CHAPTER 34

IPv4 IGMP フィルタリングおよびルータ ガードの設定

この章では、ポートの Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）トラフィックへのアクセスを制御するため、IGMP トラフィック フィルタリングおよびルータ ガードを設定する方法について説明します。IGMP トラフィック フィルタリングおよびルータ ガードは、Release 12.2(33)SXH 以降でサポートされます。

（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 URL の『Cisco IOS Master Command List, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

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

ここでは、マルチキャスト ホスト（受信者）の IGMP フィルタリングおよびルータ ガード機能について説明します。

- 「IGMP フィルタリングの概要」（P.34-2）
- 「ルータ ガードの概要」（P.34-8）

IGMP フィルタリングの概要

ここでは、IGMP フィルタリングについて説明します。

- 「IGMP フィルタリングの概要」（P.34-2）
- 「IGMP フィルタ」（P.34-3）
- 「IGMP フィルタの優先順位」（P.34-4）
- 「IGMP フィルタリングの表示」（P.34-5）
- 「IGMP フィルタリングの統計情報のクリア」（P.34-8）

IGMP フィルタリングの概要

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 フィルタリングの概要」（P.34-2）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 Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）上、ポート単位、または ポート単位 /Virtual LAN（VLAN; 仮想 LAN）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、Single Sign-on（SSO; シングル サインオン）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、イーサネットツーホームの配置シナリオでのエンドユーザ 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。

（注）　IGMP は、マルチキャスト ルータのレイヤ 3 で稼動し、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 の詳細については、第 32 章「IPv4 マルチキャスト レイヤ 3 スイッチングの概要」を参照してください。

IGMP フィルタ

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 アクセス制御、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 ポートの場合、フィルタはこのトランク ポートをパススルーする VLAN ごとに別々に設定されることもあります。

ここでは、各タイプのフィルタについて詳細に説明します。

- 「IGMP グループおよびチャネル アクセス制御」（P.34-3）
- 「IGMP グループおよびチャネル数の制限」（P.34-4）
- 「IGMP の最小バージョン」（P.34-4）

IGMP グループおよびチャネル アクセス制御

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 Command Line Interface（CLI; コマンドライン インターフェイス）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、Access Control List（ACL; アクセス制御リスト）で複数の Access Control Entry（ACE; アクセス制御エントリ）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ようにできます。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数の制限

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ようにできます。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 の最小バージョン

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）ことが可能です。このフィルタリングは、メンバシップ 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。

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 フィルタの優先順位

ここでは、各種ポート上の異なるフィルタの階層について説明します。

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。

フィルタ階層の例

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：

```
Switch(config-if)# ip igmp snooping limit 20
```

