IPマルチキャストの最適化：マルチキャスト向けSSMチャネル ベース フィルタリング

マルチキャスト境界向け SSM チャネル ベース フィルタリングの前提条件

IP マルチキャストをデバイスで有効にするには、『*IP Multicast: PIM Configuration Guide*』の「Configuring Basic IP Multicast」モジュールに記載されているタスクを使用します。

マルチキャスト境界向け SSM チャネル ベース フィルタリングについて

ここでは、マルチキャスト境界向けの SSM チャネル ベース フィルタリング機能について説明します。

マルチキャスト境界のルール

マルチキャスト境界向けのSSMチャネルベースフィルタリング機能は、**ip multicast boundary** コマンドを拡張して、コントロール プレーン フィルタリングをサポートします。1 つのインターフェイスに複数の **ip multicast boundary** コマンドを適用できます。

次のルールで **ip multicast boundary** コマンドは制御されます。

- 1 つのインターフェイスに設定できるのは、**in** および **out** キーワードの一方のインスタンスです。
- **in** および **out** キーワードは、標準アクセスリストまたは拡張アクセスリストに使用できます。
- **filter-autorp** キーワードまたは no キーワードを使用する場合、標準のアクセスリストだけが許可されます。
- コマンドの最大 3 つのインスタンスが 1 つのインターフェイスで許可されます。**in** の 1 つのインスタンス、**out** の 1 つのインスタンス、および **filter-autorp** または no キーワードの 1 つのインスタンスです。
- コマンドの複数のインスタンスを使用すると、フィルタリングは累積的になります。キーワードなしの境界ステートメントが、**in** キーワードが含まれる境界ステートメントと存在する場合、両方のアクセスリストが入力方向に適用され、どちらか一方での一致で十分です。
- コマンドのすべてのインスタンスは、制御トラフィックおよびデータ プレーン トラフィックの両方に適用されます。
- 拡張アクセス リストのプロトコル情報は解析され、一貫性の再利用とフィルタリングが許可されます。アクセス リストがすべてのプロトコルの（S,G）トラフィックをフィルタリングする場合、（S,G）オペレーションは、キーワードについて記述されたすべての条件で拡張アクセス リストによってフィルタリングされます。

マルチキャスト境界向け SSM チャネル ベース フィルタリングの利点

- この機能によって、送信元インターフェイスでの入力が可能になります。
- アクセス制御機能は、SSM および Any Source Multicast（ASM）の場合と同じです。

マルチキャスト境界向け SSM チャネル ベース フィルタリングの設定方法

ここでは、マルチキャスト境界に SSM チャネルベースのフィルタリングを設定する手順について説明します。

マルチキャスト境界の設定

手順の概要

1. **enable**
2. **configure terminal**

3. **ip access-list** {**standard**| **extended**} *access-list-name*
4. **permit** *protocol* **host** *address* **host** *address*
5. **deny** *protocol* **host** *address* **host** *address*
6. 必要に応じて、ステップ 4 またはステップ 5 を繰り返します。
7. **interface** *type* **interface-number** *port -number*
8. **ip multicast boundary** *access-list-name* [**in**| **out** | **filter-autorp**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list** {**standard**| **extended**} *access-list-name* 例： `Device(config)# ip access-list 101`	標準または拡張のアクセス リストを設定します。
ステップ 4	**permit** *protocol* **host** *address* **host** *address* 例： `Device(config-ext-nacl)# permit ip host 181.1.2.201 host 232.1.1.11`	指定された ip ホスト トラフィックを許可します。
ステップ 5	**deny** *protocol* **host** *address* **host** *address* 例： `Device(config-acl-nacl)# deny ip host 181.1.2.203 host 232.1.1.1`	指定されたマルチキャスト ip グループおよび送信元トラフィックを拒否します。
ステップ 6	必要に応じて、ステップ 4 またはステップ 5 を繰り返します。	指定されたホストおよび送信元トラフィックを許可および拒否します。
ステップ 7	**interface** *type* **interface-number** *port -number* 例： `Device(config)# interface gigabitethernet 2/3/0`	インターフェイス コンフィギュレーション モードをイネーブルにします。
ステップ 8	**ip multicast boundary** *access-list-name* [**in**| **out**	**filter-autorp**]	マルチキャスト境界を設定します。

