



CHAPTER 43

IPv4 IGMP フィルタリング

- 「IGMP フィルタリングの前提条件」 (P.43-1)
- 「IGMP フィルタリングの制約事項」 (P.43-1)
- 「IGMP フィルタリングについて」 (P.43-2)
- 「IGMP フィルタリングのデフォルト設定」 (P.43-4)
- 「IGMP フィルタの設定方法」 (P.43-4)
- 「IGMP フィルタリングの設定の確認」 (P.43-6)
- 「IGMP フィルタリングの設定例」 (P.43-8)



(注)

- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html

- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。



ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

IGMP フィルタリングの前提条件

なし。

IGMP フィルタリングの制約事項

なし。

IGMP フィルタリングについて

- 「IGMP フィルタリングの概要」(P.43-3)
- 「IGMP フィルタの優先順位」(P.43-4)

IGMP フィルタリングの概要



(注)

IGMP は、マルチキャスト ルータのレイヤ 3 で稼働し、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。IGMP については、[第 39 章「IPv4 マルチキャスト レイヤ 3 機能について」](#)を参照してください。

IGMP スヌーピングは、レイヤ 2 レベルでマルチキャスト グループ メンバーシップを学習し、維持するプロトコルです。IGMP スヌーピングは、IGMP トラフィックを確認して、特定の送信元およびグループからのマルチキャスト トラフィックを受信できるポートを決定します。この情報は、マルチキャスト トラフィックを関係するポートにだけ転送するのに使用されます。IGMP スヌーピングの主な利点は、パケットのフラッディングを軽減することです。IGMP スヌーピングの詳細については、「[IGMP フィルタリングについて](#)」(P.43-2)を参照してください。

IGMP フィルタリングを使用することにより、ユーザはスイッチ仮想インターフェイス (SVI) 上、ポート単位、またはポート単位/VLAN 単位でフィルタを設定し、ネットワークを経由する IGMP トラフィックの伝播を制御できるようになります。IGMP フィルタリングは、IGMP トラフィックを管理することにより、IGMP スヌーピングを管理する機能を提供し、その結果マルチキャスト トラフィックの転送を制御します。

IGMP パケットを受信すると、IGMP フィルタリングはユーザによって設定されたフィルタを使用して、IGMP パケットを廃棄するか、または既存の IGMP スヌーピング コードによる処理を許可するかを決定します。IGMP バージョン 1 または 2 のパケットの場合、パケット全体が廃棄されます。IGMPv3 パケットの場合、パケットはフィルタによって拒否されたメッセージ エレメントを削除するよう書き換えられます。

IGMP フィルタリング機能は、シングル サインオン (SSO) に準拠します。

IGMP トラフィック フィルタは、ポートのマルチキャスト トラフィックへのアクセスを制御します。アクセスは、次の事項に基づいて制限されます。

- ポート上に追加できるマルチキャスト グループまたはチャネル。チャネルには、グループおよびマルチキャスト トラフィックの送信元の両方を指定する IGMPv3 ホストが加入します。
- 特定のポートまたはインターフェイス上で許可されるグループまたはチャネルの最大数（サービスを要求するホスト数とは関係なく）。
- IGMP プロトコル バージョン（たとえば、すべての IGMPv1 メッセージを許可しない）。

IGMP フィルタリング コマンドを入力すると、ユーザ ポリシーがレイヤ 3 SVI インターフェイス、レイヤ 2 ポート、またはレイヤ 2 トランク ポート上の特定の VLAN に適用されます。レイヤ 2 ポートは、アクセス ポートまたはトランク ポートとなる可能性があります。IGMP フィルタリング機能は、IGMP スヌーピングがイネーブルの場合に限り動作します（インターフェイス上またはグローバルに）。

IGMP フィルタリングは通常、エンドユーザ デバイスに接続されたアクセス スイッチで使用されます。

IGMP フィルタには、以下の 3 つの異なるタイプがあります。IGMP グループとチャネル アクセス コントロール、複数の IGMP グループとチャネル制限、および IGMP の最小バージョンです。これらのフィルタは、異なるタイプのポート上で設定可能で、別々に動作します。

- SVI 単位
- ポート単位
- トランク ポート上での VLAN 単位

トランク ポートを経由する各 VLAN のためのフィルタを個別に設定できます。

IGMP フィルタの優先順位

- 「アクセス モード」 (P.43-4)
- 「トランク モード」 (P.43-4)

