IP マルチキャスト ルーティング コマンド

cache-memory-max

キャッシュに使用するシステム メモリの割合を設定するには、**cache-memory-max** コマンドを使用します。キャッシュに使用するシステム メモリの割合を削除するには、このコマンドの **no** 形式を使用します。

cache-memory-max *cache-config-percentage*
no cache-memory-max *cache-config-percentage*

構文の説明

cache-config-percentage	キャッシュに使用するシステム メモリの割合。

コマンド デフォルト

デフォルトでは、システム メモリは 10 パーセントに設定されています。

コマンド モード

mDNS 設定

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

ネットワークで学習されるサービスの数が大きくなる可能性があるため、使用できるキャッシュ メモリの容量には上限があります。

（注） デフォルト値は、次のコマンドを使用してオーバーライドできます。

新しいレコードを追加しようとする場合、キャッシュがいっぱいになると、キャッシュ内の期限切れに近いレコードが削除され、新しいレコードのためのスペースが確保されます。

例

次に、キャッシュに使用するシステム メモリの割合を 20% に設定する例を示します。

```
(config-mdns)# cache-memory-max 20
```

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発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。

```
Device# 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。

```
Device# 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。

```
Device# 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** 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、グループのメンバー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。

```
Device# 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。

```
Device# clear ip mroute 224.2.205.42 228.3.0.0
```

clear ip pim snooping vlan

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 **clearippimsnoopingvlan** 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 Fuji 16.8.1a	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
ippimsnooping	PIM スヌーピングをグローバルにイネーブルにします。
showippimsnooping	IP PIM スヌーピングに関する情報を表示します。

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、 スタックまたはスランドアロン 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 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。

```
Device(config)# ip igmp profile 40
Device(config-igmp-profile)# permit
Device(config-igmp-profile)# range 233.1.1.1 233.255.255.255
Device(config-igmp-profile)# exit
Device(config)# interface gigabitethernet1/0/2
Device(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.
Device(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、 スタックまたはスタンドアロン 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、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。

- 最大グループ制限がデフォルト（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無効です。

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。

```
Device(config)# interface gigabitethernet1/0/2
Device(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 を設定する方法を示します。

```
Device(config)# interface gigabitethernet2/0/1
Device(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、スタックまたはスタンドアロンで **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。

```
Device(config)# ip igmp profile 40
Device(config-igmp-profile)# permit
Device(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

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、 スタックまたはスタンドアロン 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

上で、IGMP スヌーピングはグローバルにイネーブルです。

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。

```
Device(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。

```
Device(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 **ipigmpsnoopinglast-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（からホストへのクエリーパケット、またはホストから 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、 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。

```
Device(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 *interval*	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。1 または 2 を選択します。

コマンド デフォルト

IGMP スヌーピング クエリア機能は、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。

```
Device(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。

```
Device(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。

```
Device(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 クエリー カウントを 25 に設定する方法を示します。

```
Device(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。

```
Device(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。

```
Device(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、 スタックまたはスタンドアロン 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 クエリーに 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、クエリーに IGMPv3 レポートが含まれている場合はサポートされません。

は IGMP レポート抑制を使用して、1 つのマルチキャスト 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、 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。 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、 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、 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。

```
Device(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 vlan mrouter

マルチキャスト ルータ ポートの追加、 スタックまたはスタンドアロン 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。

```
Device(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、スタックまたはスタンドアロン 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。

```
Device(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、認可、アカウンティング（AAA）の有効化をサポートするには、**ipmulticastauto-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。

```
Device(config)# ip multicast auto-enable
```

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 ［**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 メンバー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。

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

ip pim bsr-candidate

候補 BSR になるように Device 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 Device 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 Device 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

Device 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 Device 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 Device 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 Device 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 Device 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長い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 Device 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。

```
Device(config)# ip pim bsr-candidate GigabitEthernet1/0/1 0 192
```

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 Device 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 Device 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

