



CHAPTER 26

IGMP スヌーピングとフィルタリングの設定

この章では、Catalyst 4500 シリーズ スイッチ上でインターネット グループ管理プロトコル (IGMP) スヌーピングを設定する方法について説明します。設定上の注意事項、設定手順、および設定例も示します。

この章で説明する主な内容は、次のとおりです。

- 「IGMP スヌーピングについて」 (P.26-1)
- 「IGMP スヌーピングの設定」 (P.26-5)
- 「IGMP スヌーピング情報の表示」 (P.26-15)
- 「IGMP フィルタリングの設定」 (P.26-20)
- 「IGMP フィルタリングの設定の表示」 (P.26-24)



(注) Cisco Group Management Protocol (CGMP) クライアント デバイスをサポートするには、スイッチを CGMP サーバとして設定します。詳細については、次の URL の『Cisco IOS IP and IP Routing Configuration Guide, Cisco IOS Release 12.1』の「IP Multicast」および「Configuring IP Multicast Routing」の章を参照してください。

http://www.cisco.com/en/US/docs/ios/12_1/iproute/configuration/guide/ip_c.html



(注) この章で使用するスイッチ コマンドの構文および使用方法の詳細については、次の URL で『Cisco Catalyst 4500 Series Switch Command Reference』と関連資料を参照してください。

<http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html>

『Catalyst 4500 Series Switch Command Reference』に掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で『Catalyst 4500 Series Switch Cisco IOS Command Reference』と関連資料を参照してください。

<http://www.cisco.com/en/US/products/ps6350/index.html>

IGMP スヌーピングについて

ここでは、次の内容について説明します。

- 「即時脱退処理」 (P.26-3)

- 「IGMP 脱退タイマーの設定」 (P.26-4)
- 「IGMP スヌーピング クエリア」 (P.26-4)
- 「明示的ホスト トラッキング」 (P.26-5)



(注) QoS (Quality of Service) は、IGMP パケットに適用しません。

IGMP スヌーピングにより、スイッチはホストとルータ間で送信される IGMP パケットの情報をスヌーピングまたはキャプチャします。この情報に基づいて、スイッチはアドレス テーブルに対してマルチキャスト アドレスの追加または削除を行い、マルチキャスト トラフィックの個々のホストポートへのフローをイネーブル (またはディセーブル) に設定します。IGMP スヌーピングは、IGMPv1、IGMPv2、および IGMPv3 のすべてのバージョンの IGMP をサポートします。

IGMPv1 および IGMPv2 とは対照的に、IGMPv3 スヌーピングはデフォルトで即時脱退処理を提供します。これによって明示的ホスト トラッキング (EHT) が提供され、ネットワーク管理者は IGMPv3 をサポートするレイヤ 2 デバイス上に SSM 機能を配置できます (「明示的ホスト トラッキング」 (P.26-5) を参照してください)。IGMP が設定されているサブネットにおいて、IGMP スヌーピングはレイヤ 2 でマルチキャスト トラフィックを管理します。switchport キーワードを使用して、受信に関心のあるインターフェイスにのみマルチキャスト トラフィックを動的に転送するようにインターフェイスを設定できます。

IGMP スヌーピングは、MAC マルチキャスト グループ 0100.5e00.0001 ~ 01-00-5e-ff-ff-ff のトラフィックを制限します。IGMP スヌーピングは、ルーティング プロトコルによって生成されたレイヤ 2 マルチキャスト パケットを制限しません。



(注) IP マルチキャストおよび IGMP の詳細については、RFC 1112、RFC 2236、RFC 3376 (IGMPv3) を参照してください。

(ルータ上で設定された) IGMP は定期的に IGMP 一般クエリーを送信します。ホストは、関心のあるグループの IGMP メンバーシップ レポートでこれらのクエリーに応答します。IGMP スヌーピングがイネーブルの場合、スイッチは IGMP Join 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、VLAN ごとに 1 つのエントリを作成します。このマルチキャスト トラフィックに関心を示しているすべてのホストは IGMP メンバーシップ レポートを送信し、転送テーブル エントリに追加されます。

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、ip igmp snooping static コマンドを使用して、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。静的にグループ メンバーシップを指定する場合、その設定は IGMP スヌーピングによる自動的な処理より優先されます。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 スヌーピング設定値の両方で構成できます。

0100.5E00.0001 ~ 0100.5E00.00FF 範囲のマルチキャスト MAC アドレスにマッピングする 224.0.0.0 ~ 224.0.0.255 の範囲の IP アドレスを持つグループは、ルーティング制御パケット専用です。これらのグループは、IGMPv3 メンバーシップ レポートに使用される 224.0.0.22 を除いて、VLAN のすべての転送ポートにフラッドされます。



(注) VLAN でスパンニングツリー トポロジが変更された場合、PortFast がイネーブルになっていないすべての VLAN ポート、および Topology Change Notification (TCN; トポロジ変更通知) クエリー カウント期間に no igmp snooping tcn flood コマンドが設定されたポートに、IP マルチキャスト トラフィックがフラッドされます。

レイヤ 2 IGMPv2 ホスト インターフェイスは IP マルチキャスト グループに加入するため、IP マルチキャスト グループの IGMP メンバーシップ レポートを送信します。ホストをマルチキャスト グループから脱退させるには、そのホストで定期的な IGMP 一般クエリーを無視するか、または IGMP Leave メッセージを送信します。スイッチはホストから IGMP Leave メッセージを受け取ると、IGMP グループ固有のクエリーを送信して、そのインターフェイスに接続されたデバイスが特定のマルチキャスト グループのトラフィックに関心を示しているかどうかを判別します。スイッチはそのレイヤ 2 マルチキャスト グループのテーブル エントリを更新して、グループのマルチキャスト トラフィックの受信に関心を示しているホストだけがリストされるようにします。

対照的に、IGMPv3 ホストは、特定のマルチキャスト グループに加入するために (**allow** グループ レコード モードで) IGMPv3 メンバーシップ レポートを送信します。IGMPv3 ホストが、以前の送信元リストにあるすべての送信元からのトラフィックを拒否するために (**block** グループ レコードで) メンバーシップ レポートを送信する場合、EHT がイネーブルにされていると、ポートの最後のホストは即時脱退によって削除されます。

即時脱退処理

IGMP スヌーピングの即時脱退処理を使用すると、スイッチはインターフェイスに IGMP グループ固有のクエリーを事前に送信せず、そのインターフェイスを転送テーブル エントリから削除します。VLAN インターフェイスは、オリジナルの IGMP Leave メッセージで指定されたマルチキャスト グループのマルチキャスト ツリーからプルーニングされます。複数のマルチキャスト グループが同時に使用される場合でも、即時脱退処理により、スイッチド ネットワーク上のすべてのホストに対して最適な帯域幅管理が可能になります。

