



セグメントルーティングパス計算要素の設定

セグメントルーティングパス計算要素（SR-PCE）は、既存の IOS-XR PCEP 機能に追加機能を拡張してステートフル PCE 機能を提供します。SR-PCE は、MPLS データプレーンと IPv4 コントロールプレーンでサポートされています。



(注) SR-PCE をインストールするには、Cisco IOS XRv 9000 ルータのインスタンスをインストールする必要があります。詳細については、『[Cisco IOS XRv 9000 Router Installation and Configuration Guide](#)』を参照してください。

- [SR-PCE について](#) (1 ページ)
- [SR-PCE の設定](#) (2 ページ)
- [トラフィック管理の PCE 開始 SR ポリシー](#) (6 ページ)
- [PCEP 接続の ACL サポート](#) (7 ページ)

SR-PCE について

パス計算要素プロトコル（PCEP）は、パス計算クライアント（PCC）が PCC を起点とするヘッドエンドラベルスイッチドパス（LSP）の制御を PCE ピアに報告し委任できる一連の手順を記述しています。PCE は、PCC が制御している LSP のパラメータの更新と変更を PCC に要求することができます。また、ステートフルモデルでは、PCC は PCE が計算を開始することを許可でき、PCE はネットワーク全体のオーケストレーションを実行できます。

SR-PCE は、IGP（OSPF または IS-IS）または BGP リンクステート（BGP-LS）経由でトポロジ情報を学習します。

SR-PCE は、以下の方法を使用してパスを計算できます。

- TE メトリック：SR-PCE は TE メトリックを使用してパス計算を行い、累積 TE メトリックを最適化します。

- IGP メトリック：SR-PCE は IGP メトリックを使用してパス計算を行い、到達可能性を最適化します。
- LSP ディスジョイントネス：SR-PCE はパス計算アルゴリズムを使用して、ディスジョイント LSP のペアを計算します。ディスジョイントパスの起点は、同じヘッドエンドまたは異なるヘッドエンドです。ディスジョイントレベルとは、2つの計算されたパスで共有すべきではないリソースのタイプを指します。SR-PCE は、次のディスジョイントパス計算をサポートしています。
 - リンク：リンクが計算されたパスで共有されないことを指定します。
 - ノード：ノードが計算されたパス上で共有されないことを指定します。
 - SRLG：同じ SRLG 値を持つリンクが計算されたパスで共有されないことを指定します。
 - SRLG ノード：SRLG とノードが計算されたパス上で共有されないことを指定します。

所定のディスジョイントグループ ID で最初の要求が受信されると、最初の LSP が計算され、最初の送信元から最初の宛先への最短パスがエンコードされます。2つ目の LSP 要求が同じディスジョイントグループ ID で受信されると、両方の要求で受信された情報を使用して2つのディスジョイントパス（1つは最初の送信元から最初の宛先へのパス、もう1つは2つ目の送信元から2つ目の宛先へのパス）が計算されます。両方のパスが同時に計算されます。

SR-PCE の設定

このタスクでは、SR-PCE を設定する方法について説明します。

始める前に

必要に応じて、Cisco IOS XRv 9000 ルータのインスタンスをインストールして設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure	
ステップ 2	pce 例： RP/0/RP0/cpu 0: router(config)# pce	PCE を有効にし、PCE 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	address ipv4 address 例：	PCE IPv4 アドレスを設定します。

	コマンドまたはアクション	目的
	RP/0/RP0/cpu 0: router(config-pce)# address ipv4 192.168.0.1	
ステップ 4	state-sync ipv4 address 例 : RP/0/RP0/cpu 0: router(config-pce)# state-sync ipv4 192.168.0.3	リモートピアに状態同期を設定します。
ステップ 5	tcp-buffer size 例 : RP/0/RP0/cpu 0: router(config-pce)# tcp-buffer 1024000	各 PCEP セッションの送受信 TCP バッファサイズをバイト単位で設定します。デフォルトのバッファサイズは 256000 です。有効な範囲は 204800 ~ 1024000 です。
ステップ 6	password {clear encrypted} password 例 : RP/0/RP0/cpu 0: router(config-pce)# password encrypted pwd1	すべての PCEP ピアの TCP 認証を有効にします。設定されたパスワードと一致する MAC を含まない PCC から来る TCP セグメントはすべて拒否されます。パスワードが暗号化されているか、またはクリアテキストであるかを指定します。
ステップ 7	segment-routing {strict-sid-only te-latency} 例 : RP/0/RP0/cpu 0: router(config-pce)# segment-routing strict-sid-only	厳格な SID または TE のレイテンシを使用するようにセグメントルーティングアルゴリズムを設定します。 (注) この設定はグローバルで、このコントローラからパスを要求するすべての LSP に適用されます。
ステップ 8	timers 例 : RP/0/RP0/cpu 0: router(config-pce)# timers	タイマーコンフィギュレーションモードを開始します。
ステップ 9	keepalive time 例 : RP/0/RP0/cpu 0: router(config-pce-timers)# keepalive 60	ローカルで生成されたキープアライブメッセージのタイマー値を設定します。デフォルトの時間は 30 秒です。