Device 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 Device 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 Device 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。

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

ip pim send-rp-announce

Auto-RP を使用して、Device 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。Device 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*］
no ip pim ［**vrf** *vrf-name*］ **send-rp-announce** *interface-id*

構文の説明

vrf *vrf-name*	（任意）Device 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。

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。

使用上のガイドライン

RP にする Device 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。

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 Device 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

PIM（Protocol Independent Multicast）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 **ippimsnooping** コマンドを使用します。PIM スヌーピングをグローバルに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 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 Fuji 16.8.1a	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
clearippimsnooping	インターフェイス上の PIM スヌーピングを削除します。
showippimsnooping	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

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 **ippimsnoopingdr-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 Fuji 16.8.1a	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。

noippimsnoopingdr-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
clearippimsnooping	インターフェイス上の PIM スヌーピングを削除します。
showippimsnooping	IP PIM スヌーピングに関する情報を表示します。

ip pim snooping vlan

インターフェイスで PIM（Protocol Independent Multicast）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 **ippimsnoopingvlan** 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 Fuji 16.8.1a	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
clearippimsnooping	インターフェイス上の PIM スヌーピングを削除します。
ippimsnooping	PIM スヌーピングをグローバルにイネーブルにします。
showippimsnooping	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* 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。

```
Device(config)# ip pim spt-threshold infinity group-list 16
```

match message-type

サービス リストの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	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 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** オプションでのみ使用できます。

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。

```
(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** オプションでのみ使用できます。

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。

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

match service-instance

サービス リストの照合するサービス 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** オプションでのみ使用できます。

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。

```
(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。

```
Device# 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

redistribute mdns-sd

サブネット全体にサービスやサービス アナウンスメントを再配布するには、**redistribute mdns-sd** コマンドを使用します。サブネット全体へのサービスやサービス アナウンスメントの再配布を無効にするには、このコマンドの **no** 形式を使用します。

redistribute mdns-sd
no redistribute mdns-sd

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

サブネット全体へのサービスやサービス アナウンスメントの再配布は無効になっています。

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

インターフェイスにサービス アナウンスメントを再配布するには、**redistribute mdns-sd** コマンドを使用します。このコマンドは、1 つのインターフェイスで受信した非要請アナウンスメントを他のすべてのインターフェイスに送信します。発信アナウンスメントはインターフェイスに定義された出力サービス ポリシーに従って、または、インターフェイスごとのサービス ポリシーがない場合はグローバル出力サービス ポリシーに基づいてフィルタ処理されます。

再配布オプションがない場合は、サービス プロバイダーに対してローカルでないレイヤ 3 ドメインでクエリすることで、サービスを検出できます。

例

次に、サブネット全体にサービスやサービス アナウンスメントを再配布する例を示します。

```
(config-mdns)# redistribute mdns-sd
```


（注） 再配布がグローバルに有効になっている場合は、グローバル コンフィギュレーションがインターフェイス コンフィギュレーションよりも優先順位が高くなります。

service-list mdns-sd

でmDNSサービス検出サービスリストモードを開始するには、**service-list mdns-sd** コマンドを使用します。mDNS サービス検出サービスリスト モードを終了するには、このコマンドの **no** 形式を使用します。

service-list mdns-sd *service-list-name* {**permit** | **deny**} *sequence-number* [**query**]
no service-list mdns-sd *service-list-name* {**permit** | **deny**} *sequence-number* [**query**]

構文の説明

service-list-name	サービス リストの名前。
permit *sequence number*	シーケンス番号に対するサービス リストのフィルタの適用を許可します。
deny *sequence number*	シーケンス番号に対するサービス リストのフィルタの適用を拒否します。
query	サービス リスト名のクエリを関連付けます。

コマンド デフォルト

ディセーブル

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

サービス フィルタは、アクセス リストとルートマップに関してモデル化されています。

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。

このコマンドはmDNSサービス検出サービスリスト モードを開始するために使用できます。

このモードでは、次の操作を実行できます。

- サービス リストを作成し、シーケンス番号に適用された **permit** または **deny** オプションに従って、サービス リストにフィルタを適用します。

例

次に、サービス リストを作成し、シーケンス番号に適用された **permit** または **deny** オプションに従って、サービス リストにフィルタを適用する例を示します。