IGMP スヌーピングをイネーブルにしたスイッチが IGMPv2 または IGMPv3 Leave メッセージを受け取ると、Leave メッセージを受け取ったインターフェイスから IGMP グループ固有のクエリーを送信し、MAC マルチキャスト グループへの加入に関心を示した他のホストがそのインターフェイスに接続するタイミングを判断します。スイッチがクエリー応答間隔で IGMP Join メッセージを受信しない場合、レイヤ 2 転送テーブルのポート リスト (MAC-group、VLAN) エントリからインターフェイスが削除されます。



(注) デフォルトでは、すべての IGMP Join はすべてのマルチキャスト ルータ ポートに転送されます。

VLAN 上で即時脱退処理をイネーブルに設定すると、マルチキャスト ルータがポート上で学習されている場合を除き、IGMP Leave メッセージを受信した時点で、レイヤ 2 エントリのポート リストからインターフェイスをただちに削除できます。



(注) IGMPv2 スヌーピングを使用する場合、即時脱退処理は各インターフェイスに 1 つのホストしか接続されていない VLAN でのみ使用してください。インターフェイスに複数のホストが接続されている VLAN 上で即時脱退処理をイネーブルにすると、一部のホストが偶発的にドロップされる可能性があります。IGMPv3 を使用する場合、即時脱退処理がデフォルトでイネーブルにされており、明示的ホスト トラッキングにより、スイッチはポートに IGMPv3 ホストのスイッチによって維持されるホストが単一または複数であるときに検出できます。その結果、スイッチは特定のポートの背後で単一ホストを検出すると即時脱退処理を実行できます。



(注) IGMPv3 は、古いバージョンの IGMP との相互運用が可能です。

特定の VLAN での IGMP バージョンを表示するには、**show ip igmp snooping querier vlan** コマンドを使用します。

スイッチが IGMPv3 スヌーピングをサポートするかどうかを表示するには、**show ip igmp snooping vlan** コマンドを使用します。

IGMPv2 の即時脱退をイネーブルにするには、**ip igmp snooping immediate-leave** コマンドを使用します。



(注) IGMPv3 では、デフォルトで即時脱退処理がイネーブルに設定されています。

IGMP 脱退タイマーの設定

複数のホストが単一インターフェイスに接続されている VLAN では、即時脱退処理は使用できません。このような状況での脱退の遅れを減少させるため、IGMPv3 では設定可能な脱退タイマーを提供します。

Cisco IOS Release 12.2(25)SG 以前のリリースでは、IGMP スヌーピング脱退時間はクエリーの応答時間に基づいていました。クエリーのクエリー応答時間が満了する前にスイッチがメンバーシップ レポートを受信しなかった場合、ポートはマルチキャスト グループ メンバーシップから削除されます。

Cisco IOS Release 12.2(31)SG 以降のリリースでは、ホストの特定マルチキャスト グループへの関心が続いているかどうかを判断するために、グループ固有のクエリーを送信したあとにスイッチが待機する時間を設定できます。IGMP 脱退応答時間は、100 ~ 5000 ミリ秒の間で設定できます。このタイマーは、グローバルでも、VLAN 単位でも設定できます。VLAN に脱退時間を設定すると、グローバルに設定した脱退時間は上書きされます。

設定手順については、「[IGMP 脱退タイマーの設定](#)」(P.26-9)を参照してください。

IGMP スヌーピング クエリア

IGMP スヌーピング クエリア サポートは、Cisco IOS Release 12.2(50) SG で導入されました。これは、マルチキャスト トラフィックではルーティングが必要ないため PIM および IGMP が設定されていない VLAN 内で、IGMP スヌーピングをサポートするために必要なレイヤ 2 機能です。

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、一般クエリーを送信することにより、IP マルチキャスト ルータが IGMP クエリアとして機能します。VLAN 内の IP マルチキャスト トラフィックにおいてレイヤ 2 スイッチだけが必要な場合、IP マルチキャスト ルータは必要ありません。VLAN 上に IP マルチキャスト ルータがない場合は、クエリーを送信できるように別のスイッチを IGMP クエリアとして設定する必要があります。

イネーブルにすると、IGMP スヌーピング クエリアは定期的な IGMPv2 クエリーを送信します。このクエリーにより、IP マルチキャスト トラフィックを要求するスイッチからの IGMP レポートメッセージがトリガーされます。IGMP スヌーピングはこれらの IGMP レポートを待ち受けて、適切な転送を確立します。

IGMP を使用して IP マルチキャスト トラフィックへの関与を報告するするスイッチにおいて、サポートされている各 VLAN の IGMP スヌーピング クエリアとして少なくとも 1 つのスイッチを設定します。

IP マルチキャスト ルーティングがイネーブルであるかどうかに関係なく、VLAN 上で IGMP クエリーを生成するようにスイッチを設定できます。

明示的ホスト トラッキング

明示的ホスト トラッキング (EHT) は、IGMPv3 メンバーシップ レポートを送信するホストを追跡することによって、グループ メンバーシップをモニタリングします。この追跡によって、スイッチは各ポートのグループに対応付けられたホスト情報を検出できます。また、ユーザも EHT によってメンバーシップおよび各種の統計情報を追跡できます。

EHT では、スイッチはポート単位でメンバーシップを追跡できます。そのため、スイッチは各ポートに存在するホストを認識し、ポートの背後にホストが 1 つだけ存在する場合に即時脱退処理を実行できます。

EHT が VLAN 上でイネーブルにされているかどうかを判別するには、`show ip igmp snoop vlan` コマンドを使用します。

IGMP スヌーピングの設定



(注) IGMP を設定する場合は、VLAN データベース モードで VLAN を設定してください。第 16 章「VLAN、VTP、および VMPS の設定」を参照してください。

IGMP スヌーピングにより、スイッチで IGMP パケットを調べたり、パケットの内容に基づいて転送先を決定したりできます。

ここでは、IGMP スヌーピングを設定する手順について説明します。

- 「IGMP スヌーピングのデフォルト設定」 (P.26-5)
- 「IGMP スヌーピングのグローバルなイネーブル化」 (P.26-6)
- 「VLAN 上での IGMP スヌーピングのイネーブル化」 (P.26-7)
- 「学習方式の設定」 (P.26-7)
- 「マルチキャスト ルータへの静的な接続の設定」 (P.26-8)
- 「IGMP 即時脱退処理のイネーブル化」 (P.26-9)
- 「IGMP 脱退タイマーの設定」 (P.26-9)
- 「IGMP スヌーピング クエリアの設定」 (P.26-10)
- 「明示的ホスト トラッキングの設定」 (P.26-11)
- 「ホストの静的な設定」 (P.26-12)
- 「マルチキャスト フラッドの抑制」 (P.26-12)

IGMP スヌーピングのデフォルト設定

表 26-1 に、IGMP スヌーピングのデフォルト設定値を示します。

表 26-1 IGMP スヌーピングのデフォルト設定値

機能	デフォルト値
IGMP スヌーピング	イネーブル
マルチキャスト ルータ	未設定

表 26-1 IGMP スヌーピングのデフォルト設定値 (続き)

