



PIM 許可 RP の構成

この章では、IPv4 ネットワークおよび IPv6 ネットワークの Cisco NX-OS デバイスに Protocol Independent Multicast (PIM) および PIM6 機能を設定する方法を説明します。

- [はじめに \(1 ページ\)](#)
- [PIM 許可 RP の注意事項と制限事項 \(1 ページ\)](#)
- [PIM 許可 RP に関する情報 \(2 ページ\)](#)
- [PIM-SM の RP の構成 \(3 ページ\)](#)
- [PIM Allow RP の有効化 \(4 ページ\)](#)
- [許可 RP ポリシーに関する情報の表示 \(6 ページ\)](#)

はじめに

この章では、異なるランデブーポイント (RP) を持つ Protocol Independent Multicast (PIM) Sparse Mode (SM) ドメインを相互接続するために、IPv4 および IPv6 ネットワークで PIM Allow RP 機能を設定する方法について説明します。PIM Allow RP を使用すると、着信 (*, G) Join が処理され、別の RP が識別されたときに、受信側デバイスが独自の RP を使用して状態を作成し、共有ツリーを構築できるようになります。これにより、受信デバイスは別の RP からの (*, G) Join を受け入れることができます。

PIM 許可 RP の注意事項と制限事項

- PIM 許可 RP は、PIM SM ドメインの接続のみをサポートします。
- PIM 許可 RP はダウンストリームトラフィックにのみ適用されます。つまり、共有ツリーの構築にのみ適用されます。
- PIM 許可 RP は、ルートマップのみを使用するように制限されています。
- PIM 許可 RP は、Cisco NX-OS リリース 10.2(2)F より前では IPv6 マルチキャストをサポートしていません。
- IPv6 PIM 許可 RP は、Cisco NX-OS リリース 10.2(2)F からサポートされています。

- PIM 許可 RP は、「送信元」を持つ RPM をサポートしていません。PIM 許可 RP PIM 許可 RP に関する情報。
- 存在しない RPM を使用して Allow-RP 設定を追加すると、すべての結合/プルーニングが拒否されます。
- PERMIT-ALL または DENY-ALL を持つ RPM を使用して Allow-RP 構成を追加すると、すべての結合/プルーニングがそれに応じて受け入れられるか破棄されます。

PIM 許可 RP に関する情報

ランデブーポイント

ランデブーポイント (RP) は、デバイスが PIM (Protocol Independent Multicast) スパースモード (SM) で動作している場合にデバイスが実行するロールです。RP が必要になるのは、PIM SM を実行しているネットワークだけです。PIM-SM モデルでは、マルチキャストデータを明示的に要求したアクティブなレシーバを含むネットワークセグメントだけにトラフィックが転送されます。マルチキャストデータの配信方法は、PIM デンスモード (PIMDM) とは対照的です。PIMDM では、マルチキャストトラフィックが最初にネットワークのすべてのセグメントにフラッディングされます。ダウンストリームネイバーを持たないルータ、または直接レシーバに接続されているルータは、不要なトラフィックをプルーニングします。RP は、マルチキャストデータのソースとレシーバの接点として機能します。PIM SIM ネットワークでは、ソースが RP にトラフィックを送信する必要があります。このトラフィックは、それから共有配信ツリーを下ってレシーバに転送されます。

デフォルトでは、レシーバのファーストホップデバイスがソースを認識すると、ソースに Join メッセージを直接送信し、ソースからレシーバへのソースベースの配信ツリーを作成します。ソースとレシーバ間の最短パス内に RP が配置されていない限り、このソースツリーに RP は含まれません。ほとんどの場合、ネットワークにおける RP の配置は複雑な判断を必要としません。

デフォルトでは、RP が必要になるのは、ソースおよびレシーバとの新しいセッションを開始する場合だけです。その結果、RP では、トラフィックのフローまたは処理によるオーバーヘッドはほとんど発生しません。PIM バージョン 2 で実行される処理は PIM バージョン 1 よりも少なくなっています。これは、ソースを定期的に RP に登録するだけでステートを作成できるためです。