アクセス モード

アクセス モードの場合、フィルタはポートおよび SVI の両方に設定できます。IGMP パケットがアクセス モードのポート上で受信された場合、最初にポート フィルタが確認されます。ポート フィルタが存在する場合は、これが適用され、SVI フィルタは無視されます。ポート単位のフィルタが存在しない場合、SVI フィルタが使用されます。

この階層はフィルタのタイプごとに別々に適用されます。たとえば、ポート上に設定された制限フィルタは、SVI 上のデフォルトの制限フィルタを無効にしますが、その他のフィルタには影響を与えません。

トランク モード

トランク モードのポートの場合、トランク ポート上の VLAN のいずれかに対応する SVI に設定できるフィルタ、トランク ポート自身に設定できるフィルタ、およびトランクをパススルーするレイヤ 2 VLAN のいずれかに設定できるフィルタがあります。IGMP パケットが受信されると、最初にトランクの VLAN 単位の固有フィルタが確認されます。このフィルタが存在する場合は、これが適用されます。メイン トランク ポート フィルタおよび SVI フィルタは無視されます。トランクの VLAN 単位のフィルタが存在しない場合は、メイン トランク ポート フィルタが使用されます。これらのフィルタがいずれも存在しない場合は、VLAN の SVI フィルタがトランク モードのポートの最後のデフォルトとして使用されます。

IGMP フィルタリングのデフォルト設定

なし。

IGMP フィルタの設定方法

- 「IGMP グループおよびチャネル アクセス コントロールの設定」 (P.43-4)
- 「IGMP グループおよびチャネル制限の設定」 (P.43-5)
- 「IGMP バージョン フィルタリングの設定」 (P.43-5)
- 「IGMP フィルタリングの統計情報のクリア」 (P.43-6)

IGMP グループおよびチャネル アクセス コントロールの設定

IGMP グループまたはチャネル上でフィルタリングすることにより、ユーザはポート上に、またはトランク ポート上の VLAN 単位で追加できる IGMP グループまたはチャネルを制御します。

IGMP グループまたはチャネルにフィルタリングを設定するには、次の CLI コマンドを使用します。

```
ip igmp snooping access-group acl [vlan vlan_id]
```

複数のグループまたはチャネルを許可または拒否するには、アクセス コントロール リストで複数のアクセス コントロール エントリ (ACE) を設定する必要があります。ACL が許可か拒否のいずれに設定されるかに応じて、対応するグループまたはチャネルが許可、あるいは拒否されます。指定される ACL は、単一の ACL または拡張 ACL のいずれかになります。

IGMP グループまたはチャネルによるフィルタリングは、レイヤ 3 SVI 上でデフォルト フィルタとして、この SVI の下のアクセス モードのすべてのポート、およびこれに対応する VLAN を伝送するすべてのトランク ポート上の VLAN に対して設定できます。また、フィルタはレイヤ 2 ポート上でも設定できます。ポートがアクセス モードの場合、このフィルタはすべてのデフォルトの SVI フィルタを無効にします。ポートがトランク モードの場合、このフィルタはそのトランク上のすべての VLAN に対してデフォルトとして動作し、対応する各 VLAN の SVI フィルタを無効にします。

ポートがトランク ポートの場合、**vlan** キーワードにより指定のレイヤ 2 VLAN に着信する IGMP パケットに対してだけフィルタを適用することができます。この VLAN 単位のフィルタ (**vlan** キーワードにより設定) は、同一 VLAN のすべてのインターフェイス レベルのフィルタおよびすべての SVI フィルタを無効にします。

IGMP グループおよびチャネル制限の設定

IGMP グループおよびチャネルの数を制限することにより、ポートまたはトランク ポートの VLAN 単位で追加できる IGMP グループおよびチャネルの数を制御できるようになります。

IGMP グループまたはチャネル数を制限するには、次のインターフェイス コマンドの CLI を使用します。

```
ip igmp snooping limit n [except acl] [vlan vlan_id]
```

最大 n 数のグループまたはチャネルが、ポートまたはインターフェイスに許可されます。**except** キーワードにより、設定された制限から除外するグループまたはチャネルを指定できます。**except** キーワードを使用した ACL の場合、単一 ACL または拡張 ACL のいずれかになります。