機能	デフォルト値
明示的ホスト トラッキング	IGMPv3 ではイネーブル。IGMPv2 では使用不可
即時脱退処理	IGMPv3 ではイネーブル。IGMPv2 ではディセーブル
レポート抑制	イネーブル
IGMP スヌーピングの学習方式	PIM/DVMRP ¹

1. PIM/DVMRP = Protocol Independent Multicast/Distance Vector Multicast Routing Protocol

IGMP スヌーピングのグローバルなイネーブル化

IGMP スヌーピングをグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ1	Switch# 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2	Switch(config)# [no] ip igmp snooping	IGMP スヌーピングをイネーブルにします。 IGMP スヌーピングをディセーブルにするには、 no キーワードを使用します。
ステップ3	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ4	Switch# show ip igmp snooping include	設定を確認します。

次に、IGMP スヌーピングをグローバルにイネーブルにし、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping
Switch(config)# end
Switch# show ip igmp snooping
Global IGMP Snooping configuration:
-----
IGMP snooping           : Enabled
IGMPv3 snooping         : Enabled
Report suppression      : Enabled
TCN solicit query       : Disabled
TCN flood query count   : 2

Vlan 1:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave  : Disabled
Explicit host tracking   : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY

Vlan 2:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave  : Disabled
Explicit host tracking   : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
```

VLAN 上での IGMP スヌーピングのイネーブル化

VLAN 上で IGMP スヌーピングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ1	Switch(config)# [no] ip igmp snooping vlan vlan_ID	IGMP スヌーピングをイネーブルにします。 IGMP スヌーピングをディセーブルにするには、no キーワードを使用します。
ステップ2	Switch(config)# end	コンフィギュレーションモードを終了します。
ステップ3	Switch# show ip igmp snooping vlan vlan_ID	設定を確認します。

次に、VLAN 2 上で IGMP スヌーピングをイネーブルにし、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 2
Switch(config)# end
Switch# show ip igmp snooping vlan 2
Global IGMP Snooping configuration:
-----
IGMP snooping           : Enabled
IGMPv3 snooping        : Enabled
Report suppression     : Enabled
TCN solicit query      : Disabled
TCN flood query count  : 2

Vlan 2:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave : Disabled
Explicit host tracking  : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
```

学習方式の設定

ここでは IGMP スヌーピングの学習方式について説明します。

- 「PIM/DVMRP 学習方式の設定」(P.26-7)
- 「CGMP 学習方式の設定」(P.26-8)

PIM/DVMRP 学習方式の設定

IGMP スヌーピングを PIM/DVMRP パケットから学習するように設定するには、次の作業を行います。

コマンド	目的
Switch(config)# ip igmp snooping vlan vlan_ID mrouter learn [cgmp pim-dvmrp]	VLAN の学習方式を指定します。

次に、IP IGMP スヌーピングが PIM/DVMRP パケットから学習するように設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

```
Switch(config)# end
Switch#
```

CGMP 学習方式の設定

IGMP スヌーピングを CGMP self-join パケットから学習するように設定するには、次の作業を行います。

コマンド	目的
Switch(config)# ip igmp snooping vlan <i>vlan_ID</i> mrouter learn [cgmp pim-dvmrp]	VLAN の学習方式を指定します。

次に、IP IGMP スヌーピングが CGMP self-join パケットから学習するように設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 mrouter learn cgmp
Switch(config)# end
Switch#
```

マルチキャスト ルータへの静的な接続の設定

マルチキャスト ルータへの静的な接続を設定するには、スイッチ上で **ip igmp snooping vlan mrouter interface** コマンドを入力します。

マルチキャスト ルータへの静的な接続を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# 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 2	Switch(config)# ip igmp snooping vlan <i>vlan_ID</i> mrouter interface <i>interface_num</i>	VLAN のマルチキャスト ルータとの静的な接続を指定します。 (注) ルータとのインターフェイスは、コマンドを入力する VLAN 内になければなりません。ルータとラインプロトコルはアップ状態である必要があります。
ステップ 3	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show ip igmp snooping mrouter vlan <i>vlan_ID</i>	設定を確認します。

次の例では、マルチキャスト ルータへの静的な接続を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 mrouter interface fastethernet 2/10
Switch# show ip igmp snooping mrouter vlan 200
vlan  ports
-----+-----
 200  Fa2/10
Switch#
```


IGMP 即時脱退処理のイネーブル化

VLAN 上で IGMP 即時脱退処理をイネーブルにした場合、インターフェイス上で IGMPv2 Leave メッセージを検出すると、スイッチはマルチキャスト グループからインターフェイスを削除します。



(注) IGMPv3 では、EHT とのデフォルトで即時脱退処理がイネーブルに設定されています。

IGMPv2 インターフェイスで即時脱退処理をイネーブルにするには、次の作業を行います。

コマンド	目的
Switch(config)# ip igmp snooping vlan vlan_ID immediate-leave	VLAN で即時脱退処理をイネーブルにします。 (注) このコマンドは、IGMPv2 ホストだけに適用します。

次に、VLAN 200 インターフェイス上で IGMP 即時脱退処理をイネーブルにし、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 immediate-leave
Configuring immediate leave on vlan 200
Switch(config)# end
Switch# show ip igmp interface vlan 200 | include immediate leave
Immediate leave           : Disabled
Switch(config)#
```

IGMP 脱退タイマーの設定

IGMP 脱退タイマーを設定するときには、次の注意事項に従ってください。

- 脱退時間は、グローバルでも、VLAN 単位でも設定できます。
- VLAN 上に脱退時間を設定すると、グローバルに設定された内容は上書きされます。
- デフォルトの脱退時間は 1000 ミリ秒です。
- IGMP の脱退時間の設定は、IGMP バージョン 2 が稼働しているホストでのみサポートされます。
- ネットワークで実際の脱退にかかる待ち時間は、通常、設定した脱退時間どおりになります。ただし、脱退時間は、リアルタイムの CPU の負荷の状態、およびネットワークの遅延状態、インターフェイスから送信されたトラフィック量によって、設定された時間を前後することがあります。

IGMP の設定可能な脱退タイマーをイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ1	Switch# 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2	Switch(config)# ip igmp snooping last-member-query-interval time	IGMP 脱退タイマーをグローバルに設定します。指定できる範囲は 100 ~ 5000 ミリ秒です。デフォルト値は 1000 秒です。 IGMP 脱退タイマーをグローバルにリセットしてデフォルト設定に戻すには、 no ip igmp snooping last-member-query-interval グローバル コンフィギュレーション コマンドを使用します。

■ IGMP スヌーピングの設定

	コマンド	目的
ステップ 3	Switch(config)# ip igmp snooping vlan vlan_ID last-member-query-interval time	(任意) VLAN インターフェイス上で IGMP 脱退時間を設定します。指定できる範囲は 100 ~ 5000 ミリ秒です。 特定の VLAN から設定した IGMP 脱退時間設定を削除するには、 no ip igmp snooping vlan vlan-id last-member-query-interval グローバル コンフィギュレーション コマンドを使用します。 (注) VLAN 上に脱退時間を設定すると、グローバルに設定されたタイマーは上書きされます。
ステップ 4	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# show ip igmp snooping	(任意) 設定された IGMP 脱退時間を表示します。
ステップ 6	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、IGMP 設定可能な脱退タイマーをイネーブルにし、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping last-member-query-interval 200
Switch(config)# ip igmp snooping vlan 10 last-member-query-interval 500
Switch(config)# end
Switch# show ip igmp snooping show ip igmp snooping
Global IGMP Snooping configuration:
-----

IGMP snooping           : Enabled
IGMPv3 snooping        : Enabled
Report suppression     : Enabled
TCN solicit query      : Disabled
TCN flood query count  : 2
Last Member Query Interval : 200

Vlan 1:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave : Disabled
Explicit host tracking  : Enabled
Multicast router learning mode : pim-dvmrp
Last Member Query Interval : 200
CGMP interoperability mode : IGMP_ONLY

Vlan 10:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave : Disabled
Explicit host tracking  : Enabled
Multicast router learning mode : pim-dvmrp
Last Member Query Interval : 500
CGMP interoperability mode : IGMP_ONLY

Switch#
```