PIM 許可 RP

ネットワークには、パブリッシャ、コンシューマ、トランスポートの 3 種類があります。多くのパブリッシャネットワークはコンテンツを発信でき、多くのコンシューマネットワークがそのコンテンツに関心を持つことがあり得ます。サービスプロバイダーが所有および運用するトランスポートネットワークは、パブリッシャとコンシューマネットワークを接続します。

コンシューマとトランスポートネットワークは、次のように接続されます。特定のグループ範囲またはすべてのグループ範囲 (デフォルトルートと同様) に対して、サービスプロバイダーは、RP-A などの特定のランデブーポイント (RP) を定義します。コンシューマデバイスからの RP-A のリバースパス転送により、(*, G) Join がトランスポートネットワークに送信されま

す。同じグループに対して、サービスプロバイダーは、RP-B などの異なる RP を定義できます。RP-B は、G のトランスポート ネットワーク内で共有ツリーを構築するために使用されます。RP-A と RP-B は通常、異なる RP であり、各 RP は異なるグループ範囲に対して定義されます。RFC 4601 では、デバイスが (*, G) Join を受信したとき、(*, G) Join で指定された RP が、受信デバイスが予期するものと異なる場合（不明な RP）、着信 (*, G) Join は無視する必要がありますと定めています。

PIM 許可 RP 機能は、Cisco NX-OS Release 8.4(1) で導入されました。この機能により、受信デバイスは、着信 (*, G) Join が処理されて別の RP が識別されたとき、独自の RP を使用して状態を作成し、共有ツリーを構築できます。これにより、受信デバイスは別の RP からの (*, G) Join を受け入れることができます。ルートマップは、(*, G) join の対象となる RP アドレスまたはグループアドレス（あるいはその両方）を制御するために使用されます。(*, G) join メッセージの RP アドレスとグループアドレスは、ルートマップで指定された RP とグループアドレスと照合されます。

PIM Allow RP は、ダウンストリーム トラフィックにのみ適用されます。

PIM-SM の RP の構成

始める前に

すべてのアクセスリストは、設定作業を開始する前に設定しておく必要があります。アクセスリストの構成方法については、[Cisco Nexus 9000 Series NX-OS Security Configuration Guide](#) の「Configuring IP ACLs」の章を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	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 2	interface interface 例： switch(config)# interface gigabitethernet 1/0/0 switch(config-if)#	PIM をイネーブルにできるホストに接続されているインターフェイスを選択します。 interface type number 。
ステップ 3	ip pim sparse-mode 例： switch(config-if)# ip pim sparse-mode	PIM をイネーブルにします。スパースモードを使用する必要があります。
ステップ 4	no shut 例： switch(config-if)# no shut	インターフェイスを有効化します。

	コマンドまたはアクション	目的
ステップ 5	Exit 例： switch(config-if)# exit	グローバル コンフィギュレーション モードに戻ります。 IP マルチキャストを使用するすべてのインターフェイスでステップ 3～5 を繰り返します。
ステップ 6	ip pim rp-address rp-address[group-listip-prefix route-mappolicy-name] 例： switch(config)# ip pim rp-address 30.2.2.2 group-list 224.0.0.0/4	マルチキャストグループ範囲に、PIM スタティック RP アドレスを設定します。match ip multicast コマンドで、使用するグループプレフィックスを示すルートマップポリシー名を指定できます。このコマンドは、VRF モードでも使用できます。
ステップ 7	end 例： Switch (config-route-map)# end	ルートマップ構成モードを終了します。
ステップ 8	(任意) show ip pim rp [vrf rp-address] 例： switch# show ip pim rp	(任意) ネットワークで既知の RP を表示し、ルータが各 RP について学習する方法を示します。
ステップ 9	(任意) show ip mroute 例： switch# show ip mroute	IP mroute テーブルの内容を表示します。

PIM Allow RP の有効化

次の構成手順では、次のような RPM の組み合わせのいずれかを一度に設定できます：グループのみ、RP のみ、グループ RP、グループ範囲のみです。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	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 2	route-map map-name permitsequence-numberdeny 例： switch(config)# route-map mcast-grp permit 10	ルートマップ構成モードを開始します。この構成モードでは、permit キーワードを使用する点に注意してください。