	コマンドまたはアクション	目的
ステップ 10	minimum-peer-keepalive time 例 : <pre>RP/0/RP0/cpu 0: router(config-pce-timers)# minimum-peer-keepalive 30</pre>	セッション確立中にリモートピアが PCEOPEN メッセージで提案できる最小の許容キープアライブタイマーを設定します。デフォルトの時間は20秒です。
ステップ 11	reoptimization time 例 : <pre>RP/0/RP0/cpu 0: router(config-pce-timers)# reoptimization 30</pre>	再最適化タイマーを設定します。デフォルトタイマーは60秒です。
ステップ 12	exit 例 : <pre>RP/0/RP0/cpu 0: router(config-pce-timers)# exit</pre>	タイマーコンフィギュレーションモードを終了し、PCE コンフィギュレーションモードに戻ります。

ディスジョイントポリシーの設定 (オプション)

次のタスクでは、PCEP 要求に PCEP 関連グループ ID オブジェクトを含まない PCC によってシグナリングされた LSP のペアのディスジョイントネスを計算するように SR-PCE を設定する方法について説明します。これは、PCC がこの PCEP オブジェクトをサポートしていない場合、またはネットワークオペレータが LSP ディスジョイント設定を一元管理する場合の展開に便利です。

手順

	コマンドまたはアクション	目的
ステップ 1	disjoint-path 例 : <pre>RP/0/RP0/cpu 0: router(config-pce)# disjoint-path</pre>	ディスジョイント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	group-id value type {link node srlg srlg-node} [sub-id value] 例 : <pre>RP/0/RP0/cpu 0:</pre>	ディスジョイントグループ ID を設定し、ディスジョイントネスの優先レベル (2つのパスで共有されるべきでないリソースのタイプ) を定義します。

	コマンドまたはアクション	目的
	<pre>router(config-pce-disjoint) # group-id 1 type node sub-id 1</pre>	<ul style="list-style-type: none"> • link : リンクが計算されたパス上で共有されないことを指定します。 • node : ノードが計算されたパス上で共有されないことを指定します。 • srlg : 同じ SRLG 値を持つリンクが計算されたパスで共有されないことを指定します。 • srlg-node : SRLG とノードが計算されたパス上で共有されないことを指定します。 <p>要求されたディスジョイントネス レベルを満たすパスのペアが見つからない場合、パスは自動的に下位レベルにフォールバックされます。</p> <ul style="list-style-type: none"> • 要求されたディスジョイントネス レベルが SRLG またはノードの場合、リンクディスジョイントパスが計算されます。 • 要求されたディスジョイントネス レベルがリンクの場合、または SRLG またはノードのディスジョイントネスからの最初のフォールバックが失敗した場合は、2つの最短パスをエンコードするセグメントのリストが、ディスジョイントネスの制約なしで計算されます。
ステップ 3	<p>strict</p> <p>例 :</p> <pre>RP/0/RP0/cpu 0: router(config-pce-disjoint) # strict</pre>	<p>(任意) 優先レベルのディスジョイントネスの自動フォールバック動作を防止します。要求されたディスジョイントネスレベルを満たすパスのペアが見つからない場合、ディスジョイントの計算は終了し、新しいパスは提供されません。既存のパスは変更されません。</p>
ステップ 4	<p>lsp {1 2} pcc ipv4 address lsp-name lsp_name [shortest-path]</p> <p>例 :</p> <pre>RP/0/RP0/cpu 0:</pre>	<p>ディスジョイント グループに LSP を追加します。</p> <p>shortest-path キーワードは、ディスジョイントパスの1つに、送信元から宛先までの最短パスに従うよう強制します。</p>

	コマンドまたはアクション	目的
	<pre>router(config-pce-disjoint)# lsp 1 pcc ipv4 192.168.0.1 lsp-name rtrA_t1 shortest-path RP/0/RP0/cpu 0: router(config-pce-disjoint)# lsp 2 pcc ipv4 192.168.0.5 lsp-name rtrE_t2</pre>	このオプションは、指定された最初の LSP にのみ適用できます。