IGMP スヌーピング クエリアの設定

IGMP スヌーピング クエリア機能は、グローバルまたは VLAN 単位のいずれでもイネーブルにできます。



(注) IGMP スヌーピング クエリアはデフォルトでディセーブルです。

IGMP スヌーピング クエリアを設定するには、次の作業を行います。

	コマンド	目的
ステップ1	Switch# 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2	Switch(config)# [no] ip igmp snooping [vlan vlan_id] querier	IGMP スヌーピング クエリアをイネーブルにします。
ステップ3	Switch(config)# [no] ip igmp snooping [vlan vlan_id] querier address abcd	IGMP スヌーピング クエリアの送信元 IP アドレスを設定します。
ステップ4	Switch(config)# [no] ip igmp snooping [vlan vlan_id] querier version [1 2]	IGMP スヌーピング クエリアの IGMP バージョンを設定します。
ステップ5	Switch(config)# ip igmp snooping [vlan vlan_id] querier query-interval interval	IGMP スヌーピング クエリアのクエリー間隔を設定します。
ステップ6	Switch(config)# ip igmp snooping [vlan vlan_id] querier max-response-time value	IGMP スヌーピング クエリアの IGMP クエリーの最大応答時間を設定します。
ステップ7	Switch(config)# ip igmp snooping [vlan vlan_id] querier timer expiry value	IGMP スヌーピング クエリアの有効期限タイムアウトを設定します。
ステップ8	Switch(config)# ip igmp snooping [vlan vlan_id] querier tcn query count value	IGMP スヌーピング クエリアの IGMP クエリー カウントを設定します。
ステップ9	Switch(config)# ip igmp snooping [vlan vlan_id] querier tcn query interval value	IGMP スヌーピング クエリアの tcn クエリー間隔を設定します。
ステップ10	Switch(config)# end	特権 EXEC モードに戻ります。

スヌーピング クエリア情報を表示する方法の例については、「[IGMP スヌーピング クエリア情報の表示](#)」(P.26-19) を参照してください。

明示的ホスト トラッキングの設定

IGMPv3 では、EHT はデフォルトでイネーブルに設定されており、VLAN 単位でディセーブルにできません。

VLAN 上で EHT 処理をディセーブルにするには、次の作業を行います。

コマンド	目的
Switch(config)# [no] ip igmp snooping vlan vlan_ID explicit-tracking	VLAN 上で EHT をイネーブルにします。 EHT をディセーブルにするには、 no キーワードを使用します。

次に、VLAN 200 上で IGMP EHT をディセーブルにし、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 200 explicit-tracking
Switch(config)# end
```

```
Switch# show ip igmp snooping vlan 200 | include Explicit host tracking
Explicit host tracking          : Disabled
```

ホストの静的な設定

ホストは通常、マルチキャスト グループに動的に加入しますが、インターフェイス上でホストを静的に設定することもできます。

インターフェイス上でホストを静的に設定するには、次の作業を行います。

コマンド	目的
Switch(config-if)# ip igmp snooping vlan vlan_ID static mac_address interface interface_num	VLAN でホストを静的に設定します。 (注) このコマンドは、特定の送信元 IP アドレスのトラフィックを受信するには設定できません。

次に、VLAN 200 でファスト イーサネット インターフェイス 2/11 にホストを静的に設定する例を示します。

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 200 static 0100.5e02.0203 interface fastethernet
2/11
Configuring port FastEthernet2/11 on group 0100.5e02.0203 vlan 200
Switch(config)# end
```

マルチキャスト フラッドイングの抑制

IGMP スヌーピングがイネーブルに設定されたスイッチは、スパニングツリー Topology Change Notification (TCN) を受信すると、VLAN のすべてのポートにマルチキャスト トラフィックをフラッドイングします。マルチキャスト フラッドイングの抑制により、スイッチはこのようなトラフィックの送信を停止します。フラッドイングの抑制をサポートするために、Cisco IOS Release 12.1(11b)EW では次のインターフェイス コマンドおよびグローバル コマンドが導入されました。

- **[no | default] ip igmp snooping tcn flood** (インターフェイス コマンド)
- **[no | default] ip igmp snooping tcn flood query count [1 - 10]** (グローバル コマンド)
- **[no | default] ip igmp snooping tcn query solicit** (グローバル コマンド)

Cisco IOS Release 12.1(11b)EW よりも前のリリースでは、スイッチがスパニングツリー TCN を受信すると、3 回の IGMP クエリー インターバルの間、VLAN のすべてのポートにマルチキャスト トラフィックがフラッドイングされていました。これは冗長構成に必要でしたが、Cisco IOS Release 12.1(11b)EW では、スイッチがマルチキャスト フラッドイングを停止するまでのデフォルト時間は、2 回の IGMP クエリー インターバルに変更されました。

このフラッドイング動作は、フラッドイングを行うスイッチが別のグループに属する多くのポートを保有している場合には望ましくありません。トラフィックがスイッチとエンドホスト間でリンク容量を超え、パケットが失われることもあります。

no ip igmp snooping tcn flood コマンドを使用すると、トポロジ変更後にスイッチ インターフェイス上のマルチキャスト フラッドイングをディセーブルにできます。トポロジが変更されている間でも、ポートが加入しているマルチキャスト グループだけがそのポートに送信されます。

IGMP クエリーしきい値を設定して、トポロジ変更後すぐにスイッチ インターフェイス上のマルチキャスト フラッディングをイネーブルにするには、**ip igmp snooping tcn flood query count** コマンドを使用します。

