入メッセージを送信した後、すべてのレシーバがマルチキャスト グループに追加されたはずです。
3. 10 秒後（デフォルトの IGMP max-response-time）、別の IGMP 一般クエリが送信され、すべてのレシーバが追加されるようにします。すべてのレシーバがマルチキャスト グループ再加入を確認するために、このステップが数回繰り返されます。この例で太字で示されているように、すべてのポートがマルチキャスト グループに追加されています。**ポート1：レシーバPC 1ポート2：レシーバPC 2ポート3：レシーバPC 3**ポート4：レシーバPC 4ではありませんポート 5 — 他のスイッチ（このスイッチにはレシーバやルータは備わっていません）**ポート 48 — IGMP と CGMP を実行している Cisco IOS ルータ**

Catalyst スイッチの動作

Catalyst スイッチは、種類によってその動作に多少の違いがあります。CGMP 対応のすべてのスイッチがこのドキュメントの「CGMP およびトポロジーの変更 」セクションで説明されているとおりに行います。ただし、CGMP に加えた改良はすべてのプラットフォームで実装されているわけではありません。次の表で、Catalyst スイッチのリストと、Catalyst スイッチの CGMP に対する反応を記述します。

	CGMP スイッチ	CGMP ルータ	Spanning Tree Protocol（STP; スパニング ツリー プロトコル）ルート時にグローバル Leave を送信する
Cisco IOS ソフトウェアを実行している Catalyst 6500	N	Y	Y
CatOS を実行している Catalyst 6500	N	N	N
Catalyst 5500、Catalyst 2926/2926G	Y	N	Y
Catalyst 4000 スーパバイザ エンジン I/II、Catalyst 2948G/2980G、Catalyst 4912G	Y	N	Y
Catalyst 4000/4500 Supervisor Engine III/IV	N	Y	Y
Catalyst 2900XL/3500XL	Y	N	Y

Catalyst 2940	N	N	N
Catalyst 2950	N	N	N
Catalyst 2970	N	N	N
Catalyst 3550	N	Y	Y
Catalyst 3750	N	Y	Y

注：Supervisor Engine III/IVを搭載したCatalyst 4000/4500では、トポロジの変更とCGMPに関する動作を設定できます。このコマンドを発行して、Catalyst 4000 がスパニング ツリーのルートでない場合に、IGMP グローバル Leave メッセージを送信するかどうかを設定します。

- ip igmp snooping tcn query solicit

注：このコマンドを無効にするには、次の「no」形式を発行します。

- no ip igmp snooping tcn query solicit

関連情報

- スパニングツリー プロトコル トポロジの変更について
- キャンパス ネットワークにおけるマルチキャスト：CGMP および IGMP スヌーピング
- Catalyst OS が稼働する Catalyst スイッチ上で同じ VLAN 上に送信側と受信側が存在する場合のマルチキャスト トラフィックの制限
- Catalyst 4000 Cisco IOS ソフトウェアの構成ガイド：IGMP スヌーピングの理解と設定
- スパニング ツリーに関するテクニカル サポート ページ
- LAN 製品に関するサポート ページ
- LAN スイッチングに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems