IP マルチキャスト ルーティング コマンド

clear ip mfib counters

すべてのアクティブIPV4マルチキャスト転送情報ベース（MFIB）トラフィックカウンタをクリアするには、特権 EXEC モードで **clear ip mfib counters** コマンドを使用します。

clear ip mfib ［**global** | **vrf** ***］ **counters** ［*group-address*］［*hostname* | *source-address*］

構文の説明

global	（任意）IP MFIB キャッシュをグローバルデフォルト設定にリセットします。
vrf *	（任意）すべての VPN ルーティングおよび転送インスタンスの IP MFIB キャッシュをクリアします。
group-address	（任意）アクティブ MFIB トラフィックカウンタを指定されたグループアドレスに制限します。
hostname	（任意）アクティブ MFIB トラフィックカウンタを指定されたホスト名に制限します。
source-address	（任意）アクティブ MFIB トラフィックカウンタを指定された送信元アドレスに制限します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

例

次に、すべてのマルチキャストテーブルのアクティブ MFIB トラフィックカウンタをすべてリセットする例を示します。

```
デバイス# clear ip mfib counters
```

次に、IP MFIB キャッシュカウンタをグローバルデフォルト設定にリセットする例を示します。

```
デバイス# clear ip mfib global counters
```

次に、すべての VPN ルーティングおよび転送インスタンスの IP MFIB キャッシュをクリアする例を示します。

```
デバイス# clear ip mfib vrf * counters
```

clear ip mroute

IP マルチキャスト ルーティング テーブルのエントリを削除するには、特権 EXEC モードで **clear ip mroute** コマンドを使用します。

clear ip mroute [**vrf** *vrf-name*] {***** | *ip-address* | *group-address*} [*hostname* | *source-address*]

構文の説明

vrf *vrf-name*	（任意）マルチキャスト VPN ルーティング/転送（VRF）インスタンスに割り当てられている名前を指定します。
*****	すべてのマルチキャストルートを指定します。
ip-address	IP アドレスのマルチキャストルート。
group-address	グループ アドレスのマルチキャストルート。
hostname	（任意）ホスト名のマルチキャストルート。
source-address	（任意）送信元アドレスのマルチキャストルート。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

group-address 変数は、次のいずれかを指定します。

- DNS ホストテーブルまたは **ip host** コマンドで定義されるマルチキャストグループ名
- 4 分割ドット表記によるマルチキャストグループの IP アドレス

group の名前またはアドレスを指定する場合、source 引数を入力して、グループに送信するマルチキャスト送信元の名前またはアドレスも指定できます。送信元は、グループのメンバである必要はありません。

例

次に、IP マルチキャスト ルーティング テーブルからすべてのエントリを削除する例を示します。

```
デバイス# clear ip mroute *
```

次に、マルチキャストグループ 224.2.205.42 に送信する 228.3.0.0 サブネット上のすべての送信元を IP マルチキャスト ルーティング テーブルから削除する例を示します。

この例では、ネットワーク 228.3 上の個別の送信元ではなく、すべての送信元が削除されます。

```
デバイス# clear ip mroute 224.2.205.42 228.3.0.0
```

clear ip pim snooping vlan

（注） このコマンドは Cisco Catalyst 9500 シリーズ スイッチの C9500X-28C8D モデル に適用されます。

特定の VLAN 上の Protocol Independent Multicast（PIM）スヌーピングエントリを削除するには、ユーザ EXEC または特権 EXEC モードで **clear ip pim snooping vlan** コマンドを使用します。

clear ip pim snooping vlan *vlan-id* [{**neighbor** | **statistics** | **mroute** [{*source-ipgroup-ip*}]}]

構文の説明

vlan *vlan-id*	VLAN ID。有効な値の範囲は 1 ～ 4094 です。
neighbor	すべてのネイバーを削除します。
statistics	VLAN 統計の情報を削除します。
mroute *group-addr src-addr*	指定したグループおよび送信元 IP アドレスの mroute エントリを削除します。

コマンド デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

例

次に、特定の VLAN 上の IP PIM スヌーピングエントリをクリアする例を示します。

```
Router# clear ip pim snooping vlan 1001
```

関連コマンド

コマンド	説明
ip pim snooping	PIM スヌーピングをグローバルにイネーブルにします。
show ip pim snooping	IP PIM スヌーピングに関する情報を表示します。

debug condition vrf

デバッグ出力を特定の仮想ルーティングおよび転送（VRF）インスタンスに制限するには、特権 EXEC モードで **debug condition vrf** コマンドを使用します。条件を削除するには、このコマンドの **no** 形式を使用します。

debug condition vrf {**default** | **global** | **green** | **name** {*vrf-name* | **green**}}

no debug condition vrf {**default** | **global** | **green** | **name** {*vrf-name* | **green**}}

構文の説明

構文	説明
default	デフォルトのルーティングテーブルを指定します。
global	グローバルルーティングテーブルを指定します。
green	VRF 名を指定します。
name *vrf-name*	ルーティングテーブルの名前を指定します。

コマンド モード

特権 EXEC モード（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、デバッグ出力を単一の VRF に制限します。

⚠

注意 デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。ネットワークトラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が低くなります。

例

次に、VRF red にデバッグ出力を制限する例を示します。

```
Device# debug condition vrf red
```

debug ip pim

送受信された PIM パケット、および PIM 関連のイベントを表示するには、特権 EXEC モードで **debug ip pim** コマンドを使用します。デバッグ出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ip pim [{**vrf** *vrf-name* }][{*ip-address* | **atm** | **auto-rp** | **bfd** | **bsr** | **crimson** | **df** *rp-address* | **drlb** | **hello** | **timers**}]

no debug ip pim [{**vrf** *vrf-name* }][{*ip-address* | **atm** | **auto-rp** | **bfd** | **bsr** | **crimson** | **df** *rp-address* | **drlb** | **hello** | **timers**}]

構文の説明

構文	説明
vrf *vrf-name*	（任意）VPN ルーティングおよび転送インスタンスを指定します。 このキーワードは、**debug condition vrf** *vrf-name* コマンドで指定された VRF のデバッグを上書きします。
ip-address	（任意）IP グループアドレスを指定します。
atm	（任意）PIM ATM シグナリングアクティビティに関するデバッグ情報を表示します。
auto-rp	（任意）Auto-RP 情報のデバッグ情報を表示します。
bfd	（任意）BFD コンフィギュレーションのデバッグ情報を表示します。
bsr	（任意）PIM Candidate-RP および BSR アクティビティに関するデバッグ情報を表示します。
crimson	（任意）Crimson データベースアクティビティに関するデバッグ情報を表示します。
df *rp-address*	（任意）PIM RP 指定フォワーダ選択アクティビティに関するデバッグ情報を表示します。
drlb	（任意）PIM 指定ルータのロード バランシング アクティビティに関するデバッグ情報を表示します。

構文	説明
hello	（任意）送受信された PIM Hello パケットに関するデバッグ情報を表示します。
timers	（任意）PIM タイマーイベントに関するデバッグ情報を表示します。

コマンド モード

特権 EXEC モード（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

注意 デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。ネットワークトラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が低くなります。

PIM で一度に最大 8 つの VRF をデバッグできます。複数の VRF を同時にデバッグするには、次の一連の手順を実行します。

```
debug condition vrf vrf-name1
debug condition vrf vrf-name2
.
.
.
debug condition vrf vrf-name8
debug ip pim
```

例

次に、Crimson データベースアクティビティを表示する例を示します。

```
Device# debug ip pim crimson
```

次に、PIM の 2 つの VRF red と green を同時にデバッグする例を示します。

```
Device# debug condition vrf red
Device# debug condition vrf green
Device# debug ip pim
```

debug ipv6 pim

Protocol Independent Multicast（PIM）プロトコルアクティビティのデバッグを有効にするには、特権 EXEC モードで **debug ipv6 pim** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

```
debug ipv6 pim
[{vrf vrf-name }]
[{bfd interface-type interface-number |bsr |crimson |df-election [{interface
interface-type interface-number |rp rp-address}]|drlb|group group-address|interface
interface-type interface-number |limit [{group-address}]|neighbor interface-type interface-number
}]

no debug ipv6 pim
[{vrf vrf-name }]
[{bfd interface-type interface-number |bsr |crimson |df-election [{interface
interface-type interface-number |rp rp-address}]|drlb|group group-address|interface
interface-type interface-number |limit [{group-address}]|neighbor interface-type interface-number
}]
```

構文の説明

構文	説明
vrf *vrf-name*	（任意）VPN ルーティングおよび転送インスタンスを指定します。 このキーワードは、**debug condition vrf** *vrf-name* コマンドで指定された VRF のデバッグを上書きします。
bfd	（任意）BFD コンフィギュレーションのデバッグ情報を表示します。
bsr	（任意）送受信された PIM Candidate-RP および BSR に関するデバッグ情報を表示します。
crimson	（任意）Crimson データベースアクティビティに関するデバッグ情報を表示します。
df-election	（任意）PIM 指定フォワーダ選択アクティビティに関するデバッグ情報を表示します。
drlb	（任意）PIM 指定ルータのロード バランシング アクティビティに関するデバッグ情報を表示します。

構文	説明
group *group-address*	（任意）グループ関連アクティビティに関するデバッグ情報を表示します。
interface	（任意）指定されたインターフェイスのプロトコルアクティビティに関するデバッグ情報を表示します。
limit	（任意）インターフェイス制限に関するデバッグ情報を表示します。
neighbor	（任意）送受信された PIM Hello メッセージに関するデバッグ情報を表示します。
interface-type interface-number	（任意）指定されたインターフェイスに関するデバッグ情報を表示します。
rp *rp-address*	（任意）指定された RP に関するデバッグ情報を表示します。

コマンド モード

特権 EXEC モード（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

⚠

注意 デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。ネットワークトラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が低くなります。

PIM で一度に最大 8 つの VRF をデバッグできます。複数の VRF を同時にデバッグするには、次の一連の手順を実行します。

```
debug condition vrf vrf-name1
debug condition vrf vrf-name2
.
.
.
debug condition vrf vrf-name8
debug ip pim
```

例

次に、Crimson データベースアクティビティを表示する例を示します。

```
Device# debug ipv6 pim crimson
```

次に、VRF red をデバッグする例を示します。

```
Device# debug vrf red ipv6 pim
```

ip igmp filter

Internet Group Management Protocol（IGMP）プロファイルをインターフェイスに適用することで、レイヤ 2 インターフェイスのすべてのホストが 1 つ以上の IP マルチキャストグループに参加できるかどうかを制御するには、device スタックまたはスタンドアロン device で **ip igmp filter** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスから指定されたプロファイルを削除するには、このコマンドの **no** 形式を使用します。

ip igmp filter *profile number*
no ip igmp filter

構文の説明

profile number	適用する IGMP プロファイル番号。範囲は 1 ～ 4294967295 です。

コマンド デフォルト

IGMP フィルタは適用されていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

IGMP フィルタはレイヤ 2 の物理インターフェイスだけに適用できます。ルーテッドポート、Switch Virtual Interface（SVI）、または EtherChannel グループに属するポートに対して IGMP フィルタを適用することはできません。

IGMP プロファイルは 1 つまたは複数のdevice ポートインターフェイスに適用できますが、1 つのポートに対して 1 つのプロファイルだけ適用できます。

例

次に、IGMP プロファイル 40 を設定して、指定した範囲の IP マルチキャストアドレスを許可し、その後、プロファイルをフィルタとしてポートに適用する例を示します。

```
デバイス(config)# ip igmp profile 40
デバイス(config-igmp-profile)# permit
デバイス(config-igmp-profile)# range 233.1.1.1 233.255.255.255
デバイス(config-igmp-profile)# exit
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# switchport
*Jan  3 18:04:17.007: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to
down.
NOTE: If this message appears, this interface changes to layer 2, so that you can apply
 the filter.
デバイス(config-if)# ip igmp filter 40
```

設定を確認するには、特権 EXEC モードで **show running-config** コマンドを使用してインターフェイスを指定します。

ip igmp max-groups

レイヤ 2 インターフェイスが参加可能な Internet Group Management Protocol（IGMP）グループの最大数を設定するか、最大数のエントリが転送テーブルにあるときの IGMP スロットリングアクションを設定するには、device スタックまたはスタンドアロン device で **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値（無制限）に戻すか、デフォルトのスロットリングアクション（レポートをドロップ）に戻すには、このコマンドの **no** 形式を使用します。

ip igmp max-groups {*max number* | **action** { **deny** | **replace**}}
no ip igmp max-groups {*max number* | **action**}

構文の説明

max number	インターフェイスが参加できる IGMP グループの最大数。範囲は 0 ～ 4294967294 です。デフォルト設定は無制限です。
action deny	最大数のエントリが IGMP スヌーピング転送テーブルにある場合は、次の IGMP 参加レポートをドロップします。これがデフォルトのアクションになります。
action replace	最大数のエントリが IGMP スヌーピング転送テーブルにある場合に、IGMP レポートを受信した既存のグループを新しいグループで置き換えます。

コマンド デフォルト

デフォルトの最大グループ数は制限なしです。

インターフェイス上に IGMP グループエントリの最大数があることをdeviceが学習した後の、デフォルトのスロットリングアクションでは、インターフェイスが受信する次の IGMP レポートをドロップし、インターフェイスに IGMP グループのエントリを追加しません。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、レイヤ 2 物理インターフェイスおよび論理 EtherChannel インターフェイスでだけ使用できます。ルーテッドポート、Switch Virtual Interface（SVI）、または EtherChannel グループに属するポートに対して IGMP 最大グループ数を設定することはできません。

IGMP スロットリングアクションを設定する場合には、次の注意事項に従ってください。

- スロットリングアクションを deny として設定して最大グループ制限を設定する場合、以前転送テーブルにあったエントリは、削除されませんが期限切れになります。これらのエントリの期限が切れた後で、エントリの最大数が転送テーブルにある場合は、インターフェイス上で受信された次の IGMP レポートを device がドロップします。

- スロットリングアクションを replace として設定して最大グループ制限を設定する場合、以前転送テーブルにあったエントリは削除されます。最大数のエントリが転送テーブルにある場合、deviceはランダムに選択したマルチキャストエントリを受信した IGMP レポートで置き換えます。
- グループの最大数に関する制限がデフォルト（制限なし）に設定されている場合、**ip igmp max-groups {deny | replace}** コマンドを入力しても効果はありません。

例

次に、ポートが加入できる IGMP グループ数を 25 に制限する例を示します。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# ip igmp max-groups 25
```

次に、最大数のエントリが転送テーブルにあるときに、IGMP レポートを受信した既存のグループを新しいグループと置き換えるようにdeviceを設定する方法を示します。

```
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# ip igmp max-groups action replace
```

設定を確認するには、**show running-config** 特権 EXEC コマンドを使用してインターフェイスを指定します。

ip igmp profile

Internet Group Management Protocol（IGMP）プロファイルを作成し、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、device スタックまたはスタンドアロン device で **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。このモードで、スイッチポートからの IGMP メンバーシップレポートをフィルタリングするための IGMP プロファイルの設定を指定できます。IGMP プロファイルを削除するには、このコマンドの **no** 形式を使用します。

ip igmp profile *profile number*
no ip igmp profile *profile number*

構文の説明

profile number	設定する IGMP プロファイル番号。範囲は 1 ～ 4294967295 です。

コマンド デフォルト

IGMP プロファイルは定義されていません。設定された場合、デフォルトの IGMP プロファイルとの一致機能は、一致するアドレスを拒否する設定になります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

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することで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ように指定します（デフォルト設定の状態）。
- **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、またはデフォルトにリセットします。
- **permit**：一致するアドレスを許可するように指定します。
- **range**：プロファイルの IP アドレスの範囲を指定します。1 つの IP アドレス、またはアドレスの最初と最後で範囲を指定することもできます。

  範囲を入力する場合、低い方の IP マルチキャストアドレスを入力してからスペースを入力し、次に高い方の IP マルチキャストアドレスを入力します。

IGMP のプロファイルを、1 つまたは複数のレイヤ 2 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。

例

次の例では、指定された範囲の IP マルチキャストアドレスを許可する IGMP プロファイル 40 の設定方法を示します。

```
デバイス(config)# ip igmp profile 40
デバイス(config-igmp-profile)# permit
デバイス(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

設定を確認するには、特権 EXEC モードで **show ip igmp profile** コマンドを使用します。

ip igmp snooping

device で Internet Group Management Protocol（IGMP; インターネットグループ管理プロトコル）スヌーピングをグローバルにイネーブルにするか、または VLAN 単位でイネーブルにするには、device スタックまたはスタンドアロン device で **ip igmp snooping** 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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping ［**vlan** *vlan-id*］
no ip igmp snooping ［**vlan** *vlan-id*］

構文の説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングをイネーブルにします。範囲は 1 ～ 1001 および 1006 ～ 4094 です。

コマンド デフォルト

device 上で、IGMP スヌーピングはグローバルに有効になっています。

VLAN インターフェイス上で、IGMP スヌーピングはイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

IGMP スヌーピングがグローバルにイネーブルである場合は、すべての既存 VLAN インターフェイスでイネーブルになります。IGMP スヌーピングがグローバルにディセーブルである場合、すべての既存 VLAN インターフェイスで IGMP スヌーピングがディセーブルになります。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

例

次の例では、IGMP スヌーピングをグローバルにイネーブルにする方法を示します。

```
デバイス(config)# ip igmp snooping
```

次の例では、IGMP スヌーピングを VLAN 1 でイネーブルにする方法を示します。

```
デバイス(config)# ip igmp snooping vlan 1
```

設定を確認するには、特権 EXEC モードで **show ip igmp snooping** コマンドを入力します。

ip igmp snooping last-member-query-count

Internet Group Management Protocol（IGMP）スヌーピングが IGMP 脱退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回数を設定するには、グローバル コンフィギュレーション モードで **ip igmp snooping last-member-query-count** コマンドを使用します。*count* をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

ip igmp snooping ［**vlan** *vlan-id*］ **last-member-query-count** *count*
no ip igmp snooping ［**vlan** *vlan-id*］ **last-member-query-count** *count*

構文の説明

vlan *vlan-id*	（任意）特定の VLAN ID のカウント値を指定します。範囲は 1 ～ 1001 です。先頭の 0 は入力しないでください。
count	クエリーメッセージの送信インターバルを、ミリ秒単位で設定します。範囲は 1 ～ 7 です。デフォルトは 2 です。

コマンド デフォルト

クエリーが 2 ミリ秒ごとに送信されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

マルチキャストホストがグループから脱退すると、ホストはIGMP脱退メッセージを送信します。このホストがグループを脱退する最終ホストかどうかを確認するために、脱退メッセージが確認されると、**last-member-query-interval** タイムアウト期間が過ぎるまで IGMP クエリーメッセージが送信されます。タイムアウト期限が切れる前に last-member クエリーへの応答が受信されないと、グループレコードは削除されます。

タイムアウト期間を設定するには、**ip igmp snooping last-member-query-interval** コマンドを使用します。

IGMP スヌーピング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、即時脱退処理が優先されます。

（注） カウントを 1 に設定しないでください。単一パケットの損失（device からホストへのクエリーパケット、またはホストから device へのレポートパケット）により、受信者がまだいてもトラフィックの転送が停止される場合があります。トラフィックは、次の一般クエリーが device から送信された後も転送され続けますが、受信者がクエリーを受信しない間隔は 1 分間（デフォルトのクエリー間隔で）となる可能性があります。

Cisco IOS ソフトウェアの脱退遅延は、device が last-member-query-interval（LMQI）内で複数の脱退を処理しているときに、1 つの LMQI 値まで増やすことができます。このシナリオでは、平均脱退遅延は (カウント数 + 0.5) * LMQI によって決まります。その結果、デフォルトの脱退遅延は 2.0 ～ 3.0 秒の範囲となり、IGMP 脱退処理の負荷が高い状態では平均 2.5 秒となります。100 ミリ秒でカウントが 1 という LMQI の最小値の負荷条件下では、脱退遅延は 100 ～ 200ミリ秒となり、平均は 150 ミリ秒です。これは、高レートの IGMP 脱退メッセージから受ける影響を抑えるために行われます。

例

次に、最後のメンバクエリーの数を 5 に設定する例を示します。

```
デバイス(config)# ip igmp snooping last-member-query-count 5
```

ip igmp snooping querier

レイヤ 2 ネットワークで Internet Group Management Protocol（IGMP）クエリア機能をグローバルにイネーブルにするには、**ip igmp snooping querier** 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。キーワードとともにコマンドを入力すると、VLANインターフェイスのIGMP クエリア機能をイネーブルにし、設定できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip igmp snooping ［**vlan** *vlan-id*］ **querier** ［**address** *ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** {**count** *count* | **interval** *interval*} | **timer expiry** *expiry-time* | **version** *version*］
no ip igmp snooping ［**vlan** *vlan-id*］ **querier** ［**address** | **max-response-time** | **query-interval** | **tcn query** {**count** | **interval**} | **timer expiry** | **version**］

構文の説明

vlan *vlan-id*	（任意）指定された VLAN で IGMP スヌーピングおよび IGMP クエリア機能をイネーブルにします。範囲は 1 ～ 1001 および 1006 ～ 4094 です。
address *ip-address*	（任意）送信元 IP アドレスを指定します。IP アドレスを指定しない場合、クエリアはIGMP クエリアに設定されたグローバルIP アドレスを使用します。
max-response-time *response-time*	（任意）IGMP クエリアレポートを待機する最長時間を設定します。範囲は 1 ～ 25 秒です。
query-interval *interval-count*	（任意）IGMP クエリアの間隔を設定します。範囲は 1 ～ 18000 秒です。
tcn query	（任意）トポロジ変更通知（TCN）に関連するパラメータを設定します。
count *count*	TCN 時間間隔に実行される TCN クエリの数を設定します。範囲は 1 ～ 10 です。
interval 間隔	TCN クエリの時間間隔を設定します。範囲は 1 ～ 255 です。
timer expiry *expiry-time*	（任意）IGMP クエリアが期限切れになる時間を設定します。範囲は 60 ～ 300 秒です。
version *version*	（任意）クエリア機能が使用するIGMPバージョン番号を選択します。選択できる番号は 1 または 2 です。

コマンド デフォルト

IGMP スヌーピングクエリア機能は、device でグローバルにディセーブルに設定されています。

IGMP スヌーピングクエリアは、イネーブルの場合でも、マルチキャストルータからの IGMP トラフィックが検出されると、自らをディセーブルにします。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

クエリアとも呼ばれる IGMP クエリメッセージを送信するデバイスの IGMP バージョンおよび IP アドレスを検出するために IGMP スヌーピングをイネーブルにするには、このコマンドを使用します。

デフォルトでは、IGMP スヌーピングクエリアは、IGMP バージョン 2（IGMPv2）を使用するデバイスを検出するよう設定されていますが、IGMP バージョン 1（IGMPv1）を使用しているクライアントは検出しません。デバイスが IGMPv2 を使用している場合、**max-response-time** 値を手動で設定できます。デバイスが IGMPv1 を使用している場合は、max-response-time を設定できません（値を設定できず、0 に設定されています）。

IGMPv1 を実行している RFC に準拠していないデバイスは、**max-response-time** 値としてゼロ以外の値を持つ IGMP 一般クエリメッセージを拒否することがあります。デバイスで IGMP 一般クエリメッセージを受け入れる場合、IGMP スヌーピングクエリアが IGMPv1 を実行するように設定します。

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

例

次の例では、IGMP スヌーピングクエリア機能をグローバルにイネーブルにする方法を示します。

```
デバイス(config)# ip igmp snooping querier
```

次の例では、IGMP スヌーピングクエリアの最大応答時間を 25 秒に設定する方法を示します。

```
デバイス(config)# ip igmp snooping querier max-response-time 25
```

次の例では、IGMP スヌーピングクエリアの時間間隔を 60 秒に設定する方法を示します。

```
デバイス(config)# ip igmp snooping querier query-interval 60
```

次の例では、IGMP スヌーピングクエリアの TCN クエリカウントを 25 に設定する方法を示します。

```
デバイス(config)# ip igmp snooping querier tcn count 25
```

次の例では、IGMP スヌーピングクエリアのタイムアウト値を 60 秒に設定する方法を示します。

```
デバイス(config)# ip igmp snooping querier timer expiry 60
```

次に、IGMP スヌーピングクエリア機能をバージョン 2 に設定する例を示します。

```
デバイス(config)# ip igmp snooping querier version 2
```

設定を確認するには、**show ip igmp snooping** 特権 EXEC コマンドを入力します。

ip igmp snooping report-suppression

Internet Group Management Protocol（IGMP）レポート抑制をイネーブルにするには、device スタックまたはスタンドアロン device で **ip igmp snooping report-suppression** 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 レポート抑制をディセーブルにして、すべての IGMP レポートをマルチキャストルータに転送するには、このコマンドの **no** 形式を使用します。

ip igmp snooping report-suppression
no ip igmp snooping report-suppression

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IGMP レポート抑制はイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

IGMP レポート抑制は、マルチキャストクエリに IGMPv1 レポートと IGMPv2 レポートがある場合にだけサポートされます。この機能は、クエリに IGMPv3 レポートが含まれている場合はサポートされません。

device は IGMP レポート抑制を使用して、マルチキャストルータクエリごとに 1 つの IGMP レポートのみをマルチキャストデバイスに転送します。IGMP レポート抑制がイネーブル（デフォルト）である場合、device は最初の IGMP レポートをグループのすべてのホストからすべてのマルチキャストルータに送信します。deviceは、グループの残りの IGMP レポートをマルチキャストルータに送信しません。この機能により、マルチキャストデバイスにレポートが重複して送信されることを防ぎます。

マルチキャストルータクエリに IGMPv1 および IGMPv2 レポートに対する要求のみが含まれている場合、device は最初の IGMPv1 レポートまたは IGMPv2 レポートのみを、グループのすべてのホストからすべてのマルチキャストルータに転送します。マルチキャストルータクエリに IGMPv3 レポートに対する要求も含まれる場合、deviceはグループのすべての IGMPv1、IGMPv2、および IGMPv3 レポートをマルチキャストデバイスに転送します。

no ip igmp snooping report-suppression コマンドを入力して IGMP レポート抑制をディセーブルにした場合、すべての IGMP レポートがすべてのマルチキャストルータに転送されます。

例

次の例では、レポート抑制をディセーブルにする方法を示します。

```
デバイス(config)# no ip igmp snooping report-suppression
```

設定を確認するには、特権 EXEC モードで **show ip igmp snooping** コマンドを入力します。

ip igmp snooping tcn flood

インターフェイスで TCN フラッディングを明示的に無効にした後、インターフェイスのスパニングツリーのトポロジ変更通知（TCN）イベント中にマルチキャストトラフィックのフラッディングを有効にするには、グローバル コンフィギュレーション モードで **ip igmp snooping tcn flood** コマンドを使用します。インターフェイスでTCNフラッディングを無効にするには、このコマンドの **no** 形式を使用します。

ip igmp snooping tcn flood
no ip igmp snooping tcn flood

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

TCN フラッディングはインターフェイスで有効になっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

インターフェイスで TCN フラッディングを無効または有効にするには、このコマンドを使用します。TCNフラッディングはデフォルトでは、すべてのインターフェイスで有効になっています。

スパニングツリープロトコル（STP）は、仮想ポートレベルで動作します。仮想ポートがTCNイベントを受信すると、その仮想ポートで動作するすべてのインターフェイスが、そのインターフェイスが属するブリッジドメインとともに識別されます。フラッディングは、TCN フラッディングが明示的に無効になっているインターフェイスを除き、ブリッジドメイン上のすべてのインターフェイスに対して開始されます。このフラッディングは仮想ポートのキャパシティを超え、パケット損失を引き起こす可能性があります。スパニングツリーの TCN イベント中にインターフェイスのマルチキャストトラフィックのフラッディングを無効にするには、**no ip igmp snooping tcn flood** コマンドを使用します。

例

次の例では、インターフェイス上のホストをスタティックに設定する方法を示します。

```
デバイス(config)#  int twe1/0/3
 (config-if)# no ip igmp snooping tcn flood
```

例

次に、TCN フラッディングを無効にする例を示します。

```
Device# sh pl so fed sw ac ip igmp snooping vlan 100
Vlan 100
---------
IGMPSN Enabled  : On
PIMSN Enabled   : Off
Flood Mode      : Off
Oper State      : Up
STP TCN Flood   : Off
Routing Enabled : On
PIM Enabled     : On
PVLAN           : No
In Retry        : 0x0
CCK Epoch       : 0x35
IOSD Flood Mode : Off
EVPN Proxy Enabled : Off
L3mcast Adj      :
Mrouter PortQ   :
TwentyFiveGigE1/0/2
Svl Link        : Enabled
Flood PortQ     : TwentyFiveGigE1/0/2
                  TwentyFiveGigE1/0/3
                  TwentyFiveGigE1/0/34
TCN PortQ     :
REP RI handle   : 0x0
```

STP TCN Flood が on に設定されると、no ip igmp snooping tcn flood が設定されたポートは TCN PortQ から除外されます。マルチキャストトラフィックでフラッディングされるポートは、それぞれのローカルまたはリモート TCN PortQ に追加されます。次の例では、インターフェイス TwentyFiveGigE1/0/3 が no ip igmp snooping tcn flood コマンドで設定され、TCN portQ から除外されます。

```
Device(config) interface TwentyFiveGigE1/0/3
Device(config-if)# switchport access vlan 101
Device(config-if)# switchport mode access
Device(config-if)# no ip igmp snooping tcn flood
Device(config-if)# end

lannister#sh pl so fed sw ac ip igmp snooping vlan 101
Vlan 101
---------
IGMPSN Enabled  : On
PIMSN Enabled   : Off
Flood Mode      : Off
Oper State      : Up
STP TCN Flood   : On
Routing Enabled : On
PIM Enabled     : On
PVLAN           : No
In Retry        : 0x0
CCK Epoch       : 0x35
IOSD Flood Mode : Off
EVPN Proxy Enabled : Off
L3mcast Adj      :
Mrouter PortQ   : TwentyFiveGigE1/0/29
Svl Link        : Enabled
Flood PortQ     : TwentyFiveGigE1/0/29
                  TwentyFiveGigE1/0/2
                  TwentyFiveGigE1/0/3
TCN PortQ: TwentyFiveGigE1/0/2
TCN Remote Ports:TwentyFiveGigE2/0/2
REP RI handle: 0x0
```

ip igmp snooping vlan mrouter

マルチキャストルータポートの追加を行うには、deviceスタックまたはスタンドアロンdeviceで **ip igmp snooping mrouter** 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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

コマンド デフォルト

デフォルトでは、マルチキャストルータポートはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

VLAN ID 1002 ～ 1005 は、トークンリングおよびFDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

設定は、NVRAM に保存されます。

例

次の例では、ポートをマルチキャストルータポートとして設定する方法を示します。

```
デバイス(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/0/2
```

設定を確認するには、**show ip igmp snooping** 特権 EXEC コマンドを入力します。

ip igmp snooping vlan static

Internet Group Management Protocol（IGMP）スヌーピングをイネーブルにし、マルチキャストグループのメンバとしてレイヤ 2 ポートをスタティックに追加するには、device スタックまたはスタンドアロン device で **ip igmp snooping vlan static** 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。静的マルチキャストグループのメンバとして指定されたポートを削除するには、このコマンドの **no** 形式を使用します。

ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*
no ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

構文の説明

vlan-id	指定した VLAN で IGMP スヌーピングをイネーブルにします。範囲は 1 ～ 1001 および 1006 ～ 4094 です。
ip-address	指定のグループ IP アドレスを持ったマルチキャストグループのメンバとして、レイヤ 2 ポートを追加します。
interface *interface-id*	メンバポートのインターフェイスを指定します。 *interface-id* には次のオプションがあります。 • *fastethernet interface number*：ファストイーサネット IEEE 802.3 インターフェイス。 • *gigabitethernet interface number*：ギガビットイーサネット IEEE 802.3z インターフェイス。 • *tengigabitethernet interface number*：10 ギガビットイーサネット IEEE 802.3z インターフェイス。 • *port-channel interface number*：チャネルインターフェイス。範囲は 0 ～ 128 です。

コマンド デフォルト

デフォルトでは、マルチキャストグループのメンバとしてスタティックに設定されたポートはありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

設定は、NVRAM に保存されます。

例

次の例では、インターフェイス上のホストをスタティックに設定する方法を示します。

```
デバイス(config)# ip igmp snooping vlan 1 static 224.2.4.12 interface
gigabitEthernet1/0/1

Configuring port gigabitethernet1/0/1 on group 224.2.4.12
```

設定を確認するには、特権 EXEC モードで **show ip igmp snooping** コマンドを入力します。

ip multicast auto-enable

IP マルチキャストの認証、許可、およびアカウンティング（AAA）の有効化をサポートするには、 **ip multicast auto-enable** コマンドを使用します。このコマンドによって、RADIUS サーバから、AAA 属性を使用しているダイヤルアップ インターフェイスでのマルチキャストルーティングをダイナミックに有効化できます。AAA の IP マルチキャストを無効にするには、このコマンドの **no** 形式を使用します。

ip multicast auto-enable
no ip multicast auto-enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

なし

例

次の例は、IP マルチキャスト上の AAA をイネーブルにする方法を示します。

```
デバイス(config)# ip multicast auto-enable
```

ip multicast-routing

IP マルチキャストルーティングをイネーブルにするには、グローバル コンフィギュレーション モードで **ip multicast-routing** コマンドを使用します。IP マルチキャストルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip multicast-routing ［**vrf** *vrf-name* ］
no ip multicast-routing ［**vrf** *vrf-name* ］

構文の説明

vrf *vrf-name*	（任意）*vrf-name* 引数に指定されたマルチキャスト VPN ルーティングおよび転送（MVRF）インスタンスのための IP マルチキャストルーティングを有効にします。

コマンド デフォルト

IP マルチキャストルーティングはディセーブルになっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.6.1	このコマンドが導入されました。

使用上のガイドライン

IP マルチキャストルーティングがディセーブルになっている場合、Cisco IOS XE ソフトウェアはどのマルチキャストパケットも転送しません。

（注） IPマルチキャストの場合は、IPマルチキャストルーティングを有効にした後に、PIMをすべてのインターフェイスに設定する必要があります。IPマルチキャストルーティングを無効にしても PIM は削除されません。PIM は、インターフェイスの設定から明示的に削除する必要があります。

例

次に、IP マルチキャストルーティングをイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip multicast-routing
```

次に、特定の VRF の IP マルチキャストルーティングを有効にする例を示します。

```
Device(config)# ip multicast-routing vrf vrf1
```

関連コマンド

コマンド	説明
ip pim	インターフェイスに対して PIM をイネーブルにします。

ip pim accept-register

Protocol Independent Multicast（PIM）登録メッセージをフィルタ処理するように候補ランデブーポイント（RP）スイッチを設定するには、グローバル コンフィギュレーション モードで **ip pim accept-register** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

ip pim ［**vrf** *vrf-name* ］ **accept-register** {**list** *access-list*}
no ip pim ［**vrf** *vrf-name* ］ **accept-register**

構文の説明

vrf *vrf-name*	（任意）*vrf-name* 引数に指定されたマルチキャスト バーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（MVRF）インスタンスに関連付けられている (S, G) トラフィック用の候補 RP で PIM 登録フィルタを設定します。
list *access-list*	許可または拒否する PIM 登録メッセージ内の (S, G) トラフィックを定義する数値または名前として、*access-list* 引数を指定します。指定できる範囲は 100 ～ 199 で、拡張された範囲は 2000 ～ 2699 です。IP 名前付きアクセス リストも使用できます。

コマンド デフォルト

PIM 登録フィルタは設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

不正な送信元が RP に登録されないようにするには、このコマンドを使用します。不正な送信元が RP に登録メッセージを送信すると、RP はただちに登録停止メッセージを送り返します。

ip pim accept-register コマンドに提供されるアクセスリストは IP 送信元アドレスと IP 宛先アドレスのみをフィルタ処理します。その他のフィールドのフィルタリング（たとえば、IP プロトコルまたは UDP ポート番号）は無効になっています。これらは、共有ツリーの下方の RP からマルチキャスト グループ メンバに不要なトラフィックを転送する場合があります。より複雑なフィルタリングが必要な場合は、代わりに、**ip multicast boundary** コマンドを使用します。

例

次に、SSM グループ範囲（232.0.0.0/8）に送信している送信元アドレス 172.16.10.1 を除き、任意のグループ範囲に送信している送信元アドレスの登録パケットを許可する例を示します。これらは拒否されます。候補 RP は最初のホップ ルータまたはスイッチから PIM 登録を受信するため、これらのステートメントはすべての候補 RP に設定する必要があります。

```
デバイス(config)# ip pim accept-register list ssm-range
デバイス(config)# ip access-list extended ssm-range
デバイス(config-ext-nacl)# deny ip any 232.0.0.0 0.255.255.255
デバイス(config-ext-nacl)# permit ip any any
```

ip pim bidir-enable

双方向 Protocol Independent Multicast（双方向 PIM）をイネーブルにするには、グローバル コンフィギュレーション モードで **ip pim bidir-enable** コマンドを使用します。双方向 PIM をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip pim bidir-enable

no ip pim bidir-enable

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

コマンド デフォルト

このコマンドはイネーブルになります。

コマンド モード

グローバル コンフィギュレーション（config）

使用上のガイドライン

双方向 PIM をディセーブルにすると、ルータは双方向 PIM をサポートしていないルータと同様に動作します。次の条件が適用されます。

- ルータが送信する PIM hello メッセージには、双方向モードオプションが含まれません。
- ルータは指定フォワーダ（DF）選定メッセージを送信せず、受信した DF 選定メッセージを無視します。
- **ip pim rp-address**、**ip pim send-rp-announce**、および **ip pim rp-candidate** グローバル コンフィギュレーション コマンドは次のように処理されます。
  - 双方向 PIM がディセーブルでこれらのコマンドを設定する場合、双方向モードはコンフィギュレーション オプションにはなりません。
  - 双方向 PIM がイネーブルからディセーブルになった場合に、双方向モード オプションとともにこれらのコマンドを設定すると、これらのコマンドはコマンドラインインターフェイス（CLI）から削除されます。この状況では、双方向 PIM を再度イネーブルにするときに、双方向モードオプションを指定してこれらのコマンドを再度設定する必要があります。
- **show ip pim interface** ユーザ EXEC コマンドまたは特権 EXEC コマンドと **debug ip pim** 特権 EXEC コマンドの **df** キーワードはサポートされません。

次に、双方向 PIM をイネーブルにする例を示します。

```
Device# enable
Device# configure terminal
Device(config)# ip pim bidir-enable
```

ip pim bsr-candidate

候補 BSR になるように デバイス を設定するには、グローバル コンフィギュレーション モードで **ip pim bsr-candidate** コマンドを使用します。候補 BSR としてのスイッチを削除するには、このコマンドの **no** 形式を使用します。

ip pim ［**vrf** *vrf-name*］ **bsr-candidate** *interface-id* ［*hash-mask-length*］［*priority*］
no ip pim ［**vrf** *vrf-name* ］ **bsr-candidate**

構文の説明

vrf *vrf-name*	（任意） *vrf-name* 引数に指定されたマルチキャスト バーチャル プライベート ネットワーク（MVPN）ルーティングおよび転送（MVRF）インスタンスの候補 BSR になるように デバイス を設定します。
interface-id	BSR アドレスを候補にするための、そのアドレスの派生元である デバイス のインターフェイスの ID。このインターフェイスは、**ip pim** コマンドを使用して、Protocol Independent Multicast（PIM）に対して有効にする必要があります。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。
hash-mask-length	（任意）PIMv2 ハッシュ機能がコールされる前にグループ アドレスと論理積をとるマスク長（最大 32 ビット）。同じシード ハッシュを持つグループはすべて、同じランデブー ポイント（RP）に対応します。たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。ハッシュ マスク長により、1 つの RP を複数のグループで使用できるようになります。デフォルトのハッシュ マスク長は 0 です。
priority	（任意）BSR（C-BSR）候補のプライオリティ。有効な範囲は 0 ～ 255 です。デフォルトのプライオリティは 0 です。最高のプライオリティ値を持つ C-BSR が優先されます。

コマンド デフォルト

デバイス はそれ自体を候補 BSR として通知するように設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドに指定したインターフェイスは、**ip pim** コマンドを使用して、Protocol Independent Multicast（PIM）に対して有効にする必要があります。

このコマンドは、指定されたインターフェイスのアドレスを BSR アドレスとして示す BSR メッセージをすべての PIM ネイバーに送信するように デバイス を設定します。

このコマンドは、PIM ドメイン内のすべての部分に良好に接続できるバックボーン デバイス で設定する必要があります。

BSR メカニズムは RFC 2362 で指定されています。候補 RP（C-RP）は、ユニキャスト C-RP アドバタイズメント パケットを BSR にスイッチングします。その後、BSR は、これらのアドバタイズメントを BSR メッセージに集約します。BSR メッセージは、TTL 1 で、ALL-PIM-ROUTERS グループのアドレス 224.0.0.13 に定期的にマルチキャストされます。これらのメッセージのマルチキャストは、ホップバイホップ RPF フラッディングによって処理されます。事前の IP マルチキャスト ルーティング設定は必要がありません（AutoRP とは異なる）。また、BSR は、特定のグループ範囲について指定された RP を事前に選択しません（AutoRPとは異なる）。代わりに、BSR メッセージを受信する各スイッチが BSR メッセージ内の情報に基づいてグループ範囲の RP を選択します。

シスコ デバイス は BSR メッセージを常に受け入れ、処理します。この機能を無効にするコマンドはありません。

シスコ デバイス は、次の手順で、どの C-RP がグループで使用されているかを判別します。

- BSR C-RP で通知されるグループ プレフィックスに対して最長一致ルックアップを実行します。
- 最長一致ルックアップによって BSR が学習した C-RP が複数見つかった場合は、優先順位が最低の C-RP（**ip pim rp-candidate** コマンドで設定される）が優先されます。
- 複数の BSR が学習した C-RP で優先順位が同じ場合は、グループの RP を選択するために、BSR ハッシュ関数が使用されます。
- 複数の BSR が学習した C-RP が BSR ハッシュ関数から派生された同じハッシュ値を返す場合は、最高の IP アドレスの BSR C-RP が優先されます。

例

次に、ハッシュ マスク長 0 および優先順位 192 を使用して、ギガビット イーサネット インターフェイス 1/0/0 の デバイス の IP アドレスが BSR C-RP になるように設定する例を示します。

```
デバイス(config)# ip pim bsr-candidate GigabitEthernet1/0/1 0 192
```

ip pim rp-address

マルチキャストグループの Protocol Independent Multicast（PIM）ランデブーポイント（RP）のアドレスを静的に設定するには、グローバル コンフィギュレーション モードで**ip pim rp-address** コマンドを使用します。RP アドレスを削除するには、このコマンドの **no** 形式を使用します。

ip pim［**vrf** *vrf-name*］**rp-address** *rp-address*［*access-list*］［**override** ］［**bidir**］

no ip pim［**vrf** *vrf-name*］**rp-address** *rp-address*［*access-list*］［**override** ］［**bidir**］

構文の説明

vrf *vrf-name*	（任意）vrf-name 引数に指定されているマルチキャスト バーチャル プライベート ネットワーク（MVPN）ルーティングと転送（MVRF）インスタンスに関連付けられる静的グループ-RP マッピングを指定します。
rp-address *rp-address*	静的グループ-RP マッピングに使用される RP の IP アドレス。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。
access-list	（任意）RP に静的にマッピングされるマルチキャスト グループを定義する標準アクセス リストの番号または名前。 （注） アクセスリストが定義されていない場合、RP がすべてのマルチキャストグループにマッピングされます。
override	（任意）動的グループ-RP マッピングと静的グループ-RP マッピングが一緒に使用されており、RP アドレスの競合がある場合に、静的グループ-RP マッピングに設定されている RP アドレスが優先されるように指定します。 （注） **override** キーワードが指定されておらず、RP アドレスが競合している場合、ダイナミックグループと RP 間のマッピングがスタティックグループと RP 間のマッピングに優先されます。

bidir	（任意）双方向 PIM RP に静的グループ-RP マッピングを適用するように指定します。 **bidir** キーワードを指定せずにコマンドを設定した場合、グループはスパースモードで動作します。 （注） **bidir** キーワードは、**ip pim bidir-enable** コマンドを使用して双方向 PIM がイネーブルになっている場合にのみオプションキーワードとして使用できます。

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

コマンド デフォルト

PIM の静的グループ-RP マッピングは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

使用上のガイドライン

PIM では、スパースモード（PIM-SM）または双方向モード（双方向 PIM）のマルチキャストグループは、RP を使用してソースとレシーバに接続します。PIM ドメイン内のすべてのルータが、そのモードの一貫した設定とマルチキャスト グループの RP アドレスを持っている必要があります。

Cisco IOS ソフトウェアは、静的グループ-RP マッピング コンフィギュレーション、Auto-RP、およびブートストラップ ルータ（BSR）の 3 つのメカニズムを通じて、マルチキャスト グループのモードと RP アドレスを学習します。

PIM-SM または双方向 PIM グループの RP アドレスを静的に定義するには、**ip pim rp-address** コマンドを使用します（**ip pim rp-address** コマンド コンフィギュレーションは、静的グループ-RP マッピングと呼ばれます）。

アクセス リストを使用して、複数のグループに対して単一の RP を設定できます。アクセスリストを指定しなかった場合は、その静的 RP はすべてのマルチキャストグループにマッピングされます。

複数の RP を設定できますが、グループ範囲ごとに設定できる RP は 1 つだけです。

複数の **ip pim rp-address** コマンドを設定した場合は、次の規則が適用されます。

- 到達可能性に関係なく、最も高い RP IP アドレスが選択される。設定済みの複数の **ip pim rp-addres** コマンドのアクセスリストに一致するマルチキャストグループの RP は、設定されている RP アドレスが最も高い RP によって決まります。
- コマンドごとに 1 つの RP アドレス。複数の **ip pim rp-address** コマンドが設定されている場合、各静的グループ-RP マッピングが、固有の RP アドレスで設定されている必要があります（重複していると、上書きされます）。この制限は、それぞれのスパースモードま

たは双方向モードグループに RP 機能を提供するために使用できる RP アドレスは 1 つだけだということも意味します。双方向モードとスパース モード両方用の静的グループ-RP マッピングを設定したい場合は、それぞれのモードに固有の RP アドレスを指定する必要があります。

- コマンドごとに 1 つのアクセスリスト。複数の **ip pim rp-address** コマンドが設定されている場合に、静的グループ-RP マッピングごとに設定できるアクセスリストは 1 つだけです。アクセス リストを同じルータ上で設定されている他の静的グループ-RP マッピングに再使用することはできません。

動的グループ-RP マッピングと静的グループ-RP マッピングが一緒に使用されている場合、マルチキャストグループには、**override** キーワードが使用されていないかぎり、動的グループ-RP マッピングが静的グループ-RP マッピングよりも優先されるという規則が適用されます。

次の例は、マルチキャストグループ範囲 239/8 の双方向 PIM RP アドレスを 172.16.0.2 に設定する方法を示しています。

```
Device(config)# access list 10 239.0.0.0 0.255.255.255
Device(config)# ip pim rp-address 172.16.0.2 10 bidir
```

ip pim rp-candidate

自身を Protocol Independent Multicast（PIM）バージョン 2（PIMv2）候補ランデブーポイント（C-RP）として BSR にアドバタイズするように デバイス を設定するには、グローバル コンフィギュレーション モードで **ip pim rp-candidate** コマンドを使用します。C-RP としての デバイス を削除するには、このコマンドの **no** 形式を使用します。

ip pim ［**vrf** *vrf-name*］ **rp-candidate** *interface-id* ［**group-list** *access-list-number*］
no ip pim ［**vrf** *vrf-name*］ **rp-candidate** *interface-id* ［**group-list** *access-list-number*］

構文の説明

vrf *vrf-name*	（任意） *vrf-name* 引数に指定されたマルチキャスト バーチャル プライベート ネットワーク（MVPN）ルーティングおよび転送（MVRF）インスタンスの PIMv2 C-RP として自身を BSR にアドバタイズするようにスイッチを設定します。
interface-id	対応する IP アドレスが候補 RP アドレスとしてアドバタイズされるインターフェイスの ID。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。
group-list *access-list-number*	（任意）RPアドレスに関連してアドバタイズされるグループプレフィックスを定義する標準 IP アクセス リスト番号を指定します。

コマンド デフォルト

デバイス は PIMv2 C-RP として自身を BSR に通知するように設定されていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

自身を候補 RP として BSR アドバタイズするために PIMv2 メッセージを送信するように デバイス を設定するには、このコマンドを使用します。

このコマンドは、PIM ドメイン内のすべての部分に良好に接続できるバックボーン デバイス で設定する必要があります。

interface-id によって指定されたインターフェイスに関連付けられている IP アドレスは C-RP アドレスとしてアドバタイズされます。

このコマンドに指定したインターフェイスは、**ip pim** コマンドを使用して、Protocol Independent Multicast（PIM）に対して有効にする必要があります。

オプションの **group-list** キーワードと *access-list-number* 引数が設定されている場合は、RP アドレスとのアソシエーション時に、標準 IP アクセスリストによって定義されたグループプレフィックスもアドバタイズされます。

例

次に、自身を C-RP として PIM ドメイン内の BSR にアドバタイズするようにスイッチを設定する例を示します。標準アクセス リスト番号 4 により、ギガビット イーサネット インターフェイス 1/0/1 で識別されるアドレスを持つ RP に対応するグループ プレフィックスが指定されます。

```
デバイス(config)# ip pim rp-candidate GigabitEthernet1/0/1 group-list 4
```

ip pim send-rp-announce

Auto-RP を使用して、デバイスがランデブーポイント（RP）として動作するグループを設定するには、グローバル コンフィギュレーション モードで **ip pim send-rp-announce** コマンドを使用します。デバイスの RP としての設定を解除するには、このコマンドの **no** 形式を使用します。

ip pim ［**vrf** *vrf-name*］ **send-rp-announce** *interface-id* **scope** *ttl-value* ［**group-list** *access-list-number*］［**interval** *seconds*］［**bidir**］
no ip pim ［**vrf** *vrf-name*］ **send-rp-announce** *interface-id*

構文の説明

vrf *vrf-name*	（任意）デバイスがランデブーポイント（RP）として動作するグループを設定するには、*vrf-name* 引数に Auto-RP を使用します。
interface-id	RP アドレスを識別するインターフェイスのインターフェイス ID を入力します。有効なインターフェイスは、物理ポート、ポート チャネル、VLAN などです。
scope *ttl-value*	Auto-RP アナウンスメントの数を制限するホップでの存続可能時間（TTL）を指定します。RP アナウンス メッセージがネットワーク内のすべてのマッピング エージェントに確実に到達するように、十分な大きさのホップ数を入力します。デフォルト設定はありません。範囲は 1 ～ 255 です。
group-list *access-list-number*	（任意）RP アドレスに関連してアドバタイズされるグループ プレフィックスを定義する標準 IP アクセス リスト番号を指定します。IP 標準アクセス リスト番号を入力します。指定できる範囲は 1 ～ 99 です。アクセス リストが設定されていない場合は、すべてのグループに RP が使用されます。
interval *seconds*	（任意）RP アナウンスメント間の間隔を秒単位で指定します。RP アナウンスメントの合計保留時間は、間隔値の 3 倍に自動設定されます。デフォルト インターバルは 60 秒です。範囲は 1 ～ 16383 です。
bidir	（任意）access-list 引数で指定したマルチキャスト グループが双方向モードで動作することを指定します。このキーワードを指定せずにコマンドを設定した場合、指定したグループは Protocol Independent Multicast スパース モード（PIM-SM）で動作します。

コマンド デフォルト

Auto-RP はディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが変更されました。**bidir** キーワードが追加されました。

使用上のガイドライン

RP にするデバイスで次のコマンドを入力します。Auto-RP を使用してグループ/RP マッピングを配信すると、ルータはこのコマンドにより既知のグループ CISCO-RP-ANNOUNCE（224.0.1.39）に Auto-RP アナウンスメント メッセージを送信します。このメッセージは、ルータがアクセス リストで規定される範囲内のグループに対する候補 RP であることを通知します。

このコマンドは、双方向転送を行う場合、および Auto-RP を使用してグループ/RP のマッピングを分散する場合に、**bidir** キーワードを指定して使用します。他のオプションは、次のとおりです。

- PIM バージョン 2 ブートストラップルータ（PIMv2 BSR）メカニズムによりグループ/RP のマッピングを分散する場合は、**ip pim rp-candidate** コマンドで **bidir** キーワードを使用します。
- Auto-RP または PIMv2 BSR メカニズムのどちらによってもグループ/RP のマッピングを分散しない場合は、**ip pim rp-address** コマンドで **bidir** キーワードを使用します。

例

次に、最大 31 ホップのすべての Protocol Independent Multicast（PIM）対応インターフェイスに RP アナウンスメントを送信するようにデバイスを設定する例を示します。スイッチを RP として識別するために使用される IP アドレスは、120 秒間隔でギガビット イーサネット インターフェイス 1/0/1 に関連付けられる IP アドレスです。

```
Device(config)# ip pim send-rp-announce GigabitEthernet1/0/1 scope 31 group-list 5
interval 120
```

ip pim snooping

（注） このコマンドは Cisco Catalyst 9500 シリーズ スイッチの C9500X-28C8D モデル に適用されます。

Protocol Independent Multicast（PIM）スヌーピングをグローバルに有効にするには、グローバル コンフィギュレーション モードで **ip pim snooping** コマンドを使用します。PIM スヌーピングをグローバルに無効にするには、このコマンドの **no** 形式を使用します。

ip pim snooping
no ip pim snooping

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

PIM スヌーピングは有効になっていません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

予約されている MAC アドレス範囲（たとえば 0100.5e00.00xx）をエイリアスとして使用するグループでは、PIM スヌーピングはサポートされません。

PIM スヌーピングをグローバルにディセーブルにすると、PIM スヌーピングはすべての VLAN 上でディセーブルになります。

例

次の例は、PIM スヌーピングをグローバルにイネーブルにする方法を示します。

```
ip pim snooping
```

次の例は、PIM スヌーピングをグローバルにディセーブルにする方法を示します。

```
no ip pim snooping
```

関連コマンド

コマンド	説明
clear ip pim snooping	インターフェイス上の PIM スヌーピングを削除します。
show ip pim snooping	IP PIM スヌーピングに関する情報を表示します。

ip pim snooping dr-flood

（注） このコマンドは Cisco Catalyst 9500 シリーズ スイッチの C9500X-28C8D モデル に適用されます。

指定ルータへのパケットのフラッディングを有効にするには、グローバル コンフィギュレーション モードで **ip pim snooping dr-flood** コマンドを使用します。指定ルータへのパケットのフラッディングを無効にするには、このコマンドの **no** 形式を使用します。

ip pim snooping dr-flood
no ip pim snooping dr-flood

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

指定ルータへのパケットのフラッディングは、デフォルトでは有効になっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

予約されている MAC アドレス範囲（たとえば 0100.5e00.00xx）をエイリアスとして使用するグループでは、PIM スヌーピングはサポートされません。

no ip pim snooping dr-flood コマンドは、指定ルータが接続されていないスイッチ上でのみ入力します。

指定ルータは、（S,G）O リストで自動的にプログラムされます。

例

次に、指定ルータへのパケットのフラッディングをイネーブルにする例を示します。

```
ip pim snooping dr-flood
```

次に、指定ルータへのパケットのフラッディングをディセーブルにする例を示します。

```
no ip pim snooping dr-flood
```

関連コマンド

コマンド	説明
clear ip pim snooping	インターフェイス上の PIM スヌーピングを削除します。
show ip pim snooping	IP PIM スヌーピングに関する情報を表示します。

ip pim snooping vlan

（注） このコマンドは Cisco Catalyst 9500 シリーズ スイッチの C9500X-28C8D モデル に適用されます。

インターフェイスで Protocol Independent Multicast（PIM）スヌーピングを有効にするには、グローバル コンフィギュレーション モードで **ip pim snoopingvlan** コマンドを使用します。PIM スヌーピングをインターフェイスで無効にするには、このコマンドの **no** 形式を使用します。

ip pim snooping vlan *vlan-id*
no ip pim snooping vlan *vlan-id*

構文の説明

vlan-id	VLAN ID 値。範囲は 1 ～ 1001 です。先頭の 0 は入力しないでください。

コマンド デフォルト

PIM スヌーピングはインターフェイスで無効になっています。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

予約されている MAC アドレス範囲（たとえば 0100.5e00.00xx）をエイリアスとして使用するグループでは、PIM スヌーピングはサポートされません。

このコマンドは、未設定の VLAN を自動的に設定します。設定は、NVRAM に保存されます。

例

次に、VLAN インターフェイス上で PIM スヌーピングをイネーブルにする例を示します。

```
Router(config)# ip pim snooping vlan 2
```

次に、VLAN インターフェイス上で PIM スヌーピングをディセーブルにする例を示します。

```
Router(config)# no ip pim snooping vlan 2
```

関連コマンド

コマンド	説明
clear ip pim snooping	インターフェイス上の PIM スヌーピングを削除します。
ip pim snooping	PIM 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	説明
show ip pim snooping	IP PIM スヌーピングに関する情報を表示します。

ip pim spt-threshold

最短パスツリー（spt）に移行する上限値となるしきい値を指定するには、グローバル コンフィギュレーション モードで **ip pim spt-threshold** コマンドを使用します。しきい値を削除するには、このコマンドの **no** 形式を使用します。

ip pim {*kbps* | **infinity**} [**group-list** *access-list*]
no ip pim {*kbps* | **infinity**} [**group-list** *access-list*]

構文の説明

kbps	最短パス ツリー（spt）に移行する上限値となるしきい値を指定します。有効な範囲は 0 ～ 4294967 ですが、0 が唯一有効なエントリです。0 エントリは、常に送信元ツリーに切り替わります。
infinity	指定されたグループのすべての送信元が共有ツリーを使用し、送信元ツリーに切り替わらないように指定します。
group-list *access-list*	（任意）アクセス リスト番号を指定するか、または作成した特定のアクセス リストを名前で指定します。値 0 を指定する場合、または **group-list** *access-list* オプションを使用しない場合、しきい値はすべてのグループに適用されます。

コマンド デフォルト

PIM 最短パス ツリー（spt）に切り替わります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

例

次に、アクセス リスト 16 のすべての送信元が共有ツリーを使用するように指定する例を示します。

```
デバイス(config)# ip pim spt-threshold infinity group-list 16
```

match message-type

サービス リストを照合するメッセージ タイプを設定するには、**match message-type** コマンドを使用します。

match message-type {**announcement** | **any** | **query**}

構文の説明

announcement	デバイス のサービス アドバタイズメントまたはアナウンスメントのみを許可します。
any	任意の照合タイプを許可します。
query	ネットワーク内の特定の デバイス に対するクライアントからクエリのみを許可します。

コマンド デフォルト

なし

コマンド モード

サービス リスト コンフィギュレーション。

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

異なるシーケンス番号を持つ同じ名前の複数のサービスマップを作成することができ、フィルタの評価順序はシーケンス番号に基づきます。サービス リストは、それぞれが許可または拒否の結果を持つ個々の文を一定の順序で並べたものです。サービス リストの評価は、事前に定義された順序でのリストのスキャンと、一致する各文の基準の評価で構成されています。リストのスキャンは、文の一致が初めて見つかり、その文に関連付けられたアクション permit または deny が実行されると停止します。リスト全体をスキャンした後のデフォルトのアクションは deny です。

（注） **service-list mdns-sd** *service-list-name* **query** コマンドを使用していた場合、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションに対してのみ使用できます。

例

次に、照合されるアナウンスメント メッセージ タイプを設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match message-type announcement
```

match service-type

照合する mDNS サービス タイプ文字列値を設定するには、**match service-type** コマンドを使用します。

match service-type *line*

構文の説明

line	パケット内のサービス タイプを照合するための正規表現。

コマンド デフォルト

なし

コマンド モード

サービス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

service-list mdns-sd *service-list-name* **query** コマンドを使用していた場合、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションに対してのみ使用できます。

例

次に、照合する mDNS サービス タイプ文字列値を設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match service-type _ipp._tcp
```

match service-instance

サービス リストを照合するサービス インスタンスを設定するには、**match service-instance** コマンドを使用します。

match service-instance *line*

構文の説明

line	パケット内のサービスインスタンスを照合するための正規表現。

コマンド デフォルト

なし

コマンド モード

サービス リスト コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

service-list mdns-sd *service-list-name* **query** コマンドを使用していた場合、**match** コマンドは使用できません。**match** コマンドは、**permit** または **deny** オプションに対してのみ使用できます。

例

次に、照合するサービス インスタンスを設定する例を示します。

```
デバイス(config-mdns-sd-sl)# match service-instance servInst 1
```

mrinfo

ピアとして動作している隣接するマルチキャストルータまたはマルチレイヤスイッチをクエリするには、ユーザ EXEC モードまたは特権 EXEC モードで **mrinfo** コマンドを使用します。

mrinfo ［**vrf** *route-name*］［*hostname* | *address*］［*interface-id*］

構文の説明

vrf *route-name*	（任意）VPN ルーティングおよび転送インスタンスを指定します。
hostname | *address*	（任意）クエリするマルチキャスト ルータまたはマルチレイヤ スイッチのドメイン ネーム システム（DNS）名または IP アドレス。省略すると、スイッチは自身をクエリします。
interface-id	（任意）インターフェイス ID。

コマンド デフォルト

このコマンドはディセーブルです。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

mrinfo コマンドは、マルチキャストルータまたはスイッチのピアとして動作している隣接するマルチキャストルータまたはスイッチを判別するためのマルチキャストバックボーン（MBONE）のオリジナルのツールです。シスコルータは、Cisco IOS リリース 10.2 から **mrinfo** 要求をサポートしています。

mrinfo コマンドを使用して、マルチキャストルータまたはマルチレイヤスイッチをクエリすることができます。出力フォーマットは、マルチキャスト ルーテッド バージョンのディスタンス ベクター マルチキャスト ルーティング プロトコル（DVMRP）と同じです（mrouted ソフトウェアは、DVMRP を実装する UNIX ソフトウェアです）。

例

次に、**mrinfo** コマンドの出力例を示します。

```
デバイス# mrinfo
 vrf 192.0.1.0
192.31.7.37 (barrnet-gw.cisco.com) [version cisco 11.1] [flags: PMSA]:
  192.31.7.37 -> 192.31.7.34 (sj-wall-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.47 (dirtylab-gw-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.44 (dirtylab-gw-1.cisco.com) [1/0/pim]
```

（注） フラグの意味は次のとおりです。

- P：プルーニング対応
- M：mtrace 対応
- S：シンプル ネットワーク管理プロトコルに対応
- A：Auto RP に対応

service-policy-query

サービスリストクエリの周期を設定するには、**service-policy-query** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

service-policy-query ［*service-list-query-name service-list-query-periodicity*］
no service-policy-query

構文の説明

service-list-query-name service-list-query-periodicity	（任意）サービスリストクエリの周期。

コマンド デフォルト

ディセーブル

コマンド モード

mDNS コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

非要請アナウンスメントを送信しないデバイスがあるため、そのようなデバイスにサービスを強制的に学習させ、それらをキャッシュ内で最新に維持するために、このコマンドには、アクティブ クエリ リストに一覧されているサービスが確実にクエリされるようにするアクティブ クエリ機能が含まれています。

例

次に、サービス リストのクエリの周期を設定する例を示します。

```
デバイス(config-mdns)# service-policy-query sl-query1 100
```

service-policy

サービスリストの着信または発信サービス検出情報にフィルタを適用するには、**service-policy** コマンドを使用します。フィルタを削除するには、このコマンドの **no** 形式を使用します。

service-policy *service-policy-name* {**IN** | **OUT**}
no service-policy *service-policy-name* {**IN** | **OUT**}

構文の説明

IN	着信サービス検出情報にフィルタを適用します。
OUT	発信サービス検出情報にフィルタを適用します。

コマンド デフォルト

ディセーブル

コマンド モード

mDNS コンフィギュレーション

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

例

次の例に、サービス リストの着信サービス検出情報にフィルタを適用する方法を示します。

```
デバイス(config-mdns)#  service-policy serv-pol1 IN
```

show ip igmp filter

Internet Group Management Protocol（IGMP）フィルタ情報を表示するには、特権 EXEC モードで **show ip igmp filter** コマンドを使用します。

show ip igmp ［**vrf** *vrf-name*］ **filter**

構文の説明

vrf *vrf-name*	（任意）マルチキャスト VPN ルーティングおよび転送（VRF）インスタンスをサポートします。

コマンド デフォルト

IGMP フィルタはデフォルトで有効になっています。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

show ip igmp filter コマンドは、deviceに定義されているすべてのフィルタに関する情報を表示します。

例

次に、**show ip igmp filter** コマンドの出力例を示します。

```
デバイス# show ip igmp filter

IGMP filter enabled
```

show ip igmp profile

設定済みのすべての Internet Group Management Protocol（IGMP）プロファイルまたは指定された IGMP プロファイルを表示するには、特権 EXEC モードで **show ip igmp profile** コマンドを使用します。

show ip igmp ［**vrf** *vrf-name*］ **profile** ［*profile number*］

構文の説明

vrf *vrf-name*	（任意）マルチキャスト VPN ルーティングおよび転送（VRF）インスタンスをサポートします。
profile number	（任意）表示する IGMP プロファイル番号。指定できる範囲は 1 ～ 4294967295 です。プロファイル番号が入力されていない場合、すべての IGMP プロファイルが表示されます。

コマンド デフォルト

IGMP プロファイルはデフォルトでは定義されていません。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、device のプロファイル番号 40 に対する **show ip igmp profile** コマンドの出力例を示します。

```
デバイス# show ip igmp profile 40
IGMP Profile 40
    permit
    range 233.1.1.1 233.255.255.255
```

次に、device に設定されているすべてのプロファイルに対する **show ip igmp profile** コマンドの出力例を示します。

```
デバイス# 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
```

show ip igmp snooping

deviceまたは VLAN の Internet Group Management Protocol（IGMP）スヌーピング構成を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip igmp snooping** コマンドを使用します。

show ip igmp snooping ［**groups** | **mrouter** | **querier**］ ［**vlan** *vlan-id*］［**detail**］

構文の説明

groups	（任意）IGMP スヌーピング マルチキャスト テーブルを表示します。
mrouter	（任意）IGMP スヌーピング マルチキャスト ルータ ポートを表示します。
querier	（任意）IGMP クエリアの設定情報と動作情報を表示します。
vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。
detail	（任意）動作状態の情報を表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

VLAN ID 1002 ～ 1005 は、トークンリングおよびFDDI VLANに予約されていて、IGMP スヌーピングでは使用できません。

文字列では、大文字と小文字が区別されます。たとえば、「|**exclude output**」と入力した場合、「output」を含む行は表示されませんが、「Output」を含む行は表示されます。

例

次に、**show ip igmp snooping vlan 1** コマンドの出力例を示します。ここでは、特定の VLAN のスヌーピング特性を表示します。

```
デバイス# show ip igmp snooping vlan 1

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
```

```
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
```

次に、**show ip igmp snooping** コマンドの出力例を示します。ここでは、device 上のすべての VLAN のスヌーピング特性を表示します。

```
デバイス# show ip igmp snooping

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
Vlan 2:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
-
.
.
.
```

show ip igmp snooping groups

device またはマルチキャスト情報の Internet Group Management Protocol（IGMP）スヌーピング マルチキャスト テーブルを表示するには、特権 EXEC モードで **show ip igmp snooping groups** コマンドを使用します。

show ip igmp snooping groups ［**vlan** *vlan-id* ］［［**count**］ | *ip_address*］

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。指定できる範囲は 1 ～ 1001 および 1006 ～ 4094 です。指定されたマルチキャスト VLAN のマルチキャスト テーブル、または特定のマルチキャスト情報を表示するには、このオプションを使用します。
count	（任意）実エントリの代わりに、指定のコマンド オプションのエントリ総数を表示します。
ip_address	（任意）指定グループ IP アドレスのマルチキャスト グループの特性を表示します。

コマンド モード

特権 EXEC

ユーザ EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

文字列では、大文字と小文字が区別されます。たとえば、「|**exclude output**」と入力した場合、「output」を含む行は表示されませんが、「Output」を含む行は表示されます。

例

次に、キーワードを指定しない **show ip igmp snooping groups** コマンドの出力例を示します。device のマルチキャスト テーブルが表示されます。

```
デバイス# show ip igmp snooping groups

Vlan      Group           Type        Version     Port List
------------------------------------------------------------
1         224.1.4.4       igmp                    Gi1/0/11
1         224.1.4.5       igmp                    Gi1/0/11
2         224.0.1.40      igmp        v2          Gi1/0/15
104       224.1.4.2       igmp        v2          Gi2/0/1, Gi2/0/2
104       224.1.4.3       igmp        v2          Gi2/0/1, Gi2/0/2
```

次に、**show ip igmp snooping groups count** コマンドの出力例を示します。device 上のマルチキャスト グループの総数が表示されます。

```
デバイス# show ip igmp snooping groups count

Total number of multicast groups: 2
```

次に、**show ip igmp snooping groups vlan vlan-id ip-address** コマンドの出力例を示します。指定された IP アドレスのグループのエントリを表示します。

```
デバイス# show ip igmp snooping groups vlan 104 224.1.4.2

Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi2/0/1, Gi1/0/15
```

show ip igmp snooping mrouter

deviceまたは指定されたマルチキャスト VLAN の Internet Group Management Protocol（IGMP）スヌーピングの動的に学習され、手動で設定されたマルチキャストルータポートを表示するには、特権 EXEC モードで **show ip igmp snooping mrouter** コマンドを使用します。

show ip igmp snooping mrouter ［**vlan** *vlan-id*］

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。範囲は 1 ～ 1001 と 1006 ～ 4094 です。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

VLAN ID 1002 ～ 1005 は、トークンリングおよびFDDI VLAN に予約されていて、IGMP スヌーピングでは使用できません。

マルチキャストVLAN レジストレーション（MVR）がイネーブルの場合、**show ip igmp snooping mrouter** コマンドは MVR マルチキャストルータの情報および IGMP スヌーピング情報を表示します。

式では大文字と小文字が区別されます。たとえば、「|exclude output」と入力した場合、output を含む行は表示されませんが、Output を含む行は表示されます。

例

次に、**show ip igmp snooping mrouter** コマンドの出力例を示します。deviceのマルチキャスト ルータ ポートを表示する方法を示します。

```
デバイス# show ip igmp snooping mrouter

Vlan    ports
----    -----
   1    Gi2/0/1(dynamic)
```

show ip igmp snooping querier

device で設定されている IGMP クエリアの設定と操作情報を表示するには、ユーザ EXEC モードで **show ip igmp snooping querier** コマンドを使用します。

show ip igmp snooping querier ［**vlan** *vlan-id*］ ［**detail** ］

構文の説明

vlan *vlan-id*	（任意）VLAN を指定します。範囲は 1 ～ 1001 と 1006 ～ 4094 です。
detail	（任意）IGMP クエリアの詳細情報を表示します。

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

IGMP クエリ メッセージを送信する検出デバイス（クエリアとも呼ばれます）の IGMP バージョンと IP アドレスを表示するには、**show ip igmp snooping querier** コマンドを使用します。サブネットは複数のマルチキャストルータを保有できますが、IGMP クエリアは 1 つしか保有できません。IGMPv2 を実行しているサブネットでは、マルチキャスト ルータの 1 つがクエリアとして設定されます。クエリアには、レイヤ 3 device を指定できます。

show ip igmp snooping querier コマンド出力では、クエリアが検出された VLAN およびインターフェイスも表示されます。クエリアが device の場合、出力の Port フィールドには「Router」と表示されます。クエリアがルータの場合、出力の Port フィールドにはクエリアを学習したポート番号が表示されます。

show ip igmp snooping querier detail ユーザ EXEC コマンドは、**show ip igmp snooping querier** コマンドに似ています。ただし、**show ip igmp snooping querier** コマンドでは、device クエリアによって最後に検出されたデバイスの IP アドレスのみが表示されます。

show ip igmp snooping querier detail コマンドでは、device クエリアによって最後に検出されたデバイスの IP アドレスのほか、次の追加情報が表示されます。

- VLAN で選択されている IGMP クエリア
- VLAN で設定された device クエリア（存在する場合）に関連する設定情報と動作情報

式では大文字と小文字が区別されます。たとえば、「|**exclude output**」と入力した場合、output を含む行は表示されませんが、Output を含む行は表示されます。

例

次に、**show ip igmp snooping querier** コマンドの出力例を示します。

```
デバイス> show ip igmp snooping querier
Vlan      IP Address     IGMP Version        Port
---------------------------------------------------
1         172.20.50.11   v3                  Gi1/0/1
2         172.20.40.20   v2                  Router
```

次に、**show ip igmp snooping querier detail** コマンドの出力例を示します。

```
デバイス> show ip igmp snooping querier detail

Vlan      IP Address     IGMP Version   Port
-------------------------------------------------------------
1         1.1.1.1        v2             Fa8/0/1
Global IGMP device querier status

-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 0.0.0.0
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
Vlan 1:   IGMP device querier status
-----------------------------------------------------------
elected querier is 1.1.1.1         on port Fa8/0/1
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 10.1.1.65
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
operational state              : Non-Querier
operational version            : 2
tcn query pending count        : 0
```

show ip mroute

マルチキャストルーティング（mroute）テーブルの内容を表示するには、ユーザー EXEC モードまたは特権 EXEC モードで **show ip mroute** コマンドを使用します。

show ip mroute [**vrf** { *vrf-name* | ***** }] [{ [{ **active** [*kbps*] [**interface** *type number*] | **bidirectional** | **count** [**terse**] | **dense** | **interface** *type number* | **proxy** | **pruned** | **sparse** | **ssm** | **static** | **summary** }] | [*group-address* [*source-address*]] [{ **count** [**terse**] | **interface** *type number* | **proxy** | **pruned** | **summary** }] | [*source-address group-address*] [{ **count** [**terse**] | **interface** *type number* | **proxy** | **pruned** | **summary** }] | [*group-address*] **active** [*kbps*] [{ **interface** *type number* | **verbose** }] }]

構文の説明

vrf *vrf-name*	（任意）出力をフィルタ処理して、*vrf-name* 引数で指定された、マルチキャスト バーチャル プライベート ネットワーク（MVPN）ルーティングおよび転送（MVRF）インスタンスに関係する mroute テーブルの内容だけを表示します。
vrf *	（任意）すべての VRF インスタンスを指定します。
active *kbps*	（任意）アクティブ ソースがマルチキャスト グループに送信されている速度（単位：キロビット/秒（kbps））を表示します。アクティブな送信元は、この *kbps* 値またはそれ以上で送信しています。範囲は 1 ～ 4294967295 です。*kbps* 値のデフォルトは 4 kbps です。
interface *type number*	（任意）出力をフィルタ処理して、*type number* 引数で指定されたインターフェイスに関係する mroute テーブル情報だけを表示します。
bidirectional	（任意）出力をフィルタして、mroute テーブルの双方向ルートに関する情報だけを表示します。
count	（任意）パケット数、パケット/秒、平均パケットサイズ、および、バイト/秒などのグループとソースの統計情報を表示します。
terse	（任意）出力をフィルタして、mroute テーブルの各 mroute エンティティに対する、ソースとグループの統計情報を除いた、mroute 統計情報のサブセットを表示します。
dense	（任意）出力をフィルタして、mroute テーブルの dense（デンス）モード ルートに関する情報だけを表示します。
proxy	（任意）マルチキャストデバイスで受信されたリバース パス フォワーディング（RPF）ベクトルプロキシに関する情報を表示します。
pruned	（任意）出力をフィルタして、mroute テーブルのプルーン ルートに関する情報だけを表示します。

sparse	（任意）出力をフィルタして、mroute テーブルのスパース モード ルートに関する情報だけを表示します。
ssm	（任意）出力をフィルタして、mroute テーブルの Source Specific Multicast（SSM）ルートに関する情報だけを表示します。
static	（任意）出力をフィルタして、mroute テーブルのスタティック ルートに関する情報だけを表示します。
summary	（任意）出力をフィルタして、mroute テーブルの各エントリに対し、1 行の簡略サマリーを表示します。
group-address	（任意）マルチキャスト グループの IP アドレス、またはドメイン ネーム システム（DNS）名
source-address	（任意）マルチキャスト ソースの IP アドレスまたは DNS 名
verbose	（任意）追加情報を表示します。

コマンド デフォルト

show ip mroute コマンドは、mroute テーブル内のすべてのエントリを表示します。

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。
Cisco IOS XE Cupertino 17.7.1	すべての VRF インスタンスに関連する情報を表示するために、アスタリスク（*）が導入されました。

使用上のガイドライン

mroute テーブルの mroute エントリに関する情報を表示するには、**show ip mroute** コマンドを使用します。アスタリスク（*）はすべての送信元アドレスを指します。この場合、アスタリスクを使用すると、マルチキャスト ルーティング テーブルに関連するすべての VRF の情報が表示されます。

例

次に、**show ip mroute** コマンドの出力例を示します。

```
Device# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode
(*, 224.0.255.3), uptime 5:29:15, RP is 192.168.37.2, flags: SC
```

```
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57
(192.168.46.0/24, 224.0.255.3), uptime 5:29:15, expires 0:02:59, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57
```

次に、IP マルチキャスト グループ アドレスに 232.6.6.6 を指定した場合の **show ip mroute** コマンドの出力例を示します。

```
Device# show ip mroute 232.6.6.6
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 232.6.6.6), 00:01:20/00:02:59, RP 224.0.0.0, flags:sSJP
  Incoming interface:Null, RPF nbr 224.0.0.0
  Outgoing interface list:Null

(10.2.2.2, 232.6.6.6), 00:01:20/00:02:59, flags:CTI
  Incoming interface:Ethernet3/3, RPF nbr 224.0.0.0
  Outgoing interface list:
    Ethernet3/1, Forward/Sparse-Dense, 00:00:36/00:02:35
```

次に、**show ip mroute vrf *** コマンドの出力例を示します。

```
Device# show ip mroute vrf *
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group, c - PFP-SA cache created entry,
       * - determined by Assert, # - iif-starg configured on rpf intf,
       e - encap-helper tunnel flag, l - LISP Decap Refcnt Contributor
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
                          t - LISP transit group
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

VRF IPv4 default
(100.99.99.99, 232.101.100.138), 1w1d/00:02:58, flags: sT
  Incoming interface: Null0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0/1, Forward/Sparse, 1w1d/00:02:58, flags:

(100.99.99.99, 232.101.100.157), 1w1d/00:03:27, flags: sT
  Incoming interface: Null0, RPF nbr 0.0.0.0
  Outgoing interface list:
```

```
    Ethernet0/1, Forward/Sparse, 1w1d/00:03:27, flags:

(100.88.88.88, 232.134.100.138), 1w1d/00:01:54, flags: sT
  Incoming interface: Ethernet0/0, RPF nbr 40.10.2.1
  Outgoing interface list:
    Null0, Forward/Dense, 1w1d/stopped, flags:
(100.88.88.88, 232.134.100.157), 1w1d/00:01:54, flags: sT
  Incoming interface: Ethernet0/0, RPF nbr 40.10.2.1
  Outgoing interface list:
    Null0, Forward/Dense, 1w1d/stopped, flags:

(*, 224.0.1.40), 1w1d/00:02:53, RP 0.0.0.0, flags: DP
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list: Null

VRF red
(*, 225.64.64.1), 1w1d/00:03:23, RP 5.5.5.5, flags: Sl
  Incoming interface: LISP0.101, RPF nbr 100.88.88.88
  Outgoing interface list:
    LISP0.101, (100.99.99.99, 232.101.100.157), Forward/Sparse, 1w1d/stopped, flags:

(*, 225.32.32.32), 1w1d/00:03:05, RP 5.5.5.5, flags: Sl
  Incoming interface: LISP0.101, RPF nbr 100.88.88.88
  Outgoing interface list:
    LISP0.101, (100.99.99.99, 232.101.100.138), Forward/Sparse, 1w1d/stopped, flags:
```

表 *1 : show ip mroute* のフィールドの説明

フィールド	説明
Flags:	エントリに関する情報を提供します。 • D：デンス。エントリはデンス モードで動作しています。 • S：スパース。エントリはスパース モードで動作しています。 • B：双方向グループ。マルチキャスト グループが双方向モードで動作していることを示します。 • s：SSM グループ。マルチキャスト グループが SSM の IP アドレス範囲内であることを示します。このフラグは、SSM の範囲が変更されるとリセットされます。 • C：接続済み。マルチキャストグループのメンバは、直接接続されたインターフェイス上に存在します。

フィールド	説明
Flags：（続き）	

フィールド	説明
	• L：ローカル。デバイス自体が、マルチキャストグループのメンバです。グループは、**ip igmp join-group** コマンド（設定済みグループの場合）、**ip sap listen** コマンド（ウェルノウンセッションディレクトリグループの場合）、およびランデブーポイント（RP）マッピング（ウェルノウングループ 224.0.1.39 および 224.0.1.40 の場合）によってローカルに参加します。ローカルで参加したグループは、ファストスイッチングではありません。 • P：プルーニング済み。ルートがプルーニングされています。Cisco IOS ソフトウェアは、この情報を保持して、ダウンストリームメンバが送信元に加入できるようにします。 • R：RP ビットを設定。(S,G) エントリが RP をポイントしていることを示します。通常、このフラグは特定の送信元に関する共有ツリーに沿ったプルーニング状態を示します。 • F：登録フラグ。ソフトウェアがマルチキャスト送信元に登録されていることを示します。 • T：SPT ビットを設定。パケットが最短パス送信元ツリーで受信されていることを示します。 • J：SPT に参加。(*, G) エントリの場合、共有ツリーの下方向に流れるトラフィックの速度が、グループの SPT しきい値設定を超えていることを示します（デフォルトの SPT しきい値設定は 0 kbps です）。J - Join 最短パスツリー（SPT）フラグが設定されている場合に、共有ツリーの下流で次の (S,G) パケットが受信されると、送信元の方向に (S,G) join がトリガーされます。これにより、デバイスは送信元ツリーに加入します。 (S, G) エントリの場合、グループの SPT しきい値を超過したためにエントリが作成されたことを示します。(S,G) エントリに J - Join SPT フラグが設定されている場合、デバイスは送信元ツリー上のトラフィック速度をモニターします。送信元ツリーのトラフィック速度がグループの SPT しきい値を下回っている状況が 1 分以上継続した場合、デバイスはこの送信元の共有ツリーに再び切り替えようとします。 （注） デバイスは共有ツリー上のトラフィック速度を測定し、この速度とグループの SPT しきい値を 1 秒ごとに比較します。トラフィック速度が SPT しきい値を超えた場合は、トラフィック速度の次の測定が行われるまで、(*, G) エントリに J - Join SPT フラグが設定されます。共有ツリーに次のパケットが着信し、新しい測定間隔が開始されると、フラグが解除されます。グループにデフォルトの SPT しきい値（0 Kbps）が使用されている場合、(*, G) エントリには常に J - Join SPT フラグが設定され、解除されません。デフォルトの

フィールド	説明
	SPT しきい値が使用されている場合に、新しい送信元からトラフィックを受信すると、デバイスは最短パス送信元ツリーにただちに切り替えます。

フィールド	説明
	• M：MSDP が作成したエントリ。(*, G) エントリが Multicast Source Discovery Protocol（MSDP）ピアを介して学習されたことを示します。このフラグは、MSDP を実行している RP にのみ適用されます。 • E：エクストラネット送信元 mroute エントリ。VRF ルーティング テーブル内の (*, G) または (S, G) エントリが送信元マルチキャスト VRF（MVRF）エントリであり、エクストラネット受信先 MVRF エントリがリンクされていることを示します。 • X：プロキシ参加タイマーが実行中。プロキシ参加タイマーが実行中であることを示します。このフラグは、RP または「turnaround」デバイスの (S, G) エントリに対してのみ設定されます。「turnaround」デバイスは、共有パス (*, G) ツリーと送信元から RP への最短パスが交差する場所に配置されます。 • A：MSDP アドバタイズメントの候補。(S, G) エントリが MSDP ピアを介してアドバタイズされたことを示します。このフラグは、MSDP を実行している RP にのみ適用されます。 • U：URD。(S, G) エントリに関して URL Rendezvous Directory（URD）チャネル サブスクリプション レポートが受信されたことを示します。 • I：送信元固有のホストレポートを受信。(S,G) エントリが (S,G) レポートによって作成されたことを示します。この (S, G) レポートは、Internet Group Management Protocol Version 3（IGMPv3）、URD、または IGMP v3lite によって作成された可能性があります。このフラグは、代表デバイス（DR）上にのみ設定されます。 • Z：マルチキャストトンネル。このエントリがマルチキャスト配信ツリー（MDT）トンネルに属する IP マルチキャストグループであることを示します。この IP マルチキャスト状態で受信されたすべてのパケットは、カプセル化解除のために MDT トンネルに送信されます。 • Y：結合された MDT データグループ。この送信元およびグループ専用に設定された MDT トンネルを介してトラフィックが受信されたことを示します。このフラグは、仮想プライベートネットワーク（VPN）mroute テーブルでのみ設定されます。 • y：MDT データグループに送信中。この送信元およびグループ専用に設定された MDT トンネルを介してトラフィックが送信されたことを示します。このフラグは、VPN mroute テーブルでのみ設定されます。

フィールド	説明
Outgoing interface flags:	エントリに関する情報を提供します。 • H：スイッチされたハードウェア。このエントリに対してマルチキャスト マルチレイヤ スイッチング（MMLS）転送パスが確立されていることを示します。
Timers:Uptime/Expires	「Uptime」は、エントリが IP マルチキャスト ルーティング テーブルに格納されていた期間（時間、分、秒）をインターフェイスごとに示します。「Expires」は、IP マルチキャスト ルーティング テーブルからエントリが削除されるまでの期間（時間、分、秒）をインターフェイスごとに示します。
Interface state:	着信インターフェイスまたは発信インターフェイスの状態を示します。 • [Interface]。タイプと、着信インターフェイスまたは発信インターフェイスのリストに記載されているインターフェイスの数を示します。 • Next-Hop or VCD。「Next-Hop」は、ダウンストリームネイバーの IP アドレスを指定します。「VCD」は、仮想回線記述子番号を指定します。「VCD0」は、グループがスタティックマップ仮想回線を使用していることを意味します。 • State/Mode。「State」は、アクセスリストまたは存続可能時間（TTL）しきい値による制限があるかどうかに応じて、インターフェイス上で転送、プルーニング、ヌル値化のいずれの処理がパケットに対して実行されることを示します。「Mode」は、インターフェイスがデンスモード、スパースモード、またはスパース-デンスモードのいずれで動作しているかを示します。
(*, 224.0.255.1) and (192.168.37.100, 224.0.255.1)	IP マルチキャスト ルーティング テーブルのエントリです。エントリは、送信元の IP アドレスと、それに続くマルチキャスト グループの IP アドレスで構成されます。送信元の位置に置かれたアスタリスク（*）は、すべての送信元デバイスを意味します。 最初の形式のエントリは、(*,G) または「スター カンマ G」エントリと呼ばれます。2 番目の形式のエントリは、(S,G) または「S カンマ G」エントリと呼ばれます。(*,G) エントリは、(S,G) エントリを作成するために使用されます。
RP	RP デバイスのアドレス。スパースモードで動作するデバイスおよびアクセスサーバーの場合、このアドレスは常に 224.0.0.0 です。
flags:	エントリに関する情報です。
Incoming interface:	送信元からのマルチキャスト パケット用のインターフェイスです。パケットがこのインターフェイスに着信しなかった場合、破棄されます。

フィールド	説明
RPF neighbor or RPF nbr	送信元に対するアップストリームデバイスの IP アドレス。Tunneling は、このデバイスが RP へのデータを Register パケットにカプセル化して送信していることを示します。カッコ内の 16 進数は、登録先の RP を示します。1 つのグループに複数の RP が使用されている場合、各ビットは異なる RP を示します。このフィールドの IP アドレスの後にアスタリスク（*）が表示されている場合、RPF ネイバーはアサートによって学習されています。
Outgoing interface list:	パケットが転送される際に通過したインターフェイス。 **ip pim nbma-mode** コマンドがインターフェイスで有効になっている場合、Protocol Independent Multicast（PIM）ネイバーの IP アドレスも表示されます。 インターフェイスが RSVP マルチキャスト CAC によってブロック（拒否）されている場合、Blocked キーワードが出力に表示されます。

show ip pim autorp

Auto-RP に関するグローバル情報を表示するには、特権 EXEC モードで **show ip pim autorp** コマンドを使用します。

show ip pim ［ **vrf** { *vrf-name* | ***** } ］ **autorp**

vrf *vrf-name*	（任意）マルチキャスト VPN ルーティングおよび転送（VRF）インスタンスを指定します。
vrf *	（任意）すべての VRF インスタンスを指定します。

コマンド デフォルト

Auto RP は、デフォルトでは有効になっています。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。
Cisco IOS XE Cupertino 17.7.1	すべての VRF インスタンスに関連する情報を表示するために、アスタリスク（*）が導入されました。

使用上のガイドライン

このコマンドは、Auto-RP が有効になっているか、無効になっているかを表示します。アスタリスク（*）はすべての VRF を指します。この場合、アスタリスクを使用すると、該当するすべての VRF の autorp 情報が表示されます。

例

次に、Auto-RP が有効になっている場合のコマンドの出力例を示します。

```
デバイス# show ip pim autorp

AutoRP Information:
  AutoRP is enabled.
  RP Discovery packet MTU is 0.
  224.0.1.40 is joined on GigabitEthernet1/0/1.

PIM AutoRP Statistics: Sent/Received
  RP Announce: 0/0, RP Discovery: 0/0
```

次に、**show ip pim vrf * autorp** コマンドの出力例を示します。

```
Device#show ip pim vrf * autorp
VRF IPv4 default

AutoRP Information:
  AutoRP is enabled.
  RP Discovery packet MTU is 0.
```

```
  224.0.1.40 is joined on Loopback0.
  AutoRP groups over sparse mode interface is enabled

PIM AutoRP Statistics: Sent/Received
  RP Announce: 453427/0, RP Discovery: 0/152194

VRF ENG

AutoRP Information:
  AutoRP is enabled.
  RP Discovery packet MTU is 1500.
  224.0.1.40 is joined on GigabitEthernet4.
  AutoRP groups over sparse mode interface is enabled

PIM AutoRP Statistics: Sent/Received
  RP Announce: 0/151143, RP Discovery: 151923/0
```

show ip pim bsr-router

Protocol Independent Multicast（PIM）ブートストラップルータ（BSR）プロトコル処理に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip pim bsr-router** コマンドを使用します。

show ip pim ［ **vrf** { *vrf-name* | ***** } ］ **bsr-router**

vrf *vrf-name*	（任意）マルチキャスト VPN ルーティングおよび転送（VRF）インスタンスを指定します。
vrf *	（任意）すべての VRF インスタンスを指定します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。
Cisco IOS XE Cupertino 17.7.1	すべての VRF インスタンスに関連する情報を表示するために、アスタリスク（*）が導入されました。

使用上のガイドライン

Auto-RP に加えて、BSR RP メソッドを設定できます。BSR RP メソッドを設定すると、このコマンドでBSRルータの情報が表示されます。アスタリスク（*）はすべてのVRFを指します。この場合、アスタリスクを使用すると、該当するすべての VRF の BSR ルータ情報が表示されます。

次に、 **show ip pim bsr-router** コマンドの出力例を示します。

```
デバイス# show ip pim bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim bsr

Protocol Independent Multicast（PIM）ブートストラップルータ（BSR）プロトコル処理に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip pim bsr** コマンドを使用します。

show ip pim ［ **vrf** { *vrf-name* | ***** } ］ **bsr**

vrf *vrf-name*	（任意）マルチキャスト VPN ルーティングおよび転送（VRF）インスタンスを指定します。
vrf *	（任意）すべての VRF インスタンスを指定します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。
Cisco IOS XE Cupertino 17.7.1	すべての VRF インスタンスに関連する情報を表示するために、アスタリスク（*）が導入されました。

使用上のガイドライン

Auto-RP に加えて、BSR RP メソッドを設定できます。BSR RP メソッドを設定すると、このコマンドでBSRルータの情報が表示されます。アスタリスク（*）はすべてのVRFを指します。この場合、アスタリスクを使用すると、該当するすべての VRF の BSR プロトコル情報が表示されます。

次に、 **show ip pim bsr** コマンドの出力例を示します。

```
デバイス# show ip pim bsr

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim interface df

双方向 Protocol Independent Multicast（PIM）用に設定されたインターフェイス上の各ランデブーポイント（RP）の選択された指定フォワーダ（DF）に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip pim interface df** コマンドを使用します。

show ip pim ［ **vrf** { *vrf-name* | ***** } ］ **interface** ［ *interface-type* | *interface-name* ］ **df** ［ *rp-address* ］

vrf *vrf-name*	（任意）マルチキャスト VPN ルーティングおよび転送（VRF）インスタンスを指定します。
vrf *	（任意）すべての VRF インスタンスを指定します。
interface［*interface-type*| *interface-name*］	インターフェイスタイプまたはインターフェイス番号を指定します。
rp-address	（任意）RP の IP アドレスを指定します。

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。
Cisco IOS XE Cupertino 17.7.1	すべての VRF インスタンスに関連する情報を表示するために、アスタリスク（*）が導入されました。

コマンド デフォルト

インターフェイスが指定されていない場合、すべてのインターフェイスが表示されます。アスタリスク（*）はすべての VRF を指します。この場合、アスタリスクを使用すると、該当するすべての VRF について、インターフェイス上の各ランデブーポイントの指定フォワーダの情報が表示されます。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

次に、**show ip pim interface df** コマンドの出力例を示します。

```
Device# show ip pim interface df
Interface          RP               DF Winner        Metric          Uptime
Ethernet3/3        10.10.0.2        10.4.0.2         0               00:03:49
                   10.10.0.3        10.4.0.3         0               00:01:49
                   10.10.0.5        10.4.0.4         409600          00:01:49
Ethernet3/4        10.10.0.2        10.5.0.2         0               00:03:49
                   10.10.0.3        10.5.0.2         409600          00:02:32
                   10.10.0.5        10.5.0.2         435200          00:02:16
Loopback0          10.10.0.2        10.10.0.2        0               00:03:49
                   10.10.0.3        10.10.0.2        409600          00:02:32
```

```
                10.10.0.5       10.10.0.2       435200          00:02:16
```

次に、インターフェイスを指定した場合の **show ip pim interface df** コマンドの出力例を示します。

```
Device# show ip pim interface Ethernet3/3 df 10.10.0.3
Designated Forwarder election for Ethernet3/3, 10.4.0.2, RP 10.10.0.3
  State                          Non-DF
  Offer count is                 0
  Current DF ip address          10.4.0.3
  DF winner up time              00:02:33
  Last winner metric preference  0
  Last winner metric             0
```

次の表に、**show ip pim interface df** コマンドの出力フィールドの説明を示します。

フィールド	説明
RP	RP の IP アドレス。
DF Winner	選択された DF の IP アドレス。
Metric	DF によってアナウンスされた RP に対するユニキャスト ルーティング メトリック。
Uptime	RP の稼働時間（日数と時間数）。時間が 1 日未満の場合は、時:分:秒で表示されます。
State	指定したインターフェイスが DF として選択されているかどうかを示します。
Offer count is	現在の選択間隔の間にルータがインターフェイスから送信した PIM DF 選択オファーメッセージの数。
Current DF IP address	現在の DF の IP アドレス。
DF winner uptime	現在の DF の稼働時間（日数と時間数）。時間が 1 日未満の場合は、時:分:秒で表示されます。
Last winner metric preference	DF によってアナウンされた RP に対するユニキャストルーティング メットリックを選択するために使用されたプリファレンス値。
Last winner metric	DF によってアナウンスされた RP に対するユニキャスト ルーティング メトリック。

show ip pim rp

関連付けられたマルチキャスト ルーティング エントリでキャッシュされたアクティブなランデブーポイント（RP）を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip pim rp** コマンドを使用します。

show ip pim ［ **vrf** { *vrf-name* | ***** } ］ **rp** ［ **mapping** [**elected** | **in-use**] | **metric** ］［ *rp-address* ］

構文の説明

vrf *vrf-name*	（任意）マルチキャスト VPN ルーティングおよび転送（VRF）インスタンスを指定します。
vrf *	（任意）すべての VRF インスタンスを指定します。
mapping [**elected** | **in-use**]	（任意）ルータによって認識されているすべてのグループ/RP マッピングを表示します（設定されたか Auto-RP から学習されたもの）。 • **elected**：Auto-RP で選択された RP を表示します。 • **in-use**：学習された使用中の RP を表示します。
metric	（任意）静的に設定されたか Auto-RP またはブートストラップルータ（BSR）を通じて学習された RP に対するユニキャスト ルーティング メトリックを表示します。
rp-address	（任意）RP の IP アドレスを指定します。

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。
Cisco IOS XE Cupertino 17.7.1	すべての VRF インスタンスに関連する情報を表示するために、アスタリスク（*）が導入されました。

コマンド デフォルト

RP が指定されていない場合は、すべてのアクティブな RP が表示されます。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

使用上のガイドライン

RP で認識される Protocol Independent Multicast（PIM）バージョンは、アクティブな送信元の代表ルータ（DR）として動作するときにルータが送信する PIM 登録メッセージのタイプ（バージョン 1 またはバージョン 2）に影響します。RP が静的に設定されている場合、RP の PIM バージョンは設定されず、ルータから登録パケットを送信する必要があるときは PIM バージョン 2 の登録パケットの送信が試行されます。PIM バージョン 2 のパケットの送信に失敗すると、ルータは PIM バージョン 1 の登録パケットを送信します。

show ip pim rp コマンドの出力に表示される RP のバージョンは、 ルータの動作に応じて変わることがあります。グループが作成されている場合、表示されるバージョンは RP マッピング キャッシュ内の RP のバージョンになります。この場合、このコマンドで表示されるバージョンが後で変わることがあります。このルータがアクティブな送信元の DR として動作している場合、ルータは PIM 登録メッセージを送信します。この PIM 登録メッセージに対し、RP は PIM 登録停止メッセージで応答します。ルータは、それらの PIM 登録停止メッセージから RP の実際の PIM バージョンを学習します。RP の実際の PIM バージョンが学習されると、このコマンドはそのバージョンのみを表示するようになります。ルータがこのグループのアクティブな送信元の DR として動作していない場合は、グループの RP に対して表示されるバージョンは変わりません。この場合、RP のバージョンはこのルータが送信する必要がある PIM 登録メッセージにしか影響しないため、RP の PIM バージョンがルータに応じて変わることはありません。

show ip pim rp mapping コマンドを入力した場合、出力に表示される RP のバージョンは RP が学習された方法のみで決まります。RP が Auto-RP から学習された場合、表示される RP のバージョンは「v1」または「v2, v1」のいずれかになります。RP がスタティック RP 定義から学習された場合、RP のバージョンは特定されず、出力に表示されません。RP が BSR から学習された場合、表示される RP のバージョンは「v2」になります。

アスタリスク（*）はすべての VRF を指します。この場合、アスタリスクを使用すると、該当するすべての VRF について、関連付けられたマルチキャスト ルーティング エントリとともにキャッシュされているアクティブ RP に関連する情報が表示されます。

次に、**show ip pim rp** コマンドの出力例を示します。

```
Device# show ip pim rp
Group:227.7.7.7, RP:10.10.0.2, v2, v1, next RP-reachable in 00:00:48
```

次に、**mapping** キーワードを指定した場合の **show ip pim rp** コマンドの出力例を示します。

```
Device# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent
Group(s) 227.0.0.0/8
  RP 10.10.0.2 (?), v2v1, bidir
    Info source:10.10.0.2 (?), via Auto-RP
         Uptime:00:01:42, expires:00:00:32
Group(s) 228.0.0.0/8
  RP 10.10.0.3 (?), v2v1, bidir
    Info source:10.10.0.3 (?), via Auto-RP
         Uptime:00:01:26, expires:00:00:34
Group(s) 229.0.0.0/8
  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir
    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP
```

```
        Uptime:00:00:52, expires:00:00:37
Group(s) (-)230.0.0.0/8
  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir
    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP
        Uptime:00:00:52, expires:00:00:37
```

次に、**metric** キーワードを指定した場合の **show ip pim rp** コマンドの出力例を示します。

```
Device# show ip pim rp metric
RP Address      Metric Pref    Metric       Flags   RPF Type   Interface
10.10.0.2       0              0              L     unicast    Loopback0
10.10.0.3       90             409600         L     unicast    Ethernet3/3
10.10.0.5       90             435200         L     unicast    Ethernet3/3
```

次に、**show ip pim vrf * rp mapping** コマンドの出力例を示します。

```
Device# show ip pim vrf * rp mapping
VRF IPv4 default
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)

Group(s) 224.0.0.0/4
  RP 3.3.3.3 (?), v2v1
    Info source: 2.2.2.2 (?), elected via Auto-RP
        Uptime: 4w3d, expires: 00:02:27
Group(s): 224.0.0.0/4, Static
    RP: 1.2.3.4 (?)
Acl: abc, Static
    RP: 1.1.1.1 (?)