トポロジが変更された場合、通常スパニングツリー ルート スイッチはグループ マルチキャスト アドレス 0.0.0.0 を使用してグローバル IGMP Leave メッセージ（「クエリー要求」と呼ばれる）を発行します。スイッチはこの要求を受け取ると、スパニングツリーが変更された VLAN のすべてのポートで要求をフラッディングします。アップストリーム ルータがこの要求を受け取ると、ただちに IGMP 一般クエリーを発行します。

ip igmp snooping tcn query solicit コマンドを使用すると、スパニングツリー以外のルート スイッチに同じクエリー要求を入力するように指示できます。

次の項では、新しいコマンドの詳細と、その使用方法について説明します。

IGMP スヌーピング インターフェイスの設定

VLAN でトポロジが変更されると、それまでに学習された IGMP スヌーピング情報が無効になる場合があります。トポロジ変更前に 1 つのポートに存在していたホストは、トポロジ変更後に別のポートに移動することがあります。トポロジが変更される場合、Catalyst 4500 シリーズ スイッチは、マルチキャスト トラフィックが VLAN 内のすべてのマルチキャスト受信者に送信されるように特別なアクションを実行します。

スパニングツリー プロトコル (STP) が VLAN で実行されている場合、VLAN のルート スイッチによってスパニングツリー TCN が発行されます。Catalyst 4500 シリーズ スイッチは、IGMP スヌーピングがイネーブルに設定されている VLAN で TCN を受信すると、ただちにマルチキャスト フラッディング モードを開始します。このモードは、トポロジが再度安定し、すべてのマルチキャスト受信者の新しい位置が学習されるまでの間、継続します。

マルチキャスト フラッディング モードの IP マルチキャスト トラフィックは、マルチキャスト グループ メンバが検出されたポートだけでなく、VLAN のすべてのポートに送られます。

Cisco IOS Release 12.1(11b)EW 以降、スイッチ ポート上で **no ip igmp snooping tcn flood** コマンドを使用すると、IP マルチキャスト トラフィックがそのポートにフラッディングされるのを手動で防ぐことができます。

トランク ポートの場合、この設定はすべての VLAN に適用されます。

デフォルトでは、マルチキャスト フラッディングはイネーブルです。フラッディングをディセーブルにするには **no** キーワードを、デフォルトの動作（フラッディングがイネーブル）に戻すには **default** を使用します。

インターフェイス上のマルチキャスト フラッディングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# interface {fastethernet gigabitethernet tengigabitethernet} slot/port	設定するインターフェイスを選択します。
ステップ 2	Switch(config-if)# no ip igmp snooping tcn flood	スイッチが TCN を受信した場合、インターフェイス上のマルチキャスト フラッディングをディセーブルにします。 インターフェイス上のマルチキャスト フラッディングをイネーブルにするには、次のコマンドを入力します。 default ip igmp snooping tcn flood
ステップ 3	Switch(config)# end	コンフィギュレーション モードを終了します。
ステップ 4	Switch# show running interface {fastethernet gigabitethernet tengigabitethernet} slot/port	設定を確認します。

次に、ファストイーサネット インターフェイス 2/11 上でマルチキャスト フラッディングをディセーブルにする例を示します。

```
Switch(config)# interface fastethernet 2/11
Switch(config-if)# no ip igmp snooping tcn flood
Switch(config-if)# end
Switch#
```

IGMP スヌーピング スイッチの設定

デフォルトでは、スイッチが 2 つの IGMP 一般クエリーを受信するまでフラッディング モードが継続します。この期間を変更するには、**ip igmp snooping tcn flood query count *n*** コマンドを使用します。*n* は 1 ~ 10 の数値です。

このコマンドはグローバル コンフィギュレーション レベルで作用します。

クエリーのデフォルト値は 2 です。**no** および **default** キーワードでデフォルトに戻ります。

IGMP クエリーのしきい値を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# ip igmp snooping tcn flood query count <n>	スイッチがマルチキャスト トラフィックのフラッディングを停止するまでの、IGMP クエリーの数を変更します。 スイッチを IGMP クエリーのデフォルトの数に戻すには、次のコマンドを入力します。 default ip igmp snooping tcn flood query count
ステップ 2	Switch(config)# end	コンフィギュレーション モードを終了します。

次に、4 回のクエリー実行後にマルチキャスト トラフィックのフラッディングを停止するように、スイッチを修正する例を示します。

```
Switch(config)# ip igmp snooping tcn flood query count 4
Switch(config)# end
Switch#
```

IGMP スヌーピングがイネーブルの VLAN でのトポロジ変更をスパニングツリー ルート スイッチが受信すると、Cisco IOS ルータが 1 つまたは複数の一般クエリーを送信するというクエリー要求がスイッチから発行されます。この新しいコマンド **ip igmp snooping tcn query solicit** によって、スイッチはスパニングツリー ルートでない場合も、トポロジ変更を確認すると、常にクエリー要求を送信します。

このコマンドはグローバル コンフィギュレーション レベルで作用します。

デフォルトでは、スイッチがスパニングツリー ルートの場合を除き、クエリー要求はディセーブルに設定されています。**default** キーワードでデフォルトの動作に戻ります。

スイッチにクエリー要求を送信するように指示するには、次の作業を行います。

	コマンド	目的
ステップ1	Switch(config)# ip igmp snooping tcn query solicit	TCN が検出された場合に、クエリー要求を送信するようにスイッチを設定します。 スイッチによるクエリー要求の送信を停止するには (スイッチがスパニングツリー ルート スイッチでない場合)、 no ip igmp snooping tcn query solicit コマンドを入力します。
ステップ2	Switch(config)# end	コンフィギュレーション モードを終了します。

次に、TCN を検出したあと、クエリー要求を送信するようにスイッチを設定する例を示します。

```
Switch(config)# ip igmp snooping tcn query solicit
Switch(config)# end
Switch#
```

IGMP スヌーピング情報の表示

ここでは IGMP スヌーピング情報を表示する方法について説明します。

- 「クエリア情報の表示」 (P.26-15)
- 「IGMP ホスト メンバーシップ情報の表示」 (P.26-16)
- 「グループ情報の表示」 (P.26-17)
- 「マルチキャスト ルータ インターフェイスの表示」 (P.26-18)
- 「MAC アドレス マルチキャスト エントリの表示」 (P.26-18)
- 「VLAN インターフェイス上の IGMP スヌーピング情報の表示」 (P.26-19)
- 「IGMP フィルタリングの設定」 (P.26-20)

クエリア情報の表示

クエリア情報を表示するには、次の作業を行います。

コマンド	目的
Switch# show ip igmp snooping querier [vlan vlan_ID]	マルチキャスト ルータ インターフェイスを表示します。

次に、スイッチ上のすべての VLAN の IGMP スヌーピング クエリア情報を表示する例を示します。

```
Switch# show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----
2         10.10.10.1      v2                 Router
3         172.20.50.22   v3                 Fa3/15
```