```
(config)# service-list mdns-sd sl1 permit 3
```

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。

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

service-routing mdns-sd

デバイスの mDNS ゲートウェイ機能を有効にし、マルチキャスト DNS コンフィギュレーション モードを開始するには、**service-routing mdns-sd** コマンドを使用します。デフォルト設定を復元し、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を入力します。

service-routing mdns-sd
no service-routing mdns-sd

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

ディセーブル

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

mDNS ゲートウェイ機能は、インターフェイス単位ではなく、グローバルでのみ有効または無効にすることができます。サービス フィルタ ポリシーと再配布は、グローバルでも、インターフェイス単位でも設定できます。インターフェイス固有の設定は、グローバルな設定より優先されます。

例

次に、デバイスの mDNS ゲートウェイ機能を有効にして、マルチキャスト DNS コンフィギュレーション モードを開始する例を示します。

```
(config)# service-routing mdns-sd
```

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。フィルタを除去するには、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。

```
(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、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。

```
Device# 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、 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。

```
Device# show ip igmp profile 40
IGMP Profile 40
    permit
    range 233.1.1.1 233.255.255.255
```

次に、 に設定された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。

```
Device# 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

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 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。

```
Device# 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、 上のすべての VLAN のスヌーピング特性を表示します。

```
Device# 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

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。 のマルチキャスト テーブルが表示されます。

```
Device# 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。 上のマルチキャスト グループの総数が表示されます。

```
Device# 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。

```
Device# 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

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。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。

```
Device# show ip igmp snooping mrouter

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

show ip igmp snooping querier

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 を指定できます。

show ip igmp snooping querier コマンドの出力にも、クエリアが検出された VLAN およびインターフェイスが表示されます。クエリアが 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** コマンドに類似しています。ただし、**show ip igmp snooping querier** コマンドでは、 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、 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 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。

```
Device> 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。

```
Device> show ip igmp snooping querier detail

Vlan      IP Address     IGMP Version   Port
-----------------------------------------------------------
1         1.1.1.1        v2             Fa8/0/1
Global IGMP  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  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 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 autorp

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

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。

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。

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。

```
Device# 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
```

show ip pim bsr-router

PIM（Protocol Independent Multicast）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 bsr-router

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

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

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。

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

```
Device# 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

PIM（Protocol Independent Multicast）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 bsr

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

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

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。

次に、**show ip pim bsr** コマンドの出力例を示します。

```
Device# 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 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 **showippimsnooping** コマンドを使用します。

GlobalStatus
show ip pim snooping

VLANStatus
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 Fuji 16.8.1a	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 *1 : 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
clearippimsnoopingvlan	インターフェイス上の PIM スヌーピングを削除します。
ippimsnooping	PIM スヌーピングをグローバルにイネーブルにします。
ippimsnoopingvlan	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 PIM（Protocol Independent Multicast）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。
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。

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
```

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。

```
Device# 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 mdns cache

の mDNS キャッシュ情報を表示するには、特権 EXEC モードで **show mdns cache** コマンドを使用します。

show mdns cache [**interface** *type number* | **name** *record-name* [**type** *record-type*] | **type** *record-type*]

構文の説明

interface *type-number*	（任意）mDNS キャッシュ情報を表示する特定のインターフェイスのタイプと番号を指定します。
name *record-name*	（任意）mDNS キャッシュ情報を表示する特定の名前を指定します。
type *record-type*	（任意）mDNS キャッシュ情報を表示する特定のタイプを指定します。