VRF ENG
PIM Group-to-RP Mappings
This system is an RP-mapping agent

Group(s) 224.0.0.0/4
  RP 8.8.8.8 (?), v2v1
    Info source: 8.8.8.8 (?), elected via Auto-RP
        Uptime: 4w3d, expires: 00:02:07
```

show ip pim snooping

IP PIM スヌーピングに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show ip pim snooping** コマンドを使用します。

Global Status
show ip pim snooping

VLAN Status
show ip pim snooping vlan *vlan-id* [{**neighbor** | **statistics** | **mroute** [{*source-ipgroup-ip*}]}]

構文の説明

vlan *vlan-id*	特定の VLAN の情報を表示します。有効な値は 1 ～ 4094 です。
neighbor	（任意）近接データベースに関する情報を表示します。
statistics	（任意）VLAN 統計情報を表示します。
mroute	（任意）mroute データベースに関する情報を表示します。
source-ip	（任意）送信元 IP アドレス。
group-ip	（任意）グループ IP アドレス。

コマンド デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

ユーザ EXEC、特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

例

次に、グローバル ステータスに関する情報を表示する例を示します。

```
Router# show ip pim snooping

Global runtime mode: Enabled
Global admin mode  : Enabled
DR Flooding status : Disabled
SGR-Prune Suppression: Enabled
Number of user enabled VLANs: 1
User enabled VLANs: 1001
```

次に、特定の VLAN に関する情報を表示する例を示します。

```
Router# show ip pim snooping vlan 1001

4 neighbors (0 DR priority incapable, 4 Bi-dir incapable)
5000 mroutes, 0 mac entries
DR is 10.10.10.4
```

```
RP DF Set:
QinQ snooping : Disabled
```

次に、特定の VLAN の近接データベースに関する情報を表示する例を示します。

```
Router# show ip pim snooping vlan 1001 neighbor

IP Address       Mac address     Port            Uptime/Expires    Flags
VLAN 1001: 3 neighbors
10.10.10.2        000a.f330.344a  Po128           02:52:27/00:01:41
10.10.10.1        000a.f330.334a  Hu1/0/7         04:54:14/00:01:38
10.10.10.4        000a.f330.3c00  Hu1/0/1         04:53:45/00:01:34 DR
```

次に、特定の VLAN の詳細統計情報を表示する例を示します。

```
Router# show ip pim snooping vlan 1001 statistics

PIMv2 statistics:
Total                                          : 56785
Process Enqueue                                : 56785
Process PIMv2 input queue current outstanding  : 0
Process PIMv2 input queue max size reached     : 110
Error - Global Process State not RUNNING       : 0
Error - Process Enqueue                        : 0
Error - Drops                                  : 0
Error - Bad packet floods                      : 0
Error - IP header generic error                : 0
Error - IP header payload len too long         : 0
Error - IP header payload len too short        : 0
Error - IP header checksum                     : 0
Error - IP header dest ip not 224.0.0.13       : 0
Error - PIM header payload len too short       : 0
Error - PIM header checksum                    : 0
Error - PIM header checksum in Registers       : 0
Error - PIM header version not 2               : 0
```

次に、特定の VLAN におけるすべてのマルチキャスト ルータの mroute データベースに関する情報を表示する例を示します。

```
Router# show ip pim snooping vlan 10 mroute

Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
       SGR-P - (S,G,R) Prune

VLAN 1001: 5000 mroutes
(*, 225.0.1.0), 00:14:54/00:02:59
  10.10.10.120->10.10.10.105, 00:14:54/00:02:59, J
  Downstream ports: Po128
  Upstream   ports: Hu1/0/7
  Outgoing   ports: Hu1/0/7 Po128

(11.11.11.10, 225.0.1.0), 00:14:54/00:02:59
  10.10.10.130->10.10.10.120, 00:14:54/00:02:59, SGR-P
  Downstream ports:
  Upstream   ports: Hu1/0/7
  Outgoing   ports:

(*, 225.0.5.0), 00:14:53/00:02:57
  10.10.10.105->10.10.10.10, 00:14:53/00:02:57, J
  Downstream ports: Po128
  Upstream   ports: Hu1/0/7
  Outgoing   ports: Hu1/0/7 Po128
```

```
(11.11.11.10, 225.0.5.0), 00:14:53/00:02:57
  10.10.10.105->10.10.10.130, 00:14:53/00:02:57, SGR-P
  Downstream ports:
  Upstream   ports: Hu1/0/7
  Outgoing   ports:
Number of matching mroutes found: 4
```

次に、特定の送信元アドレスの PIM mroute に関する情報を表示する例を示します。

```
Router# show ip pim snooping vlan 10 mroute 172.16.100.100

(*, 172.16.100.100), 00:16:36/00:02:36
  10.10.10.1->10.10.10.2, 00:16:36/00:02:36, J
  Downstream ports: 3/12
  Upstream   ports: 3/13
  Outgoing   ports: 3/12 3/13
```

次に、特定の送信元アドレスおよびグループ アドレスの PIM mroute に関する情報を表示する例を示します。

```
Router# show ip pim snooping vlan 10 mroute 192.168.0.0 172.16.10.10

(192.168.0.0, 172.16.10.10), 00:03:04/00:00:25
  10.10.10.1->10.10.10.2, 00:03:04/00:00:25, j
  Downstream ports: 3/12
  Upstream   ports: 3/13
  Outgoing   ports: 3/12 3/13
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *2 : show cable-diagnostics tdr* コマンドで出力されるフィールドの説明

フィールド	説明
Downstream ports	PIM が参加しているポートが受信されました。
Upstream ports	RP と送信元に向かうポート。
Outgoing ports	マルチキャスト フローのすべてのアップストリーム ポートおよびダウンストリーム ポートのリスト。

関連コマンド

コマンド	説明
clear ip pim snooping vlan	インターフェイス上の PIM スヌーピングを削除します。
ip pim snooping	PIM スヌーピングをグローバルにイネーブルにします。
ip pim snooping vlan	インターフェイス上の PIM スヌーピングをイネーブルにします。

show ip pim tunnel

インターフェイス上の Protocol Independent Multicast（PIM）レジスタのカプセル化およびカプセル化解除トンネルに関する情報を表示するには、 **show ip pim tunnel** コマンドを使用します。

show ip pim [**vrf** { *vrf-name* | ***** }] **tunnel** [**Tunnel** *interface-number* | **verbose**]

構文の説明

vrf *vrf-name*	（任意）Virtual Routing and Forwarding（VRF）コンフィギュレーションを指定します。
vrf *	（任意）すべての VRF インスタンスを指定します。
Tunnel *interface-number*	（任意）トンネル インターフェイス番号を指定します。
verbose	（任意）MAC カプセル化ヘッダーおよびプラットフォーム固有情報などの追加情報を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。
Cisco IOS XE Cupertino 17.7.1	すべての VRF インスタンスに関連する情報を表示するために、アスタリスク（*）が導入されました。

使用上のガイドライン

PIM トンネルインターフェイスに関する情報を表示するには、 **show ip pim tunnel** を使用します。

PIM トンネル インターフェイスは、PIM スパース モード（PIM-SM）登録プロセスの IPv4 マルチキャスト転送情報ベース（MFIB）で使用されます。IPv4 MFIB では、2 種類の PIM トンネル インターフェイスが使用されます。

- PIM カプセル化トンネル（PIM Encap トンネル）
- PIM カプセル化解除トンネル（PIM Decap トンネル）

PIM Encap トンネルは、（Auto-RP、ブートストラップ ルータ（BSR）、またはスタティック RP の設定を介して）グループからランデブー ポイント（RP）へのマッピングを学習するたびに動的に作成されます。PIM Encap トンネルは、送信元が直接接続されているファーストホッ

プ代表ルータ（DR）から送信されるマルチキャスト パケットをカプセル化するために使用されます。

PIM Encap トンネルと同様、PIM Decap トンネル インターフェイスは動的に作成されますが、グループから RP へのマッピングを学習するたびに RP 上でのみ作成されます。PIM Decap トンネル インターフェイスは、PIM レジスタのカプセル化解除メッセージのために RP によって使用されます。

（注） PIM トンネルは実行コンフィギュレーションには表示されません。

PIM トンネル インターフェイスが作成されると、次の syslog メッセージが表示されます。

```
* %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel<interface_number>,
changed state to up
```

アスタリスク（*）はすべての VRF を指します。この場合、アスタリスクを使用すると、該当するすべての VRF のトンネルインターフェイスに関連する情報が表示されます。

次に、RP から取得した **show ip pim tunnel** の出力例を示します。この出力は、RP 上の PIM Encap および Decap トンネルを確認するために使用されます。

```
デバイス# show ip pim tunnel

Tunnel0
   Type  : PIM Encap
  RP    : 70.70.70.1*
  Source: 70.70.70.1
Tunnel1*
  Type  : PIM Decap
  RP    : 70.70.70.1*
  Source: -R2#
```

（注） アスタリスク（*）は、そのルータが RP であることを示します。RP には、PIM Encap トンネル インターフェイスおよび PIM Decap トンネル インターフェイスが常にあるとは限りません。

show platform software fed switch ip multicast groups

プラットフォーム依存 IP マルチキャストグループの情報を表示するには、特権 EXEC モードで **show platform software fed switch ip multicast groups** コマンドを使用します。

show platform software fed switch {*switch-number* | **active** | **standby** } **ip multicast groups** [**vrf-id** *vrf-id* | **vrf-name** *vrf-name*] [*group-address* [**source** *source-address*] [**detail**] | **count** | **summary**]

構文の説明

switch {*switch_num* | **active** | **standby** }	情報を表示するデバイス。 • *switch_num*：スイッチ ID を入力します。指定されたスイッチに関する情報を表示します。 • **active**：アクティブスイッチの情報を表示します。 • **standby**：存在する場合、スタンバイスイッチの情報を表示します。
vrf *vrf-id*	（任意）マルチキャスト Virtual Routing and Forwarding（VRF）の ID を指定します。
vrf *vrf-name*	（任意）マルチキャスト Virtual Routing and Forwarding（VRF）の名前を指定します。
group-address	（任意）IP マルチキャスト グループ アドレスを指定します。
source *source-address*	（任意）IP マルチキャスト送信元アドレスを指定します。
detail	（任意）IP マルチキャストグループの詳細を指定します。
count	（任意）IP マルチキャストグループ数を指定します。
summary	（任意）マルチキャストグループの概要を指定します。

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが追加されました。

コマンド モード

特権 EXEC（#）

使用上のガイドライン

このコマンドは、テクニカル サポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

show platform software fed switch ip multicast

プラットフォーム依存 IP マルチキャストテーブルおよびその他の情報を表示するには、特権 EXEC モードで **show platform software fed switch ip multicast** コマンドを使用します。

show platform software fed switch{*switch-number* | **active** | **standby**} **ip multicast** {**groups** | **hardware**[{**detail**}] | **interfaces** | **retry**}

構文の説明

switch {*switch_num* | **active** | **standby** }	情報を表示するデバイス。 • *switch_num*：スイッチ ID を入力します。指定されたスイッチに関する情報を表示します。 • **active**：アクティブスイッチの情報を表示します。 • **standby**：存在する場合、スタンバイスイッチの情報を表示します。
groups	グループごとの IP マルチキャスト ルートを表示します。
hardware [**detail**]	ハードウェアにロードされた IP マルチキャスト ルートを表示します。任意指定の **detail** キーワードは、宛先インデックスおよびルートインデックスのポートメンバを表示するために使用します。
interfaces	IP マルチキャスト インターフェイスを表示します。
retry	リトライ キューの IP マルチキャスト ルートを表示します。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

例

次に、グループごとのプラットフォーム IP マルチキャスト ルートを表示する例を示します。

```
デバイス# show platform software fed active ip multicast groups

Total Number of entries:3
MROUTE ENTRY vrf 0 (*, 224.0.0.0)
```

```
Token: 0x0000001f6  flags:  C
No RPF interface.
Number of OIF: 0
Flags: 0x10   Pkts : 0
OIF Details:No OIF interface.

DI details
----------
Handle:0x603cf7f8 Res-Type:ASIC_RSC_DI Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
Hardware Indices/Handles: index0:0x51f6  index1:0x51f6

Cookie length 56
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x4 0xe0 0x0 0x0 0x0 0x0 0x0

0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Detailed Resource Information (ASIC# 0)
----------------------------------------

al_rsc_di
RM:index = 0x51f6
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f6
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
----------------------------------------

al_rsc_di
RM:index = 0x51f6
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f6
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
```

```
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0

==================================================================

<output truncated>
```

show platform software fed switch ip multicast df

プラットフォーム依存IPマルチキャスト指定フォワーダ（DF）に関する情報を表示するには、特権 EXEC モードで **show platform software fed switch ip multicast df** コマンドを使用します。

show platform software fed switch{*switch-number* | **active** | **standby**} **ip multicast df**[{**vrf-id** *vrf-id* | **vrf-name** *vrf-name*}][{*df-index*}]

構文の説明

switch {*switch_num* | **active** | **standby** }	情報を表示するデバイス。 • *switch_num*：スイッチ ID を入力します。指定されたスイッチに関する情報を表示します。 • **active**：アクティブスイッチの情報を表示します。 • **standby**：存在する場合、スタンバイスイッチの情報を表示します。
vrf-id *vrf-id*	（任意）マルチキャスト Virtual Routing and Forwarding（VRF）の ID を指定します。
vrf *vrf-name*	（任意）マルチキャスト Virtual Routing and Forwarding（VRF）の名前を指定します。
df-index	（任意）DF インデックスを指定します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.12.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、テクニカルサポート担当者とともに問題解決を行う場合にだけ使用してください。テクニカルサポート担当者がこのコマンドの使用を推奨した場合以外には使用しないでください。

次に、show platform software fed switch ip multicast df コマンドの出力例を示します。

```
Device# show platform software fed switch active ip multicast df
VRF-ID  DF-Index        Ref-Count       DF Set
================================================
2       1               1               Vlan254
                                        Vlan186
                                        Vlan305
                                        Vlan135
                                        Tunnel4
```

```
Null0
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。