次に、VLAN 3 の IGMP スヌーピング クエリア情報を表示する例を示します。

```
Switch# show ip igmp snooping querier vlan 3
Vlan      IP Address      IGMP Version      Port
-----
```

3

172.20.50.22 v3

Fa3/15

IGMP ホスト メンバーシップ情報の表示



(注)

デフォルトでは、EHT は EHT データベースに最大 1000 エントリを維持します。上限に達すると、エントリはそれ以上作成されません。追加エントリを作成するには、**clear ip igmp snooping membership vlan** コマンドでデータベースをクリアします。

ホスト メンバーシップ情報を表示するには、次の作業を行います。

コマンド	目的
Switch# show ip igmp snooping membership [interface interface_num] [vlan vlan_ID] [reporter a.b.c.d] [source a.b.c.d group a.b.c.d]	EHT 情報を表示します。 (注) このコマンドは、スイッチ上で EHT がイネーブルにされている場合にのみ有効です。

次に、VLAN 20 のホスト メンバーシップ情報を表示し、EHT データベースを削除する例を示します。

```
Switch# show ip igmp snooping membership vlan 20
#channels: 5
#hosts : 1
Source/Group Interface Reporter Uptime Last-Join Last-Leave
40.40.40.2/224.10.10.10 Gi4/1 20.20.20.20 00:23:37 00:06:50 00:20:30
40.40.40.3/224.10.10.10 Gi4/2 20.20.20.20 00:23:37 00:06:50 00:20:30
40.40.40.4/224.10.10.10Gi4/1 20.20.20.20 00:39:42 00:09:17 -
40.40.40.5/224.10.10.10Fa2/1 20.20.20.20 00:39:42 00:09:17 -
40.40.40.6/224.10.10.10 Fa2/1 20.20.20.20 00:09:47 00:09:17 -
```

```
Switch# clear ip igmp snooping membership vlan 20
```

次に、インターフェイス gi4/1 のホスト メンバーシップを表示する例を示します。

```
Switch# show ip igmp snooping membership interface gi4/1
#channels: 5
#hosts : 1
Source/Group Interface Reporter Uptime Last-Join Last-Leave
40.40.40.2/224.10.10.10 Gi4/1 20.20.20.20 00:23:37 00:06:50 00:20:30
40.40.40.4/224.10.10.10Gi4/1 20.20.20.20 00:39:42 00:09:17 -
```

次に、VLAN 20 およびグループ 224.10.10.10 のホスト メンバーシップを表示する例を示します。

```
Switch# show ip igmp snooping membership vlan 20 source 40.40.40.2 group 224.10.10.10
#channels: 5
#hosts : 1
Source/Group Interface Reporter Uptime Last-Join Last-Leave
40.40.40.2/224.10.10.10 Gi4/1 20.20.20.20 00:23:37 00:06:50 00:20:30
```


グループ情報の表示

グループに対応付けられた詳細な IGMPv3 情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
Switch# show ip igmp snooping groups [vlan vlan_ID]	グループ、グループ (ホスト タイプ) に対して受信されたレポート タイプ、およびレポートが受信されたポートのリストを表示します。 レポート リストには、マルチキャスト ルータポートまたはグループの詳細な転送ポート設定は含まれません。レポートが受信されたポートのリストを表示します。 グループの詳細な転送ポート設定を表示するには、 show mac-address-table multicast コマンドを使用して、このグループに対応する MAC アドレスの CLI 出力を表示します。
Switch# show ip igmp snooping groups [vlan vlan_ID a.b.c.d] [summary sources hosts]	グループ アドレス固有の情報を表示します。送信元およびホストに対してグループの現在のステータの詳細を提供します。 (注) このコマンドは、完全な IGMPv3 スヌーピング サポートにのみ適用され、IGMPv1、IGMPv2、または IGMPv3 グループに使用できません。
Switch# show ip igmp snooping groups [vlan vlan_ID] [count]	グローバルまたは VLAN 単位でシステムによって学習されたグループ アドレスの総数を表示します。

次に、VLAN 1 のホスト タイプおよびグループのポートを表示する例を示します。

```
Switch# show ip igmp snooping groups vlan 10 226.6.6.7
Vlan      Group      Version    Ports
-----
10        226.6.6.7  v3         Fa7/13, Fa7/14
Switch>
```

次に、送信元 IP アドレスに対する現在のグループのステータを表示する例を示します。

```
Switch# show ip igmp snooping groups vlan 10 226.6.6.7 sources
Source information for group 226.6.6.7:
Timers: Expired sources are deleted on next IGMP General Query

SourceIP      Expires      Uptime      Inc Hosts  Exc Hosts
-----
2.0.0.1       00:03:04    00:03:48    2          0
2.0.0.2       00:03:04    00:02:07    2          0
Switch>
```

次に、ホスト MAC アドレスに対する現在のグループのステータを表示する例を示します。

```
Switch# show ip igmp snooping groups vlan 10 226.6.6.7 hosts
IGMPv3 host information for group 226.6.6.7
Timers: Expired hosts are deleted on next IGMP General Query

Host (MAC/IP)  Filter mode  Expires      Uptime      # Sources
```

```
-----
175.1.0.29    INCLUDE      stopped    00:00:51    2
175.2.0.30    INCLUDE      stopped    00:04:14    2
```

次に、IGMPv3 グループのサマリー情報を表示する例を示します。

```
Switch# show ip igmp snooping groups vlan 10 226.6.6.7 summary
Group Address (Vlan 10)      : 226.6.6.7
Host type                    : v3
Member Ports                 : Fa7/13, Fa7/14
Filter mode                  : INCLUDE
Expires                     : stopped
Sources                     : 2
Reporters (Include/Exclude) : 2/0
```

次に、システムによってグローバルに学習されたグループアドレスの総数を表示する例を示します。

```
Switch# show ip igmp snooping groups count
Total number of groups: 54
```

次に、VLAN 5 で学習されたグループアドレスの総数を表示する例を示します。

```
Switch# show ip igmp snooping groups vlan 5 count
Total number of groups: 30
```

マルチキャスト ルータ インターフェイスの表示

IGMP スヌーピングをイネーブルにすると、スイッチはマルチキャスト ルータの接続先インターフェイスを自動的に学習します。

マルチキャスト ルータ インターフェイスを表示するには、次の作業を行います。

コマンド	目的
Switch# <code>show ip igmp snooping mrouter vlan vlan_ID</code>	マルチキャスト ルータ インターフェイスを表示します。

次に、VLAN 1 のマルチキャスト ルータ インターフェイスを表示する例を示します。

```
Switch# show ip igmp snooping mrouter vlan 1
vlan          ports
-----+-----
1             Gi1/1,Gi2/1,Fa3/48,Router
Switch#
```