コマンド デフォルト

なし

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 mdns cache** コマンドの出力例を示します。

```
# show mdns cache
```

```
[<NAME>]
[<TYPE>][<CLASS>][<TTL>/Remaining][Accessed][If-name][Mac Address][<RR Record Data>]

_airplay._tcp.local                   PTR     IN      4500/4455         0        Vl121
 b878.2e33.c7c5 CAMPUS APPLE TV1._airplay._tcp.local

CAMPUS APPLE TV1._airplay._tcp.local SRV     IN      120/75            2        Vl121
 b878.2e33.c7c5 CAMPUS-APPLE-TV1.local

CAMPUS-APPLE-TV1.local                A       IN      120/75            2        Vl121
 b878.2e33.c7c5  121.1.0.254

CAMPUS APPLE TV1._airplay._tcp.local TXT     IN      4500/4455         2        Vl121
 b878.2e33.c7c5  (162) 'deviceid=B8:78:2E:33:C7:C6'

                 'features=0x5a7ffff7''flags=0x4'
```

```
                'model=AppleT~'~

_ipp._tcp.local                       PTR     IN      4500/4465         2        V12
 2894.0fed.447f  EPSON XP-400 Series._ipp._tcp.local

EPSON XP-400 Series._ipp._tcp.local  SRV     IN      120/85            2        V12
 2894.0fed.447f  EPSONC053AA.local

EPSONC053AA.local                     A       IN      120/85            2        V12
 2894.0fed.447f  121.1.0.251

EPSON XP-400 Series._ipp._tcp.local  TXT     IN      4500/4465         2        V12
 2894.0fed.447f  (384)'txtvers=1' N XP-400 Series'

                'usbFG=EPSON''usb_MDL=XP~'~

_smb._tcp.local                       PTR     IN      4500/4465         2        V12
 2894.0fed.447f  EPSON XP-400 Series._smb._tcp.local

EPSON XP-400 Series._smb._tcp.local  SRV     IN      120/85            2        V12
 2894.0fed.447f  EPSONC053AA.local

EPSON XP-400 Series._smb._tcp.local  TXT     IN      4500/4465         2        V12
 2894.0fed.447f  (1)'' R2-Access1#
```

show mdns requests

のレコード名とレコード タイプ情報を含む、未処理の mDNS 要求の情報を表示するには、特権 EXEC モードで **show mdns requests** コマンドを使用します。

show mdns requests [**detail** | **name** *record-name* | **type** *record-type* [**name** *record-name*]]

構文の説明

detail	詳細な mDNS 要求の情報を表示します。
name *record-name*	名前に基づいた詳細な mDNS 要求の情報を表示します。
type *record-type*	タイプに基づいた詳細な mDNS 要求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

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 mdns requests** コマンドの出力例を示します。

```
# show mdns requests
MDNS Outstanding Requests
==================================================
Request name  :   _airplay._tcp.local
Request type  :   PTR
Request class :   IN
--------------------------------------------------
Request name  :   *.*
Request type  :   PTR
Request class :   IN
```

show mdns statistics

の mDNS 統計を表示するには、特権 EXEC モードで **show mdns statistics** コマンドを使用します。

show mdns statistics {**all** | **service-list** *list-name* | **service-policy** {**all** | **interface** *type-number* }}

構文の説明

all	サービス ポリシー、サービス リスト、インターフェイス情報を表示します。
service-list *list-name*	サービス リスト情報を表示します。
service-policy	サービス ポリシー情報を表示します。
interface *type number*	インターフェイス情報を表示します。

コマンド デフォルト

なし

コマンド モード

特権 EXEC

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

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 mdns statistics all** コマンドの出力例を示します。

```
# show mdns statistics all

 mDNS Statistics
 mDNS packets sent       : 0
 mDNS packets received   : 0
 mDNS packets dropped    : 0
 mDNS cache memory in use: 64224(bytes)
```

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 コマンドで **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。

```
Device# 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>
```