同一インターフェイス上の (*,G1) および (S1,G1) に対して Join が受信された場合、これらは 2 つの別個の Join としてカウントされます。インターフェイス上での制限が 2 と設定されていて、(*,G1) および (S1,G1) に対して Join が受信された場合、その他のすべての Join (これら 2 つ以外のグループまたはチャネルに対する) は廃棄されます。

このフィルタは、レイヤ 3 SVI 上でデフォルト フィルタとして、この SVI の下のアクセス モードのすべてのポート、およびこれに対応する VLAN を伝送するすべてのトランク ポート上の VLAN に対して設定できます。また、フィルタはレイヤ 2 ポート上でも設定できます。レイヤ 2 ポートがアクセス モードの場合、このフィルタはすべてのデフォルトの SVI フィルタを無効にします。レイヤ 2 スイッチ ポートがトランク モードの場合、このフィルタはそのトランク上のすべての VLAN に対してデフォルトとして動作し、対応する各 VLAN の SVI フィルタを無効にします。レイヤ 2 スイッチ ポートがトランク ポートの場合、**vlan** キーワードにより指定のレイヤ 2 VLAN に着信する IGMP パケットに対してだけフィルタを適用することができます。この VLAN 単位のフィルタ (**vlan** キーワードにより設定) は、同一 VLAN のすべてのインターフェイス レベルのフィルタおよびすべての SVI フィルタを無効にします。

IGMP バージョン フィルタリングの設定

IGMP プロトコルでのフィルタリングにより、SVI 上で許可される IGMP ホストの最小バージョンを設定できます。たとえば、すべての IGMPv1 ホストを禁止する (IGMP バージョン 2 以上を許可するなど)、またはすべての IGMPv1 および IGMPv2 ホストを禁止する (IGMP バージョン 3 以上を許可するなど) が可能です。このフィルタリングは、メンバーシップ レポートにだけ適用されます。

IGMP プロトコルにフィルタリングを設定するには、次の CLI コマンドを使用します。

■ IGMP フィルタリングの設定の確認

```
ip igmp snooping minimum-version 2 | 3
```

このフィルタは、レイヤ 3 SVI 上でデフォルト フィルタとして、この SVI の下のアクセス モードのすべてのポート、およびすべてのトランク ポート上の対応する VLAN に対して設定できます。

IGMP フィルタリングの統計情報のクリア

IGMP フィルタリングの統計情報をクリアするには、次のいずれかの作業を行います。

コマンド	目的
Router# clear ip igmp snooping filter statistics	すべてのアクセス ポート、およびすべてのトランク ポート上のすべての VLAN に関する IGMP フィルタリングの統計情報をクリアします。
Router# clear ip igmp snooping filter statistics interface interface_name	特定のアクセス ポート、または特定のトランク ポート上のすべての VLAN の統計情報をクリアします。
Router# clear ip igmp snooping filter statistics interface interface_name vlan vlan_ID	トランク ポート上の特定の VLAN の統計情報をクリアします。

IGMP フィルタリングの設定の確認

- ・「IGMP フィルタリングの設定の表示」(P.43-6)
- ・「IGMP フィルタリングの統計情報の表示」(P.43-7)

IGMP フィルタリングの設定の表示

IGMP フィルタリングの規則を表示するには、次の作業を行います。

コマンド	目的
Router(config-if)# show ip igmp snooping filter interface interface-name [details]	指定のインターフェイスに設定されたフィルタを表示します。

次に、SVI 上に設定されたデフォルトのフィルタを表示する例を示します。

```
Router# show ip igmp snooping filter interface vlan 20
Access-Group: Channel1-Acl
Groups/Channels Limit:100 (Exception List: Channel6-Acl)
IGMP Minimum-Version:Not Configured
```

次に、SVI の下でアクセス モードのすべてのポート、および対応する VLAN を伝送するすべてのトランク ポートに設定されたフィルタを表示する例を示します。

```
Router# show ip igmp snooping filter interface g3/48
Access-Group: Channel4-Acl
Groups/Channels Limit:10 (Exception List: Channel3-Acl)
```

次に、この SVI の下でアクセス モードのすべてのポートに設定されたフィルタを表示する例を示します。

```
Router# show ip igmp snooping filter interface vlan 20 detail
```

```
GigabitEthernet3/47 :
  Access-Group: Not Configured
  Groups/Channels Limit: Not Configured
GigabitEthernet3/48 :
  Access-Group: Channel4-ACL
  Groups/Channels Limit: 10 (Exception-list: Channel3-Acl)
```