MAC アドレス マルチキャスト エントリの表示

VLAN の MAC アドレス マルチキャスト エントリを表示するには、次の作業を行います。

コマンド	目的
Switch# <code>show mac-address-table multicast vlan vlan_ID [count]</code>	VLAN の MAC アドレス マルチキャスト エントリを表示します。

次に、VLAN 1 の MAC アドレス マルチキャスト エントリを表示する例を示します。

```
Switch# show mac-address-table multicast vlan 1
Multicast Entries
  vlan      mac address      type      ports
-----+-----+-----+-----
    1      0100.5e01.0101    igmp    Switch,Gi6/1
    1      0100.5e01.0102    igmp    Switch,Gi6/1
    1      0100.5e01.0103    igmp    Switch,Gi6/1
    1      0100.5e01.0104    igmp    Switch,Gi6/1
    1      0100.5e01.0105    igmp    Switch,Gi6/1
    1      0100.5e01.0106    igmp    Switch,Gi6/1
Switch#
```

次に、VLAN 1 の MAC アドレス エントリの総数を表示する例を示します。

```
Switch# show mac-address-table multicast vlan 1 count
Multicast MAC Entries for vlan 1:    4
Switch#
```

VLAN インターフェイス上の IGMP スヌーピング情報の表示

特定の VLAN 上の IGMP スヌーピング情報を表示するには、次の作業を行います。

コマンド	目的
Switch# <code>show ip igmp snooping vlan vlan_ID</code>	特定の VLAN インターフェイス上の IGMP スヌーピング情報を表示します。

次に、VLAN 5 上の IGMP スヌーピング情報を表示する例を示します。

```
Switch# show ip igmp snooping vlan 5
Global IGMP Snooping configuration:
-----
IGMP snooping                :Enabled
IGMPv3 snooping support      :Full
Report suppression           :Enabled
TCN solicit query            :Disabled
TCN flood query count        :2

Vlan 5:
-----
IGMP snooping                :Enabled
Immediate leave               :Disabled
Explicit Host Tracking        :Disabled
Multicast router learning mode :pim-dvmrp
CGMP interoperability mode    :IGMP_ONLY
```

IGMP スヌーピング クエリア情報の表示

IGMP スヌーピング クエリア情報を表示するには、次の作業を行います。

コマンド	目的
Switch# <code>show ip igmp snooping querier [vlan vlan_ID] [detail]</code>	IGMP スヌーピング クエリアの状態を表示します。

次に、スヌーピング クエリア情報を表示する例を示します。

```
switch# show ip igmp snooping querier vlan 2 detail
IP address           : 1.2.3.4
IGMP version         : v2
Port                 : Router/Switch
Max response time    : 12s
```

```
Global IGMP switch querier status
```

```
-----
admin state           : Enabled
admin version        : 2
source IP address    : 1.2.3.4
query-interval (sec) : 130
max-response-time (sec) : 10
querier-timeout (sec) : 100
tcn query count      : 2
tcn query interval (sec) : 10
```

```
Vlan 2: IGMP switch querier status
```

```
-----
admin state           : Enabled
admin version        : 2
source IP address    : 1.2.3.4
query-interval (sec) : 55
max-response-time (sec) : 12
querier-timeout (sec) : 70
tcn query count      : 10
tcn query interval (sec) : 8
operational state    : Querier
operational version  : 2
tcn query pending count : 0
```

IGMP フィルタリングの設定

ここでは、次の内容について説明します。

- 「IGMP フィルタリングのデフォルト設定」(P.26-21)
- 「IGMP プロファイルの設定」(P.26-21)
- 「IGMP プロファイルの適用」(P.26-22)
- 「IGMP グループの最大数の設定」(P.26-23)



(注)

IGMP フィルタリング機能は、IGMPv1 および IGMPv2 だけで動作します。

メトロポリタンまたは Multiple-Dwelling Unit (MDU) インストールなど一部の環境では、管理者はスイッチポート上のユーザが所属するマルチキャストグループを制御できます。管理者は加入計画またはサービス計画の種類に基づいて、IP/TV などのマルチキャストサービスの配布を制御できます。

管理者はこのような制御を実行する場合に、IGMP フィルタリング機能を使用します。この機能を使用すると、IP マルチキャストプロファイルを設定して、これらを個々のスイッチポートに関連付けることで、ポート単位でマルチキャスト加入をフィルタリングできます。IGMP プロファイルにはマルチキャストグループを1つまたは複数格納して、グループへのアクセスを許可するか拒否するかを指定できます。マルチキャストグループへのアクセスを拒否するIGMPプロファイルがスイッチポートに適用されると、IP マルチキャストトラフィックのストリームを要求するIGMP Join レポートが廃棄さ

れ、ポートはそのグループからの IP マルチキャストトラフィックを受信できなくなります。マルチキャストグループへのアクセスがフィルタリングアクションで許可されている場合は、ポートからの IGMP レポートが転送されて、通常の処理が行われます。

IGMP フィルタリングは、IGMP メンバーシップの Join 要求のみを制御し、IP マルチキャストトラフィックの転送指示機能には関与しません。

ip igmp max-groups *n* コマンドを使用すると、レイヤ 2 インターフェイスが加入できる IGMP グループの最大数も設定できます。

IGMP フィルタリングのデフォルト設定

表 26-2 に、IGMP フィルタリングのデフォルト設定を示します。

表 26-2 IGMP フィルタリングのデフォルト設定

機能	デフォルト設定
IGMP フィルタ	フィルタリングなし
IGMP グループの最大数	制限なし
IGMP プロファイル	未定義

IGMP プロファイルの設定

IGMP プロファイルを設定し、IGMP プロファイル コンフィギュレーション モードを開始するには、**ip igmp profile** グローバル コンフィギュレーション コマンドを使用します。IGMP プロファイル コンフィギュレーション モードで、ポートからの IGMP Join 要求のフィルタリングに使用される IGMP プロファイルのパラメータを指定できます。IGMP プロファイル コンフィギュレーション モードでは、次のコマンドを使用してプロファイルを作成できます。

- **deny** : 一致するアドレスを拒否すること（デフォルトの状態）を指定します。
- **exit** : IGMP プロファイル コンフィギュレーション モードを終了します。
- **no** : コマンドを無効にするか、デフォルト設定にします。
- **permit** : 一致するアドレスを許可することを指定します。
- **range** : プロファイルの IP アドレスの範囲を指定します。単一の IP アドレスまたは開始アドレスと終了アドレスを指定した IP アドレス範囲を入力します。

デフォルトでは、IGMP プロファイルは設定されていません。**permit** または **deny** キーワード以外でプロファイルが設定されている場合、デフォルトは IP アドレス範囲へのアクセス拒否になります。

ポートの IGMP プロファイルを作成するには、次の作業を行います。

	コマンド	目的
ステップ1	Switch# 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2	Switch(config)# ip igmp profile profile number	IGMP プロファイル コンフィギュレーション モードを開始し、設定するプロファイルに数値を割り当てます。1 ~ 4、294、967、295 の数値を指定できます。

