



PIM 許可 RP の設定

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 許可 RP を使用すると、着信 (*, G) Join を処理し、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 に関する情報

- 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) スペース 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 (PIM DM) とは対照的です。PIM DM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ると定めています。

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 シリーズ NX-OS セキュリティ構成ガイドの「IP ACL の構成」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
Step 1	configure terminal 例: <pre>switch# configure terminal switch(config)#</pre>	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
Step 2	interface interface 例: <pre>switch(config)# interface gigabitethernet 1/0/0 switch(config-if)#</pre>	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 タイプ番号です。
Step 3	ip pim sparse-mode 例: <pre>switch(config-if)# ip pim sparse-mode</pre>	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。
Step 4	no shut 例: <pre>switch(config-if)# no shut</pre>	インターフェイスを有効化します。
Step 5	Exit 例:	グローバルコンフィギュレーションモードに戻ります。

PIM Allow RP の有効化

	コマンドまたはアクション	目的
	switch(config-if)# exit	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。
Step 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。
Step 7	end 例: Switch (config)# end	ルートマップ構成モードを終了します。
Step 8	(任意) show ip pim rp [vrf rp-address] 例: switch# show ip pim rp	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。
Step 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

次の設定手順では、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
Step 1	configure terminal 例: switch# configure terminal switch(config)#	グローバル設定モードを開始します。
Step 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。
Step 3	match ip multicast group group-address 例:	IP マルチキャストグループの照合を行います。 (注)

	コマンドまたはアクション	目的
	Switch(config-route-map) # match ip multicast group 224.0.0.0/4	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。
Step 4	match ip multicast group-range {group address_start to group address_end} 例: switch(config-route-map) # match ip multicast group-range 230.1.1.1 to 230.1.1.255	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。
Step 5	match ip multicast rprp-address 例: switch (config-route-map) # match ip multicast 222.0.0.0/4	IP マルチキャストと指定された RP を照合します。
Step 6	match ip multicast rp rp-addressrp-type type 例: switch (config-route-map) # match ip multicast rp 1.1.1.1/32 rp-type ASM	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。
Step 7	match ip multicast group addressrpaddress 例: switch(config-route-map) # match ip multicast group 230.1.1.1/4 rp 1.1.1.1/32	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。
Step 8	match ip multicast group-range {group address_start to group address_end}rpaddress 例: switch (config-route-map) # match ip multicast group-range 230.1.1.1 to 230.1.1.255 rp 1.1.1.1/32	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。
Step 9	ip pim allow-rp route-map-name 例: switch(config-route-map) # ip pim allow-rp test-route-map	PIM Allow RP を有効にします。スペースモードの 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。

■ 許可 RP ポリシーに関する情報の表示

	コマンドまたはアクション	目的
Step 10	ipv6 pim allow-rp route-map-name 例: <pre>switch(config-route-map)# ipv6 pim allow-rp test-route-map</pre>	IPv6 PIM Allow RP を有効にします。
Step 11	(任意) show ip pim policy statistics allow-rp-policy show ipv6 pim policy statistics allow-rp-policy 例: <pre>switch(config)# show ip pim policy statistics allow-rp-policy</pre>	ポリシー統計を表示するには、次の手順に従います。
Step 12	end 例: <pre>Switch (config-route-map)# end</pre>	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
Step 1	Enable 例: <pre>switch# enable</pre>	特権 EXEC モードを有効にします。
Step 2	show ip pim policy statistics allow-rp-policy 例: <pre>switch# show ip pim policy statistics allow-rp-policy</pre>	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。
Step 3	show ipv6 pim policy statistics allow-rp-policy 例: <pre>switch# show ipv6 pim policy statistics allow-rp-policy</pre>	現在の許可 RP ポリシーに関する IPv6 統計を表示します。
Step 4	clear ip pim policy statistics allow-rp-policy 例: <pre>switch# clear ip pim policy statistics allow-rp-policy</pre>	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
Step 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。

■ 許可 RP ポリシーに関する情報の表示

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。