ポート g1/1：

```
Switch(config-if)# ip igmp snooping limit 35
```

ポート g1/2：

```
Switch(config-if)# no limit filter
```

ポート g1/3：

```
Switch(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。

IGMP フィルタリングの表示

ここでは、IGMP フィルタリングの表示方法について説明します。

- 「IGMP フィルタリング設定の表示」（P.34-6）
- 「IGMP フィルタリングの統計情報の表示」（P.34-7）

IGMP フィルタリング設定の表示

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
Switch(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、トランクの下のすべての 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、トランクの下の特定の 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 ポートの下の特定の 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。

ルータ ガードの概要

ここでは、ルータ ガードについて説明します。

- 「ルータ ガードの概要」（P.34-8）
- 「ルータ ガードの設定」（P.34-9）
- 「ルータ ガード設定の表示」（P.34-10）
- 「ルータ ガードのインターフェイスの表示」（P.34-11）

ルータ ガードの概要

ルータ ガード機能により、指定のポートをマルチキャスト ルータ ポートではなく、マルチキャスト ホスト ポートとしてだけ指定できます。このポートで受信されたマルチキャスト ルータ制御パケットは、ドロップされます。

スイッチが、マルチキャスト ルータ制御パケット（IGMP 一般クエリー、Protocol Independent Multicast[PIM] hello、Cisco Group Management Protocol[CGMP] hello など）の 1 つを受信した場合、ポートはマルチキャスト ルータ ポートとなります。ポートがマルチキャスト ルータ ポートとなると、すべてのマルチキャスト トラフィック（既知および未知両方の送信元トラフィック）がすべてのマルチキャスト ルータ ポートに送信されます。これは、ルータ ガード機能がなければ防止できません。

ルータ ガード機能が設定されている場合、指定のポートをホスト ポートだけにすることができます。マルチキャスト ルータ制御パケットを受信した場合でも、ポートはルータ ポートになりません。

さらに、マルチキャスト ルータから通常どおり受信されたすべての制御パケット（IGMP クエリーおよび PIM Join など）も、このフィルタにより廃棄されます。

ルータ ガード 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。

ルータ ガード機能では、IGMP スヌーピングをイネーブルにする必要はありません。

ルータ ガードは、IPv4 にだけ実装されます。

ルータ ガードは通常、イーサネットツーホームの配置シナリオでのエンドユーザ ボックスに接続されたアクセス スイッチで使用されます。

IPv4 マルチキャスト ルータ ガード機能は、SSO に準拠します。

ルータ ガードがイネーブルであるポート上で次のパケット タイプが受信された場合は、廃棄されます。

- IGMP クエリー メッセージ
- IPv4 PIMv2 メッセージ
- IGMP PIM メッセージ（PIMv1）
- IGMP Distance Vector Multicast Routing Protocol（DVMRP）メッセージ
- Router-Port Group Management Protocol（RGMP）メッセージ
- CGMP メッセージ

これらのパケットが廃棄されると、統計情報が更新され、パケットがルータ ガードによりドロップされていることが示されます。

ルータ ガードの設定

ルータ ガード機能は、グローバルおよびインターフェイス単位で設定できます。通常、グローバルに設定すると、システム内のすべてのレイヤ 2 ポートに対してルータ ガードが開始されます。インターフェイス単位の設定は、マルチキャスト ルータが実際に接続されているポートなど、特定のポートに対するルータ ガードを無効にするのに使用できます。

次に、各タイプの設定について説明します。

- 「ルータ ガードのグローバルなイネーブル化」（P.34-9）
- 「ルータ ガードの統計情報のクリア」（P.34-10）
- 「ポート上のルータ ガードのディセーブル化」（P.34-10）

ルータ ガードのグローバルなイネーブル化

ルータ ガード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
`Router# router-guard ip multicast switchports`	ルータ ガードをグローバルにイネーブルにします。

ルータ ガードの統計情報のクリア

ルータ ガードの統計情報をクリアするには、次の作業を行います。

	コマンド	目的
ステップ 1	`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。
ステップ 2	`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。

ポート上のルータ ガードのディセーブル化

マルチキャスト ルータが接続されているレイヤ 2 ポート上でルータ ガード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
`Router(config-if)# no router-guard ip multicast [vlan vlan_id]`	レイヤ 2 ポート上でルータ ガードをディセーブルにします。 **（注）** **vlan** キーワードは、ポートがトランク モードの場合に限り有効です。このキーワードを使用すると、トランク ポート上の特定の VLAN に対するルータ ガードだけを無効にできます。

次に、トランク ポート Gigabit Ethernet 3/46、VLAN 20 上でマルチキャスト ルータ メッセージを許可する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 3/46
Router(config-if)# no router-guard ip multicast vlan 20
```

ルータ ガード設定の表示

グローバルなルータ ガード設定および特定のインターフェイスのルータ ガード設定を表示するには、次の作業を行います。

コマンド	目的
`Router# show router-guard`	グローバルなルータ ガードの設定を表示します。
`Router# show router-guard interface interface_name`	特定のインターフェイスのルータ ガードの設定を表示します。

次に、ルータ ガードがアクティブではないアクセス モードのポートのインターフェイス コマンド出力を表示する例を示します。

```
Router# show router-guard interface g3/48
  Router Guard for IP Multicast:
Globally enabled for all switch ports
Enabled on this interface
Packets denied:
```

```
  IGMP Queries:
  PIMv2 Messages:
  PIMv1 Messages:
  DVMRP Messages:
  RGMP Messages:
  CGMP Messages:
```

次に、トランク モードのポートのインターフェイス コマンド出力を表示する例を示します。

```
Router# show router-guard interface g3/48
  Router Guard for IP Multicast:
Globally enabled for all switch ports
Disabled on this interface
```

次に、トランク ポートが VLAN 10 および 20 を伝送していることを確認する例を示します。

```
Router# show router-guard interface g3/46
  Router Guard for IP Multicast:
Globally enabled for all switch ports
Default: Enabled for all VLANs on this interface
VLAN 10:
Enabled on this VLAN
Packets denied:
  IGMP Queries:
  PIMv2 Messages:
  PIMv1 Messages:
  DVMRP Messages:
  RGMP Messages:
  CGMP Messages:
VLAN 20 :
Disabled on this VLAN
```

（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、ステータスは表示されません。**show running-config interface** *xxxx* コマンドを使用すると、ルータ ガード設定を表示できます。

ルータ ガードのインターフェイスの表示

ルータ ガードがディセーブルなすべてのインターフェイスのリストを表示するには、次の作業を行います。

コマンド	目的

`Router# show router-guard interface`
`Router Guard for IP Multicast:`
`Globally enabled for all switchports`
 	
`Interfaces:`
`Gi3/46: Disabled on this port for VLANS: ALL`
	ルータ ガードがディセーブルなすべてのインターフェイスのリストを表示します。

ルータ ガードの統計情報のクリア

ルータ ガード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(config)# **clear router-guard ip multicast 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 に関する統計情報をクリアします。
Router(config)# **clear router-guard ip multicast statistics interface** *interface_name*	アクセス ポート、およびトランク ポート上のすべての VLAN に関する統計情報をクリアします。
Router(config)# **clear router-guard ip multicast statistics interface** *interface_name* **vlan** *v*	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。

次に、トランク ポート上の特定の VLAN の統計情報をクリアする例を示します。

```
Router# clear router-guard ip multicast statistics interface interface_name vlan v
```

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

ヒント