■ IGMP フィルタリングの設定

	コマンド	目的
ステップ3	Switch(config-igmp-profile)# permit deny	(任意) IP マルチキャスト アドレスへのアクセスを許可または拒否するアクションを設定します。アクションを設定しないと、プロファイルのデフォルト設定はアクセス拒否になります。
ステップ4	Switch(config-igmp-profile)# range ip multicast address	アクセスを制御する IP マルチキャストアドレスまたは IP マルチキャストアドレスの範囲を入力します。範囲を入力する場合は、IP マルチキャストアドレスの下限値、スペースを1つ、IP マルチキャストアドレスの上限値を入力します。複数のアドレスまたはアドレスの範囲を入力する場合は、 range コマンドを繰り返し使用します。
ステップ5	Switch(config-igmp-profile)# end	特権 EXEC モードに戻ります。
ステップ6	Switch# show ip igmp profile profile-number	プロファイルの設定を確認します。
ステップ7	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

プロファイルを削除するには、**no ip igmp profile profile-number** グローバル コンフィギュレーション コマンドを使用します。

IP マルチキャスト アドレスまたは IP マルチキャスト アドレス範囲を削除するには、**no range ip multicast address** IGMP プロファイル コンフィギュレーション コマンドを使用します。

次に、IGMP プロファイル 4 を作成し (単一の IP マルチキャスト アドレスへのアクセスを許可)、設定を確認する例を示します。アクションが **deny** (デフォルト) である場合、**show ip igmp profile** コマンドの出力には表示されません。

```
Switch# configure terminal
Switch(config)# ip igmp profile 4
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 4
IGMP Profile 4
    permit
    range 229.9.9.0 229.9.9.0
```

IGMP プロファイルの適用

IGMP プロファイルの定義に従ってアクセスを制御するには、**ip igmp filter** インターフェイス コンフィギュレーション コマンドを使用して、プロファイルを該当するインターフェイスに適用します。1 つのプロファイルを複数のインターフェイスに適用できますが、各インターフェイスに適用できるプロファイルは 1 つだけです。



(注)

IGMP プロファイルは、レイヤ 2 ポートにだけ適用できます。ルーテッド ポート (または Switch Virtual Interface (SVI; スイッチ仮想インターフェイス)) あるいは EtherChannel ポート グループに属するポートに IGMP プロファイルは適用できません。

スイッチ ポートに IGMP プロファイルを適用するには、次の作業を行います。

	コマンド	目的
ステップ1	Switch# 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2	Switch(config)# interface interface-id	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、設定する物理インターフェイス (fastethernet2/3 など) を入力します。インターフェイスは、EtherChannel ポート グループに属さないレイヤ 2 ポートでなければなりません。
ステップ3	Switch(config-if)# ip igmp filter profile number	インターフェイスに指定された IGMP プロファイルを適用します。プロファイル番号には、1 ~ 4,294,967,295 を指定できます。
ステップ4	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ5	Switch# show running configuration interface interface-id	設定を確認します。
ステップ6	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスからプロファイルを削除するには、**no ip igmp filter** コマンドを使用します。

次に、IGMP プロファイル 4 をインターフェイスに適用し、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet2/12
Switch(config-if)# ip igmp filter 4
Switch(config-if)# end
Switch# show running-config interface fastethernet2/12
Building configuration...

Current configuration : 123 bytes
!
interface FastEthernet2/12
 no ip address
 shutdown
 snmp trap link-status
 ip igmp max-groups 25
 ip igmp filter 4
end
```

IGMP グループの最大数の設定

レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定するには、**ip igmp max-groups** インターフェイス コンフィギュレーション コマンドを使用します。最大数をデフォルト設定 (制限なし) に戻すには、このコマンドの **no** 形式を使用します。



(注)

この制限はレイヤ 2 ポートにだけ適用できます。ルーテッド ポート (または SVI) あるいは EtherChannel ポート グループに属するポートには、IGMP グループの最大数を設定できません。

スイッチ ポートに IGMP プロファイルを適用するには、次の作業を行います。

IGMP フィルタリングの設定の表示

	コマンド	目的
ステップ1	Switch# 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2	Switch(config)# interface interface-id	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、設定する物理インターフェイス (gigabitethernet1/1 など) を入力します。インターフェイスは、EtherChannel グループに属さないレイヤ 2 ポートでなければなりません。
ステップ3	Switch(config-if)# ip igmp max-groups number	インターフェイスが加入できる IGMP グループの最大数を設定します。指定できる範囲は 0 ~ 4,294,967,294 です。デフォルトでは最大数が設定されていません。 最大グループ制限を削除し、最大数なしのデフォルトに戻すには、 no ip igmp max-groups コマンドを使用します。
ステップ4	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ5	Switch# show running-configuration interface interface-id	設定を確認します。
ステップ6	Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、インターフェイスが加入できる IGMP グループの数を 25 に制限する例を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet2/12
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)# end
Switch# show running-config interface fastethernet2/12
Building configuration...

Current configuration : 123 bytes
!
interface FastEthernet2/12
 no ip address
 shutdown
 snmp trap link-status
 ip igmp max-groups 25
 ip igmp filter 4
end
```

IGMP フィルタリングの設定の表示

スイッチ上のすべてのインターフェイス、または指定されたインターフェイスの IGMP プロファイルと最大グループ設定を表示できます。

IGMP プロファイルを表示するには、次の作業を行います。

コマンド	目的
Switch# show ip igmp profile [profile number]	指定された IGMP プロファイル、またはスイッチ上で定義されたすべての IGMP プロファイルを表示します。

インターフェイス コンフィギュレーションを表示するには、次の作業を行います。

コマンド	目的
Switch# show running-configuration [interface interface-id]	指定されたインターフェイスまたはスイッチ上のすべてのインターフェイスに関する、(設定されている場合は) インターフェイスが所属できる IGMP グループの最大数と、インターフェイスに適用された IGMP プロファイルを含む設定を表示します。

次に、プロファイル番号が入力されていない場合の **show ip igmp profile** 特権 EXEC コマンドの例を示します。スイッチ上で定義されたすべてのプロファイルが表示されます。

```
Switch# show ip igmp profile
IGMP Profile 3
    range 230.9.9.0 230.9.9.0
IGMP Profile 4
    permit
    range 229.9.9.0 229.255.255.255
```

次に、インターフェイスに IGMP の最大設定グループ数が指定され、IGMP プロファイル 4 がインターフェイスに適用されている場合の **show running-config** 特権 EXEC コマンドの例を示します。

```
Switch# show running-config interface fastethernet2/12
Building configuration...
Current configuration : 123 bytes
!
interface FastEthernet2/12
  no ip address
  shutdown
  snmp trap link-status
  ip igmp max-groups 25
  ip igmp filter 4
end
```

■ IGMP フィルタリングの設定の表示