トラフィック管理の PCE 開始 SR ポリシー

SR-TE ポリシーは、リンクの輻輳を軽減したり、ネットワーク タッチ ポイントの数を最小限に抑えたりするようにパス計算要素 (PCE) で設定することができます。



(注) PCE 開始 SR-TE ポリシーは PCE コンフィギュレーション モードで入力されます。SR-TE ポリシーの設定に関する詳細については、[SR-TE ポリシーの概要](#)を参照してください。

PCE は、トラフィック需要やリンク使用率などのネットワーク情報を収集します。PCE はリンクが輻輳していると判断すると、輻輳の原因となっている 1 つ以上のフローを特定します。PCE は適切なパスを見つけ、ネットワークの別の部分に輻輳を移動せずに、そのフローを転送するように SR-TE ポリシーを展開します。リンクの輻輳がない場合、ポリシーは削除されます。

ネットワーク タッチ ポイントの数を最小限に抑えるために、ネットワーク サービス オーケストレータ (NSO) などのアプリケーションは PCE に SR-TE ポリシーを作成するように要求できます。PCE は、PCC-PCE 通信プロトコル (PCEP) を使用して SR-TE ポリシーを展開します。

1. PCE は PCInitiate メッセージを PCC に送信します。
2. PCInitiate メッセージが有効な場合、PCC は PCRpt メッセージを送信します。それ以外の場合は、PCErr メッセージが送信されます。
3. PCInitiate メッセージが受け入れられると、PCE は PCUpd メッセージを送信して SR-TE ポリシーを更新します。

SR-TE ポリシーを使用して複数の PCE を設定すると、ハイアベイラビリティを実現できます。ヘッドエンド (PCC) が 1 つの PCE との接続を失った場合、別の PCE が SR-TE ポリシーの制御を引き継ぐことになります。

設定例

PCE 開始 SR-TE ポリシーを設定するには、次の設定を完了する必要があります。

1. PCE コンフィギュレーション モードを開始します。
2. セグメント リストを作成します。

3. ポリシーを作成します。

```
/* Enter PCE configuration mode and create the SR-TE segment lists */
Router# configure
Router(config)# pce

/* Create the SR-TE segment lists */
Router(config-pce)# segment-routing
Router(config-pce-sr)# traffic-eng
Router(config-pce-sr-te)# segment-list name addr2a
Router(config-pce-sr-te-sl)# index 1 address ipv4 14.14.14.4
Router(config-pce-sr-te-sl)# exit

/* Create the SR-TE policy */
Router(config-pce-sr-te)# peer ipv4 1.1.1.1
Router(config-pce-sr-te)# policy P1
Router(config-pce-sr-te-policy)# color 2 end-point ipv4 2.2.2.2
Router(config-pce-sr-te-policy)# candidate-paths
Router(config-pce-sr-te-policy-path)# preference 50
Router(config-pce-sr-te-pp-index)# explicit segment-list addr2a
Router(config-pce-sr-te-pp-info)# end
Router(config)#
```

ランニング コンフィギュレーション

```
pce
segment-routing
traffic-eng
segment-list name addr2a
index 1 address ipv4 14.14.14.4
!
peer ipv4 1.1.1.1
policy P1
color 2 end-point ipv4 2.2.2.2
candidate-paths
preference 50
explicit segment-list addr2a
!
!
```

PCEP 接続の ACL サポート

PCE プロトコル (PCEP) (RFC5440) は TCP/IP を介して実行されているクライアントサーバモデルであり、サーバ (PCE) がポートをオープンし、クライアント (PCC) が接続を開始します。ピアが TCP 接続を確立すると、その接続上で PCE セッションを作成します。

PCEP 接続の ACL サポート機能は、アクセス コントロール リスト (ACL) を使用して PCE サーバを保護し、クライアントの送信元アドレスに基づいて TCP 接続が作成されたときに IPv4 PCC ピアを制限する方法を提供します。クライアントが TCP 接続を開始すると、ACL が参照され、クライアントの送信元アドレスが比較されます。ACL はアドレスを許可または拒否し、TCP 接続を続行するかどうかを選択できます。

ACL 設定情報については、『*IP Addresses and Services Configuration Guide for*』の「」の章を参照してください。

ACL を PCE に適用するには、**pce peer-filter ipv4 access-list** *acl_name* コマンドを使用します。