	コマンドまたはアクション	目的
	例： `Device(config-if)# ip multicast boundary acc_grp1 out`	（注） **filter-autorp** キーワードは、拡張アクセス リストをサポートしていません。

マルチキャスト境界向け SSM チャネル ベース フィルタリングの設定例

ここでは、マルチキャスト境界向け SSM チャネル ベースフィルタリング機能の設定例を紹介します。

トラフィックを許可および拒否するマルチキャスト境界の設定例

次の例では、(181.1.2.201, 232.1.1.1) および (181.1.2.202, 232.1.1.1) への発信トラフィックを許可し、他のすべての (S,G) を拒否します。

```
configure terminal
 ip access-list extended acc_grp1
 permit ip host 0.0.0.0 232.1.1.1 0.0.0.255
 permit ip host 181.1.2.201 host 232.1.1.1
 permit udp host 181.1.2.202 host 232.1.1.1
 permit ip host 181.1.2.202 host 232.1.1.1
 deny igmp host 181.2.3.303 host 232.1.1.1
 interface gigabitethernet 1/0/1
 ip multicast boundary acc_grp1 out
```

トラフィックを許可するマルチキャスト境界の設定例

次の例では、(192.168.2.201, 232.1.1.5) および (192.168.2.202, 232.1.1.5) への発信トラフィックを許可します。

```
configure terminal
ip access-list extended acc_grp6
 permit ip host 0.0.0.0 232.1.1.1 5.0.0.255
 deny udp host 192.168.2.201 host 232.1.1.5
 permit ip host 192.168.2.201 host 232.1.1.5
 deny pim host 192.168.2.201 host 232.1.1.5
 permit ip host 192.168.2.202 host 232.1.1.5
 deny igmp host 192.2.3.303 host 232.1.1.1
interface gigabitethernet 1/0/1
 ip multicast boundary acc_grp6 out
```

トラフィックを拒否するマルチキャスト境界の設定例

次に、候補 RP でアナウンスされるグループ範囲を拒否する例を示します。グループ範囲が拒否されるため、pim auto-rp マッピングは作成されません。

```
configure terminal
ip access-list standard acc_grp10
 deny 225.0.0.0 0.255.255.255
 permit any
 access-list extended acc_grp12
 permit pim host 181.1.2.201 host 232.1.1.8
 deny udp host 181.1.2.201 host 232.1.1.8
 permit pim host 181.1.2.203 0.0.0.255 host 227.7.7.7
 permit ip host 0.0.0.0 host 227.7.7.7
 permit ip 181.1.2.203 0.0.0.255 host 227.7.7.7
 permit ip host 181.1.2.201 host 232.1.1.7
ip access-list extended acc_grp13
 deny ip host 181.1.2.201 host 232.1.1.8
 permit ip any any
interface gigabitethernet 1/0/1
 ip multicast boundary acc_grp10 filter-autorp
 ip multicast boundary acc_grp12 out
 ip multicast boundary acc_grp13 in
```

IP マルチキャストの最適化：マルチキャスト向け SSM チャネル ベース フィルタリングに関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Command Reference (Catalyst 9200 Series Switches)* の「IP マルチキャスト ルーティング コマンド」の項を参照してください。

IP マルチキャストの最適化に関する機能履歴：マルチキャスト向け SSM チャネル ベース フィルタリングの機能履歴と情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : IP* マルチキャストの最適化：マルチキャスト向け *SSM* チャネル ベース フィルタリングの機能情報

機能名	リリース	機能情報
IP マルチキャストの最適化：マルチキャスト向け SSM チャネル ベース フィルタリング	Cisco IOS XE Fuji 16.9.2	マルチキャスト境界のための SSM チャネル ベース フィルタリング機能は、ip multicast boundary コマンドを拡張して、コントロール プレーン フィルタリングをサポートします。複数の ip multicast boundary コマンドをインターフェイスに適用できます。