次に、デフォルトのトランク ポート フィルタを表示する例を示します。

```
Router# show ip igmp snooping filter interface g3/46
  Access-Group: Channel1-Acl
  Groups/Channels Limit: 10 (Exception List: Channel3-Acl)
```

次に、このトランク上のすべての VLAN の VLAN 単位フィルタを表示する例を示します。

```
Router# show ip igmp snooping filter interface g3/46 detail
Vlan 10 :
  Access-Group: Not Configured
  Groups/Channels Limit: Not Configured
Vlan 20 :
  Access-Group: Not Configured
  Groups/Channels Limit: 8 (Exception List: Channel4-Acl)
```

次に、このトランク上の特定の VLAN の VLAN 単位フィルタを表示する例を示します。

```
Router# show ip igmp snooping filter interface g3/46 vlan 20
  Access-Group: Not Configured
  Groups/Channels Limit: 8 (Exception List: Channel4-Acl)
```



(注)

ポートがシャットダウン ステートの場合、ポートがトランク モードかアクセス モードかを判別できないため、フィルタ ステータスは表示されません。この場合、**show running-config interface xxxx** コマンドを使用して設定を確認します。

IGMP フィルタリングの統計情報の表示

統計情報は、アクセス モードのポートにはインターフェイス単位で、トランク モードのポートには VLAN 単位で維持されます。

IGMP フィルタリングの統計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(config-if)# show ip igmp snooping filter interface interface-name [statistics]	指定のインターフェイスから収集されるフィルタリングの統計情報を表示します。

次に、SVI の下のアクセス モードの各ポートの統計情報を表示する例を示します。

```
Router# show ip igmp snooping filter interface vlan 20 statistics
GigabitEthernet3/47 :
  IGMP Filters are not configured

GigabitEthernet3/48 :
  Access-group denied : 0
  Limit denied : 2
  Limit status : 0 active out of 2 max
  Minimum-version denied : 0
```

次に、アクセス モードの特定ポートに関する統計情報を表示する例を示します。

```
Router# show ip igmp snooping filter interface g3/48 statistics
```

```

Access-group denied : 0
Limit denied : 2
Limit status : 0 active out of 2 max
Minimum-version denied : 0

```

次に、デフォルトの SVI フィルタもポートフィルタも設定されていない、アクセスモードのポート Gigabit Ethernet 3/47 の統計情報を表示する例を示します。

```

Router# show ip igmp snooping filter interface g3/47 statistics
IGMP Filters are not configured

```

次に、トランクの下すべての VLAN に関する統計情報を表示する例を示します。

```

Router# show ip igmp snooping filter interface g3/46 statistics
Vlan 10 :
IGMP Filters are not configured

```

```

Vlan 20 :
Access-group denied : 0
Limit denied : 0
Minimum-version denied : 0

```

次に、トランクの下特定の VLAN に関する統計情報を表示する例を示します。

```

Router# show ip igmp snooping filter interface g3/46 vlan 20 statistics
Access-group denied : 0
Limit denied : 0
Minimum-version denied : 0

```

次に、トランクおよび VLAN フィルタが設定されていないトランクポートの下特定の VLAN の統計情報を表示する例を示します。

```

Router# show ip igmp snooping filter interface g3/46 vlan 10 statistics
IGMP Filters are not configured

```



(注) ポートがシャットダウンステートの場合、ポートがトランクモードかアクセスモードかを判別できないため、フィルタの統計情報は表示されません。

IGMP フィルタリングの設定例

次に、フィルタ階層の例を示します。次の SVI VLAN 100 の設定には、3 つのアクセスポート (g1/1、g1/2、および g1/3) が含まれます。

```

VLAN 100 :
Router(config-if)# ip igmp snooping limit 20

```

```

ポート g1/1 :
Router(config-if)# ip igmp snooping limit 35

```

```

ポート g1/2 :
Router(config-if)# no limit filter

```

```

ポート g1/3 :
Router(config-if)# no limit filter

```


この例では、g1/1 の制限値が 35 で、g1/2 の制限値が 20、また g1/3 の制限値も 20 となります。



ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

[技術マニュアルのアイデア フォーラムに参加する](#)