	コマンドまたはアクション	目的
ステップ 3	match ip multicast group <i>group-address</i> 例 : <pre>Switch(config-route-map)# match ip multicast group 224.0.0.0/4</pre>	IP マルチキャスト グループの照合を行います。 (注) 一度に構成できる RPM の組み合わせは、グループのみ、RP のみ、グループ RP、グループ範囲のみのいずれか 1 つだけです。たとえば、この手順 (グループのみ) を構成する場合は、手順 9 に進む必要があります。 これは、以下の手順 (手順 4 から手順 8) にも当てはまります。
ステップ 4	match ip multicast group-range {<i>group address_start to group address_end</i>} 例 : <pre>switch(config-route-map) # match ip multicast group-range 230.1.1.1 to 230.1.1.255</pre>	指定されたグループアドレスとの間で IP マルチキャスト グループ範囲を照合します。
ステップ 5	match ip multicast rprp-address 例 : <pre>switch (config-route-map) # match ip multicast 222.0.0.0/4</pre>	IP マルチキャストと指定された RP を照合します。
ステップ 6	match ip multicast rp <i>rp-addressrp-type</i> 例 : <pre>switch (config-route-map)# match ip multicast rp 1.1.1.1/32 rp-type ASM</pre>	IP マルチキャスト RP アドレスと指定された RP タイプを照合します。サポートされている RP タイプは ASM のみです。
ステップ 7	match ip multicast group <i>addressrpaddress</i> 例 : <pre>switch(config-route-map)# match ip multicast group 230.1.1.1/4 rp 1.1.1.1/32</pre>	IP マルチキャスト グループアドレスと RP アドレスを照合します。
ステップ 8	match ip multicast group-range {<i>group address_start to group address_end</i>}<i>rpaddress</i> 例 : <pre>switch (config-route-map)# match ip multicast group-range 230.1.1.1 to 230.1.1.255 rp 1.1.1.1/32</pre>	指定されたアドレスと RP アドレスとの間で IP マルチキャスト グループ範囲を照合します。
ステップ 9	ip pim allow-rp <i>route-map-name</i> 例 : <pre>switch(config-rooute-map)# ip pim allow-rp test-route-map</pre>	PIM Allow RP を有効にします。スパースモードの RP アドレスを許可します。このコマンドは、VRF レベルでも構成されます。ルート マップは、(*,G) join の対象となる RP アドレスまたはグループアドレス (あるいはその両方) を制御するために使用されます。(*,G) join メッセージの RP アドレスとグ

	コマンドまたはアクション	目的
		ループアドレスは、ルートマップで指定された RP とグループアドレスと照合されます。
ステップ 10	ipv6 pim allow-rp route-map-name 例： switch(config-route-map)# ipv6 pim allow-rp test-route-map	IPv6 PIM Allow RP を有効にします。
ステップ 11	(任意) show ip pim policy statistics allow-rp-policy show ipv6 pim policy statistics allow-rp-policy 例： switch(config)# show ip pim policy statistics allow-rp-policy	ポリシー統計を表示するには、次の手順に従います。
ステップ 12	end 例： Switch (config-route-map)# end	ルートマップ構成モードを終了します。

許可 RP ポリシーに関する情報の表示

次のコマンドは、VRF モードでも使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Enable 例： switch# enable	特権 EXEC モードを有効にします。
ステップ 2	show ip pim policy statistics allow-rp-policy 例： switch# show ip pim policy statistics allow-rp-policy	現在の許可 RP ポリシーとそのカウンタに関する統計を表示します。
ステップ 3	show ipv6 pim policy statistics allow-rp-policy 例： switch# show ipv6 pim policy statistics allow-rp-policy	現在の許可 RP ポリシーに関する IPv6 統計を表示します。
ステップ 4	clear ip pim policy statistics allow-rp-policy 例： switch# clear ip pim policy statistics allow-rp-policy	許可 RP ポリシーのポリシーとカウンタをクリアします。

	コマンドまたはアクション	目的
ステップ 5	clear ipv6 pim policy statistics allow-rp-policy 例 : switch# clear ipv6 pim policy statistics allow-rp-policy	IPv6 の許可 RP ポリシーのポリシーとカウンタをクリアします。

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。